NSG Series Firewalls CLI Reference Guide

Models: NSG-3100; NSG-5100; NSG-8100

CLI REFERENCE GUIDE

Contents

Command Line Interface

Overview

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

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

CLI Modes and Prompts

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

Execution Mode

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

```
hostname#
```

Global Configuration Mode

Commands in the global configuration mode are used to change device settings. To enter the global configuration mode, in the execution mode, use the command configuration. The global configuration mode prompt is shown as follows:

```
hostname(config)#
```

Sub-module Configuration Mode

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

```
hostname(config-if-eth0/0)#
```

Switching between CLI Modes

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

Mode	Command

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

CLI Error Message

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

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

Command Input

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

Command Short Form

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

Listing Available Commands

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

- If you type a question mark (?) behind an incomplete command, the system gives available commands (with short description) started with the last typed letter.

- If you type a question mark (?) at any level, the system displays a list of the available commands along with a short description of each command.

Completing Partial Commands

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

Using CLI

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

Previous Commands

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

Shortcut Keys

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

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

Shortcut Key	Action
META-B	Moves cursor to the beginning of the word.
META-D	Deletes the word after the cursor.
META-F	Moves cursor to the end of the word.
META-Backspace	Deletes the word before the cursor.
META-Ctrl-H	Deletes the word before the cursor.

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

Filtering Output of Show Commands

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

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

CLI output filter syntax is shown as follows:

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

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

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

Regular Expression	Meaning
. (period)	Represents any character.
* (star)	Indicates that there is zero or more of the preceding element.
+ (plus)	Indicates that there is one or more of the preceding element.
^ (caret)	Used at the beginning of an expression, denotes where a match should begin.

Regular Expression	Meaning
$ (dollar)	Used at the end of an expression, denotes that a term must be matched exactly up to the point of the $ character.
_(underscore)	Represents “,” , “{” , “}” , “(” , “)” , beginning of a line, end of a line or space.
[] (square bracket)	Matches a single character that is contained within the brackets.
- (hyphen)	Separates the start and the end of a range.

CLI Page Display

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

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

Specifying Screen Size

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

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

- Width: **terminal width** *character-number*
  character-number – Specifies the number of characters. The value range is 64 to 512.
- Length: **terminal length** *line-number*
  line-number – Specifies the number of lines. CLI displays message lines one line less than the value specified here, but if the value is 1, the screen shows one line. The value range is 0 to 256. Setting the length to 0 disables page display option, which means it displays all messages without page split.

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

Specifying Connection Timeout

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

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

console timeout *timeout-value*

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

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

ssh timeout*timeout-value*

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

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

telnet timeout *timeout-value*

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

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

Redirecting the Output of Show Commands

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

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

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

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

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

Diagnostic Commands

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

Chapter 1 Firewall

The chapter introduces the following topics:

- Configuration Environment describes how to access a device via Console port, Telnet, SSH and WebUI.
- Application Mode describes three types of application modes: transparent mode, mix mode, and routing mode.
- Deployment Mode describes three types of deployment modes: inline mode, bypass mode, and mix mode.
- FSOS Architeture describes the basic components of FSOS: interface, zone, VSwitch, VRouter, policy rule, and VPN.
- Zone describes the zone. Zones divide network into multiple segments, for example, trust, untrust, and so on. You can apply proper policy rules to zones to make the devices control the traffic transmission among zones.
- Interface describes the interface. Interfaces are used to connect devices, and transmit data.
- Address describes the address book. The address book contains address information, and can be used by multiple modules, such as policy rules, NAT rules, QoS, session limit rules, etc.
- Service and Application describes the service book and application book. All of these applications and applications groups are stored in and managed by application book. All these service and service groups are stored in and managed by service book.
- DNS describes the function of Domain Name System. It is designed for TCP/IP network to look for Internet domain names (e.g., www.xxxx.com) and translate them into IP addresses (e.g., 10.1.1.1) to locate related computers and services.
- DDNS describes the function of Dynamic Domain Name Server. It is designed to resolve fixed domain names to dynamic IP addresses.
- DHCP describes the function of Dynamic Host Configuration Protocol. It is designed to allocate appropriate IP addresses and related network parameters for subnets.
- PPPoE describes the function of Point-to-Point Protocol over Ethernet. It combines PPP protocol and Ethernet to implement access control, authentication and accounting on clients during IP address allocation.

- NAT describes the protocol for IP address translation in an IP packet header. When the IP packets pass through a firewall or router, the device or router will translate the source IP address and/or the destination IP address in the IP packets.
- Application Layer Identification and Control describes the function of Application Layer Gate. It can assure the data transmission for the applications that use multiple channels and assure the proper operation of VoIP applications in the strictest NAT mode.
- RSTP describes the function of Rapid Spanning Tree Protocol. It is designed to block the redundant links to avoid broadcast storm.

Configuration Environment

Overview

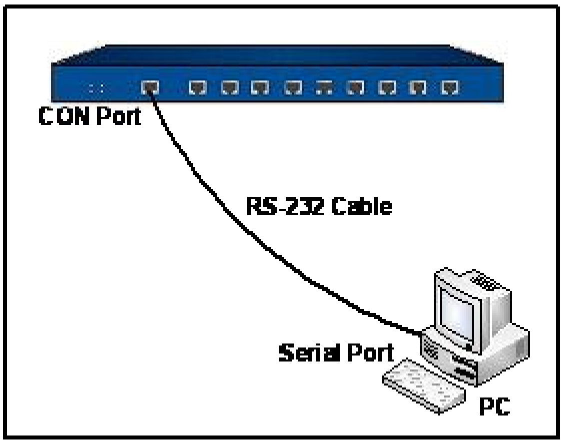
When the device has been properly installed, you need to set up an initial configuration environment before enabling the device to forward traffic. Use the following methods to set up configuration environment:

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

Accessing a Device via Console Port

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

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



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

Parameter	Value
Baud	9600 bit/s
Data	8
Parity	None
Stop	1
Flow Control	None

3. Power on the device and FSOS starts up. Type the default login name (admin) and password (admin), and press Enter to log in.

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

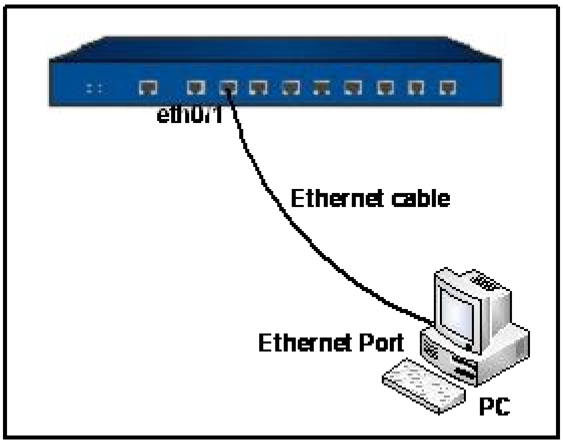
Accessing a Device via Telnet

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

- An IP address has been assigned to the access port with Telnet service enabled. (To enable Telnet on an interface, in the interface configuration mode, use the command **manage telnet**.)
- There is a correct route between the computer and the device.

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

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



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

3. Run a Telnet client program in your computer.

4. Type telnet and the IP address. If the connection is successfully established, the Telnet window shows "login". Type the default login name (admin) and password (admin), and press Enter to log in.

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

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

Accessing a Device over SSH

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

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

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

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

3. Run a SSH client software in your computer. You need to configure some SSH parameters, including IP address of the device, SSH version and RSA key, etc.

4. If the connection is successfully established, a login: prompt will appear. Enter the default administrator username "admin" and press Enter. Behind the prompt for password, enter the default password "admin" and press Enter to log in.

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

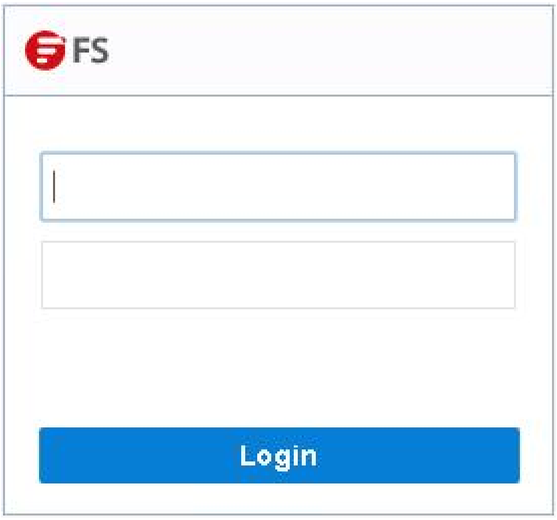
Accessing a Device via WebUI

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

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

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

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



3. Type the default username (admin) and password (admin) into the boxes respectively.

4. To select a system language, click the corresponding language on the upper-right.

5. Click **Login** to enter FSOS home page.

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

Logging in by Using Certificate Authentication

To improve the security, you can log into the device by using certificate 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. Two-factor authentication is not only needing the user name and password authentication, but also needing other authentication methods, such as certificate or fingerprint. After enabling this authentication method and logging into the device over HTTPS, you need to first select certificate and then enter the password.

Note:

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

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

Configuring the Device Side

To configure the device side, take the following steps:

1. To enable certificate authentication mode:
   In the global configuration mode, execute the **https client-auth enable**command.

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

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

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

   c. In the global configuration mode, execute the **https client-auth trust-domain** *trust-domain-name* command to specify the trust domain of certificate authentication. The trust domain is the one that you create in the above steps.

3. If needed, you can configure to check that if the entered username matches the CN value of the CA certificate or not. When the two names match, the user can log into the device successfully.
   In the global configuration mode, execute the **https client-auth match cn**command. This function is enabled by default.

Configuring the Client Side

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

1. Import the digital certificate to the client Web browser.

   a. In the Web browser, for example, Internet Explorer, select **Tools > Internet options > Content > Certificate > Personal**.

   b. Click **Import**.

   c. In the pop-up window, follow the wizard to import the certificate.

2. In the PC, launch a Web browser and visit the address https://IP-Address(IP-Address refers to the IP address of manageable interface).

3. A dialog appears and asks you to select the proper certificate from the certificate list.
4. Click **OK**. The login page appears.
5. Enter the username and password and click Login. If you have configured the https client-auth match cn command, the username you entered must be the same as the CN value of the CA certificate.

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

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

Application Mode

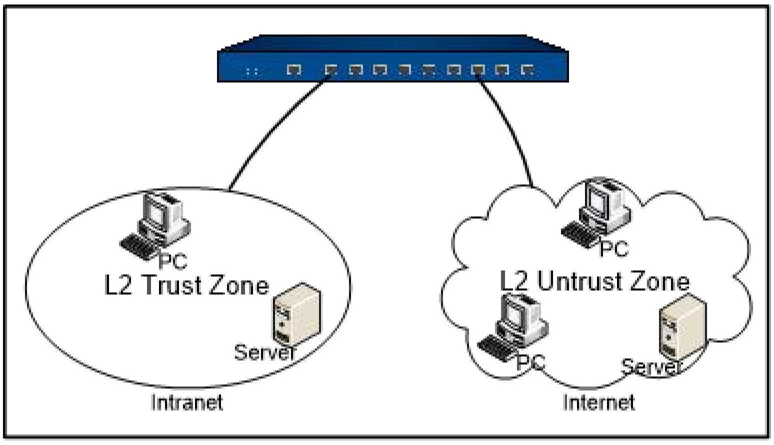
Overview

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

Transparent Mode

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

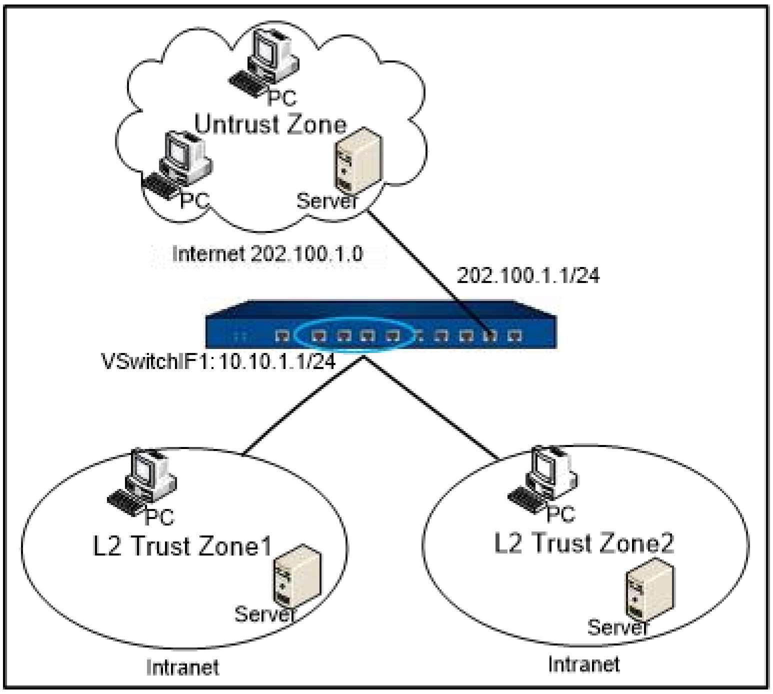
- Do not have to change the IP addresses of the protected network.
- No NAT rules are needed.



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

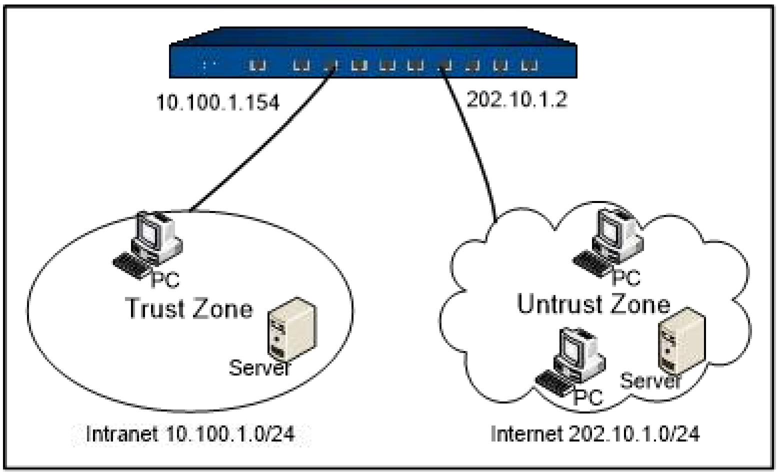
Mix Mode

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



Routing Mode

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



VSwitch

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

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

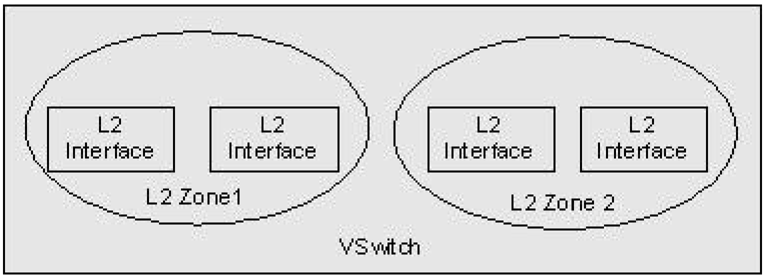
> Tip: For more information about VSwitch configuration, see Interface.

Basic Concepts

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

L2 Zones

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



L2 Interfaces

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

Forwarding Rules in VSwitch

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

The forwarding rules for IP packets are:

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

   If no egress interfaces (unknown unicast) is found in the MAC address table, jump to Step 6 directly.
4. Figure out the source zone and destination zone according to the ingress and egress interfaces.
5. Look up the policy rules and forward or drop the packet according to the matched policy rules.

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

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

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

```
l2-nonip-action {drop | forward}
```

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

Configuring a VSwitch

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

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

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

vswitch vswitch*Number*

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

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

no vswitch vswitch*Number*

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

show vswitch [*vswitch-name*]

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

Viewing MAC Table Information

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

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

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

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

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

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

Virtual Wire

FS devices support VSwitch-based Virtual Wire. With this function enabled and Virtual Wire interface pair configured, two Virtual Wire interfaces form a virtual wire that connects the two sub-networks attaching to Virtual Wire interface pair together. The two connected sub-networks can communicate directly on Layer 2, without 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 the mix mode. Any PC connected to the Virtual Wire interface can neither manage the device nor access Internet over this interface.
- Non-Strict Virtual Wire mode: Packets can be transmitted between Virtual Wire interfaces, and the VSwitch also supports data forwarding in Mix mode. That is, this mode only restricts Layer 2 packets' transmission between Virtual Wire interfaces, and does not affect Layer 3 packets' forwarding.

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

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

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

Configuring a Virtual Wire

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

Enabling Virtual Wire

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

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

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

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

```
no virtual-wire enable
```

Configuring a Virtual Wire Interface Pair

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

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

```
virtual-wire set interface-name1 interface-name2
```

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

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

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

Viewing Virtual Wire Configuration Information

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

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

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

VLAN Transparent in the Transparent Mode

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

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

```
forward-tagged-packet
```

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

```
no forward-tagged-packet
```

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

```
forward-double-tagged-packet
```

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

```
no forward-double-tagged-packet
```

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

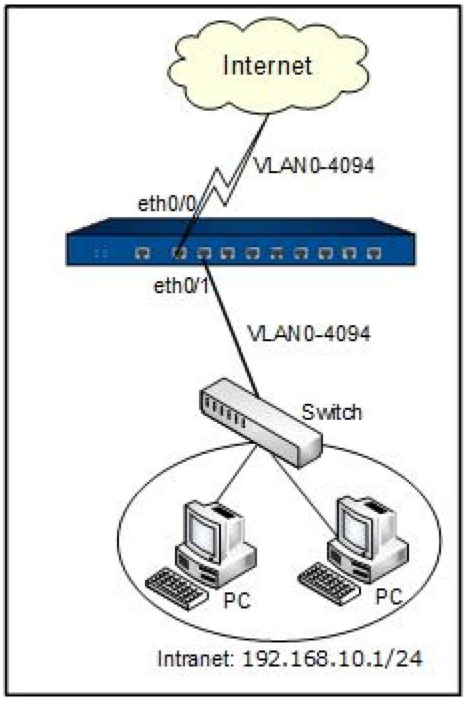
- VSwitch that contains sub-interfaces cannot enable VLAN transparent.
- The L2 zone in the VSwitch with VLAN transparent enabled cannot bind sub-interfaces.

- Transparently transmitted VLAN tagged packets cannot be transmitted in Layer 3.

Configuration Example

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

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



Configuration Steps

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

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

hostname(config-if-eth0/0)# exit

hostname(config)#
```

Step 2: Create VSwitch2 for the VLAN packets tagged 2

```
hostname(config)# vswitch vswitch2

hostname(config-vswitch)# exit

hostname(config)# zone l2-trust2 l2

hostname(config-zone-l2-tru~)# bind vswitch2

hostname(config-zone-l2-tru~)# exit

hostname(config)# zone l2-untrust2 l2

hostname(config-zone-l2-tru~)# bind vswitch2

hostname(config-zone-l2-tru~)# exit

hostname(config)# interface ethernet0/0.2

hostname(config-if-eth0/0.2)# zone l2-untrust2

hostname(config-if-eth0/0.2)# exit

hostname(config)#
```

Step 3: Configure the policy rules

```
hostname(config)# address address1

hostname(config-addr)# ip 192.168.10.1/24

hostname(config-addr)# exit

hostname(config)# policy-global

hostname(config-policy)# rule from address1 to any from-zone l2-trust2 to-zone l2-untrust2
service any permit

hostname(config)# rule id 2

hostname(config-policy-rule)# src-zone l2-trust2

hostname(config-policy-rule)# dst-zone l2-untrust2

hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config-policy)# rule from any to any from-zone l2-trust to-zone l2-untrust service any
permit
Rule id 3 is created
hostname(config-policy)# exit
hostname(config)#
```

Configuring Transparent ARP

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

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

Configuring a VRouter

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

Enabling and Disabling Mult-VR

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

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

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

After multi-VR is enabled or disabled, the system must reboot to make it take effect. After rebooting, the 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-VR 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-VR is enabled, traffic can traverse up to 3 VRs, and any traffic that has to traverse more than 3 VRs will be dropped.

Creating a VRouter

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

```
ip vrouter vrouter-name
```

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

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

```
no ip vrouter vr-name
```

Viewing VRouter Information

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

```
show ip vrouter [vrouter-name]
```

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

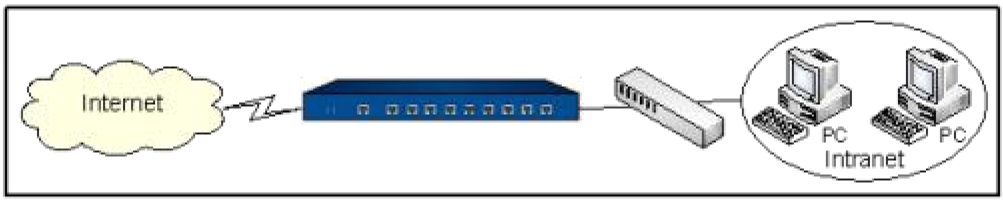
Deployment Mode

Overview

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

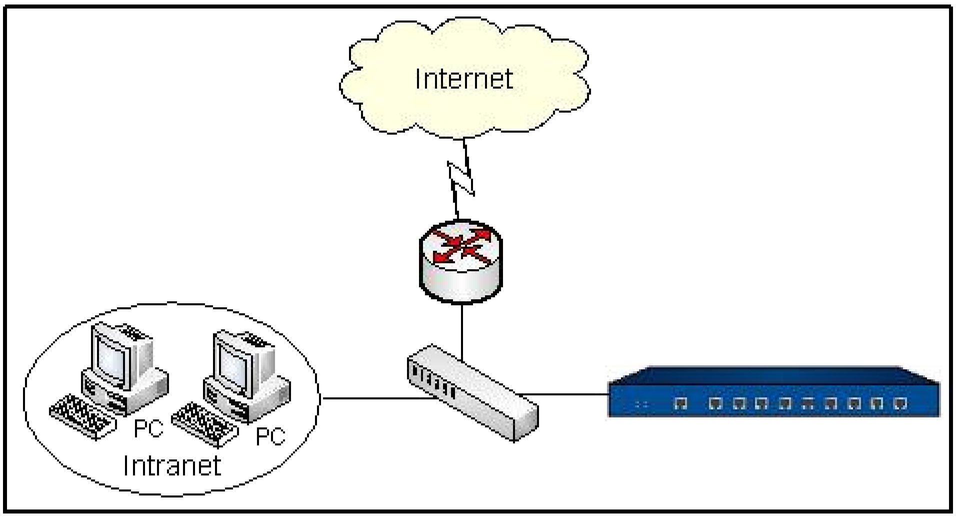
Inline Mode

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



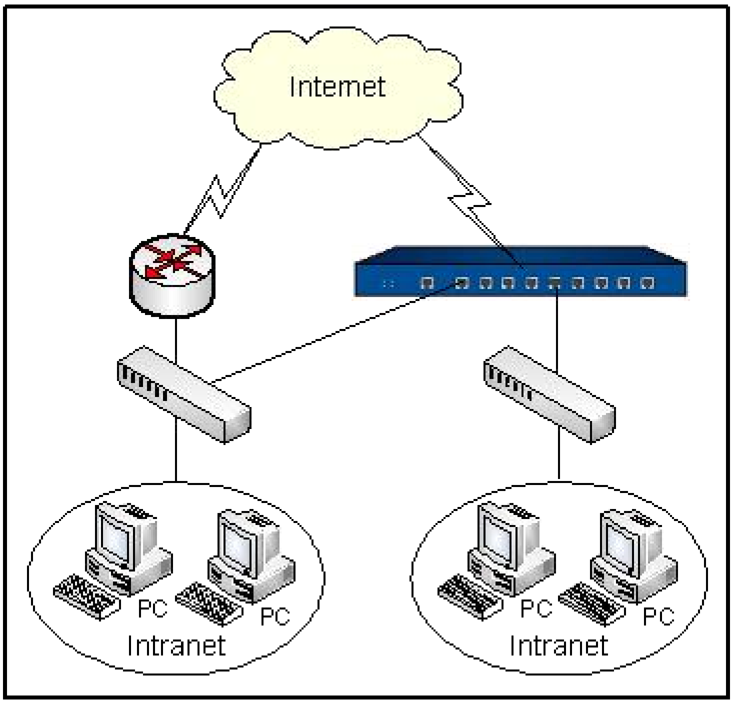
Bypass Mode

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



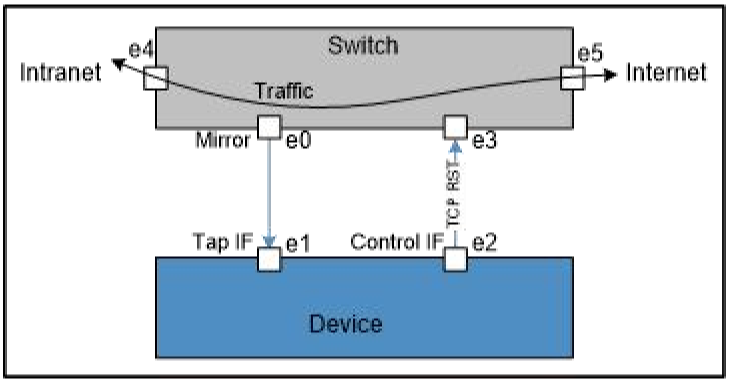
Mix Mode

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



Working Principle of Bypass Mode

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



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

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

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

Configuring Bypass Mode

Configurations of bypass mode include:

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

Creating a Tap Zone

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

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

zone *zone-name* tap

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

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

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

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

no zone zone-name.

Binding an Interface to a Tap Zone

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

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

zone *zone-name*

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

Configuring a Bypass Control Interface

A bypass control interface is used to send control packets (TCP RST packet is supported in current version). After configuring IPS, AV, or network behavior control on the FS device, if the device detects network intrusions, virus, or illegal network behaviors, it will send TCP RST packet from e2 to the switch to tell it to reset the connections. By default, the bypass control interface is the bypass interface itself.

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

tap control-interface *interface-name*

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

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

Specifying a Statistical Range

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

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

tap lan-address *address-entry*

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

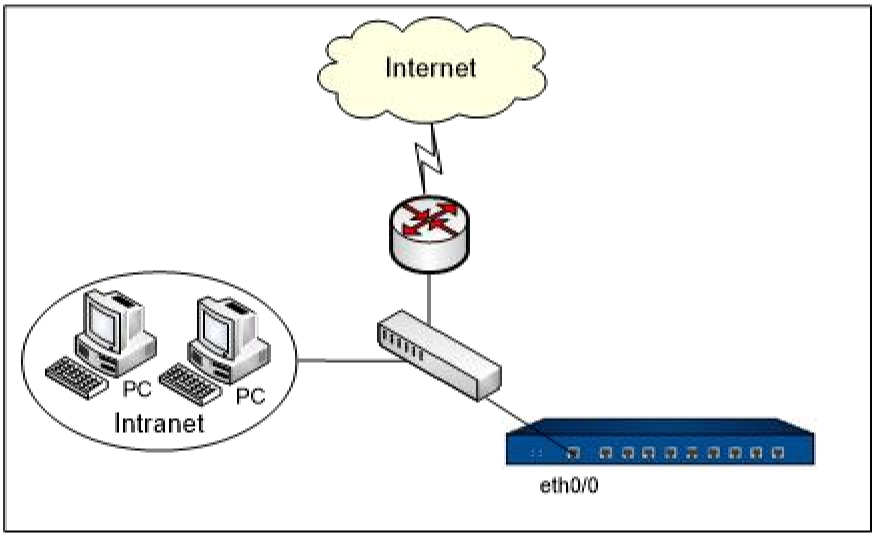
To cancel the specified statistical range, in the bypass interface configuration mode, use the command **no tap lan-address**.

Example of Configuring Bypass Mode

This section describes a bypass mode configuration example.

Topology

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



Configuration Steps

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

```
hostname(config)# zone tap1 tap
hostname(config-zone-tap1)# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone tap1
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Because etherent0/0 is configured as the bypass interface, it also is the default bypass control interface

Step 2: Bind the IPS profile to the Tap zone

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

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

FSOS Architecture

Overview

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

Interfaces

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

Tip: For more information about interfaces, see Interface.

Zones

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

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

VSwitches

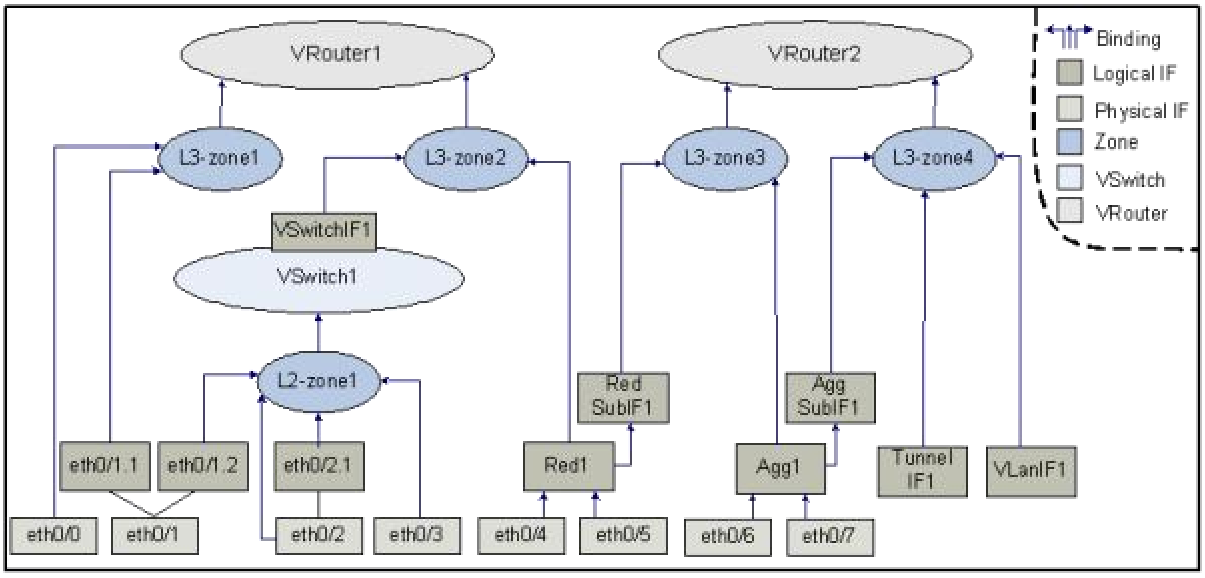
VSwitch is short for Virtual Switch. A VSwitch functions as a switch in Layer 2. After binding a Layer 2 zone to a VSwitch, all the interfaces in the zone are also bound to the VSwitch. There is a default VSwitch named VSwitch1. By default, all Layer 2 zones will be bound to VSwitch1. You can create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

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

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

VRouter

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



As shown above, the binding relationships among them are:

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

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

Policy

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

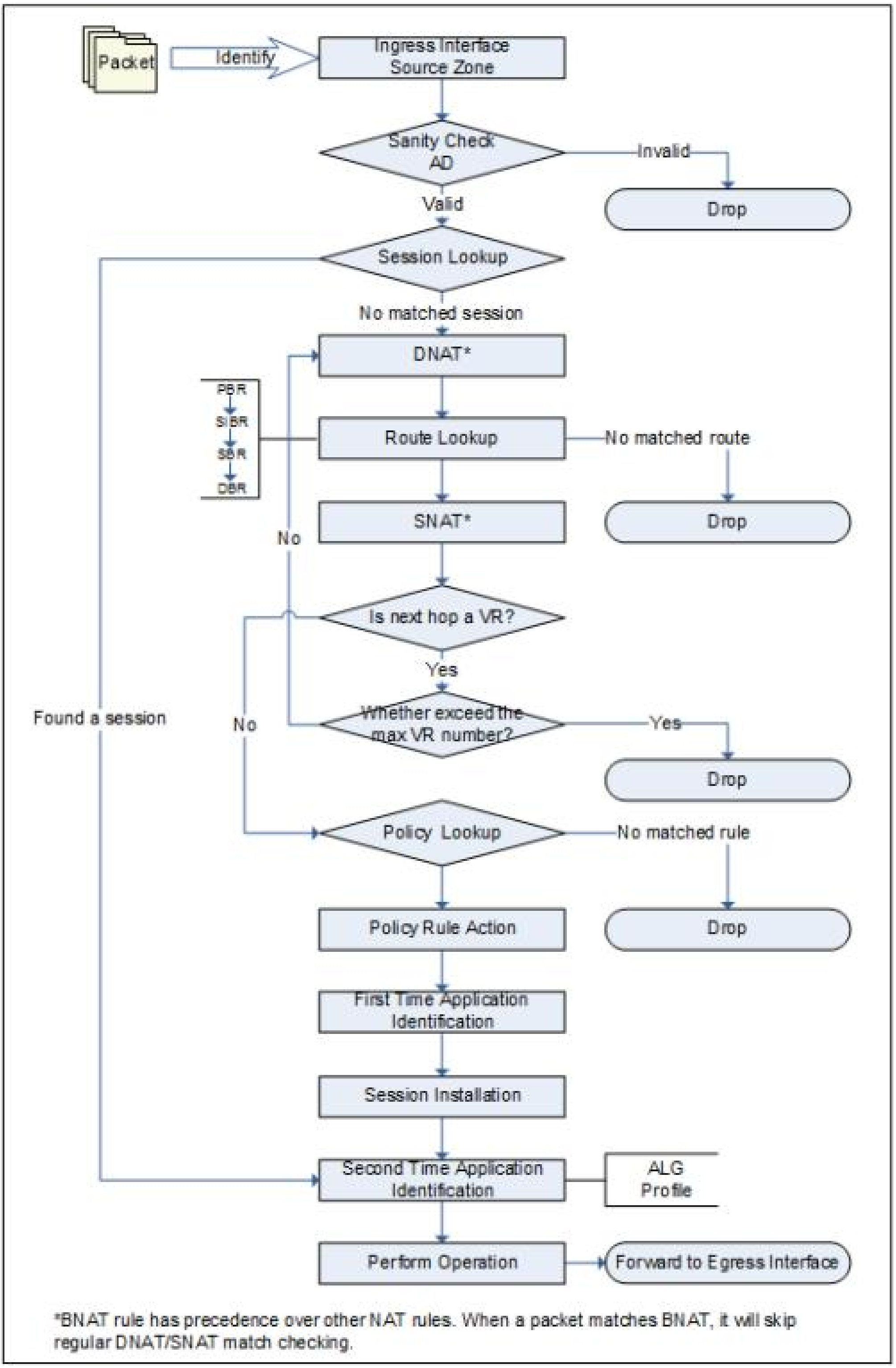
VPN

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

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

Packet Handling Process

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


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

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

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

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

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

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

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

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

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

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

9. First time application identification. The system tries to identify the type of the application according to the port number and service specified in the policy rule.

10. Establish the session.

11. If necessary, the system will perform the second time application identification. It is a precise identification based on the packet contents and traffic action.

12. Application behavior control. After knowing the type of the application, the system will deal with the packet according to the configured profiles and ALG.

13. Perform operations according to the records in the session, for example, the NAT mark.

14. Forward the packet to the egress interface.

Deny Session

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

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

The system will create deny sessions in the following situations:

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

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

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

Configuring the Deny Session Function

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

Specifying the Deny Session Type

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

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

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

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

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

Specifying the Maximum Number of Deny Sessions

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

```
deny-session percentage number
```

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

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

```
no deny-session percentage
```

Specifying the Timeout Value

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

deny-session timeout *time*

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

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

no deny-session timeout

Viewing the Deny Session Configuration Information

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

show flow deny-session

Viewing the Deny Session Information

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

show session deny

TCP RST Packet Check

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

tcp-rst-bit-check

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

Global Network Parameters

To provide a better traffic transmission service, the device supports a set of global network parameters, including TCP MSS (Maximum Segment Size), TCP sequence number check, TCP three-way handshaking timeout check, TCP SYN packet check, and IP fragment options.

Configuring MSS

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

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

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

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

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

TCP Sequence Number Check

The TCP sequence number check function checks the TCP sequence number of the packet, and if the sequence number exceeds the TCP window, the system will drop the packet. This function is enabled by default. To configure the TCP sequence number check function, in the global configuration mode, use the following commands:

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

TCP Three-way Handshaking Timeout Check

The device can check the TCP three-way handshaking time, and if the three-way handshaking has not been completed after timeout, the connection will be reset. To configure this function, in the global configuration mode, use the following command:

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

- *timeout-value* – Specifies the timeout value. The value range is 1 to 1800 seconds. The default value is 20.

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

no tcp-syn-check

TCP Connection State Age-time

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

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

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

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

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

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

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

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

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

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

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

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

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

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

TCP SYN Packet Check

TCP SYN packet check: Select the Enable checkbox to enable this function, and only when a packet is a TCP SYN packet can a connection be established.

After TCP SYN packet check is enabled, only when a packet is a TCP SYN packet can a connection be established. This function is disabled by default. To configure this function, in the global configuration mode, use the following commands:

- Enable: **tcp-syn-bit-check**
- Disable: **no tcp-syn-bit-check**

IP Fragment

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

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

fragment chain *number*

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

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

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

fragment timeout *time*

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

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

Session Information

You can perform the following actions on the session information:

- Show session information
- Clear session information

Showing Session Information

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

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

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

show session [**id** *number* [*end-id*]] [**src-ip** *A.B.C.D* [*netmask*| *wildcard*]] [**dst-ip** *A.B.C.D* [*netmask* | *wildcard*]] [**protocol** *protocol-number*][**src-port** *port-number* [*port-number*]] [**dst-port** *port-number* [*port-number*]] [**application** *name*] [**policy** *policy-id*] [**vrouter** *vrouter-name*] [**vsys** *vsys-name*][**vsys** *vsys-name*] [**ipv4**] [**ipv6**] [**detail**] [{**flow0-interface** | **flow1-interface**} *interface-name*]

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

- **vrouter** *vrouter-name* – Shows the session information of the specified virtual router.
- **vsys** *vsys-name* – Shows the session information of the specified VSYS.
- **ipv4** – Shows the session information of the IPv4 protocol.
- **ipv6** – Shows the session information of the IPv6 protocol.
- **detail** – Shows the detail session information.
- {**flow0-interface** | **flow1-interface**} *interface-name* - Shows the session information of the ingress interface of the specified flow0 or flow 1.

Clearing Session Information

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

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

- **h323** – Clears the H323 session information.
- **id***number* [*end-id*] – Clears the session information of the specified ID. To show the session information of a specified range of IDs, continue entering the end ID of the range.
- **src-ip***A.B.C.D* – Clears the session information of the specified source IP address or specified range of IP addresses.
- **dst-ip***A.B.C.D* – Clears the session information of the specified destination IP address or specified range of IP addresses.
- *netmask* | *wildcard* – Clears the netmask or the wildcard mask.
- *protocol-number* – Clears the session information of the specified protocol number.
- **src-port***port-number* [*port-number*] – Clears the session information of the specified source port.
- **dst-port***port-number* [*port-number*] – Clears the session information of the specified destination port.
- **vrouter***vrouter-name* – Clears the session information of the specified virtual router.
- **vsys***vsys-name* – Clears the session information of the specified VSYS.
- **ipv4** – Clears the session information of the IPv4 protocool.
- **ipv6** – Clears the session information of the IPv6 protocol.

- detail – Clears the detail session information.

Zone

Overview

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

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

Predefined Security Zone

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

Configuring a Security Zone

You can perform the following operations to a security zone:

- Viewing the zone information
- Creating a zone
- Specifying the description
- Binding a Layer 2 zone to VSwitch
- Binding a Layer 3 zone to VRouter

Viewing the Zone Information

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

show zone [*zone-name*]

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

Creating a Zone

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

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

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

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

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

no zone *zone-name* [l2].

Note:The predefined zones cannot be deleted.

Specifying the Description

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

```
description description
```

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

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

Binding a Layer 3 Zone to a VRouter

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

```
vrouter vrouter-name
```

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

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

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

Binding a Layer 2 Zone to a VSwitch

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

bind *vswitch-name*

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

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

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

Configuration Example

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

```
hostname(config)# vswitch vswitch2

hostname(config-vswitch)# exit

hostname(config)# zone zone1 l2

hostname(config-zone-zone1)# bind vswitch2

hostname(config-zone-zone1)# exit

hostname(config)# interface ethernet0/2

hostname(config-if-eth0/2)# zone zone1

hostname(config-if-eth0/2)# exit

hostname(config)#
```

Interface

Overview

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

Interface Types

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

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

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

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

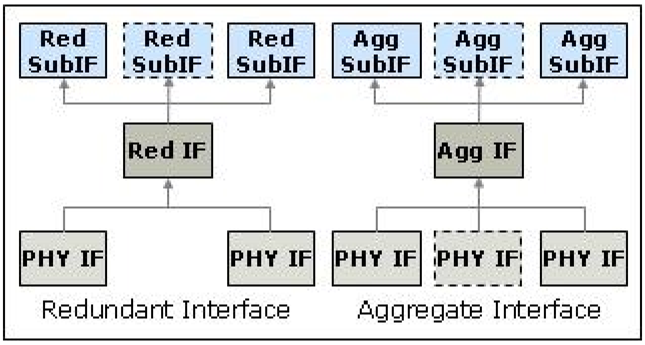
Different interface has different functions. Table below describes all logical interfaces.

Type	Description
Sub-interface	The naming rule of sub-interface is to add an extension number to the name of its source interface, e.g. ethernet0/2.1. FSOS supports the following types of sub-interface: Ethernet sub-interface, aggregate sub-interface, PPPoE sub-interface and redundant sub-interface. An Interface and its sub-interface can be bound to the same zone or to different zones.
VSwitch interface	VSwitch interface is Layer 3 interface. It is an assembled interface of all interfaces in VSwitch. The VSwitch interface is actually working as the upstream port of a switch, and it allows packets to be forwarded between Layer 2 and Layer 3.
Loopback interface	Loopback interface is a logical interface. As long as the device which the loopback interface belongs to is in the working status, the loopback interface is in the working status. Therefore, loopback interface is often stable.
Tunnel interface	Tunnel interface is the ingress port of VPN tunnel. Data flow accesses and

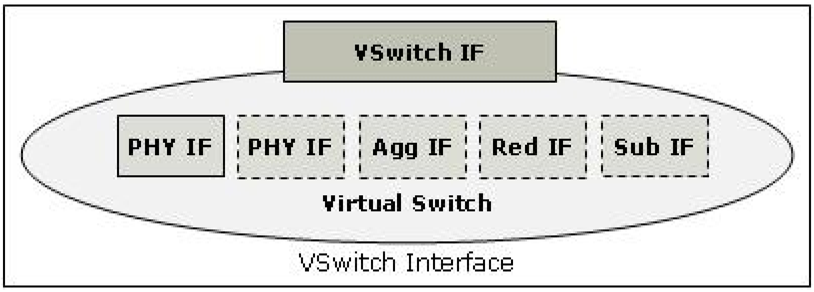
Type	Description
	leaves the VPN tunnel by going through the tunnel interface. Tunnel interface must be a Layer 3 interface.
Aggregate interface	An aggregate interface is an assembly of 1 to 16 physical interfaces. The physical interfaces equally share the data flow that passes the aggregate interface. Therefore, the aggregate interface can increase the available bandwidth for one IP address. If one of the physical interfaces malfunctions, other physical interfaces can carry on to process the data flow, only that the available bandwidth will become smaller.
Redundant interface	Redundant interface refers to the binding of two physical interfaces. A physical interface works as the master interface and processes the data flow, and the alternative interface stands by. The alternative interface will go on to process the data flow when the master interface fails to function.
PPPoE interface	A logical interface based on Ethernet interface that allows connection to PPPoE servers over PPPoE protocol.
Virtual forward interface	In HA environment, the Virtual forward interface is HA group's interface designed for traffic transmission.

Interface Dependency

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



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



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

Viewing Interface Information

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

Viewing All Interfaces

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

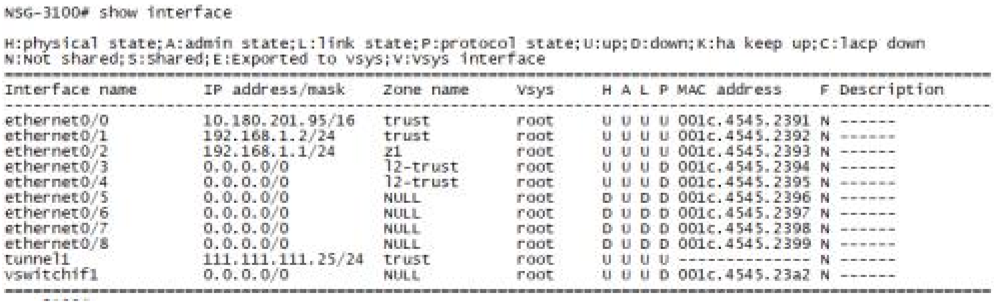
Item	Description
Interface name	Shows the name of interface.
IP address/mask	Shows the IP address of interface.
Zone name	Shows the bound zone of interface.
Vsys	Shows the VSYS name of interface.
H (Physical state)	Shows the physical availability state of interface (UP/DOWN).
A (Admin state)	Shows the administration availability state of the interface (UP/DOWN).
L (Link state)	Shows the link availability state of the interface.
P (Protocol state)	Shows the protocol availability state of the interface (UP/DOWN).
MAC address	Shows the interface MAC address.
Description	Shows the interface description.

The following description explains the meaning of H, A, L and P states:

- H (Physical state): the physical connectivity state of the interface. The UP state indicates that the interface is physically connected, while the DOWN state means otherwise.

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

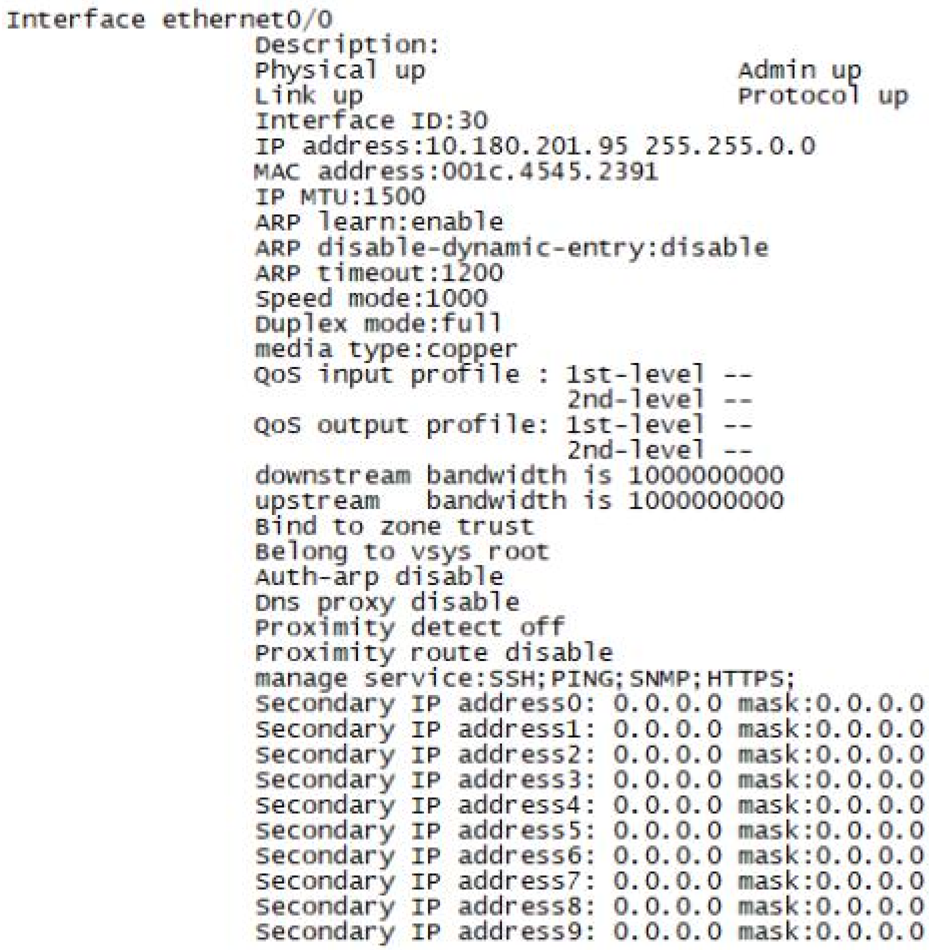
Here is an example of the show interface command:



```
NSG-3100# show interface

H:physical state;A:admin state;L:link state;P:protocol state;U:up;D:down;K:ha keep up;C:lacp down
N:Not shared;S:Shared;E:Exported to vsys;V:vsys interface
=====================================================================================================
Interface name       IP address/mask    Zone name     Vsys      H A L P MAC address     F Description
-----------------------------------------------------------------------------------------------------
ethernet0/0          10.180.201.95/16   trust         root      U U U U 001c.4545.2391 N ------
ethernet0/1          192.168.1.2/24     trust         root      U U U U 001c.4545.2392 N ------
ethernet0/2          192.168.1.1/24     z1            root      U U U U 001c.4545.2393 N ------
ethernet0/3          0.0.0.0/0          l2-trust      root      U U U D 001c.4545.2394 N ------
ethernet0/4          0.0.0.0/0          l2-trust      root      U U U D 001c.4545.2395 N ------
ethernet0/5          0.0.0.0/0          NULL          root      D U D D 001c.4545.2396 N ------
ethernet0/6          0.0.0.0/0          NULL          root      D U D D 001c.4545.2397 N ------
ethernet0/7          0.0.0.0/0          NULL          root      D U D D 001c.4545.2398 N ------
ethernet0/8          0.0.0.0/0          NULL          root      D U D D 001c.4545.2399 N ------
tunnel1              111.111.111.25/24  trust         root      U U U U -------------- N ------
vswitchif1           0.0.0.0/0          NULL          root      U U U D 001c.4545.23a2 N ------
=====================================================================================================
```

Viewing a Specific Interface

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



```
Interface ethernet0/0
                Description:
                Physical up                    Admin up
                Link up                        Protocol up
                Interface ID:30
                IP address:10.180.201.95 255.255.0.0
                MAC address:001c.4545.2391
                IP MTU:1500
                ARP learn:enable
                ARP disable-dynamic-entry:disable
                ARP timeout:1200
                Speed mode:1000
                Duplex mode:full
                media type:copper
                QoS input profile : 1st-level --
                                    2nd-level --
                QoS output profile: 1st-level --
                                    2nd-level --
                downstream bandwidth is 1000000000
                upstream   bandwidth is 1000000000
                Bind to zone trust
                Belong to vsys root
                Auth-arp disable
                Dns proxy disable
                Proximity detect off
                Proximity route disable
                manage service:SSH;PING;SNMP;HTTPS;
                Secondary IP address0: 0.0.0.0 mask:0.0.0.0
                Secondary IP address1: 0.0.0.0 mask:0.0.0.0
                Secondary IP address2: 0.0.0.0 mask:0.0.0.0
                Secondary IP address3: 0.0.0.0 mask:0.0.0.0
                Secondary IP address4: 0.0.0.0 mask:0.0.0.0
                Secondary IP address5: 0.0.0.0 mask:0.0.0.0
                Secondary IP address6: 0.0.0.0 mask:0.0.0.0
                Secondary IP address7: 0.0.0.0 mask:0.0.0.0
                Secondary IP address8: 0.0.0.0 mask:0.0.0.0
                Secondary IP address9: 0.0.0.0 mask:0.0.0.0
```

Configuring an Interface

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

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

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

- Binding an interface to a zone

- Configuring an interface IP address
- Configuring an interface MTU value
- Configuring interface force shutdown
- Configuring interface ARP timeout
- Configuring an interface protocol
- Configuring interface ARP authentication
- Configuring interface proxy ARP
- Configuring interface mirroring
- Configuring traffic mirroring
- Configuring an interface reverse route
- Configuring interface backup
- Configuring a loopback interface
- Configuring an Ethernet interface
- Configuring a VSwitch interface
- Configuring an aggregate interface
- Configuring a redundant interface
- Configuring a tunnel interface
- Configuring a PPPoE sub-interface
- Bypassing the device
- Configuring an Out-of-band Management Interface
- Configuring the keepalive function of interface

Binding an Interface to a Zone

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

```
zone zone-name
```

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

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

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

Specifying the Description

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

description *description*

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

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

Configuring an Interface IP Address

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

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

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

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

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

Enter the interface ethernet0/0 configuration mode:

```
hostname(config)# interface ethernet0/0
```

Configure the primary IP address for ethernet0/0:

```
hostname (config-if-eth0/0)# ip address 1.1.1.1/24
```

Exit the interface ethernet0/0 configuration mode:

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

Pay attention to the following two points:

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

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

Configuring Interface Secondary IP

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

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

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

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

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

Configuring an Interface MTU Value

By default, the Maximum Transmission Unit (MTU) value is 1500 bytes. To set the MTU value, in the interface configuration mode, use the following command:

ip mtu *value*

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

Configuring Interface Force Shutdown

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

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

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

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

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

Configuring Interface ARP Timeout

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

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

```
arp timeout value
```

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

Configuring an Interface Protocol

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

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

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

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

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

Configuring FTP on the Interface

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

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

```
ftp user user-name password password
```

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

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

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

```
ftp port number
```

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

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

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

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

```
show ftp {port | user}
```

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

Configuring Interface Mirroring

The Ethernet interface mirroring allows users to mirror the traffic of one interface to another interface (analytic interface) for analysis and monitoring.

To configure an analytic interface, in the global configuration mode, use the following command:

```
mirror to interface-name
```

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

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

mirror enable {both | rx | tx}

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

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

Configuring Mirror Filter

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

The system supports the following filtering conditions:

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

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

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

- **interface** *interface-name* – Specifies the interface that enables mirror filter.
- **src-ip** *address-entry* – Specifies the source IP of the traffic. The system only mirrors traffic originating from the IP address to the analytic interface.
- **src-port** *port-num* – Specifies the source port of the traffic. The value range is 1 to 65535. The system only mirrors traffic originating from the port to the analytic interface.
- **dst-ip** *address-entry* – Specifies the destination IP of the traffic. The system only mirrors traffic destined to the IP address to the analytic interface.

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

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

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

no mirror filter id *id*

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

Note:

- Not all platforms support mirror filter. Refer to the actual product for the application of the function.
- NAT interfaces do not support mirror filter.
- The mirrored traffic should not exceed the workload of the analytic interface.
- The logical interfaces do not support the mirror filter.

Configuring Traffic Mirroring

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

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

Configuring a Mirror Profile

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

mirror-profile *mirror-profile-name*

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

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

no mirror-profile *mirror-profile-name*

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

Mirroring Traffic to an Interface

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

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

- *interface-name* - Specify the interface name. The traffic that matches the policy will be mirrored to this interface.
- **direction** {**forward** | **backward** | **bidirection**} - Use **forward** to only mirror the forward traffic to the specified interface; use **backward** to only mirror the backward traffic to the specified interface. Use **bidirection** to mirror both forward traffic and backward traffic to the specified interface.

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

no destination interface *interface-name*

Mirroring Traffic to an IP Address

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

destination ip *ip-address-1 interface-name* [*ip-address-2*] [**direction** {**forward** | **backward**}]

- *ip-address-1* – Specify the destination IP address. The traffic that matches the policy will be mirrored to this IP address.
- *interface-name* – Specify the egress interface of the traffic that matches the policy.
- *ip-address-2* – Specify the next-hop IP address. The traffic that matches the policy will be forwarded to this IP address via the egress interface.
- **direction** {**forward** | **backward**} – Use **forward** to only mirror the forward traffic to the specified IP address; use **backward** to only mirror the backward traffic to the specified IP address. Use **bidirection** to mirror both forward traffic and backward traffic to the specified IP address.

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

no destination ip *ip-address*

Binding a Mirror Profile to a Policy

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

mirror *profile-name*

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

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

no mirror *profile-name*

Viewing Mirror Profile Information

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

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

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

Interface Reverse Route

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

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

reverse-route [**force** | **prefer**]

- **force** – Forces to use reverse route. If the reverse path is found, forward the reverse data by reserve route; if not, drop the packet. By default, reverse route is forced on Layer 3 interfaces.
- **prefer** – Uses reverse path in preference to other route. If the reverse route is found, use it to forward data; if not, use the original return path (i.e. the current interface).

To cancel the reverse route settings, use the command **no reverse-route**.

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

Configuring Interface Backup

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

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

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

- *interface-name* – Specifies which interface is the backup interface.
- *schedule-name* – Specifies the schedule. During the specified schedule time period, data flow is directed to the backup interface.
- *time* - The migrating time before data being completely switched to the backup interface. The value range is 1 to 60 seconds. The parameter is disabled by default, i.e. all data flow is transferred to the backup interface immediately without migrating time.

- *track-object-name* – Specifies the track object. If the track object fails to response, data flow will be migrated from the primary to backup interface. If the object tracking is restored to normal, data flow will be switched back to the primary interface.

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

```
no backup-interface
```

Configuring Hold Time

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

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

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

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

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

Configuring the Keepalive Function of Interface

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

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

```
keepalive IP-address
```

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

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

```
no keepalive
```

Configuring the Interface Group

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

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

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

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

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

interface *interface-name*

- *interface-name* – Specifies the interface name which will be added to the interface group. The maximum number of interfaces is 8.

For example, adding ethernet0/0 and ethernet0/1 to the interface group test to achieve the interface linkage, in the global configuration mode, use the following command:

```
hostname(config)# interface-group test type linkage
hostname(config-if-group)# interface ethernet0/0
hostname(config-if-group)# interface ethernet0/1
```

In the global configuration mode, use the no form to delete the specified interface group:

no interface-group *group-name*

To view the status of the specified interface group, in any mode, use the following command:

show interface-group *group-name*

Configuring Local Property

System supports to configure an editable Local property for all interfaces (except VSwitch) to avoid the duplicate MAC address when managing huge amount of HA devices in the same Layer 2 Network. The sub-interface and virtual forward interface don’ t need to configure Local property, which inherit the primary interface directly. If you configure Local property for an interface , the system will not synchronize this configuration with the backup device. In the interface configuration mode, use the following command:

```
local
```

To delete HA Local property, in interface configuration mode, use command **no local**.

Configuring Interface Proxy ARP

When the device receives ARP request with a destination IP of a different network segment, proxy ARP feature allows the device to reply with its own MAC address as the source address.

Proxy ARP can work only on Layer-3 interface.

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

```
proxy-arp [dns]
```

- **proxy-arp** – Enables proxy ARP on the interface.
- **dns** – This parameter is for PnP IP

To disable proxy ARP, use the command **no proxy-arp**.

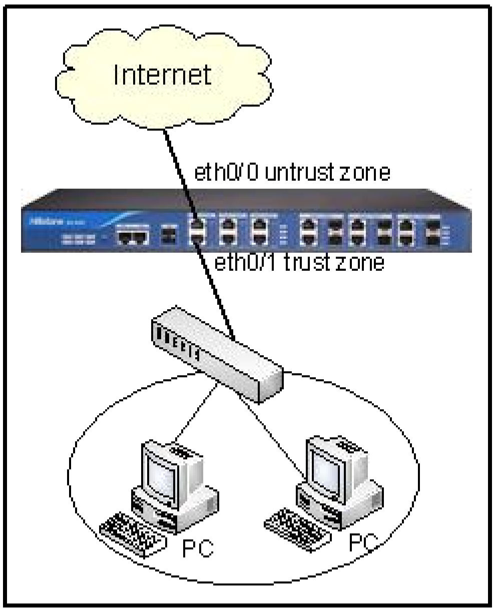
If an interface has been enabled with proxy ARP (with the parameter dns configured) and DNS proxy, it is a plug-and-play (PnP) interface, which means the internal computers with dynamic IP and DNS are able to access to the Internet through this interface. However, you should keep in mind that:

- If a computer and the PnP interface are in the same network segment, to allow the computer to visit the Internet, make sure that the computer uses the interface IP address as its gateway. For instance, an interface IP is 192.168.1.1/24 and a computer IP is 192.168.1.55/24. In order to allow the computer to visit the Internet through this interface, make the computer gateway address as 192.168.1.1.
- It is suggested to assign an unusual IP address with 32 bit mask to a PnP interface, like 10.199.199.199/32, which can ensure that there will be no identical IP address in the subnet.

Tip: For information on DNS proxy configuration, see Configuring a DNS Proxy.

PnP IP Configuration Example

The goal is to enable the PnP IP function on an interface to allow LAN users to visit the Internet. The topology is shown in Figure below: ethernet0/0 is connected to the Internet; ethernet0/1 is connected to the Intranet; DNS server IP is 202.106.1.1.



Take the following steps:

Step1: Configure an interface

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 2: Configure a DNS server

```
hostname(config)# ip name-server 202.106.1.1
hostname(config)# dns-proxy rule
hostname(config-dns-proxy-rule)# ingress-interface ethernet0/1
hostname(config-dns-proxy-rule)# src-addr any
hostname(config-dns-proxy-rule)# dst-addr any
hostname(config-dns-proxy-rule)# domain any
hostname(config-dns-proxy-rule)# action proxy
hostname(config-dns-proxy-rule)# name-server 202.106.1.1
hostname(config-dns-proxy-rule)# exit
```

Step 3: Configure the PnP IP feature (i.e. DNS proxy and proxy ARP)

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# dns-proxy
hostname(config-if-eth0/1)# proxy-arp dns
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 4: Configure a policy

```
hostname(config)# policy-global
hostname(config-policy)# rule from any to any from-zone trust to-zone untrust service any
permit
hostname(config-policy)# exit
hostname(config)#
```

Configuring a Loopback Interface

As a logical interface, loopback interface always remains in working state until the device shuts down. The naming rule for loopback interface is loopbackNumber (Number is an integer number from 1 to 256). The unique identifier for a loopback interface is its name.

Creating a Loopback Interface

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

interface loopback*Number*

- *Number* – The ID number of the loopback interface.

If loopback interface already exists, this command leads you into the interface configuration mode directly.

For example, to create a loopback named loopback1, in the global configuration mode, use the following command:

```
hostname(config)# interface loopback1
hostname(config-if-loo1)#
```

To delete a loopback interface, in the global configuration mode, use the command **no interface loopback***Number*.

Configuring an Ethernet Interface

All the Ethernet interfaces of FS devices are gigabit interfaces. Gigabit Ethernet interface conforms to 1000Base-T physical layer specifications. They can work under the rate of 10Mbit/s, 100Mbit/s and 1000Mbit/s. Both full-duplex and half-duplex modes are supported, but Gigabit half-duplex mode is not supported.

Configuring an Ethernet Sub-interface

Ethernet interface is allowed to have sub-interfaces.

To create a sub-interface, in the global configuration mode, use the following command:

interface ethernetm/n.*tag*

- *.tag* – Specifies a number to mark the sub-interface. The value range is 1 to 4094. For example, the command **interface ethernet0/0.1** creates a sub-interface named ethernet0/0.1 for interface ethernet0/0.

If the sub-interface exists, this command leads you into the interface configuration mode directly.

To delete a sub-interface, use the command **no interface ethernetm/n**.*tag*.

The Ethernet sub-interface supports PPPoE. One Ethernet interface can only be bound to one PPPoE instance.

Entering the Ethernet Configuration Mode

You must the enter Ethernet configuration mode in order to configure settings like interface speed, duplex modes and Combo type, etc.

To enter the Ethernet configuration mode, in the global configuration mode, use the following command:

interface *ethernetm/n*

- *ethernetm/n* – Specifies the Ethernet interface.

Configuring the Ethernet Interface Speed

Copper interface can adapt to link speed of 10Mbit/s, 100Mbit/s and 1000Mbit/s, while fiber-optic interface supports 1000Mbit/s only. Therefore, fiber-optic interface does not need speed setting.

To configure the link speed for an interface, in the interface configuration mode, use the following command:

speed *value*

- *value* - This parameter can be auto, 10, 100 or 1000. auto is the default value, which means the system automatically detects and assigns a proper link speed. The link speed specified here must conform to the actual network link speed of this end and of the peer device.

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

Note:If the interface link speed is auto, the interface duplex mode should be set to auto as well.

Configuring an Interface Duplex Mode

Ethernet copper interface can work under full and half duplex mode, while Gigabit Ethernet fiber-optic interface can work only in full duplex mode.

To configure a duplex mode for an interface, in interface configuration mode, use the following command:

duplex *method*

- *method* - This parameter can be auto, full (for full-duplex mode) or half (for half-duplex mode). The default value is auto, which means the system assigns a proper mode for the interface.

For example, to configure ethernet0/2 link speed to 1000Mbit/s with full duplex, use the following commands:

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# speed 1000
hostname(config-if-eth0/2)# duplex full
hostname(config-if-eth0/2)# exit
hostname(config)#
```

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

Note:When the duplex mode is auto, the interface link speed must be set to auto as well.

Cloning a MAC Address

To clone a MAC address to the Ethernet sub-interface, in the Ethernet sub-interface configuration mode, use the following command:

mac-clone *H.H.H*

- *H.H.H* – Specifies the MAC address.

To delete the specified MAC address, in the Ethernet sub-interface configuration mode, use the command **no mac-clone**.

If the MAC address changes after the PPPoE connection has been established, you need to re-connect the PPPoE client to make the new MAC address take effect.

Configuring a Combo Type

A Combo port is the combination of a fiber-optic port and a copper port. By default, if both of the ports have cables connected, fiber-optic port has the priority. If the copper port was used at first, after restarting the device, the fiber-optic port will be activated and used to transfer data if it is connected with cable. You can also select one of the two ports via CLI.

To select a copper or fiber-optic port, in the interface configuration mode, use the following command:

combo {**copper-forced** | **copper-preferred** | **fiber-forced** | **fiber-preferred**}

- **copper-forced** – Forces to use the copper port.
- **copper-preferred** – Prioritizes the copper port.
- **fiber-forced** – Forces to use the fiber-optic port.
- **fiber-preferred** – Prioritizes the fiber-optic port. When this parameter is configured, the data flow will switch from the copper port to the fiber-optic port automatically and there is no need to restart device.

To resume to the default setting, use the command **no combo**.

Configuring a VSwitch Interface

VSwitch interface is a Layer-3 interface. It is an assembly of all interfaces in the VSwitch. When you create a VSwitch, its corresponding VSwitch interface is automatically created.

Creating a VSwitch Interface

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

vswitch vswitch*Number*

- *Number* - Specifies a number as the identifier of the VSwitch and its interface. The value range may vary from different platform models.

To clear the VSwitch and its corresponding interface, use the command **no vswitch vswitch***Number*.

Configuring an Aggregate Interface

An aggregate interface is an assembly of two or more physical interfaces. The data flow passing through the aggregate interface is shared equally by its physical interfaces. This method can increase the usable bandwidth. If one of the interfaces fails to work, other interface(s) can take over its data flow and process data, but bandwidth is reduced. The following sections introduce basic configurations of aggregate interface.

Creating an Aggregate Interface and Sub-interface

To create an aggregate interface, in the global configuration mode, use the following command:

interface aggregate*Number*

- *Number* - Specifies the ID of the aggregate interface. For different product models, the range of Number is different. For example, the command interface aggregate2 creates an aggregate interface named "aggregate2".

This command leads you into the aggregate interface configuration mode. If the specified interface exists, you will enter its configuration mode directly.

To delete an aggregate interface, in the global configuration mode, use the command

no interface aggregate*Number*. Before deleting it, you must clear all the settings and zone referencing of the interface.

To create a sub-interface for an aggregate interface, in the global configuration mode, use the following command:

interface aggregateNumber*.tag*

- *.tag* – Specifies the ID of the sub-interface. The parameter is an integer number from 1 to 4094. For example, the command interface aggregate2.1 creates a sub-interface named aggregate2.1 for aggregate interface named aggregate2.

To delete an aggregate sub-interface, in the global configuration mode, use the command **no interface aggregateNumber***.tag*. Before deleting an interface, you should clear all settings of it, including the binding and referencing with other interfaces and zones, etc.

Adding a Physical Interface

An aggregate interface includes two or more physical interfaces.

To add a physical interface to an aggregation interface, in the physical interface configuration mode, use the following command:

aggregate *aggregatenumber*

- *aggregatenumber* - Specifies the name of the aggregation interface to which the physical interface is added. Ensure that the physical interface does not belong to any other interface or zone.

To remove a physical interface from the aggregation interface, in the physical interface configuration mode, use the command **no aggregate**.

Example of Configuring an Aggregate Interface

Here is a configuration example. The goal is to create aggregation interface aggregate2, and add ethernet0/3 and ethernet0/4 to the aggregate2, then delete ethernet0/3 from it.

Use the following commands:

```
hostname(config)# interface aggregate2
hostname(config-if-agg2)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# aggregate aggregate2
hostname(config-if-eth0/3)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# aggregate aggregate2
hostname(config-if-eth0/4)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# no aggregate
```

Configuring a Redundant Interface

A redundant interface consists of two physical interfaces, one of which works as the primary interface processing the traffic flow through the redundant interface, the other one stands by and substitutes the primary interface to process data flow when it fails to work.

Creating a Redundant Interfaces and Sub-interface

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

interface redundant*Number*

- *Number* - Specifies the ID of the redundant interface. For example, the command interface redundant2 creates a redundant interface named redundant2.

This command takes you into the redundant interface configuration mode. If the specified interface exists, you will directly enter its configuration mode.

To delete a redundant interface, in the global configuration mode, use the command **no interface redundant***Number*.

Before deleting it, you should clear all settings, including the binding and referencing with other interfaces and zones, etc.

To create a sub-interface for an existing redundant interface, in the global configuration mode, use the following command:

interface redundantNumber*.tag*

- *.tag* − Specifies the ID of the sub-interface. This parameter should be an integer from 1 to 4094. For example, the command interface redundant2.1 creates a sub-interface called redundant2.1 for the redundant interface named redundant2.

To delete a redundant sub-interface, in the global configuration mode, use the command **no interface redundantNumber***.tag*.

Adding a Physical Interface

To add a physical interface to a redundant interface, in the physical interface configuration mode, use the following command:

redundant *interface-name*

- *interface-name* − Specifies the name of the redundant interface to which the physical interface is added. Make sure that the physical interface does not belong to any other interface or zone.

To remove a physical interface from a redundant interface, use the command **no redundant**. If the deleted interface serves as the primary interface, you need to clear the master interface setting first.

Specifying the Primary Interface

To specify a physical interface in the redundant interface as the primary interface, in the redundant interface configuration mode, use the following command:

primary *interface-name*

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

To cancel the primary interface, in the redundant interface configuration mode, use the command **no primary**.

Example of Configuring a Redundant Interface

Here is a configuration example. The goal is to create a redundant interface named redundant1, add the interface ethernet0/4 and interface ethernet0/5 to redundant1, and to make ethernet0/4 as the primary interface, then remove ethernet0/5 from redundant1.

Use the following commands:

```
hostname(config)# interface redundant1
hostname(config-if-red1)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# redundant redundant1
hostname(config-if-eth0/4)# exit
hostname(config)# interface ethernet0/5
hostname(config-if-eth0/5)# redundant redundant1
hostname(config-if-eth0/5)# exit
hostname(config)# interface redundant1
hostname(config-if-red1)# primary ethernet0/4
hostname(config-if-red1)# exit
hostname(config)# interface ethernet0/5
hostname(config-if-eth0/5)# no redundant
```

Configuring a Tunnel Interface

Tunnel interface serves as the entrance of VPN tunnel and the VPN traffic goes through the tunnel interface. Tunnel interface is a Layer-3 interface.

Creating a Tunnel Interface

To create a tunnel interface, in the global configuration mode, use the following command below:

interface tunnel*Number*

- *Number* - Specifies the ID of the tunnel interface. For example, the command interface tunnel2 creates the tunnel interface named tunnel 2.

This command leads you to the tunnel interface configuration mode. If the tunnel interface of the specified name exists, you will directly enter the tunnel interface configuration mode.

To delete a tunnel interface, use the command **no interface tunnel***Number*.

Binding a Tunnel

You can bind a tunnel interface to an IPsec VPN, GRE, SCVPN or L2TP tunnel. A tunnel interface can be bound to multiple IPsec VPN or GRE tunnels, but only one SCVPN (or L2TP) tunnel.

To bind a tunnel to the tunnel interface, in the tunnel interface configuration mode, use the following command:

tunnel {{**ipsec** | **gre**} *tunnel-name* [**gw** *ip-address*] | **scvpn** *vpn-name* | **l2tp** *tunnel-name* }

- {**ipsec** | **gre**} *tunnel-name* – Specifies the tunnel type and its name.
- **gw** *ip-address* – Specifies the next hop IP address of the tunnel interface, which can be the IP address of the peer tunnel interface or the IP address of the egress interface on the other end. This parameter is only valid for an interface which binds to multiple IPsec VPN or GRE VPN tunnels. The default value is 0.0.0.0.
- **scvpn** *vpn-name* – Specifies the name of SCVPN tunnel bound to this interface. A tunnel interface can be bound to only one SCVPN tunnel.
- **l2tp** *tunnel-name* – Specifies the name of L2TP tunnel bound to this interface. A tunnel interface can be bound to only one L2TP tunnel.

Repeat this command to bind more IPsec VPN tunnels or GRE tunnels.

To cancel the binding relationship, use the command **no tunnel** {**ipsec** *vpn-name* | **gre** *tunnel-name* | **scvpn** *vpn-name* | **l2tp** *tunnel-name* }.

Multi-tunnel OSPF

In some site-to-site VPN connections, a tunnel interface binds with multiple tunnels. If OSPF dynamic routing is used to manage data exchange among different sites, you need to enable point-to-multipoint tunnel interface (the default tunnel interface is point-to-point network type).

To configure point-to-multipoint type, in the tunnel interface configuration mode, use the following command:

ip ospf network point-to-multipoint

To restore to the default point-to-point type, use the following command:

no ip ospf network point-to-multipoint

Borrowing an IP Address (IP Unnumbered)

In some cases, like when tunnel interface is used to forward packets which go through the device, configuring an IP address is not required for that interface. In situation like that, you can use the IP address borrowing feature (IP unnumbered) to borrow IP addresses from other interfaces.

To enable the IP address borrowing feature, in the tunnel interface configuration mode, use the following command:

ip address unnumber *interface-name*

- *interface-name* – Specifies the name of the interface from which the IP address is borrowed.

To clear the borrowed IP, use following command:

no ip address unnumber

Note: Interfaces on the two ends of the tunnel are not allowed to use borrowed IP address at the same time.

Viewing Tunnel Information

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

show interface bind-tunnels *tunnel-name*

- *tunnel-name* – Specifies the name of the tunnel interface to be shown.

Configuring a PPPoE Sub-interface

One physical interface can have multiple PPPoE sub-interfaces so that multiple ISPs can be accessed through this one interface.

To create a PPPoE sub-interface, in the global configuration mode, use the following command:

interface ethernet*X/Y***-pppoe***Z*

- ethernet*X/Y* – Specifies the name of the Ethernet port. For instance, ethernet0/5.
- -pppoe*Z* – Specifies the name of PPPoE sub-interface. Z indicates the ID of the PPPoE sub-interface. The value range varies with platforms.

To clear a PPPoE sub-interface, in the global configuration mode, use the following command:

no interface ethernet*X/Y***-pppoe***Z*

Link Aggregation

Link aggregation combines multiple network connections in parallel to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links fails.

The device supports forced link aggregation and LACP (Link Aggregation Control Protocol). The forced link aggregation is implemented by the aggregate interface. For more information, see Configuring an Aggregate Interface. This section mainly describes the usage of LACP.

LACP

LACP (Link Aggregation Control Protocol) is designed to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that is also enabled with LACP).

FS devices use the aggregate interface to implement the LACP function. The aggregate interface with LACP enabled is named as aggregate group, and the physical interfaces in the aggregate group is the member of the aggregate group. After enabling LACP on an aggregate interface, the member interface sends the LACPDU packets to the peer to notify its system priority, system MAC address, port priority, port number, and operating key. The peer receives the LACPDU and compare the information with the local information to select a proper member interface, thus the both sides can decide which link will be used to transfer data.

Member Status in an Aggregate Group

There are four statuses for the member interfaces in an aggregate group:

- Unselected: The interface is selected by the aggregate group and cannot forward traffic. This status is usually caused by physical reasons, e.g., the interface mode is non-duplex, rates of both sides are inconsistent, physical connection failure, etc.
- Selected: The interface is in aggregate group, but its peer is not ready, so the interface cannot forward traffic. When it receives LACPDU packets from the peer, and learns the status of its peer is Selected, the status of the interface will switch to Active. The interface in Active status can forward traffic.
- Standby: The interface is a backup interface, and cannot forward traffic. If the LACP priority of the interface is promoted, the interface will replace the existing Selected interface and change its own status to Selected, and the status of the replaced interface will switch to Standby. When other interfaces become Unselected, the Standby interface will change to Selected interface automatically.

- Active: The interface is aggregated successfully and forwards traffic. If the interface has not received LACPDU packets from the peer in three LACPDU timeouts, it will be concluded as link down. In such a case, the status of the interface will switch to Selected, and the interface will stop forwarding traffic.

Configuring LACP

The configurations of LACP include:

- Enabling/Disabling LACP
- Specifying LACP System Priority
- Specifying Interface LACP Priority
- Specifying LACP Timeout
- Specifying the Maximum Active Links
- Specifying the Minimum Active Links
- Specifying Load Balance Mode

Enabling/Disabling LACP

LACP can be enabled on the aggregate interfaces (aggregate sub-interface, aggregate virtual forward interface do not support LACP). To enable/disable LACP, in the aggregate interface configuration mode, use the following commands:

- Enable: **lacp enable**
- Disable: **no lacp enable**

Specifying LACP System Priority

LACP system priority is used to determine the priority between devices in both sides. The interface with higher LACP system priority will be defined as the standard selected interface. The smaller the number is, the higher the priority will be. If both sides have the same LACP system priority, the system will choose the interface with smaller MAC address to be the standard selected interface.

To configure the LACP system priority, in the aggregate interface configuration mode, use the following command:

lacp system-priority *value*

- *value* – Specifies the LACP system priority. The value range is 1 to 32768. The default value is 32768.

To restore to the default LACP system priority, in the aggregate interface configuration mode, use the following command:

```
no lacp system-priority
```

Specifying Interface LACP Priority

Interface LACP priority determines the sequence of becoming the Selected status for the members in the aggregate group. The smaller the number is, the higher the priority will be. Link in the aggregate group that will be aggregated is determined by the interface LACP priority and the LACP system priority.

To configure the interface LACP priority, in the configuration mode of the interface in the aggregate group, use the following command:

lacp port-priority *value*

- *value* − Specifies the interface LACP priority. The value range is 1 to 32768. The default value is 32768.

To restore to the default interface LACP priority, in the configuration mode of the interface in the aggregate group, use the following command:

```
no lacp port-priority
```

Specifying LACP Timeout

The LACP timeout refers to the time interval for the members waiting to receive the LACPDU packets. If the local member does not receive the LACPDU packet from its peer in three timeout values, the peer will be conclude as down, and the status of the local member will change from Active to Selected, and stop traffic forwarding. The system supports short timeout (1 second) and long timeout (30 seconds, the default value).

To specify the LACP timeout for the member interface, in the configuration mode of the interface in the aggregate group, use the following command:

```
lacp period-short
```

To restore to long timeout, in the configuration mode of the interface in the aggregate group, use the following command:

```
no lacp period-short
```

Specifying the Maximum Active Links

The number of maximum active link refers to the maximum Active interface number. When the Active interface number reaches the maximum number, status of other legal interfaces will become Standby. For instance, there are 4 Active interfaces in the aggregate group. If the maximum active links is specified to 2, system will choose two interfaces as the Active interfaces according to the priority, and the status of the other two interfaces with lower priority will become Standby. When the Active interface down causes the link down, system will switch the status of the Standby interface to Active, thus the LACP works as the redundant way.

To specify the maximum active links, in the aggregate interface configuration mode, use the following command:

```
lacp max-bundle number
```

- *number* – Specifies the number of the maximum active links. The value range is 1 to 16. The default value is 16.

To restore to the default maximum active link number, in the aggregate interface configuration mode, use the following command:

```
no lacp max-bundle
```

Specifying the Minimum Active Links

The number of minimum active link refers to the minimum Active interface number. When the number of Active interface is less than the minimum active link number in the aggregate group, status of all the legal interfaces in the aggregate group will become Standby. The minimum active links must be less than the maximum active links.

To specify the minimum active links, in the aggregate interface configuration mode, use the following command:

```
lacp min-bundle number
```

- *number* – Specifies the number of the minimum active links. The value range is 1 to 8. The default value is 1.

To restore to the default minimum active link number, in the aggregate interface configuration mode, use the following command:

```
no lacp min-bundle
```

Specifying the Load Balance Mode

You can specify the load balance mode for the aggregate group. System supports flow-based load balance and 7-tuple based load balance. When the members of the aggregate group is Layer-2 interfaces, the system can only support the load balance mode based on the source MAC address and destination MAC address. For instance, if the source IP is specified to be the load balance condition, all the packets with the same source IP will be forwarded by the same interface in the aggregate group.

To specify the load balance mode, in the aggregate interface configuration mode, use the following command:

```
load-balance mode {flow | tuple {dest-ip dest-mac dest-port protocol src-ip src-mac src-port}}
```

- **flow** – Gets the load balance mode from the traffic. It is the default mode.
- **tuple [dest-ip dest-mac dest-port protocol src-ip src-mac src-port]** – Uses tuples as the load balance condition. It can be one of the 5 tuples or the combination of the tuples.

To restore to the default load balance mode, in the aggregate interface configuration mode, use the following command:

```
no load-balance
```

Viewing Aggregate Group Information

You can view the LACP aggregate information in any CLI mode. To view the aggregate group information, use the following command:

show lacp *aggregate-name*

- *aggregate-name* – Specifies the name of the aggregate group you want to view.

Bypassing the Device

Some of FS models are designed with bypass functionality. To reduce the risk of single point of failure, bypassing the device can ensure network continuity during device reboot, power failure or other malfunctions. When a bypass module is working, the networks accessed to the security device are physically connected by the bypass module.

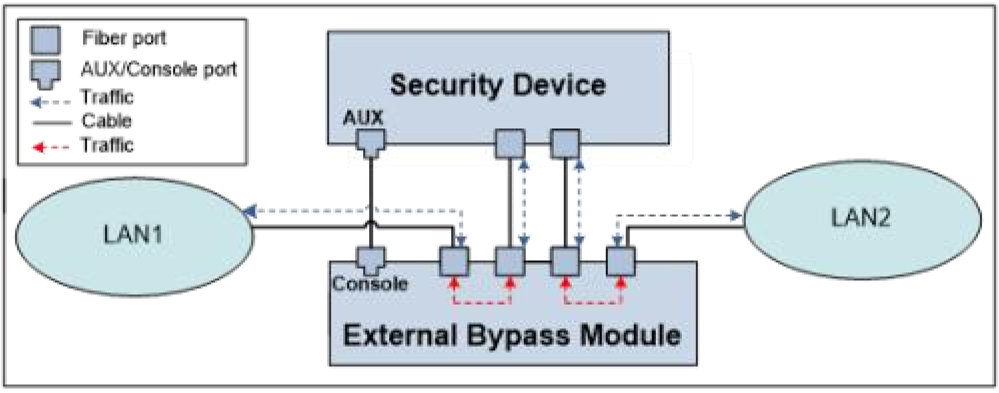
Note:

- Not all FS platforms support bypass functionality.
- Built-in bypass modules are bundled with FS products. External bypass module is the BSSF-CEM module provided by Silicom. Currently, only part of FS devices (SG-6000-E3965) support the external bypass module.

Network Layout with Bypass Module

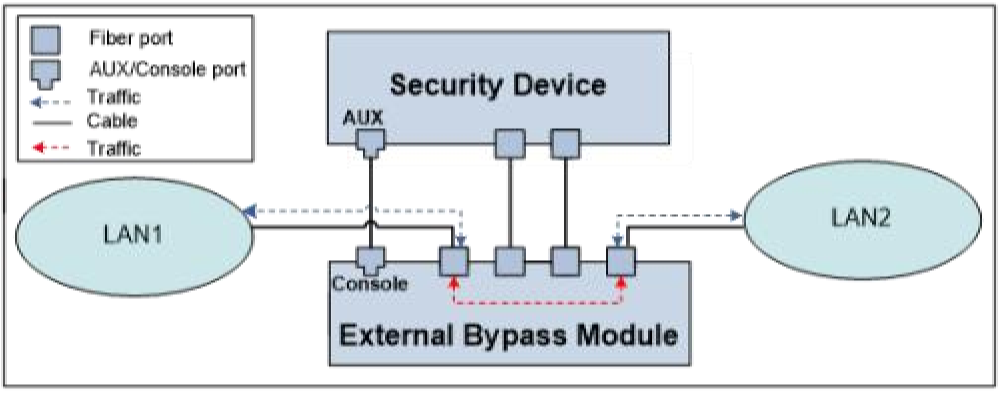
To install a built-in bypass module, see the installation manual of your device module for detailed instructions.

For external bypass modules, connect the AUX port of the security device to Console port of Silicom bypass module with a cable. See the figure below for cable connection (black line) and traffic flow directions.



As shown above, connect LAN1 and LAN2 to the bypass module and connect the module Console port to the device AUX port. When the network functions well, the two LANs can gain access to each other through the device.

However, in particular situations like power failure or device rebooting, the device is bypassed and LAN1 and LAN2 are physically connected through the bypass module.



Note: The following points when you bypass the device with an external bypass module:

- Use fiber cable with LC-type connector.
- The heartbeat cable, a cable with RJ-45 connector on one end and RJ-11 on the other, which is used to connect the device AUX port and bypass module Console port, is provided by Silicom. Connect the RJ-45 end to the AUX port of device and RJ-11 end to the Console port of bypass module.
- Make sure that the Tx and Rx are correctly connected.
- Make sure all cables are properly connected.

Enabling External Bypassing

If you choose to use external bypass module to bypass the device, you need to enable this feature, which is off by default, when all connections are properly established.

To enable/disable external bypassing function, in the global configuration module, use the following commands:

- Enable: **external-bypass enable**
- Disable: **no external-bypass enable**

Force to Close the Bypass Function of Device

System will enter Bypass state if the device fails to forward traffic under certain state (such as system restart, abnormal operation, and device power off). In Bypass state, the two Bypass interface is directly connected physically, and can forward traffic for each other to ensure the reliability of the business. By default, Bypass function is enabled. If you want to avoid this situation, try to avoid setting the pair of Bypass interfaces as the tap zone or close the Bypass function.

In the global configuration mode, use the command below to force to close the bypass function:

```
force-close-bypass
```

Use the no form to restore bypass functionality: **no force-close-bypass**.

> Note: During device restart, if the system configuration information is not loaded, the device is in Bypass state, and the pair of Bypass interfaces can still forward traffic to each other.

Viewing External Bypassing

To view the external bypass module working status, type, version, etc., in any mode, use the following command:

```
show external-bypass
```

Here is an example:

```
hostname# show external-bypass

======================================================================
========

external-bypass:enable

device status:present

current mode:normal

device info:BSFT,version 28

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

Address

Overview

In FSOS, IP address is an important element for the configurations of multiple modules, such as policy rules, NAT rules and session limit rules. Therefore, FSOS supports address book to facilitate IP address reference and flexible configuration. You can specify a name for an IP range, and only reference the name during configuration. Address book is the database in FSOS that is used to store the mappings between IP ranges and the corresponding names. The mapping entry between an IP address and its name in the address book is known as an address entry.

Address Entry

FSOS provides a global address book. You need to specify an address entry for the global address book. In an address entry, you can replace the IP range with a DNS name. You can use them for NAT conveniently. Furthermore, an address entry also has the following features:

- All address books contain a default address entry named Any. The IP address of Any is 0.0.0.0/0, i.e., any IP address. Any can neither be edited nor deleted.
- One address entry can contain another address entry in the address book.
- If the IP range of an address entry changes, FSOS will update other modules that reference the address entry automatically.

Configuring an Address Book

You can perform the following operations on an address book through CLI:

- Adding or deleting an address entry
- Specifying the IP range of an address entry
- Viewing the address book information

Adding or Deleting an Address Entry

To add an address entry to the address book and enter the address configuration mode, in the global configuration mode, use the following command:

address *address-entry*

- *address-entry* - Specifies the name of the address entry that will be added.

To delete the specified address entry from the address book, in the global configuration mode, use the following command:

no address *address-entry*

Note:The address entry being referenced by other modules or address entries can not be deleted.

Specifying the IP Range of an Address Entry

In FSOS, the IP range of an address entry is the collection of all the IP members within the range. The members of the address entry consist of the following types:

- IP address: includes two types. One is IP address/subnet mask, such as 10.100.2.0/24; the other is IP address with a wildcard mask, such as 192.168.0.1 255.255.0.255.
- Host name, such as host1.fs.com. Support the host name which contains the wildcard, such as *.baidu.com.
- IP range, such as 10.100.2.3 - 10.100.2.100
- Country or region: A set of IP addresses that belong to a country or a region.
- Other address entries

To add an IP member to the specified address entry, or delete the specified member from the address entry, in the address configuration mode, use the following commands:

- ip {*ip-address* {*netmask* | *wildcardmask*} | *ip/netmask*}
  - *ip-address* – Specifies the IP address of the IP member.
  - *netmask* / *wildcardmask* – Specifies the subnet wildcard mask. FSOS does not support the wildcard mask which has more than 8 zeros (consecutive or non-consecutive) before the first 1 from the right side of its binary form. For example, 255.0.0.255 is an invalid wildcard mask, while 255.0.255.0 and 255.32.255.0 are valid wildcard masks.
  - *ip/netmask* – Specifies the IP and netmask of the IP member.
- no ip {*ip-address* {*netmask* | *wildcardmask*} | *ip/netmask*}

To add a host member to an address entry or delete the specified member, in the address configuration mode, use the following commands:

- host *host-name* [**vrouter** *vrouter-name*]
  - *host-name* – Specifies the host name. Support the host name which contains the wildcard. You can specify up to 255 characters.

  - *vrouter-name* - Specifies the VRouter of the host.

- **no host** *host-name* [**vrouter** *vrouter-name*]

To add an IP range member to an address entry, or delete the specified member from the address entry, in the address configuration mode, use the following commands:

- **range** *min-ip* [*max-ip*]
- **no range** *min-ip* [*max-ip*]

To add a set of IP addresses that belong to a country or a region, in the address configuration mode, use the country command. To delete this member from the address entry, use the no form of this command.

- **country** *country-name*
- **no country** *country-name*

You can press the **Tab** key after the country keyword to see the available values of the country-name parameter.

To add another address entry to an address entry, or delete the specified address entry from the address entry, in the address configuration mode, use the following commands:

- **member** *address-entry*
- **no member** *address-entry*

Note:

- The country or region member is supported in the address entry of the IPv4 type.
- Only the security policy and the policy-based route support the address entry with the country or region member added.
- The address entry with the country or region member added does not support the exclude range min-ip max-ip settings in Excluding Address Entries.
- In a device, you can use wildchart for up to 128 host members.

Excluding Address Entries

Both IPv4 and IPv6 address entries are supported in address books. By configuring the excluded entries, you can rule out IPv4 or IPv6 addresses from an address book. The types of address entries that can be excluded are the following two types:

- IP address: IPv4 type: both IP/netmask (e.g. 10.100.2.0/24) and IP/wildcard netmask (192.168.0.1 255.255.0.255) can be excluded; IPv6 type, like 2001::1/64, is also supported.
- IP range: a range of IP addresses, e.g. 10.100.2.3 – 10.100.2.100 or 2002::0-2002::10.

Note: The maximum percentage of excluded members is 10% of the total number in this address book.

Excluding an IPv4 Address Entry

To exclude an IPv4 address entry, under address book configuration mode, use the following command:

exclude ip *ip-address* {*netmask* | *wildcardmask*}

- *ip-address* – Specify the IP address to be excluded.
- *netmask* | *wildcardmask* – Specify the *netmask* or *wildcardmask*. Wildcard netmaks is to signify a sequence of less than 8 wildcard characters (i.e. less than eight zeros) in a binary netmask (the last binary number of the netmask must be 1, not 0). For example, 255.0.0.255 is not supported in this wildcard netmask format; 255.0.255.0 and 255.32.255.0 are legitimate.

To resume an IPv4 address entry, use the command **no exclude ip** *ip-address* {*netmask* | *wildcardmask*}.

To exclude an IP range address entry, under address book configuration mode, use the following command:

exclude range *min-ip max-ip*

- *min-ip max-ip* – Specify the start and end IP addresses.

To resume an exclude address range, use the command **no exclude range** *min-ip max-ip*.

Excluding IPv6 Address Entries

To exclude IPv6 address entries from an address book, under this address book' s configuration mode, use the following command:

exclude ip *ipv6-prefix / prefix-length*

- *ipv6-prefix / prefix-length* – Specify the IPv6 prefix and its length. The range is 65 to 128.

To resume an excluded IPv6 address entry, use the command **no exclude ip** *ipv6-prefix / prefix-length*.

To exclude IPv6 range address entry from an address book, under address book configuration mode, use the following command:

exclude range *min-ipv6-address max-ipv6-address*

- *min-ipv6-address* – Specify the start IPv6 address.
- *max-ipv6-address* – Specify the end IPv6 address.

To resume an excluded IP range back to address book, use the command **no exclude range** *min-ipv6-address max-ipv6-address*.

Renaming an Address Entry

To rename an existing address entry, in the address configuration mode, use the following command:

rename *name*

- *name* - Specifies the new name for the address entry. If the name is repeated with an existing one, the command will void.

Viewing the Reference Address of an Address Entry

In FSOS, an address entry can be referenced by other modules, such as policy rules, NAT rules or session limit rules. To view the reference of an address entry by other modules, i.e., the reference address of the address entry, in any mode, use the following command:

show reference address *address-entry*

- *address-entry* - Shows the reference address of the specified address entry.

Example:

```
hostname(config)# show reference address 10.101.0.194

==================================================

Name: | 10.101.0.194  (name of the address entry)

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

Address: | -  (referenced by other address entries)

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

Policy rule: | policy 20 src-addr (referenced by policy rules)

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

SNAT rule: | - (referenced by SNAT rules)

----------------------------------------------------
```

```
DNAT rule: | - (referenced by DNAT rules)

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

Statistics: | - (referenced by stat-sets)

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

Session limit: | rule 1  (referenced by session limit rules)

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

PBR: | -  (referenced by PBR rules)

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

QoS: | - (referenced by QoS rules)

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

ExStats: | - (referenced by extended stat-
sets)=====================================================
```

Viewing the Address Book Details

To view the details of the global address book, including the entries of the address book, number of the members, and detailed information of the members, in any mode, use the following command:

show address [**filter-ip** *A.B.C.D*] | [*address-entry*]

- **show address** - Shows the information of all the address entries in the address book.
- **filter-ip** *A.B.C.D* - Shows the information of address entries that contain the specified IP address.
- *address-entry* - Shows the information of specified address entry.

To check where the IP address is from, in any mode, use the following command:

show country ip *A.B.C.D*

- *A.B.C.D* – Enter the IP address to check which country or region this IP address belongs to.

Address Book Configuration Example

Configuration Example 1

The goal is to create address entries named address1 and address2 for the address book; add the following members to address1: 10.200.1.0/16, 192.168.1.0/24, 192.168.0.1/255.255.0.255 and fs.com;

add the following members to address2: 10.100.3.1 to 10.100.3.10 and address1. Use the following commands:

```
hostname(config)# address address1
hostname(config-addr)# ip 10.200.1.0/16
hostname(config-addr)# ip 192.168.1.0 255.255.255.0
hostname(config-addr)# ip 192.168.0.1 255.255.0.255
hostname(config-addr)# host fs.com
hostname(config-addr)# exit
hostname(config)# address address2
hostname(config-addr)# range 10.100.3.1 10.100.3.10
hostname(config-addr)# member address1
hostname(config-addr)# exit
hostname(config)#
```

Configuration Example 2

Users can configure the host name which contains the wildcard in address book. To specify a host name as *.baidu.com, use the following commands:

```
hostname(config)# addr baidu
hostname(config-addr)# host *.baidu.com
```

Service and Application

This chapter introduces the following topics:

- Service
- Application

Service Overview

Service is information stream designed with protocol standards. Service has some specific features, like corresponding protocol, port number, etc. For example, the FTP service uses TCP protocol, and its port number is 21. Service is an essential element for the configuration of multiple FSOS modules including policy rules, NAT rules, etc. FSOS ships with over 100 predefined services and over 10 service groups.

Besides, you can also customize user-defined services and service groups as needed. All these services and service groups are stored in and managed by FSOS service book. Each service in the service book contains its specific service entry.

Viewing Service Information via CLI

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

show service {**predefined** | **userdefined** | **name** *service-name*}

- **predefined** – Shows the predefined service information.
- **userdefined** – Shows the user-defined service information.
- **name** *service-name* - Shows the information of the specified service.

Viewing Service References

In FSOS, a service can be referenced by other modules, such as policy rules, NAT rules or session limit rules. To view the reference of a service or service group by other modules, i.e., the service or service group address, in any mode, use the following command:

show reference service *service-name*

- *service-name* – Shows the reference of the specified service or service group.

Example:

```
hostname(config)# show reference service ftp
================================================================
Name: | ftp (name of the service or service group)
-----------------------------------------------------
Service group: | SRV_INTERNET_PROTOCOL (reference by other service groups)
-----------------------------------------------------
Policy rule: | policy 105 , policy 100(reference by policy rules)
-----------------------------------------------------
DNAT rule: | - (reference by DNAT rules)
-----------------------------------------------------
SNAT rule: | -(reference by SNAT rules)
-----------------------------------------------------
```

```
Statistics: | - (reference by stat-sets)

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

Policy route: | - (reference by PBR rules)

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

Predefined Services

FSOS provides more than 100 predefined services. To view all the predefined services supported by the current version, use the above **show** command or WebUI.

The following section describes several common predefined services.

RSH

RSH ALG (Remote Shell) allows authenticated users to run shell command on the remote host. FS device supports RSH services of transparent mode, NAT mode and router mode.

Sun RPC

Sun RPC (Sun Remote Procedure Call) allows the program running on a host to call the programs running on other hosts. Because of the large number of RPC services and the requirement for broadcasting, RPC services’ transmission addresses are dynamically negotiated based on the number and version of the services. You can define some binding protocols to map the number of RPC programs and service versions to the transmission addresses.

FS devices support a predefined Sun RPC service for users to permit or deny traffic according to policies configured. You can define a policy rule to permit or deny all the RPC requests. For example, if you need to use the network file system (NFS), then configure a policy rule that allows Sun RPC services.

MS RPC

Microsoft Remote Procedure Call (MS RPC) is the RPC implementation of the Microsoft distributed computing environment. MS RPC allows the program running on a host to call programs running on other hosts. Because of the large number of RPC services and the requirement for broadcasting, RPC services' transmission addresses are dynamically negotiated based on the UUID (Universal Unique Identifier) of the server.

FS devices support a predefined MS RPC service for users to permit or deny traffic according to policies configured. You can define a policy rule to permit or deny all the RPC requests. For example, if you need to use the Outlook/Exchange or MSqueue service, configure a policy rule that allows MS RPC services.

Predefined Service Group

The predefined service group includes some associated predefined services to facilitate users' configuration. FSOS provides more than 10 predefined service groups. The service group that contains dynamically identified predefined services is known as a dynamically identified predefined service group, and such a service group needs to be configured individually. When the dynamically identified predefined services are updated by the signature database, the corresponding dynamically identified predefined service group will also be updated. You can view and use the predefined service groups, but cannot edit or delete them.

To view the predefined service group, in any mode, use the following command:

```
show servgroup predefined
```

User-defined Service

Besides the above predefined services, you can also create your own user-defined services. A user-defined service can include up to eight service entries. The parameters that you can specify for the user-defined service entries are:

- Name
- Protocol type
- The source and destination port for TCP or UDP service, type and code value for ICMP service.
- Timeout
- Application type

Creating/Deleting a User-defined Service

To create a service and add it to the service book via CLI, or to delete the specified service, in the global configuration mode, use the following commands:

service *service-name*

no service *service-name*

- *service-name* – Specifies the name of the user-defined service. The length is 1 to 31 characters. The name must be unique in the entire system. After executing the command, the CLI will enter the configuration mode of created service.

If you need to enable the long connection, in the global mode, use the longlife-sess-percent command to configure the percent of long connection. The default value is 0.

Adding/Deleting a User-defined Service Entry

Each user-defined service can contain up to 8 service entries. The command that is used to add a service entry may vary from different protocol types of the service entries.

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

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

- **dst-port** *min-port* [*max-port*] – Specifies the destination port number of the user-defined service. If the destination port number is a number range, then *min-port* is the minimum destination port number, and *max-port* is the maximum destination port number. The value range is 0 to 65535, and the destination port number should not be a single 0. For example, the destination port number can be 0 to 20, but cannot only be 0.
- **src-port** *min-port* [*max-port*] – Specifies the source port number of the user-defined service. If the source port number is a number range, then *min-port* is the minimum source port number, and *max-port* is the maximum source port number. The value range is 0 to 65535.
- **timeout** *time-out-value* – Specify the timeout value. The unit is second. The value varies from 1 to 65525. The connection will disconnect after the timeout.
- **timeout-day** *time-out-value* – Specify the timeout value of the persistent connection. The unit is day. The value varies from 1 to 1000. The connection will disconnect after the timeout. You need to set the persistent connection percent before configuring the timeout value of the persistent connection in the global mode.

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

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

- *type-value* – Specifies the ICMP type value of the user-defined service. The value range is 3 (Destination-Unreachable), 4 (Source Quench), 5 (Redirect), 8 (Echo), 11 (Time Exceeded), 12 (Parameter Problem), 13 (Timestamp), 15 (Information) and any (all the above type values).
- **code** *min-code* [*max-code*] – Specifies the ICMP code value for the user-defined service. The value range is 0 to 5.
- **timeout** *time-out-value* – Specify the timeout value. The unit is second. The value varies from 1 to 65525. The connection will disconnect after the timeout.

- **timeout-day** *time-out-value* – Specify the timeout value of the persistent connection. The unit is day. The value varies from 1 to 1000. The connection will disconnect after the timeout. You need to set the persistent connection percent before configuring the timeout value of the persistent connection in the global mode.

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

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

- *protocol-number* – Specifies the protocol number of the user-defined service. The value range is 1 to 255.
- **timeout** *time-out-value* – Specify the timeout value. The unit is second. The value varies from 1 to 65525. The connection will disconnect after the timeout.
- **timeout-day** *time-out-value* – Specify the timeout value of the persistent connection. The unit is day. The value varies from 1 to 1000. The connection will disconnect after the timeout. You need to set the persistent connection percent before configuring the timeout value of the persistent connection in the global mode.

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

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

Configuration Example

The goal is to create a user-defined service named my-service, and add the following 3 service entries to my-service:

- A service of TCP type, the destination port is 2121, and the source port is 80.
- A service of ICMP type, the type is 8, the code is 0.
- A service of other types, the protocol number is 47.

Use the following commands:

```
hostname(config)# service my-service

hostname(config-service)# tcp dst-port 2121 src-port 80
hostname(config-service)# icmp type 8 code 0
hostname(config-service)# protocol 47
hostname(config-service)# exit
hostname(config)#
```

Service Group

You can organize some services together to form a service group, and apply the service group to FSOS policies directly. The service group of FSOS 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 FSOS supports up to 8 layers of nests.

The service group also has the following limitations:

- Service and service group should not use the same name.
- The service group being used by any policy cannot be deleted. To delete such a service group, you must first end its association with other modules.
- If a user-defined service is deleted from the service group, the service will also be deleted from all the service groups using it.

Creating/Deleting a Service Group

To create a service group and add the service group to the service book via CLI, in the global configuration mode, use the following command:

servgroup *servicegroup-name*

Note:The name of the service group must be unique.

After executing this command, the CLI will enter the service group configuration mode.

To delete a service group, in the global configuration mode, use the following command:

no servgroup *servicegroup-name*

Adding/Deleting a Service/Service Group

The member of the service group can be either a service or a service group. To add a service to the service group or delete a service from the service group, in the service group configuration mode, use the following commands:

service {*service-name* | *servicegroup-name*}

no service {*service-name* | *servicegroup-name*}

When adding a service or service group to the service group, note that:

- Service in the service group must be unique.
- Each service group can contain up to 64 services; one service group supports up to 8 layers of nests of another service group.

Adding/Deleting Description to a Service/Service Group

To add description to a service/service group, in the service/service group configuration mode, use the following command:

description *description*

- *description* – Specifies the description of the service/service group.

Use no description to delete the description information.

Application Overview

Application has some specific features, like corresponding protocol, port number, application type, etc. Application is an essential element for the configuration of multiple FSOS modules including policy rules, NAT rules, application QoS management, etc. FSOS ships with over 100 predefined services and over 20 predefined application group. Besides, you can also customize user-defined application and application groups as needed. All these applications and application groups are stored in and managed by FSOS application book.

If IPv6 is enabled, IPv6 applications will be recognized by FSOS.

Predefined Application

FSOS provides more than 100 predefined applications. You can view all the supported predefined applications by using the **show application predefined** command.

Predefined Application Groups

The predefined application group includes some associated predefined applications to facilitate users' configuration. Upgrading the signature database will dynamically identify the predefined applications. Currently, FSOS provides more than 20 predefined application groups. You can view and use the predefined application groups, but cannot delete or edit them.

> Tip: For more information about upgrading signature database and dynamical identification, see Application Identification.

Userdefined Application

Besides the above predefined applications, you can also create your own user-defined applications. By configuring the customized application signature rules, FSOS can identify and manage the traffic that crosses into the device, thus identifying the type of the traffic.

Configurations of user-defined application groups include the following items:

- Create/delete the user-defined applications
- Create/delete the application signature rules
- Configure the entry of the application signature rule
- Configure the application timeout value
- Modify the order of the user-defined application signature

Creating/Deleting the User-defined Applications

To create a user-defined application and add this newly-created one to the application book, use the following command in the global configuration mode:

application *application-name*

After executing this command, the system enters the application configuration mode.

To delete the user-defined application, use the following command:

no application *application-name*

Enabling the User-defined Application Signature Configuration Mode

To enable the user-defined application signature configuration mode, use the following command in the global configuration mode:

app-signature

Creating/Deleting the User-defined Application Signature Rule

System supports create an user-defined application signature rule in two configuration mode:

- User-defined application signature configuration mode: Configure all signatures of an user-defined application.
- Application signature rule configuration mode: Configure any signature of an user-defined application.

Configuring Rules in User-defined Application Signature Configuration Mode

In user-defined application signature configuration mode, use the following command:

signature from { *src-addr* | *src-ip* } **to** { *dst-addr* | *dst-ip* } **protocol** {**tcp** | **udp**} **dst-port** *min-port* [*max-port*] [**src-port** *min-port* [*max-port*]] **application** *application-name*

- *src-addr* − Specifies the source addresses of the **address entry** type.
- *src-ip* − Specifies the source addresses of the **member IP** type.
- *dst-addr* − Specifies the source addresses of the **address entry** type.
- *dst-ip* − Specifies the source addresses of the **member IP** type.
- **dst-port** *min-port*[*max-port*] − Specify the destination port number of the user-defined application signature. If the destination port number is within a range, FSOS will identify the value of *min-port* as the minimum port number and identify the value of *max-port* as the maximum port number. The range of destination port number is 0 to 66535. The port number cannot be 0. For example, the destination port number is in the range of 0 to 20, but it cannot be 0.
- **src-port***min-port* [*max-port*] − Specify the source port number of the user-defined application signature. If the source port number is within a range, FSOS will identify the value of *min-port* as the minimum port number and identify the value of *max-port*as the maximum port number. The range of source port number is 0 to 66535.
- *application-name* − Specifies the application name of the signature rule.

Configuring Rules in Application Signature Rule Configuration Mode

In the user-defined application signature configuration mode, use the following command to create a user-defined application signature rule and enter the application signature rule configuration mode. If the specified ID already exists, the system will enter the application signature rule configuration mode.

signature id *id*

To delete this user-defined application signature rule, use the following command in the user-defined application configuration mode:

```
no signature id id
```

Configuring the Entry of the User-defined Application Signature Rule

A user-defined application signature rule can contain multiple signature rule entries. The logical relationship between each entry is **AND**. **AND** represents that FSOS can identify the traffic type when the traffic satisfies all entries in this user-defined application signature rule.

Configuring the entry of the user-defined application signature rule includes the following sections:

- Source security zone
- Source/destination IP address
- Source/destination port number of applications of TCP type or UDP type; The type value and the code value of applications of ICMP type
- Application name

To specify the source security zone of the signature rule, use the following command in the application signature rule configuration mode:

```
src-zone zone-name
```

- *zone-name* – Specifies the name of the source security zone.

To specify the source address of the **address entry** type, use the following command in the application signature rule configuration mode:

```
src-addr src-addr
```

- *src-addr* – Specifies the source addresses of the **address entry** type.

To specify the source address of the **member IP** type, use the following command in the application signature rule configuration mode:

```
src-ip src-ip
```

- *src-ip* – Specifies the source addresses of the **member IP** type.

To specify the destination address of the **address entry** type, use the following command in the application signature rule configuration mode:

dst-addr *dst-addr*

- *dst-addr* − Specifies the source addresses of the **address entry** type.

To specify the destination address of the **member IP** type, use the following command in the application signature rule configuration mode:

dst-ip *dst-ip*

- *dst-ip* − Specifies the source addresses of the **member IP** type.

For the application signature of TCP type or UDP type, specify the type and corresponding parameters using the following command in the application signature rule configuration mode:

protocol {**tcp** | **udp**} **dst-port** *min-port* [*max-port*] [**src-port** *min-port* [*max-port*]]

- **dst-port***min-port* [*max-port*] − Specify the destination port number of the user-defined application signature. If the destination port number is within a range, FSOS will identify the value of *min-port* as the minimum port number and identify the value of *max-port* as the maximum port number. The range of destination port number is 0 to 66535. The port number cannot be 0. For example, the destination port number is in the range of 0 to 20, but it cannot be 0.
- **src-port***min-port* [*max-port*] − Specify the source port number of the user-defined application signature. If the source port number is within a range, FSOS will identify the value of *min-port* as the minimum port number and identify the value of *max-port* as the maximum port number. The range of source port number is 0 to 66535.

For the application signature of ICMP type, specify the type and corresponding parameters using the following command in the application signature rule configuration mode:

protocol icmp type *type-value* [**code** *min-code* [*max-code*]]

- *type-value* − Specifies the value of the ICMP type of the application signature. The options are as follows: 3 (Destination-Unreachable), 4 (Source Quench)， 5 (Redirect), 8 (Echo), 11 (Time Exceeded), 12 (Parameter Problem), 13 (Timestamp), 15 (Information), and any (any represents all above values).
- **code** *min-code* [*max-code*] − Specifies the value of the ICMP code of the application signature. The ICMP code is in the range of 0 to 5. The default value is 0-5.

For the application signature of other types, use the following command in the application signature rule configuration mode:

protocol other-protocol *protocol-number*

- *protocol-number* – Specifies the protocol number of the application signature. The protocol number is in the range of 1 to 255.

To specify the application name of the signature rule, use the following command in the application signature rule configuration mode :

application *application-name*

- *application-name* – Specifies the application name of the signature rule.

To delete the signature rule, use the no form of the above commands. For the existing signature rules, you cannot edit them but can delete them.

Configuring the Application Timeout Value

You can configure the application timeout value. If not, FSOS will use the default value of the protocol. To configure it, use the following command in the application configuration mode:

timeout {**tcp** | **udp** | **icmp** | **other-protocol**} *timeout-value*

- **tcp** | **udp** | **icmp** | **other-protocol** – Specifies the protocol type.
- *timeout-value* – Specifies the timeout value of the application. The range is 1 to 864,000.

Modifying the Order of the User-defined Application Signature Rule

Each user-defined application signature rule has a unique ID. When traffic flows into the device, FSOS will search the user-defined application signature rule in the order of priority to see which signature rule matches the traffic. Once the traffic satisfies a specific application signature rule, FSOS will process the traffic according to this matched rule. The order of searching signature rule is not related to the order of the signature ID but the order of priority. To view the order of priority, use the **show app-signature static** command. And then FSOS will list all application signatures according to the priority. The signature rule with the highest priority will be listed at the top and the signature rule with the lowest priority will be listed at the bottom. When you create a signature rule, you can specify its priority. And you can also modify its priority in the user-defined application signature configuration mode. You can adjust the priority of the signature rule to be at the top or at the bottom or between two signature rules. To modify the priority, use the following command in the user-defined application signature configuration mode:

move *id* {**top** | **bottom** | **before** *id* | **after** *id*}

User-defined Application Group

An application group contains multiple applications. You can apply the application group to the policy. An application group has the following features:

- Each application in the application book can be used in one or more application groups.
- Each application group can contain predefined applications and user-defined applications.
- Each application group can contain one or more application groups. FSOS supports the nested application group. An application group within an application group can continue referencing one or more application groups. FSOS can support up to 8-level nested application groups.

An application group also has its restrictions:

- The names of an application group and an application cannot be identical.
- The application group referenced by the policy cannot be deleted. To delete an application group, make sure that no module references this application group.
- When you delete an application from the application book, this application will also be deleted from the application groups that contain this application group.

Creating/Deleting an Application Group

To create an application group and add it to the application book, use the following command in the global configuration mode:

application-group *application-group-name*

Note: Make sure the application group name is unique in FSOS.

After executing this command, the system enters the application group configuration mode.

To delete an application group, use the following command in the global configuration mode:

no application-group *application-group-name*

Adding/Deleting an Application or Application Group

An application group can contain applications or application groups. To add an application to an application group, use the following command in the application group configuration mode:

application {*application-name* | *application-group-name*}

Note the following matters when adding an application:

- The application in the application group must be unique.
- Each application group can contain up to 64 applications and support up to 8-level nested application groups.

To delete an application or application group from an application group, use the following command in the application group configuration mode:

```
no application { application-name | application-group-name}
```

Adding/Deleting a Description for an Application or Application Group

In the application configuration mode or the application group configuration mode, you can use the following command to add the description:

```
description description
```

- *description* – Specify the description for the application or application group. You can enter up to 255 characters.

In the application configuration mode or the application group configuration mode, use the following command to delete the corresponding description:

```
no description
```

Application Identification

A number of functional modules in the system process data stream based on the type of application (to view the mapping relationship between Application IDS and Application names, use the command **show application list**), for example, stat-set and QoS. Therefore, system needs to identify the data stream first, and then implements the statistics and management functions based on the identification result (Application ID) and configuration.

Dynamic Identification

Dynamic identification allows the system to identify an application automatically by its signature. The automatic identification of application is based on the security zone. By default, the automatic identification function of all the security zones is disabled. To enable the dynamic identification function of a security zone, in the security zone configuration mode, use the following command:

```
application-identify
```

With dynamic identification enabled, the system will identify all the supported dynamically identified application. To view the identified session information, use the command show session. To disable the dynamic identification functions of a security zone, in the security zone configuration mode, use the following command:

```
no application-identify
```

Even if the automatic identification function of a security zone is disabled, the system can still identify some specific applications if being configured with appropriate policy rules. For example, to identify QQ, configure the following two rules (take policy rules from the zone untrust to the zone trust as the example):

```
hostname(config)# policy-global

hostname(config-policy)# rule from any to any application QQ permit

Rule id 5 is created

hostname(config-policy)# rule from any to any application any permit

Rule id 6 is created

hostname(config-policy)# exit

hostname(config)#
```

Application Identification Cache Table

Application identification cache table can store application information to provide support for application identification and PBR. The system supports dynamic and static application identification cache tables.

- Dynamic application identification cache table: stores application information that is dynamically learned (the result of dynamic application identification).
- Static application identification cache table: stores static application information. This table is included in the application signature database.

You can configure application cache tables as needed for different scenarios.

Enabling/Disabling Application Identification Cache Table

Both the dynamic and static application identification cache tables are enabled by default. If the dynamic application identification cache table is disabled, the system will still write entries to the table, but will not identify any application based on the entries in the table. The static application identification cache table will not take effect unless the dynamic application identification cache table is enabled, i.e., disabling the dynamic application identification cache table will also disable the static application identification cache table.

To disable/enable the dynamic application identification cache table, in the global configuration mode, use the following commands:

- Disable: **app cache disable**
- Enable: **no app cache disable**

To disable/enable the static application identification cache table, in the global configuration mode, use the following commands:

- Disable: **app cache static disable**
- Enable: **no app cache static disable**

Specifying a Working Mode for the Dynamic Application Identification Cache Table

To specify a working mode for the dynamic application identification cache table, in the global configuration mode, use the following command:

```
app cache {cache-strict | response-check | pbr-check-strict}
```

- **cache-strict** – Applicable for SNAT scenarios (Intranet users visit Internet via NAT devices). In such a scenario, enabling this option can effectively evade false positive. This option is disabled by default.
- **response-check** – When the system is possibly subjected to single-directional packet attacks, this option is recommended to assure the accuracy of application identification. This option is disabled by default.
- **pbr-check-strict** – Specifies the application identification method for PBR. By default even if the system has already identified the application in PBR based on dynamic application identification cache table, it will still go on with the identification procedure and select a policy-based route based on the final identification result. With this option enabled, the system will not go on with the identification procedure once the application is identified based on the dynamic application identification cache table, and will directly select a policy-based route based on the above identification result.

To cancel the above configuration, in the global configuration mode, use the following command:

```
no app cache {cache-strict | response-check | pbr-check-strict}
```

Clearing the Application Identification Cache Table

To clear all the entries in the dynamic application identification cache table, in any mode, use the following command:

clear app cache table

To clear all the entries in the static application identification cache table, in any mode, use the following command:

clear app cache table static

Viewing Application Identification Cache Table Information

To view if the dynamic or static application identification cache table is enabled and related configuration information, in any mode, use the command **show app cache status**.

Updating the Signature Database

Applications are updated frequently. FS devices allow you to update the application signature database to assure the devices can adapt to these changes in time and identify the latest software version. You can download the latest signature file and upload to the device. FS regularly uploads new signature files on the FS website. You need to download the files, and then upload them to the device.

To upload the signature file via CLI, in the execution mode, use the following command:

import application-signature from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address*} *file-name*

- *ip-address* – Specifies the name of the FTP or TFTP server.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP server.
- *file-name* – Specifies the name of the signature file that will be uploaded.

After uploading the signature file, restart the device if new application is added; do not restart if there is no new application and only existing applications are updated.

Specifying a HTTP Proxy Server

When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update automatically and normally.

To specify the HTTP proxy server for the application signature database updating, use the following command in the global configuration mode:

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

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

To cancel the proxy server configurations, use the **no app update proxy-server** {**main** | **backup**} command.

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.

Configure the application filter group as follows:

1. To create a application filter group
2. To specify application category
3. To specify application subcategory
4. To specify application technology
5. To specify risk value for application
6. To specify characteristic for application

Creating Application Filter Group

To create an application filter group, in the global configuration mode, use the following commands:

application-filter *filter-name*

- *filter-name* – Specifies a name for the application filter group.

Use **no application-filter** *filter-name* to delete the application filter group.

Specifying Application Category

To specify application category, in the application-filter-group configuration mode, use the following commands:

category *category-type*

- *category-type* – Specifies the category type for the application filter group.

Use **no category** *category-type* to delete the category type.

Specifying Application Subcategory

To specify application subcategory, in the application-filter-group configuration mode, use the following commands:

subcategory *subcategory-type*

- *subcategory-type* – Specifies the subcategory type for the application filter group.

Use **no subcategory** *subcategory-type* to delete the subcategory type.

Specifying Application Technology

To specify application technology, in the application-filter-group configuration mode, use the following commands:

technology *technology-type*

- *technology-type* – Specifies the technology type for the application filter group.

Use **no technology** *technology-type* to delete the technology type.

Specifying Risk Value for Application

To specify the risk value, in the application-filter-group configuration mode, use the following commands:

risk *risk-value*

- *risk-value* – Specifies the application risk value. The range is from 1 to 5. 5 means the highest risk.

Use **no risk** *risk-value* to delete the risk value.

Specifying Application Characteristics

To specify the application characteristics, in the application-filter-group configuration mode, use the following commands:

- Specifies "evasive" attributes: **evasive** [**yes** | **no**]
- Specifies "excessive bandwidth" attributes: **excessive-bandwidth** [**yes** | **no**]
- Specifies "file transfer" attributes: **file-transfer** [**yes** | **no**]
- Specifies "known vunerabilities" attributes: **known-vunerabilities** [**yes** | **no**]
- Specifies "prone to misuse" attributes: **prone-to-misuse** [**yes** | **no**]

- Specifies “tunnels other apps” attributes: **tunnels-other-apps** [**yes** | **no**]
- Specifies “used by malware” attributes: **used-by-malware** [**yes** | **no**]
- Specifies “widely used” attributes: **widely-used** [**yes** | **no**]

Configuration Example

In the configuration example, you create an application named my-application and configure the following settings for this application:

- Create a user-defined application signature rule for my-application and specify the ID of the signature as 1.
- Configure the entry of the application signature rule as follows:
  - Source zone: untrust
  - Source address: any
  - Destination address: any
  - Application type: TCP type; destination port number: 2121

See the following detailed commands:

```
hostname(config)# app-signature
hostname(config-appsig)# signature id 1
hostname(config-appsig-rule)# application my-application
hostname(config-appsig-rule)# src-zone untrust
hostname(config-appsig-rule)# src-addr any
hostname(config-appsig-rule)# dst-addr any
hostname(config-appsig-rule)# protocol tcp dst-port 2121
hostname(config-appsig-rule)# exit
hostname(config-appsig)# exit
hostname(config)#
```

After completing the configurations, traffic that satisfies the signature rule 1 will be identified as the application of my-application.

DNS

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

Overview

FS devices' DNS provides the following functions:

- Server: Configures DNS servers and default domain names for the FS device.
- Proxy: The FS device acts as a DNS proxy server and provides proxy service for the connected PCs and other clients. Besides, the FS device can also choose different DNS servers according to domain names.
- Resolver: Sets retry times and timeout for FS device's DNS service.
- Cache: Stores DNS mappings to cache to speed up query.

Configuring a DNS Server

The configuration of DNS server includes:

- Configuring a domain name for the device
- Configuring a DNS domain name server for the device

Configuring a Domain Name

You can specify a domain name for the FS device. The FSOS will append the domain name as a suffix to the incomplete name. For example, if you specify the domain name as yahoo.com, and ping www on the device, then the FSOS will append the domain name to look for www.yahoo.com. In addition, the resolution sequence is different when specifying the domain name to yahoo.com and com: if you specify the domain name as yahoo.com and ping www, the system will first look for www.yahoo.com; if you specify the domain name as com and ping www.yahoo, the system will first look for www.yahoo, and then look for www.yahoo.com.

To specify a domain name, in the global configuration mode, use the following command:

ip domain name *domain-name*

- *domain-name* – Specifies the domain name. The length is 1 to 255 characters, but the maximum length between the two periods (.) is only 63 characters.

To restore to the default domain name, in the global configuration mode, use the command **no ip domain name** .

The following command specifies the default domain name as FSnet.com:

```
hostname(config)# ip domain name FSnet.com
```

Configuring a DNS Domain Name Server

DNS domain name server is used by the FS device to resolve DNS. To specify a DNS domain name server, in the global configuration mode, use the following command:

ip name-server *server-address1* [*server-address2*] ... [*server-address6*] [**vrouter** *vrouter-name*]

- *server-address1* – Specifies the IP address of the domain name server. You can configure up to 6 domain name servers by one command or multiple commands, i.e., running command **ip name-server 1.1.1.1 2.2.2.2** and running commands **ip name-server 1.1.1.1** and **ip name-server 2.2.2.2** make no difference. You can configure up to 64 domain name servers.
- *vrouter-name* – Specifies a DNS server for the specified VRouter.

To cancel the specified DNS domain name server, in the global configuration mode, use the command **no ip name-server** *server-address1* [*server-address2*] ... [*server-address6*].

Configuring a DNS Proxy

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

Each proxy rule is labeled with a unique ID which is automatically generated when the rule is created. You can also specify a proxy rule ID at your own choice. All proxy rules in FSOS are arranged in a specific order. When DNS traffic flows into a FS device, the device will query for proxy rules in the list by turns, and processes the traffic according to the first matched rule.

The configuration of DNS proxy on FS devices includes:

- Configuring a DNS proxy rule
- Moving a DNS Proxy Rule
- Configuring Time Interval of Tracking for DNS Proxy

- Enabling/Disabling Calculating the Checksum of UDP Packet for DNS Proxy
- Specifying the TTL for DNS-proxy Response Packets

Configuring a DNS Proxy Rule

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

- Creating a DNS proxy rule
- Configuring the Filtering Condition of a DNS Proxy rule
- Specifying the Action of a DNS Proxy Rule
- Configuring DNS Proxy Servers
- Enabling/Disabling a DNS Proxy Rule
- Modifying/Deleting the Descriptions of a Proxy Rule

Creating a DNS Proxy Rule

To create a DNS proxy rule or enter the DNS Proxy rule configuration mode, in the global configuration mode, use the following command:

dns-proxy rule [**id** *id*]

- **id** *id* – Specifies the ID of the DNS proxy rule. If not specified, the system will automatically assign an ID to the DNS proxy rule. The ID must be unique in the entire system.

To delete the DNS proxy rule, in the global configuration mode, use the command **no dns-proxy rule id** *id*.

Configuring the Filtering Condition of a DNS Proxy rule

The filtering conditions of a DNS Proxy rule include the ingress interface, source address, destination address and DNS domain name of DNS request. You should configure these four conditions simultaneously, and then system will filter the DNS requests after configuration. Only if the DNS request meets the above four conditions can it is considered a successful match.

Specifying Ingress Interface

You can specify the ingress interface of DNS request in the rule to filter the DNS request message. It is permissible to specify numbers of interfaces. To add or delete the ingress interface of request, in DNS proxy rule configuration mode, use the following command:

- Add the ingress interface of DNS traffic: **ingress-interface** *interface-name*
- Delete the ingress interface of DNS traffic: **no ingress-interface** *interface-name*

Specifying Source Address

You can specify the source address of DNS request in the rule to filter the DNS request message. It is permissible to specify multiple source address filtering conditions. To add or delete the source address of DNS request, in DNS proxy rule configuration mode, use the following command:

- Add the source address of the address entry type: **src-addr** { *addr-name* | **any**}
- Delete the source address of the address entry type: **no src-addr** { *addr-name*| **any**}
- Add the source address of the IP member type: **src-ip** {*ip/netmask* | *ip-address netmask*}
- Delete the source address of the IP member type: **no src-ip** {*ip/netmask* | *ip-address netmask*}
- Add the source address of the IP range type: **src-range** *min-ip max-ip*
- Delete the source address of the IP range type: **no src-range** *min-ip max-ip*

Specifying Destination Address

You can specify the destination address of DNS request in the rule to filter the DNS request message. It is permissible to specify multiple destination address filtering conditions. To add or delete the destination address of request, in DNS proxy rule configuration mode, use the following command:

- Add the destination address of the address entry type: **dst-addr** { *addr-name* | **any**}
- Delete the destination address of the address entry type: **no dst-addr** { *addr-name* | **any**}
- Add the destination address of the IP member type: **dst-ip** {*ip/netmask* | *ip-address netmask*}
- Delete the desalination address of the IP member type: **no dst-ip** {*ip/netmask* | *ip-address netmask*}
- Add the destination address of the IP range type: **dst-range** *min-ip max-ip*
- Delete the destination address of the IP range type: **no dst-range** *min-ip max-ip*

Specifying Domain Name

You can specify the domain name of DNS request in the rule to filter the DNS request message. It is permissible to specify multiple domain name filtering conditions. To add or delete the domain name, in DNS proxy rule configuration mode, use the following command:

domain { **any** | *domain-name* | **host-book** *host-book-entry* }

- *domain-name* - Specifies the domain name that will be matched.
- **any** – Specifies as any domain name that will be matched.
- **host-book** *host-book-entry* – Specifies the name of the host entry that will be matched.

In DNS proxy rule configuration mode ,use the following command to delete the domain name that will be matched:

no domain any | *domain-name* | **host-book** *host-book-entry.*

Specifying the Action of a DNS Proxy Rule

For the DNS request that meets the filtering conditions, system can proxy, bypass and block the traffic. You can specify the action for a DNS proxy rule, in the DNS proxy rule configuration mode, using the following command:

action {**proxy** [**rollback**]| **bypass** | **block**}

- **proxy** [**rollback**] – Specifies the action of a DNS proxy rule as proxy. The DNS request will be resolved through the proxy server. You can configure the **rollback** property as needed. After **rollback** is configured, when there is no DNS server or DNS server unable to resolve the DNS address, system will bypass the DNS request and forward it to the DNS server originally requested by the message.
- **bypass** – Specifies the action of a DNS proxy rule as bypass. That is, the DNS request will be forwarded to the DNS server originally requested by the message.
- **block** – Specifies the action of a DNS proxy rule as block. That is, the DNS request will be discarded.

Configuring DNS Proxy Servers

When the action of the proxy rule is specified as proxy, you need to configure the DNS proxy servers. You can specify up to six DNS server and you can configure the interface and preferred properties for the DNS server as needed. When you configure multiple DNS servers, the DNS server with preferred property will be selected for domain name resolution. If no preferred server is specified, the system will query whether there are DNS servers that have specified the egress interface; If so, select these DNS server in a round robin; Except for the two DNS servers, which means that you only have a regular DNS server, then select this kind of DNS servers in a round robin. To add a DNS proxy server, in the DNS proxy rule configuration mode, use the following command:

name-server *server-ip* [**vrouter** *vrouter-name*| **egress-interface** *interface-name*| **preferred**]

- *server-ip* – Specifies the IP address of the DNS proxy.
- *vrouter-name* – Specifies a VRouter for the DNS proxy.
- *interface-name* – Bind the egress interface to the DNS proxy server. After binding, system will forward the DNS request to the DNS proxy server through this interface.
- *preferred* – Specifies the DNS proxy 4dserver as the preferred server, and a DNS proxy rule can only specify one server as the preferred server.

To delete the DNS proxy server, in the DNS proxy rule configuration mode , use the command **no name-server** *server-ip* [**vrouter** *vrouter-name*].

Modifying/Deleting the Descriptions of a Proxy Rule

In the DNS proxy rule configuration mode, use the following command to modify the description of a rule.

description *description*

- *description* – Specifies the description for the dns proxy rule.

In the DNS Proxy Rule configuration mode, use the command **no description** to delete the description.

Enabling/Disabling a DNS Proxy Rule

DNS proxy rule is enabled by default. To disable or enable the function, in the DNS proxy rule configuration mode, use the following command:

- Disable a DNS proxy rule : **disable**
- Enable a DNS proxy rule: **enable**

Moving a DNS Proxy Rule

Each DNS proxy rule is labeled with a unique ID. When traffic flowing into the FS device, the device will query for DNS proxy rules by turns, and then process the DNS request according to the first matched rule. However, the rule ID is not related to the matching sequence during the query. The sequence displayed by the command show dns-proxy is the query sequence for the matching. You can move a DNS proxy rule to modify the matching sequence. To move a DNS proxy rule, in the global configuration mode, use the following command:

dns-proxy move *rule-id* {**top** | **bottom** | **before** *rule-id* | **after** *rule-id* }

- **move** *rule-id* – Specifies the DNS proxy rule that will be moved.
- **top** – Move the DNS proxy rule to the top of all the rules.
- **bottom** – Moves the DNS proxy rule to the bottom of all the rules.
- **before** *rule-id* – Move the DNS proxy rule before the rule id.
- **after** *rule-id* – Move the DNS proxy rule after the rule id.

Configuring Time Interval of Tracking for DNS Proxy

This function is to track the reach ability of the DNS proxy server. System will periodically detect the DNS proxy server at a specific time interval. When the server cannot be tracked, the IP address of server will be removed from the DNS resolution list until the link is restored. By default, the tracking for DNS proxy server is enabled. To configure the time interval of tracking for DNS proxy server, in the global configuration mode, use the following command:

dns-proxy server-track [**interval** *interval-time*]

- *interval-time* – Specifies the tracking interval time. The value range is 0 to 30 seconds. The default value is 10.

To disable tracking for DNS proxy server, in the global configuration mode, use the following command:

no dns-proxy server-track

Enabling/Disabling Calculating the Checksum of UDP Packet for DNS Proxy

The system will calculate the checksum of UDP packet for DNS proxy when the DNS proxy on interfaces is enabled. If you need to improve the performance of the device, you can disable this function.

To enable/disable calculating the checksum of UDP packet for DNS proxy, in the global configuration mode, use the following command:

- Enable: **dns-proxy udp-checksum enable**
- Disable: **dns-proxy udp-checksum disable**

Specifying the TTL for DNS-proxy Response Packets

TTL refers to the survival time of the DNS records in DNS-proxy server. To specify the TTL of DNS-proxy response packets, in the global configuration mode, use the following command:

dns-proxy ttl *ttl-time*

- *ttl-time* – Specifies the TTL for DNS-proxy's response packets. If the DNS-proxy requests are not responded after the TTL, the DNS client will clear all DNS records. The value range is 30 to 600 seconds. The default value is 60.

To disable this function, in the global configuration mode, use the command **dns-proxy ttl disable**.

Viewing the DNS Proxy Rule

To view the DNS proxy rule in details, in any mode, use the following command:

show dns-proxy [**rule id** *rule-id*]

- *rule-id* – Shows the details of the specified DNS proxy rule. If it's not specified, all DNS proxy rules will be displayed.

Resolution

Users can specify the retry times and timeout of DNS requests for the DNS function of FS devices, TTL for the DNS-proxy response packets and DNS load balancing.

Specifying the Timeout of DNS Requests

FSOS will wait for DNS server's response after sending the DNS request, and will send the request again if no response returns after a specified time. The period of waiting for response is known as timeout. To specify the timeout of DNS requests, in the global configuration mode, use the following command:

ip domain timeout *timeout-value*

- *timeout-value* – Specifies the timeout value. The value range is 1 to 3 seconds. The default value is 2.

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

Specifying the Retry Times of DNS Requests

If the DNS request is not responded after timeout, FSOS will send the request again; if still not responded after the specified retry times (i.e., the repetition times of the DNS request), FSOS will send the request to the next DNS server. To specify the retry times, in the global configuration mode, use the following command:

```
ip domain retry times
```

- *times* – Specifies the retry times. The value range is 1 to 3 times. The default value is 2.

To restore to the default retry times, in the global configuration mode, use the command **no ip domain retry**.

Specifying the TTL for DNS Resolution Dynamic Cache

TTL refers to the survival time of the DNS domain name resolution dynamic cache. To specify the TTL of DNS resolution dynamic cache, in the global configuration mode, use the following command:

```
ip domain ttl ttl-time
```

- *ttl-time* – Specifies the TTL for DNS resolution dynamic cache. If the DNS resolution dynamic cache are not responded after the TTL, the system will clear all domain name records. The value range is 60 to 600 seconds. The default value is 60.

Enabling the DNS Resolution Log

You can enable the DNS resolution log function to record the result of DNS resolution, and generate the log information, the log content including the domain name, IP address of the DNS and generation time. By default, the function is closed. To enable the DNS resolution log function, in the global configuration mode, use the following command:

```
ip domain response-log
```

To disable the DNS resolution log function, in the global configuration mode, use the command **no ip domain response-log**.

DNS Cache

When using DNS, a system might store the DNS mappings to its cache to speed up the query. There are 3 ways to obtain DNS mappings:

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

You can add static DNS mappings to cache, view DNS mappings and delete dynamic mappings.

Adding a Static DNS Mapping

To manually add a DNS mapping to the cache, in the global configuration mode, use the following command:

ip host *host-name* {*address1* [*address2*] ... [*address8*]} [**vrouter** *vrouter-name*]

- *host-name* – Specifies the host name. The length is 1 to 255 characters.
- {*address1* [*address2*] ... [*address8*]} – Specifies the IP Address of the host. You can specify up to 8 IP addresses.
- *vrouter-name* – Specifies the VRouter for the host.

To delete the specified DNS mapping, in the global configuration mode, use the command **no ip host** *host-name*.

Viewing a DNS Mapping

To view a DNS mapping, in any mode, use the following command:

show ip hosts [*host-name*] [**vrouter** *vrouter-name*]

- *host-name* – Shows the DNS mapping of the specified host.
- *vrouter-name* - Shows the DNS mapping of the specified VRouter.

Deleting a Dynamic DNS Mapping

To manually remove a dynamic DNS mapping, in the execution mode, use the following command:

clear host [*host-name* [**vrouter** *vrouter-name*]]

- *host-name* – Deletes the DNS mapping of the specified host.
- *vrouter-name* – Deletes the host DNS mapping of the specified VRouter.

This command is used to delete the specified or all the dynamic DNS mappings. To delete the static DNS mappings that are manually added, use the command **no ip host**.

DNS Snooping

System will monitor the DNS response packets after the DNS proxy function is enabled. And it will create a snooping list when finding the packets which are match with the wildcard host including the host name contains the wildcard, domain name, age time, IP address and VRouter name. etc. Meanwhile the system will send the IP addresses in the snooping list to the address book. The device can access to the host according to specified links through referencing address book in a PBR rule.

Note: Before using this function, please make sure the DNS proxy function is enabled, the host name contains the wildcard and the TTL of the DNS-proxy response packets are configured. see Configuring a DNS Proxy

Specifying the Age Time for DNS Snooping Lists

System will clear call records in the DNS snooping lists when reaching the age time. In the global configuration mode, use the following command:

ip dns-resp-snooping ttl *ttl-time*

- *ttl-time* – Specifies the age time for DNS snoop list. The value range is 60 to 86400 seconds. The default value is 86400. Bigger value is suggested.

Enabling the Specific Domain Name Detection

When the DNS traffic flows through the device, system supports the function of specific domain name detection function. When the function is enabled, system will detect the DNS response packets, try to match the domain name of packets with that in the address book, and then record and issue the IP address of the matched domain name to the address book. By default, the specific domain name detection function is disabled. When the function is disabled, system will initiate a DNS request and get the IP address of corresponding domain name after resolution.

To enable the specific domain name detection, in the global configuration mode, use the following command:

ip dns-resp-snooping enable-specific

To disable the specific domain name detection, in the global configuration mode, use the **no ip dns-resp-snooping enable-specific** command.

Specifying the DNS Packet Rate Limit

You can configure the receiving rate of the DNS response packets. If the number of DNS response packets received per second exceeds the specified value, the system will drop the exceeded packets. In the global configuration mode, use the following command to configure DNS packet rate limit value:

ip dns-resp-snooping pak-limit *packet-limit*

- *packet-limit* – Specifies the number of DNS’ s response packets receiver per second. The value range is 0 to 4294967295. The default value is 0, i.e., no rate limit.

Viewing the DNS Snooping list

To view the specified DNS snooping list entry, in any mode, use the following command:

show ip dns-resp-snooping [**host**] [**vrouter** *vrouter-name*]

- *host* − Specifies the host name, system supports to specify names contained the wildcard or specific domain name. If this parameter is not specified, system will show you all DNS response packets.
- *vrouter-name* − Specifies the VRouter name.

To view the specified or wildcard DNS snooping list entry, in any mode, use the following command:

show dp-dns-resp-snooping {**specific** | **wildcard**} [*host*] [**vrouter** *vrouter-name*]

- **specific** − To view the specified DNS snooping list entry.
- **wildcard** - To view the wildcard DNS snooping list entry.
- *host* − Specifies the host name, system supports to specify names contained the wildcard or specific domain name. If this parameter is not specified, system will show you all DNS response packets.
- **vrouter** *vrouter-name* − Specifies the VRouter name.

To view the specified and wildcard DNS snooping list entry, in any mode, use the following command:

show dp-dns-resp-snooping all [**vrouter** *vrouter-name*]

- **vrouter** *vrouter-name* − Specifies the VRouter name.

To clear all or the specified DNS snooping list entry, in any mode, use the following command:

clear dns-resp-snooping [*host*] [**vrouter** *vrouter-name*]

- *host* − Specifies the host name, system supports to specify names contained the wildcard or specific domain name. If this parameter is not specified, system will show you all DNS response packets.
- *vrouter-name* − Specifies the VRouter name.

Enabling/Disabling DNS

By default, DNS is disabled on FS devices. To enable/disable the DNS function, in the global configuration mode, use the following commands:

- Enable: **ip domain lookup**
- Disable: **no ip domain lookup**

Viewing DNS configuration information

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

```
show dns
```

DNS Configuration Example

This section describes a typical DNS configuration example.

Requirement

The FS device allows PC1 within the trust zone to access Internet via DNS proxy. The IP address of DNS server in the public network is 202.106.0.20; the IP address of the device's ethernet0/0 interface is 192.168.10.1/24; the IP address of PC1 in the trust zone, which is connected to the above interface, is 192.168.10.3/24; the IP address of ethernet0/1 interface, which is connected to the public network in the untrust zone, is 10.160.65.31/24.

Configuration Steps

Step 1: Bind security zones and configure IP addresses for FS device's interfaces

```
hostname# configure
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.10.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.160.65.31/24
hostname(config-if-eth0/1)# exit
```

Step 2: Configure DNS proxy rule on the FS device

```
hostname(config)# dns-proxy rule
hostname(config-dns-proxy-rule)# ingress-interface ethernet0/0
hostname(config-dns-proxy-rule)# src-addr any
hostname(config-dns-proxy-rule)# dst-addr any
hostname(config-dns-proxy-rule)# domain any
hostname(config-dns-proxy-rule)# action proxy
hostname(config-dns-proxy-rule)# name-server 202.106.0.20
hostname(config-dns-proxy-rule)# exit
```

Step 3: ping www.sina.com.cn. This address can be resolved on PC1

DDNS

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

In order to enable DDNS, you will have to register in a DDNS provider to obtain a dynamic domain name. FS devices support the following 5 DDNS providers:

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

Visit one of the above websites to complete registration.

Configuring DDNS

When the IP address of the interface connecting to the external network changes, the FS device will send an update request to the DDNS server (over HTTP) to update the IP address and the binding domain. You can configure different DDNS names, then configure DDNS parameters for the DDNS names (such as the update method, DDNS server and update interval), and finally bind the configured DDNS names to interfaces to enable the DDNS function.

This section describes the following configurations:

- Configuring a DDNS name
- Binding the DDNS name to an interface

Configuring a DDNS Name

The DDNS service parameters need to be configured in the DDNS name configuration mode. To create a DDNS name, specify the type of update and enter the specified DDNS service configuration mode, in the global configuration mode, use the following command:

ddns name *ddns-name* **type http**

- *ddns-name* – Specifies the DDNS name.
- **type http** – Specifies how to update the DDNS service, i.e., sending the DDNS update requests over HTTP.

The command leads you into the configuration mode of the specified DDNS name. You can configure DDNS parameters for the DDNS service, including the DDNS provider, DDNS server name and port number, the minimum and maximum update interval, as well as the username and password of the DDNS provider.

To delete the specified DDNS name, in the global configuration mode, use the command **no ddns name** *ddns-name* **type http**.

Specifying the DDNS Provider

FS devices support 5 DDNS servers: 3322.org, Huagai.net, ZoneEdit.com, no-ip.com and dyndns.org. To specify the DDNS provider, in the DDNS name configuration mode, use the following command:

type {**dyndns** | **huagai** | **no-ip** | **qdns** | **zoneedit**}

- **dyndns** - Use dyndns.org as the DDNS provider.
- **huagai** - Use Huagai.net as the DDNS provider.
- **no-ip** - Use no-ip.com as the DDNS provider.
- **qdns** - Use 3322.org as the DDNS provider.
- **zoneedit** - Use ZoneEdit.com as the DDNS provider.

To cancel the specified DDNS provider, in the DDNS name configuration mode, use the command **no type**.

Specifying the DDNS Server Name and Port

Different DDNS servers are configured with different server names and port numbers. To specify the DDNS server name and port number, in the DDNS name configuration mode, use the following command:

server name *server-name* **port** *port-number*

- *server-name* – Specifies the server name for the configured DDNS.
- *port-number* – Specifies the server port number for the configured DDNS. The value range is 1 to 65535.

To cancel the specified DDNS server name and port number, in the DDNS name configuration mode, use the command **no server**.

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

Specifying the Minimum Update Interval

When the IP address of the interface with DDNS enabled changes, FSOS will send an update request to the DDNS server. If the request is not responded, FSOS will send the request again according to the configured minimum update interval. For example, if the minimum update interval is set to 5 minutes, then FSOS will send the second request 5 minutes after the first request failure; if it fails again, FSOS will send the request again 10 (5x2) minutes later; and 20 (10x2) minutes later, so and forth. The value will not increase anymore when reaching 120, i.e., FSOS will send the request at a fixed interval of 120 minutes. To configure the minimum update interval, in DDNS name configuration mode, use the following command:

minupdate interval *time-value*

- *time-value* – Specifies the minimum update interval. The value range is 1 to 120 minutes. The default value is 5.

To restore to the default minimum update interval, in DDNS name configuration mode, use the command **no minupdate**.

Specifying the Maximum Update Interval

On the condition that IP address has not changed, FSOS will send an update request to the DDNS server at the maximum update interval. To configure the maximum update interval, in the DDNS name configuration mode, use the following command:

maxupdate interval *time-value*

- *time-value* – Specifies the maximum update interval. The value range is 24 to 8760 hours. The default value is 24.

To restore to the default maximum update interval, in DDNS name configuration mode, use the command **no maxupdate**.

Specifying the DDNS Username/Password

This command is to specify the user information registered in the DDNS provider. To configure the user information, in the DDNS name configuration mode, use the following command:

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

- *user-name* - Specifies the username registered in the DDNS provider.
- *user-password* - Specifies the corresponding password.

To cancel the specified user information, in the DDNS name configuration mode, use the command **no user**.

Binding a DDNS Name to an Interface

The domain names will not be updated according to the configured DDNS parameters upon any interface IP address changes unless the DDNS name is bound to an interface. To bind the DDNS name to an interface, in the global configuration mode, use the following command:

ddns enable *ddns-name* **interface** *interface-name* **hostname** *host-name*

- *ddns-name* – Specifies the DDNS name.
- *interface-name* – Specifies the name of the binding interface.
- *host-name* – Specifies the domain name obtained from the corresponding DDNS provider.

To cancel the specified binding, in the global configuration mode, use the command **no ddns enable** *ddns-name* **interface** *interface-name*.

Viewing DDNS Information

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

- Show the DDNS configuration information: **show ddns config** *ddns-name*
- Show the DDNS state: **show ddns state** *ddns-name*

Example of Configuring DDNS

This section describes a typical DDNS configuration example.

Requirement

The interface ethernet0/1 of the FS device locates at the untrust zone, and the interface obtains IP address by PPPoE. If the IP address changes during PPPoE connection, the interface will send an update request to the DDNS server.

Configuration Steps

Step 1: Create a PPPoE instance named pppoe1

```
hostname(config)# pppoe-client group pppoe1
hostname(config-pppoe-group)# auto-connect 10
hostname(config-pppoe-group)# idle-interval 5
 hostname(config-pppoe-group)# route distance 2
hostname(config-pppoe-group)# route weight 10
hostname(config-pppoe-group)# authentication any
hostname(config-pppoe-group)# user user1 password 123456
hostname(config-pppoe-group)# exit
hostname(config)#
```

Step 2: Configure ethernet0/1

```
hostname# configure
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address pppoe setroute
hostname(config-if-eth0/1)# pppoe enable group pppoe1
hostname(config-if-eth0/1)# exit
```

Step 3: Configure DDNS on the device

```
hostname(config)# ddns name 3322 type http
hostname(config-ddns)# type qdns
hostname(config-ddns)# user test password 123456
hostname(config-ddns)# exit
```

Step 4: Bind ethernet0/1 to the DDNS named 3322 (the domain name obtained from 3322.org is fs.3322.org)

```
hostname(config)# ddns enable 3322 interface ethernet0/1 hostname fs.3322.org
```

Step 5: Configure DNS on the device in order to parse domain names

```
hostname(config)# ip name-server 202.106.0.20
```

Step 6: Launch a PPPoE connection to trigger DDNS when the IP address of the interface changes

```
hostname(config)# pppoe-client group pppoe1 connect
```

DHCP

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

DHCP on FS Devices

FS devices support DHCP client, DHCP server and DHCP relay proxy.

- DHCP client: A FS device's interface can be configured as a DHCP client and obtain IP addresses from the DHCP server.
- DHCP server: A FS device's interface can be configured as a DHCP server and allocate IP addresses chosen from the configured address pool for the connected hosts.
- DHCP relay proxy: A FS device's interface can be configured as a DHCP relay proxy to obtain DHCP information from the DHCP server and forward the information to connected hosts.

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

Configuring a DHCP Client

You can configure an interface of the FS device as the DHCP client that obtains IP address from the DHCP server. The DHCP client should be configured in the interface configuration mode. The configuration includes:

- Obtaining an IP address via DHCP

- Releasing and renewing the IP address
- Configuring the route priority (administration distance) and route weight

Obtaining an IP Address via DHCP

To enable the interface to obtain an IP address via DHCP, in the interface configuration mode, use the following command:

```
ip address dhcp [setroute]
```

- **setroute** – Uses the gateway specified by the DHCP server as the default route gateway.

To cancel the configuration, in the interface configuration mode, use the command **no ip address dhcp**.

For example, to enable etherenet0/1 to obtain the IP address dynamically via DHCP, and set the default gateway route, use the following commands:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address dhcp setroute
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Releasing and Renewing the IP Address

The interface that has obtained a dynamic IP address via DHCP can release and renew its IP address. To release and renew the IP address, in the interface configuration mode, use the following commands:

- Release: **dhcp-client ip release**
- Renew: **dhcp-client ip renew**

To view the DHCP IP address information allocated to an interface, in the interface configuration mode, use the following command:

```
dhcp-client ip show
```

Configuring the Route Priority (Administration distance) and Route Weight

After the DHCP interface is configured with the default route (**ip address dhcp setroute**), to configure the route priority (administration distance) and route weight, in the interface configuration mode, use the following command:

dhcp-client route {**distance** *value*| **weight** *value*}

- **distance** *value* – Specifies the route priority. The value range is 1 to 255. The default value is 1.
- **weight** *value* – Specifies the route weight. The value range is 1 to 255. The default value is 1.

To restore to the default route priory and weight, in the interface configuration mode, use the command **no dhcp-client route** {**distance** | **weight**}.

Enable/ Disable Classless Static Routing Options

After the DHCP interface is configured with the default gateway route (**ip address dhcp setroute**), you can enable the classless static routing function via the DHCP options. When it is enabled, the DHCP client will send a request message with the Option121 (i.e., classless static routing option) to the server, and then the server will return the classless static route information. Finally, the client will add the classless static routing information to the routing table. To enable the classless static routing function via DHCP, in the interface configuration mode, use the following command:

dhcp-client classless-static-route

To disable the function of obtaining classless static route via DHCP, in the interface configuration mode, use the following command:

no dhcp-client classless-static-route

Note:

- The priority of classless static route is higher than the default gateway route, i.e. when the device receives classless static routing options and default gateway routing options at the same time, the device will only add classless static routing information to the routing table.
- By default, it is enabled on interface eth0/0, while it is disabled on other interfaces. You can enable or disable the function on all interfaces.

Viewing DHCP Client Configuration Information

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

show dhcp-client interface {*interface-name*}

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

Configuring a DHCP Server

The FS devices can act as a DHCP server to allocate IP addresses for the DHCP clients in the subnets. The DHCP server should to be configured in the DHCP server configuration mode. To enter the DHCP server configuration mode, in the global configuration mode, use the following command:

dhcp-server pool *pool-name*

- *pool-name* – Specifies the name of the DHCP address pool.

After executing the above command, the system will create a new DHCP address pool and enter the DHCP server configuration mode of the address pool; if the specified address pool exists, the system will directly go to the DHCP server configuration mode:

To delete the specified address pool, in the global configuration mode, use the command **no dhcp-server pool** *pool-name*.

The DHCP server functions you can configure in the DHCP server configuration mode are:

- Basic configuration of the DHCP address pool
- Configuring auto-config
- Configuring DNS/WINS servers and domain name for the DHCP client
- Configuring SMTP/ POP3/news servers for the DHCP client
- Configure the IP address of the relay agent
- IP-MAC Binding
- Configuring option 49

After configuring the DHCP server address pool, you need to bind the DHCP address pool to an interface in order to enable the DHCP server on the interface. For more specific commands, see Binding the Address Pool to an Interface.

In addition, you can view the DHCP configuration of the system anytime by the command **show**.

Basic Configuration of the DHCP Address Pool

This section describes how to configure DHCP address pool.

Configuring an IP Range

You need to specify the IP range used for external allocation. To specify the IP range of the address pool, in the DHCP server configuration mode, use the following command:

address *start-ip-address* [*end-ip-address*]

To cancel the specified IP range, in the DHCP server configuration mode, use the command **no address** *start-ip-address*.

Configuring a Reserved Address

IP addresses in the reserved address, within the IP range of the address pool, are reserved for the DHCP server and will not be allocated. To configure the reserved address, in the DHCP server configuration mode, use the following command:

exclude address *start-ip-address* [*end-ip-address*]

- *start-ip-address* – Specifies the start IP address of the reserved address.
- *end-ip-address* – Specifies the end IP address of the reserved address.

To cancel the specified IP range, in the DHCP server configuration mode, use the command **no exclude address** *start-ip-address*.

Configuring a Gateway

To configure the IP address of the gateway for the client, in the DHCP server configuration mode, use the following command:

gateway *ip-address*

- *ip-address* – Specifies the IP address of the gateway.

To cancel the specified IP address of the gateway, in the DHCP server configuration mode, use the command **no gateway**.

Configuring a Netmask

To configure the netmask for the client, in the DHCP server configuration mode, use the following command:

netmask *netmask*

- *netmask* – Specifies the netmask, such as 255.255.255.0.

To cancel the specified netmask, in the DHCP server configuration mode, use the command **no netmask**.

Configuring a DHCP Lease Time

Lease is the period during which a client is allowed to use an IP address, starting from the time the IP address is allocated. After the lease expired, the client will have to request an IP address again from the DHCP server. To configure the lease of DHCP server, in the DHCP server configuration mode, use the following command:

lease *lease-time*

- *lease-time* – Specifies the lease time. The value range is 300 to 1048575 seconds. The default value is 3600.

To restore to the default lease time, in the DHCP server configuration mode, use the command **no lease**.

Configuring Auto-config

Auto-config is able to function when an interface in a DHCP server configured gateway has been enabled as DHCP client. When auto-config is enabled, if the DHCP server (FS) does not have DNS, WINS or domain name configured, the DHCP client (DHCP) will distribute the DNS, WINS and domain name information obtained from a connected DHCP server to the host that obtains such information from the DHCP server (FS). However, the DNS, WINS and domain name that are configured manually still have the priority. To configure auto-config, in the DHCP server configuration mode, use the following command:

auto-config interface *interface-name*

- *interface-name* – Specifies the interface with the DHCP client enabled on the same device.

To disable the function, in the DHCP server configuration mode, use the command **no auto-config**.

Configuring DNS/WINS Servers and Domain Name for the DHCP Client

To configure DNS, WINS servers and domain name for the DHCP client, in the DHCP server configuration mode, use the following commands:

dns *ip-address1* [*ip-address2*]

- *ip-address1* – Specifies the IP address of the primary DNS server.
- *ip-address2* – Specifies the IP address of the alternative DNS server.

wins *ip-address1* [*ip-address2*]

- *ip-address1* – Specifies the IP address of the primary WINS server.

- *ip-address2* – Specifies the IP address of the alternative WINS server.

domain *domain-name*

- *domain-name* – Specifies the domain name.

To cancel the configured DNS, WINS server and domain name, in the DHCP server configuration mode, use the following commands:

- no dns
- no wins
- no domain

Configuring SMTP/ POP3/news Servers for the DHCP Client

To configure the SMTP, POP3 and news servers for the DHCP client, in the DHCP server configuration mode, use the following commands:

- smtp *ip-address*
- pop3 *ip-address*
- news *ip-address*

To cancel the configured SMTP, POP3 and news servers, in the DHCP server configuration mode, use the following commands:

- no smtp
- no pop3
- no news

Configure the IP Address of the Relay Agent

When the device (FS1) with DHCP server enabled is connected to another device(FS2) with DHCP relay enabled, and the PC obtains FS1's DHCP information from FS2, then only when the relay agent's IP address and netmask are configured on FS1 can the DHCP information be transmitted to the PC successfully. To configure a relay agent, in the DHCP server configuration mode, use the following command:

relay-agent *ip-address netmask*

- *ip-address netmask* – Specifies the IP address and netmask of the relay agent, i.e., the IP address and netmask for the interface with relay agent enabled on FS2.

To cancel the specified relay agent, in the DHCP server configuration mode, use the command **no relay-agent** *ip-address netmask*.

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, in the DHCP server configuration mode, use the following command:

ipmac-bind *ip-address* **mac** [**description** *description*]

- *ip-address* – Specifies the IP address. The IP address must be the address defined in the address pool.
- *mac* – Specifies the binding MAC address.
- **description** *description* – Specifies a description for this IP-MAC binding entry. You can specify up to 63 characters.

To cancel the specified IP-MAC binding, in the DHCP server configuration mode, use the command **no ipmac-bind** *ip-address*.

Binding the Address Pool to an Interface

If the address pool is bound to an interface, the interface will run DHCP server based on the configuration parameters of the address pool. To bind the address pool to an interface, in the interface configuration mode, use the following command:

dhcp-server enable pool *pool-name*

- *pool-name* – Specifies the address pool defined in the system.

To disable the DHCP server on the interface, in the interface configuration mode, use the command **no dhcp-server enable**.

Configuring DHCP Options

When the interface acts as the DHCP server, the system supports the option 43, option 49, option 60, option 66, option 67, option 138, option 150 and option 242.

Configuring Option 43

Option 43 is used to exchange specific vendor specific information (VSI) between DHCP client and DHCP server. The DHCP server uses option 43 to assign Access Controller (AC) addresses to wireless Access Point (AP), and the wireless AP use DHCP to discover the AC to which it is to connect.

Configuring the VSI Carried by Option 43 for DHCP Server

To configure the VSI carried by option 43 for DHCP server, use the following command in the DHCP server configuration mode:

option 43 {**ascii** *value*| **hex** *value*}

- **ascii** *value* – Specify the VSI in ASCII. If the string contains spaces, it must be enclosed in quotes.
- **hex** *value* – Specify the VSI in hex.

To cancel the option 43 settings, use the **no option 43** command.

Note:

- If the VCI matching string has been configured, first of all, you need to verify the VCI carried by the option 60 field in client' s DHCP packets. When the VCI matches the configured one, the IP address, option 43 and corresponding information will be offered. If not, DHCP server will drop client' s DHCP packets and will not reply to the client.
- For verifying VCI carried by option 60, see Verifying VCI Carried by Option 60 section.

Configuring Option 49

To make the DHCP client obtain the list of the IP addresses of systems that are running the X window System Display Manager, configure the option 49 settings. Use the following command to configure the option 49 settings in the DHCP server configuration mode:

option 49 ip *ip-address*

- *ip-address* – Specifies the IP address of the server that is running the X window System Display Manager.

To cancel the option 49 configurations, in the DHCP server configuration mode, use the command **no option 49 ip** *ip-address*.

Configuring Option 60

Option 60 is used by DHCP clients to optionally identify the type and configuration of a DHCP client. The information is a string of n octets, interpreted by servers. Vendors and sites may choose to define specific vendor class identifiers (VCI) to convey particular configuration or other identification information about a client.

You can configure the following functions:

- Verify the VCI carried by the option 60 field in client’s DHCP packets. When the VCI matches the configured one, the IP address and corresponding information will be offered.
- Set the VCI carried by the option 60 for the DHCP server.

Verifying VCI Carried by Option 60

The DHCP server can verify the VCI carried by option 60 in the client’s DHCP packets. When the VCI in client’s DHCP packet matches the VCI matching string you configured in the DHCP server, DHCP server will offer the IP address and other corresponding information. If not, DHCP server will drop client’s DHCP packets and will not reply to the client. If you do not configure a VCI matching string for the DHCP server, it will ignore the VCI carried by option 60. To configure the VCI matching string, use the following command in the DHCP server configuration mode:

vci-match-string {**ascii** *value*| **hex** *value*}

- **ascii** *value* – Specify the VCI matching string in ASCII. If the string contains spaces, it must be enclosed in quotes.
- **hex** *value* – Specify the VCI matching string in hex.

In each specified DHCP server configuration mode, you can only set one VCI matching string. The newly configured VCI matching string will replace the previous one.

To cancel the VCI matching string settings, use the **no vci-match-string** command.

Configuring the VCI Carried by Option 60 for DHCP Server

After configuring the VCI carried by option 60 for DHCP server, the DHCP packets sent by the DHCP server will carry this option and the corresponding VCI. To configure the VCI carried by option 60 for DHCP server, use the following command in the DHCP server configuration mode:

option 60 {**ascii** *value*| **hex** *value*}

- **ascii** *value* − Specify the VCI in ASCII. If the string contains spaces, it must be enclosed in quotes.
- **hex** *value* − Specify the VCI in hex.

To cancel the option 60 settings, use the **no option 60** command.

Configuring Option 66

The option 66 is used to configure the TFTP server name option. By configuring Option 66, the DHCP client get the domain name or the IP address of the TFTP server. You can download the startup file specified in the Option 67 from the TFTP server.

To configure option 66, in the DHCP server configuration mode, use the following command:

option 66 {**ascii** *string* | **hex** *value*}

- **ascii** *string* − Specify the domain name or the IP address of the TFTP server in ASCII. The length is 1 to 255 characters, but the maximum length between the two periods (.) is only 63 characters.
- **hex** *value* − Specify the domain name or the IP address of the TFTP server in hex.

To cancel the option 66 configurations, in the DHCP server configuration mode, use the command **no option 66**.

Note: The TFTP server name must start with a letter or number, and cannot end with ”.” (dot). The "-" (hyphen) and"." (dot) cannot appear continuously.

Configuring Option 67

The option 67 is used to configure the startup file name option for the TFTP server. By configuring option 67, the DHCP client can get the name of the startup file.

To configure option 67, in the DHCP server configuration mode, use the following command:

option 67 {**ascii** *string* | **hex** *value*}

- **ascii** *string* − Specify the startup file name in ASCII. The length is 1 to 255 characters.
- **hex** *value* − Specify the startup file name in hex.

To cancel the option 67 configurations, in the DHCP server configuration mode, use the command **no option 67**.

Configuring Option 138

The Control And Provisioning of Wireless Access Points Protocol (CAPWAP) allows a Wireless Termination Point (WTP) to use DHCP to discover the Access Controllers (AC) to which it is to connect.

The DHCP server uses option 138 to carry a list of 32-bit (binary) IPv4 addresses indicating one or more CAPWAP ACs available to the WTP. Then the WTP discovers and connects to the AC according to the provided AC list.

If you do not set the option 138 for the DHCP server or the DHCP client does not request option 138, DHCP server will not offer the option 138 settings.

To add an AC IP address into the list carried by option 138, use the following command in the DHCP server configuration mode:

option 138 ip *A.B.C.D*

- *A.B.C.D* − Specify the IP address of the AC.

Repeat this command to add multiple ACs. Each DHCP server supports up to 4 ACs.

To cancel the specified AC, use the **no option 138 ip** *A.B.C.D* command.

Configuring Option 150

The option 150 is used to configure the address options for the TFTP server. By configuring option 150, the DHCP client can get the address of the TFTP server.

To configure option 150, in the DHCP server configuration mode, use the following command:

option 150 ip *ip-address*

- *ip-address* − Specify the IP address of the TFTP server. You can configure up to 8 TFTP servers.

To cancel the option 150 configurations, in the DHCP server configuration mode, use the command **no option 150 ip** *ip-address*.

Configuring Option 242

The option 242 is a private DHCP private option for IP phones. By configuring option 242, the specific parameters information of IP phone can be exchanged between DHCP server and DHCP client, such as call server address (MCIPADD), call the server port (MCPORT), the address of the TLS server (TLSSRVR), HTTP (HTTPSRVR) HTTP server address and server port (HTTPPORT) etc.

To configure option 242, in the DHCP server configuration mode, use the following command:

```
option 242 {ascii string | hex value}
```

- **ascii** *string* – Specify the specific parameters of the IP phone in ASCII. The length is 1 to 255 characters.
- **hex** *value* – Specify the specific parameters of the IP phone in hex.

To cancel the option 242 configurations, in the DHCP server configuration mode, use the command **no option 242**.

Viewing DHCP Configuration Information

To view the DHCP address pool binding information or statistics, use one of the following commands:

```
show dhcp-server {binding | pool | statistics} pool-name
```

- **binding** *pool-name* – Shows the binding information of the specified address pool.
- **statistics** *pool-name* – Shows the statistics of the specified address pool.
- **pool** *pool-name* – Shows the information of the specified address pool.

Configuring a DHCP Relay Proxy

The FS device can act as a DHCP relay proxy to receive requests from a DHCP client and send requests to the DHCP server, and then obtain DHCP information from the server and return it to the client. The DHCP relay proxy should be configured in the interface configuration mode. The configurations include:

- Specifying the IP address of the DHCP server
- Enabling DHCP relay proxy on an interface

Specifying the IP Address of the DHCP Server

To specify the IP address of the DHCP server, in the interface configuration mode, use the following command:

```
dhcp-relay server ip-address
```

- *ip-address* – Specifies the IP address of the DHCP server.

To cancel the specified IP address, in the interface configuration mode, use the command **no dhcp-relay server** *ip-address*.

Enabling DHCP Relay Proxy on an Interface

To enable DHCP relay proxy on an interface, in the interface configuration mode, use the following command:

```
dhcp-relay enable
```

To disable the specified DHCP relay proxy, in the interface configuration mode, use the command **no dhcp-relay enable**.

PPPoE

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

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

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

FS devices' interfaces can be configured as PPPoE clients to accept PPPoE connections.

Configuring PPPoE

FS devices allow you to configure multiple PPPoE instances, and then bind the configured PPPoE instances to interfaces. If an interface is configured to obtain its IP address via PPPoE, the interface will launch a PPPoE connection based on the parameters configured in PPPoE instances. The PPPoE configurations include:

- Configuring a PPPoE instance
- Binding the PPPoE instance to an interface
- Obtaining an IP address via PPPoE
- Manually Connecting or Disconnecting PPPoE
- Viewing PPPoE configuration

Configuring a PPPoE Instance

You can configure various PPPoE parameters in the PPPoE instance, including access concentrator, authentication method, PPPoE connection method, netmask, route distance and weight, service, static IP, PPPoE user information, schedule and DNS preference. The PPPoE instances must be configured in the PPPoE instance configuration mode. To enter the PPPoE instance configuration mode, in the global configuration mode, use the following command:

pppoe-client group *group-name*

- *group-name* – Specifies the name of the PPPoE instance. After executing the command, the system will create a new PPPoE instance, and enter the instance configuration mode; if the specified name exists, the system will enter the instance configuration mode directly.

To delete the specified PPPoE instance, in the global configuration mode, use the command **no pppoe-client group** *group-name*.

Specifying the Access Concentrator

To use PPPoE connections, you need to specify the access concentrator first. To specify the access concentrator, in the instance configuration mode, use the following command:

ac *ac-name*

- *ac-name* - Specifies the name of the concentrator.

To cancel the specified access concentrator, in the instance configuration mode, use the command **no ac**.

Specifying the Authentication Method

FS devices will have to pass PPPoE authentication when trying to connect to a PPPoE server. The supported authentication methods include CHAP, PAP and any. The configured authentication must be the same with that configured in the PPPoE server. To specify the authentication method, in the instance configuration mode, use the following command:

authentication {chap | pap | any}

- **chap** - Specifies the authentication as CHAP.
- **pap** - Specifies the authentication as PAP.
- **any** - Specifies the authentication as either CHAP or PAP. This is the default option.

To restore to the default authentication method, in the instance configuration mode, use the command **no authentication**.

Configuring a PPPoE Connection Method

PPPoE supports two connection methods:

- Automatic connection: If the PPPoE connection has been disconnected due to any reasons for a certain period, i.e., the specified re-connect interval, FSOS will try to re-connect automatically.
- On-demand dial-up: If the PPPoE interface has been idle (no traffic) for a certain period, i.e., the specified idle interval, FSOS will disconnect the Internet connection; if the interface requires Internet access, FSOS will connect to Internet automatically.

The above two methods are mutually exclusive. When the schedule is not configured, the system will select the on-demand dial-up by default; if both of the above methods are configured, the system will select the automatic connection.

To specify the re-connect interval, in the instance configuration mode, use the following command:

auto-connect *time-value*

- *time-value* - Specifies the re-connect interval. The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled.

To restore to the default re-connect interval, in the instance configuration mode, use the command **no auto-connect**.

To specify the idle interval, in the instance configuration mode, use the following command:

idle-interval *time-value*

- *time-value* - Specifies the idle interval. The value range is 0 to 10000 minutes. The default value is 30.

To restore to the default idle interval, in the instance configuration mode, use the command **no idle-interval**.

Specifying the Netmask

You can specify the netmask for the IP address obtained via PPPoE. To specify the netmask, in the instance configuration mode, use the following command:

netmask *netmask*

- *netmask* - Specifies the network mask, such as 255.255.255.0.

To cancel the specified netmask, in the instance configuration mode, use the command **no netmask**. After that the system will used the default netmask 255.255.255.255.

Specifying the Route Distance/Weight

To specify the route distance and weight, in the instance configuration mode, use the following command:

route {**distance** *value*| **weight** *value*}

- **distance** *value* – Specifies the route distance. The value range is 1 to 255. The default value is 1.
- **weight** *value* – Specifies the route weight. The value range is 1 to 255. The default value is 1.

To restore to the default route distance and weight, in the instance configuration mode, use the command **no route** {**distance** | **weight**}.

Specifying the Service

To specify the allowed service, in the instance configuration mode, use the following command:

service *service-name*

- *service-name* – Specifies the allowed service. The specified service must be the same with that provided by the PPPoE server. If no service is specified, FS devices will accept any service returned from the server automatically.

To cancel the specified service, in the instance configuration mode, use the command **no service**.

Specifying the Static IP

You can specify a static IP address and negotiate to use this address to avoid IP change. To specify the static IP address, in the instance configuration mode, use the following command:

static-ip *ip-address*

- *ip-address* – Specifies the static IP address.

To cancel the specified static IP address, in the instance configuration mode, use the command **no static-ip**.

Specifying the PPPoE User Information

To specify the PPPoE user information, in the instance configuration mode, use the following command:

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

- *user-name* – Specifies the PPPoE username.
- *password* – Specifies the corresponding password.

To cancel the specified PPPoE user information, in the instance configuration mode, use the command **no user**.

Configuring the Schedule

FS devices support schedules. You can specify a schedule for the PPPoE instance to make the PPPoE interface maintain the Internet connection or disconnect from the Internet during the specified period. To configure the schedule, in the instance configuration mode, use the following command:

schedule *schedule-name* [**disconnect** | **sch-auto-connection** *time-value* | **sch-idle-timeout** *time-value*]

- *schedule-name* – Specifies the name of the schedule.
- **disconnect** – If this keyword is selected, the system will disconnect PPPoE connection during the specified period.
- **sch-auto-connection** *time-value* – If this keyword is selected, the system will connect to the Internet during the specified period automatically. *time-value* is used to specify the re-connect interval. The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled.
- **sch-idle-timeout** *time-value* – If this keyword is selected, the system will dial up to the Internet on demand during the specified period. *time-value* is used to specify the idle interval. The value range is 0 to 10000 minutes. The default value is 30.

To cancel the specified schedule, in the instance configuration mode, use the command **no schedule**.

Tip: For more information about how to create a schedule, see Creating a Schedule of System Management.

Specifying the MAC Address of the PPPoE Server

If the MAC address of the PPPoE server is known, you can specify the MAC address of the PPPoE server so that the FS device can quickly connect to the PPPoE server. To specify the MAC address of the PPPoE server, in the instance configuration mode, use the following command:

mac *mac-address*

- *mac-address* – Specifies the MAC address of the PPPoE server.

To cancel the specified MAC address, in the instance configuration mode, use the command **no mac**.

Configuring Connection Status Detection

To detect the status of the PPPoE connection, you can enable the device to send a LCP Echo request to the PPPoE server. If the device has not yet received response to the request from the PPPoE server after timeout, it will send the request once again; if the retry times reach the specified number, and the device still did not receive any response, then the system will determine the PPPoE server is disconnected, and identify the status of the PPPoE interface as disconnected.

To configure the timeout, in the instance configuration mode, use the following command:

ppp lcp-echo-timeout *timeout-value*

- *timeout-value* – Specifies the timeout value. The value range is 1 to 1000 seconds. The default value is 180.

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

no ppp lcp-echo-timeout

To configure the retry times, in the instance configuration mode, use the following command:

ppp lcp-echo-retries *times*

- *times* – Specifies the retry times. The value range is 1 to 30. The default value is 10.

To restore to the default retry times, in the instance configuration mode, use the following command:

no ppp lcp-echo-retries

Obtaining an IP Address via PPPoE

To enable the interface to obtain an IP address via PPPoE, in the interface configuration mode, use the following command:

ip address pppoe [**setroute**]

- **setroute** – Uses the gateway specified by the PPPoE server as the default route gateway.

To cancel the configuration, in the interface configuration mode, use the command **no ip address pppoe**.

Binding a PPPoE Instance to an Interface

After binding the configured PPPoE instance to an interface, the interface will adopt the parameters of the instance to establish PPPoE connections. To bind the PPPoE instance to an interface, in the interface configuration mode, use the following command:

pppoe enable group *group-name*

- *group-name* – Specifies the name of the PPPoE instance.

To cancel the specified binding, in the interface configuration mode, use the command **no pppoe enable group**.

Manually Connecting or Disconnecting PPPoE

To connect to or disconnect from the PPPoE, in the global configuration mode, use the following command:

pppoe-client group *group-name* {**connect** | **disconnect**}

- *group-name* – Specifies the name of the PPPoE instance.
- **connect** – Connects to PPPoE.
- **disconnect** – Disconnects from PPPoE.

Viewing PPPoE Configuration Information

To view the PPPoE instance parameter information and the connection status, in any mode, use the following command:

show pppoe-client {**all** | **group** *group-name*}

- **all** – Shows the information of all the PPPoE instances.
- **group** *group-name* – Shows the information of the specified PPPoE instance.

Example of Configuring PPPoE

This section describes a typical PPPoE configuration example.

Requirement

The FS device acts as the PPPoE and sends requests to the PPPoE server; the PPPoE server returns response to the client.

Configuration Steps

Step 1: Create a PPPoE instance named pppoe1 and specify the parameters

```
hostname(config)# pppoe-client group pppoe1
hostname(config-pppoe-group)# auto-connect 10
hostname(config-pppoe-group)# idle-interval 5
hostname(config-pppoe-group)# route distance 2
hostname(config-pppoe-group)# route weight 10
hostname(config-pppoe-group)# authentication any
hostname(config-pppoe-group)# user user1 password 123456
hostname(config-pppoe-group)# exit
hostname(config)#
```

Step 2: Enable ethernet0/3 to obtain its IP address via PPPoE, and bind the PPPoE instance to ethernet0/3

```
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone untrust
hostname(config-if-eth0/3)# ip address pppoe setroute
hostname(config-if-eth0/3)# pppoe enable group pppoe1
hostname(config-if-eth0/3)# exit
hostname(config)#
```

Step 3: Create a schedule named schedule1, and enable ethernet0/3 to launch PPPoE connections via on-demand dial-up from 9:00 to 15:30 everyday. The idle time of the on-demand dial-up is 20 minutes

```
hostname(config)# schedule schedule1
hostname(config-schedule)# absolute start 10/15/2007 09:30 end 11/05/2007 15:00
hostname(config-schedule)# periodic daily 09:00 to 15:30
hostname(config-schedule)# exit
hostname(config)# pppoe-client group pppoe1
hostname (config-pppoe-group)# schedule schedule1 sch-idle-timeout 20
hostname (config-pppoe-group)# exit
hostname(config)#
```

NAT

Overview

NAT (Network Address Translation) is a protocol for IP address translation in an IP packet header. When the IP packets pass through a firewall or router, the device or router will translate the source IP address and/or the destination IP address in the IP packets. In practice, NAT is mostly used to allow the private network to access the public network, or vice versa. NAT has the following advantages:

- Helps to solve the problem of IP address resources exhaustion by using a small number of public IP addresses to represent the majority of the private IP addresses.
- Hides the private network from external networks, for the purpose of protecting private networks.

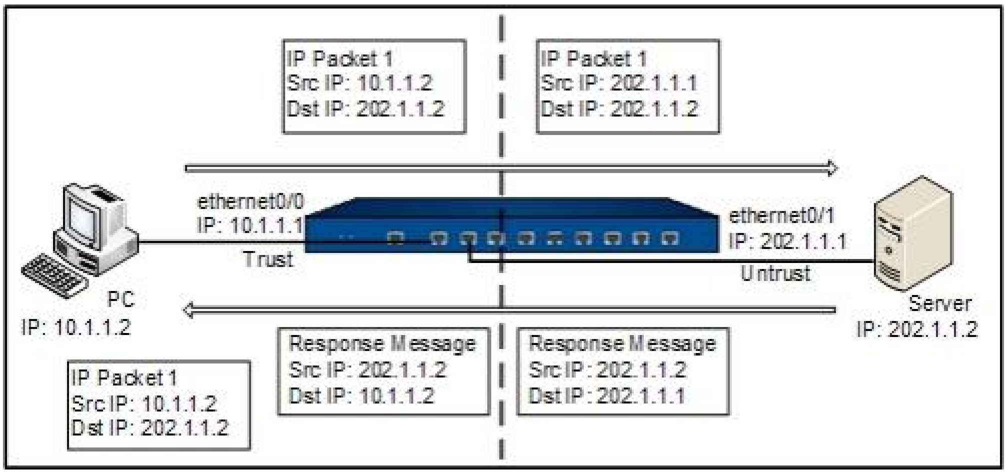
Typically private networks use private IP addresses. RFC1918 defines three types of private IP addresses as follows:

- Class A: 10.0.0.0 - 10.255.255.255 (10.0.0.0 / 8)
- Class B: 172.16.0.0 - 172.31.255.255 (172.16.0.0/12)
- Class C: 192.168.0.0 - 192.168.255.255 (192.168.0.0/16)

IP addresses in the above three ranges will not be allocated on the Internet. You can use those IP addresses in an enterprise network freely without requesting them from an ISP (Internet Service Provider) or registration center.

Basic Translation Process

When a firewall is implementing the NAT function, it locates between the public network and the private network. Figure below illustrates the basic translation process of NAT.



As shown above, the firewall lies between the private network and the public network. When the internal PC at 10.1.1.2 sends an IP packet (IP packet 1) to the external server at 202.1.1.2 through the firewall, the appliance checks the packet header. Finding that the IP packet is destined to the public network, the appliance translates the source IP address 10.1.1.2 of packet 1 to the public IP address 202.1.1.1 which can get routed on the Internet, and then forwards the packet to the external server. At the same time, the appliance also records the mapping between the two addresses in its NAT table. When the response packet of IP packet 1 reaches the firewall, the appliance checks the packet header again and finds the mapping records in its NAT table, then replaces the destination address with the private address 10.1.1.2. In this process, the firewall is transparent to the PC and the Server. To the external server, it considers that the IP address of the internal PC is 202.1.1.1 and knows nothing about the private address 10.1.1.2. Therefore, NAT hides the private network of enterprises.

NAT of FS Devices

The NAT function of the FS devices translates the IP address and port number of the internal network host to the external network address and port number of the device, and vice versa. That is translation between the "private IP address + port number" and the "public IP address + port number".

The FS devices achieve the NAT function through the creation and implementation of NAT rules. There are two types of NAT rules, which are source NAT rules (SNAT rules) and destination NAT rules (DNAT rules). SNAT translates source IP addresses, thereby hiding the internal IP addresses or sharing the limited IP addresses; DNAT translates destination IP addresses, usually translating IP addresses of internal servers (such as the WWW server or SMTP server) protected by the device to public IP addresses.

Configuring a NAT Rule

NAT rules are created based on VRouters. You can create, move and delete SNAT/DNAT rules in the VRouter configuration mode, or configure NAT rules for the default VR trust-vr in the NAT configuration mode (to enter the NAT configuration mode, in global configuration mode, use the command nat).

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

ip vrouter *vrouter-name*

- *vrouter-name* − Specifies the name of VRouter.

Creating a BNAT Rule

A static one-to-one address translation is called bidirectional NAT (BNAT). It usually maps internal address to its external address and vise versa. BNAT can be seen as a combination of DNAT and SNAT, which uses just one rule to achieve both source and destination translation.

In the packet processing flow, BNAT has precedence over DNAT. When a packet mataches a BNAT rule, it follows the destination translation and source translation defined in that BNAT rule. It will not check for other regular NAT rules. After it finishes BNAT mapping, it will start to match policy.

To create a BNAT rule, under VRouter configuration mode, use the command below:

bnatrule [**id** *id*] **interface** *interface-name* **virtual** {**ip** {*A.B.C.D/M* | *X:X:X:X:X::X/M*} | **address-book** *address-name* } **real** {**ip** {*A.B.C.D* | *A.B.C.D/M* | *X:X:X:X:X::X/M*} | **address-book** *address-name* }

- **id** *id* – Specifies an ID for this BNAT rule. Each BNAT has its unique ID. If you skip entering ID for it, the system will assign an ID number automatically. If you specify an existing ID, the new rule will replace the existing rule.
- **virtual** {**ip** { *A.B.C.D/M* | *X:X:X:X:X::X/M*} | **address-book** *address-name* } – Specifies the external IP address for Internet users to visit. This is normmaly 1-to-1 mapping. If the address is an address book or range, you should make sure the virtual address has the same the number of the real addresses. The mapping order is from top to bottom.
  Note: Netmask must be specified. An IP address without netmask is not supported.
- **real** {**ip** {*A.B.C.D/M* | *X:X:X:X:X::X/M*} | **address-book** *address-name* } - Specifies the real internal address. This address is invisible to the external network, and it is the real Intranet address of the server.
  Note: Netmask must be specified. An IP address without netmask is not supported.

To delete a BNAT rule, use the following command:

no bnatrule id *id*

Creating an SNAT Rule

SNAT rules are used to specify whether to implement NAT on the source IP address of the matched traffic. If NAT is implemented, you also need to specify the translated IP address and translation mode. To configure an SNAT rule, in the VRouter configuration mode, use the following command:

snatrule [**id** *id*] [**ingress-interface** *interface-name*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] [**eif** *egress-interface* | **evr** *vrouter-name*] **trans-to** {**addressbook** *trans-to-address* | **eif-ip**} **mode** {**static** | **dynamicip** | **dynamicport** [**sticky** | **round-robin**]} [**log**] [**group** *group-id*] [**disable**] [**track** *track-name*] [**description** *description*]

- **id** *id* − Specifies the ID of the SNAT rule. Each SNAT rule has a unique ID. If the ID is not specified, the system will automatically assign one. If the specified SNAT ID exists, the original rule will be overwritten.

- **ingress-interface** *interface-name* − Specifies the ingress interface of the SNAT rule. When the interface is specified, only the traffic from this interface will continue to match this SNAT rule, and traffic from other interfaces will not.

- **before** *id* | **after** *id* | **top** − Specifies the position of the rule. The position can be top, before id or after id. If the position is not specified, the rule would be located at the end of all the SNAT rules. By default, the newly-created SNAT rule is located at the end of all the rules.

- **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] − Specifies conditions of the rule that the traffic should be matched. The conditions include:

    - **from** *src-address* - Specifies the source IP address of the traffic. *src-address* should be an IP address (IPv4 type or IPv6 type) or an address entry in the address book(IPv4 type or IPv6 type).

    - **to** *dst-address* - Specifies the destination IP address of the traffic. *dst-address* should be an IP address (IPv4 type or IPv6 type) or an address entry in the address book (IPv4 type or IPv6 type).

    - **service** *service-name* − Specifies the service type of the traffic. *service-name* should be a service defined in the service book.

    - **eif** *egress-interface* | **evr** *vrouter-name* - Specifies the egress interface (**eif** *egress-interface*) or the next-hop VRouter (**evr** *vrouter-name*) of the traffic.

- **addressbook** *trans-to-address* | **eif-ip** − Specifies the translated IP address. It can be either an address entry in the address book or the address of the egress interface (`eif-ip`).

- **mode** {**static** | **dynamicip** | **dynamicport** [**sticky** | **round-robin**]} − Specifies the translation mode. FSOS supports three translation modes: static, dynamicip and dynamicport. For more details, see the table below:

Mode	Description
static	Static mode means one-to-one translation. This mode requires the translated address entry (*trans-to-address*) contains the same number of IP addresses as that of the source address entry (*src-address*).
dynamicip	Dynamic IP mode means multiple-to-one translation. This mode translates the source address to a specific IP address. Each source address will be mapped to a unique IP address, until all specified

Mode	Description
	addresses are occupied.
dynamicport	Namely PAT. Multiple source addresses will be translated to one specified IP address in an address entry. If Sticky is enabled, all sessions from an IP address will be mapped to the same fixed IP address. If Round-robin, all sessions from an IP address will be polled to map the IP address. If Sticky and Round-robin are not enabled, the first address in the address entry will be used first; when port resources of the first address are exhausted, the second address will be used. **Note**: Sticky function and Round-robin function are mutually exclusive and cannot be configured at the same time.

- **log** – Enables the log function for this SNAT rule (Generating a log when the traffic is matched to this NAT rule).

- **group** *group-id* - Specifies the HA group the SNAT rule belongs to. If the parameter is not specified, the SNAT rule being created will belong to HA group0.

- **disable** – Enter this command to disable the SNAT rule.

- **track** *track-name* – Specifies a track object name that is configured in the system. After configuring this option, the system will track whether the translated public address is valid. The configured track object can be a Ping track object, HTTP track object, TCP track object. For more details, see Configuring a Track Object of System Management. This function only supports dynamicport mode, and the translated address should be an IP address or an address in address book (i.e., **trans-to address book** *trans-to-address*). The system will prioritize the translated address which is tracked successfully. When a translated address failed to visit a website or a host, it will be temporarily disabled until being tracked successfully again. When the tracking object fails, the system will disable the address and generate a log in the next tracking cycle, and no longer translate the private address to a public address until the address restores to reachable. If all the address in the public address book of SNAT rules are unreachable, the system will not disable any translated address and generate a log.

- **description** *description* – Specifies the description for this SNAT rule. You can specify at most 63 characters.

For example, the following example achieves the interface-based NAT of ethernet0/0 in the untrust zone:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule from any to any eif ethernet0/0 trans-to eif-ip
```

```
mode dynamicport
rule id=1
```

To configure an SNAT rule that disables NAT, in the NAT configuration mode, use the following command:

snatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] **no-trans** [**group** *group-id*] [**description** *description*]

Enabling/Disabling SNAT Rule

To enable or disable an SNAT rule, under NAT configuration mode, use the following command:

snatrule id *id* [**enable** | **disable**]

- **enable** – Enable an SNAT rule of the specified ID.
- **disable** – Disable an SNAT rule of the specified ID.

Moving an SNAT Rule

Each SNAT rule is labeled with a unique ID. When traffic flows into the FS device, the device will query for SNAT rules in the list by turns, and then implement NAT on the source IP of the traffic according to the first matched rule. However, the rule ID is not related to the matching sequence during the query. The sequence displayed by the command **show snat** is the query sequence for the matching. You can move an SNAT rule to modify the matching sequence. To move an SNAT rule, in the NAT configuration mode, use the following command:

snatrule move *id* {**before** *id* | **after** *id*| **top** | **bottom**}

- *id* – Specifies the ID of the SNAT rule that will be moved.
- **before** *id* – Moves the SNAT rule before the specified ID.
- **after** *id* – Moves the SNAT rule after the specified ID.
- **top** – Moves the SNAT rule to the top of the SNAT rule list.
- **bottom** – Moves the SNAT rule to the bottom of the SNAT rule list.

Enabling/Disabling Expanded PAT Port Pool

When the translation mode of SNAT is set to dynamicport, you can enable or disable the expanded PAT port pool to expand the network address port resources after NAT. This function is disabled by default. To enable the function, in the global configuration mode, use the following command:

expanded-port-pool

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

no expanded-port-pool

Note:

- Only some of FS models support the expanded PAT port pool, and the supported port resources also vary from different platforms.
- The function is only applicable to the SNAT rules that have not been enabled yet; if the SNAT rule is already enabled, reboot the system to make the function take effect.

The function is only applicable to the SNAT rules that have not been enabled yet; if the SNAT rule is already enabled, reboot the system to make the function take effect.

Deleting an SNAT Rule

To delete the SNAT rule with the specified ID, in the NAT configuration mode, use the following command:

no snatrule id *id*

Modifying/Deleting the Descriptions of a SNAT Rule

In the NAT configuration mode, use the following command to modify the description of a specific SNAT rule:

snatrule id *id* **description** *description*

- *id* − Specifies the ID of the SNAT rule whose description you want to modify.
- **description** *description* − Specifies the new description. You can enter at most 64 characters.

In the NAT configuration mode, use the following command to delete the description of a specific SNAT rule:

no snatrule id *id* **description**

Viewing SNAT Configuration Information

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

show snat [**id** *id*] [**resource** [**ip**] [**detail**]] [**vrouter** *vrouter-name*]

show snat [**vrouter** *vrouter-name*] [**src** *src-address*] [**dst** *dst-address*] [**service** *service-name*] [**trans-to** *trans-to-address*] [**description** *description*]

- *id* - Shows the SNAT rule information of the specified ID.

- **resource** [**ip**] [**detail**] - When the translation mode of SNAT is set to dynamicport, this parameter is used to show the source utilization of the source port address pool. **ip** means to show the port resource ultilization of the specified IP in the translation address pool. **detail** means to show the detail information of port resource ultilization of the translation address pool. Such as the allocated state, translation mode and port range.

- **vrouter** *vrouter-name* - Shows the SNAT configuration information of the specified VRouter. If this parameter is not specified, the system will show the SNAT rule information of the default VRouter (trust-vr).

- **src** *src-address* - Shows the SNAT configuration information of the specified source address.

- **dst** *dst-address* - Shows the SNAT configuration information of the specified destination address.

- **service** *service-name* - Shows the SNAT configuration information of the specified service.

- **trans-to** *trans-to-address* - Shows the SNAT configuration information of the specified translated IP.

- **description** *description* - Shows the SNAT configuration information of the specified description.

Viewing Tracked Failed Information of SNAT Translated Address

To view the tracked failed information of SNAT translated address, in any mode, use the following command:

show snat track-failed [**vrouter** *vrouter-name*] [**slot** *slot-number*] [**cpu** *cpu-number*]

- **track-failed** – Displays the tracked failed information of SNAT translated address.

- **vrouter** *vrouter-name* – Displays the tracked failed SNAT translated address of the specified VRouter. If this parameter is not specified, the system will display the information of the default VRouter (trust-vr).

- **slot** *slot-number* – Displays the tracked failed SNAT translated address of the specified slot.

- **cpu** *cpu-number* – Displays the tracked failed SNAT translated address of the specified CPU.

Creating a DNAT Rule

DNAT rules are used to specify whether to implement NAT on the destination IP address of the matched traffic. To configure a DNAT rule for NAT, in the VRouter configuration mode, use the following command:

dnatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] [**ingress-interface** *interface*] **from** *src-address* **to** *dst-address* [**service** *service-name*] **trans-to** *trans-to-address* [**redirect**] [**port** *port*] [**load-balance**] [**track-tcp** *port*] [**track-ping**] [**log**] [**group** *group-id*] [**disable**] [**description** *description*]

- **id** *id* – Specifies the ID of the DNAT rule. Each DNAT rule has a unique ID. If the ID is not specified, the system will automatically assign one. If the specified DNAT ID exists, the original rule will be overwritten.
- **before** *id* | **after** *id* | **top** – Specifies the position of the rule. The position can be **top**, **before** *id* or **after** *id*. If the position is not specified, the rule would be located at the end of all the DNAT rules. By default, the newly-created DNAT rule is located at the end of all the rules.
- **ingress-interface** *interface* – Specifies the ingress interface whose traffic will match this dnat rule. When this interface is designated, only the traffic from this interface will continue to match this DNAT rule. Traffic from other interfaces will not.
- **from** *src-address* **to** *dst-address* [**service** *service-name*] – Specifies conditions of the rule that the traffic should be matched. The conditions are:
  - **from** *src-address* – Specifies the source IP address /netmask of the traffic. *src-address* should be an IP address /netmask or an address entry in the address book.
  - **to** *dst-address* – Specifies the destination IP address/netmask of the traffic. *dst-address* should be an IP address /netmask or an address entry in the address book.
  - **service** *service-name* – Specifies the service type of the traffic. If the port number needs to be translated together (specified by port), the specified service can only be configured with one protocol and one port. For example, the TCP port number can be 80, but cannot be 80 to 100.
- **trans-to** *trans-to-address* – Specifies the translated IP address. *trans-to-address* is an IP address/netmask or an address entry in the address book. When the number of this translated IP address be different from the destination IP address of the traffic (specified by **to** *dst-address*) or the destination IP address is **any**, you must enable the redirect function for this DNAT rule (specified by **redirect**). If the DNAT rule is enabled with**load-balance**, the number of translated IP addresses can be allowed different from the destination IP address of the traffic, but the destination IP address cannot be **any**.

- **redirect** - Enables **redirect** for this DNAT rule, allows the destination IP address of the traffic to be **any**.
- **port** *port* – Specifies port number of the internal network server.
- **load-balance** – Enables **load-balance** for this DNAT rule. The system will adopt persistent algorithm to distribute traffic and balance the traffic to different servers in the internal network based on the hash of user IP.
- **track-tcp** *port* – If this parameter is configured and the port number of the internal network server is specified, the system will send TCP packets to the internal network server every 3 seconds to monitor if the specified port is reachable. If no response is returned for 3 packets in succession, the system will conclude the server fails.
- **track-ping** – If this parameter is configured, the system will send Ping packets to the internal network server every 3 seconds to monitor if the server is reachable. If no response is returned for 3 packets in succession, the system will conclude the server fails.
- **log** – Enables the log function for this DNAT rule (Generating a log when the traffic is matched to this NAT rule).
- [**group** *group-id*] - Specifies the HA group that the DNAT rule belongs to. If the parameter is not specified, the DNAT rule being created will belong to HA group0.
- **disable** – Enter this command to disable the DNAT rule.
- **description** *description* – Specifies the description for this DNAT rule. You can specify at most 63 characters.

For example, the following command will translate the IP address of the request from addr1 to the IP address of addr2, but will not translate the port number:

```
hostname(config-vrouter)# dnatrule from any to addr1 service any trans-to addr2
rule id=1
```

To configure a DNAT rule that disables NAT, in the NAT configuration mode, use the following command:

dnatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] **no-trans** [**group** *group-id*] [**description** *description*]

Enableing/Disabling DNAT Rule

To enable or disable a DNAT rule, under NAT configuration mode, use the following command:

dnatrule id *id* [**enable** | **disable**]

- **enable** − Enable the DNAT rule of the specified ID.
- **disable** − Disable the DNAT rule of the specified ID.

Moving a DNAT Rule

Each DNAT rule is labeled with a unique ID. When traffic flowing into the FS device, the device will query for DNAT rules by turns, and then implement NAT on the source IP of the traffic according to the first matched rule. However, the rule ID is not related to the matching sequence during the query. The sequence displayed by the command show dnat is the query sequence for the matching. You can move a DNAT rule to modify the matching sequence. To move a DNAT rule, in the NAT configuration mode, use the following command:

dnatrule move *id* {**before** *id* | **after** *id*| **top** | **bottom**}

- *id* − Specifies the ID of the DNAT rule that will be moved.
- **before** *id* − Moves the DNAT rule before the specified ID.
- **after** *id* − Moves the DNAT rule after the specified ID.
- **top** − Moves the DNAT rule to the top of the DNAT rule list.
- **bottom** − Moves the DNAT rule to the bottom of the DNAT rule list.

Modifying/Deleting the Descriptions of a DNAT Rule

In the NAT configuration mode, use the following command to modify the description of a specific DNAT rule:

dnatrule id *id* **description** *description*

- *id* − Specifies the ID of the DNAT rule whose description you want to modify.
- **description** *description* − Specifies the new description. You can enter at most 64 characters.

In the NAT configuration mode, use the following command to delete the description of a specific DNAT rule:

no dnatrule id *id* **description**

Deleting a DNAT Rule

To delete the DNAT rule with the specified ID, in the NAT configuration mode, use the following command:

no dnatrule id *id*

Viewing DNAT Configuration Information

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

show dnat [**id** *id* | [**vrouter** *vrouter-name*] [**src** *src-address*] [**dst** *dst-address*] [**service** *service-name*] [**trans-to** *trans-to-address*] [**trans-port** *port-number*] [**description** *description*]]

- *id* - Shows the DNAT rule information of the specified ID.
- **vrouter** *vrouter-name* - Shows the DNAT configuration information of the specified VRouter. If this parameter is not specified, the system will show the DNAT rule information of the default VRouter (trust-vr).
- **src** *src-address* - Shows the DNAT configuration information of the specified source address.
- **dst** *dst-address* - Shows the DNAT configuration information of the specified destination address.
- **service** *service-name* - Shows the DNAT configuration information of the specified service.
- **trans-to** *trans-to-address* - Shows the DNAT configuration information of the specified translated IP.
- **trans-port** *port-number* - Shows the DNAT configuration information of the specified translated port.
- **description** *description* - Shows the DNAT configuration information of the specified description.

To show the information of the DNAT rule with load balancing configured, in any mode, use the following command:

show load-balance rule [*id*]

- *id* – Shows the DNAT rule information (with load balancing) of the specified ID.

To view the status of the load-balancing server, in any mode, use the following command:

show load-balance server [*ip-address*] [**vrouter** *vrouter-name*]

- *ip-address* – Shows status of the load-balancing server of the specified IP address.

- **vrouter** *vrouter-name* – Shows status of the load-balancing server of the specified VRouter. If this parameter is not specified, the system will show status of the load-balancing server of the default VRouter (trust-vr).

To view the status of the internal network server, in any mode, use the following command:

show dnat server [*ip-address*] [**vrouter** *vrouter-name*] [**tcp-port** *port*] [**ping**]

- *ip-address* – Shows status of the internal network server of the specified IP address.
- **vrouter** *vrouter-name* – Shows status of the internal network server of the specified VRouter. If this parameter is not specified, the system will show status of the internal network server of the default VRouter (trust-vr).
- **tcp-port** *port* – Shows status of the internal network server of the specified port number.
- **ping** – Shows Ping monitor status of the internal network server.

Configuring an Excluding Port Rule

By configuring the excluded port rules, you can rule out port or port range. The system will not convert the specified port when the source address is translated.

To configure the excluding port function, take the following steps:

1. Create a SNAT port group.
2. Configure the SNAT port group, and specify the description excluded port number.
3. Bind the SNAT port group to the specified VRouter to make the function take effect.

Creating a SNAT Port Group

To create a SNAT port group, in the global configuration mode, use the following command:

snat-port-group *snat-port-group-name*

- *snat-port-group-name* - Specifies the SNAT port group name and enters the SNAT port group configuration mode. If the specified name exists, then the system will directly enter the SNAT port group configuration mode. The name range is 1 to 95 characters.

Note:System supports at most 8 SNAT port groups.

To delete a SNAT port group, in the global configuration mode, use the following command:

no snat-port-group *snat-port-group-name*

Specifying the Description of SNAT Port Group

To specify the description of SNAT port group, in the SNAT port group configuration mode, use the following command:

description *description*

- *description* − Specifies the description of SNAT port group, the range is 0 to 256 characters.

To delete the description of SNAT port group, in the SNAT port group configuration mode, use the following command:

no description

Specifying the Excluding Port Number

To specify the port range that needs to be excluded, in the SNAT port group configuration mode, use the following command:

port {**TCP** | **UDP**} **min-port** *min-port* [**max-port** *max-port*]

- **TCP** | **UDP** − Specifies the protocol type of excluded ports.
- **min-port** *min-port* [**max-port** *max-port*]- Specifies the excluded port number. If the port number is a number range, then *min-port* is the minimum port number, and *max-port*is the maximum port number.

To cancel the above configuration, in the SNAT port group configuration mode, use the following command:

no port {**TCP** | **UDP**} **min-port** *min-port* [**max-port** *max-port*]

Binding the SNAT Port Group to VRouter

After binding the SNAT port group to the specified VRouter, the SNAT rule of all dynamic ports of the VRouter excludes the port number specified in the SNAT port group, in the VRouter configuration mode, use the following command:

snat-exclude-port *snat-port-group-name*

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

no snat-exclude-port

Viewing the SNAT Port Group Information

To view the configuration information of SNAT port group, in any mode, use the following command:

show snat-port-group [*snat-port-group-name*]

- *snat-port-group-name* – Display the SNAT port group configuration information of the specified name.

Viewing the SNAT Port Group References

To view the SNAT port group references, in any mode, use the following command:

show reference snat-port-group [*snat-port-group-name*]

- *snat-port-group-name* – Display the SNAT port group references of the specified name.

DNS Rewrite

When the client initiates a DNS request, DNS server in Internet will return DNS response to the client. The security device can rewrite the IP address in DNS response packet to private IP in order to protect the private network configurations. In NAT configuration mode, type the following command:

dns-rewrite-rule [**id** *id*] **dns-response** {**ip** *ip-address* | **address-book** *address-name*} **rewrite-to** {**ip** *ip-address* | **address-book** *address-name*}[**group** *group-id*] **dynamic-mapping**

- **id** *id* – Specifies the rule ID. Each rule has a unique ID. If the ID is not specified, the system will automatically assign one. If the specified ID exists, the original rule will be overwritten.

- **dns-response** {**ip** *ip-address* | **address-book** *address-name*} - Specifies public IP or address book in DNS response.

- **rewrite-to** {**ip** *ip-address*| **address-book** *address-name*} – Specifies private IP or address book which the security device rewrites.

- **group** *group-id* – Specifies the group ID of HA group which the rule belongs to.

In any mode, use **show dns-rewrite-rule** [**id** *id* | **vrouter** *vr-name*] **dynamic-mapping** to view DNS rewrite rules:

- **id** *id* | **vrouter** *vr-name* – View the DNS rewrite rules of the specified ID or VRouter.

NAT444

FS devices support NAT444. NAT444 is carrier-grade NAT that is designed to extend the service life of IPv4 during the transition from IPv4 to IPv6 and win some time for the deployment of IPv6.

With NAT444 configured, the system will create a mapping table according to user’s address pool (source IP), public address pool (translated IP), available port range and port block size, and implement NAT for the source IPs and ports of matched traffic based on the mapping table.

Configuring NAT444

NAT444 on FS devices is implemented by creating and executing SNAT rules. Compared with traditional SNAT rules, NAT444 SNAT rules are featured with some new parameters. This section mainly describes these new parameters. To configure an SNAT rule for NAT444, in the VRouter configuration mode, use the following command:

snatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] [**eif** *egress-interface* | **evr** *vrouter-name*] **trans-to addressbook** *trans-to-address* **mode dynamicport** [**fixed-block** | **random-block**] **start** *start-port* **end** *end-port* **size** *port-block-size* [**max-block-per-user** *blocks*] [**log** {[**port-block** {**allocate** | **release** | **all**}] [**session** {**allocate** | **release** | **all**}] | **session** {**allocate** | **release** | **all**} | **all**]} [**group** *group-id*] [**description** *description*]

- **mode dynamicport** [**fixed-block** | **random-block**] **start** *start-port* **end** *end-port* **size** *port-block-size* [**max-block-per-user** *blocks*] – All the sessions originating from one source IP will be mapped to one specified IP address in an address entry. The source IP corresponds to one or more port blocks of the mapped IP. If the port resources in the block are exhausted, the translation will fail. For detailed mapping relationship, see the NAT444 SNAT example below.
    - **fixed-block** – Uses the static port block mapping mode . Each source IP address corresponds to a fixed port block of the mapped IP.
    - **random-block** – Uses the dynamic port block mapping mode. Each source IP address can correspond to one or more port blocks and the parameter **max-block-per-user** *blocks* determines how many port blocks that each source IP address can correspond to.
    - **start** *start-port* **end** *end-port* – Specifies the start port and end port of the available port range. The value range is 1024 to 65535.
    - **size** *port-block-size* – Specifies the size of the port block. The value range is 64 to 64512, and the value must be the integer multiple of 64.
    - **max-block-per-user** *blocks* – Specifies the maximum number of port blocks that each user in the intranet can occupy. When using the dynamic port block mapping mode, you can set this parameter. The default value is 1.
- **log** {[**port-block** {**allocate** | **release** | **all**}] [**session** {**allocate** | **release** | **all**}] | **session** {**allocate** | **release** | **all**} | **all**]} – Configures log for NAT444 (generates logs for matched traffic):

- **port-block** {**allocate** | **release** | **all**} – Generates logs when the system is allocating (**allocate**) or releasing (**release**) port block. **all** indicates generating logs for both of the above events.
- **session** {**allocate** | **release** | **all**} – Generates logs when the system is creating (**allocate**) or disconnecting (**release**) a NAT session. **all** indicates generating logs for both of the above events.
- **all** – Generates log when the system is either allocating/releasing a port block or creating/disconnecting a NAT session.

The following is a NAT444 SNAT example:

Suppose the source IP is src_addr: 192.168.1.0/24, and the translated IP is global_addr: 200.1.2.10~200.1.2.100

```
hostname(config-vrouter)# snatrule id 1 from src_addr to any trans-to address-book global_addr mode dynamicport fixed-block start 1024 end 65000 size 4096
rule id=1
```

The mapping relationship is shown as below:

```
hostname(config-vrouter)# show snat id 1 ports-map
--------------------------------------------------------------
=====================================================================
from translate to start port end port
-----------------------------------------------------------------
192.168.1.0 200.1.2.10 1024 5119
192.168.1.1 200.1.2.10 5120 9215
192.168.1.2 200.1.2.10 9216 13311
……
192.168.1.14 200.1.2.10 58368 62463
192.168.1.15 200.1.2.11 1024 5119
192.168.1.16 200.1.2.11 5120 9215
192.168.1.17 200.1.2.11 9216 13311
……
```

To configure an SNAT rule that disables NAT444, in the NAT configuration mode, use the following command:

snatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] **no-trans** [**group** *group-id*]

Monitoring the Port Utilization and Port Block Utilization

The system can monitor the port utilization and port block utilization. When the real utilization is higher than the specified threshold, the system will send the corresponding alarms. This monitor function is available to all NAT444 rules.

To configure the port utilization or port block utilization monitor, in the global configuration mode, use the following command:

nat444-resource monitor {**port-utilization threshold** *value* | **port-block-utilization threshold** *value*} **log**

- **port-utilization threshold** *value* – Specifies the threshold of the port utilization. When the actual value is higher than the threshold specified here, the system will send the corresponding alarm. The value range is from 1 to 99.
- **port-block-utilization threshold** *value* – Specifies the threshold of the port block utilization. When the actual value is higher than the threshold specified here, the system will send the corresponding alarm. The value range is from 1 to 99.

In the global configuration mode, use the command to cancel the monitor configuration.

no nat444-resource monitor {**port-utilization** | **port-block-utilization**}

Viewing NAT444 Configuration Information

To view SNAT rule information of NAT444, in any mode, use the following command:

show snat [**id** *id*] **ports-map** {**src** *src-address* [**detail**] | **trans-to** *trans-to-address* | **vrouter** *vrouter-name* {**src** *src-address* [**detail**] | **trans-to** *trans-to-address*}}

- **id** *id* – Shows the mapping information of the SNAT rule with the specified ID.
- **src** *src-address* – Shows the mapping information of the specified source IP.
- **detail** – Shows the mapping information of the specified source IP and port block utilization.
- **trans-to** *trans-to-address* – Shows the mapping information of the translated IP address.

- **vrouter** *vrouter-name* - Shows the SNAT rule mapping information of the specified VRouter.

Viewing IP Addresses and Port Resources Allocation Mode

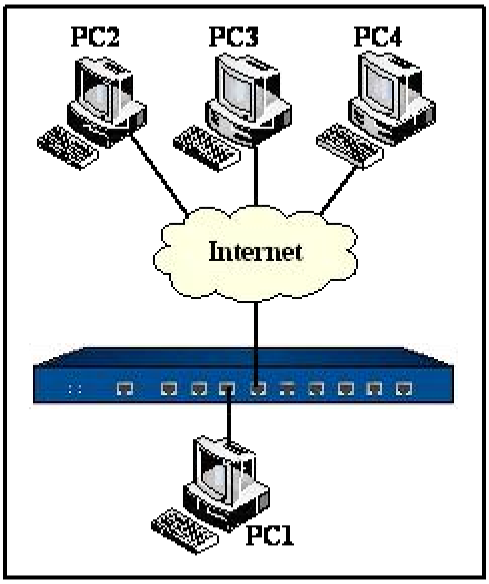
To view the IP addresses and port resources distribution mode, use the following command in any mode:

show flow snat-port-allocation mode

Full-cone NAT

Full-cone NAT, also known as one-to-one NAT, will map all the requests from one IP/port in the private network to one IP/port in the public network, and thereafter all the hosts in the public network will be able to communicate with the host that initiated the request by making use of the mapping relationship.

As shown below, suppose PC1 in the Intranet has already established a connection with PC2 in the Internet after NAT translation, and the device translates the IP/port of PC1 (Private IP:Private port) to a public IP/port (Public IP:Public port). Since there exists a session, PC2 can connect to PC1 reversely by matching the session. However, due to no session matching information, by default PC3 and PC4 cannot communicate with PC1 even if the translated public IP/port (Public IP:Public port) is routable. With Full-cone NAT enabled, the device will create and maintain a Full-cone NAT entry and advertise the mapping between the public and private IPs/ports (Local IP:Local port <==> Public IP:Public port) by the entry. In such a condition, if only PC3 and PC4 can reach the public IP/port of PC1 (Public IP:Public port), they can tranverse the NAT device and connect to PC1 proactively by making use of the mapping information.



To enable Full-cone NAT, in the global configuration mode, use the following command:

```
nat type full-cone
```

To disable Full-cone NAT, in the global configuration mode, use the following command:

```
no nat type full-cone
```

To specify the protocol that is enabled with Full-cone NAT, in the global configuration mode, use the following command:

```
nat protocol {tcp | udp}
```

- tcp- Enables Full-cone NAT on TCP.
- udp - Enables Full-cone NAT on UDP. This is the default option.

To cancel the configuration, in the global configuration mode, use the following command:

```
no nat protocol {tcp | udp}
```

Viewing Full-cone NAT Configuration Information

To view the configuration information of Full-cone NAT, in any mode, use the following command:

```
show nat {config | generic | entry | control}
```

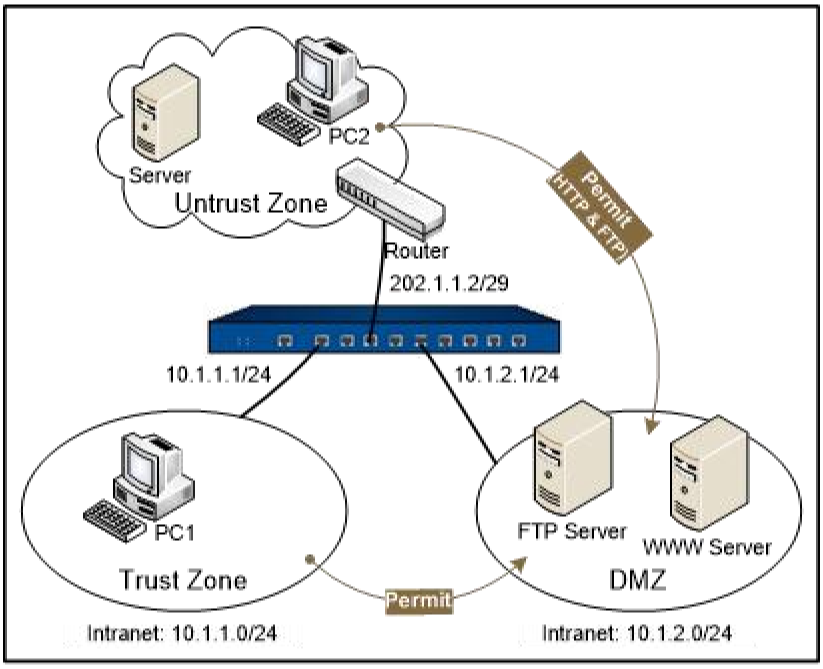
- config - Shows the configuration of Full-cone NAT.
- generic - Shows the general information of Full-cone NAT entry.
- entry - Shows the detailed information of Full-cone NAT entry.
- control – Shows the status of the following functions: full-cone NAT, expanded PAT port pool, and SNAT port split under HA peer mode.

Example of Configuring NAT

This section describes a typical NAT configuration example.

Requirement

The company network is divided into three zones by a FS device: Trust Zone, DMZ Zone and Untrust Zone. Employees work in the Trust zone, they are allocated with the private network segment of 10.1.1.0/24 and get the highest security priority; WWW server and FTP server are in the DMZ zone, they are allocated with the private network segment of 10.1.2.0/24 and can be accessed by internal employees and external users; external networks are in the Untrust zone. The network topology is shown in Figure below:



There are three requirements:

- Requirement 1: Employees in segment 10.1.1.0/24 in the trust zone are able to access the Internet, while PCs in other segments of the zone cannot access the Internet. The legitimate IP address range provided to access the external network is 202.1.1.3 to 202.1.1.5. Because there are not enough public network addresses, NAT address multiplexing function is needed.
- Requirement 2: Two internal servers are provided for users and can be accessed from the external networks, including an FTP server (the internal IP address is 10.1.2.2, port number is 21) and a WWW server (the internal IP address is 10.1.2.3, port number is 80); external mapping IP address is 202.1.1.6.
- Requirement 3: After any PC in the Trust zone has gained access to the host in the Untrust zone, all the hosts in the Untrust zone can connect to the PC in the Trust zone reversely by making use of Full-cone NAT.

Configuration Steps

Step 1: Configure security zones and IP addresses

```
hostname# configure

hostname(config)# interface ethernet0/1

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

hostname(config-if-eth0/1)# ip address 10.1.1.1/24

hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ip address 202.1.1.2/29
hostname(config-if-eth0/2)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone dmz
hostname(config-if-eth0/3)# ip address 10.1.2.1/24
hostname(config-if-eth0/3)# exit
hostname(config)#
```

Step 2: Configure address entries

```
hostname(config)# address addr1
hostname(config-addr)# ip 10.1.1.1/24
hostname(config-addr)# exit
hostname(config)# address addr2
hostname(config-addr)# range 202.1.1.3 202.1.1.5
hostname(config-addr)# exit
hostname(config)# address test1
hostname(config-addr)# ip 202.1.1.6/32
hostname(config-addr)# exit
hostname(config)# address test2
hostname(config-addr)# ip 10.1.2.2/32
hostname(config-addr)# exit
hostname(config)# address test3
hostname(config-addr)# ip 10.1.2.3/32
hostname(config-addr)# exit
```

Step 3: Configure policy rules

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr addr1
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone dmz
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone dmz
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service http
hostname(config-policy-rule)# service ftp
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 4: Configure NAT rules

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule id 1 from addr1 to any eif ehternet0/2 trans-to address-book
```

```
addr2 mode dynamicport sticky
rule id=1
hostname(config-vrouter)# dnatrule id 2 from any to test1 service ftp trans-to test2 port 21
rule id=2
hostname(config-vrouter)# dnatrule id 3 from any to test1 service http trans-to test3 port 80
rule id=3
hostname(config-vrouter)# exit
hostname(config)# nat type full-cone
hostname(config)# nat protocol tcp
```

Application Layer Identification and Control

Overview

FS devices provide a wide range of application layer monitoring, statistics and filtering functions. These functions can identify applications such as FTP, HTTP, P2P, IM tools and VoIP, and based on the security policy rules configured, ensure the proper communication of the applications or perform the specified operations on the traffic, such as monitoring, statistics, traffic control and blocking. By making use of the fragment reassembling and transport layer proxy technique, the FS devices can adapt to the complex network environment, reassemble the packets, and identify the applications effectively even when the complete application layer data is fragmented and disordered during the transmission, thus ensuring the effective implementation of security policies.

Fragment Reassembly

Typically the intermediate network device such as a router or switch does not reassemble the fragmented packets it receives. The destination host reassembles the fragmented packets after all the fragments have arrived. Due to the complexity of the network environment, fragmented packets may be dropped or disordered during the transmission, while the reassembling needs to receive and sort all the fragments, which will consume certain system resources. From the aspect of the main function and forwarding efficiency, the network devices usually only forward the fragments and will not reassemble them. However, for security devices, the application of security policies requires an analysis of application layer information, in order to filter the malicious messages that contain potential security risks, or block any attempt of intrusions and attacks. All the operation will only be finally determined after the device receives the complete information of the application layer. Powered by the transport layer proxy function, FSOS can buffer, sort and reassemble the fragmented packets first, and then re-encapsulate and forward the normal data after a complete analysis and identification.

Application Layer Gateway (ALG)

Some applications use multi-channels for data transmission, such as the widely used FTP. In such a condition the control channel and data channel are separated. FS devices under strict security policy control set strict limits on each data channel, for example, only allow FTP data from internal network to external network to transfer on the well-known port TCP 21. Once in the FTP active mode, if an FTP server in the public network tries to initiate a connection to a random port of the host in the internal network, FS devices will reject the connection and the FTP server will not work properly in such a condition. This requires FS 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, FS 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.

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

- Under strict security policy rules, ensures the normal communication of multi-channel applications, such as FTP, TFTP, PPTP, RTSP, RSH, MSRPC, SUNRPC and SQLNET.
- Ensures the proper operation of VoIP applications such as SIP and H.323 in NAT mode, and performs monitoring and filtering according to the policies.

HTTP, P2P and IM

Powered by the fragment reassembly and transport layer proxy functions, FSOS supports the identification and control of 3 main types of applications: HTTP applications, P2P applications and IM applications. The FS devices can perform various operations like monitoring, restricting and blocking traffic on each application by creating Profiles. For example:

- Filtering HTTP Java Applets to ensure users are protected from harmful Java Applets.
- Filtering HTTP ActiveX to prevent malicious ActiveX programs from damaging the user's system.
- Identifying, monitoring and blocking P2P applications, like BT, eMule, Thunder, etc.
- Operations on IM tools, such as identifying and controlling IM chatting and file transfer. The supported IM clients include MSN Messenger, QQ, Yahoo

Configuring ALG

FSOS allows you to enable or disable ALG for different applications. FS devices support ALG for the following applications: FTP, HTTP, MSRPC, PPTP, Q.931, RAS, RSH, RTSP, SIP, SQLNetV2, SUNRPC, TFTP, DNS, and H323. You can not only enable or disable ALG for applications, but also specify H323's session timeout.

To enable or disable the ALG control function for applications, in the global configuration mode, use the following command:

Enable: **alg** {**all** | **auto** | **TFTP** | **FTP** | **RSH** |…}

Disable: **no alg** {**all** | **auto** | **TFTP** | **FTP** | **RSH** | …}

- **all** − Enables or disables the ALG control function for all the applications.
- **auto** − Enables or disables the ALG control function based on the result of application identification.
- **TFTP** | **FTP** | **RSH** | … - Enables or disables the ALG control function for the specific application.

Note: If ALG for HTTP is disabled, the Web content filter function on the device will be void.

ALG supports strict mode and non-strict mode. In the strict mode, the newly-created pinhole has the SNAT port which is the same as the SNAT port of the control session. By default, the strict mode is enabled. To enable the ALG strict mode, use the following command in the global configuration mode:

alg strict-mode

Use the **no alg strict-mode** command to enable the non-strict mode. In the scenario below, FS recommends the users to enable the non-strict mode:

- The third-party pinhole exists.
- SNAT is configured and port expansion is enabled.
- The IP address and port number in the payload for negotiating the data session is the same as the IP address and port number of the control session.

To specify the timeout value for the H323 protocol, in global configuration mode, use the following command:

alg h323 session-time *time-value*

- *time-value* - Specifies the timeout value for H323. The value range is 60 to 1800 seconds. The default value is 60.

To cancel the specified timeout value, in global configuration mode, use the following command:

```
no alg h323 sesstion-time
```

To limit the number of the SIP messages that can be processed per second, use the following command in the global configuration mode:

Enable: **alg sip-message-rate** *number*

- *number* - Specifies the maximum number of the SIP messages that can be processed per second. The value is in the range of 1 to 65535.

Disable: **no alg sip-message-rate**

To view the status and configuration of ALG, in any mode, use the following commands:

- To view if ALG is enabled: **show alg**
- To view the ALG configuration and status of SIP gateway: **show alg sip-capacity**

Specifying SIP Proxy Server Mode

The Session Initiation Protocol (SIP) is a communications protocol for signaling and controlling multimedia communication sessions. The most common applications of SIP are in Internet telephony for voice and video calls. Multimedia transited by SIP usually are voice, video and text.

SIP proxy server acts as an intermediary entity when the SIP user agent clients are making requests. When SIP user agent clients exchange media data packets, they can transfer data with or without a SIP proxy server. To avoid communication error, the firewall should select a mode that complies with the actual data transmission mode.

Under global configuration mode, use the command below to inform the firewall that SIP user agent clients are communicating media data directly without SIP proxy server. This is the default setting on the firewall. This command ensures normal communication among SIP user agents.

```
no alg sip media-proxied-by-server
```

Under global configuration mode, use the command below to inform the firewall that SIP user agent clients are exchanging media data packets through SIP proxy server.

```
alg sip media-proxied-by-server
```

Showing ALG SIP

To show ALG SIP information, including if the firewall has enabled SIP server proxy, SIP message rate maximum, registered client number and busy client number, under any mode, use the following command:

show alg sip

Examples of Configuring Application Layer Identification and Control

This section describes two application layer identification and control examples:

- Example 1: The goal is to strictly restrict internal users' access to TFTP, FTP and RTSP services running on the external network only on the well-known ports, while also ensuring the normal communication of these applications on multiple channels.
- Example 2: The goal is to block ActiveX controls and Java applets from the external network.

Configuration Steps for Example 1

Step 1: Restrict service types in security policy rules

```
The address entry “internal” includes all the IPs of internal clients
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr internal
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service tftp
hostname(config-policy-rule)# service ftp
hostname(config-policy-rule)# service rtsp
hostname(config-policy-rule)# application tftp
hostname(config-policy-rule)# application ftp
hostname(config-policy-rule)# application rtsp
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 2: Enable ALG for these applications

```
hostname(config)# alg tftp
hostname(config)# alg ftp
hostname(config)# alg rtsp
```

Configuration Steps for Example 2

Step 1: Enable ALG for the HTTP application

```
hostname(config)# alg http
```

Step 2: Configure a Profile to control Java applets and ActiveX

```
hostname(config)# behavior-profile test
hostname(config-bhv-profile)# object active-x deny
hostname(config-bhv-profile)# object java-applet deny
hostname(config-bhv-profile)# exit
hostname(config)#
```

Step 3: Bind the profile to policy rules

```
The address entry “internal” includes all the IPs of internal clients
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr internal
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service http
hostname(config-policy-rule)# application http
hostname(config-policy-rule)# behavior test
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

RSTP

RSTP, the abbreviation for Rapid Spanning Tree Protocol defined by IEEE 802.1D-2004, is the enhancement and supplement to STP (8021.D). The protocol can provide faster spanning tree convergence after a topology changes.

RSTP is a loop network solution that is designed to block the redundant links to avoid broadcast storms. When a link fails in the network, the redundant link will quickly switch to the forwarding state, and ensure that the traffic will not be interrupted. The root of the Rapid Spanning Tree is known as a root bridge in the RSTP protocol. The root bridge is autonomously selected among the network device by comparing the bridge priorities (the smaller the value is, the higher the priority will be). The farthest port to the root bridge on the other device (the largest cost) will be blocked, and the link corresponding to the blocked port will become a redundant link.

Configuring RSTP

The configurations of RSTP include:

- Creating RSTP
- Enabling RSTP
- Configuring the bridge priority
- Configuring the Hello interval
- Configuring the Forward Delay time
- Configuring the maximum age of BPDU message
- Enabling RSTP on an interface
- Configuring the RSTP priority on an interface
- Configuring the RSTP cost on an interface

Creating RSTP

To create RSTP and enter the RSTP configuration mode, in the global configuration mode, use the following command:

stp

The command creates RSTP and leads you to the RSTP configuration mode; if the RSTP is existing, the system will directly enter the RSTP configuration mode.

To delete RSTP, in the global configuration mode, use the command **no stp**.

Enabling RSTP on the Device

The RSTP function is a global switch. You need to enable both the global function switch and the interface RSTP switch to control RSTP function jointly. By default, RSTP is disabled on the device. To enable RSTP, in the RSTP configuration mode, use the following command:

```
enable
```

To disable RSTP, in the RSTP configuration mode, use the command **no enable**.

Enabling RSTP on an Interface

By default, RSTP on an interface is disabled. To enable RSTP on an interface, in the Ethernet interface or aggregate interface configuration mode, use the following command:

```
stp enable
```

To disable RSTP on an interface, in the Ethernet interface or aggregate interface configuration mode, use the following command:

```
no stp enable
```

Configuring the Bridge Priority

To configure the bridge priority, in the RSTP configuration mode, use the following command:

bridge priority *value*

- *value* – Specifies the bridge priority. The value must be the integer multiples of 4096. The value range is 0 to 61440. The default value is 32768.

To restore to the default bridge priority, in the RSTP configuration mode, use the following command:

```
no bridge priority
```

Configuring the Hello Interval

Hello packets are used to confirm whether the link between devices is normal. The Hello interval is used to specify how often the device sends a Hello packet. To configure the Hello interval, in the RSTP configuration mode, use the following command:

hello *seconds*

- *seconds* – Specifies the Hello interval. The value range is 1 to 10 seconds. The default value is 2.

To restore to the default Hello interval, in the RSTP configuration mode, use the following command:

```
no hello
```

Configuring the Forward Delay Time

When any link fails, the system will re-calculate the spanning tree network. It's impossible for the system to spread the new BPDU (Bridge Protocol Data Unit, used for data exchanging between bridges) configuration information throughout the network immediately, so if the data transmission starts too early, it may cause a temporary loop. To avoid such a problem, RSTP defines a forwarding delay timer, i.e., the forward delay time.

To configure the forward delay time, in the RSTP configuration mode, use the following command:

```
forward-delay value
```

- *value* – Specifies the forward delay time. The value range is 4 to 30 seconds. The default value is 15.

To restore to the default forward delay time, in the RSTP configuration mode, use the following command:

```
no forward-delay
```

Configuring the Maximum Age of BPDU Message

The maximum age of BPDU messages indicates the lifetime of a BPDU message on the device. When the lifetime runs out, the BPDU message will be deleted.

To configure the maximum age of BPDU message, in the RSTP configuration mode, use the following command:

```
maximum-age value
```

- *value* – Specifies the maximum age of BPDU message. The value range is 6 to 40 seconds. The default value is 20.

To restore to the default maximum age, in the RSTP configuration mode, use the following command:

```
no maximum-age
```

Configuring the RSTP Priority on an Interface

To configure the RSTP priority on an interface, in the Ethernet interface or aggregate interface configuration mode, use the following command:

```
stp priority value
```

- *value* – Specifies the RSTP priority of the current interface. The value must be the integer multiples of 16. The value range is 0 to 240. The default value is 128.

To restore to the default RSTP priority, in the Ethernet interface or aggregate interface configuration mode, use the following command:

```
no stp priority
```

Configuring the RSTP Cost on an Interface

To configure the RSTP cost on an interface, in the Ethernet interface or aggregate interface configuration mode, use the following command:

```
stp cost value
```

- *value* – Specifies the RSTP cost value on the interface. The value range is 1 to 200000000. If this parameter is not specified, the system will calculate a value based on the interface type (a single interface or aggregate interface), speed (10Mbps, 100Mbps or 1000Mbps) and duplex status (full-duplex or half-duplex).

To restore to the default RSTP cost (calculated based on the above factors), in the Ethernet interface or aggregate interface configuration mode, use the following command:

```
no stp cost
```

Viewing RSTP Configuration

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

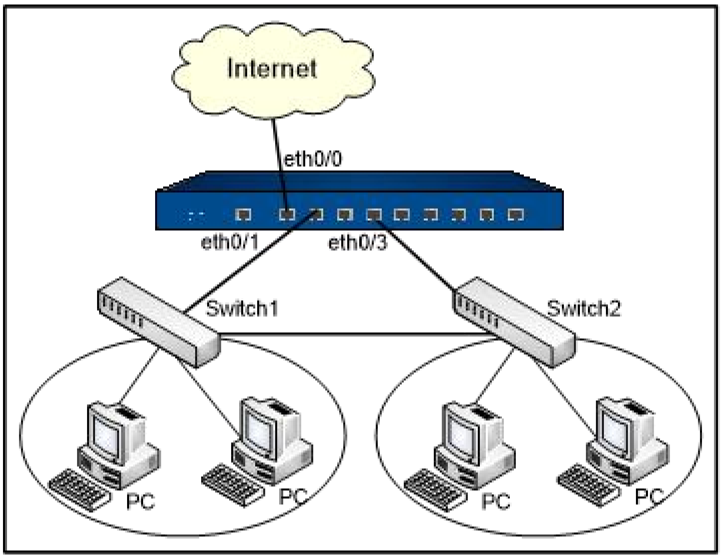
```
show stp [port interface-name]
```

Configuration Example

The section describes a RSTP example.

Requirement

As shown below, the FS device acts as gateway and is connected to Internet. The requirement is: when the link between Switch1 (or Switch2) and the FS device fails, enable STP on the switches and device to implement the Layer 2 link redundancy, and ensure the PC in the LAN is still able to access the Internet.



Configuration Steps

First, ensure that STP on Switch1 and Switch2 can function properly, and then take the following steps:

Step 1: Create a VLAN named VLAN1, and add ethernet0/1 and ethernet0/3 to VLAN1

```
hostname(config)# vlan 1
hostname(config-vlan)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# switchmode access vlan 1
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# switchmode access vlan 1
hostname(config-if-eth0/3)# exit
hostname(config)#
```

Step 2: Create a VLAN interface named vlan1, bind it to the zone trust and configure the IP address

```
hostname(config)# interface vlan1
hostname(config-if-vla1)# zone trust
hostname(config-if-vla1)# ip address 192.168.1.1 255.255.255.0
hostname(config-if-vla1)# exit
hostname(config)#
```

Step 3: Ethernet0/0 belongs to the zone untrust. Configure the policy rule from trust to untrust

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 4: Create RSTP, configure necessary parameters, and enable RSTP

```
hostname(config)# stp
hostname(config-stp)# bridge priority 0
hostname(config-stp)# enable
hostname(config-stp)# exit
hostname(config)#
```

Chapter 2 Policy

This section contains the following contents:

- "Security Policy": This section introduces the basic concepts of security policies, including policy rules, policy groups, web page redirection, and viewing policy rules.
- "Share Access": This section introduces how to configure shared access rules, configure shared access signature database, and share access logs.

Security Policy

Overview

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

Basic Elements of Policy Rules

Policy rules permit or deny traffic between security zone(s)/segment(s). The basic elements of policy rules are service type of the traffic, source and destination address/zone, and action.

- Source zone/address - The source zone/address of the traffic.
- Destination Zone/Address - The destination zone/address of the traffic.
- Service - The service type of the traffic.
- Action - The actions for processing traffic include Permit, Deny, Tunnel, From tunnel and WebAuth.

Below is a CLI example which permits the ICMP traffic from any address in the trust zone to any address in the untrust zone to pass through.

```
hostname(config)# policy-global
hostname(config-policy)# rule from any to any service icmp permit
```

- Source Address - Any, i.e., any address. It is the default address entry in the address book.
- Destination Address - Any, i.e., any address. It is the default address entry in the address book.

- Service － ICMP
- Action - Permit, i.e., this kind of traffic is permitted to pass through the device.

Defining a Policy Rule

Generally a policy rule consists of two parts: filtering condition and action. You can set the filtering condition by specifying traffic's source zone/address, destination zone/address, service type, and role. Each policy rule is labeled with a unique ID which is automatically generated when the rule is created. You can also specify a policy rule ID at your own choice. All policy rules in FSOS are arranged in a specific order. When traffic flows into a FS device, the device will query for policy rules in the list by turns, and processes the traffic according to the first matched rule.

The maximum global policy rule numbers may vary from different FS models.

Introduction to Profile

The combination of the profile and security policy allows the FS devices to implement fine-grained control over the application layer security policy. Profile defines different operations for different kinds of applications, which can simplify system configurations. FSOS support nine types of profiles, namely URL filter profile, Web content profile, Web posting profile, email filter profile, IM control profile, HTTP/FTP control profile, anti-virus profile, IPS profile and GTP profile. Each profile category can be configured with an action for a specific application.

QoS Tag

FSOS supports the QoS tag function in policy rules. You can add the QoS tag to a policy rule that permits the traffic to pass through.

Tip: For more information about QoS, see “QoS" of “Traffic Management”.

Configuring a Policy Rule

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

- Creating a policy rule
- Editing a policy rule
- Specifying the default action

Entering the Policy Configuration mode

To enter the policy configuration mode, in the global configuration mode, use the following command:

policy-global

Creating a Policy Rule

To create a policy rule, in the global configuration mode or policy configuration mode, use the following command:

rule [**id** *id*] [**name** *name*] [**top** | **before** {**name** *rule-name*| *id*} | **after** {**name** *rule-name*| *id*}] [**role** {**UNKNOWN** | *role-name*} | **user** *aaa-server-name user-name* | **user-group** *aaa-server-name user-group-name*] [**from** {**host** *host-name* | **range** *min-ip max-ip* | *src-addr* }] [**to** {**host** *host-name* | **range** *min-ip max-ip* | *dst-addr* }] [**from-zone** *zone-name* **to-zone** *zone-name*] [**service** *service-name*] [**application** *app-name*] [**permit** | **deny** | **tunnel** *tunnel-name* | **fromtunnel** *tunnel-name* | **webauth** | **portal-server** *server-name*]

- **id** *id* - Specifies the ID of the policy rule. If not specified, the system will automatically assign an ID to the policy rule. The ID must be unique in the entire system.
- **name** *name* – Specifies the name of the policy rule.
- **top** | **before** {**name** *rule-name*| *id*} | **after** {**name** *rule-name*| *id* - Specifies the location of the policy rule. By default, the newly-created policy rule is located at the end of all the rules.
  - **top** Specifies the location of the policy rule to the top of all rules.
  - **before** {**name** *rule-name*| *id*} – Specifies the location of the policy rule before the rule of specified ID or name.
  - **after** {**name** *rule-name*| *id* – Specifies the location of the policy rule after the rule of specified ID or name.
- **role** {**UNKNOWN** | *role-name*} | **user** *aaa-server-name user-name* | **user-group** *aaa-server-name user-group-name* - Specifies the role/user/user group for the policy rule.
  - **role** {**UNKNOWN** | *role-name*} – Specifies the role name. **UNKNOWN** is the role reserved by the system, i.e., the role that is neither authenticated nor statically bound.
  - **user** *aaa-server-name user-name* – Specifies the user. *aaa-server-name* is the AAA server the user belongs to, and *user-name* is the name of the user.
  - **user-group** *aaa-server-name user-group-name* – Specifies the user group. *aaa-server-name* is the AAA server the user group belongs to, and *user-group-name* is the name of the user group.
- **from** {**host** *host-name* | **range** *min-ip max-ip* | *src-addr* } – Specifies the source address of the policy rule.

- **host** *host-name* - The source address entry for the host defined in the address book.
- **range** *min-ip max-ip* – The source address entry for the IP addresses defined in the address book.
- *src-addr* – The address entry defined in the address book.

- **to** {**host** *host-name* | **range** *min-ip max-ip* | *dst-addr* } – Specifies the destination address of the policy rule.
  - **host** *host-name* – The destination address entry for the host defined in the address book.
  - **range** *min-ip max-ip* – The destination entry for the IP addresses defined in the address book.
  - *dst-addr* - The address entry defined in the address book.
- **from-zone** *zone-name* – Specifies the source zone of the policy rule.
- **to-zone** *zone-name* - Specifies the destination zone of the policy rule.
- **service** *service-name* - Specifies the service name of the policy rule. *service-name* is the service defined in the service book.
- **application** *app-name* – Specifies the application name for the policy rule. *app-name* is the application name you defined in the application book.
- **permit** | **deny** | **tunnel** *tunnel-name* | **fromtunnel** *tunnel-name*| **webauth** } - Specifies the action of the policy rule, including:
  - **permit** - Permits the traffic to pass through.
  - **deny** - Denies the traffic.
  - **tunnel** - For the traffic from local to a peer, this option allows the traffic to pass through the VPN tunnel.
  - **fromtunnel** - For the traffic from a peer to local, if this action is selected, FSOS will first determine if the traffic originates from a tunnel. Only such traffic will be permitted.
  - **webauth** - Performs Web authentication on the matched traffic.

For example, to create a policy rule that permits ICMP service from any address to any address, use the following commands:

```
hostname(config)# policy-global
hostname(config-policy)# rule from any to any service icmp permit
Rule id 5 is created.
```

To delete the policy rule, in the global configuration mode or policy configuration mode, use the following command:

no rule {**id** *id* | **name** *name*}

- **id** *id* – Deletes the policy rule of the specified ID.
- **name** *name* - Deletes the policy rule of the specified name.

Tip: For information about how to configure parameters of a policy rule, see "Editing a Policy Rule" .

Editing a Policy Rule

You can edit improper parameters for the policy rule in the policy rule configuration mode. To enter the policy rule configuration mode, in the global configuration or policy configuration mode, use the following command:

rule [**id** *id*] [**top** | **before** {**name** *name* | *id*} | **after** {**name** *name* | *id*]

After entering the policy rule configuration mode, to edit the policy rule, use the following commands:

- Name/rename a policy rule: **name** *policy-name*
- Specify/edit the source security zone:**src-zone** *src-zone*
- Delete the source security zone: **no src-zone**(after executing the command, there is no source zone restriction on the policy rule)
- Specify/edit the destination security zone: **dst-zone** *dst-zone*
- Delete the destination security zone: **no dst-zone**(after executing the command, there is no destination zone restriction on the policy rule)
- Add the source address of the address entry type: **src-addr** *src-addr*
- Delete the source address of the address entry type:**no src-addr** *src-addr*
- Add the source address of the IP member type: **src-ip** *ip/netmask*
- Delete the source address of the IP member type: **no src-ip** *ip/netmask*
- Add the source address of the host member type: **src-host** *host-name*

- Delete the source address of the host member type: **no src-host** *host-name*
- Add the source address of the IP range type: **src-range** *min-ip* [*max-ip*]
- Delete the source address of the IP range type: **no src-range** *min-ip* [*max-ip*]
- Add the destination address of the address entry type: **dst-addr** *dst-addr*
- Delete the destination address of the address entry type: **no dst-addr** *dst-addr*
- Add the destination address of the IP member type: **dst-ip** {*ip/netmask* | *ip-address netmask*}
- Delete the destinaion address of the IP member type: **no dst-ip** {*ip/netmask* | *ip-address netmask*}
- Add the destination address of the host member type: **dst-host** *host-name*
- Delete the destination address of the host member type: **no dst-host** *host-name*
- Add the destination address of the IP range type: **dst-range** *min-ip* [*max-ip*]
- Delete the destination address of the IP range type: **no dst-range** *min-ip* [*max-ip*]
- Add the service type: **service** *service-name*
- Delete the service type: **no service** *service-name*
- Add the application type: **application** *application-name*
- Delete the application type: **no application** *application-name*
- Specify the role: **role** {UNKNOWN | *role-name*}
- Delete the role: **no role** {UNKNOWN | *role-name*}
- Specify the user: **user** *aaa-server-name user-name*
- Delete the user: **no user** *aaa-server-name user-name*
- Specify the user group: **user-group** *aaa-server-name user-group-name*
- Delete the user group: **no user-group** *aaa-server-name user-group-name*
- Edit the action: **action** {**permit** | **deny** | **tunnel** | **fromtunnel** | **webauth**}
- Configure the schedule: **schedule** *schedule-name*
- Delete the schedule: **no schedule** *schedule-name*

Tip: By default, the configured policy rule will take effect immediately. If you apply a schedule to the policy rule, the rule will only take effect in the specified time defined in the schedule. You can configure up to 8 schedules for a policy rule, and the effective time of the policy rule is the sum of all time configured in the schedules.

- Adding the description: **description** *description*(the length of *description* is 1 to 255 bytes)
- Delete the description: **no description** *description*
- Edit the QoS tag of the rule: **policy-qos-tag** *tag*(the value range of *tag* is 1 to 1024)
- Delete the QoS tag of the rule: **no policy-qos-tag** *tag*
- Bind the anti-virus profile: **av** {*av-profile-name* | **no-av**} (**no-av** indicates binding the predefined Anti-Virus Profile named no-av, i.e., no Anti-Virus detection.)
- Cancel the anti-virus profile binding: **no av**
- Bind the IPS profile: **ips** {*ips-profile-name* | **no-ips**} (**no-ips** indicates binding the predefined IPS Profile named no-ips, i.e., no IPS detection.)
- Cancel the IPS profile binding: **no ips**
- Bind the HTTP/FTP control profile: **behavior** {*behavior-profile-name* | **no-behavior**} (**no-behavior** indicates binding the predefined HTTP/FTP control profile named no-behavior, i.e., no HTTP/FTP control.)
- Cancel the HTTP/FTP control profile binding： **no behavior**
- Bind the Web content profile： **contentfilter** {*contentfilter-profile-name* | **no-contentfilter**} (**no-contentfilter** indicates binding the predefined Web content profile named no-contentfilter, i.e., no Web content filter.)
- Cancel the Web content profile binding： **no contentfilter**
- Bind the Email filter profile： **mail** {*mail-profile-name* | **no-mail**} (**no-mail** indicates binding the predefined Email filter Profile named no-mail, i.e., no Email filter.)
- Cancel the Email filter profile binding： **no mail**
- Bind the IM control profile： **im** {*im-profile-name* | **no-im**} (**no-im** indicates binding the predefined IM control Profile named no-im, i.e., no IM control.)
- Cancel the IM control profile binding： **no im**

- Bind the Web posting profile: **webpost** {*webpost-profile-name* | **no-webpost**}（**no-webpost** indicates that you bind the predefined profile no-webpost to the policy rule and the system will not check the Web posting information.）
- Cancel the Web posting profile binding：**no webpost**
- Bind the URL filter profile: **url** {*url-profile-name* | **no-url**}（**no-url** indicates that you bind the predefined profile no-url to the policy rule and the system will not check and filter the URLs.）
- Cancel the URL filter profile binding：**no url**
- Bind the GTP profile：**gtp-profile** *profile-name*
- Cancel the GTP profile binding：**no gtp-profile**

Enabling/Disabling a Policy Rule

By default, the configured policy rule will take effect immediately. You can terminate its control over the traffic by disabling the rule. To enable or disable the policy rule, in the policy rule configuration mode, use the following commands:

- Disable：**disable**
- Enable：**enable**

Log Management of Policy Rules

- For the policy rules of action Permit, logs will be generated when the matched traffic session starts and ends.
- For the policy rules of action Deny, logs will be generated when the matched traffic is denied.

Before using this function, make sure the log function for the traffic is enabled. In the global configuration mode, use the command **logging traffic on**. To configure the log management of policy rules, in the policy rule configuration mode, use the following command:

```
log {policy-deny | session-start | session-end}
```

- **policy-deny** - Generates logs when the matched traffic is denied. This parameter is applicable to the policy rules of action Deny.
- **session-start** - Generates logs when the matched traffic starts its session. This parameter is applicable to the policy rules of action Permit.

- **session-end** - Generates logs when the matched traffic ends its session. This parameter is applicable to the policy rules of action Permit.

To cancel the log management configuration, in the policy rule configuration mode, use the command **no log** {**policy-deny** | **session-start** | **session-end**}.

In addition, for the traffic from the source security zone to the destination security zone that is not matched to any policy rule, you can specify whether to generate logs. By default, the system does not generate log for such kind of traffic. To generate log for such traffic, in the global policy configuration mode, use the following command:

log policy-default

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

no log policy-default

Specifying the Default Action

You can specify the default action for the traffic that is not matched to any configured policy rule. FSOS will process the traffic according to the specified default action. By default FSOS will deny such traffic. To specify the default action as Permit, in the global policy configuration mode, use the following command:

default-action permit

To restore to the default action of Deny, in the global policy configuration mode, use the following command:

no default-action permit

Moving a Policy Rule

Each policy rule is labeled with a unique ID and name. When traffic flows into a FS device, the device will query policy rules by turn, and processes the traffic according to the first matched rule. However, the policy rule ID is not related to the matching sequence during the query. The sequence displayed by the command show policy is the query sequence for policy rules (in the descending order). You can also specify the position for the policy rule when creating it, or modifying the position of the policy rule in the policy configuration mode. The rule position can be an absolute position, i.e., at the top or bottom, or a relative position, i.e., before or after an ID or a name. To move a policy rule, in the policy rule configuration mode, use the following command:

move {**name** *name* | *id*} {**top** | **bottom** | **before** {**name** *rule-name* | *id*} | **after** {**name** *rule-name* | *id*} }

- **name** *name* | *id* − Specifies the policy rule ID or name that you want to move.

- **top** – Moves the policy rule to the top of all rules.
- **before** {**name** rule-name | id} – Moves the policy rule before the rule of specified ID or name.
- **after** {**name** rule-name | id} – Moves the policy rule after the rule of specified ID or name.

Rule Redundancy Check

In order to make the rules in the policy are 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.

In any mode, use the following command to start redundancy check:

```
exec policy redundancy-check start
```

The check will last a few minuets, please wait. After checking, you can use **show policy redundancy-check** command to view the policy rule ID which is overshadowed.

You can also use **exec policy redundancy-check stop** command to stop check or use **exec policy redundancy-check clear** command to clear cache of last redundancy check results.

Policy Group

You can organize some policy rules together to form a policy group, and configure the policy group directly.

Configuring Policy Group

You can perform the following operations on a policy group through CLI:

- Creating/Deleting a policy group
- Enabling/Disabling a policy group
- Modifying/Deleting the Descriptions of a policy group
- Adding/Deleting a policy rule member
- Renaming a Policy Group
- Configuring a policy group for VSYS Profile

Creating/Deleting a Policy Group

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

policy-group *group-name*

- *group-name* – Specifies the name of the policy group. The length is 1 to 95 characters.

After executing this command, the CLI will enter the policy group configuration mode.

To delete a policy group, in the global configuration mode, use the following command:

no policy-group *group-name*

Enabling/Disabling a Policy Group

Policy group is enabled by default. To disable or enable the policy group, in the policy group configuration mode, use the following command:

- Enable: **enable**
- Disable: **disable**

Note:

- After disable or enable the policy group, the enabled status of policy rules in policy group are modified at the same time.
- Policy rules cannot be disabled or enabled when they are referenced.

Modifying/Deleting the Descriptions of a policy group

In the policy group configuration mode, use the following command to modify the description of a policy group.

description *description*

- *group-name* – Specifies the new description. You can enter at most 255 characters.

In the policy group configuration mode, use the following command to delete the description of a policy group.

no description

Adding/Deleting a Policy Rule Member

To add a policy rule member to the policy group, in the policy group configuration mode, use the following command:

rule *id*

- *id* – Specifies the policy rule ID.

To delete a policy rule member to the policy group, in the policy group configuration mode, use the following command:

no rule *id*

Note:A policy rule only can be added to a policy group.

Renaming a Policy Group

To rename a policy group entry, in the global configuration mode, use the following command:

rename policy-group *old-name new-name*

- *old-name* – Specifies the old name for the policy group.
- *new-name* – Specifies the new name for the policy group.

Configuring a policy group for VSYS Profile

To configure a policy group for VSYS Profile, in the VSYS Profile configuration mode, use the following command:

policy-group max *max-num* **reserve** *reserve-num*

- **max** *max-num* **reserve** *reserve-num* – Specifies the maximum quota (*max-num*) and reserved quota (**reserve** *reserve-num*) of policy group in VSYS. The reserved quota and maximum quota vary from different platforms. The reserved quota should not exceed the maximum quota.

Viewing Policy Group Information

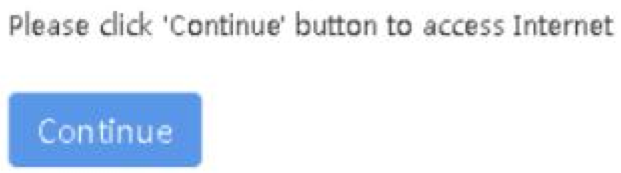
To view the policy group information, in any mode, use the following command:

show policy-group [*name*]

- *name* – Specifies the name of policy group for viewing the information.

User Online Notification

The user online notification function redirects your HTTP request to a new notification page when you visit Internet for the first time. In the process, a prompt page (see the picture below) will be shown first, and after you click **Continue** on this page, the system will redirect to the specified notification page. If you want to visit your original URL, you need to type the URL address in your Web browser.



Please click 'Continue' button to access Internet

To configure the user online notification function, take the following steps:

1. Enable WebAuth.
2. Create a policy rule to specify the traffic that will be redirected and the network resources accessible to the traffic.
3. Configure the notification page URL for the controlled traffic.

Note:To make the user online notification function take effect, the action for the policy rule must be Permit.

Configuring the User Online Notification URL

To configure the user online notification URL, in the policy rule configuration mode, use the following command:

web-redirect [*url*]

- *url* – Specifies the user online notification URL. The length is 1 to 127 characters. The URL format should be http://www.abc.com or https://www.abc.com. If the parameter is not specified, the webpage will be redirected to the URL originally specified by the user.

To cancel the user online notification URL, in the policy rule configuration mode, use the following command:

no web-redirect

Note:For more information about how to enter the policy rule configuration mode, see Entering the Policy Configuration mode

Configuring the Idle Time

The idle time refers to the time that a user keeps online without traffic transmitting. If an HTTP request exceeds the idle time, it will be redirected to the user online notification page again. To configure the idle time, in the global configuration mode, use the following command:

web-redirect idle-time *time-value*

- *time-value* – Specifies the idle time. The value range is 3 to 1440 minutes. The default value is 30.

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

no web-redirect idle-time

Customizing the Logo Picture

You can change the logo picture and customize your own user online notification page. To import the logo picture, you need zip the picture first, and then in the execution mode, use the following command:

import customize webredirect from {**ftp server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] | **tftp server** *ip-address* [**vrouter** *vrouter-name*]} *file-name*

- **ftp server** *ip-address* [**user** *user-name* **password** *password* [**vrouter** *vrouter-name*]] - Obtains the logo picture from the FTP server, and specifies the IP address, VRouter, username and password of the server. If no username and password are specified, you will log into the server anonymously.
- **tftp server** *ip-address* [**vrouter** *vrouter-name*] - Obtains the logo picture from the TFTP server, and specifies the IP address and VRouter of the TFTP server.
- *file-name* - Specifies the name of the zip file.

Note:The uploaded zip file should include the “logo.jpg” file.

To restore to the default logo picture, in any mode, use the following command:

exec customize webredirect default

Viewing Online Notification Users

To view the detailed information of online notification users, in any mode, use the following command:

show web-redirect-user

Viewing Policy Rule Information

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

show policy [**id** *id*] [**from** *src-zone*] [**to** *dst-zone*] [**src-addr** *src-addr*] [**dst-addr** *dst-addr*] [**service** *service-name*] [**application** *application-name*] [**description** *description*] [**name** *name*] [**name-filter** *filter-name*]

- **id** *id* - Shows the detailed information of the specified policy rule.
- **from** *src-zone* - Shows the detailed information of the policy rule whose source security zone is the specified zone.
- **to** *dst-zone* - Shows the detailed information of the policy rule whose destination security zone is the specified zone.
- **src-addr** *src-addr* – Shows the detailed information of the specified source address of the IP range type.
- **dst-addr** *dst-addr* – Shows the detailed information of the specified the destination address of the address entry type.
- **service** *service-name* – Shows the detailed information of the specified service type.
- **application** *application-name* – Shows the detailed information of the specified application type.
- **description** *description* – Shows the detailed information of the specified name rule.
- **name** *name* – Shows the detailed information of the specified name rule.
- **name-filter** *filter-name* – Shows the detailed information of all rules whose name includes the specified keyword.

Viewing the current policy configuration information of the device

To view the current policy configuration information of the device, in any mode, use the following command:

show configuration policy [**name** *name* | **id** *id* | **by-line**]

- **name** *name* – Shows the policy configuration information of the specified policy name in a single line.
- **id** *id* – Shows the policy configuration information of the specified policy ID in a single line.
- **by-line** – Shows all the policy configuration information in a single line.

Policy Hit Count

FSOS supports statistics on policy hit counts, i.e., it counts how many times the traffic matches a policy rule. Each time the inbound traffic matches a certain policy rule, the hit count will increment by one automatically. To view the policy hit count statistics, in any mode, use the following command:

show policy hit-count [**id** *id* | **name** *name* | [**from** *src-zone*] [**to** *dst-zone*] **top** {**10** | **20** | **50** | **all** }]

- **id** *id* - Shows the policy hit count statistics of the specified ID rule.
- **name** *name* – Shows the policy hit count statistics of the specified name rule.
- **from** *src-zone* - Shows the policy hit count statistics of the rule whose source security zone is the specified zone.
- **top** {**10** | **20** | **50** | **all** } - Shows the policy hit count statistics of the top 10, 20, 50 matched rules , or shows the policy hit count statistics of all policy rules in descending order.

Examples:

```
Shows the policy hit count statistics of all matched rules.

hostname(config)# show policy hit-count

Most hit policy rules:

==================================================================================

No. Id Src-zone Dst-zone Src-addr Dst-addr Service Applica~ Action Hit-count

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

1 14 trust trust Any Any Any PERMIT 0

2 4 untrust trust Any Any Any PERMIT 1

3 3 trust untrust Any Any Any PERMIT 761697

4 1 Any Any Any Any Any PERMIT 64203455

==================================================================================

Show the policy hit count statistics of the specified ID rule.

hostname(config)# show policy hit-count id 1

Policy id 1 is hit 342424 times
```

Show the policy hit count statistics of the specified name rule.

```
hostname(config)# show policy hit-count name a
Policy "a" is hit 0 times
```

Show the policy hit count statistics of the top 10 matched rules.

```
hostname(config)# show policy hit-count top 10
Most hit policy rules:
=============================================================
=========
No. Id Src-zone Dst-zone Src-addr Dst-addr Service Action Hit-count
----------------------------------------------------------------------
1 4 trust trust any any http permit 40029
2 6 zone2 untrust addr1 any any deny 7487
3 3 zone2 untrust s1 d1 ftp permit 3834
4 29 trust untrust any any any permit 2899
5 14 zone1 zone2 s2 any pop3 permit 2046
```

Show the policy hit count statistics of the all policy rules in descending order.

```
hostname(config)# show policy hit-count top all
Most hit policy rules:
=============================================================
==================
No. Id Src-zone Dst-zone Src-addr Dst-addr Service Applica~ Action Hit-count
--------------------------------------------------------------------------------
1 1 Any Any Any Any Any PERMIT 64212319
2 3 trust untrust Any Any Any PERMIT 762070
3 4 untrust trust Any Any Any PERMIT 1
4 14 trust trust Any Any Any PERMIT 0
=============================================================
==================
```

To clear the policy hit count statistics, in any mode, use the following command:

clear policy hit-count {**all** | **id** id | **name** name}

- **all** - Clears the policy hit count statistics of all the rules.
- **id** *id* - Clears the policy hit count statistics of all the specified ID rules.
- **name** *name* – Clears the policy hit count statistics of all the specified name rules.

To clear the policy hit count statistics of the default action, in any mode, use the following command:

clear policy hit-count default-action

Share Access

Share access means multiple endpoints access network with the same IP. The function of share access can block access from unknown device and allocate bandwidth for users, so as to prevent possible risks and ensure good online experience.

Share Access Rule

You can change the update configurations of share access rules as needed. The update configurations include:

- Creating share access rules
- Configuring share access rules
- Viewing share access rules

Creating Share Access Rules

To create the name of share access rule and enter the share access configuration mode, in the global configuration mode, use the following commands:

share-access-detect rule *rule-name*

- *rule-name* – Specifies the name of share access rule. If the rule of specified name already exists, enter the share access configuration mode directly.

To delete the share access rule, in the global configuration mode, use the following command:

no share-access-detect rule *rule-name*

Configuring Share Access Rules

To configure a share access rule, in the share access configuration mode, use the following commands:

- Specify the source zone of share access: **src-zone** *zone-name*
- Delete the source zone of share access: **no src-zone**
- Specify the source IP address segment of share access: **src-ip**{*ip/mask-len* | *ip netmask*}
- Delete the source IP address segment of share access: **no src-ip**{*ip/mask-len* | *ip netmask*}
- Specify the source IP address range of share access: **src-range** *begin-ip end-ip*
- Delete the source IP address range of share access: **no src-range** *begin-ip end-ip*
- Specify the source IP address book of share access: **src-addr** *addr*
- Delete the source IP address book of share access: **no src-addr** *addr*
- Enable/Disable the share access rule: **enable** | **disable**(enabled by default)
- Specify the schedule of share access: **schedule** *schedule-name*(The share access rule takes effect in the period specified by the schedule. If the schedule is not configured, the share access rule will always be effective.)
- Delete the schedule of share access: **no schedule**
- Specify the maximum number of share access endpoints: **access-limit** *limit-num*（(The range is 1-15. The default value is 2)
- Restore the default number of share access endpoints:**no access-limit**
- Specify the action when the number of endpoints exceeds the maximum: **action** {**log-only** | **warning**}(Actions include Warning and Log Only. The default action is Log Only.)
- Restore to the default action: **no action**
- Specify the control duration of warning:**control-duration** *duration*(When the selected action is Warning, system will send waring to all endpoints if the number of them exceeds the maximum. The range is 30-3600s and the default value is 60s)
- Restore the default control duration of warning: **no control-duration**
- Specify the timeout time of endpoint: **detected-endpoint-timeout** *time*(After the timeout time, when the endpoint no longer accesses network with the IP, system will clear the endpoint information. The range is 300-86400s. The default value is 600s)
- Restore the default timeout time of endpoint: **no detected-endpoint-timeout**
- Specify the sequence number of share access rules: **sequence** {**first** | **last** | *seq-id*}

- **first** – Specifies the sequence number of share access rule as No.1.
- **last** – Specifies the sequence number of share access rule as the last.
- *seq-id* – Specifies the sequence number of share access rules. The range is 1-8. The smaller the number, the higher the priority.

Viewing Share Access Rules

To view share access rules, in any mode, use the flowing command:

show share-access-detect rule [*rule-name*]

- *rule-name* – Specifies the name of share access rule. If you do not specify the name of rule, system will display the configurations of all rules by default.

Share Access Signature Database

You can change the update configurations of share access signature database as needed. The update configurations include:

- Configuring the update mode of share access signature database
- Updating now
- Importing a share access signature file
- Viewing update information of share access signature database
- Viewing information of share access signature database

Configuring the Update Mode of Share Access Signature Database

To update the share access signature database, in the global configuration mode, use the following command:

share-access-detect signature update [**mode** {**auto** | **manual**} | **proxy-server** {**main** | **backup**} *proxy-ip proxy-port* | **schedule** {**daily** [*HH:MM*] | **weekly** {**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**} } | **server1** {*domain* | *ip*} [**vrouter** *vrouter-name*] | **server2** {*domain* | *ip*} [**vrouter** *vrouter-name*] | **server3** {*domain* | *ip*} [**vrouter** *vrouter-name*]]

- **mode** {**auto** | **manual**} – Specifies the update mode of share access. System supports automatic and manual update modes. The default mode is automatic update.
- **proxy-server** {**main** | **backup**} *proxy-ip proxy-port* – Specifies the proxy server of share access database update.

- **schedule** {**daily** [*HH:MM*] | **weekly** {**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**} } – Specifies the automatic update schedule of share access database.
- **server1** {*domain* | *ip*} [**vrouter** *vrouter-name*] – Specifies the domain, IP address and VRouter of update server 1.
- **server2** {*domain* | *ip*} [**vrouter** *vrouter-name*] – Specifies the domain, IP address and VRouter of update server 2.
- **server3** {*domain* | *ip*} [**vrouter** *vrouter-name*] – Specifies the domain, IP address and VRouter of update server 3.

Updating Share Access Signature Database

To update the share access signature database immediately, in the execution mode, use the following command:

exec share-access-detect signature update

Importing a Share Access Signature File

In some cases, your device may be unable to connect to the update server to update the share access signature database. To solve this problem, FSOS provides the file import function of share access signature database, i.e., importing the share access signature files to the device from an FTP or TFTP server, so that the device can update the share access signature database locally. To import the share access signature file, in the execution mode, use the following command:

import share-access-detect signature from {**ftp server** { *A.B.C.D* | *X:X:X:X::X* } [**vrouter** *vrouter-name*] [**user** *username* **password** *string*] | **tftp server** { *A.B.C.D* | *X:X:X:X::X* }[**vrouter** *vrouter-name*]} *file-name*

- **ftp server** { *A.B.C.D* | *X:X:X:X::X* } [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] – Specifies the IP address, VRouter, user name and password of FTP server to import share access signature files. You can log in the server anonymously without typing user name and password.
- **tftp server** { *A.B.C.D* | *X:X:X:X::X* } [**vrouter** *vrouter-name*] – Specifies the IP address and VRouter of TFTP server to import share access signature files.
- *file-name* – Specifies the name of the share access signature file to be imported.

Viewing Update Information of Share Access Signature Database

To view the update information of share access signature database, in any mode, use the following command:

show share-access-detect signature update

Viewing Information of Share Access Signature Database

To view the information of share access signature database, in any mode, use the following command:

show share-access-detect signature info

Viewing Statistics of Share Access

To view the statistics of share access, in any mode, use the following command:

show share-access-detect statistics [**rule** *rule-name*] [**src-ip** *ip-address*] [**src-zone** *zone-name*] [**status** {**normal** | **logging** | **warning**}] [**endpoint-num** {**gt** | **lt** | **eq**} *number*]

- **rule** *rule-name* – Displays the endpoints statistics of the specified share access rule.
- **src-ip** *ip-address* – Displays the endpoints statistics of the specified source IP.
- **src-zone** *zone-name* – Displays the endpoints statistics of the specified source zone.
- **status** {**normal** | **logging** | **warning**} – Displays the endpoints statistics in the specified status.
    - **normal** – Displays the endpoints statistics when the status of endpoint IP address is normal.
    - **logging** – Displays the endpoints statistics when the status of endpoint IP address is logging.
    - **warning** – Displays the endpoints statistics when the status of endpoint IP address is warning.
- **endpoint-num** {**gt** | **lt** | **eq**} *number* – Displays the statistics of endpoints which meets the specified number.
    - **gt** – Displays the statistics of endpoints whose number is more than the specified number.
    - **lt** – Displays the statistics of endpoints whose number is less than the specified number.
    - **eq** – Displays the statistics of endpoints whose number is equal to the specified number.
    - *number* – Displays the number of endpoints.

Share Access Log

You can change the update configurations of share access log as needed. The update configurations include:

- Configuring the status of share access log
- Configuring the output destination of share access log
- Viewing share access logs

Configuring the Status of Share Access Log

To enable the share access log, in the global configuration, use the following command. The function is enabled by default.

logging share-access-detect on

To disable the share access log, in the global configuration, use the following command:

no logging share-access-detect on

Configuring the Output Destination of Share Access Log

You can specify the output destination of share access log as needed, including syslog server, buffer and console. The default destination is buffer. In the global configuration mode, use the following command:

logging share-access-detect to { **syslog** | **buffer** [**size** *buffer-size*] | **console**}

- **syslog** – Sends the share access logs to the syslog server.
- **buffer** [**size** *buffer-size*] – Sends the share access log to the buffer and specifies the memory of buffer. The range is 4096-524288 bytes. The default value is 524288.
- **console** – Sends the share access log to the console.

To cancel the output destination configuration of share access log, in the global configuration mode, use the following command:

no logging share-access-detect to { **syslog** | **buffer** [**size** *buffer-size*] | **console**}

Viewing Share Access Logs

To view the share access log, in any mode, use the following command:

show logging share-access-detect

Chapter 3 Routing

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

FS devices are designed with Layer 3 routing. This function allows you to configure routing options and forward various packets via VRouter. The routings supported by the FS devices include Destination Routing, ISP Routing, Source-Based Routing (SBR), Source-Interface-Based Routing (SIBR), Destination-Interface-Based Routing (DIBR), Policy-Based Routing (PBR), Proximity Routing, Dynamic Routing (including RIP, OSPF and BGP), Equal Cost MultiPath Routing (ECMP) and Static Multicast-routing.

This section contains the following contents:

- "Destination Route"： A manually-configured route which determines the next routing hop according to the destination IP address.
- "Destination Interface Route"： A manually-configured route which determines the next routing hop according to the destination IP address and ingress interface.
- "ISP Route”： A kind of route which determines the next hop based on different ISPs.
- "Source Route"： Source IP based route which selects routers and forwards data according to the source IP address.
- "Src-If Route "： Source IP and ingress interface based route.
- "Policy-based Route": A route which forwards data based on the source IP, destination IP address and service type.
- Proximity routing: Selects routers and forwards data according to the result of proximity detection.
- "Dynamic Routing"： Selects routers and forwards data according to the dynamic routing table generated by dynamic routing protocols (RIP, OSPF, IS-IS, or BGP).
- "ECMP"： Load balancing traffic destined to the same IP address or segment in multiple routes with equal administration distance.
- "Static Multicast Routing"： a manually-configured route which broadcasts packets from a multicasting source to all the members within a group.

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

Enabling/Disabling Static Routing Query

For PBR, SBR , SIBR and DIBR, you can control the query on them separately (the system requires that the destination routing query must be enabled). By default, the BR, SBR , SIBR and DIBR query are enabled. To enable/disable the query on them, in the global configuration mode, use the following commands (applicable to all VRouters):

- Enable: **route enable** {**pbr** | **sibr** | **sbr** |**dibr**}
- Disable: **route disable** {**pbr** | **sibr** | **sbr** | **dibr**}

Tip: For the configuration example of enabling/disabling static routing query, see "Example of Configuring Static Route Query" .

Enabling/Disabling the Route Rematch by Session

By default, the function of route rematch by session is enabled. When you add, modify or delete the route, the session will match the optimal route again. During the process, the session which corresponds to the following rules will be deleted:

- When the route or the egress interface of the route that the session matched before is deleted, the session will be deleted.
- When the route that the session matched before is not the optimal route and the egress interface of the matched route later is changed, the session will be deleted.

In some cases (such as adding or deleting the application bound with PBR rule), a large number of sessions may be deleted, which will lead to traffic anomaly. Meanwhile, you should disable the function of route rematch by session.

To disable or enable this function, in the Flow configuration mode, use the following command:

- **session rematch route disable**
- **session rematch route enable**

VRouter

VR virtually acts as a router, and different VRouters have their own independent routing tables. A VRouter named trust-vr is bundled with the system. FS devices support multiple VRouters (a function known as multi-VR). All the routing configuration of the FS devices must be performed in an appropriate VRouter configuration mode. To enter the VRouter configuration mode, in global configuration mode, use the following command:

ip vrouter *vrouter-name*

- *vrouter-name* - Specifies the name of VRouter.

In the VRouter Configuration mode, you can configure static routing entries, dynamic routing protocols, or specify the maximum number of routing entries supported by the VRouter, as well as import routing entries from other VRouters.

To use the multi-VR function, you need to run **exec vrouter enable** first, and then reboot the system to make multi-VR take effect.

Tip: For the multi-VR configuration examples, see "Example of Configuring Multi-VR".

Specifying the Maximum Number of Routing Entries

To specify the maximum number of routing entries permitted by a VRouter (including all direct routes, static routes and dynamic routes of the VRouter), in the VRouter configuration mode, use the following command:

max-routes *number*

- *number* - Specifies the maximum number of routing entries. The value range is 1 to 100000.

To cancel the specified maximum number of routing entries, in the VRouter configuration mode, use the following command:

no max-routes

When reaching the maximum number of routing entries, the system will issue an alarm.

Importing VRouter Routing Entries

You can import routing entries from other VRouters to your own VRouter. In the VRouter configuration mode, use the following command:

import vrouter *vrouter-name* {**connected** | **static** | **rip** | **ospf** | **bgp**}

- *vrouter-name*- Specifies the name of the VRouter the imported routing entry belongs to.
- **connected** | **static** | **rip** | **ospf** | **bgp** - Specifies the type of the routing entry that will be imported.

Repeat the above command to import routing entries of different types.

Note:The priority of routing entries imported from other VRouters is lower than the priority of the entries bundled with the original VRouter.

Disable the Highest Priority of Direct Route

Direct route has the highest route priority, when you configure other roures in the same time, the direct route will be used first, makes the other route is not effective. Therefore, you can according to need, disable the highest priority of direct route. In the VRouter configuration mode, use the following command:

fib-lookup connect-first-disable

To restore the he highest priority of direct route, in the VRouter configuration mode, use the following command:

no fib-lookup connect-first-disable

Destination Route

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

Configuring a Destination Route

You can add a destination route and view the route's information through CLI.

Adding a Destination Route

You can add a destination routing entry to VRouter. However, before adding the entry, you need to enter the VRouter configuration mode. In the global configuration mode, use the following command:

ip vrouter *vrouter-name*

- *vrouter-name* - Specifies the name of the VRouter.

To add a destination route, in the VRouter configuration mode, use the following command:

ip route {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**tag** *tag-value*] [**description** *description*] [**schedule** *schedule-name*]

- *A.B.C.D/M* | *A.B.C.D A.B.C.D* - Specifies the destination address. The FS devices support two formats: A.B.C.D/M or A.B.C.D A.B.C.D, for example, 1.1.1.0/24 or 1.1.1.0 255.255.255.0.

- *A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*- Specifies the type of next hop which can be a gateway address (*A.B.C.D*), interface (*interface-name*) or VRouter (**vrouter** *vrouter-name*). If the next hop type is interface, you can select a tunnel interface (for multi-tunnel interface, you must specify the next hop IP address of IPsec VPN, GRE or SCVPN tunnel by the *A.B.C.D* parameter, and this address must be the same as the next hop IP address of the corresponding tunnel bound to the tunnel interface), Null0 interface or PPPoE interface.

- *distance-value* - Specifies the administration distance of the route. This parameter is used to determine the precedence of the route. The smaller the value is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route is invalid.

- **weight** *weight-value* - Specifies the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.

- **tag** *tag-value* – Specifies the tag value of the destination route. When OSPF redistributes routes, if the configured routing tag values here are matched to the rules in the routing mapping table, the route will be redistributed to filter its information. The value range is 1 to 4294967295.

- **description** *description* – Specifies the description of this route. You can enter at most 63 characters.

- **schedule** *schedule-name*- Specifies the name of the schedule defined in the system. The configuration will only take effect during the specified period. Repeat the command to specify more schedules (up to 8). To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.

Repeat the above command to add more destination routes.

To delete the specified static destination route, use the following command:

no ip route {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*}[**description** *description*] [**schedule** *schedule-name*]

Viewing destination routing information

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

show ip route static [**vrouter** *vrouter-name*]

- *vrouter-name* - Specifies the destination route information of the specified VRouter.

Destination Interface Route

Destination-Interface-Based Routing(DIBR) is a manually-configured route which determines the next routing hop according to the destination IP address and ingress interface.

Adding a Destination Interface Route

You can add a destination interface routing entry to VRouter. However, before adding the entry, you need to enter the VRouter configuration mode. In the global configuration mode, use the following command:

ip vrouter *vrouter-name*

- *vrouter-name* - Specifies the name of the VRouter.

To add a destination interface route, in the VRouter configuration mode, use the following command:

ip route in-interface *interface-name* {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**description** *description*] [**schedule** *schedule-name*]

- **in-interface** *interface-name* - Specifies the ingress interface of the route.
- *A.B.C.D/M* | *A.B.C.D A.B.C.D* - Specifies the destination address. The FS devices support two formats: *A.B.C.D/M* or *A.B.C.D A.B.C.D*, for example, 1.1.1.0/24 or 1.1.1.0 255.255.255.0.
- *A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name* - Specifies the type of next hop which can be a gateway address (*A.B.C.D*), interface (*interface-name*) or VRouter (*vrouter vrouter-name*). If the next hop type is interface, you can select a tunnel interface (for multi-tunnel interface, you must specify the next hop IP address of IPsec VPN, GRE or SCVPN tunnel by the *A.B.C.D* parameter, and this address must be the same as the next hop IP address of the corresponding tunnel bound to the tunnel interface), Null0 interface or PPPoE interface.
- *.distance-value*- Specifies the administration distance of the route. This parameter is used to determine the precedence of the route. The smaller the value is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route is invalid.
- **weight** *weight-value* - Specifies the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
- **description** *description* – Specifies the description of this route. You can enter at most 63 characters.

- **schedule** *schedule-name* - Specifies the name of the schedule defined in the system. The configuration will only take effect during the specified period. Repeat the command to specify more schedules (up to 8). To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.

Repeat the above command to add more destination interface routes.

To delete the specified destination interface route, use the following command:

no ip route in-interface *interface-name* {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*} [**description** *description*] [**schedule** *schedule-name*]

Viewing Destination Interface Route Information

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

show {ipv4| ipv6} fib in-interface *interface-name*

- **in-interface** *interface-name* - Specifies the ingress interface of the route.

Viewing FIB Information about Destination Interface Route

To view the FIB information about destination interface route, in any mode, use the following command:

show ip fib in-interface *interface-name*

- **in-interface** *interface-name* - Specifies the ingress interface of the route.

ISP Route

Generally many users might apply for multiple lines for load balancing purpose. However, a typical balance will not function based on the traffic's direction. If a server in ISP A is accessed through ISP B, the speed will be rather low. For such a scenario, FSOS provides ISP Route which allows traffics 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.

In an ISP route configuration, you can perform the following operations:

- Configuring ISP information
- Configuring an ISP route

- Uploading an ISP route configuration file
- Viewing ISP route configuration information
- Deleting an uploaded predefined ISP configuration file

Configuring ISP Information

To configure ISP information on the device, first, you need to enter the ISP information configuration mode. To create an ISP name and enter the ISP information configuration mode, in the global configuration mode, use the following command:

isp-network *isp-name*

- *isp-name* - Specifies the name of ISP.

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

no isp-network *isp-name*

To add a subnet entry to ISP, in the ISP information configuration mode, use the following command:

subnet *A.B.C.D/M*

- *A.B.C.D/M* - Specifies the subnet for the ISP, in the form of IP address/netmask, for example, 1.1.1.0/24.

In the ISP information configuration mode, repeat the above command to add multiple subnets for the ISP.

To delete the specified subnet, in the ISP information configuration mode, use the following command:

no subnet *A.B.C.D/M*

Configuring an ISP Route

To configure an ISP route, you need to enter the VRouter configuration mode. In the global configuration mode, use the following command:

ip vrouter *vrouter-name*

- *vrouter-name* - Specifies the name of VRouter.

To configure an ISP route, in the VRouter configuration mode, use the following command:

ip route *isp-name* {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**description** *description*] [**schedule** *schedule-name*]

- *isp-name* - Specifies an existing ISP in the system as the destination address of the route.
- *A.B.C.D* | *interface-name* | **vrouter** *vrouter-name*- Specifies the type of next hop which can be a gateway address (*A.B.C.D*), interface (*interface-name*) or VRouter (**vrouter** *vrouter-name*). If the next hop type is interface, you can select a tunnel interface, Null0 interface or PPPoE interface.
- *distance-value* - Specifies the administration distance of the route. This parameter is used to determine the precedence of the route. The smaller the value is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route is invalid.
- **weight** *weight-value* - Specifies the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
- **description** *description* – Specifies the description of this route. You can enter at most 63 characters.
- **schedule** *schedule-name* - Specifies the name of the schedule defined in the system. The configuration will only take effect during the specified period. Repeat the command to specify more schedules (up to 8). To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.

Repeat the above command to add multiple ISP routes.

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

no ip route *isp-name* {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* } [*distance-value*] [**weight** *weight-value*] [**description** *description*] [**schedule** *schedule-name*]

Viewing ISP Route Configuration Information

To view the ISP route configuration information, use the following commands:

- View the ISP information configured in the device:
  show isp-network {**all** | *isp-name*}
- View the ISP route:
  show ip route isp [*isp-name* | **vrouter***vrouter-name*]

Uploading an ISP Profile

The ISP profiles can only be uploaded through WebUI. FS devices support two types of ISP profiles: user-defined ISP profiles and predefined ISP profiles.

Follow the format example shown below to compile a user-defined profile. Otherwise, even if the file is uploaded successfully, it will not take effect in the system. One single predefined/user-defined ISP profile can contain up to 26 ISPs, i.e., the number of the alphabetic letters that are used as the index.

```
# NOTICE: Keep the following comment lines intact!!!
E --- China-55
R --- China-66
# China-55
E:55.10.2.0/24
E:55.10.3.0/24
# China-66
R:66.20.2.0/24
R:66.20.3.0/24
```

Uploading a Predefined ISP Profile

The predefined ISP profile shipped with FSOS is encrypted. If the predefined profile has been updated, you need to upload the new profile. To upload an ISP profile, take the following steps:

1. On the navigation pane, click **Configure** > **Network** > **Routing** to visit the Routing page.
2. On the **ISP Profile** tab, click **Upload**.
3. In the Upload ISP Configuration from PC dialog, click **Upload predefined IPS file** or **Upload user-defined IPS file**.
4. Click **Browse** to select an ISP profile in your PC, and click **Upload** to upload it to FSOS. The version number is displayed in the Current predefined ISP line below.

Saving a User-defined ISP Profile

To save a user-defined ISP profile to your PC, take the following steps:

1. On the Navigation pane, click **Configure** > **Network** > **Routing** to visit the Routing page.
2. On the **ISP Profile** tab, click **Save**.
3. In the Save User-defined ISP Configuration to PC dialog, select an ISP profile from the **ISP profile** drop-down list.
4. Click **Save** to save the profile to a specified location in PC.

Deleting an Uploaded Predefined ISP Profile

If the predefined ISP profile has already been uploaded, you can delete the profile from the system. To do that, in the execution mode, use the following command:

exec isp-network clear-predefine

After executing the above command and rebooting, the system will be restored to use the original predefined ISP profile (the default predefined ISP profile shipped with the system).

Source Route

The source route can only be configured in the VRouter configuration mode. To enter the VRouter configuration mode, in global configuration mode, use the following command:

ip vrouter *vrouter-name*

Adding a Source Route

To add a source route, in the VRouter configuration mode, use the following command:

ip route source {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**schedule** *schedule-name*]

- *A.B.C.D/M* | *A.B.C.D A.B.C.D* - Specifies the destination address. The FS devices support two formats: *A.B.C.D/M* or *A.B.C.D A.B.C.D*, for example, 1.1.1.0/24 or 1.1.1.0 255.255.255.0.
- *A.B.C.D* | *interface-name* - Specifies the type of next hop which can be a gateway address (*A.B.C.D*), interface (*interface-name*) or VRouter (**vrouter** *vrouter-name*).If the next hop type is interface, you can select a tunnel interface, Null0 interface or PPPoE interface.
- *distance-value* - Specifies the administration distance of the route. This parameter is used to determine the precedence of the route. The smaller the value is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route is invalid.
- **weight** *weight-value* - Specifies the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
- **schedule** *schedule-name*- Specifies the name of the schedule defined in the system. The configuration will only take effect during the specified period. Repeat the command to specify more schedules (up to 8). To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.

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

no ip route source { *A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name*}

Viewing Source Route Information

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

show ip route source [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the source route information of the specified VRouter.

Src-If Route

The Src-If route can only be configured in the VRouter configuration mode. To enter the VRouter configuration mode, in global configuration mode, use the following command:

ip vrouter *vrouter-name*

Adding a Src-If Route

To add a Src-If route, in the VRouter configuration mode, use the following command:

ip route source in-interface *interface-name* { *A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**schedule** *schedule-name*]

- *interface-name* - Specifies the ingress interface of the route.
- *A.B.C.D/M* | *A.B.C.D A.B.C.D* - Specifies the destination address. The FS devices support two formats: *A.B.C.D/M* or *A.B.C.D A.B.C.D*, for example, 1.1.1.0/24 or 1.1.1.0 255.255.255.0.
- *A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* - Specifies the type of next hop which can be a gateway address (*A.B.C.D*), interface (*interface-name*) or VRouter (**vrouter** *vrouter-name*). If the next hop type is interface, you can select a tunnel interface or Null0 interface.
- *distance-value* - Specifies the administration distance of the route. This parameter is used to determine the precedence of the route. The smaller the value is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route is invalid.
- **weight** *weight-value* - Specifies the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.

- **schedule** *schedule-name*- Specifies the name of the schedule defined in the system. The configuration will only take effect during the specified period. Repeat the command to specify more schedules (up to 8). To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.

To delete the specified Src-If route, in the VRouter configuration mode, use the following command:

no ip route source in-interface *interface-name* { *A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* }

Viewing Src-If Route Information

To view the Src-If route information, in any mode, use the following command:

show ip route source in-interface *interface-name*

Policy-based Route

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

Creating a PBR Policy

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

pbr-policy *name*

- *name* - Specifies the name of the PBR policy. The length is 1 to 31 characters. If the policy exists, the system will directly enter the PBR policy configuration mode.

To delete the specified PBR policy, use the command**no pbr-policy** *name*.

Creating a PBR Rule

To create a PBR rule, in the PBR policy configuration mode, use the following command:

{**match** | **match-v6** } [**id** *rule-id*] [**before***rule-id* | **after** rule-id | **top**] *src-addr dst-addr service-name* [*application-name*] **nexthop** {*interface-name* | *A.B.C.D* | **vrouter** *vrouter-name* | **vsys** *vsys-name*} [**weight** *value*] [**track** *track-object-name*]

- **id** *rule-id*- Specifies the ID of the new PBR rule. The value range is 1 to 255. If no ID is specified, the system will automatically assign an ID. The rule ID must be unique in its corresponding PBR policy.

- **before** *rule-id* | **after** *rule-id* | **top** - Specifies the position of the PBR rule. The new PBR rule can be located before a rule (**before** *rule-id*), after a rule (**after** *rule-id*) or at the top of all the rules (**top**). By default, the system will put the new rule at the end of all the rules.
- *src-addr* - Specifies the source address which should be an entry defined in the address book.
- *dst-addr* - Specify the destination address which should be an entry defined in the address book.
- *service-name* – - Specifies the name of the service.*service-name*should be the service defined in the service book.
- *application-name* – Specifies the name of the application.*application-name* should be the application defined in the application book.
- **nexthop** {*interface-name* | *A.B.C.D* | **vrouter** *vrouter-name* | **vsys** *vsys-name*} - Specifies the next hop. *interface-name* is the name of egress interface, *A.B.C.D* is the IP address of the next hop, **vrouter** *vrouter-name* is a VRouter, and **vsys** *vsys-name* is the name of VSYS.
- **weight** *value* - Specifies the weight for the next hop. The value range is 1 to 255. The default value is 1. If a PBR rule is configured with multiple next hops, the system will distribute the traffic in proportion to the corresponding weight.
- **track** *track-object-name* - Specifies the track object for the next hop. If the track object fails, the PBR rule will fail as well. For more information about track object, see "Configuring a Track Object" in "System Management".

To delete the specified rule, in the PBR policy configuration mode, use the following command:

no match id *rule-id*

In addition, you can also use the following command in PBR policy configuration mode to create a PBR rule ID, and then in the PBR policy rules configuration mode, further configure other relevant parameters of the PBR rule:

match [**id** *rule-id*] [**before** *rule-id* | **after** *rule-id* | **top**]

- **id** *id* - Specifies the ID of the new PBR rule. If no ID is specified, the system will automatically assign an ID. The rule ID must be unique in the whole system. However, the PBR rule ID is not related to the matching sequence.
- **top** | **before** *rule-id* | **after** *rule-id* - Specifies the position of the PBR rule. The new PBR rule can be located before a rule (**before** *rule-id*), after a rule (**after** *rule-id*) or at the top of all the rules (**top**). By default, the system will put the newly created rule at the end of all the rules.

Note:For more information about how to configure other policy-related parameter, see "Editing a PBR Rule"。

Editing a PBR Rule

You can edit an existing PBR rule by modifying its inappropriate parameters. However, this modification can only be performed in the PBR policy configuration mode. To enter the PBR policy configuration mode, use the following commands:

- **match** [**id** *rule-id*] [**before** *rule-id* | **after** *rule-id* | **top**]
- **match id** *rule-id*(only applicable to the existing rule ID. To delete the rule, use the command**no match id** *rule-id*)

To edit the rule, in the PBR policy rules configuration mode, use the following commands:

- Add a source address of address entry type: **src-addr** *src-addr*
- Delete a source address of address entry type: **no src-addr** *src-addr*
- Add a source address of IP address type: **src-ip** {*ip/netmask* | *ip-addressnetmask*}
- Delete a source address of IP address type: **no src-ip** {*ip/netmask* | *ip-address netmask*}
- Add a source address of host name type: **src-host** *host-name*
- Delete a source address of host name type: **no src-host** *host-name*
- Add a source address of IP range type: **src-range** *min-ip max-ip*
- Delete a source address of IP range type: **no src-range** *min-ip max-ip*
- Add a destination address of address entry type: **dst-addr** *dst-addr*
- Delete a destination address of address entry type: **no dst-addr** *dst-addr*
- Add a destination address of IP address type: **dst-ip** *ip/netmask*
- Delete a destination address of IP address type: **no dst-ip** *ip/netmask*
- Add a destination address of host name type: **dst-host** *host-name*
- Delete a destination address of host name type: **no dst-host** *host-name*
- Add a destination address of IP range type: **dst-range** *min-ip* [*max-ip*]
- Delete a destination address of IP range type: **no dst-range** *min-ip* [*max-ip*]
- Add a source user of role type: **role** *role-name*

- Delete a source user of role type: **no role** *role-name*
- Add a source user of user type: **user** *aaa-server-name user-name*
- Delete a source user of user type: **no user** *aaa-server-name user-name*
- Add a source user of user group type: **user-group** *aaa-server-name user-group-name*
- Delete a source user of user group type: **no user-group** *aaa-server-name user-group-name*
- Add a service: **service** *service-name*
- Delete a service: **no service** *service-name*
- Add an application: **application** *application-name*
- Delete an application: **no application** *application-name*
- Specify the next hop: **nexthop** {*interface-name* | *A.B.C.D* | *vrouter-name* | **vsys** *vsys-name*}
- Cancel the next hop: **no nexthop**
- Specify a schedule: **schedule** *schedule-name*
- Delete the schedule: **no schedule**
- Add a rule description: **description** *string*
- Delete a rule description: **no description**
- Enable the logging function for PBR rules： **log enable**
- Disable the logging function for PBR rules： **no log enable**

Enabling/Disabling a PBR Rule

By default the configured PBR rules will take effect immediately. You can disable a rule to end its control over traffic. To enable or disable a PBR rule, in the PBR policy rules configuration mode, use the following commands:

- Disable: **disable**
- Enable: **enable**

Moving a PBR Rule

Each PBR rule is labeled with a unique ID. When traffic flows into a FS device, the device will query for PBR rules by turn, and processes the traffic according to the first matched rule. However, the PBR rule

ID is not related to the matching sequence during the query. The rule sequence displayed by the command show pbr-policy is the actual sequence for the rule matching (the system will match the rules from the top to the bottom). You can specify the location of a PBR policy rule when creating the rule or moving its position in the PBR policy rule configuration mode. The positions of a PBR policy rule can be either an absolute position, i.e., at the top or bottom, or a relative position, i.e., before or after a specific rule ID. To move a PBR rule, in the PBR policy configuration mode, use the following command:

move *rule-id* {**top** | **bottom** | **before** *rule-id* | **after** *rule-id*}

Configuring Prioritized Destination Routing Lookup

By default, when forwarding the inbound packets, the device selects a route in the following sequence: PBR > SIBR > SBR > Destination Routing. In some cases, users need to prioritized the destination route for the packets that are matching a PBR rule, that is the sequence is Destination Routing >PBR. To configure the prioritized destination routing (DBR) lookup, in the PBR policy configuration mode, use the following command:

fib-lookup dbr-first

To cancel prioritized destination routing (DBR) lookup, in the PBR policy configuration mode, use the following command:**no fib-lookup dbr-first**

Applying a PBR Rule

You can apply a PBR rule by binding it to an interface, zone or VRouter. In the interface configuration mode , security zone configuration mode or VRouter configutation mode, use the following command:

bind pbr-policy *name*

- *name* - The interface , security zone or VRouter the specified PBR rule is bound to.

To cancel the PBR rule binding to the interface, security zone or VRouter, in the interface configuration mode , security zone configuration mode or VRouter configutation mode, use the following command:

no bind pbr-policy

Configuring the Global Match Order of PBR

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

pbr-match order *index*

- *index* – Specifies the index of global match order of PBR, including 1 to 6, the order index is expressed as follows:
  - 1 – Interface >Zone >Vrouter, it is the default match order of PBR.
  - 2 – Zone >interface >Vrouter.
  - 3 - Vrouter >Zone > Interface.
  - 4 - Interface -> Vrouter >Zone.
  - 5 - Vrouter > Interface > Zone.
  - 6 – Zone > Vrouter > Interface.

To restore to the default match order, in the global configuration mode, use the command **no pbr-match**.

Viewing the the Global Match Order of PBR

In any mode, use the following command:

```
show pbr-match order
```

Configuring TTL Range for a PBR Rule

You can configure TTL range of packets for a PBR rule, and packet which matches the PBR rule will be forwarded to the specific export link. To configure TTL range, you need to enter PBR policy rule configuration mode first, use the following commands:

- **match** [**id** *rule-id*] [**before** *rule-id* | **after** *rule-id* | **top**]
- **match id** *rule-i*d(only applicable to the existing rule ID)

In the PBR policy rule configuration mode, use the following commands:

ttl-range *min-ttl max-ttl*

- *min-ttl max-ttl* - Specifies the TTL range for the PBR rule. *min-ttl* specifies the minimum value of TTL, and it is in the range of 1 to 255. *max-ttl* specifies the maximum value of TTL, and it is in the range of 1 to 255.

In the PBR policy rule configuration mode, use **no ttl-range** command to cancel the TTL configuration.

Viewing PBR Rule Information

To view the specific PBR rule information, in any mode, use the following command to:

show pbr-policy [*name*]

- *name* - Shows the specified PBR rule information. If no name is specified, the command will show the details of all the PBR rules.

DNS Redirect

The DNS redirect function redirects the DNS requests to a specified DNS server. In this version, the DNS redirect function is mainly used to redirect the video traffic for load balancing. With the policy based route working together, the system can redirect the Web video traffic to different links, improving the user experience.

To enable or disable the DNS redirect function, in the global configuration mode, use the following command:

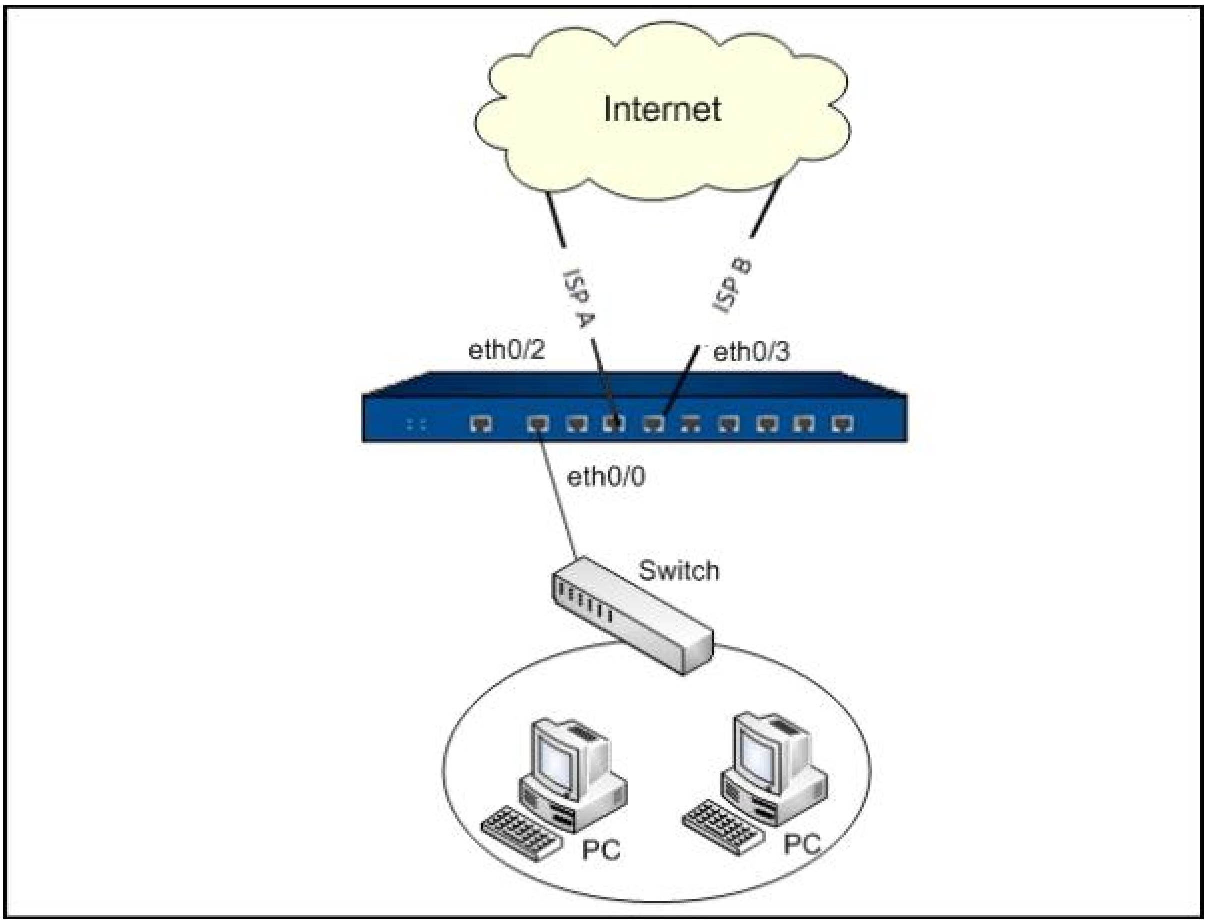
```
app cache dns-redirect {enable | disable}
```

- **enable** – Enable the DNS redirect function. After enabling this function, specify the DNS server address according to the prompts provided by the system. Then the DNS requests will be redirect to the specified DNS server.
- **disable** – Disable the DNS redirect function. It is the default status of the function.

In any mode, use the **show dns-redirect** command to show the binding status between the DNS server and the ingress interface that is bound to the PBR policy.

Configuration Example of Web Video Traffic Redirection

FS device is deployed at the ingress interface of the internet. The ethernet0/0 interface connects to the PC, and the ethernet0/2 and ethernet0/3 interfaces connect to two ISP lines, ISP A and ISP B. After configuring the DNS redirect settings and the PBR policies, the traffic that matches the default route will flow out from the ethernet0/2, and the traffic that matches the policy-based route will flow out from the ehternet0/3. The topology is shown as below:



The configurations are shows as follows:

Step 1: Configure the interfaces and security zones:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone dmz
hostname(config-if-eth0/2)# ip address 10.180.41.52/20
hostname(config-if-eth0/2)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone dmz
hostname(config-if-eth0/3)# ip address 172.31.1.240/24
hostname(config-if-eth0/3)# exit
hostname(config)#
```

Step 2: Configure the policies:

```
hostname(config)# rule id 1 from any to any service any permit
```

Step 3: Configure SNAT settings:

```
hostname(config)# nat
hostname(config-nat)# snatrule from any to any service any trans-to eif-ip mode dynamicport
```

Step 4: Configure the default routes:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 0.0.0.0/0 10.180.32.1
```

Step 5: Configure a policy-based route and bind it to the interface:

```
hostname(config)# pbr-policy test
hostname(config-pbr)# match top any any any YOUKU-DNS nexthop 172.31.1.1
Match id 1 is created.
hostname(config-pbr)# match id 1
hostname(config-pbr-match)# application YOUKU
hostname(config-pbr-match)# application RTMFP
hostname(config-pbr-match)# exit
hostname(config-pbr)# exit
hostname(config)# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# bind pbr-policy test
hostname(config-if-eth0/0)# exit
```

Step 6: Configuring ISP routes:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route China-netcom 172.31.1.1
hostname(config-vrouter)# exit
```

Step 7: Upgrading APP signature database:

```
hostname(config)# exec app update professional
```

Step 8: Enabling the application identification:

```
hostname(config)# zone trust
hostname(config-zone-trust)# application-identify
```

Step 9: Enabling the DNS redirect and configuring the IP address of the DNS server:

```
hostname(config)# app cache dns-redirect enable
Please specify the IP address for the DNS server
hostname(config)# ip name-server 58.240.57.33
```

Dynamic Routing

Dynamic routing refers to the routing that will be automatically adjusted based on the operation status of network. FS devices will automatically adjust the dynamic routing table according to the routing protocol being used. FSOS support 4 dynamic routing protocols: RIP, OSPF, IS-IS, and BGP.

Configuring RIP

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

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

Basic Options

The basic options of RIP configuration include version, metric, distance, information originate and timer (update interval, invalid time, holddown time and flush time). You can configure RIP protocol for different VRouter respectively. The basic options of RIP must be configured in the RIP routing configuration mode. To enter the RIP routing configuration mode, in the global configuration mode, use the following commands:

ip vrouter *vrouter-name* (enters the VRouter configuration mode)

router rip (enters the RIP routing configuration mode, and at the same time enables the RIP function on the device)

To disable RIP, in the VRouter configuration mode, use the command **no router rip**.

Specifying a Version

FS devices support RIP-1 and RIP-2. RIP-1 transmits packets by broadcasting, while RIP-2 transmits packet by multicasting. To specify the RIP version, in the RIP routing configuration mode, use the following command:

version *version-number*

- *version-number* - Specifies the version number which can be 1 (RIP-1) or 2 (RIP-2). The default version number is 2.

To restore to the default version, in the RIP routing configuration mode, use the command **no version**.

Specifying a Metric

RIP measures the distance to the destination network by hops. This distance is known as metric. The metric from a router to a directly connected network is 1, and increments by 1 for every additional router between them. The maximum metric is 15, and the network with metric larger than 15 is not reachable. The default metric will take effect when the route is redistributed. To specify the default metric, in the RIP routing configuration mode, use the following command:

default-metric *value*

- *value* - Specifies the default metric value. The value range is 1 to 15. If no value is specified, the value of 1 will be used.

To restore to the metric value of 1, in the RIP routing configuration mode, use the command **no default-metric**.

Specifying a Distance

To specify the default distance for RIP, in the RIP routing configuration mode, use the following command:

distance *distance-value*

- *distance-value* - Specifies the default administration distance value. The value range is 1 to 255. If no value is specified, the value of 120 will be used.

To restore to the distance value of 120, in the RIP routing configuration mode, use the command **no distance**.

Configuring the Default Information Originate

You can specify if the default route will be redistributed to other routers with RIP enabled. By default RIP will not redistribute the default route. To configure the default information originate, in the RIP routing configuration mode, use the following commands:

Redistribute: **default-information originate**

Do not redistribute: **no default-information originate**

Specifying a Timer

The timers you can configure for RIP include update interval, invalid time, holddown time and flush time, as described below:

- Update interval: Specifies the interval at which all RIP routes will be sent to all the neighbors. The default value is 30 seconds.
- Invalid time: If a route has not been updated for the invalid time, its metric will be set to 16, indicating an unreachable route. The default value is 180 seconds.
- Holddown time: If the metric becomes larger (e.g., from 2 to 4) after a route has been updated, the route will be assigned with a holddown time. During the holddown time, the route will not accept any update. The default value is 180 seconds.
- Flush time: FSOS will keep on sending the unreachable routes (metric set to 16) to other routers during the flush time. If the route still has not been updated after the flush time ends, it will be deleted from the RIP information database. The default value is 240 seconds.

To modify the above four timers, in the RIP routing configuration mode, use the following command:

timers basic *interval-time invalid-time holddown-time flush-time*

- *interval-time* - Specifies the update interval time. The value range is 0 to 16777215 seconds. The default value is 30.
- *invalid-time* - Specifies the invalid time. The value range is 1 to 16777215 seconds. The default value is 180.
- *holddown-time* - Specifies the holddown time. The value range is 1 to 16777215 seconds. The default value is 180.
- *flush-time* - Specifies the flush time. The value range is 1 to 16777215 seconds. The default value is 240.

To restore to the default timer value, in the RIP routing configuration mode, use the command **no timers basic**.

Configuring Redistribute

RIP allows you to introduce information from other routing protocols (BGP, connected, static and OSPF) and redistribute the information. To configure the redistribute metric, in the RIP routing configuration mode, use the following commands:

```
redistribute {bgp | connected | static | ospf} [metric value]
```

- **bgp** | **connected** | **static** | **ospf**- Specifies the protocol type which can be **bgp**, **connected**, **static** or **OSPF**.
- **metric** *value*- Specifies a metric value for the redistribute. The value range is 1 to 15. If the value is not specified, the system will use the default RIP metric configured by the command default-metric value.

Repeat the above command to redistribute different types of protocols.

To cancel the redistribute of the specified protocol, in the RIP routing configuration mode, use the command**no redistribute** {**bgp** | **connected** | **static** | **ospf**}.

Configuring a Passive IF

You can configure some interfaces to only receive but not to send data. This kind of interfaces is known as a passive interface. To configure a passive interface, in the RIP routing configuration mode, use the following command:

```
passive-interface interface-name
```

- *interface-name* - Specifies the interface as a passive interface.

Repeat the above command to configure multiple passive interfaces.

To cancel the specified passive interface, in the RIP routing configuration mode, use the command **no passive-interface** *interface-name*.

Configuring a Neighbor

You can specify some neighbors to allow P2P (non-broadcasting) RIP information exchanges between the neighbors and FS devices. To configure a neighbor, in the RIP routing configuration mode, use the following command:

```
neighbor ip-address
```

- *ip-address* - Specifies the IP address of the neighbor.

Repeat the above command to configure more passive neighbors.

To delete the specified neighbor, in the RIP routing configuration mode, use the command **no neighbor** *ip-address*.

Configuring a Network

You can configure some networks so that only the interfaces within the specified networks can receive and send RIP update. To configure a network, in the RIP routing configuration mode, use the following command:

network *ip-address/netmask*

- *ip-address/netmask* - Specifies the IP address of the network, for example, 10.200.0.0/16.

Repeat the above command to configure more networks.

To delete the specified network, in the RIP routing configuration mode, use the command **no network** *ip-address/netmask*.

Configuring a Distance

You can specify an administration distance for the routes that are obtained from the specified networks. To configure a distance, in the RIP routing configuration mode, use the following command:

distance *distance-value ip-address/netmask*

- *distance-value* - Specifies the administration distance value. The value range is 1 to 255. The priority of this distance is higher than that of the default distance configured in the basic RIP options specified by the command
- *ip-address/netmask* - Specifies the IP address of the network, for example, 10.200.0.0/16.

Repeat the above command to configure a distance for the routes that are obtained from different networks.

To delete the specified distance, in the RIP routing configuration mode, use the command **no distance** *ip-address/netmask*.

RIP Database

When a FS device is running RIP, it will own a RIP route database which can store all routing entries for all the reachable networks. The routing entry information includes destination address, next hop, metric, source, and timer information. To view the RIP database information, in any mode, use the following command:

show ip rip database [*A.B.C.D/M*] [**vrouter** *vrouter-name*]

- *A.B.C.D/M* - Shows the RIP information of the specified destination IP address.
- **vrouter** *vrouter-name*- Shows the RIP information of the specified VRouter. At present FSOS only supports VRouter named trust-vr.

Configuring RIP for Interfaces

The RIP configuration for the interfaces of FS devices includes: authentication mode, transmit and receive version, and split horizon. The RIP configuration for the interfaces must be done in the interface configuration mode.

Configuring an Authentication Mode

Only RIP-2 supports authentication on RIP packets. The packet authentication mode includes plain text and MD5. The plain text authentication, during which unencrypted string is transmitted together with the RIP packet, cannot assure security, so it cannot be applied to the scenarios that require high security. The default mode is plain text authentication. To configure the authentication mode and authentication string for the RIP packets, in the interface configuration mode, use the following commands:

- Authentication mode: **ip rip authentication mode** {**md5** | **text**}
- Authentication string: **ip rip authentication string** *string*

To cancel the specified authentication mode and authentication string, in the interface configuration mode, use the following commands:

- **no ip rip authentication mode**
- **no ip rip authentication string**

Specifying RIP Version

By default RIP-2 information will be transmitted. To specify the RIP version number that will be transmitted, in the interface configuration mode, use the following command:

ip rip send version [1][2]

- **1** - Only RIP-1 information will be transmitted.
- **2** - Only RIP-2 information will be transmitted.

To restore to the default version number, in the interface configuration mode, use the command **no ip rip send version**.

By default RIP-2 information will be received. To specify the RIP version number that will be received, in the interface configuration mode, use the following command:

```
ip rip receive version [1][2]
```

- **1** - Only RIP-1 information will be received.
- **2** - Only RIP-2 information will be received.

To restore to the default version number, in the interface configuration mode, use the command **no ip rip receive version**.

Configuring Split Horizon

In split horizon, routes learned from an interface will not be sent from the same interface, in order to avoid routing loop and assure correct broadcasting to some extent. To enable or disable split horizon, in the interface configuration mode, use the following commands:

Enable: **ip rip split-horizon**

Disable: **no ip rip split-horizon**

Viewing System RIP Information

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

show ip rip

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

show ip *route rip* [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the RIP router information of the specified VRouter.

Configuring OSPF

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

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

Configuring OSPF Protocol

You can configure OSPF protocol for different VRouters respectively. The configuration of OSPF protocol includes:

- Configuring a Router ID
- Configuring area authentication
- Configuring route aggregation for an area
- Configuring the default cost for an area
- Configuring the virtual link for an area
- Specify the ID and password for MD5 authentication.
- Configuring the default cost for sending OSPF packets
- Configuring a default metric
- Configuring the default information originate
- Configuring the default distance
- Configuring an OSPF timer
- Specifying the network that runs OSPF protocol
- Configuring redistribute
- Configuring a distance
- Configuring a Passive IF

The basic options of OSPF protocol must be configured in the OSPF routing mode. To enter the OSPF routing mode, in the global configuration mode, use the following commands:

ip vrouter *vrouter-name* (enters the VRouter configuration mode)

router ospf [*process-id*]（(enters the OSPF routing mode, and at the same time enables OSPF on the device)

- *process-id* − Specify the OSPF process ID. The default value is 1. The value ranges from 1 to 65535. Each OSPF process is individual, and has its own link state database and the related OSPF routing table. Each VRouter supports up to 4 OSPF processes and multiple OSPF processes maintain a routing table together.

When specifying the OSPF process ID, note the following matters:

- When running multiple OSPF processes in a VRouter, the network advertised in interfaces in each OSPF process cannot be same.
- When route entries with the same prefix exist in multiple OSPF processes, the system will compare the administrative distance of each route entry and the route entry with the lower administrative distance will be added to the VRouter's routing table. If their AD is the same, the route entry that was first discovered will be added to the routing table.
- If the OSPF route entries are redistributed to other routing protocols, the routing information of process 1 will be redistributed by default. If this process does not exist, the routing information of OSPF will not be redistributed.

To disable OSPF, in the VRouter configuration mode, use the command **no router ospf** [*process-id*].

Configuring a Router ID

Each router running OSPF protocol must be labeled with a Router ID. The Router ID is the unique identifier of an individual router in the whole OSPF domain, represented in the form of an IP address. To configure a Router ID for the FS device that is running OSPF protocol, in the OSPF routing mode, use the following command:

router-id *A.B.C.D* [**local**]

- *A.B.C.D* - Specifies the Router ID used by OSPF protocol, in form of an IP address.
- **local** - Specifies the Router ID as a local configuration. This kind of configuration is applicable to HA A/A mode, and is not synchronized to HA configuration. By default the router ID is not a local configuration.

Configuring Area Authentication

By default, there is no area authentication. To configure an area authentication mode, in the OSPF routing mode, use the following command:

area {*id* | *A.B.C.D*} **authentication** [**message-digest**]

- *id* | *A.B.C.D* - Specifies an area ID, in form of a 32-bit digital number, or an IP address.

- **[message-digest]** - Specifies the MD5 authentication. If the keyword is not specified, then the system will use the plain text authentication.

The authentication mode specified by the above command must be the same as that of the other routers within the area; the authentication password for routers that communicate over OSPF in the same network must be the same.

To cancel the specified area authentication mode, in the OSPF routing mode, use the command **no area** {*id* | *A.B.C.D*} **authentication**.

Specifying the Network Type for an Interface

In OSPF, the network types of an interface have the following options: broadcast, point-to-point, and point-to-multipoint. By default, the network type of an interface is broadcast. To configure the network type of an interface, in the interface configuration mode, use the following command:

```
ip ospf network {point-to-point | point-to-multipoint}
```

- **point-to-point** – Specifies the network type of an interface as the point-to-point type.
- **point-to-multipoint** - Specifies the network type of an interface as the point-to-multipoint type.

To set the network type as the default broadcast type, use the following command:

```
no ip ospf network
```

Configuring Route Aggregation for an Area

Route aggregation refers to aggregating the routing information with the same prefix together through ABR, and then only advertising one route to other areas. You can configure multiple aggregation segments in one area, so that OSPF can aggregate multiple segments. By default, the route aggregation function is disabled. To configure route aggregation for an area, in the OSPF routing mode, use the following command:

area {*id* | *A.B.C.D*} **range** {*A.B.C.D/M*} [**advertise** | **not-advertise**]

- *id* | *A.B.C.D*- Specifies an area ID that will perform the route aggregation, in form of a 32-bit digital number, or an IP address.
- **range** {*A.B.C.D/M*} - Specifies the network segment that will be aggregated.
- **advertise** - Specifies to aggregate the routes of the segment and advertises the aggregated route.

- **not-advertise** -Specifies to aggregate the routes of the segment, but do not advertise the aggregated route.

The route aggregation function is only applicable to an area border router (also known as ABR, the router that connects the backbone area and non-backbone area).

To cancel the route aggregation, in the OSPF routing mode, use the command **no area** {*id* | *A.B.C.D*} **range** {*A.B.C.D/M*} [**advertise** | **not-advertise**].

Configuring the Default Cost for an Area

The default cost of an area refers to the default routing cost for sending a packet to the stub area. To configure default cost for an area, in the OSPF routing mode, use the following command:

area {*id* | *A.B.C.D*} **default-cost** *cost-value*

- *id* | *A.B.C.D* - Specifies an area ID the default cost will be applied to, in form of a 32-bit digital number, or an IP address.
- *cost-value* - Specifies a cost value. The value range is 0 to 16777214. If no value is specified, the system will use the value of 1.

To restore to the cost value of 1, in the OSPF routing mode, use the command **no area** {*id* | *A.B.C.D*} **default-cost**.

Note:This command is only applicable to NSSA.

Configuring the Virtual Link for an Area

Virtual link is used to connect the discontinuous backbone areas, so that they can maintain logical continuity. To configure virtual link parameters and its timer parameters, in the OSPF routing mode, use the following command:

area {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* [**hello-interval** *interval-value*] [**retransmit-interval** *interval-value*] [**transmit-delay** *interval-value*] [**dead-interval** *interval-value*]

- *id* | *A.B.C.D* - Specifies an area ID that requires virtual link, in form of a 32-bit digital number, or an IP address.
- **virtual-link** *A.B.C.D* - Specifies the Router ID that is used as a virtual link router.
- **hello-interval** *interval-value* - Specifies the interval for sending the Hello packets. The value range is 1 to 65535 seconds. The default value is 10.
- **retransmit-interval** *interval-value* - After sending a LSA packet to its neighbor, a router will wait for the acknowledge from the peer. If no ACK packet is received after the specified

interval, the router will retransmit this LSA packet to the neighbor. The parameter is used to specify the retransmit interval. The value range is 3 to 65535 seconds. The default value is 5.

- **transmit-delay** *interval-value* - Specifies the transmit delay time of the update packets. The value range is 1 to 65535 seconds. The default value is 1.
- **dead-interval** *interval-value* - If a router has not received the Hello packet from its peer for a certain period, it will determine the peering router is dead. This period is known as the dead interval between the two adjacent routers. This parameter is used to specify the value of dead interval. The value range is 1 to 65535 seconds. The default value is 40.

To restore to the default timer values, in the OSPF routing mode, use the command **no area** {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* [**hello-interval**] [**retransmit-interval**] [**transmit-delay**] [**dead-interval**].

To configure the authentication mode of the virtual link, in the OSPF routing mode, use the following command:

area {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* **authentication** [**message-digest**] [**authentication-key** *string*] [**message-digest-key** *ID* **md5** *string*] [**null**]

- *id* | *A.B.C.D* - Specifies an area ID that requires virtual link, in form of a 32-bit digital number, or an IP address.
- **virtual-link** *A.B.C.D* - Specifies the Router ID that is used as a virtual link router.
- **authentication-key** *string* - Specifies the password for the plain text authentication.
- **message-digest-key** *ID* **md5** *string* - Specifies to use MD5 authentication.
- **null** - No authentication.

To cancel the authentication mode, in the OSPF routing mode, use the command **no area** {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* **authentication** [**message-digest**] [**authentication-key** *string*] [**message-digest-key** *ID*].

Configuring a Stub Area

The stub area refers to the area that does not send or receive Type-5 LSA (AS-external-LSAs). For the network that generates large amount of Type-5 LSAs, this approach can effectively reduce the router LSDB size within the stub area, and the resource occupation arising from SPF calculation on the router. The stub area is usually located at the border of the autonomy system. To configure the stub area of OSPF, in the OSPF routing mode, use the following command:

area {*id* | *A.B.C.D*} **stub** [**no-summary**]

- *id* | *A.B.C.D* - Specifies an ID for the stub area, in form of a 32-bit digital number, or an IP address.

- **no-summary** - Stops ABR from sending Type 3 or Type 4 Summary LSA to the stub area.

To cancel the specified stub area, in the OSPF routing mode, use the command **no area** {*id* | *A.B.C.D*} **stub** [**no-summary**].

Configuring a NSSA Area

A stub area cannot redistribute routes. You can configure the area as an NSSA area to allow for route redistribution by keeping other stub area characteristics. To configure the NSSA area of OSPF, in the OSPF routing mode, use the following command:

area {*id* | *A.B.C.D*} **nssa** [**no-summary** | **no-redistribution** | **default-information-originate**]

- *id* / *A.B.C.D* - Specifies an ID for the NSSA area, in form of a 32-bit digital number, or an IP address.
- **no-summary** | **no-redistribution** | **default-information-originate** - **no-summary** allows an area to be a not-so-stubby area but not have summary routes injected into it. **no-redistribution** is used when the router is an NSSA ABR and you want the **redistribute** command to import routes only into the normal areas, but not into the NSSA area. **default-information-originate** is used to generate a Type 7 default into the NSSA area. This keyword only takes effect on an NSSA ABR or an NSSA ASBR.

To cancel the specified NSSA area settings, in the OSPF routing mode, use the command **no area** {*id* | *A.B.C.D*} **nssa** [**no-summary** | **no-redistribution** | **default-information-originate**]

Configuring the Reference Bandwidth for OSPF

OSPF can calculate the cost of sending OSPF packets for an interface based on the interface bandwidth. To configure reference bandwidth, in the OSPF routing mode, use the following command:

auto-cost reference-bandwidth *bandwidth*

- *bandwidth* - Specifies the bandwidth value. The value range is 1 to 4294967 Mbps. The default value is 100.

To calculate the cost of sending OSPF packets for an interface based on the interface type, in the OSPF routing mode, use the command**no auto-cost reference-bandwidth**

Configuring the Default Metric

The default metric configured here will take effect when redistributing. To specify the default metric for OSPF, in the OSPF routing configuration mode, use the following command:

default-metric *value*

- *value* - Specifies the default metric value. The value range is 1 to 16777214.

To restore to the original metric value, in the OSPF routing configuration mode, use the command **no default-metric**.

Configuring the Default Information Originate

You can specify if the default route will be redistributed to other routers with OSPF enabled. By default OSPF will not redistribute the default route. To configure the default information originate, in the OSPF routing configuration mode, use the following command:

```
default-information originate [always] [type {1 | 2}] [metric value]
```

- **always** - OSPF unconditionally generates and redistributes the default route.
- **type** {1 | 2} - Specifies the type of the external route associated with the default route that is sent to OSPF routing area. 1 refers to type1 external route, 2 refers to type2 external route.
- **metric** *value* - Specifies the metric value for the default route that will be sent. If no default metric value is specified by this command or by the command default-metric value, then OSPF will use the value of 20. The value range is 0 to16777214.

To restore to the value of 20, in the OSPF routing configuration mode, use the command **no default-information originate**.

Configuring the Default Distance

To configure the default distance for OSPF route, in the OSPF routing configuration mode, use the following command:

```
distance distance-value
```

- *distance-value* - Specifies the default administration distance value. The value range is 1 to. 255. If no value is specified, OSPF will use the value of 110.

To restore to the value of 110, in the OSPF routing configuration mode, use the command **no distance**.

Configuring a Timer for OSPF

You can specify the following two OSPF protocol timers: how long OSPF will re-calculate the path after receiving an update, and the interval between the two OSPF calculations. To configure an OSPF timer, in the OSPF routing configuration mode, use the following command:

```
timers spf delay1 delay2
```

- *delay1* - After receiving the update, OSPF will re-calculate the path within the specified period. The value range is 0 to 65535 seconds. The default value is 5.
- *delay2* - Specifies the interval between the two calculations. The value range is 0 to 65535 seconds. The default value is 10.

To restore to the value of 5 or 10, in the OSPF routing configuration mode, use the command **no timers spf**.

Specifying an OSPF Network Interface

To specify the network interface that enables OSPF and add the network to the specified area, in the OSPF routing configuration mode, use the following command:

network *A.B.C.D/M* **area** {*id* | *A.B.C.D*}

- *A.B.C.D/M* - Specifies the network interface that enables OSPF protocol.
- **area** {*id* | *A.B.C.D*} - Specifies the area ID the network will be added to, in form of a 32-bit digital number, or an IP address.

To cancel the specified network interface, in the OSPF routing configuration mode, use the command **no network** *A.B.C.D/M* **area** {*id* | *A.B.C.D*}.

Configuring Redistribute

OSPF allows you to introduce information from other OSPF processes and routing protocols (BGP, IS-IS, connected, static, RIP and VPN) and redistribute the information. You can set the metric and type of the external route for the redistribute, or filter the routing information based on a route map and only distribute specific routing information. To configure the redistribute metric, in the OSPF routing configuration mode, use the following command:

redistribute {**bgp** | **connected** | **isis** | **ospf** *process-id* | **static** | **rip** | **vpn**} [**type** {**1** | **2**}] [**metric** *value*] [**route-map** *name*] [**tag** *tag-value*]

- **bgp** | **connected** | **isis** | **ospf** *process-id* | **static** | **rip** | **vpn** - Specifies the protocol type which can be **bgp**, **connected**, **isis**, **ospf**, **static**, **rip** or **VPN**. When introducing information from other OSPF processes, specify the process.
- **type** {1 | 2} - Specifies the type of the external route. **1** refers to type1 external route, **2** refers type2 external route.
- **metric** *value* - Specifies a metric value for the redistribute. The value range is 0 to 16777214. If the value is not specified, the system will use the default OSPF metric configured by the command default-metric value.

- **route-map** *name* - Specifies the route map that is used to filter the routing information introduced from other routing protocols. For more information about route map, see Configuring a Route Map.
- **tag** *tag-value* – Specifies the tag values of the redistributed route. The value range is 1 to 4294967295.

Repeat the above command to redistribute a different type of routes.

To cancel the redistribute of specified route, in the OSPF routing configuration mode, use the command **no redistribute** {**bgp** | **connected** | **static** | **rip**}.

Configuring a Route Map

By default the system will introduce all the routing information. You can filter the routing information introduced from other routing protocols by referencing a route map. The route map mainly consists of two parts: matching rules and actions (permit or deny) for the matched routing information. If introduced routing information hits any matching rule, the system will take the configured action, i.e., permit or deny the introduced routing information.

Note:

- If the action is set to Permit, the system will only permit the matched routing information and deny all the unmatched routing information.
- If the action is set to Deny, the system will deny the matched routing information, but still permit all the unmatched routing information.

To configure a route map and filter the introduced routing information, take the following steps:

1. Create a route map and add matching rules to the route map. Matching rules are differentiated by IDs. The smaller the ID is, the higher the matching priority will be. By default if the routing information hits any matching rule, the system will not continue to match the subsequent rules; if no matching rule is hit, the system will take the Deny action.
2. Add matching conditions to the matching rules. The matching condition can be the metric, destination address, next-hop IP address or next-hop interface of the introduced routing information. One matching rule may contain multiple matching conditions, and the relation between these conditions is AND, i.e., in order to hit a matching rule, the routing information information must satisfy all the matching conditions in the rule.
3. If the matching condition is the destination address or next-hop IP address, also configure a route access-list that will be referenced. For more information about route access-list, see Configuring a Route Access-list.

4. If needed, require the system to continue to match another rule after the routing information hits a matching rule.

5. If needed, modify partial attrubutes of the introduced routing information before redistribution.

To create a route map and add a matching rule to the route map, in the global configuration mode, use the following command:

route-map *name* {**deny** | **permit**} *sequence*

- **route-map** *name* - Specifies the name of the route map, and enters the route map configuration mode. The value range is 1 to 31 characters. If the name already exists in the system, you will directly enter the route map configuration mode.
- **deny** | **permit** - Specifies the action for the matched routing information.
- *sequence* - Specifies the sequence number for the matching rule in the route map. The value range is 1 to 65535.

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

no route-map *name* [*sequence*]

- *sequence* - Only deletes the specified matching rule from the route map.

To add a matching condition to the matching rule, in the route map configuration mode, use the following command:

match {**as-path** *access-list-number* | **community** {*community-list-name* | *community-list-number*} [*exact-match*] | **metric** *metric-value* | **interface** *interface-name* | **ip address** *access-list* | **ip next-hop** *access-list* | **tag** *tag-value* }

- **as-path** *access-list-number* – Matches the AS path of the introduced routing information. access-list-number is the number of the AS-path access list configured by yourself. If the AS path of the route matches the AS path that is permitted in this AS-path access list, the system concludes that the matching is successful. For more information about configuring an AS-path access list, see Configuring an AS-path Access List.
- **community** {*community-list-name* | *community-list-number*} [*exact-match*] – Matches the communities path attributes of the introduced routing information. community-list-name is the name of the community list. community-list-number is the number of the community list. **exact-match** indicates that the system will execute the exact matching. For more information about configuring community list, see Configuring BGP Communities.

- **metric** *metric-value* - Specifies to match the metric of the introduced routing information. The value range is 0 to 4294967295.

- **interface** *interface-name* - Specifies to match the next-hop interface of the introduced routing information.

- **ip address** *access-list* - Specifies to match the destination address of the introduced routing information. *access-list* is the route access-list configured in the system. If the destination address of the routing information is the permitted address in the route access-list, the system will conclude the matching succeeds. For more information about route access-list, see Configuring a Route Access-list.

- **ip next-hop** *access-list* - Specifies to match the next-hop IP address of the introduced routing information. *access-list* is the route access-list configured in the system. If the next-hop IP address of the routing information is the permitted address in the route access-list, the system will conclude the matching succeeds. For more information about route access-list, see Configuring a Route Access-list.

- **tag** *tag-value* – Matches the route tag value of OSPF protocol. If the configured tag value of the route here matches the tag value in the static route, the match is considered successful. The value range is 1 to 4294967295.

Repeat the above command to add more matching conditions to the matching rule. To delete the specified matching condition from the matching rule, in the route map configuration mode, use the following command:

no match {**metric** | **interface** | **ip address** | **ip next-hop**}

Note:If you only created a route map but did not add any matching rule, by default the system will conclude all the introduced routing information is matched.

For example, the following commands will only allow OSPF to redistribute the routing information from BGP with the next-hop interface set to eth0/1 and metric set to 50:

```
hostname(config)# route-map test permit 10

hostname(config-route-map)# match interface ethernet0/1

hostname(config-route-map)# match metric 50

hostname(config-route-map)# exit

hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# router ospf

hostname(config-router)# redistribute bgp route-map test
hostname(config-router)# end
```

Continuing to Match Another Matching Rule

By default if the introduced routing information hits any matching rule, the system will not continue to match any other matching rules. For fine-grained control, you can require the system to continue to match another matching rule even after hitting a matching rule. To continue to match another matching rule, in the route map configuration mode, use the following command:

continue [*sequence*]

- *sequence* - Specifies the sequence number for the matching rule that will be continued. The value range is 1 to 65535. This sequence number must be larger than the sequence number of the current matching rule. If this parameter is not specified, the system will continue to match the next rule after hitting the current rule.

To cancel the above configuration, in the route map configuration mode, use the following command:

no continue

For example, the following commands will also only allow OSPF to redistribute the routing information from BGP with the next-hop interface set to eth0/1 and metric set to 50:

```
hostname(config)# route-map test permit 10
hostname(config-route-map)# match interface ethernet0/1
hostname(config-route-map)# continue 20
hostname(config-route-map)# exit
hostname(config)# route-map test permit 20
hostname(config-route-map)# match metric 50
hostname(config-route-map)# exit
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# redistribute bgp route-map test
hostname(config-router)# end
```

Modifying Attributes of Introduced Routing Information

For the introduced routing information, you can modify partial attributes before redistribution. To modify the attribute of the introduced routing information, in the route map configuration mode, use the following command:

set {**metric** *metric-value* | **metric-type** {**type-1** | **type-2**}| **tag** *tag-value*}

- **metric** *metric-value* - Specifies the metric of the introduced routing information. The value range is 0 to 4294967295.
- **metric-type** {**type-1** | **type-2**} - Specifies the metric type of the external route. **type-1** indicates type1 external route metric, and **type-2** indicates type2 external route metric.
- **tag** *tag-value* – Specifies the tag value of OSPF protocol’s redistributed route. The value range is 1 to 4294967295.

To cancel the modification and restore to the metric setting when the routing information was introduced, in the route map configuration mode, use the following command:

no set {**metric** | **metric-type** | **tag** }

Configuring a Route Access-list

The destination address and next-hop IP address in the matching conditions are matched by route access-list. A route access-list mainly consists of two parts: IP address matching rules and actions (Permit or Deny) for the matched IP addresses. If the destination address or next-hop IP address matches the IP address defined in the route access-list, the system will take the specified action. One route access-list may contain multiple IP address matching rules. The system will match these rules in the sequence of rule creation time, and will stop matching if any rule is hit; if no rule is hit, the system will take the action of Deny.

To configure a route access-list, in the global configuration mode, use the following command:

access-list route *name* {**deny** | **permit**} {*A.B.C.D/M* [**exact-match**] | **any**}

- *name* - Specifies the name of the route access-list. The value range is 1 to 31 characters.
- **deny** | **permit** - Specifies the action for the matched IP address.
- *A.B.C.D/M* - Specifies the IP address or IP prefix (excluding the netmask) to be matched.
- **exact-match** - Specifies to match the exact IP prefix (including the netmask).
- **any** - Specifies to match any IP address.

To delete the specified route access-list, in the global configuration mode, use the following command:

no access-list route *name* [{**deny** | **permit**} {*A.B.C.D/M* [**exact-match**] | **any**}]

If any IP address matching rule is specified, the command will only delete the rule from the route access-list, but will not delete the route access-list.

To add description to the route access-list, in the global configuration mode, use the following command:

access-list route *name* **description** *description*

- *name* - Specifies the name of the route access-list. The value range is 1 to 31 characters.
- *description* - Specifies the description of the route access-list. The value range is 1 to 31 characters.

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

no access-list route *name* **description**

For example, the following commands will disallow OSPF to redistribute the routing information from BGP with the next-hop IP address set to 192.168.1.1 or any IP address in 192.168.2.0 segment:

```
hostname(config)# route-map test deny 10
hostname(config-route-map)# match ip next-hop access_list
hostname(config-route-map)# exit
hostname(config)# access-list route access_list permit 192.168.1.1/32
hostname(config)# access-list route access_list permit 192.168.2.0/24
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# redistribute bgp route-map test
hostname(config-router)# end
```

Configuring a Distance

You can specify the administration distance based on the type of route. To configure the distance, in the OSPF routing configuration mode, use the following command:

distance ospf {**intra-area** *distance-value* | **inter-area** *distance-value* | **external** *distance-value*}

- **intra-area** *distance-value* - Specifies the administration distance for the routes within an area. The value range is 1 to 255. The default value is 110.
- **inter-area** *distance-value* - Specifies the administration distance for the routes between areas. The value range is 1 to 255. The default value is 110.
- **external** *distance-value*- Specifies the administration distance for the external type5 route. The value range is 1 to 255. The default value is 110.

To restore to the default value, in the OSPF routing configuration mode, use the command **no distance ospf**.

Configuring a Passive IF

You can configure some interfaces to only receive but not to send data. This kind of interfaces is known as a passive interface. To configure a passive interface, in the OSPF routing configuration mode, use the following command:

passive-interface *interface-name*

- *interface-name* - Specifies the interface as a passive interface.

Repeat the above command to configure more passive interfaces.

To cancel the specified passive interface, in the OSPF routing configuration mode, use the command **no passive-interface** *interface-name*.

Configuring Route Filters Based on the Route Access-list

OSFP uses the route access-list to filter the introduced route. To configure the route filter function based on the route access-list, use the following command in the OSPF routing configuration mode:

distribute-list *access-list-name* **in** [*interface-name*]

- *access-list-name* – Specifies name of the route access-list. For more information about route access-list, see Configuring a Route Access-list .
- **in** – Use **in** to filter the introduced routes.
- *interface-name* – Specifies name of the interface. After specifying this interface, the system will filter the OSPF route from the specified interface. If the interface name is not specified, the system will filter all OSPF routes.

Use the following command to cancel the above configurations:

no distribute-list *access-list-name* **in** [*interface-name*]

Configuring OSPF for an Interface

The OSPF function for an interface must be configured in the interface configuration mode. The OSPF configuration for the FS device’ s interfaces includes:

- Configuring OSPF authentication for an interface
- Specifying the link cost for an interface
- Configuring the timer for an interface
- Specifying the router priority for an interface
- Specifying the network type for an interface

Configuring OSPF Authentication for an Interface

The priority of OSPF authentication for an interface is higher than that of the OSPF authentication for an area. FS devices support the plain text and MD5 authentication. By default the OSFP authentication for an interface is disabled. To enable or disable it, in the interface configuration mode, use the following commands:

ip ospf authentication

no ip ospf authentication

To configure the password for the plain text authentication, in the interface configuration mode, use the following command:

ip ospf authentication-key *string*

- *string* - Specifies the password (up to eight characters).

To cancel the specified password, in the interface configuration mode, use the command **no ip ospf authentication-key**.

To configure the MD5 authentication ID and password, in the interface configuration mode, use the following command:

ip ospf message-digest-key *ID* **md5** *string*

- *ID* - Specifies the authentication ID.
- *string* - Specifies the password.

To cancel the specified password, in the interface configuration mode, use the command **no ip ospf message-digest-key** *ID*.

Specifying the Link Cost for an Interface

To specify the link cost for an interface, in the interface configuration mode, use the following command:

ip ospf cost *cost-value* [**local**]

- *cost-value* - Specifies the link cost for an interface. The value range is 1 to 65535.
- **local** - Specifies the link cost for an interface as local. When the device is operating in the HA AA mode, the parameter will prevent the device from synchronizing the cost value to the backup device. Thus the two devices’ link costs will be different, avoiding asymmetrical OSPF routes.

To cancel the specified link cost, in the interface configuration mode, use the command **no ip ospf cost** [**local**].

Configuring the Timer for an Interface

There are four interface timers: the interval for sending Hello packets, the dead interval of adjacent routers, the interval for retransmitting LSA, and the transmit delay for updating packets.

To specify the interval for sending Hello packets for an interface, in the interface configuration mode, use the following command:

ip ospf hello-interval *interval*

- *interval* - Specifies the interval for sending Hello packets for an interface. The value range is 1 to 65535 seconds. The default value is 10.

To restore to the default interval, in the interface configuration mode, use the command **no ip ospf hello-interval**.

If a router has not received the Hello packet from its peer for a certain period, it will determine the peering router is dead. This period is known as the dead interval between the two adjacent routers. To configure the dead interval for an interface, in the interface configuration mode, use the following command:

ip ospf dead-interval *interval*

- *interval* - Specifies the dead interval of adjacent routes for an interface. The value range is 1 to 65535 seconds. The default value is 40 (4 times of sending the Hello packets).

To restore to the default dead interval, in the interface configuration mode, use the command **no ip ospf dead-interval**.

To specify the LSA retransmit interval for an interface, in the interface configuration mode, use the following command:

ip ospf retransmit-interval *interval*

- *interval* - Specifies the LSA retransmit interval for an interface. The value range is 3 to 65535 seconds. The default value is 5.

To restore to the default retransmit interval, in the interface configuration mode, use the command **no ip ospf retransmit-interval**.

To specify the transmit delay for updating packet for an interface, in the interface configuration mode, use the following command:

ip ospf transmit-delay *interval*

- *interval* - Specifies the transmit delay for updating packet for an interface. The value range is 1 to 65535 seconds. The default value is 1.

To restore to the default transmit delay, in the interface configuration mode, use the command **no ip ospf transmit-delay**.

Specifying the Router Priority for an Interface

The router priority is used to determine which router will act as the designated router. The designated router will receive the link information of all the other routers in the network, and broadcast the received link information. To specify the router priority for an interface, in the interface configuration mode, use the following command:

ip ospf priority *level*

- *level* - Specifies the router priority. The value range is 0 to 255. The default value is 1. The router with priority set to 0 will not be selected as the designated router. If two routers within a network can both be selected as the designated router, the router with higher priority will be selected; if the priority level is the same, the one with higher Router ID will be selected.

To restore to the default priority, in the interface configuration mode, use the command **no ip ospf priority**.

Specifying the Network Type for an Interface

In OSPF, the network types of an interface have the following options: broadcast, point-to-point, and point-to-multipoint. By default, the network type of an interface is broadcast. To configure the network type of an interface, in the interface configuration mode, use the following command:

ip ospf network {**point-to-point** | **point-to-multipoint**}

- **point-to-point** – Specifies the network type of an interface as the point-to-point type.。
- **point-to-multipoint** - Specifies the network type of an interface as the point-to-multipoint type.

To set the network type as the default broadcast type, use the following command:

no ip ospf network

Viewing OSPF Route Information

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

show ip route ospf [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the OSPF route information of the specified VRouter name.

To view the OSPF information of the FS device, in any mode, use the following command:

show ip ospf [**vrouter** *vrouter-name*] [**process** *process-id*]

- *vrouter-name* - Specifies the VRouter name.
- **process** *process-id* – Specifies the OSPF process.

To view the OSPF protocol's database information of the FS device, in any mode, use the following commands:

show ip ospf database {**asbr-summary** | **external** | **nssa-external** | **network** | **router** | **summary**} [*A.B.C.D*] [{**adv-router** *A.B.C.D*} | **self-originate**] [**vrouter** *vrouter-name*] [**process** *process-id*]

- **asbr-summary** - Shows the LSAs of the AS border router
- **external** - Shows the LSAs of the external network.
- **nssa-external** - Shows the external LSAs information of NSSA.
- **network** Shows the LSAs of the network.
- **router** - Shows the LSAs of the router.
- **summary** - Shows the LSAs summary.
- *A.B.C.D* - Shows the IP address of link status ID.
- **adv-router** *A.B.C.D* - Shows the LSAs of the specified router.

- self-originate - Only shows self- originated LSAs(from local router).
- *vrouter-name* - Specifies the VRouter name.
- process *process-id* − Specifies the OSPF process.

show ip ospf database [**max-age** | **self-originate**] [**vrouter** *vrouter-name*] [**process** *process-id*]

- max-age - Specify the maximum age time.
- self-originate - Only shows self- originated LSAs(from local router).
- *vrouter-name* - Specifies the VRouter name.
- process *process-id* − Specifies the OSPF process.

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

show ip ospf interface [*interface-name*] [**vrouter** *vrouter-name*] [**process** *process-id*]

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

show ip ospf virtual-links [**vrouter** *vrouter-name*] [**process** *process-id*]

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

show ip ospf neighbor [*A.B.C.D* | **detail**] [**vrouter** *vrouter-name*] [**process** *process-id*]

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

show ip ospf route [*A.B.C.D*] [**vrouter** *vrouter-name*] [**process** *process-id*]

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

show route-map [*name*]

To view the route access-list information, in any mode, use the following command:

show access-list route [*name*]

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

show ip ospf distribute-list [**vrouter** *vrouter-name*] [**process** *process-id*]

Configuring IS-IS

IS-IS (Intermedia System-to-Intermediate System) is a dynamic routing protocol that is designed by ISP for CLNP (Connection-Less Network Protocol). To make it support IP, IETF (Interface Engineering Task Force) modified IS-IS in RFC 1195. With the modifications added, the new IS-IS, which is called Integrated IS-IS or Dual IS-IS, can be used in both TCP/IP environment and OSI environment. FSOS supports the application of IS-IS in the TCP/IP environment.

You can configure the IS-IS for each virtual router. Configuring IS-IS includes the following sections:

- Configuring the Router Type
- Enabling IS-IS at Interfaces
- Configuring the Interface Type
- Configuring the Network as Point-to-Point Type
- Configuring the NET Address
- Configuring the Administrative Distance
- Configuring the Metric Style
- Configuring the Interface Metric
- Configuring Redistribute
- Configuring the Default Route Advertisement
- Configuring the Interval for Sending Hello Packets
- Configuring the Multiplier for Hello Packets
- Configuring Padding for Hello Packets
- Configuring the Passive Interface
- Configuring Priority for DIS Election
- Configuring LSP Generation Interval
- Configuring Maximum Age of LSPs
- Configuring LSP Refresh Interval
- Configuring SPF Calculation Interval
- Configuring the Overload Bit
- Configuring Hostname Mappings
- Configuring the Authentication Methods
- Configuring the Interface Authentication

Basic Settings

To configure the IS-IS dynamic routing protocol, you need to enter the IS-IS routing configuring mode by executing the following commands:

ip vrouter *vrouter-name* – In the global configuration mode, enter the VRouter configuration mode.

router isis – Enter the IS-IS routing configuration mode and create the IS-IS process. The IS-IS processes in each VRouter are independent.

To close the IS-IS process, use **no router isis** command in the VRouter configuration mode.

Configuring the Router Type

The types include Level-1 router, Level-2 router, and Level-1-2 router. To configure the router type, use the following command in the IS-IS routing configuration mode:

is-type [level-1 | level-1-2 | level-2-only]

- **level-1** | **level-1-2** | **level-2-only** – Configure the type as Level-1 router (**level-1**) , Level-2 router (**level-2-only**), or Level-1-2 router (**level-1-2**). The default type is Level-1-2. Only when the type is Level-1-2, you are allowed to configure the interface type as Level-1 or Level-2.

To cancel the type settings, use the **no is-type** command in the IS-IS routing configuration mode.

Enabling IS-IS at Interfaces

By default, the IS-IS function is disabled at the interface. After creating an IS-IS process at the current router, proceed to enable the IS-IS function at the interface. Use the following command in the interface configuration mode:

isis enable

Use the **no isis enable** command to disable the IS-IS function at the interface.

Configure the Interface Type

When the router type is Level-1, the interface type can only be Level-1 and it can only establish the Level-1 adjacency. When the router type is Level-2, the interface type can only be Level-2 and it can only establish the Level-2 adjacency. When the router type is Level-1-2, the interface type can be Level-1 and Level-2. To configure the interface type, use the following command in the interface configuration mode:

isis circuit-type [level-1 | level-1-2 | level-2-only]

- **level-1** | **level-1-2** | **level-2-only** – Specify the interface type as Level-1 interface (**level-1**), Level-2 interface (**level-2-only**), or Level-1-2 interface (**level-1-2**).

Configuring the Network as Point-to-Point Type

If there are two devices in the broadcast network, you can configure the link that the interface locates as the point-to-point type. For point-to-point type link, IS-IS does not execute the DIS election and CSNP flooding. Use the following command in the interface configuration mode:

```
isis network point-to-point
```

Use the **no isis network point-to-point** command to cancel the above settings.

Routing Information Settings

Configuring the NET Address

NET (Network Entity Title) represents the network layer information of the IS, excluding the transmission layer information. The NET address is used to mark the device with the IS-IS process enabled. An IS-IS process can have at most three NET addresses and these NET addresses must have the same System IDs. To specify the NET address for the device, use the following command in the IS-IS routing configuration mode:

net *net*

- *net* – Specify the NET address for the device. When you use this device as level-1 router, it must have the same area ID with other devices in the same area. When you use this device as level-2 router, the process of establishing the adjacency will not check the area ID.

To cancel the NET address configurations, use the **no net** *net* command.

Configuring the Administrative Distance

To configure the administrative distance, use the following command in the IS-IS routing configuration mode:

distance *distance-value*

- *distance-value* – Specify the administrative distance. The value ranges from 1 to 255. The default value is 115.

To cancel the configurations, use the **no distance** command.

Configuring the Metric Style

If the metric style is Narrow, the router only generates and receives packets whose metric field is narrow. The metric value of the interface ranges from 0 to 63. For the large network environment, the maximum allowed metric of a route is 1023. When the metric value exceeds 1023, the destination is considered to be unreachable. If the metric style is Wide, the router only generates and receives packets whose metric field is wide. The metric value of the interface ranges from 0 to 16777215. If the metric style is transition, the router can generate and receive packets whose metric field is wide or narrow. To configure the metric style, use the following command in the IS-IS routing configuration mode:

metric-style {**wide** | **narrow** | **transition**}

- **wide** - The router only generates and receives packets whose metric field is Wide.
- **narrow** - The router only generates and receives packets whose metric field is Narrow.
- **transition** - The router can generate and receive packets whose metric field is Wide or Narrow.

To cancel the metric style configurations, use the **no metric-style** command.

Configuring the Interface Metric

The metric is used to calculate the cost to the destination network via the selected link. To configure the metric of the link, use the following command in the interface configuration mode:

isis metric *value* [**level-1** | **level-2**]

- *value* − Configure the metric value of the link that the interface locates. The value ranges from 1 to 16777214 and the default value is 10.
- **level-1** | **level-2** − Use **level-1** to configure the metric value for Level-1 routes. Use **level-2** to configure the metric value for Level-2 routes. Without specifying **level-1** or **level-2**, the metric value is effective for both Level-1 and Level-2 routes.

Use the **no isis metric** command to restore the metric value to the default one.

Configuring Redistribute

IS-IS allows you to introduce routing information from other routing protocols (connected, static, OSPF, BGP and RIP) and redistribute the information. To configure the redistribute and the corresponding metric, in the IS-IS routing configuration mode, use the following commands:

redistribute {**connected** | **static** | **ospf** | **bgp** | **rip**} [**level-1** | **level-1-2** | **level-2**] [**metric** *value*] [**metric-type** {**external** | **internal**}]

- **connected** | **static** | **ospf** | **bgp** | **rip** - Specify the protocol type which can be **connected**, **static**, OSPF, **bgp**, or **rip**.
- **level-1** | **level-1-2** | **level-2** − Specify the level for the introduced route, including the level-1 route (**level-1**), level-2 route (**level-2**), and both levels (**level-1-2**).

- **metric** *value* - Specify a metric value for the introduced route. The value range is 0 to 4294967296. The default value is 0. When the metric type of the router is narrow, the metric value of the introduced route cannot exceed 63.
- **metric-type** {**external** | **internal**} – If you select the external metric type (**external**), the metric value will be the sum of the value configured in metric value and 64. If you select the internal metric type (**internal**), the metric value will be the one you configured in the metric value command. The default option is internal.

To cancel the redistribute configurations, use the **no redistribute** {**connected** | **static** | **ospf** | **bgp** | **rip**} [**level-1** | **level-1-2** | **level-2**] command.

Configuring the Default Route Advertisement

The default route in the introduced routing information will not be used by the routers. To advertise the default route in the routing domain, in the IS-IS routing configuration mode, use the following command:

default-information originate

If there is a default route in the router with the above command configured, the IS-IS process in this router will advertise this route via Level-2 LSPs.

To cancel the default route advertisement, use the **no default-information originate** command.

Network Optimization

Configuring the Interval for Sending Hello Packets

To configure the interval that the interface sends Hello packets, use the following command in the interface configuration mode:

isis hello-interval *value* [**level-1** | **level-2**]

- *value* – Specify the interval that the interface sends Hello packets. The value ranges from 1 to 600. The unit is second. The default value is 3.
- **level-1** | **level-2** – Use **level-1** to configure the interval for sending Level-1 Hello packets. Use **level-2** to configure the interval for sending Level-2 Hello packets.

Use the **no isis hello-interval** command to restore the interval to the default value.

Configuring the Multiplier for Hello Packets

Within the hold time, if a router does not receive Hello packets form its neighbor, it considers the neighbor down and will re-calculate the routes. The hold time is to multiply the Hello multiplier and the

Hello interval. To configure the Hello multiplier, use the following command in the interface configuration mode:

isis hello-multiplier *value* [**level-1** | **level-2**]

- *value* − Specify the multiplier for Hello packets. The value ranges from 2 to 100. The default value is 10.
- **level-1** | **level-2** − Use **level-1** to configure the multiplier for Level-1 Hello packets. Use **level-2** to configure the multiplier for Level-2 Hello packets. Without specifying **level-1** or **level-2**, the multiplier value is effective for both Level-1 and Level-2 Hello packets.

To restore the multiplier value to the default value, use the **no isis hello-multiplier** command.

Configuring Padding for Hello Packets

Use the padding function to pad the hello packets and make them as large as the MTU of the interface. To configure the padding function, use the following command in the interface configuration mode:

isis hello padding

To cancel the padding function, use the **no isis hello padding** command.

Configuring Priority for DIS Election

In the broadcast network, you can specify the DIS priority for the interface to influence the DIS election. In the DIS election, the router whose interface has higher DIS priority will be selected as the DIS. If interfaces have the same priority, the router whose interface has larger MAC address will be selected as the DIS. To configure the DIS priority for the interface, use the following command in the interface configuration mode:

isis priority *value* [**level-1** | **level-2**]

- *value* − Specify the DIS priority for this interface. The value ranges from 0 to 127. The default value is 64.
- **level-1** | **level-2** − Use **level-1** to specify the priority for the Level-1 interface. Use **level-2** to specify the priority for the Level-2 interface. Without specifying **level-1** or **level-2**, the priority is effective for both Level-1 and Level-2 interfaces.

Use the **no isis priority** [**level-1** | **level-2**] command to restore the priority of the specified interface level to the default one.

Configuring the Passive Interface

After configure an interface as a passive interface, this interface will not send and receive any IS-IS packets, and it will not establish adjacency with neighbors. But you can redistribute the connected routing information about this network to other interfaces via LSPs. To configure an interface as a passive interface, use the following command in the interface configuration mode:

isis passive

Use the **no isis passive** command to cancel the above settings.

Configuring LSP Generation Interval

When the network topology changes, the router will generate LSPs. To avoid the frequent generation of LSPs consuming a larger amount of router resources and bandwidth, you can configure the LSP generation interval. In the IS-IS routing configuration mode, use the following command to configure the LSP generation interval:

lsp-gen-interval *value* [**level-1** | **level-2**]

- *value* − Specify the LSP generation interval. The value ranges from 1 to 120. The default value is 30. The unit is second.
- **level-1** | **level-2** − Enter **level-1** to specify the LSP generation interval for level-1 LSPs only, and enter **level-2** to specify the LSP generation interval for level-2 LSPs only. If you enter no parameter, the configured interval value will be used for both level-1 LSPs and level-2 LSPs.

To restore the value to the default one, use the **no lsp-gen-interval** command.

Configuring Maximum Age of LSPs

Each LSP has a maximum age. The LSP with an age of 0 will be deleted from the LSDB. To configure the maximum age of LSPs, in the IS-IS routing configuration mode, use the following command:

max-lsp-lifetime *value*

- *value* − Specify the maximum age of LSP. The value ranges from 350 to 65535. The default value is 1200. The unit is second.

To restore the value to the default one, use the **no max-lsp-lifetime** command.

Configuring LSP Refresh Interval

Since each LSP has a maximum age, the router must refresh the LSPs generated by itself. To configure the LSP refresh interval, in the IS-IS routing configuration mode, use the following command:

lsp-refresh-interval *value*

- *value* − Specify the LSP refresh interval. The value ranges from 1 to 65535. The default value is 900. The unit is second. FS recommends that the refresh interval is 300s less than the maximum age, which ensures that the LSP refresh can reach the routes within the area before the arrival of the maximum age.

Use the **no lsp-refresh-interval** command to restore the value to the default one.

Configuring SPF Calculation Interval

If the LSDB changes, the router will re-calculate the SPF. To configure the SPF calculation interval, use the following command in the IS-IS routing configuration mode:

spf-interval *value* [**level-1** | **level-2**]

- *value* − Specify the SPF calculation interval. The value ranges from 1 to 120. The default value is 10. The unit is second.
- **level-1** | **level-2** − Enter **level-1** to specify the SPF calculation interval for level-1 SPFs only, and enter **level-2** to specify the SPF generation interval for level-2 SPFs only. If you enter no parameter, the configured interval value will be used for both level-1 SPFs and level-2 SPFs.

Use the **no spf-interval** command to restore the value to the default one.

Configuring the Overload Bit

The lack of resources can lead to the result that the LSDB is inaccurate or incomplete. The router whose resource is lack will add the overload bit in the LSPs. After other routers receive these LSPs, they will not use this router whose resource is lack to forward packets. If the packets whose destination address is the network that is connected to this router, the packets will still be forward to this router. To configure the overload bit for the router, use the following command in the IS-IS routing configuration mode:

set-overload-bit

To cancel the overload bit configuration, use the **no set-overload-bit** command.

Configuring Hostname Mappings

In the IS-IS routing domain, System ID, as part of the NET address, is used to identify the host or the router. Hostname mapping maps the System ID to the hostname. The router will maintain a mapping table which records the mapping settings between the System ID and the hostname. To configure the hostname mapping, use the following command in the IS-IS routing configuration mode:

hostname dynamic

To cancel the hostname mapping, use the **no hostname dynamic** command.

Authentication

Configuring the Authentication Methods

Configure the authentication methods for the LSP packets, CSNP packets, and PSNP packets. With the authentication configured, routers will authenticate the preceding packets when they receive them. But this will not affect the Hello packets for establishing neighbors. There are two authentication methods, clear text authentication and MD5 authentication. As the default option, the clear text authentication cannot secure the communication and the password is forwarded together with the packets. To configure the authentication method, use the following command in the IS-IS routing configuration mode:

authentication {md5 | text} [level-1 | level-2]

- **md5** | **text** – Use the MD5 authentication (**md5**) or the clear text authentication (**text**).
- **level-1** | **level-2** – Use **level-1** to configure the authentication method for the packets between Level-1 routers, which prevents Level-1 routers learning the routing information from the untrusted routers . The Level-1 routers in the same area must use the same authentication method and password. Use **level-2** to configure the authentication method for the packets between level-2 routers, whichi prevents Level-2 routers learning the routing information from the untrusted routers. The Level-2 routers in the same routing domain must use the same authentication method and password.

To cancel the authentication configurations, use the **no authentication mode** command in the IS-IS routing configuration mode.

After configuring the authentication methods, proceed to configure the passwords. To specify the password for the packet authentication between level-1 routers, use the following command in the IS-IS routing configuration mode:

area-password *word*

- *word* – Specify the password. You can specify at most 32 characters. To delete the password, use the no area-password command.

To delete the password, use the **no area-password** command.

To specify the password for the packet authentication between level-2 routers, use the following command in the IS-IS routing configuration mode:

domain-password *word*

- *word* – Specify the password. You can specify at most 32 characters.

To delete the password, use the **no domain-password** command.

Configuring the Interface Authentication

Interface authentication is used to verify the legality of its neighbors and avoid the adjacency establishment with illegal routers. After configuring interface authentication, the password will be encapsulated in the Hello packets. After the packets were verified, the routers can become neighbors. To become neighbors, two interfaces must use the same interface authentication method and password. To configure the interface authentication, use the following command in the interface configuration mode:

isis authentication {**md5** | **text**} [**level-1** | **level-2**]

- **md5** | **text** – Use the MD5 authentication（**md5**or the clear text authentication (**text**).
- **level-1** | **level-2** – Use **level-1** to configure the authentication method for the Hello packets between Level-1 routers. Use **level-2** to configure the authentication method for the Hello packets between level-2 routers.

To cancel the interface authentication, use the **no isis authentication** command.

After configuring the interface authentication method, proceed to specify the password for the authentication. Use the following command in the interface configuration mode:

isis password *word* [**level-1** | **level-2**]

- *word* – Specify the password. You can specify at most 32 characters.
- **level-1** | **level-2** – Use **level-1** to configure the password for the Hello packets between Level-1 routers. Use **level-2** to configure the password for the Hello packets between level-2 routers.

Use the **no isis password** command to cancel the specified password.

Viewing IS-IS Information

To show the IS-IS process and corresponding information, use the following command in any mode:

show isis [**vrouter** *vrouter-name*]

- *vrouter-name* – Show the information of the specified vrouter.

To show the link state database, use the following command in any mode:

show isis database [**detail**] [**vrouter** *vrouter-name*]

- **detail** – Show the detailed information.

- *vrouter-name* – Show the information of the specified vrouter.

To show the IS-IS interface information, use the following command in any mode:

show isis interface [*interface-name*]

To show the IS-IS neighbor information, use the following command in any mode:

show isis neighbor [**detail**] [**vrouter** *vrouter-name*]

To show the dynamic host information, use the following command in any mode:

show isis hostname [**vrouter** *vrouter-name*]

To show the IS-IS routing information, use the following command in any mode:

show isis route [*A.B.C.D/M*] [**vrouter** *vrouter-name*]

To show the routing redistribute information, use the following command in any mode:

show isis route redistribute [**level-1** | **level-2**] [*A.B.C.D/M*] [**vrouter** *vrouter-name*]

Configuring BGP

BGP, the abbreviation for Border Gateway Protocol, is a routing protocol that is used to exchange dynamic routing information among the autonomous systems (An autonomous system is the router and network group under the control of a management institution. All the routers in the autonomous system must run the same routing protocol). It is also the protocol used between ISPs. BGP runs over port TCP 179, and supports Classless Inter-Domain Routing (CIDR). BGP operates in two ways: when running between the autonomous systems, it is known as EBGP; when running within the autonomous system, it is know as IBGP. BGP has the following characteristics:

- After the initial TCP connection has been established, BGP neighbors exchange the entire BGP routing tables, then they only exchange the updated routing information.
- Periodically sending KEEPALIVE packets to check TCP connectivity.
- BGP routers only advertise the shortest path to the neighbors.
- BGP is a distance vector routing protocol that is designed to avoid the routing loop.

The router that sends BGP messages is known as a BGP speaker. The BGP speaker will receive or generate new routing information, and advertise to other speakers. When a speaker receives a new route from another autonomous system, if the route is shorter than all the known routes, or there is no known route at all, the speaker will advertise the route to all the other speakers. The BGP speaker that is exchanging information is knows as a peer to its counterpart, and multiple associated peers can constitute a peer group. The purpose of the peer group is to simplify the configuration. It does not affect the establishment of the actual peer relationship or the advertisement of routes.

There are four types of BGP packets: OPEN, UPDATE, NOTIFICATION, and KEEPALIVE. BGP peers send OPEN packets to exchange their versions, autonomous system numbers, holddown time, BGP identifiers and other information, and negotiate with each other. The OPEN packet is mainly used to establish neighbor (BGP Peer) relationship. It is the initial handshake message between BGP routers, and should be sent before advertising any message. When a peer receives an OPEN message, it will respond with a KEEPALIVE message. Once the handshake has been completed successfully, these BGP neighbors will be able to exchange UPDATE, KEEPALIVE, NOTIFICATION and other messages. The UPDATE packet carries the routing update information, including the revoked routes, reachable routes and the reachable routes' paths. When detecting any error (connection interruption, negotiation error, packet error, etc.), BGP will send a NOTIFICATION packet, and drop the connection to the peer. The KEEPALIVE packets are transmitted between BGP peers periodically, in order to ensure connectivity.

Configuring BGP Protocol

You can configure the BGP protocol for different VRouters respectively. The BGP protocol configuration includes:

- Entering the BGP configuration mode
- Specifying a Router ID
- Creating a route aggregation
- Adding a static BGP route
- Configuring a timer
- Specifying the administration distance of BGP route
- Specifying the default metric
- Configuring redistribute
- Creating a BGP peer group
- Adding a BGP peer to the peer group
- Configuring a BGP peer
- Activating a BGP connection
- Configuring the default information originate
- Configuring description
- Configuring a BGP peer timer

- Configuring the next hop as itself
- Configuring EBGP multihop
- Disabling a peer or peer group
- Resetting a BGP connection
- Configuring an AS-path access list
- Configuring BGP communities
- Redistributing routes into BGP
- Configuring a route map
- Modifying attributes of introduced routing information
- Configuring route filters based on the AS-path access list
- Sending communities path attributes to peers or peer groups
- Configuring route filters based on the route map
- Configuring equal cost multipath routing

Entering the BGP Configuration Mode

The BGP protocol options must be configured in the BGP routing mode. To enter the BGP routing mode, in the global configuration mode, use the following commands:

ip vrouter *vrouter-name* (enters the VRouter configuration mode)

router bgp *number*

- *number* - Specifies the number of the autonomous system. The value range is 1 to 4,294,967,295.

The above command will enable the BGP function on the system, create a BGP instance for the specified autonomous system, and switch to the BGP instance configuration mode.

To delete the specified BGP instance, in the VRouter configuration mode, use the command **no router bgp** *number*.

Specifying a Router ID

Each router running BGP protocol must be labeled with a Router ID. The Router ID is the unique identifier of an individual router in the whole BGP domain, represented in the form of an IP address. If the Router ID is not specified, the system will set the largest IP address of the loopback interface on the device as the Router ID; if there is no loopback interface or the IP address of the loopback interface is not configured, the system will select the largest IP address of other interfaces as the Router ID. To specify the Router ID, in the BGP instance configuration mode, use the following command:

router-id *A.B.C.D*

- *A.B.C.D* - Specifies the Router ID used by BGP protocol, in form of an IP address.

To cancel the specified Router ID, in the BGP instance configuration mode, use the following command:

no router-id

Creating a Route Aggregation

You can aggregate the routing entries in the BGP routing table. To create a route aggregation, in the BGP instance configuration mode, use the following command:

aggregate-address {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} [**as-set**] [**summary-only**]

- *A.B.C.D/M* | *A.B.C.D A.B.C.D* - Specifies the network address for the aggregation. FS devices support two formats: *A.B.C.D/M* or *A.B.C.D A.B.C.D,* for example, 1.1.1.0/24 or 1.1.1.0 255.255.255.0.
- **as-set**- If this parameter is specified, the system will advertise the aggregated path information to other routers as its own path information.
- **summary-only** - If this parameter is specified, the system will only advertise the aggregated route.

To cancel the specified route aggregation, in the BGP instance configuration mode, use the following command:

no aggregate-address {*A.B.C.D/M* | *A.B.C.D A.B.C.D}*

Adding a Static BGP Route

To add a static BGP route, in the BGP instance configuration mode, use the following command:

network {*A.B.C.D/M* | *A.B.C.D A.B.C.D*}

- *A.B.C.D/M* | *A.B.C.D A.B.C.D* - Specifies the static BGP routing entry. FS devices support two formats: *A.B.C.D/M* or *A.B.C.D A.B.C.D*, for example, 1.1.1.0/24 or 1.1.1.0 255.255.255.0.

To delete the specified static routing entry, in the BGP instance configuration mode, use the following command:

no network {*A.B.C.D/M* | *A.B.C.D A.B.C.D*}

Configuring a Timer

You can configure two BGP timers which are KEEPALIVE and HOLDDOWN, as described below:

- KEEPALIVE: The interval of sending the KEEPALIVE message to the BGP peer. By default FSOS sends the message every 60 seconds.
- HOLDDOWN: If the local router still has not received the KEEPALIVE message from any peer after the HOLDDOWN time, then it will determine the peer is not active any more. The default value is 180 seconds.

To configure a timer, in the BGP instance configuration mode, use the following command:

timers *keepalive holddown*

- *keepalive* - Specifies the interval for sending the KEEPALIVE message. The value range is 0 to 65535 seconds, but should not be larger than HOLDDOWN/3. The default value is 60. If the value is larger than HOLDDOWN/3, the actual effective time will be HOLDDOWN/3. The value 0 indicates never sending the KEEPALIVE message.
- *holddown* - Specifies the HOLDDOWN time. The value range is 0 to 65535 seconds or 3 to 65535 seconds. The default value is 180. The value 0 indicates never checking the HOLDDOWN time.

To restore to the default timer value, in the BGP instance configuration mode, use the following command:

no timers

Specifying the Administration distance of BGP Route

You can specify the administration distance for the local BGP routes or the BGP routes acquired from other peers. To specify the administration distance for a BGP route, in the BGP instance configuration mode, use the following command:

distance *ebgp-distance ibgp-distance local-distance*

- *ebgp-distance* - Specifies the administration distance for the EBGP route. The value range is 1 to 255. The default value is 20.

- *ibgp-distance* - Specifies the administration distance for the IBGP route. The value range is 1 to 255. The default value is 200.
- *local-distance* - Specifies the administration distance for the local route. The value range is 1 to 255. The default value is 200.

To restore to the default administration distance for a BGP route, in the BGP instance configuration mode, use the following command:

no distance

Specifying the Default Metric

By default, the metric of the redistributed IGP route remains unchanged, and the metric of the redistributed connected route is 0. To specify the default metric of the redistributed routing, in the BGP instance configuration mode, use the following command:

default-metric *value*

- *value* - Specifies the default metric value. The value range is 1 to 4294967295. To restore to the default metric value, in the BGP instance configuration mode, use the following command:

To restore to the default metric value, in the BGP instance configuration mode, use the following command:

no default-metric

Creating a BGP Peer Group

The BGP peer group is designed to simplify the configuration, and update the information in a more effective way. To create a BGP peer group, in the BGP instance configuration mode, use the following command:

neighbor *peer-group-name* **peer-group**

- *peer-group-name* - Specifies a name for the new peer group.

To delete the specified BGP peer group, in the BGP instance configuration mode, use the following command:

no neighbor *peer-group-name* **peer-group**

Adding a BGP Peer-to-peer Group

To add a BGP peer-to-peer group, in the BGP instance configuration mode, use the following command:

neighbor *A.B.C.D* **peer-group** *peer-group-name*

- *A.B.C.D* - Specifies the IP address of the BGP peer that will be added.
- *peer-group-name* - Specifies the peer group that has been created in the system.

To delete the specified BGP peer from the BGP peer group, in the BGP instance configuration mode, use the following command:

no neighbor *A.B.C.D* **peer-group** *peer-group-name*

Configuring a BGP Peer

To exchange BGP routing information, you need to specify a BGP peer (peer group) for the device. To configure a BGP peer, in the BGP instance configuration mode, use the following command:

neighbor {*A.B.C.D* | *peer-group*} **remote-as** *number*

- *A.B.C.D* | *peer-group* - Specifies the IP address of the peer or the name of the peer group.
- *number* - Specifies the number of autonomous system the configured peer or peer group belongs to.

To cancel the specified BGP peer or peer group, in the BGP instance configuration mode, use the following command:

no neighbor {*A.B.C.D* | *peer-group*} **remote-as**

Configuring BGP MD5 Authentication

To improve BGP security, you can configure MD5 authentication for the BGP peer or peer group. With this function enabled, the two ends of a peer will have to pass the MD5 authenticatoin in order to establish a TCP connection. To configure BGP MD5 authentication, in the BGP instance configuration mode, use the following command:

neighbor {*A.B.C.D* | *peer-group*} **password** *password*

- *A.B.C.D* | *peer-group* - Specifies the IP address of the peer or the name of peer group.
- **password** *password* - Specifies the MD5 password string. The value range is 1 to 32 characters.

To cancel the BGP MD5 authentication,in the BGP instance configuration mode, use the following command:

no neighbor {*A.B.C.D* | *peer-group*} **password**

Note:The MD5 password configured on the peers or peer groups must be consistent.

Activating a BGP Connection

By default, the BGP connection between the configured BGP peer or peer group and the device is activated. You can de-activate or re-activate the BGP connection. To activate the BGP connection, in the BGP instance configuration mode, use the following command:

neighbor {*A.B.C.D* | *peer-group*} **activate**

- *A.B.C.D* | *peer-group* - Specifies the IP address of the peer or the name of the peer group.

To de-activate the BGP connection to the specified BGP peer or peer group, in the BGP instance configuration mode, use the following command:

no neighbor {*A.B.C.D* | *peer-group*} **activate**

Configuring the Default Information Originate

You can specify if the default route will be redistributed to other BGP peers or peer groups. By default BGP will not redistribute the default route.

To configure the default information originate, in the BGP instance configuration mode, use the following command:

default-information originate

If there is no default route in the routing table,the system will not redistribute default route any more.

To cancel the default information originate, in the BGP instance configuration mode, use the following command:

no default-information originate

To configure the default information originate, in the BGP instance configuration mode, use the following command:

neighbor {*A.B.C.D* | *peer-group*} **default-originate**

- *A.B.C.D* | *peer-group* - Specifies the IP address of the peer or the name of the peer group.

If there is no default route in the routing table,the system will construct a default route to redistribute.

To cancel the default information originate, in the BGP instance configuration mode, use the following command:

no neighbor {*A.B.C.D* | *peer-group*} **default-originate**

Configuring Description

To configure description for a peer or peer group, in the BGP instance configuration mode, use the following command:

neighbor {*A.B.C.D* | *peer-group*} **description** *description*

- *A.B.C.D* | *peer-group* - Specifies the IP address of the peer or the name of the peer group.
- *description* - Specifies the description. The length is 1 to 80 characters.

To cancel the description of the specified peer or peer group, in the BGP instance configuration mode, use the following command:

no neighbor {*A.B.C.D* | *peer-group*} **description**

Configuring a BGP Peer Timer

By default, the timer of BGP peers or peer groups in the whole BGP system is set to the value specified by timer keepalive holddown. You can specify a different timer value for a specific BGP peer or peer group. The priority of the specified value is higher than that of the value specified by timer keepalive holddown. To specify a timer value for a BGP peer or peer group, in the BGP instance configuration mode, use the following command:

neighbor {*A.B.C.D* | *peer-group*} **timers** *keepalive holddown*

- *A.B.C.D* | *peer-group* - Specifies the IP address of the peer or the name of the peer group.
- *keepalive* - Specifies the interval for sending the KEEPALIVE message. The value range is 0 to 65535 seconds, but should not be larger than HOLDDOWN/3. The default value is 60. If the value is larger than HOLDDOWN/3, the actual effective time will be HOLDDOWN/3. The value 0 indicates never sending the KEEPALIVE message.
- *holddown* - Specifies the HOLDDOWN time. The value range is 0 to 65535 or 3 to 65535 seconds. The default value is 180. The value 0 indicates never checking the HOLDDOWN time.

To cancel the specified timer for the BGP peer or peer group, in the BGP instance configuration mode, use the following command:

no neighbor {*A.B.C.D* | *peer-group*} **timers**

Configuring the Next Hop as Itself

With this function configured, the router will advertise the next hop of the BGP route for the BGP peer or peer group is the router itself. To configure the next hop as itself, in the BGP instance configuration mode, use the following command:

neighbor {*A.B.C.D* | *peer-group*} **next-hop-self**

- *A.B.C.D* | *peer-group* - Specifies the IP address of the peer or the name of the peer group.

To cancel next hop as itself, in the BGP instance configuration mode, use the following command:

no neighbor {*A.B.C.D* | *peer-group*} **next-hop-self**

Configuring EBGP Multihop

For BGP running between different AS (i.e., EBGP), if the BGP peers or peer groups are not directly connected, you need to configure EBGP multihop in order to establish neighbor between devices. To configure EBGP multihop, in the BGP instance configuration mode, use the following command:

neighbor {*A.B.C.D* | *peer-group*} **ebgp-multihop** [*ttl*]

- *A.B.C.D* | *peer-group* - Specifies the peer IP address or the name of peer group.
- *ttl*- Specifies the count of maximum hops to the peer IP address or peer group. The value range is 1 to 255, and the default value is 255. If no peer or peer group can be found after the maximum hops, the system will conclude neighbor cannot be established.

To cancel EBGP multihop, in the BGP instance configuration mode, use the following command:

no neighbor {*A.B.C.D* | *peer-group*} **ebgp-multihop**

Disabling a Peer/Peer Group

If a peer or peer group is disabled, all the sessions to the peer or peer group will be dropped, and all the relevant routing information will be deleted. To disable a peer or peer group, in the BGP instance configuration mode, use the following command:

neighbor {*A.B.C.D* | *peer-group*} **shutdown**

- *A.B.C.D* | *peer-group* - Specifies the IP address of the peer or the name of the peer group.

To re-enable the specified peer or peer group, in the BGP instance configuration mode, use the following command:

no neighbor {*A.B.C.D* | *peer-group*} **shutdown**

Resetting a BGP Connection

To reset a BGP connection, in the execution mode, use the following command:

clear ip bgp {* | *A.B.C.D* | **external** | **peer-group** *peer-group-name* | *number*} [**vrouter** *vrouter-name*]

- * - Resets all the existing BGP connections.
- *A.B.C.D* - Resets BGP connections to the specified peer.
- **external** - Resets all the existing EBGP connections.
- **peer-group** *peer-group-name* Resets BGP connections to the specified peer group.
- *number* - Resets BGP connections in the specified autonomous system.
- **vrouter** *vrouter-name* - Specifies the VRouter where the reset operation is performed.

Configuring an AS-path Access List

An AS-path access list is the sequence of the AS numbers that the route has traversed before reaching the destination network. Before reaching the destination network, the BGP route will add the AS number to the AS-path access list each time it traversed an AS.

With an AS-path access list, you can use the route filter function. The AS-path access list mainly consists of a set of regular expressions and the actions that will be performed when the route matches the regular expressions (permit or deny). When the regular expression matches the AS path of the route, the system will execute the specified action. If not, the system will deny the route. The system supports up to 64 AS-path access list and each AS-path access list supports up to 8 regular expressions.

To configure the AS-path access list, use the following command in the global configuration mode:

ip as-path access-list *access-list-number* {**deny** | **permit**} *regular-expression*

- *access-list-number* – Specifies the number of the AS-path access list. The range is 1 to 500.
- **deny** | **permit** – Specifies the action that will be performed to the route that matches the AS-path access list.
- *regular-expression* – Specifies the regular expressions to match the AS path. FSOS supports the PCRE.

To delete the AS-path access list, use the following command in the global configuration mode:

no ip as-path access-list *access-list-number* [{**deny** | **permit**} *regular-expression*]

In the example below, you can configure an AS-path access list whose number is 1, refuse the route that has traversed AS 31, and allow other routes.

```
hostname(config)# ip as-path access-list 1 deny _31_
hostname(config)# ip as-path access-list 1 permit .*
hostname(config)#
```

Configuring BGP Communities

The communities path attribute provides a way to group the routing information that has the same characteristics and it does not relate to the IP subnet and AS where it locates. Besides the customized communities path attribute, the system supports the following well-known community values that you can specify for BGP routes:

- No-export − Routes with this communities path attribute cannot be advertised to peers that are outside the AS.
- No-adverties − Route with this communities path attribute cannot be advertised to any BGP peers.
- Local-as − Route with this communities path attribute can be advertised to other peers in the local AS and cannot be advertised to peers outside the local AS.
- Internet − Route with this communities path attribute can be advertised to any BGP neighbor. By default, each route carries this communities path attribute.

A community list consists of attributes and actions that will be performed after the successful matching. If the communities path attribute of the route matches the specified attributes, the system will perform the specified action. If not, the system will deny the route. The system supports up to 128 community list and in each list, you can configure one permit rule and one deny rule.

To configure the community list, use the following command in the global configuration mode:

ip community-list {**standard** *community-list-name* | *community-list-number*} {**deny** | **permit**} {[**internet**] [**local-as**] [**no-advertise**] [**no-export**] [*community-number*]}

- **standard** *community-list-name* − Specifies the name of the community list. You can specify up to 31 characters.
- *community-list-number* − Specifies the number of the community list. The number is in the range of 1 to 99.

- **deny** | **permit** – Specifies the actions performed to the route that matched the list. deny means the route will be denied and permit means the route will be permitted.
- [**internet**] [**local-as**] [**no-advertise**] [**no-export**] [*community-number*] – Specifies the communities path attributes. You can specify one or more attributes and use one space to separate them. The value of *community-number*is in the range of 1 to 4294967295.

To delete the community list, use the following command in the global configuration mode:

no ip community-list {**standard** *community-list-name* | *community-list-number*}

Redistributing Routes into BGP

The BGP supports the function that redistributes routes of other protocols into BGP and advertises the routing information. Besides, you can set the metric of the redistributed route and use the route map to filter the routing information. To redistribute routes into BGP, use the following command in the BGP instance configuration mode:

redistribute {**ospf** | **connected** | **static** | **rip**} [**metric** *value*] [**route-map** *name*]

- **ospf** | **connected** | **static** | **rip** - Specifies the protocol type which can be **ospf**, **connected**, **static** or **rip**.
- **metric** *value* Specifies a metric value for the redistributed route. The value range is 0 to 16777214. If the value is not specified, the system will use the default BGP metric configured by the **default-metric** *value* command.
- **route-map** *name* - Specifies the route map that is used to filter the routing information introduced from other routing protocols. For more information about route map, see Configuring a Route Map.

You can use the command above to redistribute route of different types.。

To cancel the redistributed route, use the following command: **no redistribute** {**ospf** | **connected** | **static** | **rip**}.

Configuring a Route Map

By default the system will introduce all the routing information. You can filter the routing information introduced from other routing protocols by referencing a route map. The route map mainly consists of two parts: matching rules and actions (permit or deny) for the matched routing information. If introduced routing information hits any matching rule, the system will take the configured action, i.e., permit or deny the introduced routing information.

Note:

- If the action is set to Permit, the system will only permit the matched routing information and deny all the unmatched routing information.
- If the action is set to Deny, the system will deny the matched routing information, but still permit all the unmatched routing information.

To configure a route map and filter the introduced routing information, take the following steps:

1. Create a route map and add matching rules to the route map. Matching rules are differentiated by IDs. The smaller the ID is, the higher the matching priority will be. By default if the routing information hits any matching rule, the system will not continue to match the subsequent rules; if no matching rule is hit, the system will take the Deny action.
2. Add matching conditions to the matching rules. The matching condition can be the AS path, communities path attribute, metric, destination IP address, or next-hop IP address of the introduced routing information. One matching rule may contain multiple matching conditions, and the relation between these conditions is AND, i.e., in order to hit a matching rule, the routing information must satisfy all the matching conditions in the rule.
3. If needed, require the system to continue to match another rule after the routing information hits a matching rule.
4. If needed, modify partial attributes of the introduced routing information before redistribution.

To create a route map and add a matching rule to the route map, in the global configuration mode, use the following command:

route-map *name* {**deny** | **permit**} *sequence*

- **route-map** *name* - Specifies the name of the route map, and enters the route map configuration mode. The value range is 1 to 31 characters. If the name already exists in the system, you will directly enter the route map configuration mode.
- **deny** | **permit** - Specifies the action for the matched routing information.
- *sequence* - Specifies the sequence number for the matching rule in the route map. The value range is 1 to 65535.

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

no route-map *name* [*sequence*]

- *sequence* - Only deletes the specified matching rule from the route map.

To add a matching condition to the matching rule, in the route map configuration mode, use the following command:

match {**as-path** *access-list-number* | **community** {*community-list-name* | *community-list-number*} [*exact-match*] | **metric** *metric-value* | **ip address** *access-list* | **ip next-hop** *access-list*}

- **as-path** *access-list-number* – Matches the AS path of the introduced routing information. *access-list-number* is the number of the AS-path access list configured by yourself. If the AS path of the route matches the AS path that is permitted in this AS-path access list, the system concludes that the matching is successful. For more information about configuring an AS-path access list, see Configuring an AS-path Access List"。

- **community** {*community-list-name* | *community-list-number*} [*exact-match*] – Matches the communities path attributes of the introduced routing information. *community-list-name* is the name of the community list. *community-list-number* is the number of the community list. exact-match indicates that the system will execute the exact matching. For more information about configuring community list, see Configuring BGP Communities.

- **metric** *metric-value* – Matches the metric of the introduced routing information. The value range is 0 to 4294967295.

- **ip address** *access-list* – Matches the destination address of the introduced routing information. *access-lis*t is the route access-list configured in the system. If the destination address of the routing information is the permitted address in the route access-list, the system will conclude the matching succeeds. For more information about route access-list, see Configuring an AS-path Access List.

- **ip next-hop** *access-list* - Specifies to match the next-hop IP address of the introduced routing information. *access-list* is the route access-list configured in the system. If the next-hop IP address of the routing information is the permitted address in the route access-list, the system will conclude the matching succeeds. For more information about route access-list, see Configuring a Route Access-list.

Repeat the above command to add more matching conditions to the matching rule. To delete the specified matching condition from the matching rule, use the following command:

no match {**as-path** | **community** | **metric** | **ip address** | **ip next-hop**}

Note:If you only created a route map but did not add any matching rule, by default the system will conclude all the introduced routing information is matched.

Modifying Attributes of Introduced Routing Information

For the introduced routing information that satisfies the matching conditions, you can modify partial attributes before the redistribution. To modify the attribute of the introduced routing information, in the route map configuration mode, use the following command:

set {**as-path prepend** *as-number* | **commu-list** {*community-list-name* | *community-list-number*} **delete** | **community** {[**internet**] [**local-AS**] [**no-advertise**] [**no-export**] [*community-list-number*]} [**additive**] | **ip next-hop** *ip-address* | **local-preference** *value* | **metric** *metric-value* | **origin** {**egp** | **igp** | **incomplete**} }

- **as-path prepend** *as-number* − Add a new AS path after the existing AS path of the introduced route. The rang is 1 to 65535 and you can use spaces to separate multiple values.
- **commu-list** {*community-list-name* | *community-list-number*} **delete** − Uses *community-list-name* to specifies the name of the community list or use *community-list-number* to specify the number of the community list. Delete the matched communities path attribute.
- **community** {[**internet**] [**local-AS**] [**no-advertise**] [**no-export**] [*community-list-number*]} [**additive**] − Modifies the communities path attributes of the introduced route. You can use additive to add new attributes to the ones of the introduced route.
- **ip next-hop** *ip-address* − Modifies the next-hop IP address of the introducted route.
- **local-preference** *value* − Modifies the attribute of the local preference of the route. The range is 0 to 4294967295.
- **metric** *metric-value* - Specifies the metric type of the external route. type-1 indicates type1 external route metric, and type-2 indicates type2 external route metric.
- **origin** {**igp** | **egp** | **incomplete**} − Modifies the source attribute of the introduced route. *igp* means the route comes from internal AS; *egp* means the route is obtained from EGP. *incomplete* means the route is obtained by other methods.

To cancel the modification and restore to the settings when the routing information was introduced, use the following command:

no set {**as-path prepend** | **commu-list** | **community** | **ip next-hop** | **local-preference** | **origin** | **metric** | **metric-type**}

Configuring Route Filters Based on the AS-path Access List

BGP uses the AS-path access list to filter the route introduced by the peers or peer groups or the route advertised. To configure the route filter function based on the AS-path access list, use the following command in the BGP instance configuration mode:

neighbor {*A.B.C.D* | *peer-group*} **filter-list** *access-list-number* {**in** | **out**}

- *A.B.C.D* | *peer-group* – Specifies the IP address or the name of the BGP peer.
- *access-list-number* – Specifies number of the AS-path access list. For more information about AS-path access list, see Configuring an AS-path Access List.
- **in** | **out** – Use **in** to filter the introduced routes or use **out** to filter the advertised routes.

Use the following command to cancel the above configurations:

no neighbor {*A.B.C.D* | *peer-group*} **filter-list** {**in** |**out**}

Sending Communities Path Attributes to Peers or Peer Groups

To send communities path attributes to peers or peer groups, use the following command in the BGP instance configuration mode:

neighbor {*A.B.C.D* | *peer-group*} **send-community** {**standard** | **extended** | **both**}

- *A.B.C.D* | *peer-group* - Specifies the IP address of the BGP peer or the name of the peer group.
- **standard** | **extended** | **both** – Specifies the type of the communities path attributes. There are three types: **standard** means the standard communities path attributes, **extended** means the extended communities path attributes, and **both** means both of the communities path attributes and extended communities path attributes.

Use the following command to cancel the above configurations:

no neighbor {*A.B.C.D* | *peer-group*} **send-community**

Configuring Route Filters Based on the Route Map

BGP uses the route map to filter the route introduced by the peers or peer groups or the route advertised. To configure the route filter function based on the route map, use the following command in the BGP instance configuration mode:

neighbor {*A.B.C.D* | *peer-group*} **route-map** {**in** |**out**}

- *A.B.C.D* | *peer-group* – Specifies the IP address of the BGP peer or the name of the peer group.
- **in** | **out** – Use **in** to filter the introduced routes or use **out** to filter the advertised routes.

Use the following command to cancel the above configurations:

no neighbor {*A.B.C.D* | *peer-group*} **route-map** {**in** |**out**}

Configuring Equal Cost Multipath Routing

To configure the maximum number of equal cost multipath (ECMP) routes for BGP, use the following command in the BGP instance configuration mode:

maximum-paths {**ebgp** | **ibgp**} *maximum-number*

- *maximum-number* – Specifies the maximum number of ECMP routes for IBGP/EBGP. When there are eligible ECMP paths, they will be added to the routing table according to the maximum number you specified. With these configurations, ECMP assists with load-balancing of BGP on multiple routes. The range is 1 to 8 and the default value is 1.

Use the following command in the BGP instance configuration mode to cancel the above settings:

no maximum-paths {**ebgp** | **ibgp**}

Note:Before configuring this ECMP routing, you must first enable the ECMP function. For more information, see ECMP.

Viewing BGP Information

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

show ip route bgp [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the BGP routing information of the specified vRouter.

To view the routing information of the entire BGP routing table, in any mode, use the following command:

show ip bgp [*A.B.C.D* | *A.B.C.D/M*] [**vrouter** *vrouter-name*]

- *A.B.C.D* | *A.B.C.D/M* - Shows the BGP routing information of the specified network.
- *vrouter-name* - Shows the BGP routing information of the specified VRouter.

To view the path information of all the autonomous systems stored in the BGP database, in any mode, use the following command:

show ip bgp paths [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the paths information of autonomous systemof the specified VRouter.

To view the status parameters of all BGP connections, including the prefix, path, attribute, etc., in any mode, use the following command:

show ip bgp summary [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the BGP connecting status parameters of the specified VRouter.

To view the BGP peer status, in any mode, use the following command:

show ip bgp neighbor [*A.B.C.D*] [**vrouter** *vrouter-name*]

- *A.B.C.D* - Specifies the peer.
- *vrouter-name* - Shows the BGP peer status of the specified VRouter.

To view the BGP community list, use the following commands in any mode:

show ip community [*community-list-name*]

- *community-list-name* – Shows the information of the specified community list. Without this parameter specified, the information of all community lists will be displayed.

show ip as-path-access-list [*access-list-number*]

- *access-list-number* – Shows the information of the specified AS-path access list. Without this parameter specified, the information of all AS-path access lists will be displayed.

ECMP

Equal Cost Multi-Path Routing (ECMP) is a routing strategy where the next-hop packet forwarding to a single destination can occur over multiple best paths which tie for top place in routing metric calculations.

Configuring ECMP

By default the ECMP function is enabled, and allows up to 40 equal-cost routes for the purpose of load balancing. To enable or disable ECMP, in the VRouter configuration mode, use the following command:

ecmp enable *ecmp-route-num*

- *ecmp-route-num* - Specifies the maximum number of ECMP routes permitted in the system. The value range is 1 to 1000. The value of 1 indicates ECMP is disabled.

Configuring ECMP Route Selection

To configure the method for selecting an ECMP route, in the global configuration mode, use the following command:

```
ecmp-route-select {by-5-tuple | by-src | by-src-and-dst}
```

- **by-5-tuple** - Selects a route based on network quintuple (source IP address, destination IP address, source port, destination port and service type).
- **by-src** - Selects a route based on the source IP address.
- **by-src-and-dst** - Selects a route based on the source IP address and destination IP address. This is the default method.

Static Multicast Routing

Multicast refers to the communication method of transmitting data from one source to multiple destination nodes. The source that sends data is known as the multicast source, and the nodes that receive data form a multicast group. The destination address to which the multicast source sends data is known as a multicast address. Its range is 224.0.0.0 to 239.255.255.255 (Class D addresses).

Any host in the Internet can be used as a multicast source. Once the multicast source sends one copy of data to the multicast address, all the nodes in the group will receive the data. Information transmission by multicast can effectively save the network bandwidth. Increasing the number of users accessing the network will not lead to a heavier burden on the host that is sending data, thus reducing network workload.

To transmit data from the multicast source to the members in the multicast group, you need to manually configure the following options for the multicast routing rule:

- Multicast source and multicast address: the source IP and destination IP of the multicast.
- Ingress and egress interface: the data that match the corresponding multicast source and multicast address flows in from the ingress interface specified in the multicast routing rule, and flows out from the specified egress interface.

Enabling/Disabling a Multicast Route

By default the multicast route is disabled. To enable or disable the multicast route, in the VRouter configuration mode, use the following commands:

- Enable: **ip multicast-routing**
- Disable: **no ip multicast-routing**

Configuring a Static Multicast Route

To create a static multicast route, in the VRouter configuration mode, use the following command:

ip mroute *A.B.C.D A.B.C.D* [**iif** *interface-name*] [**eif** *interface-name*]

- *A.B.C.D A.B.C.D* - Specifies the multicast source and multicast address. The first *A.B.C.D* is the IP address of the multicast source, and the second *A.B.C.D* is the multicast address. The value range is 224.0.0.0 to 239.255.255.255.
- **iif** *interface-name* - Specifies an ingress interface. You can specify up to two ingress interfaces.
- **eif** *interface-name* - Specifies an egress interface. You can specify up to four egress interfaces.

To delete the specified static multicast route, in the VRouter configuration mode, use the following command:

no ip mroute *A.B.C.D A.B.C.D* [**iif** *interface-name*] [**eif** *interface-name*]

Specifying an Ingress/Egress Interface

You can configure an ingress or egress interface for the existing static multicast route. Each multicast route can have up to two ingress interfaces, and up to 32 egress interfaces. The options of ingress and egress interface must be configured in the static multicast route configuration mode. To enter the static multicast route configuration mode, in the VRouter configuration mode, use the following command:

ip mroute *A.B.C.D A.B.C.D*

- *A.B.C.D A.B.C.D* - Specifies the multicast source and multicast address. The first *A.B.C.D* is the IP address of the multicast source, and the second *A.B.C.D* is the multicast address.

To specify an ingress and egress interface for the existing static multicast routing entry, in the static multicast route configuration mode, use the following command:

- Specify an ingress interface: **iif** *interface-name*
- Specify an egress interface: **eif** *interface-name*

Repeat the above command to configure multiple ingress or egress interfaces.

Viewing Multicast Route Information

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

show ip mroute [*A.B.C.D A.B.C.D* | **static** | **summary**] [**vrouter** *vr-name*]

- **show ip mroute** - Shows all the multicast route information.

- *A.B.C.D A.B.C.D* - Shows the multicast route information of the specified multicast source and multicast address. The first *A.B.C.D* is the IP address of the multicast source, and the second *A.B.C.D* is the multicast address.
- **static** - Shows the static multicast route information.
- **summary** - Shows the summary of multicast route.
- **vrouter** *vr-name* - Shows the multicast route information of the specified VRouter.

Viewing Multicast FIB Information

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

show mfib [*A.B.C.D A.B.C.D* | **summary**] [**vrouter** *vr-name*]

- **show mfib**- Shows all the multicast FIB information.
- *A.B.C.D A.B.C.D* - Shows the multicast FIB information of the specified multicast source and multicast address. The first *A.B.C.D* is the IP address of the multicast source, and the second *A.B.C.D* is the multicast address.
- **summary** - Shows the summary of multicast FIB.
- **vrouter** *vr-name* - Shows the multicast FIB information of the specified VRouter.

IGMP

Internet Group Message Protocol (IGMP) is used to establish and maintain multicast group membership between hosts and routers. A host reports its membership of a group to its local router over IGMP, and a router listens to reports from hosts and periodically sends out queries to check if any group member is alive. If no report is received from the member, the router side will determine there is no member in the multicast group.

The latest version of FSOS supports IGMPv1 (defined in RFC1112) , IGMPv2 (defined in RFC2236) and IGMPv3 (defined in RFC3376). And it also supports IGMP Proxy (operating on the Application Layer) and IGMP Snooping (operating on the Link Layer).

IGMP Proxy

IGMP Proxy is designed to create multicast routing tables and forward multicast data by intercepting the IGMP packets between the hosts and routers. IGMP Proxy acts differently on the two interfaces of the FS device:

On the upstream interface that connects to the multicast router, it acts as a host, responsible for responding to the queries from the router. When a new member is added to the multicast group, or when the last member exits, the proxy will proactively send a packet to report the member status on the upstream interface.

On the downstream interface that connects to the host, it acts as a router, responsible for the registration, query and deletion of group members.

To configure a IGMP proxy, take the following steps:

1. Enable multicast. For detailed operation, see Enabling/Disabling a Multicast Route.
2. Enable an IGMP proxy.
3. Configure the upstream interface to the host mode.
4. Configure the downstream interface to the router mode.
5. Configure a policy rule.

Enabling an IGMP Proxy

To enable or disable the IGMP proxy function, in the VRouter configuration mode, use the following commands:

- Enable: **ip igmp-proxy enable**
- Disable: **no ip igmp-proxy enable**

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

ip vrouter *vrouter-name*

- *vrouter-name* - Specifies a Vrouter. If the name exists, the system will directly enter the Vrouter configuration mode.

Configuring an IGMP Proxy Mode for an Interface

To configuring an IGMP proxy mode (either router mode or host mode) for an interface, in the interface configuration mode, use the following command:

ip igmp-proxy {**router-mode** | **host-mode**} [*A.B.C.D*] [**v2** | **v3**]

- **router-mode** - Configures the IGMP proxy mode of the downstream interface to the router mode.
- **host-mode** - Configures the IGMP proxy mode of the upstream interface to the host mode.

- [*A.B.C.D*] - Specifies the multicast address. The IGMP proxy mode will only be applied to this address.
- **v2** – Specifies the protocol version of the IGMP message is IGMPv2. By default, the IGMPv2 protocol is used.
- **v3** – Specifies the protocol version of the IGMP message is IGMPv3.

To cancel the IGMP proxy mode for the specified interface, in the interface configuration mode, use the following command:

no ip igmp-proxy {**router-mode** | **host-mode**} [*A.B.C.D*]

Viewing IGMP Proxy Information

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

show ip igmp-proxy [*A.B.C.D*] [**vrouter** *vrouter-name*]

- **show ip igmp-proxy** - Shows all the IGMP Proxy information in the system.
- [*A.B.C.D*] - Shows the IGMP Proxy information of the specified multicast address.
- [**vrouter** *vrouter-name*] - Shows the IGMP Proxy information of the specified VRouter.

IGMP Snooping

IGMP Snooping is designed to create multicast routing entries for a specific multicast address on a Layer 2 device by listening to the IGMP packets between hosts and routers. With IGMP Snooping enabled, the FS device can forward multicast data based on the created multicast routing entries, efficiently reducing the cost of multicast communication. If IGMP Snooping is disabled, FS device only advertises multicast data.

To configure IGMP Snooping, take the following steps:

1. Enable multicast. For detailed operation, see Enabling/Disabling a Multicast Route.
2. Enable IGMP Snooping.
3. Configure IGMP Snooping.
4. Configure a policy rule.

Enabling IGMP Snooping

To enable or disable the IGMP Snooping function, in the VSwitch configuration mode, use the following commands

- Enable: **ip igmp-snooping enable**
- Disable: **no ip igmp-snooping enable**

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

vswitch vswitch *Number*

- *Number* - Specifies the VSwitch' s identifier. The value range may vary from different platforms. For example, the command vswitch vswitch2 will create a VSwitch named VSwitch2, as well as an interface named VSwitchif2. Besides the system will enter the configuration mode of VSwitch2. If the specified VSwitch exists, the system will directly enter the VSwitch configuration mode.

Configuring IGMP Snooping

To configuring IGMP Snooping, in the interface configuration mode, use the following command:

ip igmp-snooping {**router-mode** [*A.B.C.D*] | **host-mode** [*A.B.C.D*] | **disable** | **auto**}

- **router-mode** - Configures the IGMP Snooping mode of the downstream interface to the router mode.
- **host-mode** - Configures the IGMP Snooping mode of the upstream interface to the host mode.
- [*A.B.C.D*] - Specifies the multicast address.
- **disable** - Disables IGMP Snooping for the interface.
- **auto** - The system will determine the interface mode automatically based on the IGMP packet.

To cancel the IGMP Snooping mode, in the interface configuration mode, use the following command:

no ip igmp-snooping {**router-mode** *A.B.C.D* | **host-mode** *A.B.C.D*}

Dropping Unknown Multicast

By default dropping unknown multicast is disabled. With this function enabled, the device will drop the packets that are destined to unknown multicast groups, thus saving the bandwidth. To enable the function, in the VSwitch configuration mode, use the following command:

unknown-multicast drop

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

```
no unknown-multicast drop
```

Viewing IGMP Snooping Information

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

show ip igmp-snooping [*A.B.C.D*] [**vswitch** *name*]

- **show ip igmp-snooping** - Shows all the IGMP Snooping information.
- [*A.B.C.D*] - Shows the IGMP Snooping information of the specified multicast address.
- [**vswitch** *name*] - Shows the IGMP Snooping information of the specified VSwitch.

BFD

BFD (Bidirectional Forwarding Detection) is a unified detection mechanism for the entire network, which is used to fast detect and monitor the forwarding and connection status of the link and the IP route. To enhance the network performance, the protocol neighbor must have the ability to detect the communication failures quickly. Thus, the backup communication can be established to restore the communication in time.

BFD creates sessions between two routers for monitoring the bidirectional forwarding path between these two routers, which provides services for the upper level protocol, for example, routing protocol. BFD does not have the discovering mechanism and upper level protocol will notify BFD to create sessions with specifies objects. If no BFD packets are received from the peer during the detection period after creating sessions, BFD will notify the upper-level service and the upper-level service will execute the corresponding operations.

In the current FSOS, BFD can integrate with static route, OSPF route, and BGP route. Thus, FSOS can realize the detection of the forwarding and connection status on the link that runs static route, OSPF route, and BGP route.

BFD Work Mode

Establishing a BFD session has two modes: active mode and passive mode. FSOS now supports the active mode.

- Active mode: No matter whether BFD control packets are received or not from the peer before creating sessions, the BFD control packets will be sent actively.
- Passive mode: BFD control packets will not be sent before creating sessions until the control packets, which are sent from the peer, are received. During the process of initiating the sessions, one of the two sides must run in the active mode.

BFD has two detection modes that will work after creating sessions: asynchronous mode and inquiry mode. Two sides in the communication must be in the same mode.

- Asynchronous mode: Devices that works in the asynchronous mode send the BFD control packets periodically. If the peer does not receive the BFD control packets during the detection period, the session is considered as the down status.
- Inquiry mode: Assume that there is an independent method to confirm the connection status with the peer system. In this way, after creating the BFD session, the device will stop sending the BFD control packets periodically except for the requirements of verifying the connection apparently.

BFD Echo

The BFD Echo function makes the local device send the BFD Echo packets periodically and the peer device only returns the packets to the local device via the forwarding channel. You can use the Echo function to discover failures fast.

The Echo function can integrate with the detection methods. If you enable the Echo function in the asynchronous mode, the device will reduce the sending of the control packets. If you enable the Echo function in the inquiry mode, you can cancel the sending of BFD packets after the BFD session is established.

Note:To use the Echo function, ensure the peer device can forward the Echo packets after you enable the Echo function in the local device.

Configuring BFD

Configuring BFD involved the following sections:

- Configuring the BFD detection methods
- Configuring the BFD session parameters
- Enabling/Disabling the Echo function
- Specifying the interval of receiving Echo packets
- Configuring the source IP address of the Echo packets

Configuring the BFD Detection Methods

There are two detection methods after creating the BFD session: asynchronous mode and the inquiry mode. Two sides in the communication must be in the same mode. By default, the detection mode of the BFD session is the asynchronous mode. You can change the mode according to your requirements. To use the inquiry mode, use the following command:

```
bfd demand enable
```

To change back to the asynchronous mode, use the following command:

```
no bfd demand enable
```

Configuring the BFD Session Parameters

After creating the BFD sessions, you can modify the minimum interval of receiving/sending BFD session packets and edit the multiple for calculating the timeout value. To configure the BFD session parameters, use the following command in the interface configuration mode:

bfd min-tx *min-tx-value* **min-rx** *min-rx-value* **detect-multiplier** *value*

- *min-tx-value* – Specifies the minimum interval of sending BFD packets. The unit is millisecond. The default value is 100 and it is in the range of 100 to 1000.
- *min-rx-value* – Specifies the minimum interval of receiving BFD packets. The unit is millisecond. The default value is 100 and the range is 100 to 1000.
- *value* – Specifies the multiple for calculating the timeout value. The detailed information of

To restore the value to the default one, use the following command in the interface configuration mode: **no bfd min-tx min-rx detect-multiplier**.

Note:

- In the asynchronous mode, the system compares the value of the *min-tx-value* parameter of the local device with the value of the *min-rx-value* of the peer device, uses the bigger one times the value of the *value parameter* configured for the peer device, and uses the result as the timeout value.
- In the inquire mode with the Echo function enabled, the system compares the value of the *min-tx-value* parameter of the local device with the interval of receiving Echo packets configured for the peer device, uses the bigger one times the value of the *value* parameter configured for the local device, and uses the result as the timeout value.
- In the asynchronous mode with the Echo function enabled, the system compares the value of the *min-tx-value* parameter of the local device with the interval of receiving Echo packets configured for the peer device, uses the bigger one times the value of the *value* parameter configured for the peer device, and uses the result as the timeout value.

For more information about configuring the interval of receiving Echo packets, see Specifying the Interval of Receiving Echo Packets.

Enabling/Disabling the Echo Function

By default, the Echo function is disabled. To enable this function, use the following command in the interface configuration mode:

```
bfd echo enable
```

Use the following command in the interface configuration mode to disable the function:

no bfd echo enable

Specifying the Interval of Receiving Echo Packets

To specify the interval of receiving Echo packets, use the following command in the interface configuration mode:

bfd min-echo-rx *value*

- *value* – Specifies the interval of receiving BFD Echo packets. The unit is millisecond. The default value is 0 and the range is 100 to 1000.

To restore the value to the default one, use the following command in the interface configuration mode: no bfd min-echo-rx.

Configuring the Source IP Address of the Echo Packets

A large number of ICMP redirection packets sent from the peer leads to the network congestion. To avoid the network congestion, you can configure the source IP address of the Echo packets. To configure the source IP address, use the following command in the global configuration mode:

bfd echo-source-ip *echo-src-address*

- *echo-src-address* – Specifies the source IP addresses of the BFD Echo packets.

To delete the configured source IP address, use the following command in the global configuration mode: no bfd echo-source-ip.

Note:

- You can specify a random source IP address of the Echo packets. FS recommends you use an IP address which does not belong to the network segments where interfaces of the device locate.
- The destination IP address of the Echo packets that sent from the local device is the interface IP address of the local device.

Integrating BFD with Routing Protocols

BFD can integrate with following routing protocols:

- Integrating BFD with the static route
- Integrating BFD with the OSPF route
- Integrating BFD with the BGP route

Integrating BFD with the Static Route

The static route does not have the neighbor discovering mechanism. Thus, when BFD integrates with the static route, a failure detected by the BFD session indicates that the next hop is not reachable and this route will not be added to the routing table.

To integrate BFD with the static route and enable the BFD detection function for the specified next hop, use the following command in the VRouter configuration mode:

ip route {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} *interface-name A.B.C.D* **bfd**

- *A.B.C.D/M* | *A.B.C.D A.B.C.D* – Specifies the network address of the static route. FS devices support two formats: *A.B.C.D/M* or *A.B.C.D A.B.C.D*, for example, 1.1.1.0/24 or 1.1.1.0 255.255.255.0.
- *interface-name A.B.C.D* – Specifies the IP address of the next-hop interface.
- **bfd** – Enables the BFD detection function for the specified next hop.

To cancel the integration, use the following command in the VRouter configuration mode:

no ip route {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} *interface-name A.B.C.D* **bfd**

Integrating BFD with the OSPF Route

By integrating BFD with the OSPF route, the system realizes the quick link detection which has higher performance than the Hello detection mechanism of the OSPF protocol. With the integration, OSPF protocol improves its convergence performance.

To integrate BFD with the OSPF rout and enable the BFD detection function on the specified interfaces that corresponds to the OSPF route, use the following command in the interface configuration mode:

ip ospf bfd

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

no ip ospf bfd

Integrating BFD with the BGP Route

To integrate BFD with the BGP route and enable the BFD detection function for the specified BGP neighbor, use the following command in the BGP instance configuration mode:

neighbor *A.B.C.D* **fall-over bfd**

- *A.B.C.D* – Specifies the IP address of the BGP peer.

To cancel the integration, use the following command in the BGP instance configuration mode:

no neighbor *A.B.C.D* **fall-over bfd**

Viewing BFD Session Information

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

show bfd session [**interface** *interface-name* | **neighbor***A.B.C.D* | **detail**]

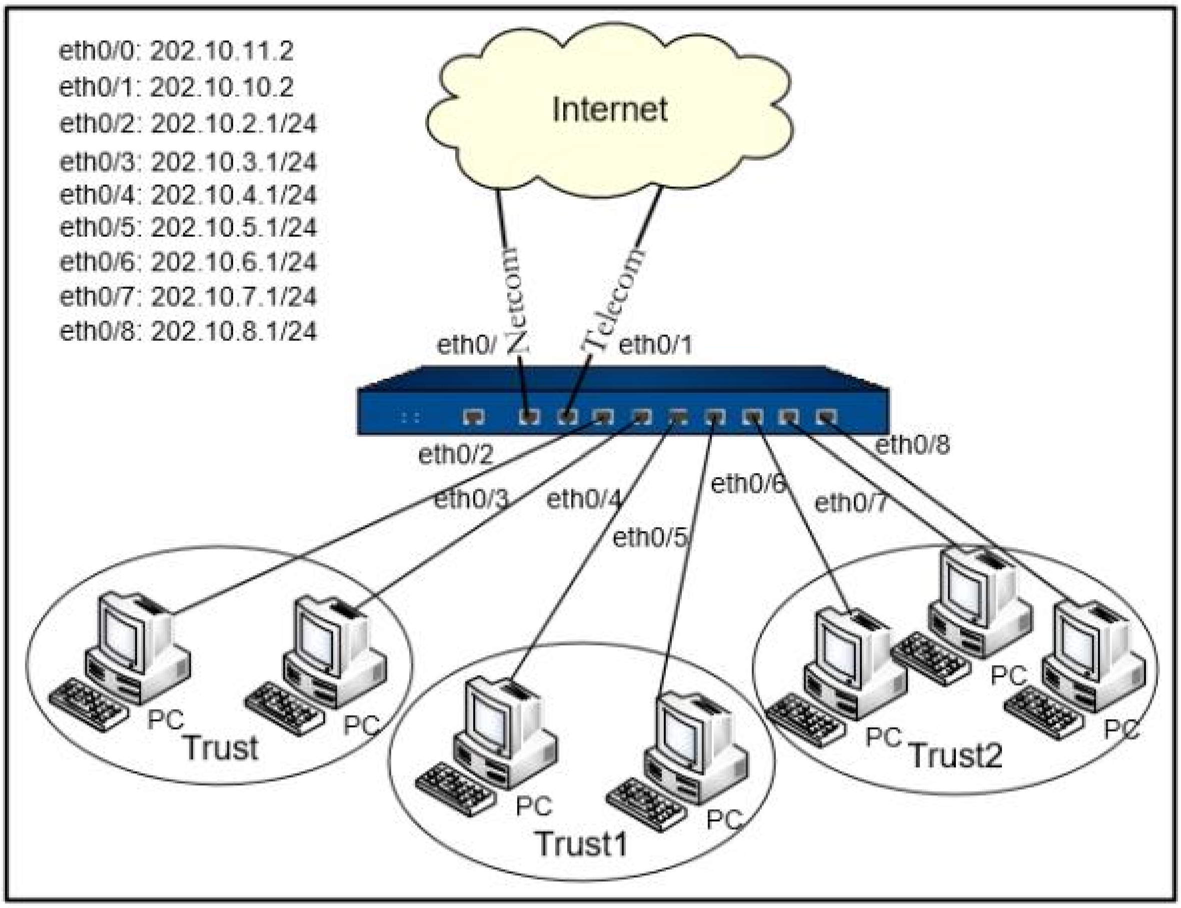
- **interface** *interface-name* - Shows the information of the BFD sessions of the specified interface.
- *A.B.C.D* – Specifies ID of the neighbor router.
- **detail** – Shows the detailed information of the BFD sessions of all routers.

Examples of Configuring Routes

This section describes several route-related configuration examples, including an enabling/disabling static route query configuration example, multi-VR configuration examples, a static multicast route configuration example, an IGMP Proxy configuration example and an inbound LLB configuration example.

Example of Configuring Static Route Query

The interface ethernet0/0 and ethernet0/1 of the device connect to ISP Netcom and Telecom respectively; the traffic from Trust and Trust1 in the Intranet goes to Netcom, and other traffic goes to Telecom. The network topology is shown below:



As shown above, etherent0/0 and ethernet0/1 belong to the untrust zone, and their IPs are 202.10.11.2 and 202.10.10.2 respectively; etherent0/2 and ethernet0/3 belong to the Trust zone, and their IPs are 202.10.2.1/24 and 202.10.3.1/24 respectively; etherent0/4 and ethernet0/5 belong to the Trust1 zone, and their IPs are 202.10.4.1/24 and 202.10.5.1/24 respectively; etherent0/6, ethernet0/7 and etherent0/8 belong to the Trust2 zone, and their IPs 202.10.6.1/24, 202.10.7.1/24 and 202.10.8.1/24 respectively.

Configuration Steps

Configurations of the security zones and interfaces are omitted. Only the configuration example of routes is as follows:

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

hostname(config-vrouter)# ip route 0.0.0.0/0 202.10.10.2(the traffic from this segment goes to
Telecom by default)

hostname(config-vrouter)# ip route source 202.10.2.1/24 202.10.11.2(the traffic from this
segment goes to Netcom by default)

hostname(config-vrouter)# ip route source 202.10.3.1/24 202.10.11.2(the traffic from this
segment goes to Netcom by default)
hostname(config-vrouter)# ip route source 202.10.4.1/24 202.10.11.2(the traffic from this
segment goes to Netcom by default)
hostname(config-vrouter)# ip route source 202.10.5.1/24 202.10.11.2(the traffic from this
segment goes to Netcom by default)
```

In the above source routing configuration, the traffic from the Trust and Trust1 zone will go to Netcom, while the traffic from other zones will go to Telecom. If the Netcom line fails for any reason, users in the Trust and Trust1 zones will not be able to access the Internet. In such a case only when all the above 4 source routes are deleted will the traffic be completely migrated to the Telecom line. If there are too many relevant source routes, the workload of deleting routes and then adding routes after troubleshooting will be very heavy; besides the trivial work also possibly leads to errors. The FS's solution is: when any line fails, disable the source route query, and then users in the Trust and Trust1 zones will use the default route and be able to access the Internet through the Telecom line. Use the following command:

```
hostname(config)# route disable sbr
```

After troubleshooting, to re-enable the source route query function, use the following command:

```
hostname(config)# hostname(config)# route enable sbr
```

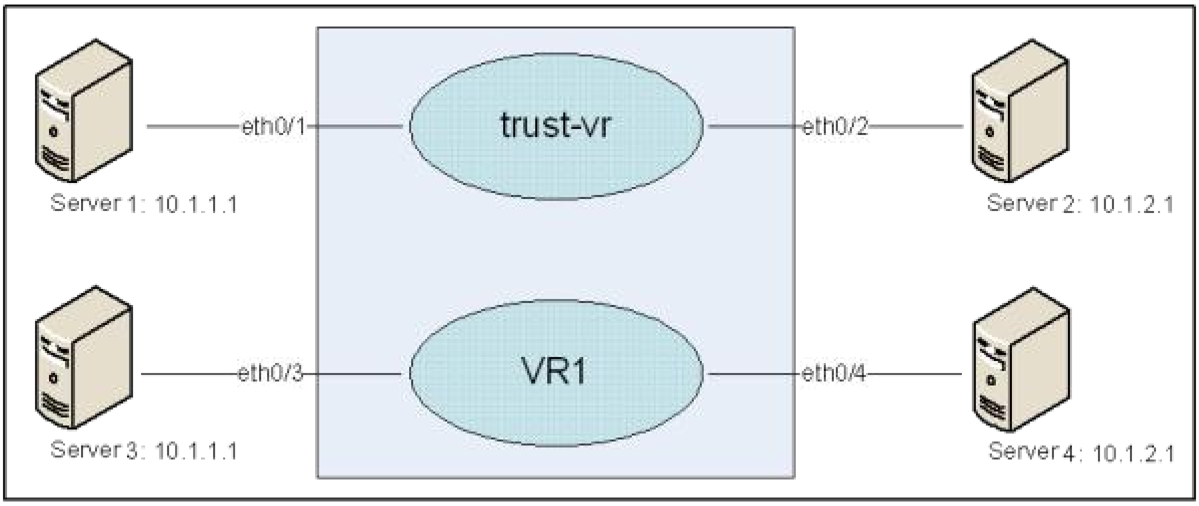
Example of Configuring Multi-VR

This section describes two multi-VR configuration examples, including:

- Independent multi-VR forwarding
- Inter-VR forwarding

Independent Multi-VR Forwarding

There are overlapped IP addresses in Trust-vr and VR1, but the data transmission of the two VRs should be independent, and should not affect each other. The network topology is shown below:



There are two VRs in the system: trust-vr and VR1. ethernet0/1 belongs to zone1, ethernet0/2 belongs to zone2, both zone1 and zone2 belong to trust-vr; ethernet0/3 belongs to zone3, ethernet0/4 belongs to zone4, belong zone3 and zone4 belong to VR1. The IP address of ethernet0/1 and ethernet0/3 is overlapped; the IP address of ethernet0/2 and ethernet0/4 is overlapped as well.

Configuration Steps

Step 1: Enable multi-VR on the device:

```
hostname# exec vrouter enable
Warning: please reboot the device to make the change validation!
hostname# reboot
System reboot, are you sure? y/[n]: y
```

Step 2: After rebooting, create VR1:

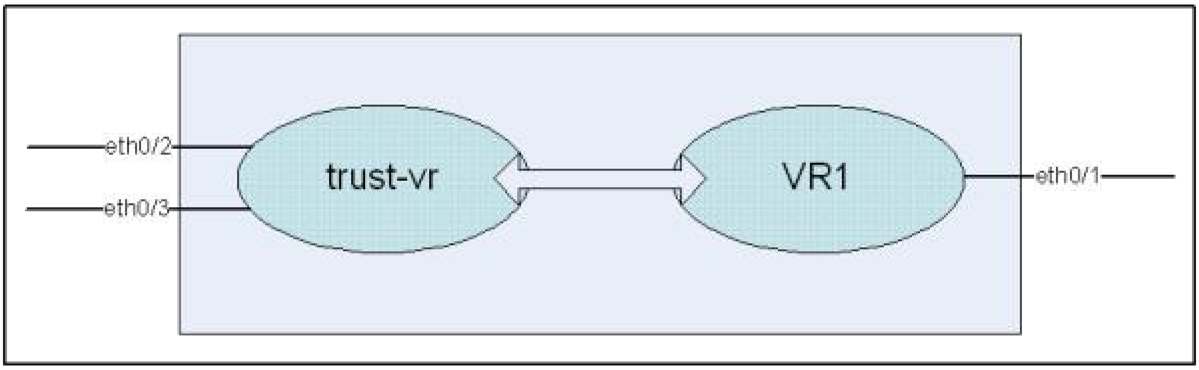
```
hostname(config)# ip vrouter VR1
```

Step 3: Configure interfaces and security zones (by default zone1 and zone2 belong to trust-vr):

```
hostname(config)# zone zone1
hostname(config-zone-zone1)# exit
hostname(config)# zone zone2
hostname(config-zone-zone2)# exit
hostname(config)# zone zone3
hostname(config-zone-zone3)# vrouter VR1
hostname(config-zone-zone3)# exit
hostname(config)# zone zone4
hostname(config-zone-zone4)# vrouter VR1
hostname(config-zone-zone4)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone zone1
hostname(config-if-eth0/1)# ip address 10.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone zone2
hostname(config-if-eth0/2)# ip address 10.1.2.1/24
hostname(config-if-eth0/2)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone zone3
hostname(config-if-eth0/3)# ip address 10.1.1.1/24
hostname(config-if-eth0/3)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# zone zone3
hostname(config-if-eth0/4)# ip address 10.1.2.1/24
hostname(config-if-eth0/4)# exit
hostname(config)#
```

Inter-VR Forwarding

There are two VRs in the system: trust-vr and VR1. The goal is to allow trust-vr forwarding data through VR1. The network topology is shown below:



There are two VRs in the system: trust-vr and VR1. ethernet0/0 belongs to zone1, and zone1 belongs to trust-vr; ethernet0/2 and ethernet0/3 belong to zone2, and zone2 belongs to trust-vr. The following configuration example allows trust-vr to forward data through VR1.

Configuration Steps

Step 1: Enable multi-VR on the device:

```
hostname# exec vrouter enable
Warning: please reboot the device to make the change validation!
hostname# reboot
System reboot, are you sure? y/[n]: y
```

Step 2: After rebooting, create VR1:

```
hostname(config)# ip vrouter VR1
```

Step 3: Configure interfaces and security zones (by default zone1 and zone2 belong to trust-vr):

```
hostname(config)# zone zone1
hostname(config-zone-zone1)# vrouter VR1
hostname(config-zone-zone1)# exit
hostname(config)# zone zone2
hostname(config-zone-zone2)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone zone1
hostname(config-if-eth0/1)# ip address 1.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone zone2
hostname(config-if-eth0/2)# ip address 10.1.1.1/24
hostname(config-if-eth0/2)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone zone2
hostname(config-if-eth0/3)# ip address 10.1.2.1/24
hostname(config-if-eth0/3)# exit
hostname(config)#
```

Step 4: Configure an inter-VR forwarding route:

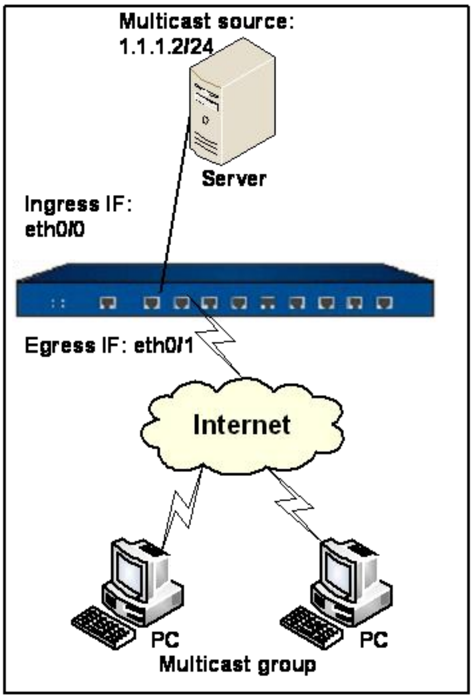
```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 0.0.0.0/0 vrouter VR1
hostname(config-vrouter)# exit
hostname(config)# ip vrouter VR1
hostname(config-vrouter)# ip route 10.1.1.0/24 vrouter trust-vr
hostname(config-vrouter)# ip route 10.1.2.0/24 vrouter trust-vr
hostname(config-vrouter)# exit
hostname(config)#
```

Example of Configuring Static Multicast Route

This section describes a static multicast route configuration example.

Requirement

The multicast source sends data to multicast group. The multicast address is 224.91.91.2. Interface ethernet0/0, the ingress interface of the multicast data, belongs to the trust zone; ethernet0/1, the egress interface of the multicast data, belongs to the untrust zone. The goal is to configure a static multicast route so that the multicast data can be properly transmitted to the client PC that belongs to the multicast group. The network topology is shown below:



Configuration Steps

Step 1: Configure interfaces and security zones:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 1.1.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 2.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 2: Enable and configure a multicast route:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip multicast-routing
hostname(config-vrouter)# ip mroute 1.1.1.2 224.91.91.2 iif ethernet0/0 eif ethernet0/1
hostname(config-vrouter)# exit
hostname(config)#
```

Step 3: Configure a policy rule:

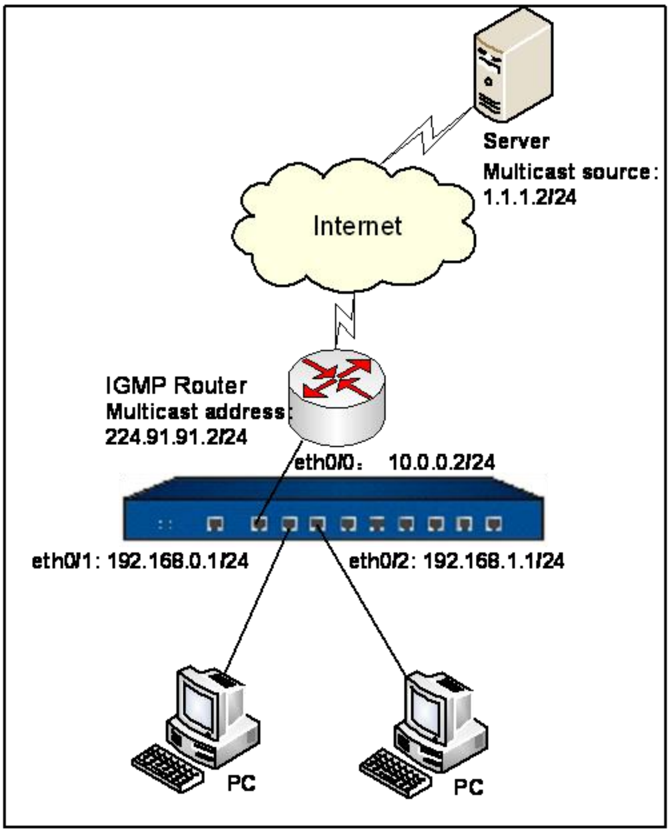
```
hostname(config)# address src
hostname(config-addr)# ip 1.1.1.2/32
hostname(config-addr)# exit
hostname(config)# address dst
hostname(config-addr)# ip 224.91.91.2/32
hostname(config-addr)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr src
hostname(config-policy-rule)# dst-addr dst
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Example of Configuring IGMP Proxy

This section describes an IGMP Proxy configuration example.

Requirement

The multicast source sends data to the multicast group. The multicast address is 224.91.91.2. Interface ethernet0/0 is the upstream interface; ethernet0/1 and ethernet0/2 are the downstream interfaces. Configure an IGMP Proxy so that the multicast data can be properly forwarded to the client PC that belongs to the multicast group. The network topology is shown below:



Configuration Steps

Step 1： Configure interfaces and security zones:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 10.0.0.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.0.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone trust
hostname(config-if-eth0/2)# ip address 192.168.1.1/24
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Step 2: Enable a multicast route:

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

Step 3: Enable and configure an IGMP Proxy:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip igmp-proxy enable
hostname(config-vrouter)# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# ip igmp-proxy host-mode
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# ip igmp-proxy router-mode
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# ip igmp-proxy router-mode
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Step 4: Configure a policy rule:

```
hostname(config)# address src
hostname(config-addr)# ip 1.1.1.2/32
hostname(config-addr)# exit
hostname(config)# address dst
hostname(config-addr)# ip 224.91.91.2/32
hostname(config-addr)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr src
hostname(config-policy-rule)# dst-addr dst
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Example of Configuring IGMP Snooping

This section describes an IGMP Snooping configuration example.

Requirement

The multicast source sends data to the multicast group. The multicast address is 224.91.91.2. The device is working in the transparent mode. Interface ethernet0/0 is the upstream interface; ethernet0/1 and ethernet0/2 are the downstream interfaces. The goal is to configure IGMP snooping so that the multicast data can be properly forwarded to the client PC that belongs to the multicast group.

Configuration Steps

Step 1: Configure interfaces and security zones:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone l2-untrust
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone l2-trust
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone l2-trust
hostname(config-if-eth0/2)# exit
hostname(config)# interface vswitchif1
hostname(config-if-vsw1)# ip address 192.30.1.100 255.255.255.0
hostname(config-if-vsw1)# exit
hostname(config)#
```

Step 2: Enable a multicast route:

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

Step 3: Enable and configure IGMP Snooping:

```
hostname(config)# vswitch vswitch1
hostname(config-vswitch)# ip igmp-snooping enable
hostname(config-vswitch)# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# ip igmp-snooping host-mode
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# ip igmp-snooping router-mode
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# ip igmp-snooping router-mode
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Step 4: Configure a policy rule:

```
hostname(config)# address src
hostname(config-addr)# ip 1.1.1.2/32
hostname(config-addr)# exit

hostname(config)# address dst

hostname(config-addr)# ip 224.91.91.2/32

hostname(config-addr)# exit

hostname(config)# policy-global

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone l2-untrust

hostname(config-policy-rule)# dst-zone l2-trust

hostname(config-policy-rule)# src-addr src

hostname(config-policy-rule)# dst-addr dst

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config-policy)# exit

hostname(config)#
```

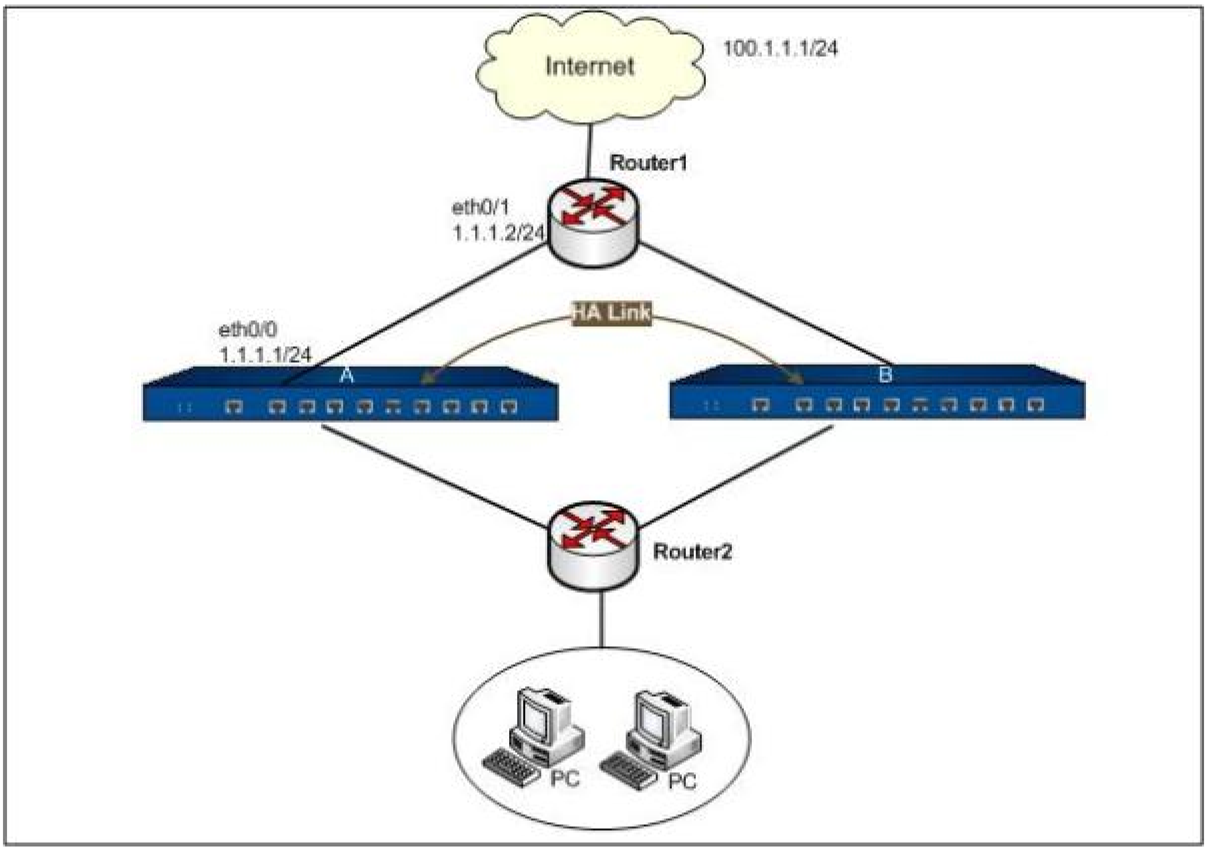
Example of Configuring BFD

This section lists three examples of configuring BFD as follows:

- Integrating BFD with the static route
- Integrating BFD with the OSPF route
- Integrating BFD with the BGP route

Requirement

The redundant link consists of two FS devices and two routers. The BFD detection function is enabled between the routers and the FS devices. The reachable network segment of Router1 is 100.1.1.1/24. The following examples individually integrate BFD with the static route, the OSPF route, and the BGP route between the Router1 and the device A. The network topology is shown in the figure below:



Configuration Steps

Integrating BFD with the Static Route

Step 1: Configure interfaces of the device A:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 2: Configure the BFD session parameters on the interface of the device A. The default detection method is asynchronous:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# bfd min-tx 100 min-rx 100 detect-multiplier 3
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 3: Configure the device A to integrate BFD with the static route Router1:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 100.1.1.1/24 ethernet0/1 1.1.1.2 bfd
hostname(config-vrouter)# exit
hostname(config)#
```

Step 4: Configure the interface of Router1 and the BFD functions. The IP address of the interface is 1.1.1.2/24.

Integrating BFD with the OSPF Route

Step 1: Configure interfaces of the device A:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 2: Configure the BFD session parameters on the interface of the device A, specify the detection method as the inquiry method, enable the Echo function, and integrate BFD with the OSPF route:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# bfd demand enable
hostname(config-if-eth0/0)# bfd min-echo-rx 100
hostname(config-if-eth0/0)# bfd echo enable
hostname(config-if-eth0/0)# ip ospf bfd
hostname(config)#
```

Step 3: Configure the OSPF route on the device A:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# route id 1.1.1.1
hostname(config-router)# network 1.1.1.1/24 area 0
hostname(config-router)# exit
hostname(config)#
```

Step 4: Configure the interface of Route1, BFD functions, and OSPF route. The IP address of the interface is 1.1.1.2/24. Use the inquiry method, enable the Echo function, and ensure the Echo packets can be forwarded.

Integrating BFD with the BGP Route

Step 1: Configure interfaces of the device A:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 2: Configure the BFD session parameters on the interface of the device A, specify the detection method as the inquiry method and enable the Echo function.

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# bfd demand enable
hostname(config-if-eth0/0)# bfd min-echo-rx 100
hostname(config-if-eth0/0)# bfd echo enable
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 3: Configure the BGP protocol on the device A and integrate BFD with BGP:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router bgp 100
hostname(config-router)# route id 1.1.1.1
hostname(config-router)# neighbor 1.1.1.2 fall-over bfd
hostname(config-router)# network 1.1.1.1/24
hostname(config-router)# exit
hostname(config)#
```

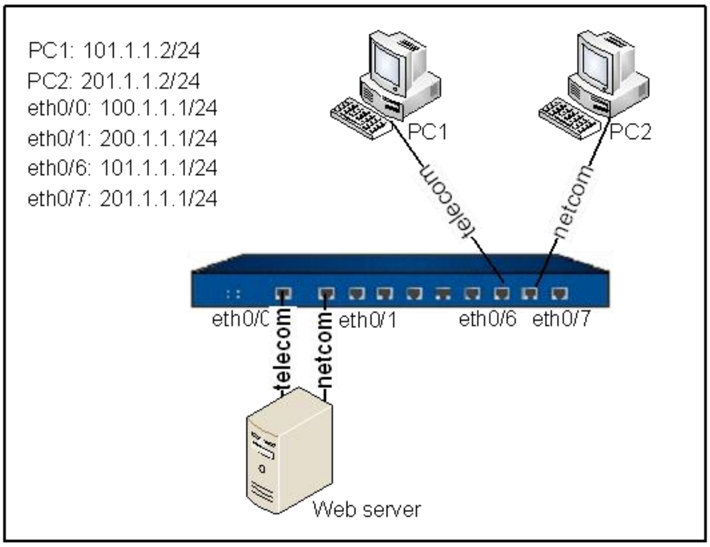
Step 4: Configure the interface of Route1, BFD functions, and BGP route. The IP address of the interface is 1.1.1.2/24. Use the inquiry method, enable the Echo function, and ensure the Echo packets can be forwarded.

Example of Configuring LLB

This section describes an inbound LLB configuration example.

Requirement

Ethernet0/6 and ethernet0/7 are connected to telecom and netcom links respectively. With inbound LLB enabled, the device will return the IP address defined in the ISP static address named telecom after receiving a DNS request from netcom users, and will return the IP address defined in the ISP static address named telecom after receiving a DNS request from telecom users. The network topology is shown below:



Configuration Steps

Configurations of interfaces are omitted. Only the configurations of ISP information and inbound LLB are provided.

Step 1: Configure ISP information:

```
hostname(config)# isp-network telecom

hostname(config-isp)# 101.1.1.0/24

hostname(config-isp)# exit

hostname(config)# isp-network netcom

hostname(config-isp)# 201.1.1.0/24

hostname(config-isp)# exit
```

Step 2: Enable SmartDNS and configure SmartDNS rules:

```
hostname(config)# llb inbound smartdns enable

hostname(config)# llb inbound smartdns test

hostname(config-llb-smartdns)# domain www.test.com

hostname(config-llb-smartdns)# ip 100.1.1.2 isp telecom interface ethernet0/0 weight 10

hostname(config-llb-smartdns)# ip 200.1.1.2 isp netcom interface ethernet0/0 weight 10

hostname(config-llb-smartdns)# exit
```

Step 3: Confirm the above configurations have taken effect by command show:

```
hostname(config)# show isp-network all

ISP telecom status: Active

Binding to nexthop: 0

Subnet(IP/Netmask): 1

101.1.1.0/24

ISP netcom status: Active

Binding to nexthop: 0

Subnet(IP/Netmask): 1

201.1.1.0/24

hostname(config)# show llb inbound smart test

domain:domain name; IP: ip address; ISP: isp name; IF: interface;

PROXY: proximity address book status; E: enable; D:disable

TRACK: track object name; W: ip weight; S:ip status;A:active;
```

```
I: inactive

=============================================================
=

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

name: test

domain count: 1

rule count: 2

status: enable

domains: www.test.com;

ip addresses:

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

ID IP ISP IF PROX TRACK W S

1 100.1.1.2 telecom ethernet0/0 D 10 A

3 200.1.1.2 netcom ethernet0/1 D 10 A

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

When PC1 requests www.test.com, the device will return the IP address for telecom link (100.1.1.2); when PC2 requests www.test.com, the device will return the IP address for netcom link (200.1.1.2).

Chapter 4 System Management

This section contains the following contents:

Naming Rules

When you name an object, follow the conventions below:

- FS recommends you to not use the following special characters: comma (,), single quotation marks (‘ ‘), quotation marks (“”), tab, space, semicolons (;), backslash (\), slash (/), angle brackets (<>), and other special characters (&, #). It is recommend that you should use figures (0-9) and letters (a-z, A-Z) in the name.
- If an object name has space in it, you need to enclose the entire name in quotation marks when you use CLI, but this does not apply to WebUI operations.

Configuring a Host Name

A host name distinguishes one device from another. The default host name is the platform model.

To edit a host name, in the global configuration mode, use the following command:

hostname *host-name*

- *host-name* – Specifies the host name of the FS device. You can specify up to 63 characters. After executing the command, the command prompt will be changed to the specified host name.

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

For example, the following commands change the host name to FS:

```
hostname# configure
hostname(config)# hostname FS
FS(config)#
```

Configuring System Admin Users

Device administrators of different roles have different privileges. The system supports pre-defined administrator roles and customized administrator roles.

By default, the system supports the following administrators, which cannot be deleted or edited:

- **admin**: can write, execute and write the system. Administrator role can manage all functions of the device, view configurations and execute commands like import, export and save etc. under configuration mode.

- **admin-read-only**: can write and execute, view configurations, and execute export command under configuration mode.

- **operator**: can write, execute and write the system. Operator can modify settings others than administrator privileges, reboot the system, restore factory defaultand upgrade FSOS, view configurations, but operators cannot view log messages, and execute some commands.

- **auditor**: can manage log messages, including view, export and clear logs. The table lists admin user's permissions.

Operation	Permissions			
	Adminisrator	Administrator-read-only	Operator	Auditor
Configure (including save configuration)	√	χ	√	χ
Managing admin users	√	χ	χ	χ
Restore factory default	√	χ	χ	χ
Delete configuration file	√	χ	√	χ
Roll back configuration	√	χ	√	χ
Reboot	√	χ	χ	χ
View configuration information	√	√	√	χ
View log information	√	√	χ	√
Modify current admin password	√	√	√	√
Command import	√	χ	√(except upgrading FSOS)	χ
Command export	√	√	χ	√
Command clear	√	√	√	√
Command ping/traceroute	√	√	√	χ
Command debug	√	√	√	χ
Command exec	√	√	√	√
Command terminal width	√	√	√	√

- The system has a default administrator "admin". This default administrator can be edited, but not deleted.

- Except administrator, other roles cannot edit properties of a system admin user, but only its own password.

- Auditor can manage one or more log messages, but an auditor's log types are defined by users of administrator role.

The property settings of a system administrator are:

- Creating administrator roles
- Specifying administrator role's privileges
- Specifying administrator role's description
- Creating an admin user
- Assigning a role
- Configuring password
- Configuring accesses for admin users
- Configuring log types for auditors
- Specifying login limit
- Viewing Admin roles
- Viewing admin users
- VSYS admin users

Creating Administrator Roles

To create a new administrator role, use the following command in the global configuration mode:

admin role *role-name*

- *role-name* − Specifies the name of the administrator role. The length varies from 4 characters to 95 characters. After executing this command, the system will create the administrator role and enter the administrator role configuration mode. If the name already exists, it will enter the administrator role configuration mode directly.

To delete an administrator role, use the **no admin role** *role-name* command.

Specifying Administrator Role's Privileges

To specify the administrator role's privileges of CLI, use the following command in the administrator role configuration mode:

cli-privilege all {**rw** | **none**}

- **rw** | **none** − **rw** represents the administrator role has the read-write privilege to all CLI commands. **none** represents the administrator role does not have privilege of CLI and cannot use CLI.

Specifying Administrator Role's Description

To specify administrator role's description, use the following command in the administrator role configuration mode:

description *description*

- *description* − Specify the description for the administrator role. You can specify up to 255 characters.

Use the **no description** command to delete the description.

Creating an Admin User

To create an admin user and enters its configuration mode, under global configuration mode, use the following command:

admin user *user-name*

- *user-name* - Specifying a name for the admin user. The length is from 4 to 31 characters. This command not only creates the admin user, also enters the user's configuration mode; if the admin user exists, it enters its configuration mode directly.

To delete an admin user, under global configuration mode, use the command **no admin user** *user-name*.

When you are under an admin user's mode, you can edit its role, password, access methods and log types (for auditor roles).

Assigning a Role

To assign a role for an admin user, in the user's configuration mode, use the following command:

role {**admin** | **operator** |**auditor** |**admin-read-only**}

- **admin** - Specifying the role of this user as an Administrator.
- **operator** - Specifying the role of this user as an Operator.
- **auditor** - Specifying the role of this user as an Auditor.
- **admin-read-only** - Specifying the role of this user as an Administrator-read-only.

Configuring Password

Password is required for an admin account. To define a password, in the admin user's configuration mode, use the following command:

```
password password
```

- *password* – Specify a password for admin user. The length is from 4 to 31 characters.

To cancel a password, under the admin user's configuration mode, use the command **no password**.

If you login as an operation, auditor or administrator-read-only, you can edit your own password under any mode:

```
exec admin user password update password
```

- *password* – Enter the new password. The length is from 4 to 31.

Note:If you use an Administrator account, you have the privilege to edit the password of every user.

Configuring Password Policy for Admin Users

Password policy defines admin user's password complexity. The password complexity controls the total length of the password, the length of each element, and the validity period of the password. A password can be a combination of elements from the following types:

- Capital letters A to Z.
- Lowercase letters a to z.
- Figures 0 to 9.
- Other visible characters such as semicolon,slash(only support DBC case).

You must enter the password policy mode before you can change the complexity requirement. Use the command password-policy to enter **password policy** configuration mode.

You can set the password complexity if the default-settings can not fit the security requirement. You must enable password complexity checking before setting the password complexity.

To enable or disable password complexity checking, in password policy configuration mode, use the following command:

```
admin complexity {enable | disable}
```

- **enable** | **disable** – Enable or disable password complexity checking. By default, the password complexity checking is disabled. After the feature is enabled, the default complexity requires that the password must contain all the four types of formats: two capitalized letters, two lowercase letters, two figures and two other visible characters (e.g.@).

To define the length of password elements, in password policy configuration mode, use the following command:

```
admin {capital-letters | non-alphanumeric-letters | numeric-characters | small-letters} value
```

- **capital-letters** *value* − Specify the length of capital letters in password. The default value is 2 and the range is 0 to 16.
- **non-alphanumeric-letters** *value* − Specify the length of visible characters except letters and figures in password. The default value is 2 and the range is 0 to 16.
- **numeric-characters** *value* − Specify the length of figures in password. The default value is 2 and the range is 0 to 16.
- **small-letters** *value* − Specify the length of lowercase letters in password. The default value is 2 and the range is 0 to 16.

To define the minimum length of password for the admin users, in password policy configuration mode, use the following command:

```
admin min-length length-value
```

- **min-length** *length-value* − Specify the minimum length of the password. The default value is 4, and the range is 4 to 16. After password complexity checking is enabled, the default value is 8(two capitalized letters, two lowercase letters, two figures and two other visible characters), and the range is 8 to 16.

Note:You can define the minimum length of the password in order to strengthen the security whether the password complexity checking is enabled or not.

The validity period of the password is used to limit the time that you use password. When you log in, if the entered password has expired, the system will prompt to reset the password. After pressing Enter, please enter the new password again. If the new password does not meet the password complexity requirements or the new passwords for the two times are not consistent, you need to re-input. Given that continuous input for three times does not meet the requirement of the password, you can not connect to the device. You are still required to set a new password when logging in again. The new password can be the same as the old one.

To define the validity period of the password for the admin users, in password policy configuration mode, use the following command:

```
admin password-expiration value
```

- **password-expiration** *value* − Specify the validity period of the password. The unit is day. The range is 0 to 365. The default value is 0, which indicates that there is no restriction on validity period of the password.

Under the password policy configuration mode, use the command **no admin complexity** to resume the default setting of password complexity checking.

Viewing Password Policy for Admin Users

To view password policy for admin users, in any mode, use the command:

```
show password-policy
```

Configuring Accesses for Admin Users

By default, a newly created admin user does not have its access opened to visit the device.

```
access {console | http | https | ssh | telnet | any}
```

- **console** − Allows admin user to use Console port to access the device.
- **http** − Allows admin user to use Console port to access the device.
- **https** − Allows admin user to use Console port to access the device.
- **ssh** − Allows admin user to use Console port to access the device.
- **telnet** − Allows admin user to use Console port to access the device.
- **any** − Allows admin user to use Console port to access the device.

Use this command to add access for admin user.

To cancel an access, use the command **no access** {**console** | **http** | **https** | **ssh** | **telnet** | **any**}.

Configuring Log Types for Auditors

An admin user of auditor role is only allowed to view, export and clear log messages. The log types that can be visited by auditor is also defined by Administrator. To specify the log types, under auditor's configuration mode, use the command:

```
log {config | event | ips | traffic | network | security}
```

- **config** − Specify that the auditor can manage configuration logs.
- **event** − Specify that the auditor can manage event logs.
- **ips** − Specify that the auditor can manage IPS logs.

- **traffic** – Specify that the auditor can manage traffic logs.
- **network** – Specify that the auditor can manage network logs.
- **security** – Specify that the auditor can manage security logs.

Repeat this command to specify more than one log types.

To cancel access to a log type, use the command **no log** {**config** | **event** | **ips** | **traffic** | **network** | **security**}.

Specifying Login Limit

If an admin user fails to enter correct password for the specified times, the user will be disallowed to login again within the specified duration. To specify a lockout duration, under global configuration mode, use the following command:

admin lockout-duration *time*

- **lockout-duration** *time* – Specifying lockout duration. The unit is minute. The length is 1 to 65525. The default value is 2.

Use the command **no admin lockout-duration** to resume to the default value.

To specify the maximum login failure time, under the global configuration mode, use the command:

admin max-login-failure *times*

- **max-login-failure** *times* – Specify the maximum error password times. The default value is 3, and the range is 1 to 256.

Use the command **no admin max-login-failure** to resume to the default failure time.

Note:This command is available only for admin user of administrator role.

Viewing Admin roles

To show admin roles： **show admin role** [*role-name*]

Viewing Admin Users

To view admin users, under any mode, use the command:

- To show admin users: **show admin user**
- To show details of an admin user: **show admin user** *user-name*
- To show lockout duration: **show admin lockout-duration**

- To show maximum login failure time: **show admin max-login-failure**

VSYS Admin Users

The admin users of each VSYS are independent from other VSYS. VSYS admin users also have different roles of Administrator, Administrator-ready-only, operator and auditor. Their roles and privileges are the same with normal admin users.

When creating VSYS administrators, you must follow the requirements listed below:

- Backslash (\) cannot be used in administrator names.
- The non-root administrators are created by root administrators or root operators after logging into non-root VSYS.
- After logging into root VSYS, the root administrators can switch to non-root VSYS and configure it.
- Non-root administrators can enter the corresponding non-root VSYS after the successful login, but the non-root administrators cannot switch to the root VSYS.
- Each administrator name should be unique in the VSYS it belongs to, while administrator names can be the same in different VSYSs. In such a case, when logging in, you must specify the VSYS the administrator belongs to in the format of vsys_name\admin_name. If no VSYS is specified, you will enter the root VSYS.

The table lists VSYS admin user's permissions.

Operation	Permissions							
	Root VSYS Administrator	Root VSYS Adminisrator-read-only	Root VSYS Operator	Root VSYS Auditor	Non-root VSYS Administrator	Non-root VSYS Adminisrator-read-only	Non-root VSYS Operator	Non-root VSYS Auditor
Configure (including save configuration)	√	χ	√	χ	√	χ	√	χ
Managing admin users	√	χ	χ	χ	√	χ	χ	χ
Restore factory default	√	χ	χ	χ	χ	χ	χ	χ
Delete	√	χ	√	χ	√	χ	√	χ

Operation	Permissions							
	Root VSYS Adminisrator	Root VSYS Adminisrator-read-only	Root VSYS Operator	Root VSYS Auditor	Non-root VSYS Adminisrator	Non-root VSYS Administrator-read-only	Non-root VSYS Operator	Non-root VSYS Auditor
configuration file								
Roll back configuration	√	χ	√	χ	√	χ	√	χ
Reboot	√	χ	√	χ	χ	χ	χ	χ
View configuration information	√	√	√	χ	View info in current VSYS	View info in current VSYS	View info in current VSYS	χ
View log information	√	√	χ	√	√	√	χ	√
Modify current admin password	√	√	√	√	√	√	√	√
Command import	√	χ	√	χ	√	χ	√	χ
Command export	√	√	√	√	√	√	√	√
Command clear	√	√	√	√	√	√	√	√
Command ping/traceroute	√	√	√	χ	√	√	√	χ
Command debug	√	√	√	χ	χ	χ	χ	χ
Command exec	√	√	√	√	√	√	√	√
Command terminal width	√	√	√	√	√	√	√	χ

Creating a Trusted Host

FS device allows only trusted host to manage the system. Trusted hosts are recognized by their IP addresses. If the host IP address is in the specified IP range, the host is a trusted host.

By default, the trusted IP range is 0.0.0.0/0, which means all hosts are trusted. Therefore, you are suggested to configure a proper trusted IP range and delete the default range afterwards.

Note:When you cannot access the device from a particular host, check the IP settings of trusted host.

To set the IP range for the trusted host, in the global configuration mode, use the following command:

admin host {*A.B.C.D A.B.C.D* | **range** *A.B.C.D A.B.C.D* | *A.B.C.D/M* | **any**} {**http** | **https** | **ssh** | **telnet**| **any** }

- *A.B.C.D A.B.C.D* | **range** *A.B.C.D A.B.C.D* | *A.B.C.D/M* | **any** - Specifies the start IP and end IP of trusted hosts, for example, "1.1.1.1 255.255.0.0" . **any** means you can access the device from any host.
- **http** | **https** | **ssh** | **telnet** | **any** - Specifies the protocol you can use to access the device from a trusted host. **any** means all the four protocols are enabled.

You can specify up to 128 trusted IP ranges.

To delete a trusted IP range, use the command **no admin host** *A.B.C.D A.B.C.D.*

To disable access to the device over the specified protocol, use the command **no admin host** {*A.B.C.D A.B.C.D* | **range** *A.B.C.D A.B.C.D* | *A.B.C.D/M* | **any**} {**http** | **https** | **ssh** | **telnet**| **any** }.

Viewing Trusted Host IP

To view information on configured trusted IP range, in any mode, use the following command:

show admin host

Configuring NetBIOS Name Resolution

The feature of NetBIOS name resolution enables the system to get all registered NetBIOS names of computers in the managed network, and store them in the cache, so that it can provide IP address-NetBIOS name resolution service for functional modules.

So far, NetBIOS name resolution is only used by the traffic logging feature to display the host name in its logs. Therefore, you should enable the NetBIOS name resolution if you want to view host names in traffic logs. For information about how to configure traffic log, see "Displaying Hostname/Username in the Traffic Logs" of "Logs" .

To configure NetBIOS name resolution, take the following steps:

1. Enable the NetBIOS host name resolution service for the specified zone (the zone should not the one being connected to WAN).
2. FSOS automatically looks up NetBIOS names for IP addresses in the stat-sets.

This process may take a while and the results are stored in the NetBIOS cache table. The table is updated regularly by the system.

Note:The computer's host name cannot be searched unless it is enabled with NetBIOS.

Enabling NetBIOS Name Resolution

To enable NetBIOS name resolution for a zone, in the zone configuration mode, use the following command:

nbt-cache enable

To disable NetBIOS name resolution, use the following command:

no nbt-cache enable

Tip: To enter a zone configuration mode, use the command zone zone-name**zone***zone-name*.

Resolving an IP to NetBIOS Name

To resolve an IP address of a host to its NetBIOS host name and MAC address, in the global configuration mode, use the following command:

nbtstat ip2name *ip-address* [**vrouter** *vrouter-name*]

- *ip-address* - Specifies the IP address to be resolved.
- **vrouter** *vrouter-name* - Specifies the VR of the host. If this parameter is not defined, FSOS uses the default VR (trust-vr).

Clearing NetBIOS Cache

To clear NetBIOS cache, in the global configuration mode, use the following command:

clear nbt-cache [*ip-address*] [**vrouter** *vrouter-name*]

- *ip-address* - Specifies the IP address and NetBIOS cache data related to this IP address are cleared by the system. If this parameter is not defined, all NetBIOS cache data are cleared.
- **vrouter** *vrouter-name* - Specifies the VR and NetBIOS cache data related to this VR are cleared by the system. If this parameter is not specified, all NetBIOS cache data are cleared.

Viewing NetBIOS Cache

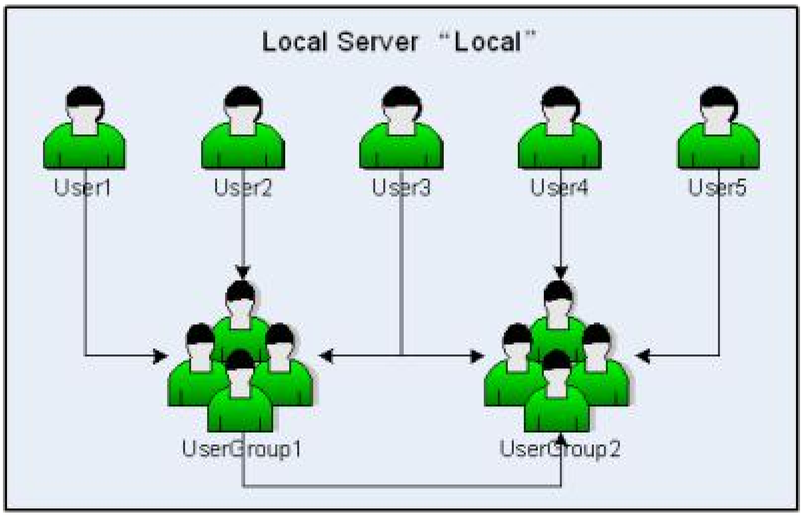
To view NetBIOS cache data (including IP address, host name, MAC address and VR), in any mode, use the following command:

show nbt-cache [*ip-address*] [**vrouter** *vrouter-name*]

- *ip-address* - Shows NetBIOS cache data related to the specified IP address. If this parameter is not defined, all NetBIOS cache data are displayed.
- **vrouter** *vrouter-name* - Shows NetBIOS data of the specified VR. If this parameter is not defined, all NetBIOS cache data are displayed.

Management of System User

In FSOS, user refers to the user who uses the functions and services provided by the FS 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. FSOS 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 takes the default AAA server Local as an example and shows the relationship between users and user groups:



As shown above, User1, User2 and User3 belong to UserGroup1, while User3 also belongs to UserGroup2, and UserGroup2 also contains User4, User5 and UserGroup1.

Roles are designed with certain privileges. For example, a specific role can gain access to some specified network resources, or exclusively use some bandwidth. In FSOS, users and privileges are not directly associated. Instead, they are associated by roles. The mappings between roles and users are defined by role mapping rules. When a role is assigned with some services, its mapped users receive the corresponding services as well. FSOS supports the AND, NOT or OR logical calculation of roles.

FS device supports the following role-based functions:

- Role-based policy: Access control over users according to their roles.
- Role-based iQoS: Bandwidth control over users according to their roles.
- Role-based stat-set: Collects statistics on bandwidth, sessions and new sessions based on roles.
- Role-based session limit: Implements session limits for specific users.
- SCVPN role-based host security check: Resource access control over users according to roles.
- Role-based PBR: Implements routing for users of different types.

Configuring Users

User configurations include static user binding configuration and authenticated user configuration.

Binding an IP/MAC Address to a User

To bind an IP address or MAC address to a user, in the global configuration mode, use the following command:

user-binding *aaa-server-name user-name* {**ip** *ip-address* [**auth-check-only** | **vrouter** *vr-name*] | **mac** *mac-address*}

- *aaa-server-name* - Specifies the name of the user's AAA server.
- *user-name* - Specifies the user name.
- **ip** *ip-address* - Specifies the IP address.
- **auth-check-only** - If this parameter is configured, the system checks if the user IP address conforms with the bound IP of this user. If it conforms, the user is allowed to enter authentication stage.
- **vrouter** *vr-name* - Specifies the VR of the designated IP/MAC address. The default value is the default VR (trust-vr).
- **mac** *mac-address* - Specifies the MAC address.

To remove the binding of IP/MAC and user, in the global configuration mode, use the following command:

no user-binding *aaa-server-name user-name* {**ip** *ip-address* [**auth-check-only**] | **mac** *mac-address*} [**vrouter** *vr-name*]

Configuring Users in the Local AAA Servers

You can configure users/user groups to a local AAA server. To enter the local AAA server configuration mode, in the global configuration mode, use the command **aaa-server** *aaa-server-name* **type local**

user *user-name*

To create a local user, in the local AAA server configuration mode, use the following command:

- *user-name* - Specifies the user name. You can specify up to 63 characters.

This command creates a user and leads you into its configuration mode; if the user name exists, you will directly enter the user configuration mode. To delete the specified user, in the AAA server configuration mode, use the following command:

no user *user-name*

Configurations of a local user include:

- Basic settings: password, expiration, description and user group configuration.
- Dial-up VPN settings: IKE ID configuration.
- PnPVPN settings: DNS server, WINS server, IP/netmask/gateway/tunnel routing of DHCP address pool and tunnel routes. For detailed information, see "Configuring User's Network" of "VPN".

Configuring Password

To specify a password, in the user configuration mode, use the following command:

password *password*

- *password* - Specifies the user password. You can specify up to 31 characters.

To delete a password, in the user configuration mode, use the following command:

no password

Specifying a User Expiration Date

An expired user cannot pass the authentication, so it becomes an invalid user. By default, all users have no expiration date set.

To specify the expiration date and time for a user, in the user configuration mode, use the following command:

expire *Month/day/year HH:MM*

- *Month/day/year HH:MM* - Specifies the date and time in the format of month/date/year hour:minute. For example, expire 02/12/2010 12:00 indicates that the user is invalid since 12:00, February 12nd, 2010.

To cancel the expiration date configuration, in the user configuration mode, use the following command:

no expire

Describing a User

To give some description for a user, in the user configuration mode, use the following command:

desc *string*

- *string* - Specifies description at a maximum of 31 characters.

To delete the description, in the user configuration mode, use the following command:

no desc

Specifying an IKE ID

The Dial-up VPN users need IKE IDs. To specify an IKE ID, in the user configuration mode, use the following command:

ike_id {fqdn *string* | asn1dn *string* | key-id *string* }

- fqdn *string* - Uses IKE ID of the FQDN (Fully Qualified Domain Name) type. *string* is the ID content.
- asn1dn *string*- Uses IKE ID of the Asn 1dn type, which is only applicable to the user with a certificate. *string* is the ID content.
- key-id *string* – Specifies the ID that uses the type of the Key ID. This type can only be used in the XAUTH function.

To delete the IKE ID of a user, in the user configuration mode, use the following command:

```
no ike_id
```

Specifying a User Group

You can categorize users into a group according to your need. One user is allowed to be in multiple groups.

To specify a group for a user, in the user configuration mode, use the following command:

group *user-group-name*

- *user-group-name* - Specifies the name of an existing group in the system. You can specify up to 127 characters.

Repeat this command to define more user groups for a user.

To cancel a user-user group relationship, in the user configuration mode, use the following command:

no group *user-group-name*

Tip: For more information about user group settings, see Configuring a User Group.

Viewing User/User Group Information

To view the information of user/user group, in any mode, use the following commands:

- Show all users:
  show user
- Show a specific user:
  show user aaa-server *server-name* [**name** *user-name*]
- Show the IP/MAC and user bindings:
  show user-binding aaa-server *server-name*
- Show user groups:
  show user-group aaa-server *server-name*

Configuring a User Group

You can configure users or user groups on a local AAA server. To enter the local AAA server configuration mode, in the global configuration mode, use the command **aaa-server** *aaa-server-name* **type local**.

To create a local user group, in the local AAA server configuration mode, use the following command:

user-group *user-group-name*

- *user-group-name* - Specifies a name for the user group.

This command creates the user group and leads you into the user group configuration mode; if the user group of the specified name exists, you will enter the user group configuration mode directly.

To delete the specified user group, use the following command:

no user-group *user-group-name*

To add a member (either a user or another user group) to the user group, in the user group configuration mode, use the following command:

member {**user** *user-name* | **group** *user-group-name*}

- *user-name* - Specifies the user name.
- *user-group-name* - Specifies the user group name. A user group can include up to five nested layers, but a group cannot add itself as a member.

Repeat this command to add more members to a group.

To delete a member from a user group, in the user group configuration mode, use the following command:

no member {**user** *user-name* | **group** *user-group-name*}

Configuring a Role

Role configurations include:

- Creating a role
- Creating a role mapping rule
- Configuring a role combination

Creating a Role

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

role *role-name*

- *role-name* - Specifies a name for the role. You can specify up to 31 characters.

To delete a role, in the global configuration mode, use the following command:

no role *role-name*

Creating a Role Mapping Rule

Role mapping rule defines the mapping relationship between a role and user/user group. FSOS supports up to 64 role mapping rules, and each rule has a maximum number of 256 entries.

When the authentication for SCVPN is set to USB Key only, the system can map a role for the user according to the CN or OU field of the USB Key certificate. For more information about USB Key authentication, see "Authentication With USB Key Certificate" of "VPN".

To enter the role mapping rule configuration mode, in the global configuration mode, use the following command:

role-mapping-rule *rule-name*

- *rule-name* - Specifies a name for the role mapping rule. You can specify up to 31 characters. This command creates a rule and leads you in the role mapping rule configuration mode; if this rule exists, you will enter its configuration mode directly.

To delete the specified role mapping rule, in the global configuration mode, use the following command:

no role-mapping-rule *rule-name*

To configure a role mapping rule, in the role mapping rule configuration mode, use the following command:

match {**any** | **user** *user-name* | **user-group** *user-group-name* | **cn** *cn-field* | **ou** *ou-field*} **role** *role-name*

- **any** | **user** *user-name* | **user-group** *user-group-name* | **cn** *cn-field* | **ou** *ou-field* - Specifies the user, user group, certificate name or organization unit for the mapping. **any** refers to any user, user group, certificate name or organization unit in the system.
- **role** *role-name* - Specifies a role to be mapped in this rule.

Repeat this command to add more mapping rules.

To delete the specified mapping rule, in the role mapping rule configuration mode, use the following command:

no match {**any** | **user** *user-name* | **user-group** *user-group-name* | **cn** *cn-field* | **ou** *ou-field* } **role** *role-name*

Configuring a Role Combination

Roles can be grouped using logical calculation into a role combination. To configure a role combination, in the global configuration mode, use the following command:

role-expression [**not**] *r1* [{**and** | **or**} [**not**] *r2*] **role** *r3*

- [**not**] *r1* - Specifies the first role in this combination. **not** means excluded; *r1* refers to the name of an existing role. For example, "not testrole1" means all roles other than testrole1.
- **and** | **or** - Specifies the logical operator.
- [**not**] *r2* - Specifies the second role in this combination. *r2* refers to the name of an existing role.
- **role** *r3* - Specifies the calculated result. *r3* refers to the name of the result.

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

```
no role-expression [not] r1 [{and | or} [not] r2] role r3
```

Viewing Role Information

To view role related information, use the following commands:

- Show role information: **show role**
- Show role mapping rule information: **show role-mapping-rule** [*rule-name*]
- Show role combination information: **show role-expression**

Configuring a MGT Interface

You can login to the FS device over Console port, Telnet, SSH, or WebUI and configure their timeout settings, port number and PKI trust domain of HTTPS.

If you fail to login to the device three times in one minute over Telnet, SSH, HTTP or HTTPS, your login attempts will be refused in two minutes.

Configuring a Console MGT Port

This section describes how to configure the baud rate and timeout value of the console port.

Configuring the Baud Rate

To configure the baud Rate of console port, in any mode, use the following command:

```
exec console baudrate {9600 | 19200 | 38400 | 57600 | 115200}
```

- **9600** | **19200** | **38400** | **57600** | **115200** - Specifies the baud rate. The unit is bps and the default value is 115200.

Note:When you login to the device, the baud rate of your console terminal should conform to the console baud rate specified here.

Configuring Timeout

If there is no configuration performed by the logged-in administrator until timeout, the system will disconnect the connection.

To configure the console timeout value, in the global configuration mode, use the following command:

console timeout *timeout-value*

- *timeout-value* - Specifies console timeout value. The value range is 0 to 60 minutes; the value of 0 means no time limit. The default value is 10.

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

no console timeout

Configuring a Telnet MGT Interface

When you login to the device over Telnet, your Telnet port should conform with the device Telnet port specified here. If an established Telnet connection does not send Telnet request until timeout, it will be disconnected.

To configure the Telnet timeout value, in the global configuration mode, use the following command:

telnet timeout *timeout-value*

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

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

no telnet timeout

To configure the allowed maximum number of sessions, in the global configuration mode, use the following command:

telnet max-session *max-session*

- *max-session* – Specifies the allowed maximum number of sessions. The maximum number of sessions of difference platforms differs. The default value of each platform is the maximum number of sessions.

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

no telnet max-session

To specify the port number of Telnet, in the global configuration mode, use the following command:

```
telnet port port-number
```

- *port-number* - Specifies Telnet port number. The range is 1 to 65535. The default value is 23.

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

```
no telnet port
```

Telnet maximum login number defines how many times you can try to login to the device over Telnet. If you fail more than the maximum times, your Telnet login attempts will be refused.

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

```
telnet authorization-try-count count-number
```

- *count-number* - Specifies the maximum login number. The value range is 1 to 10 times. The default value is 3.

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

```
no telnet authorization-try-count
```

Configuring a SSH MGT Interface

This section describes how to configure SSH timeout value, port number and connection interval.

SSH timeout value defines the maximum idle time of a SSH connection. If an established SSH connection does not send any SSH request until timeout, it will be disconnected.

To configure the SSH timeout value, in the global configuration mode, use the following command:

```
ssh timeout timeout-value
```

- *timeout-value* - Specifies the SSH maximum idle time. The value range is 1 to 60 minutes. The default value is 10.

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

```
no ssh timeout
```

To configure the allowed maximum number of sessions, in the global configuration mode, use the following command:

```
ssh max-session max-session
```

- *max-session* − Specifies the allowed maximum number of sessions. The maximum number of sessions of difference platforms differs. The default value of each platform is the maximum number of sessions.

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

no ssh max-session *max-session*

To set up the SSH port number, in the global configuration mode, use the following command:

ssh port *port-number*

- *port-number* - Specifies the SSH port number. The value range is 1 to 65535. The default value is 22.

To restore to the default SSH port number, in the global configuration mode, use the following command:

no ssh port

SSH connection interval specifies the frequency of receiving SSH requests. When an SSH connection is established, the device receives the next SSH connection request at an interval of the time specified here.

ssh connection-interval *interval-time*

- *interval-time* - Specifies an interval time. The value range is 2 to 3600 seconds. The default value is 2.

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

no ssh connection-interval

Configuring a WebUI MGT Interface

This section describes how to configure parameters of WebUI (HTTP or HTTPS) access.

To define the WebUI timeout value, in the global configuration mode, use the following command:

web timeout *timeout-value*

- *timeout-value* - Specifies the WebUI timeout value. The value range is 1 to 1440 minutes. The default value is 10.

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

no web timeout

To specify the HTTP port number, in the global configuration mode, use the following command:

http port *port-number*

- *port-number* - Specifies the port number of HTTP. When visiting WebUI over HTTP, the browser's HTTP port must be the same as the port number specified here. The value range is 1 to 65535. The default value is 80.

To restore to the default HTTP port number, in the global configuration mode, use the following command:

no http port

To configure the anti-XSS service, in the global configuration mode, use the following command:

http anti-xss { **disable** | **enable** | **mode** {**normal**| **strict**}}

- **disable** | **enable** – Disables/Enables the anti-XSS service. By default, this service is enabled.
- **mode** {**normal**| **strict**} – Specifies the mode of the anti-XSS service, including the character matching mode and the regular expression mode.

In the global configuration mode, use the following command to restore the configurations to the default.

no http anti-xss { **disable** | **enable** | **mode** {**normal**| **strict**}}

To specify the HTTPS port number, in the global configuration mode, use the following command:

https port *port-number*

- *port-number* - Specifies the HTTPS port number. When visiting WebUI over HTTPS, the browser’ s HTTPS port number must be the same as the port number specified here. The value range is 1 to 65535. The default value is 443.

To restore to the default HTTPS port number, in the global configuration mode, use the following command:

no https port

To specify the PKI trust domain of HTTPS, in the global configuration mode, use the following command:

https trust-domain *trust-domain-name*

- *trust-domain-name* - Specifies the name of PKI trust domain. When HTTPS starts, HTTPS server uses the certificates of the specified PKI trust domain. If no trust domain is specified, the default PKI domain (trust_domain_default) will be used.

To restore the default PKI trust domain, in the global configuration mode, use the following command:

```
no https trust-domain
```

Viewing MGT Interface Configuration Information

To view management interface configuration information, in any mode, use the following commands:

- Show console port configuration information: **show console**
- Show Telnet configuration information: **show telnet**
- Show SSH configuration information: **show ssh**
- Show Web configuration information: **show http**

Configuring a Storage Device

FS network behavior control feature allows you to keep full records of user network behaviors. The logs are stored in a local database in form of a database file.

The storage device that can accommodate local database can be an SD card, USB disk or the storage expansion module provided by FS.

Formatting a Storage Device

If a storage device cannot function, or its file system is not supported by FSOS, or it has not been formatted yet, you can execute formatting command to repair it, change its file system or format it.

To format a storage device, in any mode, use the following command:

```
exec format [sd0 | usb0 | usb1 | storageX]
```

- **sd0** - Formats the SD card in the SD slot.
- **usb0** | **usb1** - Formats the USB disk inserted to the device’ s USB port.
- **storage***X* - Formats the storage expansion module in the specified slot. X is the slot number and its value range varies from platform types.

Note:Formatting a storage device erases all the data in it. You should back up your files.

Removing a Storage Device

If you pull out the storage device with force, unsaved data may be lost. To ensure data integrity, you should use the command below to safely remove the device.

To safely remove a storage device, in any mode, use the following command:

```
exec detach [sd0 | usb0 | usb1 | storageX]
```

- sd0 - Removes the SD card from the SD slot.
- usb0 | usb1 - Removes the USB disk from the specified USB port.
- storage*X* - Removes the storage expansion module from the specified slot.

Managing Configuration Files

All information of system configuration, such as its initial and current configuration information, is stored in the configuration files. You can use command lines or visit the WebUI to view all sorts of system configurations. The information is stored and displayed in the format of command line.

Managing Configuration Information

This section describes how to view, import, export and save the configuration information.

Note:Passwords of local users won't be exported when you export configuration information.

Viewing Configuration Information

Initial configuration information, stored in the configuration file, is used to configure the system parameters when the device is powered on. If no proper initial configuration information is found, the device uses default parameters to initialize the system. Similarly, the parameter settings the system is using now are called current configuration information.

FSOS saves ten versions of initial configuration information. The latest one is used by the system as its initial configuration information when it starts up; the other versions are backup files. The last saved configuration information is marked as “current” and the nine backup versions are marked by number from 0 to 8 based on their saved time.

To view the initial configuration information, in any mode, use the following command: **show configuration** [**startup**]

To view configuration information other than the current one, in any mode, use the following command:

```
show configuration backup number
```

- *number* - Specifies the number of the configuration information.

To view the configuration information record other than the current one, in any mode, use the following command:

show configuration

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

show configuration interface [*interface-name* | **last** *number*]

- *interface-name* − Specifies the interface name of the configuration information need to displayed.
- last *number* − Specifies the interface entry number of configuration information need to be displayed. System will display the interface configuration information from the last specified value entry to the end entry.

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

show configuration record

To view the current configuration information the system is using, in any mode, use the following command:

show configuration running

To view the current address book configuration information the system is using, in any mode, use the following command:

show configuration address [**last** *number*]

- last *number* − Specifies the address entry number of the configuration information need to be displayed. System will display the address configuration information from the last specified value entry to the end entry.

To view the current policy configuration information the system is using, in any mode, use the following command:

show configuration policy [**last** *number*]

- *last number* − Specifies the policy entry number of the configuration information need to be displayed. System will display the policy configuration information from the last specified value entry to the end entry.

To view the current routing configuration information the system is using, in any mode, use the following command:

show configuration vrouter [**last** *number*]

- **last** *number* – Specifies the routing entry number of the configuration information need to be displayed. System will display the routing configuration information from the last specified value entry to the end entry.

Output the current configuration information using the XML format, in any mode, use the following command:

show configuration xml

Rolling Back to Previous Configurations

To roll back to the previous configuration, there are two ways:

In the execution mode, use the following command to roll back to the previous configuration. FSOS saves the latest ten versions of system configurations as initial configuration files for you to use in system initiation. When the system restarts, the specified configuration will be used.

rollback configuration backup *number*

- *number* - Specifies the number of initial configuration file.

In the configuration rollback mode, use the following command to roll back to the previous configuration and exit the configuration rollback mode. The configuration will be valid without restarting the device.

exec configuration rollback

> Note:In the execution mode, you should use **exec configuration start** command to enter the rollback mode.

For example:

```
hostname# exec configuration start (Enter the configuration rollback mode)

hostname[TRN]# configure (Enter the global configuration mode)

…… (Execute any configuration, and the configuration will be valid immediately)

hostname[TRN](config)# exec configuration rollback (Roll back the configuration and exit the
configuration rollback mode)

hostname#
```

Exiting the Configuration Rollback Mode

To exit the configuration rollback mode directly, you can use the following two ways:

In the configuration rollback mode, use the following command to exit the configuration rollback mode directly.

exec configuration commit

For example:

```
hostname# exec configuration start (Enter the configuration rollback mode)

hostname[TRN]# configure  (Enter the global configuration mode)

…… (Execute any configuration, and the configuration will be valid immediately)

hostname[TRN](config)# exec configuration commit (Exit the configuration rollback mode directly)

hostname#
```

In the configuration rollback mode, use the command **exit**to exit the terminal directly.

Tip:

- When different users log in the device meanwhile, only the user who enters the configuration rollback mode first can do further configuration, and the later users cannot.
- When a user log in the device through different access methods, the user of a certain access method enters in the configuration rollback mode first can do further configuration, and the later users of other access methods cannot. The user of other access methods can force the user of that access method to exit the configuration rollback mode through command.

Configuring the Action

When exiting the configuration rollback mode by using command **exit**, system will exit the configuration rollback mode directly by default. To roll back to the previous configuration and exit the configuration rollback mode, in the global configuration mode, take the following command:

cli-exit-action rollback

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

cli-exit-action commit

Deleting a Configuration File

To delete a configuration file from the system, in the configuration mode, use the following command:

delete configuration {**startup** | **backup** *number*}

- **startup** - Deletes the current configuration file.

- **backup** *number* - Deletes the specified backup configuration file.

Saving Configuration Information

When the current configurations are saved, they become the initial configuration information used by the system as next start-up configurations.

To save the current configurations, in any mode, use the following command:

save [*string*]

- *string* - Give some description for the saved configuration. If you leave this parameter blank, the former configurations will be replaced.

Backing up Configuration File Automatically

You can configure the function of back up the configuration file automatically, the device will check the configuration file regularly, when the configuration file changes, the system will update the configuration files to a FTP server or a TFTP server.

To back up configuration file to a FTP server automatically, in the global configuration mode, use the following command：

configuration auto-backup ftp *ip-address* [**user** *user-name* **password** *password*] [**vrouter** *vrouter-name*] **path** *path* [**interval** *time-value*]

- *ip-address* - Specifies the IP address of FTP server.
- **user** *user-name* **password** *password* - Specifies the user name and password accessing FTP server.
- **vrouter** *vrouter-name* – Specifies the VRouter name.
- **path** *path* - Specifies the path of transferring the configuration files.
- **interval** *time-value* – Specifies the update interval. The value range is 1 to 7*24 hours. The default value is 1 hour. If this parameter is not specified, the system will check the configuration file hourly, and back up the changed configuration files to FTP server when configurations are changed.

In the global configuration mode, use **no configuration auto-backup ftp** command to cancel the settings of backing up configuration file to a FTP server automatically.

To back up configuration file to a TFTP server automatically, in the global configuration mode, use the following command：

configuration auto-backup tftp *ip-address* [**vrouter** *vrouter-name*] **path** *path* [**interval** *time-value*]

In the global configuration mode, use **no configuration auto-backup tftp** command to cancel the settings of backing up configuration file to a TFTP server automatically.

Viewing backing up configuration file automatically Information

To view backing up configuration file automatically Information, in any mode, use the following command:

show configuration auto-backup

Exporting Configuration Information

Current startup, backup and current startup of VSYS configurations can be exported to external destinations, including FTP server, TFTP server and USB flash disk.

To export system configurations to an FTP server, in the execution mode, use the following command:

export configuration {**startup** | **backup** *number* | **all-vsys**} **to ftp server** *ip-address* [**vrouter** *vrouter-name*][**user** *user-name* **password** *password*] [*file-name*]

- **startup** | **backup** *number* | **all-vsys** - Exports the current startup configurations or the specified backup configurations or the current startup configurations of VSYS.
- *ip-address* - Specifies the IP address of FTP server.
- *vrouter-name* - Exports the configuration information of the specified VRouter.
- **user** *user-name* **password** *password* - Specifies the username and password of the FTP server.
- *file-name* - Specifies the name for the file.

To export configurations to a TFTP server, in the execution mode, use the following command:

export configuration {**startup** | **backup** *number* | **all-vsys**} **to tftp server** *ip-address* [**vrouter** *vrouter-name*] [*file-name*]

To export system configurations to USB flash disk, in the execution mode, use the following command:

export configuration {**startup** | **backup** *number*} **to** {**usb0** | **usb1**} [**vrouter** *vrouter-name*] [*file-name*]

Importing Configuration Information

Configuration files can be imported into the system from the FTP server, TFTP server, or USB flash disk inserted to the device USB port.

To import configurations from an FTP server, in the execution mode, use the following command:

import configuration [all-vsys] from ftp server *ip-address* **user** *user-name* **password** *password* [**vrouter** *vrouter-name*] *file-name*

- **all-vsys** - Imports configuration information of all VSYS.
- *ip-address* - Specifies the IP address of FTP server.
- **user** *user-name* **password** *password* - Specifies the username and password of the FTP server.
- *vrouter-name* - Exports configuration information for the specified VRouter.
- *file-name* - Specifies a name for the configuration file.

To import configurations from a TFTP server, in the execution mode, use the following command:

import configuration [all-vsys] from tftp server *ip-address* [**vrouter** *vrouter-name*] *file-name*

To import configurations from a USB flash disk, in the execution mode, use the following command:

import configuration from {**usb0** | **usb1**} [**vrouter** *vrouter-name*] *file-name*

Restoring Factory Defaults

You can either press the CLR button on the device or use the command in this section to reset the device and restore factory defaults.

unset all

Note:Use this command with caution. It clears all configurations on the device.

Interface Working Modes

For the interface module of IOC-8SFP+, partial FS devices can switch the working modes of the interface. The interface working modes support 10G and 1G. Switching the working modes can realize the following functions:

- Make the 10G interface work in the working mode of 1G interface and realize the connection between the 10G interface and the 1G interface.

The default working mode of 10G interface is 10G. In the interface configuration mode, use the following command to switch the working mode to 1G:

channel-speed 1000

In the interface configuration mode, use the **no channel-speed** command to restore the working mode to the default one.

Note: Before specifying the interface working mode, you need to delete the corresponding configurations of the interface.

Viewing the Configuration of Current Object

After the configuration of the specific object is completed, in the current configuration mode, you can use the command **show this** to view the configuration of current object.

The table below shows the object names and its configuration mode that system supported to view.

Object Name	Configuration Mode	Configuration Mode Prompt
Admin	Administrator configuration mode	hostname(config-admin)#
AAA server	AAA service configuration mode	hostname(config-aaa-server)#
Interface	Interface configuration mode	hostname(config-if-eth0/0)#
Zone	Zone configuration mode	hostname(config-zone-trust)#
Address	Address configuration mode	hostname(config-addr)#
Service	Service configuration mode	hostname(config-service)#
Service group	Service group configuration mode	hostname(config-svc-group)#
Policy-based Route	PBR configuration mode	hostname(config-pbr)#
VRouter	VRouter configuration mode	hostname(config-vrouter)#
Configure NAT rules for the default VR trust-v	NAT configuration mode	hostname(config-nat)#

Viewing the Information of Optical Module

To view the information of optical module, including serial number, power, temperature and voltage, and module type. In any in any mode, use the following commands:

show transceiver [*interface-name*]

- *interface-name* – Specifies the interface name of optical module.

Configuring Banner

Banner used to display the statement after logining the system, the user can customize the Banner information content. To edit the Banner, in the global configuration mode, use the following command:

admin login-banner *Banner-content*

- *Banner-content* - Specifies the Banner content. The length varies from 1 characters to 4096 characters. After executing this command, the system will create the Banner of specified content. If the Banner already exists, it will modify the Banner for the specified content.

In the global configuration mode, use **no admin login-banner** command to delete the Banner.

Note:

- In the edit Banner content, if you need to wrap, enter "\n", if you need a space, enter the double quotes "".
- Support for displaying Banner when login to the device over SSH, Telnet, or Console port.

System Maintenance and Debugging

Testing tools, the commands Ping and Traceroute, are used to test network availability and diagnose system errors. FS device also provides debugging feature for users to check and analyze the system.

Ping

Ping is used mainly for testing network connection and host accessibility.

To check network availability, in any mode, use the following command:

ping [**ipv6**] {*ip-address* | *hostname*} [**count** *number*] [**size** *number*] [**source** *ip-address*] [**timeout** *time*] [**vrouter** *vrouter-name*]

- *ip-address* | *hostname* - Specifies the IP address or hostname of the destination. When using the dual-stack firmware, you can specify the IPv6 address.
- **count** *number* - Specifies the number of Ping packets. The value range is 1 to 65535. By default, packet number is not limited.
- **size** *number* - Specifies the size of ping packet. The value range is 28 to 65500 bytes.
- **source** *ip-address* - Specifies the source interface name of ping packets.

- **timeout** *time* - Specifies the timeout value for the ping packets. The range is 0 to 3600 seconds. The default number is 0, which means no timeout.
- **vrouter** *vrouter-name* - Specifies the VRouter of the interface sending ping packets. The default value is trust-vr.

The output of ping command includes the response status for each Ping packet and the final statistics:

- The response status for each Ping packet. If there is no response, the output is "Destination Host Not Responding"; otherwise, the output is the packet sequence, TTL and responding time of the response packet. If the Ping packet does not reach the destination route or the interface that sends the Ping packet changes, the output is "Network is unreachable". If the destination address of the Ping packet cannot be resolved, the output is "unknown host hostname".
- Final statistics. The final statistics includes sent packet number, received packet number, lost packet percentage and time.

Here is a **ping** command example:

```
hostname(config)# ping 10.200.3.1
Sending ICMP packets to 10.200.3.1
Seq ttl time(ms)
1 128 2.53
2 128 1.48
3 128 1.48
4 128 1.47
5 128 1.46
statistics:
5 packets sent, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.464/1.689/2.536/0.423 ms
```

Traceroute

Traceroute is used to test and record gateways of packets from source host to the destination. It is mainly used to check whether the destination is reachable, and analyze the fault gateway in the network. The common Traceroute function is performed as follows: first, send a packet with TTL 1, so the first hop sends back an ICMP error message to indicate that this packet cannot be sent (because of the TTL timeout); then this packet is re-sent, with TTL 2, TTL timeout is sent back again; repeat this process till the packet reaches the destination. In this way, each ICMP TTL timeout source address is recorded. As result, the path from the originating host to the destination is identified.

To trace the gateways the command traceroute has traversed, in any mode, use the following command:

traceroute {*ip-address* | *hostname*} [**numberic**] [**port** *port-number*] [**probe** *probe-number*] [**timeout** *time*] [**ttl** [*min-ttl*] [*max-ttl*]] [**source** *interface*] [**use-icmp**] [**vrouter** *vrouter-name*]

- *ip-address* | *hostname* - Specifies the destination IP address or host name of traceroute.
- **numberic** - Specifies to display the address in numeric format without resolution.
- **port** *port-number* - Specifies the UDP port number. The value range is 1 to 65535. The default value is 33434.
- **probe** *probe-number* - Specifies the number of probe packet in each hop. The range is 1 to 65535. The default value is 3.
- **timeout** *time* - Specifies the timeout value of next probe packet. The range is 1 to 3600 seconds. The default value is 5.
- **ttl** [*min-ttl*] [*max-ttl*] - *min-ttl* is the minimum TTL value, with range from 1 to 255 and default value being 1. *max-ttl* is the maximum TTL value, with range from 1 to 255 and default value being 30. Specifying TTL is used to display the echo from the *min-ttl* hop to the *max-ttl* hop.
- **source** *interface* - Specifies the the name of the interface sending traceroute probe packets.
- **use-icmp** - Uses ICMP packets to probe. If this parameter is not defined, the system uses UDP packets to probe.
- **vrouter** *vrouter-name* - Specifies the VRouter of the egress interface of traceroute probe packets. The default value is the default VRouter (trust-vr).

Here is an example of applying command **traceroute** in network analysis:

```
hostname(config)# traceroute 210.74.176.150

traceroute to 210.74.176.150 (210.74.176.150), 30 hops max, 52 byte packets

1 10.200.3.1 (10.200.3.1) 0.572 ms 0.541 ms 0.359 ms

2 192.168.3.1 (192.168.3.1) 0.601 ms 0.754 ms 0.522 ms

3 202.106.149.177 (202.106.149.177) 1.169 ms 1.723 ms 1.104 ms
```

```
4 61.148.16.133 (61.148.16.133) 2.272 ms 1.940 ms 2.370 ms

5 61.148.4.17 (61.148.4.17) 2.770 ms 61.148.4.101 (61.148.4.101) 6.030 ms 61.148.4.21
(61.148.4.21) 2.584 ms

6 202.106.227.45 (202.106.227.45) 4.893 ms 5.010 ms 3.917 ms

7 202.106.193.70 (202.106.193.70) 5.407 ms 202.106.193.126 (202.106.193.126) 4.247 ms
202.106.193.70 (202.106.193.70) 6.954 ms

8 61.148.143.30 (61.148.143.30) 3.459 ms 3.758 ms 2.853 ms

9 * * *

10 * * *
```

This example shows which gateways the packets have traversed during the process from source host to destination host and fault gateways.

System Debugging

System debugging helps you to diagnose and identify system errors. Basically, all the protocols and functions can be debugged. By default, debugging of all functions is disabled. The debugging function can only be configured through CLI.

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

debug {**all** | *function-name*}

- **all** - Enables all debugging functions.
- *function-name* - Enables the specified protocol or feature debugging.

To disable all or one debugging function, in any mode, use the following command:

undebug {**all** | *function-name*}

You can disable debugging by pressing ESC key. As some debugging information has been cached, the closing process may take several minutes.

To see the status of the debugging function, in any mode, use the following command:

show debug

Note:If you want to view debugging information on your terminal, enable debug logging function (execute the command **logging debug on**).

Collecting and Saving Tech-support Information to File

In order to locate the system fault, you should collect the displayed information of all the **show** commands and save as tech-support file. To collect and save the tech-support information to file, in any mode, use the following command:

show tech-support [**cpu** cpu-number | **all**]

- *cpu-number* – Collects and saves the tech-support information of specified CPU to file. You can configure this parameter only in system with multiple CPUs.
- **all** – Collects and saves all the tech-support information to file. You can configure this parameter only in system with multiple CPUs.

Note:You can collect and save all the tech-support information to file through command **show tech-support** in system with single CPU.

Collecting the Tech-support Information Automatically

To collect the Tech-support Information Automatically, in any mode, use the following command:

show tech-support-auto interval *interval-time* **count** *count-time*

- *interval-time* – Specifies the interval time to collect the tech-support information automatically. The range is 10 to 1440. The unit is minute.
- *count-time* – Specifies the times to collect the tech-support information automatically. The range is 1 to 10.

Note:

- System can save 10 tech-support files at most. When the number of file exceeds 10, the new file will cover the older file.
- When system executes this command, if you configure another command to collect the tech-support information automatically, the new configuration will cover the previous configuration.

Viewing the Information of Nvramlog or Watchdoglog File

To view the log information of nvramlog or watchdoglog in tech-support file, in any mode, use the following command:

show tech-support *log-name*

- *log-name* – Specifies the name of log information which is required to be displayed. You can specify the name as vramlog or watchdoglog.

Deleting the Function of Automatically Collecting Tech-support Information

To delete the function of automatically collecting tech-support information, in any mode, use the following command:

```
show tech-support-auto clear
```

Rebooting the System

Turning off the device and powering it on again can reboot it. In addition, you can also use command line or WebUI to restart the system.

To reboot the device, in the configuration mode, use the following command: **reboot**

```
hostname# reboot
System configuration has been modified. Save? [y]/n (type y or press Enter to save the settings; type n to give up changes.)
Building configuration..
Saving configuration is finished
System reboot, are you sure? y/[n]  (type y to reboot the system; type n or press Enter to go back to the configuration mode.)
```

Save the current settings before rebooting the device if you don't want to lose unsaved configurations. Be careful when you execute this command, because network disconnection occurs during the rebooting process.

Upgrading FSOS

This section introduces FSOS starting-up system and describes how to upgrade FSOS.

Starting Process

The start-up system consists of three parts, which are Bootloader, Sysloader and FSOS. There functions are listed below:

- Bootloader - The first started program when the device is powered on. Bootloader loads FSOS or Sysloader and makes them start.

- Sysloader - The program that upgrades FSOS.
- FSOS - The operating system running on the device.

When a device is powered on, the Bootloader tries to start FSOS or Sysloader. The Sysloader is used to select existing FSOS in the system and upgrade FSOS via FTP, TFTP or USB port. The upgrade of Sysloader is performed by the Bootloader via TFTP.

Bootloader

The Bootloader has two working modes: automatic mode and interactive mode.

In the automatic mode, Bootloader starts the existing FSOS first. If no FSOS exists or only illegal ones present, the system stops and you must upgrade FSOS in Sysloader.

To enter the interactive mode, press ESC during the starting process according to the prompt. In the interactive mode, you can select a Sysloader stored in the flash to start, or download a new version of Sysloader from the TFTP server and then start it.

FSOS Quick Upgrading (TFTP)

The Sysloader downloads FSOS from TFTP server, ensuring a fast system upgrading from network.

To upgrade FSOS, take the following steps:

Power on the device and enter Sysloader:

```
FS

FS Bootloader 1.4.8 Oct 31 2019-12:41:54

DRAM: 2048 MB

BOOTROM: 512 KB

Press ESC to stop autoboot: 4  (Press ESC during the 5-second countdown.)

Run on-board sysloader? [y]/n: y (Type y or press Enter)

Loading: ###########################
```

Select **Load firmware via TFTP** from the menu:

```
Sysloader 1.4.8 Oct 31 2019-12:54:30

1 Load firmware via TFTP

2 Load firmware via FTP

3 Load firmware from USB disks (not available)
```

```
4 Select backup firmware as active

5 Show on-board firmware

6 Reset

Please select: 1 (Type 1 and press Enter)
```

Specify Sysloader IP, TFTP server IP, gateway IP, and the name of FSOS:

```
Local ip address [ ]: 10.2.2.10/16(Type the IP address of Sysloader and press Enter.)Server ip address [ ]: 10.2.2.3 (Type the IP address of TFTP server and press Enter.)

Gateway ip address [ ]: 10.2.2.1 (If Sysloader and TFTP server are not in the same network segment, you need to provide the gateway IP address and press Enter; otherwise, just press Enter.)

File name : FSOS-5.5R6 (Type the name of FSOS and press Enter, and then the system begins to transfer the file.)

####################################################################
####################################################################
########################
```

Save FSOS. Take the following steps:

```
File total length 10482508

Checking the image...

Verified OK

Save this image? [y]/n: y (Type y or press Enter to save the transferred FSOS.)

Saving ........................................

Set FSOS-5.5R6 as active boot image
```

Reboot the device.

```
Please reset board to boot this image

1 Load firmware via TFTP

2 Load firmware via FTP

3 Load firmware from USB disks (not available)

4 Select backup firmware as active
```

```
5 Show on-board firmware

6 Reset

Please select: 6 (Type 6 and press Enter. The system reboots.)
```

The device can save only two versions of FSOS. If you want to save a new one, delete an existing one according to the prompt.

Other Upgrading Methods

Though downloading FSOS from TFTP server is often used to upgrade the system, the device also supports upgrading from FTP server and USB flash disk.

Upgrading FSOS via FTP

To download FSOS from FTP server and upgrade it, in the Sysloader program, take following steps:

1. In Sysloader, select 2 and press Enter.
2. Type the Sysloader IP address behind the prompt *Local ip address [ ]:* and press Enter.
3. Type the FTP server IP address behind the prompt *Server ip address [ ]:* and press Enter.
4. If the Sysloader and FTP server are not in the same network segment, type the gateway IP address of Sysloader behind the prompt *Gateway ip address [ ]:* and press Enter.
5. Type FTP user name behind the prompt *User Name [anonymous]:* and press Enter.
6. Type the password of that user behind *Password :* and press Enter.
7. Type the file name of FSOS behind the prompt *File name :* and press Enter. The system starts to download the specified FSOS.
8. When the downloading is complete, type **y** to save this version of FSOS into the device flash.
9. After the new FSOS is saved, the system shows Sysloader menu and you can type **6** and press Enter to start the system with the new FSOS.

Tip: If an FTP server allows anonymous login, just press Enter when it requires a username and password.

Upgrading FSOS via USB

To upgrade FSOS to a version saved in the USB flash disk, take the following steps:

1. Copy the FSOS you want to use in your USB flash disk.

2. Plug the USB flash disk into the device USB port.
3. Enter Sysloader, select **3** in its menu, and press Enter.
4. Select the FSOS you want and type **y**. The system starts to upload the FSOS.
5. When it’ s complete, type **y** if you want to save the FSOS into the device flash.
6. In the Sysloader menu, select **6** and press Enter. The system starts with the new FSOS.

Introduction to Sysloader Menu

This section introduces the function of each Sysloader menu item. Type the number of the operation you want, and press Enter, then follow instructions to continue.

Option	Description
1. Load firmware via TFTP	Upgrades FSOS by downloading an OS file from a TFTP server.
2. Load firmware via FTP	Upgrades FSOS by downloading an OS file from an FTP server.
3. Load firmware from USB disks	Upgrades FSOS by fetching an OS file from an USB disk on the device.
4. Select backup firmware as active	Switches the saved backup FSOS to be the active FSOS used when the system rebooting.
5. Show on-board firmware	Shows all saved FSOS with their status.
6. Reset	Reboot the system.

Upgrading FSOS Using CLI

Besides Sysloader, you can upgrade FSOS by typing command lines.

To upgrade FSOS via FTP, in the configuration mode, use the following commands:

import image from ftp server *ip-address* [**user** *user-name* [**password** *password*]] [**vrouter** *vrouter-name*] *file-name*

- *ip-address* - Specifies the IP address of FTP server.
- **user** *user-name* **password** *password* - Specifies username and password of FTP server.
- *vrouter-name* - Updates FSOS by using the specified VRouter.
- *file-name* - Specifies the name of FSOS you want to use.

To upgrade FSOS via TFTP, in the configuration mode, use the following command:

import image from tftp server *ip-address* [**vrouter** *vrouter-name*] *file-name*

To upgrade FSOS via USB, in the configuration mode, use the following commands:

import image from {**usb0** | **usb1**} [**vrouter** *vrouter-name*] *file-name*

Reboot the device to make the new FSOS take effect.

License Management

License is used to authorize users features, services or extending the performance. If you do not buy and install the corresponding License, the features, services and performances which is based on License will not be used, or can not achieve the higher performance.

License classes and rules.

Platform License	Description	Valid Time
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 preinstalled platform trial license for 15 days in the factory.	You cannot modify the existing configuration when License expired. System will restore to factory defaults when the device reboot.
Platform Base	You can install the platform base license after the device formal sale. The license provide basic firewall and VPN function.	System cannot upgrade the OS version when License expired. But system could work normally.
Function License	**Description**	**Valid Time**
VSYS	Authorizing the available number of VSYS.	Permanent
SSL VPN	Authorizing the maximum number of SSL VPN access. Through installing multiple SSL VPN licenses, you can add the maximum number of SSL VPN access.	Permanent
QoS	Enable iQoS function.	System cannot upgrade the iQoS function and cannot provide the maintenance service when License expired.
Service License	**Description**	**Valid Time**
AntiVirus	Providing antivirus function and antivirus	System cannot update the

	signature database update.	antivirus signature database when License expired. But antivirus function could be used normally.
IPS	Providing IPS function and IPS signature database update.	System cannot update the IPS signature database when License expired. But IPS function could be used normally.
URL	Providing URL database and URL signature database update.	System cannot provide to search URL database online function when License expired. But user-defined URL and URL filtering function could 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 License expires. But the functions included and rules could be used normally.

Applying for a License

To apply for a license, take the following steps:

Use the command **exec license apply applicant** *string* to generate a license application request. For more information, see Managing a License Using CLI” 。

Send the request to the FS agent.

Installing a License

A license contains a string of characters. When you get the license, take the following steps to install it in the device:

If you use CLI to install a license, in any mode, use the command **exec license install** *license-string*. For more information, see Managing a License Using CLI. After installing, you need to reboot system to make the license effective.

Note: Although license can be removed, you are strongly suggested not to uninstall any license.

Managing a License Using CLI

This section describes how to apply, install and uninstall a license using command lines.

Generating a Request for License

To generate a request for license, in any mode, use the following command:

```
exec license apply applicant string
```

- *string* - Specifies the name of the applicant.

Installing/Uninstalling a License

After obtaining the license, to install it, in any mode, use the following command:

```
exec license install license-string
```

- *license-string* - Pastes the license string.

To uninstall a license, in any mode, use the following command:

```
exec license uninstall license-name
```

- *license-name* - Specifies the name of the license you want to uninstall.

After installing some licenses, you need to type the command **reboot** to reboot system.

The following licenses will take effect after the reboot and other licenses will take effect directly.

- After installing the following licenses for the first time, you need to reboot the system: Platform Trial, Platform Base, AV, IPS, URL.
- The system needs to be rebooted each time the following licenses are installed: VSYS.

Batch Installing Licenses

When installing licenses to a large amount of devices, using this batch method will simplify the process and minimize the mistakes.

Batch Installing Procedure

To install licenses in batch, take the following steps:

1. If you require many licenses, you need provide the device serial numbers and license types information to FS. For information about license, consult the local agent.

2. FS generates license files according to your requests and send them to you in proper ways, like email.

3. When you receive the license files, copy them to a FAT32 USB disk under the directory named "\license" (the name must be in lower case). The license files cannot be changed; otherwise they are unable to be installed.

4. Install the licenses to all the devices in the USB disk. See the section below.

Installing a License

After copying the license files to the proper directory in the USB disk, insert the USB disk into the USB port of the device, the device automatically scans the USB disk and install the matched license. You can view the status by checking the LED lights.

Power on the device, wait until it shows login prompt.

Insert the USB disk into the USB port.

The device automatically scans the USB disk, searches for a license with the same serial number of the device, and installs it. The ALM light shows the installation status, as shown in the table below:

Status	ALM Indicator
Searching for a matched license from the directory "license" in USB disk.	Blinking green until installation completes
The installation is completed.	Restore to former status
No matched license is found.	Blinking red for 10 seconds and then restore to the former status.
No "license" directory is found.	No change.

Remove the USB disk from the device and you can install licenses to other devices using the same method.

All matched licenses can be installed into the devices. To avoid reinstallation, used licenses are removed from the "license" directory to a "license_installed" directory (automatically created).

Reboot system to make license effective.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is an application layer protocol for managing devices on IP networks. It consists of four key components: Network Management System (NMS), Network Management Protocol, SNMP agent and Management Information Base (MIB).

- Network Management System (NMS): A software system which uses the network managers (like adventnet, solarwinds) to send requests, such as Get and Set, and receives the responses from the SNMP agent so that it can manage and monitor network devices.

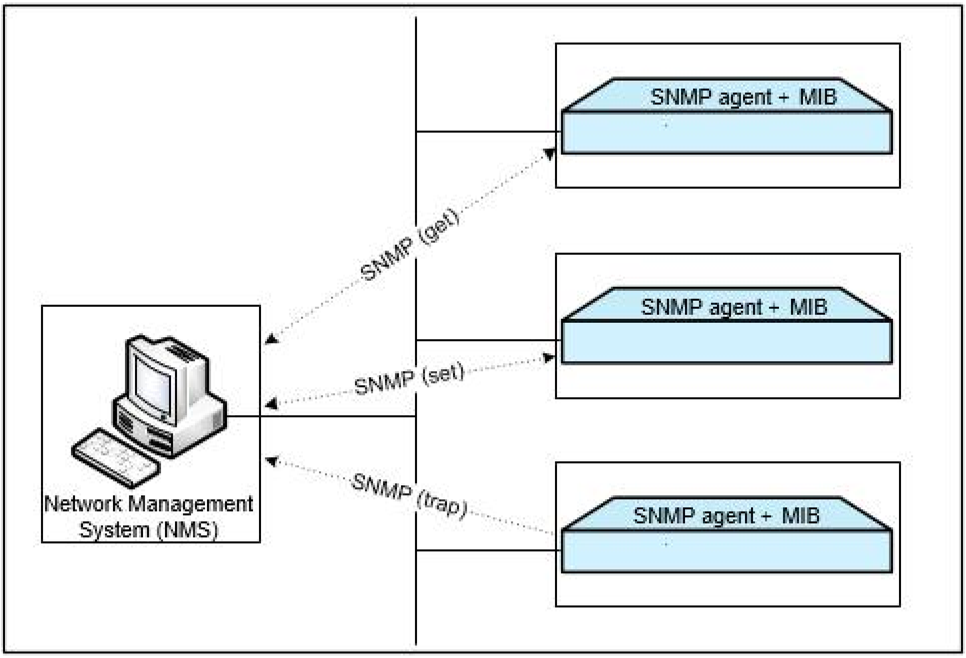
- SNMP Agent: A software module on a managed network device, which sends the local device information to NMS.

- Network Management Protocol: It is used to exchange SNMP packets between NMS and SNMP agent. It supports three basic functions, which are GET, SET and Trap. Get is used by NMS to fetch the MIB value from the SNMP agent; Set is used by NMS to configure the MIB value of the SNMP agent; Trap is used by the SNMP agent to sent event notifications to NMS.

- Management Information Base (MIB): An information database maintained by SNMP Agent, which contains specific characteristics of managed network devices, comprises object variables. The object variables can be requested or set by NMS.

FS SNMP

FS devices support SNMP agent function, which receives requests from and responds the device information to NMS. Figure below illustrates how a NMS interacts with a security device via SNMP.



Supported RFCs

FS security device supports the following SNMP versions:

- SNMPv1: Simple Network Management Protocol. See RFC-1157.

- SNMPv2: See the following RFCs:

  - RFC-1901 - Introduction to Community-based SNMPv2;
  - RFC-1905 - Protocol Operations for Version 2 of the Simple Network Management Protocol;
  - RFC-1906 - Transport Mappings for Version 2 of the Simple Network Management Protocol.
- SNMPv3: See the following RFCs:
  - RFC-2263 - SNMPv3 Applications;
  - RFC-2264 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3);
  - RFC-2265 - View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).

SNMPv1 protocol and SNMPv2 protocol use community-based strings to limit the NMS to get device information. SNMPv3 protocol introduces a user-based security module for information security and a view-based access control module for access control.

Supported MIBs

FS 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, FSOS offers a private MIB, which contains the system information, IPsec VPN information and statistics information of the device. You can use the private MIB by loading it into a SNMP MIB browser on the management host.

Supported Traps

Trap is an asynchronous notification from SNMP agent to SNMP client. The following traps are supported in FSOS:

- Warm start
- Authentication failure
- Interface link down/up
- VPN SA negotiation status change
- HA status change
- System status changes, including CPU utilization over 80%, fan status change, memory low, etc.

- Network attacks, including ARP spoofing, IP Spoofing, SYN Flood attack, etc.
- Configuration changes

Configuring SNMP

FS device provides the following SNMP configuration options:

- Enabling/Disabling the SNMP agent function
- Configuring the SNMP port number
- Configuring SNMP engineID
- Creating an SNMPv3 user group
- Creating an SNMPv3 user
- Configure the IP address of the management host
- Configuring the recipient of a SNMP trap
- Configuring sysContact
- Configuring sysLocation
- Specifying the VRouter on which the SNMP is enabled

Enabling/Disabling the SNMP Agent Function

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

snmp-server manager

To disable it, use the command **no snmp-server manager**.

Configuring the SNMP Port Number

To specify the port number of the SNMP agent, in the global configuration mode, use the following command:

snmp-server port *port-number*

- *port-number* - Specifies the port number. The value range is 1 to 65535. The default value is 161.

Configuring SNMP Engine ID

SNMP EngineID is a unique identifier for the SNMP engine. The SNMP engine is the essential component of the SNMP entity (NMS or network devices managed by SNMP). The functions of the SNMP engine are sending/receiving SNMP messages, authenticating, extracting PDU, assembling messages, communicating with SNMP applications, etc.

To configure the SNMP engineID of the local device, in the global configuration mode, use the following command:

snmp-server engineID *string*

- *string* - Specifies the engineID. The length is 1 to 23 characters.

Creating an SNMPv3 User Group

To configure a SNMPv3 user group, in the global configuration mode, use the following command:

snmp-server group *group-name* **v3** {**noauth** | **auth** | **auth-enc**} [**read-view** *read-view*] [**write-view** *writeview*]

- *group-name* - Specifies a name for the user group. The value range is 1 to 31 characters.
- **noauth** | **auth** | **auth-enc** - Specifies the security level of the user group. The security level determines the security mechanism used when handling a SNMP packet. **noauth** means no authentication nor encryption; **auth** means it requires MD5 or SHA authentication; **auth-enc** indicates that it uses MD5 or SHA authentication and AES or DES packet encryption.
- **read-view** *read-view* - Specifies the read-only MIB view names of the user group. If this parameter is not specified, all MIB views are none.
- **write-view** *writeview* - Specifies the writable MIB view names of the user group. If this parameter is not specified, all MIB views are none.

The system allows up to five user groups, each of which with a maximum of five users. To delete the specified user group, in the global configuration mode, use the command **no snmp-server group** *group-name*.

Creating an SNMPv3 User

To configure a SNMPv3 user, in the global configuration mode, use the following command:

snmp-server user *user-name* **group** *group-name* **v3 remote** *A.B.C.D/M* [**auth-protocol** {**md5** | **sha**} *auth-pass* [**enc-protocol** {**des** | **aes**} *enc-pass*]]

- **user** *user-name* - Specifies a name for the user. The value range is 1 to 31 characters.

- **group** *group-name* - Specifies a configured user group to the user.
- **remote** *A.B.C.D/M* - Specifies the IP address of the remote management host and network mask.
- **auth-protoco**l {**md5** | **sha**} - Specifies that the user should be authenticated with MD5 or SHA algorithm. If this parameter is not specified, no authentication nor encryption is required for the user.
- **auth-pass** - Specifies authentication password. Use 8 to 40 characters.
- **enc-protocol** {**des** | **aes**} - Specifies that the user is encrypted with DES or AES.
- *enc-pass* - Specifies the encryption password. Use 8 to 40 characters.

The system allows up to 25 users. To delete the specified user, in the global configuration mode, use the command **no snmp-server user** *user-name*.

Configuring the IP Address of the Management Host

To configure the management host' s address, in the global configuration mode, use the following command:

snmp-server host { *ip-address* | *ip-address/mask* | **range** *start-ip end-ip*} {**version** [*1* | *2c*] **community** *string* [**ro** | **rw**] | **version** *3*}

- *ip-address* | *ip-address/mask* | **range** *start-ip end-ip* - Specifies the IP address or IP range of the management host.
- **version** [*1* | *2c*] - Specifies that SNMP version is SNMPv1 (1) or SNMPv2C (2c).
- **community** *string* - Community strings are shared password between the managing process and agent process, therefore, an SNMP packet whose community string does not match that of the security device will be dropped. Specifies the community string (31 characters at most) here and it only works for SNMPv1 and SNMPv2C.
- **ro** | **rw** - Specifies the read and write privileges of community string. The **ro** (read-only) community string can only read MIB; **rw** (read and write) community string can read and change MIB. This is optional. By default, community string has read-only privilege.
- **version** *3* - Specifies that the SNMP version is version 3.

To delete the specified management host, in the global configuration mode, use the command **no snmp-server host** {*host-name* | *ip-address* | *ip-address/mask* | **range** *start-ip end-ip*}.

Configuring Recipient of SNMP Trap

To configure the recipient of the SNMP trap packets, in the global configuration mode, use the following command:

snmp-server trap-host { *host-ip*} {**version** {*1* | *2c*} **community** *string* | **version** *3* **user** *user-name* **engineID** *string* } [**port** *port-number*]

- *host-ip* - Specifies the IP address of SNMP trap recipient.
- **port** *port-number* - Specifies the SNMP version used to send trap packets. It can be SNMPv1 or SNMPv2C.
- **version** {*1* | *2c*} - Specifies to use SNMPv3 to send trap packets.
- **community** *string* - Specifies the community string of SNMPv1 or SNMPv2C.
- **version** *3* - Specifies the SNMPv3 user name.
- **user** *string* - Specifies the engineID of trap recipient.
- **engineID** *string* - Specifies the engineID of trap recipient.
- **port** *port-number* - Specifies the recipient host port number. The value range is 1 to 65535.The default value is 162.

To delete the specified trap recipient host, in the global configuration mode, use the command **no snmp-server trap-host** {*host-name* | *ip-address*}.

Configuring sysContact

sysContact specifies the contact name for this managed device (here refers to the security device), as well as information about how to contact this person.

To configure a sysContact, in the global configuration mode, use the following command:

snmp-server contact *string*

- *string* - Specifies the contact string. You can specify up to 255 characters.

To delete the contact, in the global configuration mode, use the command **no snmp-server contact**.

Configuring sysLocation

sysLocation specifies the physical location of this managed device (here refers to the security device).

To configure sysLocation, in the global configuration mode, use the following command:

snmp-server location *string*

- *string* - Specifies the location string. You can specify up to 255 characters.

To delete the sysLocation, in the global configuration mode, use the command **no snmp-server location**.

Specifying the VRouter on Which the SNMP is Enabled

You can specify the VRouter on which the SNMP function is enabled. To specify the VRouter, in the global configuration mode, use the following command:

snmp-server vrouter *vrouter-name*

- *vrouter-name* – Specifies the name of the VRouter.

To disable the SNMP function in the VRouter, in the global configuration mode, use **no snmp-server vrouter**.

Configuring SNMP Server

You can configure the SNMP server to get the ARP information through the SNMP protocol. To configure the SNMP server, in the global configuration mode, use the following command:

arp-mib-query server *ip-address* **community** *string* [**vrouter** *vrouter-name*] [**source** *interface-name*] [**port** *port-number*] [**interval** *value*]

- *ip-address* – Specifies the IP address of SNMP server.
- **community** *string* – Specifies the community string (31 characters at most) here and it only works for SNMPv1 and SNMPv2C.
- **vrouter** *vrouter-name* – Specifies the name of VRouter.
- **source** *interface-name* – Specifies the name of the source interface for receiving ARP information on the SNMP server.
- **port** *port-number* – Specifies the port number of SNMP server. The value range is 1 to 65535, the default value is 161.
- **interval** *value* – Specifies the interval for receiving ARP information on the SNMP server. The value range is 5 to 1800 seconds, the default value is 60 seconds.

To delete the SNMP server, use the command **no arp-mib-query server** *ip-address*.

Clearing the ARP Table Information of SNMP Server

To clear the ARP table information of SNMP server, in any mode, use the following command:

clear arp-mib-query

Viewing the SNMP Server Information

To view SNMP server information, in any mode, use the following commands:

- Show SNMP server status: **show snmp-server**
- Show the ARP table information of the SNMP server: **show snmp-group**
- Show SNMP server configurations: **show snmp-user**

Viewing SNMP Information

To view SNMP configurations, in any mode, use the following commands:

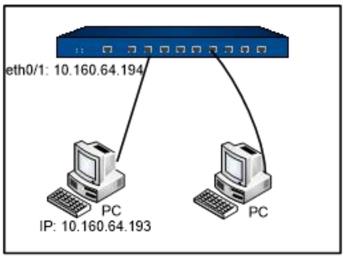
- Show SNMP configurations: **show arp-mib-query status**
- Show SNMP configurations: **show arp-mib-query table** [*ip-address*]
- Show SNMP configurations: **show configuration arp-mib-query**

SNMP Configuration Examples

This section provides two SNMP configuration examples.

Requirements

The goal is to connect the NMS (PC with IP address 10.160.64.193) to a security device on interface eth0/1 (IP: 10.160.64.194), as shown below:



- Example 1: Use NMS (PC of 10.160.64.193) to manage the security device through SNMPv2C with community string "public". In addition, the device is allowed to send trap packets to NMS with community string "private".
- Example 2: Use PC of IP 10.160.64.193 to manage the security device through SNMPv3, with security level of MD5 authentication (password: password1) and DES encryption (password: password2). PC can read MIB-II and only has the right to modify usm MIB. Besides, the security device is allowed to send trap packets.

Example 1

Take the following steps:

Step 1: Configure the security device:

To enter the global configuration mode:

```
hostname# configure
```

To enable the SNMP service on the interface:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# manage snmp
```

To enable SNMP of the device:

```
hostname(config)# snmp-server manager
```

To configure community and access privilege:

```
hostname(config)# snmp-server host 10.160.64.193 version 2c community public ro
```

To configure sysContact and sysLocation:

```
hostname(config)# snmp-server contact cindy-Tel:218
hostname(config)# snmp-server location Hostname-Network
```

To allow sending trap packets to NMS 10.160.64.193 with community string "private":

```
hostname(config)# snmp-server trap-host 10.160.64.193 version 2c community private
```

Step 2: Configure Network Management System (NMS).

Example 2

Step 1: Configure the security device:

To enter the global configuration mode:

```
hostname# configure
```

To enable the SNMP service on the interface:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# manage snmp
```

To enable SNMP of the device:

```
hostname(config)# snmp-server manager
```

To configure the local engineID:

```
hostname(config)# snmp-server engineID FS
```

To specify that the NMS can only read MIB-II but has write privilege over usm MIB:

```
hostname(config)# snmp-server group group1 v3 auth-enc read-view mib2 write-view usm
```

To specify user with MD5 authentication and DES encryption:

```
hostname(config)# snmp-server user user1 group group1 v3 remote 10.160.64.193 auth md5 password1 enc des password2
```

To configure address of NMS:

```
hostname(config)# snmp-server host 10.160.64.193 version 3
```

To configure trap recipient host so that it can send trap packets to NMS:

```
hostname(config)# snmp-server trap-host 10.160.64.193 version 3 user user1 engineID remote-engineid
```

To configure sysContact and sysLocation:

```
hostname(config)# snmp-server contact cindy-Tel:218
hostname(config)# snmp-server location Hostname-Network
```

Step 2: Configure Network Management System (NMS).

Network Time Protocol (NTP)

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of operating systems based on UDP with dedicated port 123.

Tip: For more information about NTP synchronization, see RFC1305.

For a security device, system time influences many functional modules, like VPN tunnel, schedule and signature certificate, etc. NTP is used to synchronize the system time with NTP server. There are two ways to synchronize time: manual setting and using NTP.

Note:When using the signature license for the first time, do synchronize the system time with the computer time in advance.

Configuring NTP

Configuring System Clock Manually

To configure the system clock manually, in the global configuration mode, use the following command:

clock time *HH:MM:SS Month Day Year*

- *HH:MM:SS Month Day Year* - Specifies the system clock. *HH, MM* and *SS* indicate hour, minute and second respectively, *Month*, *Day* and *Year* indicate month, day and year respectively.

Configuring Time Zone Manually

The system provides multiple predefined time zone. To configure time zone more accurately, you can configure a customized time zone, and configure summer time for the customized time zone.

The default time zone of the system is GMT+8. To configure a time zone, in the global configuration mode, use the following command:

clock zone {*timezone-name* | *cus-timezone-name hours minutes*}

- *timezone-name* - Specifies the name of the pre-efined time zone.
- *cus-timezone-name* - Specifies the name of customized time zone. The value range is 1 to 6 characters.
- *hours minutes* - Specifies the offset to UTC (Universal Time Coordinated). The value range of *hours* is -13 to 12; the value range of *minutes* is 0 to 59.

For example, to configure a customized time zone named test, and set the offset to UTC to 6 hours and 30 minutes, use the following command:

```
hostname(config)# clock zone test 6 30
```

Configuring Summer Time

Summer time is a local time regulation for saving energy. According to the law issued by the authority, during summer the clock will jump forward for one hour, and will jump backward for one hour when the summer ends. You can specify the absolute time period and the periodic time period of the summer time for the customized time zone.

To specify the absolute time period of the summer time, in the global configuration mode, use the following command:

clock summer-time *cus-timezone-name* **date** *start-date start-time end-date end-time* [*compensation-time*]

- *cus-timezone-name* - Specifies the name of customized time zone. The value range is 1 to 6 characters.
- **date** – Specifies the absolute time period of the summer time.

- *start-date* - Specifies the start date of summer time. The format is month/day/year, for example, 7/20/2011.
- *start-time* - Specifies the start time of summer time. The format is hour:minute, for example, 10:30.
- *end-date* - Specifies the end date of summer time. The format is month/day/year, for example, 7/20/2011.
- *end-time* - Specifies the end time of summer time. The format is hour:minute, for example, 10:30.
- *compensation-time* − Specifies the compensation time when the summer time starts. The default value is 0. For example, when the summer time starts, in some places the clock will jump forward for 1 hour and 30 minutes; when the summer time ends, the clock will jump backward for 1 hour and 30 minutes. In such a case, the compensation time is 1 hour and 30 minutes. The format is hour:minute, such as 1:30.

For example, to configure a customized time zone named test, set the start time and end time of summer time to 6/22/2011 10:30 and 9/23/2011 10:00 respectively, and the summer time is 2 hours and 30 minutes earlier than the non-summer time, use the following command:

```
hostname（config）# clock summer-time test date 6/22/2011 10:30 9/23/2011 10:00 2:30
```

To specify the periodical time period of the summer time, i.e. executing the summer time in a specified time period in every year, in the global configuration mode, use the following command:

clock summer-time *cus-timezone-name* **recurring** { [**Mon**] |[···] | [**Sun**] }{**after** | **before**}*start-day start-month start-time* { [**Mon**] |[···] |[**Sun**]} {**after** | **before**}*end-day end-month end-time* [**compensation-time**]

- *cus-timezone-name* − Specifies the name of customized time zone. The value range is 1 to 6 characters.
- **recurring** − Specifies the periodical time period of the summer time.
- { [**Mon**] |[···] | [**Sun**] }{**after** | **before**}*start-day start-month start-time* − Specifies the start time of the periodical time period. For example, Mon before 22 6 10:30 means the start time of the summer time in every year is 10:30 on the Monday of the first week before 22nd, June.
- { [**Mon**] |[···] |[**Sun**]} {**after** | **before**}*end-day end-month end-time* - Specifies the end time of the periodical time period. For example, Fri after 23 9 10:00 means the end time of the summer time in every year is 10:00 on the Friday of the first week after 23rd, September.

- *compensation-time* – Specifies the compensation time of the summer time when the summer time takes effect. The default value is 0. For example, when the summer time starts, the system adjust the time of certain zones 1.5 hours ahead, and when the summer time ends, adjust the time of certain zones 1.5 hours back. 1.5 hours is the compensation time you defined. The format is "hour:minute", for example, 1:30.

For example, to configure a customized time zone named test, set the start time as 10:30 on the Monday of the first week before 22nd, June and set the end time as 10:00 on the Friday of the first week after 23rd, September. The time during the summer time is 2.5 hours ahead.

```
hostname（config）# clock summer-time test recurring Mon before 22 6 10:30 Fri after 23 9 10:00 2:30
```

Note:The summer time may affect logs and modules that rely on time. For example, in the above example, when the summer time ends on 9/23/2011 10:00, the clock will jump backward for 2 hours and 30 minutes, i.e., jump backward to 7:30. Therefore, time range from 7:30 to 10:00 will appear twice on 9/23/2011.

To cancel the summer time configuration, in the global configuration mode, use the command **no clock summer-time** *cus-timezone-name* **date**.

Viewing System Clock Configuration Information

To view the time zone settings, in any mode, use the command **show clock**.

To view the summer time settings, in any mode, use the command **show config**.

Configuring NTP Service

NTP is used to synchronize the system clock with NTP server. The system supports the following NTP configurations:

- Enabling/Disabling NTP Service
- Configuring an NTP Sever
- Configuring the Max Adjustment Value
- Configuring the Query Interval
- Enabling/Disabling NTP Authentication
- Configuring NTP Authentication

Enabling/Disabling NTP Service

By default, NTP service on FS devices is disabled.

To enable/disable NTP service, in the global configuration mode, use the following commands:

- Enable: **ntp enable**
- Disable: **no ntp enable**

Configuring an NTP Server

You can specify up to three NTP servers, one of which with keyword "prefer" is the primary NTP server, or, if no "prefer" is specified, the earliest configured NTP server is the first one for time synchronization.

To configure an NTP server, in the global configuration mode, use the following command:

ntp server {*ip-address* | *host-name*} [**key** *number*] [**source** *interface-name*] [**prefer**] [**vrouter** *vrouter-name*]

- *ip-address* | *host-name*- Specifies the IP address or host name of the NTP server. The length of the host name can be 1 to 127 characters.
- **key** *number* - Specifies the password of the NTP server if it requires so.
- **source** *interface-name* - Specifies the interface on which the security device sends and receives NTP packets.
- **prefer**- If more than one NTP servers are specified, use this keyword to determine the primary server.
- *vrouter-name* - Specifies NTP server for the specified VRouter.

To cancel the NTP server settings, use the command **no ntp server** {*ip-address* | *host-name*}.

Here is an example of configuring a NTP server:

```
hostname(config)# ntp server 10.160.64.5 prefer
```

Configuring the Max Adjustment Value

The maximum time adjustment value represents the acceptable time difference between the device system clock and the time received from an NTP server. The device only adjusts its clock with the NTP server time if the time difference between its clock and the NTP server time is within the maximum time adjustment value.

To set the maximum adjustment value, in the global configuration mode, use the following command:

ntp max-adjustment *time-value*

- *time-value* - Specifies the time value. The value range is 0 to 3600 seconds. The value of 0 means no adjustment time. The default value is 10.

To restore to the default value, use the command **no ntp max-adjustment**.

Configuring the Query Interval

The device updates its clock with NTP servers at intervals of the value you set here.

To configure the query interval, in the global configuration mode, use the following command:

ntp query-interval *time-interval*

- *time-interval* - The query interval. The value range is 1 to 60 minutes. The default value is 5.

To restore to the default value, use the command **no ntp query-interval**.

Enabling/Disabling NTP Authentication

By default, NTP authentication is disabled.

To enable/disable NTP authentication, in the global configuration mode, use the following commands:

- Enable: **ntp authentication**
- Disable: **no ntp authentication**

Configuring NTP Authentication

If you choose to use NTP authentication, the security device only interact with servers that pass the authentication.

To configure NTP authentication key ID and key, in the global configuration mode, use the following command:

ntp authentication-key *number* **md5** *string*

- *number* - Specifies the key ID number. The value range is 1 to 65535.
- *string* - Specifies MD5 authentication key. The length is 1 to 31 characters.

To cancel the authentication private key settings, in the global configuration mode, use the command **no ntp authentication-key** *number*.

Viewing NTP Status

To view the current NTP configurations, in any mode, use the command **show ntp status**.

NTP Configuration Example

Requirements of this configuration example are:

- NTP server IP address is 10.10.10.10;
- Authentication private key ID and key are 1 and aaaa respectively;
- The query interval is 3 minutes;
- The maximum adjustment time is 5 seconds.

Configure the following commands on the device:

```
hostname(config)# ntp authentication-key 1 md5 aaaa
hostname(config)# ntp server 10.10.10.10 key 1 prefer
hostname(config)# ntp query-interval 3
hostname(config)# ntp max-adjustment 5
hostname(config)# ntp authentication
hostname(config)# ntp enable
hostname(config)# show ntp status
ntp client is enabled, authentication is enabled
ntp query-interval is 3, max-adjustment time is 5
ntp server 10.10.10.10, key 1, prefer
```

Configuring Schedule

Schedules control the effective time for some functional modules, such as allowing a policy rule to take effect in a specified time, and controls the duration for the connection between a PPPoE interface and Internet. There are two types of schedule: periodic schedule and absolute schedule. The periodic schedule specifies a time point or time range by periodic schedule entries, while the absolute schedule decides a time range in which the periodic schedule will take effect.

Creating a Schedule

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

schedule *schedule-name*

- *schedule-name* - Specifies a name for the schedule. The length of it can be 1 to 31 characters.

This command creates a schedule and leads you into the schedule configuration mode; if the schedule exists, you will enter its configuration mode directly.

To delete a schedule, use the command **no schedule** *schedule-name*. Note that you should unbind the schedule from all the functional modules before deleting it.

Configuring an Absolute Schedule

Absolute schedule is a time range in which periodic schedule will take effect. If no absolute schedule is specified, the periodic schedule will take effect as soon as it is referenced by any module.

To configure an absolute schedule, in the schedule configuration mode, use the following command:

absolute {[**start** *start-date start-time*] [**end** *end-date end-time*]}

- **start** *start-date start-time* - Specifies the start date and time. *start-date* specifies the start date in the format of month/date/year, e.g. 10/23/2007; *start-time* specifies the start time in the format of hour:minute, e.g. 15:30. If this parameter is not specifies, it uses the present time.
- **end** *end-date end-time* - Specifies the end date and time. *end-date* specifies the finish date in the format of month/date/year, e.g. 11/05/2007; *end-time* specifies the finish time in the format of hour:minute, e.g. 09:00. If the parameters are not specifies, there is no end time for the absolute time.

To disable absolute schedule, use the command **no absolute**.

Configuring a Periodic Schedule

A periodic schedule is the collection of all the schedule entries within the schedule. You can add up to 16 schedule entries to a periodic schedule. These entries can be divided into three types:

- Daily: The specified time of every day, such as Everyday 09:00 to 18:00.
- Days: The specified time of a specified day during a week, such as Monday Tuesday Saturday 09:00 to 13:30.
- Due: A continuous period during a week, such as from Monday 09:30 to Wednesday 15:00.

To specify a periodic schedule, in the schedule configuration mode, use the following command:

periodic {**daily** | **weekdays** | **weekend** | [**monday**] [···] [**sunday**]} *start-time* **to** *end-time*

- **daily** To specify a periodic schedule, in the schedule configuration mode, use the following command:
- **weekdays** - Workday (from Monday to Friday).
- **weekend** - Weekends (Saturday and Sunday).
- [**monday**] [···] [**sunday**] - Specifies particular days. For example, if you want Tuesday, Wednesday and Saturday, type the key words tuesday wednesday saturday.
- *start-time* - Specifies the start time in the format of hour:minute, e.g. 09:00.
- *end-time* - Specifies the end time in the format of hour: minute, e.g. 16:30.

Repeat the command to add more entries.

To delete a periodic entry, use the command **no periodic** {**daily** | **weekdays** | **weekend** | [**monday**] [···] [**sunday**]} *start-time* **to** *end-time*.

To configure an entry which specifies a period of time in a week, in the schedule configuration mode, use the following command:

periodic {[**monday**] | [···] | [**sunday**]} *start-time* **to** {[**monday**] | [···] | [**sunday**]} *end-time*

- [**monday**] | [···] | [**sunday**] - Specifies the start day in a week.
- *start-time* - Specifies the start time in the format of hour:minute, e.g. 09:00.
- [**monday**] | [···] | [**sunday**] - Specifies the end day.
- *end-time* - Specifies the end time in the format of hour:minute, e.g. 16:30.

Repeat this command to add more entries.

To delete an entry, use the command **no periodic** {[**monday**] | [···] | [**sunday**]} *start-time* **to** {[**monday**] | [···] | [**sunday**]} *end-time*.

Configuring a Track Object

Track object is used to track if the specified object (IP address or host) is reachable and if the specified interface is connected, and if the specified object or link is congested. If the object is not reachable or the link is not connected, the system will directly conclude the track fails; if the object is reachable or the link is connected, the system will continue to detect if the object or link is congested based on packet delay or interface bandwidth. Track is mainly used in HA, PBR, LLB scenarios. By configuring track, you can assure the system is always selecting a comparatively healthy link.

Note:

- When the track failed, the system will drop all the sessions to the track object.
- When the track object is congested, the system will still keep all the existing sessions to the object, but will not allow any new session.

To configure a track object, in the global configuration mode, use the following command:

track *track-object-name* [**local**]

- *track-object-name* - Specifies a name for the track object. The length of it can be 1 to 31 characters.
- **local** - If you enter this parameter, the system will not synchronize configuration of this track with the backup device. Without entering this parameter, this configuration will not be synchronized with the backup device.

This command creates the track object and leads you into the track object configuration mode; if the object exists, you will enter its configuration mode directly.

To delete the specified track object, use the following command:

no track *track-object-name*

You are allowed to track your object by using five protocols of Ping, HTTP, ARP, DNS and TCP. Besides, the object also can be tracked by counting the traffic information of specified interface.

Track by Ping Packets

To track an object using Ping packets, in the object configuration mode, use the following command:

ip {*A.B.C.D* | **host** *host-name*} **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**src-interface** *interface-name* [**prior-used-srcip**]] [**weight** *value*] [**delay high-watermark** *value* **low-watermark** *value*] [**delay-weight** *value*]

- *A.B.C.D* | **host** *host-name* - Specifies the IP address or host name of the tracked object. The length of the host name can be 1 to 63 characters.
- **interface** *interface-name* - Specifies the egress interface sending Ping packets.
- **interval** *value* - Specifies the interval of sending Ping packets . The value range is 1 to 255 seconds. The default value is 3.
- **threshold** *value* - Specifies the number which determines the tracking fails. If the system does not receive response packets of the number specified here, it determines that the tracking has failed, namely, the destination is unreachable. The value range is 1 to 255. The default value is 3.

- **src-interface** *interface-name* - Specifies the source interface of Ping packets.
- **prior-used-srcip** – If the secondary IP is specified for the source interface and specifies the IP to be **prior-used-srcip**, system will use the IP to send track packets priorly. If the parameter is not specified, system will use default IP of the source interface to send track packets.
- **weight** *value* - Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.
- **delay high-watermark** *value* **low-watermark** *value* - Specifies the high watermark and low watermark for the object' s delay in responding Ping packets. The value range is 1 to 65535 milliseconds. When the delay is below the specified high watermark, the system will conclude the link is normal; when the delay exceeds or equals to the specified high watermark, the system will conclude the link is congested; if congestion occurred, the system will not conclude the link restores to normal until the delay is below or equals to the specified low watermark. Such a design can avoid link status' frequent switching between normal and congested.
- **delay-weight** *value* – Specifies how important this link congestion is to the judgment of track object congestion. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more Ping tracking entries.

To delete the specified tracking entry, use the following command:

no ip {*A.B.C.D* | **host** *host-name*} **interface** *interface-name* [**delay**]

Track by HTTP Packets

To track an object using HTTP packets, in the track object configuration mode, use the following command:

http {*A.B.C.D* | **host** *host-name*} **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**src-interface** *interface-name*] [**weight** *value*] [**delay high-watermark** *value* **low-watermark** *value*] [**delay-weight** *value*]

- *A.B.C.D* | **host** *host-name* - Specifies the IP address or host name of the track object. The length of the host name can be 1 to 63 characters.
- **interface** *interface-name* - Specifies the egress interface of sending HTTP test packets.
- **interval** *value* - Specifies the interval of sending HTTP packets. The value range is 1 to 255 seconds. The default value is 3.
- **threshold** *value* - Specifies the number which concludes the tracking fails. If the system does not receive response packets of the number specified here, it concludes that the tracking has failed. The value range is 1 to 255. The default value is 1.

- **src-interface** *interface-name* - Specifies the source interface of the HTTP packets.
- **weight** *value* - Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.
- **delay high-watermark** *value* **low-watermark** *value* - Specifies the high watermark and low watermark for the object's delay in responding HTTP packets. The value range is 1 to 65535 milliseconds. When the delay is below the specified high watermark, the system will conclude the link is normal; when the delay exceeds or equals to the specified high watermark, the system will conclude the link is congested; if congestion occurred, the system will not conclude the link restores to normal until the delay is below or equals to the specified low watermark. Such a design can avoid link status' frequent switching between normal and congested.
- **delay-weight** *value* − Specifies how important this link congestion is to the judgment of track object congestion. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more HTTP tracking entries.

To delete the specified tracking entry, use the following command:

no http {*A.B.C.D* | **host** *host-name*} **interface** *interface-name* [**delay**]

Track by ARP Packets

To track an object using ARP packets, in the track object configuration mode, use the following command:

arp {*A.B.C.D*} **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**weight** *value*]

- *A.B.C.D* - Specifies the IP address of the track object.
- **interface** *interface-name* - Specifies the egress interface of sending ARP test packets.
- **interval** *value* - Specifies the interval of sending ARP packets. The value range is 1 to 255 seconds. The default value is 3.
- **threshold** *value* - Specifies the threshold number which concludes the tracking fails. If the system does not receive response packets of the number specified here, it concludes that the tracking has failed. The value range is 1 to 255. The default value is 3.
- **weight** *value* - Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more ARP tracking entries.

To delete the specified tracking entry, use the following command:

no arp {*A.B.C.D*} **interface** *interface-name*

Track by DNS Packets

To track an object using DNS packets, in the track object configuration mode, use the following command:

dns *A.B.C.D* **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**weight** *value*] [**src-interface** *interface-name*] [**delay high-watermark** *value* **low-watermark** *value*] [**delay-weight** *value*]

- *A.B.C.D* - Specifies the IP address of track object.
- **interface** *interface-name* - Specifies the egress interface of sending DNS test packets.
- **interval** *value* - Specifies the interval of sending DNS packets. The value range is 1 to 255 seconds. The default value is 3.
- **threshold** *value*- Specifies the threshold number which concludes the tracking fails. If the system does not receive response packets of the number specified here, it concludes that the tracking has failed. The value range is 1 to 255. The default value is 3.
- **weight** *value* - Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.
- **src-interface** *interface-name* - Specifies the source interface of DNS test packets.
- **delay high-watermark** *value* **low-watermark** *value* - Specifies the high watermark and low watermark for the object's delay in responding DNS packets. The value range is 1 to 65535 milliseconds. When the delay is below the specified high watermark, the system will conclude the link is normal; when the delay exceeds or equals to the specified high watermark, the system will conclude the link is congested; if congestion occurred, the system will not conclude the link restores to normal until the delay is below or equals to the specified low watermark. Such a design can avoid link status' frequent switching between normal and congested.
- **delay-weight** *value* - Specifies how important this link congestion is to the judgment of track object congestion. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more DNS tracking entries.

To delete the specified tracking entry, use the following command:

no dns *A.B.C.D* **interface** *interface-name* [**delay**]

Track by TCP Packets

To track an object using TCP packets, in the track object configuration mode, use the following command:

tcp {A.B.C.D | **host** *host-name*} **port** *port-number* **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**src-interface** *interface-name*] [**weight** *value*] [**delay high-watermark** *value* **low-watermark** *value*] [**delay-weight** *value*]

- *A.B.C.D* | **host** *host-name* - Specifies the IP address or host name of track object. The length of the host name can be 1 to 63 characters.
- **port** *port-number* - Specifies the destination port of the track object. The value range is 0 to 65535.
- **interface** *interface-name* - Specifies the egress interface for sending TCP test packets.
- **interval** *value* - Specifies the interval of sending TCP packets. The value range is 1 to 255 seconds. The default value is 3.
- **threshold** *value* - Specifies the threshold number which concludes the tracking fails. If the system does not receive response packets of the number specified here, it concludes that the tracking has failed. The value range is 1 to 255. The default value is 3.
- **src-interface** *interface-name* - Specifies the source interface of TCP test packets.
- **weight** *value* - Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.
- **delay high-watermark** *value* **low-watermark** *value* - Specifies the high watermark and low watermark for the object's delay in responding TCP packets. The value range is 1 to 65535 milliseconds. When the delay is below the specified high watermark, the system will conclude the link is normal; when the delay exceeds or equals to the specified high watermark, the system will conclude the link is congested; if congestion occurred, the system will not conclude the link restores to normal until the delay is below or equals to the specified low watermark. Such a design can avoid link status' frequent switching between normal and congested.
- **delay-weight** *value* - Specifies how important this link congestion is to the judgment of track object congestion. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more TCP tracking entries. For one single track object, you cannot configure both the HTTP track on the host and TCP track on port 80 simultaneously.

To delete the specified tracking entry, use the following command:

no tcp {*A.B.C.D* | **host** *host-name*} **port** *port-number* **interface** *interface-name* [**delay**]

Interface Status Track

To track interface status, in the track object configuration mode, use the following command:

interface *interface-name* [**weight** *value*]

- *interface-name* - Specifies the interface name.
- **weight** *value* - Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more tracking entries.

To delete the specified tracking entry, use the following command:

no interface *interface-name*

Interface Bandwidth Track

To track interface bandwidth, in the track object configuration mode, use the following command:

bandwidth interface *interface-name* **direction** {**in** | **out** | **both**} **high-watermark** *value* **low-watermark** *value* [**interval** *value*] [**threshold** *value*] [**weight** *value*]

- *interface-name* - Specifies the interface name.
- **direction** {**in** | **out** | **both**} - Specifies the traffic direction to be tracked. in indicates ingress, out indicates egress (the default direction), both indicates the both directions.
- **high-watermark** *value* **low-watermark** *value* – Specifies the high watermark and low watermark for the interface bandwidth. The value range is 1 to 100000000 kbps. When the interface bandwidth is below the specified high watermark, the system will conclude the link is normal; when the interface bandwidth exceeds or equals to the specified high watermark, the system will conclude the link is congested; if congestion occurred, the system will not conclude the link restores to normal until the interface bandwidth is below or equals to the specified low watermark. Such a design can avoid link status' frequent switching between normal and congested.
- **interval** *value* - Specifies the tracking interval. The value range is 1 to 255 seconds. The default value is 3.
- **threshold** *value* – Specifies the threshold number which concludes the entry is congested. If the system detected interface overload for the times specified here in succession, it concludes the entry is congested. The value range is 1 to 255. The default value is 1.
- **weight** *value* - Specifies how important this link congestion is to the judgment of track object congestion. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more tracking entries.

To delete the specified tracking entry, use the following command:

no bandwidth interface *interface-name*

Interface Quality Track

To track the link state of specified interface by counter the sampling traffic , in the track object configuration mode, use the following command:

traffic-condition interface *interface-name* [**condition-threshold** *low-watermark high-watermark*] [**interval** *value*] [**threshold** *value*] [**weight** *value*]

- *interface-name* － Specifies the tracked interface name.
- **condition-threshold** *low-watermark high-watermark* － Specifies the threshold value of new session success rate. By default, the threshold low watermark is 30, and the threshold high watermark is 50. The value range is 0 to 100. During a track period, when the new session success rate is below the specified low watermark, system will conclude the track is failed; when the new session success rate exceeds the specified high watermark, system will conclude the track is successful; when the new session success rate is equal to or exceeds the low watermark, and equal to or below the low watermark, system will keep the previous track state.
- **interval** *value* － Specifies the duration of per track period. The unit is second. The value range is 1 to 255. The default value is 3. After a track period is finished, system will reset the tracked value of new session.
- **threshold** *value* － Specifies the threshold value which concludes the track entry is failed. The value range is 1 to 255. The default value is 3.
- **weight** *value* － Specifies how important this track failure is to the judgment of track object failure. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more tracking entries.

To delete the specified tracking entry, use the following command:

no traffic-condition interface *interface-name*

Configuring a Threshold

Threshold is used to conclude if the track object failed or is congested. When the total weight sum of the track entries that belong to the same category in the track object exceeds or equals to the corresponding threshold, the system will conclude the track object failed or is congested.

Monitor Object Failure Threshold

If the sum of weight values of all track entries exceeds or equals to a certain value, the system concludes that the tracking fails. The value is known as the track object failure threshold value.

To configure the track object failure threshold value, in the track object configuration mode, use the following command:

threshold *value*

- *value* - Specifies the threshold value. The value range is 1 to 255. The default value is 255.

To restore to the default threshold value, in the track object configuration mode, use the following command:

no threshold

Monitor Alarm

The monitor alarm function is designed to monitor the utilization of system resources, and issue an alarm according to the configuration. The current version supports log and SNMP Trap alarms.

You need to enter the monitor configuration mode to configure the monitor alarm function. To enter the monitor configuration mode, in the global configuration mode, use the following command:

monitor

After entering the monitor configuration mode, you can configure a monitor rule as needed for the system resource object:

{**cpu** | **memory utilization** | **interface-bandwidth** *interface-name* **utilization** | **log-buffer** { **config** | **event** | **ips** | **network** | **security** | **traffic**{**session** | **nat** | **urlfilter**}} **utilization** | **policy utilization** | **session utilization** | **snat-resource utilization**} **interval** *interval-value* **absolute rising-threshold** *threshold-value* **sample-period** *period-value* [**count** *count-value*] {**log** [***snmp-trap***] | **snmp-trap**}

- **cpu** | **memory utilization** | **interface-bandwidth** *interface-name* **utilization** | **log-buffer** { **config** | **event** | **ips** | **nbc** | **network** | **security** | **traffic** {**session** | **nat** | **urlfilter**}} **utilization** | **policy utilization** | **session utilization** | **snat-resource utilization** - Specifies the monitor object which can be **cpu**, **memory**, **interface-bandwidth**, **log-buffer**, **policy**, **session** or **snat-resource**. When you use the X platforms and enter the cpu keyword, proceed to select modules.
  - *interface-name* - Specifies the name of interface.
  - **config** | **event** | **ips** | **network** | **security** | **traffic** {**session** | **nat** | **urlfilter**} - Specifies the log type.

- **utilization** - Specifies the value of monitor object as the utilization of each object. Since the default value for **cpu** is utilization, so you do not need to specify this parameter for the monitor object of CPU.

- **interval** *interval-value* - Specifies the monitor interval, i.e., the interval for acquiring the value of monitor object within the sampling period (**sample-period** *period-value*). The value range is 3 to 10 seconds.
- **absolute** - Specifies the value of monitor object as an absolute value.
- **rising-threshold** *threshold-value* - Specifies the rising threshold. The system will issue an alarm if the value of monitor object exceeds the percentage specified here. The value range is 1 to 99.
- **sample-period** *period-value* - Specifies the sample period. The value range is 30 to 3600 seconds.
- **count** *count-value* - Specifies the count for the conditions the value of monitor object exceeds the **rising-threshold** within the sampling period (**sample-period**). The value range is 1 to 1000. If this parameter is configured, when the count exceeds the **rising-threshold** within the sampling period, the system will issue an alarm; if this parameter is not configured, when the average value of monitor object exceeds the **rising-threshold**, the system will issue an alarm.
- **log** [**snmp-trap**] | **snmp-trap** - Specifies the method which can be **log**, **snmp-trap** or **both**.

For example:

To configure the peak CPU utilization monitor:

```
hostname(config)# monitor
hostname(config-monitor)# cpu interval 5 absolute rising-threshold 65 sample-period 600 count 50 log
```

After the configuration, if the CPU utilization exceeds the rising threshold of 65% within 600 seconds, and such a condition occurs at least 50 times, then the system will issue a log.

To configure the average session utilization monitor:

```
hostname(config)# monitor
hostname(config-monitor)# session utilization interval 8 absolute rising-threshold 90 sample-period 600 log
```

After the configuration, if the average session utilization exceeds the rising threshold of 90% within 600 seconds, then the system will issue a log.

To delete the specified monitor rule, in the monitor configuration mode, use the following command:

no {**cpu** | **memory utilization** | **interface-bandwidth** interface-name **utilization** | **log-buffer** { **config** | **event** | **ips** | **network** | **security** | **traffic** {**session** | **nat** | **urlfilter**}} **utilization** | **policy utilization** | **session utilization** | **snat-resource utilization**}

Note:

- For every monitor object, only the last configured monitor rule takes effect.
- The system does not support monitor alarm for port resources whose IP address is translated into an egress IP address (eif-ip) after SNAT.

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

show monitor

The Maximum Concurrent Sessions

If multi-VR, AV, IPS and/or URL signature database is enabled on FS devices, or IPv6 firmware version is used, the maximum concurrent sessions might change. For more information, see the table below:

Platform	Firmware	Max Concurrent Sessions
NSG-3100 NSG-5100 NSG-8100	FSOS IPv4 version	• With multiple virtual routers enabled: the maximum concurrent sessions will drop by 15%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions*(1-0.15); • With anti-virus, IPS and/or URL signature database enabled: the maximum concurrent sessions will drop by 50%. The formula is: Actual maximum sessions*(1-0.15)*(1-0.5).concurrent sessions =

Platform	Firmware	Max Concurrent Sessions
		original maximum concurrent sessions*(1-0.5); • With multiple virtual routers plus anti-virus, IPS and/or URL signature database enabled simultaneously, the maximum concurrent sessions will further drop by 50%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions*(1-0.15)*(1-0.5).
	FSOS IPv6 version	The maximum concurrent sessions is 50% of the IPv4 version. IPv6 version does not support multiple virtual routers, anti-virus, IPS and URL signature database.

Chapter 5 Virtual System (VSYS)

Virtual systems (VSYS) divide a physical device into multiple logical virtual firewalls. Each VSYS has its own system resources, performs most of the firewall functionalities, working as a completely independent firewall. VSYSs cannot communicate directly from each other.

VSYS has the following characters:

- Each VSYS has its own administrators;
- Each VSYS has independent virtual routers, zones, address book, service book, etc;
- Each VSYS has independent physical and logical interfaces;
- Each VSYS has independent policy rules.
- Each VSYS has independent logs.

The supported default VSYS number varies from different platforms. You can expand the number by purchasing and installing the license.

VSYS Objects

This section describes VSYS objects, including root VSYS, non-root VSYS, administrator, VRouter, VSwitch, zone, and interface.

Root VSYS and Non-root VSYS

The system contains only one root VSYS which cannot be deleted. You can create or delete non-root VSYSs after installing a VSYS license and rebooting the device. When creating or deleting non-root VSYSs, you must follow the rules listed below:

- When creating or deleting non-root VSYSs through CLI, you must be under the root VSYS configuration mode.
- Only the root VSYS administrators and root VSYS operators can create or delete non-root VSYS. For more information about administrator permissions, see "Administrator" .
- When creating a non-root VSYS, the following corresponding objects will be created simultaneously:
- A non-root VSYS administrator named admin. The password is *vsys_name-admin.*
  - A VRouter named vsys_name-vr.

  - A L3 zone named vsys_name-trust.

  For example, when creating the non-root VSYS named vsys1, the following objects will be created:

  - The non-root administrator named admin with the password vsys1-admin.
  - The default VRouter named vsys1-vr.
  - The L3 zone named vsys1-trust and it is bound to vsys1-vr automatically.

- When deleting a non-root VSYS, all the objects and logs in the VSYS will be deleted simultaneously.
- The root VSYS contains a default VSwitch named VSwitch1, but there is no default VSwitch in a newly created non-root VSYS. Therefore, before creating l2 zones in a non-root VSYS, a VSwitch must be created. The first VSwitch created in a non-root VSYS will be considered as the default VSwitch, and the l2 zone created in the non-root VSYS will be bound to the default VSwitch automatically.

Administrator

The admin users of each VSYS are independent from other VSYS. VSYS admin users also have different roles of Administrator, Administrator-ready-only, operator and auditor. Their roles and previleges are the same with normal admin users.

When creating VSYS administrators, you must follow the rules listed below:

- Backslash (\) cannot be used in administrator names.
- The non-root administrators are created by root administrators or root operators after logging into non-root VSYS.
- After logging into root VSYS, the root administrators can switch to non-root VSYS and configure it.
- Non-root administrators can enter the corresponding non-root VSYS after the successful login, but the non-root administrators cannot switch to the root VSYS.
- Each administrator name should be unique in the VSYS it belongs to, while administrator names can be the same in different VSYSs. In such a case, when logging in, you must specify the VSYS the administrator belongs to in the format of vsys_name\admin_name. If no VSYS is specified, you will enter the root VSYS.

Table below shows the permissions to different types of VSYS administrators.

Operation	Permissions							
	Root VSYS Adminisrator	Root VSYS Adminisrator-read-only	Root VSYS Operator	Root VSYS Auditor	Non-root VSYS Adminisrator	Non-root VSYS Administrator-read-only	Non-root VSYS Operator	Non-root VSYS Auditor
Configure (including save configuration)	√	χ	√	χ	√	χ	√	χ
Managing admin users	√	χ	χ	χ	√	χ	χ	χ
Restore factory default	√	χ	χ	χ	χ	χ	χ	χ
Delete configuration file	√	χ	√	χ	√	χ	√	χ
Roll back configuration	√	χ	√	χ	√	χ	√	χ
Reboot	√	χ	√	χ	χ	χ	χ	χ
View configuration information	√	√	√	χ	View info in current VSYS	View info in current VSYS	View info in current VSYS	χ
View log information	√	√	χ	√	√	√	χ	√
Modify current admin password	√	√	√	√	√	√	√	√
Command import	√	χ	√	χ	√	χ	√	χ
Command export	√	√	√	√	√	√	√	√
Command clear	√	√	√	√	√	√	√	√
Command	√	√	√	χ	√	√	√	χ

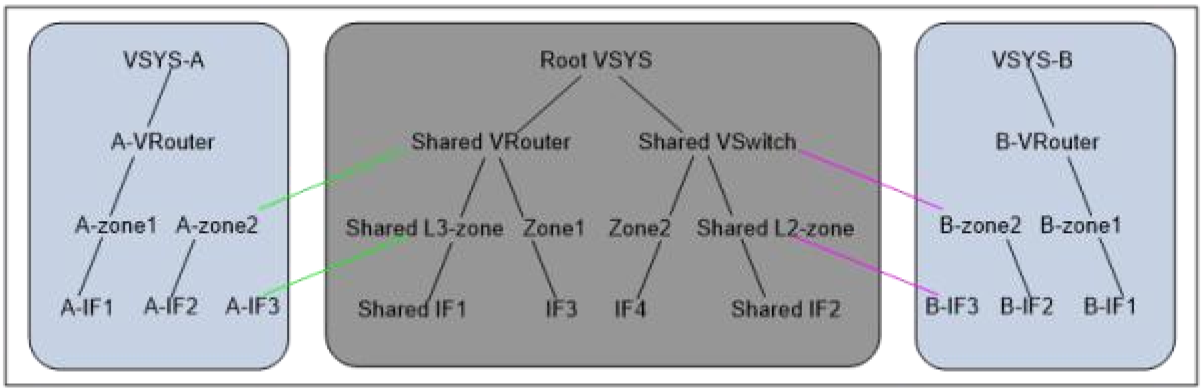
Operation	Permissions							
	Root VSYS Adminisrator	Root VSYS Adminisrator-read-only	Root VSYS Operator	Root VSYS Auditor	Non-root VSYS Adminisrator	Non-root VSYS Adminisrator-read-only	Non-root VSYS Operator	Non-root VSYS Auditor
ping/traceroute								
Command debug	√	√	√	χ	χ	χ	χ	χ
Command exec	√	√	√	√	√	√	√	√
Command terminal width	√	√	√	√	√	√	√	χ

VRouter, VSwitch, Zone, Interface

VRouter, VSwitch, zone, and interface in VSYS have two properties which are shared and dedicated. Objects with dedicated property are dedicated objects, while doing specific operations to the object with the shared property will make it a shared object. The dedicated object and shared object have the following characters:

- **Dedicated object:** A dedicated object belongs to a certain VSYS, and cannot be referenced by other VSYSs. Both root VSYS and non-root VSYS can contain dedicated objects.
- **Shared object:** A shared object can be shared by multiple VSYSs. A shared object can only belong to the root VSYS and can only be configured in the root VSYS. A non-root VSYS can reference the shared object, but cannot configure them. The name of the shared object must be unique in the whole system.

Figure below shows the reference relationship among dedicated and shared VRouter, VSwitch, zone, and interface.



As shown in the figure above, there are three VSYSs in FSOS: Root VSYS, VSYS-A, and VSYS B. Root VSYS contains shared objects (including Shared VRouter, Shared VSwitch, Shared L3-zone, Shared L2-zone, Shared IF1, and Shared IF2) and dedicated objects.

VSYS-A and VSYS-B only contain dedicated objects. The dedicated objects VSYS-A and VSYS-B can reference the shared objects in Root VSYS. For example, A-zone2 in VSYS-A is bound to the shared object Shared VRouter in Root VSYS, and B-IF3 in VSYS-B is bound to the shared object Shared L2-zone in Root VSYS.

Shared VRouter

A shared VRouter contains the shared and dedicated L3 zones of the root VSYS. Bind a L3 zone to a shared VRouter and configure this L3 zone to have the shared property. Then this zone becomes a shared zone.

Shared VSwitch

A shared VSwitch contains the shared and dedicated L2 zones of the root VSYS. Bind a L2 zone to a shared VSwitch and configure this L2 zone to have the shared property. Then this zone becomes a shared zone.

Shared Zone

The shared zones consist of L2 shared zones and L3 shared zones. After binding the L2 zone with the shared property to a shared VSwitch, it becomes a shared L2 zone; after binding the L3 zone with the shared property to a shared VRouter, it becomes a shared L3 zone. A shared zone can contain interfaces in both root VSYS and non-root VSYS. All function zones cannot be shared.

Shared Interface

After binding an interface in the root VSYS to a shared zone, it becomes a shared interface automatically.

Interface Configuration

Only RXW administrator in the root VSYS can create or delete interfaces. Configurations to an interface and its sub-interfaces must be performed in the same VSYS.

Configuring VSYS

VSYS configurations include:

- Creating a Non-root VSYS
- Creating a VSYS Profile
- Entering the VSYS
- Configuring the Shared Property
- Exporting a Physical Interface
- Allocating a Logical Interface
- Configuring VSYS Log
- Configuring Cross-VSYS Traffic Forwarding

Creating a Non-root VSYS

The root administrator can create non-root VSYS. To create a non-root VSYS, in the global configuration mode of the root VSYS, use the following command:

vsys *vsys-name*

- *vsys-name* - Specifies the name of the VSYS to be created. It is a string composed of 1 to 23 characters. The word **root** cannot be configured and the backslash (\) cannot be used in the specified name.

After executing the command, the system creates a non-root VSYS with the specified name and enters the configuration mode of the created non-root VSYS. If the specified name exists, the system enters the configuration mode of the non-root VSYS directly.

To delete the specified non-root VSYS, in the global configuration mode of the root VSYS, use the following command:

no vsys *vsys-name*

Creating a VSYS Profile

VSYSs work independently in functions but share system resources including concurrent sessions, zone number, policy rule number, SNAT rule number, DNAT rule number, session limit rules number, memory buffer, URL resources and IPS resources. You can specify the reserved quota and maximum quota for each type of system resource in a VSYS by creating a VSYS profile. Reserved quota refers to the resource number reserved for the VSYS; maximum quota refers to the maximum resource number available to the VSYS. The root administrator has the permission to create VSYS profiles. The total for each resource of all VSYSs cannot exceed the system capacity.

To create a VSYS profile, in the global configuration mode of the root VSYS, use the following command:

vsys-profile *vsys-profile-name*

- *vsys-profile-name* - Specifies the name of the VSYS profile to be created. It is a string composed of 1 to 31 characters.

After executing the command, the system creates a VSYS profile with the specified name and enters the configuration mode of the created VSYS profile. If the specified name exists, the system enters the configuration mode of the VSYS profile directly.

To delete the specified VSYS profile, in the global configuration mode of the root VSYS, use the following command:

no vsys-profile *vsys-profile-name*

Note:

- Up to 128 VSYS profiles are supported.
- The default VSYS profile of the root VSYS named root-vsys-profile and the default VSYS profile of non-root VSYS named default-vsys-profile cannot be edited or deleted.
- Before deleting a VSYS profile, you must delete all the VSYSs referencing the VSYS profile.

Configuring QoS

Root RXW administrators can configure whether enable QoS or not in a VSYS Profile. Then you can bind a VSYS Profile to a non-root VSYS to enable or disable QoS. You can specify the reserved quota and maximum quota for root-pipe.

To enable QoS or configure QoS Profile resources in a VSYS Profile, you need to enter QoS configuration mode first, in the VSYS profile configuration mode, use the following command:

iqos

To enable or disable QoS, in the QoS configuration mode, use the following command:

- Enable: **enable**
- Disable: **no enable**

To configure QoS Profile resources quota, in the QoS configuration mode, use the following command:

root-pipe max *max-num* **reserve** *reserve-num*

- **max** *max-num* **reserve** *reserve-num* - Specifies the maximum quota (**max** *max-num*) and reserved quota (**reserve** *reserve-num*) of root-pipe in a VSYS. The reserved quota should not exceed the maximum quota. The default value of maximum quota and reserved quota is 0.

Configuring Resource Quota

To configuring the resource quota of a VSYS, in the VSYS profile configuration mode, use the following command:

{**cpu** | **session** | **zone** | **keyword** | **keyword-category** | **policy** | **snat** | **dnat** | **session-limit** | **statistic-set**{**non-session-based** | **session-based**} | **tunnel-ipsec**} {**simple** | **regexp**} **max** *max-num* **reserve** *reserve-num* [**alarm** *alarm-num*]

- {**simple** | **regexp**} - Only applicable to **keyword. simple** is used to specify the quota of simple keyword. **regexp** is used to specify the quota of regular expression keyword.
- **max** *max-num* **reserve** *reserve-num* - Specifies the maximum quota (**max** *max-num*) and reserved quota (**reserve** *reserve-num*) of CPU (**cpu**), concurrent sessions (**session**), zones (**zone**), keywords (**keyword**), keyword categories (**keyword-category**), policy rules (**policy**), SNAT rules (**snat**), DNAT rules (**dnat**), session limit rules number, statistics set, and IPSec VPN tunnels in the VSYS. The reserved quota and maximum quota vary from different platforms. The reserved quota should not exceed the maximum quota. Table below shows the value range of the maximum quota and minimum number of reserved quota.
- **alarm** *alarm-num* - Only applicable to CPU. With this parameter configured, the system will generate alarm logs when the CPU utilization exceeds the specified percentage. The value range is 50 to 99.

System Resource	Value range of maximum quota	Minimum number of reserved quota
CPU	1 – max-num1①	0
Concurrent sessions	min (max-num1①/2, 256) – max-num1①	0

System Resource	Value range of maximum quota	Minimum number of reserved quota
Zones	1 － max-num2②	0
Keywords in each keyword category	• Simple:0 － capacity • Regular expression:0 － 10	0
Keyword categories	0 － capacity	0
Policy rules	0 － max-num2②	0
SNAT rules	0 － max-num2②	0
DNAT rules	0 － max-num2②	0
Session Limit Rules Number	• root VSYS Profile:128(fixed value) • non-root VSYS Profile:0 － 118	• root VSYS Profile:10(fixed value) • non-root VSYS Profile:0
Statistics set	0 - 6	0
IPSec VPN tunnels	0 － max-num2②	0

max-num1①: max (capacity*2/max-vsys-num, capacity/2)

max-num2②: max (capacity*2/max-vsys-num, capacity/10)

For example：

> If the capacity of concurrent sessions is 2000000 and up to 100 VSYS can be configured, when configuring the resource quota, the maximum quota value range can be calculated as below:
>
> - Parameter **max-num1**： max (capacity*2/max-vsys-num, capacity/2) = max (2000000*2/100, 2000000/2) = 1000000
> - Minimum value of max quota: min (max-num1/2, 256) = min (1000000/2, 256) = 256
>
> According to the above calculating formula, the value range of max quota is **min (max-num1/2, 256) - max-num1**, namely from 256 to 1000000.

To restore to the default quota, in the VSYS profile configuration mode, use the following command:

```
no {cpu | session | zone | keyword | keyword-category | policy | snat | dnat | session-limit}
{simple | regexp} max reserve [alarm]
```

Configuring the Quota of Log Buffer

After configuring to send logs to the memory buffer, you can specify the reserved buffer quota and maximum buffer quota for each type of logs in a VSYS by creating a VSYS profile. Reserved quota refers to the memory buffer value reserved for each type of logs; maximum quota refers to the maximum memory buffer value available to each type of logs. The root administrator has the permission to create VSYS profiles. If the logs' capacity in a VSYS exceeds its maximum quota, the new logs will override the earliest logs in the buffer.

To configure the quota of buffer for each type of logs, in the VSYS profile configuration mode, use the following command:

```
log {configuration | operation | event | network | threat | traffic {session | nat | websurf}}
buffer-size max max-num reserve reserve-num
```

- **max** *max-num* **reserve** *reserve-num*- Specifies the maximum quota (**max** *max-num*) and reserved quota (**reserve** *reserve-num*) of configuration logs, operation logs, event logs, network logs, threat logs, traffic logs(including session logs, NAT logs and websurf logs) in a VSYS. The range of reserved quota or maximum quota varies from different platforms. The reserved quota should not exceed the maximum quota.

Configuring URL Filter

The root administrator can configure whether enable URL filter or not in a VSYS Profile. Then you can bind a VSYS Profile to a non-root VSYS to enable or disable URL filter. VSYSs share URL resources including URL, URL category and URL Profile. You can specify the reserved quota and maximum quota for each type of URL resources.

To enable URL filter or configure URL resources in a VSYS Profile, you need to enter urlfilter configuration mode first, in the VSYS profile configuration mode, use the following command:

```
urlfilter
```

To enable or disable URL filter, in the urlfilter configuration mode, use the following command:

- Enable: **enable**
- Disable: **no enable**

To configure URL resources quota, in the urlfilter configuration mode, use the following command:

```
{url | url-category | url-profile} max max-num reserve reserve-num
```

- **max** *max-num* **reserve** *reserve-num* - Specifies the maximum quota (**max** *max-num*) and reserved quota (**reserve** *reserve-num*) of total URLs, user-defined URL category and URL Profile in a VSYS. The range of reserved quota or maximum quota varies from different platforms. The reserved quota should not exceed the maximum quota. Table below shows the value range of the maximum quota and minimum number of reserved quota. The default value of maximum quota is the system capacity. The default value of minimum quota is 0.

URL Resource	Value range of maximum quota	Minimum number of reserved quota
URL	0 – Capacity	0
User-defined URL category	0 – 26	0
URL Profile	0 – 32	0

Configuring IPS

The root administrator can configure whether enable IPS or not in a VSYS Profile. Then you can bind a VSYS Profile to a non-root VSYS to enable or disable IPS. VSYSs share IPS Profile resources. You can specify the reserved quota and maximum quota.

To enable IPS or configure IPS Profile resources in a VSYS Profile, you need to enter IPS configuration mode first, in the VSYS profile configuration mode, use the following command:

```
ips
```

To enable or disable IPS, in the IPS configuration mode, use the following command:

- Enable: **enable**
- Disable: **no enable**

To configure IPS Profile resources quota, in the IPS configuration mode, use the following command:

profile max *max-num* **reserve** *reserve-num*

- **max** *max-num* **reserve** *reserve-num* - Specifies the maximum quota (**max** *max-num*) and reserved quota (**reserve** *reserve-num*) of IPS Profile in a VSYS. You can create one IPS Profile at most in non-root VSYS, i.e., the range of maximum quota varies from 0 to 1. The reserved quota should not exceed the maximum quota. The default value of maximum quota and reserved quota is 0, which means only predefined IPS Profiles can be used in non-root VSYS.

Enabling/Disabling the CPU Resource Quota

By default, the configured CPU resource quota will take effect immediately. You can also use the following command to disable the VSYS CPU resource check. That is, the configured CPU resource quota will not take effect and each VSYS will preempt the CPU resource in system. To disable or enable CPU resource quota, in the global configuration mode of the root VSYS, use the following command:

- Disable: **vsys-resource cpu disable**
- Enable: **vsys-resource cpu enable**

Binding a VSYS Profile to a VSYS

To bind a VSYS profile to an existing VSYS, in the VSYS configuration mode, use the following command:

profile *vsys-profile-name*

- *vsys-profile-name* - Specifies the name of the VSYS profile to be bound.

To restore to the default binding, in the VSYS configuration mode, use the command **no profile**.

Note:

- When binding a VSYS profile to a VSYS, if the total number of the reserved quota in all VSYSs exceeds the current capacity, the binding operation will fail.
- Only after canceling the binding can you delete the VSYS profile.

Entering the VSYS

Start a connection client on the local PC, type the management IP and port to connect with the device, and then type the username and password according to the prompt. For example, if the management IP of root VSYS is 10.90.89.1, after typing the username (admin) and password (admin), you can enter the root VSYS. After creating the non-root VSYS (vsys1), you should type the management IP 10.90.89.1, the non-root administrator username (vsys1\admin) and password (vsys1-admin), and then you can enter the non-root VSYS directly.

Besides, the root VSYS administrator can enter the non-root VSYS from root VSYS. The administrator in the root VSYS can configure the functions of the non-root VSYS after entering it. To enter a non-root VSYS, in the execution mode or the global configuration mode of the root VSYS, use the following command:

enter-vsys *vsys-name*

- *vsys-name* - Specifies the name of the non-root VSYS.

To exit the current non-root VSYS and back to the execution mode or global configuration mode of the root VSYS, in the execution mode or global configuration mode of the non-root VSYS, use the command **exit-vsys**.

> Note:If you enter the non-root VSYS directly, you cannot back to the root VSYS by using the command.

Configuring the Shared Property

To make the VRouter, VSwitch, or zone in the root VSYS shared, in the VRouter/VSwitch/zone configuration mode of the root VSYS, use the following command:

vsys-shared

To remove the shared property, in the VRouter/VSwitch/zone configuration mode of the root VSYS, use the command **no vsys-shared**.

Exporting a Physical Interface

By default, all the physical interfaces on the device belong to the root VSYS. RXW administrator in the root VSYS can export physical interfaces in the root VSYS to non-root VSYSs, and also, the root administrator in the root VSYS can export the physical interfaces in non-root VSYSs back to the root VSYS. The physical interfaces to be exported should not be bound to any zone, or be the member of BGroup interface, aggregate interface or redundant interface, or have any sub-interface. All the interfaces that are related to the physical interface in the non-root VSYS (e.g., the sub-interface created after the physical interface is exported from the root VSYS to non-root VSYS) can only be used in the non-root VSYS.

To export a physical interface to a non-root VSYS, in the interface configuration mode, use the following command:

export-to *vsys-name*

- *vsys-name* − Specifies the non-root VSYS name to which the interface will be exported.

To export the physical interface in the non-root VSYS back to the root VSYS, in the interface configuration mode, use the command **no export-to**.

Allocating a Logical Interface

The root administrator in the root VSYS can allocate the logical interfaces in the root VSYS to non-root VSYSs, and also, can restore the allocated logical interfaces to the root VSYS.

To allocate a logical interface in the root VSYS to a non-root VSYS, in the interface configuration mode, use the following command:

vsys *vsys-name*

- *vsys-name* - Specifies the name of the non-root VSYS to which the interface will be allocated.

To restore the interface to the root VSYS, in the interface configuration mode, use the command **no vsys**.

Binding a Track Object

You can bind a track objet to a non-root VSYS, thus monitoring the status of this VSYS. To complete the binding, in the non-root VSYS configuration mode, use the followonig command:

vsys-track-status track *track-name*

- *track-name* - Specifies the name of the track object. Ensure that this track object is created in this non-root VSYS.

To cancel the binding, in the non-root VSYS configuration mode, use the following command:

no vsys-track-status track *track-name*

Note:

- After you cancel the binding, you can delete the track object.
- For more information about configuring track object, see "Configuring a Track Object" of "System Management".

Monitoring a Specified VSYS

In the root VSYS, you can monitor the status of a specified VSYS. According to the change of the status, you can take corresponding actions. To monitor a specified VSYS, use the following command in the track object configuration mode in the root VSYS

vsys *vsys-name* **weight** *value*

- *vsys-name* – Specifies the VSYS name. This is the one that you want to monitor.
- **weight** *value* – Specifies the weight. Specifies how important this entry failure is to the judgment of track object failure. The value range is 1 to 255. The default value is 255.

Note:Monitoring the status of a specified VSYS is only available in High Availability.

Configuring VSYS Log

At the time of writing, the system supports logs for AAA, NAT/NAT444, policy, routing, attack defense, interface, DNS, service, DHCP and system management events in VSYS. For more information about how to configure and view logs, see "Logs" .

Note:In non-root VSYS, the system does not support debugging, IPS logs.

Configuring Cross-VSYS Traffic Forwarding

In order to realize the cross-VSYS traffic forwarding function, the system introduces the concept of Simple-Switch, it is a special VSwitch, which can only learn MAC address, forward the known unicast packet or flooding. You can create a VWANIF interface, and assigned to the designated VSYS, the different VSYS can communicate with each other through the VWANIF interface, so that the device is now directly forwarded across different VSYS traffic data packets.

To configure the cross-VSYS traffic forwarding function, take the following steps:

1. Enabling the cross-VSYS traffic forwarding.
2. Configuring a Simple-Switch.
   Including create a Simple-Switch, create a L2 zone and binding the L2 zone to the Simple-Switch.
3. Creating a VWANIF interface.
   Each time you create a VWANIF interface, system will create a corresponding VPort interface for the VWANIF interface automatically.
4. Configuring the VPort interface.
   Binding the VPort interface to the L2 zone that has been added to the Simple-Switch.
5. Configuring the VWANIF interface.
   Allocating the VWANIF interface to a VSYS, configuring the zone and IP address for the VWANIF interface.

Enabling/Disabling the Cross-VSYS Traffic Forwarding

By default, the cross-VSYS traffic forwarding function is disabled. To enable/disable the cross-VSYS traffic forwarding function, in the global configuration mode, use the following commands:

- Enable: **vsys-switch-mode**
- Disable: **no vsys-switch-mode**

Configuring a Simple-Switch

Simple-Switch is a special VSwitch, which can only learn MAC address, forward the known unicast packet or flooding. You can create multiple Simple-Switchs, each Simple-Switch is virtually an independent broadcast domain.

Creating a Simple-Switch

To create a Simple-Switch, in the global configuration mode, use the following commands:

vswitch vswitch *Number* [**simple-switch**]

- *Number* - Specifies the numeric identification for the VSwitch. The value range varies from different platforms. Cannot be specified as VSwitch1.
- **simple-switch** - Specifies this parameter to create the Simple-Switch and enter the Simple-Switch configuration mode .

To delete the Simple-Switch, in the global configuration mode, use the following command:

no vswitch vswitch *Number*

Binding the L2 Zone to the Simple-Switch

Binding the L2 zone to a Simple-Switch in two steps.

First, create a L2 zone. In the global configuration mode, use the following command:

zone *zone-name* **l2**

- *zone-name* - Specifies the name of Layer 2 zone.
- **l2** - Specifies the zone as a Layer 2 zone.

Then, in the zone configuration mode, use the following command to bind the L2 zone to a Simple-Switch:

bind *vswitch-name*

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

Creating a VWANIF interface

VWANIF interface is a Layer 3 interface, each time you create a VWANIF interface, system will create a corresponding VPort interface for the VWANIF interface automatically.

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

interface vwanif *id*

- *id* - Specifies the ID of the VWANIF interface. If the specified VWANIF interface does not exist, this command creates a VWANIF interface and leads you to its configuration mode. If the specified VWANIF interface exists, you will enter its configuration mode directly.

To clear the specified VWANIF interface, use the command **no interface vwanif** *id*

Configuring the VPort Interface

To bind the VPort interface to the L2 zone that has been added to the Simple-Switch, in the global configuration mode, use the following command:

```
zone zone-name
```

- *zone -name* - Specifies the L2 zone name that has been added to the Simple-Switch.

Configuring the VWANIF Interface

In order to realize the cross-VSYS traffic forwarding, you also need to allocate the VWANIF interface to a VSYS, and configure the zone , IP address for the VWANIF interface.

> Note:How to configure the zone and IP address for the VWANIF interface, refer to Configuring Interface section.

Allocating a VWANIF Interface

After you create the VWANIF interface, you need to allocate the VWANIF interface to a VSYS, in the interface configuration mode, use the following command:

```
vsys vsys-name
```

- *vsys-name* - Specifies the name of the VSYS to which the VWANIF interface will be allocated.

Viewing Cross-VSYS Traffic Forwarding Information

To view the cross-VSYS traffic forwarding information, in any mode, use the following command:

```
show vsys-switch-mode
```

Viewing the VWANIF interface Configuration Information

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

```
show interface vwanif id
```

Viewing VSYS Information

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

show vsys [*vsys-name*]

- *vsys-name* - Specifies the name of the VSYS whose information you want to view. If this parameter is not specified, the information of all the VSYSs in the system will be displayed.

Viewing VSYS Profile Information

To view the VSYS profile information, in any mode of the root VSYS, use the following command:

show vsys-profile [*vsys-profile-name*]

- *vsys-profile-name* - Specifies the name of the VSYS profile whose information you want to view. If this parameter is not specified, the information of all the VSYS profiles in the system will be displayed.

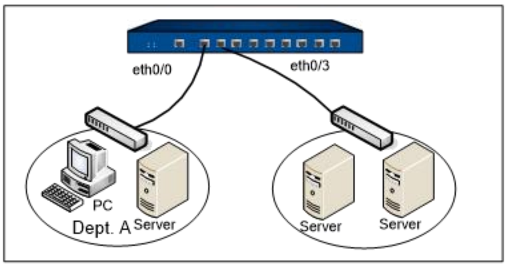
VSYS Configuration Examples

This section describes three typical VSYS configuration examples:

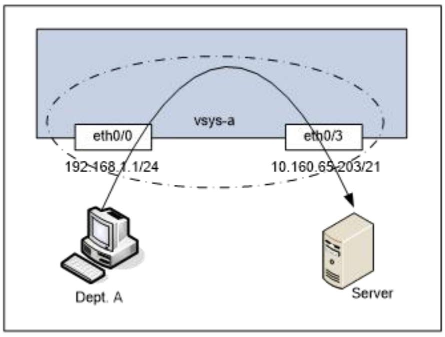
- Example 1: L3 traffic transmitting in a single VSYS
- Example 2: L3 traffic transmitting among multiple VSYSs via shared VRouter
- Example 3: L2 traffic transmitting among multiple VSYSs via shared VSwitch

Example 1: L3 Traffic Transmitting in a Single VSYS

An enterprise deploys FS device in its network. The goal is to enable Dept. A to visit Intranet server through ethernet0/0 and ethernet0/3 in a single VSYS. The topology is shown as below:



To meet the above requirement, a VSYS and corresponding policy rules are needed. Below is the logical illustration.



Configuration Steps

Step 1: Create VSYS-a

```
hostname(config)# vsys vsys-a
hostname(config-vsys)# exit
hostname(config)#
```

Step 2: Export ethernet0/0 and ethernet0/3 to VSYS-a by the root administrator of the root VSYS:

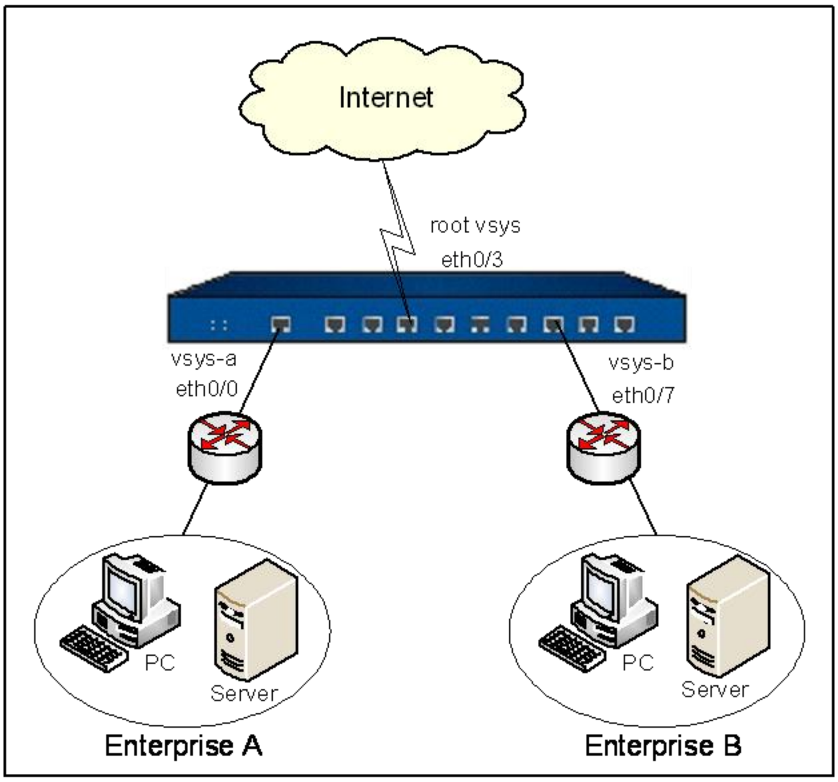
```
hostname(config)# interface ethernet0/0
hostname (config-if-eth0/0)# export-to vsys-a
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/3
hostname (config-if-eth0/3)# export-to vsys-a
hostname(config-if-eth0/3)# exit
hostname(config)#
```

Step 3: Enter VSYS-a to configure ethernet0/0, ethernet0/3 and related policy rules:

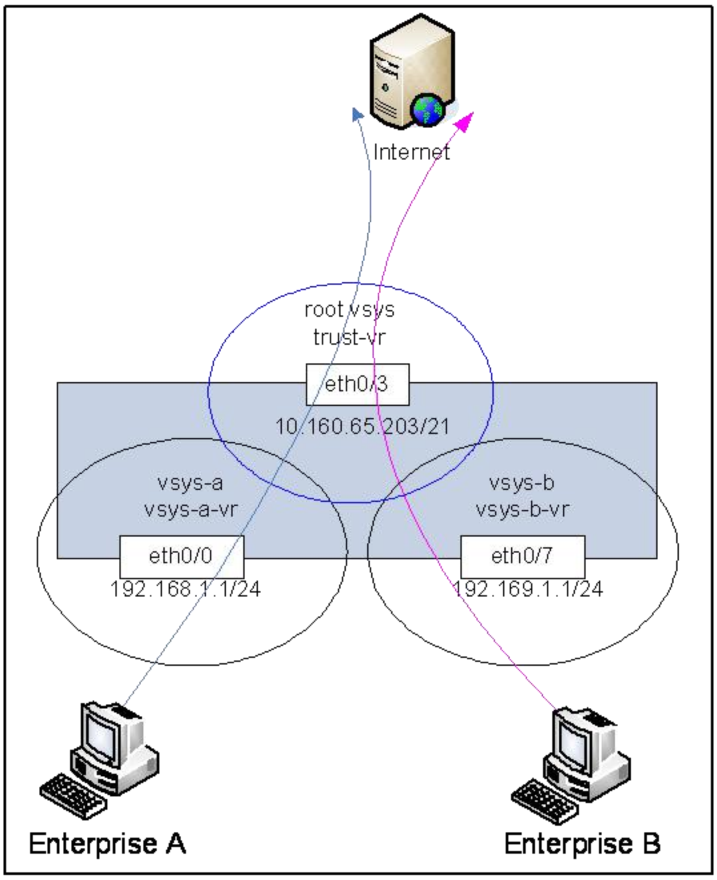
```
hostname(config)# enter-vsys vsys-a
hostname(vsys-a)(config)# zone vsys-a-trust
hostname(vsys-a)(config-zone-vsys-a-trust)# exit
hostname(vsys-a)(config)# interface ethernet0/0
hostname(vsys-a)(config-if-eth0/0)# zone vsys-a-trust
hostname(vsys-a)(config-if-eth0/0)# ip address 192.168.1.1/24
hostname(vsys-a)(config-if-eth0/0)# exit
hostname(vsys-a)(config)# zone vsys-a-untrust
hostname(vsys-a)(config-zone-vsys-a-untrust)# exit
hostname(vsys-a)(config)# interface ethernet0/3
hostname(vsys-a)(config-if-eth0/3)# zone vsys-a-untrust
hostname(vsys-a)(config-if-eth0/3)# ip address 10.160.65.203/21
hostname(vsys-a)(config-if-eth0/3)# exit
hostname(vsys-a)(config)# policy-global
hostname(vsys-a)(config-policy)# rule
hostname(vsys-a)(config-policy-rule)# src-zone vsys-a-trust
hostname(vsys-a)(config-policy-rule)# dst-zone vsys-a-untrust
hostname(vsys-a)(config-policy-rule)# src-addr any
hostname(vsys-a)(config-policy-rule)# dst-addr any
hostname(vsys-a)(config-policy-rule)# service any
hostname(vsys-a)(config-policy-rule)# action permit
hostname(vsys-a)(config-policy-rule)# exit
hostname(vsys-a)(config-policy)# exit
hostname(vsys-a)(config)# exit-vsys
hostname(config)#
```

Example 2: L3 Traffic Transmitting among Multiple VSYSs via Shared VRouters

A FS device is deployed for enterprise A and enterprise B. VSYS-a is configured for enterprise A and VSYS-b is configured for enterprise B. The interface ethernet0/0 is used by enterprise A only and ethernet0/7 is used by enterprise B only. The interface ethernet0/3 is shared by enterprise A and B, and the two enterprises visit Internet through enthernet0/3. See the topology below:



To meet the above requirement, the shared VRouter, corresponding routes, SNAT rules, and policy rules are needed. Below is the logical illustration.



Configuration Steps

Step 1: Configure Root VSYS:

```
Create vsys-a and vsys-b
hostname(config)# vsys vsys-a
hostname(config-vsys)# exit
hostname(config)# vsys vsys-b
hostname(config-vsys)# exit
hostname(config)#
Configure ethernet0/3, routes, SNAT rules, and DNS server
hostname(config)# interface ethernet0/3
hostname(config -if-eth0/3)# zone untrust
hostname(config -if-eth0/3)# ip address 10.160.65.203/21
hostname(config -if-eth0/3)# exit
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 0.0.0.0/0 10.160.64.1
hostname(config-vrouter)# snatrule from any to any eif ethernet0/3 trans-to eif-ip mode dynamicport
rule ID=3
hostname(config-vrouter)# exit
hostname(config)# ip name-server 202.106.0.20
hostname(config)#
Share trust-vr in Root VSYS
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# vsys-shared
hostname(config-vrouter)# exit
hostname(config)#
Share untrust zone in Root VSYS
hostname(config)# zone untrust
hostname(config-zone-untrust)# vsys-shared

hostname(config-zone-untrust)# exit

hostname(config)#
```

Step 2: Configure VSYS-a:

```
Login the system using the root administrator’ s credential of Root VSYS, and export ethernet0/0 to VSYS-a

hostname(config)# interface ethernet0/0

hostname (config-if-eth0/0)# export-to vsys-a

hostname(config-if-eth0/0)# exit

hostname(config)#

Enter VSYS-a and configure ethernet0/0, policy rules, and cross-VR routes

hostname(config)# enter-vsys vsys-a

hostname(vsys-a)(config)# interface ethernet0/0

hostname(vsys-a)(config-if-eth0/0)# zone vsys-a-trust

hostname(vsys-a)(config-if-eth0/0)# ip address 192.168.1.1/24

hostname(vsys-a)(config-if-eth0/0)# exit

hostname(vsys-a)(config)# policy-global

hostname(vsys-a)(config-policy)# rule

hostname(vsys-a)(config-policy-rule)# src-zone vsys-a-trust

hostname(vsys-a)(config-policy-rule)# dst-zone untrust

hostname(vsys-a)(config-policy-rule)# src-addr any

hostname(vsys-a)(config-policy-rule)# dst-addr any

hostname(vsys-a)(config-policy-rule)# service any

hostname(vsys-a)(config-policy-rule)# action permit

hostname(vsys-a)(config-policy-rule)# exit

hostname(vsys-a)(config-policy)# exit

hostname(vsys-a)(config)# ip vrouter vsys-a-vr

hostname(vsys-a)(config-vrouter)# ip route 0.0.0.0/0 vrouter trust-vr
hostname(vsys-a)(config-vrouter)# exit
hostname(vsys-a)(config)# exit-vsys
hostname(config)#
```

Step 3: Configure VSYS-b:

Login the system using the root administrator's credential of Root VSYS, and export ethernet0/7 to VSYS-b

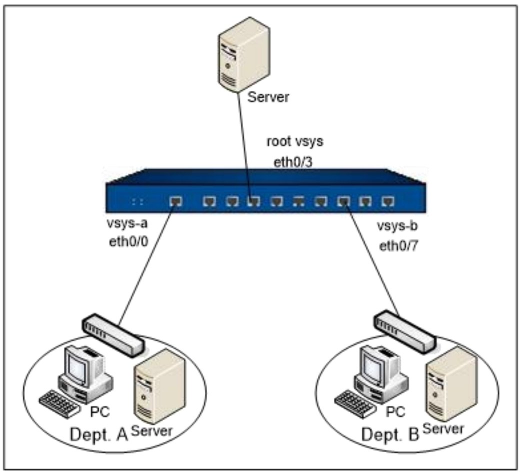
```
hostname(config)# interface ethernet0/7
hostname (config-if-eth0/7)# export-to vsys-b
hostname(config-if-eth0/7)# exit
hostname(config)#
```

Enter VSYS-b and configure ethernet0/7, policy rules, and cross-VR routes

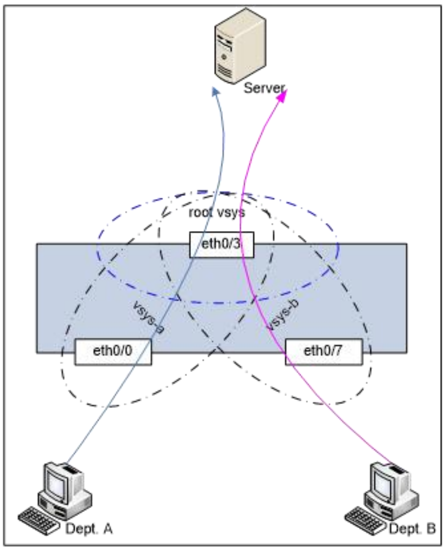
```
hostname(config)# enter-vsys vsys-b
hostname(vsys-b)(config)# interface ethernet0/7
hostname(vsys-b)(config-if-eth0/7)# zone vsys-b-trust
hostname(vsys-b)(config-if-eth0/7)# ip address 192.169.1.1/24
hostname(vsys-b)(config-if-eth0/7)# exit
hostname(vsys-b)(config)# policy-global
hostname(vsys-b)(config-policy)# rule
hostname(vsys-b)(config-policy-rule)# src-zone vsys-b-trust
hostname(vsys-b)(config-policy-rule)# dst-zone untrust
hostname(vsys-b)(config-policy-rule)# src-addr any
hostname(vsys-b)(config-policy-rule)# dst-addr any
hostname(vsys-b)(config-policy-rule)# service any
hostname(vsys-b)(config-policy-rule)# action permit
hostname(vsys-b)(config-policy-rule)# exit
hostname(vsys-b)(config-policy)# exit
hostname(vsys-b)(config-policy)# exit
hostname(vsys-b)(config)# ip vrouter vsys-b-vr
hostname(vsys-b)(config-vrouter)# ip route 0.0.0.0/0 vrouter trust-vr
hostname(vsys-b)(config-vrouter)# exit
hostname(vsys-b)(config)# exit-vsys
hostname(config)#
```

Example 3: L2 Traffic Transmitting among Multiple VSYSs via Shared VSwitch

An enterprise deploys a FS device in its network. VSYS-a is configured for Dept. A, and VSYS-b is configured for Dept. B. The interface ethernet0/0 is used by VSYS-a only and etherent0/7 is used by VSYS-b only. The interface etherenet0/3 is shared by Dept. A and Dept. B, and the two departments visit an Intranet server through ethernet0/3. See the topology below:



To meet the above requirement, the shared VSwitch and corresponding policy rules are needed. Below is the logical illustration.



Configuration Steps

Step 1: Configure Root VSYS:

```
Create vsys-a and vsys-b
hostname(config)# vsys vsys-a
hostname(config-vsys)# exit
hostname(config)# vsys vsys-b
hostname(config-vsys)# exit
hostname(config)#
Share VSwitch1 in Root VSYS
hostname(config)# vswitch vswitch1
hostname(config-vswitch)# vsys-shared
hostname(config-vswitch)# exit
Share L2-trust zone in Root VSYS
hostname(config)# zone l2-trust
hostname(config-zone-l2-tru~)# vsys-shared
hostname(config-zone-l2-tru~)# exit
hostname(config)#
Configure ethernet0/3
hostname(config)# interface ethernet0/3
hostname(config -if-eth0/3)# zone l2-trust
hostname(config -if-eth0/3)# exit
hostname(config)#
```

Step 2: Configure VSYS-a:

```
Log into the system using the root administrator’ s credential of Root VSYS, and export ethernet0/0 to VSYS-a
hostname(config)# interface ethernet0/0
hostname (config-if-eth0/0)# export-to vsys-a
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Enter VSYS-a, and create a VSwitch and a L2 zone. Bind the created L2 zone to the shared VSwitch1

```
hostname(config)# enter-vsys vsys-a
hostname(vsys-a)(config)# zone a-l2 l2
hostname(vsys-a)( config-zone-a-l2)# bind vswitch1
hostname(vsys-a)( config-zone-a-l2)# exit
hostname(vsys-a)(config)#
```

Configure ethernet0/0 and policy rules

```
hostname(vsys-a)(config)# interface ethernet0/0
hostname(vsys-a)(config-if-eth0/0)# zone a-l2
hostname(vsys-a)(config-if-eth0/0)# exit
hostname(vsys-a)(config)# policy-global
hostname(vsys-a)(config-policy)# rule
hostname(vsys-a)(config-policy-rule)# src-zone a-l2
hostname(vsys-a)(config-policy-rule)# dst-zone l2-trust
hostname(vsys-a)(config-policy-rule)# src-addr any
hostname(vsys-a)(config-policy-rule)# dst-addr any
hostname(vsys-a)(config-policy-rule)# service any
hostname(vsys-a)(config-policy-rule)# action permit
hostname(vsys-a)(config-policy-rule)# exit
hostname(vsys-a)(config-policy)# exit
hostname(vsys-a)(config)# exit-vsys
hostname(config)#
```

Step 3: Configure VSYS-b:

Log into the system using the root administrator's credential of Root VSYS, and export ethernet0/7 to VSYS-b

```
hostname(config)# interface ethernet0/7
hostname (config-if-eth0/7)# export-to vsys-b
```

```
hostname(config-if-eth0/7)# exit
hostname(config)#
```

Enter VSYS-b, and create a VSwitch and a L2 zone. Bind the created L2 zone to the shared VSwitch1

```
hostname(config)# enter-vsys vsys-b
hostname(vsys-b)(config)# zone b-l2 l2
hostname(vsys-b)( config-zone-b-l2)# bind vswitch1
hostname(vsys-b)( config-zone-b-l2)# exit
hostname(vsys-b)(config)#
```

Configure ethernet0/7 and policy rules

```
hostname(vsys-b)(config)# interface ethernet0/7
hostname(vsys-b)(config-if-eth0/7)# zone b-l2
hostname(vsys-b)(config-if-eth0/7)# exit
hostname(vsys-b)(config)# policy-global
hostname(vsys-b)(config-policy)# rule
hostname(vsys-b)(config-policy-rule)# src-zone b-l2
hostname(vsys-b)(config-policy-rule)# dst-zone l2-trust
hostname(vsys-b)(config-policy-rule)# src-addr any
hostname(vsys-b)(config-policy-rule)# dst-addr any
hostname(vsys-b)(config-policy-rule)# service any
hostname(vsys-b)(config-policy-rule)# action permit
hostname(vsys-b)(config-policy-rule)# exit
hostname(vsys-b)(config-policy)# exit
hostname(vsys-b)(config)# exit-vsys
hostname(config)#
```

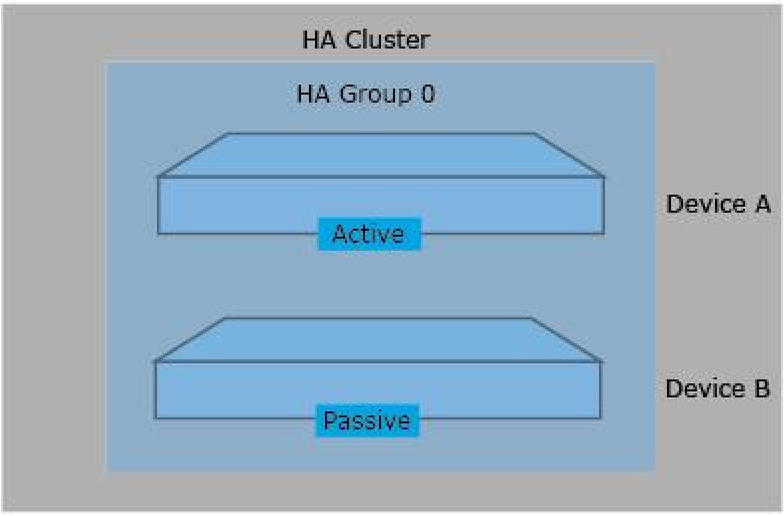
Chapter 6 High Availability (HA)

Overview

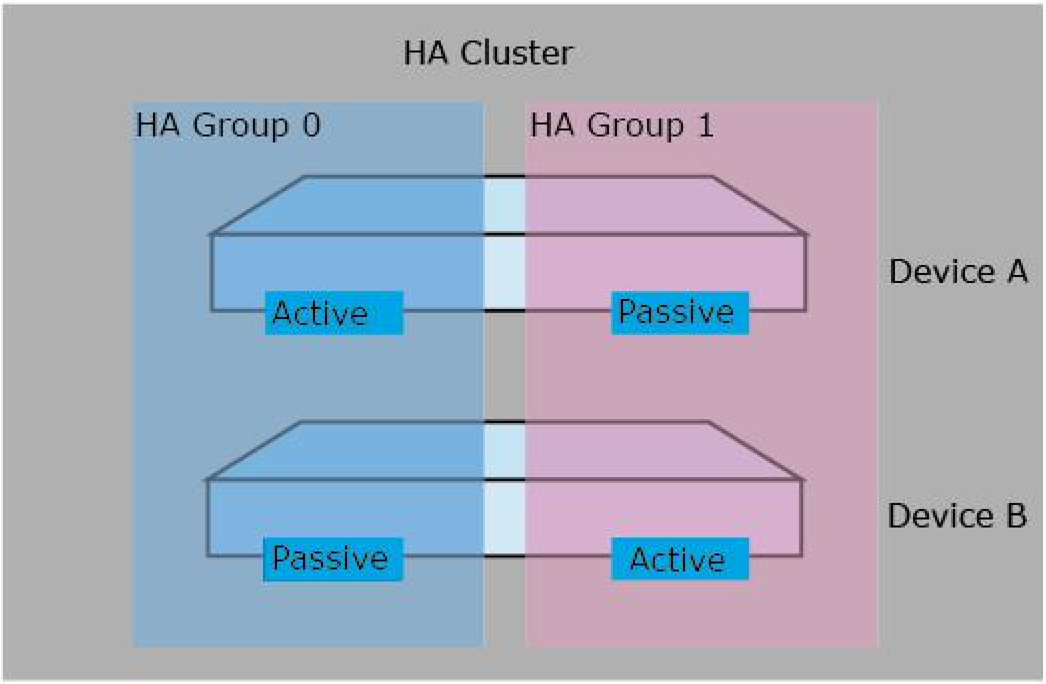
HA (High Availability) provides a failover solution for malfunction of the communication line or devices in order to ensure smooth communication and effectively improve the network reliability. To implement the HA function, you need to group two FS devices as an HA cluster, using the identical hardware platform, firmware version, and licenses. When one device is unavailable or cannot handle the request from the client properly, the request will be promptly directed to the other device that works normally, thus ensuring uninterrupted network communication and greatly improving the reliability of communications.

FS devices support three HA modes: Active-Passive (A/P), Active-Active (A/A), and Peer mode.

- Active-Passive (A/P) mode: In the HA cluster, configure two devices to form an HA group, with one device acting as a master device and the other acting as its backup device. The master device is active, forwarding packets, and meanwhile synchronizes all of its network and configuration information and current session information to the backup device. When the master device fails, the backup device will be promoted to master and take over its work to forward packets. This A/P mode is redundant, and features a simple network structure for you to maintain and manage. The relationship between the devices in A/P mode is shown below:



- Active-Active (A/A) mode: When the security device is in NAT mode, routing mode or a combination of both, you can configure both the FS devices in the HA cluster as active, so that they can 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 to ensure uninterrupted work. This mode is known as the Active-Active mode. The A/A mode ensures high-performance and is able to provide load-balancing function. The relationship between the devices in A/A mode is shown below:



As shown above, Device A acts as the master device of HA Group 0 and backup device of HA Group 1; HA Device B acts as the master device of HA Group 1 and backup device of HA Group 0. The master device of HA Group 0 is known as Admin Master, and the master device of HA Group 1 is known as Master.

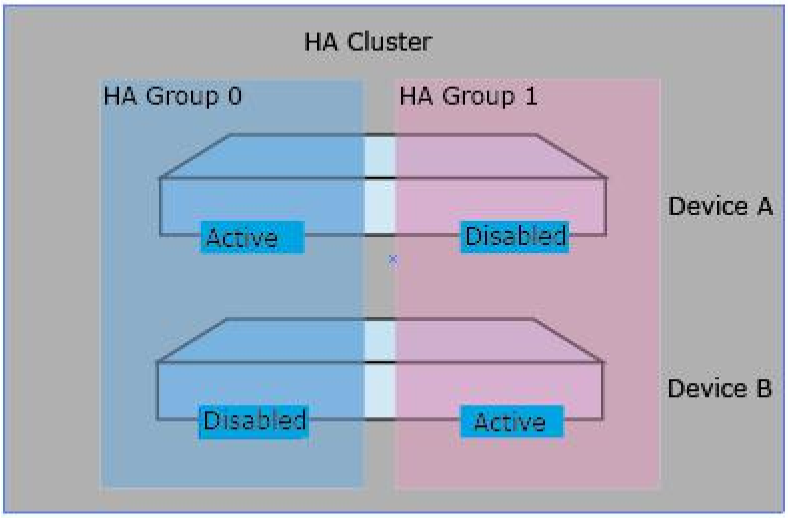
When configuring the HA Active-Active mode, you're recommended to take the following steps to avoid configuration synchronization failure between the master and backup device:

- Configure parameters in the Admin Master
- First enable HA on Admin Master, and then enable HA on Master;

Note:If possible, configure the devices that are enabled with HA when the operation status of HA is stable, in order to avoid configuration synchronization failure or slow execution of the configuration commands.

- 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.

The relationship between the devices in the Peer mode is shown in the figure below:



HA Cluster

For the external network devices, an HA cluster is a single device which handles network traffic and provides security services. The HA cluster is identified by its cluster ID. After specifying an HA cluster ID for the device, the device will be in the HA state to implement HA function.

HA Group

System will select the master and backup device of the same HA group ID in an HA cluster according to the HCMP protocol and the HA configuration. The master device is in active state and processes network traffic. When the master device fails, the backup device will take over its work.

When assigning a cluster ID to the device, the HA group with ID 0 will be automatically created. In Active-Passive (A/P) mode, the device only has HA group 0. In Active-Active (A/A) mode, the latest FS version supports two HA groups, i.e., Group 0 and Group 1.

HA Node

To distinguish the HA device in an HA group, you can use the value of HA Node to mark the devices. FSOS support the values of 0 and 1.

In the HA Peer mode, the system can decide which device is the master according to the HA Node value. In the HA group 0, the device whose HA Node value is 0 will be active and the device whose HA Node value is 1 is at the disabled status. In the HA group 1, the device whose HA Node value is 0 is at the disabled status and the device whose HA Node value is 0 is active.

HA Group Interface and Virtual MAC

In the HA environment, each HA group has an interface to forward traffic, which is known as Virtual Forward Interface. The master device of each HA group manages a virtual MAC (VMAC) address which corresponds to its interface and the traffic is forwarded on the interface. Different HA groups in an HA cluster cannot forward data among each other. VMAC address is defined by HA base MAC, HA cluster ID, HA group ID and the physical interface index.

HA Selection

In an HA cluster, if the group ID of the HA devices is the same, the one with higher priority will be selected as the master device.

HA Synchronization

To ensure the backup device can take over the work of the master device when it fails, the master device will synchronize its information with the backup device. There are 3 types of information that can be synchronized: configuration information, files and RDO (Runtime Dynamic Object). The specific content of RDO includes:

- Session information (The following types of session information will not be synchronized: the session to the device itself, tunnel session, deny session, ICMP session, and the tentative session)
- IPsec VPN information
- 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 master device has just been selected successfully, the batch synchronization will be used to synchronize all information of the master 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.

Note:

- If you configure Local property for an interface , the system will not synchronize this configuration with the backup device. For this reason, it is recommended not to configure the Local property for the business interface.

Configuring HA

To configure the HA function, take the following steps:

1. Configure an HA group, including specifying the device priority (for selection) and HA packets-related parameters.
2. Configure an HA virtual forward interface.
3. Configure HA link interface which is used for the device synchronization and HA packets transmission.
4. Configure an HA cluster. Specify the ID of HA cluster and enable the HA function.

WebUI: Select **System** > **HA** from the menu bar. In the HA dialog, configure the options.

Configuring an HA Group

The HA group need to be configured in the HA group configuration mode. To enter the HA group configuration mode, in the global configuration mode, use the following command:

ha group *group-id*

- *group-id* – Specifies the HA group ID. The value range is 0 to 1.

After executing the command, the system will enter the HA group configuration mode. To delete the specified HA group, in the global configuration mode, use the following command:

no ha group *group-id*

In the HA group configuration mode, you can perform the following configurations:

- Specifying the priority
- Specifying the Hello interval

- Specifying the Hello threshold
- Configuring the preempt mode
- Specifying the gratuitous ARP packet number
- Specifying the description
- Specifying the track object

Specifying the Priority

The priority specified by the command is for used for HA selection. The device with higher priority (the smaller number) will be selected as the master device. To specify the priority, in the HA group configuration mode, use the following command:

priority *number*

- *number* – Specifies the priority. The value range is the 1 to 254. The default value is 100.

To restore to the default priority, in the HA group configuration mode, use the following command:

no priority

> Tip: When the priorities are identical, the device with smaller value in the 10th to 14th bit of the device S/N will be prioritized.

Specifying the Hello Interval

Hello interval refers to the interval for the HA device to send heartbeats (Hello packets) to other devices in the HA group. The Hello interval in the same HA group must be identical. To specify the Hello interval, in the HA group configuration mode, use the following command:

hello interval *time-interval*

- *time-interval* – Specifies the interval for sending heartbeats. The value range is 50 to 10000 milliseconds. The default value is 1000.

To restore to the default Hello interval, in the HA group configuration mode, use the following command:

no hello interval

Specifying the Hello Threshold

If the device does not receive the specified number of Hello packets from the other device, it will judge that the other device’ s heartbeat fails. To specify the Hello threshold, in the HA group configuration mode, use the following command:

```
hello threshold value
```

- *value* – Specifies the Hello threshold value. The value range is 3 to 255. The default value is 3.

To restore to the default Hello threshold, in the HA group configuration mode, use the following command:

no hello threshold

Configuring the Preempt Mode

When the preempt mode is enabled, once the backup device find its own priority is higher than the master device, it will upgrade itself to the master device and the original master device will become the backup device. When the preempt mode is disabled, even if the device's priority is higher than the master device, it will not take over the master device unless the master device fails. When configuring the preempt mode, you can also set the delay time to make the backup device take over the master device after the specified delay time. To configure the preempt mode, in the HA group configuration mode, use the following command:

```
preempt [delay-time]
```

- *delay-time* – Specifies the delay time. The value range is 1 to 600 seconds. The default value is 30.

To cancel the preempt mode, in the HA group configuration mode, use **no preempt** command.

Specifying the Gratuitous ARP Packet Number

When the backup device is selected as the master device, it will send an ARP request packet to the network to inform the relevant network devices to update its ARP table. This command is used to specify the number of ARP packets the upgraded master device will send. The maximum number of gratuitous ARP packages sent by new master device is determined by the number of sending gratuitous ARP packets specified by this command. The system will send five gratuitous ARP packets immediately after device switching, and sending one ARP packets per second until the number of gratuitous ARP packets reaches the number specified by this command. To specify the gratuitous ARP packet number, in the HA group configuration mode, use the following command:

```
arp number
```

- *number* – Specify the gratuitous ARP packet number. The value range is 10 to 180. The default value is 15.

To restore to the default gratuitous ARP packet number, in the HA group configuration mode, use **no arp** command.

Sending Gratuitous ARP Packets

When the backup device is promoted to the master device, since the new master device only sent rather limited ARP packets to the network, some servers in the network may be unable to receive any ARP packets and therefore unable to update the ARP table. As a result, these servers may be unable to provide normal service within a short period. To solve the problem, the system supports sending gratuitous ARP packets manually via a specified interface. To send gratuitous ARP packets via the specified interface, in the execution mode, use the following command:

send gratuitous-arp interface *interface-name* [**count** *num* | **interval** *num*]

- **interface** *interface-name* – Specifies the interface on which gratuitous ARP packets are sent. This interface can be a physical interface, VSwitch interface, aggregate interface or redundant interface with an IP address configured.
- **count** *num* – Specifies the count for sending ARP packets. The value range is 0 to 60. The default value is 5. Value 0 indicates sending the packets consistently. You can stop sending by pressing Ctrl+C.
- **interval** *num* – Specifies the interval for sending ARP packets. The value range is 1 to 60 seconds. The default value is 1.

Specifying the Description

To specify description information, in the HA group configuration mode, use the following command:

description *string*

- *string* – Specifies the description information.

To cancel the description information, in the HA group configuration mode, use **no description** command.

Specifying the Track Object

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

monitor track *track-object-name*

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

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

> Note: It is recommended that the track object in the HA group should be configured with the Local property. For more information about how to configure the track object, see "Configuring a Track Object" of "System Management".

Configuring an HA group interface

To configure the interface for HA Group 0, in the global configuration mode, use the following command:

interface {**ethernet***m/n* | **redundant***number* | **aggregate***number* | **tunnel***number* | **loopback***number* | **bgroup***number* | **ethernet***m/n.tag* | **redundant***number.tag* | **aggregate***number.tag*}

> Tip: For more information about how to create and configure an interface, see "Interface" of "Firewall".

To configure the interface for HA Group 1, in the global configuration mode, use the following command:

interface {**ethernet***x/y:z* | **redundant***x:z* | **aggregate***x:z* | **tunnel***x:z* | **loopback***x:z* | **ethernet***x/y.u:z* | **redundant***x.y:z* | **aggregate***x.y:z*}

- **ethernet***x/y:z*: Specifies ethernetx/y as the interface for Group z and uses this interface for data forwarding.
- **redundant***x:z*: Specifies redundantx as the interface for Group z and uses this interface for data forwarding.
- **aggregate***x:z*: Specifies aggregatex as the interface for Group z and uses this interface for data forwarding.
- **tunnel***x:z*: Specifies tunnelx as the interface for Group z and uses this interface for data forwarding.
- **loopback***x:z*: Specifies loopbackx as the interface for Group z and uses this interface for data forwarding.
- **ethernet***x/y.u:z*: Specifies ethernetx/y.u as the interface for Group z and uses this interface for data forwarding.
- **redundant***x.y:z*: Specifies redundantx.y as the interface for Group z and uses this interface for data forwarding.
- **aggregate***x.y:z*: Specifies aggregatex.y as the interface for Group z and uses this interface for data forwarding.

To cancel the specified interface, in the global configuration mode, use the following command:

no interface {**ethernet***x/y:z* | **redundant***x:z* | **aggregate***x:z* | **tunnel***x:z* | **loopback***x:z* | **ethernet***x/y.u:z* | **redundant***x.y:z* | **aggregate***x.y:z*}

Configuring the Next-hop IP Address of the Interface

In the HA Peer mode network environment, to avoid the situation that fails to find the routes when synchronizing data with the peer device, you can configure the next-hop IP address of the interface, which ensures the successful creation of the sessions. To specify the next-hop IP address of the interface, use the following command in the interface configuration mode:

direct-send default-nexthop *A.B.C.D* [**local**]

- *A.B.C.D* – Specifies the next-hop IP address of the interface.
- **local** – If you enter this parameter, the system will not synchronize this configuration with the backup device. Without entering this parameter, this configuration will not be synchronized with the backup device.

In the interface configuration mode, use the following command to cancel the above configurations:

no direct-send default-nexthop [*A.B.C.D*] [**local**]

Configuring SNAT Port Distribution

HA supports the SNAT port distribution function. The function is that when you configure the same SNAT address pools for two HA devices, the system will averagely distribute the SNAT port resources according to the values of HA Node. If you disable this function, the SNAT address pool configured for each HA device must differ and each device will occupy the entire port resources. The SNAT port distribution function can only take effect I the HA Peer mode.

To enable the SNAT port distribution function, use the following command in the global configuration mode:

split-port-pool by ha-node

In the global configuration mode, use the following command to disable this function:

no split-port-pool by ha-node

Configuring an HA Link

The synchronization between the master and backup device and the Hello packets are transmitted over the HA link. There are two types of HA links, control Link and data Link. The control link is used to synchronize all data between two devices and the data link is used to synchronize the data packet information such as session information. According to your requirements, you can choose whether to configure the data link. If you configure the data ink, the Hello packets will be transmitted over the data link and the information of data synchronization and others will be transmitted over the control link. Without the data link configured, all synchronization information will be transmitted over the control link.

You need to specify the HA link interface first, and then specify the IP address of the interface.

Specifying an HA Link Interface

You can specify up to two HA control link interfaces. The later configured HA link interface serves as the backup interface for the first configured one. When the first interface disconnects, the later configured interface will take over the task of transmitting HA packets. To specify an HA control link interface, in the global configuration mode, use the following command:

ha link interface *interface-name*

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

To specify an HA data link interface, in the global configuration mode, use the following command:

ha link data interface *interface-name*

- *interface-name* – Specifies the name of the interface.
- **data** – Specify the type of the HA link as the data link. After specifying this data link, the session information will be synchronized over this data link. You can configure the physical interface or aggregate interface as the interface of the data link and you can specify at most 1 HA data link interface.

To delete the specified HA link interface, in the global configuration mode, use the following command:

no ha link interface *interface-name*

no ha link data interface *interface-name*

Specifying the IP Address of HA link Interface

After specifying the HA link interface, to configure the IP address of the HA link interface, in the global configuration mode, use the following command:

ha link ip *ip-address netmask*

- *ip-address netmask* – Specifies the IP addresses and the netmask of the HA link interface.

To cancel the specified IP address, in the global configuration mode, use the following command:

no ha link ip *ip-address netmask*

Configuring an HA Cluster

After configuring the HA group, HA group interface and HA link interface, you need to add the device to the HA cluster to make the HA function take effective. If there are more than one pair of HA devices in the network, you need to configure different HA cluster IDs, otherwise the MAC addresses may conflict. To configure an HA cluster, in the global configuration mode, use the following command:

ha cluster *cluster-id* [[**peer-mode node** *ID* [**symmetric-routing**]] | **node** *ID*]

- *cluster-id* – Specifies the HA cluster ID. The value varies depending on the HA virtual MAC prefix.
- **peer-mode node** *ID* – Configures the HA Peer mode and specifies the role of this device in the HA cluster. The range is 0 to 1. By default, the group 0 in the device whose HA Node ID is 0 will be active and the group 0 in the device whose HA Node ID is will be in the disabled status.
- **symmetric-routing** - If you enter this parameter, the device will work in the symmetrical routing environment.
- **node** *ID* - Specifies the HA Node value for the device. The values 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 value by automatic negotiation.

To disable the specified HA cluster, in the global configuration mode, use **no ha cluster** command.

Configuring a Management IP

To manage the HA backup device, you need to configure a management IP for the backup device. To configure a management IP address, in the interface configuration mode, use the following command:

manage ip *ip-address*

- *ip-address* - Specifies the management IP address.

Manually Synchronizing HA Information

In some exceptional circumstances, the master and backup configurations may not be synchronized. In such a case you need to manually synchronize the configuration information of the master and backup device. To determine if you need to manually synchronize the HA information, take the following steps:

1. View the relevant configuration information of both master and backup device by using the command **show**.

2. According to the displayed configuration information, determine whether you need to manually synchronize the HA information:

- If the configuration information is consistent, then you don't need to synchronize manually;
- If the configuration information is inconsistent, you need to run the corresponding commands to manually synchronize the configuration (for more information about the relevant commands, see table below).

Note:

- You do not need to manually synchronize the inconsistent local configuration information, such as the interface timeout information.
- For dynamic information, such as session information, you do not need to synchronize the information manually unless the dynamic information is not synchronized properly.

Commands to synchronize HA information manually are shown as below:

HA synchronization information	show command	Manual synchronization command
Configuration information	**show configuration**	**exec ha sync configuration**
File information	**show file**	**exec ha sync file** *file-name*
ARP table	**show arp**	**exec ha sync rdo arp**
DNS configuration information	**show ip hosts**	**exec ha sync rdo dns**
DNS rewrite rule information	**show dns-rewrite-rule**	**exec ha sync rdo dns-rewrite**
DHCP configuration information	**show dhcp**	**exec ha sync rdo dhcp**
MAC address table	**show mac**	**exec ha sync rdo mac**
PKI configuration information	**show pki key** **show pki trust-domain**	**exec ha sync rdo pki**

HA synchronization information	show command	Manual synchronization command
Session information	show session	exec ha sync rdo session
IPSec VPN information	show ipsec sa	exec ha sync rdo vpn
	show isakmp sa	
SCVPN information	show scvpn client test	exec ha sync rdo scvpn
	show scvpn host-check-profile	
	show scvpn pool	
	show scvpn user-host-binding	
	show scvpn session	
	show auth-user scvpn	
L2TP information	show l2tp tunnel	exec ha sync rdo l2tp
	show l2tp pool	
	show l2tp client {tunnel-name *name* [user *user-name*] | tunnel-id *ID*}	
	show auth-user l2tp [interface *interface-name* | vrouter *vrouter-name* | slot *slot-no*]	
WebAuth information	show auth-user webauth	exec ha sync rdo webauth
NTP information	show ntp	exec ha sync rdo ntp
SCVPN information	show scvpn	exec ha sync rdo scvpn
Route information	show ip route	exec ha sync rdo route
IGMP information	show ha sync statistic igmp	exec ha sync rdo igmp
	show ha sync state igmp	

Enabling/Disabling Automatic HA Session Synchronization

By default the system will synchronize sessions between HA devices automatically. Session synchronization will generate some traffic, and will possibly impact device performance when the device is overloaded. You can enable or disable automatic HA session synchronization according to the device workload to assure stability.

To enable or disable automatic HA session synchronization, in the global configuration mode, use the following command:

- Enable: **ha sync rdo session**
- Disable: **no ha sync rdo session**

Manually Switching Main and Backup Device Status of HA

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

exec ha master switch-over

Note:

- This command is only supported on the main device of HA.
- As the switching operation executes, this device is executing batch synchronization, which will result in failed switching of HA main and backup device status.

Backing up Statistical Data

In HA cluster, when one device fails, the other will take over the work of the failed device and also run its original work simultaneously to ensure uninterrupted work. In order to keep statistical data(such as monitor and log data) consistent after device switching, you can configure statistical data backup. After this feature is enabled, the system will send statistical data to both devices in the HA state, so that all data and configurations of two devices can be backed up. Due to the large amount of data to back up, we recommend that you configure Ten-GigabitEthernet interface (interface expansion module which owns Ten-GigabitEthernet interface is needed) or aggregate interface as ha link interface, otherwise it may cause inconsistent data. By default, this feature is disabled.

To back up statistical data to the other HA member, in the global configuration mode, use the following command:

ha analysis-data multicast

In the global configuration mode, use the following command to disable backup:

no ha analysis-data multicast

Note:Currently, you can only back up statistical data via CLI, not WebUI.

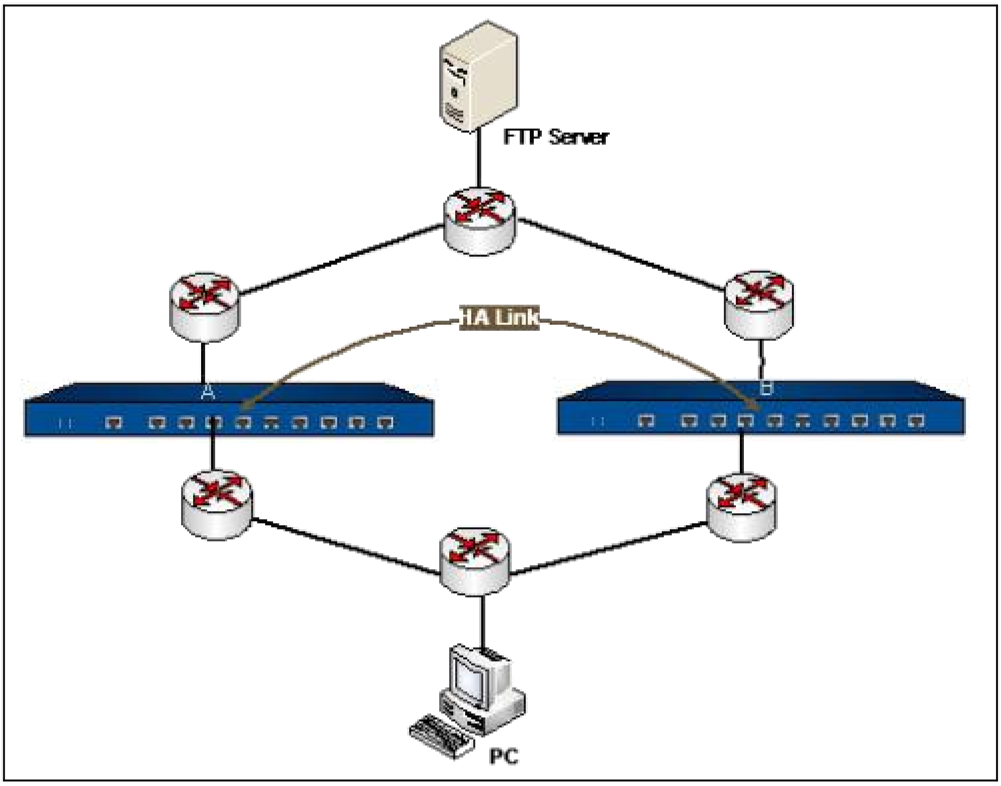
Viewing the Backup Status of Statistical Data

You can view the backup status of statistical data as needed, including whether statistical data backup is enabled or not, device online status, device priority, etc. To view the backup status of statistical data, in any mode, use the following command:

show ha apm state

Configuring HA Traffic

For the HA devices that are deployed in asymmetric routing environment (i.e., inbound and outbound traffic may take different routes), you can enable HA traffic to assure the inbound and outbound packets of a session are processed on the same device, thus avoiding session failure. Figure below illustrates a typical HA traffic application topology.



As shown in the figure above, the left route is from PC to the FTP server by the way of Device A. the right route is the same start and ending by the way of Device B. the metric value of these two routes are different from each other, making the network an asymmetric route. In addition, the FTP requests from PC are sent to the FTP server via Device A. In order to assure the response packets from the FTP server are returned to PC via Device A, you need to enable HA traffic on both Device A and Device B.

To enable HA traffic, use the following two steps:

1. Configure the two HA device to HA Peer mode;
2. Enable HA traffic.

Enabling HA Traffic

HA traffic is disabled by default. To enable or disable the function, in the global configuration mode, use the following commands:

- To enable: **ha traffic enable**
- To disable: no **ha traffic enable**

Note: After enabling the HA traffic function, the traffic between devices increase. FS recommends you first configure the interface of the data link.

Configuring HA Traffic Delay

When processing outbound packets, the device with HA traffic enabled will synchronize packet-related information with the pairing device. If the peer device responses (i.e., inbound packet) before the synchronization is completed, the sessions will not be matched and the response to the request packet will be dropped. To solve this problem, in the transparent mode, you can configure HA traffic delay. The device will wait for the specified delay time so that the synchronization will be completed, and then process inbound packets.

To configure HA traffic delay, in the global configuration mode, use the following commands:

ha traffic delay *num*

- *num* - Specifies the delay time. The value range is 1 to 50 ms. The default value is 3.

To cancel the above configurations, use the following command in the global configuration mode:

no ha traffic delay

Configuring First Packet Forwarding

In the routing mode, you can configure the first packet forwarding function to ensure that when processing outbound packets, the device will synchronize packet-related information with the pairing device. To configure the first packet forwarding function, use the following command in the global configuration mode:

ha traffic first-packet [**max-size** *num*]

- **max-size** *num* – Specifies the size of the first packet. The unit is byte. The value is 64 to 1024. Without configuring this parameter, the default value is 124.

To cancel the above configurations, use the following command in the global configuration mode:

no ha traffic first-packet

Viewing HA Configuration

To view the HA configuration information, use the following commands:

- Show the HA cluster configuration information: **show ha cluster**

- Show the HA group configuration information: **show ha group** {**config** | *group-id*}
- Show the HA link status: **show ha link status**
- Show the HA synchronization state: **show ha sync state** {**pki** | **dns** | **dhcp** | **vpn** | **ntp** | **config** | **flow** | **scvpn** | **route** | **igmp** }
- Show the HA traffic status: **show ha traffic**
- Show the HA synchronization statistics: **show ha sync statistic** {**pki** | **dns** | **dhcp** | **vpn** | **ntp** | **config** | **scvpn** | **route** | **igmp** }
- Show the HA protocol statistics: **show ha protocol statiscitc**
- Show the synchronized or unsynchronized HA session information: **show session** {**sync** | **unsync**}
- Show the HA statistics: **show ha flow** [[**slot** *slot-number*] | [**cpu** *cpu-number*]]**statistics**

Twin-mode HA

Introduction

Currently , data centers providing important data information and office services in many industries. In order to improve the reliability, companies generally build two or more data centers, and the extended mode of L2 (DCI: Data Center Interconnection) is used for inter-connections between two data centers. Two data centers running independently, providing business services and mutual backup, constitute a redundant data center.

The FS devices are deployed in the data center under the routing mode, used to check traffic and isolated by policy across different regions. Because of the DCI, the asymmetric L3 traffic that across the data center and different regions may occurs (i.e., inbound and outbound traffic may take different routes), the policy isolation will not take effect. To resolve this problem, system provides the Twin-mode HA function. This function will optimizes the traffic forwarding, ensuring the business continuity and efficiency of redundant data centers.

Note:

- This function only supports NSG-8100.
- Before configuring Twin Mode, make sure you have already installed Twin-mode License。
- This version does not support IPv6 function.

- You must enable HA function before enable the Twin-mode HA function, and the devices must in Active-Passive (A/P) mode.
- In twin-mode A/P mode or twin-mode A/A mode, you must configure the same HA cluster ID for the data center.

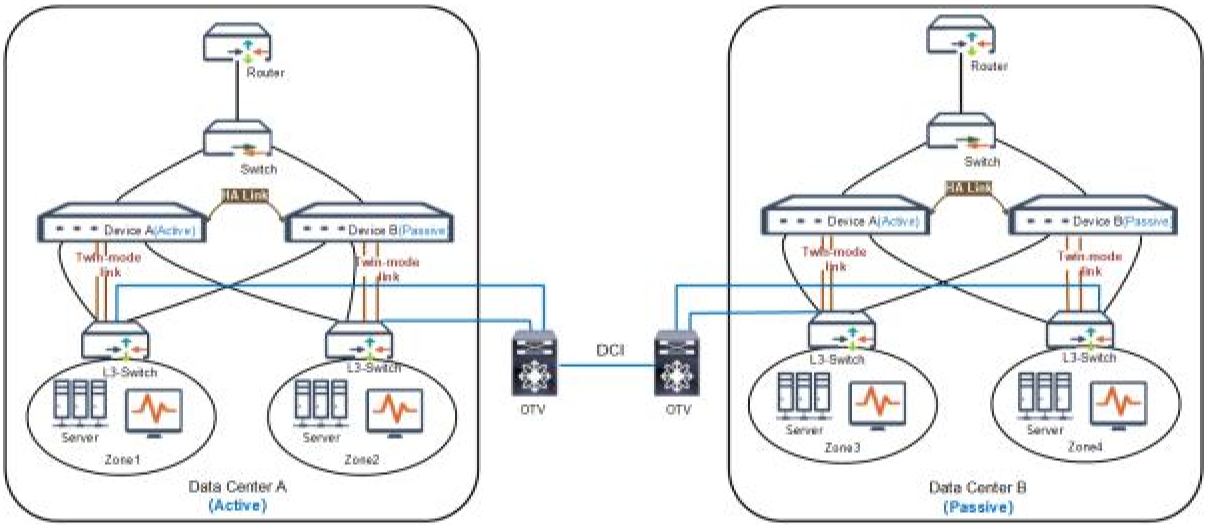
Currently, The system supports functions for Twin-mode HA listed in Table below. For more details and configuration, see relevant section.

Function			
Application Layer Gateway (ALG)	Interface	High Availablity (HA)	Routing
Application Layer Identification and Control	System Management	Log	Virtual System (VSYS)
Network Address Translation (NAT)	Monitor	Report	SNMP
Attack Defense	Firewall		

Twin-mode HA Deployment Scenarios

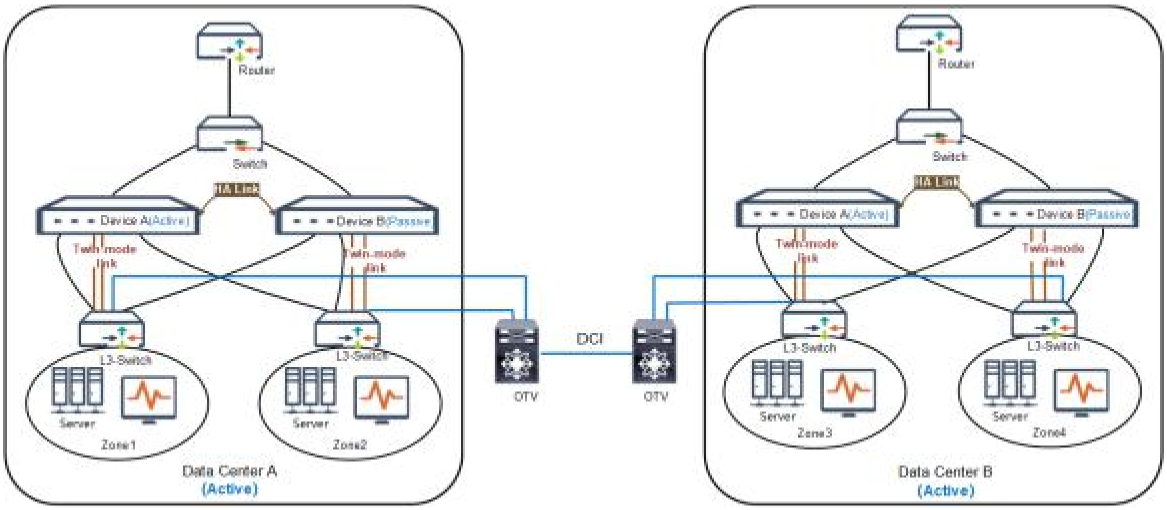
There are three kinds of typical L2TP twin-mode deployment scenarios:

- Active-Passive（A/P）deployment scenarios



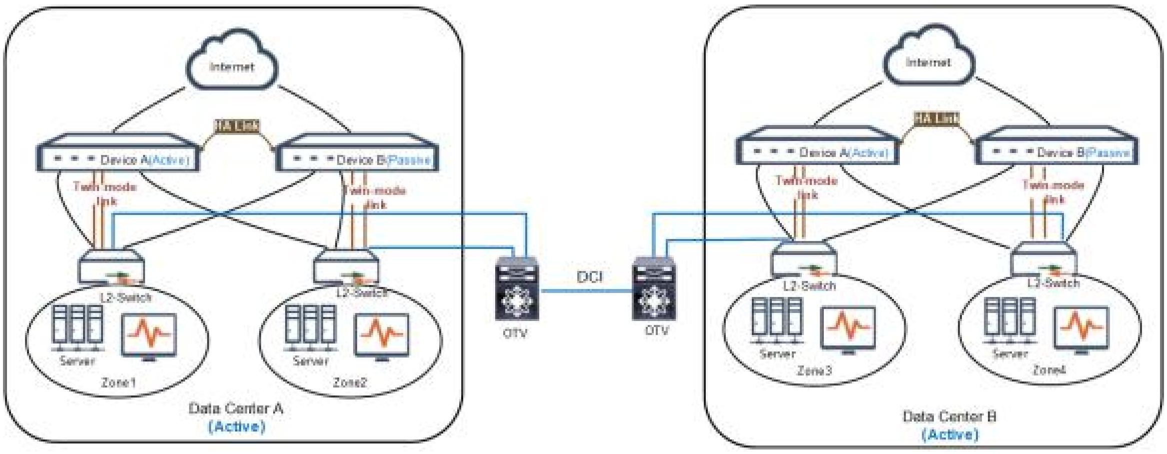
As shown in the figure above, configure two data center to form an HA group, with one data center acting as a master device and the other acting as its backup device. When the master data center fails, the backup data center will be promoted to master and take over its work to forward packets. The FS devices are deployed on each data center (you can use 3 straight series deployment or deploy the device in the gateway location), and make up the HA A/P mode.

- Active-Active（A/A）deployment scenarios



As shown in the figure above, the two data centers perform their own tasks simultaneously, and monitor the operation status of each other. When one data center fails, the other will take over the work of the failure device and also run its own tasks simultaneously to ensure uninterrupted work. The FS devices are deployed on each data center and make up the HA A/P mode. Through Twin-mode HA function, the problem of asymmetric L3 traffic that across the data center and different regions is solved.

- Gateway deployment scenarios: This deployment scenarios is a special Active-Active（A/A）deployment scenarios.



As shown in the figure above, the FS devices are deployed in the data center as a gateway and make up the HA A/P mode. The two data centers consist of twin-mode A/A mode, and backup each other. Since the extended device of L2 filters the same IP address and MAC address of the data center gateway, this problem is solved by deploying the gateway mode and configuring the twin-mode HA gateway function.

Twin-mode HA Synchronization

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

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

- Configuration information
- Session information
- ARP tabel
- Pinhole
- Track information
- Route information
- NTP information
- Signature file

In twin-mode HA A/A mode, the system supports two synchronous mode: Part synchronization and No synchronization. About configuration steps, refer to Specifying the deployment mode and synchronization mode. The types of information that can be synchronized includes:

- Configuration information (Policy/Service Book/Address Book/IPS/AV/URL/Schedule)
- Session information
- Pinhole
- Signature file

Configuring Twin-mode HA

The Twin-mode HA need to be configured in the Twin-mode configuration mode. To enter the Twin-mode configuration mode, in the global configuration mode, use the following command:

twin-mode

After executing the command, the system will enter the Twin-mode configuration mode.

In the Twin-mode configuration mode, you can perform the following configurations:

- Specifying the deployment mode and synchronization mode for Twin-mode HA

- Specifying the Node
- Specifying the Priority
- Configuring the Preempt Mode
- Specifying the Hello Interval
- Specifying the Hello Threshold
- Configuring Twin-mode HA Link
- Enabling/Disabling Twin-mode HA

Note:

- Before configuring the twin-mode function, you should install the Twin-mode License first.
- The deployment mode, node value, link must be specified.

Specifying the deployment mode and synchronization mode

Currently, supports two deployment modes for Twin-mode HA: A/A mode and A/P mode. The system supports two synchronization mode: Part synchronization and No synchronization. In the Twin-mode configuration mode, use the following command:

mode {**active-active** [**no-sync** | **part-sync**] | **active-passive** }

- **active-active** [**no-sync** | **part-sync**] – Specifies the deployment mode is A/A mode.
- **no-sync** - Specifies the synchronization mode is no synchronization.
- **part-sync** - Specifies the synchronization mode is part synchronization mode. About specific synchronization information content, refer to Twin-mode HA Synchronization
- **active-passive** – Specifies the deployment mode is A/P mode.

To cancel the specified deployment mode, in the Twin-mode configuration mode, use the following command:

no mode

Specifying the Node

To distinguish the data center, you can use the value of Node to mark the data center. To specify the Node, in the global configuration mode, use the following command:

node *node-ID*

- *node-ID* – Specifies the Node. The range is 0 to 1.

To cancel the specified Node, in the Twin-mode configuration mode, use the following command:

no node

Note:

- You must specify the different Node for each data center.
- User needs to restart the device to make it take effect after modifying the Node.

Specifying the Priority

The priority specified by the command is for used for HA selection. The device with higher priority (the smaller number) will be selected as the master device of data center. To specify the priority, in the Twin-mode configuration mode, use the following command:

priority *number*

- *number* – Specifies the priority. The value range is the 1 to 254. The default value is 100.

To restore to the default priority, in the Twin-mode configuration mode, use the following command:

no priority

Tip: When the priorities are identical, the device with Node 0 will be prioritized.

Configuring the Preempt Mode

When the preempt mode is enabled, once the backup device find its own priority is higher than the master device, it will upgrade itself to the master device and the original master device will become the backup device. When the preempt mode is disabled, even if the device's priority is higher than the master device, it will not take over the master device unless the master device fails. When configuring the preempt mode, you can also set the delay time to make the backup device take over the master device after the specified delay time. To configure the preempt mode, in the Twin-mode configuration mode, use the following command:

preempt [*delay-time*]

- *delay-time* - Specifies the delay time. The value range is 1 to 600 seconds. The default value is 3.

To cancel the preempt mode, in the Twin-mode configuration mode, use the following command:

no preempt

Specifying the Hello Interval

Hello interval refers to the interval for the HA device to send heartbeats (Hello packets) to other devices in the HA group. The Hello interval in the same HA group must be identical. To specify the Hello interval, in the Twin-mode configuration mode, use the following command:

hello interval *time-interval*

- *time-interval* - Specifies the interval for sending heartbeats. The value range is 1 to 100 seconds. The default value is 1s.

To restore to the default Hello interval, in the Twin-mode configuration mode, use the following command:

no hello interval

Specifying the Hello Threshold

If the device does not receive the specified number of Hello packets from the other device, it will judge that the other device's heartbeat fails. To specify the Hello threshold, in the Twin-mode configuration mode, use the following command:

hello threshold *value*

- *value* - Specifies the Hello threshold value. The value range is 5 to 255. The default value is 10.

To restore to the default Hello threshold, in the Twin-mode configuration mode, use the following command:

no hello threshold

Configuring Twin-mode HA Link

There are two types of Twin-mode HA links, control Link and data Link. Currently, system only support to specify the physical interfaces and aggregation interfaces as a Twin-mode HA link interface.

You need to specify the Twin-mode HA link interface first, and then specify the IP address and peer IP address of the interface.

Specifying a Twin-mode HA Link Interface

To specify a Twin-mode HA link interface, in the Twin-mode configuration mode, use the following command:

link {**control** | **data** } **interface** *interface-name*

- **control** | **data** - Specifies the Twin-mode HA link type.
- *interface-name* – Specifies the name of the interface.

To delete the specified Twin-mode HA link interface, in the Twin-mode configuration mode, use the following command:

no link { **control** | **data** } **interface** *interface-name*

Note:

- Control Link and Data Link can specify up to two interfaces.
- When asymmetric data traffic is larger, it is recommended that users use two data links or using a aggregate interface to ensure sufficient bandwidth for transmitting data traffic.

Specifying the IP Address of Twin-mode HA link Interface

After specifying the Twin-mode HA link interface, to configure the IP address of the Twin-mode HA link interface, in the Twin-mode configuration mode, use the following command:

link ip *ip-address netmask*

- *ip-address netmask* - Specifies the IP addresses and the netmask of the Twin-mode HA link interface.

To cancel the specified IP address, in the Twin-mode configuration mode, use the following command:

no link ip *ip-address netmask*

Specifying the Peer IP Address

To configure the peer IP address, in the Twin-mode configuration mode, use the following command:

link peer-ip *ip-address*

- *ip-address* – Specifies the peer IP addresses.

To cancel the specified peer IP address, in the Twin-mode configuration mode, use the following command:

no link peer-ip

Enabling/Disabling Twin-mode HA

By default the Twin-mode HA function is disabled. To enable or disable Twin-mode HA, in the Twin-mode configuration mode, use the following command:

- Enable: **enable**
- Disable: **no enable**

Specifying the Forwarding Mode of Asymmetric Traffic

For the asymmetric traffic, Twin-mode HA provides two forwarding mode: tunnel mode and layer 2 tunnel mode.

- Tunnel Mode: The encapsulated package will be sent to the peer data center through Data Link, after the traffic was de-encapsulated , the peer data center will transfer it. By default, the forwarding mode is tunnel mode.
- Layer 2 Tunnel Mode: The MAC address of the packet is modified as the virtual MAC (VMAC) address which corresponds to its interface of peer data center, the traffic is forwarded through layer 2 tunnel. With this mode, the user needs to enable the layer 2 tunnel forwarding mode at all business interfaces of the device.

To enable the layer 2 tunnel forwarding mode, in the interface configuration mode, , use the following command:

twin-mode-l2-tunnel-enable

To restore to the default forwarding mode, in the interface configuration mode, use the following command:

no twin-mode-l2-tunnel-enable

> Note:The forwarding mode must be specified. The two modes cannot be mixed, otherwise the function is not effective.

Configuring Twin-mode HA Gateway

In the gateway deployment scenarios, because the extended device of L2 filters the same IP address and MAC address of the data center gateway, the asymmetric traffic blocked. In order to avoid this problem, you needs to enable the twin-mode gateway function, and configure gateway interface IP address for sending the ARP request message, the system will take this IP address as the source of IP, Twin-mode virtual MAC (VMAC) as the source MAC address to send the ARP request message, and forward the data traffic with Twin-mode virtual MAC (VMAC) address as the source address, so as to solve the problem of asymmetric traffic.

To enable the twin-mode gateway function and configure gateway interface IP address for sending the ARP request message, in the interface configuration mode, use the following command:

twin-mode-gateway sender-ip *ip-address*

- *ip-address* － Specifies the gateway interface IP address for sending the ARP request message. This IP address must be in the same network segment as the IP address of the gateway interface.

To disable this function and delete the specified IP address, in the interface configuration mode, use the following command:

no twin-mode-gateway sender-ip *ip-address*

Note:The gateway interface IP for sending ARP request messages of both data centers must be different.

Configuring the Switching Mode of Twin-mode HA Session State

In the twin-mode HA A/A mode, system supports two switching modes of twin-mode HA session state, including unidirectional switching and bidirectional switching.

- Unidirectional switching: When a link of access extranet server fails in the data center, the system will quickly switch the inactive twin-mode HA session state to the active state, and ensure that the traffic will not be interrupted.
- Bidirectional switching: When you need to modify the traffic forwarding path of data center, you can use this switching mode, the system will quickly switch the inactive twin-mode HA session state to the active state, so as to optimize the traffic paths.

To configure the switching mode of twin-mode HA session state, in the Flow configuration mode, use the following command:

twin-mode-sess-owner-change {**follow-init-direction** | **follow-two-direction**}

- **follow-init-direction** － Unidirectional switching, when the traffic hits the upstream traffic of the inactive session, the system will switch the session state.
- **follow-two-direction** － Bidirectional switching, when the traffic hits both the upstream and downstream traffic of the inactive session, the system will switch the session state.

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

no twin-mode-sess-owner-change

Tip: To enter the flow configuration mode, in the global configuration mode, use the command **flow**.

Manually Synchronizing Twin-mode HA Configuration Information

In some exceptional circumstances, the master and backup configurations of data center may not be synchronized. In such a case you need to manually synchronize the twin-mode HA configuration information of the master and backup data center. To determine if you need to manually synchronize the twin-mode HA information, take the following steps:

1. View the relevant configuration information of both master and backup data center by using the command **show twin-mode configuration difference** on the master device.

2. According to the displayed configuration information, determine whether you need to manually synchronize the twin-mode HA information:

- If the configuration information is consistent, then you don’t need to synchronize manually;

- If the configuration information is inconsistent, you need to run the command**exec twin-mode sync configuration**to manually synchronize the configuration.

Note:The command **exec twin-mode sync configuration** can only be executed on the master HA device of the master data center.

Viewing/Clearing the Transfer Packet Count of Twin-mode HA

To view the transfer packet count of Twin-mode HA, in any mode, use the following command:

show twin-mode-counter

To clear the transfer packet count of Twin-mode HA, in any mode, use the following command:

clear twin-mode-counter

Viewing Twin-mode HA Configuration

To view the Twin-mode HA configuration information, use the following commands:

- Show the Twin-mode HA configuration information: **show twin-mode configuration**

- Show the Twin-mode HA link information: **show twin-mode link**

- Show the Twin-mode HA peer status: **show twin-mode peer**

- Show the Twin-mode HA status: **show twin-mode status**

Examples of HA

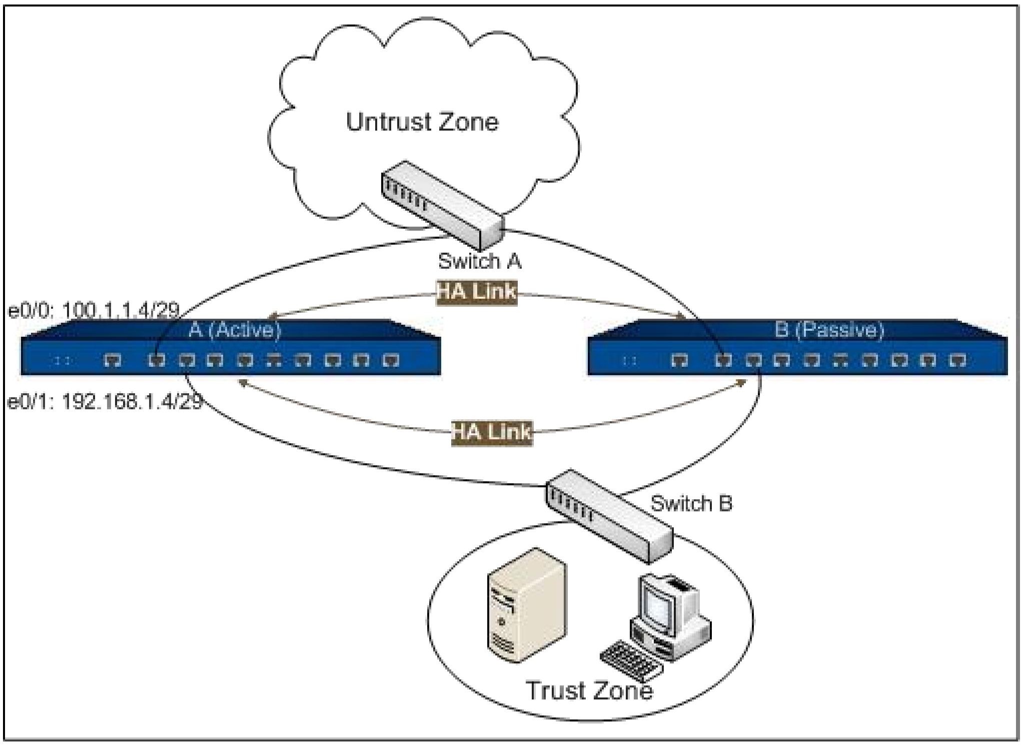
This section describes three HA configuration examples:

- Example 1: configuration example of HA in A/P mode
- Example 2: configuration example of HA in A/A mode
- Example 3: configuration example of HA Peer mode and HA traffic
- Example 4: configuration example of specific scenarios of HA A/A mode

Example 1: Example of HA in A/P Mode

Requirement

To goal is use two FS devices, which are of the same hardware platform, firmware version, and license, to a form an HA cluster in Active-Passive mode. In addition, the two devices are using the same interface to connect to the network. The network topology is shown below:



Configuration Steps

Step 1: Configure the interfaces and policy rules on Device A:

```
Device A
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 100.1.1.4/29
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.1.4/29
hostname(config-if-eth0/1)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 2: Configure a track object which is used for tracking the status of interface of the master device, and if the interface ethernet0/0 fails, the device will implement failover:

```
hostname(config)# track trackobj1
hostname(config-trackip)# interface ethernet0/0 weight 255
hostname(config-trackip)# exit
hostname(config)#
```

Step 3: Configure an HA group:

```
Device A
hostname(config)# ha group 0
hostname(config-ha-group)# priority 50
hostname(config-ha-group)# monitor track trackobj1
hostname(config-ha-group)# exit
hostname(config)#
```

```
Device B
hostname(config)# ha group 0
hostname(config-ha-group)# priority 100
hostname(config-ha-group)# exit
hostname(config)#
```

Step 4: Configure HA link interfaces and enable the HA function:

```
Device A
hostname(config)# ha link interface ethernet0/2
hostname(config)# ha link interface ethernet0/3
hostname(config)# ha link ip 1.1.1.1/24
hostname(config)#
```

```
Device B
hostname(config)# ha link interface ethernet0/2
hostname(config)# ha link interface ethernet0/3
hostname(config)# ha link ip 1.1.1.2/24
hostname(config)#
```

Step 5: Configure an HA cluster to enable HA:

```
Device A
hostname(config)# ha cluster 1
Device B
hostname(config)# ha cluster 1
```

Step 6: Configure the management IPs of the master device and backup device after synchronization:

```
Device A
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# manage ip 192.168.1.253
```

```
Device B
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# manage ip 192.168.1.254
```

Step 7: Configure a track object on Device B, and if the interface ethernet0/0 on Device B fails, the device will implement failover:

```
Device B
hostname(config)# ha group 0
hostname(config-ha-group)# monitor track trackobj1
hostname(config-ha-group)# exit
hostname(config)#
```

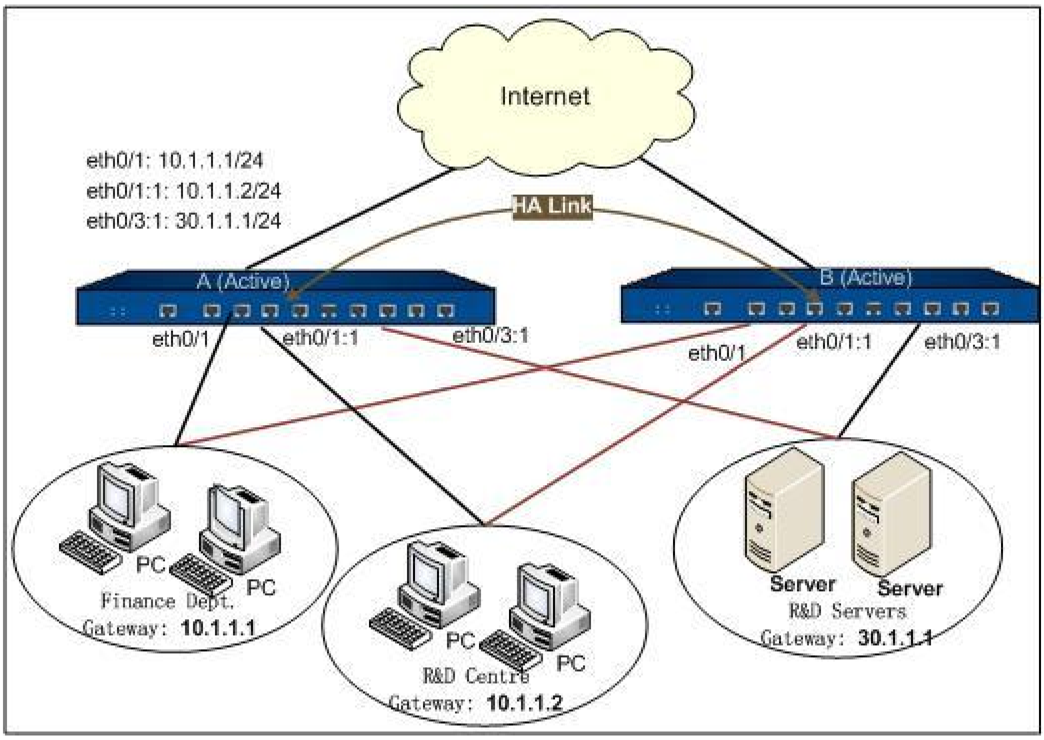
After the above configuration, the system will select Device A as the master device for forwarding traffic. Device B acts as the backup device. Device A will synchronize its configuration information and status to Device B. When Device A fails and cannot forward traffic, or the ethernet0/0 of Device A is disconnected, Device B will switch to the master device without interrupting user’ s communication, and continue to forward the traffic.

Example 2: Example of HA in A/A Mode

Requirement

This section describes a typical redundant HA Active-Active mode configuration example. Before configuring, make sure the two FS devices constructing the HA structure are using the same hardware platform, firmware version, and license, been installed with anti-virus licenses, and the two devices are using the same interface to connect to the network.

After completing the configuration, both of the two devices enable the HA function. Device A is selected as the master device of HA group0, and synchronizes information to Device B. And Device B will preempt to be the master device of HA group1. Under normal conditions, Device A and Device B operate independently, Device A forwarding the traffic of Finance Department and R&D Center, Device B forwarding the traffic of R&D servers. If one of the two devices fails, the other can take over its work and go on forwarding traffic without interruption. For example, if Device B fails, Device A will forward the traffic of Finance Department, R&D Center and R&D servers. The network topology is shown below:



Configuration Steps

Step 1: Configure HA groups:

```
Device A
hostname(config)# ha group 0
hostname(config-ha-group)# priority 10
hostname(config-ha-group)# arp 15
hostname(config-ha-group)# preempt 3
hostname(config-ha-group)# exit
hostname(config)# ha group 1
hostname(config-ha-group)# priority 200
hostname(config-ha-group)# preempt 3
hostname(config-ha-group)# exit
```

```
Device B
hostname(config)# ha group 0
hostname(config-ha-group)# priority 200
hostname(config-ha-group)# arp 15
hostname(config-ha-group)# preempt 3
hostname(config-ha-group)# arp 15
hostname(config-ha-group)# exit
hostname(config)# ha group 1
hostname(config-ha-group)# priority 20
hostname(config-ha-group)# arp 15
hostname(config-ha-group)# preempt 3
hostname(config-ha-group)# exit
```

Step 2: Configure the interfaces and zone on Device A:

```
Device A
hostname(config)# zone caiwu
hostname(config-zone-caiwu)# exit
hostname(config)# zone yanfa
hostname(config-zone-yanfa)# exit
hostname(config)# zone internet
hostname(config-zone-intern~)# exit
hostname(config)# zone server
hostname(config-zone-server)# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone internet
hostname(config-if-eth0/0)# ip address 192.168.1.1 255.255.255.0
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone caiwu
hostname(config-if-eth0/1)# ip address 10.1.1.1 255.255.255.0
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet 0/0:1
hostname(config-if-eth0/0:1)# zone internet
hostname(config-if-eth0/0:1)# ip address 192.168.1.2 255.255.255.0
hostname(config-if-eth0/0:1)# exit
hostname(config)# interface ethernet 0/1:1
hostname(config-if-eth0/1:1)# zone yanfa
hostname(config-if-eth0/1:1)# ip address 10.1.1.2 255.255.255.0
hostname(config-if-eth0/1:1)# exit
hostname(config)# interface ethernet 0/3:1
hostname(config-if-eth0/3:1)# zone server
```

```
hostname(config-if-eth0/3:1)# ip address 30.1.1.1 255.255.255.0
hostname(config-if-eth0/3:1)# exit
hostname(config)#
```

Step 3: Configure track objects which are used for tracking the status of interfaces of device A and device B. If the interfaces fail, the device will implement failover:

```
 Device A
hostname(config)# track group0
hostname(config-trackip)# interface ethernet0/0
hostname(config-trackip)# exit
hostname(config)# track group1
hostname(config-trackip)# interface ethernet0/1:1
hostname(config-trackip)# interface ethernet0/3:1
hostname(config-trackip)# exithostname(config)# ha group 0
hostname(config-ha-group)# monitor track group0
hostname(config-ha-group)# exit
hostname(config)# ha group 1
hostname(config-ha-group)# monitor track group1
hostname(config-ha-group)# exit
```

```
Device B
hostname(config)# track group0
hostname(config-trackip)# interface ethernet0/0
hostname(config-trackip)# exit
hostname(config)# track group1
hostname(config-trackip)# interface ethernet0/1:1
hostname(config-trackip)# interface ethernet0/3:1
hostname(config-trackip)# exit
hostname(config)# ha group 0
hostname(config-ha-group)# monitor track group0
hostname(config-ha-group)# exit
hostname(config)# ha group 1
hostname(config-ha-group)# monitor track group1
hostname(config-ha-group)# exit
```

Step 4: Configure interfaces of HA links:

```
Device A
hostname(config)# ha link interface ethernet0/4
hostname(config)# ha link ip 100.0.0.1 255.255.255.0
hostname(config)#
```

```
Device B
hostname(config)# ha link interface ethernet0/4
hostname(config)# ha link ip 100.0.0.100 255.255.255.0
hostname(config)#
```

Step 5: Configure SNAT on Device A:

```
Device A
```

```
hostname(config)# address caiwu
hostname(config-addr)# ip 10.1.1.1/24
hostname(config-addr)# exit
hostname(config)# address yanfa
hostname(config-addr)# ip 10.1.1.2/24
hostname(config-addr)# exit
hostname(config)# nat
hostname(config-nat)# snatrule id 1 from caiwu to any eif ethernet0/0 trans-to eif-ip
mode dynamicport
rule ID=1
hostname(config-nat)# snatrule id 2 from yanfa to any eif ethernet0/0:1 trans-to eif-ip
mode dynamicport group 1
rule ID=2 mode dynamicport group 1
hostname(config-nat)# exit
hostname(config)#
```

Step 6: Configure policy rules on Device A:

Device A

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone caiwu
hostname(config-policy-rule)# dst-zone internet
hostname(config-policy-rule)# src-addr caiwu
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone yanfa
hostname(config-policy-rule)# dst-zone internet
hostname(config-policy-rule)# src-addr yanfa
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone yanfa
hostname(config-policy-rule)# dst-zone server
hostname(config-policy-rule)# src-addr yanfa
hostname(config-policy-rule)# dst-addr server
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
```

Step 7: Configure an HA cluster to enable HA:

```
Device A
hostname(config)# ha cluster 1
```

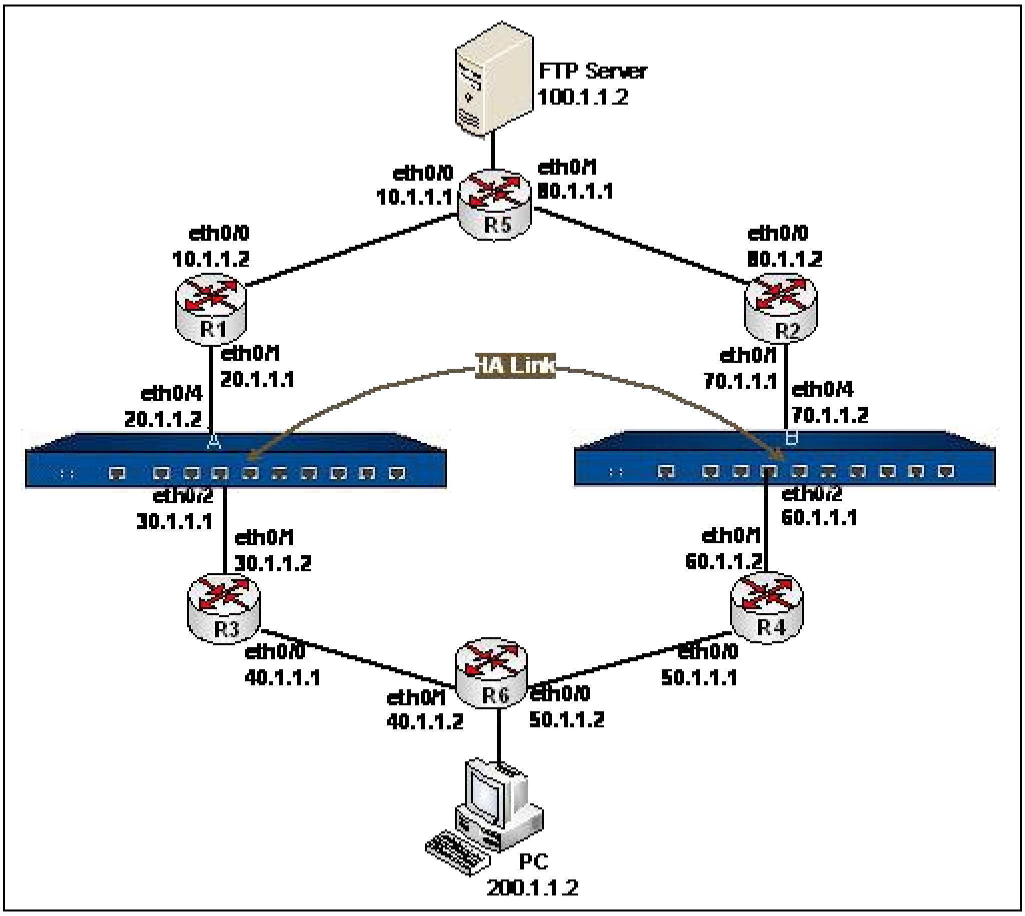
```
Device B
hostname(config)# ha cluster 1
```

Example 3: Example of HA Peer Mode and HA Traffic

Requirement

This section describes how to configure HA Peer mode and HA traffic in asymmetrical routing environment. Before configuring, make sure the two FS devices that will adopt HA Peer mode are using the same hardware platform, firmware version, license, and the interfaces that are connected to the network belong to the same security zone.

After completing the configuration, both of the two devices enable HA traffic. When PC requests any virus file in zip format from the FTP server, this function can assure the inbound and outbound packets will be processed on Device A, and related logs will also be generated on Device A. The network topology is shown below:



Configuration Steps

The following steps omit the configuration of interfaces and zones, and only focus on the configuration of HA Peer mode and HA traffic.

Step 1: Configure HA Peer mode and HA link interfaces:

Device A

```
hostname(config)# ha link interface eth0/1
hostname(config)# ha link ip 1.1.1.1/24
hostname(config)# ha link data interface eth0/3
hostname(config)# ha cluster 1 peer-mode node 0
hostname(config)# exit
```

Device B

```
hostname(config)# ha link interface eth0/1
hostname(config)# ha link ip 1.1.1.2/24
hostname(config)# ha link data interface eth0/3
hostname(config)# ha cluster 1 peer-mode node
hostname(config)# exit
```

Step 2: Enable HA traffic:

```
Device A
hostname(M0D1) (config)# ha traffic enable
hostname(M0D1) (config)# exit
```

```
Device B
hostname(D0M1) (config)# ha traffic enable
hostname(D0M1) (config)# exit
```

Step 3: Configure the asymmetric routing environment. Assume that all routers use the OSPF protocols and you have set the default metric and cost:

```
Device A
hostname(M0D1) (config) # ip vrouter trust-vr
hostname(M0D1) (config-vrouter)# router ospf
hostname(M0D1) (config-router) # router-id 1.1.1.1 local
hostname(M0D1) (config-router) # network 20.1.1.1/24 area 0
hostname(M0D1) (config-router) # network 30.1.1.1/24 area 0
hostname(M0D1) (config-router)# network 60.1.1.1/24 area 0
hostname(M0D1) (config-router)# network 70.1.1.1/24 area 0
hostname(M0D1) (config-router)# exit
hostname(M0D1)# config
hostname(M0D1) (config)# interface eth0/2
hostname(M0D1) (config-if-eth0/2)# zone trust
hostname(M0D1) (config-if-eth0/2)# ip address 30.1.1.1/24
hostname(M0D1) (config-if-eth0/2)# exit
hostname(M0D1) (config)# interface eth0/2:1
hostname(M0D1) (config-if-eth0/2:1)# zone trust
hostname(M0D1) (config-if-eth0/2:1)# ip address 60.1.1.1/24
hostname(M0D1) (config-if-eth0/2:1)# exit
hostname(M0D1) (config)# interface eth0/4
hostname(M0D1) (config-if-eth0/4)# zone trust
hostname(M0D1) (config-if-eth0/4)# ip address 20.1.1.2/24
hostname(M0D1) (config-if-eth0/4)# exit
hostname(M0D1) (config)# interface eth0/4:1
hostname(M0D1) (config-if-eth0/4:1)# zone trust
hostname(M0D1) (config-if-eth0/4:1)# ip address 70.1.1.2/24
hostname(M0D1) (config-if-eth0/4:1)# exit
hostname(M0D1) (config-if-eth0/4:1)# end
```

```
Device B
hostname(D0M1) (config)# ip vrouter trust-vr
hostname(D0M1) (config-vrouter)# router ospf
hostname(D0M1) (config-router)# router-id 1.1.1.2 local
```

Step 4: Configure a track object to monitor the status of ethernet0/1 on R3. If the interface fails, all the sessions will be switched to Device B:

```
Device A
hostname(M0D1) (config)# track track1
hostname(M0D1) (config-trackip)# ip 30.1.1.2 interface eth0/2
hostname(M0D1) (config-trackip)# exit
hostname(M0D1) (config)# ha group 0
hostname(M0D1) (config-ha-non-group)# monitor track track1
hostname(M0D1) (config-ha-non-group)# exit
```

Step 5: Configure an AV profile on Device A and bind to the security zone:

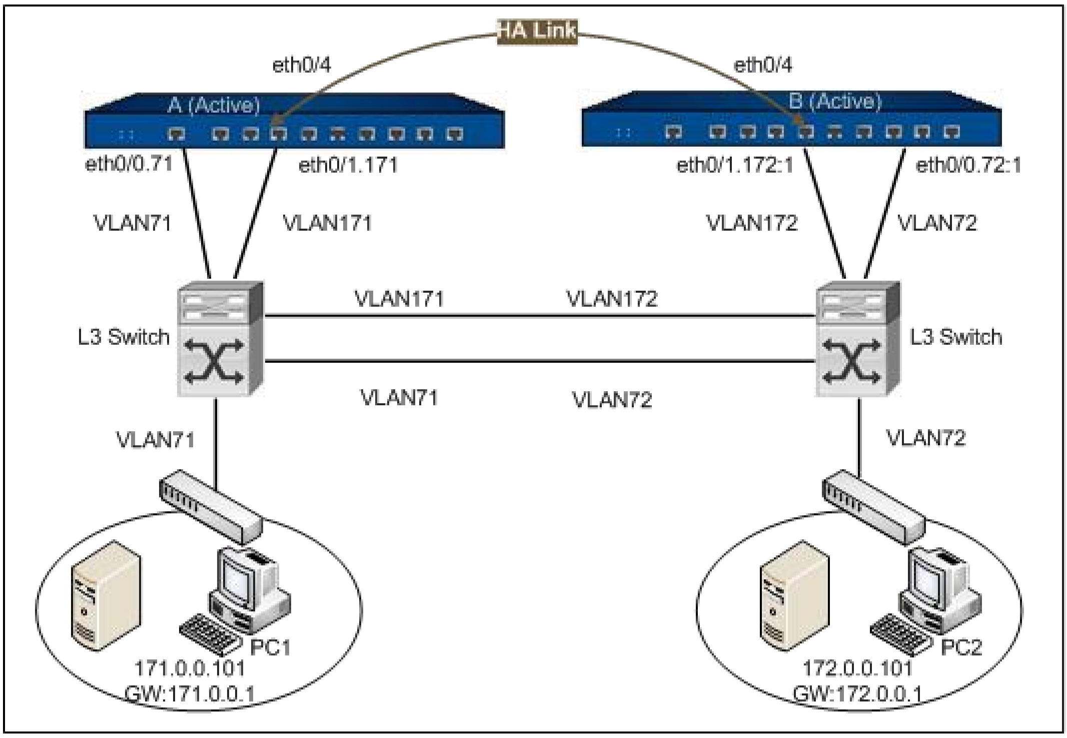
```
Device A
hostname(M0D1) (config)# av-profile av
hostname(M0D1) (config-av-prifile)# profile-type ftp action log-only
hostname(M0D1) (config-av-prifile)# file-type zip
hostname(M0D1) (config-av-prifile)# exit
hostname(M0D1) (config)# zone untrust
hostname(M0D1) (config-zone-untrust)# av enable av
hostname(M0D1) (config-zone-untrust)# exit
```

Example 4: Example of Configuring Specific Scenarios of HA A/A Mode

Requirement

PC1 and PC2 individually belong to different VLANs, and by configuring VRRP and STP, they accomplish the redundant backup.

PC1 and PC2 individually belong to different VLANs; the redundancy is implemented via VRRP and STP in L3 switches. Two FS devices are accessed in bypass mode. The goal is to implement HA A/A redundancy and access control between VLANs. The network topology is shown as below:



Configure as follows:

- Configure the two devices to HA A/A mode;
- Configure Virtual Wire to allow traffic between VLANs;
- Configure policy rules to implement access control between VLANs.

Configuration Steps

Step 1: Configure a track object to monitor the interface status of Device A and Device B. If the interface fails, all the sessions will be switched to Device B:

Device A

```
hostname(config)# track group0
hostname(config-trackip)# interface ethernet0/0.71
hostname(config-trackip)# interface ethernet0/1.171
hostname(config-trackip)# exit
hostname(config)# track group1
hostname(config-trackip)# interface ethernet0/0.72:1
hostname(config-trackip)# interface ethernet0/1.172:1
hostname(config-trackip)# exit
hostname(config)#
```

Step 2: Configure an HA group:

```
Device A
hostname(config)# ha group 0
hostname(config-ha-group)# priority 50
hostname(config-ha-group)# preempt 1
hostname(config-ha-group)# monitor track group0
hostname(config-ha-group)# exit
hostname(config)# ha group 1
hostname(config-ha-group)# priority 150
hostname(config-ha-group)# preempt 1
hostname(config-ha-group)# exit
hostname(config)#
```

```
Device B
hostname(config)# ha group 0
hostname(config-ha-group)# priority 150
hostname(config-ha-group)# preempt 1
hostname(config-ha-group)# exit
hostname(config)# ha group 1
hostname(config-ha-group)# priority 50
hostname(config-ha-group)# preempt 1
hostname(config-ha-group)# monitor track group0
hostname(config-ha-group)# exit
hostname(config)#
```

Step 3: Configure HA link interfaces:

```
Device A
hostname(config)# ha link interface ethernet0/4
hostname(config)# ha link ip 77.77.77.1 255.255.255.0
```

```
Device B
hostname(config)# ha link interface ethernet0/4
hostname(config)# ha link ip 77.77.77.2 255.255.255.0
```

Step 4: Configure interfaces and zones of Device A:

```
Device A
hostname(config)# zone l2-trust-1 l2
hostname(config-zone-l2-tru~)# exit
hostname(config)# zone l2-trust-2 l2
hostname(config-zone-l2-tru~)# exit
hostname(config)# zone l2-untrust-1 l2
hostname(config-zone-l2-unt~)# exit
hostname(config)# zone l2-untrust-2 l2
hostname(config-zone-l2-unt~)# exit
hostname(config)# interface ethernet0/0.71
hostname(config-if-eth0/0.71)# zone l2-trust-1
hostname(config-if-eth0/.71)# exit
hostname(config)# interface ethernet0/0.72:1
hostname(config-if-eth0/0.72:1)# zone l2-trust-2
hostname(config-if-eth0/0.72:1)# exit
hostname(config)# interface ethernet0/1.171
hostname(config-if-eth0/1.171)# zone l2-untrust-1
hostname(config-if-eth0/1.171)# exit
hostname(config)# interface ethernet0/1.172:1
hostname(config-if-eth0/1.172:1)# zone l2-untrust-2
hostname(config-if-eth0/1.172:1)# exit
hostname(config)#
```

Step 5: Configure Virtual Wire on Device A:

```
Device A
hostname(config)# vswitch vswitch1
hostname(config-vswitch)# ha-gratuious-mac-enable
hostname(config-vswitch)# virtual-wire set ethernet0/0.71 ethernet0/1.171
hostname(config-vswitch)# virtual-wire set ethernet0/0.72:1 ethernet0/1.172:1
hostname(config-vswitch)# virtual-wire enable unstrict
hostname(config-vswitch)# exit
hostname(config)#
```

Step 6: Configure policy rules on Device A:

```
Device A
hostname(config)# policy-global
hostname(config-policy)# rule
Rule id 1 is created
hostname(config-policy-rule)# src-zone l2-trust-1
hostname(config-policy-rule)# dst-zone l2-untrust-1
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
Rule id 2 is created
hostname(config-policy-rule)# src-zone l2-untrust-1
hostname(config-policy-rule)# dst-zone l2-trust-1
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
Rule id 3 is created
hostname(config-policy-rule)# src-zone l2-trust-2
hostname(config-policy-rule)# dst-zone l2-untrust-2
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
```

```
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
Rule id 4 is created
hostname(config-policy-rule)# src-zone l2-untrust-2
hostname(config-policy-rule)# dst-zone l2-trust-2
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 7: Configure the HA cluster and enable the HA function:

```
Device A
hostname(config)# ha cluster 1
```

```
Device B
```

```
hostname(config)# ha cluster 1
```

Chapter 7 IPv6

System supports IPv6 (Internet Protocol Version 6). Compared with IPv4, IPv6's noticeable advantages include larger address space, simplified header, flexible header expansion and options, hierarchical address allocation, automatic stateless address allocation, data security supported by IPsecIPSec header, stronger QoS management support, etc.

FSOS is dual-stack firmware that supports both IPv4 and IPv6. It also supports tunneling technique (the latest version supports manual IPv6 tunnel) for IPv6 communication.

This chapter describes IPv6 configuration of FSOS, including:

Note:All the IPv6-related functions in the current firmware version support multiple VRs, i.e. system support the default VR trust-vr.

Configuring an IPv6 Address

FS devices support dual stacks, so the interfaces can support IPv4 and IPv6 addresses simultaneously. By default only IPv4 is enabled. To enable IPv6 on an interface, in the interface configuration mode, use the following command:

ipv6 enable

After enabling IPv6 on the interface, the system will also generate a link-local unicast IPv6 address for the interface.

To disable IPv6 and delete the link-local address allocated to the interface automatically, use the command **no ipv6 enable**. However, if the interface is configured with other IPv6 options, this command is not allowed.

For example, to enable IPv6 on ethernet0/1, use the following command:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# ipv6 enable
```

After enabling IPv6 on an interface, you can configure the following IPv6 options for the interface:

- Specifying a global IPv6 address
- Specifying address auto-config
- Specifying an EUI-64 address
- Specifying a link-local address
- Specifying an IPv6 MTU
- Viewing IPv6 Configuration

Specifying a Global IPv6 Address

Typically the global IPv6 address specified for an interface follows the format of IPv6 address prefix/prefix length. Besides, the system also supports the format of IPv6 general prefix, i.e., an address consisting of general prefix and sub-prefix. The general prefix need to be configured in the global configuration mode, and can be referenced when users are specifying an address for an interface. To specify a global IPv6 unicast address for an interface, in the interface configuration mode, use the following command:

ipv6 address {*ipv6-address/Mask* | *general-prefix-name sub-prefix/Mask*}

- *ipv6-address* – Specifies the IPv6 address prefix.

- *Mask* − Specifies the prefix length. The value range is 1 to 128.
- *general-prefix-name* − Specifies the name of general prefix.
- *sub-prefix/Mask* − Specifies the sub-prefix.

Suppose the name of general prefix is test-prefix, the IPv6 address prefix is 2002:ae3:1111::/48, the sub-prefix is 0:0:0:2222::1/64, then the command **ipv6 address test-prefix 0:0:0:2222::1/64** will specify the IPv6 address 2002:ae3:1111:2222::1/64 for the interface.

To cancel the specified global IPv6 unicast address, use the following commands:

no ipv6 address (cancels all the IPv6 addresses on the interface)

no ipv6 address {*ipv6-address/Mask* | *general-prefix-name sub-prefix/Mask*} (cancels the specified IPv6 address on the interface)

Configuring an IPv6 General Prefix

The system supports IPv6 and 6to4 general prefix. The 6to4 general prefix follows the format of 2002:a.b.c.d::/48, where a.b.c.d is the IPv4 address of the referenced interface (specified by interface-name). To configure an IPv6 general prefix, in the global configuration mode, use the following command:

ipv6 general-prefix *prefix-name* {*X:X:X:X::X/M* | **6to4** *interface-name*}

- *prefix-name* − Specifies the name of general prefix.
- *X:X:X:X::X/M* − Specifies the IPv6 address prefix for the general prefix.
- **6to4** − Specifies to use 6to4 general prefix.
- *interface-name* − Specifies the interface referenced by the 6to4 general prefix (references the IPv4 address of the interface).

To delete the specified IPv6 general prefix, in the global configuration mode, use the following command:

no ipv6 general-prefix *prefix-name* {*X:X:X:X::X/M* | **6to4** *interface-name*}

To view the IPv6 general prefix defined in the system, in any mode, use the following command:

show ipv6 general-prefix

Specifying Address Auto-config

In the address auto-config mode, the interface receives the address prefix in RA packets first, and then combines it with the interface identifier to generate a global address. To specify address auto-config, in the interface configuration mode, use the following command:

ipv6 address autoconfig [**default**]

- **default** − If the interface is configured with a default router, this option will generate a default route to the default router.

To cancel address auto-config, in the interface configuration mode, use the following command:

no ipv6 address autoconfig

Specifying an EUI-64 Address

To specify an IPv6 address that uses EUI-64 interface ID, in the interface configuration mode, use the following command:

ipv6 address *ipv6-address/Mask* **eui-64**

- *ipv6-address* − Specifies the IPv6 address prefix.
- *Mask* − Specifies the prefix length. The value range is 1 to 128. If the length value is not larger than 64, the last 64 bits of the address will use the generated interface ID; if the length value is larger than 64, the last (128-prefix) bits of the address will use the generated interface ID.

To cancel the specified EUI-64 address, in the interface configuration mode, use the command:

no ipv6 address *ipv6-address/Mask* **eui-64**

Specifying a Link-local Address

Link-local address is used for communication between adjacent nodes of a single link, for example, communication between hosts when there is no router on the link. By default the system will generate a link-local address for the interface automatically if the interface is enabled with IPv6 (in the interface configuration mode, use the command ipv6 enable). You can also specify a link-local address for the interface as needed, and the specified link-local address will replace the automatically generated one. To specify a link-local for an interface, in the interface configuration mode, use the following command:

ipv6 address *ipv6-address* **link-local**

- *ipv6-address* − Specifies an IPv6 address.

To cancel the specified link-local address (and restore to the default link-local address), in the interface configuration mode, use the command **no ipv6 address** *ipv6-address* **link-local**.

Specifying an IPv6 MTU

To specify an IPv6 MTU for an interface, in the interface configuration mode, use the following command:

ipv6 mtu *value*

- *value* – Specifies the MTU value. The value range is 1280 to 1500 byte. The default value is 1500.

To restore to the default MTU, in the interface configuration mode, use the command **no ipv6 mtu**.

Viewing IPv6 Configuration

To view IPv6 configuration of an interface, in any mode, use the following command:

show ipv6 interface [*interface-name*] [**prefix**]

- *interface-name* – Shows IPv6 configuration of the specified interface. If this parameter is not specified, the system will show all the interfaces which are enabled with IPv6.
- **prefix** – Shows IPv6 prefix of the specified interface.

Configuring IPv6 Neighbor Discovery Protocol

NDP (Neighbor Discovery Protocol) is a basic component of IPv6. This protocol operates on the link layer, and is responsible for looking for other nodes on the link, determining link layer addresses of other nodes, looking for available routers and maintaining information of other reachable nodes. Except for IPv4 ARP, router discovery and redirection functions of ICMP, NDP also provides more advanced functions, e.g., detection mechanism for unreachable neighbors.

FSOS supports the following NDP configurations:

- Configuring DAD
- Specifying reachable time
- Configuring RA parameters
- Specifying a RA interval
- Specifying RA lifetime

- Specifying DRP
- Configuring RA suppress on LAN interfaces
- Adding/Deleting static IPv6 neighbor cache

Configuring DAD

This function is implemented by sending NS (Neighbor Solicitation) requests. After receiving an NS packet, if any other host on the link finds the address of the NS requester is duplicated, it will send an NA (Neighbor Advertisement) packet advertising the address is already in use, and then the NS requester will mark the address as Duplicate, indicating the address is an invalid IPv6 address.

The configuration of DAD includes specifying NS packets attempts times and interval.

To specify NS packet attempts times for an interface, in the interface configuration mode, use the following command:

ipv6 nd dad attempts *times*

- *times* – Specifies NS packet attempts times. The value range is 0 to 20. The default value is 1. Value 0 indicates DAD is not enabled on the interface. If the system does not receive any NA response packet after sending NS packets for the attempts times, it will verify the IPv6 address is the unique available address.

To restore to the default attempts time, in the interface configuration mode, use the command **no ipv6 nd dad attempts**.

To specify an NS packet interval for an interface, in the interface configuration mode, use the following command:

ipv6 nd ns-interval *interval*

- *interval* – Specifies an interval for sending NS packets. The value range is 1000 to 3600000 milliseconds. The default value is 1000.

To restore to the default NS packet interval, in the interface configuration mode, use the command **no ipv6 nd ns-interval**.

Specifying Reachable Time

After sending an NS packet, if the interface receives acknowledge from a neighbor within the specified time, it will consider the neighbor as reachable. This time is known as reachable time. To configure reachable time, in the interface configuration mode, use the following command:

ipv6 nd reachable-time *time*

- *time* – Specifies reachable time. The value is 0 to 3600000 milliseconds. The default value is 30000.

To restore to the default value, in the interface configuration mode, use the command **no ipv6 nd reachable-time**.

Specifying RA Parameters

Routers send RA (Router Advertisement) packets periodically to advertise availability information and link/Internet parameters, including address prefix, recommended hop limit value, local MTU, auto-config type flag used by the node, etc.

Specifying a Hop Limit

Hop limit refers to the maximum number of hops for IPv6 or RA packets sent by the interface. To specify a hop limit, in the interface configuration mode, use the following command:

ipv6 nd hoplimit *number*

- *number* - Specifies the hop limit. The value range is 0 to 255. The default value is 64.

To restore to the default hop limit, in the interface configuration mode, use the following command:

no ipv6 nd hoplimit

Advertising MTU

You can specify whether to include MTU in RA packets sent on device interfaces and advertise to other routers. By default MTU is advertised. To specify to advertise MTU, in the interface configuration mode, use the following command:

ipv6 nd adv-linkmtu

To specify not to advertise MTU, in the interface configuration mode, use the following command:

no ipv6 nd adv-linkmtu

Specifying an Auto-config Type Flag

You can notify the connected hosts whether to obtain IP addresses and other configuration parameters via auto-config method (e.g., DHCP) by specifying an auto-config type flag in the RA packets. To specify to obtain IP addresses via auto-config, in the interface configuration mode, use the following command:

ipv6 nd managed-config-flag

To cancel the above configuration, in the interface configuration mode, use the command **no ipv6 nd managed-config-flag**.

To specify to obtain other configuration parameters other than IP addresses via auto-config, in the interface configuration mode, use the following command:

ipv6 nd other-config-flag

To cancel the above configuration, in the interface configuration mode, use the command **no ipv6 nd other-config-flag**.

Specifying an IPv6 Prefix and Parameters

RA packets will advertise the IPv6 prefix of interface. You can also specify the IPv6 prefix to be advertised, and configure its related parameters. In the interface configuration mode, use the following command:

ipv6 nd prefix {*ipv6-prefix/M* | **default**} [**no-advertise** | [*valid-lifetime preferred-lifetime* [**off-link** | **no-autoconfig**]]] | [**at** *valid-date* [*preferred-date* [**off-link** | **no-autoconfig**]]]

- *ipv6-prefix/M* – Specifies the IPv6 prefix and its length to be advertised.
- **default** – Specifies the default parameter for all the prefixes.
- **no-advertise** – Do not advertise IPv6 prefix in RA packets.
- *valid-lifetime* – Specifies valid lifetime for the IPv6 prefix. The value range is 0 to 4294967295 seconds. The default value is 2592000 (30 days).
- *preferred-lifetime* – Specifies the preferred lifetime for the IPv6 prefix. The default value is 604800 (7 days). The preferred lifetime should not be larger than the valid lifetime.
- **off-link** – Specifies off-link status for the prefix, i.e., the node that receives the RA packets will not write the prefix to its own routing table; if the prefix already exists in the routing table, the node will delete it.
- **no-autoconfig** – Advertises the host that receives the packets not to use the prefix as an IPv6 auto-configured address.
- *valid-date* – Specifies a valid date for the prefix, i.e., the prefix is only valid before the date. The format is MM/DD/YYYY HH:MM, such as 09/20/2010 09:30.
- *preferred-date* – Specifies a preferred valid date for the prefix. The format is MM/DD/YYYY HH:MM. This date must be earlier than the valid date.

To cancel the above IPv6 prefix parameters, in the interface configuration mode, use the following command:

no ipv6 nd prefix {*ipv6-prefix/M* | **default**}

Specifying a RA Interval

RA interval refers to the interval at which interface sends RA packets. This interval should not be larger than the lifetime of RA packets configured via CLI. To reduce the possibility of sending RA packets simultaneously with other routers on the same link, the system usually select a random number between the maximum and minimum interval as the actual RA interval. To configure a RA interval, in the interface configuration mode, use the following command:

ipv6 nd ra interval *max-interval* [*min-interval*]

- *max-interval* − Specifies the maximum interval. The value range is4 to 1800 seconds. The default value is 600.
- *min-interval* − Specifies the minimum interval. The value range is 3 to 1350 seconds. The minimum interval should not be larger than 75% of the maximum interval and must be larger than 3. If this parameter is not specified, the system will use 1/3 of the maximum interval as the minimum interval.

To restore to the default RA interval, in the interface configuration mode, use the following command:

no ipv6 nd ra interval

Specifying RA Lifetime

RA lifetime refers to the valid time during which the router is used as the default router of the interface. To specify RA lifetime, in the interface configuration mode, use the following command:

ipv6 nd ra lifetime *time*

- *time* − Specifies RA lifetime. The value range is 0 to 9000 seconds. The default value is 1800. Value 0 indicates the router is not the default route of the interface. For other values other than 0, the value should not be smaller than the RA interval.

To restore to the default RA lifetime, in the interface configuration mode, use the following command:

no ipv6 nd ra lifetime

Specifying DRP

DRP is the abbreviation for Default Router Preference. When a node receives an equal-cost route from different routers, it will select a preferred router based on DRP. To specify DRP, in the interface configuration mode, use the following command:

ipv6 nd router-preference {**high** | **medium** | **low**}

- **high** − Specifies DRP as high.

- **medium** − Specifies DRP as medium.
- **low** − Specifies DRP as low.

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

no ipv6 nd router-preference

Configuring RA Suppress on LAN Interfaces

By default FDDI interfaces with IPv6 unicast route configured will send RA packets automatically, and interfaces of other types will not send RA packets. To configure RA suppress on a LAN interface, in the interface configuration mode, use the following command:

ipv6 nd ra suppress

The above command will disable the interface to transfer RA packets. To re-enable the interface to transfer RA packets, in the interface configuration mode, use the following command:

no ipv6 nd ra suppress

Adding/Deleting a IPv6 Neighbor Cache Entry

IPv6 neighbor cache entries, key for unicast address connections, are a group of entries that store a single neighbor's information respectively. To view IPv6 neighbor cache entries in the system, in any mode, use the following command:

show ipv6 neighbor [**interface** *interface-name* | **static** | **vrouter** *vr-name* | *ipv6-address* | **generic**]

- *interface-name* − Shows IPv6 neighbor cache entries of the specified interface.
- *ipv6-address* − Shows IPv6 neighbor cache entries of the specified address.
- **vrouter** *vr-name* − Shows IPv6 neighbor cache entries of the specified VRouter.
- **static** − Shows static IPv6 neighbor cache entries.
- **generic** − Shows statistics of neighbor cache entries.

To add a static IPv6 cache entry, in the global configuration mode, use the following command:

ipv6 neighbor *ipv6-address interface-name mac-address*

- *ipv6-address* − Specifies the IPv6 address.
- *interface-name* − Specifies the name of interface.
- *mac-address* − Specifies the MAC address corresponding to the IPv6 address.

To delete a static IPv6 cache entry, in the global configuration mode, use the following command:

clear ipv6 neighbor [*ipv6-address*] [**vrouter** *vr-name*]

- *ipv6-address* – Deletes the IPv6 neighbor entry of the specified address.
- **vrouter** *vr-name* – Deletes the IPv6 neighbor cache entries of the specified VRouter.

IPv6 System Management

FSOS supports FTP, TFTP, HTTP and HTTPS protocols for IPv6, i.e., it allows you to visit FTP and TFTP servers by IPv6 addresses; besides it also allows you to visit its WebUI by the IPv6 address. HTTP and HTTPS services for IPv4 and IPv6 share the same protocol port number.

You can export the following objects to the IPv6 address of an FTP or TFTP server: configuration file, system firmware, license, partial logs (alarm, event, security), PKI certificate, SCVPN user-host binding list and URL database. In the execution mode, use the following commands:

- To export the configuration file: **export configuration** {{**startup** | **backup**} *number*} **to** {**ftp server** *ipv6-address* [**vrouter** *vrouter-name*] [**user** *username* **password** *string*] | **tftp server** *ipv6-address* [**vrouter** *vrouter-name*]} [*file-name*]
- To export the system firmware: **export image** *name* **to** {**ftp server** *ipv6-address* [**vrouter** *vrouter-name*] [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} [*file-name*]
- To export the license: **export license** *name* **to** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} [*file-name*]
- To export logs: **export log** { **event** | **security**} **to** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} [*file-name*]
- To export the PKI certificate: **export pki** *trust-domain-name* {**cacert** | **cert** | **pkcs12** *password*} **to** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} [*file-name*]
- To export the SCVPN user-host binding list: **export scvpn user-host-binding to** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} [*file-name*]
- To export the URL database: **export urlfilter-database to** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} [*file-name*]

You can import the following objects from the IPv6 address of an FTP or TFTP server: application signature database, configuration file, custom firmware for SCVPN and WebAuth webpage, system firmware, ISP file, license, PKI certificate, SCVPN user-host binding list and URL database. In the execution mode, use the following commands:

- To import the application signature database: **import application-signature from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- To import the configuration file: **import configuration from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- To import the customized picture for SCVPN or WebAuth webpage: **import customize** {**scvpn • To import the license:**| **webauth**} **from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- To import the system firmware: **import image from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- To import the ISP file: **import ispfile from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- To import the license: **import license from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- To import the PKI license: **import pki** *trust-domain-name* {**cacert** | **cert** | **pkcs12** *password*} **from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- To import the SCVPN user-host binding list: **import scvpn user-host-binding from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- To import the URL database: **import urlfilter-database from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*

Tip: For more detailed information about the command parameters, see related chapters.

Configuring IPv6 SNMP

FSOS allows you to view the general IPv6-related MIB information via SNMP. The configuration of SNMP IPv6 includes:

- Configuring an IPv6 management host
- Configuring an IPv6 trap destination host
- Creating an SNMPv3 user (IPv6 remote management host)

Tip: For more information about the SNMP configuration, see "Configuring SNMP" of "System Management" .

Configuring an IPv6 Management Host

To configure an IPv6 management host, in the global configuration mode, use the following command:

snmp-server ipv6-host {*host-name* | *ipv6-address*} {**version** [*1* | *2c*] **community** *string* [**ro** | **rw**] | **version** *3*}

- *host-name* | *ipv6-address* – Specifies hostname or IPv6 address of the management host.
- **version** [*1* | *2c*] – Specifies the SNMP version as SNMP v1 or SNMP v2C.
- **community** *string* – Specifies the community string. The length is 1 to 31 bits. The community string is a password between the management and proxy processes; therefore, SNMP packets with inconsistent community strings will be dropped. This parameter only applies for SNMP v1 and v2C.
- **ro** | **rw** – Specifies a privilege for the community string. ro stands for read-only, and such a community string can only read information in the MIB; **rw** stands for read-write, and such a community string can not only read but also modify information in the MIB. This parameter is optional. By default the privilege is **ro**.
- **version** *3* – Specifies the SNMP version as SNMP v3.

To delete the specified IPv6 management host, in the global configuration mode, use the command **no snmp-server ipv6-host** {*host-name* | *ipv6-address*}.

Configuring an IPv6 Trap Destination Host

You can configure an IPv6 destination host that is used to receive SNMP trap packets. To configure an IPv6 trap destination host, in the global configuration mode, use the following command:

snmp-server ipv6-trap-host {*host-name* | *ipv6-address*} {**version** {*1* | *2c*} **community** *string* | **version** *3* **user** *user-name* **engineID** *string* } [**port** *port-number*]

- *host-name* / *ipv6-address* – Specifies the hostname or IPv6 address of the trap destination host.
- **version** {*1* / *2c*} – Specifies to send trap packets via SNMPv1 or SNMPv2C.
- **community** *string* – Specifies the community string for SNMPv1 or SNMPv2C.
- **version** *3* – Specifies to send trap packets via SNMPv3.

- **user** *user-name* – Specifies the SNMPv3 username.
- **engineID** *string* – Specifies engine ID of the trap destination host.
- **port** *port-number* – Specifies the port number of the destination host that receives trap packets. The value range is 1 to 65535. The default value is 162.

To delete the specified trap destination host, in the global configuration mode, use the command **no snmp-server ipv6-trap-host** {*host-name* / *ip-address*}.

Creating an SNMPv3 User

To configure an SNMPv3 user, in the global configuration mode, use the following command:

snmp-server user *user-name* **group** *group-name* **v3** {**remote** *remote-ip* | **ipv6-remote** *ipv6-address*} [**auth-protocol** {**md5** | **sha**} *auth-pass* [**enc-protocol** {**des** | **aes**} *enc-pass*]]

- **user** *user-name* – Specifies the username. The length is 1 to 31 characters.
- **group** *group-name* – Specifies a user group defined in the system for the user.
- **remote** *remote-ip* – Specifies the IP address of the remote management host.
- **ipv6-remote** *ipv6-address* – Specifies the IPv6 address of the remote management host.
- **auth-protocol** {**md5** | **sha**} – Specifies the authentication protocol as MD5 or SHA. If this parameter is not specified, the default security level will be no authentication and no encryption.
- *auth-pass* – Specifies the authentication password. The length is 8 to 40 characters.
- **enc-protocol** {**des** | **aes**} – Specifies the encryption protocol as DES or AES.
- *enc-pass* – Specifies the encryption password. The length is 8 to 40 characters.

The system supports up to 25 users. To delete the specified user, in the global configuration mode, use the command **no snmp-server user** *user-name*.

Configuring IPv6 Debugging

System supports ping to an IPv6 address. To ping an IPv6 address, in any mode, use the following command:

ping ipv6 *ipv6-address* [**count** *number*] [**size** *number*] [**source** {*ipv6-address* | *interface-name*}] [**timeout** *time*] [**vrouter** *vr-name*]

- *ipv6-address* − Specifies the destination address to which ping packets are sent.
- **count** *number* − Specifies the number of ping packets. The value range is 1 to 65535. The default value is 5.
- **size** *number* − Specifies the size of ping packets. The length is 28 to 65535 bytes.
- **source** {*ipv6-address* | *interface-name*} − Specifies the source address where ping packets originate. It can be either an IP address or an interface.
- **timeout** *time* − Specifies timeout for ping packets. The value range is 0 to 3600 seconds. The default value is 0, i.e., never timeout.
- **vrouter** *vr-name* − Specifies the VRouter that sends ping packets.

Configuring IPv6 Routing

FSOS supports IPv6 DBR, SBR and SIBR. To configure an IPv6 static route, you need to enter the VRouter configuration mode. In the global configuration mode, use the following command:

ip vrouter *vrouter-name*

- *vrouter-name* − Specifies the name of VRouter, and enter the VRouter configuration mode.

Configuring an IPv6 DBR Entry

To add an IPv6 DBR entry, in the VRouter configuration mode, use the following command:

ipv6 route *ipv6-address/M* {**null0** | *ipv6-address* | **vrouter** *vrouter-name* | *interface-name* [*ipv6-address*]} [*distance-value*] [**name** *name*][**weight** *weight-value*]

- *ipv6-address/M* − Specifies the segment of the destination address.
- **null0**- Specifies the Null0 interface.
- *ipv6-address* | **vrouter** *vrouter-name* | *interface-name* [*ipv6-address*] − Specifies the next hop which can be a gateway address (*ipv6-address*) , VRouter（**vrouter** *vrouter-name*）or an interface (*interface-name*).
- *distance-value* − Specifies the administration distance of the route. This parameter is used to determine the precedence of the route. The smaller the value is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route is invalid.

- *name* − Specifies the name of router.
- *weight-value* − Specifies the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.

Repeat the above command to add multiple DBR entries.

To delete the specified IPv6 DBR entry, in the VRouter configuration mode, use the following command:

no ipv6 route *ipv6-address/M* { **null0** | *ipv6-address* | **vrouter** *vrouter-name* | *interface-name* [*ipv6-address*]}

Configuring an IPv6 SBR Entry

To add an IPv6 SBR entry, in the VRouter configuration mode, use the following command:

ipv6 route source *ipv6-address/M* { **null0** | *ipv6-address* / *interface-name* | **vrouter** *vrouter-name* } [*distance-value*] [**name** *name*] [**weight** *weight-value*]

- *ipv6-address/M* − Specifies the segment of the source address.
- **null0** − Specifies the Null0 interface.
- *A.B.C.D* / *interface-name* | **vrouter** *vrouter-name* − Specifies the next hop which can be a gateway address (*ipv6-address*) , VRouter（**vrouter** *vrouter-name*） or an interface (*interface-name*).
- *distance-value* − Specifies the administration distance of the route. This parameter is used to determine the precedence of the route. The smaller the value is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route is invalid.
- *name* − Specifies the name of router.
- *weight-value* − Specifies the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.

Repeat the above command to add multiple SBR entries.

To delete the specified IPv6 SBR entry, in the VRouter configuration mode, use the following command:

no ipv6 route source *ipv6-address/M* { **null0** | *ipv6-address* / *interface-name* | **vrouter** *vrouter-name*}

Configuring an IPv6 SIBR Entry

To add an IPv6 SIBR entry, in the VRouter configuration mode, use the following command:

ipv6 route source in-interface *interface-name ipv6-address/M* { **null0** | *ipv6-address* / *interface-name*| **vrouter** *vrouter-name* } [*distance-value*] [**name** *name*] [**weight** *weight-value*]

- *interface-name* – Specifies the ingress interface of the routing entry.
- **null0**- Specifies the Null0 interface.
- *ipv6-address/M* – Specifies the segment of the source address.
- *ipv6-address* / *interface-name* | **vrouter** *vrouter-name* – Specifies the next hop which can be a gateway address (*ipv6-address*) , VRouter（**vrouter** *vrouter-name*） or an interface (*interface-name*).
- *distance-value* – Specifies the administration distance of the route. This parameter is used to determine the precedence of the route. The smaller the value is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route is invalid.
- *name* – Specifies the name of router.
- *weight-value* – Specifies the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.

Repeat the above command to add multiple SIBR entries.

To delete the specified IPv6 SIBR entry, in the VRouter configuration mode, use the following command:

no ipv6 route source in-interface *interface-name ipv6-address/M* { **null0** | *ipv6-address* / *interface-name* | **vrouter** *vrouter-name* }

Viewing IPv6 Routing Information

To view IPv6 routing information, in any mode, use the following commands:

- To view DBR information: **show ipv6 route static** [**vrouter** *vr-name*]
- To view SBR information: **show ipv6 route source** [**vrouter** *vr-name*]
- To view SIBR information: **show ipv6 route source in-interface** *interface-name*
- To view connected route information: **show ipv6 route connected** [**vrouter** *vr-name*]
- To view routing information of the specified destination address: **show ipv6 route** *ipv6-address/[M]* [**vrouter** *vr-name*]

- To view IPv6 routes statistics: **show ipv6 route summary** [**vrouter** *vr-name*]
- To view IPv6 FIB information: **show ipv6 fib** [**source** | **source in-interface** *interface-name* | *ipv6-address/[M]* | **summary**] [**vrouter** *vr-name*]

Configuring RIPng

RIPng (RIP next generation) is an extension to the RIP-2 in IPv4. Most concepts of RIP are applicable to RIPng.

Compared with RIP, RIPng modifies following items:

- UDP port: Uses the UDP port 521 to send and receive routing information.
- Multicast address: Uses FF02::9 as the multicast address of the RIPng router in the local-link address range.
- Prefix length: The destination address uses prefix length of 128 bits.
- Next-hop address: Use the 128 bits IPv6 address.
- Source address: Uses the link-local address FE80::/10 as the source address to send RIPng routing information update packets.

RIPng configuration includes basic options, redistribute, passive IF, network and distance. Besides, you also need to configure RIP parameters for different interfaces, including split horizon and poison reverse.

Basic Options

The basic options of RIPng configuration include metric, distance, information originate and timer (update interval, invalid time, and flush time). You can configure RIPng protocol for different VRouter respectively. The basic options of RIPng must be configured in the RIPng routing configuration mode. To enter the RIPng routing configuration mode, in the global configuration mode, use the following commands:

ip vrouter *vrouter-name* (enters the VRouter configuration mode)

ipv6 router rip (enters the RIPng routing configuration mode, and at the same time enables the RIPng function on the device. Each RIPng process is individual and you can create one RIPng process in a VRouter.)

To disable the RIPng function, in the VRouter configuration mode, use the command **no ipv6 router rip**.

Specifying a Default Metric

RIPng measures the distance to the destination network by counting the number of hops. This distance is known as metric. The metric from a router to a directly connected network is 1, and increments by 1 for every additional router between them. The maximum metric is 15, and the network with metric larger than 15 is not reachable. The default metric will take effect when the route is redistributed. To specify the default metric, in the RIPng routing configuration mode, use the following command:

default-metric *value*

- *value* − Specifies the default metric value. The value range is 1 to 15. If no value is specified, the value of 1 will be used.

To restore the metric value to 1, in the RIPng routing configuration mode, use the command **no default-metric**.

Specifying a Default Distance

To specify the default distance for RIPng, in the RIPng routing configuration mode, use the following command:

distance *distance-value*

- *distance-value* − Specifies the default administration distance value. The value range is 1 to 255. If no value is specified, the value of 120 will be used.

To restore to the distance value of 120, in the RIPng routing configuration mode, use the command **no distance**.

Specifying a Timer

The timers you can configure for RIPng include update interval, invalid time, holddown time and flush time, as described below:

- Update interval: Specifies the interval at which all RIPng routes will be sent to all the neighbors. The default value is 30 seconds.
- Invalid time: If a route has not been updated for the invalid time, its metric will be set to 16, indicating an unreachable route. The default value is 180 seconds.
- Flush time: FSOS will keep on sending the unreachable routes (metric set to 16) to other routers during the flush time. If the route still has not been updated after the flush time ends, it will be deleted from the RIPng information database. The default value is 240 seconds.

To modify the above three timers, in the RIPng routing configuration mode, use the following command:

timers basic *interval-time invalid-time flush-time*

- *interval-time* − Specifies the update interval time. The value range is 0 to 16777215 seconds. The default value is 30.
- *invalid-time* − Specifies the invalid time. The value range is 1 to 16777215 seconds. The default value is 180.
- *flush-time* − Specifies the flush time. The value range is 1 to 16777215 seconds. The default value is 120.

To restore to the default timer value, in the RIPng routing configuration mode, use the command **no timers basic**.

Configuring the Default Information Originate

You can specify if the default route will be redistributed to other routers with RIPng enabled. By default RIPng will not redistribute the default route. To configure the default information originate, in the RIPng routing configuration mode, use the following commands:

- Redistribute: **default-information originate**
- Do not redistribute: **no default-information originate**

Configuring Redistribute

RIPng allows you to introduce information from other routing protocols (IPv6 BGP, connected, static, OSPFv3 and IS-IS) and redistribute the information. To configure the redistribute metric, in the RIP routing configuration mode, use the following commands:

redistribute {**bgp** | **connected** | **static** | **ospf** | **isis**} [**metric** *value*]

- **bgp** | **connected** | **static** | **ospf**| **isis** − Specifies the protocol type: IPv6 BGP (**bgp**), connected route (**connected**), static route (**static**) , OSPFv3 (**OSPF**) or IS-IS (**isis**).
- **metric** *value* − Specifies a metric value for the redistribute. The value range is 1 to 15. If the value is not specified, the system will use the default metric configured by the command **default-metric** *value*.

Repeat the above command to redistribute different types of protocols.

To cancel the redistribute of the specified protocol, in the RIPng routing configuration mode, use the command **no redistribute** {**bgp** | **connected** | **static** | **ospfv3**}.

Configuring a Network

You can configure some networks so that only the interfaces within the specified networks can receive and send RIPng update. To configure a network, in the RIPng routing configuration mode, use the following command:

network {*interface-name* | *X:X:X:X::X/M*}

- *interface-name* – Specified the interface name. This interface is located at the network that you want to specify.
- *X:X:X:X::X/M* – Specifies the IPv6 address of the network.

Repeat the above command to configure more networks.

To delete the specified network, in the RIPng routing configuration mode, use the command **no network** {*interface-name* | *X:X:X:X::X/M*}.

Configuring a Passive IF

You can configure some interfaces to only receive but not to send data. This kind of interfaces is known as a passive interface. To configure a passive interface, in the RIPng routing configuration mode, use the following command:

passive-interface *interface-name*

- *interface-name* – Specifies the interface as a passive interface.

Repeat the above command to configure multiple passive interfaces.

To cancel the specified passive interface, in the RIP routing configuration mode, use the command **no passive-interface** *interface-name*.

Configuring Split Horizon

When using split horizon, routes learned from an interface will not be sent from the same interface, in order to avoid routing loop and assure correct broadcasting to some extent. To enable or disable split horizon, in the interface configuration mode, use the following commands:

- Enable: **ipv6 rip split-horizon**
- Disable: **no ipv6 rip split-horizon**

Configuring Poison Reverse

When using poison reverse, RIPng will send the poison messages to all neighbor routers, including the router whose sends the poison message, and will not obey the split horizon rule. This poison message advertise the invalid route. To configure the poison reverser function , use the following command in the interface configuration mode:

- Enable: **ipv6 rip poison-reverse**
- Disable: **no ipv6 rip poison-reverse**

Viewing RIPng Information

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

show ipv6 rip

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

show ip route rip [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the RIP router information of the specified VRouter.

When a FS device is running RIPng, it will own a RIPng route database which can store all routing entries for all the reachable networks. The routing entry information includes destination address, next hop, metric, source, and timer information. To view the RIPng database information, in any mode, use the following command:

show ipv6 rip database [**vrouter** *vrouter-name*]

- **vrouter** *vrouter-name* – Shows the RIPng information of the specified VRouter.

Configuring OSPFv3

OSPFv3 is the third version of Open Shortest Path First and it mainly provides the support of IPv6.

The similarities between OSPFv3 and OSPFv2 are as follows:

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

The differences between OSPFv3 and OSPFv2 are as follows:

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

You can configure the OSPFv3 protocol for each VRouter respectively. Configuring OSPFv3 includes the following options:

- Configuring a Router ID
- Configuring the virtual link for an area
- Configuring the default metric
- Configuring the default administrative distance
- Configuring the default information originate
- Configuring the interface area and instance
- Configuring redistribute
- Configuring a passive interface
- Configuring the timer for an interface
- Configuring the router priority for an interface
- Configuring the link cost for an interface
- Configure the MTU check for an interface
- Disabling or Enabling OSPFv3

The basic options of OSPFv3 protocol must be configured in the OSPFv3 routing mode. To enter the OSPFv3 routing mode, in the global configuration mode, use the following commands:

ip vrouter *vrouter-name* (enters the VRouter configuration mode)

ipv6 router ospf (enters the OSPFv3 routing configuration mode, and at the same time enables OSPFv3 on the device. The OSPFv3 processes among different VRouters are individual and you can create only one OSPFv3 process in a VRouter.)

To disable OSPFv3, in the VRouter configuration mode, use the command **no ipv6 router ospf**.

Configuring a Router ID

Each router running OSPFv3 protocol must be labeled with a Router ID. The Router ID is the unique identifier of an individual router in the whole OSPFv3 domain, represented in the form of an IP address. To configure a Router ID for the FS device that is running OSPFv3 protocol, in the OSPF routing mode, use the following command:

router-id *A.B.C.D*

- *A.B.C.D* – Specifies the Router ID used by OSPFv3 protocol, in form of an IP address.

Configuring the Virtual Link for an Area

Virtual link is used to connect the discontinuous backbone areas, so that they can maintain logical continuity. To configure virtual link parameters and its timer parameters, in the OSPFv3 routing mode, use the following command:

area { *id* | *A.B.C.D* } **virtual-link** *A.B.C.D*

- *id* | *A.B.C.D* – Specifies an area ID that requires virtual link, in form of a 32-bit digital number, or an IP address.
- *A.B.C.D* – Specifies the Router ID that is used as a virtual link router.

Configuring the Default Metric

The default metric configured here will take effect if the redistributed route has no configured metric. To specify the default metric for OSPFv3, in the OSPFv3 routing configuration mode, use the following command:

default-metric *value*

- *value* – Specifies the default metric value. The value range is 1 to 16777214.

To restore to the original metric value, in the OSPFv3 routing configuration mode, use the command **no default-metric**.

Configuring the Default Administrative Distance

You can configure the default administrative distance according to the route type. To configure the default administrative distance, in the OSPFv3 routing configuration mode, use the following command:

distance {*distance-value* | **ospf** [**intra-area** *distance-value* | **inter-area** *distance-value* | **external** *distance-value*}

- *distance-value* － You can configure the default administrative distance according to the route type. To configure the default administrative distance, in the OSPFv3 routing configuration mode, use the following command:

- **intra-area** *distance-value* － Specifies the administrative distance value of the intra-area route. The default value is 110 and the value ranges from 1 to 255.

- **inter-area** *distance-value* － Specifies the administrative distance value of the inter-area route. The default value is 110 and the value ranges from 1 to 255.

- **external** *distance-value* － Specifies the administrative distance value of the external route. The default value is 110 and the value ranges from 1 to 255.

To restore to the value of 110, in the OSPFv3 routing configuration mode, use the command **no distance ospf**.

Configuring the Default Information Originate

You can specify if the default route will be redistributed to other routers. To configure the default information originate, in the OSPFv3 routing configuration mode, use the following command:

default-information originate [**always**] [**type** {1 | 2}] [**metric** value]

- **always** － When using **always**, OSPFv3 of this router unconditionally generates and redistributes the default route. If there is no default route in the current router, it will generate a route whose next hop is the router itself. Without using always, the router will not redistribute the default route if it has no one.

- **type** {1 | 2} － Specifies the type of the external route associated with the default route that is sent to OSPFv3 routing area. 1 refers to type1 external route, 2 refers to type2 external route.

- **metric** *value* － Specifies the metric value for the default route that will be sent. If no default metric value is specified by this command or by the command **default-metric** *value*, then OSPFv3 will use the value of 20. The value range is 0 to16777214.

To restore to the value of 20, in the OSPFv3 routing configuration mode, use the command **no default-information originate**.

Configuring the Interface Area and Instance

To specify the area and instance that the interface belongs to, in the OSPFv3 routing configuration mode, use the following command:

ipv6 ospf area { *A.B.C.D* / *id*} {**instance** *id*}

- **area** { *A.B.C.D* / *id*} – Specifies the area ID that the interface belongs to. The area ID is in form of a 32-bit digital number, or an IP address.
- **instance** *id* – Specifies the instance ID that the interface belongs to. To establish the neighbor relationship, interfaces must belong to the same instance. The value ranges from 0 to 255. The default value is 0.

To cancel the area and instance configuration, in the OSPFv3 routing configuration mode, use the command **no ipv6 ospf area** { *A.B.C.D* | *id*}.

Configuring Redistribute

OSPFv3 allows you to introduce information from other routing protocols (IPv6 BGP, connected, static and RIPng) and redistribute the information. You can set the metric and type of the external route for the redistribute. To configure the redistribute, in the OSPFv3 routing configuration mode, use the following command:

redistribute {**bgp** | **connected** | **static** | **ripng**} [**type** {1 | 2}] [**metric** *value*]

- **bgp** | **connected** | **static** | **ripng** – Specifies the protocol type which can be IPv6 BGP (**bgp**), connected route (connected), static route (**static**) or OSPFv3 (**OSPF**).
- **type** {1 | 2} – Specifies the type of the external route. 1 refers to type1 external route, 2 refers type2 external route.
- **metric** *value* – Specifies a metric value for the redistribute. The value range is 0 to 16777214. If the value is not specified, the system will use the default OSPFv3 metric configured by the command **default-metric** *value*.

Repeat the above command to redistribute a different type of routes. To cancel the redistribute of specified route, in the OSPF routing configuration mode, use the command

no redistribute {**bgp** | **connected** | **static** | **rip**}.

Configuring a Passive Interface

You can configure some interfaces to only receive but not to send data. This kind of interfaces is known as a passive interface. To configure a passive interface, in the interface configuration mode, use the following command:

ipv6 ospf passive

Repeat the above command to configure more passive interfaces.

To cancel the specified passive interface, in the interface configuration mode, use the command **no ipv6 ospf passive**.

Configuring the Timer for an Interface

There are four interface timers: the interval for sending Hello packets, the dead interval of adjacent routers, the interval for retransmitting LSA, and the transmit delay for updating packets.

To specify the interval for sending Hello packets for an interface, in the interface configuration mode, use the following command:

ipv6 ospf hello-interval *interval*

- *interval* – Specifies the interval for sending Hello packets for an interface. The value range is 1 to 65535 seconds. The default value is 10.

To restore to the default interval, in the interface configuration mode, use the command **no ipv6 ospf hello-interval**.

If a router has not received the Hello packet from its peer for a certain period, it will determine the peering router is dead. This period is known as the dead interval between the two adjacent routers. To configure the dead interval for an interface, in the interface configuration mode, use the following command:

ipv6 ospf dead-interval *interval*

- *interval* – Specifies the dead interval of adjacent routes for an interface. The value range is 1 to 65535 seconds. The default value is 40 (4 times of sending the Hello packets).

To restore to the default dead interval, in the interface configuration mode, use the command **no ipv6 ospf dead-interval**.

To specify the LSA retransmit interval for an interface, in the interface configuration mode, use the following command:

ipv6 ospf retransmit-interval *interval*

- *interval* – Specifies the LSA retransmit interval for an interface. The value range is 3 to 65535 seconds. The default value is 5.

To restore to the default retransmit interval, in the interface configuration mode, use the command **no ipv6 ospf retransmit-interval**.

ipv6 ospf transmit-delay *interval*

- *interval* – Specifies the transmit delay for updating packet for an interface. The value range is 1 to 65535 seconds. The default value is 1.

To restore to the default transmit delay, in the interface configuration mode, use the command **no ipv6 ospf transmit-delay**.

Configuring the Router Priority for an Interface

The router priority is used to determine which router will act as the designated router. The designated router will receive the link information of all the other routers in the network, and send the received link information. To specify the router priority for an interface, in the interface configuration mode, use the following command:

ipv6 ospf priority *level*

- *level* – Specifies the router priority. The value range is 0 to 255. The default value is 1. The router with priority set to 0 will not be selected as the designated router. If two routers within a network can both be selected as the designated router, the router with higher priority will be selected; if the priority level is the same, the one with higher Router ID will be selected.

To restore to the default priority, in the interface configuration mode, use the command **no ipv6 ospf priority**.

Configuring the Link Cost for an Interface

You can use one of the following methods to configure the link cost for an interface:

- Specify the cost directly
- Specify the bandwidth reference value and OSPFv3 computes the cost automatically based on the bandwidth reference value

To specify the cost directly, use the following command in the interface configuration mode:

ipv6 ospf cost *cost-value*

- *cost-value* – Specifies a cost value. The value range is 0 to 16777214.

To cancel the configuration, use **no ipv6 ospf cost**.

To compute the cost according to the specified bandwidth reference value, specify the bandwidth of the interface in the OSPFv3 configuration mode:

auto-cost reference-bandwidth *bandwidth*

- *bandwidth* – Specifies the bandwidth reference value. The unit is Mbps, and the default value is 100. The value ranges from 1 to 4294967. The cost equals to the value of dividing interface bandwidth by the bandwidth reference value.

To restore the bandwidth reference value to the default value, use **no auto-cost reference-bandwidth**.

Configuring the MTU Check for an Interface

OSPFv3 uses DBD packets to check whether the interface MTU set is matched or not between the neighbors. If the MTU set is not matched, the neighbors cannot establish the adjacency. You can modify the MTU set to solve this issue. For the interfaces whose MTU set cannot be modified, you can ignore the MTU check.

To ignore the MTU check, use the following command in the interface configuration mode:

ipv6 ospf mtu-ignore

Use the no form to restore the MTU check:

no ipv6 ospf mtu-ignore

Disabling or Enabling OSPFv3

Disable OSPFv3 protocol on interface, in the interface configuration mode, use **ipv6 ospf shutdown**.

Enable OSPFv3 protocol on interface, in the interface configuration mode, use **no ipv6 ospf shutdown**.

Viewing OSPFv3 Information

To view the OSPFv3 routing information of the FS device, in any mode, use the following command:

show ipv6 ospf [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the OSPF route information of the specified VRouter name.

To view the OSPFv3 protocol's database information of the FS device, in any mode, use the following commands:

show ipv6 ospf database

show ipv6 ospf database {**inter-router** | **external** | **network** | **router** | **inter-prefix** | **link** | **intra-prefix**} [*A.B.C.D*] [{**adv-router** *A.B.C.D*} | **self-originate**] [**vrouter** *vrouter-name*]

- **inter-router** – Shows the LSAs originated by ABRs and these LSAs are flooded throughout the LSA's associated area. Each inter-router LSA describes a route to ASBR.
- **external** – Shows the LSAs originate by ASBRs and these LSAs are flooded throughout the AS (except Stub and NSSA areas). Each external LSA describes a route to another AS.
- **network** – Shows the LSAs of the network. These LSAs are originated for broadcast and NBMA networks by the designated router. This LSA contains the list of routers connected to the network, and is flooded throughout a single area only.

- **router** – Shows the LSAs of the router. These LSAs are originated by all routers. This LSA describes the collected states of the router's interfaces to an area, and is flooded throughout a single area only.
- **inter-prefix** – Shows the LSAs originated by ABRs and these LSAs are flooded throughout the LSA's associated area. Each inter-prefix LSA describes a route with IPv6 address prefix to a destination outside the area, yet still inside the AS (an inter-area route).
- **link** – Shows the LSAs originated by a router. This link LSA is originated for each link and it has link-local flooding scope. Each link LSA describes the IPv6 address prefix of the link and link-local address of the router.
- **intra-prefix** - Shows the LSAs that contains IPv6 prefix information on a router, stub area or transit area information, and it has area flooding scope. The intra-prefix LSAs were introduced because router LSAs and network LSAs contain no address information now.
- *A.B.C.D* - Shows the IP address of link status ID.
- **adv-router** *A.B.C.D* – Shows the LSAs of the specified router.
- **self-originate** - Only shows self-originated LSAs (from local router).
- *vrouter-name* - Specifies the VRouter name.

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

show ipv6 ospf interface [*interface-name*] [**vrouter** *vrouter-name*]

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

show ip ospf neighbor [*A.B.C.D* | **detail**][**vrouter** *vrouter-name*]

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

show ipv6 ospf border-routers [*A.B.C.D*][**vrouter** *vrouter-name*]

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

show ip ospf route [*X:X:X:X::X/M* [**vrouter** *vrouter-name*]

Configuring IPv6 BGP

BGP-4 was designed to carry only IPv4 routing information, and other network layer protocols such as IPv6 are not supported. To support multiple network layer protocols, IETF extended BGP-4 by introducing multiprotocol BGP (MP-BGP). MP-BGP for IPv6 is called IPv6 BGP. IPv6 BGP uses the extension attribute of BGP to achieve the goal of using BGP in IPv6 network and it has the same messaging and routing mechanisms as BGP.

To configure the following items, see "Configuring BGP" of "Routing".

- Configuring a peer/peer group
- Configuring equal cost multipath routing
- Configuring a timer
- Configuring MD5 authentication
- Disabling a peer/peer group
- Configuring EBGP multihop
- Configuring description
- Configuring a peer timer

This section introduces the following configurations:

- Configuring IPv6 unicast route
- Activating a connection
- Sending community path attributes to a peer/peer group
- Specifying Upper Limit of Prefixes

Entering the IPv6 Unicast Routing Configuration Mode

To configure the settings of IPv6 unicast route, you must enter into the IPv6 unicast routing configuration mode. Execute the following command in the BGP instance configuration mode:

address-family ipv6 unicast

Configuring IPv6 Unicast Route Redistribute

IPv6 BGP supports IPv6 unicast route redistribute. It allows users to introduce information from other routing protocols (connected, static, OSPFv3 and RIPng) and redistribute the information. To configure the redistribute metric, in the IPv6 unicast routing configuration mode, use the following command:

redistribute {**ospf** | **connected** | **static** | **rip**} [**metric** *value*]

- **ospf** | **connected** | **static** | **rip** – Specifies the protocol type which can be connected route (**connected**), static route (**static**), RIPng (**rip**) or OSPFv3 (**ospf**).
- **metric** *value* – Specifies the redistribute metric value. The value range is 0 to 4294967295.

Repeat the above command to redistribute different types of protocols.

To cancel the redistribute of the specified protocol, in the IPv6 unicast routing configuration mode, use the following command:

no redistribute {**ospf** | **connected** | **static** | **rip**}

Activating a BGP Connection

By default, the IPv6 BGP connection between the configured BGP peer or peer group and the device is activated. You can de-activate or re-activate the IPv6 BGP connection. To activate the IPv6 BGP connection, in the IPv6 unicast routing configuration mode, use the following command:

neighbor {*X:X:X:X::X* / *A.B.C.D* / *peer-group*} **activate**

- *X:X:X:X::X* / *A.B.C.D* / *peer-group* – Specifies the IPv4/IPv6 address of the peer or the name of the peer group.

To de-activate the IPv6 BGP connection to the specified BGP peer or peer group, in the IPv6 unicast routing configuration mode, use the following command:

no neighbor {*X:X:X:X::X* / *A.B.C.D* / *peer-group*} **activate**

Sending Community Path Attributes to a Peer/Peer Group

To configure the upper limit of prefixes that can be received from IPv6 peer/peer group, use the following command in the IPv6 unicast routing configuration mode:

neighbor {*X:X:X:X::X* / *A.B.C.D* / *peer-group*} **send-community** {**standard** | **extended** | **both**}

- {*X:X:X:X::X* / *A.B.C.D* / *peer-group*} – Specifies the IPv4/IPv6 address of the peer or the name of the peer group.
- **standard** | **extended** | **both** – Specifies the type of the communities path attributes. There are three types: **standard** means the standard communities path attributes, **extended** means the extended communities path attributes, and **both** means both of the communities path attributes and extended communities path attributes.

Use the following command to cancel the above configurations:

no neighbor {*X:X:X:X::X* / *A.B.C.D* / *peer-group*} **send-community**

Specifying Upper Limit of Prefixes

To configure the upper limit of prefixes that can be received from IPv6 peer/peer group, use the following command in the IPv6 unicast routing configuration mode:

neighbor {*X:X:X:X::X* / *A.B.C.D* / *peer-group*} **maximum-prefix** *maximum* [*threshold*] [**restart** *restart-interval*] [**warning-only**]

- *{X:X:X:X::X | A.B.C.D | peer-group}* – Specifies the IPv4/IPv6 address of the peer or the name of the peer group.
- *maximum* - Specifies the upper limit of prefixes that can be received from IPv6 peer/peer group.
- *threshold* – Specifies the threshold that will trigger the generation of log information. The default value is 75, and it ranges from 1 to 100.
- **restart** *restart-interval* – After the received prefixes reaches the threshold, the connection to the peer will be disconnected and the connection will be re-established after the specified interval here. The unit is minute and the value ranges from 1 to 65525.
- **warning-only** – After the received prefixes reaches the threshold, the system generates the corresponding log information.

Use the no form to cancel the above configurations:

no neighbor {*X:X:X:X::X* | *A.B.C.D* | *peer-group*} **maximum-prefix**

Viewing BGP Routing Information

To view the routing information of the entire IPv6 BGP routing table, in any mode, use the following command:

show ip bgp ipv6 unicast {*X:X:X:X::X/Mask* | **vrouter** *vrouter-name*}

- *X:X:X:X::X/Mask* – Shows the IPv6 BGP routing information of the specified network.
- *vrouter-name* - Shows the IPv6 BGP routing information of the specified VRouter.

To view the status parameters of all BGP connections, including the prefix, path, attribute, etc., in any mode, use the following command:

show ip bgp ipv6 unicast summary [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the IPv6 BGP routing information of the specified VRouter.

To view the BGP peer status, in any mode, use the following command:

show ip bgp ipv6 unicast neighbor [*X:X:X:X::X* | *A.B.C.D*] [**vrouter** *vrouter-name*]

- *X:X:X:X::X* | *A.B.C.D* – Shows the BGP peer status of the specified IPv4/IPv6 address.
- *vrouter-name* - Shows the IPv6 IPv6 BGP routing information of the specified VRouter.

Configuring IPv6 Policy-based Route

Policy-based Route (PBR) is designed to select a router and forward data based on the source IP address, destination IP address and service type of a packet, and specify the next hop of the packets which match the policy. System supports to configure PBR rules using IPv6 address.

To configure the following items, see Policy-based Route in FSOS_CLI_User_Guide_Routing:

- Editing a PBR Rule
- Enabling/Disabling a PBR Rule
- Moving a PBR Rule
- Applying a PBR Rule

Creating a PBR Policy

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

pbr-policy *name*

- *name* – Specifies the name of the PBR policy. The length is 1 to 31 characters. If the policy exists, the system will directly enter the PBR policy configuration mode.

To delete the specified PBR policy, use the command **no pbr-policy** *name*.

Creating a IPv6 PBR Rule

To create a IPv6 PBR rule, in the PBR policy configuration mode, use the following command:

match-v6 [**id** *rule-id*] [**before** *rule-id* | **after** *rule-id* | **top**] *src-addr dst-addr service-name* [*application-name*] **nexthop** {*interface-name* / *A.B.C.D* | **vrouter** *vrouter-name* | **vsys** *vsys-name*} [**weight** *value*] [**track** *track-object-name*]

- **id** *rule-id* – Specifies the ID of the new PBR rule. The value range is 1 to 255. If no ID is specified, the system will automatically assign an ID. The rule ID must be unique in its corresponding PBR policy.
- **before** *rule-id* | **after** *rule-id* | **top** – Specifies the position of the PBR rule. The new PBR rule can be located before a rule (**before** *rule-id*), after a rule (**after** *rule-id*) or at the top of all the rules (**top**). By default, the system will put the new rule at the end of all the rules.
- *src-addr* – Specifies the source address which should be an entry defined in the address book. The address should be IPv6 address.

- *dst-addr* – Specify the destination address which should be an entry defined in the address book. The address should be IPv6 address.

- *service-name* – Specifies the name of the service. service-name should be the service defined in the service book.

- *application-name* – Specifies the name of the application. application-name should be the application defined in the application book.

- **nexthop** {*interface-name* / *A.B.C.D* | **vrouter** *vrouter-name* | **vsys** *vsys-name*} – Specifies the next hop. *interface-name* is the name of egress interface, or local-address. *A.B.C.D* is the IP address of the next hop, **vrouter** *vrouter-name* is a VRouter, and **vsys** *vsys-name* is the name of VSYS.

- **weight** *value* – Specifies the weight for the next hop. The value range is 1 to 255. The default value is 1. If a PBR rule is configured with multiple next hops, the system will distribute the traffic in proportion to the corresponding weight.

- **track** *track-object-name* – Specifies the track object for the next hop. If the track object fails, the PBR rule will fail as well. For more information about track object, see "Configuring a Track Object" in "System Management" .

To delete the specified rule, in the PBR policy configuration mode, use the following command:

no match-v6 id *rule-id*

In addition, you can also use the following command in PBR policy configuration mode to create a PBR rule ID, and then in the PBR policy rules configuration mode, further configure other relevant parameters of the PBR rule:

match-v6 [**id** *rule-id*] [**before** *rule-id* | **after** *rule-id* | **top**]

- **id** *id* – Specifies the ID of the new PBR rule. If no ID is specified, the system will automatically assign an ID. The rule ID must be unique in the whole system. However, the PBR rule ID is not related to the matching sequence.

- **top** | **before** *rule-id* | **after** *rule-id* – Specifies the position of the PBR rule. The new PBR rule can be located before a rule (**before** *rule-id*), after a rule (**after** *rule-id*) or at the top of all the rules (**top**). By default, the system will put the newly created rule at the end of all the rules.

Configuring IPv6 IS-IS

The IS-IS routing protocol (Intermediate System-to-Intermediate System intra-domain routing information exchange protocol) supports multiple network protocols, including IPv6. The IS-IS routing protocol that supports IPv6 is named IPv6 IS-IS routing protocol. In the IPv6 network environment, you can configure the IPv6 IS-IS routing protocol to realize the connectivity between IPv6 networks.

To configure the following items, see Configuring IS-IS in FSOS_CLI_User_Guide_Routing:

- Configuring the router type
- Configuring the interface type
- Configuring the network as point-to-point type
- Configuring the NET address
- Configuring the metric style
- Configuring the parameters for Hello packets
- Configuring the priority for DIS election
- Configuring the passive interface
- Configuring the parameters for LSP packets
- Configuring the hostname mappings
- Configuring the authentication methods
- Configuring the interface authentication

This section introduces the following configurations:

- Enabling IPv6 IS-IS at interfaces
- Configuring the interface metric
- Entering into the IPv6 unicast routing configuration mode
- Configuring the default route advertisement
- Configuring the administrative distance
- Configuring redistribute
- Configuring the overload bit
- Configuring the SPF calculation interval
- Configuring Multiple-Topology routing
- Viewing IPv6 IS-IS information

Enabling IPv6 IS-IS at interfaces

By default, the IPv6 IS-IS function is disabled at the interface. After creating an IS-IS process at the current router, proceed to enable the IPv6 IS-IS function at the interface. Use the following command in the interface configuration mode:

isis ipv6 enable

Use the **no isis ipv6 enable**command to disable the IPv6 IS-IS function at the interface.

Configuring the Interface Metric

The metric is used to calculate the cost to the destination network via the selected link. To configure the metric of the link where the interface locates in IPv6 network, use the following command in the interface configuration mode:

isis ipv6 metric *value* [**level-1** | **level-2**]

- *value* − Configure the metric value of the link that the interface locates. The value ranges from 1 to 16777214 and the default value is 10.
- **level-1** | **level-2** − Use level-1 to configure the metric value for Level-1 routes. Use level-2 to configure the metric value for Level-2 routes. Without specifying level-1 or level-2, the metric value is effective for both Level-1 and Level-2 routes.

Use the **no isis ipv6 metric** command to restore the metric value to the default one.

Entering into the IPv6 Unicast Routing Configuration Mode

To configure the settings for IPv6 IS-IS unicast route, you must enter into the IPv6 unicast routing configuration mode. Execute the following commands to enter into this configuration mode:

ip vrouter *vrouter-name* − In the global configuration mode, execute this command to enter into the VRouter configuration mode.

router isis − Enter into the IS-IS routing configuration mode and create the IS-IS process. The IS-IS processes in each VRouter are independent.

address-family ipv6 unicast - Enter into the IPv6 unicast routing configuration mode.

Configuring the Default Route Advertisement

The default IPv6 route in the introduced routing information will not be used by the routers. To advertise the default IPv6 route in the routing domain, in the IS-IS IPv6 unicast routing configuration mode, use the following command:

default-information originate

If there is a default route in the router with the above command configured, the IS-IS process in this router will advertise this route via Level-2 LSPs.

To cancel the default IPv6 route advertisement, use the **no default-information originate** command.

Configuring the Administrative Distance

To configure the administrative distance of the IPv6 IS-IS route, use the following command in the IS-IS IPv6 unicast routing configuration mode:

distance *distance-value*

- *distance-value* – Specify the administrative distance. The value ranges from 1 to 255. The default value is 115.

To restore the value to the default one, use the **no distance** command.

Configuring Redistribute

IPv6 IS-IS allows you to introduce routing information from other routing protocols (connected, static, OSPFv3, IPv6 BGP and RIPng) and redistribute the information. To configure the redistribute and the corresponding metric, in the IS-IS IPv6 unicast routing configuration mode, use the following commands:

redistribute {**connected** | **static** | **ospf** | **bgp** | **rip**} [**level-1** | **level-1-2** | **level-2**] [**metric** *value*] [**metric-type** {**external** | **internal**}]

- **connected** | **static** | **ospf** | **bgp** | **rip** – Specifies the protocol type which can be **connected**, **static**, **OSPF**(OSPFv3), **bgp**(IPv6 BGP), or **rip**(RIPng).
- **level-1** | **level-1-2** | **level-2** – Specifies the level for the introduced route, including the level-1 route (**level-1**), level-2 route (**level-2**), and both levels (**level-1-2**).
- **metric** *value* – Specifies a metric value for the introduced route. The value range is 0 to 4294967296. The default value is 0. When the metric type of the router is narrow, the metric value of the introduced route cannot exceed 63.
- **metric-type** {**external** | **internal**} – If you select the external metric type (**external**), the metric value will be the sum of the value configured in **metric** *value* and 64. If you select the internal metric type (**internal**), the metric value will be the one you configured in the **metric** *value* command. The default option is internal.

To cancel the redistribute configurations, use the **no redistribute** {**connected** | **static** | **ospf** | **bgp** | **rip**} [**level-1** | **level-1-2** | **level-2**] command.

Configuring the Overload Bit

If a router is lack of resources, its LSDB might be inaccurate or incomplete. You can configure the overload bit for this router, which will suppress the advertisement of the introduced routes. The routes introduced from other routing protocol will not be advertised. And this reduces the number of packets that are forwarded via this router. However, the packets whose destination is the directly connected network of this router or the packets whose destination is within the same routing domain, can be forwarded to this router as before. To configure the overload bit for the router, use the following command in the IS-IS IPv6 unicast routing configuration mode:

set-overload-bit suppress external

To cancel the overload bit configuration, use the command **no set-overload-bit**.

Configuring the SPF Calculation Interval

If the LSDB changes, the router will re-calculate the SPF. To configure the SPF calculation interval for IPv6 IS-IS, use the following command in the IPv6 IS-IS unicast routing configuration mode:

spf-interval *value* [**level-1** | **level-2**]

- *value* – Specify the SPF calculation interval. The value ranges from 1 to 120. The default value is 10. The unit is second.
- **level-1** | **level-2** – Enter **level-1** to specify the SPF calculation interval for level-1 SPFs only, and enter **level-2** to specify the SPF generation interval for level-2 SPFs only. If you enter no parameter, the configured interval value will be used for both level-1 SPFs and level-2 SPFs.

Use the **no spf-interval**command to restore the value to the default one.

Configuring Multiple-Topology Routing

When using IPv6 IS-IS, the device supports both unique topology routing and multiple-topology routing. When using unique topology routing, the device calculates the mixed routing for both IPv4 topo and IPv6 topo.

When using multiple-topology routing, the device will perform the SFP calculation for IPv4 topo and IPv6 topo individually, and generate the routing information individually.

By default, the system uses the unique topology routing. To enable the multiple-topology routing, first change the metric type to wide in the IS-IS routing configuration mode by using the **metric-style wide** command. Then perform the following command in the IS-IS IPv6 unicast routing configuration mode:

multi-topology

To disable the multiple-topology routing, use the command **no multi-topology**.

Viewing IPv6 IS-IS Information

To show the routing information of the IPv6 IS-IS, use the following command in any mode:

show isis ipv6 route

To show the IS-IS process and corresponding information, use the following command in any mode:

show isis [**vrouter** *vrouter-name*]

- *vrouter-name* - Show the information of the specified vrouter.

To show the link state database, use the following command in any mode:

show isis database [**detail**] [**vrouter** *vrouter-name*]

- **detail** – Show the detailed information.
- *vrouter-name* - Show the information of the specified vrouter.

To show the IS-IS interface information, use the following command in any mode:

show isis interface [*interface-name*]

Configuring IPv6 DHCP

DHCP, the abbreviation for Dynamic Host Configuration Protocol, is designed to allocate appropriate IPv6 addresses and related network parameters for subnets automatically, thus reducing requirement on network administration. Besides, DHCP can avoid address conflict to assure the re-allocation of idle resources.

FS devices support IPv6 DHCP client, DHCP server and DHCP relay proxy.

- DHCP client: A FS device's interface can be configured as a DHCP client and obtain IP addresses from the DHCP server.
- DHCP server: A FS device's interface can be configured as a DHCP server and allocate IP addresses chosen from the configured address pool for the connected hosts.
- DHCP relay proxy: A FS device's interface can be configured as a DHCP relay proxy to obtain DHCP information from the DHCP server and forward the information to connected hosts.

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

Configuring a DHCP Client

You can configure an interface of the device as the DHCP client that obtains IPv6 address from the DHCP server. The DHCP client should be configured in the interface configuration mode. The configuration includes:

- Obtaining an IPv6 address via DHCP
- Releasing and renewing the IPv6 address

Obtaining an IPv6 address via DHCP

To enable the interface to obtain an IPv6 address via DHCP, in the interface configuration mode, use the following command:

ipv6 address dhcp [**rapid-commit**]

- **ipv6 address dhcp** – Enable the interface to obtain an IP address via DHCP.
- **rapid-commit** – Specifying this option can help fast get IPv6 address from the server. You need to enable both of the DHCP client and the server's Rapid-commit function.

To cancel the configuration, in the interface configuration mode, use the command **no ipv6 address dhcp**.

Releasing and Renewing the IPv6 Address

The interface that has obtained a dynamic IPv6 address via DHCP can release and renew its IPv6 address. To release and renew the IPv6 address, in the interface configuration mode, use the following commands:

- Release: **dhcpv6-client ip release**
- Renew: **dhcpv6-client ip renew**

To view the DHCP IPv6 address information allocated to an interface, in the interface configuration mode, use the following command:

show dhcpv6-client interface *interface-name*

Configuring a DHCP Server

The FS devices can act as a DHCP server to allocate IP addresses for the DHCP clients in the subnets. The DHCP server should to be configured in the DHCP server configuration mode. To enter the DHCP server configuration mode, in the global configuration mode, use the following command:

dhcpv6-server pool *pool-name*

- *pool-name* – Specifies the name of the DHCP address pool.

After executing the above command, the system will create a new DHCP address pool and enter the DHCP server configuration mode of the address pool; if the specified address pool exists, the system will directly go to the DHCP server configuration mode.

To delete the specified address pool, in the global configuration mode, use the command **no dhcpv6-server pool** *pool-name*.

The DHCP server functions you can configure include:

- Basic configuration of the DHCP address pool
- Binding the address pool to an interface

Basic Configuration of the DHCP Address Pool

This section describes how to configure DHCP address pool.

Configuring an IP Range

You need to specify the IP range used for external allocation. To specify the IP range of the address pool, in the DHCP server configuration mode, use the following command:

address prefix *ipv6-address/prefix-length* [**lifetime** {*valid-lifetime* | **infinite**} | {*preferred-lifetime* | **infinite**}]

- *ipv6-address/prefix-length* – Specifies the IPv6 address prefix and prefix length.
- *valid-lifetime* – Specifies the lifetime of the address.
- **infinite** – If specified the parameter, the address will be valid permanently.
- *preferred-lifetime* – Specifies the preferred lifetime for the IPv6 address. The preferred lifetime should not be larger than the valid lifetime.

To cancel the specified IP range, in the DHCP server configuration mode, use the command **no address prefix**.

Configuring Domain Name for the DHCP Client

To configure domain name for the DHCP client, in the DHCP server configuration mode, use the following commands:

domain *domain-name*

- *domain-name* – Specifies the domain name.

To cancel the configured domain name, in the DHCP server configuration mode, use the command **no domain**.

Configuring DNS Servers for the DHCP Client

To configure DNS servers for the DHCP client, in the DHCP server configuration mode, use the following commands:

dns-server ipv6-address [*ipv6-address1*] [*ipv6-address2*]

- *ipv6-address1* – Specifies the IP address of the primary DNS server.
- *ipv6-address2* – Specifies the IP address of the alternative DNS server.

To cancel the configured DNS, WINS server and domain name, in the DHCP server configuration mode, use the command **no dns-server**.

Binding the Address Pool to an Interface

If the address pool is bound to an interface, the interface will run DHCP server based on the configuration parameters of the address pool. To bind the address pool to an interface, in the interface configuration mode, use the following command:

dhcpv6-server enable pool *pool-name* [**rapid-commit**] [**preference** *preference*]

- *pool-name* – Specifies the address pool defined in the system.
- **rapid-commit** – Specifying this option can help fast get IPv6 address from the server. You need to enable both of the DHCP client and the server's Rapid-commit function.
- **preference** *preference* – Specifies the priority of the DHCP server. The range should be from 0 to 255. The bigger the value is, the higher the priority is.

To disable the DHCP server on the interface, in the interface configuration mode, use the command **no dhcpv6-server enable**.

Configuring a DHCP Relay Proxy

The FS device can act as a DHCP relay proxy to receive requests from a DHCP client and send requests to the DHCP server, and then obtain DHCP information from the server and return it to the client. The DHCP relay proxy should be configured in the interface configuration mode. The configurations include:

- Specifying the IP address of the DHCP server
- Enabling DHCP relay proxy on an interface

Enabling DHCP Relay Proxy on an Interface

To enable DHCP relay proxy on an interface, in the interface configuration mode, use the following command:

dhcpv6-relay enable

To disable the specified DHCP relay proxy, in the interface configuration mode, use the command **no dhcpv6-relay enable**.

Specifying the IP Address of the DHCP Server

To specify the IP address of the DHCP server, in the interface configuration mode, use the following command:

dhcpv6-relay server *ipv6-address* [**interface** *interface-name*]

- *ip-address* – Specifies the IP address of the DHCP server.
- **interface** *interface-name* – If the DHCP server is specified as link-local address, you need to specify the egress interface name.

To cancel the specified IP address, in the interface configuration mode, use the command **no dhcpv6-relay server** *ipv6-address* [**interface** *interface-name*].

Viewing DHCP Configuration Information

In any mode, use the following command to view DHCP configuration information:

- **show dhcpv6 duid**: Shows device’s IPv6 UID information.
- **show dhcpv6 interface**: Shows all the interfaces information which enabling DHCP IPv6.
- **show dhcpv6-client interface** *interface-name*: Shows the interface information which enabling DHCP client IPv6.
- **show dhcpv6-server binding** *pool-name*: Shows the binding relationship between DHCP server and client.
- **show dhcpv6-server pool** *pool-name*: Shows the address pool information of the DHCP server.

Configuring IPv6 DNS

FSOS supports IPv6 DNS for the translation between domain names and IPv6 addresses. IPv6 introduces new DNS records to resolve IPv6 addresses and translate domain names to IPv6 addresses.

> Note:This section only describes IPv6-related configurations. For more information about DNS and its configurations, see "DNS" of "Firewall".

Configuring IPv6 DNS Servers

IPv6 DNS servers are used for domain name resolution. To configure IPv6 DNS servers, in the global configuration mode, use the following command:

ipv6 name-server *ipv6-address1* [*ipv6-address2*] ... [*ipv6-address6*] [**vrouter** *vr-name*]

- *ipv6-address1* – Specifies the IPv6 address of DNS server. You can configure up to six DNS servers by one or multiple commands, i.e., running command **ipv6 name-server 2002:ae3:1111:2222::1 2001:0db8::3** and running commands **ipv6 name-server 2002:ae3:1111:2222::1** and **ipv6 name-server 2001:0db8::3**make no difference.
- **vrouter** *vr-name* – Specifies the VRouter the IPv6 DNS server belongs to.

To cancel the specified IPv6 DNS servers, in the global configuration mode, use the command **no ipv6 name-server** *ipv6-address1* [*ipv6-address2*] ... [*ipv6-address6*] [**vrouter** *vr-name*].

Configuring an IPv6 DNS Proxy Server List

IPv6 DNS proxy server list contains mapping entries for domain names and corresponding IPv6 DNS servers. The list contains up to six mapping entries. To add a mapping entry to the IPv6 DNS proxy server list, in the global configuration mode, use the following command:

ipv6 dns-proxy domain {*domain-suffix* | **any**} **name-server** {**use-system** | *ipv6-address1* [*ipv6-address2*] ... [*ipv6-address6*]} [**vrouter** *vr-name*]

- *domain-suffix* | **any** – Specifies the suffix of domain name that is used to match the domain names in IPv6 DNS requests. any indicates any suffix.
- **name-server** {**use-system** | *server-ip1* [*server-ip2*] ... [*server-ip6*]} – Specifies IPv6 addresses for DNS servers. The servers can either be device's built-in IPv6 DNS server (**use-system**) or specified IPv6 addresses (*ipv6-address1* [*ipv6-address2*] ··· [*ipv6-address6*]). You can specify up to six IP addresses for IPv6 DNS servers.
- **vrouter** *vr-name* – Specifies the VRouter the IPv6 DNS server belongs to.

To delete the specified mapping entry, in the global configuration mode, use the command **no ipv6 dns-proxy domain** {*domain-suffix* | **any**} [**vrouter** *vr-name*].

For example, to add a mapping entry whose suffix is com and IP address of IPv6 DNS server is 2010::1, use the following command:

```
hostname(config)# ipv6 dns-proxy domain com name-server 2010::1
```

Enabling/Disabling IPv6 DNS Proxy

The IPv6 DNS proxy on interfaces is disabled by default. To enable IPv6 DNS proxy on an interface, in the interface configuration mode, use the following command:

dns-proxy

To disable DNS proxy, in the interface configuration mode, use the command **no dns-proxy**.

Adding a Static IPv6 DNS Mapping Entry

To add a static IPv6 DNS mapping entry to the cache manually, in the global configuration mode, use the following command:

ipv6 host *host-name* {*ipv6-address1* [*ipv6-address2*] ... [*ipv6-address8*]} [**vrouter** *vr-name*]

- *host-name* − Specifies the hostname. The length is 1 to 255 characters.
- {*ipv6-address1* [*ipv6-address2*] ... [*ipv6-address8*]} − Specifies the IPv6 addresses of the host. You can specify up to eight IPv6 addresses.
- **vrouter** *vr-name* − Specifies the VRouter the host belongs to.

To delete the specified static IPv6 DNS mapping entry, in the global configuration mode, use the command **no ipv6 host** *host-name* [**vrouter** *vr-name*].

Clearing a Dynamic IPv6 DNS Mapping Entry

To clear a dynamic IPv6 DNS mapping entry manually, in the execution mode, use the following command:

clear ipv6 host [*host-name* [**vrouter** *vr-name*]]

- *host-name* − Clears IPv6 DNS mapping entries of the specified host.
- **vrouter** *vr-name* − Specifies the VRouter the host belongs to.

This command is used to clear the specified or all the dynamic IPv6 DNS mapping entries. To clear static IPv6 DNS mapping entries that are configured manually, in the global configuration mode, use the command **no ipv6 host** *host-name* [**vrouter** *vr-name*].

Viewing IPv6 DNS Mapping Entries

To view IPv6 DNS mapping entries, in any mode, use the following command:

show ipv6 host [*host-name*] [**vrouter** *vr-name*]

- *host-name* – Shows IPv6 DNS mapping entries of the specified host.
- **vrouter** *vr-name* – Specifies the VRouter the host belongs to.

Viewing IPv6 DNS Configuration

To view IPv6 DNS configuration, in any mode, use the following command:

show ipv6 dns

Configuring PMTU

When an IPv6 node sends large amount of data to another node, the data is transferred in form of a series of IPv6 packets. If possible, the size of these packets should not exceed the size limit for packets that requires fragmentation in the path from the source node to the destination node. This size is known as path MTU (PMTU) which equals to the smallest MTU of each hop in the path. IPv6 defines a standard mechanism that is used to discover PMTU in any path. FSOS supports this PMTU discovery mechanism.

By default the PMTU discovery mechanism in FSOS is enabled. To enable or disable the PMTU discovery mechanism, in the flow configuration mode, use the following commands:

- Enable: **ipv6 pmtu enable**
- Disable: **no ipv6 pmtu enable**

> Tip: To enter the flow configuration mode, in the global configuration mode, use the command **flow**.

With PMTU enabled, the system will generate a PMTU entry to record the destination address, interface, PMTU value and aging out time after receiving an ICMPv6 Packet Too Big error. If any session to the destination address specified by the PMTU entry is established within the aging out time, the system will refresh the aging out time, i.e., restart counting; if no session matches to the PMTU entry within the aging out time, the entry will be aged out and deleted. You can specify an appropriate aging out time for the PMTU entry as needed.

To specify an aging out time, in the flow configuration mode, use the following command:

ipv6 pmtu ageout-time *time*

- *time* – Specifies the aging out time. The value range is 10 to 600 seconds. The default value is 300.

To restore to the default aging out time, in the flow configuration mode, use the following command:

no ipv6 pmtu ageout-time

You can also clear a PMTU entry immediately as needed. To clear a PMTU entry, in any mode, use the following command (if no optional parameter is specified, the command will clear all the existing PMTU entries):

clear ipv6 pmtu [**dst-ip** *ipv6-address* **interface** *interface-name*]

- *ipv6-address* – Specifies the IPv6 address of the PMTU entry that will be deleted.
- *interface-name* – Specifies the interface of the PMTU entry that will be deleted.

To view PMTU entry information, in any mode, use the following command (if no optional parameter is specified, the command will show the information of all the existing PMTU entries):

show ipv6 pmtu [**dst-ip** *ipv6-address* **interface** *interface-name*]

- *ipv6-address* – Shows the PMTU entry of the specified IPv6 address.
- *interface-name* – Shows the PMTU entry of the specified interface.

To view the status of PMTU, e.g., if the function is enabled, or the aging out time, in any mode, use the following command:

show ipv6 pmtu status

Configuring User-defined Application

Besides the predefined applications, you can also create your own user-defined applications based on IPv6 address. By configuring the customized application signature rules, FSOS can identify and manage the IPv6 traffic that crosses into the device, thus identifying the type of the IPv6 traffic.

The configurations of IPv6 User-defined Application includes:

- Configuring IPv6 source address
- Configuring IPv6 destination address

Tip: This section only describes IPv6-related configurations. For more information about User-defined Application and its configurations, see "Service and Application" of "Firewall".

Creating/Deleting the User-defined Applications

To create a user-defined application and add this newly-created one to the application book, use the following command in the global configuration mode:

application *application-name*

- *application-name* – Specifies the name of the user-defined application. You can specify up to 31 characters. This name must be unique in the entire system.

After executing this command, the system enters the application configuration mode.

To delete the user-defined application, use the following command:

no application *application-name*

Enabling the User-defined Application Signature Configuration Mode

To enable the user-defined application signature configuration mode, use the following command in the global configuration mode:

app-signature

Configuring IPv6 Source Address

To specify the IPv6 source address for the user-defined application signature, use the following command in the user-defined application signature configuration mode:

src-ipv6 *ipv6-address*

- *ipv6-address* – Specifies the IPv6 source address for the user-defined application signature.

Configuring IPv6 Destination Address

To specify the IPv6 destination address for the user-defined application signature, use the following command in the user-defined application signature configuration mode:

dst-ipv6 *ipv6-address*

- *ipv6-address* – Specifies the IPv6 destination address for the user-defined application signature.

Configuring an IPv6 Policy Rule

Policy is a basic function of network security devices. Network traffic is controlled by policy rules. FSOS supports both IPv4 and IPv6 policy rules. The basic components of a policy rule include addresses (source and destination address), service and action. This section describes IPv6 configuration of the above components.

Configuring an IPv6 Address Entry

FSOS address book supports both IPv4 and IPv6 address entries. IPv4 address entries only contain members of IPv4 addresses, IPv4 segments, IPv4 hosts and other IPv4 address entries; IPv6 address entries only contain members of IPv6 addresses, IPv6 segments and other IPv6 address entries. The address book contains a default address entry named ipv6-any that contains all the IPv6 addresses; the address entry named Any contains all the IPv4 addresses.

> Tip: This section only describes the configuration of IPv6-related policy rules. For more information about policy rule configurations, see “Policy” .

To create an address entry and enter the address entry configuration mode, in the global configuration mode, use the following command:

address *address-entry* ipv6

If the specified address entry already exists, the system will directly enter the address entry configuration mode. To add an IPv6 address to the address entry or delete an IPv6 address from the address entry, in the address entry configuration mode, use the following commands:

ip *ipv6-address/M*

no ip *ipv6-address/M*

To add an IPv6 address range to the address entry or delete an IPv6 address range from the address entry, in the address entry configuration mode, use the following commands:

range *min-ipv6-address max-ipv6-address*

no range *min-ipv6-address max-ipv6-address*

When creating an IPv6 address entry, keep in mind that:

- An IPv6 address entry cannot nest an IPv4 address entry, and vice versa;
- The first 64 bits of an IPv6 address range must be identical. For example, the address range from 2005::1 to 2006::1 is not permitted, while the address range from 2005::1 to 2005::1000 is permitted;
- The current version does not support hosts with IPv6 addresses.

Configuring an IPv6 Service

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

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

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

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

service *service-name*

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

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

icmpv6 type *type-value* [**code** *min-code* [*max-code*]]

- *type-value* – Specifies the ICMPv6 type value. For more information about the value range, see Appendix 1: ICMPv6 Type and Code. The default value is Any, which indicates all the ICMPv6 type values.

- **code** *min-code* [*max-code*] – Specifies the minimum code value (*min-code*) and maximum code value (*max-code*) for ICMPv6. The value range is 0 to 6 and Any (any ICMPv6 code value). If the code value is not specified, by default the system will use the code value that corresponds to the Type value (defined in RFC); if the maximum code value is not specified, by default the system will use the minimun code value as the maximum code value.

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

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

Configuring an Action for IPv6 Policy Rule

IPv4 policy rules support the following five actions: deny, permit, fromtunnel, tunnel and webauth; in the current version IPv6 policy rules only support two basic actions: deny and permit.

Configuring an IPv6 Policy Rule

When configuring a policy rule, you must specify the same type of source address and destination address, i.e., if the source address is an IPv6 address, the destination address must be an IPv6 address.

To configure an IPv6 policy rule, in the policy configuration mode (to enter the policy configuration mode, in the global configuration mode, use the command policy-global), use the following command:

rule [**id** *id*] [**top** | **before** *id* | **after** *id*] **from** {*src-addr* / *ipv6-address*} **to** {*dst-addr* / *ipv6-address*} **service** *service-name* [**application** *app-name*] {**permit** | **deny**}

- **id** *id* − Specifies the ID of the policy rule. If not specified, the system will automatically assign an ID to the policy rule. The ID must be unique in the entire system.
- **top** | **before** *id* | **after** *id* − Specifies the location of the policy rule. The location can be **top** | **before** *id* | **after** *id*. By default, the newly-created policy rule is located at the end of all the rules.
- **from** *src-addr* − Specifies the source address of the policy rule. src-addr can be an IPv6 address, an IPv6 address entry defined in the address book, or ipv6-any.
- **to** *dst-addr* − Specifies the destination address of the policy rule. dst-addr can be an IPv6 address, an IPv6 address entry defined in the address book, or ipv6-any.
- **service** *service-name* − Specifies the service name of the policy rule. service-name is the service defined in the service book.
- **permit** | **deny** − Specifies the action of the policy rule. **permit**means system will permit the traffic to pass through. **deny** means system will deny the traffic.

Besides you can also use the following command in the policy configuration mode to create a policy rule ID and enter the policy rule configuration mode for further configurations:

rule {**id** *id* | {**top** | **before** *id* | **after** *id*}}

- **id** *id* − Specifies the ID of the policy rule. If the policy exists, the system will directly enter the policy configuration mode. If not specified, the system will automatically assign an ID to the policy rule. The ID must be unique in the entire system. The policy rule ID is not related to the matching sequence of the policy rule.
- **top** | **before** *id* | **after** *id* − Specifies the location of the policy rule. The location can be **top** | **before** *id* | **after** *id*. By default, the newly-created policy rule is located at the end of all the rules.

Editing an IPv6 Policy Rule

You can edit improper parameters for the policy rule in the policy rule configuration mode. To enter the policy rule configuration mode via CLI, in the global configuration mode, use the following commands:

- **rule** {**id** *id* | {**top** | **before** *id* | **after** *id*}}
- **rule id** *id*(The command applies to the case that ID is existing. To delete the rule, use the command **no rule id** *id*.)

After entering the policy rule configuration mode, to edit the policy rule, use the following commands:

- To add the source address of the IP member type: **src-ip** *ipv6-address/M*
- To delete the source address of the IP member type: **no src-ip** *ip-address/M*
- To add the source address of the IP range type: **src-range** *min-ipv6-address* [*max-ipv6-address*]
- To delete the source address of the IP range type: **no src-range** *min-ipv6-address* [*max-ipv6-address*]
- To add the destination address of the IP member type: **dst-ip** *ipv6-address/M*
- To delete the destination address of the IP member type: **no dst-ip** *ipv6-address/M*
- To add the destination address of the IP range type: **dst-range** *min-ipv6-address* [*max-ipv6-address*]
- To delete the destination address of the IP range type: **no dst-range** *min-ipv6-address* [*max-ipv6-address*]

Configuring Access Control for an IPv6 Policy

The combination of the ACL Profile and policy rule allows the FS devices to access control over the IPv6 message based on an IPv6 policy, such as IPv6 extended header, source / destination MAC address etc.

To configure the access control function, take the following three steps:

1. Configure a ACL profile, which contains access control rules.
2. Configure an access control rule, which is used to specify the IPv6 extended message, rule type, and control action required to be controlled.
3. Binding the ACL profile to a policy rule. Only after the configured ACL profile is bound to a policy rule can access control function on the device.

Configuring an ACL Profile

The ACL profile needs to be configured in the ACL profile configuration mode. To enter the ACL profile configuration mode, in the global configuration mode, use the following command:

acl-profile *acl-profile-name*

- *acl-profile-name* – Specifies the name of the ACL profile. After executing the command, the system will create a ACL profile with the specified name, and enter the ACL profile configuration mode; if the specified name exists, the system will directly enter the ACL profile configuration mode. You can specify up to 64 ACL profiles.

To delete the specified ACL Profile, in the global configuration mode, use the command **no acl-profile** *acl-profile-name*.

Configuring an Access Control Rule

To configure an access control rule, in the ACL Profile configuration mode, use the following command:

sequence *id* {**drop** |**pass**} [**both** |**forward** |**backward**] [**src-mac** *src-mac-address*] [**dst-mac** *dst-mac-address*][**dscp** *dscp-value*] [**flow-label** *flow-label-value* [*end-flow-label-value*]] [**ext-header** [**ah**][**fragment**][**esp**][**hop**][**none**][**dest** [*dest-value1* [*dest-value2* |**home-address**]]][**mobility** [*mobility-value1 [mobility-value2*]|**bind-refresh** | **bind-ack** |**bink-err** | **bind-update** | **cot** | **coti**| **hot** |**hoti**]][**routing** [*routing-value1* [*routing-value2*]]]]

- *id* – Specifies the ID of the access control rule. .The range is 1 to 32.
- **drop** | **pass** – Specifies the action for the access control rule, drop or pass.
- **both** |**forward** |**backward** – Specifies the traffic direction of the access control rule.
- **src-mac** *src-mac-address* – Specifies the source MAC address of the access control rule.
- **dst-mac** *dst-mac-address* – Specifies the destination MAC address of the access control rule.
- **dscp** *dscp-value* – Specifies the DSCP value, the range is 0 to 63.
- **flow-label** *flow-label-value* [*end-flow-label-value*] – Specifies the IPv6 flow label or flow label range, the range is 0 to 1048575.
- [**ext-header** [**ah**][**fragment**][**esp**][**hop**][**none**][**dest** [*dest-value1* [*dest-value2* |**home-address**]]][**mobility** [*mobility-value1 [mobility-value2*]|**bind-refresh** | **bind-ack** |**bink-err** | **bind-update** | **cot** | **coti**| **hot** |**hoti**]][**routing** [*routing-value1* [*routing-value2*]]]] – Specifies the IPv6 extended header and parameter values.

To delete the specified access control rule, in the ACL Profile configuration mode, use the command **no sequence** *id*.

Configuring the Default Action

When there is no access control rule is hit, the system will take the specified default access control action. To configure the default action, in the ACL Profile configuration mode, use the following command:

default-action {**drop** |**pass**}

- **drop** | **pass** – Specifies the default action for the access control rule, drop or pass.

To delete the default action, in the ACL Profile configuration mode, use the command **no default-action**.

Binding the ACL Profile to a Policy Rule

The configured ACL profiles will not take effect until being bound to a policy rule. To bind an ACL Profile to a policy rule, in the policy configuration mode, use the following command:

acl *acl-profile-name*

- *acl-profile-name* – Specifies the name of the ACL profile that will be bound.

To cancel the binding, in the ACL Profile configuration mode, use the command **no acl**.

Viewing ACL Profile Information

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

show acl-profile [*acl-profile-name*]

- *acl-profile-name* – Shows the configuration of the specified ACL profile. If this parameter is not specifies, the command will show the configurations of all the ACL profiles.

Configuring IPv6 ALG

Compared with IPv4 ALG, the system supports IPv6 ALG for the following protocols: FTP, TFTP, HTTP, RSH. Besides, you can also specify IPv6 addresses for the IPs that are not restricted by the URL filter. When configuring an ALG-related policy rule, make sure the rule references IPv6 addresses, for example, **rule from ipv6-any service to ipv6-any ftp permit**.

NDP Protection

NDP is a key IPv6 protocol, but it is not designed with any authentication mechanism, resulting in untrusted network nodes and attacks against the protocol. The main attacks include:

- Address spoofing: Attackers modify the MAC address of victim host by RS (Router Solicitation)/NS(Neighbor Solicitation)/NA(Neighbor Advertisement)/RA(Router Advertisement)/Redirect packets, or modify the MAC address of gateway by RS/NS/NA/RA packets, resulting in communication errors between the victim host and network.
- DAD attack: When the victim host performs DAD query, attackers interfere with the process by NS or NA packets, resulting in DAD failure and inability to obtain the IP address on the victim host.
- RA spoofing: Attackers launch spoofing attacks by forging RA packets, resulting in network configuration error on the victim host.
- Flooding: Attackers send huge amount of NS/RS/NA/RA packets to flood the ND table entries on the gateway.
- Redirection: Attackers use link layer address as the source address and send redirection packets to the victim host; when the victim host receives the erroneous redirection message, its routing table will be modified.

FSOS provides a series of NDP protection measures for the above attacks to assure the security of IPv6 network, including:

- IP-MAC binding
- NDP learning
- NDP inspection
- NDP spoofing defense (NDP reverse query, IP number per MAC check, unsolicited NA packets rate)
- NDP spoofing statistics

You can adopt different protection measures for different network applications. For example, to implement Layer 2 NDP protection, you can enable NDP inspection (configuring an NDP packet rate limit, configuring a trusted interface, denying RA packets); to implement Layer 3 protection, you can disable NDP learning or dynamic entry learning, enable ND reverse query, or enable one-click binding to convert dynamic IP-MAC entries to static entries.

The following section describes the configuration and usage of the above protection measures.

IP-MAC Binding

To reinforce network security control, the device supports IP-MAC binding. The binding information can be obtained statically or dynamically: the information learned via NDP is known as dynamic binding information, and the information manually configured is known as static binding information. To simplify the configuration of static IP-MAC binding, you can convert the dynamic binding information to static binding information by one-click binding. Both the static and dynamic binding information is stored in the IPv6 ND cache table.

Adding a Static IP-MAC Binding Entry

To add a static IP-MAC binding entry to the cache table, in the global configuration mode, use the following command:

ipv6 neighbor *ipv6-address interface-name mac-address*

- *ipv6-address* – Specifies the IPv6 address of the static binding entry.
- *interface-name* – Specifies the interface of the static binding entry.
- *mac-address* – Specifies the MAC address of the static binding entry.

To delete the specified static IP-MAC binding entry, in the global configuration mode, use the following command:

no ipv6 neighbor {**all** | *ipv6-address interface-name*}

One-click Binding

One-click binding allows you to convert dynamic IP-MAC binding entries that are obtained via NDP learning to static binding entries when all the hosts in the Intranet can visit Internet. To configure one-click binding, in the execution mode, use the following command:

exec ipv6 nd-dynamic-to-static [**vrouter** *vr-name*]

- *vr-name* – Specifies the VRouter on which the function is implemented. The default value is the default VR **trust-vr**.

The above command will convert all the dynamic IP-MAC binding entries in the system to static binding entries.

Permitting Static IP-MAC Binding Hosts Only

By default the system allows hosts that are dynamically learned via NDP to visit Internet. To only allow hosts in the static IP-MAC binding entries to visit Internet, in the interface configuration mode, use the following command:

ipv6 nd-disable-dynamic-entry

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

no ipv6 nd-disable-dynamic-entry

Viewing IP-MAC Binding Information

To view IP-MAC binding information, in any mode, use the following command (if no parameter is specified, the command will show all the static and dynamic IP-MAC binding entries in the system):

show ipv6 neighbor [**generic** | **interface** *interface-name* | **slot** *slot-num* | **static** | **vrouter** *vr-name* | *ipv6-address*]

- **generic** – Shows IP-MAC binding entry statistics.
- **interface** *interface-name* – Shows IP-MAC binding entries of the specified interface.
- **slot** *slot-num* – Shows IP-MAC binding entries of the specified slot. Only for some devices (X6150, X6180, X7180).
- **vrouter** *vr-name* – Shows IP-MAC binding entries of the specified VRouter.
- **static** – Shows IP-MAC binding entries.
- *ipv6-address* – Shows IP-MAC binding information of the specified IPv6 address.

Clearing Dynamic IP-MAC Binding Information

To clear dynamic IP-MAC binding information, in any mode, use the following command (if not parameter is specified, the command will clear all the dynamic IP-MAC binding information in the system):

clear ipv6 neighbor [*ipv6-address*]

- *ipv6-address* – Clears IP-MAC binding information of the specified IP address.

NDP Learning

FS devices obtain IP-MAC binding information in the Intranet via NDP learning, and add the binding information to the ND table. By default NDP learning is enabled, i.e., the device will keep on NDP learning and add all the learned IP-MAC binding information to the ND table. If any IP or MAC address changes during NDP learning, the device will update the IP-MAC binding information and add it to the ND table. With NDP learning disabled, the system will only allow hosts whose IP addresses are in the ND table to forward packets.

To configure NDP learning, in the interface configuration mode, use the following command:

- Enable: **ipv6 nd-learning**
- Disable: **no ipv6 nd-learning**

NDP Inspection

FS devices support NDP inspection on interfaces. With this function enabled, the system will check all the NDP packets passing through the specified interface, and compare the IP addresses of the NDP packets with the static binding entries in the ND cache table:

- If the IP address is in the ND cache table, and the MAC address and interface of the packet are also consistent with the binding entry, then the system will forward the NDP packet;
- If the IP address is in the ND cache table, but the MAC address or interface of the packet is not consistent with the binding entry, then the system will drop the NDP packet;
- If the IP address is not in the ND cache table, then the system will drop or forward the packet according to the configuration (**ipv6 nd-inspection** {**drop** | **forward**}).

Enabling/Disabling NDP Inspection

The BGroup and VSwitch interfaces of FSOS support NDP inspection. This function is disabled by default. To enable NDP inspection on a BGroup or VSwitch interface, in the BGroup or VSwitch interface configuration mode, use the following command:

ipv6 nd-inspection {**drop** | **forward**}

- **drop** – Drops NDP packets whose IP addresses are not in the ND cache table.
- **forward** – Forwards NDP packets whose IP addresses are not in the ND cache table.

To disable NDP inspection, in the BGroup or VSwitch interface configuration mode, use the following command:

no ipv6 nd-inspection

Configuring a Trusted Interface

You can configure a physical interface in BGroup or VSwitch as the trusted interface. Packets passing through the trusted interface are exempt from NDP inspection. By default all the interfaces on the device are untrusted. To configure a trusted interface, in the interface configuration mode, use the following command:

ipv6 nd-inspection trust

To cancel the specified trusted interface, in the interface configuration mode, use the following command:

no ipv6 nd-inspection trust

Denying RA Packets

To prevent interfaces from sending RA packets arbitrarily, you can specify to deny RA packets on some specific interfaces (physical interfaces only). Such a measure can prevent against RA attacks and improve LAN security effectively. To deny RA packets on an interface, in the interface configuration mode, use the following command:

ipv6 nd-inspection deny-ra

To cancel the above restriction, in the interface configuration mode, use the following command:

no ipv6 nd-inspection deny-ra

Configuring an NDP Packet Rate Limit

To configure an NDP packet rate limit, in the interface (physical interface only) configuration mode, use the following command:

ipv6 nd-inspection rate-limit *number*

- *number* – Specifies the number of NDP packets that are allowed per second. If the number of NDP packets received per second exceeds the value, the system will drop excessive NDP packets. The value range is 0 to 10000. The default value is 0, i.e., no rate limit.

To cancel the specified rate limit, in the interface configuration mode, use the following command:

no ipv6 nd-inspection rate-limit

Viewing NDP Inspection Configuration

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

show ipv6 nd-inspection configuration

Configuring NDP Spoofing Defense

NDP spoofing defense is designed to protect Intranet from NDP spoofing attacks. To configure NDP spoofing defense, in the security zone configuration mode, use the following command:

ad ipv6 nd-spoofing {**reverse-query** | **ip-number-per-mac** *number* [**action** [**drop** | **alarm**]] | **unsolicited-na-send-rate** *number*}

- **reverse-query** – Enables reverse query. When the system receives an NDP request, it will log the IP address and reply with another NDP request; and then the system will check if any packet with a different MAC address will be returned, or if the MAC address of the returned packet is the same as that of the NDP request packet. To disable the function, use the command **no ad ipv6 nd-spoofing reverse-query**.

- **ip-number-per-mac** *number* – Specifies whether to check the IP number per MAC in NDP table. If the parameter is set to 0 (the default value), the system will not check the IP number; if set to a value other than 0, the system will check the IP number, and if the IP number per MAC is larger than the parameter value, the system will take the action specified by action [**drop** | **alarm**]. The available actions include **drop** (give an alarm and drop the ARP packets) and **alarm** (give an alarm but still allow the packets to pass through). The value range is 0 to 1024. To restore to the default value, use the command **no ad ipv6 nd-spoofing ip-number-per-mac**.

- **unsolicited-na-send-rate** *number* – Specifies whether to send gratuitous NA packet(s). If the parameter is set to 0 (the default value), the system will not send any gratuitous NA packet; if set to a value other than 0, the system will send gratuitous NA packet(s), and the number sent per second is the specified parameter value. The value range is 0 to 10. To restore to the default value, use the command **no ad ipv6 nd-spoofing unsolicited-na-send-rate**.

Viewing NDP Spoofing Statistics

After configuring NDP spoofing defense, to view attack statistics, use the following command:

show ipv6 nd-spoofing-statistics

NDP Spoofing Prevention

With NDP learning, NDP inspection and NDP spoofing defense configured, FSOS is able to prevent against NDP attacks efficiently. Besides, the system also supports statistics on NDP spoofing attacks. To view NDP spoofing attack statistics, in any mode, use the following command:

show ipv6 nd-spoofing-statistics [*number*]

- *number* – Shows statistics of the top number records.

To clear NDP spoofing attack statistics, in any mode, use the following command:

clear ipv6 nd-spoofing-statistics

Attack Defense

The system supports IPv6 attack defense functions listed in Table below. For more details and configuration, see "Attack Defense" of "Threat Prevention".

Attack defense	Configuration (in the security zone configuration mode)
Huge ICMP packet defense	**ad huge-icmp-pak** [**threshold** *number* | **action** {**alarm** | **drop**}]
IP sweeping	**ad ip-sweep** [**threshold** *value*| **action** {**alarm** | **drop**}]

Attack defense	Configuration (in the security zone configuration mode)
defense	
L3 IP spoofing defense	**ad ip-spoofing**
ICMP Flood defense	**ad icmp-flood** [**threshold** *number* | **action** {**alarm** | **drop**}]
UDP Flood defense	**ad udp-flood** [**threshold** *number* | **action** {**alarm** | **drop**}]
SYN Flood defense	**ad syn-flood** [**source-threshold** *number* | **destination-threshold** *number* | **action** {**alarm** | **drop**} | **destination** [**ip-based** | **port-based** [**address-book** *address-book-name* | *ip-address/netmask*]]]
SYN-Proxy SYN-Cookie	**ad syn-proxy** [**min-proxy-rate** *number* | **max-proxy-rate** *number* | **proxy-timeout** *number* | **cookie**]
Teardrop defense	**ad tear-drop**
IP fragment defense	**ad ip-fragment** [**action** {**alarm** | **drop**}]
Ping of Death defense	**ad ping-of-death**
Port scan defense	**ad port-scan** [**threshold** *value* | **action** {**alarm** | **drop**}]
TCP anomaly defense	**ad tcp-anomaly** [**action** {**alarm** | **drop**}]
Land attack defense	**ad land-attack** [**action** {**alarm** | **drop**}]

Configuring an IPv6 6to4 Tunnel

At the time of writing IPv4 networks are still mainstream networks, while IPv6 networks are comparatively isolated. Tunnel technique is designed for the communication between isolated IPv6 networks via IPv4 networks. FSOS supports processing of IPv6 packets, and inter-communication between IPv4 and IPv6 via tunnel technique. The current version supports manual and automatic 6to4 tunnel.

- Manual 6to4 tunnel: Provides one-to-one connection. The end point of the tunnel is manually configured.

- Automatic 6to4 tunnel: An automatic one-to-many tunnel that is used to connect multiple isolated IPv6 networks via IPv4 networks. FS devices can either be used as 6to4 routes or 6to4 relay routers, specifically relying on network environment.

The configuration of 6to4 tunnel includes:

- Creating a tunnel
- Specifying an egress interface
- Specifying a destination address for the manual tunnel
- Specifying IPv6 6to4 Subtunnel Limit
- Binding a tunnel to the tunnel interface

Creating a Tunnel

To create an IPv6 6to4 tunnel, in the global configuration mode, use the following command:

tunnel ip6in4 *tunnel-name* {**manual** | **6to4**}

- *tunnel-name* – Specifies the name of IPv6 6to4 tunnel.
- **manual** | **6to4** – Specifies a tunnel type which can be a manual 6to4 tunnel (**manual**) or automatic 6to4 tunnel (**6to4**).

After executing the above command, the system will create an IPv6 6to4 tunnel with the specified name and enter the tunnel configuration mode; if the specified name already exists, the system will directly enter the tunnel configuration mode.

To delete the specified IPv6 6to4 tunnel, in the global configuration mode, use the following command:

no tunnel ip6in4 *tunnel-name* {**manual** | **6to4**}

Specifying an Egress Interface

To specify an egress interface for the tunnel, in the tunnel configuration mode, use the following command:

interface *interface-name*

- *interface-name* – Specifies the name of egress interface which can be a physical interface or logical interface (except for tunnel interface).

To cancel the specified egress interface, in the tunnel configuration mode, use the following command:

no interface

Specifying a Destination Address for the Manual Tunnel

The destination address of automatic 6to4 tunnel can be obtained automatically by the IPv4 address embedded in the compatible IPv6 address. Therefore, you need not to specify the destination for the automatic 6to4 tunnel. To specify a destination address for the manual IPv6 6to4 tunnel, in the tunnel configuration mode, use the following command:

destination *ipv4-address*

- *ipv4-address* − Specifies a destination address (must be an IPv4 address) for the manual tunnel.

To cancel the specified destination address, in the tunnel configuration mode, use the following command:

no destination

Specifying IPv6 6to4 Subtunnel Limit

The maximum number of 6to4 tunnels in a system is 10, and one interface can have only one 6to4 tunnel. Each tunnel can have a maximum of 1200 sub-tunnels. To specify the subtunnel number of a 6to4 tunnel, under tunnel configuration mode, use the following command:

subtunnel-limit *maximum*

- *maximum* − Specify the subtunnel number of a 6to4 tunnel. The rang is 1 to 1200, and the default value is 200.

Under tunnel configuration mode, use the command to resume the default value:

no subtunnel-limit

Binding a Tunnel to the Tunnel Interface

To bind an IPv6 6to4 tunnel to the tunnel interface, in the tunnel configuration mode (to enter the tunnel configuration mode, in the global configuration mode, use the command **interface tunnel***X*), use the following command:

tunnel ip6in4 *ipv6-tunnel-name*

- *ipv6-tunnel-name* − Specifies the name of IPv6 6to4 tunnel.

To cancel the binding between the IPv6 6to4 tunnel and tunnel interface, in the tunnel configuration mode, use the following command:

no tunnel ip6in4 *ipv6-tunnel-name*

Viewing IPv6 6to4 Tunnel Configuration

To view IPv6 6to4 tunnel configuration, in any mode, use the following command:

show ip6in4 {**manual-tunnel** | **6to4-tunnel**}

Configuring an IPv6 4to6 Tunnel

At the time of writing IPv4 networks are still mainstream networks, while the application of IPv6 networks keeps growing. To solve the problems caused by wide deployment of IPv6 networks, FSOS supports IPv6 4to6 tunnel technique to enable communication between isolated IPv4 networks via IPv6 networks.

The current version only supports manual 4to6 tunnel. Manual 4to6 tunnel enables one-to-one connection. Its end point is manually configured.

The configuration of manual 4to6 tunnel includes:

- Creating a tunnel
- Specifying a source address/interface for the tunnel
- Specifying a destination address for the tunnel
- Binding a tunnel to the tunnel interface

Creating a Tunnel

To create an IPv6 4to6 tunnel, in the global configuration mode, use the following command

tunnel ip4in6 *tunnel-name* **manual**

- *tunnel-name* – Specifies the name of IPv6 4to6 tunnel.

After executing the above command, the system will create an IPv6 4to6 tunnel with the specified name and enter the tunnel configuration mode; if the specified name already exists, the system will directly enter the tunnel configuration mode.

To delete the specified IPv6 4to6 tunnel, in the global configuration mode, use the following command:

no tunnel ip4in6 *tunnel-name* **manual**

Specifying the Source Address/Interface

To specify the egress interface and source address of IPv6 4to6 tunnels, under tunnel configuration mode, use the following command:

interface *interface-name* **source** *ipv6-address*

- *interface-name* − Specify the egress interface for the tunnel.
- *ipv6-address* − Specfiy source address of IPv6 4to6 tunnel. This address should be an IPv6 address.

Under tunnel configuration mode, use the command to delete egress interface and source address:

no interface

Specifying a Destination Address for the Tunnel

To specify a destination address for the IPv6 4to6 tunnel, in the tunnel configuration mode, use the following command:

destination *ipv6-address*

- *ipv6-address* − Specifies a destination address (must be an IPv6 address) for the IPv6 4to6 tunnel.

To cancel the specified destination address, in the tunnel configuration mode, use the following command:

no destination

Binding a Tunnel to the Tunnel Interface

To bind an IPv6 4to6 tunnel to the tunnel interface, in the tunnel configuration mode (to enter the tunnel configuration mode, in the global configuration mode, use the command **interface tunnel***X*), use the following command:

tunnel ip4in6 *tunnel-name*

- *tunnel-name* − Specifies the name of IPv6 4to6 tunnel.

To cancel the binding between the IPv6 4to6 tunnel and tunnel interface, in the tunnel configuration mode, use the following command:

no tunnel ip4in6 *tunnel-name*

Viewing IPv6 4to6 Tunnel Configuration

To view IPv6 4to6 tunnel configuration, in any mode, use the following command:

show ip4in6 manual-tunnel

Configuring DS-lite

FSOS supports DS-lite technology. DS-lite integrates with IPv4-in-IPv6 tunnel with NAT. The IPv4 client uses the B4 (Base Bridge Broadband) device and the AFTP (Address Family Transition Router) device to create a tunnel in the IPv6 network. And then it uses this tunnel to communicate with the resource in the IPv4 network. In the end of this tunnel, the AFTR device uses NAT to translate the private IPv4 address.

FS device can act as the AFTR device to support DS-lite and NAT. Configuring DS-lite includes the following sections:

- Create a DS-lite tunnel
- Specify an interface and IP address for the DS-lite tunnel
- Specify the maximum number of the sub tunnels

When using DS-lite, you must also configure the corresponding NAT settings.

Creating a DS-lite Tunnel

Each device can have at most 10 DS-lite tunnels. To create a DS-lite tunnel, use the following command in the global configuration mode. After executing this command, FSOS creates the DS-lite tunnel and enters the DS-lite tunnel configuration mode. If the name already exists, FSOS will enter the DS-lite tunnel configuration mode directly.

tunnel ip4in6 *tunnel-name* **ds-lite**

- *tunnel-name* – Enter the name of the DS-lite tunnel.

To delete a tunnel, use the following command in the global configuration mode:

no tunnel ip4in6 *tunnel-name* **ds-lite**

Specifying an Interface and IP Address for the DS-lite Tunnel

To specify an interface and IP address for the DS-lite tunnel, use the following command in the DS-lite tunnel configuration mode:

interface *interface-name* **src-ip** *X:X:X:X::X*

- *interface-name* - Specify the egress interface for the DS-lite.
- *X:X:X:X::X* – Specify the IPv6 address owned by this egress interface.

To cancel the above settings, use the **no interface** command in the DS-lite tunnel configuration mode.

Specifying the Maximum Number of Sub Tunnels

When a B4 device accesses the DS-lite tunnel, AFTR will dynamically create a sub tunnel. To specify the maximum number of sub tunnels, use the following command in the DS-lite tunnel configuration mode:

subtunnel-limit *value*

- *value* – Specify the maximum number of sub tunnels that AFTR can create. The default value is 200. The value ranges from 1 to 1200.

Use the **no** form to restore the value to the default one.

Viewing DS-lite Tunnel Information

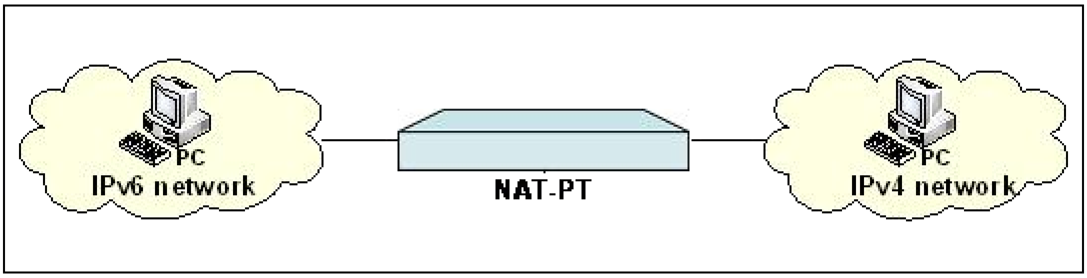
To view the configuration information of the DS-lite tunnel, use the following command in any mode:

show ip4in6 ds-lite-tunnel

Configuring NAT-PT

IPv6 can solve the problem of increasingly exhausted IP addresses, and will replace IPv4 to become the core of next generation Internet. However, it' s not possible to upgrade the existing IPv4 networks to IPv6 networks overnight; for quite a long time, IPv6 and IPv4 networks will co-exist and communicate with each other.

NAT-PT (Network Address Translation - Protocol Translation) is a transitional mechanism that is designed for the inter-communication between pure IPv6 and IPv4 networks. NAT-PT adopts NAT for the translation between IPv4 and IPv6 addresses, and adopts PT for the translation of protocols (including network layer protocols, transport layer protocols and application layer protocols) on the basis of semantically equivalent rules. Powered by NAT-PT, you can implement the inter-communication between IPv6 and IPv4 networks without any change to the existing IPv4 networks. Figure below shows an illustration of intercommunication between a pure IPv6 and IPv4 network via a FS device with NAT-PT enabled.



Note:NAT-PT on the current firmware version supports translation of IP, TCP, UDP and ICMP protocols, and supports FTP-ALG, TFTP-ALG and HTTP-ALG controls.

Configuring a NAT-PT Rule

NAT-PT rules are created based on VRouters. You can create, move and delete SNAT/DNAT rules in the VRouter configuration mode.

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

ip vrouter *vrouter-name*

- *vrouter-name* – Specifies the name of VRouter.

Creating an SNAT Rule

SNAT rules are used to specify whether to implement NAT-PT on the source IPv6/IPv4 address of the matched traffic. If NAT-PT is implemented, you also need to specify the translated IP address and translation mode. To configure an SNAT rule for NAT-PT, in the VRouter configuration mode, use the following command:

snatrule [**id** *id*] [**before** i*d* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] **trans-to** {**addressbook** *trans-to-address* | **eif-ip**} **mode** {**static** | **dynamicip** | **dynamicport** [**sticky**]} [**log**] [**group** *group-id*][**description** *description*]

- **id** *id* – Specifies the ID of the SNAT rule. Each SNAT rule has a unique ID. If the ID is not specified, the system will automatically assign one. If the specified SNAT ID exists, the original rule will be overwritten.
- **before** *id* | **after** *id* | **top** – Specifies the position of the rule. The position can be **before** *id*, **after** *id*, **top**. If the position is not specified, the rule would be located at the end of all the SNAT rules. By default, the newly-created SNAT rule is located at the end of all the rules.
- **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] – Specifies conditions of the rule that the traffic should be matched. The conditions include:
  - **from** *src-address* - Specifies the source IP address of the traffic. *src-address* should be an IPv4 address, IPv6 address or an address entry in the address book.
  - **to** *dst-address* - Specifies the destination IP address of the traffic. *dst-address* should be an IPv4 address, IPv6 address or an address entry in the address book.
  - **eif** *egress-interface* | **evr** *vrouter-name* - Specifies the egress interface (**eif** *egress-interface*) or the next-hop VRouter (**evr** *vrouter-name*) of the traffic.
- **addressbook** *trans-to-address* | **eif-ip** – Specifies the translated IP address. It can be an IPv4 or IPv6 address, an address entry in the address book, or the IP address of the egress interface (**eif-ip**).When you configure the NAT46, system does not support to specifies the **eif-ip**.

- **mode** {**static** | **dynamicip** | **dynamicport** [**sticky**]} − Specifies the translation mode. FSOS supports three modes for the translation between IPv4 and IPv6 addresses: static, dynamicip and dynamicport. For more details, see the table below:
  - **static** - Static mode means one-to-one translation. This mode requires the translated address entry (*trans-to-address*) contains the same number of IP addresses as that of the source address entry (*src-address*).
  - **dynamicip** - Dynamic IP mode means many-to-many translation. This mode translates the source address to a specific IP address. Each source address will be mapped to a unique IP address, until all specified addresses are occupied.
  - **dynamicport** - Namely NAPT-PT (Network Address Port Translation - Protocol Translation). Multiple source addresses will be translated to one specified IP address in an address entry. If Sticky is not enabled, the system will select an IP address in the address entry, when port resources of the first address are exhausted, the second address will be used. If Sticky is enabled, all sessions from an IP address will be mapped to the same fixed IP address.
- **log** − Enables the log function for this SNAT rule (Generating a log when the traffic is matched to this NAT rule).
- **group** *group-id* - Specifies the HA group the SNAT rule belongs to. If the parameter is not specified, the SNAT rule being created will belong to HA group0.

For example, the following example achieves the interface-based NAT of ethernet0/0 in the untrust zone:

```
hostname(config-vrouter)# snatrule from ipv6-any to ipv6-any eif ethernet0/0 trans-
to eif-ip mode dynamicport
rule id=1
```

To configure an SNAT rule that disables NAT-PT, in the VRouter configuration mode, use the following command:

snatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] **no-trans** [**group** *group-id*]

Moving an SNAT Rule

Each SNAT rule is labeled with a unique ID. When traffic flows into the FS device, the device will query for SNAT rules in the list by turns, and then implement NAT-PT on the source IP of the traffic according to the first matched rule. However, the rule ID is not related to the matching sequence during the query. The sequence displayed by the command show snat is the query sequence for the matching.

You can move an SNAT rule to modify the matching sequence. To move an SNAT rule, in the VRouter configuration mode, use the following command:

snatrule move *id* {**before** *id* | **after** *id*| **top** | **bottom**}

- *id* – Specifies the ID of the SNAT rule that will be moved.
- **before** *id* – Moves the SNAT rule before the specified ID.
- **after** *id* – Moves the SNAT rule after the specified ID.
- **top** – Moves the SNAT rule to the top of the SNAT rule list.
- **bottom** – Moves the SNAT rule to the bottom of the SNAT rule list.

Deleting an SNAT Rule

To delete the SNAT rule with the specified ID, in the VRouter configuration mode, use the following command:

no snatrule id *id*

Viewing SNAT Configuration Information

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

show snat [**id** *id*] [**vrouter** *vrouter-name*]

- **id** *id* – Shows the SNAT rule information of the specified ID.
- **vrouter** *vrouter-name* – Shows the SNAT configuration information of the specified VRouter.

When the SNAT translation mode is set to dynamicport, to view the usage of port resources in the source address pool, in any mode, use the following command:

show snat resource [**vrouter** *vrouter-name*]

- **vrouter** *vrouter-name* – Shows the port usage of SNAT source address pool of the specified VRouter.

Creating a DNAT Rule

DNAT rules are used to specify whether to implement NAT-PT on the destination IPv6/IPv4 address of the matched traffic. To configure a DNAT rule for NAT-PT, in the VRouter configuration mode, use the following command:

dnatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] **trans-to** *trans-to-address* [**port** *port*] [**load-balance**] [**track-tcp** *port*] [**track-ping**] [**log**] [**group** *group-id*] [**description** *description*]

- id id − Specifies the ID of the DNAT rule. Each DNAT rule has a unique ID. If the ID is not specified, the system will automatically assign one. If the specified DNAT ID exists, the original rule will be overwritten.
- **before** *id* | **after** *id* | **top** − Specifies the position of the rule. The position can be **top**, **before** *id* or **after** *id*. If the position is not specified, the rule would be located at the end of all the DNAT rules. By default, the newly-created DNAT rule is located at the end of all the rules. When traffic flows into the FS device, the device will query for DNAT rules in the list by turns, and then implement NAT on the destination IP of the traffic according to the first matched rule.
- **from** *src-address* **to** *dst-address* [**service** *service-name*] − Specifies conditions of the rule that the traffic should be matched. The conditions are:
  - **from** *src-address* − Specifies the source IP address of the traffic. *src-address* should be an IPv4 or IPv6 address, or an address entry in the address book.
  - **to** *dst-address* − Specifies the destination IP address of the traffic. *dst-address* should be an IPv4 or IPv6 address, or an address entry in the address book.
  - **service** *service-name* − Specifies the service type of the traffic. If the port number needs to be translated together (specified by **port** *port*), the specified service can only be configured with one protocol and one port. For example, the TCP port number can be 80, but cannot be 80 to 100.
- **trans-to** *trans-to-address* − Specifies the translated IP address. *trans-to-address* should be an IPv4 or IPv6 address, or an address entry in the address book. The number of this translated IP address must be the same as that of the destination IP address of the traffic (specified by **to** *dst-address*).
- **port** *port* − Specifies port number of the internal network server.
- **load-balance** − Enables load balancing for this DNAT rule, i.e., balances the traffic to different servers in the internal network.
- **track-tcp** *port* − If this parameter is configured and the port number of the internal network server is specified, the system will send TCP packets to the internal network server to monitor if the specified TCP port is reachable.
- **track-ping** − If this parameter is configured, the system will send ping packets to the internal network server to monitor if the server is reachable.

- **log** – Enables the log function for this DNAT rule (Generating a log when the traffic is matched to this DNAT rule).
- **group** *group-id* - Specifies the HA group that the DNAT rule belongs to. If the parameter is not specified, the DNAT rule being created will belong to HA group0.

For example, the following command will translate the IP address of the request from addr1 to the IP address of addr2, but will not translate the port number:

```
hostname(config-vrouter)# dnatrule from ipv6-any to addr1 service any trans-to addr2
rule id=1
```

To configure a DNAT rule that disables NAT-PT, in the VRouter configuration mode, use the following command:

dnatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] **no-trans** [**group** *group-id*]

Moving a DNAT Rule

Each DNAT rule is labeled with a unique ID. When traffic flowing into the FS device, the device will query for DNAT rules by turns, and then implement NAT on the source IP of the traffic according to the first matched rule. However, the rule ID is not related to the matching sequence during the query. The sequence displayed by the command show dnat is the query sequence for the matching. You can move a DNAT rule to modify the matching sequence. To move a DNAT rule, in the VRouter configuration mode, use the following command:

dnatrule move *id* {**before** *id* | **after** *id*| **top** | **bottom**}

- *id* – Specifies the ID of the DNAT rule that will be moved.
- **before** *id* – Moves the DNAT rule before the specified ID.
- **after** *id* – Moves the DNAT rule after the specified ID.
- **top** – Moves the DNAT rule to the top of the DNAT rule list.
- **bottom** – Moves the DNAT rule to the bottom of the DNAT rule list.

Deleting a DNAT Rule

To delete the DNAT rule with the specified ID, in the VRouter configuration mode, use the following command:

no dnatrule id *id*

Viewing DNAT Configuration Information

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

show dnat [**id** *id*] [**vrouter** *vrouter-name*]

- **id** *id* – Shows the DNAT rule information of the specified ID.
- **vrouter** *vrouter-name* – Shows the DNAT configuration information of the specified VRouter.

To show the information of the DNAT rule with load balancing configured, in any mode, use the following command:

show dnat server [*ip-address*] [**vrouter** *vrouter-name*] [**tcp-port** *port*] [**ping**]

- *ip-address* – Shows status of the internal network server of the specified IP address.
- **vrouter** *vrouter-name* – Shows status of the internal network server of the specified VRouter.
- **tcp-port** *port* – Shows status of the internal network server of the specified port number.
- **ping** – Shows ping monitor status of the internal network server.

Configuring DNS64 and NAT64

DNS64 and NAT64 are transitional mechanisms for the intercommunication between IPv6-only and IPv4-only networks. These mechanisms are designed to support IPv6 clients’ request for network resources on IPv4 servers, and addresses most of the deficiencies of NAT-PT in the intercommunication between IPv6 and IPv4 networks.

If an IPv6 client does not receive any response from an IPv6 DNS server after sending a DNS request, it will use DNS64 to re-send the DNS request to an IPv4 DNS server; if any response is replied from the server, DNS64 will convert IPv4 response packets to IPv6 response packets and returned to the client.

NAT64 is mainly used for the address translation from IPv6 to IPv4 addresses. During source address translation, NAT64 translates source IPv6 addresses to source IPv4 addresses via the IPv4 address pool; during destination address translation, NAT64 directly extracts destination IPv4 addresses from the IPv6 addresses returned by DNS64.

DNS64 and NAT64 on FS devices are implemented by DNS64 and NAT64 rules respectively. NAT64 rules include SNAT and DNAT rules. The configuration of SNAT rules is the same as that of SNAT rules in NAT-PT. For more information, see "Creating an SNAT Rule" of "Firewall".

Creating a DNS64 Rule

Only be available on some firmwares. To create a DNS64 rule, in the global configuration mode, use the following command:

ipv6 dns64-proxy id *id* **prefix** *ipv6-address/Mask* [**source** {*ipv6-address/Mask* | *address-entry-v6*} | **trans-mapped-ip** {*ipv4-address/Mask* / *address-entry-v4*}]

- **id** *id* – Specifies the ID of the DNS64 rule. The value range is 1 to 16. Each DNS64 rule has a unique ID. If the specified DNS64 ID exists, the original rule will be overwritten.
- **prefix** *ipv6-address/Mask* – Specifies the IPv6 prefix and length of the prefix. DNS64 uses the prefix to translate IPv4 addresses to IPv6 addresses. The value range of prefix length is 0 to 96.
- **source** {*ipv6-address/Mask* / *address-entry-v6*} – Specifies the source IP address of traffic which can be an IPv6 address or an IPv6 address entry in the address book.
- **trans-mapped-ip** {*ipv4-address/Mask* / *address-entry-v4*} – Specifies the response address of IPv4 DNS server which can be an IPv4 address or an IPv4 address entry in the address book.

To delete the specified DNS64 rule, in the global configuration mode, use the following command:

no ipv6 dns64-proxy id *id*

Creating a DNAT Rule

To create a DNAT rule, in the VRouter configuration mode, use the following command:

dnatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] **v4-mapped** [**log**] [**group** *group-id*]

- **id** *id* – Specifies the ID of the DNAT rule. Each DNAT rule has a unique ID. If the ID is not specified, the system will automatically assign one. If the specified DNAT ID exists, the original rule will be overwritten.
- **before** *id* | **after** *id* | **top** – Specifies the position of the rule. The position can be **top**, **before** *id* or **after** *id*. If the position is not specified, the rule would be located at the end of all the DNAT rules. By default, the newly-created DNAT rule is located at the end of all the rules.

When traffic flows into the FS device, the device will query for DNAT rules in the list by turns, and then implement NAT on the destination IP of the traffic according to the first matched rule.

- **from** *src-address* **to** *dst-address* [**service** *service-name*] – Specifies conditions of the rule that the traffic should be matched. The conditions are:
  - **from** *src-address* – Specifies the source IP address of the traffic. src-address should be an IPv6 address, or an IPv6 address entry in the address book.
  - **to** *dst-address* – Specifies the destination IP address of the traffic. src-address should be an IPv6 address, or an IPv6 address entry in the address book.
  - *service-name* – Specifies the service type of the traffic. The specified service can only be configured with one protocol and one port. For example, the TCP port number can be 80, but cannot be 80 to 100.
- **v4-mapped** – Extracts the destination IPv4 address from the destination IPv6 address of the packet directly.
- **log** – Enables the log function for this DNAT rule (Generating a log when the traffic is matched to this DNAT rule).
- **group** *group-id* - Specifies the HA group that the DNAT rule belongs to. If the parameter is not specified, the DNAT rule being created will belong to HA group0.

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

no dnatrule id *id*

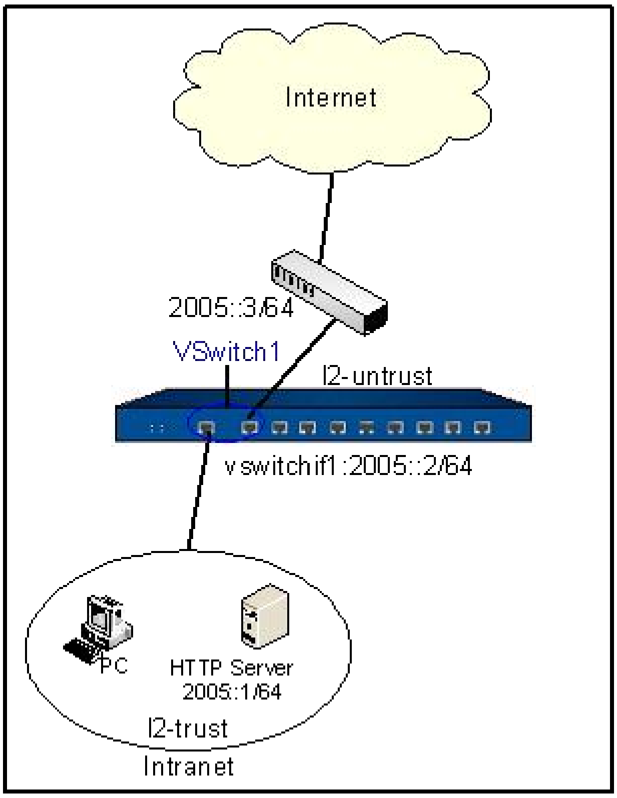
IPv6 Configuration Examples

This section describes several configuration examples of IPv6, including:

- Example 1: IPv6 transparent mode configuration
- Example 2: IPv6 routing mode configuration
- Example 3: Manual IPv6 tunnel configuration
- Example 4: IPv6 6to4 tunnel configuration
- Example 5: IPv6 SNMP configuration example
- Example 6: IPv6 NAT-PT configuration example

Example 1: IPv6 Transparent Mode Configuration

FS device is deployed in the transparent mode. Ethernet0/0 belongs to the l2-trust zone, and is connected to the Intranet; ethernet0/1 belongs to the l2-untrust zone; both l2-trust and l2-untrust belong to VSwitch1. The goal is to allow the hosts in the Intranet to visit Internet, and allow hosts in the Internet to visit the HTTP server in the Intranet. The network topology is shown below.



Take the following steps:

Step 1: Configure interfaces:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone l2-trust
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone l2-untrust
hostname(config-i f-eth0/1)# exit
hostname(config)# interface vswitchif1
 hostname(config-if-vsw1)# zone trust
hostname(config-if-vsw1)# ipv6 enable
```

```
 hostname(config-if-vsw1)# ipv6 address 2005::2/64
hostname(config-if-vsw1)# exit
hostname(config)#
```

Step 2: Configure an address entry:

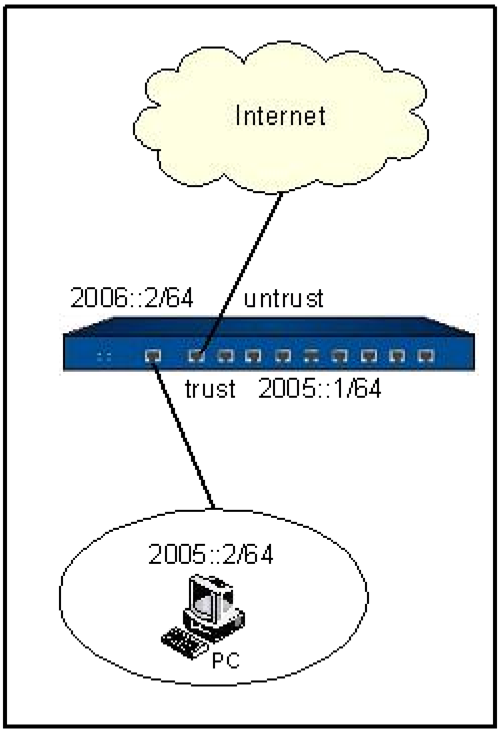
```
hostname(config)# address http-server ipv6
hostname(config-addr)# ip 2005::1/64
hostname(config-addr)# exit
hostname(config)#
```

Step 3: Configure policy rules:

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone l2-trust
hostname(config-policy-rule)# dst-zone l2-untrust
hostname(config-policy-rule)# src-addr ipv6-any
hostname(config-policy-rule)# dst-addr ipv6-any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone l2-untrust
hostname(config-policy-rule)# dst-zone l2-trust
hostname(config-policy-rule)# src-addr ipv6-any
hostname(config-policy-rule)# dst-addr http-server
hostname(config-policy-rule)# service http
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Example 2: IPv6 Routing Mode Configuration

FS device is deployed in the routing mode. Ethernet0/0 belongs to the trust zone, and is connected to the Intranet; ethernet0/1 belongs to the untrust zone, and is connected to the Internet. The public address provided by the ISP is 2006::1/64. The goal is to allow the PC in the Intranet to visit Internet. The network topology is shown below.



Take the following steps:

Step 1: Configure interfaces:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ipv6 enable
hostname(config-if-eth0/0)# ipv6 address 2005::1/64
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ipv6 enable
hostname(config-if-eth0/1)# ipv6 address 2006::2/64

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

hostname(config)#
```

Step 2: Configure a default router:

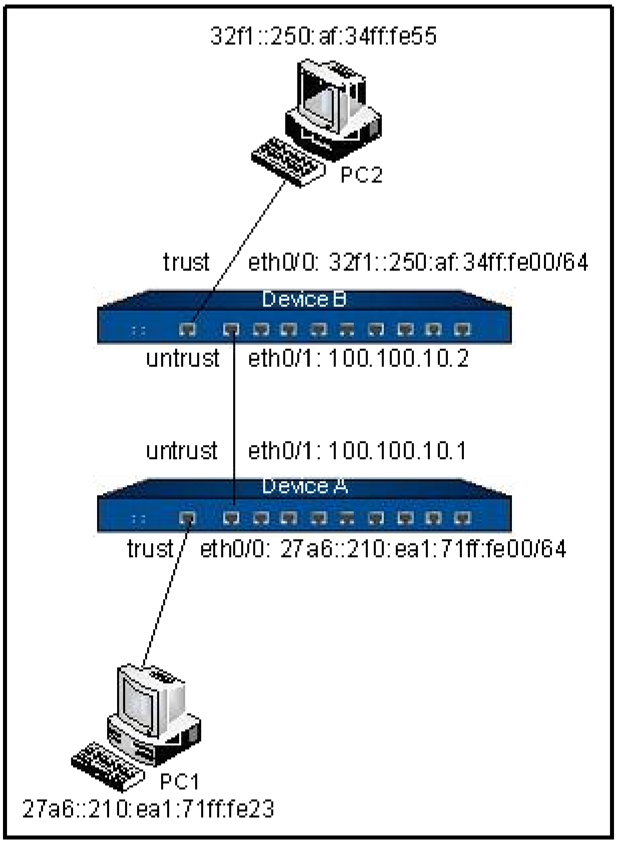
```
hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# ipv6 route ::/0 2006::1

hostname(config-vrouter)# exit

hostname(config)#
```

Step 3: Configure a policy rule:

```
hostname(config)# policy-global

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone trust

hostname(config-policy-rule)# dst-zone untrust

hostname(config-policy-rule)# src-addr 2005::2/64

hostname(config-policy-rule)# dst-addr ipv6-any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config)#
```

Example 3: Manual IPv6 Tunnel Configuration

PC1 and PC2 use IPv6 addresses and belong to different subnets. The goal is to allow the intercommunication between PC1 and PC2 via a manual IPv6 tunnel. The network topology is shown below.



Take the following steps:

Step 1: Configure interfaces:

```
Device A
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ipv6 enable
hostname(config-if-eth0/0)# ipv6 address 27a6::210:ea1:71ff:fe00/64
 hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 100.100.10.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

```
Device B
```

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ipv6 enable
hostname(config-if-eth0/0)# ipv6 address 32f1::250:af:34ff:fe00/64
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 100.100.10.2/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 2: Configure tunnels:

```
Device A
hostname(config)# tunnel ip6in4 test-tunnelA manual
hostname(config-ip6in4-manual)# interface ethernet0/1
hostname(config-ip6in4-manual)# destination 100.100.10.2
hostname(config-ip6in4-manual)# exit
hostname(config)#
```

```
Device B
hostname(config)# tunnel ip6in4 test-tunnelB manual
hostname(config-ip6in4-manual)# interface ethernet0/1
hostname(config-ip6in4-manual)# destination 100.100.10.1
hostname(config-ip6in4-manual)# exit
hostname(config)#
```

Step 3: Bind the manual IPv6 tunnel to tunnel interfaces:

```
Device A
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ipv6 enable
hostname(config-if-tun1)# tunnel ip6in4 test-tunnelA
hostname(config-if-tun1)# exit
hostname(config)#
```

Device B

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ipv6 enable
hostname(config-if-tun1)# tunnel ip6in4 test-tunnelB
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 4: Configure policy rules:

Device A

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr ipv6-any
hostname(config-policy-rule)# dst-addr ipv6-any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Device B

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr ipv6-any
 hostname(config-policy-rule)# dst-addr ipv6-any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

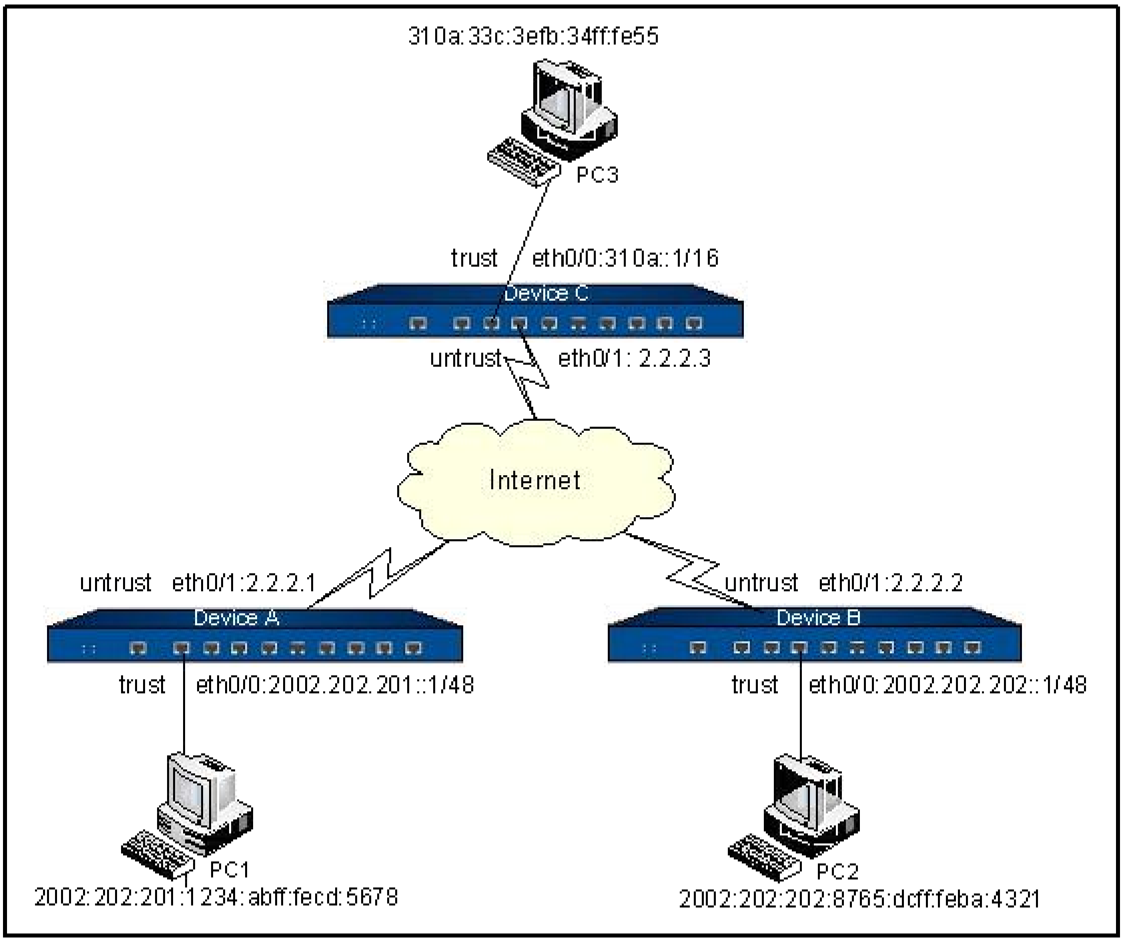
Step 5: Configure routes:

```
Device A
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ipv6 route 32f1::/64 tunnel1
hostname(config-vrouter)# exit
hostname(config)#
```

```
Device B
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ipv6 route 27a6::/64 tunnel1
hostname(config-vrouter)# exit
hostname(config)#
```

Example 4: IPv6 6to4 Tunnel Configuration

PC1, PC2 and PC3 are IPv6 hosts, among which PC1 and PC2 use 6to4 addresses, while PC3 uses a general IPv6 address. The goal is to configure 6to4 tunnels on Device A, Device B and Device C for the intercommunication among PC1, PC2 and PC3. The network topology is shown below.



Take the following steps:

Step 1: Configure interfaces:

Device A

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ipv6 enable
hostname(config-if-eth0/0)# ipv6 address 2002:202:201::1/48
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 2.2.2.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

```
Device B
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ipv6 enable
hostname(config-if-eth0/0)# ipv6 address 2002:202:202::1/48
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 2.2.2.2/24
hostname(config-if-eth0/1)# exit
hostname(config)#
Device C
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ipv6 enable
hostname(config-if-eth0/0)# ipv6 address 310a::1/16
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 2.2.2.3/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 2: Configure tunnels:

```
Device A
hostname(config)# tunnel ip6in4 test-tunnelA 6to4
hostname(config-ip6in4-6to4)# interface ethernet0/1
hostname(config-ip6in4-6to4)# exit
hostname(config)#
```

```
Device B
hostname(config)# tunnel ip6in4 test-tunnelB 6to4
hostname(config-ip6in4-6to4)# interface ethernet0/1
hostname(config-ip6in4-6to4)# exit
hostname(config)#
Device C
hostname(config)# tunnel ip6in4 test-tunnelC 6to4
hostname(config-ip6in4-6to4)# interface ethernet0/1
hostname(config-ip6in4-6to4)# exit
hostname(config)#
```

Step 3: Bind the 6to4 tunnels to tunnel interfaces:

```
Device A
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ipv6 enable
hostname(config-if-tun1)# tunnel ip6in4 test-tunnelA
hostname(config-if-tun1)# exit
hostname(config)#
Device B
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ipv6 enable
hostname(config-if-tun1)# tunnel ip6in4 test-tunnelB
hostname(config-if-tun1)# exit
hostname(config)#
Device C
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ipv6 enable

hostname(config-if-tun1)# tunnel ip6in4 test-tunnelC

hostname(config-if-tun1)# exit

hostname(config)#
```

Step 4: Configure a policy rule (on all the three devices):

```
Device A, Device B, Device C

hostname(config)# policy-global

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone trust

hostname(config-policy-rule)# dst-zone untrust

hostname(config-policy-rule)# src-addr ipv6-any

hostname(config-policy-rule)# dst-addr ipv6-any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config)#
```

Step 5: Configure routes:

```
Device A

hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# ipv6 route 2002:202:202::/48 tunnel1

hostname(config-vrouter)# ipv6 route 310a::/16 tunnel1 2002:202:203::1

hostname(config-vrouter)# exit

hostname(config)#

Device B

hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# ipv6 route 2002:202:201::/48 tunnel1

hostname(config-vrouter)# ipv6 route 310a::/16 tunnel1 2002:202:203::1
hostname(config-vrouter)# exit
hostname(config)#
Device C
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ipv6 route 2002::/16 tunnel1
hostname(config-vrouter)# exit
hostname(config)#
```

Example 5: IPv6 SNMP Configuration

This section describes the following two IPv6 SNMP configuration examples:

- Viewing IPv6 MIB information via an IPv4 network
- Viewing IPv6 MIB information via an Ipv6 network

Viewing IPv6 MIB Information via an IPv4 Network

The host address is 1.1.12/24; the host is connected to etherenet0/0 that belongs to the untrust zone with address of 1.1.1.1/24. Take the following steps:

Step 1: Configure an interface:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 1.1.1.1/24
hostname(config-if-eth0/0)# manage snmp
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 2: Configure SNMP (only required configuration is listed):

```
hostname(config)# snmp-server manager
hostname(config)# snmp-server host 1.1.1.2 community public ro
```

Finishing the above configuration, you can view IPv6-related MIB information via a MIB browser on the management host.

Viewing IPv6 MIB Information via an Ipv6 Network

The host address is 2008::2/64; the host is connected to etherenet0/0 that belongs to the untrust zone with address of 2008::1/24. Take the following steps:

Step 1: Configure an interface:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ipv6 enable
hostname(config-if-eth0/0)# ipv6 address 2008::1/64
hostname(config-if-eth0/0)# manage snmp
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 2: Configure SNMP (only required configuration is listed):

```
hostname(config)# snmp-server manager
hostname(config)# snmp-server ipv6-host 2008::2 community public ro
```

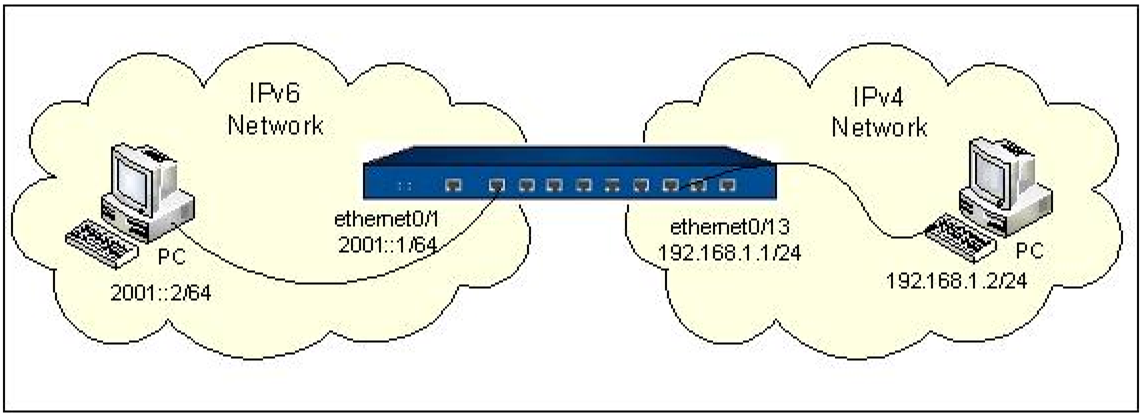
Finishing the above configuration, you can view IPv6-related MIB information via a MIB brower on the management host.

Example 6: IPv6 NAT-PT Configuration

IPv6 and IPv4 networks are connected via a FS device. The goal for NAT-PT configuration is:

- **Requirement 1**: The host in the IPv6 network can initiate access to the host in the IPv4 network, while the host in the IPv4 network cannot initiate access the host in the IPv6 network;
- **Requirement 2**: The host in the IPv4 network can initiate access to the host in the IPv6 network, while the host in the IPv6 network cannot initiate access the host in the IPv4 network.

The network topology is shown below:



Requirement 1

The host in the IPv6 network can initiate access to the host in the IPv4 network, while the host in the IPv4 network cannot initiate access the host in the IPv6 network. Assume the situation below: for the host in the IPv6 network, the mapping IPv6 address of the host in the IPv4 network is 2003::2.

Take the following steps:

Step 1: Configure interfaces:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ipv6 enable
hostname(config-if-eth0/1)# ipv6 address 2001::1/64
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/13
hostname(config-if-eth0/13)# zone trust
hostname(config-if-eth0/13)# ip address 192.168.1.1/24
hostname(config-if-eth0/13)# exit
hostname(config)#
```

Step 2: Configure NAT-PT rules:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule from ipv6-any to 2003::2 service any trans-to eif-ip mode
dynamicport
rule ID=1
```

```
hostname(config-vrouter)# dnatrule from ipv6-any to 2003::2 service any trans-to 192.168.1.2

rule ID=1

hostname(config-vrouter)# exit

hostname(config)#
```

Step 3: Configure a policy rule:

```
hostname(config)# policy-global

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone trust

hostname(config-policy-rule)# dst-zone trust

hostname(config-policy-rule)# src-addr 2001::2/64

hostname(config-policy-rule)# dst-addr 2003::2/128

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config)#
```

Requirement 2

The host in the IPv4 network can initiate access to the host in the IPv6 network, while the host in the IPv6 network cannot initiate access the host in the IPv4 network. Assume the situation below: for the host in the IPv4 network, the mapping IPv4 address of the host in the IPv6 network is 192.168.2.2.

Take the following steps:

Step 1: Configure interfaces:

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

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

hostname(config-if-eth0/1)# ipv6 enable

hostname(config-if-eth0/1)# ipv6 address 2001::1/64

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

hostname(config)# interface ethernet0/13
hostname(config-if-eth0/13)# zone trust
hostname(config-if-eth0/13)# ip address 192.168.1.1/24
hostname(config-if-eth0/13)# exit
hostname(config)#
```

Step 2: Configure NAT-PT rules:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule from any to 192.168.2.2 service any trans-to 2001::2 mode
dynamicport
rule ID=2
hostname(config-vrouter)# dnatrule from any to 192.168.2.2 service any trans-to 2001::2
rule ID=2
hostname(config-vrouter)# exit
hostname(config)#
```

Step 3: Configure a policy rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr 192.168.1.2/24
hostname(config-policy-rule)# dst-addr 192.168.2.2/32
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Appendix 1: ICMPv6 Type and Code

ICMPv6 Type	ICMPv6 Code	Reference

ICMPv6 Type	ICMPv6 Code	Reference
1 Destination Unreachable	0 - no route to destination	[RFC4443]
	1 - communication with destination administratively prohibited	[RFC4443]
	2 - beyond scope of source address	[RFC4443]
	3 - address unreachable	[RFC4443]
	4 - port unreachable	[RFC4443]
	5 - source address failed ingress/egress policy	[RFC4443]
	6 - reject route to destination	[RFC4443]
2 Packet Too Big	0	[RFC4443]
3 Time Exceeded	0 - hop limit exceeded in transit	[RFC4443]
	1 - fragment reassembly time exceeded	[RFC4443]
4 Parameter Problem	0 - erroneous header field encountered	[RFC4443]
	1 - unrecognized Next Header type encountered	[RFC4443]
	2 - unrecognized IPv6 option encountered	[RFC4443]
100 Private experimentation	-	[RFC4443]
101 Private experimentation	-	[RFC4443]
102-126 Unassigned	-	[RFC4443]
127 Reserved for expansion of ICMPv6 error messages	-	[RFC4443]
128 Echo Request	0	[RFC4443]
129 Echo Reply	0	[RFC4443]
130 Multicast Listener Query	0	[RFC2710]
131 Multicast Listener Report	0	[RFC2710]
132 Multicast Listener Done	0	[RFC2710]
133 Router Solicitation	0	[RFC4861]
134 Router Advertisement	0	[RFC4861]
135 Neighbor Solicitation	0	[RFC4861]

ICMPv6 Type	ICMPv6 Code	Reference
136 Neighbor Advertisement	0	[RFC4861]
137 Redirect Message	0	[RFC4861]
138 Router Renumbering	0 - Router Renumbering Command	[Crawford] [RFC2894]
	1 - Router Renumbering Result	[Crawford] [RFC2894]
	255 - Sequence Number Reset	[Crawford] [RFC2894]
139 ICMP Node Information Query	0 - The Data field contains an IPv6 address which is the Subject of this Query	[RFC4620]
	1 - The Data field contains a name which is the Subject of this Query, or is empty, as in the case of a NOOP.	[RFC4620]
	2 - The Data field contains an IPv4 address which is the Subject of this Query.	[RFC4620]
140 ICMP Node Information Response	0 - A successful reply. The Reply Data field may or may not be empty.	[RFC4620]
	1 - The Responder refuses to supply the answer. The Reply Data field will be empty.	[RFC4620]
	2 - The Qtype of the Query is unknown to the Responder. The Reply Data field will be empty.	[RFC4620]
141 Inverse Neighbor Discovery Solicitation Message	0	[RFC3122]
142 Inverse Neighbor Discovery Advertisement Message	0	[RFC3122]
143 Version 2 Multicast Listener Report	-	[RFC3810]
144 Home Agent Address Discovery Request Message	0	[RFC3775]
145 Home Agent Address Discovery Reply Message	0	[RFC3775]

ICMPv6 Type	ICMPv6 Code	Reference
146 Mobile Prefix Solicitation	0	[RFC3775]
147 Mobile Prefix Advertisement	0	[RFC3775]
148 Certification Path Solicitation Message	-	[RFC3971]
149 Certification Path Advertisement Message	-	[RFC3971]
150 ICMP messages utilized by experimental mobility protocols such as Seamoby	-	[RFC4065]
151 Multicast Router Advertisement	-	[RFC4286]
152 Multicast Router Solicitation	-	[RFC4286]
153 Multicast Router Termination	-	[RFC4286]
154 FMIPv6 Messages	-	[RFC5268]
200 Private experimentation	-	[RFC4443]
201 Private experimentation	-	[RFC4443]
255 Reserved for expansion of ICMPv6 informational messages	-	[RFC4443]

Chapter 8 User Authentication

The chapter introduces the following topics:

- Authentication, Authorization and Accounting describes the AAA function: Authentication, Authorization and Accounting.
- User Identification describesdescribes various methods of user identification, which is used to authenticate users who access the Internet via the device.
- 802.1X Authentication describes the function of 802.1X authentication. 802.1X is a standard defined by IEEE for Port-based Network Access Control.
- PKI describes the function of Public Key Infrastructure, which provides public key encryption and digital signature service.

Authentication, Authorization and Accounting

Overview

AAA is the abbreviation for Authentication, Authorization and Accounting. Details are as follows:

- Authentication: Authenticates users' identities.
- Authorization: Grants certain privileges according to the configuration.
- Accounting: Records the fees users should pay for their network resource usage.

FS devices support the following authentication methods:

- Local authentication: Configures user information (including username, password and properties) on FS devices. Local authentication is fast, and can reduce operation cost, but the amount of information that will be stored is limited by the hardware of the device. By default, FS devices use local authentication.
- External authentication: FS devices also support external authentication over RADIUS, AD, LDAP and TACACS+ protocol. User information is stored in an external RADIUS, AD, LDAP or TACACS+ server, and FS devices authenticate users by the external server.

FS devices support the following authorization methods:

- Local authorization: Authorizes user privileges according to the configurations of FS devices.

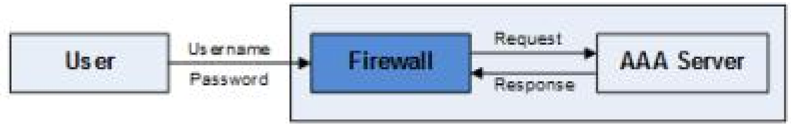
- Authorization after external authentication: RADIUS/LDAP/AD/TACACS+ authentication is mapped to an authorization.

FS devices support the following accounting methods:

- None accounting: No accounting required.
- External accounting: Performs Accounting for authenticated users via a RADIUS server.

External Authentication Procedure

When a user has established a connection from a terminal to a FS device and gained access or management privilege, the FS device can authenticate the user via the configured RADIUS or LDAP server. The figure below shows the external authentication procedure:



As shown above, the procedure is:

1. The user sends username and password to the FS device.
2. The FS device receives the username and password, and sends an authentication request to the RADIUS/LDAP/AD/TACACS+/WeChat server.
3. If the request is legal, the RADIUS/LDAP/AD/TACACS+ server performs authentication. If passed, the RADIUS/LDAP/AD/TACACS+server returns the user information to the FS device, otherwise returns denial information. The security between the FS device and RADIUSTACACS+ server is guaranteed by the shared secret (secret key or cipher text).

Configuring an AAA Server

The configurations of an AAA server include:

- Creating an AAA server
- Configuring a local authentication server
- Configuring a RADIUS authentication server
- Configuring an Active-Directory authentication server
- Configuring a TACACS+ authentication server
- Configuring an LDAP authentication server

- Configuring a RADIUS accounting server
- Specifying an authentication server for the system administrator

Creating an AAA Server

AAA configurations need to be done in the AAA service configuration mode. To create an AAA server, in the global configuration mode, use the following command:

```
aaa-server aaa-server-name [type] {local | radius | active-directory | ldap | tacacs+}
```

- *aaa-server-name* – Specifies the name of the AAA server. The length is 1 to 31 characters and is case sensitive.
- **type {local | radius | active-directory | ldap | tacacs+}** – Specifies the type of the AAA server to be created. It can be a local server (`local`), RADIUS server (`radius`), Active-Directory server (`active-directory`), LDAP server (`ldap`) or TACACS+ server (`tacacs+`).

After executing this command, the system will create an AAA server with the specified name, and enter the AAA server configuration mode. If the specified name exists, the system will directly enter the AAA server configuration mode.

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

```
no aaa-server aaa-server-name
```

Configuring a Local Authentication Server

To enter the local server configuration mode, in the global configuration mode, use the command **aaa-server** *aaa-server-name* **type local**. The local authentication server configuration includes:

- Configuring the password control
- Configuring a role mapping rule
- Configuring a user blacklist
- Configuring a backup authentication server

Configuring the Password Control

To prevent account security problem caused by not changing passwords for a long time, you can enable the password control function to set the password validity and the days how long users will be reminded of password expiry before it expires. You can also configure the history password check function to ensure the new password is different from the history passwords.

To enter the password control mode, use the following command:

password-control

To configure the password validity and password expiry warning, in the password control mode, use the following command:

aging *aging-day* [**alert-before-expire** *alert-day*]

- *aging-day* - Specifies the valid period of password. The value range is 1 to 365 days. The default value is 90.
- *alert-day* - Specifies the days to remind the user to change the password before the password expires. The value range is 1 to 30 days. The default value is 7.

To cancel the settings of password validity and password expiry warning, use the **no aging** command.

When the history password check function is enabled, system will verify the newly changed password with verifying the historical passwords, ensuring the new password is different from the history passwords. To configure the history password check function, in the password control mode, use the following command:

history-check *count*

- *count* - Configure the newly changed passwords is different from the passwords set in the recent specified times. The value range is 1 to 5. The default value is 3.

To cancel the history password check configuration, use the **no history-check** command.

Configuring a Role Mapping Rule

After specifying a role mapping rule, the system will assign a role for users who have been authenticated by the server according to the specified role mapping rule. To configure a role mapping rule for the server, in the local server configuration mode, use the following command:

role-mapping-rule *rule-name*

- *rule-name* – Specifies the name of the existing role mapping rule.

To cancel the specified role mapping rule configuration, in the local server configuration mode, use the following command:

no role-mapping-rule

Configuring a User Blacklist

After configuring a user blacklist for the local server, the system will not allow blacklist users who are authenticated by the server to access any network resource. To configure a user blacklist, in the local server configuration mode, use the following command:

user-black-list username *user-name*

- *user-name* – Specifies the username of blacklist user. The value range is 1 to 63 characters.

To delete a user from the blacklist, in the local server configuration mode, use the following command:

no user-black-list username *user-name*

Configuring a Backup Authentication Server

After configuring a backup authentication server for the local server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be any existing local, Active-Directory, RADIUS or LDAP server defined in the system. To configure a backup authentication server, in the local server configuration mode, use the following command:

backup-aaa-server *aaa-server-name*

- *aaa-server-name* – Specifies an AAA server defined in the system.

To cancel the specified backup authentication server, in the local server configuration mode, use the following command:

no backup-aaa-server

Note:

- The backup authentication server and primary server should belong to the same VSYS. For more information about VSYS, see Virtual System.
- The backup authentication server should not nest another backup authentication server.
- Before deleting an AAA server, make sure the server is not specified as a backup authentication server.

Configuring a RADIUS Authentication Server

To enter the RADIUS server configuration mode, in the global configuration mode, use the command **aaa-server** *aaa-server-name* **type radius**.

The RADIUS authentication server configuration includes:

- Configuring the IP address or domain name of the primary server
- Configuring the IP address or domain name of the backup server 1
- Configuring the IP address or domain name of the backup server 2
- Configuring the port number
- Configuring the secret
- Configuring the retry times
- Configuring the timeout
- Specifying a role mapping rule
- Configuring a user blacklist
- Configuring a backup authentication server

Configuring the IP Address, Domain Name, or VRouter of the Primary Server

To configure the IP address, domain name, or VRouter of the primary authentication server, in the RADIUS server configuration mode, use the following command:

host {*ip-address* | *host-name* }[**vrouter** *vrouter-name*]

- *ip-address* | *host-name* – Specifies the IP address or domain name of the primary authentication server.
- **vrouter** *vrouter-name* – Specifies the VRouter that the primary server belongs to. The default Vrouter is trust-vr.

To delete the above configurations of the primary authentication server, in the RADIUS server configuration mode, use the command:

no host

Configuring the IP Address, Domain Name, or VRouter of the Backup Server 1

This configuration is optional. Backup server must be of the same type of primary server. When the authentication does not pass primary server’ s check, the backup server 1 and 2 will start checking its credentials consecuritvely. To configure the IP address, domain name, or VRouter of the backup authentication server 1, in the RADIUS server configuration mode, use the following command:

backup1 {*ip-address* | *host-name* }[**vrouter** *vrouter-name*]

- *ip-address* | *host-name* – Specifies the IP address or domain name of the backup server 1.
- **vrouter** *vrouter-name* – Specifies the VRouter that the back server 1 belongs to. The default Vrouter is trust-vr.

To delete the IP address or domain name configuration of the backup authentication server 1, in the RADIUS server configuration mode, use the command:

```
no backup1
```

Configuring the IP Address, Domain Name, or VRouter of the Backup Server 2

This configuration is optional. Backup server must be of the same type of main server. When the authentication does not pass main server’ s check, the backup server 1 and 2 will start checking its credentials consecuritvely.To configure the IP address or domain name of the backup authentication server 2, in the RADIUS server configuration mode, use the following command:

backup2 {*ip-address* | *host-name* }[**vrouter** *vrouter-name*]

- *ip-address* | *host-name* – Specifies the IP address or domain name of the backup server 2.
- **vrouter** *vrouter-name* – Specifies the VRouter that the back server 2 belongs to. The default Vrouter is trust-vr.

To delete the IP address or domain name configuration of the backup authentication server 2, in the RADIUS server configuration mode, use the command:

```
no backup2
```

Configuring the Port Number

To configure the port number of the RADIUS server, in the RADIUS server configuration mode, use the following command:

port *port-number*

- *port-number* – Specifies the port number of the RADIUS server. The value ranges from 1024 to 65535. The default value is 1812.

To restore the default value of the port number, in the RADIUS server configuration mode, use the command:

```
no port
```

Configuring the Secret

To configure the secret of the RADIUS server, in the RADIUS server configuration mode, use the following command:

```
secret secret
```

- *secret* − Specifies the secret string of the RADIUS server. The length is 1 to 31 characters.

To cancel the secret configuration of the RADIUS server, in the RADIUS server configuration mode, use the command

```
no secret
```

Configuring the Retry Times

If the security device does not receive the response packets from the AAA server, it will resend the authentication packets. Retry times refers to the times for the authentication packets resent to the AAA server. To configure the retry times, in the RADIUS server configuration mode, use the following command:

```
retries times
```

- *times* − Specifies a number of retry times for the authentication packets sent to the AAA server. The value range is 1 to 10. The default value is 3.

To restore to the default value, in the RADIUS server configuration mode, use the command:

```
no retries
```

Configuring the Timeout

If the security device does not receive response packets from the AAA server when the server response time ends, the device will resend the authentication packets. To configure the timeout, in the RADIUS server configuration mode, use the following command:

```
timeout time-value
```

- *time-value* − Specifies the response timeout for the server. The value range is 1 to 30 seconds. The default value is 3.

To restore to the default timeout, in the RADIUS server configuration mode, use the command:

```
no timeout
```

Specifying a Role Mapping Rule

After specifying the role mapping rule, the system will assign a role for users who have been authenticated by the server according to the specified role mapping rule. To configure a role mapping rule, in the RADIUS server configuration mode, use the following command:

role-mapping-rule *rule-name*

- *rule-name* − Specifies the name of the existing role mapping rule.

To cancel the role mapping rule configuration, in the RADIUS server configuration mode, use the command:

no role-mapping-rule

Configuring a User Blacklist

After configuring a user blacklist for the RADIUS server, the system will not allow blacklist users who are authenticated by the server to access any network resource. To configure a user blacklist, in the RADIUS server configuration mode, use the following command:

user-black-list username *user-name*

- *user-name* − Specifies the username of blacklist user. The value range is 1 to 63 characters.

To delete a user from the blacklist, in the RADIUS server configuration mode, use the following command:

no user-black-list username *user-name*

Configuring a Backup Authentication Server

After configuring a backup authentication server for the RADIUS server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be different from main server. It can be any existing local, Active-Directory, RADIUS or LDAP server defined in the system. To configure a backup authentication server, in the RADIUS server configuration mode, use the following command:

backup-aaa-server *aaa-server-name*

- *aaa-server-name* − Specifies an AAA server defined in the system.

To cancel the specified backup authentication server, in the RADIUS server configuration mode, use the following command:

no backup-aaa-server

Note:

- The backup authentication server and primary server should belong to the same VSYS. For more information about VSYS, see Virtual System.
- The backup authentication server should not nest another backup authentication server.
- Before deleting an AAA server, make sure the server is not specified as a backup authentication server.
- If a RADIUS server is configured with backup server 1 (backup1), backup server 2 (backup2) and backup authentication server (backup-aaa-server), when user's authentication request is not responded on the primary server, the system will re-authenticate the user in the following order: backup server 1 -> backup server 2 -> backup authentication server; when user's authentication failed on the primary server, the system will re-authenticate the user in the following order: backup server 1 -> backup server 2 -> backup authentication server.

Configuring an Active-Directory Authentication Server

To enter the Active-Directory server configuration mode, in the global configuration mode, use the command **aaa-server** *aaa-server-name* **type active-directory**.

The Active-Directory authentication server configuration includes:

- Configuring the IP address or domain name of the primary server
- Configuring the IP address or domain name of the backup server 1
- Configuring the IP address or domain name of the backup server 2
- Configuring the port number
- Configuring the authentication or synchronization method
- Refreshing the connection with the server
- Specifying the Base-DN
- Specifying the login DN
- Specifying sAMAccountName
- Specifying the login password
- Specifying a role mapping rule
- Configuring a user blacklist
- Configuring the security agent

- Configuring automatic user information synchronization
- Configuring user filter
- Configuring synchronization mode of user information
- Configuring a backup authentication server
- Configuring the User-Groups under Base-DN Synchronization

Configuring the IP Address, Domain Name, and VRouter of the Primary Server

To configure the IP address, domain name, or VRouter of the primary authentication server, in the Active-Directory server configuration mode, use the following command:

host {*ip-address* | *host-name* }[**vrouter** *vrouter-name*]

- *ip-address* | *host-name* – Specifies the IP address or domain name of the primary authentication server.
- **vrouter** *vrouter-name* – Specifies the VRouter that the primary server belongs to. The default VRouter is trust-vr.

To delete the IP address or domain name configuration of the primary authentication server, in the Active-Directory server configuration mode, use the command:

no host

Configuring the IP Address, Domain Name, VRouter of the Backup Server 1

This configuration is optional. Backup server must be of the same type of primary server. When the authentication does not pass primary server’ s check, the backup server 1 and 2 will start checking its credentials consecuritvely. To configure the IP address or domain name of the backup authentication server 1, in the Active-Directory server configuration mode, use the following command:

backup1 {*ip-address* | *host-name* }[**vrouter** *vrouter-name*]

- *ip-address* | *host-name* – Specifies the IP address or domain name of the backup authentication server 1.
- **vrouter** *vrouter-name* – Specifies the VRouter that the backup server 1 belongs to. The default VRouter is trust-vr.

To delete the IP address or domain name configuration of the backup authentication server 1, in the Active-Directory server configuration mode, use the command:

no backup1

Configuring the IP Address or Domain Name of the Backup Server 2

This configuration is optional. Backup server must be of the same type of primary server. When the authentication does not pass primary server’s check, the backup server 1 and 2 will start checking its credentials consecuritvely. To configure the IP address or domain name of the backup authentication server 2, in the Active-Directory server configuration mode, use the following command:

backup2 {*ip-address* | *host-name* }[**vrouter** *vrouter-name*]

- *ip-address* | *host-name* – Specifies the IP address or domain name of the backup authentication server 2.
- **vrouter** *vrouter-name* – Specifies the VRouter that the backup server 2 belongs to. The default VRouter is trust-vr.

To delete the IP address or domain name configuration of the backup authentication server 2, in the Active-Directory server configuration mode, use the command:

no backup2

Configuring the Port Number

To configure the port number of the Active-Directory server, in the Active-Directory server configuration mode, use the following command:

port *port-number*

- *port-number* – Specifies the port number of the Active-Directory server. The value range is 1 to 65535. The default value is 389.

To restore to the default port number, in the Active-Directory server configuration mode, use the command:

no port

Configuring the Authentication or Synchronization Method

Plain text and MD5 method can be configured to authenticate or synchronize user between the Active-Directory server and the system. To configure the authentication or synchronization method, in the Active-Directory server configuration mode, use the following command:

auth-method {**plain** | **digest-md5**}

- **plain** – Specifies the authentication or synchronization method to be plain text.
- **digest-md5** – Specifies the authentication or synchronization method to be MD5. The default method is MD5.

To restore to the default authentication or synchronization method, in the Active-Directory server configuration mode, use the command:

```
no auth-method
```

Note: If the sAMAccountName is not configured after you specify the MD5 method, the plain method will be used in the process of synchronizing user from the server, and the MD5 method will be used in the process of authenticating user.

Specifying the Base-DN

Base-DN is the starting point at which your search will begin when the AD server receives an authentication request. To specify the Base-DN, in the Active-Directory server configuration mode, use the following command:

base-dn *string*

- *string* – Specifies the Base-DN for the Active-Directory server, such as dc = fs.

To cancel the Base-DN configuration, in the Active-Directory server configuration mode, use the command:

```
no base-dn
```

Specifying the Login DN

If plain text method is configured to authenticate or synchronize user, the system will send the login DN and the login password to the server to be authenticated, in order to connect to the server for user authentication or synchronization. The login DN is typically a user account with query privilege predefined by the Active-Directory server. To specify the login DN, in the Active-Directory server configuration mode, use the following command:

login-dn *string*

- *string* – Specify the login DN for the Active-Directory server, which is a string of 1 to 255 characters and is not case sensitive.

To cancel the login DN configuration, in the Active-Directory server configuration mode, use the command:

```
no login-dn
```

Specifying sAMAccountName

If MD5 method is configured to authenticate or synchronize user, the system will send the sAMAccountName and the login password to the server to be authenticated, in order to connect to the server for user authentication or synchronization. To specify the sAMAccountName, in the Active-Directory server configuration mode, use the following command:

login-dn sAMAccountName *string*

- *string* – Specifies the sAMAccountName, which is a string of 1 to 63 characters and is case sensitive.

To cancel the sAMAccountName configuration, in the Active-Directory server configuration mode, use the command:

no login-dn sAMAccountName

Specifying the Login Password

The login password here should correspond to the password for Login DN. To configure the login password, in the Active-Directory server configuration mode, use the following command:

login-password *string*

- *string* – Specifies the login password for the Active-Directory server.

To cancel the password configuration, in the Active-Directory server configuration mode, use the command:

no login-password

Specifying a Role Mapping Rule

After specifying the role mapping rule, the system will assign a role for users who have been authenticated by the server according to the specified role mapping rule. To configure role mapping rules, in the Active-Directory server configuration mode, use the following command:

role-mapping-rule *rule-name*

- *rule-name* – Specifies the name of the existing mapping rule.

To cancel the role mapping rule configuration, in the Active-Directory server configuration mode, use the command:

no role-mapping-rule

Configuring a User Blacklist

After configuring a user blacklist for the Active-Directory server, the system will not allow blacklist users who are authenticated by the server to access any network resource. To configure a user blacklist, in the Active-Directory server configuration mode, use the following command:

```
user-black-list username user-name
```

- *user-name* – Specifies the username of blacklist user. The value range is 1 to 63 characters.

To delete a user from the blacklist, in the Active-Directory server configuration mode, use the following command:

```
no user-black-list username user-name
```

Configuring the Security Agent

With the security agent function enabled, FSOS 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 Single Sign On is implemented. Besides, by making use of the obtained mappings, FSOS can also implement other user-based functions, like security statistics, logging, behavior auditing, etc.

To enable security agent on the Active-Directory server, you need to first install and run AD Agent on the server or other PCs in the domain. After that, when a domain user is logging in or logging out, AD Agent will record the user's username, IP address, current time and other information, and add the mapping between the username and IP address to FSOS. In this way FSOS can obtain every online user's IP address. AD Agent can be used in Windows Server 2003 (32-bit/64-bit), Windows Server 2008 (32-bit/64-bit), and Windows Server 2008 R2 (64-bit).

Note:The installation and configuration of AD Agent, please refer to Configuring AD Agent for SSO.

Enabling/Disabling the Security Agent

To enable the Active-Directory security agent, in the Active-Directory server configuration mode, use the following command:

```
agent
```

To disable the security agent, in the Active-Directory server configuration mode, use the command:

```
no agent
```

Specifying the Agent Port and Login Info Timeout

FSOS communicates with AD Agent on the agent port, obtaining the mappings between the usernames of the domain users and IP addresses. When the communication is disconnected, if the connection does not reconnect within the specified login info timeout, FSOS will delete the obtained mappings. To specify the agent port and login info timeout, in the Active-Directory server configuration mode, use the following command:

agent [**port** *port-number*] [**disconn-del-timeout** *time*]

- **port** *port-number* − Specifies the agent port. FSOS 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 be failed to communicate with the AD Agent.
- **disconn-del-timeout** *time* − Specifies the login info timeout. The value range is 0 to 1800 seconds. The default value is 300. The value of 0 indicates never timeout.

To cancel the agent port and login info timeout configurations, in the Active-Directory server configuration mode, use the command:

no agent

Viewing the Agent User Information

To view the information of the online agent users, in any mode, use the following command:

show auth-user agent [**interface** *interface-name* | **vrouter** *vrouter-name* | **slot** *slot-no*]

Deleting the User Mapping Information

To delete the user mapping information of the specified IP, in any mode, use the following command:

exec user-mappping agent kickout ip *ip-address* **vrouter** *vrouter-name*

User Synchronization

User synchronization specifies that the system will synchronize user information on the configured Active-Directory server to the local. By default, the system will synchronize user information every 30 minutes.

Enable or Disable User Synchronization

Before synchronizing user information, you need to enable synchronization function. By default, it is enabled. To enable or disable user synchronization function, in the Active-Directory configuration mode, use the following command:

- Enable user synchronization: **sync enable**

- Disable user synchronization: **sync disable**

Configuring User Synchronization

System supports two synchronization modes: manual synchronization and automatic synchronization.

Manul Synchronization

In the Active-Directory configuration mode, use the following command to update the connections with Active-Directory server and manually synchronize user information:

```
manual-sync
```

After executing the command, system will synchronize information immediately. If reconfigure the command during synchronization process, the system will clear the existed user information and resynchronize.

Automatic Synchronization

To configure the automatic synchronization, in the Active-Directory server configuration mode, use the following command:

auto-sync {**periodically** *interval* | **daily** *HH:MM* | **once**}

- *interval* – Specifies the time interval of automatic synchronization. The value range is 30 to 1440 minutes. The default value is 30.
- *HH:MM* – Specifies the time when the user information is synchronized everyday. HH and MM indicates hour and minute respectively.
- *once* – If this parameter is specified, the system will synchronize automatically when the configuration of Active-Directory server is modified. After executing this command , the system will synchronize user information immediately.

By default, the system will synchronize the user information on the authentication server to the local every 30 minutes. To restore the automatic synchronization mode to default, in the Active-Directory server configuration mode, use the following command:

```
no auto-sync
```

Configuring User Filter

After configuring user filters, the system can only synchronize and authenticate users that are match the filters on the authentication server. You must enter AAA server configuration mode before configuring user filter.

To enter the Active-Directory server configuration mode, in the global configuration mode, use the command:

aaa-server *aaa-server-name* **type active-directory**

To configure user-filter, in the Active-Directory server configuration mode, use the following command:

user-filter *filter-string*

- *filter-string* – Specifies the user filters. The length is 0 to 120 characters. For example, when you configure an Active-Directory server, if the *filter-string* is configured to "memberOf=CN=Admin, DC=test, DC=com", which indicates that the system only can synchronize or authenticate user whose DN is "memberOf=CN=Admin, DC=test, DC=com".

The commonly used operators are as follows:

Operator	Meaning
=	Equals a value.
&	and
|	or
!	not
*	Wildcard. It represents zero or more characters.
～=	fuzzy query
>=	Be equal or greater than a specified value in lexicographical order.
<=	Be equal or less than a specified value in lexicographical order.

Note:

- The FS system supports all the operators that Active-Directory server supports.
- If the entered format does not comply with the rules of the Active-Directory server, the system may fail to synchronize or authenticate users from the server.

In the Active-Directory server configuration mode, use **no user-filter** to cancel the above configuration.

Configuring Synchronization Mode of User Information

Two synchronization modes can be selected to synchronize organization structure and user information to local from Active-Directory server: OU-based and Group-based, so that you can configure above two types of user group in security policy rules. By default, user information will be synchronized to the local based on Group.

To configure the synchronization mode of user information, in the Active-Directory server configuration mode, use the following command:

```
sync-type {ou | group}
```

- **ou** – Synchronizes user information to the local based on OU.
- **group** – Synchronizes user information to the local based on Group.

If the OU mode is selected, you can configure the maximum depth of OU to be synchronized. In the Active-Directory server configuration mode, use the following command:

sync-ou-depth *depth-value*

- *depth-value* – Specifies the maximum depth of OU to be synchronized. The value range is 1 to 12, and the default value is 12. OU structure that exceeds the maximum depth will not be synchronized, but users that exceed the maximum depth will be synchronized to the specified deepest OU where they belong to. If the total characters of the OU name for each level(including the "OU=" string and punctuation) is more than 128, OU information that exceeds the length will not be synchronized to the local.

Configuring a Backup Authentication Server

After configuring a backup authentication server for the Active-Directory server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be any existing local, Active-Directory, RADIUS or LDAP server defined in the system. To configure a backup authentication server, in the Active-Directory server configuration mode, use the following command:

backup-aaa-server *aaa-server-name*

- *aaa-server-name* – Specifies an AAA server defined in the system.

To cancel the specified backup authentication server, in the Active-Directory server configuration mode, use the following command:

```
no backup-aaa-server
```

Note:

- The backup authentication server and primary server should belong to the same VSYS. For more information about VSYS, see Virtual System.
- The backup authentication server should not nest another backup authentication server.

- Before deleting an AAA server, make sure the server is not specified as a backup authentication server.
- If an Active-Directory server is configured with backup server 1 (backup1), backup server 2 (backup2) and backup authentication server (backup-aaa-server), when user's authentication request is not responded on the primary server, the system will re-authenticate the user in the following order: backup server 1 -> backup server 2 -> backup authentication server; when user's authentication failed on the primary server, the system will re-authenticate the user in the following order: backup server 1 -> backup server 2 -> backup authentication server.

Configuring the User-Groups under Base-DN Synchronization

When you sync the users and user-groups from Active-Directory server, you can enable or disable the user-groups under Base-DN Synchronization as need. In the Active-Directory server configuration mode, use the following command:

- Enable: **sync-group-under-basedn enable**
- Disable: **no sync-group-under-basedn enable**

Configuring an LDAP Authentication Server

To enter the LDAP server configuration mode, in the global configuration mode, use the command **aaa-server** *aaa-server-name* **type ldap**.

The LDAP authentication server configuration includes:

- Configuring the IP address or domain name of the primary server
- Configuring the IP address or domain name of the backup server 1
- Configuring the IP address or domain name of the backup server 2
- Configuring the port number
- Configuring the authentication or synchronization method
- Refreshing the connection with the Server
- Specifying the Base-DN
- Specifying the login DN
- Specifying Authid
- Specifying the login password

- Specifying the name attribute
- Specifying the Group-class
- Specifying the member attribute
- Specifying a role mapping rule
- Configuring a user blacklist
- Configuring automatic user information synchronization
- Configuring user filter
- Configuring synchronization mode of user information
- Configuring a backup authentication server

Configuring the IP Address, Domain Name, or VRouter of the Primary Server

To configure the IP address or domain name of the primary authentication server, in the LDAP server configuration mode, use the following command:

host {*ip-address* | *host-name* }[**vrouter** *vrouter-name*]

- *ip-address | host-name – Specifies the IP address or domain name of the primary authentication server.*
- **vrouter** *vrouter-name* – Specifies the VRouter that the primary server belongs to. The default VRouter is trust-vr.

To cancel the IP address or domain name configuration of the primary authentication server, in the LDAP server configuration mode, use the command:

no host

Configuring the IP Address, Domain Name, or VRouter of the Backup Server 1

This configuration is optional. Backup server must be of the same type of primary server. When the authentication does not pass primary server's check, the backup server 1 and 2 will start checking its credentials consecutively. To configure the IP address or domain name of the backup authentication server 1, in the LDAP server configuration mode, use the following command:

backup1 {*ip-address* | *host-name* }[**vrouter** *vrouter-name*]

- *ip-address* | *host-name* – Specifies the IP address or domain name of the backup authentication server 1.

- **vrouter** *vrouter-name* – Specifies the VRouter that the backup server belongs to. The default VRouter is trust-vr.

To cancel the IP address or domain name configuration of the backup authentication server 1, in the LDAP server configuration mode, use the command:

no backup1

Configuring the IP Address, Domain Name, VRouter of the Backup Server 2

This configuration is optional. Backup server must be of the same type of primary server. When the authentication does not pass primary server’ s check, the backup server 1 and 2 will start checking its credentials consecutively. To configure the IP address or domain name of the backup authentication server 2, in the LDAP server configuration mode, use the following command:

backup2 {*ip-address* | *host-name* }[**vrouter** *vrouter-name*]

- *ip-address* | *host-name* – Specifies the IP address or domain name of the backup authentication server 2.
- **vrouter** *vrouter-name* – Specifies the VRouter that the backup server belongs to. The default VRouter is trust-vr.

To cancel the IP address or domain name configuration of the backup authentication server 2, in the LDAP server configuration mode, use the command

no backup2

Configuring the Port Number

To configure the port number of the LDAP server, in the LDAP server configuration mode, use the following command:

port *port-number*

- *port-number* – Specifies the port number of the LDAP server. The value range is 1 to 65535. The default value is 389.

To restore to the default value, in the LDAP server configuration mode, use the command:

no port

Configuring the Authentication or Synchronization Method

Plain text and MD5 method can be configured to authenticate or synchronize user between the LDAP server and the system. To configure the authentication or synchronization method, in the LDAP server configuration mode, use the following command:

```
auth-method {plain | digest-md5}
```

- **plain** − Specifies the authentication or synchronization method to be plain text.
- **digest-md5** − Specifies the authentication or synchronization method to be MD5. The default method is MD5.

To restore to the default authentication or synchronization method, in the LDAP server configuration mode, use the command:

```
no auth-method
```

Note:If the Authid is not configured after you specify the MD5 method, the plain method will be used in the process of synchronizing user from the server, and the MD5 method will be used in the process of authenticating user.

Specifying the Base-DN

Base-DN is the starting point at which your search will begin when the LDAP server receives an authentication request. To specify the Base-DN, in the LDAP server configuration mode, use the following command:

```
base-dn string
```

- *string* − Specifies the Base-DN for the LDAP server, such as dc = fs.

To cancel the Base-DN configuration, in the LDAP server configuration mode, use the command:

```
no base-dn
```

Specifying the Login DN

If plain text method is configured to authenticate or synchronize user, the system will send the login DN and the login password to the server to be authenticated, in order to connect to the server for user authentication or synchronization. The login DN is typically a user account with query privilege predefined by the LDAP server. To specify the login DN, in the LDAP server configuration mode, use the following command:

```
login-dn string
```

- *string* − Specify the login DN for the LDAP server, which is a string of 1 to 255 characters and is not case sensitive.

To cancel the login DN configuration, in the LDAP server configuration mode, use the command:

```
no login-dn
```

Specifying Authid

If MD5 method is configured to authenticate or synchronize user, the system will send the Authid and the login password to the server to be authenticated, in order to connect to the server for user authentication or synchronization. To specify the Authid, in the LDAP server configuration mode, use the following command:

login-dn authid *string*

- *string* − Specifies the Authid, which is a string of 1 to 63 characters and is case sensitive.

To cancel the Authid configuration, in the LDAP server configuration mode, use the command:

no login-dn Authid

Configuring the Login Password

The login password here should correspond to the password for Login DN. To configure the login password, in the LDAP server configuration mode, use the following command:

login-password *string*

- *string* − Specifies the login password for the LDAP server.

To cancel the password configuration, in the LDAP server configuration mode, use the command:

no login-password

Specifying the Name Attribute

The name attribute is a string that uniquely identifies name in the LDAP server. To specify the name attribute, in the LDAP server configuration mode, use the following command:

naming-attribute *string*

- *string* − Specifies the name attribute. The length is 1 to 63 characters. The string is usually uid (User ID) or cn (Common Name). The default name attribute is uid.

To restore to the default value, in the LDAP server configuration mode, use the command:

no naming-attribute

Specifying the Name Attribute

The name attribute is a string that uniquely identifies group name in the LDAP server. To specify the group name attribute, in the LDAP server configuration mode, use the following command:

group-naming-attribute *string*

- *string* − Specifies the group name attribute. The length is 1 to 63 characters. The string is usually uid (User ID) or cn (Common Name). The default name attribute is uid.

To restore to the default value, in the LDAP server configuration mode, use the command:

no group-naming-attribute

Specifying the Group-class

To specify the ObjectClass of the Group-class, in the LDAP server configuration mode, use the following command:

group-class *string*

- *string* − Specifies the Group-class. The length is 1 to 63 characters. The default value is groupOfUniqueNames.

To restore to the default value, in the LDAP server configuration mode, use the command:

no group-class

Specifying the Member Attribute

To specify the member attribute of the Group-class, in the LDAP server configuration mode, use the following command:

member-attribute *string*

- *string* − Specifies the member attribute. The length is 1 to 63 characters. The default value is uniqueMember.

To restore the default value, in the LDAP server configuration mode, use the command:

no member-attribute

Specifying a Role Mapping Rule

After specifying the role mapping rule, the system will assign a role for users who have been authenticated by the server according to the specified role mapping rule. To configure role mapping rules, in the LDAP server configuration mode, use the following command:

role-mapping-rule *rule-name*

- *rule-name* − Specifies the name of the existing mapping rule.

To cancel the role mapping rule configuration, in the LDAP server configuration mode, use the command

```
no role-mapping-rule
```

Configuring a User Blacklist

After configuring a user blacklist for the LDAP server, the system will not allow blacklist users who are authenticated by the server to access any network resource. To configure a user blacklist, in the LDAP server configuration mode, use the following command:

user-black-list username *user-name*

- *user-name* − Specifies the username of blacklist user. The value range is 1 to 63 characters.

To delete a user from the blacklist, in the LDAP server configuration mode, use the following command:

no user-black-list username *user-name*

User Synchronization

User synchronization specifies that the system will synchronize user information on the configured LDAP server to the local. By default, the system will synchronize user information every 30 minutes.

Enable or Disable User Synchronization

Before synchronizing user information, you need to enable synchronization function. By default, it is enabled. To enable or disable user synchronization function, in the LDAP configuration mode, use the following command:

- Enable user synchronization: **sync enable**
- Disable user synchronization: **sync disable**

Configuring User Synchronization

System supports two synchronization modes: manual synchronization and automatic synchronization.

Manul Synchronization

In the LDAP configuration mode, use the following command to update the connections with LDAP server and manually synchronize user information:

manual-sync

After executing the command, system will synchronize information immediately. If reconfigure the command during synchronization process, the system will clear the existed user information and resynchronize.

Automatic Synchronization

To configure the automatic synchronization, in the LDAP server configuration mode, use the following command:

auto-sync {**periodically** *interval* | **daily** *HH:MM* | **once**}

- *interval* – Specifies the time interval of automatic synchronization. The value range is 30 to 1440 minutes. The default value is 30.
- *HH:MM* – Specifies the time when the user information is synchronized everyday. HH and MM indicates hour and minute respectively.
- once – If this parameter is specified, the system will synchronize automatically when the configuration of LDAP server is modified. After executing this command , the system will synchronize user information immediately.

By default, the system will synchronize the user information on the authentication server to the local every 30 minutes. To restore the automatic synchronization mode to default, in the LDAP server configuration mode, use the following command:

no auto-sync

Configuring User Filter

After configuring user filters, the system can only synchronize and authenticate users that are match the filters on the authentication server. You must enter AAA server configuration mode before configuring user filter.

To enter the LDAP server configuration mode, in the global configuration mode, use the command:

aaa-server *aaa-server-name* **type ldap**

To configure user-filter, in the LDAP server configuration mode, use the following command:

user-filter *filter-string*

- filter-string – Specifies the user filters. The length is 0 to 120 characters. For example, when you configure a LDAP server, if the filter-string is configured to “(|(objectclass=inetOrgperson)(objectclass=person))” , which means that the system only can synchronize or authenticate users which are defined as inetOrgperson or person.

The commonly used operators are as follows:

Operator	Meaning
=	equals a value
&	and
|	or
!	not
*	Wildcard. It represents zero or more characters.
～=	fuzzy query
>=	Be equal or greater than a specified value in lexicographical order.
<=	Be equal or less than a specified value in lexicographical order.

Note:

- The FS system supports all the operators that LDAP server supports.
- If the entered format does not comply with the rules of the LDAP server, the system may fail to synchronize or authenticate users from the server.

In the LDAP server configuration mode, use **no user-filter** to cancel the above configuration.

Configuring Synchronization Mode of User Information

Two synchronization modes can be selected to synchronize organization structure and user information to local from LDAP server: OU-based and Group-based, so that you can configure above two types of user group in security policy rules. By default, user information will be synchronized to the local based on Group.

To configure the synchronization mode of user information, in the LDAP server configuration mode, use the following command:

sync-type {**ou** | **group**}

- **ou** – Synchronizes user information to the local based on OU.
- **group** – Synchronizes user information to the local based on Group.

If the OU mode is selected, you can configure the maximum depth of OU to be synchronized. In the LDAP server configuration mode, use the following command:

sync-ou-depth *depth-value*

- *depth-value* – Specifies the maximum depth of OU to be synchronized. The value range is 1 to 12, and the default value is 12. OU structure that exceeds the maximum depth will not be synchronized, but users that exceed the maximum depth will be synchronized to the specified deepest OU where they belong to. If the total characters of the OU name for each level(including the "OU=" string and punctuation) is more than 128, OU information that exceeds the length will not be synchronized to the local.

Configuring a Backup AAA Server

After configuring a backup authentication server for the LDAP server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be any existing local, Active-Directory, RADIUS or LDAP server defined in the system. To configure a backup authentication server, in the LDAP server configuration mode, use the following command:

backup-aaa-server *aaa-server-name*

- *aaa-server-name* – Specifies an AAA server defined in the system.

To cancel the specified backup authentication server, in the LDAP server configuration mode, use the following command:

no backup-aaa-server

Note:

- The backup authentication server and primary server should belong to the same VSYS. For more information about VSYS, see Virtual System.
- The backup authentication server should not nest another backup authentication server.
- Before deleting an AAA server, make sure the server is not specified as a backup authentication server.
- If an LDAP server is configured with backup server 1 (**backup1**), backup server 2 (**backup2**) and backup authentication server (**backup-aaa-server**), when user' s authentication request is not responded on the primary server, the system will re-authenticate the user in the following order: backup server 1 -> backup server 2 -> backup authentication server; when user' s authentication failed on the primary server, the system will re-authenticate the user in the following order: backup server 1 -> backup server 2 -> backup authentication server.

Configuring TACACS+ Authentication Server

Unser global mode, use the command aaa-server aaa-server-name type tacacs+ to enter TACACAS+ server configuration mode.

Configuration of TACACS+ server includes:

- Configuring IP or Domain Name of Primary Authentication Server
- Configuring IP or Domain Name of Backup Server 1
- Configuring IP or Domain Name of Backup Server 2
- Configuring Port of TACACS+ Server
- Configuring Secret of TACACS+ Server
- Configuring Role Mapping Rule

Configuring IP or Domain Name of Primary Authentication Server

To configure the IP address or domain name of TACACS+ authentication server, under TACACS+ server configuration mode, use the command below:

host {*ip-address* | *host-name* }[**vrouter** *vrouter-name*]

- *ip-address* | *host-name* – Specify the IP address or domain name of the current primary TACACS+ server.
- **vrouter** *vrouter-name* – Specify the VRouter which the current TACACS+ server belongs to. The default VR is trust-vr.

Under TACACS+ server configuration mode, use the no command to delete its IP or domain name configuraiton :

no host

Configuring IP Address or Domain Name of Backup Server 1

This configuration is optional. Backup server must be of the same type of primary server. When the authentication does not pass primary server’ s check, the backup server 1 and 2 will start checking its credentials consecuritvely.To configure the IP address or domain name of the backup authentication server 1, in the TACACS+ server configuration mode, use the following command:

backup1 {*ip-address* | *host-name* }[**vrouter** *vrouter-name*]

- *ip-address* | *host-name* – Specifies the IP address or domain name of the backup authentication server 1.
- **vrouter** *vrouter-name* – Specifies the VRouter that the backup server belongs to. The default VRouter is trust-vr.

To cancel the IP address or domain name configuration of the backup authentication server 1, in the TACACS+ server configuration mode, use the command:

no backup1

Configuring IP Address or Domain Name of Backup Server 2

This configuration is optional. Backup server must be of the same type of primary server. When the authentication does not pass primary server’ s check, the backup server 1 and 2 will start checking its credentials consecuritvely.To configure the IP address or domain name of the backup authentication server 1, in the TACACS+ server configuration mode, use the following command:

backup2 {*ip-address* | *host-name* }[**vrouter** *vrouter-name*]

- *ip-address* | *host-name* – Specifies the IP address or domain name of the backup authentication server 2.
- **vrouter** *vrouter-name* – Specifies the VRouter that the backup server belongs to. The default VRouter is trust-vr.

To cancel the IP address or domain name configuration of the backup authentication server 1, in the TACACS+ server configuration mode, use the command:

no backup2

Configuring Port Number of TACACS+ Server

To configure the port number of the TACACS+ server, in its TACACS+ server configuration mode, use the following command:

port *port-number*

- *port-number* – Specifies the port number of the LDAP server. The default value is 49.

To restore to the default value, in the TACACS+ server configuration mode, use the command:

no port

Configuring Secret of TACACS+ Server

To configure the secret of TACACS+ server, under TACACS+ server configuration mode, use the command below:

secret *secret*

- *secret* – Specifies the secret string of TACACS+ server. The range is 1 to 31 characters.

To delete secret, under TACACS+ server configuration mode, use the no command:

no secret

Specifying Role Mapping Rule

The role mapping rule can allocate a role for the authenticated users in this server.

To assign a role mapping rule to users in TACACS+ server, under TACACS+ server configuration mode, use the command below:

```
role-mapping-rule rule-name
```

- *rule-name* – Enter an existing role mapping rule name.

To cancel this rule, under TACACS+ server configuration mode, use the command:

```
no role-mapping-rule
```

Configuring TACACS+ Server

TACACS+ server should also be configured if it wants to communicate with FSOS system. The configuration is to add some user defined attributes.

You should make the following changes in TACACS+ server:

- For tac_plus in Linux: add FS attributes, seet the table below:
- For Cisco acs 4.2 and above:add new server with name “fs” and edit the service attributes to include fs characters, see table below:

Attribute	Description
user-type	User type. admin type=16 all=31 Other types of user do not need this value.
user-vsys-id	vSYS ID value. Admin user must have this attribute. Now, only ID=0 is supported.
user-admin-privilege	Read and Write privilege. Read and write=4294967295 Only read=0

Attribute	Description
user-admin-role	Administrator role privilege. admin＝Permission for reading, executing and writing. This role has the authority over all features. You can view the current or historical configuration information. operator＝Permission for reading, executing and writing. You have the authority over all features except modify the Administrator's configuration, view the current or historical configuration information , but no permission for check the log information. auditor＝You can only operate on the log information, including view, export and clear. admin-read-only＝ Permission for reading and executing. You can view the current or historical configuration information. Note: This attribute property is higher than **user-admin-privilege**. If the two attributes are configured at the same time, the **user-admin-role** will take effect. You are suggested to use **user-admin-role** directly.
user-login-type	Admin login type. telnet＝2 SSH＝4 CONSOLE＝1 HTTP＝8 HTTPS＝16 all＝31 If you want a combination, the value should the total of selected types (e.g. telnet+SSH＝6).
user-group	This attribute is optional. It defines the user group of the specified user. User group is for user group based policy control.

Configuring a RADIUS Accounting Server

FS devices support accounting for authenticated users via a RADIUS server. To enter the RADIUS server configuration mode, in the global configuration mode, use the command **aaa-server** *aaa-server-name* **type radius**.

The RADIUS accounting server configuration includes:

- Enabling/Disabling the accounting function
- Configuring the IP address or domain name of the primary/backup server
- Configuring the port number
- Configuring the Secret

Enabling/Disabling the Accounting Function

To enable/disable the accounting function of the RADIUS server, in the RADIUS server configuration mode, use the following commands:

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

After enabling the accounting function, you can continue to configure other parameters.

Configuring the IP Address or Domain Name of the Primary/Backup Server

To configure the IP address or domain name of the primary or backup accounting server, in the RADIUS server configuration mode, use the following command:

accounting {**host** {*ip-address* | *host-name*} | **backup1** {*ip-address* | *host-name*} | **backup2** {*ip-address* | *host-name*}}

- **host** {*ip-address* | *host-name*} – Specifies the IP address or domain name of the primary server.
- **backup1** {*ip-address* | *host-name*} – Specifies the IP address or domain name of the backup server 1.
- **backup2** {*ip-address* | *host-name*} – Specifies the IP address or domain name of the backup server 2.

To cancel the IP address or domain name configuration of the primary or backup server, in the RADIUS server configuration mode, use the command:

```
no accounting {host | backup1 | backup2}
```

Configuring the Port Number

To configure the port number of the accounting server, in the RADIUS server configuration mode, use the following command:

accounting port *port-number*

- *port-number* − Specifies the port number of the accounting server. The value range is 1024 to 65535. The default value is 1813.

To restore to the default value of the port number, in the RADIUS server configuration mode, use the command:

```
no accounting port
```

Configuring the Secret

To configure the secret of the accounting server, in the RADIUS server configuration mode, use the following command:

accounting secret *secret*

- *secret* − Specifies the secret string of the accounting server. The length is 1 to 31 characters.

To cancel the secret configuration of the accounting server, in the RADIUS server configuration mode, use the command:

```
no accounting secret
```

Enabling/Disabling the Offline Management of Accounting User

After the offline management of accouting user is enabled,the system will disconnect from the specified offline user and stop charging according to the offline user information on the Radius server (including the name of the offline user, the IP address of the offline user, the accounting ID). By default, the function is disabled.

To enable the offline management of accouting user, in the RADIUS server configuration mode, use the following command:

```
unsolicited-message enable
```

To disable the offline management of accouting user, in the RADIUS server configuration mode, use the following command:

```
no unsolicited-message enable
```

Specifying an Authentication Server for the System Administrator

After configuring the AAA authentication server, you need to specify one as the authentication server for the system administrator. By default, the server named local is the default authentication server and cannot be deleted. To specify the authentication server for the system administrator, in the global configuration mode, use the following command:

admin auth-server *server-name*

- *server-name* - Specifies the name of the authentication server.

To restore to the default authentication server, in the global configuration mode, use the command **no admin auth-server**.

If the external authentication server configured is not reachable or the authentication service is not available, the system will use the server named Local as the authentication server. For Radius servers, you can disable Local, i.e., forbid to use Local for authentication when the specified Radius server is not reachable or the authentication service is not available.

To disable/enable Local for Radius servers, in the global configuration mode, use the following commands:

- Disable: **admin auth-server** *radius-server-name* **disable-retry-local**
- Enable: **admin auth-server** *radius-server-name*

Viewing Local Server Authentication Enabled Status

To view the local server authentication enabled status, in any mode ,use the following command:

show admin console local-auth-prior

Viewing and Debugging AAA

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

show aaa-server [*server-name*]

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

show user-black-list

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

debug aaa [**accounting** | **authentication** | **authorization** | **internal** | **radius** | **ldap** | **user**]

- **accounting** - Shows debug information for accounting.
- **authentication** - Shows debug information for authentication.

- **authorization** - Shows debug information for authorization.
- **internal** - Shows debug information when local users access to the device via local authentication.
- **radius** - Shows debug information for the RADIUS authentication.
- **ldap** - Shows debug information for the LDAP (including Active-Directory server and LDAP server) authentication.
- **user** － Shows debug information when the local user attributes change.

RADIUS Packet Monitoring

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.

Enabling/Disabling the RADIUS Packet Monitoring Function

The interfaces bound to the Tap zone support the RADIUS packet monitoring function. By default, the function is disabled. To enable the RADIUS packet monitoring function, use the following command in the bypass interface configuration mode:

radius-snooping

To disable this function, use the following command:

no radius-snooping

Note: The interfaces with the RADIUS packet monitoring function enabled must be bound to the Tap zone.

Configuring the Timeout Value

If the device does not receive the mirrored RADIUS packets within the specified timeout value, it will delete the mappings between the usernames and the IP addresses. To configure the timeout value, use the following command in the global configuration mode:

radius-snooping-user timeout *time-value*

- *time-value* － Specifies the timeout value (in seconds). The value ranges from 180 to 86400. The default value is 300.

To restore the timeout value to the default one, use the following command:

```
no radius-snooping-user timeout
```

Deleting the User Information

To delete the mappings between the usernames and the IP addresses that are recorded on the device, use the following command in the execution mode:

```
exec radius kickout user-name
```

- *user-name* – Specifies the username whose information you want to delete.

Viewing the Configuration Information

To view the configuration information of the RADIUS packet monitoring function, use the following command in any mode:

```
show radius-snooping configuration
```

Viewing the User Information

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

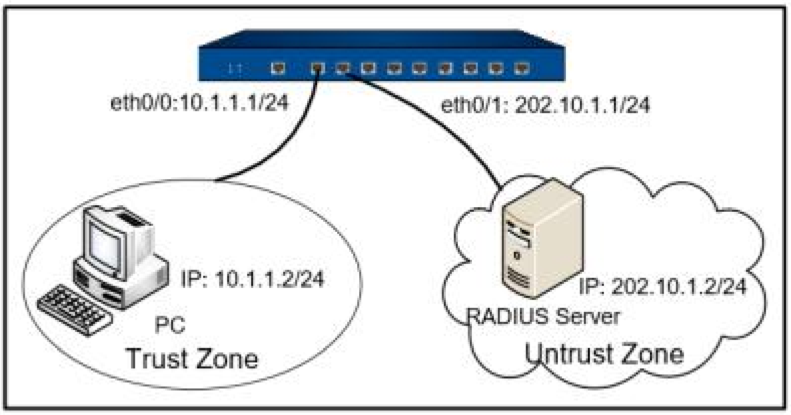
```
show auth-user radius-snooping [interface interface-name | vrouter vrouter-name | slot slot-no]
```

Configuration Example

This example shows how to use the external RADIUS authentication server to authenticate Telnet users. Specific requirements and configurations are described as below.

Requirement

The goal is to authenticate the Telnet users via RADIUS server. IP address of the RADIUS authentication server is 202.10.1.2, and there is no back-up server. The retry time is the default value 3. The response timeout is the default value 3. Port 1812 is used for RADIUS authentication. The figure below shows the networking topology.



Configuration Steps

Step 1: Configure the interface

```
hostname# configure
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# manage telnet
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 10.1.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 202.10.1.1/24
```

Step 2: Enter the AAA server configuration mode

```
hostname(config-aaa-server)# aaa-server rad type radius
```

Step 3: Configure the RADIUS authentication server

```
hostname(config-aaa-server)# host 202.10.1.2
hostname(config-aaa-server)# port 1645
hostname(config-aaa-server)# secret testing123
hostname(config-aaa-server)# exit
```

Step 4: Specify the authentication server for the system

```
hostname(config)# admin auth-server radius
```

Step 5: Verify the results of the configuration

```
hostname(config)# show aaa-server radius
============================================================
==
aaa-server: radius
type: radius
```

```
role-mapping-rule :

backup-aaa-server :

server address: 202.10.1.2(trust-vr)

first backup :

second backup :

radius setting:

port: 1812 secret: a3UfKjOGP80IGeggG9kuvDJ7I8Ye

retries 3 time(s), timeout 3 second(s).

accounting: enable (optional)

accounting setting:

port: 2000 secret: hq8DNiGMUL4Pq2A9tf1422uLRWcF

server address: 202.10.1.2(trust-vr)

first backup :

second backup :

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

User Identification

Overview

System supports various methods of user identification, which is used to authenticate users who access the Internet via the device.

Web Authentication

After the Web authentication (WebAuth) is configured, when you open a browser to access the Internet, the page will redirect to the WebAuth login page. According to different authentication modes, you need to provide corresponded authentication information. With the successful Web authentication, system will allocate the role for IP address according to the policy configuration, which provides a role-based access control method.

If you use HTTPS request to trigger WebAuth, it only supports unilateral SSL proxy. System will enable the SSL connection during the authentication. After the authentication is completed, SSL proxy will be invalid. The client and server communicate directly without SSL encryption.

In addition, system supports customizing WebAuth page. For more information, refer to Customizing WebAuth Login Pages.

Entering the WebAuth Configuration Mode

To enter the WebAuth configuration mode, in the global configuration mode, use the following command:

```
webauth
```

Enabling/Disabling WebAuth

By default, the WebAuth is disabled. To enable the WebAuth function, in the WebAuth configuration mode, use the following commands:

```
enable
```

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

```
disable
```

Configuring the WebAuth Mode

The WebAuth includes the following mode:

- Password Authentication: Using username and password during the Web authentication.

Configuring the Authentication Mode

To configure the authentication mode, in the WebAuth configuration mode, use the following command:

```
mode { password}
```

- password – Specifies the password authentication mode as the authentication mode.

To restore to the default password authentication mode, in the WebAuth configuration mode, use the following command:

```
no mode
```

Configuring the Protocol Type of Authentication

System supports HTTP and HTTPS. HTTP mode is faster, and HTTPS mode is more secure. To configure the protocol type, in the WebAuth configuration mode, use the following command:

```
protocol {http | https}
```

- http | https – Specifies the protocol type, HTTP or HTTPS.

To restore to the default HTTP protocol type, in the WebAuth configuration mode, use the following command:

```
no protocol
```

Specifying the WebAuth Global Default Configuration of Interface

After the WebAuth function is enabled, the WebAuth function of all interfaces is disabled by default. To specify the Webauth global default configuration of the interface, in the WebAuth configuration mode, use the following command:

```
interface global-default {enable | disable}
```

- enable – Specifies that the WebAuth function of all interfaces is enabled by default.
- disable – Specifies that the WebAuth function of all interfaces is disabled by default .

Tip: For more information about configuring the WebAuth of interface, refer to Enabling/Disabling the WebAuth of Interface.

Configuring the Port Number

To configure the HTTP or HTTPS port number for the authentication server, in the WebAuth configuration mode, use the following commands:

http-port *port-number*

- *port-number* – Specifies the HTTP port number. The value range is 1 to 65535. The default value is 8181.

https-port *port-number*

- *port-number* – Specifies the HTTPS port number. The value range is 1 to 65535. The default value is 44433.

To restore to the default value of the HTTP or HTTPS port number, in the WebAuth configuration mode, use the following commands:

```
no http-port
no https-port
```

Note:HTTP port number and HTTPS port number should be different.

Specifying HTTP Proxy Server Port

After enabling the Web authentication, the device will authenticate the HTTP request whose destination port is 80. When the HTTP traffic of accessing network needs to have a proxy by the HTTP proxy server, you need to specify the HTTP proxy server port in the device. Then, the device can authenticate the HTTP request sent to the proxy server.

To specify the HTTP proxy server port, in the WebAuth configuration mode, use the following command:

proxy-port *port-number*

- *port-number* – Specify the port that the HTTP proxy server used for the HTTP request proxy. The value ranges from 1 to 65535.

Use the **no proxy-port** command to cancel the HTTP proxy server port settings. The device will authenticate the HTTP request whose destination port is 80.

After enabling the Web authentication function and specifying the HTTP proxy server port, each user must add the IP address of the device to the **Exceptions** list in the **Proxy Settings** in the Web browser. With this operation, the Web authentication can be performed.

Configuring the HTTPS Trust Domain

To configure the HTTPS trust domain name, in the WebAuth configuration mode, use the following command:

https-trust-domain *trust-domain-name*

- *trust-domain-name* – Specifies the name of the HTTPS trust domain. Before executing this command, this new PKI trust domain must have been added into system, and you should make sure that the local certificate purchased from the certificate authority has been imported into it. By default, HTTPS trust domain is trust_domain_default, which will result in the untrusted certificate warning.

To restore to the default HTTPS trust domain trust_domain_default, in the WebAuth configuration mode, use the following command:

no https-trust-domain

Specifying the Address Type

By default, the address type of authentication user is IP address. To specify the address type of authentication user, in the WebAuth configuration mode, use the following command:

address-type {ip | mac}

- **ip** – Specifies IP address as the address type of authentication user.

- **mac** – Specifies MAC address as the address type of authentication user. The device needs to be deployed in the same Layer 2 network environment with the client. Otherwise, system will fail to get the MAC address of the client or get the incorrect MAC address.

To restore to the default address type, in the WebAuth configuration mode, use the following command:

```
no address-type
```

Configuring Multi-logon Function

By default, the multi-logon function is disabled. If it is enabled, you can log into multiple clients using the same username simultaneously. To enable the multi-logon function, in the WebAuth configuration mode, use the following command:

```
multi-logon
```

After executing this command, the multi-logon function is enabled, and the number of clients using one username is limited. To specify the number of clients, in the WebAuth configuration mode, use the following command:

multi-logon *number*

- *number* – Specifies how many times the same username can be logged in simultaneously. The value range is 2 to 1000 times.

To disable this function, in the WebAuth configuration mode, use the command:

```
no multi-logon
```

Configuring Auto-kickout Function

The auto-kickout function means that only one user is allowed to login on one client. When the same user logs in again, according to the configuration, system will kick out the registered user or prevent the same user from logging in again.

Kicking out the registered user, that is, the system will disconnect the original connection and use the new logon information to replace the original logon information. To kick out the registered user, in the WebAuth configuration mode, use the following commands:

```
auto-kickout
```

To prevent the same user from logging in again, in the WebAuth configuration mode, use the following commands:

```
no auto-kickout
```

Enabling/Disabling Proactive WebAuth

You can enable the proactive WebAuth under L3 interface of device. After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port numbe is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http:// 192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https:// 192.168.3.1:44434 certification.

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

webauth aaa-server *aaa-server-name*

- *aaa-server-name* – Specifies the name of the configured AAA server.

To disable the proactive WebAuth function, in the interface configuration mode, use the following command:

no webauth aaa-server

Note:

- When enable proactive WebAuth in L3 interface, you need to ensure that the system's WebAuth function is enabled, otherwise it will not work.
- If the HTTP/HTTPS port of the authentication server is respectively configured as the protocol’ s default port 80/443, the port number of the authentication address can be omitted.

Enabling/Disabling the WebAuth of Interface

After the WebAuth function is enabled, the WebAuth function of all interfaces is disabled by default. To enable the WebAuth function of the specified interface, in the interface configuration mode, use the following command:

webauth enable

To disable the WebAuth function of the specified interface, in the interface configuration mode, use the following command:

webauth disable

To specify that the interface uses the global default configuration of WebAuth, in the interface configuration mode, use the following command:

webauth global-default

Tip:

- It is recommended to use the command after the WebAuth is enabled, otherwise the configuration is invalid.
- For more information about WebAuth global default configuration, see Specifying the WebAuth Global Default Configuration of Interface.

Disconnecting a User

You can disconnect a specific user from a WebAuth system by CLI. To disconnect a user, in any mode, use the following command:

exec user-mapping webauth { **password**} **kickout** {{**ip** *ip-address*| **mac** *mac-address*} **vrouter** *vrouter* | **username** *username* { **auth-server** *auth-server-name*}}

- *ip-address* – Specifies the IP address of the WebAuth user.
- *mac-address* – Specifies the MAC address of the WebAuth user.
- *vrouter* – Specifies the VRouter of the WebAuth user.
- *username* – Specifies the name of the WebAuth user.
- *auth-server-name* – Specifies the authentication server name of the WebAuth user.

Note: You need to specify the VRouter or the authentication server to avoid disconnecting too many users with the same name from the WebAuth system.

Allowing Password Change by Local Users

Local users can change their password on the login page after successful authentication. By default, this function is disabled. To enable or disable password change by local users, in the local sever configuration mode, use the following commands:

- Enable: **allow-pwd-change**
- Disable: **no allow-pwd-change**

To change the login password, local users can take the following steps:

1. Enter the correct username and password on the WebAuth login page, and then click **Login**.
2. After successful login, click **Modify** on the login page.

3. In the password change dialog, type the correct old password into the **Old password** box, type the new password into the **New password** box, and then type the new password again into the **Confirm New password** box to make confirmation.

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

Configuring a Policy Rule for WebAuth

You should configure corresponding policy rules to make WebAuth take effect. To configure WebAuth parameters for a policy rule, in the policy rule configuration mode, use the following commands:

Specify the role: **role unknown**

Specify the action and authentication server for WebAuth:

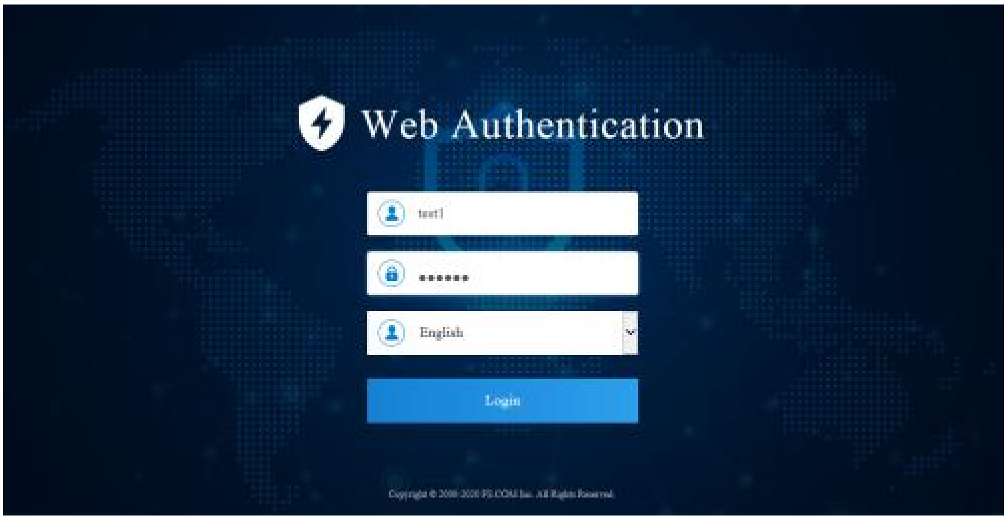
action webauth *aaa-server-name*

- *aaa-server-name* – Specifies the authentication server which is a configured AAA authentication server in the system.

Tip: For information about how to configure a policy rule, see Policy.

Customizing WebAuth Login Pages

The system supports the customizing WebAuth login page function. After WebAuth is enabled, the default login page is shown as the figure below:



test1

••••••

English

Customizing the Login Page

You can customize the WebAuth login page by downloading the zip file and modifying the contents. To import the modified zip file you need to the system, in the execution mode, use the following command:

import customize webauth from {**ftp server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] | **tftp server** *ip-address* [**vrouter** *vrouter-name*]} *file-name*

- **ftp server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] – Specify to get the zip file from the FTP server, and configure the IP address, VRouter, username and password of the server. If the username and password are not specified, you will login anonymously by default.

- **tftp server** *ip-address* [**vrouter** *vrouter-name*] – Specify to get the zip file from the TFTP server, and configure the IP address and VRouter of the server.

- *file-name* – Specify the name of the zip file.

To restore to the default WebAuth login page, in any mode, use the following command:

exec customize webauth default

Note:

- After upgrading the previous version to the 5.5 version, the WebAuth login page you already specified will be invalid and restored to the default page. You should re-download the template after the version upgrade and customize the login page.

- After upgrading the system version, you should re-download the template, modify the source file, and then upload the custom page compression package. If the uploaded package version is not consistent with the current system version, the function of the custom login page will not be used normally.

- The zip file should comply with the following requirements: the file format should be zip; the maximum number of the file in the zip file is 50; the upper limit of the zip file is 1M; the zip file should contain "index.html".

- System can only save one file of the default template page and the customized page. When you upload the new customized page file, the old file will be covered. It is suggested to back up the old file.

- When you modify the zip file, see "readme_cn.md" file or "readme_en.md" file.

Exporting the Login Page

To export the default modified zip file, in the execution mode, use the following command:

export webauth default-page to {**ftp server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] | **tftp server** *ip-address* [**vrouter** *vrouter-name*]} *file-name*

- **ftp server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] – Specify to export the zip file to the FTP server, and configure the IP address, VRouter, username and password of the server. If the username and password are not specified, you will login anonymously by default.

- **tftp server** *ip-address* [**vrouter** *vrouter-name*] – Specify to export the zip file to the TFTP server, and configure the IP address and VRouter of the server.
- *file-name* – Specify the name of the zip file.

Password Authentication

To enable password authentication, in the WebAuth configuration mode, use the following command:

```
mode password
```

Configuring the Re-auth Interval

System can re-authenticate a user after a successful authentication. By default, the re-authentication function is inactive. To configure the re-authenticate interval, in the WebAuth configuration mode, use the following command:

password reauth-interval {*time* | **disable**}

- *time* – Specifies the interval to re-authenticate a user. The value range is 10 to 60*24 minutes.
- **disable** – Disables the re-auth function.

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

```
no password reauth-interval
```

Configuring the Redirect URL Function

The redirect URL function redirects the client to the specified URL after successful authentication. You need to turn off the pop-up blocker of your web browser to ensure this function can work properly. To configure the redirect URL function, in the WebAuth configuration mode, use the following command:

password popup-url *url*

- *url* – Specifies the redirect URL. The length is 1 to 127 characters. The format of URL should be "http://www.abc.com" or "https://www.abc.com".

To delete the redirect URL configuration, in the WebAuth configuration mode, use the command:

```
no password popup-url
```

Note:

- You can specify the username and password in the URL address. When the specified redirect URL is the application system page with the authentication needed in the intranet, you do not need the repeat authentication and can access the application system.

- The corresponding keywords are $USER, $PWD, or $HASHPWD. Generally, you can select one keyword between $PWD and $HASHPWD. The formart of the URL is "URL" +" username=$USER&password=$PWD".
- When entering the redirect URL in CLI, add double quotations to the URL address if the URL address contains question mark. For example, "http://192.10.5.201/oa/login.do?username=$USER&password=$HASHPWD"

Configuring the Forced Timeout Value

If the forced timeout function is enabled, users must re-login after the configured interval ends. By default, the forced re-login function is disabled. To configure the forced timeout value, in the WebAuth configuration mode, use the following command:

password force-timeout {*timeout-value* | **disable**}

- *timeout-value* - Specifies the forced timeout value. The value range is 10 to 60*24*100 minutes.
- **disable** – Disables the forced timeout function, that is , system does not force the user to login again.

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

no password force-timeout

Configuring the Idle Timeout Value

If there is no traffic during a specified time period after the successful authentication, the system will disconnect the connection. By default, the system will not disconnect the connection if there is no traffic after the successful authentication. To specify the idle timeout value, namely the idle time, use the following command in the WebAuth configuration mode:

password idle-timeout {*timeout* | **disable**}

- *timeout* – Specifies the idle timeout value (in minutes). The value range is 1 to 60*24 minutes.
- **disable** – Disables the idle timeout function, which indicates that system will not disconnect the connection if there is no traffic after the successful authentication.

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

no password idle-timeout

Note:

- If you pass the web authentication by using the mobile phones running on iOS or Android, enable this function and specify the idle time. Then the mobile phones can keep online when they generate traffic.

Configuring the Heartbeat Timeout Value

When authentication is successful, the system will automatically refresh the login page before the configured timeout value ends in order to maintain the login status. If configuring the idle time at the same time,you will log off from the system at the smaller value.To configure the heartbeat timeout value, in the WebAuth configuration mode, use the following command:

```
password heartbeat-timeout {interval | disable}
```

- *interval* – Specifies the heartbeat timeout value. The value range is 1 to 60*24*100 minutes. The default value is 10 minutes.
- disable – Disables the heartbeat timeout function.

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

```
no password heartbeat-timeout
```

Single Sign-On

When the user authenticates successfully for one time, system will obtain the user's authentication information. Then the user can access the Internet without authentication later.

SSO can be realized through three methods, which are independent from each other, and they all can achieve the "no-sign-on"(don't need to enter user name and password) authentication.

Configuring AD Scripting for SSO

With the Single Sign-on (SSO) agent function enabled, users will automatic pass the authentication after they pass the Active-Directory authentication.

To use the AD Scripting function, you should firstly add the script program named LogonScript.exe, which is provided by FS, to the logon/logout script of the Active-Directory server.

Entering the AD Scripting Configuration Mode

To enter the AD-Scripting configuration mode, use the following command in the global configuration mode:

```
user-sso server ad-scripting default
```

Enabling the AD Scripting Function

By default, the AD Scripting function is disabled. To enable this function, use the following command in the AD-Scripting configuration mode:

```
enable
```

To disable the function, use the following command:

```
no enable
```

Specifying the AAA Server

To specify the AAA server referenced by system, use the following command in the sso-agent configuration mode:

aaa-server *aaa-server-name*

- *aaa-server-name* – Specifies the name of the AAA server. The Local, AD or LDAP server is available to select on the AAA server. You' re suggested to directly select the configured authentication AD server. After selecting the AAA server, system can query the corresponding user group and role of the online user on the referenced AAA server, so as to achieve the policy control based on the user group and role.

To cancel the above configurations, use the following command in the AD-Scripting configuration mode:

```
no aaa-server
```

Configuring the Idle Time

If there is no traffic during a specified time period after the successful authentication, system will delete the user authentication information. To specify the time period, namely the idle time, use the following command in the AD Scripting configuration mode:

idle-timeout *timeout*

- *timeout* – Specifies the idle time (in minutes). The value ranges from 1 to 1440.

By default, system will not delete the user authentication information if there is no traffic.To restore the idle time to the default value, use the following command in the global configuration mode:

```
no idle-timeout
```

Configuring Simultaneously Online Settings

By default, if a user logs on again after hi or her successful logon, the system will disconnect the original connection and use the new logon information to replace the original logon information. Thus, users with the same credentials cannot be online simultaneously. If you want users with the same credentials to be online simultaneously, you can use the following commands in the AD-Scripting configuration mode:

no auto-kickout

To restore the settings to the default, use the following command in the AD-Scripting configuration mode:

auto-kickout

Viewing Configuration Information

To view the configuration information of the AD Scripting function, use the following command in any mode:

show user-sso server ad-scripting default

Viewing the User Mapping Information

To view the mapping information between user name and IP of AD Scripting, in any mode, use the following command:

show user-mapping user-sso ad-scripting default

Viewing the Authenticated User Table

The user authentication information are stored in the authenticated user table. To view the user authentication information, use the following command in any mode:

show auth-user ad-scripting

Deleting the User Mapping Information

To delete the user mapping information of the specified IP, in any mode, use the following command:

exec user-mappping user-sso ad-scripting kickout ip *ip-address* **vrouter** *vrouter-name*

Configuring SSO Radius for SSO

Receiving Radius Accounting Packets

The device can receive the accounting packets that based on the Radius standard protocol, and then perform the following actions according to the content of the packets:

- Generate user authentication information and add them to the authenticated user table.
- Reset the timeout value of the authenticated user.

- Delete the authenticated user from the table.

To enable the function above, take the following steps:

To enter the SSO-Radius configuration mode, in the global configuration mode, use the following command:

```
user-sso server sso-radius default
```

In the SSO-Radius configuration mode, use the following command:

```
enable
```

To disable the function, in the SSO-Radius configuration mode, use the following command:

```
no enable
```

Specifying the AAA Server

Specify the AAA server that user belongs to. To specify the AAA server, in the SSO-Radius configuration mode, use the following command:

aaa-server *aaa-server-name*

- *aaa-server-name* – Specifies the name of the AAA server. You can select Local, AD or LDAP server on the AAA server. After selecting the AAA server, system can query the corresponding user group and role information of the online user on the referenced AAA server, so as to realize the policy control based on the user group and role.

To delete the AAA server, in the SSO-Radius configuration mode, use the following command:

```
no aaa-server
```

Specifying the Port Number for Receiving Radius Packets

To specify the port number for receiving Radius packets (Don’t configure port in non-root VSYS), in the SSO-Radius configuration mode, use the following command:

port *port*

- *port* – Specifies the port number. The range is 1 to 65535. The default port is 1813.

Use the **no port** command to restore the port number to default.

Configuring the Radius Client

Specify the IP address of the Radius client. You can specify up to 8 clients. To specify the IP address of the Radius clients and enter the Radius client configuration mode, in the SSO-Radius configuration mode, use the following command:

client {**any** | *A.B.C.D*}

- **any** – Receive the packets sent from any Radius client.
- *A.B.C.D* – Receive the packets sent from the Radius Client with specified IP address.

To delete the configured Radius client, in the global configuration mode, use the **no client** {**any** | *A.B.C.D*} command.

Configuring the Shared Secret

System will verify the packet by the shared secret key, and parse the packet after verifying successfully. If system fails to verify the packet, the packet will be dropped. The packet can be verified successfully only when SSO Radius client is configured the same shared secret key with system or both of them aren't configured a shared secret key.. To configure the shared secret key, in the Radius client configuration mode, use the following command:

shared-secret *key-value*

- *key-value* – Specifies the shared secret key. The length range is from 1 to 31 characters.

To delete the shared secret key, use the **no shared-secret** command.

Configuring the Idle Interval

Idle interval is used to configure the effective time for user authentication information of Radius packets in the device. If there' s no update or delete packet of the user during the idle interval, the device will delete the user authentication information.

To configure the idle interval, in the Radius client configuration mode, use the following command:

timeout *timeout-value*

- *timeout-value* – Specifies the timeout value. The unit is minute. The default value is 30. 0 means it will never timeout.

To restore the idle interval to default, use the **no timeout** command.

Viewing the SSO Radius Configuration Information

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

show user-sso server sso-radius default

Viewing the User Mapping Information

To view the mapping information between the user name and IP of SSO Radius, in any mode, use the following command:

show user-mapping user-sso sso-radius default

Viewing the Authentication User Table

The user authentication information generated by the device is saved in the authentication user table. In any mode, use the following command:

show auth-user sso-radius

Deleting the User Mapping Information

To delete the user mapping information of the specified IP, in any mode, use the following command:

exec user-mappping user-sso sso-radius kickout ip *ip-address* **vrouter** *vrouter-name*

Portal Authentication

The portal authentication function identifies and authenticates the users when they want to access the Internet via the device. After configuring the portal authentication function, the HTTP requests will be redirected to the specified authentication page of the portal server. In this page, you can visit free resources. If you want to access the other resources in the Internet, provide your username and password in this page. After passing the portal authentication successfully, the system will assign a role to the user’s IP address according to the policy configuration. And assigning a role can control the resource that the IP address can access.

The portal server is configured by the third party and it receives the portal authentication requests, identifies and authenticates the users, exchanges the authentication information with the device.

Configuring portal authentication involves the configurations in the following modules:

- Configure interfaces, zones, and role mapping rules.
- Configure the security agent function and the authentication information exchange with the portal server.
- Create policy rules to define the traffic that will be authenticated, and trigger the portal authentication function.

This section introduces how to define the traffic that will be authenticated, and how the policy rule triggers the function.

Note:

- For more information on security agent function, see Configuring the Security Agent.
- For more information on the third-party portal authentication server, see the third-party user guide.

Configuring a Policy Rule that Triggers the Portal Authentication

To trigger the portal authentication function, you must configure the corresponding policy rule. In the global configuration mode, use the following command:

rule [**role** {**UNKNOWN** | *role-name*} | **user** *aaa-server-name user-name* | **user-group** *aaa-server-name user-group-name*] **from** *src-addr* **to** *dst-addr* **service** *service-name* **application** *app-name* {**permit** | **deny** | **tunnel** *tunnel-name* | **fromtunnel** *tunnel-name* | **webauth** | **portal-server** *portal-server-url*}

action portal-server *portal-server-url*

- *portal-server-url* – Use the portal authentication to the traffic that matches the policy rule and enter the URL of the portal server. The URL can contain up to 63 characters and the format is http://www.acertainurl.com or https://www.acertainurl.com.

Besides, you must specify the other required information in this command to define the traffic that will be authenticated. For more information, see Configuring a Policy Rule in Policy.

Example of Configuring WebAuth

Example of Configuring HTTP WebAuth

In this example, WebAuth user access control is demonstrated. It allows only user1 who is authenticated using WebAuth to access the Internet. All other accesses are denied. The WebAuth server is the local AAA server named local.

Step 1: Configure the user, role and role mapping rule

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

hostname(config-aaa-server)# user-group usergroup1

hostname(config-user-group)# exit

hostname(config-aaa-server)# user user1

hostname(config-user)# password test1

hostname(config-user)# group usergroup1

hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)# role role1
hostname(config)# role-mapping-rule role-mapping1
hostname(config-role-mapping)# match user-group usergroup1 role role1
hostname(config-role-mapping)# exit
hostname(config)#
```

Step 2: Specify the role mapping rule for the local authentication server

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# role-mapping-rule role-mapping1
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 3: Configure interfaces and security zones

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.1/16
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/10
hostname(config-if-eth0/10)# zone untrust
hostname(config-if-eth0/10)# ip address 66.1.200.1/16
hostname(config-if-eth0/10)# exit
hostname(config)#
```

Step 4: Enable WebAuth function

```
hostname(config)# webauth
hostname(config-webauth)# enable
hostname(config-webauth)# protocal http
hostname(config-webauth)# exit
hostname(config)# policy-global
hostname(config-policy)# rule from any to any from-zone trust to-zone untrust service dns permit
hostname(config-policy)# rule role UNKNOWN from 192.168.1.1/16 to any service any webauth local
Rule id 4 is created
hostname(config-policy)# exit
hostname(config)#
```

Step 5: Configure policy rules

```
hostname(config)# policy-global
hostname(config-policy)# rule role role1 from 192.168.1.1/16 to any from-zone trust to-zone untrust service any permit
hostname(config-policy)# exit
hostname(config)#
```

After above configurations, the system will authenticate all HTTP requests (external IP addresses with reachable route) from 192.168.1.1/16. Users can access the Internet after providing the username user1 and password test1 on the login page.

Example of Configuring SSO

Example of Configuring AD Scripting for SSO

This section describes a typical AD Scripting example. After the configuration, you can be authenticated by the device if only you have been authenticated by the Active Directory server.

The following steps only describe configurations related to AAA Server and AD Scripting, and omit other configurations.

Step 1: Configure an AAA server of Active-Directory type

```
hostname(config)# aaa-server ad type active-directroy
hostname(config-aaa-server)# host 1.1.1.1
hostname(config-aaa-server)# base-dn dc=fs
hostname(config-aaa-server)# login-dn cn=user,dc=fs
hostname(config-aaa-server)# login-password admin

hostname(config-aaa-server)# exit

hostname(config)#
```

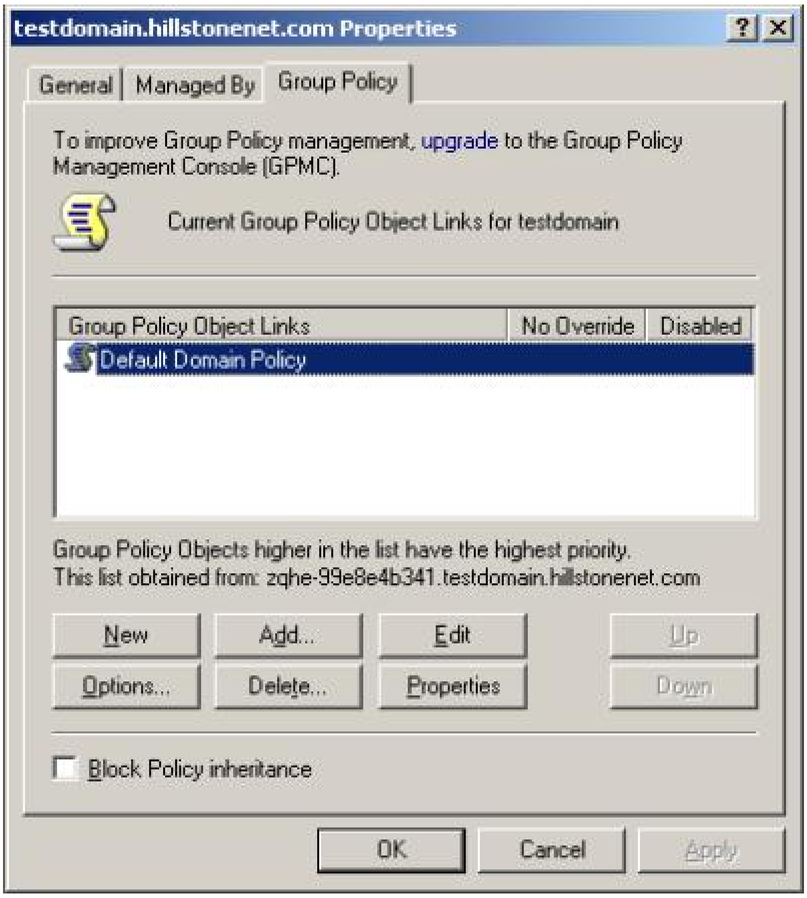
Step 2: Configure the AD Scripting

```
hostname(config)# user-sso server ad-scripting default

hostname(config-ad-scripting)# enable

hostname(config-ad-scripting)# aaa-server ad

hostname(config-ad-scripting)# exit

hostname(config)#
```

Step 3: In the Active-Directory server, import the logon/logout script

1. Visit FS.COM or contact related sales staff to get the script "Logonscript.exe".
2. In AD server, go to Start menu, select **Mangement Tools> Active Directory User and Computer**.

3. In the prompt, right click the domain of SSO, and select **Properties**, then click <Group Properties> tab.



testdomain.hillstonenet.com Properties

To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).

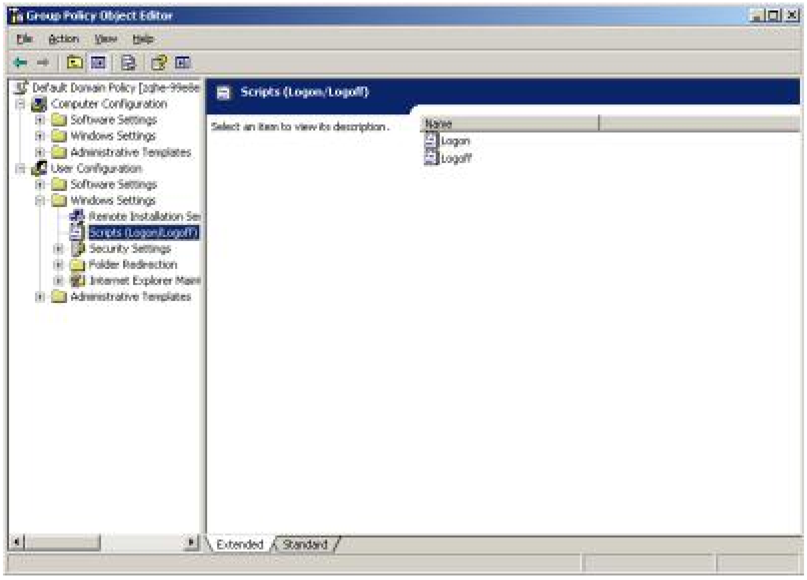
Current Group Policy Object Links for testdomain

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. Double click the group policy of SSO, and in the prompt, select **User Configuration>Windows>Script (Logon/Logout)**.

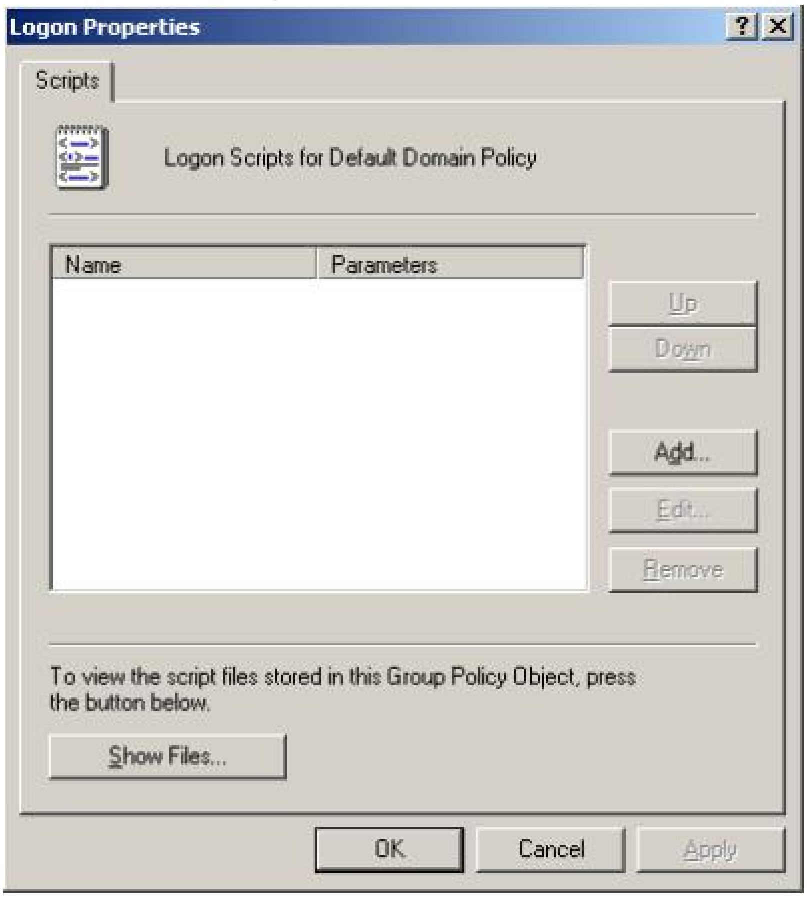


Group Policy Object Editor

Scripts (Logon/Logoff)

Select an item to view its description.

5. Double click **Logon** on the right, and click **Add** in the prompt.



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 prompt, click **Browse** and select the logon script (logonscript.exe), and then enter IP address of FSOS for authentication, followed by a space and text “logon”.

7. Click **OK**.

8. Similarly, import the script into the logout setting, repeat 5-7, and use “logoff” in the step 6.

Note: The directory of saving the script must be accessible to all domain users, otherwise, when a user who does not have access will not trigger the script when he logs in or out.

Configuration Examples of SSO Radius Login

The following is a configuration example for SSO Radius function. After configuring the SSO Radius function, system can receive the accounting packets that based on the Radius standard protocol. System will obtain user authentication information, update online user information and manage user's login and logout according to the packets.

To use SSO Radius for SSO, take the following steps:

Step 1: Configure the AAA server referenced by SSO Radius. You can select the configured Local, AD or LDAP server. For the configuration method, see Configuring an AAA Server. Here take AD server as the example.

```
hostname(config)# aaa-server ad type active-directroy
hostname(config-aaa-server)# host 1.1.1.1
hostname(config-aaa-server)# base-dn dc=fs
hostname(config-aaa-server)# login-dn cn=user,dc=fs
hostname(config-aaa-server)# login-password admin
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 2: Enable SSO Radius function, as well as specify the referenced AAA server, IP address of the client and so on.

```
hostname(config)# user-sso server sso-radius default
hostname(config-sso-radius)# enable
hostname(config-sso-radius)# aaa-server ad
hostname(config-sso-radius)# client 2.2.2.2
hostname(config-sso-radius-client)# exit
hostname(config-sso-radius)# exit
hostname(config)#
```

Example of Configuring Portal Authentication

This section describes a typical portal authentication configuration example.

This example allows only user1 who is authenticated using portal authentication to access the Internet. All other accesses are denied. The authentication server is the portal authentication server and the URL of the portal server is 192.168.1.2.

Step 1: Configure the role and role mapping rule

```
hostname(config)# role role1
hostname(config)# role-mapping-rule role-mapping1
hostname(config-role-mapping)# match user-group usergroup1 role role1
hostname(config-role-mapping)# exit
hostname(config)#
```

Step 2: Configure interfaces and security zones

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.1/16
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 66.1.200.1/16
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone dmz
hostname(config-if-eth0/2)# ip address 192.168.2.1/16
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Step 3: Configure the role mapping rule of the portal authentication server and enable the security agent function

```
hostname(config)# aaa-server AD type active-directory
hostname(config-aaa-server)# role-mapping-rule role-mapping1
hostname(config-aaa-server)# host 192.168.2.2
hostname(config-aaa-server)# base-dn “dc=fs”
hostname(config-aaa-server)# login-dn “user=administrators”
hostname(config-aaa-server)# login-password password1
hostname(config-aaa-server)# agent
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 4: Trigger the portal authentication function via the policy rule

```
hostname(config)# rule id 1
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-ip 192.168.2.2/16
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
hostname(config)# rule id 2
hostname(config-policy-rule)# role UNKNOWN
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# action portal-server http://192.168.2.2/
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
hostname(config)# rule id 3 from any to any service any permit
```

Step 5: Configure a policy rule that allows the access

```
hostname(config)# policy-global
hostname(config-policy)# rule role role1 from 192.168.1.1/16 to any service any permit
hostname(config-policy)# exit
hostname(config)#
```

After above configurations, the system will authenticate all HTTP. Users can access the Internet after providing the username user1 and password test1 on the login page.

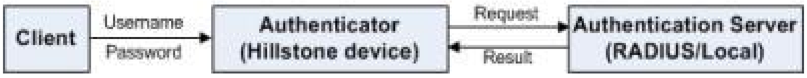
802.1X Authentication

Overview

802.1X is a standard defined by IEEE for Port-based Network Access Control. It uses Layer 2-based authentication to verify the legality of the users accessing the network trough LAN. Before authentication, the security device only allows 802.1X message to pass through the port. And after authentication, all the normal traffic can pass through.

802.1X Architecture

802.1X authentication architecture includes three components: client, authenticator and authentication server. The figure below shows the diagram of 802.1X authentication architecture.



Only when these three components are presented will 802.1X authentication be completed.

- Client: After you start the client program and enter your username and password, the client program will send requests for 802.1X authentication to the authenticator. Clients need to support EAP protocol, and should be running 802.1X client software.
- Authentication Server: The server stores users' information, verifies whether users have the right to use network resources, and returns the authentication results to the authenticator. FSOS support local authentication server or RADIUS server to implement authentication and authorization.
- Authenticator (FS device): The authenticator provides a physical interface for clients to access to LAN. It transmits users' information to the authentication server or returns it to the client, and then enables or disables the interface according to the server's authentication results. Authenticator acts as an agent between the client and authentication server.

802.1X Authentication Process

Authentication methods of 802.1X include EAP-MD5, EAP-TLS and EAP-PEAP. Different methods have different authentication processes.

Authenticating by EAP-MD5 Method

Here, take the EAP-MD5 authentication method as the example to introduce the basic 802.1X authentication process:

1. When you need to visit network, you should start the 802.1X client program, and enter your username and password to send a connection request. The authentication process starts.
2. After the authenticator receives the connection request from the client, it will ask the client to send its username.
3. The client responds and sends its username to the authenticator.
4. Authenticator will encapsulate the data received from the client and then deliver it to the authentication server.

5. Authentication server will check the username it received, comparing with the user’s information in its own database, and try to find the password of the user. After that, the server will generate random encrypted characters to encrypt the password, and send it to the authenticator.

6. Authenticator sends the encrypted characters to the client, and the client will encrypt the password and transmit it back to the authentication server.

7. Authentication server will compare the encrypted password information with their own encrypted password information. If they are matched, the authenticator will consider the user as a legitimate user, and allow the user to access the network through the interface. If not matched, authenticator will refuse the user to access network and keep the status of the interface as non-authenticated.

Authenticating by EAP-TLS Method

EAP-TLS is a kind of 802.1X authentication method that client and server can authenticate each other. Firstly, the server will send its own digital certificate to the client. When the certificate is authenticated to be valid, the client will send user’s digital certificate to the server. If the certificate is valid, the server will consider the user as a legitimate user, and allow the user to access the network. If you have deployed PKI system in your network environment, FS recommends that you configure EAP-TLS authentication method.

To use EAP-TLS method to realize 802.1X authentication, please install 802.1X client software which supports certificate authentication at the client side and import user's and CA's digital certificates; please set the authentication method to be EAP-TLS at the server side and import server's and CA's digital certificates.

Tip:

- Currently, the system does not support to realize EAP-TLS authentication via local authentication server.
- The 802.1X client software needs to be compatible with the 802.1X standard protocol.

Configuring 802.1X Authentication

802.1X authentication configurations include:

- Configuring an 802.1X profile.
- Specifying the 802.1X authentication server. FSOS support local authentication server and external authentication server (RADIUS).
- Configuring 802.1X attributes on port.

- Configuring 802.1X authentication global parameters, such as configuring the maximum number of clients to connect, etc.

Configuring an 802.1X Profile

To create an 802.1X profile, in the global configuration mode, use the following command:

dot1x profile *profile-name*

- *profile-name* - Specifies the name of 802.1X profile. After executing this command, the system will create the 802.1X profile with the specified name, and enter the dot1x configuration mode. If the profile name you specified already exists, the system will directly enter the dot1x configuration mode.

To delete the specified 802.1X profile, in the global configuration mode, use the command:

no dot1x profile *profile-name*

Configuring the Maximum Retry Times

If the authenticator initially sends the authentication request frame to the client, after a period of time when the client does not receive a response, the authenticator will resend the request to the client until exceeding the maximum times of resending the request. If exceeded, the authenticator will give up resending. To configure the maximum times of resending the authentication request frame, in the dot1x configuration mode, use the following command:

retransmission-count *value*

- *value* – Specifies the maximum times of resending authentication request frame. The value range is 1 to 10 times. The default value is 2.

To restore to the default value, in the dot1x configuration mode, use the command **no retransmission-count**.

Configuring the Re-auth Period

When the client is authorized to access network, the authenticator can re-authenticate the client. To configure the re-auth period, in the dot1x configuration mode, use the following command:

reauth-period *value*

- *value* – Specify the re-auth period. The value range is 0 to 65535 seconds. The default value is 3600. If the value is set to0, the re-authentication function is disabled.

To restore the default value, in the dot1x configuration mode, use the command **no reauth-period**.

Configuring the Quiet Period

If the authentication fails, the authenticator remains idle for a period of time before go on processing the same request from the same client. To configure the authenticator’ s quiet period, in the dot1x configuration mode, use the following command:

quiet-period *value*

- *value* – Specifies the value of quiet time. The value range is 0 to 65535 seconds. The default value is 60. The value of 0 indicates that the system will process the request from the same client all the time.

To restore to the default value, in the dot1x configuration mode, use the comman **no quiet-period**.

Configuring the Client Timeout

When the authenticator sends a request to ask the client to submit its username, the client need to responds within a specified period. If client does not respond until timeout, the system will resend the authentication request message. To specify the client timeout value, in the dot1x configuration mode, use the following command:

tx-period *value*

- *value* – Specifies the timeout value. The value range is 1 to 65535 seconds. The default value is 30.

To restore to the default value, in the dot1x configuration mode, use the command **no tx-period**.

Configuring the Server Timeout

The authenticator transmits the client’ s response data 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. To specify the authentication server timeout value, in the dot1x configuration mode, use the following command:

server-timeout *value*

- *value* – Specifies the response timeout value. The value range is 1 to 65535 seconds. The default value is 30.

To restore to the default value, in the dot1x configuration mode, use the command **no server-timeout**.

Specifying the 802.1X Authentication Server

You can specify an AAA server as the 802.1X authentication server. To specify the 802.1X authentication server, in the dot1x configuration mode, use the following command:

```
aaa-server server-name
```

- *server-name* - Specifies the AAA authentication server name. FSOS support local authentication server and RADIUS server.

To delete the specified 802.1X authentication server, in the dot1x configuration mode, use the command:

```
no aaa-server server-name
```

Note:For information about how to configure the local authentication server and RADIUS server, see Authentication, Authorization and Accounting.

Configuring 802.1X Attributes on Port

The authenticator provides a port for the client to access LAN, and the port need to be bound to Layer 2 security zone or VLAN. You can enable the 802.1X authentication function on the port, and configure attributes according to your need.

Enabling/Disabling 802.1X Authentication

To enable or disable 802.1X authentication, in interface configuration mode, use the following command:

- Enable the 802.1X authentication: **dot1x enable**
- Disable the 802.1X authentication: **no dot1x enable**

After enabling the 802.1X authentication, you can configure 802.1X attributes on the port.

Binding 802.1X Profile to a Port

To bind the created 802.1X profile to a port, in the interface configuration mode, use the following command:

```
dot1x profile profile-name
```

- *profile-name* – Specifies the 802.1X profile name.

To cancel the binding, in the interface configuration mode, use the command:

```
no dot1x profile profile-name
```

Configuring the Port Access Control Mode

To configure the access control mode on the specified port, in the interface configuration mode, use the following command:

```
dot1x port-control {auto | force-unauthorized}
```

- **auto** - Automatic mode. This is the default setting. In this mode, the authenticator decides whether the client can access the network according to the results of 802.1X authentication.
- **force-unauthorized** - Force-unauthorized mode. In this mode, the port is always in unauthorized state, and any client attempting to connect will fail.

To restore to default settings, in the interface configuration mode, use the command:

```
no dot1x port-control
```

Configuring the Port Access Control Method

To configure the method of 802.1X port access control, in the interface configuration mode, use the following command:

```
dot1x control-mode {mac | port}
```

- **mac** - MAC address-based authentication. All the clients under the port must be authenticated and then they can access network resources.
- **port** - Port-based authentication, which is the default setting. For all the clients under a port, as long as one client is authenticated, other clients can access network without authentication.

To restore the default settings, in interface configuration mode, use the command:

```
no dot1x control-mode
```

Configuring 802.1X Global Parameters

The following section describes global parameter configuration for the 802.1X.

Configuring the Maximum User Number

To configure the maximum number of clients that are allowed to connect to the port simultaneously, in the global configuration mode, use the following command:

```
dot1x max-user user-number
```

- *user-number* − Specifies the maximum user number. The value range is 1 to 1000. The default value may vary from different platforms.

To restore to the default values, in the global configuration mode, use the command **no dot1x max-user**.

Configuring the Timeout of Authenticated Clients

You can configure the authentication timeout value for authenticated clients. If the client does not respond within the specified time, it need reapply an authentication. To configure the timeout value, in the global configuration mode, use the following command:

dot1x timeout *timeout-value*

- *timeout-value* – Specifies the client authentication timeout value. The value range is 180 to 3600*24 seconds. The default value is 300.

To restore to the default value, in the global configuration mode, use the command **no dot1x timeout**.

Configuring Multi-logon Function

By default, the multi-logon function is disabled. If it is enabled, you can log into multiple clients using the same username simultaneously. To enable the multi-logon function, in global configuration mode, use the following command:

dot1x allow-multi-logon

After executing this command, the multi-logon function is enabled, and the number of clients using one username is limited. To specify the number of clients, in the global configuration mode, use the following command:

dot1x allow-multi-logon *number*

- *number* – Specifies how many times the same username can be logged in simultaneouly. The value range is 2 to 1000 times.

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

no dot1x allow-multi-logon

Configuring Auto-kickout Function

When the multi-logon function is disabled, if you enable the auto-kickout function, the user who already logged in will be kicked out by the same user who logs in later. The system will automatically cut the connection to the user who already logged in. If the auto-kickout function is disabled, the system will prohibit the same user to log in again. To enable or disable the auto-kickout function, in the global configuration mode, use the following commands:

- Enable the auto-kickout function: **dot1x auto-kickout**
- Disable the auto-kickout function: **no dot1x auto-kickout**

Configuring Manual Kick-out Client

To kick out any client manually, in any mode, use the following command:

exec dot1x kickout *port-name authenticated-user-mac*

- *port-name* – Specifies the port name the client connects to.
- *authenticated-user-mac* – Specifies the MAC address of the authenticated client that is kicked out manually.

Viewing 802.1X Configurations

To view the 802.1X configurations, in any mode, use the following command:

show dot1x [**profile** *profile-name* | **port** *port-name* | **statistics** [*port-name*]]

- **show dot1x** - Shows 802.1X global parameters.
- **profile** *profile-name* – Shows configurations of the specified 802.1X profile.
- **port** *port-name* – Shows the configurations of the specified port and its binding profile' s information.
- **statistics** [*port-name*] – Shows statistics information of the specified port.

PKI

Overview

PKI (Public Key Infrastructure) is a system that provides public key encryption and digital signature service. PKI is designed to automate secret key and certificate management, and assure the confidentiality, integrity and non-repudiation of data transmitted over Internet. The certificate of PKI is managed by a public key by binding the public key with a respective user identity by a trusted third-party, thus authenticating the user over Internet. A PKI system consists of Public Key Cryptography, CA, RA, Digital Certificate and related PKI storage library.

The following section describes PKI terminology:

- **Public Key Cryptography**: A technology used to generate a key pair that consists of a public key and a private key. The public key is widely distributed, while the private key is known only to the recipient. The two keys in the key pair complement each other, and the data encrypted by one key can only be decrypted by another key of the key pair.
- **CA**: A trusted entity that issues digital certificates to individuals, computers or any other entities. CA accepts requests for certificates and verifies the information provided by the

applicants based on certificate management policy. If the information is legal, CA will sign the certificates with its private key and issue them to the applicants.

- **RA**: The extension to CA. RA forwards requests for a certificate to CA, and also forwards the digital certificate and CRL issued by CA to directory servers in order to provide directory browsing and query services.
- **CRL**: Each certificate is designed with expiration. However, CA might revoke a certificate before the date of expiration due to key leakage, business termination or other reasons. Once a certificate is revoked, CA will issue a CRL to announce the certificate is invalid, and list the series number of the invalid certificate.

PKI Function of FS Devices

PKI is used in the following three situations:

- IKE VPN: PKI can be used by IKE VPN tunnel.
- HTTPS/SSH: PKI applies to the situation when a user accesses a FS device over HTTPS or SSH.

Configuring PKI

The PKI configuration on FS devices includes:

- Generating and deleting a PKI key pair
- Configuring a PKI trust domain
- Importing a CA certificate
- Generating a certificate request
- Importing a local certificate
- Downloading a CRL
- Importing and exporting a PKI trust domain
- Importing and exporting a local certificate

Generating/Deleting a PKI Key Pair

FSOS provides a default PKI key pair named Default-Key. To generate a PKI key pair, in the global configuration mode, use the following command:

pki key generate {**rsa** | **dsa** | **sm2**} [**label** *key-name*] [**modulus** *size*] [**noconfirm**]

- **rsa** | **dsa** – Specifies the type of key pair, either RSA or DSA.
- **label***key-name* – Specifies the name of the PKI key. The name must be unique in FSOS.
- **modulus** *size* – Specifies the modulus of the key pair. The options are 1024 (the default value), 2048, 512 and 768 bits.
- **noconfirm** – Disables prompt message on the key pair. For example, if the name of the key pair exists in the system, without this parameter configured, the system will prompt whether to overwrite key pair with the same name; with this parameter configured, the system will not allow to create a key pair with the same name. In addition, users can use the command **pki key zeroize noconfirm** to disable all the prompt information on key pairs.

To delete the existing PKI key, in the global configuration mode, use the following command:

pki key zeroize {**default** | **label** *key-name*} [**noconfirm**]

- **default** | **label** *key-name* – Specifies the key that will be deleted. **Default** indicates the default-key. **Label** *key-name* indicates the key of the specified name.
- **noconfirm** – Disables prompt message on the key pair.

Configuring a PKI Trust Domain

A PKI trust domain contains all the necessary configuration information that is used to apply for a PKI local certificate, such as key pair, enrollment type, subject, etc. To configure a PKI trust domain, you need to enter the PKI trust domain configuration mode. In the global configuration mode, use the following command:

pki trust-domain *trust-domain-name*

- *trust-domain-name* – Specifies the name of the PKI trust domain. This command creates a PKI trust domain with the specified name, and leads you into the PKI trust domain configuration mode; if the specified name exists, you will directly enter the PKI trust domain configuration mode.

To delete the specified PKI trust domain, in the global configuration mode, use the command **no pki trust-domain** *trust-domain-name*.

You can perform the following configurations in the PKI trust domain configuration mode:

- Specifying an enrollment type
- Specifying a key pair
- Configure subject content

- Configuring a CRL

Specifying an Enrollment Type

To specify an enrollment type, in the PKI trust domain configuration mode, use the following command:

```
enrollment {self | terminal}
```

- **self** − Generates a self-signed certificate.
- **terminal** − Enrolls a certificate from a terminal (by cutting and pasting).

To cancel the enrollment type, in the PKI trust domain configuration mode, use the command **no enrollment**.

Note: There is no default value for this command; therefore, you must use the command to specify an enrollment type.

Specifying a Key Pair

To specify a key pair, in the PKI trust domain configuration mode, use the following command:

keypair *key-name*

- *key-name* − Specifies the name of the key pair.

To cancel the specified key pair, in the PKI trust domain configuration mode, use the command **no keypair**.

Configuring Subject Content

To specify subject content for the PIK trust domain, in the PKI trust domain configuration mode, use the following commands:

- Configure a common name: **subject commonName** *string*
- Configure a country (optional): **subject country** *string*

Note: The name of the country can only contain two characters.

- Configure a locality (optional): **subject localityName** *string*
- Configure a state or province (optional): **subject stateOrProvinceName** *string*
- Configure an organization (optional): **subject organization** *string*
- Configure an organization unit (optional): **subject organizationUnit** *string*

To cancel the above configurations, in the PKI trust domain configuration mode, use the following commands:

- no subject commonName
- no subject country
- no subject localityName
- no subject stateOrProvinceName
- no subject organization
- no subject organizationUnit

Configuring a CRL

CRL is used to help you check whether a certificate within its validity period has been revoked by the CA. To configure a CRL check, in the PKI trust domain configuration mode, use the following command:

crl {**nocheck** | **optional** | **required**}

- nocheck – FSOS will not check the CRL. This is the default option.
- optional – FSOS will still accept the peer's authentication even if the CRL is not available.
- required – FSOS will not accept the peer’s authentication unless the CRL is available.

In addition, you can configure the URL that is used to retrieve the CRL information. The configuration needs to be performed in the CRL configuration mode. To enter the CRL configuration mode, in the PKI trust domain configuration mode, use the following command:

crl configure

To configure the URL that is used to retrieve CRL information, in the CRL configuration mode, use the following command:

url *index* {*url-http* | *url-ldap* [**username** *user-name* **password** *password* **auth-method** *auth-method*]} [**vrouter** *vrouter-name*]

- *index* – Specifies the URL index. FSOS supports up to three URLs, and uses them by turn of URL1, URL2 and URL3.
- *url-http* – Specifies the HTTP URL that is used to retrieve CRL information. The URL entered should begin with http:// and the length is 1 to 255 characters.

- *url-ldap* – Specifies the LDAP URL that is used to retrieve CRL information. The URL entered should begin with ldap:// and the length is 1 to 255 characters.
- **username** *user-name* **password** *password* **auth-method** *auth-method* – Specifies the username (**username** *user-name*), password (**password** *password*) and authentication mode (**auth-method** *auth-method*) when the system is configured to retrieve CRL information via LDAP. If this parameter is not configured, the system will retrieve CRL information anonymously by default.
  - **username** *user-name* - Specifies the login DN of the LDAP server. The login DN is typically a user account with query privilege predefined in the LDAP server.
  - **password** *password* – Specifies the password for login DN.
  - **auth-method** *auth-method* - Specifies the authentication mode for the LDAP server. Plain text authentication (`plain`) is supported.

) when the system is configured to retrieve CRL information via LDAP. If this parameter is not configured, the system will retrieve CRL information anonymously by default.
- **vrouter** *vrouter-name* – Specifies the VRouter from which the CRL information is retrieved. The default value is the default VRouter (trust-vr).

Configuring Online Certificate Status Protocol

The Online Certificate Status Protocol (OCSP), having the same function as CRL, is used to obtain the revocation status of certificates. Compared with CRL, OCSP can online check the status of certificates, thus providing more accurate result. You can configure CRL and OCSP simultaneously. If it fails to validate the certificate using either CRL or OCSP, the system will conclude that the certificate cannot be used.

In the PKI trust domain configuration mode, use the following command to make you check the certificate status using OCSP:

ocsp required

To disable this function, use the following command in the PKI trust domain configuration mode:

ocsp nocheck

To enter the OCSP configuration mode, use the following command in the PKI trust domain configuration mode:

ocsp configure

In the OCSP configuration mode, you can configure the following settings:

- Specifying the OCSP responder

- Configuring the random number for OCSP requests
- Specifying the invalidity time for OCSP response information

Specifying the OCSP Responder

To specify the OCSP responder, use the following command in the OCSP configuration mode:

url *url*

- *url* – Specifies the URL of the OCSP responder. The URL must begin with "http://" .

To cancel the configurations, use the following command:

no url。

Configuring the Random Number for OCSP Requests

When the device sends OCSP requests, you can choose to add the random number to the requests, which improves the security between the device and the OCSP responder. By default, the device adds the random number to the requests. To add random number, use the following command in the OCSP configuration mode:

nonce enable

To cancel the configurations, use the following command:

nonce disable

Specifying the Invalidity Time for OCSP Response Information

FSOS provides the function of OCSP response information cache, which improves the efficiency of certificate verification. You can specify the invalidity time for the OCSP request information that is stored in the cache of the device and the OCSP request information will be deleted from the cache after the invalidity time reaches. To specify the invalidity time, use the following command in the OCSP configuration mode:

response-cache-refresh-interval *time*

- *time* - Specifies the invalidity time (in minutes) for the OCSP response information that stored in the cache. The value ranges from 0 to 1440. 0 represents the device will not store the OCSP response information. And when the device receives the request of certificate verification, it will send request to the OCSP responder to check the certificate status. When the specified value is between 1 and 1440, the invalidity time for stored OCSP response information is calculated by comparing the time of "current system time + time" with the time when the OCSP response information will be updated. The invalidity time is the one which is shorter.

In the OCSP configuration mode, use the following command to cancel the configurations:**no response-cache-refresh-interval**

After you cancel the configurations, the invalidity time for OCSP response information is the time when the OCSP response information will be updated. This is also the default settings.

Importing a CA Certificate

To import a CA certificate, in the global configuration mode, use the following command:

pki authenticate *trust-domain-name*

- *trust-domain-name* – Specifies the name of PKI trust domain.

After executing this command, the system will prompt the user to copy the content of the certificate to the specified location. Press Enter, type a period (.), and then press Enter again. The system will begin to import the CA certificate.

If ht enrollment type is to enroll a certificate from the register server, the CA certificate will be obtained via SCEP.

Importing a Key

To import a key to the PKI trust domain, in the global configuration mode, use the following command:

pki key import {**rsa** | **dsa** | **sm2**} [**label** *label-name*]

- **rsa** – Specifies the RSA key imported to PKI.
- **dsa** – Specifies the DSA key imported to PKI.
- **sm2** – Specifies the SM2 key imported to PKI.
- *label-name* – Specifies the name of key pair. The name should be the unique in system. If the parameter is not specified, the default key Default-Key will be selected.

Importing a Key Pair

To import the key pair to the PKI trust domain, in the execution mode, use the following commands:

import pki key *key-name* **enc-key** *sig-key-name* **from** {**ftp server** *ip-address* [**vrouter** *VR-name*] [**user** *user-name* **password** *password*] *file-name* | **tftp server** *ip-address* [**vrouter** *VR-name*] *file-name*}

- *key-name* – Specifies the name of the imported key pair.
- **enc-key** – Specifies the key type as encryption key.

- *sig-key-name* – Specifies the signature key pair.
- **ftp** | **tftp** – Specifies the uploading method as FTP or TFTP.
- **server** *ip-address* – Specifies the IP address of the FTP or TFTP server.
- **vrouter** *VR-name* - Specifies the name of VRouter.
- **user** *user-name* **password** *password* – Specifies the user name and password of the specified server.
- *file-name* – Specifies the name of locol encryption key pair file.

Generate a Certificate Request

After completing the PKI trust domain configuration, you need to generate a certificate request based on the content of the PKI trust domain, and then send the request to the CA server to enroll the corresponding local certificate. To generate a certificate request, in the global configuration mode, use the following command:

```
pki enroll trust-domain-name
```

- *trust-domain-name* – Specifies the name of the PKI trust domain to generate the corresponding certificate request.

Importing a Local Certificate

After obtaining a local certificate from the CA server, you need to import the local certificate to the device. To import a local certificate, in the global configuration mode, use the following command:

```
pki import trust-domain-name certificate
```

- *trust-domain-name* – Specifies the name of the PKI trust domain where the local certificate will be imported from.

After executing this command, the system will prompt the user to copy the content of the certificate to the specified location. Press Enter, type a period (.), and then press Enter again. The system will begin to import the local certificate.

Obtaining a CRL

To obtain the CRL of the PKI trust domain, in the global configuration mode, use the following command:

```
pki crl request trust-domain-name
```

- *trust-domain-name* – Specifies the name of PKI trust domain. The system will obtain the current CRL based on CRL configuration in the specified PKI trust domain.

Importing/Exporting a PKI Trust Domain

To facilitate configuration, you can export a PKI trust zone's certificate (CA and local certificate) and the private key for the local certificate in PKSC12 format, and import them on another FS device.

Exporting the PKI Trust Domain Information

To export the PKI trust domain information, in the global configuration mode, use the following command:

pki export *trust-domain-name* **pkcs12** *pass-phrase*

- *trust-domain-name* – Specifies the name of the PKI trust domain.
- *pass-phrase* – Specifies the passphrase that is used to decrypt PKCS12 data.

You can also export the PKI trust domain information in form of a file to an FTP server, TFTP server or USB disk via CLI.

To export the PKI trust domain information to an FTP server, in the execution mode, use the following command:

export pki *trust-domain-name* **pkcs12** *password* **to ftp server** *ip-address* [**user** *user-name* **password** *password* [*file-name*] | *file-name*]

- *trust-domain-name* – Specifies the name of the PKI trust domain.
- **pkcs12** *password* – Specifies the password used to decrypt the private key.
- *ip-address* – Specifies the IP address of the FTP server.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP server.
- *file-name* – Specifies the name for the exported file.

To export the PKI trust domain information to a TFTP server, in the execution mode, use the following command:

export pki *trust-domain-name* **pkcs12** *password* **to tftp server** *ip-address* [*file-name*]

To export the PKI trust domain information to a USB disk, in the execution mode, use the following command:

export pki *trust-domain-name* **pkcs12** *password* **to** {**usb0** | **usb1**} [*file-name*]

Importing the PKI Trust Domain Information

To import the PKI trust domain information, in the global configuration mode, use the following command:

pki import *trust-domain-name* **pkcs12** *pass-phrase*

- *trust-domain-name* – Specifies the name of the PKI trust domain.
- *pass-phrase* – Specifies the passphrase that is used to decrypt PKCS12 data.

After executing this command, the system will prompt the user to copy the content of the PKI trust domain to the specified location. Press Enter, type a period (.), and then press Enter again. The system will begin to import the PKI trust domain.

You can also import the PKI trust domain information in form of a file from an FTP server, TFTP server or USB disk via CLI.

To import the PKI trust domain information from an FTP server, in the execution mode, use the following command:

import pki trust-domain *trust-domain-name* **pkcs12** *password* **from ftp server** *ip-address* {**user** *user-name* **password** *password file-name* | *file-name*}

- *trust-domain-name* – Specifies the name of the PKI trust domain.
- **pkcs12** *password* – Specifies the password used to decrypt the private key.
- *ip-address* – Specifies the IP address of the FTP server.
- **user** *user-name* **password** *password file-name* – Specifies the username and password of the FTP server.
- *file-name* – Specifies the name of the imported file.

To import the PKI trust domain information from a TFTP server, in the execution mode, use the following command:

import pki trust-domain *trust-domain-name* **pkcs12** *password* **from tftp server** *ip-address file-name*

To import the PKI trust domain information from a USB disk, in the execution mode, use the following command:

import pki trust-domain *trust-domain-name* **pkcs12** *password* **from** {**usb0** | **usb1**} *file-name*

Importing a Trust Certificate

If enabling Sandbox function, when importing a trust certificate of PE file, System will not detect the PE file. In the global configuration mode, use the following command to import a trust certificate:

import pki trusted-ca {**package** | **single**} **from** {**ftp server** *ip-address* [**vrouter** *VR-name*] [**user** *user-name* **password** *password*] *file-name* | **tftp server** *ip-address* [**vrouter** *VR-name*] *file-name*}

- **package** – Specifies the certificate package that you need to import.
- **single** – Specifies the single certificate that you need to import.
- **ftp** | **tftp** – Specifies the uploading method as FTP or TFTP.
- **server** *ip-address* – Specifies the FTP server IP or the TFTP server IP.
- **vrouter** *VR-name* - Specifies the VRouter name.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP server.
- *file-name* – Specifies the username and password of the FTP server.

Exporting/Importing a Local Certificate

To facilitate configuration, you can export a PKI trust zone's local certificate, and import it on another FS device.

Exporting a Local Certificate

To export a local certificate, in the global configuration mode, use the following command:

pki export *trust-domain-name* **certificate**

- *trust-domain-name* – Specifies the name of the PKI trust domain.

After executing this command, the system will prompt the user to copy the content of the certificate to the specified location. Press Enter, type a period (.), and then press Enter again. The system will begin to export the local certificate.

You can also export the local certificate in form of a file to an FTP server, TFTP server, or USB disk via CLI.

To export the local certificate to an FTP server, in the execution mode, use the following command:

export pki *trust-domain-name* **cert to ftp server** *ip-address* [**user** *user-name* **password** *password* [*file-name*] | *file-name*]

- *trust-domain-name* − Specifies the name of the PKI trust domain.
- *ip-address* − Specifies the IP address of the FTP server.
- **user** *user-name* **password** *password* − Specifies the username and password of the FTP server.
- *file-name* − Specifies the name of the exported file.

To export the local certificate to a TFTP server, in the execution mode, use the following command:

export pki *trust-domain-name* **cert to tftp server** *ip-address* [*file-name*]

To export the local certificate to a USB disk, in the execution mode, use the following command:

export pki *trust-domain-name* **cert to** {**usb0** | **usb1**} [*file-name*]

Importing a Local Certificate

To import a local certificate, in the global configuration mode, use the following command:

pki import *trust-domain-name* **certificate**

- *trust-domain-name* − Specifies the name of the PKI trust domain.

After executing this command, the system will prompt the user to copy the content of the certificate to the specified location. Press Enter, type a period (.), and then press Enter again. The system will begin to import the local certificate.

You can also import the local certificate in form of a file from an FTP server, TFTP server or USB disk via CLI.

To export the local certificate from an FTP server, in the execution mode, use the following command:

import pki trust-domain *trust-domain-name* **cert from ftp server** *ip-address* {**user** *user-name* **password** *password file-name* | *file-name*}

- *trust-domain-name* − Specifies the name of the PKI trust domain.
- *ip-address* − Specifies the IP address of the FTP server.
- **user** *user-name* **password** *password file-name* − Specifies the username and password of the FTP server, and name of the imported file.
- *file-name* − Specifies the name of the exported file.

To export the local certificate from a TFTP server, in the execution mode, use the following command:

import pki trust-domain *trust-domain-name* **cert from tftp server** *ip-address file-name*

To export the local certificate from a USB disk, in the execution mode, use the following command:

import pki trust-domain *trust-domain-name* **cert from** {**usb0** | **usb1**} *file-name*

Importing Customized Certificate for HTTPS WebAuth

Importing Customized Certificate

When HTTPS mode is selected in Web authentication (WebAuth), the security certificate is usually not trusted by browser. You will need to click the Continue button to start Web authentication. In order to avoid this situation, you can purchase a local certificate signed by a certificate authority and import this certificate into a new PKI trust domain. Then you can import the trusted certificate by configuring this feature. The public key of CA certificate in the browser will authenticate the imported certificate signed by the private key of CA. Therefore, the situation that security certificate is trusted by browser of client will not occurs any more.

To configure importing customized certificate for HTTPS WebAuth, in the WebAuth configuration mode, use the following command:

https-trust-domain *trust-domain-name*

- *trust-domain-name* – Specifies the name of the HTTPS trust domain. Before executing this command, this new PKI trust domain must have been added into FSOS, and you should make sure that the local certificate purchased from the certificate authority has been imported into it. By default, HTTPS trust domain is trust_domain_default, which will result in the untrusted certificate warning.

Note:Make sure that the trusted CA certificate has been imported into PC’ s browser, , otherwise the browser will still prompt that security certificate is not being trusted.

In the WebAuth configuration mode, use **no https-trust-domain** to cancel the above configuration.

Viewing Importing Customized Certificate Information

To view information on imported customized certificate, in any mode, use the following command:

show webauth

Certificate Expiry Configurations

In order to ensure the validity of the user certificate and to avoid the problems caused by certificate expiry, the system provides the following solutions:

- For the certificate or CA certificate that will expire soon, the system will generate a log of the Warning level one week before the date of expiry;

- For the certificate or the CA certificate that have already expired, the system will generate a log of the Critical level everyday;
- For the self-signed certificate, the system provides a refreshing option to allow you to re-sign the certificate.

The system defines the validity period of a self-signed certificate is 10 years. To refresh the self-signed certificate and re-sign the certificate, in the global configuration mode, use following command:

pki refresh *trust-domain-name*

- *trust-domain-name* – Specifies the name of the PKI trust domain.

Viewing the PKI Configuration Information

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

show pki key [**label** *key-name*]

- **label** *key-name* – Shows the configuration information of the specified key pair. If the parameter is not specified, the command will show the configuration information of all the key pairs in the system.

To view the configuration information of PKI trust domain, in any mode, use the following command:

show pki trust-domain [*trust-domain-name*]

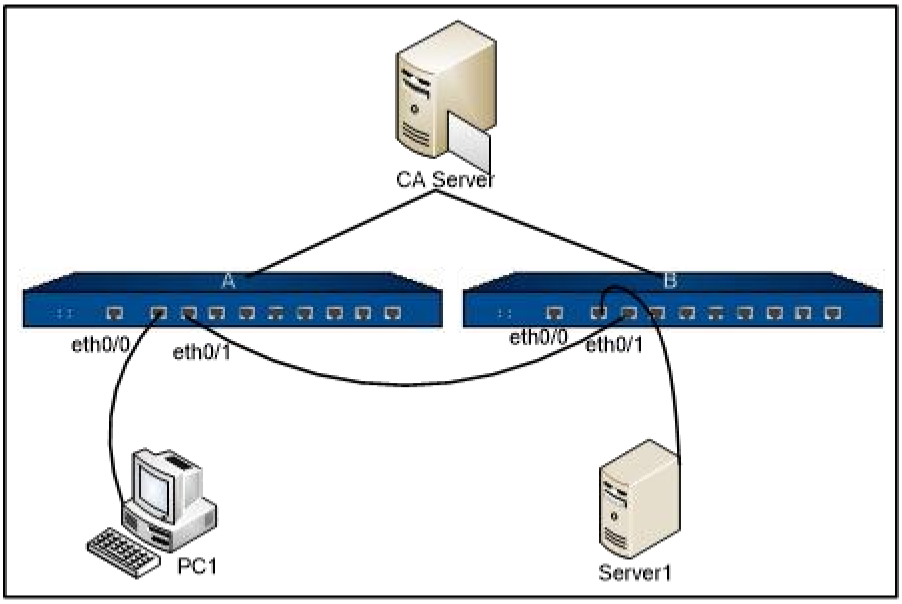
- *trust-domain-name* – Shows the configuration information of the specified PKI trust domain. If the parameter is not specified, the command will show the configuration information of all the PKI trust domains in the system.

Example for Configuring IKE

This section describes an example of creating a security alliance by IKE. The authentication policy of IKE adopts PKI certificate system.

Requirement

The goal is to create a secure tunnel between FS Device A and FS Device B. PC1 is used as the host of FS Device A, whose IP address is 10.1.1.1, and the gateway address is 10.1.1.2; Server1 is used as the server of FS Device B, whose IP address is 192.168.1.1, and the gateway address is 192.168.1.2. The requirement is: protecting the traffic between the subnet represented by PC1 (10.1.1.0/24) and the subnet represented by server1 (192.168.1.0/24). The authentication policy adopts PKI certificate system, using security protocol ESP and encryption algorithm 3DES, and the Hash algorithm is SHA1. The networking topology is shown in the figure below:



Configuration Steps

Step 1: Configure FS devices' interfaces

FS Device A

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 10.1.1.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# exit
```

FS Device B

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# exit
```

Step 2: Configure policy rules

FS Device A

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit

hostname(config)#
```

FS Device B

```
hostname(config)# policy-global

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone trust

hostname(config-policy-rule)# dst-zone trust

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone untrust

hostname(config-policy-rule)# dst-zone trust

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config-policy)# exit

hostname(config)#
```

Step 3: Configure Phase1 proposal

FS Device A

```
hostname(config)# isakmp proposal p1

hostname(config-isakmp-proposal)# authentication rsa-sig
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash sha
hostname(config-isakmp-proposal)# encryption 3des
hostname(config-isakmp-proposal)# exit
```

FS Device B

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication rsa-sig
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash sha
hostname(config-isakmp-proposal)# encryption 3des
hostname(config-isakmp-proposal)# exit
```

Step 4: Configure PKI

FS Device A

Generate a key pair

```
hostname(config)# pki key generate rsa label 111 modulus 1024
```

Configure a PKI trust domain

```
hostname(config)# pki trust-domain td1
hostname(config-trust-domain)# keypair 111
hostname(config-trust-domain)# enrollment terminal
hostname(config-trust-domain)# subject commonName aa
hostname(config-trust-domain)# subject country cn
hostname(config-trust-domain)# subject stateOrProvinceName bj
hostname(config-trust-domain)# subject localityName hd
hostname(config-trust-domain)# subject organization fs
hostname(config-trust-domain)# subject organizationunit rd
hostname(config-trust-domain)# exit
```

Generate a certificate request and send it to the CA server to enroll local certificate

```
hostname(config)# pki enroll td1
```

Authenticate the CA certificate

```
hostname(config)# pki authenticate td1
```

Import a local certificate

```
hostname(config)# pki import td1 certificate
```

FS Device B

Generate a key pair

```
hostname(config)# pki key generate rsa label 222 modulus 1024
```

Configure a PKI trust domain

```
hostname(config)# pki trust-domain td2
hostname(config-trust-domain)# keypair 222
hostname(config-trust-domain)# enrollment terminal
hostname(config-trust-domain)# subject commonName aa
hostname(config-trust-domain)# subject country cn
hostname(config-trust-domain)# subject stateOrProvinceName bj
hostname(config-trust-domain)# subject localityName hd
hostname(config-trust-domain)# subject organization fs
hostname(config-trust-domain)# subject organizationunit rd
hostname(config-trust-domain)# exit
```

Generate a certificate request and send it to the CA server to enroll local certificate

```
hostname(config)# pki enroll td2
```

Authenticate the CA certificate

```
hostname(config)# pki authenticate td2
```

Import a local certificate

```
hostname(config)# pki import td2 certificate
```

Step 5: Configure ISAKMP gateways

FS Device A

```
hostname(config)# isakmp peer east
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 1.1.1.2
hostname(config-isakmp-peer)# local-id asn1dn
hostname(config-isakmp-peer)# peer-id asn1dn CN=bb,OU=rd,O=fs,L=hd,ST=bj,C=cn
hostname(config-isakmp-peer)# trust-domain td1
hostname(config-isakmp-peer)# exit
```

```
FS Device Bhostname(config)# isakmp peer east
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 1.1.1.1
hostname(config-isakmp-peer)# local-id asn1dn
hostname(config-isakmp-peer)# peer-id asn1dn CN=aa,OU=rd,O=fs,L=hd,ST=bj,C=cn
hostname(config-isakmp-peer)# trust-domain td2
hostname(config-isakmp-peer)# exit
```

Step 6: Configure Phase2 proposal

FS Device A

```
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash sha
hostname(config-ipsec-proposal)# encryption 3des
hostname(config-ipsec-proposal)# exit
```

FS Device B

```
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash sha
hostname(config-ipsec-proposal)# encryption 3des
hostname(config-ipsec-proposal)# exit
```

Step 7: Configure a tunnel named VPN

FS Device A

```
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer east
hostname(config-tunnel-ipsec-auto)# id local 10.1.1.0/24 remote 192.168.1.0/24 service any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# tunnel ipsec vpn
hostname(config-if-tun1)# exit
```

FS Device B

```
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer east
hostname(config-tunnel-ipsec-auto)# id local 192.168.1.0/24 remote 10.1.1.0/24 service any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# tunnel ipsec vpn
hostname(config-if-tun1)# exit
```

Step 8: Configure routes

FS Device A

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 192.168.1.0/24 tunnel1
hostname(config-vrouter)# exit
```

FS Device B

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 10.1.1.0/24 tunnel1
hostname(config-vrouter)# exit
```

Chapter 9 VPN

This chapter introduces the following topics:

IPsec Protocol

Overview

IPsec is a widely used protocol suite for establishing VPN tunnel. IPsec is not a single protocol, but a suite of protocols for securing IP communications. It includes Authentication Headers (AH), Encapsulating Security Payload (ESP), Internet Key Exchange (IKE) and some authentication methods and encryption algorithms. IPsec protocol defines how to choose the security protocols and algorithms, as well as the method of exchanging security keys among communication peers, offering the upper layer protocols with network security services including access control, data source authentication and data encryption, etc.

- Authentication Header (AH): AH is a member of the IPsec protocol suite. AH guarantees connectionless integrity and data source verification of IP packets, and furthermore, it protects against replay attacks. AH can provide sufficient authentications for IP headers and upper-layer protocols.
- Encapsulating Security Payload (ESP): ESP is a member of the IPsec protocol suite. ESP provides encryption for confidential data and implements data integrity check of IPsec ESP data in order to guarantee confidentiality and integrity. Both ESP and AH can provide service of confidentiality (encryption), and the key difference between them is the coverage.
- Internet Key Exchange (IKE): IKE is used to negotiate the AH and ESP password algorithm and put the necessary key of the algorithm to the right place.

Note:The Russia version does not support the IPsec protocol and the related IPsec VPN function.

Security Association

IPsec provides encrypted communication between two peers which are known as IPsec ISAKMP gateways. Security Association (SA) is the basis and essence of IPsec. SA defines some factors of communication peers like the protocols, operational modes, encryption algorithms (DES, 3DES, AES-128, AES-192 and AES-256), shared keys of data protection in particular flows and the lifetime of SA, etc.

SA is used to process data flow in one direction. Therefore, in a bi-directional communication between two peers, you need at least two security associations to protect the data flow in both of the directions.

Establishing a SA

You can establish a SA in two ways: manual and IKE auto negotiation (ISAKMP).

Manually configuring a SA is complicated as all the information will be configured by yourself and some advanced features of IPsec are not supported (e.g. timed refreshing), but the advantage is that the manually configured SA can independently fulfill IPsec features without relying on IKE. This method applies to the condition of a small number of devices, or the environment of static IP addresses.

IKE auto negotiation method is comparatively simple. You only need to configure information of IKE negotiation and leave the rest jobs of creating and maintaining a SA to the IKE auto negotiation function. This method is for medium and large dynamic network. Establishing SA by IKE auto negotiation consists of two phases. The Phase 1 negotiates and creates a communication channel (ISAKMP SA) and authenticates the channel to provide confidentiality, data integrity and data source authentication services for further IKE communication; the Phase 2 creates an IPsec SA using the established ISAKMP. Establishing a SA in two phases can speed up key exchanging.

Phase 1 SA

The Phase 1 SA refers to the Security Association for establishing the channel. The negotiation procedure is:

1. Parameter configuration, including:
   - Authentication method: Pre-shared key or digital signature
   - Diffie-Hellman group selection
2. Policy negotiation, including:
   - Encryption algorithm: DES, 3DES, AES-128, AES-192 or AES-256
   - Hash algorithm: MD5, SHA-1 or SHA-2

3. DH exchange. Although it is known as key exchange, actually the two hosts will not exchange any real key at any time during the communication, and instead they only exchange the basic element information that is used by the DH algorithm to generate shared key. The DH exchange can be either open to the public or protected. After exchanging elements for generating the key, the two hosts of the both ends can generate the identical shared master key respectively to protect the authentication process hereafter.

4. Authentication. The DH exchange needs to be further authenticated. If the authentication fails, the communications will not continue. The master key, along with the negotiation algorithm specified in the Phase 1, will be used for authentication of the communication entities and communication channel. During this procedure, the entire payload that will be authenticated, including the entity type, port number and protocol, will be protected by the previously generated master key to assure the confidentiality and integrity.

Phase 2 SA

The Phase 2 SA, a fast SA, refers to the Security Association established for data transmission. This phase will negotiate to establish an IPsec SA, and provide IPsec service for data exchange. The negotiation messages in Phase 2 are protected by the Phase 1 SA, and any message that is not protected by the Phase 1 SA will be rejected. The Phase 2 negotiation (fast negotiation mode) procedure is:

1. Policy negotiation. The peers exchange protection requirements:
   - IPsec protocol: AH or ESP
   - Hash algorithm: MD5, SHA-1, SHA-2 or NULL
   - Encryption: DES, 3DES, AES-128, AES-192, AES-256 or NULL
   - Compression algorithm: DEFLATE
   - After the above four requirements reach an agreement, two SAs will be established and used for inbound and outbound communications respectively.
2. Refreshing or exchanging session key elements.
   In this step, the session key for IP packet encryption will be generated through DH exchange.
3. Submitting the SA to the IPsec driver.
   During the Phase 2 negotiation process, if the response is timeout, then the system will automatically retry the Phase 2 SA negotiation.

Hash Algorithm

Both AH and ESP can verify the integrity of IP packets, and determine whether the packets have been tampered during transmission. The verification algorithm is mainly implemented by the hash function.

The hash function can accept a message input of random length, and produces an output of fixed length. The output is known as the message digest. IPsec peers will compute the message digest. If the two digests are identical, the message proves to be complete and not having been tampered. In general IPsec adopts the following Hash algorithms:

- MD5: Use message input of a random length to produces a 128-bit message digest.
- SHA-1: Use a message with a length less than 264 bits to produce a 160-bit message digest. The digest of SHA-1 is longer than that of MD5, so it is more secure.
- SHA-2: Consists of SHA-256, SHA-384 and SHA-512. This algorithm can produce a longer message digest. For SHA-256, a message input with a length less than 264 bits can produce a 256-bit message digest; for SHA-384, a message input with a length less than 2128 bits produces a 384-bit message digest; for SHA-512, a message input with a length less than 2128 bits produces a 512-bit message digest.

Encryption Algorithm

ESP can provide encryption protection for the content of IP packets, and prevent against sniffing during the transmission. The encryption algorithm is implemented mainly through symmetric key system which uses the same key to encrypt and decrypt data. FSOS supports 3 encryption algorithms:

- DES (Data Encryption Standard): Uses a 56-bit key to encrypt each 64-bit plain text block.
- 3DES (Triple DES): Uses three 56-bit DES keys (168 bits in total) to encrypt plain text.
- AES (Advanced Encryption Standard): FSOS supports AES algorithms of 128-bit, 192-bit and 256-bit keys.

Compression Algorithm

IPComp (IP Payload Compression) is a protocol designed to reduce the length of IP datagram. This protocol compresses the IP datagram payload by different compression algorithms, and achieves the effect of transmitting data of heavy payload under the conditions of low bandwidth.

The prerequisite for a successful IPComp communication is to establish an IPComp Association (IPCA) between the two ends of the communication. The association includes all the information needed for IPComp operation, such as the compression algorithm and the parameters for the compression algorithm. When compressing the network data stream of IPsec by IPComp, you can create an IPCA manually or by dynamic negotiation. For the dynamic negotiation approach, ISAKMP gateway offers all the mechanisms necessary for establishing the IPCA. The IPsec function of FS devices provides the following IPComp compression algorithm:

- DEFLATE: A free lossless compression algorithm that can be implemented in IPComp, adopts LZ77 algorithm and Huffman decoding.

References

The IPsec function of FS devices follows the IPsec protocol specifications defined in RFC. For more detailed information about IPsec Protocol, see the relevant sections of the RFC documents below:

- Security Architecture for the Internet Protocol: RFC2401/RFC4301
- ESP: RFC2406/RFC4303
- AH: RFC2402/RFC4302
- Encryption algorithm: RFC2410 (Null Encryption), RFC2405 (DES-CBC), RFC2451 (3DES-CBC) and RFC3602 (AES-CBC)
- Hash algorithm: FIPS180-2 (SHA), RFC2404 (SHA-1), RFC4868 (SHA-2) and RFC2403 (MD5)
- Compression algorithm: RFC2393 (IPComp) and RFC2394 (DEFLATE)

Applying an IPsec VPN

You can apply the configured VPN tunnels to FS devices through the policy-based VPN and route-based VPN to assure the security of traffic encryption and decryption.

- Policy-based VPN: Applies a configured VPN tunnel in a policy rule, and only permits the matched traffic to pass through the VPN tunnel.
- Route-based VPN: Bind the configured VPN tunnel to a tunnel interface; when configuring the static route, you need to specify the tunnel interface as the next-hop route.

Configuring an IPsec VPN

You can configure IPsec VPN in two ways:

- Manual key VPN
- IKE VPN. The system supports both IKEv1 and IKEv2.

Manual Key VPN

The configuration options of manual key VPN include the operation mode of IPsec protocol, SPI, protocol type, encryption algorithm, hash algorithm and compression algorithm.

Creating a Manual Key VPN

To create a manual key VPN, in the global configuration mode, use the following command:

tunnel ipsec *name* **manual**

- *name* – Specifies the name of the manual key VPN tunnel that will be created.

After executing the above command, the CLI is in the manual key VPN configuration mode. You need to configure all the parameters of the manual key VPN in this mode.

To delete the specified manual key VPN, in the global configuration mode, use the following command:

no tunnel ipsec *name* **manual**

Specifying the Operation Mode of IPsec Protocol

To specify the operation mode of IPsec protocol (either transport mode or tunnel mode), in the manual key VPN configuration mode, use the following command:

mode {transport | tunnel}

- **transport** – Specifies the operation mode of IPsec protocol as transport.
- **tunnel** – Specifies the operation mode of IPsec protocol as tunnel. This is the default mode.

To restore to the default mode, in the manual key VPN configuration mode, use the command **no mode**.

Specifying a SPI

SPI (Security Parameter Index) is a unique 32-bit identifier generated by SA and transmitted in the AH and ESP header. SPI is used to find the corresponding VPN tunnel for decryption. To specify a SPI, in the manual key VPN configuration mode, use the following command:

spi *spi-number out-spi-number*

- *spi-number* – Specifies the local SPI.
- *out-spi-number* – Specifies the remote SPI.

To cancel the SPI, in the manual key VPN configuration mode, use the command **no spi**.

When configuring an SA, you should configure the parameters of both the inbound and outbound direction. Furthermore, SA parameters of the two ends of the tunnel should be totally matched. The local inbound SPI should be the same with the outbound SPI of the other end; the local outbound SPI should be the same with the inbound SPI of the other end.

Specifying a Protocol Type

The IPsec protocol types include ESP and AH. To specify the protocol type for the manual key VPN tunnel, in the manual key VPN configuration mode, use the following command:

protocol {esp | ah}

- esp – Uses ESP. This is the default protocol type.
- ah – Uses AH.

To restore to the default protocol type, in the manual key VPN configuration mode, use the command no protocol.

Specifying an Encryption Algorithm

To specify an encryption algorithm for the manual key VPN tunnel, in the manual key VPN configuration mode, use the following command:

encryption {3des | des | aes | aes-192 | aes-256 | null}

- 3des – Uses the 3DES encryption. The key length is 192-bit. This is the default algorithm.
- des – Uses the DES encryption. The key length is 64 bits.
- aes – Uses the AES encryption. The key length is 128 bits.
- aes-192 – Uses the 192-bit AES encryption. The key length is 192 bits.
- aes-256 – Uses the 256-bit AES encryption. The key length is 256 bits.
- null – No encryption.

To restore to the default encryption algorithm, in the manual key VPN configuration mode, use the command no encryption.

Specifying a Hash Algorithm

To specify a hash algorithm for the manual key VPN tunnel, in the manual key VPN configuration mode, use the following command:

hash {md5 | sha | sha256 | sha384 | sha512 | null}

- md5 – Uses the MD5 hash algorithm. The digest length is 128 bits.
- sha – Uses the SHA-1 hash algorithm. The digest length is 160 bits. This is the default hash algorithm.

- **sha256** − Uses the SHA-256 hash algorithm. The digest length is 256 bits.
- **sha384** − Uses the SHA-384 hash algorithm. The digest length is 384 bits.
- **sha512** − Uses the SHA-512 hash algorithm. The digest length is 512 bits.
- **null** − No hash algorithm.

To restore to the default hash algorithm, in the manual key VPN configuration mode, use the command **no hash**.

Specifying a Compression Algorithm

By default, the manual key VPN does not use any compression algorithm. To specify a compression algorithm (DEFLATE for the manual key VPN tunnel), in the manual key VPN configuration mode, use the following command:

compression deflate

To cancel the specified compression algorithm, in the manual key VPN configuration mode, use the command **no compression**.

Specifying a Peer IP Address

To specify a peer IP address, in the manual key VPN configuration mode, use the following command:

peer *ip-address*

- *ip-address* − Specifies the IP address of the peer.

To cancel the specified peer IP address, in the manual key VPN configuration mode, use the command **no peer**.

Configuring a Hash Key for the Protocol

You should configure the keys of both ends of the tunnel. The local inbound hash key should be the same with the peer's outbound hash key, and the local outbound hash key should be the same with the peer's inbound hash key. To configure a hash key, in the manual key VPN configuration mode, use the following command:

hash-key inbound *hex-number-string* **outbound** *hex-number-string*

- **inbound** *hex-number-string* − Configures the local inbound hash key.
- **outbound** *hex-number-string* − Configures the local outbound hash key.

To cancel the specified hash key, in the manual key VPN configuration mode, use the command **no hash-key**.

Configuring an Encryption Key for the Protocol

You should configure the keys of both ends of the tunnel. The local inbound encryption key should be the same with the peer's outbound encryption key, and the local outbound encryption key should be the same with the peer's inbound encryption key. To configure an encryption key for the protocol, in the manual key VPN configuration mode, use the following command:

encryption-key inbound *hex-number-string* **outbound** *hex-number-string*

- **inbound** *hex-number-string* – Configures the local inbound encryption key.
- **outbound** *hex-number-string* – Configures the local outbound encryption key.

To cancel the specified encryption key, in the manual key VPN configuration mode, use the command **no encryption-key**.

Specifying an Egress Interface

To specify an egress interface, in the manual key VPN configuration mode, use the following command:

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

To cancel the specified egress interface, in the manual key VPN configuration mode, use the command **no interface**.

Note:The egress interface in the non-root VSYS cannot be the VSYS shared interface.

IKEv1 VPN

The configurations of IKEv1 VPN include:

- Configuring a P1 proposal
- Configuring an ISAKMP gateway
- Configuring a P2 proposal
- Configuring a tunnel

Configuring a P1 Proposal

P1 proposal is the IKE security proposal that can be applied to the ISAKMP gateway, and is used in the Phase 1 SA. The configurations of IKE security proposal include specifying an authentication method, encryption algorithm, hash algorithm and lifetime of SA and DH group.

Creating a P1 Proposal

To create a P1 proposal, i.e., an IKE security proposal, in the global configuration mode, use the following command:

isakmp proposal *p1-name*

- *p1-name* – Specifies the name of the P1 proposal that will be created. After executing the command, the CLI will enter the P1 proposal configuration mode. You can configure parameters for P1 proposal in this mode.

To delete the specified P1 proposal, in the global configuration mode, use the command **no isakmp proposal** *p1-name*.

Specifying an Authentication Method

Specify the method of IKE identity authentication. Identity authentication is used to confirm the identities of both the ends during the communication. There are two methods: pre-shared key authentication and digital signature authentication. For the pre-shared key authentication, the authentication string is used as an input to generate a key, and different authentication strings will definitely generate different keys. In the non-root VSYS, only the pre-share key authentication mode is supported. To specify the authentication method of IKE security proposal, in the P1 proposal configuration mode, use the following command:

authentication {**pre-share** | **rsa-sig** | **dsa-sig** | **gm-de** }

- **pre-share** – Uses the pre-shared key authentication. This is the default method.
- **rsa-sig** – Uses the RSA digital signature authentication.
- **dsa-sig** – Uses the DSA digital signature authentication. The corresponding Hash algorithm can only be SHA-1.
- **gm-de** – Uses the envelope authentication mode. When the authentication mode is selected, only encryption algorithm SM4 is supported and verification algorithm SHA or SM3 are supported.

To restore to the default authentication method, in the P1 proposal configuration mode, use the command **no authentication**.

Specifying an Encryption Algorithm

FSOS provides the following five encryption algorithms: 3DES, DES, 128bit AES, 192-bit AES and 256-bit AES. To specify the encryption algorithm of IKE security proposal, in the P1 proposal configuration mode, use the following command:

```
encryption {3des | des | aes | aes-192 | aes-256 | sm4}
```

- **3des** – Uses the 3DES encryption. The key length is 192 bits. This is the default algorithm for FSOS.
- **des** – Uses the DES encryption. The key length is 64 bits.
- **aes** – Uses the AES encryption. The key length is 128 bits.
- **aes-192** – Uses the 192-bit AES encryption. The key length is 192 bits.
- **aes-256** – Uses the 256-bit AES encryption. The key length is 256 bits.
- **sm4** – Uses the SM4 block cipher algorithm. The key length is 128 bits.

To restore to the default encryption algorithm, in the P1 proposal configuration mode, use the command **no encryption**.

Specifying a Hash Algorithm

FSOS supports the following hash algorithms: MD5, SHA-1 and SHA-2 (including SHA-256, SHA-384 and SHA-512). To specify the hash algorithm of IKE security proposal, in the P1 proposal configuration mode, use the following command:

```
hash {md5 | sha | sha256 | sha384 | sha512 | sm3}
```

- **md5** – Uses the MD5 hash algorithm. The digest length is 128 bits.
- **sha** – Uses the SHA-1 hash algorithm. The digest length is 160 bits. This is the default hash algorithm.
- **sha256** – Uses the SHA-256 hash algorithm. The digest length is 256 bits.
- **sha384** – Uses the SHA-384 hash algorithm. The digest length is 384 bits.
- **sha512** – Uses the SHA-512 hash algorithm. The digest length is 512 bits.

- **sm3** – Uses the SM3 hash algorithm. The digest length is 256 bits. The algorithm can be used in the digital signature and verification, generating message verification code and other application scenarios.

To restore to the default hash algorithm, in the P1 proposal configuration mode, use the command **no hash**.

Selecting a DH Group

Diffie-Hellman (DH) is designed to establish a shared secret key. DH group determines the length of the element generating keys for DH exchange. The strength of keys is partially decided by the robustness of the DH group. The longer the key element is, the more secure the generated key will be, and the more difficult it will be to decrypt it. The selection of DH group is important, because the DH Group is only determined in the Phase 1 SA negotiation, and the Phase 2 negotiation will not re-select a DH group. The two phases use the same DH group; therefore the selection of DH group will have an impact on the keys generated for all sessions. During negotiation, the two ISAKMP gateways should select the same DH group, i.e., the length of key element should be equal. If the DH groups do not match, the negotiation will fail.

To select a DH group, in the P1 proposal configuration mode, use the following command:

group {1 | 2 | 5 | 14 | 15 |16}

- 1 – Selects DH Group1. The key length is 768 bits.
- 2 – Selects DH Group2. The key length is 1024 bits. This is the default value.
- 5 – Selects DH Group5. The key length is 1536 bits.
- 14 – Selects DH Group14. The key length is 2048 bits.
- 15 – Selects DH Group15. The key length is 3072 bits.
- 16 – Selects DH Group16. The key length is 4096 bits.

To restore the DH group to the default, in the P1 proposal configuration mode, use the command **no group**.

When configuring PFS in the P2 proposal, you can also select the DH group.

Specify the Lifetime of SA

The Phase 1 SA is configured with a default lifetime. When the SA lifetime expires, the device will send an SA P1 deleting message to its peer, notifying that the P1 SA has expired and it requires a new SA negotiation. To specify the lifetime of SA, in the P1 proposal configuration mode, use the following command:

lifetime *time-value*

- *time-value* – Specifies the lifetime of SA Phase1. The value range is 300 to 86400 seconds. The default value is 86400.

To restore to the default lifetime, in the P1 proposal configuration mode, use the command **no lifetime**.

Configuring an ISAKMP Gateway

After creating an ISAKMP gateway, you can configure the IKE negotiation mode, IP address and type of the ISAKMP gateway, IKE security proposal, pre-shared key, PKI trust zone, local ID, ISAKMP gateway ID, ISAKMP connection type, NAT traversal, etc.

Creating an ISAKMP Gateway

To create an ISAKMP gateway, in the global configuration mode, use the following command:

isakmp peer *peer-name*

- *peer-name* – Specifies the name of the ISAKMP gateway.

After executing the command, the CLI will enter the ISAKMP gateway configuration mode. You can configure parameters for the ISAKMP gateway in this mode.

To delete the specified ISAKMP gateway, in the global configuration mode, use the command **no isakmp peer** *peer-name*.

Binding an Interface to the ISAKMP Gateway

To bind an interface to the ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

interface *interface-name*

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

To cancel the binding, in the ISAKMP gateway configuration mode, use the command **no interface** *interface-name*.

Configuring an IKE Negotiation Mode

The IKE negotiation consists of two modes: the main mode and aggressive mode. The aggressive mode cannot protect identity. You have no choice but use the aggressive mode in the situation that the IP address of the center device is static and the IP address of client device is dynamic. To configure the IKE negotiations mode, in the ISAKMP gateway configuration mode, use the following command:

mode {main | aggressive}

- **main** – Uses the main mode, and provides ID protection. This is the default mode.
- **aggressive** – Uses the aggressive mode.

To restore to the default negotiations mode, in the ISAKMP gateway configuration mode, use the command **no mode**.

Configuring the Custom IKE Negotiation Port

You can configure a custom UDP port for IKE negotiation, and establish the IPSec connection. To configure a custom IKE negotiation port, in the ISAKMP gateway configuration mode, use the following command:

ipsec-over-udp port *port-number*

- *port-number* – Specifie the UDP port number, the range is 1 to 65535.

To cancel the configuration, in the ISAKMP gateway configuration mode, use the command **no ipsec-over-udp**.

Specifying the IP Address and Peer Type

You can specify the IP address and address type (static or dynamic) for the peer of the created ISAKMP gateway. To specify the IP address and the type of the peer, in the ISAKMP gateway configuration mode, use the following command:

type {dynamic | static}

- **dynamic** – Specifies the dynamic IP address.
- **static** – Specifies the static IP address. This is the default option.

To restore to the default type, in the ISAKMP gateway configuration mode, use the command **no type**.

peer *ip-address*

- *ip-address* - Specifies the IP address or the host name of the peer. This parameter is only valid when the IP address of the peer is static.

To cancel the IP address or the host name, in the ISAKMP gateway configuration mode, use the command **no peer**.

Accepting the Peer ID

To make the ISAKMP gateway accept any peer ID without check, in the ISAKMP gateway configuration mode, use the following command:

accept-all-peer-id

To disable the function, use the command **no accept-all-peer-id**.

Specifying a P1 Proposal

To specify the P1 proposal for the ISAKMP gateway, in ISAKMP the gateway configuration mode, use the following command:

isakmp-proposal p1-proposal1 [p1-proposal2] [p1-proposal3] [p1-proposal4]

- p1-proposal1 – Specifies the name of the P1 proposal. You can specify up to four P1 proposals for the ISAKMP gateway.

To cancel the specified P1 proposal, in ISAKMP the gateway configuration mode, use the command **no isakmp-proposal**.

Configuring a Pre-shared Key

If the pre-shared key authentication method is used, you need to specify a pre-shared key. To specify the pre-shared key for the ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

pre-share *string*

- *string* – Specifies the content of the pre-shared key.

To cancel the specified pre-shared key, in the ISAKMP gateway configuration mode, use the command **no pre-share**.

Configuring a PKI Trust Domain

If the digital signature authentication mode is used, you need to specify a PKI trust domain for the digital signature. To specify the PKI trust domain for the ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

trust-domain *string*

- *string* – Specifies the PKI trust domain.

To cancel the specified PKI trust domain, in the ISAKMP gateway configuration mode, use the command **no trust-domain**.

> Tip: For more information about how to configure a PKI trust domain, see "PKI" in the "User Authentication".

Configuring the Trust Domain of Peer Certificate

The peer certificate is used for encrypting and authenticating data in the negotiation. The initiator of VPN connection should import the peer certificate first. The command is supported only in the GM 1.0 version. To configure the trust domain of peer certificate , in the ISAKMP gateway configuration mode, use the following command:

remote-trust-domain *string*

- *string* – Specifies the trust domain for the peer certificate.

To cancel the configuration, use the command **no remote-trust-domain**.

Configuring the Trust Domain of Encryption Certificate

The encryption certificate is used for encrypting data in the negotiation. The command is supported only in the GM 1.1 version. To configure the trust domain for the encryption certificate, in the ISAKMP gateway configuration mode, use the following command:

trust-domain-enc *string*

- string – Specifies the trust domain for the encryption certificate.

To cancel the configuration, use the command **no trust-domain-enc**.

Configuring the Negotiation Protocol Standard

There are two negotiation protocol standards: IKEv1 and GM standard. By default, IKEv1 is used in system. To configure the negotiation protocol standard, in the ISAKMP gateway configuration mode, use the following command:

protocol-standard {**ikev1** | **guomi**[**v1.0** | **v1.1**]}

- **ikev1** – Specifies the IKEv1 as the negotiation protocol standard.
- **guomi**[**v1.0** | **v1.1**] – Specifies the GM standard as the negotiation protocol standard. If the version is specified as v1.0 or v1.1, the versions for the devices in the negotiation should be the same.

To cancel the configuration, use the command **no protocol-standard**.

Configuring a Local ID

To configure the local ID, in the ISAKMP gateway configuration mode, use the following command:

local-id {**fqdn** *string* | **asn1dn** [*string*] | **u-fqdn** *string* | **key-id** *string* |**ip** *ip-address* }

- **fqdn** *string* – Specifies the ID type of FQDN. *string* is the specific content of the ID.
- **asn1dn** [*string*] – Specifies the ID type of Asn1dn. This type is only applicable to the case of using a certificate. *string* is the specific content of the ID, but this parameter is optional. If *string* is not specified, the system will obtain the ID from the certificate.
- **u-fqdn** *string* – Specifies the ID type of U-FQDN, i.e., the email address type, such as user1@fs.com.
- **key-id** *string* - Specifies the ID that uses the Key ID type. This type is applicable to the XAUTH function.
- **ip** *ip-address* - Specifies the ID type of IP address. *string* is the specific content of the ID.

To cancel the specified local ID, in the ISAKMP gateway configuration mode, use the command no local-id.

Configuring a Peer ID

FSOS supports the ID types of FQDN and Asn1dn. To configure the peer ID, in the ISAKMP gateway configuration mode, use the following command:

```
peer-id {fqdn | asn1dn | u-fqdn | key-id | ip } string
```

- **fqdn** – Specifies the ID type of FQDN. *string* is the specific content of the ID.
- **asn1dn** – Specifies the ID type of Asn1dn. This type is only applicable to the case of using a certificate. *string* is the specific content of the ID.
- **u-fqdn string** – Specifies the ID type of U-FQDN, i.e., the email address type, such as user1@fs.com.
- **key-id** - Specifies the ID using key ID type. The type is only supported for XAUTH function.
- **ip** - Specifies the ID type of IP address.

To cancel the specified peer ID, in the ISAKMP gateway configuration mode, use the command **no peer-id**.

Specifying a Connection Type

The created ISAKMP gateway can be an initiator, responder, or both the initiator and responder. To specify the connection type, in the ISAKMP gateway configuration mode, use the following command:

```
connection-type {bidirectional | initiator-only | responder-only}
```

- **bidirectional** – Specifies the ISAKMP gateway as both the initiator and responder. This is the default option.
- **initiator-only** – Specifies the ISAKMP gateway as the initiator only.
- **responder-only** – Specifies the ISAKMP gateway as the responder only.

To restore to the default connection type, in the ISAKMP gateway configuration mode, use the command **no connection-type**.

Enabling NAT Traversal

The NAT traversal function must be enabled when there is a NAT device in the IPsec or IKE tunnel and the device implements NAT. By default, NAT traversal is disabled. To enable NAT traversal, in the gateway ISAKMP configuration mode, use the following command:

```
nat-traversal
```

To disable NAT traversal, in the gateway ISAKMP configuration mode, use the command **no nat-traversal**.

Configuring DPD

DPD (Dead Peer Detection) is used to detect the state of the security tunnel peer. 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 detect if the ISAKMP gateway exists. By default, this function is disabled. To configure DPD, in the ISAKMP gateway configuration mode, use the following command:

dpd [**interval** *seconds*] [**retry** *times*]

- **interval** *seconds* – Specifies the interval of sending DPD requests to the peer. The value range is 0 to 10 seconds. The default value is 0, indicating DPD is disabled.
- **retry** *times* – Specifies the times of sending DPD requests to the peer. The device will keep sending discovery requests to the peer until it reaches the specified times of DPD retires. If the device does not receive response from the peer after the retry times, it will determine that the peer ISAKMP gateway is down. The value range is 1 to 20 times. The default value is 3.

To resort the settings to the default DPD settings, use the command **no dpd**.

Specifying Description

To specify description for the ISAKMP Gateway, in the ISAKMP gateway configuration mode, use the following command:

description *string*

- *string* – Specifies the description for the ISAKMP gateway.

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

Configuring a P2 Proposal

P2 proposal is used in the Phase 2 SA. The configurations of P2 proposal include encryption algorithm, hash algorithm, compression algorithm and lifetime.

Creating a P2 Proposal

To create a P2 proposal, i.e., an IPsec security proposal, in the global configuration mode, use the following command:

ipsec proposal *p2-name*

- *p2-name* – Specifies the name of the P2 proposal that will be created. After executing the command, the CLI is in the P2 proposal configuration mode. You can configure parameters for P2 proposal in this mode.

To delete the specified P2 proposal, in the global configuration mode, use the command **no ipsec proposal** *p2-name*.

Specifying a Protocol Type

The protocol types available to P2 proposal include ESP and AH. To specify a protocol type for P2 proposal, in the P2 proposal configuration mode, use the following command:

protocol {esp | ah}

- **esp** – Uses ESP. This is the default protocol type.
- **ah** – Uses AH.

To restore to the default protocol type, in the P2 proposal configuration mode, use the command **no protocol**.

Specifying an Encryption Algorithm

You can specify 1 to 4 encryption algorithms for P2 proposal. To specify the encryption algorithm for P2 proposal, in the P2 proposal configuration mode, use the following command:

encryption {3des | des | aes | aes-192 | aes-256 | sm4 | null} [3des | des | aes | aes-192 | aes-256 | sm4 | null] [3des | des | aes | aes-192 | aes-256 | sm4 | null]……

- **3des** – Uses the 3DES encryption. The key length is 192-bit. This is the default method for FSOS.
- **des** – Uses the DES encryption. The key length is 64 bits.
- **aes** – Uses the AES encryption. The key length is 128 bits.

- **aes-192** – Uses the 192-bit AES encryption. The key length is 192 bits.
- **aes-256** – Uses the 256-bit AES encryption. The key length is 256 bits.
- **sm4** – Uses the SM4 block encryption algorithm. The key length is 128 bits.
- **null** – No encryption.

To restore to the default encryption algorithm, in the P2 proposal configuration mode, use the command **no encryption**.

Specifying a Hash Algorithm

You can specify 1 to 3 hash algorithms for P2 proposal. To specify the hash algorithm for P2 proposal, in the P2 proposal configuration mode, use the following command:

hash {**md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3** | **null**} [**md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3** | **null**] [**md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3** | **null**]

- **md5** – Uses the MD5 hash algorithm. The digest length is 128 bits.
- **sha** – Uses the SHA-1 hash algorithm. The digest length is 160 bits. This is the default hash algorithm.
- **sha256** – Uses the SHA-256 hash algorithm. The digest length is 256 bits.
- **sha384** – Uses the SHA-384 hash algorithm. The digest length is 384 bits.
- **sha512** – Uses the SHA-512 hash algorithm. The digest length is 512 bits.
- **sm3** – Uses the SM3 hash algorithm. The digest length is 256 bits.
- **null** – No hash algorithm.

To restore to the default hash algorithm, in the P2 proposal configuration mode, use the command **no hash**.

Specifying a Compression Algorithm

By default, the P2 proposal does not use any compression algorithm. To specify a compression algorithm (DEFLATE) for the P2 proposal, in the P2 proposal configuration mode, use the following command:

compression deflate

To cancel the specified compression algorithm, in the P2 proposal configuration mode, use the command **no compression**.

Configuring PFS

The PFS (Perfect Forward Security) function is designed to determine how to generate the new key instead of the time of generating the new key. PFS ensures that no matter what phase it is in, one key can only be used once, and the element used to generate the key can only be used once. The element will be discarded after generating a key, and will never be re-used to generate any other keys. Such a measure will assure that even if a single key is disclosed, the disclosure will only affect the data that is encrypted by the key, and will not threaten the entire communication. PFS is based on the DH algorithm. To configure PFS, in the P2 proposal configuration mode, use the following command:

group {nopfs | 1 | 2 | 5 | 14 | 15 |16}

- **nopfs** – Disables PFS. This is the default option.
- **1** – Selects DH Group1. The key length is 768 bits.
- **2** – Selects DH Group2. The key length is 1024 bits.
- **5** – Selects DH Group5. The key length is 1536 bits.
- **14** – Selects DH Group14. The key length is 2048 bits.
- **15** – Selects DH Group15. The key length is 3072 bits.
- **16** – Selects DH Group16. The key length is 4096 bits.

To restore to the default PFS configuration, in the P2 proposal configuration mode, use the command **no group**.

Specifying a Lifetime

You can evaluate the lifetime by two standards which are time length and traffic volume. When the SA lifetime runs out, the SA will get expired and requires a new SA negotiation. To specify the lifetime for the P2 proposal, in the P2 proposal configuration mode, use the following commands:

lifetime *seconds*

- *seconds* – Specifies the lifetime of time length type. The value range is 180 to 86400 seconds. The default value is 28800.

lifesize *kilobytes*

- *kilobytes* – Specifies the lifetime of traffic volume type. The default value is 0.

To cancel the specified lifetime, in the P2 proposal configuration mode, use the following commands:

no lifetime

no lifesize

Configuring a Tunnel

When configuring an IPsec tunnel through IKE, you need to configure the following options: the protocol type, ISAKMP gateway, IKE security proposal, ID, DF-bit and anti-replay.

Creating an IKE Tunnel

To create an IKE tunnel, in the global configuration mode, use the following command:

tunnel ipsec *tunnel-name* **auto**

- *tunnel-name* - Specifies the name of the IKE tunnel that will be created.

After executing the above command, the CLI will enter the IKE tunnel configuration mode. All the parameters of the IKE tunnel need to be configured in the IKE tunnel configuration mode.

To delete the specified IKE tunnel, in the global configuration mode, use the command **no tunnel ipsec** *tunnel-name* **auto**.

Specifying the Operation Mode of IPsec Protocol

To specify the operation mode of IPsec protocol for the IKE tunnel (either transport mode or tunnel mode), in the IKE tunnel configuration mode, use the following command:

mode {**transport** | **tunnel**}

- **transport** – Specifies the operation mode of IPsec as transport.
- **tunnel** – Specifies the operation mode of IPsec as tunnel. This is the default mode.

To restore to the default mode, in the IKE tunnel configuration mode, use the command **no mode**.

Specifying an ISAKMP Gateway

To specify an ISAKMP gateway for the IKE tunnel, in the IKE tunnel configuration mode, use the following command:

isakmp-peer *peer-name*

- *peer-name* – Specifies the name of the ISAKMP gateway.

To cancel the specified ISAKMP gateway, in the IKE tunnel configuration mode, use the command **no isakmp-peer**.

Specifying a P2 Proposal

To specify a P2 proposal for the IKE tunnel, in the IKE tunnel configuration mode, use the following command:

ipsec-proposal *p2-name*

- *p2-name* – Specifies the name of the P2 proposal.

To cancel the specified P2 proposal for the IKE tunnel, in the IKE tunnel configuration mode, use the command **no ipsec-proposal**.

Specifying a Phase 2 ID

To specify a Phase 2 ID for the IKE tunnel, in the IKE tunnel configuration mode, use the following command:

id {**auto** | **local** *ip-address/mask* **remote** *ip-address/mask* **service** *service-name*}

- **auto** – Automatically assigns the Phase 2 ID. This is the default option.
- **local** *ip-address/mask* – Specifies the local ID of Phase 2.
- **remote** *ip-address/mask* – Specifies the Phase 2 ID of the peer device.
- **service** *service-name* – Specifies the name of the service.

You can configure up to 64 phase 2 IDs and use them to establish multiple IKE tunnels.

To restore the settings to the default ones, in the IKE tunnel configuration mode, use the command **no id** {**auto** | **local** *ip-address/mask* **remote** *ip-address/mask* **service** *service-name*}.

Configuring IPsec VPN Traffic Distribution and Limitation

Based on the configuration of Phase 2 IDs, the traffic distribution function can distribute the traffic at the IKE tunnel ingress interface when the traffic flow into the IKE tunnel. If the elements of source IP address, destination IP address, and the type of the traffic can match the configuration of a certain Phase 2 ID, this kind of traffic will flow into the corresponding IKE tunnel for encapsulation and sending. If the traffic cannot match any Phase 2 IDs, it will be dropped.

Based on the configuration of Phase 2 IDs, the traffic limitation function can limit the traffic at the IKE tunnel egress interface when the traffic flows out of the IKE tunnel. After the traffic was de-encapsulated, FSOS checks the elements of source IP address, destination IP address, and the type of the traffic to see whether this kind of traffic matches a certain Phase 2 ID or not. If matched, the traffic will be dealt with. If not matched, the traffic will be dropped.

To enable the traffic distribution and limitation, use the following command in the IKE tunnel configuration mode:

check-id

Use the no form of the command to cancel this function.

Accepting All Proxy ID

This function 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. If you have configured several phase 2 IDs, disable this function. To enable the accepting all proxy ID function, in the IKE tunnel configuration mode, use the following command:

accept-all-proxy-id

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

no accept-all-proxy-id

Configuring Auto-connection

The device will be triggered to establish SA in two modes: auto and traffic intrigued.

- In the auto mode, the device detects the SA status every 60 seconds and initiates negotiation request when SA is not established;
- In the traffic intrigued mode, the tunnel sends negotiation requests only when there is traffic passing through the tunnel.

By default, the traffic intrigued mode is used. To use the auto mode, in the IKE tunnel configuration mode, use the following command:

auto-connect

To restore to the default mode, in the IKE tunnel configuration mode, use the command **no auto-connect**.

> Note:Auto connection works only when the peer IP is static and the local device is acting as the initiator.

Configuring DF-bit

You can specify whether to allow the forwarding device to fragment the packets. To configure DF-bit for the IKE tunnel, in the IKE tunnel configuration mode, use the following command:

df-bit {copy | clear | set}

- **copy** – Copies the IP packet DF options from the sender directly. This is the default value.
- **clear** – Allows the device to fragment packets
- **set** – Disallows the device to fragment packets.

To restore to the default value, in the IKE tunnel configuration mode, use the command **no df-bit**.

Configuring Anti-replay

Anti-replay is used to prevent hackers from attacking the device by resending the sniffed packets, i.e., the receiver rejects the obsolete or repeated packets. By default, this function is disabled. To configure anti-replay for the IKE IPsec tunnel, in the IKE IPsec tunnel configuration mode, use the following command:

anti-replay {**32** | **64** | **128** | **256** | **512**}

- **32** – Specifies the anti-replay window as 32.
- **64** – Specifies the anti-replay window as 64.
- **128** – Specifies the anti-replay window as 128.
- **256** – Specifies the anti-replay window as 256.
- **512** – Specifies the anti-replay window as 512.

When the network condition is poor, for example, under the condition of serious packet disorder, choose a larger window.

To disable the function, in the IKE IPsec tunnel configuration mode, use the command **no anti-replay**.

Configuring VPN Track and Redundant Backup

FS devices can monitor the connectivity status of the specified VPN tunnel, and also allow backup or load sharing between two or more VPN tunnels. This function is applicable to both the route-based VPN and policy-based VPN. The practical implementation environments include:

- Configuring a backup VPN tunnel for the remote peer, at any time only one tunnel is active. Initially, the main VPN tunnel is active, if disconnection of the main tunnel is detected, the device will re-transmit the information flow through the backup tunnel;
- Configuring two or more VPN tunnels for the remote peer. All tunnels are active simultaneously, and load balance the traffic via equal-cost multi-path routing (ECMP). If disconnection of any tunnel is detected, the device will re-transmit the information flow through other tunnels.

The VPN track function tracks the status of the target tunnel by Ping packets. By default, the function is disabled. To configure the VPN track function, in IKE IPsec tunnel configuration mode, use the following command:

vpn-track [*A.B.C.D*] [**src-ip** *A.B.C.D*] [**interval** *time-value*] [**threshold** *value*]

- *A.B.C.D* – Specifies the IP address of the tracked object. When the peer is a FS device and the parameter is not specified, the system will use the IP address of the peer by default. This IP address can not be 0.0.0.0 or 255.255.255.255.
- **src-ip** *A.B.C.D* – Specifies the source IP address that sends Ping packets. When the peer device is a FS device and the parameter is not specified, the system will use the IP address of egress interface by default. This IP address cannot be 0.0.0.0 or 255.255.255.255.
- **interval** *time-value* – Specifies the interval of sending Ping packets. The value range is 1 to 255 seconds. The default value is 10.
- **threshold** *value* – Specifies the threshold for determining the track failure. If the system did not receive the specified number of continuous response packets, it will identify a track failure, i.e., the target tunnel is disconnected. The value range is 1 to 255. The default value is 10.

To disable the VPN track function, in IKE IPsec tunnel configuration mode, use the command **no vpn-track**.

By default, for route-based VPN, when the VPN track function detects disconnection of a VPN tunnel, it will inform the routing module about the information of the disconnected VPN tunnel and update the tunnel route information; for policy-based VPN, when the VPN track function detects disconnection of a VPN tunnel, it will inform the policy module about the information of the disconnected VPN tunnel and update the tunnel policy information. You can disable the VPN track failure notification function via CLI, so that the system will not send any tunnel track failure notification. By default, the system enables this function. To disable or enable the VPN track failure notification function, in the IKE IPsec tunnel configuration mode, use the following command:

track-event-notify {**disable** | **enable**}

- **disable** – Disable.
- **enable** – Enable. By default, the function is enabled.

The VPN track function can be in active or dead status. To view the VPN track status and configuration information via CLI, use the following commands:

- Show the status of VPN track: **show ipsec sa** {*id*}
- Show the configuration of VPN track: **show tunnel ipsec** {**manual** | **auto**} {*tunnel-name*}

For example:

```
Show the status of VPN track
hostname(config)# show ipsec sa 5
VPN Name: vpn1
Outbound
Gateway: 1.1.1.2
......
VPN track status: alive
Inbound
Gateway: 1.1.1.2
......
VPN track status: alive
Show the configuration of VPN track
hostname(config)# show tunnel ipsec auto vpn1
Name: vpn1
mode: tunnel
```

```
......
vpn-track: enable
tracknotify: enable
vpntrack destination 1.1.1.1
vpntrack source ip: 2.2.2.2
vpntrack interval: 3
vpntrack threshold: 3
```

Tip: For more examples of VPN track and redundant backup, see Example of Configuring Route-based VPN Track and Redundant Backup.

Setting a Commit Bit

You can set a commit bit to avoid packet loss and time difference. However, the commit bit may slow down the responding speed. To set a commit bit, in the IKE IPsec tunnel configuration mode, use the following command:

Responder sets a commit bit: **responder-set-commit**

Responder does not set a commit bit: **no responder-set-commit**

Specifying Description

To specify the description of IKE tunnel, in the IKE IPsec tunnel configuration mode, use the following command:

description *string*

- *string* – Specifies the description of the IKE tunnel.

To delete the description, in the IKE IPsec tunnel configuration mode, use the command **no description**.

Configuring Auto Routing

For IKEv1 VPN, if the address type for the peer of the created ISAKMP gateway is specified to be static or dynamic, route entry whose destination IP address is the local ID of the peer and next hop is tunnel interface will be added to the routing table automatically after you configure auto routing function and an IPSec SA is created. The auto routing function allows the device to automatically add routing entries from center to branch to avoid complexity of manual routing. When an IPSec SA is deleted, the corresponding route entry will be deleted from the routing table.

By default the auto routing is disabled. To enable it, in the ISAKMP gateway configuration mode, use the following command:

generate-route

To disable auto routing, use the command **no generate-route**.

IKEv2 VPN

The configurations of IKEv2 VPN include:

- Configuring a P1 proposal
- Configuring an IKEv2 peer
- Configuring a P2 proposal
- Configuring a tunnel

Configuring a P1 Proposal

P1 proposal is the IKEv2 security proposal that is used to store the security parameters during the IKE_SA_INIT exchange, including the encryption algorithm, hash algorithm, PRF (pseudo-random function) algorithm, and DH algorithm. A complete IKEv2 security proposal at least includes a set of parameters, including a encryption algorithm, a authentication method, a PRF algorithm, and a DH group.

Creating a P1 Proposal

To create a P1 proposal, i.e., an IKEv2 security proposal, in the global configuration mode, use the following command:

ikev2 proposoal *p1-name*

- *p1-name* – Specifies the name of the P1 proposal that will be created. After executing the command, the CLI will enter the P1 proposal configuration mode. You can configure parameters for P1 proposal in this mode.

To delete the specified P1 proposal, in the global configuration mode, use the command **no ikev2 proposoal** *p1-name*.

Specifying a Hash Algorithm

FSOS support the following hash algorithms: MD5, SHA-1, and SHA-2. SHA-2 includes SHA-256, SHA-384, and SHA-512. You can specify up to four hash algorithms. To specify the hash algorithm, in the P1 proposal configuration mode, use the following command:

```
hash {md5 | sha | sha256 | sha384 | sha512}
```

- md5 – Uses the MD5 hash algorithm. The digest length is 128 bits.
- sha – Uses the SHA-1 hash algorithm. The digest length is 160 bits. This is the default hash algorithm.
- sha256 – Uses the SHA-256 hash algorithm. The digest length is 256 bits.
- sha384 – Uses the SHA-384 hash algorithm. The digest length is 384 bits.
- sha512 – Uses the SHA-512 hash algorithm. The digest length is 512 bits.

To restore to the default hash algorithm, in the P1 proposal configuration mode, use the command **no hash**.

Specifying a PRF Algorithm

FSOS support the following PRF algorithms: MD5, SHA-1, and SHA-2. SHA-2 includes SHA-256, SHA-384, and SHA-512. You can specify up to four PRF algorithms. To specify the PRF algorithm, in the P1 proposal configuration mode, use the following command:

```
prf {md5 | sha | sha256 | sha384 | sha512}
```

- md5 – Uses the MD5 algorithm. The digest length is 128 bits.
- sha – Uses the SHA-1 algorithm. The digest length is 160 bits. This is the default hash algorithm.
- sha256 – Uses the SHA-256 algorithm. The digest length is 256 bits.
- sha384 – Uses the SHA-384 algorithm. The digest length is 384 bits.
- sha512 – Uses the SHA-512 algorithm. The digest length is 512 bits.

To restore to the default algorithm, in the P1 proposal configuration mode, use the command **no prf**.

Specifying an Encryption Algorithm

FSOS provides the following five encryption algorithms: 3DES, DES, 128bit AES, 192-bit AES and 256-bit AES. You can specify up to four algorithms. To specify the encryption algorithm of IKEv2 security proposal, in the P1 proposal configuration mode, use the following command:

```
encryption {3des | aes | aes-192 | aes-256}
```

- **3des** – Uses the 3DES encryption. The key length is 192 bits. This is the default algorithm for FSOS.
- **des** – Uses the DES encryption. The key length is 64 bits.
- **aes** – Uses the AES encryption. The key length is 128 bits.
- **aes-192** – Uses the 192-bit AES encryption. The key length is 192 bits.
- **aes-256** – Uses the 256-bit AES encryption. The key length is 256 bits.

To restore to the default encryption algorithm, in the P1 proposal configuration mode, use the command **no encryption**.

Selecting a DH Group

Diffie-Hellman (DH) is designed to establish a shared secret key. DH group determines the length of the element generating keys for DH exchange. The strength of keys is partially decided by the robustness of the DH group. To select a DH group, in the P1 proposal configuration mode, use the following command:

```
group {1 | 2 | 5 }
```

- 1 – Selects DH Group1. The key length is 768 bits.
- 2 – Selects DH Group2. The key length is 1024 bits. This is the default value.
- 5 – Selects DH Group5. The key length is 1536 bits.

To restore the DH group to the default, in the P1 proposal configuration mode, use the command **no group**.

Specifying the Lifetime of SA

The lifetime of IKEv2 SA does not need negotiation and it is determined by individual settings. The side with a less lifetime will re-negotiate and this can avoid that both sides start the negotiation at the same time. To specify the lifetime of IKEv2 SA for the local side, in the P1 proposal configuration mode, use the following command:

lifetime *time-value*

- *time-value* – Specifies the lifetime of IKEv2 SA. The value range is 180 to 86400 seconds. The default value is 28800.

To restore to the default lifetime, in the P1 proposal configuration mode, use the command **no lifetime**.

Configuring an IKEv2 Peer

After creating an IKEv2 peer, you can configure the IKE negotiation mode, IP address of the IKEv2 peer, IKE security proposal, local ID, etc.

Creating an IKEv2 Peer

To create an IKEv2 peer, in the global configuration mode, use the following command:

ikev2 peer *peer-name*

- *peer-name* – Specifies the name of the IKE peer.

After executing the command, the CLI will enter the IKEv2 peer configuration mode. You can configure parameters for the IKEv2 in this mode.

To delete the specified IKEv2 peer, in the global configuration mode, use the command **no ikev2 peer** *peer-name*.

Binding an Interface to the IKE Peer

To bind an interface to the IKEv2 peer, in the IKEv2 pper configuration mode, use the following command:

interface *interface-name*

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

To cancel the binding, in the IKEv2 peer configuration mode, use the command **no interface**.

Specifying the Remote IP Address

You can specify the remote IP address for the IKEv2 peer. To specify the remote IP address, in the IKEv2 peer configuration mode, use the following command:

match-peer *ip-address*

- *ip-address* - Specifies the remote IP address.

To cancel the IP address setting, in the IKEv2 peer configuration mode, use the command **no match-peer**.

Specifying an Authentication Method

FSOS supports the pre-shared key authentication and this is the default authentication method. To specify the authentication method as pre-shared key, use the following command:

auth psk

Specifying a P1 Proposal

To specify the P1 proposal for the IKEv2 peer, in IKEv2 peer configuration mode, use the following command:

ikev2-proposal *p1-name*

- *p1-name* – Specifies the name of the P1 proposal.

To cancel the specified P1 proposal, in IKEv2 peer configuration mode, use the command **no ikev2-proposal** *p1-name*.

Configuring a Local ID

To configure the local ID, in the IKEv2 peer configuration mode, use the following command:

local-id {**fqdn** *string* | **key-id** *string* |**ip** *ip-address* }

- **fqdn** *string* – Specifies the ID type of FQDN. *string* is the specific content of the ID.
- **key-id** *string* - Specifies the ID type of Key ID. *string* is the specific content of the ID.
- **ip** *ip-address* - Specifies the ID type of IP address. *ip-address* is the specific content of the ID.

To cancel the specified local ID, in the IKEv2 peer configuration mode, use the command **no local-id**.

Specifying a Connection Type

The created IKEv2 peer can be an initiator, responder, or both the initiator and responder. To specify the connection type, in the IKEv2 peer configuration mode, use the following command:

connection-type {**bidirectional** | **initiator-only** | **responder-only**}

- **bidirectional** – Specifies the IKEv2 peer as both the initiator and responder. This is the default option.
- **initiator-only** – Specifies the IKEv2 peer as the initiator only.
- **responder-only** – Specifies the IKEv2 peer as the responder only.

To restore to the default connection type, in the IKEv2 peer configuration mode, use the command **no connection-type**.

Creating a IKEv2 Profile

An IKEv2 profile can store the IKEv2 SA parameters that are not required negotiation, for example, the peer identity, the pre-shared key, and the information of the secured data traffic. You need to configure an IKEv2 profile at both responder side and the initiator side. To create an IKEv2 profile, in the IKEv2 peer configuration mode, use the following command:

ikev2-profile *profile-name*

- *profile-name* – Specifies the name of the IKEv2 profile.

After executing this command, the CLI will enter the IKEv2 profile configuration mode. You can configure the IKEv2 SA parameters that are not required negotiation in this mode.

In the IKEv2 peer configuration mode, use the **no ikev2-profile** *profile-name*command to delete the specified profile.

Configuring a Remote ID

To configure the remote ID, in the IKEv2 profile configuration mode, use the following command:

remote id {**fqdn** *string* | **key-id** *string* |**ip** *ip-address* }

- **fqdn** *string* – Specifies the ID type of FQDN. *string* is the specific content of the ID.

- **key-id** *string* - Specifies the ID type of Key ID. *string* is the specific content of the ID.
- **ip** *ip-address* - Specifies the ID type of IP address. *ip-address* is the specific content of the ID.

To cancel the specified remote ID, in the IKEv2 profile configuration mode, use the command **no remote id**.

Configuring a Pre-shared Key

If the pre-shared key authentication method is used, you need to specify a pre-shared key. To specify the pre-shared key, in the IKEv2 profile configuration mode, use the following command:

remote key *key-value*

- *key-value* – Specifies the content of the pre-shared key.

To cancel the specified pre-shared key, in the IKEv2 profile configuration mode, use the command **no remote key**.

Specifying the Information of the Secured Data Traffic

Use the traffic-selector parameter to specify the information of the secured data traffic. The IKEv2 tunnel can be established when the followowing conditions complete:

- The local source IP address and the remote destination IP address should be in the same segment.
- The local destination IP address and the remote source IP address should be in the same segment.

You can specify only one source IP address and one destination IP address by using the traffic-selector parameter in an IKEv2 profile. To configure the traffic-selector parameter, use the following command in the IKEv2 profile configuration mode:

traffic-selector {**src** | **dst**} **subnet** *ip/mask*

- **src** – Specifies the source IP address of the outbound traffic sent from the local.
- **dst** – Specifies the destination IP address of the inbound traffic received by the local.
- **subnet** *ip/mask* – Specifies the IP address and the netmask.

To cancel the configurations, use the command **no traffic-selector {src | dst} subnet** *ip/mask*.

Configuring a P2 Proposal

P2 proposal is the IPSec security proposal that is used to store the security parameters using by IPSec, including the security protocol, encryption algorithm, hash algorithm. The configurations of P2 proposal include protocol type, encryption algorithm, hash algorithm and lifetime.

To create a P2 proposal, i.e., an IPSec security proposal, in the global configuration mode, use the following command:

ikev2 ipsec proposal *p2-name*

- *p2-name* – Specifies the name of the P2 proposal that will be created. After executing the command, the CLI will enter the P2 proposal configuration mode. You can configure parameters for P2 proposal in this mode.

To delete the specified P2 proposal, in the global configuration mode, use the command **no ikev2 ipsec proposal** *p2-name*.

Specifying a Protocol Type

The protocol type available to P2 proposal is ESP. To specify a protocol type for P2 proposal, in the P2 proposal configuration mode, use the following command:

protocol esp

- **esp** – Uses ESP. This is the default protocol type.

Specifying a Hash Algorithm

You can specify 1 to 4 hash algorithms for P2 proposal. To specify the hash algorithm for P2 proposal, in the P2 proposal configuration mode, use the following command:

hash {md5 | sha | sha256 | sha384 | sha512 }

- **md5** – Uses the MD5 hash algorithm. The digest length is 128 bits.
- **sha** – Uses the SHA-1 hash algorithm. The digest length is 160 bits. This is the default hash algorithm.
- **sha256** – Uses the SHA-256 hash algorithm. The digest length is 256 bits.

- **sha384** – Uses the SHA-384 hash algorithm. The digest length is 384 bits.
- **sha512** – Uses the SHA-512 hash algorithm. The digest length is 512 bits.

To restore to the default hash algorithm, in the P2 proposal configuration mode, use the command **no hash**.

Specifying an Encryption Algorithm

You can specify 1 to 4 encryption algorithms for P2 proposal. To specify the encryption algorithm for P2 proposal, in the P2 proposal configuration mode, use the following command:

```
encryption {3des| des | aes-192 | aes-256 }
```

- **3des** – Uses the 3DES encryption. The key length is 192-bit. This is the default method for FSOS.
- **des** – Uses the DES encryption. The key length is 64 bits.
- **aes** – Uses the AES encryption. The key length is 128 bits.
- **aes-192** – Uses the 192-bit AES encryption. The key length is 192 bits.
- **aes-256** – Uses the 256-bit AES encryption. The key length is 256 bits.

To restore to the default encryption algorithm, in the P2 proposal configuration mode, use the command **no encryption**.

Configuring PFS

The PFS (Perfect Forward Security) function is designed to determine how to generate the new key instead of the time of generating the new key. PFS ensures that no matter what phase it is in, one key can only be used once, and the element used to generate the key can only be used once. The element will be discarded after generating a key, and will never be re-used to generate any other keys. Such a measure will assure that even if a single key is disclosed, the disclosure will only affect the data that is encrypted by the key, and will not threaten the entire communication. PFS is based on the DH algorithm. To configure PFS, in the P2 proposal configuration mode, use the following command:

```
group {nopfs | 1 | 2 | 5}
```

- **nopfs** – Disables PFS. This is the default option.
- **1** – Selects DH Group1. The key length is 768 bits.

- 2 – Selects DH Group2. The key length is 1024 bits.
- 5 – Selects DH Group5. The key length is 1536 bits.

To restore to the default PFS configuration, in the P2 proposal configuration mode, use the command **no group**.

Specifying a Lifetime

You can evaluate the lifetime by the time length. When the IPSec SA lifetime runs out, the SA will get expired and requires a new SA negotiation. To specify the lifetime for the P2 proposal, in the P2 proposal configuration mode, use the following commands:

lifetime *seconds*

- *seconds* – Specifies the lifetime of time length type. The value range is 180 to 86400 seconds. The default value is 28800.

lifesize *kilobytes*

- *kilobytes* – Specifies the lifetime of traffic volume type. The value range is 1800 to 4194303 KB. The default value is 1800.

To cancel the specified lifetime, in the P2 proposal configuration mode, use the following commands **no lifetime**.

Configuring a Tunnel

When configuring an IPSec tunnel through IKEv2, you need to configure the following options: the operation mode, IKEv2 peer, IKEv2 security proposal, and auto-connection.

Creating an IKEv2 Tunnel

To create an IKEv2 tunnel, in the global configuration mode, use the following command:

tunnel ipsec *tunnel-name* **ikev2**

- **tunnel-name** - Specifies the name of the IKEv2 tunnel that will be created.

After executing the above command, the CLI will enter the IKEv2 tunnel configuration mode. All the parameters of the IKEv2 tunnel need to be configured in the IKEv2 tunnel configuration mode.

To delete the specified IKEv2 tunnel, in the global configuration mode, use the command **no tunnel ipsec** *tunnel-name* **ikev2**.

Specifying the Operation Mode

The system supports the operation mode of IPsec protocol as transport. This is the default mode.

Specifying an IKEv2 Peer

To specify an IKEv2 peer for the IKEv2 tunnel, in the IKEv2 tunnel configuration mode, use the following command:

ikev2-peer *peer-name*

- *peer-name* – Specifies the name of the IKEv2 peer.

To cancel the specified IKEv2 peer, in the IKEv2 tunnel configuration mode, use the command **no ikev2-peer**.

Specifying a P2 Proposal

To specify a P2 proposal for the IKEv2 tunnel, in the IKEv2 tunnel configuration mode, use the following command:

ipsec-proposal p2-name1 [p2-name2] [p2-name3]

- p2-name – Specifies the name of the P2 proposal. You can specify up to 3 P2 proposals.

To cancel the specified P2 proposal for the IKEv2 tunnel, in the IKEv2 tunnel configuration mode, use the command **no ipsec-proposal**.

Configuring Auto-connection

The device supports the SA establishment by using the auto-connection mode. In the auto mode, the device detects the SA status every 60 seconds and initiates negotiation request when SA is not established. To use the auto mode, in the IKEv2 tunnel configuration mode, use the following command:

auto-connect

To restore to the default mode, in the IKE tunnel configuration mode, use the command **`no auto-connect`**.

Note: Auto connection works only when the local device is acting as the initiator.

XAUTH

XAUTH, an extension and enhancement to IKE, allows a device to authenticate users who are trying to gain access to IPsec VPN network combined with the authentication server (RADIUS and local AAA server) configured on the device. XAUTH is now widely used on mobile devices. When a remote user initiates a request for VPN connection, the XAUTH server on the device will interrupt the VPN negotiation and prompt the user to type a valid username and password. If succeeded, the XAUTH server will go on with the subsequent VPN negotiation procedure and assign IP addresses for legal clients, otherwise it will drop the VPN connection.

Tip: For more information about how to configure an authentication server, see "Authentication" .

The configuration of XAUTH includes:

- Enabling an XAUTH server
- Configuring an XAUTH address pool
- Binding an address pool to the XAUTH server
- Configuring an IP binding rule
- Configuring a WINS/DNS server

Enabling an XAUTH Server

XAUTH server is disabled by default. To enable the XAUTH server, in the ISAKMP configuration mode, use the following command:

```
xauth server
```

To disable the XAUTH server, in the ISAKMP configuration mode, use the following command:

```
no xauth server
```

Configuring an XAUTH Address Pool

XAUTH address pool is used to store IP addresses allocated to clients. When a client connects to its server, the server will take an IP address from the address pool according to the client propriety (like DNS server address or WIN server address) and give it to the client.

To configure an XAUTH address pool, in the global configuration mode, use the following command:

xauth pool *pool-name*

- *pool-name* - Specifies a name for the address pool, and enter the XAUTH address pool configuration mode; if the pool with this name exists, you will enter its configuration mode directly.

To delete the specified XAUTH address pool, in the global configuration mode, use the following command:

no xauth pool p*ool-name*

To configure the allocatable IP range of an XAUTH address pool, in the XAUTH address pool configuration mode, use the following command:

address *start-ip end-ip* **netmask** *mask*

- *start-ip* - Specifies the start IP address.
- *end-ip* - Specifies the end IP address.
- *mask* - Specifies the network mask for this IP address range.

To delete the specified IP range of an address pool, in the XAUTH address pool configuration mode, use the following command:

no address

Some addresses in the address pool need to be reserved for other devices. These reserved IP addresses are not allowed to allocate to XAUTH clients.

To configure the start IP and end IP of reserved IP range, in the XAUTH address pool configuration mode, use the following command:

exclude-address *start-ip end-ip*

- *start-ip* - Specifies the start IP for reserved IP range.
- *end-ip* - Specifies the end IP for reserved IP range.

To delete the reserved address range, in the XAUTH address pool configuration mode, use the following command:

no exclude-address

Binding an Address Pool to the XAUTH Server

The XAUTH address pool will not take effect until being bound to an XAUTH server. To bind the specified XAUTH address pool to the XAUTH server, in the ISAKMP configuration mode, use the following command:

xauth pool-name *pool-name*

- *pool-name* - Specifies the name of binding address pool.

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

no xauth pool-name

Configuring IP Binding Rules

If an XAUTH client needs static IP address, IP-user binding rule can be applied to meet this requirement. Binding the user of XAUTH client to an IP address in the address pool can guarantee that this IP address is allocated to the XAUTH client when it reaches the server. In addition, IP address for an XAUTH client can be defined to an address range by using IP-role binding which defines an IP range for this role. When a client with the role connects to the server, it gets one address from the IP addresses bound to this role.

When an XAUTH server allocates IP addresses, it follows the rules below:

1. If the client which needs a static IP has had its IP-user binding configured, the server allocates the bound IP to it. Note that if such a bound IP address is in use, the client applying for the address is not allowed to log into the server.
2. If a client uses IP-role binding rule, the server takes an IP address from the bound IP range and allocates it to the client. Otherwise, the server takes an IP address from the unbound IP range and allocates it to the client. If IP addresses in the IP range is not available, the user cannot log into the server.

Note:IP addresses in the IP-user binding rules and those in the IP-role binding rules should not conflict with each other.

To bind an IP address to a user, in the XAUTH address pool configuration mode, use the following command:

ip-binding user *user-name* **ip** *ip-address*

- **user** *user-name* - Specifies the username.
- **ip** *ip-address* - Specifies an available IP address in the address pool which will be bound to the user.

To cancel an IP-user binding, in the XAUTH address pool configuration mode, use the following command:

no ip-binding user *user-name*

To bind an IP address to a role, in the XAUTH address pool configuration mode, use the following command:

ip-binding role *role-name* **ip-range** *start-ip end-ip*

- **role** *role-name* - Specifies the role name.
- **ip-range** *start-ip end-ip* - Specifies the available IP range (start IP address and end IP address) in the address pool.

To cancel a binding between an IP range and a role, in the XAUTH address pool configuration mode, use the following command:

no ip-binding role *role-name*

Changing the Sequence of IP-Role Binding

Normally, if a user belongs to multiple roles which bind to different IP addresses, the system searches for the first rule which matches the user and applies the IP address under this rule to the user. By default, new rule is at the bottom of the rule list.

To move the position of an IP-role binding rule in the rule list, in the XAUTH address pool configuration mode, use the following command:

move *role-name1* {**before** *role-name2* | **after***role-name2*| **top** | **bottom**}

- *role* －*name1* － Specifies the role whose binding you want to move.
- **before** *role-name2* － Moves the binding rule before the IP-role binding specified here.
- **after** *role-name2* － Moves the binding rule after the IP-role binding specified here.
- **top** － Moves the binding rule to the top of the IP-role binding rule list.
- **bottom** － Moves the binding rule to the bottom of the IP-role binding rule list.

Configuring a WINS/DNS Server

To specify a DNS server, in the XAUTH address pool configuration mode, use the following command:

dns *address1* [*address2*]

- *address1* - Specifies the IP address of DNS servers. You can specify up to two addresses.

To cancel the DNS setting, in the XAUTH address pool configuration mode, use the following command:

no dns

To specify a WINS server, in the XAUTH address pool configuration mode, use the following command:

wins *address1* [*address2*]

- *address1* - Specifies the IP address of WINS servers. You can specify up to two addresses.

To cancel the WINS setting, in the XAUTH address pool configuration mode, use the following command:

no wins

Kicking out an XAUTH Client

The XAUTH server can force to disconnect with a client. To kick out an XAUTH client, in the execution mode, use the following command:

exec xauth *isakmp-peer-name* **kickout** *user-name*

- *isakmp-peer-name* - Specifies the ISAKMP peer name.
- *user-name* - Specifies the name of client to be kicked out of the server.

Viewing IPsec Configuration

To view the configuration information of IPsec, in any mode, use the following commands:

- Show the configuration information of P1 proposal: **show isakmp proposal** [**p1-name**]
- Show the configuration information of ISAKMP gateway: **show isakmp peer** [*peer-name*]
- Showing the configuration information of P2 proposal: **show ipsec proposal** [*proposal-name*]
- Show the configuration information of manual key VPN tunnel: **show tunnel ipsec manual** [*tunnel-name*]
- Showing the configuration information of IKE tunnel: **show tunnel ipsec auto** [*tunnel-name*]
- Show the configuration information of IKE SA: **show isakmp sa** [*dsp_ip*]

- Show the configuration information of IPsec SA: **show ipsec sa** [*id* | **active** | **inactive**]
- Show the XAUTH address pool information: **show xauth pool** [*pool-name*]
- Show the XAUTH client information: **show xauth client** *isakmp-peer-name* [**user** *user-name*]

Examples of Configuring IPsec VPN

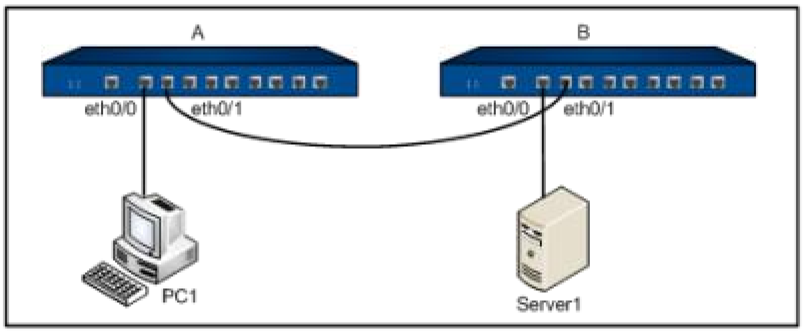
This section describes two examples of establishing SA by manual key VPN and IKE VPN respectively, an example of VPN track and redundant backup and an example of XAUTH configuration.

Example of Configuring Manual Key VPN

The manual key VPN tunnel requires that all the related SA configurations need to be completed manually. See the example below:

Requirement

There is a tunnel between FS Device A and B. PC1 is a host behind Device A, with the IP address 188.1.1.2 and gateway 188.1.1.1; Server1 is the server behind Device B, with IP address 10.110.8.210 and gateway 10.110.88.220. The goal of this configuration example is to protect the communication between the subnet of PC1 (188.1.1.0/24) and the subnet of Server1 (10.110.88.0/24), using the method of route-based VPN. Use ESP as the security protocol, 3DES as encryption algorithm, SHA1 as hash algorithm and DEFLATE as compression algorithm. The network topology is shown in the following figure.



Configuration Steps

Step 1: Configure interfaces

```
Device Ahostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 188.1.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1

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

hostname(config-if-eth0/1)# ip address 192.168.1.2/24

hostname(config-if-eth0/1)# exitip address 10.1.1.1/24

Device B

hostname(config-if-eth0/0)# zone trust

hostname(config-if-eth0/0)# ip address 10.110.88.220/24

hostname(config-if-eth0/0)# exit

hostname(config)# interface ethernet0/0

hostname(config)# interface ethernet0/1

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

hostname(config-if-eth0/1)# ip address 192.168.1.3/24

hostname(config-if-eth0/1)# exitip route 172.16.10.0/24 tunnel1 10
```

Step 2: Configure routes

```
Device Ahostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# ip route 10.110.88.0/24 192.168.1.3

hostname(config-vrouter)# exit

Device B

hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# ip route 188.1.1.0/24 192.168.1.2

hostname(config-vrouter)# exit
```

Step 3: Configure a tunnel name VPN1

```
Device Ahostname(config)# tunnel ipsec vpn1 manual

hostname(config-tunnel-ipsec-manual)# interface ethernet0/1

hostname(config-tunnel-ipsec-manual)# protocol esp

hostname(config-tunnel-ipsec-manual)# peer 192.168.1.3

hostname(config-tunnel-ipsec-manual)# hash sha
hostname(config-tunnel-ipsec-manual)# hash-key inbound 1234 outbound 5678
hostname(config-tunnel-ipsec-manual)# encryption 3des
hostname(config-tunnel-ipsec-manual)# encryption-key inbound 00ff outbound 123a
hostname(config-tunnel-ipsec-manual)# compression deflate
hostname(config-tunnel-ipsec-manual)# spi 6001 6002
hostname(config-tunnel-ipsec-manual)# exit
Device B
hostname(config)# tunnel ipsec vpn1 manual
hostname(config-tunnel-ipsec-manual)# interface ethernet0/1
hostname(config-tunnel-ipsec-manual)# protocol esp
hostname(config-tunnel-ipsec-manual)# peer 192.168.1.2
hostname(config-tunnel-ipsec-manual)# hash sha
hostname(config-tunnel-ipsec-manual)# hash-key inbound 5678 outbound 1234
hostname(config-tunnel-ipsec-manual)# encryption 3des
hostname(config-tunnel-ipsec-manual)# encryption-key inbound 123a outbound 00ff
hostname(config-tunnel-ipsec-manual)# compression deflate
hostname(config-tunnel-ipsec-manual)# spi 6002 6001
hostname(config-tunnel-ipsec-manual)# exit
```

Step 4: Configure policy rules

```
Device A
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn1
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
Device B
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn1
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn1
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

When the settings above are completed, the security tunnel between Device A and Device B has been successfully established. Then, the data transmission between the subnet 188.1.1.0/24 and subnet 10.110.88.0/24 is encrypted.

Example of Configuring IKE VPN

This section describes an example of IKE VPN configuration.

Requirement

There is a tunnel between FS Device A and B. PC1 is a host behind Device A, with the IP address 10.1.1.1 and gateway 10.1.1.2; Server1 is the server behind Device B, with IP address 192.168.1.1 and gateway 192.168.1.2. The goal of this configuration example is to protect the communication between the subnet of PC1 (10.1.1.0/24) and the subnet of Server1 (192.168.1.0/24), using the method of route-based VPN. Use ESP as the security protocol, 3DES as the encryption algorithm, SHA1 as the hash algorithm and DEFLATE as compression algorithm.

Configuration Steps

Step 1: Configure the interfaces

```
Device A
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 10.1.1.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# exit
Device B
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# exit
```

Step 2: Configure policy rules

```
Device A
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
Device B
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 3: Configure routes

```
Device A
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 192.168.1.0/24 tunnel1
hostname(config-vrouter)# exit
Device B
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 10.1.1.0/24 tunnel1
hostname(config-vrouter)# exit
```

Step 4: Configure a P1 proposal

```
Device A
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash sha
hostname(config-isakmp-proposal)# encryption 3des
hostname(config-isakmp-proposal)# exit
Device B
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash sha
hostname(config-isakmp-proposal)# encryption 3des
hostname(config-isakmp-proposal)# exit
```

Step 5: Configure an ISAKMP gateway

```
Device A
hostname(config)# isakmp peer east
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 1.1.1.2
hostname(config-isakmp-peer)# pre-share hello1
hostname(config-isakmp-peer)# exit
Device B
hostname(config)# isakmp peer west
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 1.1.1.1
hostname(config-isakmp-peer)# pre-share hello1
hostname(config-isakmp-peer)# exit
```

Step 6: Configure a P2 proposal

```
Device A
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash sha
hostname(config-ipsec-proposal)# encryption 3des
hostname(config-ipsec-proposal)# compression deflate
hostname(config-ipsec-proposal)# exit
Device B
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash sha
hostname(config-ipsec-proposal)# encryption 3des
hostname(config-ipsec-proposal)# compression deflate
hostname(config-ipsec-proposal)# exit
```

Step 7: Configure a tunnel name VPN

```
Device A
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer east
hostname(config-tunnel-ipsec-auto)# id local 10.1.1.0/24 remote 192.168.1.0/24 service any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# tunnel ipsec vpn
hostname(config-if-tun1)# exit
Device B
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer east
hostname(config-tunnel-ipsec-auto)# id local 192.168.1.0/24 remote 10.1.1.0/24 service any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# tunnel ipsec vpn
hostname(config-if-tun1)# exit
```

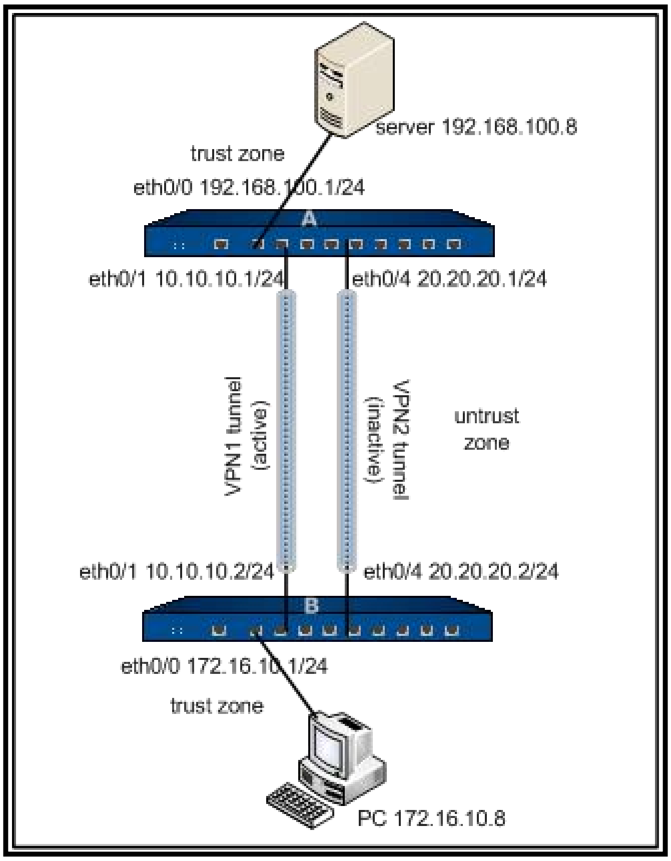
When the settings are completed, the security tunnel between Device A and Device B has been successfully established. The data transmission between the subnet 10.1.1.0/24 and subnet 192.168.1.0/24 is encrypted.

Example of Configuring Route-based VPN Track and Redundant Backup

This section describes a route-based VPN track and redundant backup example.

Requirement

There are two IKE VPN tunnels named VPN1 tunnel and VPN2 tunnel respectively between FS Device A and Device B. The server is behind Device A, with the IP address of 192.168.100.8, and gateway address of 192.168.100.1; PC is behind Device B, with the IP address of 172.16.10.8, and gateway address of 172.16.10.1. The requirement is tracking the VPN status of VPN1 tunnel and VPN2 tunnel. When the main tunnel (VPN1 tunnel) link fails, traffic will be diverted to the backup tunnel (VPN2 tunnel); when the main tunnel recovers, the flow will be switched back to the main tunnel. The network topology is shown in the following figure:



Configuration Steps

Step 1: Configure Device A

```
Configure interfaces:
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.100.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.10.10.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# zone untrust
hostname(config-if-eth0/4)# ip address 20.20.20.1/24
hostname(config-if-eth0/4)# exit
```

Configure a P1 proposal:

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash md5
hostname(config-isakmp-proposal)# encryption des
hostname(config-isakmp-proposal)# exit
```

Configure an ISAKMP gateway:

```
hostname(config)# isakmp peer gwa-peer-1
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 10.10.10.2
hostname(config-isakmp-peer)# pre-share U8FdHNEEBz6sNn5Mvqx3yWuLRWce
hostname(config-isakmp-peer)# exit
hostname(config)# isakmp peer gwa-peer-2
hostname(config-isakmp-peer)# interface ethernet0/4
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 20.20.20.2
hostname(config-isakmp-peer)# pre-share i39jnnNiCSh9rXb77oGA7Fg7BNQy
hostname(config-isakmp-peer)# exit
```

Configure a P2 proposal:

```
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash md5
hostname(config-ipsec-proposal)# encryption des
hostname(config-ipsec-proposal)# exit
```

Configure VPN tunnels:

```
hostname(config)# tunnel ipsec vpn1-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-1
hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold 9
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# tunnel ipsec vpn2-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-2
hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold 9
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)# auto-connect
hostname(config-tunnel-ipsec-auto)# exit
```

Create tunnel interfaces and bind to the VPN tunnels:

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)#
hostname(config-if-tun1)# tunnel ipsec vpn1-tunnel
hostname(config-if-tun1)# exit
hostname(config)# interface tunnel2
hostname(config-if-tun2)# zone untrust

hostname(config-if-tun2)# ip address 10.2.2.1/24

hostname(config-if-tun2)# tunnel ipsec vpn2-tunnel

hostname(config-if-tun2)# exit

Configure routes:

hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)#

hostname(config-vrouter)# ip route 172.16.10.0/24 tunnel2 20

hostname(config-vrouter)# exit

Configure policy rules:

hostname(config)# policy-global

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone trust

hostname(config-policy-rule)# dst-zone untrust

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone untrust

hostname(config-policy-rule)# dst-zone trust

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config-policy)# exit
hostname(config)#
```

Step 2: Configure Device B

Configure interfaces

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 172.16.10.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.10.10.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# zone untrust
hostname(config-if-eth0/4)# ip address 20.20.20.2/24
hostname(config-if-eth0/4)# exit
```

Configure a P1 proposal

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash md5
hostname(config-isakmp-proposal)# encryption des
hostname(config-isakmp-proposal)# exit
```

Configure an ISAKMP gateway

```
hostname(config)# isakmp peer gwb-peer-1
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 10.10.10.1
hostname(config-isakmp-peer)# pre-share U8FdHNEEBz6sNn5Mvqx3yWuLRWce
hostname(config-isakmp-peer)# exit
hostname(config)# isakmp peer gwb-peer-2
hostname(config-isakmp-peer)# interface ethernet0/4
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 20.20.20.1
hostname(config-isakmp-peer)# pre-share i39jnnNiCSh9rXb77oGA7Fg7BNQy
hostname(config-isakmp-peer)# exit
```

Configure a P2 proposal

```
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash md5
hostname(config-ipsec-proposal)# encryption des
hostname(config-ipsec-proposal)# exit
```

Configure VPN tunnels

```
hostname(config)# tunnel ipsec vpn1-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwb-peer-1
hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold 9
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)# auto-connect
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# tunnel ipsec vpn2-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwb-peer-2
hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold 9
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)# auto-connect
hostname(config-tunnel-ipsec-auto)# exit
```

Create tunnel interfaces and bind to the VPN tunnels

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ip address 10.1.1.2/24
hostname(config-if-tun1)# tunnel ipsec vpn1-tunnel
hostname(config-if-tun1)# exit
hostname(config)# interface tunnel2
hostname(config-if-tun2)# zone untrust
hostname(config-if-tun2)# ip address 10.2.2.2/24
hostname(config-if-tun2)# tunnel ipsec vpn2-tunnel
hostname(config-if-tun2)# exit
```

Configure routes

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 192.168.100.0/24 tunnel1 1
hostname(config-vrouter)# ip route 192.168.100.0/24 tunnel2 2
hostname(config-vrouter)# exit
```

Configure policy rules

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

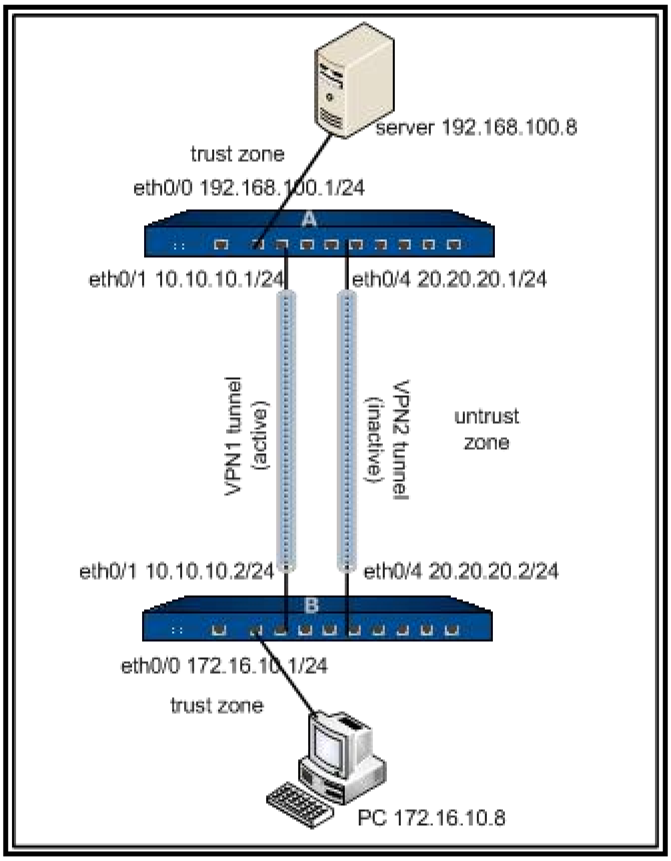
In this example both the VPN devices are FS devices, so you can use the default source and destination addresses for VPN track.

Example of Configuring Policy-based VPN Track and Redundant Backup

This section describes a policy-based VPN track and redundant backup example.

Requirement

There are two IKE VPN tunnels named VPN1 tunnel and VPN2 tunnel respectively between FS Device A and Device B. The server is behind Device A, with the IP address of 192.168.100.8, and gateway address of 192.168.100.1; PC is behind Device B, with the IP address of 172.16.10.8, and gateway address of 172.16.10.1. The requirement is tracking the VPN status of VPN1 tunnel and VPN2 tunnel. When the main tunnel (VPN1 tunnel) link fails, traffic will be diverted to the backup tunnel (VPN2 tunnel); when the main tunnel recovers, the flow will be switched back to the main tunnel. The network topology is shown in the following figure:



Configuration Steps

Step 1: Configure Device A

```
Configure interfaces:

hostname(config)# interface ethernet0/0

hostname(config-if-eth0/0)# zone trust

hostname(config-if-eth0/0)# ip address 192.168.100.1/24

hostname(config-if-eth0/0)# exit

hostname(config)# interface ethernet0/1

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

hostname(config-if-eth0/1)# ip address 10.10.10.1/24

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

hostname(config)# interface ethernet0/4

hostname(config-if-eth0/4)# zone untrust

hostname(config-if-eth0/4)# ip address 20.20.20.1/24
hostname(config-if-eth0/4)# exit
Configure the route:
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 172.16.10.0/24 20.20.20.2
hostname(config-vrouter)# exit
Configure a P1 proposal:
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash md5
hostname(config-isakmp-proposal)# encryption des
hostname(config-isakmp-proposal)# exit
Configure an ISAKMP gateway:
hostname(config)# isakmp peer gwa-peer-1
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 10.10.10.2
hostname(config-isakmp-peer)# pre-shareU8FdHNEEBz6sNn5Mvqx3yWuLRWce
hostname(config-isakmp-peer)# exit
hostname(config)# isakmp peer gwa-peer-2
hostname(config-isakmp-peer)# interface ethernet0/4
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 20.20.20.2
hostname(config-isakmp-peer)# pre-share i39jnnNiCSh9rXb77oGA7Fg7BNQy
hostname(config-isakmp-peer)# exit
Configure a P2 proposal:
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash md5
hostname(config-ipsec-proposal)# encryption des
hostname(config-ipsec-proposal)# exit
```

Configure a VPN tunnel:

```
hostname(config)# tunnel ipsec vpn1-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-1
hostname(config-tunnel-ipsec-auto)# vpn-track interval 1 threshold 5
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# tunnel ipsec vpn2-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-2
hostname(config-tunnel-ipsec-auto)# vpn-track interval 1 threshold 5
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)#auto-connect
hostname(config-tunnel-ipsec-auto)# exit
```

Configure policy rules:

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# src-ip 192.168.100.8/24
hostname(config-policy-rule)# dst-ip 172.16.10.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn1-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 2
hostname(config-policy-rule)# src-ip 172.16.10.8/24
hostname(config-policy-rule)# dst-ip 192.168.100.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn1-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# src-ip 192.168.100.8/24
hostname(config-policy-rule)# dst-ip 172.16.10.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn2-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 4
hostname(config-policy-rule)# src-ip 172.16.10.8/24
hostname(config-policy-rule)# dst-ip 192.168.100.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn2-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 5
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 2: Configure Device B

```
Configure interfaces:
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 172.16.10.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.10.10.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# zone untrust
hostname(config-if-eth0/4)# ip address 20.20.20.2/24
hostname(config-if-eth0/4)# exit
```

Configure the route:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 192.168.100.0/24 20.20.20.1
hostname(config-vrouter)# exit
```

Configure a P1 proposal:

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash md5
hostname(config-isakmp-proposal)# encryption des
hostname(config-isakmp-proposal)# exit
```

Configure an ISAKMP gateway:

```
hostname(config)# isakmp peer gwb-peer-1
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 10.10.10.1
hostname(config-isakmp-peer)# pre-shareU8FdHNEEBz6sNn5Mvqx3yWuLRWce
hostname(config-isakmp-peer)# exit
hostname(config)# isakmp peer gwb-peer-2
hostname(config-isakmp-peer)# interface ethernet0/4
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 20.20.20.1
hostname(config-isakmp-peer)# pre-sharei39jnnNiCSh9rXb77oGA7Fg7BNQy
hostname(config-isakmp-peer)# exit
```

Configure a P2 proposal:

```
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash md5
hostname(config-ipsec-proposal)# encryption des
hostname(config-ipsec-proposal)# exit
```

Configure a VPN tunnel:

```
hostname(config)# tunnel ipsec vpn1-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwb-peer-1
hostname(config-tunnel-ipsec-auto)# vpn-track interval 1threshold 5
hostname(config-tunnel-ipsec-auto)# auto-connect
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# tunnel ipsec vpn2-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-2
hostname(config-tunnel-ipsec-auto)# vpn-track interval 1 threshold 5
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)#auto-connect
hostname(config-tunnel-ipsec-auto)# exit
```

Configure policy rules:

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# src-ip 172.16.10.8/24
hostname(config-policy-rule)# dst-ip 192.168.100.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn1-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 2
hostname(config-policy-rule)# src-ip 192.168.100.8/24
hostname(config-policy-rule)# dst-ip 172.16.10.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn1-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# src-ip 172.16.10.8/24
hostname(config-policy-rule)# dst-ip 192.168.100.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn2-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 4
hostname(config-policy-rule)# src-ip 192.168.100.8/24
hostname(config-policy-rule)# dst-ip 172.16.10.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn2-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 5
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

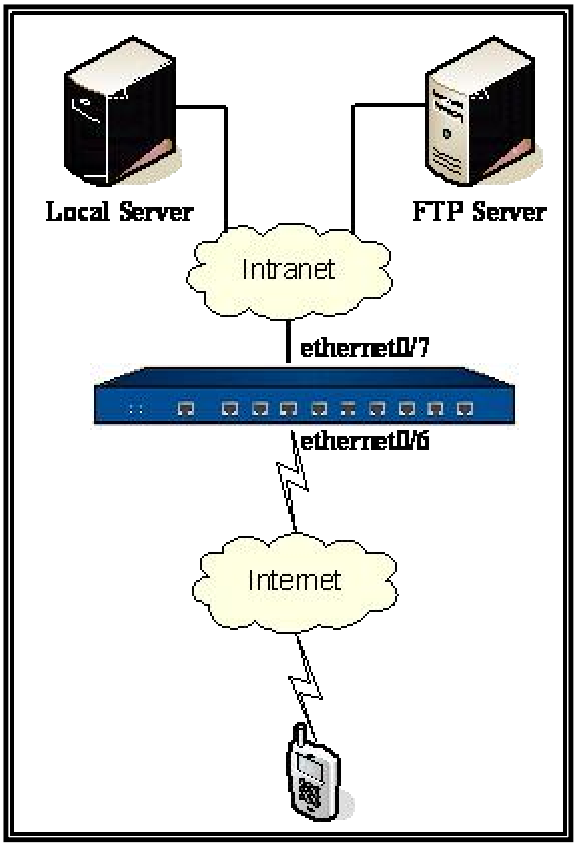
In this example both the VPN devices are FS devices, so you can use the default source and destination addresses for VPN track.

Example of Configuring XAUTH

This section describes a typical XAUTH configuration example.

Requirement

FS device is enabled with XAUTH server, and uses the local AAA server for user authentication. When a user is trying to launch a VPN connection and gain access to internal resources via a mobile phone, the XAUTH server will authenticate the user by a pre-shared key, and permit the authenticated users to access to internal resources. The network topology is shown in the following figure:



Configuration Steps

Step 1: Configure interfaces, zones and policies

```
hostname(config)# interface ethernet0/6
hostname(config-if-eth0/7)# zone trust
hostname(config-if-eth0/7)# ip address 6.6.6.6 255.255.255.0
hostname(config-if-eth0/7)# manage ping
hostname(config-if-eth0/7)# manage ssh
hostname(config-if-eth0/7)# manage http
hostname(config-if-eth0/7)# exit
hostname(config)# interface ethernet0/7
hostname(config-if-eth0/6)# zone untrust
hostname(config-if-eth0/6)# ip address 7.7.7.7 255.255.255.0
hostname(config-if-eth0/6)# exit
hostname(config)# rule top
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 2: Configure an AAA server

```
hostname(config)# aaa-server local type local
hostname(config-aaa-server)# user xauth
hostname(config-user)# password test
hostname(config-user)# ike-id key-id xauth
hostname(config-user)# end
hostname(config)#
```

Step 3: Configure an XAUTH address pool

```
hostname(config)# xauth pool pool
hostname(config-xauth-pool)# address 9.9.9.9 9.9.9.99 netmask 255.255.255.0
hostname(config-xauth-pool)# exit

hostname(config)#
```

Step 4: Configure an ISAKMP peer

```
hostname(config)# isakmp peer xauth

hostname(config-isakmp-peer)# mode aggresive

hostname(config-isakmp-peer)# type usergroup

hostname(config-isakmp-peer)# psk-sha-aes128-g2

hostname(config-isakmp-peer)# pre-share XhF44BilJO3b/2HFl5lVqXniqeMByq

hostname(config-isakmp-peer)# aaa-server local

hostname(config-isakmp-peer)# local-id key-id xauth

hostname(config-isakmp-peer)# xauth pool-name pool

hostname(config-isakmp-peer)# xauth server

hostname(config-isakmp-peer)# interfaceethernet0/7

hostname(config-isakmp-peer)# exit

hostname(config)#
```

Step 5: Configure an IKE tunnel and tunnel interface

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

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

hostname(config-tunnel-ipsec-auto)# esp-sha-aes128-g0

hostname(config-tunnel-ipsec-auto)# accept-all-proxy-id

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

hostname(config)# interface tunnel22

hostname(config-if-tun22)# zone trust

hostname(config-if-tun22)# ip address 9.9.9.1 255.255.255.0

hostname(config-if-tun22)# manage telnet

hostname(config-if-tun22)# manage ssh

hostname(config-if-tun22)# manage ping
hostname(config-if-tun22)# manage http

hostname(config-if-tun22)# manage https

hostname(config-if-tun22)# manage snmp

hostname(config-if-tun22)# tunnel ipsec xauth

hostname(config-if-tun22)# exit

hostname(config)#
```

After the above steps, the mobile phone user can complete the authentication procedure via the VPN client bundled with Android or iOS (username auth, password test, IPsec identifier/group name xauth) and gain access to internal resources.

Example of Using IPsec VPN in HA Peer Mode

The HA peer mode supports IPsec VPN. By using an example, this section introduces how to integrate HA peer mode with IPsec VPN in the asymmetric routing environment. Before configuring the relevant functions, ensure that both FS devices have the same hardware platform, firmware version, and license.

After completing the configurations, both devices are working in the HA peer mode and enable the IPsec VPN function. The traffic from the PC to the server is via the Device A and is secured by the IPsec VPN configured in Device A. The backward traffic from the server to the PC is via the Device B and is secured by the IPsec VPN configured in Device B. If one device or its relevant links are down, the traffic will be forwarded and secured by the other device. The topology is shown as below:

Configuration Steps

Step 1: Configure HA peer mode

```
Device Ahostname(config)# ha link interface eth0/4

hostname(config)# ha link ip 1.1.1.1/24

hostname(config)# ha group 0

hostname(config-ha-group)# priority 50

hostname(config-ha-group)# exit

hostname(config)# ha group 1

hostname(config-ha-group)# priority 100

hostname(config-ha-group)# exit

Device B
```

```
hostname(config)# ha link interface eth0/4

hostname(config)# ha link ip 1.1.1.2/24

hostname(config)# ha group 0

hostname(config-ha-group)# priority 100

hostname(config-ha-group)# exit

hostname(config)# ha group 1

hostname(config-ha-group)# priority 50

hostname(config-ha-group)# exit
```

Step 2: Configure VFI interface, add router and NAT rules

```
Device A

hostname(config)# interface eth0/1:1

hostname(con-if-eth0/1:1)# zone untrust

hostname(con-if-eth0/1:1)# ip address192.168.10.1/24

hostname(con-if-eth0/1:1)# exit

hostname(config)# interface eth0/0:1

hostname(con-if-eth0/2:1)# zone trust

hostname(con-if-eth0/2:1)# ip address192.168.20.1/24

hostname(con-if-eth0/2:1)# exit
```

Step 3: Configure IPsec VPN

```
Device A

hostname(M0D1)(config)# isakmp peer peer1

hostname(M0D1)(config-isakmp-peer)# interface ethernet0/1

hostname(M0D1)(config-isakmp-peer)# peer 192.168.1.2

hostname(M0D1)(config-isakmp-peer)# isakmp-proposal psk-md5-des-g2

hostname(M0D1)(config-isakmp-peer)# pre-share fs

hostname(M0D1)(config-isakmp-peer)# exit

hostname(M0D1)(config)# isakmp peer peer2
hostname(M0D1)(config-isakmp-peer)# interface ethernet0/1:1
hostname(M0D1)(config-isakmp-peer)# peer 192.168.10.2
hostname(M0D1)(config-isakmp-peer)# isakmp-proposal psk-md5-des-g2
hostname(M0D1)(config-isakmp-peer)#  pre-share fs1111
hostname(M0D1)(config-isakmp-peer)# exit
hostname(M0D1)(config)# tunnel ipsec vpn1 auto
hostname(M0D1)(config-tunnel-ipsec-auto)# isakmp-peer peer1
hostname(M0D1)(config-tunnel-ipsec-auto)# ipsec-proposal esp-md5-des-g2
hostname(M0D1)(config-tunnel-ipsec-auto)# exit
hostname(M0D1)(config)# tunnel ipsec vpn2 auto
hostname(M0D1)(config-tunnel-ipsec-auto)# isakmp-peer peer2
hostname(M0D1)(config-tunnel-ipsec-auto)# ipsec-proposal esp-md5-des-g2
hostname(M0D1)(config-tunnel-ipsec-auto)# exit
hostname(M0D1)(config)# int tunnel1
hostname(M0D1)(config-if-tun1)# zone vpn
hostname(M0D1)(config-if-tun1)# tunnel ipsec vpn1
hostname(M0D1)(config-if-tun1)# exit
hostname(M0D1)(config)# int tunnel1:1
hostname(M0D1)(config-if-tun1)# zone vpn
hostname(M0D1)(config-if-tun1)# tunnel ipsec vpn2
hostname(M0D1)(config-if-tun1)# exit
Device C
hostname(config)# isakmp peer peer1
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# peer 192.168.1.1
hostname(config-isakmp-peer)# isakmp-proposal psk-md5-des-g2
hostname(config-isakmp-peer)# pre-share fs
hostname(config-isakmp-peer)# exit
hostname(config)# isakmp peer peer2
hostname(config-isakmp-peer)# interface ethernet0/2
hostname(config-isakmp-peer)# peer 192.168.10.1
hostname(config-isakmp-peer)# isakmp-proposal psk-md5-des-g2
hostname(config-isakmp-peer)# pre-share fs1111
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec vpn1 auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer peer1
hostname(config-tunnel-ipsec-auto)# ipsec-proposal esp-md5-des-g2
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# tunnel ipsec vpn2 auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer peer2
hostname(config-tunnel-ipsec-auto)# ipsec-proposal esp-md5-des-g2
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# int tunnel1
hostname(config-if-tun1)# zone vpn
hostname(config-if-tun1)# tunnel ipsecvpn1
hostname(config-if-tun1)# exit
hostname(config)# int tunnel2
hostname(config-if-tun1)# zone vpn
hostname(config-if-tun1)# tunnel ipsec vpn2
hostname(config-if-tun1)# exit
```

Step 4: Configure policy and route for VPN

```
Device Ahostname(M0D1)(config)# ip vrouter trust-vr
hostname(M0D1)(config-vrouter)# ip route192.168.1.2/24 tunnel1
hostname(M0D1)(config-vrouter)# ip route 192.168.10.2/24 tunnel1:1
hostname(M0D1)(config-vrouter)# ip route 172.16.20.0/24 192.168.2.2
hostname(M0D1)(config-vrouter)# ip route 172.16.20.0/24 192.168.20.2
hostname(M0D1)(config-vrouter)# exit

hostname(M0D1)(config)# rule id 1 from any to any service any permit

Device C

hostname(config)# ip vrouter trust-vr

hostname(config)# ip route 172.16.20.0/24 tunnel1 20

hostname(config)# ip route 172.16.20.0/24 tunnel2 10

hostname(config)# exit

hostname(config)# rule id 1 from any to any service any permit
```

SSL VPN

Overview

The device provides an SSL based remote access solution. Remote users can access the Intranet resources safely through SSL VPN.

SSL VPN requires an SSL VPN server and an SSL VPN client. SSL VPN server provides the following functions:

- Accepting connections from the client;
- Assigning IP addresses, DNS server addresses, and WIN server addresses to SSL VPN clients;
- Authenticating and authorizing SSL VPN clients;
- Security check of SSL VPN client hosts;
- Encrypting and forwarding IPsec data.

The SSL VPN client for FS devices is called FS Security Connect. You can download and install it on your PC. When your client has successfully connected to the SSL VPN server, your communication with the server is encrypted and secured.

The default concurrent online client number may vary from hardware platforms. If you want to have a larger client number, consult your local agents to purchase new SSL VPN license.

Configuring SSL VPN Server

This section describes the following configurations about SSL VPN server:

- Configuring an SSL VPN Address Pool
- Configuring Resources List
- Configuring a UDP Port
- Configuring an SSL VPN Instance
- Binding the SSL VPN Instance to a Tunnel Interface
- Authentication Using UKey Certificate
- Host Binding
- Host Check
- Optimal Path Detection
- Force Disconnecting an SSL VPN Client
- Changing the Password of Local User

Configuring an SSL VPN Address Pool

SSL VPN address pool is used to store IP addresses allocated to SSL VPN clients. When a client connects to its server, the server will take an IP address from the address pool according to the client propriety (like DNS server address or WIN server address) and give it to the client.

scvpn pool *pool-name*

- *pool-name* – Specifies a name for the address pool.

This command creates a new address pool and leads you into the SSL VPN address pool configuration mode; if the pool with this name exists, you will enter its configuration mode directly.

To delete an SSL VPN address pool, in the global configuration mode, use the following command:

no scvpn pool *pool-name*

The following sections explain how to configure SSL VPN address pool, including:

- Configuring an address range and network mask of a pool
- Configuring excluded addresses
- Configuring an IP binding rule

- Configuring a DNS server
- Configuring a WINS server

Configuring an IP Range of the Address Pool

To configure the start ip, end ip and network mask of an SSL VPN address pool, in the address pool configuration mode, use the following command:

address *start-ip end-ip* **netmask** *A.B.C.D*

- *start-ip* – Specifies the start IP address.
- *end-ip* – Specifies the end IP address.
- **netmask** *A.B.C.D* – Specifies the network mask for this IP address range.

To delete the IP range setting of an address pool, in the SSL VPN address pool configuration mode, use the following command:

no address

Configuring Reserved Addresses

Some addresses in the address pool need to be reserved for other devices, like gateways, FTP servers, etc. These reserved IP addresses are not allowed to allocate to SSL VPN clients.

To configure the start IP and end IP of reserved IP range, in the SSL VPN address pool configuration mode, use the following command:

exclude address *start-ip end-ip*

- *start-ip* – Specifies the start IP for reserved IP range.
- *end-ip* – Specifies the end IP for reserved IP range.

To delete the reserved address range, in the SSL VPN address pool configuration mode, use the following command:

no exclude

Configuring IP Binding Rules

If an SSL VPN client needs static IP address, IP-user binding rule can be applied to meet this requirement. Binding the user of SSL VPN client to an IP address in the address pool can guarantee that this IP address is allocated to the SSL VPN client when it reaches the server. In addition, IP address for an SSL VPN client can be defined to an address range by using IP-role binding which defines an IP range for this role. When a client with the role connects to the server, it gets one address from the IP addresses bound to this role.

When an SSL VPN server allocates IP addresses, it follows the rules below:

1. Check whether the IP-user binding rule is configured for the client. If yes, allocate the bound IP to the client; if no, the server will select an IP which is not bound or used from the address pool, then allocate it to the client.
2. Check whether the IP-role binding rule is configured for the client. If yes, get an IP from the IP range and allocate to the client; if no, the server will select an IP which is not bound or used from the address pool, then allocate it to the client.

Note:IP addresses in the IP-user binding rules and those in the IP-role binding rules should not conflict with each other.

Binding an IP to a User

To bind an IP address to a user, in the SSL VPN address pool configuration mode, use the following command:

ip-binding user *user-name* **ip** *ip-address*

- **user** *user-name* − Specifies the username.
- **ip** *ip-address* − Specifies an available IP address in the address pool which will be bound to the user.

To cancel an IP-user binding, in the SSL VPN address pool configuration mode, use the following command:

no ip-binding user *user-name*

Binding an IP to a Role

To bind an IP address to a role, in the SSL VPN address pool configuration mode, use the following command:

ip-binding role *role-name* **ip_range** *start-ip end-ip*

- **role** *role -name* − Specifies the role name.
- **ip_range** *start-ip end-ip* − Specifies the available IP range (start IP address and end IP address) in the address pool.

To cancel a binding between an IP range and a role, in the SSL VPN address pool configuration mode, use the following command:

no ip-binding role *role-name*

Changing the Sequence of IP-Role Binding

Normally, if a user belongs to multiple roles which bind to different IP addresses, the system searches for the first rule which matches the user and applies the IP address under this rule to the user. By default, new rule is at the bottom of the rule list.

To move the position of an IP-role binding rule in the rule list, in the SSL VPN address pool configuration mode, use the following command:

move *role-name1* {**before** *role-name2* | **after** *role-name2*| **top** | **bottom**}

- *role –name1* – Specifies the role whose binding you want to move.
- **before** *role-name2* – Moves the binding rule before the IP-role binding specified here.
- **after** *role-name2* – Moves the binding rule after the IP-role binding specified here.
- **top** – Moves the binding rule to the top of the IP-role binding rule list.
- **bottom** – Moves the binding rule to the bottom of the IP-role binding rule list.

Configuring a DNS Server

To specify a DNS server, in the SSL VPN address pool configuration mode, use the following command:

dns *address1* [*address2*] [*address3*] [*address4*]

- *address1* – Specifies the IP address of DNS servers. You can specify up to four addresses.

To cancel the DNS setting, in the SSL VPN address pool configuration mode, use the following command:

no dns

Configuring a WINS Server

To specify a WINS server, in the SSL VPN address pool configuration mode, use the following command:

wins *address1* [*address2*]

- *address1* − Specifies the IP address of WINS server. You can specify up to two WINS servers.

To cancel the WINS server setting, in the SSL VPN address pool configuration mode, use the following command:

no wins

Viewing SSL VPN Address Pool

To view information about an SSL VPN address pool, in any mode, use the following command:

show scvpn pool [*pool-name*]

- *pool-name* − Specifies the name of SSL VPN address pool to be shown. If this parameter is not specified, you can view all SSL VPN address pools.

Here is an example of viewing SSL VPN address pool:

```
hostname(config)# show scvpn pool pool_test1

Name: pool_test1

Address range: 3.3.3.1 - 3.3.3.10 (start IP and end IP)

Exclude range: 3.3.3.1 - 3.3.3.2 (reserved IP addresses)

Netmask: 255.255.255.0 (network mask of the address pool)

Wins server: (WINS server setting)

wins1: 10.1.1.1

Dns server:  (DNS server setting)

dns1: 10.10.209.1

IP Binding User: (IP-user binding)

test 3.3.3.8

IP Binding Role: (IP-role binding)

role1 3.3.3.3 3.3.3.7
```

To view statistical information about an SSL VPN address pool, in any mode, use the following command:

show scvpn pool *pool-name* **statistics**

- *pool-name* – Specifies the name of SSL VPN address pool whose statistics you want to view.

Here is an example of viewing statistics of an SSL VPN address pool:

```
hostname(config)# show scvpn pool pool_test1 statistics
Total Ip Num 10 (total IP count in the address pool)
Exclude Ip Num 2 (reserved IP count)
Fixed Ip Num 6 (bound IP count)
Used Ip Num 2 (assigned IP count)
Fixed Used Ip Num 0 (assigned IP among the bound IP addresses)
Free Ip Num 6 (available IP count in the address pool)
```

Configuring Resources List

Resource list refers to resources configured in the system that can be easily accessible by users. Each resource contains multiple resource items. The resource item is presented in the form of resource item name followed by 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 which the user can access to the client. After that, the client will analyze and make the IE browser that your system comes with pop up a page to display the received resource list information so that the user can access the private network resource directly by clicking the URL link. The resource list page is poped up only once after the authentication is passed. If a user does not belong to any user group, the browser will not pop up the resource list page after authentication is passed.

To configure a SSL VPN resource, in the global configuration mode, use the following command:

scvpn resource-list *list-name*

- *list-name* – Specifies the resource name. The value range is 1 to 31.

After this command is executed, you will enter SSL VPN resource list configuration mode and you can continue to configure resource items for the new resource. To delete a resource, in the global configuration mode, use the following command:

no resource-list *list-name*

Tip:

- Less than 48 resources can be configured in a SSL VPN instance.
- The resource list function is only available for Windows SSL VPN clients.

Adding Resource Items

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. To add resource items for resource, in SSL VPN resource list configuration mode, use the following command:

name *name* **url** *url-string*

- *name* – Specifies the name for resource item. The value range is 1 to 63.
- *url-string* – Specifies the URL for resource item. The value range is 1 to 255.

To delete a resource item, in SSL VPN resource list configuration mode, use the following command:

no name *name*

Viewing Resource List

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

show scvpn resource-list [*list-name*]

- *list-name* – Specifies the resource name you want to view. The value range is 1 to 31. Information about all resources will be displayed if you keep this parameter unconfigured.

Configuring a UDP Port

To specify the UDP port number of SSL VPN connection, in the global configuration mode, use the following command:

scvpn-udp-port *port-number*

- *port-number* – Specifies the UDP port number. The value range is 1 to 65535. The default value is 4433.

When UDP port number is specified, all SSL VPN connections will communicate on this port.

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

no scvpn-udp-port

Configuring an SSL VPN Instance

To create an SSL VPN instance, in the global configuration mode, use the following command:

tunnel scvpn *instance-name*

- *instance-name* – Specifies a name for the SSL VPN instance.

This command creates an SSL VPN instance and leads you into the SSL VPN instance configuration mode; if the instance exists, you will enter the SSL VPN instance configuration mode directly.

To delete an SSL VPN instance, in the SSL VPN instance configuration mode, use the following command:

no tunnel scvpn *instance-name*

This section describes how to configure an SSL VPN instance, including:

- Specifying an address pool
- Specifying a server interface
- Specifying an SSL protocol version
- Specifying a PKI trust domain
- Specifying algorithms for the tunnel
- Specifying an AAA server
- Specifying an HTTPS port number
- Configuring anti-replay
- Configuring packet fragmentation
- Configuring idle time
- Configuring multi-logon
- Configuring URL redirection
- Configuring an SSL VPN tunnel route
- Clearing cache data of the host that uses the SSL VPN client
- Using SSL VPN in HA peer mode
- Binding L2TP VPN instance
- Binding Resources

Specifying an Address Pool

To specify an SSL VPN address pool for the SSL VPN instance, in the SSL VPN instance configuration mode, use the following command:

pool *pool-name*

- *pool-name* － Specifies the name of SSL VPN address pool.

To cancel the SSL VPN address pool, in the SSL VPN instance configuration mode, use the following command:

no pool

Specifying a Server Interface

The client uses HTTPS protocol to access to the device. To specify the SSL VPN interface of the device, in the SSL VPN instance configuration mode, use the following command:

interface *interface-name*

- *interface-name* － Specifies the name of the interface for the SSL VPN client to connect.

To cancel the SSL VPN interface, in the SSL VPN instance configuration mode, use the following command:

no interface *interface-name*

Specifying an SSL Protocol Version

To specify the SSL protocol version of an SSL VPN instance, in the SSL VPN instance configuration mode, use the following command:

ssl-protocol {**sslv3** | **tlsv1** | **tlsv1.2** | **gmsslv1.0** | **any**}

- **sslv3** － Uses SSLv3 protocol.
- **tlsv1** － Uses TLSv1 protocol.
- **tlsv1.2** － Uses TLSv1.2 protocol.
- **gmsslv1.0** － Uses GMSSLv1.0 protocol. After selecting this option, you’re recommended to select the trust domain that contains SM2 type key for the PKI trust domain and the encrypted trust domain. The SM4 is preferred for encryption algorithm and the SM3 is preferred for hash algorithm.
- **any** － Uses any of the following protocols: SSLv2, SSLv3, TLSv1, TLSv1.1 and TLSv1.2. This is the default option.

To restore to the default value, in the SSL VPN instance configuration mode, use the following command:

no ssl-protocol

If tlsv1.2 or any is specified to the SSL protocol in SSL VPN server, you need to convert the certificate that you are going to import to the browser or certificate in the USB Key to make it support the tlsv1.2 protocol before the digital certificate authentication via SSL VPN client, so that the SSL VPN server can be connected successfully when the Username/Password + Digital Certificate or Digital Certificate Only authentication method is selected. Prepare a PC with Windows or Linux system which has been installed with OpenSSL 1.0.1 or later before processing the certificate.

We will take the certificate file named oldcert.pfx as an example, the procedure is as follows:

1. In the OpenSSL software interface, enter the following command to convert a certificate in .pfx format to a certificate in .pem format: openssl pkcs12 －in oldcert.pfx －out cert.pem
2. Enter the following command to convert the certificate in .pem format to a .pfx format certificate that supports tlsv1.2 protocol: openssl pkcs12 －export －in cert.pem －out newcert.pfx －CSP “Microsoft Enhanced RSA and AES Cryptographic Provider”
3. Import the newly generated .pfx format certificate into your browser or USB Key.

After the above operation, you have to log into SSL VPN server with SSL VPN client whose version is 1.4.6.1239 or later. When configuring an SSL VPN function that uses the GM standard, you need to install the SSL VPN client that supports the GM standard on the PC(The current windows client version that supports GM standard is 1.4.7.1252), and log in with the username/password of GM.

Specifying a PKI Trust Domain

PKI trust domain in SSL VPN is used in HTTPS authentication.

To specify a PKI trust domain for SSL VPN instance, in the SSL VPN instance configuration mode, use the following command:

trust-domain *trust-domain-name*

- *trust-domain-name* － Specifies the name of PKI trust domain. The default domain is trust_domain_default.

To restore to the default value, in the SSL VPN instance configuration mode, use the following command:

no trust-domain

Tip: For information on how to create a PKI trust domain, see "PKI" in the "User Authentication"

Specifying an Encryption Trust Domain

To specify the encryption trust domain which is usded for the GMSSL negotiation for the SSL VPN, in the SSL VPN configuration mode, use the following command:

trust-domain-enc *enc-cert*

- *enc-cert* – Specifies the encryption for the GMSSL negotiation, trust domain that system predefined.

To delete the configured encryption trust domain, in the SSL VPN configuration mode, use the following command:

no trust-domain-enc

Specifying Algorithms for the Tunnel

Tunnel algorithms include encryption algorithm and authentication algorithm.

To specify algorithms for the tunnel, in the SSL VPN instance configuration mode, use the following command:

tunnel-cipher encryption {null | des | 3des | aes | aes192 | aes256 | sm4} hash {null | md5 | sha | sha256 | sha384 | sha512 | sm3} [compression defl]

- **null | des | 3des | aes | aes192 | aes256 | sm4** – Specifies an encryption algorithm. The default value is 3des. Null means no encryption is specified. For more information about encryption algorithms, see Encryption Algorithm.
- **null | md5 | sha | sha256 | sha384 | sha512| sm3** – Specifies an authentication algorithm. The default value is sha. Null means no authentication is specified. For more information about authentication algorithms, see Hash Algorithm.
- **compression defl** – Specifies the compression algorithm DEFALTE. The default setting is no compression. For more information on compression algorithms, see Compression Algorithm.

To restore to the default algorithm settings, in the SSL VPN instance configuration mode, use the following command:

no tunnel-cipher

Specifying an AAA Server

AAA server in SSL VPN is used for client user authentication.

To specify an AAA server, in the SSL VPN instance configuration mode, use the following command:

aaa-server *aaa-server-name* [**domain** *domain-name*] [**keep-domain-name**]

- aaa-server-name – Specifies the name of AAA server you want to use for authentication.
- **domain** *domain-name* – Specifies the domain for the AAA server so that it can be distinguished from other servers.
- **keep-domain-name** – After specifying this parameter, the AAA server uses the full name of the user, including the username and the domain name, to perform the authentication.

To cancel the AAA server in an SSL VPN, in the SSL VPN instance configuration mode, use the following command:

no aaa-server *aaa-server-name* [**domain** *domain-name*]

Specifying an HTTPS Port Number

HTTPS port is used for the clients to access the device.

To specify an HTTPS port number, in the SSL VPN instance configuration mode, use the following command:

https-port *port-number*

- *port-number* – Specifies a port number of HTTPS protocol in SSL VPN instance. The range is 1 to 65535. The default value is 4433. As Web browser uses port 443 for HTTPS, do not choose 443 as the SSL VPN HTTPS port number. If multiple SSL VPN instances use the same interface, their HTTPS ports should have different port numbers.

To restore to the default value, in the SSL VPN instance configuration mode, use the following command:

no https-port

Configuring an SCVPN Tunnel Route

To reach the destination network segment or destination domain name through SCVPN tunnel, you need to specify them by configuring the SCVPN tunnel route.

- The specified destination network segment will be distributed to the VPN client, then the client uses it to generate the route to the specified destination.

- The specified destination domain name will be distributed to the VPN client, and the client will generate the route to the specified destination according to the resolving results from DNS.

Specifying the Network Segment

To reach the destination network segment through SCVPN tunnel, in the SCVPN instance configuration mode, use the following command:

split-tunnel-route *ip-address/netmask* [**metric** *metric-number*]

- *ip-address/netmask* – Specifies the IP address and network mask of the destination network segment.
- **metric** *metric-number* – Specifies a metric value for the route. The value range is 1 to 9999. The default value is 35.

To delete a route, in the SCVPN instance configuration mode, use the following command:

no split-tunnel-route *ip-address/netmask* [**metric** *metric-number*]

Specifying the Domain Name

After specifying the domain name, the system will distribute it to the client. The client will generate the route to the specified destination according to the resolving results from DNS. To specify the domain name, in the SCVPN instance configuration mode, use the following command:

domain-route {**disable** | **enable** | **max-entries** *value* | *url*}

- **disable** – Does not distribute the specified domain name to the client. This is the default option.
- **enable** – Distributes the specified domain name to the client.
- **max-entries** *value* – The maximum numbers of routes that can be generated after obtaining the resolved IP addresses of the domain name. The default value is 1000. The value ranges from 1 to 10000.
- *url* – Specify the URL of the domain name. You can add one each time and you can add up to 64 domain names. The URL cannot exceed 63 characters and it cannot end with a dot (.). Both wildcards and a single top level domain, e.g. **com** and **.com** are not supported.

To delete the specified domain name, use the following command in the SCVPN instance configuration mode:

no domain-route *url*

Configuring Anti-replay

Anti-replay is used to prevent hackers from injecting the captured packets repeatedly by rejecting the packets.

To enable anti-replay, in the SSL VPN instance configuration mode, use the following command:

```
anti-replay {32 | 64 | 128 | 256 | 512}
```

- 32 – Specifies that the anti-replay window size is 32. This is the default value.
- 64 – Specifies that the anti-replay window size is 64.
- 128 – Specifies that the anti-replay window size is 128.
- 256 – Specifies that the anti-replay window size is 256.
- 512 – Specifies that the anti-replay window size is 512.

Bigger window size suits more in bad network conditions, such as serious packets disorder.

To restore the anti-replay window size to the default value, in the SSL VPN instance configuration mode, use the following command:

no anti-replay

Configuring Packet Fragmentation

You can specify if packet fragmentation is permitted in the device.

To configure packet fragmentation, in the SSL VPN instance configuration mode, use the following command:

```
df-bit {copy | clear | set}
```

- copy - Copies the DF value from the destination of the packet. This is the default value.
- clear - Permits packet fragmentation.
- set - Forbids packet fragmentation.

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

no df-bit

Configuring Idle Time

Idle time defines the time length a client is allowed to connect to the device without any operation. When a client takes no action for the time period of idle time specified here, it is forced to log out the device.

To specify the idle time, in the SSL VPN instance configuration mode, use the following command:

idle-time *time-value*

- *time-value* − Specifies the idle time value. The value range is 15 to 1500 minutes. The default value is 30.

To restore to the default value, in the SSL VPN instance configuration mode, use the following command:

no idle-time

Configuring Multi-logon

To allow multiple users to log in at multiple places with the same username simultaneously, in the SSL VPN configuration mode, use the following command:

allow-multi-logon

This command enables the function and does not limit the login number. If you want to specify the number of users logging in with the same username simultaneously, in the SSL VPN configuration mode, use the following command:

allow-multi-logon number *number*

- *number* − Specifies the number of users who are allowed to login with one username. The value range is 1 to 99999999.

To disable multi-login, in the SSL VPN instance configuration mode, use the following command:

no allow-multi-logon

Configuring URL Redirection

URL redirection function in SSL VPN server displays a specified URL page to the authenticated client user. By default, this function is disabled.

To enable URL redirection, in the SSL VPN instance configuration mode, use the following command:

redirect-url *url* **title-en** *name* **title-zh** *name*

- *url* – Specifies the url address of the page shown for the new authenticated client. The value range is 1 to 255 bytes. It can be an HTTP (http://) or an HTTPS (https://) address.
- **title-en** *name* – Specifies a description for the redirect page. The value range is 1 to 31 bytes. When the system language of the client PC is English, this description will be shown in the client' s menu.

To cancel URL redirection, in the SSL VPN instance configuration mode, use the following command:

no redirect-url

URL Format

You should follow the format of redirected URL pages defined by FSOS. The format may vary from URL types. Here are some format requirements for HTTP URL:

- For pages of UTF-8 encoding, type URL + username=$USER&password=$PWD, for example, type the address http://www.abc.com/oa/login.do?username=$USER&password=$PWD.
- For pages of GB2312 encoding, type URL + username=$GBUSER&password=$PWD, for example, type the address http://www.abc.com/oa/login.do?username=$GBUSER&password=$PWD.
- For other pages, type http://www.abc.com.

Note:For configuration example of URL redirection feature, see Example of Configuring URL Redirect.

Configuring an SSL VPN Tunnel Route

SSL VPN tunnel route is the route from SSL VPN to the destination network segment. The route, distributed to the SSL VPN client by the device, allows the client to reach its destination.

To configure an SSL VPN route, in the SSL VPN instance configuration mode, use the following command:

split-tunnel-route *ip-address/netmask* [**metric** *metric-number*]

- *ip-address/netmask* – Specifies the IP address and network mask of the destination.
- **metric** *metric-number* – Specifies a metric value for the route. The value range is 1 to 9999. The default value is 35.

To delete a route, in the SSL VPN instance configuration mode, use the following command:

no split-tunnel-route *ip-address/netmask* [**metric** *metric-number*]

Clearing Cache Data of the Host that Uses the SSL VPN Client

For the security of the private data in the host that uses the SSL VPN client, you can clear the cache data including the cache data in the Web temporary and other temporary files. To enable this function, use the following command in the SSL VPN instance configuration mode:

host-cache-clear enable

To disable this function, use the following command in the SSL VPN instance configuration mode:

host-cache-clear disable

Using SSL VPN in HA Peer Mode

In the network environment using HA peer mode, configure SSL VPN in both FS devices. When one device or its relevant links are down, the SSL VPN client can re-connect to the other device. You need to configure the reconnection address table. The SSL VPN client will re-connect to the SSL VPN server according to the priority of the reconnection address. If the SSL VPN client fails to re-connect to the server, it will try every address in the reconnection address table until it can connect to the server. You can at most specify four reconnection address. The priority is based on the order you specified. The first one you configured has the high priority and the last one you configured has the low priority. To configure the reconnection address table, use the following command in the SSL VPN instance configuration mode:

cluster { **ip** *A.B.C.D* | **domain** *url* } [**port** *port-number*] [{ **ip** *A.B.C.D* | **domain** *url* } [**port** *port-number*]] [{ **ip** *A.B.C.D* | **domain** *url* } [**port** *port-number*]] [{ **ip** *A.B.C.D* | **domain** *url* } [**port** *port-number*]]

- **ip** *A.B.C.D* | **domain** *url* − Enter the IP address or the domain name of the SSL VPN server.
- **port** *port-number* − Enter the port number that the SSL VPN server used. The default port is 4433.

Use the **no cluster** command to clear the above settings.

When using this new function, note the following matters:

- If you select the **Auto Reconnect** option in the SSL VPN client and use the client-auto-connect count command to set the reconnection times as unlimited, the SSL VPN client will only re-connect to the originally configured server, and will not re-connect to the server specified in the reconnection address table. If you set the reconnection times as X, the SSL VPN client will re-connect to the server in the table after X times of failed attempts to the originally configured server.

- If you does not select the **Auto Reconnect** option in the SSL VPN client, the SSL VPN client will directly re-connect to the server you specified in the reconnection address table
- When using the firmware that supports the using of SSL VPN in HA peer mode, the SSL VPN whose version is lower than 1.4.4.1207 can connect to the SSL VPN server if the server has no reconnection address table configured. FSOS will inform the users to update the SSL VPN client. If the server has configured the reconnection address table, the SSL VPN whose version is lower than 1.4.4.1207 cannot connect to SSL VPN server. You need to uninstall the client and login to the SSL VPN Web Login page to download the new version of the SSL VPN client. Then install the new version. The new version is compatible with the firmware that does not support this new function.

Binding L2TP VPN Instance

When using the SSL VPN client for iOS to connect the SSL VPN server, you need to bind a L2TP VPN instance to the SSL VPN instane and the bound L2TP VPN needs to reference an IPSec tunnel. To configure the binding settings, use the following command in the SSL VPN instance configuration mode:

client-bind-lns *tunnel-name*

- *tunnel-name* – Specifies the name of the L2TP VPN instance you want to bind. This L2TP VPN instance needs to reference an IPSec tunnel. To cancel the binding settings, use the following command: **no client-bind-lns**

The L2TP VPN instance and the IPSec tunnel mentioned above must meet the following requirements:

- The authentication method of the IPSec tunnel must be pre-shared key authentication.
- The secret string of the L2TP instance (specified by the secret secret-string command) must be the same as pre-shared key of the IPSec tunnel.
- The AAA servers used by the L2TP instance and the SSL VPN instance must be the same.
- The address pool of the L2TP instance must be configured correctly. The device will allocate the corresponding IP addresses using the address pool of the L2TP instance.

Binding Resources

Only after binding rules between resources and user groups has been configured, can the SSL VPN client make the IE browser pop up a page to display the received resource list information after the authentication is passed. 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.

To configure a binding rule, use the following command in the SSL VPN instance configuration mode:

bind resource-list *list-name* **user-group** *aaa-server-name group-name*

- *list-name* – Specifies the resource name. The value range is 1 to 31.
- *aaa-server-name* – Specifies the AAA server name which the user group belongs to. Currently, only the local authentication server and the RADIUS server are available.
- *group-name* – Specifies the user group name.

To cancel the binding settings, in the SSL VPN instance configuration mode, use the following command:

no bind resource-list *list-name* **user-group** *aaa-server-name group-name*

Binding SSL VPN Instance to a Tunnel Interface

Only when an SSL VPN instance binds to a tunnel interface can it take effect.

To bind an SSL VPN instance to a tunnel interface, in the tunnel interface configuration mode, use the following command:

tunnel scvpn *instance-name*

- *instance-name* – Specifies the name of the SSL VPN instance you want to bind.

To cancel the binding of an SSL VPN instance, in the tunnel interface configuration mode, use the following command:

no tunnel scvpn *instance-name*

Authentication with USB Key Certificate

The client is allowed to use a USB flash disk that stores a certificate to authenticate. A USB disk which supports Windows SDK (Certificate Store Functions) and has a legal UKey certificate can pass the authentication and connect to the server.

The following sections describe how to configure USB Key certificate authentication, including:

- Enabling USB Key certificate authentication
- Importing a CA certificate to a trust domain
- Configuring a trust domain

Enabling USB Key Certificate Authentication

By default, this function is disabled. To enable the USB Key certificate authentication, in the SSL VPN instance configuration mode, use the following command:

client-cert-authentication [**usbkey-only**]

- **usbkey-only** – Specifies the USB Key authentication as USB Key only. If this parameter is not specified, the authentication of Username/Password + USB Key will be used.

To disable the function, in the SSL VPN instance configuration mode, use the following command:

no client-cert-authentication [**usbkey-only**]

Importing a USB Key Certificate to a Trust Domain

CA certificates can be imported through various methods, including downloading from an FTP or TFTP server and from USB disk. To import a certificate, in the execution mode, use the following command:

import pki *trust-domain-name* **cacert from** {**ftp server** *ip-address* [**user** *user-name***password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} *file-name*

- *trust-domain-name* – Specifies the name of PKI trust domain.
- **ftp server ip-address** [**user** *user-name* **password** *password*] – Specifies the IP address of FTP server, username and password to log in. If the server supports anonymous login, skip the username and password.
- **tftp server** *ip-address* – Specifies the IP address of TFTP server.
- **usb0 | usb1** – Specifies the port to which the USB disk is plugged.
- *file-name* – Specifies the file name of CA certificate which must be in the root directory of the USB disk.

Specifying a Trust Domain for the CA Certificate

USB Key certificate authentication requires a trust domain for the CA certificate. When the certificate provided from client matches one of the trust domain certificates, it passes authentication.

To specify a trust domain, in the SSL VPN instance configuration mode, use the following command:

client-auth-trust-domain *trust-domain*

- *trust-domain* – Specifies a configured PKI trust domain for the CA certificate. Repeat this command to add more trust domains. The system supports up to 10 domains.

To cancel a PKI trust domain for a certificate, in the SSL VPN instance configuration mode, use the following command:

no client-auth-trust-domain *trust-domain*

> Tip: For information on how to create PKI trust domain, see "PKI" in the "User Authentication"

Host Binding

Host binding is used to authenticate the hosts of SSL VPN clients. When you use the SSL VPN client to log into the server, the client collects information about the PC running it, including mainboard SN, hardware SN, CPU ID and BIOS SN, and uses MD5 algorithm to generate a 32-bit string, which is the host ID. Then, the client sends the host ID with username and password to the SSL VPN server for authentication. The SSL VPN server authenticates the user by looking up the candidate list and binding list.

The candidate list and binding list are described as below:

- Candidate list: A table recording username and host ID as well as their mapping relationship.
- Binding list: A table of authorized host IDs and their usernames. You can add a pair of host ID and its username to the table or allow login user to be added automatically. When a client logs in, the SSL VPN server checks if the binding list has the host ID and matched username, if so, the user passes authentication; if not, the SSL VPN communication will be disconnected.

Enabling Host Binding

By default, host binding is disabled. To enable host binding, in the SSL VPN instance configuration mode, use the following command:

user-host-verify [**allow-multi-host**] [**allow-shared-host**] [**auto-approved-first-bind**]

- **user-host-verify** – Enables host binding. By default, a user is allowed to log into the server using one single computer.
- **allow-multi-host** – Allows one user to log in using multiple hosts.
- **allow-shared-host** – Allows multiple users to log in using one host.
- **auto-approved-first-bind** – Specifies that the server automatically adds the username and host ID to the binding list when the user logged in for the first time.

To disable host check, in the SSL VPN instance configuration mode, use the following command:

no user-host-verify

Approving a Candidate

Approving a pair of host ID and user in the candidate list means to add it to the binding list. To approve a candidate, in any mode, use the following command:

exec scvpn *instance-name* **approve-binding user** *user-name* **host** *host-id*

- **scvpn** *instance-name* – Specifies the name of SSL VPN instance.
- **user** *user-name* – Specifies the username in the candidate list.
- **host** *host-id* – Specifies the host ID of the user.

Configuring a Super User

A super user can log into the server using any host. To change a user in candidate or binding list to a super user, in any mode, use the following command:

exec scvpn *instance-name* **no-host-binding-check user** *user-name*

- **scvpn** *instance-name* – Specifies the name of SSL VPN instance.
- **user** *user-name* – Specifies the name of user who will be changed to a super user.

To cancel a super user, in any mode, use the following command:

exec scvpn *instance-name* **host-binding-check user** *user-name*

Configuring a Shared Host

If a host is considered as a shared host, users logging into the server from this host are not limited by host binding authentication. To configure a host in candidate or binding list as a shared host, in any mode, use the following command:

exec scvpn *instance-name* **no-user-binding-check host** *host-id*

- **scvpn** *instance-name* – Specifies the name of SSL VPN instance.
- **host** *host-id* – Specifies the ID of the host which will be changed to a shared host. The host must be in the candidate list or binding list.

To cancel a shared host, in any mode, use the following command:

no exec scvpn *instance-name* **no-user-binding-check host** *host-id*

Increasing/Decreasing Pre-approved Hosts

Even when multi-host login is allowed for a user, by default, the system only records the first login host-user pair into its binding list; other login pairs are in the candidate list. However, the host-user binding pair number in the binding list can be changed.

To increase the pre-approved host-user binding pair number, in any mode, use the following commands:

exec scvpn *instance-name* **increase-host-binding user** *user-name number*

- **scvpn** *instance-name* – Specifies the name of SSL VPN instance.
- **user** *user-name* – Specifies the name of user.
- *number* – Specifies the number of pre-approved host-user binding pairs to be added to the binding list for the user. The number ranges from 1 to 32. The total number of pre-approved host-user binding pairs in a binding list ranges from 0 to 100.

exec scvpn *instance-name* **decrease-host-binding user** *user-name number*

- **scvpn** *instance-name* – Specifies the name of SSL VPN instance.
- **user** *user-name* – Specifies the name of user.
- *number* – Specifies the number of pre-approved host-user binding pairs to be decreased in the binding list for the user. The number ranges from 1 to 32. The total number of pre-approved host-user binding pairs in a binding list ranges from 0 to 100.

Clearing a Binding List

To clear a binding list or an entry in the table, in any mode, use the following command:

exec scvpn *instance-name* **clear-binding** [{**user** *user-name* [**host** *host-id*] | **host** *host-id* }]

- **scvpn** *instance-name* – Specifies the name of SSL VPN instance.
- **user** *user-name* – Specifies the name of user. If the next parameter is not defined, all hosts bound to this user will be cleared.
- **host** *host-id* – Specifies the host ID of the host which will be cleared.

Exporting/Importing a Binding List

The binding list can be exported to (and imported from) an FTP server, TFTP server or USB disk.

To export a binding list, in the execution mode, use the following command:

export scvpn user-host-binding to {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} [*file-name*]

- **ftp server** *ip-address* [**user** *user-name* **password** *password*] – Specifies that the table is exported to an FTP server. Type the IP address of FTP server. Type username and password if needed; if the server supports anonymous login, skip user name and password.
- **tftp server** *ip-address* – Specifies that binding list is exported to a TFTP server. Type the IP address of the TFTP server.
- **usb0** | **usb1** – Exports the binding list to the root directory of the USB disk.
- *file-name* – Specifies a name for the file of exported binding list.

To import a binding list, in the execution mode, use the following command:

import scvpn user-host-binding from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} [*file-name*]

- **ftp server** *ip-address* [**user** *user-name* **password** *password*] – Specifies that the table is imported from an FTP server. Type the IP address of FTP server. Type username and password if needed; if the server supports anonymous login, skip user name and password.
- **tftp server** *ip-address* – Specifies that binding list is imported from a TFTP server. Type the IP address of the TFTP server.
- **usb0** | **usb1** – Imports the binding list from the root directory of the USB disk.
- *file-name* – Specifies the file name of imported binding list.

Host Check

The host check function checks the security status of the hosts running SSL VPN clients, and according to the checking result, the SSL VPN server will determine the security level for each host and assign corresponding resource access permission based on their security level. The checked factors are operating system, IE version, and the installation of some specific software.

Checked Factors

The factors to be checked by the SSL VPN server are displayed in the list below:

Factor	Description
Operating system	• Operating system, e.g., Windows 2000, Windows 2003, Windows XP, Windows Vista, etc.

Factor	Description
	• Service pack version, e.g., Service Pack 1 • Windows patch, e.g., KB958215, etc.
	• Whether the Windows Security Center and Automatic Update is enabled. • Whether the installation of AV software is compulsory, and whether the real-time monitor and the auto update of signature database are enabled • Whether the installation of anti-spyware is compulsory, and whether the real-time monitor and the online update of signature database are enabled • Whether the personal firewall is installed, and whether the real-time protection is enabled
Other configurations	Whether the IE version and security level reach the specified requirements
	Whether the specified processes are running
	Whether the specified services are installed
	Whether the specified services are running
	Whether the specified registry key values exist
	Whether the specified files exist in the system

Role Based Access Control and Host Check Procedure

Role Based Access Control (RBAC) means that the permission of the user is not determined by his user name, but his role. The resources can be accessed by a user after the login is determined by his corresponding role. So role is the bridge connecting the user and permission.

The SSL VPN host check function supports RBAC. And the concepts of primary role and guest role are introduced in the host check procedure. The primary role determines which host check profile (contains the host check contents and the security level, can be configured via WebUI) will be applied to the user and what access permission can the user have if he passes the host check. And the guest role determines the access permission for the users who failed in the host check. For more information about role and host check, see the Table 7: Relationship between Host Check Rule and Check Results.

The host check procedure is:

1. The SSL VPN client sends request for connection and passes the authentication.

2. The SSL VPN server sends host check profile to the client.

3. The client checks the host security status according to the host check profile. If it failed in the host check, the system will notify the check result.

4. The client sends the check result back to the server.

5. If the host check succeeds, the server will assign access permissions based on the primary role defined in the host check profiles; if the host check fails, the server will disconnect the client and issue a prompt, or assign access permissions based on the guest role defined in the host check profile.

The host check function also supports dynamic access permission control. On one side, when the client's security status changes, the server will send a new host check profile to the client to make it re-check; on the other side, the client can perform the security check periodically, e.g., if the AV software is disabled and it is detected by the host check function, the assigned role to the client may changed, and so does the access permission.

Configuring a Host Check Profile

Host check profile defines the checking contents and security level. You can use WebUI or CLI to create a host check profile, but the detailed settings of that profile can only be done in the WebUI.

To create a host check profile, in the global configuration mode, use the following command:

scvpn host-check-profile *hostcheck-profile-name*

- *hostcheck-profile-name* – Specifies a name for the host check profile.

To delete a host check profile, in the global configuration mode, use the following command: **no scvpn host-check-profile** *hostcheck-profile-name*.

Configuring a Host Check Profile via WebUI

To create a host check profile via WebUI, take the following steps:

1. On the Navigation pane, click **Configure** > **Network** > **SSL VPN** to visit the SSL VPN page.

2. On the Task tab in the right auxiliary pane, click **Host Check** to visit the Host Check page.

3. Click **New**.

4. On the **Basic** and **Advanced** tabs, configure the following options.

Options on the **Basic** tab:

- **Name:** Specifies the name of the host check profile.
- **OS version:** Specifies whether to check the OS version on the client host. Click one of the following options:
  - **No check** - Do not check the OS version.
  - **Must match** - The OS version running on the client host must be the same as the version specified here. Select the OS version and service pack version from the drop-down lists respectively.
  - **At least** - The OS version running on the client host should not be lower than the version specified here. Select the OS version and service pack version from the drop-down lists respectively.
- **Patch X:** Specifies the patch that must be installed on the client host. Type the patch name into the box. Up to five patches can be specified.
- **Lowest IE version:** Specifies the lowest IE version in the Internet zone on the client host. The IE version running on the client host should not be lower than the version specified here.
- **Lowest IE security level:** Specifies the lowest IE security level on the client host. The IE security level on the host should not be lower than the level specified here.

Options on the **Advanced** tab:

- **Security center:** Checks whether the security center is enabled on the client host.
- **Auto update:** Checks whether the Windows auto update function is enabled.
- **Anti-Virus software:** Checks if the client host has installed anti-virus software and others, including:
  - **Installed** - The client host must have the AV software installed.
  - **Monitor** - The client host must enable the real-time monitor of the AV software.
  - **Virus signature DB update** - The client host must enable the signature database online update function.
- **Anti-Spyware software:** Checks if the client host has installed anti-spyware and others, including:

  - **Installed** - The client host must have the anti-spyware installed.
  - **Monitor** - The client host must enable the real-time monitor of the anti-spyware.
  - **Signature DB update** - The client host must enable the signature database online update function.
- **Firewall:** Checks if the client host has installed firewall and others, including:
  - **Installed** - The client host must have the personal firewall installed.
  - **Monitor** - The client host must enable the real-time monitor function of the personal firewall.
- **Registry key value: Key X:** Checks whether the key value exists. Up to five key values can be configured. The check types are:
  - **No check** - Do not check the key value.
  - **Exist** - The client host must have the key value. Type the value into the box.
  - **No exist** - The client does not have the key value. Type the value into the box.
- **File path name: File X:** Checks whether the file exists. Up to five files can be configured. The check types are:
  - **No check** - Do not check the file.
  - **Exist** - The client host must have the file. Type the file name into the box.
  - **No check** - The client does not have the file. Type the file name into the box.
- **Running process name: Process X:** Checks whether the process is running. Up to five processes can be configured. The check types are:
  - **No check** - Do not check the process.
  - **Exist** - The client host must have the process running. Type the process name into the box.
  - **No exist** - The client cannot have the process running. Type the process name into the box.

- **Installed service name:** Checks whether the service is installed. Up to five services can be configured. The check types are:
    - **No check** - Do not check the service.
    - **Exist** - The client host must have the service installed. Type the service name into the box.
    - **No exist** - The client host cannot have the service installed. Type the service name into the box.
- **Running service name:** Checks whether the service is running. Up to five services can be configured. The check types are:
    - **No check** - Do not check the service.
    - **Exist** - The client host must have the service running. Type the service name into the box.
    - **No exist** - The client host cannot have the service running. Type the service name into the box.

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

Referencing a Host Check Profile to a Rule

To make the configured host check profile take effect, you must bind the profiles to the host check rules. And then the host check function will work in the system.

To configure a host check rule, in the SSL VPN instance configuration mode, use the following command:

host-check [**role** *role-name*] **profile** *profile-name* [**guest-role** *guestrole-name*] [**periodic-check** *period-time*]

- **role** *role-name* − Specifies a configured role in AAA server as the primary role for the user. If this parameter is defined, the host check profile works for this role; if not, the profile is the default profile and serves all users.
- **profile** *profile-name* − Specifies the name of the bound host check profile.
- **guest-role** *guestrole-name* − Specifies the guest role. If the client host fails in host check, this parameter enables the user to own the privileges of this guest role; if this parameter is not defined, the client will be disconnected.
- **periodic-check** *period-time* − Specifies the auto-check period of the user. The value range is 5 to 1440 minutes. The default value is 30.

Repeat this command to add more host check rules. If a user matches multiple host check rules, the server uses the first matched rule; in addition, if a user binds to multiple roles with matched host check rules, the server uses the first matched rule.

To cancel the host check rule setting, in the SSL VPN instance configuration mode, use the following command:

no host-check [**role** *role-name*] **profile** *profile-name* [**guest-role** *guestrole-name*] [**periodic-check** *period-time*]

- **role** *role-name* – Cancel the host check rule of the specified primary role. If you do not specify a primary role or a guest role, the default profile will be deleted.
- **guest-role** *guestrole-name* – With a primary role specified already, delete the specified guest role.
- **periodic-check** *period-time* – With a primary role specified already, restore the auto-check period to the default value.

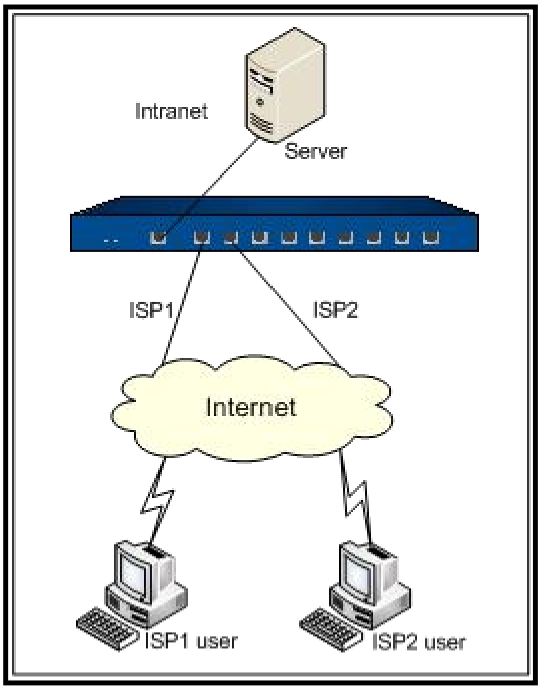
The table below lists the relationship between the policy rule and host check result.

Rule Setting	Check Result	
	Successful	Failed
Primary role: configured Profile: configured Guest role: configured	Obtain privileges of primary role	Obtain privileges of guest role
Primary role: configured Profile: configured Guest role: not configured	Obtain privileges of primary role	Be disconnected
Primary role: not configured Profile: configured Guest role: configured	In connection	Obtain privileges of guest role
Primary role: not configured Profile: configured Guest role: not configured	In connection	Be disconnected

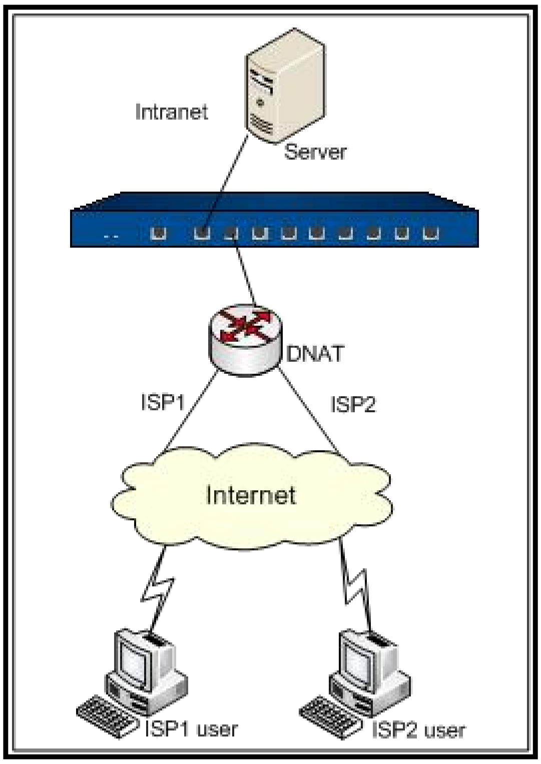
Selecting an Optimal Path

VPN networks with multiple ISPs (Internet Service Provider) can be greatly influenced by the defects of narrow bandwidth and long delay in communication among different ISPs. To solve the issue, the FS device provides optimal path check feature which enables the device to automatically select the fastest path for the client to connect to SSL VPN server.

There are two designs of network implementation for you to use optimal path selection feature.



As shown in the figure above, SSL VPN client visits the egress interface of the server. Firstly, the SSL VPN server needs to apply for different ISP services and enable interfaces for each of the ISP services as the tunnel egress interfaces. When the SSL VPN clients with different ISP accesses try to visit headquarters, the optimal path selection feature judges the ISP of the requiring client, arranges the SSL VPN interfaces in the sequence of relevancy to the ISP, and then provides the sequence of SSL VPN egress interface to the client for it to choose; if the optimal path selection feature is not enabled, the client selects a preferential link path by sending UDP probe packets.



As shown in the figure above, SSL VPN client accesses to SSL VPN server by the way of DNAT device which translates the client address to SSL VPN server egress interface. The DNAT device accesses Internet using multiple ISP links. You need to add the DNAT device’ s egress interface to an address entry in the SSL VPN server address pool. If optimal path detection on the SSL VPN server is enabled, the server judges the ISP type of client’ s access address and assigns DNAT’ s egress interface addresses to the client according to the priority of address so that the client can select its optimal path; if the server has not enabled optimal path detection feature, the client sends UDP probe packets to choose an optimal path.

To specify an interface as SSL VPN tunnel egress interface, in the SSL VPN instance configuration mode, use the following command:

interface *interface-name*

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

Repeat this command to specify more interfaces (up to two) as the tunnel egress interface.

To cancel the specified tunnel interface, in the SSL VPN instance configuration mode, use the following command:

no interface *interface-name*

To configure the optimal path selection, in the SSL VPN instance configuration mode, use the following command:

link-select [**server-detect**] [*A.B.C.D* [**https-port** *port-number*]] [**A.B.C.D** [**https-port** *port-number*]] [*A.B.C.D* [**https-port** *port-number*]] [*A.B.C.D* [**https-port** *port-number*]]

- **server-detect** – Enables the optimal link detection of the device. By default, the client selects link spontaneously.
- *A.B.C.D* – Specifies the Internet interface IP address of DNAT device. The system allows up to four IP addresses.
- **https-port** *port-number* – Specifies the HTTPS port number of the DNAT Internet interface. The value range is 1 to 65535. The default value is 4433. To avoid collision with WebUI HTTPS port number, you are not recommended to use port 443.

To cancel optimal link selection, in the SSL VPN instance configuration mode, use the command **no link-select**.

SSL VPN optimal link selection also provides multi-link redundancy, which enables the server to switch links when one link disconnects so as to guarantee the connection stability between server and client (traffic flow may be interrupted during switching).

Kicking out an SSL VPN Client

The SSL VPN server can force to disconnect with a client.

To kick out an SSL VPN client, in the configuration mode, use the following command:

exec scvpn *instance-name* **kickout** *user-name*

- *instance-name* – Specifies the name of SSL VPN instance.
- *user-name* – Specifies the name of client to be kicked out of the server.

Changing Password of Local User

By default, the local user is not allowed to change its password, but you can configure the device to enable password changing right for local users if they pass SSL VPN authentication.

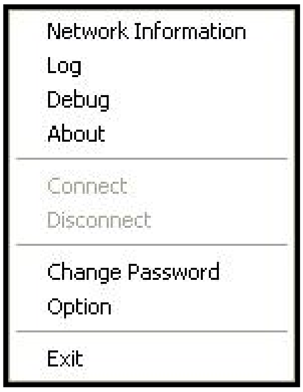
To enable/disable the right for local users to change the login password, in the local AAA server configuration mode, use the following command:

- Enable: **allow-pwd-change**
- Disable: **no allow-pwd-change**

Tip: SSL VPN client (FS Secure Connect) of version 1.2.0.1106 and later allows the local users to change password. Therefore, it’ s advised to use the latest SSL VPN client.

When the server allows the client user to change password, the user can change login password after passing SSL VPN authentication by the following steps:

1. Right-click the client icon in notification area of the taskbar on the right-bottom corner and a menu appears.

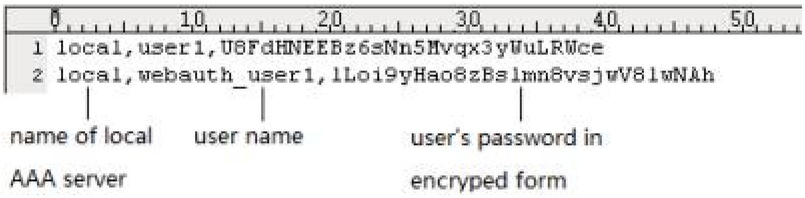


2. Click **Changing Password** and type current password and new password into the corresponding boxes.

3. Click **OK** to save the changes.

Exporting and Importing a Password File

To avoid password setting disoperation, you can export/import the password file from/to the SSL VPN server. The password file uses CSV filetype, as shown in the the figure below.



```
1 local,user1,U8FdHNEEBz6sNn5Mvqx3yWuLRWce
2 local,webauth_user1,lLoi9yHao8zBslmn8vsjwV8lwNAh
```

The principles of importing password files are:

- If the user information in the password file is the same with that in the system, this operation resets all the local user passwords according to the information in password file.

- If the password file has fewer users than those in the system, this operation resets system users who are also in the password file and remain the rest.

- If the password file has more users than those in the system, this operation only resets users in the system and deletes different users in the password file.

Note:

- If you want to use Excel to open the password file, make sure the expansion is .csv.

- When password file is imported, it takes effect immediately.
- The command line will show the number of imported users.

Exporting a Password File

To export a password file, in the global configuration mode, use the following command:

export aaa user-password to {**tftp server** *ip-address* | **ftp server** *ip-address* [**user** *user-name* **password** *password*]} [*file-name*]

- *ip-address* – Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* **password** password – Specifies the username and password of the FTP server.
- *file-name* – Specifies the file name of the exported password file.

Importing a Password File

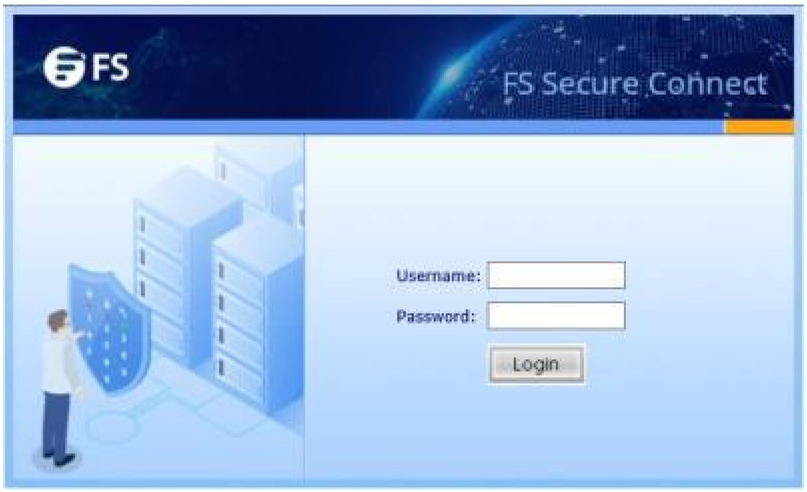
To import a password file, in the configuration mode, use the following command:

import aaa user-password from {**tftp server** *ip-address* | **ftp server ip-address** [**user** *user-name* **password** *password*]} *file-name*

- *ip-address* – Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP server.
- *file-name* – Specifies the file name of the imported password file.

SSL VPN Login Page

You can customize the SSL VPN login page by changing the background picture. The default login page is shown as below:



Customizing SSL VPN Login Page

You are allowed to change the background picture of SSL VPN login page.

To change the background, in the global configuration mode, use the following command:

import customize scvpn from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} *file-name*

- **ftp server** *ip-address* [**user** u*ser-name* **password** *password*] – Specifies that the background picture is imported from an FTP server. Type the IP address of the FTP server, username and password (skip if the server can be logged in anonymously).
- **tftp server** *ip-address* – Specifies that the background picture is imported from a TFTP server. Type the IP address of the TFTP server.
- **usb0 | usb1** – Specifies that the picture is imported from the USB disk plugged to USB0 or USB1 port.
- *file-name* – Uploaded 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.

To restore to the default background picture, in any mode, use the following command:

exec customize scvpn [**language** {**en** | **zh_cn**}] **default**

- **language** {**en** | **zh_cn**} – Choose the English or Chinese login page whose background picture will be restored.

Control the Access by Using the Radius Server

When you use the Radius authentication mode, you can set the access scope for the authenticated users. For the authenticated users, the system obtains the information that regulates the access scope of the users from the Radius server. Based on obtained information, the system will dynamically create policy that is from the source address to the regulated access scope. For the users that do not pass the authentication, the system refuses to allow them to access the network. When users logged off or were kicked out by administrators, or when the logging time of a user has timeout, the corresponding policy will be deleted automatically.

To view the regulated access scope, use the following command in any mode:

show auth-user username *user-name*

- *user-name* – Specifies the username of the user that you want to view.

Configuring Upgrade URL

The client checks and downloads the new version by using the configured upgrade URL. The system has a default URL that links to the official upgrade server and this URL cannot be deleted. When you want to use the intranet server to check and download the new version, you can configure a new upgrade URL, and this new upgrated URL will take effect intead of the default one. To configure the upgreated URL, use the following command in the global configuration mode:

scvpn-update-url *ip-address*

- *ip-address* – To use the intranet server to check and download the new version, enter the URL of the intranet server. You need to deploy the new version in this intranet server.

To use the default URL that links to the official upgrade server, use the following command in the global configuration mode:

no scvpn-update-url

Note:When the client version is 1.4.4.1199 or below and the FSOS version is 5.5R1 or above, it is recommended to uninstall the previous client and login the Web page to re-install it.

Viewing SSL VPN Settings

Use the following commands to view information about SSL VPN.

- Show SSL VPN instance:
  show tunnel scvpn [*scvpn-instance-name]*
- View HTTP sessions of the SSL VPN server being visited:
  show scvpn session *scvpn-instance-name* [**user** *user-name*]

- Show online users of the specified SSL VPN instance:

  show scvpn client *scvpn-instance-name* [**user** *user-name*]

- Show online users of all SSL VPN instances:

  show auth-user scvpn [**interface** *interface-name* | **vrouter** *vrouter-name* | **slot** *slot-no*]

- Show user-host binding list:

  show scvpn user-host-binding *scvpn-instance-name* {**host** [*host-id*] | **user** [*user-name*]}

SSL VPN Client for Windows

FS Secure Connect is the SSL VPN client. FS Secure Connect runs in the following operating systems: Windows 2000/2003/2008/XP/Vista/Windows 7/Windows 8/Windows 8.1/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 interface and route information from 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 gives instructions on how to use 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 (including USB Key certificate and file certificate)
- Digital Certificate (including USB Key certificate and file certificate) only

Downloading and Installing Secure Connect

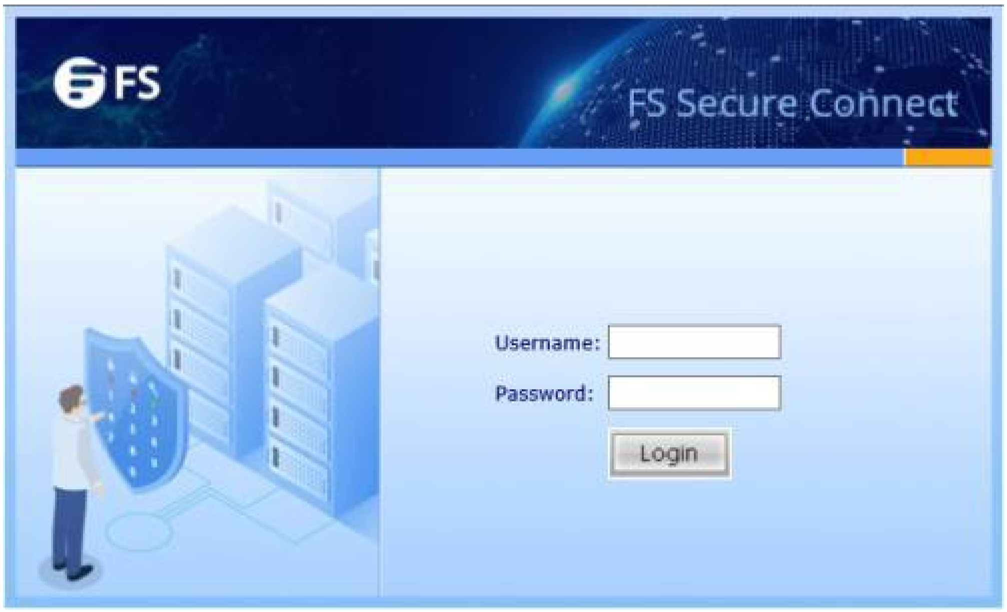
When using the SSL VPN client for the first time, you need to download and install the client software FS Secure Connect. This section describes three methods for downloading and installing the client software based on three available authentication methods. For the Username/Password + Digital Certificate authentication, the digital certificate can either be the USB Key certificate provided by the vendor, or the file certificate provided by the administrator.

Downloading and Installing (Username/Password)

When the Username/Password authentication is configured on the server, take the following steps to download and install the SSL VPN client software - FS 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 (**interface** *interface-name*) and HTTPS port number (**https-port** *port-number*) of the egress interface specified in the SSL VPN instance.

2. In the SSL VPN login page, type the user name 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 being bound to the user. Click **Login**, and in the PIN Setting page, 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. 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.



> Tip: You can customize this login page by changing the background picture. For more information, see Customizing SSL VPN Login Page.

3. After login, IE will download the client software automatically, and you can install it by the 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.

Downloading and Installing (Username/Password + USB Key Certificate)

When the Username/Password + Digital Certificate authentication is configured on the server, for the USB Key certificate, take the following steps to download and install the SSL VPN client software - FS Secure Connect:

1. Insert the USB Key to the USB port of the PC.
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 (**interface** *interface-name*) and HTTPS port number (**https-port** *port-number*) of the egress interface specified in the SSL VPN instance.
3. In the Select Digital Certificate dialog, select the certificate you want and click OK. Then in the pop-up dialog, provide the UKey' s PIN code and click **OK**.

   > Tip: To use FS UKey, the FS UKey driver and administrator software are also needed. For more information about FS UKey, see FS UKey User Manual.

4. In the SSL VPN login page shown in Figure 11, 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 in one minute, you can re-apply.
6. After login, 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.

Downloading and Installing (Username/Password + File Certificate)

When the Username/Password + Digital Certificate authentication is configured on the server, for the file certificate, take the following steps to download and install the SSL VPN client software - FS Secure Connect:

1. 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 (**interface** *interface-name*) and HTTPS port number (**https-port** *port-number*) of the egress interface specified in the SSL VPN instance.
3. In the Select Digital Certificate dialog, select the certificate you want and click **OK**.
4. In the SSL VPN login page shown in Figure 11, 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. After login, 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.

Downloading and Installing (USB Key Certificate Only)

When the Digital Certificate Only authentication is configured on the server, for the USB Key certificate, take the following steps to download and install the SSL VPN client software - FS Secure Connect:

1. Insert the USB Key to the USB port of the PC.
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 (**interface** *interface-name*) and HTTPS port number (**https-port** *port-number*) of the egress interface specified in the SSL VPN instance.
3. In the Select Digital Certificate dialog, select the certificate you want and click **OK**. In the Enter Password dialog, provide the UKey user password (1111 by default) and click **OK**.
4. After login, 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.

Downloading and Installing (File Certificate Only)

When the Digital Certificate Only authentication is configured on the server, for the file certificate, take the following steps to download and install the SSL VPN client software - FS Secure Connect:

1. 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 (**interface** *interface-name*) and HTTPS port number (**https-port** *port-number*) of the egress interface specified in the SSL VPN instance.
3. In the Select Digital Certificate dialog, select the certificate you want and click **OK**.
4. After login, 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 the software directly

Starting SSL VPN 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.

Starting via Web (Username/Password)

When the Username/Password authentication is configured on the server, to start Secure Connect via web, take the following steps:

1. Type the URL **https://IP-Address:Port-Number** into the address bar of your web browser.

2. In the login page shown in the figure, 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 being bound to the user. Click **Login**, and in the PIN Setting page, 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. 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.

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.

Starting via Web (Username/Password + USB Key Certificate)

When the Username/Password + Digital Certificate authentication is configured on the server, for the USB Key certificate, 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, select the certificate you want and click **OK**. In the Enter Password dialog, provide the UKey user password (1111 by default) and click **OK**.

4. In the login page shown in the figure, type the username and password into the **Username** and **Password** boxes respectively, and then click **Login**. The login user here should be configured before in the FS device.

5. In the USB Key PIN dialog shown the figure below, type the UKey PIN (1111 by default), and click **OK**.

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.

Starting via Web (Username/Password + File Certificate)

When the Username/Password + Digital Certificate authentication is configured on the server, for the file certificate, to start 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, select the certificate you want and click **OK**.
4. In the login page shown in the figure, type the username and password into the **Username** and **Password** boxes respectively, and then click **Login**. The login user here should be configured before in the FS device.

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.

Starting via Web (USB Key Certificate Only)

When the Digital Certificate authentication is configured on the server, for the USB Key certificate, 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, select the certificate you want and click **OK**. In the Enter Password dialog shown below, provide the UKey user password (1111 by default) and click **OK**.
4. In the USB Key PIN dialog shown in Figure 15, type the UKey PIN (1111 by default), and click **OK**.

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.

Starting via Web (File Certificate Only)

When the Digital Certificate authentication is configured on the server, for the file certificate, to start 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, select the certificate you want and click **OK**.

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.

Starting the Software Directly

This section describes how to start the SSL VPN client software FS 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 (TLS/SSL) 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:

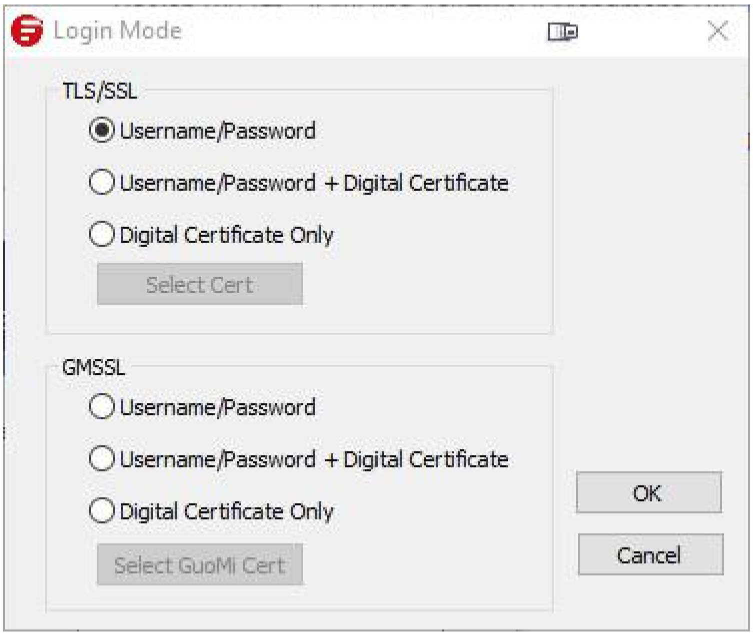
- Username/Password
- Username/Password + USB Key Certificate
- Username/Password + File Certificate
- USB Key Certificate Only
- File Certificate Only

Using Username/Password Authentication

When the Username/Password authentication is configured on the server, to start the Secure Connect client software, take the following steps:

1. In your PC, double click the shortcut to FS Secure Connect on your desktop, or from the Start menu, click **All Programs > FS Secure Connect > FS Secure Connect**.

2. In the Login dialog, click **Mode**. In the Login Mode dialog as 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

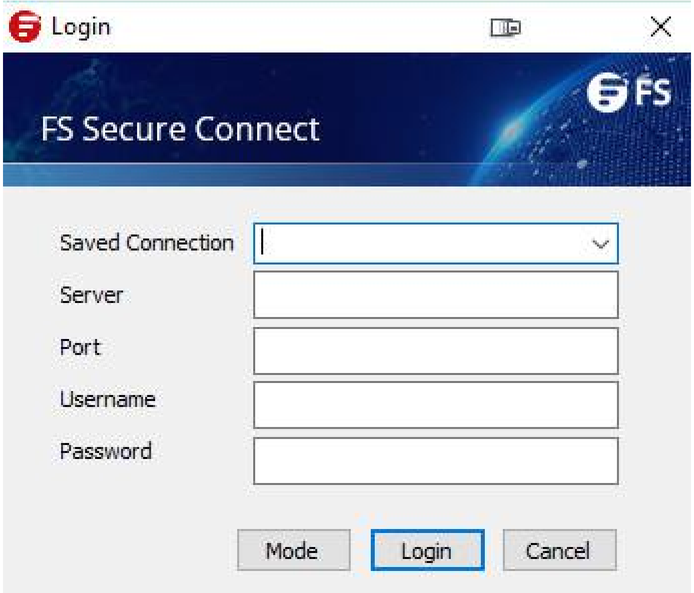
GMSSL

○ Username/Password

○ Username/Password + Digital Certificate

○ Digital Certificate Only

3. In the Login dialog of the Username/Password authentication mode, configure the options to 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 being bound to the user. Click **Login**, and in the PIN Setting page, 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.
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.



Saved Connection: Provides the connection information you have filled before. Select a connection from the drop-down list. For more information about the login options, see **Configuring Secure Connect**.

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 you enter the wrong password for three consecutive times withing one minute, the system will refuse the logon of this user for two minutes.

When the above steps are 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. And the encrypted communication between the client and server can be implemented now.

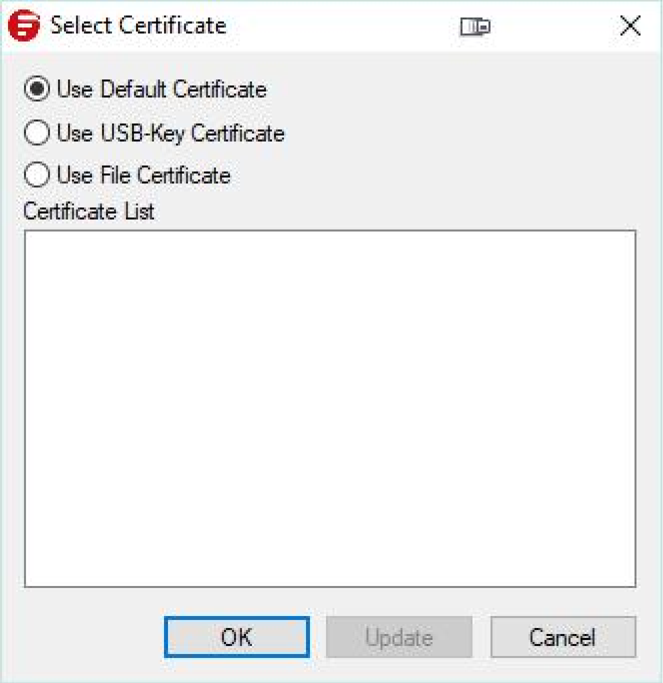
Using Username/Password + USB Key Certificate Authentication

When the Username/Password + Digital Certificate authentication is configured on the server, for the USB Key certificate, to start the Secure Connect software 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 FS Secure Connect on your desktop, or from the Start menu, click **All Programs** > **FS Secure Connect** > **FS Secure Connect**.

3. In the Login dialog, click **Mode**. In the Login Mode dialog, first click **Username/Password + Digital Certificate** in **TLS/SSL** section, and if necessary, click **Select Cert**. In the Select Certificate dialog as 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: Select the checkbox to use the default certificate for authentication. FS devices use the certificate in FS UKey as the default certificate. This is the default option.

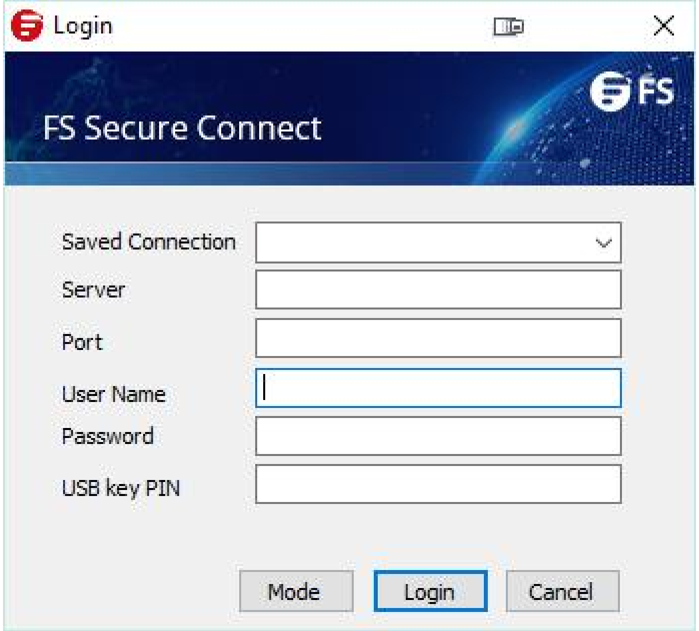
Use USB-Key Certificate: Select the checkbox to use the USB-Key certificate for authentication.

Use File Certificate: Select the checkbox to use the file certificate for authentication.

Certificate List: Lists all the certificates in the system. You can choose the certificate you want from the list.

> Tip: You can use the USB Key deployment tool named SelectUSBKey to set the third-party certificate as the default certificate.

4. In the Login dialog of the Username/Password + Digital Certificate authentication mode as shown below, configure the options to login.



Saved Connection: Provides the connection information you have filled before. Select a connection from the drop-down list. For more information about the login options, see **Configuring Secure Connect**.

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.

5. Click **Login**. If SMS authentication is enabled, type the authentication code into the box in the SMS Auth dialog and click **Verify**. If you have not received the authentication code in one minute, you can re-apply by clicking **Reapply**.

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 + File Certificate Authentication

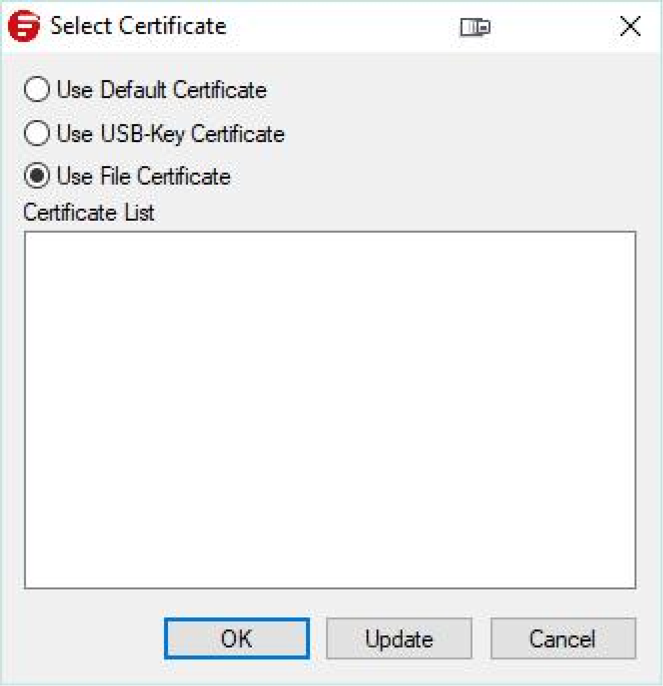
When the Username/Password + Digital Certificate authentication is configured on the server, for the file certificate, to start the Secure Connect software directly, take the following steps:

1. Import the file certificate provided by the administrator manually.

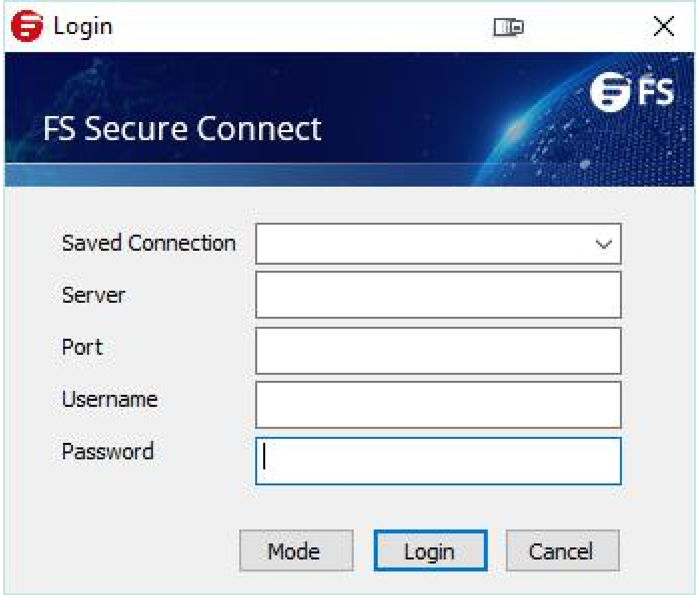
2. In your PC, double click the shortcut to FS Secure Connect on your desktop, or from the Start menu, click **All Programs > FS Secure Connect > FS Secure Connect**.

3. In the Login dialog, click **Mode**. In the Login Mode dialog, first click **Username/Password + Digital Certificate** in **TLS/SSL** section, and if necessary, click **Select**

Cert. In the Select Certificate dialog as 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**.



4. In the Login dialog of the Username/Password + Digital Certificate authentication mode (as shown below), configure the options to login.



Saved Connection: Provides the connection information you have filled before. Select a connection from the drop-down list. For more information about the login options, see.

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 USB Key Certificate Only Authentication

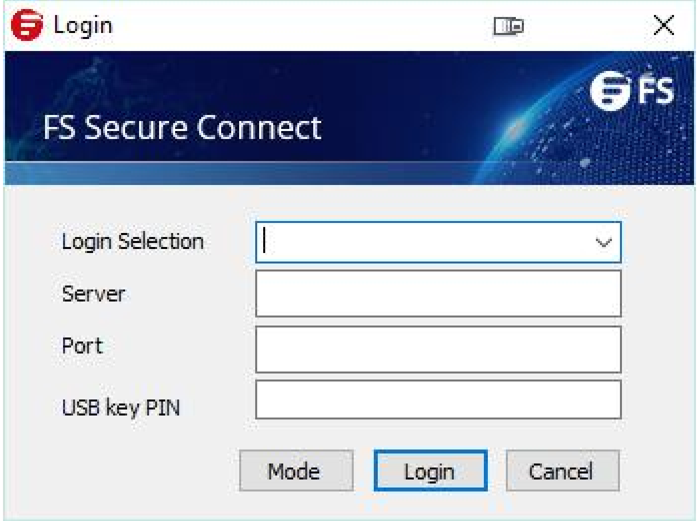
When the Digital Certificate Only authentication is configured on the server, for the USB Key certificate, to start the Secure Connect software directly, take the following steps:

1. Insert the USB Key to the USB port of the PC.

2. In your PC, double click the shortcut to FS Secure Connect on your desktop, or from the Start menu, click **All Programs** > **FS Secure Connect** > **FS Secure Connect**.

3. In the Login dialog, click **Mode**. In the Login Mode dialog, first click **Digital Certificate only** in **TLS/SSL** section, and if necessary, click **Select Cert**. In the Select Certificate dialog shown in Figure 99, select a USB Key certificate. The client will send the selected certificate to the server for authentication. Finally click **OK**.

4. In the Login dialog of the Digital Certificate Only authentication mode (as shown in the figure below), configure the options to login.



Login Selection: Provides the connection information you have filled before. Select a connection from the drop-down list. For more information about the login options, see **Configuring Secure Connect**
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.

When the above steps are 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. And the encrypted communication between the client and server can be implemented now.

Using File Certificate Only Authentication

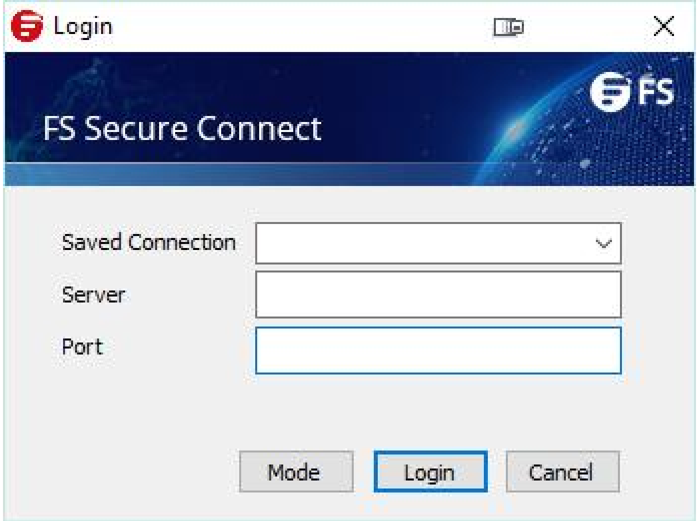
When the Digital Certificate Only authentication is configured on the server, for the file certificate, to start the Secure Connect software directly, take the following steps:

1. Import the file certificate provided by the administrator manually.

2. In your PC, double click the shortcut to FS Secure Connect on your desktop, or from the Start menu, click **All Programs > FS Secure Connect > FS Secure Connect**.

3. In the Login dialog, click **Mode**. In the Login Mode dialog, first click **Digital Certificate only** in **TLS/SSL** section, and if necessary, click **Select Cert**. In the Select Certificate dialog, select a file certificate. The client will send the selected certificate to the server for authentication. Finally click **OK**.

4. In the Login dialog of the Digital Certificate Only authentication mode (as shown in the figure below), configure the options to login.



Saved Connection: Provides the connection information you have filled before. Select a connection from the drop-down list. For more information about the login options, see Configuring Secure Connect.
Server: Enter the IP address of SSL VPN server.
Port: Enter the HTTPS port number of SSL VPN server.

When the above steps are 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. And 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. In your PC, double click the shortcut to FS Secure Connect on your desktop, or from the Start menu, click **All Programs > FS Secure Connect > FS Secure Connect**.
2. In the Login dialog, click **Mode**. In the Login Mode dialog , in **GMSSL** section, click **Username/Password**, and then click **OK**.
3. In the Login dialog of the Username/Password authentication mode, configure the options to login.
   Saved Connection: Provides the connection information you have filled before. Select a connection from the drop-down list. For more information about the login options, see Configuring Secure Connect.
   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 you enter the wrong password for three consecutive times withing one minute, the system will refuse the logon of this user for two minutes.

When the above steps are 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. 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 FS Secure Connect on your desktop, or from the Start menu, click **All Programs > FS Secure Connect > FS Secure Connect**.
   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 , select a GM certificate. Finally click **OK**.
   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.
   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.

3. In the Login dialog of the Username/Password + Digital Certificate authentication mode, configure the options to login.
   Saved Connection: Provides the connection information you have filled before. Select a connection from the drop-down list. For more information about the login options, see Configuring Secure Connect.
   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 FS Secure Connect on your desktop, or from the Start menu, click **All Programs > FS Secure Connect > FS Secure Connect**.

In the Login dialog, click **Mode**. In the Login Mode dialog, first click **Digital Certificate only** in **GMSSL** section, and if necessary, click **Select GuoMiCert**. In the Select Certificate dialog, select a file certificate. The client will send the selected certificate to the server for authentication. Finally click **OK**.
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.
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.

3. In the Login dialog of the Digital Certificate Only authentication mode , configure the options to login.
Saved Connection: Provides the connection information you have filled before. Select a connection from the drop-down list. For more information about the login options, see Configuring Secure Connect
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.

When the above steps are 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. And the encrypted communication between the client and server can be implemented now.

Automatically Starting SSL VPN Client and Logging into VPN

Before you log into the operating system, SSL VPN client can automatically start and log into VPN. You need to configure the SSL VPN client and create a task. When using this method, the login mode of the login entry can only be Password.

Configuring SSL VPN Client Settings

1. Navigate to **Start > All Programs > FS Secure Connect > FS Secure Connect**. The **Login** dialog appears.

2. At the notification area, right-click the icon of FS Secure Connect. In the pop-up menu, click **Option**. The **Secure Connect Options** window appears.

3. At the left pane, click **Saved Connection**. At the right pane, create a new login entry.

   - **Connection Name**: Specifies the name for the connection to identify it. The system will assign a name to the connection based on its server, port, and user automatically if keeping this option blank.
   - **Server**: Specifies the domain name or the IP address of the SSL VPN server.
   - **Port**: Specifies the HTTPS port number of the SSL VPN instance.
   - **Username**: Specifies the login user.
   - **Login Mode**: Selects **Password**.
   - **Remember Password**: Selects this option and enter the password in the Password text box.
   - **Proximity Auto Detection**: Select the option to enable optimal path detection function. For more information about optimal path detection, see Selecting an Optimal Path.

4. Click **Apply**. This login entry is saved.

5. At the left pane, click **General**. Then select the **Auto Login** checkbox at the right pane. From the **Default Connection** drop-down list, select the desired login entry.

6. Click **Apply** to save the configurations.

Use Windows Task Scheduler to create a task. This task makes SSL VPN client start automatically before you log into the operating system.

1. Navigate to **Start > Control Panel > Administrative Tools > Task Scheduler**. The **Task Scheduler** window appears. At the right pane, click **Create Basic Task**. The **Create Basic Task Wizard** dialog appears.

2. In the **Create a Basic Task** page, enter a name and the description for this task.

3. Click **Next**. The **Task Trigger** page appears.

4. Select **When the computer starts**. Click **Next**. The **Action** page appears.

5. Select **Start a program**. Click **Next**. The subpage **Start a Program** appears.

6. Click **Browse** to select the SSL VPN client program **SecureConnect.exe**. The default directory is C:\Program Files (x86)\FS\FS Secure Connect\bin.

7. In the **Add arguments** text box, add the following arguments:

   - -l "C:\Users\Administrator\AppData\Roaming\FS\FS Secure Connect\SecurecConfig.xml"
   - The file path in the argument is the default path of the SecureConfig.xml file when the user is Administrator. If the current logon user is not the administrator, enter the file path that is matched with the current logon user.

8. Click **Next**. The **Summary** page appears.

9. Select the **Open the Properties dialog for this task when I click Finish** checkbox. Click **Finish**.

10. In the pop-up window, select the **Run whether user is logged on or not** checkbox. Click **OK**. The **Task Scheduler** dialog appears. Specify a user with the administrative access and enter the corresponding password.

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

After completing the above settings, SSL VPN client can automatically start and log into VPN.

Third-party USB Key

FS UKey certificate is the default certificate for the USB Key authentication. When authenticating with FS UKey certificate, the client will select the FS UKey certificate automatically and send it to the server, and the server will perform the authentication with the default certificate. This authentication process is transparent to the authenticated clients, i.e., the client need not to choose the certificate. If the third-party USB Key is used, you can set the third-party certificate as the default certificate to simplify the authentication process by using the tool named SelectUSBKey.

To set the third-party certificate to the default certificate, first you have to export the CSP Name of the USB Key in form of a registry file, and then add the exported file content to the registry of the client PC.

To export the CSP Name of the USB Key, take the following steps:

1. Install the driver of the third-party USB Key.

2. Insert the third-party USB Key.

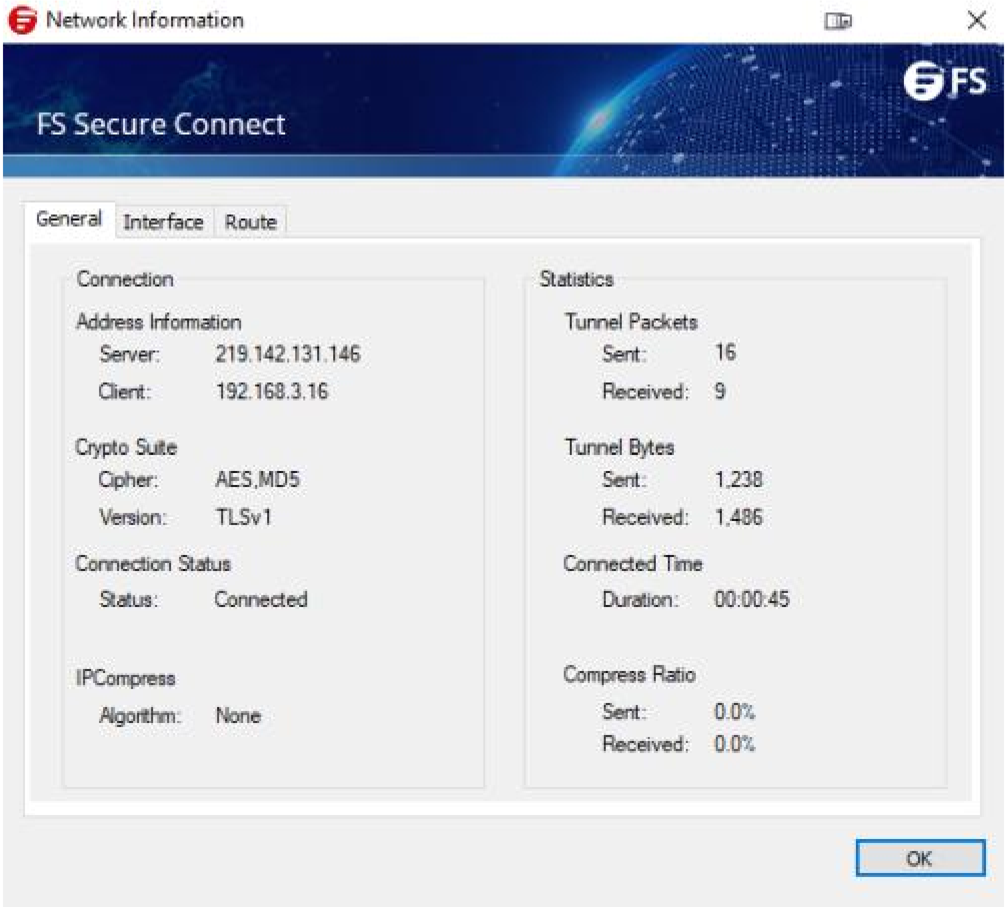
3. Double click SelectUSBKey.exe, and the Select Default Certificate dialog :
   Export: Exports the CSP Name of the USB Key in form of a registry file.
   Update: Refreshes the certificate list.
   Close: Closes the dialog.

4. Select the certificate you want from the certificate list, and then click **Export**.

After exporting the CSP Name of the USB Key, double click the exported file, and then add the content to the registry of the client PC. When authenticating with the third-party certificate, the client will automatically select the third-party USB Key certificate and send it to the server.

Secure Connect GUI

Click in the notification area, the Network Information dialog appears. This dialog shows information about statistics, interfaces, and routes.



Connection

Address Information
Server: 219.142.131.146
Client: 192.168.3.16

Crypto Suite
Cipher: AES,MD5
Version: TLSv1

Connection Status
Status: Connected

IPCompress
Algorithm: None

Statistics

Tunnel Packets
Sent: 16
Received: 9

Tunnel Bytes
Sent: 1,238
Received: 1,486

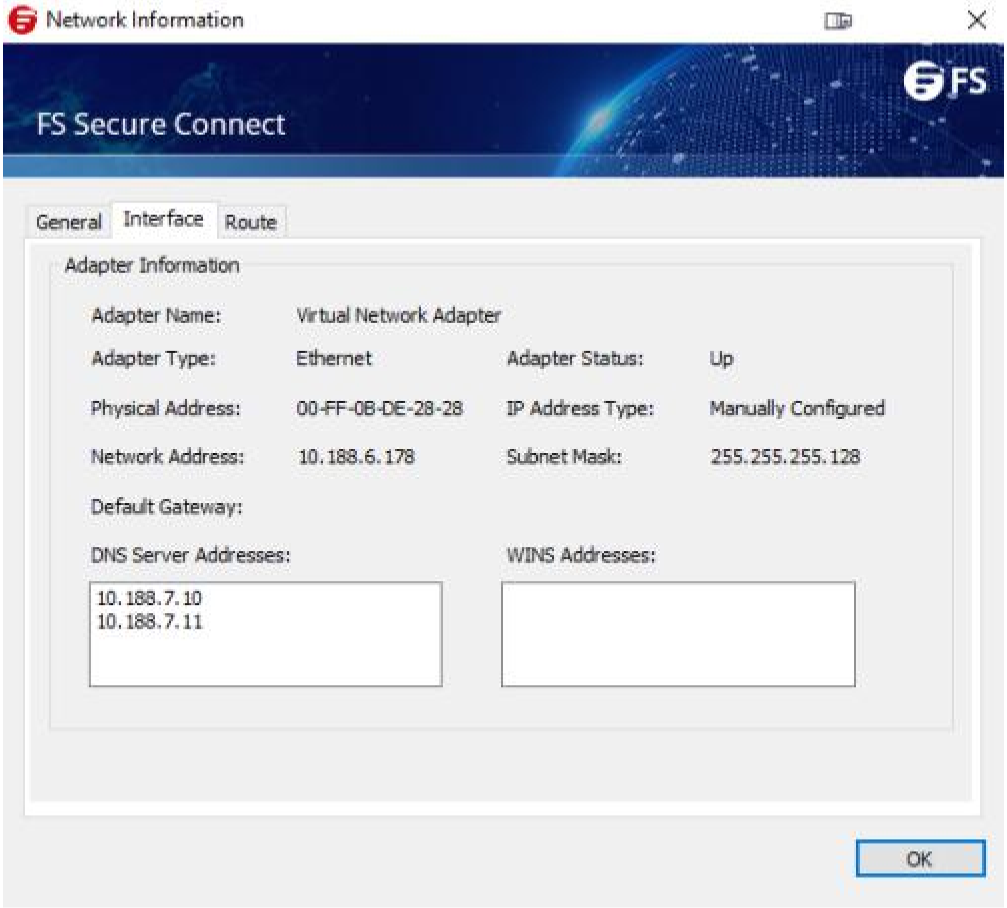
Connected Time
Duration: 00:00:45

Compress Ratio
Sent: 0.0%
Received: 0.0%

Address Information: Shows the IP addresses	
Server	The IP address of the connected SSL VPN server.
Client	The IP address of the client.
Crypto Suite: Shows the encryption information.	
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 state between the client and server. The possible states are: connecting, connected, disconnecting, and disconnected.

Address Information: Shows the IP addresses	
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	
Sent	Bytes sent through the SSL VPN tunnel.
Received	Bytes received through the SSL VPN tunnel.
Connected Time	
Time	Time period during which the client is online.
Compress Ratio	
Sent	Length ratio of sent data after compression.
Received	Length ratio of received data after compression.

Click the Interface tab to view the interface information.



Adapter Information

Adapter Name: Virtual Network Adapter

Adapter Type: Ethernet | Adapter Status: Up

Physical Address: 00-FF-0B-DE-28-28 | IP Address Type: Manually Configured

Network Address: 10.188.6.178 | Subnet Mask: 255.255.255.128

Default Gateway:

DNS Server Addresses:

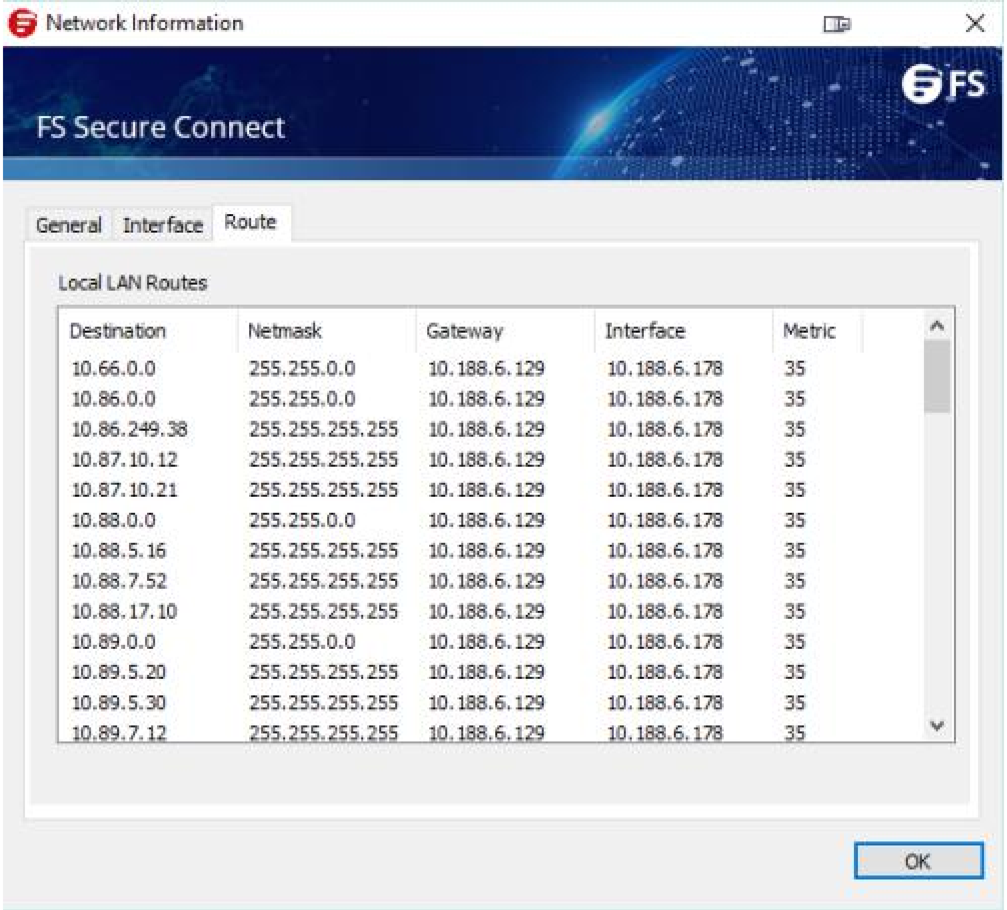
```
10.188.7.10
10.188.7.11
```

WINS Addresses:

- **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.
- **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 encrypted data.
- **Default Gateway:** The gateway address of the interface used to send SSL VPN encrypted data.
- **DNS Server Addresses:** The DNS server addresses used by the client.
- **WINS Addresses:** The WINS server addresses used by the client.
- **Physical Address:** The MAC address of the interface used to send SSL VPN encrypted data.

Click the Route tab to view the route information.



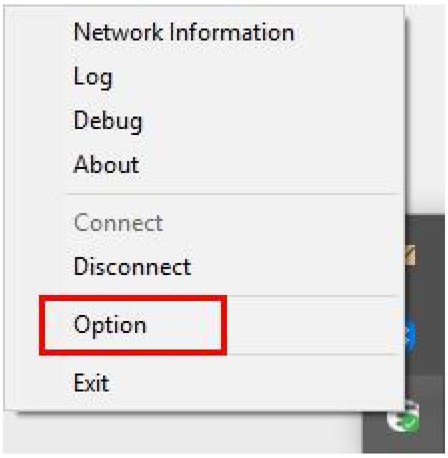
Local LAN Routes

Destination	Netmask	Gateway	Interface	Metric
10.66.0.0	255.255.0.0	10.188.6.129	10.188.6.178	35
10.86.0.0	255.255.0.0	10.188.6.129	10.188.6.178	35
10.86.249.38	255.255.255.255	10.188.6.129	10.188.6.178	35
10.87.10.12	255.255.255.255	10.188.6.129	10.188.6.178	35
10.87.10.21	255.255.255.255	10.188.6.129	10.188.6.178	35
10.88.0.0	255.255.0.0	10.188.6.129	10.188.6.178	35
10.88.5.16	255.255.255.255	10.188.6.129	10.188.6.178	35
10.88.7.52	255.255.255.255	10.188.6.129	10.188.6.178	35
10.88.17.10	255.255.255.255	10.188.6.129	10.188.6.178	35
10.89.0.0	255.255.0.0	10.188.6.129	10.188.6.178	35
10.89.5.20	255.255.255.255	10.188.6.129	10.188.6.178	35
10.89.5.30	255.255.255.255	10.188.6.129	10.188.6.178	35
10.89.7.12	255.255.255.255	10.188.6.129	10.188.6.178	35

- **Local LAN Routes:** The routes used by the virtual network adapter.

SSL VPN Client Menu

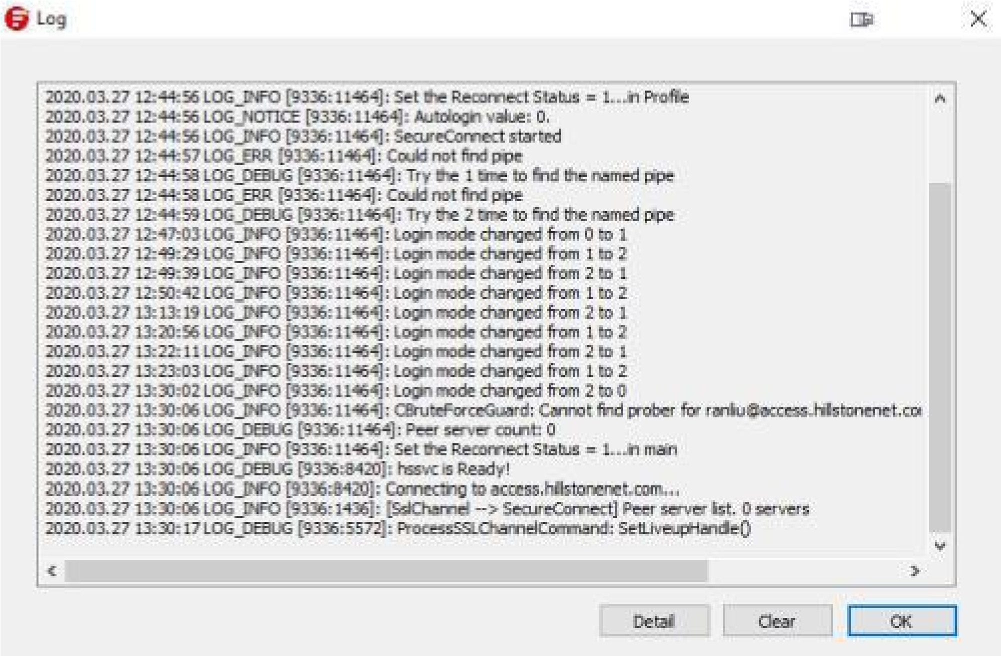
Click in the notification area, the Secure Connect menu appears.



Descriptions of the menu items:

- **Network Information**: Displays the related information in the Network Information dialog.

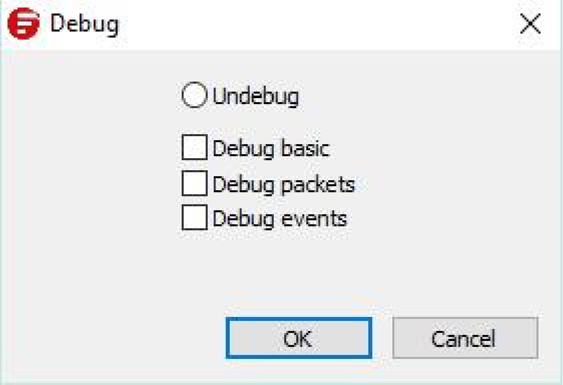
- **Log**: Shows Secure Connect log messages in the Log dialog.



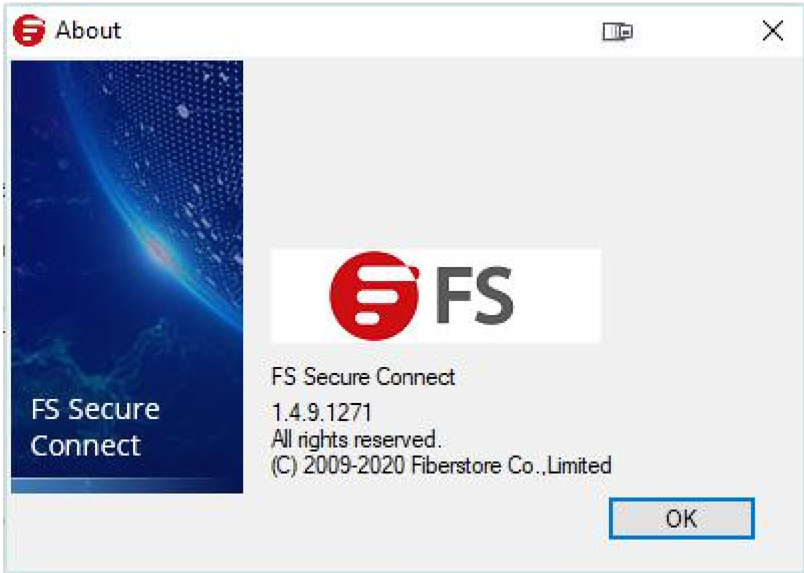
```
2020.03.27 12:44:56 LOG_INFO [9336:11464]: Set the Reconnect Status = 1...in Profile
2020.03.27 12:44:56 LOG_NOTICE [9336:11464]: Autologin value: 0.
2020.03.27 12:44:56 LOG_INFO [9336:11464]: SecureConnect started
2020.03.27 12:44:57 LOG_ERR [9336:11464]: Could not find pipe
2020.03.27 12:44:58 LOG_DEBUG [9336:11464]: Try the 1 time to find the named pipe
2020.03.27 12:44:58 LOG_ERR [9336:11464]: Could not find pipe
2020.03.27 12:44:59 LOG_DEBUG [9336:11464]: Try the 2 time to find the named pipe
2020.03.27 12:47:03 LOG_INFO [9336:11464]: Login mode changed from 0 to 1
2020.03.27 12:49:29 LOG_INFO [9336:11464]: Login mode changed from 1 to 2
2020.03.27 12:49:39 LOG_INFO [9336:11464]: Login mode changed from 2 to 1
2020.03.27 12:50:42 LOG_INFO [9336:11464]: Login mode changed from 1 to 2
2020.03.27 13:13:19 LOG_INFO [9336:11464]: Login mode changed from 2 to 1
2020.03.27 13:20:56 LOG_INFO [9336:11464]: Login mode changed from 1 to 2
2020.03.27 13:22:11 LOG_INFO [9336:11464]: Login mode changed from 2 to 1
2020.03.27 13:23:03 LOG_INFO [9336:11464]: Login mode changed from 1 to 2
2020.03.27 13:30:02 LOG_INFO [9336:11464]: Login mode changed from 2 to 0
2020.03.27 13:30:06 LOG_INFO [9336:11464]: CBruteForceGuard: Cannot find prober for ranliu@access.hillstonenet.co
2020.03.27 13:30:06 LOG_DEBUG [9336:11464]: Peer server count: 0
2020.03.27 13:30:06 LOG_INFO [9336:11464]: Set the Reconnect Status = 1...in main
2020.03.27 13:30:06 LOG_DEBUG [9336:8420]: hssvc is Ready!
2020.03.27 13:30:06 LOG_INFO [9336:8420]: Connecting to access.hillstonenet.com...
2020.03.27 13:30:06 LOG_INFO [9336:1436]: [SslChannel --> SecureConnect] Peer server list. 0 servers
2020.03.27 13:30:17 LOG_DEBUG [9336:5572]: ProcessSSLChannelCommand: SetLiveupHandle()
```

- This dialog shows the main log messages. To view the detailed log messages, click **Detail**. Click **Clear** to remove the messages in the dialog. Click **OK** to close the Log dialog.

- **Debug**: Configures Secure Connect's debug function in the Debug dialog.



- **About**: Shows Secure Connect related information in the **About** dialog.

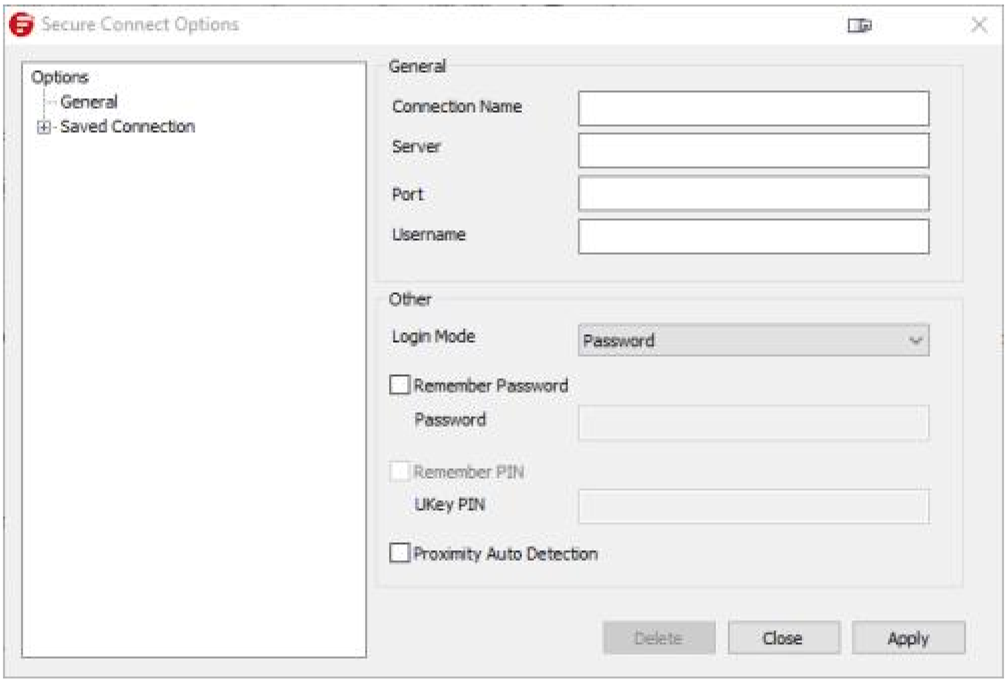


FS Secure Connect
1.4.9.1271
All rights reserved.
(C) 2009-2020 Fiberstore Co.,Limited

- **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.
- **Exit**: Click **Exit** to close the client.

Configuring Secure Connect

You can configure Secure Connect through the Secure Connect Options dialog (click **Option** from the client menu) as shown below:



This dialog allows you to make the following configurations:

- Configuring General Options
- Adding a Login Entry
- Editing a Login Entry
- Deleting a Login Entry

Configuring General Options

In the Secure Connect Options dialog, select **General** from the navigation pane and the general options will be displayed.

- **Auto Start**: Select this checkbox to automatically run the SSL VPN client when the PC is starting.
- **Auto Reconnect**: Select this checkbox to automatically reconnect to the SSL VPN server when the connection is hung up.
- **Auto Login**: Select this checkbox to allow the specified user to login automatically when the PC is starting. Select the auto login user from the Default Connection drop-down list.
- **Select Cert**: Select the USB Key certificate by click this button. For more information about login with USB Key, see Starting the Software Directly. This option is available when USB Key authentication is enabled.

Adding 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. You can login by simply choosing the wanted connection instead of filling up the options in the Login dialog.

To add a login entry, take the following steps:

1. In the Secure Connect Options dialog, select **Saved Connection** from the navigation pane and the login options will be displayed.
2. Fill up the options. The descriptions of the options are:
    - **Connection Name**: Specifies the name for the connection to identify it. The system will assign a name to the connection based on its server, port, and user automatically if keeping this option 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) or **Password + PIN** (the USB Key authentication method). If **Password** is selected, select **Remember Password** to make the system remember the password and type the password into the **Password** box. If **Password + PIN** is selected, select **Remember PIN** to make the system remember the PIN code and type PIN code into the **UKey PIN** box.
    - **Proximity Auto Detection**: Select the option to enable optimal path detection function. For more information about optimal path detection, see Selecting an Optimal Path.
3. Click **Apply**.

Editing a Login Entry

To edit a login entry, take the following steps:

1. In the Secure Connect Options dialog, expand Saved Connection from the navigation pane, and select the entry you want to edit. The corresponding login options will be displayed.
2. Modify the options according to your need.

Even if the login entry is modified, the connection name won't be changed. The connection name is used by the system to distinguish the changes to the entry, including adding a new entry and modify an existing entry:

- If the connection name is changed, the system will consider it as a new entry.
- If the connection name is kept unchanged, the system will consider it as a modified entry.

Deleting a Login Entry

To delete a login entry, take one of the following methods:

- In the Secure Connect Options dialog, expand **Saved Connection** from the navigation pane, right click the entry you want to delete, and click **Delete User** from the menu.
- In the Secure Connect Options dialog, expand **Saved Connection** from the navigation pane, select the entry you want to delete, and click **Delete** at the lower-right.

Uninstalling Secure Connect

To uninstall the Secure Connect on your PC, from the Start menu, click **All Programs** > **FS Secure Connect** > **Uninstall**.

SSL VPN Client for Android

The SSL VPN client for Android is FS Secure Connect. It can run on Android 4.0 and above. The functions of FS 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.

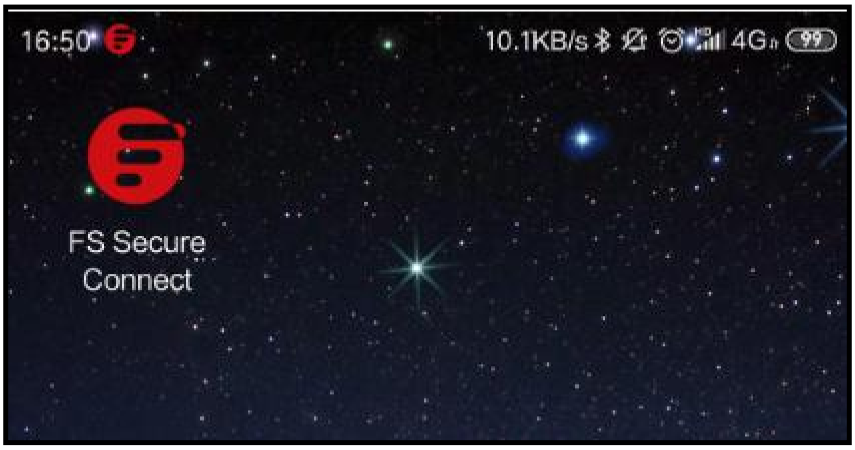
Downloading and Installing the Client

To download and install the client, take the following steps:

1. Visit //客户端下载地址 to download the installation file of the client.
2. After downloading successfully, find this file in your mobile phone.
3. Click it and the installation starts.
4. Read the permission requirements.

5. Click **Install**.

After installing the client successfully, the icon of FS 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 FS Secure Connect. The login page appears.
2. In the login page, 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 [Configuration Management.]()
   - 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.

After the client connects to the SSL VPN server, the "VPN" 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 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 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.
   - In the pop-up window, enter the following information:
   - Connection 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.
2. 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 display.
2. Click **Edit**. The Edit Configuration dialog appears.
3. In the dialog, 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 display.
2. Click **Delete**.
3. Click **Yes** in the pop-up dialog 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 display.
2. Click **Modify Password**.
3. Enter the current password and new password in the pop-up dialog.
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 display.
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, 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 will 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 keep connected while the Android system 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 Android system is in the sleep status.

- Auto Login: After turning on this switch, the client will automatically connect to the server when it stars. The server is the one that the client connects to the last time.
- Remember The Password: After turning on this switch, the client will remember the password and automatically fill in the login entry.
- Exit: Click **Exit** to exit this application.

About Us

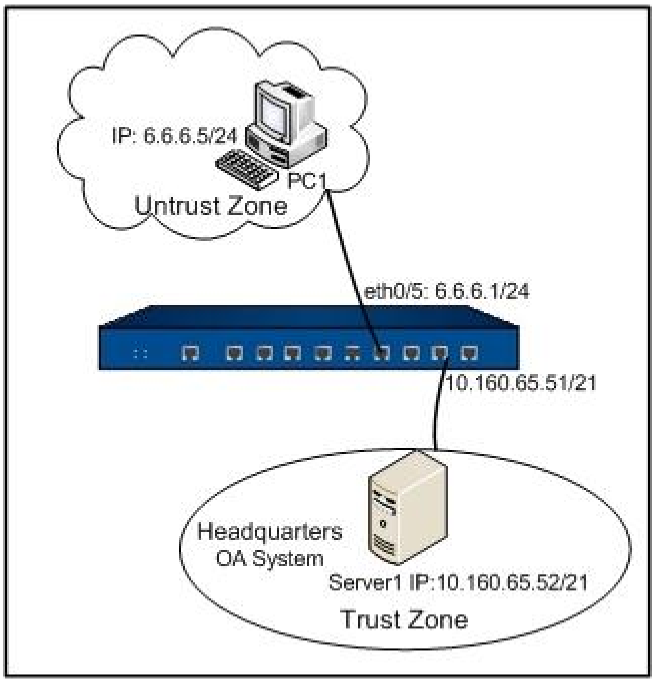
Click **About** at the bottom of the page to enter into the About US page. This page displays the version information, contact information, copyright information, etc.

Example of Configuring URL Redirect

This section describes a URL redirect configuration example.

An enterprise uses FS device as the SSL VPN server in its OA system. The goal is to log into both the SSL VPN and OA system at one time.

This requirement can be met by the URL redirect function. The topology is shown as below:



Configuration Steps

Step 1: Create a local user

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user test
hostname(config-user)# password test

hostname(config-user)# exit

hostname(config-aaa-server)# exit

hostname(config)#
```

Step 2: Configure an SSL VPN address pool

```
hostname(config)# scvpn pool pool1

hostname(config-pool-scvpn)# address 20.1.1.120.1.1.255 netmask 255.255.255.0

hostname(config-pool-scvpn)# dns 20.1.1.1

hostname(config-pool-scvpn)# wins 20.1.1.2

hostname(config-pool-scvpn)# exit

hostname(config)#
```

Step 3: Configure URL redirect in an SSL VPN instance. To limit the access range of the remote user, use the no split-tunnel-route 0.0.0.0/0 command

```
hostname(config)# tunnel scvpn ssl1

hostname(config-tunnel-scvpn)# pool pool1

hostname(config-tunnel-scvpn)# aaa-server local

hostname(config-tunnel-scvpn)# interface ethernet0/5

hostname(config-tunnel-scvpn)# https-port 4433

hostname(config-tunnel-scvpn)# redirect-url
http://192.10.5.201/oa/login.do?username=$USER&password=$PWD title-en OA title-zh

hostname(config-tunnel-scvpn)# split-tunnel-route 10.160.64.0/21

hostname(config-tunnel-scvpn)# split-tunnel-route 192.10.5.0/24

hostname(config-tunnel-scvpn)# exit

hostname(config)#
```

Step 4: Create a tunnel interface and bind the SSL VPN instance to it (the tunnel interface and SSL VPN address pool must be in the same network segment)

```
hostname(config)# zone VPN
hostname(config-zone-VPN)# exit

hostname(config)# interface tunnel1

hostname(config-if-tun1)# zone VPN

hostname(config-if-tun1)# ip address 20.1.1.1/24

hostname(config-if-tun1)# tunnel scvpn ssl1

hostname(config-if-tun1)# exit

hostname(config)#
```

Step 5: Configure a policy from VPN zone to trust zone

```
hostname(config)# policy-global

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone VPN

hostname(config-policy-rule)# dst-zone trust

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config-policy)# exit

hostname(config)#
```

Step 6: In the web browser of PC1, visit https://6.6.6.1:4433, and in the login page, type test and test into the Username and Password boxes respectively. After the authentication, download and install Secure Connect.

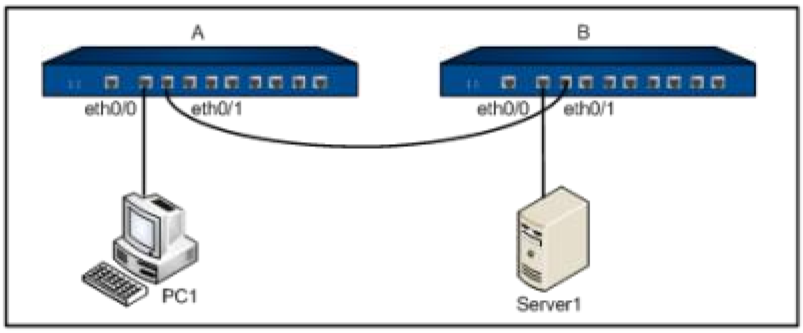
Step 7: After logging in with Secure Connect, the page will be redirected to the OA system authentication page

Examples of Configuring SSL VPN

This section describes several SSL VPN examples with the username/password authentication method.

Requirement

Server1 (10.160.65.52/21) in the Intranet is protected by a FS device. PC1 (6.6.6.5/24) in Internet wants to visit the resources on Server1 (10.160.65.52/21).



- **Requirement 1**: The goal is to control the access by encrypting the data by SSL VPN with the username/password authentication method.
- **Requirement 2:** The goal is to control the access by encrypting the data by SSL VPN with the USB Key authentication method. As long as the UKey of the client supports standard Windows SDK (Certificate Store Functions) and the stored certificate is valid, the client can log in. FS UKey is used as the example.

Example 1

Step 1: Create a local user

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user user1
hostname(config-user)# password 123456
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)#exit
```

Step 2: Configure an SSL VPN address pool

```
hostname(config)# scvpn pool pool1
hostname(config-pool-scvpn)# address 20.1.1.120.1.1.100 netmask 255.255.255.0
hostname(config-pool-scvpn)# dns 20.1.1.1
hostname(config-pool-scvpn)# wins 20.1.1.2
hostname(config-pool-scvpn)# exit
hostname(config)#
```

Step 3: Configure an SSL VPN instance. By default, the system adds the split-tunnel-route 0.0.0.0/0 route entry. To limit the access range of the remote user, use the no split-tunnel-route 0.0.0.0/0 command

```
hostname(config)# tunnel scvpn ssl1
hostname(config-tunnel-scvpn)# pool pool1
hostname(config-tunnel-scvpn)# aaa-server local
hostname(config-tunnel-scvpn)# interface ethernet0/5
hostname(config-tunnel-scvpn)# https-port 4433
hostname(config-tunnel-scvpn)# split-tunnel-route 10.160.64.0/21
hostname(config-tunnel-scvpn)# exit
hostname(config)#
```

Step 4: Create a tunnel interface and bind the SSL VPN instance to it (the tunnel interface and SSL VPN address pool should be in the same IP address segment)

```
hostname(config)# zone VPN
hostname(config-zone-VPN)#
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone VPN
hostname(config-if-tun1)# ip address 20.1.1.101/24
hostname(config-if-tun1)# tunnel scvpn ssl1
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 5: Configure a policy from VPN zone to trust zone

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone VPN
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 6: Type **https://6.6.6.1:4433** in the Web browser to visit the login page. Enter username user1 and password 123456. When you log in successfully, download the SSL VPN client FS Secure Connect

Step 7: After logging in, PC1 can access resources in the trust zone through SSL VPN

Example 2

On the basis of Example 1, add USB Key authentication feature. This feature requires that user's UKey should support standard Windows SDK (Certificate Store Functions) with a legal certificate in it. This example uses the FS UKey.

Preparations

Before using the USB Key, make the following preparations:

- Prepare the certificate and the corresponding CA certificate;
- Prepare the FS UKey and the CD provided by FS;
- Import the certificate to the UKey using FS UKey manager.

Configuration Steps

Step 1: Configure an SSL VPN server

```
#Create a PKI trust domain named stone and specify that the certificate is obtained by the method of terminal
hostname(config)# pki trust-domain stone
hostname(config-trust-domain)# enrollment terminal
hostname(config-trust-domain)# exit
hostname(config)#
```

```
#Enable USB Key certificate authentication of SSL VPN instance SSL1 and specify a CA trust domain
hostname(config)# tunnel scvpn ssl1
hostname(config-tunnel-scvpn)# client-cert-auth
hostname(config-tunnel-scvpn)# client-auth-trust-domain stone
hostname(config-tunnel-scvpn)# exit
hostname(config)#
#Import the CA certificate file to the CA trust domain
hostname(config)# exit
hostname# import pki stone cacert from tftp server 192.168.1.2 certnew.cer
```

Step 2: Operations on the clients

1. Install FS UKey driver on the client PC.
2. Insert the UKey.
3. In the SSL VPN client Login dialog, fill each option as below and click Login:
   - Server: 6.6.6.1
   - Port: 4433
   - Username: user1
   - Password: FS1111
   - PIN: 1111 (the default value)

Example of Configuring Host Check

This section describes an SSL VPN host check configuration example.

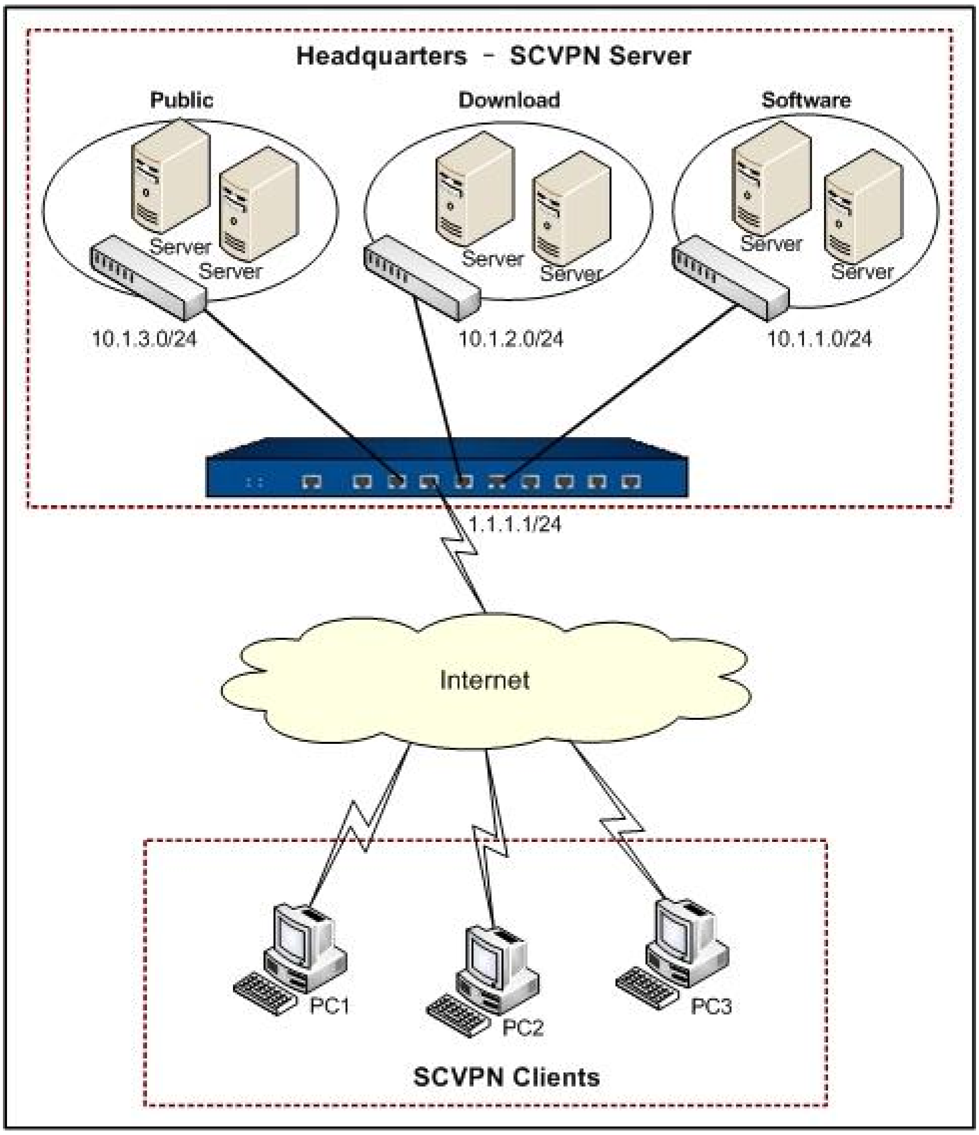
Requirements

The FS device works as the SSL VPN server for an enterprise. The goal is to meet the following requirements:

- The client can access headquarters resources with SSL VPN.

- Resources in the software network segment (10.1.1.0/24) can be accessed by role sw only; resources in the downloading network segment (10.1.2.0/24) can be accessed by role dl; and resources in public network segment (10.1.3.0/24) can be accessed by all users.
- Perform host security check to the clients and control the resources access based on the check results.

The topology is shown as below:



Configuration Steps

Step 1: Create a local user

```
hostname(config)# aaa-server local type local
hostname(config-aaa-server)# user pc1
hostname(config-user)# password xxxfcvg236

hostname(config-user)# exit

hostname(config-aaa-server)# user pc2

hostname(config-user)# password xcabuv112

hostname(config-user)# exit

hostname(config-aaa-server)# user pc3

hostname(config-user)# password xacfomg763

hostname(config-user)# exit

hostname(config-aaa-server)# exit

hostname(config)#
```

Step 2: Configure a role mapping rule

```
hostname(config)# role sw

hostname(config)# role dl

hostname(config)# role-mapping-rule rule1

hostname(config-role-mapping)# match user pc1 role sw

hostname(config-role-mapping)# match user pc1 role dl

hostname(config-role-mapping)# match user pc2 role dl

hostname(config-role-mapping)# exit

hostname(config)# aaa-server local type local

hostname(config-aaa-server)# role-mapping-rule rule1

hostname(config)#
```

Step 3: Configure an interface on the SSL VPN server

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

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

hostname(config-if-eth0/1)# ip address 1.1.1.1/24

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

hostname(config)#
```

Step 4: Configure the host check profiles

```
hostname(config)# scvpn host-check-profile dl-security-check
hostname(config-profile_scvpn)# exit
hostname(config)# scvpn host-check-profile sw-security-check
hostname(config-profile_scvpn)# exit
hostname(config)#
```

To configure a host check profile on WebUI interface, take the following steps:

1. On the Navigation pane, click **Configure > Network > SSL VPN** to visit the SSL VPN page.
2. On the **Task** tab in the right auxiliary pane, click **Host Check** to visit the Host Check page.
3. Click **New**. In the Host Checking Configuration dialog, configure the options as below:

   Basic

   - **Name**: dl-security-check
   - **OS version**: At least, Win2003, None
   - **Patch 1**: KB958215
   - **Lowest IP version**: IE6.0
   - **Lowest IP security level**: High

   Advanced

   - **Security center**: Must
   - **Anti-Virus software**: Installed, Monitor, Virus signature DB update
   - **Anti-Spyware software**: Installed, Monitor, Signature DB update
   - **Firewall**: Installed, Monitor
4. Click **OK** to save the settings and return to the SSL VPN page.
5. Repeat Step 3-4 to create the profile named sw-security-check. The profile contents are:

   Basic

   - **Name**: sw-security-check

- **OS version**: Must match, WinXP, SP3
- **Patch 1**: KB921883
- **Lowest IP version**: IE7.0
- **Lowest IP security level**: High

Advanced

- **Security center**: Must
- **Auto update**: Must
- **Anti-Virus software**: Installed, Monitor, Virus signature DB update
- **Anti-Spyware software:** Installed, Monitor, Signature DB update
- **Firewall**: Installed, Monitor
- **File path name**: File 1: Exist, C:\Program Files\McAfee\VirusScan\Enterprise.exe

6. Click **OK** to save settings.

Step 5: Configure an SSL VPN address pool

```
hostname(config)# scvpn pool pool1
hostname(config-pool-scvpn)# address11.1.1.10 11.1.1.100 netmask 255.255.255.0
hostname(config-pool-scvpn)# dns 10.1.1.1
hostname(config-pool-scvpn)# wins 10.1.1.2
hostname(config-pool-scvpn)# exit
hostname(config)#
```

Step 6: Configure an SSL VPN instance. To limit the access range of the remote user, use the no split-tunnel-route 0.0.0.0/0 command

```
hostname(config)# tunnel scvpn ssl1
hostname(config-tunnel-scvpn)# pool pool1
hostname(config-tunnel-scvpn)# aaa-server local
hostname(config-tunnel-scvpn)# interface ethernet0/1
hostname(config-tunnel-scvpn)# https-port 4433
hostname(config-tunnel-scvpn)# split-tunnel-route 10.1.1.0/24 metric 10

hostname(config-tunnel-scvpn)# split-tunnel-route 10.1.2.0/24 metric 5

hostname(config-tunnel-scvpn)# split-tunnel-route 10.1.3.0/24 metric 3

hostname(config-tunnel-scvpn)# host-check role sw profile sw-security-check guest-role dl

hostname(config-tunnel-scvpn)# host-check profile dl-security-check periodic-check 50

hostname(config-tunnel-scvpn)# exit

hostname(config)#
```

Step 7: Create a tunnel interface and bind the SSL VPN instance to it (the tunnel interface and SSL VPN address pool should be in the same IP address segment)

```
hostname(config)# zone VPN

hostname(config-zone-VPN)# exit

hostname(config)# interface tunnel1

hostname(config-if-tun1)# zone VPN

hostname(config-if-tun1)# ip address11.1.1.1/24

hostname(config-if-tun1)# tunnel scvpn ssl1

hostname(config-if-tun1)# exit

hostname(config)#
```

Step 8: Configure a policy rule

```
hostname(config)# address sw

hostname(config-addr)# ip 10.1.1.0/24

hostname(config-addr)# exit

hostname(config)# address dl

hostname(config-addr)# ip 10.1.2.0/24

hostname(config-addr)# exit

hostname(config)# address public

hostname(config-addr)# ip 10.1.3.0/24

hostname(config-addr)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone VPN
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr sw
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# role sw
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone VPN
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr dl
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# role dl
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone VPN
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr public
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

After finishing the above configurations, when the client connects the server, the server will check the host based on the configured host check profile, and assign the corresponding access right according to the check result. The following list shows the relationship between the host check rule and the access right.

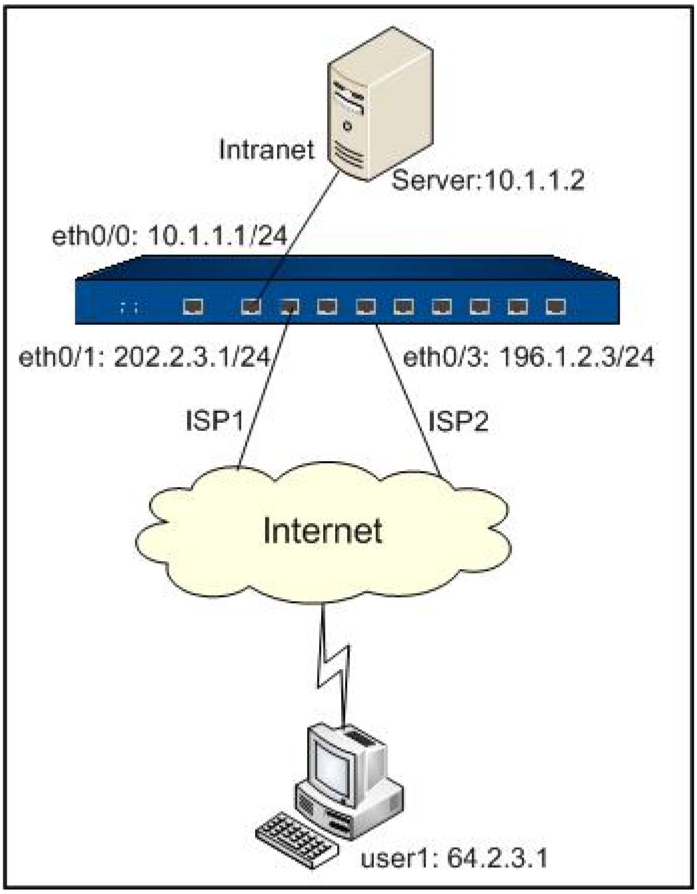
User	Host check rule	Check result and access right	
		Successful	Failed
PC1	Role: sw Profile: sw-security-check Guest role: dl Periodic: 30 minutes CLI: **host-check role sw profile sw-security-check guest-role dl**	Permit to access resources in the software network segment, and the host check will performed every 30 minutes automatically.	Permit to access resources in the download network segment, and the host check will be performed every 30 minutes automatically.
PC2	Role: Null (the access right of the default role dl will be assigned) Profile: dl-security-check Guest role: Null Periodic: 50 minutes CLI: **host-check profile dl-security-check periodic-check 50**	Permit to access resources in the software network segment, and the host check will performed every 30 minutes automatically.	Disconnect
PC3	Role: Null Profile: dl-security-check Guest role: Null Periodic: 50 minutes CLI: **host-check profile dl-security-check periodic-check 50**	Permit to access resources in the public network segment, and the host check will be performed every 50 minutes automatically.	Disconnect

Example of Configuring Optimal Path

This section provides an example of configuring SSL VPN optimal path.

Requirement 1

A company uses a FS device as the SSL VPN server which has two accesses to the Internet, ISP1 (ethernet0/1, IP: 202.2.3.1/24) and ISP2 (ethernet0/3, IP: 196.1.2.3/24). The goal is that the PC (IP: 64.2.3.1) can access the headquarters server (IP: 10.1.1.2) using optimal path detection feature.



You have two configuration methods to meet this requirement, which are:

- Using the server to choose an optimal path
- Using the client to choose an optimal path

Using SSL VPN Server to Choose an Optimal Path

Step 1: Create a local user

```
hostname(config)# aaa-server local type local
hostname(config-aaa-server)# user user1
hostname(config-user)# password drgrhrgerg231
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 2: Configure the server interface

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 10.1.1.0/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 202.2.3.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone untrust
hostname(config-if-eth0/3)# ip address 196.1.2.3/24
hostname(config-if-eth0/3)# exit
hostname(config)#
```

Step 3: Configure an SSL VPN address pool

```
hostname(config)# scvpn pool pool1
hostname(config-pool-scvpn)# address 11.1.1.10 11.1.1.100 netmask 255.255.255.0
hostname(config-pool-scvpn)# dns 10.1.1.1
hostname(config-pool-scvpn)# wins 10.1.1.2
hostname(config-pool-scvpn)# exit
hostname(config)#
```

Step 4: Configure an SSL VPN instance (with optimal path detection). To limit the access range of the remote user, use the no split-tunnel-route 0.0.0.0/0 command

```
hostname(config)# tunnel scvpn ssl1
hostname(config-tunnel-scvpn)# pool pool1
hostname(config-tunnel-scvpn)# aaa-server local
hostname(config-tunnel-scvpn)# interface ethernet0/1
hostname(config-tunnel-scvpn)# interface ethernet0/3
hostname(config-tunnel-scvpn)# https-port 4433
hostname(config-tunnel-scvpn)# split-tunnel-route 10.1.1.0/24 metric 10
hostname(config-tunnel-scvpn)# link-select server-detect
hostname(config-tunnel-scvpn)# exit
hostname(config)#
```

Step 5: Create a tunnel interface and bind the SSL VPN instance to it (the tunnel interface and SSL VPN address pool should be in the same IP address segment)

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ip address 11.1.1.1/24
hostname(config-if-tun1)# tunnel scvpn ssl1
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 6: Configure a policy rule

```
hostname(config)# address dst
hostname(config-addr)# ip 10.1.1.0/24
hostname(config-addr)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr dst
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 7: Configure an ISP

```
hostname(config)# isp-network isp1
hostname(config-isp)# subnet 202.2.3.0/24
hostname(config-isp)# subnet 64.2.3.0/24
hostname(config-isp)# exit
hostname(config)#
```

When the client PC initiates a connection request to SSL VPN server using ISP2, the server identifies that the IP addresses of SSL VPN egress interface ethernet0/1 and client PC both belong to ISP1, so it assigns an IP of egress interface with higher priority to the client and the PC can access the headquarters server using ISP1.

Using SSL VPN Client to Choose an Optimal Path

Configuration steps of using client to choose optimal path have slight differences with steps of using the server in choosing optimal path, and the different steps are:

Step 4: Configure an SSL VPN instance (with optimal path detection feature)

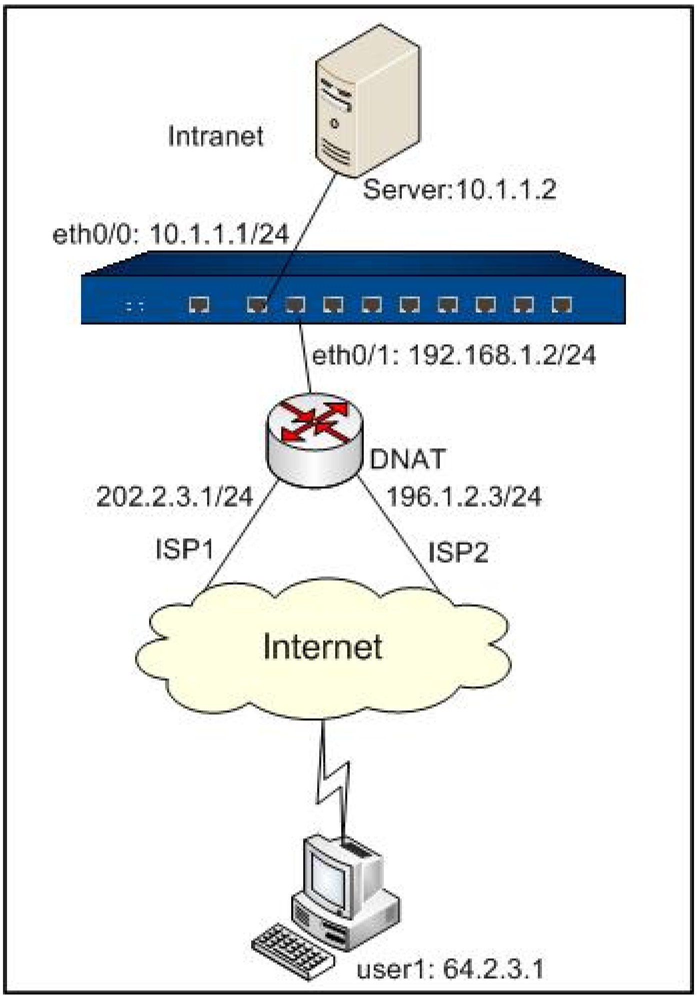
```
hostname(config)# tunnel scvpn ssl1
……
hostname(config-tunnel-scvpn)# link-select
……
```

Step 7: Skip this step

When the PC initiates connection requests to the headquarters using ISP2 link, the server will assign the IP addresses of both ethernet0/1 and ethernet 0/3 to the client and the client judges the optimal path by sending UDP probe packets.

Requirement 2

A company uses a FS device as the SSL VPN server in its headquarters and uses a DNAT device with two Internet accesses (ISP1: 202.2.3.1/24 and ISP2: 196.1.2.3/24). The goal for the client PC (64.2.3.1) is to access to the headquarters server (IP: 10.1.1.2) using optimal path detection feature.



You have two configuration methods to meet this requirement, which are:

- Using SSL VPN server to choose an optimal path
- Using SSL VPN client to choose an optimal path

Using SSL VPN Server to Choose an Optimal Path

Step 1: Create a local user

```
hostname(config)# aaa-server local type local
hostname(config-aaa-server)# user user1
hostname(config-user)# password drgrhrgerg231
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 2: Configure the server interface

```
hostname(config)# interface ethernet0/0

hostname(config-if-eth0/0)# zone trust

hostname(config-if-eth0/0)# ip address 10.1.1.0/24

hostname(config-if-eth0/0)# exit

hostname(config)# interface ethernet0/1

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

hostname(config-if-eth0/1)# ip address 192.168.1.2/24

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

hostname(config)#
```

Step 3: Configure an SSL VPN address pool

```
hostname(config)# scvpn pool pool1

hostname(config-pool-scvpn)# address 11.1.1.10 11.1.1.100 netmask 255.255.255.0

hostname(config-pool-scvpn)# dns 10.1.1.1

hostname(config-pool-scvpn)# wins 10.1.1.2

hostname(config-pool-scvpn)# exit

hostname(config)#
```

Step 4: Configure an SSL VPN instance (with optimal path detection). To limit the access range of the remote user, use the **`no split-tunnel-route 0.0.0.0/0`** command

```
hostname(config)# tunnel scvpn ssl1

hostname(config-tunnel-scvpn)# pool pool1

hostname(config-tunnel-scvpn)# aaa-server local

hostname(config-tunnel-scvpn)# interface ethernet0/1

hostname(config-tunnel-scvpn)# https-port 4433

hostname(config-tunnel-scvpn)# split-tunnel-route10.1.1.0/24 metric 10

hostname(config-tunnel-scvpn)# link-select server-detect 202.2.3.1 https-port 2234 196.1.2.3
https-port 3367

hostname(config-tunnel-scvpn)# exit
hostname(config)#
```

Step 5: Create a tunnel interface and bind the SSL VPN instance to it (the tunnel interface and SSL VPN address pool should be in the same IP address segment)

```
hostname(config)# interface tunnel1

hostname(config-if-tun1)# zone untrust

hostname(config-if-tun1)# ip address 11.1.1.1/24

hostname(config-if-tun1)# tunnel scvpn ssl1

hostname(config-if-tun1)# exit

hostname(config)#
```

Step 6: Configure a policy rule (a rule from dmz zone to trust zone)

```
hostname(config)# address dst

hostname(config-addr)# ip 10.1.1.0/24

hostname(config-addr)# exit

hostname(config)# policy-global

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone dmz

hostname(config-policy-rule)# dst-zone trust

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr dst

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config-policy)# exit

hostname(config)#
```

Step 7: Configure an ISP

```
hostname(config)# isp-network isp1
hostname(config-isp)# subnet 202.2.3.0/24

hostname(config-isp)# subnet 64.2.3.0/24

hostname(config-isp)# exit

hostname(config)#
```

When the client PC initiates a connection request to SSL VPN server using ISP2, the DNAT device translates the client address (196.1.2.3:3367) to SSL VPN server’ s egress interface address (192.168.1.2:4433). Then, the server identifies that the IP addresses of client PC and DNAT Internet interface (202.2.3.1/24) belong to ISP1, so it assigns the IP of DNAT’ s Internet interface which has higher priority to the client and the PC can access the headquarters server using ISP1.

Using SSL VPN Client to Choose an Optimal Path

Configuration steps of using client to choose optimal path have slight differences with steps of using the server in choosing optimal path, and the different steps are:

Step 4: Configure an SSL VPN instance (with optimal path detection feature)

```
hostname(config)# tunnel scvpn ssl1

……

hostname(config-tunnel-scvpn)# link-select 202.2.3.1 https-port 2234 196.1.2.3 https-port 3367

……
```

Step 7: Skip this step

When the PC initiates connection requests to the headquarters using ISP2 link, the DNAT device translates client address (196.1.2.3:3367) to SSL VPN server’ s egress interface address (192.168.1.2: 4433). The SSL VPN server will assign the IP address of DNAT device’ s Internet interface to the client, and the client judges the optimal path by sending UDP probe packets.

Dial-up VPN

Overview

Dial-up VPN means the center device has only one VPN tunnel established to allow multiple remote clients accessing to it through this VPN tunnel. The remote clients should be configured with same IKE VPN settings with the center device for data protection. Meanwhile, the center device uses pre-shared key or certificate to authenticate the clients and establishes VPN tunnel to communicate with the clients.

Applying Dial-up VPN

There are two methods of applying a configured VPN tunnel to the security device to achieve secure traffic transmissions: one is to use policy-based VPN, the other is to use route-based VPN.

- Policy-based VPN: When you use policy-based VPN, the VPN tunnel is introduced into a policy rule so that traffic which conforms to the rule can be transferred through the VPN tunnel. Policy-based VPN supports accessing from branch to center, but does not support accessing from center to branch or hub-and-spoke.
- Route-based VPN: When you use route-based VPN, the VPN tunnel binds to a tunnel interface and the next hop of static route is the tunnel interface.

Configuring the Center Device

This section introduces the following configurations of dial-up VPN center device:

- Configuring P1 proposal
- Configuring an ISAKMP gateway
- Configuring P2 proposal
- Configuring a tunnel
- Configuring a dial-up user

Configuring P1 Proposal

P1 proposal is an IKE security proposal applied to ISAKMP gateway in the SA Phase 1. Configuring an IKE proposal includes settings of authentication, encryption algorithm, DH group and SA lifetime.

Creating a P1 Proposal

To create a P1 proposal (IKE security proposal), in the global configuration mode, use the following command:

isakmp proposal *p1-name*

- *p1-name* – Type a name for the new P1 proposal. This command leads you into the P1 proposal configuration mode in which you can configure the proposal.

To delete the specified P1 proposal, use the command **no isakmp proposal** *p1-name*.

Specifying an Authentication Method

Authentication defined here refers to IKE identity authentication which is used to confirm the identities of the two communicating peers. Authentication can be performed in two ways: pre-shared key authentication and digital certificate authentication. For pre-shared key authentication, community is used to generate a private key as the input.

To specify the authentication method of IKE security proposal, in the P1 proposal configuration mode, use the following command:

```
authentication {pre-share | rsa-sig | dsa-sig}
```

- **pre-share** − Specifies that the pre-shared key is used for authentication. This is the default method.
- **rsa-sig** − Specifies that RSA digital certificate is used for authentication.
- **dsa-sig** − Specifies the DAS digital certificate is used for authentication.

To restore to the default authentication method, use the command **no authentication**.

Specifying an Encryption Algorithm

The following five encryption algorithms are supported: 3DES, DES, 128-bit AES, 192-bit AES and 256-bit AES.

To specify the encryption algorithm of IKE security proposal, in the P1 proposal configuration mode, use the following command:

```
encryption {3des | des | aes | aes-192 | aes-256}
```

- 3des − Specifies to use 3DES encryption algorithm. The private key length is 192 bits. This is the default encryption method.
- des − Specifies to use DES encryption algorithm. The private key length is 64 bits.
- aes − Specifies to use AES encryption algorithm. The private key length is 128 bits.
- aes-192 − Specifies to use 192-bit AES encryption algorithm. The private key length is 192 bits.
- aes-256 − Specifies to use 256-bit AES encryption algorithm. The private key length is 256 bits.

To restore to the default encryption algorithm, use the command **no encryption**.

Specifying a Hash Algorithm

The following authentication algorithms are supported: MD5, SHA-1 and SHA-2 (including SHA-256, SHA-384 and SHA-512).

To specify a Hash algorithm for IKE security proposal, in the P1 proposal configuration mode, use the following command:

hash {**md5** | **sha** | **sha256** | **sha384** | **sha512**}

- **md5** − Specifies to use MD5 for authentication. The hash value length is 128 bits.
- **sha** − Specifies to use SHA-1 for authentication. The hash value length is 160 bits. This is the default value.
- **sha256** − Specifies to use SHA-256 for authentication. The hash value length is 256 bits.
- **sha384** − Specifies to use SHA-384 for authentication. The hash value length is 384 bits.
- **sha512** − Specifies to use SHA-512 for authentication. The hash value length is 512 bits.

To restore to the default algorithm method, use the command **no hash**.

Selecting a DH Group

Diffie-Hellman (DH) is designed to establish a shared secret key. DH group determines the length of the element generating keys for DH exchange. The strength of keys is partially decided by the robustness of the DH group. The longer the key element is, the more secure the generated key will be, and the more difficult it will be to decrypt it. The selection of DH group is important, because the DH Group is only determined in the Phase 1 SA negotiation, and the Phase 2 negotiation will not re-select a DH group. The two phases use the same DH group; therefore the selection of DH group will have an impact on the keys generated for all sessions. During negotiation, the two ISAKMP gateways should select the same DH group, i.e., the length of key element should be equal. If the DH groups do not match, the negotiation will fail.

To select a DH group, in the P1 proposal configuration mode, use the following command:

group {**1** | **2** | **5** | **14** | **15** |**16**}

- **1** - Selects DH Group1. The key length is 768 bits.
- **2** - Selects DH Group2. The key length is 1024 bits. This is the default value.
- **5** - Selects DH Group5. The key length is 1536 bits.
- **14** - Selects DH Group14. The key length is 2048 bits.
- **15** - Selects DH Group15. The key length is 3072 bits.

- 16 - Selects DH Group16. The key length is 4096 bits.

To restore the DH group to the default, in the P1 proposal configuration mode, use the command **no group**.

Specifying a SA Lifetime

Phase 1 SA negotiation has a default lifetime. When ISAKMP SA lifetime is due, it sends an SA P1 deleting message to the peer, and then initiates a new SA negotiation.

To specify a SA lifetime, in the P1 proposal configuration mode, use the following command:

lifetime *time-value*

- *time-value* – Specifies the lifetime of SA Phase 1. The value range is 300 to 86400 seconds. The default value is 86400.

To restore to the default lifetime, use the command **no lifetime**.

Configuring an ISAKMP Gateway

This section introduces configurations about ISAKMP gateway.

Creating an ISAKMP Gateway

To create an ISAKMP gateway, in the global configuration mode, use the following command:

isakmp peer *peer-name*

- *peer-name* – Specifies a name for the ISAKMP gateway.

This command leads you into ISAKMP gateway configuration mode in which you can configure the parameters of the gateway.

To delete the specified ISAKMP gateway, in the global configuration mode, use the command **no isakmp peer** *peer-name*.

Specifying an AAA Server for ISAKMP Gateway

AAA server defined here is used to authenticate the peer device.

To specify an AAA server for the ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

aaa-server *server-name*

- *server-name* – Specifies the name of AAA server. All types of AAA server can be ISAKMP gateway, including local, Radius, AD, LDAP and TACACS+ server.

To delete the specified AAA server, in the ISAKMP gateway configuration mode, use the following command:

no aaa-server

Binding an Interface to the ISAKMP Gateway

To bind an interface to the ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

interface *interface-name*

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

To cancel the binding of interface, use the command no interface.

Configuring an IKE Negotiation Mode

There are two IKE negotiation modes: Main and Aggressive. The main mode is the default mode. The aggressive mode cannot protect identity. You have no choice but use the aggressive mode in the situation that the IP address of the center device is static while the IP address of client device is dynamic.

To configure an IKE negotiation mode, in the ISAKMP gateway configuration mode, use the following command:

mode {main | aggressive}

- main – The main mode can provide ID protection and it is the default mode.
- aggressive – Specifies to use the aggressive mode.

To cancel the IKE negotiation mode, use the command **no mode**.

Specifying a Peer Type

To specify a type for the peer device, in the ISAKMP gateway configuration mode, use the following command:

type usergroup

To cancel the specified type of a peer device, in the ISAKMP gateway configuration mode, use the following command:

no type

Specifying P1 Proposal

To specify P1 proposal for the ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

isakmp-proposal p1-proposal1[p1-proposal2] [p1-proposal3] [p1-proposal4]

- **p1-proposal1** – Specifies the name of P1 proposal. You are allowed to specify up to four P1 proposals for an ISAKMP gateway' s peer.

To cancel the specified P1 proposal, use the command **no isakmp-proposal**.

Configuring a Pre-shared Key

If you decide to use pre-shared key to authenticate, to specify a pre-shared key for ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

pre-share *string*

- *string* – Specifies the content of pre-shared key.

To cancel the specified pre-shared key, use the command **no pre-share**.

Configuring a PKI Trust Domain

If digital certificate is used to authenticate, you need to specify a PKI trust domain for the certificate. To specify a PKI trust domain, in the ISAKMP gateway configuration mode, use the following command:

trust-domain *string*

- *string* – Specifies the PKI trust domain.

To cancel the specified PKI trust domain, use the command **no trust-domain**.

Tip: For more information about PKI trust domain, see "PKI" in the "User Authentication"

Configuring a Local ID

To specify the type of local identifier (FQDN and Asn1dn are supported), in the ISAKMP gateway configuration mode, use the following command:

local-id {fqdn *string* | asn1dn [*string*] | u-fqdn *string* }

- **fqdn** *string* – Specifies to use FQDN type ID. *string* is the identifier.
- **asn1dn** [*string*] – Specifies to use Asn1dn type ID, which can only be used in authentication with certificate. *string* is the identifier which can me omitted because the system can get the identifier from certificate.

- **u-fqdn** *string* – Specifies to use U-FQDN type ID (email address type, like user1@fs.com).

To cancel the local ID setting, use the command no local-id.

Specifying a Connection Type

To specify the connection type of the ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

```
connection-type {bidirectional | initiator-only | responder-only}
```

- **bidirectional** – Specifies that the ISAKMP gateway serves as both initiation and responder. This is the default value.
- **initiator-only** – Specifies that the ISAKMP gateway serves only as the initiator.
- **responder-only** – Specifies that the ISAKMP gateway serves only as the responder.

As dial-up VPN cannot be initiator, this parameter can only be set to **bidirectional** or **responder-only**.

To restore to the default value, use the command **no connection-type**.

Enabling NAT Traversal

If an NAT device exists in an IPsec or IKE VPN tunnel and it translates VPN data, NAT traversal function must be enabled. This function is disabled by default.

To enable NAT traversal, in the ISAKMP configuration mode, use the following command:

```
nat-traversal
```

To disable NAT traversal, use the command **no nat-traversal**.

Configuring DPD

DPD (Dead Peer Detection) is used to detect the status of peer device. When this function is enabled, the responder initiates a DPD request if it cannot receive packets from the peer for a long time. This function is disabled by default.

To configure DPD, in the ISAKMP gateway configuration mode, use the following command:

```
dpd [interval seconds] [retry times]
```

- **interval** *seconds* – Specifies the interval of sending DPD requests. The value range is 0 to 10 seconds. The default value is 0, meaning the DPD function is disabled.

- **retry** *times* – Specifies the times of sending DPD request to the peer. The device will keep sending discovery requests to the peer until it reaches the specified times of DPD retires. If the device does not receive response from the peer after the retry times, it will determine that the peer ISAKMP gateway is down. The value range is 1 to 10 times. The default value is 3.

Specifying Description

To add description for an ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

description *string*

- *string* – Specifies description content for the ISAKMP gateway.

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

Configuring P2 Proposal

Phase 2 proposal is used during SA Phase 2 negotiation. This section describes how to configure P2 proposal, including protocol type, encryption algorithm, hash algorithm and lifetime.

Creating P2 Proposal

To create P2 proposal (IPsec proposal), in the global configuration mode, use the following command:

ipsec proposal *p2-name*

- *p2-name* – Specifies a name for the P2 proposal. This command leads you into P2 proposal configuration mode where you make all relative configurations.

To delete the specified IPsec proposal, use the command **no ipsec proposal** *p2-name*.

Specifying a Protocol Type

P2 proposal can use AH or ESP protocol type.

To specify a P2 proposal type, in the P2 proposal configuration mode, use the following command:

protocol {**esp** | **ah**}

- **esp** – Specifies to use ESP protocol, which is the default value.
- **ah** – Specifies to use AH protocol.

To restore to the default setting, use the command **no protocol**.

Specifying an Encryption Algorithm

P2 proposal can use one to four encryption algorithms.

To specify an encryption algorithm for P2 proposal, in the P2 proposal configuration mode, use the following command:

encryption {3des | des | aes | aes-192 | aes-256 | null} [3des | des | aes | aes-192 | aes-256 | null] [3des | des | aes | aes-192 | aes-256 | null]……

- 3des - Specifies to use 3DES encryption algorithm. The key size is 192 bits and it is the default algorithm in the system.
- des - Specifies to use DES. The key size is 64 bits.
- aes - Specifies to use AES. The key size is 128 bits.
- aes-192 - Specifies to use 192bit AES. The key size is 192 bits.
- aes-256 - Specifies to use 256bit AES. The key size is 256 bits.
- null - No encryption.

To restore to the default setting, use the command no encryption.

Specifying a Hash Algorithm

P2 proposal can use one to three hash algorithms.

To specify a hash for P2, in the P2 proposal configuration type, use the following command:

hash {md5 | sha | sha256 | sha384 | sha512 | sm3 | null} [md5 | sha | sha256 | sha384 | sha512 | null] [md5 | sha | sha256 | sha384 | sha512 |null]

- md5 - Specifies to use MD5 for authentication. The hash value is 128 bits.
- sha - Specifies to use SHA-1 for authentication. The hash value is 160 bits. This is the default value.
- sha256 - Specifies to use SHA-256 for authentication. The hash value is 256 bits.
- sha384 - Specifies to use SHA-384 for authentication. The hash value is 384 bits.
- sha512 - Specifies to use SHA-512 for authentication. The hash value is 512 bits.
- null - No hash algorithm.

To restore to the default setting, use the command no hash.

Configuring PFS

PFS (Perfect Forward Secrecy) is used to ensure that the compromise of one private key in the private key set will not result in the decryption of the entire set of private keys. When PFS is enabled, a private key can be used once and the reference for generating it can only be used once. In this way, when one private key is compromised and revealed, it will not affect the whole encrypted communication.

To enable PFS, in the P2 proposal configuration mode, use the following command:

```
group {nopfs | 1 | 2 | 5 | 14 | 15 |16}
```

- **nopfs** - Disables PFS. This is the default setting.
- **1** - Uses Group1 as the DH group. The key length is 768-bit.
- **2** - Uses Group2 as the DH group. The key length is 1024-bit.
- **5** - Uses Group5 as the DH group. The key length is 1536-bit.
- **14** - Selects DH Group14. The key length is 2048 bits.
- **15** - Selects DH Group15. The key length is 3072 bits.
- **16** - Selects DH Group16. The key length is 4096 bits.

To restore to the default setting, use the command **no group**.

Specifying a Lifetime/Lifesize

Lifetime of P2 proposal can be measured by time or by traffic volume. When SA reaches the specified traffic flow amount or runs out of time, this SA expires and new negotiation should be initiated.

To specify a lifetime of P2 proposal, in the P2 proposal configuration mode, use the following commands:

lifetime *seconds*

- *seconds* – Specifies to use time period to measure lifetime. The default value is 28800 seconds.

lifesize *kilobytes*

- *kilobytes* – Specifies to use traffic volume to measure lifetime. The default value is 0 byte, which means no limit on lifesize.

To restore to the default settings, use the following commands:

```
no lifetime
```

no lifesize

Configuring a Tunnel

This section describes how to configure an IPsec tunnel, including specifying a protocol type, ISAKMP gateway, IKE proposal, ID, fragmentation and anti-replay.

Creating an IKE Tunnel

To create an IKE tunnel, in the global configuration mode, use the following command:

tunnel ipsec *tunnel-name* **auto**

- *tunnel-name* - Type a name for the new IKE tunnel.

This command leads you into the IKE tunnel configuration mode where you configure all IKE tunnel related configurations.

To delete the specified IKE tunnel, in the global configuration mode, use the command **no tunnel ipsec** *tunnel-name* **auto**.

Specifying an IPsec Mode

To specify the operation mode (tunnel mode) for the IKE tunnel, in the IKE tunnel configuration mode, use the following command:

mode tunnel

To restore to the default mode, use the command **no mode**.

Specifying an ISAKMP Gateway

To specify an ISAKMP gateway, in the IKE tunnel configuration mode, use the following command:

isakmp-peer *peer-name*

- *peer-name* – Specifies the name of ISAKMP gateway.

To cancel the specified ISAKMP gateway, use the command **no isakmp-peer**.

Specifying P2 Proposal

To specify P2 proposal for the IKE tunnel, in the IKE tunnel configuration mode, use the following command:

ipsec-proposal *p2-name*

- *p2-name* – Specifies a name for the P2 proposal.

To cancel the specified P2 proposal, use the command **no ipsec-proposal**.

Specify a Phase 2 ID

To specify a Phase 2 ID of the IKE IPsec tunnel, in the IKE tunnel configuration mode, use the following command:

id {**auto** | **local** *ip-address/mask* **remote** *ip-address/mask* **service** *service-name*}

- **auto** – Specifies the ID of Phase 2.
- **local** *ip-address/mask* – Specifies the local ID of Phase 2 automatically.
- **remote** *ip-address/mask* – Specifies the Phase 2 ID of the peer device. As the dial-up VPN initiator has no stable ID, the Phase 2 ID should be 0.0.0.0/0.
- **service** *service-name* – Specifies the service name.

You can configure up to 64 phase 2 IDs and use them to establish multiple IKE tunnels. If the center device has been configured with multiple phase 2 IDs, it can negotiate with a remote client to create multiple IPSec SAs. After auto routing is enabled, a route entry whose destination IP address is the local ID of the peer and next hop is the egress IP address of the remote client as a gateway would be added to the routing table automatically once an IPSec SA had been created. When an IPSec SA is deleted, the corresponding route entry will be deleted from the routing table.

To restore the default configurations, use the command **no id** {**auto** | **local** *ip-address/mask* **remote** *ip-address/mask* **service** *service-name*}.

Creating an IPSec SA When There is Inclusion Relation for ID

When the remote ID of phase 2 ID configured in the center device contains the local ID of phase 2 ID configured in the remote client, an IPSec SA can still be successfully created between the center device and the remote client after this feature is configured. To enable this feature, in the IKE tunnel configuration mode, use the following command:

dialup-control-id

To restore to the default setting, use the command **no dialup-control-id**.

Configuring IPSec Balancing and Filtering

A central device can negotiate with a remote client to create multiple IPSec SAs. At the same time, encapsulated packets will be filtered when out-acrossing the IKE tunnel interface and be balanced when in-acrossing the IKE tunnel interface. If a packet's source IP address, destination IP address, and service type match a phase 2 ID, the packet will be processed by the central device; otherwise, the packet will be discarded.

To configure IPSec balancing and filtering, in the IKE tunnel configuration mode, use the following command:

check-id

To restore to the default setting, use the command **no check-id**.

Enabling Auto Connection

The device has two methods of establishing SA: auto and traffic intrigued.

- When it is auto, the device checks SA status every 60 seconds and initiates negotiation request when SA is not established
- When it is traffic intrigued, the tunnel sends negotiation requests only when there is traffic passing through the tunnel.

By default, traffic intrigued mode is used.

To enable auto connection, in the IKE tunnel configuration mode, use the following command:

auto-connect

To restore to the default setting, use the command **no auto-connect**.

Note:Auto connection works only when the peer IP is static and the local device is initiator.

Configuring Packet Fragmentation

To allow IP packet fragmentation on the forwarding device, in the IKE configuration mode, use the following command:

df-bit {**copy** | **clear** | **set**}

- **copy** – Copies the IP packet DF options from the sender directly. This is the default value.
- **clear** – Allows packet fragmentation.
- **set** – Disallows packet fragmentation.

To restore to the default value, use the command **no df-bit**.

Configuring Anti-replay

Anti-replay is used to prevent hackers from attacking the device by resending the sniffed packets, i.e., the receiver rejects the obsolete or repeated packets. By default, this function is disabled.

To configure anti-replay for IKE IPsec tunnel, in the IKE IPsec tunnel configuration mode, use the following command:

anti-replay {**32** | **64** | **128** | **256** | **512**}

- **32** - Specifies the anti-replay window as 32.
- **64** - Specifies the anti-replay window as 64.
- **128** - Specifies the anti-replay window as 128.
- **256** - Specifies the anti-replay window as 256.
- **512** - Specifies the anti-replay window as 512.

When the network condition is poor, choose a larger window.

To disable anti-replay, use the command **no anti-replay**.

Configuring Commit Bit

The commit bit function is used to avoid packet loss and time difference in the tunnel. Configuring this function on this end makes the corresponding peer to use it. However, commit bit may slow the responding speed.

To configure commit bit, in the IKE IPsec tunnel configuration mode, use the command: **responder-set-commit**

To disallow the responder to set commit bit, use the command: **no responder-set-commit**

Configuring Idle Time

Idle time length is the longest time the tunnel can exist without traffic passing through. When the time is over, SA will be cleared.

To configure the idle time, in the IKE IPsec tunnel configuration mode, use the following command:

idle-time *time-value*

- *time-value* − Specifies a time value. The value range is 120 to 3000 seconds.

To disable idle time, in the IKE IPsec tunnel configuration mode, use the following command:

no idle-time

Specifying Description

To give some description of an IKE tunnel, in the IKE tunnel configuration mode, use the following command:

description *string*

- *string* – Type the description you want.

To delete IKE tunnel description, use the command **no description**.

Configuring Auto Routing

For route-based dial-up VPN or PnPVPN, the IP addresses of the branches are always changing, causing operational inconvenience for the administrator if manual routing is used. The auto routing function allows the device to automatically add routing entries from center to branch to avoid complexity of manual routing.

By default the auto routing is disabled. To enable it, in the ISAKMP gateway configuration mode, use the following command:

generate-route

For dial-up VPN, the Phase 2 local ID of auto generated route is its destination address and its next hop is the peer IP address. For information about how to configure a Phase 2 ID, see Specify a Phase 2 ID.

For PnPVPN, the destination address of auto generated route is the AND operation result of the start IP and netmask of client DHCP address pool (dhcp-pool-addr-start & dhcp-pool-netmask), and the next hop address is the peer IP address. For information about client DHCP address pool and netmask, see Configuring a PnPVPN Server Using CLI.

To disable auto routing, use the command **no generate-route**.

Note:

- If the Phase 2 local ID of initiator in a dial-up VPN is 0.0.0.0/0, you are strongly suggested not to enable auto routing on the center device.
- When the branch office accesses the center, you can use the command **`no reverse-route`** to disable reverse routing and return all the reverse data from the original paths on the center device. The command line will show the number of imported users.

Configuring a Dial-up User

This section describes how to create a dial-up user, including user account and pre-shared key.

Creating a Dial-up User Account

To create a dial-up user account, in the global configuration mode, use the following command:

user *user-name* **aaa-server local**

- *user-name* – Type the user name.

This command leads you into the user configuration mode, where you can specify the user IKE ID with the following command:

```
ike-id {fqdn string | asn1dn string}
```

- **fqdn** *string* – Specifies to use IKE ID of FQDN type. *string* is the ID content.
- **asn1dn** *string* – Specifies to use ID of Asn1dn type, which only applies to authentication with certificate.

To cancel the IKE ID setting, in the user configuration mode, use the following command:

```
no ike-id
```

Generating a Pre-shared Key for Dial-up User

The center device generates a pre-shared key using dial-up user’ s username and IKE ID.

To generate a pre-shared key, in any mode, use the following command:

```
exec generate-user-key rootkey pre-share-key userid string
```

- *pre-share-key* – Specifies the pre-shared key of the device.
- *string* – Specifies the IKE ID of username.

Configuring the Dial-up Client

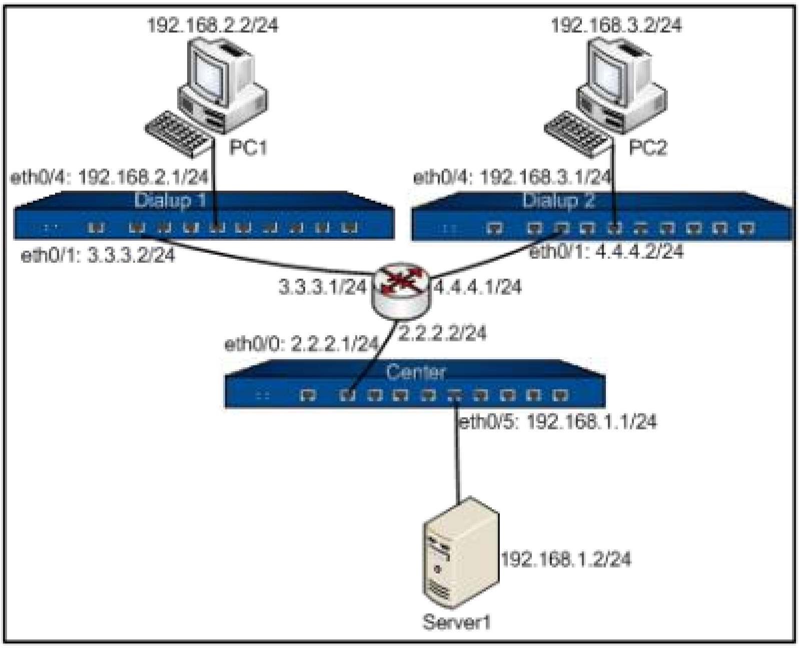
The remote client should configure parameters corresponding to the center device, including P1 proposal, P2 proposal, ISAKMP gateway and tunnel. The configuration commands are similar to those of center device, but if the local ID of initiator’ s ISAKMP gateway uses pre-shared key, the key must be the corresponding pre-shared key of the center device.

Example of Configuring Dial-up VPN

This section provides a configuration example of dial-up VPN.

Requirement

Two dial-up clients (user1 and user 2) and the center device (2.2.2.1/24) consist of a dial-up VPN. The goal is to allow two computers (PC1 and PC2) accessing the center device protected server (Server1) using secured VPN tunnel.



Configuring the Center Device

Step 1: Configure interfaces

```
hostname(config)# zone vpnzone
hostname(config-zone-vpnzone)# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone vpnzone
hostname(config-if-eth0/0)# ip address 2.2.2.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/5
hostname(config-if-eth0/5)# zone trust
hostname(config-if-eth0/5)# ip address 192.168.1.1/24
hostname(config-if-eth0/5)# exit
```

Step 2: Configure a dial-up user account and pre-shared key

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user user1
hostname(config-user)# ike_id fqdn fstest1
hostname(config-user)# exit
hostname(config-aaa-server)# user user2
hostname(config-user)# ike_id fqdn fstest2
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)# exit
hostname# exec generate-user-key rootkey 123456 userid fstest1
userkey: 3zPNDY6MmI8Wejk5fa3jhPU39p8=
hostname# exec generate-user-key rootkey 123456 userid fstest2
userkey: tAFW+48HcAr15+NcISm6TZJZzGU=
hostname# configure
hostname(config)#
```

Step 3: Configure IKE VPN

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# exit
hostname(config)# isakmp peer test
hostname(config-isakmp-peer)# aaa-server local
hostname(config-isakmp-peer)# interface ethernet0/0
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# mode aggressive
hostname(config-isakmp-peer)# pre-share 123456
hostname(config-isakmp-peer)# type usergroup
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer test
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# id local 192.168.1.2/24 remote 0.0.0.0/0 service any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

Step 4: Configure policy rules

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone vpnzone
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone vpnzone
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Configuring Dial-up Client 1

Step 1: Configure interfaces

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 3.3.3.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/5)# zone trust
hostname(config-if-eth0/5)# ip address 192.168.2.1/24
hostname(config-if-eth0/5)# exit
hostname(config)#
```

Step 2: Configure IKE VPN

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# exit
hostname(config)# isakmp peer test
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# mode aggressive
hostname(config-isakmp-peer)# peer 2.2.2.1
hostname(config-isakmp-peer)# pre-share 3zPNDY6MmI8Wejk5fa3jhPU39p8=
hostname(config-isakmp-peer)# local-id fqdn fstest1
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer test
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# id local 192.168.2.2/24 remote 192.168.1.2/24 service any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

Step 3: Configure policy rules

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Configuring Dial-up Client 2

Step1: Configure interface

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 4.4.4.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/5)# zone trust
hostname(config-if-eth0/5)# ip address 192.168.3.1/24
hostname(config-if-eth0/5)# exit
hostname(config)#
```

Step2: Configure IKE VPN

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)#
hostname(config)# isakmp peer test
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# mode aggressive
hostname(config-isakmp-peer)# peer 2.2.2.1
hostname(config-isakmp-peer)# pre-share tAFW+48HcAr15+NcISm6TZJZzGU=
hostname(config-isakmp-peer)#
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer test
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# id local 192.168.3.2/24 remote 192.168.1.2/24 service any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

Step 3: Configure policy rules

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zonetrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

PnPVPN

Overview

IPsec VPN requires sophisticated operation skills and high maintenance cost. To relieve network administrators from the heavy work, FS provides an easy-to-use VPN technology - PnPVPN (Plug-and-Play VPN). PnPVPN consists of two parts: PnPVPN Server and PnPVPN Client.

- PnPVPN Server: Normally deployed in the headquarters and maintained by an IT engineer. The PnPVPN Server issues most of the configuration commands to clients. The FS device usually works as a PnPVPN Server and one FS device can serve as multiple servers.
- PnPVPN Client: Normally deployed in the branch offices and controlled remotely by headquarters engineer. With simple configuration, such as client ID, password and server IP settings, the PnPVPN Client can receive configuration commands (e.g. DNS, WINS, DHCP address pool, etc.) from the PnPVPN Server.

Note:The FS device can serve as both a PnPVPN Server and a PnPVPN Client. When working as a PnPVPN Server, the maximum number of VPN instances and the supported client number of each device may vary from hardware platforms.

PnPVPN Workflow

The workflow for PnPVPN is as follows:

1. The client initiates a connection request and sends its own ID and password to the server.
2. The server validates the ID and password when it receives the client request. If the client passes the authentication, the server issues configuration information including DHCP address pool, DHCP mask, DHCP gateway, WINS, DNS and tunnel routes, etc. to the client.
3. The client distributes the received information to corresponding functional modules.
4. The client PC automatically gains an IP address, IP mask, gateway address and other network parameters and connects itself to the VPN.

PnPVPN Link Redundancy

The PnPVPN server supports dual VPN link dials for a PnPVPN client, and automatically generates the routing to the client. Also, it can configure the VPN monitor for the client. Two ISAKMP gateways and two tunnel interfaces need to be configured in the server. The two VPN tunnels need to refer different ISAKMP gateways and be bound to different tunnel interfaces.

The client supports to configure dual VPN dials and redundant routing. When the two VPN tunnels are negotiating with the server, the client generates routes with different priority according to the tunnel routing configuration at the server side. The high priority tunnel acts as the master link and the tunnel with low priority as the backup link, so as to realize redundant routing. The master VPN tunnel will be in the active state first. When master tunnel is interrupted, the client will use the backup tunnel to transfer the data. When the master tunnel restores to be normal, it will transfer the data again.

Configuring a PnPVPN Server

This section describes the configurations on the server, both in the command line interface and on the WebUI.

Configuring a PnPVPN Server Using CLI

Some of IPsec VPN commands also apply to PnPVPN configuration; in addition, PnPVPN has its unique configuration commands. The commands below in this chapter cannot complete PnPVPN command set alone; for complete PnPVPN settings, see Example of Configuring PnPVPN.

Configuring User’s Network

After the client successfully negotiates with the server, the server will distribute some network setting parameters, including DNS server address, WINS server address, tunnel route, DHCP address pool address/netmask and gateway address, to the client. These parameters are configured in the corresponding user configuration modes, but some of them (settings of DNS, WINS and tunnel route) can also be set in IKE tunnel configuration. When there is a conflict between the two settings, configuration in the user configuration mode has higher priority over settings in the IKE tunnel configuration mode.

To enter the local user configuration mode, use the following command:

aaa-server *aaa-server-name* **type local** (this command leads you to the local AAA server configuration mode)

user *user-name*

- user-name – Specifies the user name.

The commands below complete a user' s network settings. Among these parameters, settings of DHCP address pool, DHCP netmask and gateway are required while others are optional.

dns *A.B.C.D* [*A.B.C.D*] [*A.B.C.D*] [*A.B.C.D*]

- *A.B.C.D* – Specifies the IP address of DNS server. You can define one primary DNS server and up to three alternative servers. To cancel the DNS server setting, use the command **no dns**.

wins *A.B.C.D* [*A.B.C.D*]

- *A.B.C.D* – Specifies the IP address of WINS server. You can define one primary DNS server and one alternative WINS server. To cancel the WINS server setting, use the command **no wins**.

split-tunnel-route *A.B.C.D/Mask*

- *A.B.C.D/Mask* – Specifies the tunnel route. A.B.C.D is the IP address prefix and Mask is the digit of subnet mask. To clear the settings, use the command **no split-tunnel-route A.B.C.D/Mask**.

dhcp-pool-address *start-ipaddr end-ipaddr*

- *start-ipaddr end-ipaddr* – Specifies the start IP address and end IP address of DHCP address pool. To cancel the setting, use the command **no dhcp-pool-address**.

dhcp-pool-netmask *A.B.C.D*

- *A.B.C.D* – Specifies the network mask of DHCP address pool. To cancel the setting, use the command **no dhcp-pool-netmask**.

dhcp-pool-gateway *A.B.C.D*

- *A.B.C.D* – Specifies the gateway address of DHCP address pool. This address is the Intranet interface' s IP address of PnPVPN client and serves as the PC gateway address. As the IP address of PC is defined by the DHCP address pool and subnet mask, the gateway address and DHCP address pool should be in the same network segment. To cancel the setting, use the command **`no dhcp-pool-gateway`**.

Configuring Tunnel Network

If all or most of the clients use unified DNS, WINS or tunnel route setting, you can configure these parameters in the IKE tunnel mode to reduce workload of making settings in the user configuration mode.

To enter the IKE tunnel configuration mode, use the following command:

tunnel ipsec *tunnel-name* **auto**

- *tunnel-name* – Specifies the name of IKE tunnel.

To configure the DNS, WINS and tunnel route, use the following commands:

dns *A.B.C.D* [*A.B.C.D*] [*A.B.C.D*] [*A.B.C.D*]

- *A.B.C.D* – Specifies the IP address of DNS server. You can define one primary server and up to three alternative servers. To cancel the setting, use the command **no dns**.

wins *A.B.C.D* [*A.B.C.D*]

- *A.B.C.D* – Specifies the IP address of WINS server. You can define one primary WINS server and one alternative server. To cancel the setting, use the command **no wins**.

split-tunnel-route *A.B.C.D/Mask*

- *A.B.C.D/Mask* – Specifies the tunnel route. A.B.C.D is the IP address prefix and Mask is the digit of subnet mask. To clear the settings, use the command **`no split-tunnel-route`**.

Configuring Wildcard of ISAKMP Gateway's Peer

When PnPVPN Server uses Radius server to authenticate, you are required to configure the wildcard of ISAKMP gateway's peer. The wildcard is used to match username and determine the PnPVPN Server of the accessed client (a FS device can serve as multiple PnPVPN servers), so that the Radius server for user's authentication can be identified.

To configure the wildcard of ISAKMP gateway's peer, in the ISAKMP gateway configuration mode, use the following command:

peer-id fqdn wildcard *string*

- **fqdn** – Uses wildcard of FQDN type.
- **wildcard** *string* – Specifies the wildcard ID which is usually the client's domain name, like abc.com.

To cancel wildcard settings, use command **no peer-id**.

Configuring Tunnel Interface of PnPVPN Client

To allow the sub-networks in the branch office accessing the server, you can configure IP address and enable SNAT rule for the client tunnel interface on the PnPVPN server end. If SR Series platform is used as the PnPVPN client, make sure that the version in the platform supports this function.

Note: When this function is working, the PnPVPN server cannot access its clients.

To enter local user configuration mode, use the following command:

aaa-server *aaa-server-name* **type local** (This command leads you to the local AAA server configuration mode.)

user *user-name*

- *user-name* – Specifies the user name.

To configure tunnel interface of PnPVPN client, in the local user configuration mode, use the following command:

tunnel-ip-address *A.B.C.D* [**snat**]

- *A.B.C.D* – Specifies the IP address of client tunnel interface, but it should not conflict with the existing IP addresses in the client.
- **snat** – Enables SNAT rule. In default, the SNAT rule on tunnel interface is disabled.

To cancel tunnel interface of PnPVPN client, in the local user configuration mode, use the following command:

no tunnel-ip-address

Configuring a PnPVPN Sever Using WebUI

This section describes how to configure PnPVPN server in the WebUI, including:

- Configuring a User
- Configuring IKE VPN
- Configuring an Tunnel Interface
- Configuring a Route
- Configuring a Policy

Note: PnPVPN support two types of authentication server: Local and Radius.

Configuring a User

To configure a user, take the following steps:

1. Select **Objects > Local User** from the menu bar.
2. In the Local User dialog, select a local server from the **Local server** drop-down list. Click **New**, and select **User** from the drop-down list.
3. On the **Basic** tab in the User Configuration dialog, type a name for the user into the **Name** box.
4. Specify a password for the user in the **Password** box and confirm it in the **Confirm password** box.
5. Click **FQDN** in the IKE ID section, and type the ID's content into the text box below. The ID is used in authentication.
6. Click the **PnPVPN** tab and fill out options in the tab. If the user does not use configured DNS, WINS or tunnel route of the tunnel, these options must be configured.
7. Configure other options as needed.
8. Click **OK** to save the settings.

Configuring IKE VPN

This section introduces how to configure IKE VPN, including how to configure P1 proposal, P2 proposal, VPN peer and tunnel.

To configure P1 proposal, take the following steps:

1. On the Navigation pane, click **Configure > Network > IPsec VPN** to visit the IPsec VPN page and click the **Phase1 Proposal** tab.

2. Click **New**. In the Phase1 Proposal Configuration dialog, finish the options as described below:
    - **Proposal name**: Type the name of the Phase1 proposal.
    - **Authentication**: Select **pre-share**.
    - **HASH**: Select **Group2**.
3. You can fill out other options or leave them blank as needed.
4. Click **OK** to save the settings.

To configure P2 proposal, use the following steps:

1. On the Navigation pane, click **Configure > Network > IPsec VPN** to visit the IPsec VPN page and click the **Phase2 Proposal** tab.
2. Click **New**.
3. In the Phase2 Proposal Configuration dialog, type the name of P2 proposal into the **Proposal name** box.
4. Select a protocol, HASH algorithm, encryption algorithm and PFS group as needed.
5. You can fill out other options or use the default value as needed.
6. Click **OK** to save the settings.

To configure the peer, take the following steps:

1. On the Navigation pane, click **Configure > Network > IPsec VPN** to visit the IPsec VPN page. Click the **VPN Peer List** tab.
2. In the Peer Configuration dialog, click **New**.
3. On the **Basic** tab, configure the options below:
    - **Peer name**: Type the name of the ISAKMP gateway.
    - **Interface**: Select an interface bound to the ISAKMP gateway.
    - **Mode**: Select **Aggressive**.
    - **Type**: Select **user group**, and select the AAA server you need from the **AAA server** drop-down list.
    - **Proposal 1**: Select a P1 proposal you want from the list.

- **Pre-shared key**: Type the pre-shared key into the box.

4. Configure other options as needed or use the default values.

5. Click **Generate**. In the Generate user key dialog, type the IKE ID into the **IKE ID** box, and then click **Generate**. The generated user key will be displayed in the Generate result box. PnPVPN client uses this key as the password to authenticate the login users. Then, close the dialog.

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

Note: If Radius server works as the authentication server, wildcard must be configured.

To configure a tunnel, take the following steps:

1. On the Navigation pane, click **Configure > Network > IPsec VPN** to visit the IPsec VPN page.

2. On the upper-left of the IKE VPN List, Click **New**.

3. Under **Step 1: Peer**, click **Import** in the Peer name section, and select a peer you want from the drop down list; type the IP address of the peer into the **Peer address** box. Or, you can create a new peer (ISAKMP gateway) on this tab.

4. Click **Step 2: Tunnel** and configure the options:

   - **Name**: Type a name for the tunnel.

   - **Mode**: Select **tunnel**.

   - **P2 proposal**: Select a proposal you need from the drop down list.

5. Click the **Advanced** tab. In this tab, configure DNS, WINS and tunnel route (tunnel users will use the DNS and WINS defined here).

6. Configure other options as needed or use the default values.

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

Note: If Radius server works as the authentication server, wildcard must be configured.

Configuring a Tunnel Interface

To configure tunnel interface, take the following steps:

1. On the Navigation pane, click **Configure > Network > Network** to visit the Network page.

2. Click **New** on the upper-left of the interface list, and select **Tunnel Interface** from the drop-down list. Configure the following options:

   - **Name**: Type the number of the tunnel.
   - **Binding zone**: Select **Layer 3 zone**.
   - **Zone**: Select a zone for the interface from the drop-down list.

3. Under **Tunnel binding**, select **IPsec VPN** and select VPN tunnel from the **VPN name** drop down list. Gateway address is not needed here.

4. Click **OK** to save settings.

Configuring a Route

To allow hosts in the server network to access the client network, you need to add static routes.

To add a route, take the following steps:

1. On the Navigation pane, click **Configure > Network > Routing** to visit the Routing page.

2. On the **Destination Route** tab, click **New**.

3. In the Destination Route Configuration dialog, type the IP address for the route into the **Destination** box.

4. Type the corresponding subnet mask into the **Subnet mask** box.

5. To specify the type of next hop, click **Interface**, and select the **VPN tunnel interface** from the **Interface** drop-down list below, then type the gateway address for the tunnel's peer into the optional box below.

6. Configure other options as needed or use the default values.

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

Configuring a Policy

Policies are configured according to the network deployment (on the Navigation pane, click **Configure** > **Security** > **Policy** to visit the Policy page).

Configuring a PnPVPN Client

This section describes how to configure a PnPVPN Client. To configure a PnPVPN, take the following steps:

1. On the Navigation pane, click Configure > Network > IPsec VPN to visit the IPsec VPN page.

2. On the Task tab in the right auxiliary pane, click PnPVPN Client.

3. In the PnPVPN Configuration dialog, finish the options.

   - **Server address 1**: Type the IP address of PnPVPN Server into the box. This option is required.
   - **Server address 2**: Type the IP address of PnPVPN Server into the box. The server address 1 and the server address 2 can be the same or different. It is optional.
   - **ID**: Specifies the IKE ID assigned to the client by the server.
   - **Password**: Specifies the password assigned to the client by the server.
   - **Confirm password**: Enter the password again to make confirmation.
   - **Auto save**: Select **Enable** to auto save the DHCP and WINS information released by PnPVPN Server.
   - **Outgoing IF 1**: Specifies the interface connecting to the Internet. This option is required.
   - **Outgoing IF 2**: Specifies the interface connecting to the Internet. The IF1 and the IF2 can be the same or different. It is optional.
   - **Incoming IF**: Specifies the interface on PnPVPN Server accessed by Intranet PC or application servers. Click the interface you want. If **Incoming IF** is selected, also select an interface from the **Interface** drop-down list; if multiple Intranet interfaces connect to PnPVPN, you should click **BGroup IF**, and add interface members of that bgroup. To add interface members, select the interface(s) you want from the **Available** list, and add it to the **Selected** list. To delete an interface member, select it and remove it from the **Selected** list .

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

Example of Configuring PnPVPN

This section describes an example of PnPVPN configuration.

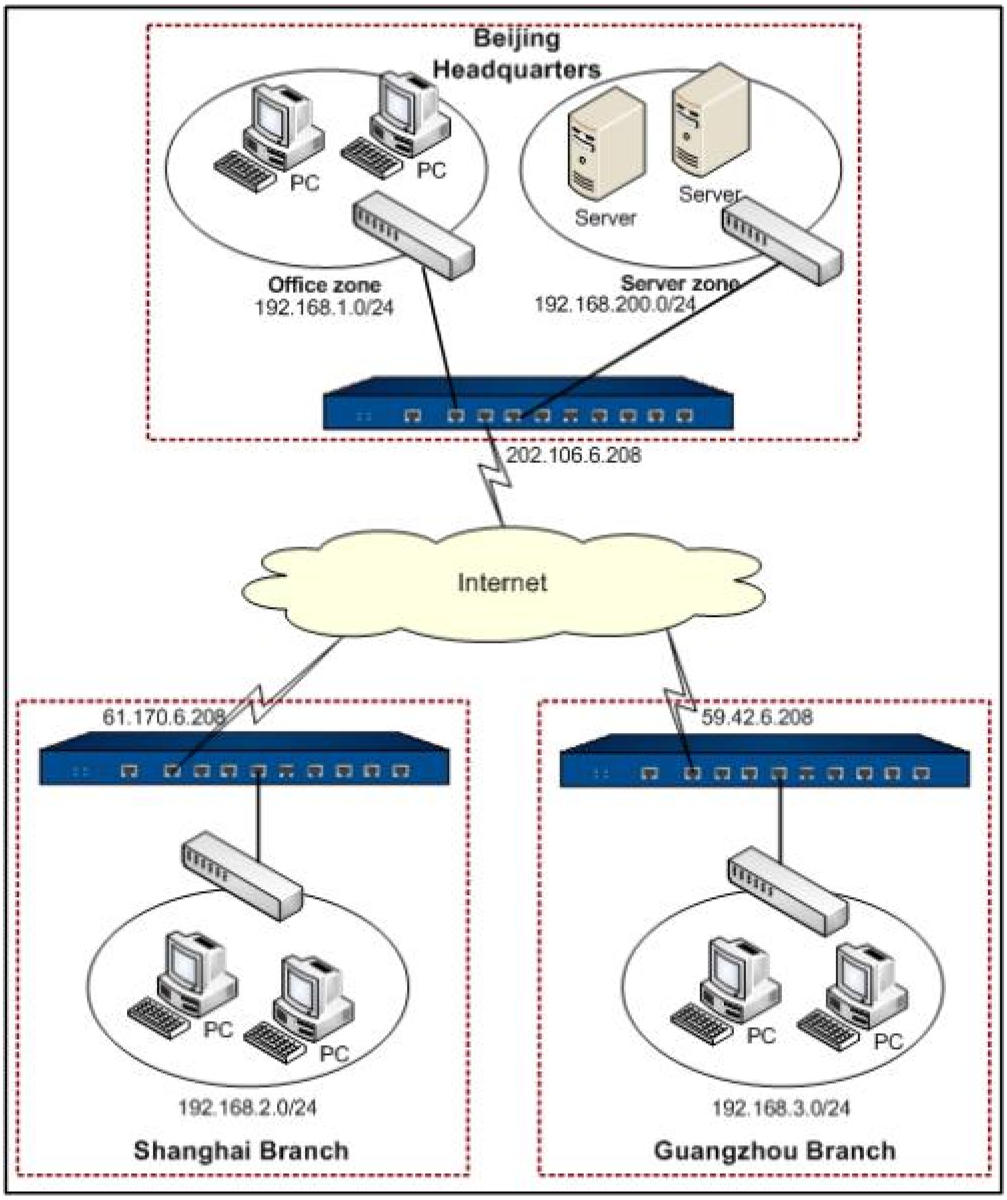
Requirement

A company has its headquarters in Beijing and two branch offices in Shanghai and Guangzhou, all three of which have Internet access. Its business demands that a VPN network should be established. The goals of the network are:

- Employees in Guangzhou Branch and Shanghai Branch can access the headquarters database via VPN;
- All the employees (including the Beijing headquarters and two branches) can share resources via VPN.

PnPVPN is a practical and easy-to-use method to meet the requirements above. Take the following steps:

- The headquarters uses a next-genration firewall as the PnPVPN Server and chooses the local authentication.
- Each of the two branches has a next-generation firewall, working as the PnPVPN Client and accessing the headquarters VPN network.
- To share resource among all employees in the three places, you should configure policies and routes.



According to the topology, the network environment can be described as follows:

- The headquarters LAN network segment is 192.168.1.0/24 and it uses ethernet0/0 of trust zone to access the network.
- The headquarters server group network segment is 192.168.200.0/24 and it uses ethernet0/2 of trust zone to access the network.
- The headquarter security device use ethernet 0/1 (IP: 202.106.6.208) of untrust zone to access the network.
- Shanghai Branch uses an interface with IP 61.170.6.208 to access the Internet, and Guangzhou Branch uses an interface with IP 59.42.6.208 to access the Internet.
- PnPVPN Server will allocate the network segment 192.168.2.0/2 to Shanghai Branch and 192.168.3.0/24 to Guangzhou Branch.

Configuration Steps

Take the steps below to configure the server end and client ends:

Configuring the Server

Step 1: Configure the local AAA server

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

Step 2: Configure the network in Shanghai Branch

```
hostname(config)# aaa-server test type local
hostname(config-aaa-server)# user shanghai
hostname(config-user)# password shanghaiuser
hostname(config-user)# ike-id fqdn shanghai
hostname(config-user)# dhcp-pool-address 192.168.2.1 192.168.2.100
hostname(config-user)# dhcp-pool-netmask 255.255.255.0
hostname(config-user)# dhcp-pool-gateway 192.168.2.101
hostname(config-user)# split-tunnel-route 192.168.200.0/24
hostname(config-user)# split-tunnel-route 192.168.1.0/24
hostname(config-user)# split-tunnel-route 192.168.3.0/24
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 3: Configure the network in Guangzhou Branch

```
hostname(config)# aaa-server test type local
hostname(config-aaa-server)# user guangzhou
hostname(config-user)# password guangzhouuser
hostname(config-user)# ike-id fqdn guangzhou
hostname(config-user)# dhcp-pool-address 192.168.3.1 192.168.3.100

hostname(config-user)# dhcp-pool-netmask 255.255.255.0

hostname(config-user)# dhcp-pool-gateway 192.168.3.101

hostname(config-user)# split-tunnel-route 192.168.200.0/24

hostname(config-user)# split-tunnel-route 192.168.1.0/24

hostname(config-user)# split-tunnel-route 192.168.2.0/24

hostname(config-user)# exit

hostname(config-aaa-server)# exit

hostname(config)#
```

Step 4: Configure a PnPVPN Server

```
hostname(config)# isakmp proposal test1

hostname(config-isakmp-proposal)# group 2

hostname(config-isakmp-proposal)# exit

hostname(config)# ipsec proposal test2

hostname(config-ipsec-proposal)# exit

hostname(config)# isakmp peer test1

hostname(config-isakmp-peer)# type usergroup

hostname(config-isakmp-peer)# mode aggressive

hostname(config-isakmp-peer)# interface ethernet0/1

hostname(config-isakmp-peer)# aaa-server test

hostname(config-isakmp-peer)# isakmp-proposal test1

hostname(config-isakmp-peer)# pre-share 123456

hostname(config-isakmp-peer)# exit

hostname(config)# tunnel ipsec test auto

hostname(config-tunnel-ipsec-auto)# ipsec-proposal test2

hostname(config-tunnel-ipsec-auto)# isakmp-peer test1

hostname(config-tunnel-ipsec-auto)# mode tunnel

hostname(config-tunnel-ipsec-auto)# id auto
hostname(config-tunnel-ipsec-auto)# dns 192.168.200.1 192.168.200.11

hostname(config-tunnel-ipsec-auto)# wins 192.168.200.2 192.168.200.12

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

hostname(config)#
```

Step 5: Generate client private keys

```
hostname(config)# exec generate-user-key rootkey 123456 userid shanghai

userkey: kyZAKmLWCc5Nz75fseDiM2r+4Vg=

hostname(config)# exec generate-user-key rootkey 123456 userid guangzhou

userkey: SdqhY4+dPThTtpipW2hs2OMB5Ps=
```

Step 6: Configure policies

```
hostname(config)# zone VPN

hostname(config-zone-VPN)# exit

hostname(config)# interface tunnel1

hostname(config-if-tun1)# zone VPN

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

hostname(config-if-tun1)# exit

hostname(config)# policy-global

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone VPN

hostname(config-policy-rule)# dst-zone trust

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone VPN
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone VPN
hostname(config-policy-rule)# dst-zone VPN
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 7: Configuring routes

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 192.168.2.0/24 tunnel1 61.170.6.208
hostname(config-vrouter)# ip route 192.168.3.0/24 tunnel1 59.42.6.208
hostname(config)#
```

Configuring the Clients

In the Shanghai Branch:

1. On the Navigation pane, click **Configure > Network > IPsec VPN** to visit the IPsec VPN page.
2. On the **Task** tab in the right auxiliary pane, click **PnPVPN Client**. In the PnPVPN Configuration dialog, configure the options as below:

- **Server address**: 202.106.6.208
- **ID**: shanghai
- **Password**: kyZAKmLWCc5Nz75fseDiM2r+4Vg=
- **Confirm password**: kyZAKmLWCc5Nz75fseDiM2r+4Vg=
- **Auto save**: Select the **Enable** checkbox
- **Outgoing IF**: ethernet0/0
- **Incoming IF**: ethernet0/3

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

In the Guangzhou Branch:

1. On the Navigation pane, click **Configure > Network > IPsec VPN** to visit the IPsec VPN page.
2. On the **Task** tab in the right auxiliary pane, click **PnPVPN Client**. In the PnPVPN Configuration dialog, configure the options as below:
   - **Server address**: 202.106.6.208
   - **ID**: guangzhou
   - **Password**: SdqhY4+dPThTtpipW2hs2OMB5Ps=
   - **Confirm password**: SdqhY4+dPThTtpipW2hs2OMB5Ps=
   - **Auto save**: Select the **Enable** checkbox
   - **Outgoing IF**: ethernet0/0
   - **Incoming IF**: ethernet0/3
3. Click **OK** to save your settings.

GRE

Overview

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork. FSOS uses GRE over IPSEC feature to ensure the security of routing information passing between networks.

Configuring GRE

This section introduces how to configure GRE, including:

- Configuring a GRE tunnel
- Binding the GRE tunnel to a tunnel interface

Configuring a GRE Tunnel

Configurations for GRE tunnel should be performed in the GRE tunnel configuration mode.

To enter the GRE tunnel configuration mode, in the global configuration mode, use the following command:

tunnel gre *gre-tunnel-name*

- *gre-tunnel-name* – Specifies the name of the new GRE tunnel. This command creates a new GRE tunnel; if the tunnel with this name exists, you will enter its configuration mode directly.

To delete the specified GRE tunnel, use the following command:

no tunnel gre *gre-tunnel-name*

In the GRE tunnel configuration mode, you need to configure the following parameters for the tunnel:

- Source interface/address
- Destination address
- Egress interface
- IPsec VPN tunnel (optional)
- Verification key

Specifying a Source Interface/Address

To define a source interface for the GRE tunnel, in the GRE tunnel configuration mode, use the following command:

source {**interface** *interface-name* [**ipv6**] | {*ipv4-address* | *ipv6-address*}

- **interface** *interface-name* [**ipv6**] – Specifies the name of interface as the source interface of the GRE tunnel.
- *ipv4-address* | *ipv6-address* – Specifies the IP address (IPv4 and IPv6).

To cancel source address setting, in the GRE tunnel configuration mode, use the following command:

no source

Specifying a Destination Address

To specify a destination address for the GRE tunnel, in the GRE tunnel configuration mode, use the following command:

destination {*ipv4-address* | *ipv6-address*}

- {*ipv4-address* | *ipv6-address*} – Specifies the destination address for the GRE tunnel (IPv4 and IPv6).

To cancel the specified destination address, in the GRE tunnel configuration mode, use the following command:

no destination

Specifying an Egress Interface

To specify the egress interface for the GRE tunnel, in the GER tunnel configuration mode, use the following command:

interface *interface-name*

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

To cancel the egress interface setting, in the GRE tunnel configuration mode, use the following command:

no interface

Specifying an IPsec VPN Tunnel

When using GRE over IPsec function, you need to specify an IPsec VPN tunnel to encapsulate the tunnel data.

To specify an IPsec VPN tunnel, in the GRE tunnel configuration mode, use the following command:

next-tunnel ipsec *tunnel-name*

- *tunnel-name* – Specifies the name of IPsec VPN tunnel.

To cancel the specified IPsec VPN tunnel, in the GRE tunnel configuration mode, use the following command:

no next-tunnel

Specifying a Verification Key

By specifying a verification key, the system encapsulates and verifies the packets. When the key carried by the packets is the same as the key configured in the receiver, the packets will be decrypted. If the keys are not the same, the packets will be dropped. To specify the verification key, in the GRE tunnel configuration mode, use the following command:

key *key-value*

- *key-value* – Specifies the verification key. The value ranges from 0 to 4294967295.

To cancel the configurations, use the following command in the GRE tunnel configuration mode:

no key

Binding the GRE Tunnel to a Tunnel Interface

A well configured GRE tunnel needs to be bound to the tunnel interface so that it can work.

To bind the GRE tunnel to a tunnel interface, in the tunnel interface configuration mode, use the following command:

tunnel gre *gre-tunnel-name* [**gw** *ip-address*]

- *gre-tunnel-name* – Specifies the name of the well configured GRE tunnel which binds to the interface.
- **gw** *ip-address* – This parameter is required when multiple tunnels bind to this interface. It defines the next hop (the peer tunnel interface) IP address of GRE tunnel. The default value is 0.0.0.0.

To cancel the binding of GRE tunnel to the tunnel interface, in the tunnel interface configuration mode, use the following command:

no tunnel gre *gre-tunnel-name*

Viewing GRE Tunnel Information

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

show tunnel gre [*gre-tunnel-name*]

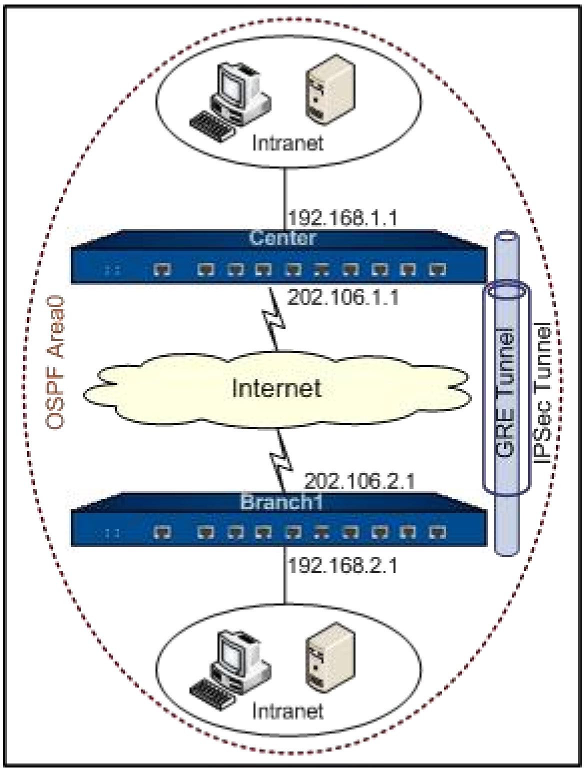
- *gre-tunnel-name* – Specifies the name of GRE tunnel you want to view.

Example of Configuring GRE Tunnel

This section provides a configuration example of GRE over IPsec with OSPF in a FS device.

Requirement

The headquarters (Center) and the branch office (Branch1) are connected by the Internet using OSPF protocol. The connection uses GRE over IPsec technique to ensure secure data transmission between the center and the branch. The figure below is the topology of the network layout.



Configuration Steps

Configurations for this requirement include settings on the headquarters device (Center) and on the branch office device (Branch1).

Configuring the Center

The following commands are the necessary settings of IPsec VPN and OSPF.

Step 1: Configure the interface

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 202.106.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#exit
```

Step 2: Configure the IPsec VPN

```
hostname(config)# isakmp proposal branch1
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal branch1
hostname(config-ipsec-proposal)# exit
hostname(config)# isakmp peer branch1
hostname(config-isakmp-peer)# interface ethernet0/0
hostname(config-isakmp-peer)# peer 202.106.2.1
hostname(config-isakmp-peer)# pre-share 111111
hostname(config-isakmp-peer)# isakmp branch1
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec branch1 auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer branch1
hostname(config-tunnel-ipsec-auto)# ipsec-proposal branch1
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

Step 3: Configure the GRE tunnel

```
hostname(config)# tunnel gre center-branch1
hostname(config-tunnel-gre)# source 202.106.1.1
hostname(config-tunnel-gre)# destination 202.106.2.1
hostname(config-tunnel-gre)# interface ethernet0/0
hostname(config-tunnel-gre)# next-tunnel ipsec branch1
hostname(config-tunnel-gre)# exit
hostname(config)#
```

Step 4: Bind the GRE tunnel to the tunnel interface

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# ip address 172.16.1.1/24
hostname(config-if-tun1)# tunnel gre center-branch1 gw 172.16.1.2
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 5: Configure OSPF

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# router-id 172.16.1.1
hostname(config-router)# network 172.16.1.1/24 area 0
hostname(config-router)# network 192.168.1.1/24 area 0
hostname(config-router)# exit
hostname(config-vrouter)# exit
hostname(config)#
```

Step 6: Configure a policy

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Configuring the Branch

Step 1: Configure the interface

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 202.106.2.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.2.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 2: Configure the IPsec VPN

```
hostname(config)# isakmp proposal center
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal center
hostname(config-ipsec-proposal)# exit
hostname(config)# isakmp peer center
hostname(config-isakmp-peer)# interface ethernet0/0
hostname(config-isakmp-peer)# peer 202.106.1.1
hostname(config-isakmp-peer)# pre-share 111111
hostname(config-isakmp-peer)# isakmp center
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec center auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer center
hostname(config-tunnel-ipsec-auto)# ipsec-proposal center
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

Step 3: Configure the GRE tunnel

```
hostname(config)# tunnel gre branch1
hostname(config-tunnel-gre)# source 202.106.2.1
hostname(config-tunnel-gre)# destination 202.106.1.1
hostname(config-tunnel-gre)# interface ethernet0/0
hostname(config-tunnel-gre)# next-tunnel ipsec center
hostname(config-tunnel-gre)# exit
hostname(config)#
```

Step 4: Bind the GRE tunnel to the tunnel interface

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# ip address 172.16.1.2/24
hostname(config-if-tun1)# tunnel gre branch1 gw 172.16.1.1
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 5: Configure OSPF

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# router-id 172.16.1.2
hostname(config-router)# network 172.16.1.2/24 area 0
hostname(config-router)# network 192.168.2.1/24 area 0
hostname(config-router)# exit
hostname(config-vrouter)# exit
hostname(config)#
```

Step 6: Configure a policy

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)#
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

L2TP

Overview

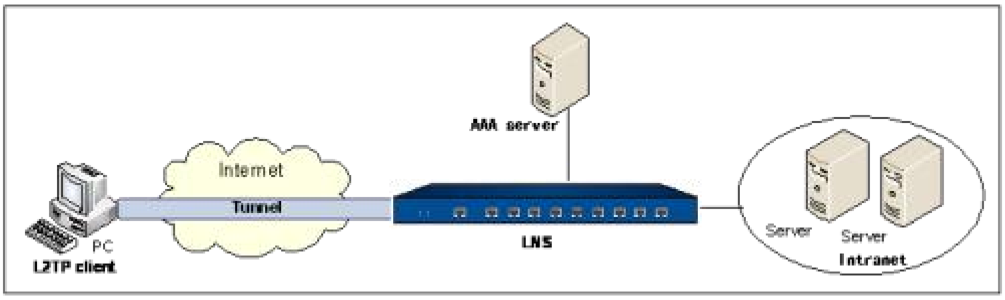
L2TP (Layer Two Tunneling Protocol) is a VPDN technique that allows dial-up users to launch VPN connection from L2TP clients or L2TP access concentrators (LAC), and connect to a L2TP network server (LNS) via PPP. After the connection has been established successfully, LNS will assign IP addresses to legal users and permit them to access the private network.

The FS device acts as 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 for legal users.

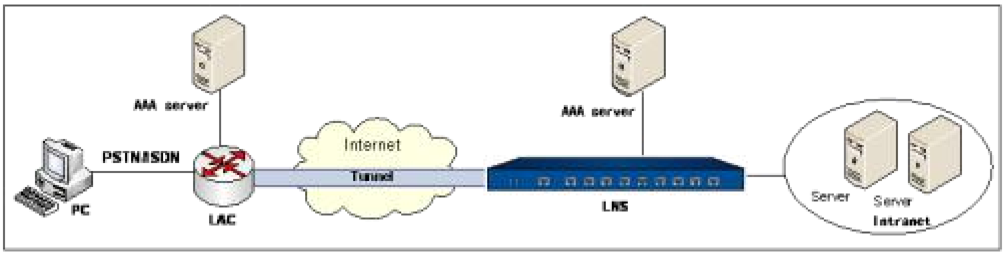
Note: For more information about L2TP, see RFC2661.

Typical L2TP Tunnel Network

There are two kinds of typical L2TP tunnel network modes:



The figure above shows the network topology where the L2TP client directly sends requests for connection to the LNS, and attempts to establish a tunnel. Any PC installed with Windows 2000/2003/XP/Vista or Linux system can serve as the L2TP client.



The figure above shows the network topology where the remote user dials up to LAC via PSTN/ISDN, and the LAC launches a VPN connection and attempts to establish a tunnel. LAC is the device that provides access service for remote dial-up users. It lies between the remote dial-up user and LNS, and is responsible for data forwarding between them. The connection between LAC and remote dial-up users adopts PPP or local connection, while the connection between LAC and LNS requires a tunnel established over L2TP.

L2TP over IPSec

L2TP does not encrypt the data transmitted through the tunnel, so it cannot assure security during the transmission. You can use L2TP in combination with IPsec, and encrypt data by IPSec, thus assuring the security for the data transmitted through the L2TP tunnel.

To configure L2TP over IPsec, take the following steps:

1. Configure a L2TP client, and make sure IPsec encryption is enabled. For more information about how to configure IPsec encryption on a client, see the user manual of your OS; for the configuration on Windows XP, see Example of Configuring L2TP over IPsec.
2. Configure IPsec VPN. For more information, see IPsec Protocol.
3. Configure a L2TP instance, and reference the configured IPsec tunnel.
4. Configure a policy rule.

When using the L2TP client on Windows systems, keep in mind that:

- The L2TP client on Windows systems only supports the IKE negotiation of the main mode; therefore, you need to configure the IKE negotiation mode to main mode on LNS. For the supported mode of the L2TP client on other systems, see related user manual.
- IPsec on Windows systems only supports the transport mode; therefore, you need to configure IPsec to transparent mode on LNS.

Configuring LNS

The configurations of LNS include:

- Configuring an address pool
- Configuring a L2TP instance
- Binding the L2TP instance to a tunnel interface
- Kicking out a user
- Restarting a tunnel

Configuring an Address Pool

LNS assigns the IP addresses in the address pool to users. After the client has established a connection to LNS successfully, LNS will choose an IP address along with other related parameters (such as DNS server address, WINS server address, etc) from the address pool, and assigns them to the client. To create a L2TP address pool, in the global configuration mode, use the following command:

l2tp pool *pool-name*

- *pool-name* – Specifies the name of the address pool.

The above command creates the address pool with the specified name, and leads you to the L2TP address pool configuration mode; if the specified name exists, the system will directly enter the L2TP address pool configuration mode.

To delete the specified L2TP address pool, in the global configuration mode, use the following command:

no l2tp pool *pool-name*

You can configure the following options in the L2TP address pool configuration mode:

- IP range of the address pool
- Reserved IP address
- IP binding rules

Configuring the IP Range of the Address Pool

To configure an IP range of the address pool, in the L2TP address pool configuration mode, use the following command:

address *start-ip end-ip*

- *start-ip* – Specifies the start IP of the IP range.
- *end-ip* – Specifies the end IP of the IP range.

You can specify up to 60000 IP addresses for an address pool.

To delete the specified IP range, in the L2TP address pool configuration mode, use the following command:

no address

Configuring the Reserved IP Address

Some IP addresses can be reserved in the reserved address pool, and they will not be allocated. When allocating IP addresses in the address pool, LNS will reserve the addresses that are occupied by other services (such as gateway, FTP server, etc.). To configure the reserved IP address, in the L2TP address pool configuration mode, use the following command:

exclude-address *start-ip end-ip*

- *start-ip* – Specifies the start IP of the reserved IP address.
- *end-ip* – Specifies the end IP of the reserved IP address.

To delete the specified reserved IP address, in the L2TP address pool configuration mode, use the following command:

no exclude *address*

Configuring IP Binding Rules

L2TP provides fixed IP addresses by creating and implementing IP binding rules that consist of static IP binding rule and role-IP binding rule. The static IP binding rule binds the client user to a fixed IP address in the address pool. Once the client has established a connection successfully, the system will assign the binding IP to the client. The rule-IP binding rule binds the role to a specific IP range in the address pool. Once the client has established a connection successfully, the system will assign an IP address within the IP range to the client.

When LNS is allocating IP addresses in the address pool, the system will check the IP binding rule and determine how to assign IP addresses for the client based on the specific checking order below:

1. Check if the client is configured with any static IP binding rule. If so, assign the binding IP address to the client; otherwise, further check other configurations. Note if the binding IP address is in use, the user will be unable to log in when it is in use.
2. Check if the client is configured with any role-IP binding rule. If so, assign an IP address within the binding IP range to the client; otherwise, the user will be unable to log in.

Note: The IP addresses defined in the static IP binding rule and role-IP binding rule should not be overlapped.

Configuring a Static IP Binding Rule

To configure a static IP binding rule, in the L2TP address pool configuration mode, use the following command:

ip-binding user *user-name ip-address*

- **user** *user-name* − Specifies the username of the client.
- *ip-address* − Specifies the binding IP address which must be an available address in the address pool.

To cancel the specified static IP binding rule, in the L2TP address pool configuration mode, use the following command:

no ip-binding user *user-name*

Configuring a Role-IP Binding Rule

To configure a role-IP binding rule, in the L2TP address pool configuration mode, use the following command:

ip-binding role *role-name* **ip_range** *start-ip end-ip*

- **role** *role-name* − Specifies the name of the role.
- **ip_range** *start-ip end-ip* − Specifies the start IP and end IP of the binding IP range which must be an available IP range in the address pool.

To cancel the specified role-IP binding rule, in the L2TP address pool configuration mode, use the following command:

no ip-binding role *role-name*

Moving a role-IP Binding Rule

One user can be bound to one or multiple roles, and different roles can be configured with different role-IP binding rules. For the user that is bound to multiple roles and the roles are also configured with their corresponding role-IP binding rules, the system will query the role-IP binding rules in turn, and assign an IP address based on the first matched rule. By default the system will put the new rule at the bottom of all rules. You can move a role-IP binding rule to change its matching sequence. To move a role-IP binding rule, in the L2TP address pool configuration mode, use the following command:

move *role-name1* {**before** *role-name2* | **after** *role-name2*| **top** | **bottom**}

- *role −name1* − Specifies the name of the role-IP binding rule that will be moved.
- **before** *role-name2* − Moves the role-IP binding rule before the rule named role-name2.
- **after** *role-name2* − Moves the role-IP binding rule after the rule named role-name2.
- **top** − Moves the role-IP binding rule to the top of all the rules.
- **bottom** − Moves the role-IP binding rule to the bottom of all the rules.

Configuring a L2TP Instance

To create an L2TP instance, in the global configuration mode, use the following command:

tunnel l2tp *tunnel-name*

- *tunnel-name* – Specifies the name of the L2TP instance.

After executing the above command, the system will create the L2TP instance with the specified name, and enter the L2TP instance configuration mode; if the specified name exists, the system will directly enter the L2TP instance configuration mode.

To delete the specified L2TP instance, in the global configuration mode, use the following command:

no tunnel l2tp *tunnel-name*

You can configure the following options in the L2TP instance configuration mode:

- IP address assignment
- Address pool
- DNS server
- WINS server
- Egress interface of the tunnel
- AAA server
- PPP authentication protocol
- Hello interval
- Tunnel authentication
- Tunnel password
- Local name of LNS
- AVP hidden
- Window size of the tunnel data
- Multi-Logon
- Enabling/disabling user-specified client IP
- Retry times of control packets

Specifying the IP Address Assignment Method

LNS assigns IP addresses and DNS server address to users using the address pool or the local AAA server. By default, LNS assigns IP addresses by address pool.

To specify the IP address assignment method for the L2TP instance, use the following command in the L2TP instance configuration mode:

assign-client-ip from { pool | aaa-server }

- pool – Uses the address pool to assign IP addresses and DNS server address.
- aaa-server – Uses the AAA server to assign IP addresses and DNS server address.

Note:The type of the local AAA server must be Radius.

Specifying an Address Pool

To specify a L2TP address pool for the L2TP instance, in the L2TP instance configuration mode, use the following command:

pool *pool-name*

- *pool-name* – Specifies the name of the L2TP address pool defined in the system.

To cancel the specified L2TP address pool, in the L2TP instance configuration mode, use the following command:

no pool

Configuring a DNS Server

To configure a DNS server, in the L2TP instance configuration mode, use the following command:

dns *address1* [*address2*]

- *address1* – Specifies the IP address of the DNS server. You can configure up to two DNS servers.

To cancel the specified DNS server, in the L2TP instance configuration mode, use the following command:

no dns

Configuring a WINS Server

To configure a WINS server, in the L2TP instance configuration mode, use the following command:

wins *address1* [*address2*]

- *address1* − Specifies the IP address of the WINS server. You can configure up to two WINS servers.

To cancel the specified WINS server, in the L2TP instance configuration mode, use the following command:

no wins

Specifying the Egress Interface of the Tunnel

To specify the egress interface of the tunnel, in the L2TP instance configuration mode, use the following command:

interface *interface-name*

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

To cancel the specified egress interface, in the L2TP instance configuration mode, use the following command:

no interface

Specifying an AAA Server

The AAA server specified here is used by LNS for L2TP authentication. To specify an AAA server, in the L2TP instance configuration mode, use the following command:

aaa-server *aaa-server-name* [**domain** *domain-name* [*keep-domain-name*]]

- *aaa-server-name* − Specifies the name of the AAA server.
- *domain domain-name* − Specifies the domain name of the AAA server to distinguish different AAA servers.
- *keep-domain-name* − After specifying this parameter, the AAA server uses the full name of the user, including the username and the domain name, to perform the authentication.

To cancel the specified AAA server, in the L2TP instance configuration mode, use the following command:

no aaa-server *aaa-server-name* [**domain** *domain-name*]

Specifying a PPP Authentication Protocol

When establishing a connection with the client or LAC, the LNS can adopt either PAP or CHAP for authentication during the PPP negotiation. To specify a PPP authentication protocol, in the L2TP instance configuration mode, use the following command:

ppp-auth {pap | chap | any}

- pap – Uses PAP for PPP authentication.
- chap – Uses CHAP for PPP authentication. This is the default option.
- any – Uses CHAP for PPP authentication by default. If CHAP is not supported, then uses PAP.

To restore to the default authentication configuration, in the L2TP instance configuration mode, use the following command:

no ppp-auth

Specifying the Hello Interval

L2TP uses Hello packets to detect if the tunnel is connected. LNS sends Hello packets to the L2TP client or LAC regularly, and will drop the connection to the tunnel if no response is returned after the specified period. To specify the Hello interval, in the L2TP instance configuration mode, use the following command:

keepalive *time*

- *time* – Specifies the Hello interval. The value range is 60 to 1800 seconds. The default value is 60.

To restore to the default Hello interval, in the L2TP instance configuration mode, use the following command:

no keepalive

Enabling Tunnel Authentication

Before establishing a tunnel, you can enable tunnel authentication to assure the security of the connection. The tunnel authentication can be launched by either LNS or LAC. The tunnel cannot be established unless the both ends are authenticated, i.e., the secret strings of the two ends are consistent. By default tunnel authentication is disabled. To enable the function, in the L2TP instance configuration mode, use the following command:

tunnel-authentication

To disable tunnel authentication, in the L2TP instance configuration mode, use the following command:

no tunnel-authentication

Specifying the Secret String

To specify the secret string that is used for LNS tunnel authentication, in the L2TP instance configuration mode, use the following command:

secret *secret-string* [**peer-name** *name*]

- *secret-string* – Specifies the secret string for the tunnel. The value range is 30 to 60 characters.
- **peer-name** *name* – Specifies the host name of LAC. If multiple LACs are connected to LNS, you can specify different secret strings for different LACs by this parameter. If this parameter is not specified, the system will use the same secret string for all the LACs.

To cancel the specified secret string, in the L2TP instance configuration mode, use the following command: **no secret** *secret-string* [**peer-name** *name*]

Specifying the Local Name of LNS

To specify the local name of LNS, in the L2TP instance configuration mode, use the following command:

local-name *name*

- *name* – Specifies the name of the LNS tunnel. The value range is 6 to 30 characters. The default name is LNS.

To restore to the default value, in the L2TP instance configuration mode, use the following command:

no local-name

Enabling AVP Hidden

L2TP uses AVP (attribute value pair) to transfer and negotiate some L2TP parameters and attributes. By default AVP is transferred in plain text. For data security consideration, you can encrypt the data by the secret string to hide the AVP during the transmission. To enable or disable AVP hidden, in the L2TP instance configuration mode, use the following commands:

- Enable: **avp-hidden**
- Disable (default): **no avp-hidden**

Note: To enable AVP hidden, you must configure the secret string for the tunnel.

Specifying the Window Size of the Tunnel Data

To configure the window size for the data transmitted through the tunnel, in the L2TP instance configuration mode, use the following command:

tunnel-receive-window *window-size*

- *window-size* – Specifies the window size. The value range is 4 to 800 packets. The default value is 8.

To restore to the default value, in the L2TP instance configuration mode, use the following command:

no tunnel-receive-window

Configuring Multi-Logon

Multi-logon function allows a user to log on and be authenticated on different hosts simultaneously. This function is enabled by default. To enable or disable multi-logon, in the L2TP instance configuration mode, use the following commands:

- Enable: **allow-multi-logon**
- Disable: **no allow-multi-logon**

Enabling/Disabling User-Specified Client IP

By default the client IP is selected from the address pool, and allocated by LNS automatically. If this function is enabled, you can specify an IP address. However, this IP address must belong to the specified address pool, and be consistent with the username and role. If the specified IP is already in use, the system will not allow the user to log on. To enable or disable user-specified client IP, in the L2TP instance configuration mode, use the following commands:

- Enable (default): **accept-client-ip**
- Disable: **no accept-client-ip**

Specifying the Retry Times of Control Packets

L2TP uses two types of packets: control packets and data packets. The control packets are responsible for establishing, maintaining and clearing the L2TP tunnel, while the data packets are responsible for transmitting data. The transmission of data packets is not reliable. Even if data is lost, the transmission will not be retried; while the transmission of control packets is reliable. If no response is received from the peer after the specified retry times, the system will determine the tunnel connection is disconnected. The interval of re-transmitting control packets starts from 1 second, and increases by the multiples of 2, i.e., 1 second, 2 seconds, 4 seconds, 8 seconds, 16 seconds…

To specify the retry times of control packets, in the L2TP instance configuration mode, use the following command:

transmit-retry *times*

- *times* − Specifies the retry times of control packets. The value range is 1 to 10 times. The default value is 5.

To restore to the default value, in the L2TP instance configuration mode, use the following command:

no transmit-retry

Referencing an IPsec Tunnel

When configuring L2TP over IPsec, you need to combine an IPsec tunnel to the L2TP tunnel in order to encrypt data. To reference an IPsec tunnel in the L2TP instance, in the L2TP instance configuration mode, use the following command:

next-tunnel ipsec *tunnel-name*

- *tunnel-name* − Specifies the name of the IPsec VPN tunnel defined in the system.

To cancel the specified IPsec tunnel, in the L2TP instance configuration mode, use the following command:

no next-tunnel ipsec

Configuring Mandatory LCP Phase

After a remote dial-up user connects to the LAC, the LAC starts the L2TP VPN to the LNS and establishes the tunnel. When the LNS authenticates the users, it can execute the LCP (Link Control Protocol) phase or not.

By default, the LNS does not execute the LCP phase with the L2TP client. Instead, it authenticates the L2TP client based on the authentication type specified by the Proxy Authen Type AVP in the ICCN (Incoming-Call-Connected) packets.

To configure the mandatory LCP phase between the LNS and the L2TP client, use the following command in the L2TP instance configuration mode:

ppp-lcp-force

To disable the mandatory LCP phase, use the **no ppp-lcp-force** command.

When a remote dial-up user connects to the LNS directly, the ICCN packets will not carry the Proxy Authen Type AVP. The LNS will always execute the LCP phase with the L2TP client.

Binding the L2TP Instance to a Tunnel Interface

The configured L2TP instance will not take effect until it is bound to a tunnel interface. When a L2TP instance is only bound to a tunnel interface and you do not specify the domain name to the L2TP tunnel (the tunnel with a L2TP instance bound), all clients that connect to a certain LNS will be divided to the VR that relates to the this LNS.

You can also bind multiple tunnel interfaces to one L2TP instance and specify a domain name for each L2TP tunnel. When clients connect to the LNS and the user pass the authentication, the system will divide users into a L2TP tunnel with the same domain name specified. Then, if the tunnel interfaces belong to different VRs, LNS, by using the authentication server, can repeatedly distribute the internal resource addresses to the clients in each L2TP tunnel

Each tunnel interface can only be bound with one L2TP instance. To bind the L2TP instance to a tunnel interface, in the tunnel interface configuration mode, use the following command:

tunnel l2tp *tunnel-name* [**bind-to-domain** *domain-name*]

- *tunnel-name* – Specifies the name of the L2TP instance defined in the system.
- **bind-to-domain** *domain-name* – Binds the domain name to the L2TP tunnel. If you bind the domain name, usernames without the domain name cannot dial up successfully. If you do not bind the domain name, LNS will omit the domain name of usernames when authenticating users.

To cancel the binding and the specified domain name, in the tunnel interface configuration mode, use the following command:

no tunnel l2tp *tunnel-name*

To cancel the specified domain name, in the tunnel interface configuration mode, user the following command:

no tunnel l2tp *tunnel-name* **bind-to-domain** *domain-name*

Kicking out a User

To kick out a user from the LNS connection, in the execution mode, use the following command:

exec l2tp *tunnel-name* **kickout user** *user-name*

- *tunnel-name* – Specifies the name of the L2TP instance.
- *user-name* – Specifies the name of the user who will be kicked out.

Restarting a Tunnel

After the tunnel is restarted, all the connections to the tunnel will be cleared. To restart a tunnel, in any mode, use the following command:

clear l2tp t*unnel-name*

- *tunnel-name* – Specifies the name of the L2TP instance.

Viewing L2TP Information

To view the L2TP information, use the following commands:

- Show the L2TP instance information:
  show tunnel l2tp [*l2tp-tunnel-name*]
- Show the L2TP tunnel status:
  show l2tp tunnel *l2tp-tunnel-name*
- Show the specified client information of the L2TP instance:
  show l2tp client {*tunnel-name l2tp-tunnel-name* [**user** *user-name*] | **tunnel-id** *ID*}
- Show the L2TP address pool configuration:
  show l2tp pool [*pool-name*]
- Show the L2TP address pool statistics:
  show l2tp pool *pool-name* **statistics**
- Show all the clients of the L2TP instance:
  show auth-user l2tp [**interface** *interface-name* | **vrouter** *vrouter-name* | **slot** *slot-no*]

Configuring L2TP Client

To establish a L2TP tunnel between the L2TP client and LNS, you need to configure a L2TP client. For more information about L2TP on Windows 2000/2003/XP/Vista, see the corresponding Windows 2000/2003/XP/Vista documents.

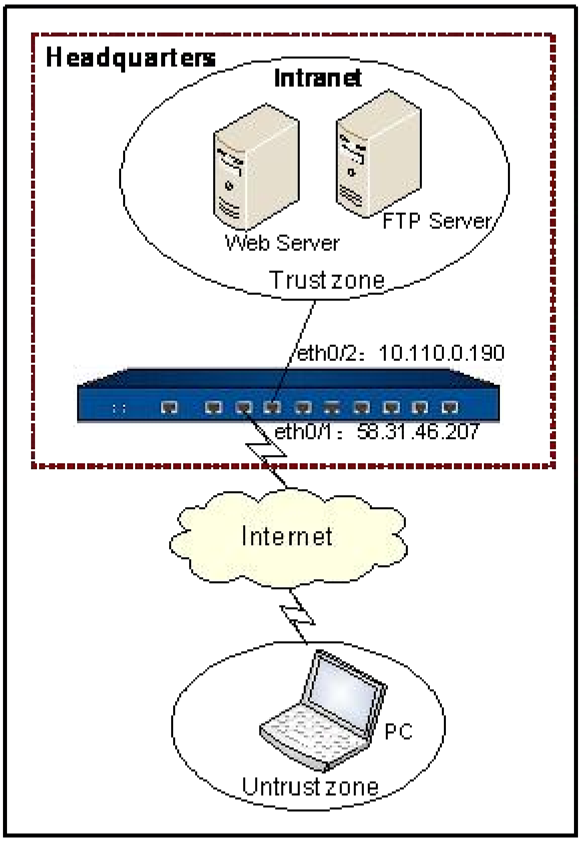
Note: When establishing a dial-up connection to LNS from the L2TP client on Windows system, make sure the system has not been not installed with FS Secure Defender.

Example of Configuring L2TP

This section describes a typical L2TP configuration example.

Requirement

A remote employee needs to visit the Intranet of the headquarters via L2TP VPN. The network topology is shown as below:



Configuration Steps

Configure LNS and L2TP client respectively.

Configurations on LNS

Step 1 : Configure interfaces

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 58.31.46.207/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone trust
hostname(config-if-eth0/2)# ip address 10.110.0.190/24
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Step 2 : Configure a local AAA server

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user shanghai
hostname(config-user)# password 123456
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 3 : Configure the LNS address pool and specify the IP range

```
hostname(config)# l2tp pool pool1
hostname(config-l2tp-pool)# address 10.232.241.2 10.232.244.254
hostname(config-l2tp-pool)# exit
hostname(config)#
```

Step 4 : Configure a L2TP instance

```
hostname(config)# tunnel l2tp test
hostname(config-tunnel-l2tp)# pool pool1
hostname(config-tunnel-l2tp)# dns 202.106.0.20 10.188.7.10
hostname(config-tunnel-l2tp)# interface ethernet0/1
hostname(config-tunnel-l2tp)# ppp-auth any
hostname(config-tunnel-l2tp)# keepalive 1800
hostname(config-tunnel-l2tp)# aaa-server local
hostname(config-tunnel-l2tp)# exit
hostname(config)#
```

Step 5 : Create a tunnel interface and bind the L2TP instance named test to the interface

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ip address 10.232.241.1 255.255.248.0
hostname(config-if-tun1)# manage ping
hostname(config-if-tun1)# tunnel l2tp test
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 6 : Configure a policy rule

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Configurations on the Client

The following sections describe how to configure the client in a Windows XP system. The configuration steps are:

1. Create a L2TP dial-up connection.
2. Configure the dial-up connection and modify the properties.
3. Modify the registry to disable IPsec encryption.

Creating a L2TP Dial-up Connection

To create a L2TP connection on Windows XP, take the following steps:

1. Click **Start** > **Control Panel** > **Network Connections**.

2. Click **Create a new connection** > **Connect to the network at my workplace**, and click **Next**.

3. In the New Connection Wizard dialog, click **Virtual Private Network Connection**, and click **Next**.

4. Type **L2TP** into the **Company Name** box, and click **Next**.

5. Select **Do not dial the initial connection**, and click **Next**.

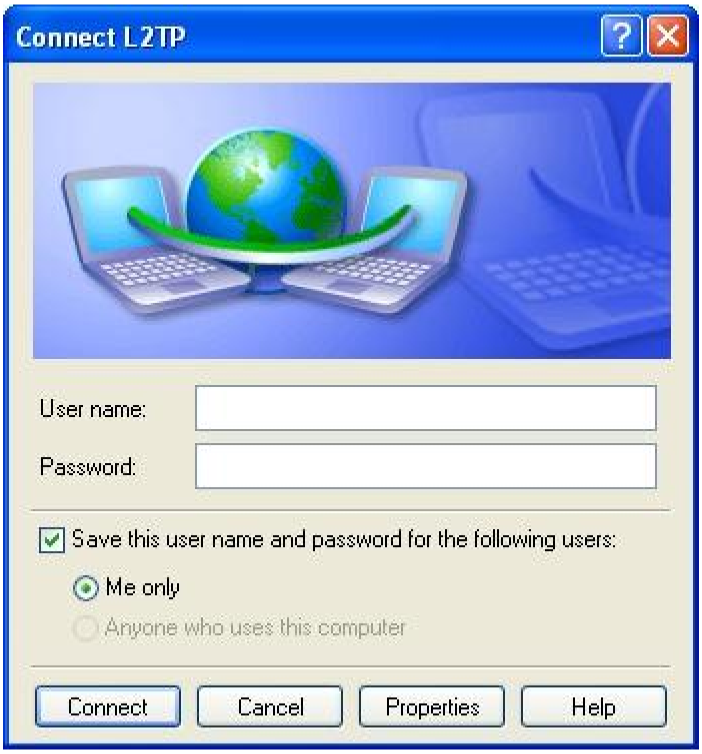
6. Type the LNS IP address 58.31.46.207 into the **Host name** or **IP address** box, and click **Next**.

7. Complete other L2TP client configurations as prompted.

Configuring L2TP Dial-up Connection

To modify the properties of the dial-up connection, take the following steps:

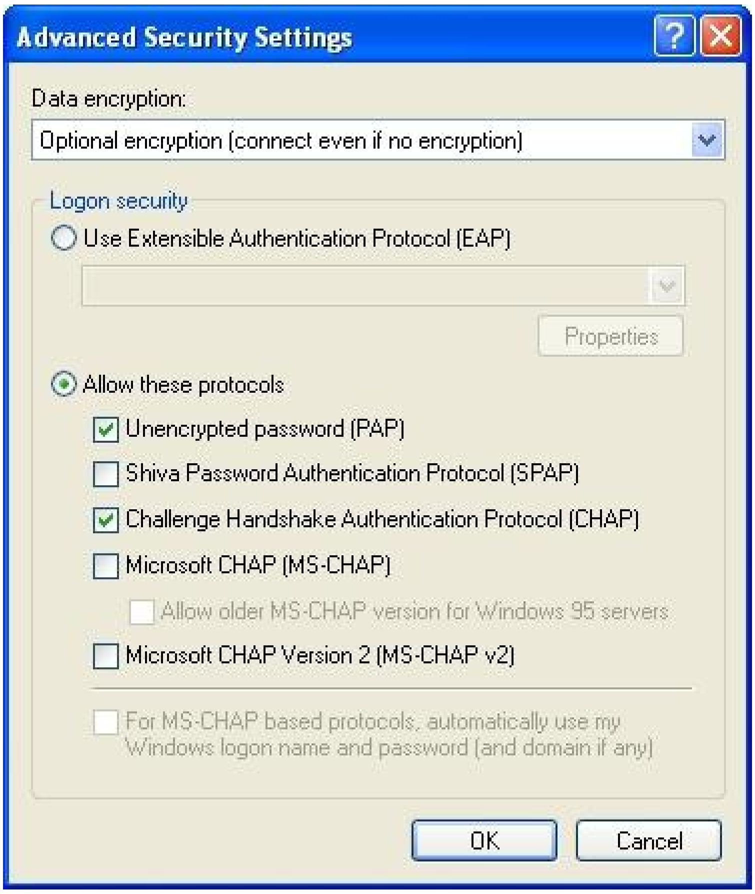
1. In My Network Places, double click the connection named L2TP.


Connect L2TP
User name:
Password:
☑ Save this user name and password for the following users:
● Me only
○ Anyone who uses this computer
Connect
Cancel
Properties
Help

2. In the Connect L2TP dialog shown below, click **Properties**.

3. In the L2TP Properties dialog, click the **Security** tab, and click **Advanced (custom settings)**. Click **Settings** behind.

4. In the Advanced Security Settings dialog, select **Optional encryption (connect even if no encryption)** from the **Data encryption** drop-down list, click **Allow these protocols** in the Logon security box, and select **Unencrypted password (PAP)** and **Challenge Handshake Authentication Protocol (CHAP)**, as shown below:



Data encryption:
Optional encryption (connect even if no encryption)

Logon security

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

☑ Unencrypted password (PAP)

□ Shiva Password Authentication Protocol (SPAP)

☑ Challenge Handshake Authentication Protocol (CHAP)

□ Microsoft CHAP (MS-CHAP)

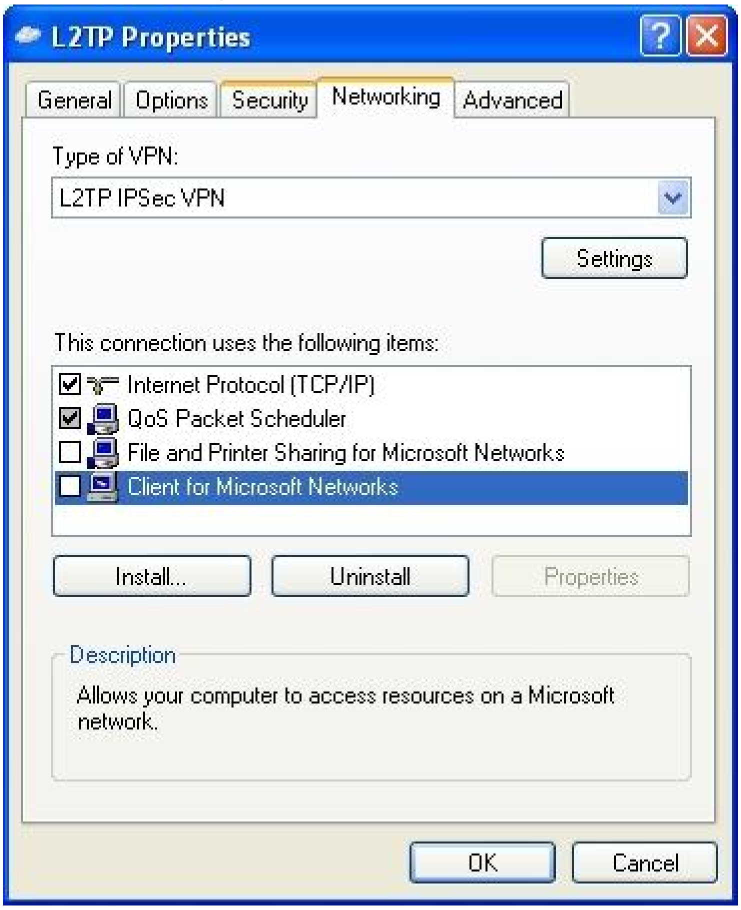
□ Allow older MS-CHAP version for Windows 95 servers

□ Microsoft CHAP Version 2 (MS-CHAP v2)

□ For MS-CHAP based protocols, automatically use my Windows logon name and password (and domain if any)

5. In the L2TP Properties dialog, click the **Network** tab. Select **L2TP IPsec VPN** from the **Type of VPN** drop-down list, and select **Internet Protocol (TCP/IP)** in the **This connection**

uses the following items box, as shown below:



Type of VPN:

L2TP IPSec VPN

This connection uses the following items:

☑ Internet Protocol (TCP/IP)
☑ QoS Packet Scheduler
□ File and Printer Sharing for Microsoft Networks
□ Client for Microsoft Networks

Description

Allows your computer to access resources on a Microsoft network.

6. Click **OK** to save the changes.

Modifying the Registry

By default Windows XP enables IPsec encryption on the L2TP connection. You can disable the default action by modifying the Windows XP registry. If IPsec encryption is not disabled, the L2TP client will be disconnected automatically during dialing up.

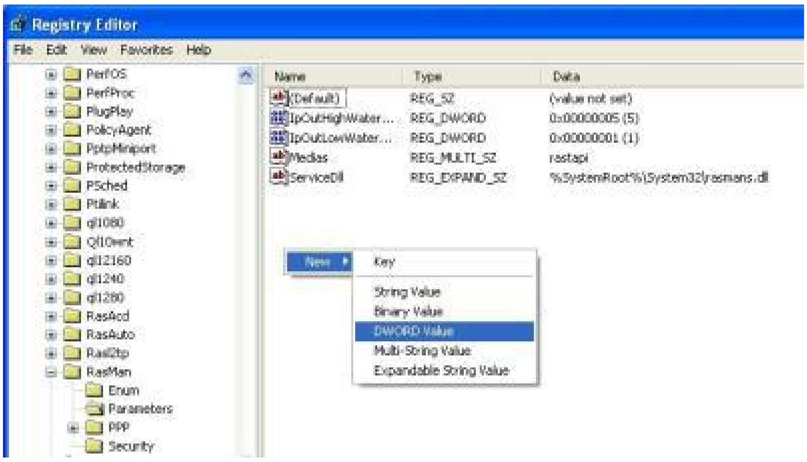
To modify the registry, take the following steps:

1. Click **Start** > **Run**, and type Regedt32 into the **Open** box.

2. In the Registry Editor dialog, navigate to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RasMan\Parameters.

3. Add a DWORD value for Parameters. Click **Parameters**, and right-click any blank place in the right pane. From the menu, click **New > DWORD** value, as shown below. Specify the

name as ProhibitIPsec, type as REG_DWORD, and value as 1. Click **OK** to save the settings.



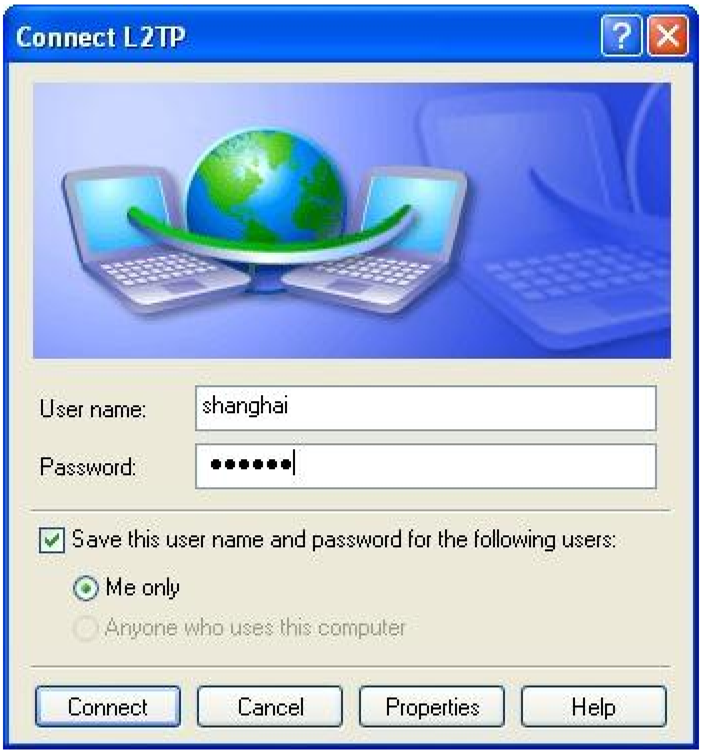
Name	Type	Data
(Default)	REG_SZ	(value not set)
IpOutHighWater...	REG_DWORD	0x00000005 (5)
IpOutLowWater...	REG_DWORD	0x00000001 (1)
Medias	REG_MULTI_SZ	rastapi
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\System32\rasmans.dll

4. Exit the registry editor and restart the system to make the modification take effect.

Connecting to LNS from the Client

After the above LNS and client configuration, you can initiate a VPN connection to LNS and establish a tunnel from the client.

In My Network Places, double click the dial-up connection named L2TP. In the Connect L2TP dialog, type shanghai and 123456 into the **User name** and **Password** boxes respectively, and click **Connect**, as shown below.



User name: shanghai

Password: ••••••

☑ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

After the dial-up connection has been established, the employee in Shanghai can gain access to the Web server and FTP server in the Intranet securely over L2TP.

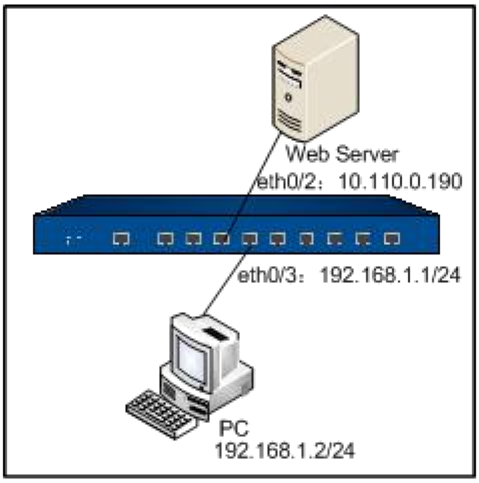
In MS-DOS, the command ipconfig will return the address in the LNS address pool 10.232.241.2 15, i.e., the IP address allocated to PC by LNS.

Example of Configuring L2TP over IPsec

This section describes a typical L2TP over IPsec configuration example.

Requirement

An employee needs to visit the Web server in the Intranet via L2TP VPN. Data transmission between the PC and LNS is encrypted by IPsec. The network topology is shown below.



Configuration Steps

Configure LNS and L2TP client respectively.

Configurations on LNS

Step 1: Configure interfaces

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone trust
hostname(config-if-eth0/2)# ip address 10.110.0.190/24
hostname(config-if-eth0/2)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone untrust
hostname(config-if-eth0/3)# ip address 192.168.1.1/24
hostname(config-if-eth0/3)# exit
hostname(config)#
```

Step 2: Configure IPsec VPN

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# hash sha
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash sha
hostname(config-ipsec-proposal)# encryption 3des
hostname(config-ipsec-proposal)# exit
hostname(config)# isakmp peer east
hostname(config-isakmp-peer)# interface ethernet0/3
hostname(config-isakmp-peer)# type usergroup
hostname(config-isakmp-peer)# accept-all-peer-id
hostname(config-isakmp-peer)# mode main
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# pre-share hello1
hostname(config-isakmp-peer)# aaa-server local
hostname(config)# tunnel ipsec vpn1 auto
hostname(config-tunnel-ipsec-auto)# mode transport
hostname(config-tunnel-ipsec-auto)# isakmp-peer east
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# accept-all-proxy-id
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

Step 3: Configure a local AAA server

```
hostname(config)# aaa-server test type local
hostname(config-aaa-server)# user shanghai

hostname(config-user)# password 123456

hostname(config-user)# exit

hostname(config-aaa-server)# exit

hostname(config)#
```

Step 4: Configure the LNS address pool and specify the IP range

```
hostname(config)# l2tp pool pool2

hostname(config-l2tp-pool)# address 10.10.10.2 10.10.10.100

hostname(config-l2tp-pool)# exit

hostname(config)#
```

Step 5: Configure a L2TP instance and reference an IPsec tunnel

```
hostname(config)# tunnel l2tp l2tp1

hostname(config-tunnel-l2tp)# pool pool2

hostname(config-tunnel-l2tp)# dns 202.106.0.20

hostname(config-tunnel-l2tp)# interface ethernet0/3

hostname(config-tunnel-l2tp)# next-tunnel ipsec vpn1

hostname(config-tunnel-l2tp)# ppp-auth chap

hostname(config-tunnel-l2tp)# keepalive 1800

hostname(config-tunnel-l2tp)# aaa-server test

hostname(config-tunnel-l2tp)# exit

hostname(config)#
```

Step 6: Create a tunnel interface and bind the L2TP instance named l2tp1 to the interface

```
hostname(config)# interface tunnel1

hostname(config-if-tun1)# zone dmz

hostname(config-if-tun1)# ip address 10.10.10.1/24

hostname(config-if-tun1)# manage ping
hostname(config-if-tun1)# tunnel l2tp l2tp1

hostname(config-if-tun1)# exit

hostname(config)#
```

Step 7: Configure a policy rule

```
hostname(config)# policy-global

hostname(config-policy)# rule

hostname(config-policy-rule)# src-zone dmz

hostname(config-policy-rule)# dst-zone trust

hostname(config-policy-rule)# src-addr any

hostname(config-policy-rule)# dst-addr any

hostname(config-policy-rule)# service any

hostname(config-policy-rule)# action permit

hostname(config-policy-rule)# exit

hostname(config-policy)# exit

hostname(config)#
```

Configurations on the Client

The following sections describe how to configure the client in a Windows XP system. The configuration steps are:

1. Create a L2TP dial-up connection.
2. Configure the dial-up connection and modify the properties.
3. Modify the registry to enable IPsec encryption.

Creating L2TP Dial-up Connection

To create a L2TP connection on Windows XP, take the following steps:

1. Click **Start** > **Control Panel** > **Network Connections**.
2. Click **Create a new connection** > **Connect to the network at my workplace**, and click **Next**.

3. In the New Connection Wizard dialog, click **Virtual Private Network Connection**, and click **Next**.

4. Type **L2TP over IPsec** into the **Company Name** box, and click **Next**.

5. Select **Do not dial the initial connection**, and click **Next**.

6. Type the LNS IP address 192.168.1.1 into the **Host name** or **IP address** box, and click **Next**.

7. Complete other L2TP client configurations as prompted.

Configuring the L2TP Dial-up Connection

To modify the properties of the dial-up connection, take the following steps:

1. In My Network Places, double click the connection named L2TP over IPsec.

2. In the Connect L2TP over IPsec dialog, click **Properties**.

3. Click tabs to configure properties, as described below:

- Security:

    - Click **Advanced (custom settings)**, and then click **Settings** behind. In the Advanced Security Settings dialog, select **Optional encryption (connect even if no encryption)** from the **Data encryption** drop-down list, click **Allow these protocols** in the Logon security box, and select **Unencrypted password (PAP)** and **Challenge Handshake Authentication Protocol (CHAP)**. Click **OK** to save the settings.

    - Click **IPsec settings**. In the IPsec Settings dialog, select **Use pre-shared key for authentication**, and type hello1 into the **Key** box. Click **OK** to save the changes.

- Network:

    - Select **L2TP IPsec VPN** from the **Type of VPN** drop-down list, and select **Internet Protocol (TCP/IP)** in the **This connection uses the following items** box.

4. Click **OK** to save the changes and close the dialog.

Enabling IPsec Encryption

By default Windows XP enables IPsec encryption on the L2TP connection. If disabled, you can re-enable the default action by modifying the Windows XP registry.

To modify the registry, take the following steps:

1. Click **Start > Run**, and type Regedt32 into the **Open** box.

2. In the Registry Editor dialog, navigate to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RasMan\Parameters.

3. Add a DWORD value for Parameters. Click **Parameters**, and right click any blank place in the right pane. From the menu, click **New > DWORD value**. Specify the name as ProhibitIPsec, type as REG_DWORD, and value as 0. Click **OK** to save the settings.

4. Exit the registry editor and restart the system to make the modification take effect.

Connecting LNS from the Client

After the above LNS and client configuration, you can initiate a VPN connection to LNS and establish a tunnel from the client.

In **My Network Places**, double click the dial-up connection named L2TP over IPsec. In the Connect L2TP over IPsec dialog, type shanghai and 123456 into the **User name** and **Password** boxes respectively, and click **Connect**. After the dial-up connection has been established, the employee in Shanghai can gain access to the Web server in the Intranet securely over L2TP.

Chapter 10 Traffic Management

This chapter introduces the following topics:

iQoS

The system provides intelligent quality of service (iQoS) which guarantees the customer's network performance, manages and optimizes the key bandwidth for critical business traffic, and helps the customer greatly in fully utilizing their bandwidth resources.

iQoS is used to provide different priorities to different traffic, in order to control the delay and flapping, and decrease the packet loss rate. iQoS can assure the normal transmission of critical business traffic when the network is overloaded or congested.

iQoS is controlled by license. To use iQoS, apply and install the iQoS license.

iQoS Implement

The packets are classified and marked after entering the system from the ingress interface. For the classified and marked traffic, the system will smoothly forward the traffic through shaping mechanism, or drop the traffic through policing mechanism. If selecting shaping mechanism to forward the traffic, the congestion management and congestion avoidance mechanisms give different priorities to different types of packets so that the packets of higher priority can pass the gateway earlier to avoid network congestion.

In general, implementing iQoS includes:

- Classification and marking mechanism: Classification and marking is the process of identifying the priority of each packet. This is the first step of iQos.
- Policing and shaping mechanisms: Policing and shaping mechanisms are used to identify traffic violation and make responses. The policing mechanism checks traffic in real time, and takes immediate actions according to the settings when it discovers violation. The shaping

mechanism works together with queuing mechanism. It makes sure that the traffic will never exceed the defined flow rate so that the traffic can go through that interface smoothly.

- Congestion management mechanism: Congestion management mechanism uses queuing theory to solve problems in the congested interfaces. As the data rate can be different among different networks, congestion may happen to both wide area network (WAN) and local area network (LAN). Only when an interface is congested will the queuing theory begin to work.

- Congestion avoidance mechanism: Congestion avoidance mechanism is a supplement to the queuing algorithm, and it also relies on the queuing algorithm. The congestion avoidance mechanism is designed to process TCP-based traffic.

Function Overview

By configuring pipes, the devices implement iQos. Pipe, which is a virtual concept, represents the bandwidth of transmission path. The system classifies the traffic by using the pipe as the unit, and control the traffic crossing the pipes according to the actions defined for the pipes. For all traffic crossing the device, they will flow into virtual pipes according to the traffic matching conditions they match. If the traffic does not match any condition, they will flow into the default pipe predefined by the system.

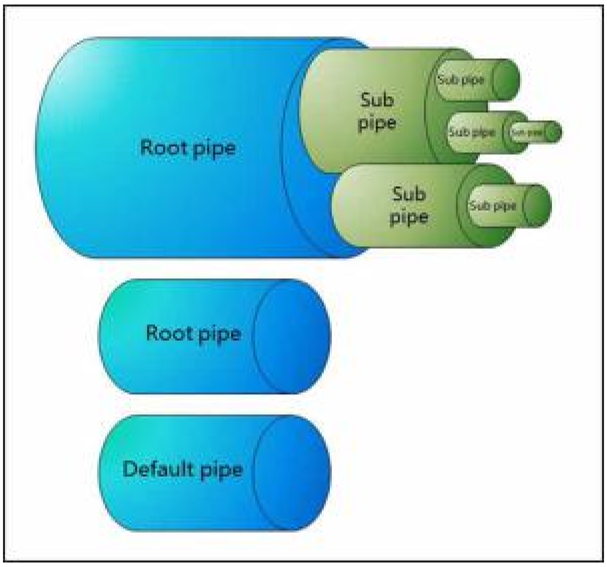
Pipes, except the default pipe, include two parts of configurations: traffic matching conditions and traffic management actions:

- Traffic matching conditions: Defines the traffic matching conditions to classify the traffic crossing the device into matched pipes. The system will limit the bandwidth to the traffic that matches the traffic matching conditions. You can define multiple traffic matching conditions to a pipe. The logical relation between each condition is OR. When the traffic matches a traffic matching condition of a pipe, it will enter this pipe.

- Traffic management actions: Defines the actions adopted to the traffic that has been classified to a pipe. The data stream control includes the forward control and the backward control. Forward control controls the traffic that flows from the source to the destination; backward control controls the traffic flows from the destination to the source.

Multiple-level Pipes

To provide flexible configurations, the system supports the multiple-level pipes. Configuring multiple-level pipes can limit the bandwidth of different applications of different users. This can ensure the bandwidth for the key services and users. Pipes can be nested to at most four levels. Sub pipes cannot be nested to the default pipe. The logical relation between pipes is shown as below:



- You can create multiple root pipes that are independent individually. At most three levels of sub pipes can be nested to the root pipe.

- For the sub pipes at the same level, the total of their minimum bandwidth cannot exceed the minimum bandwidth of their upper-level parent pipe, and the total of their maximum bandwidth cannot exceed the maximum bandwidth of their upper-level parent pipe.

- If you have configured the forward or backward traffic management actions for the root pipe, all sub pipes that belongs to this root pipe will inherit the configurations of the traffic direction set on the root pipe.

- The root pipe that is only configured the backward traffic management actions cannot work.

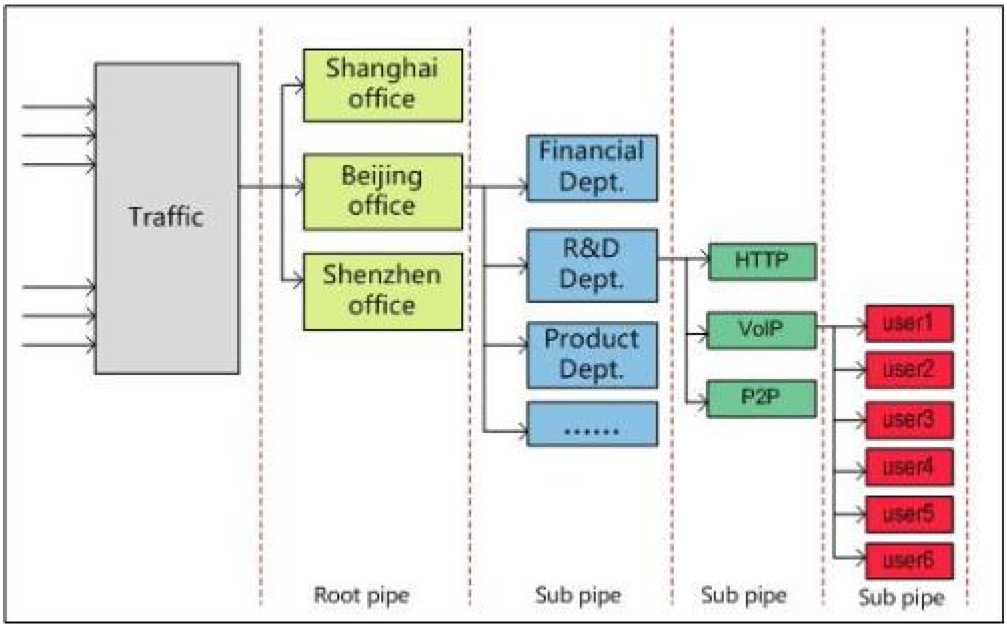
The following chart illustrates the application of multiple-level pipes in a company. The administrator can create the following pipes to limit the traffic:

1. Create a root pipe to limit the traffic of the office located in Beijing.

2. Create a sub pipe to limit the traffic of its R&D department.

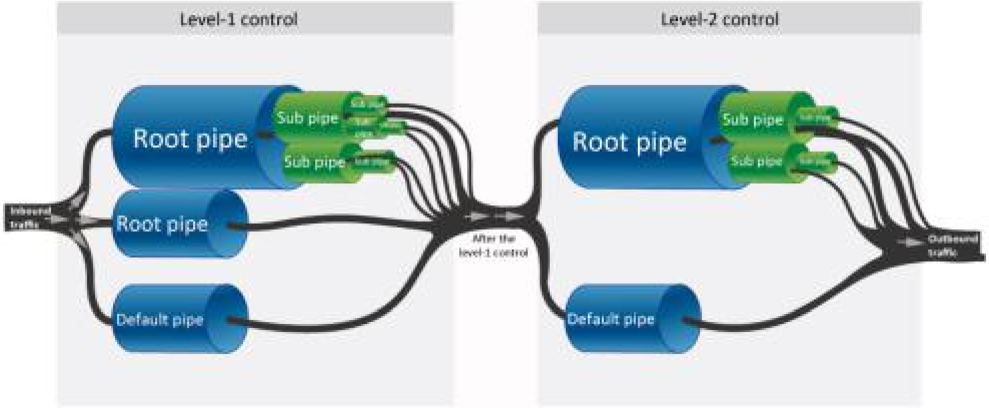
3. Create a sub pipe to limit the traffic of the specified applications so that each application has its own bandwidth.

4. Create a sub pipe to limit the traffic of the specified users so that each user owns the defined bandwidth when using the specified application.



Process of iQos

The system supports two-level traffic control: level-1 control and level-2 control. In each level, the traffic control is implemented by pipes. Traffic that is dealt with by level-1 control flows into the level-2 control, and then the system performs the further management and control according to the pipe configurations of level-2 control. After the traffic flows into the device, the process of iQos is shown as below:



According to the chart above, the process of traffic control is described below:

1. The traffic first flows into the level-1 control, and then the system classifies the traffic into different pipes according to the traffic matching conditions of the pipe of level-1 control. The traffic that cannot match any pipe will be classified into the default pipe. If the same conditions are configured in different root pipes, the traffic will first match the root pipe listed at the top of the Level-1 Control list. After the traffic flows into the root pipe, the system classifies the traffic into different sub pipes according to the traffic matching conditions of each sub pipe.

2. According to the traffic management actions configured for the pipes, the system manages and controls the traffic that matches the traffic matching conditions.

3. The traffic dealt with by level-1 control flows into the level-2 control. The system manages and controls the traffic in level-2 control. The principle of traffic matching, management and control are the same as the one of the level-1 control.

4. Complete the process of iQos.

Configuring iQoS

By using pipes, devices implement QoS. Using pipes includes the following sections:

1. Create the traffic matching conditions, which are used to control the traffic that matches these conditions. If configuring multiple traffic matching conditions for a pipe, the logical relation between each condition is OR.

2. Create a white list according to your requirements. The system will not control the traffic in the white list. Only root pipe and the default pipe support the white list.

3. Specify the traffic management actions, which are used to deal with the traffic that is classified into a pipe.

Specifying Traffic Control Level

Specify which traffic control level you want to enter, first-level traffic control or second-level traffic control and enter the traffic control mode. You can create pipes to manage the traffic. In the global configuration mode, use the following command:

```
qos-engine {first | second}
```

- **first** – Enter the traffic control mode of the first-level traffic control.
- **second** – Enter the traffic control mode of the second-level traffic control.

Enabling/Disabling Traffic Control Level/Root Pipe/Sub Pipe

To enable/disable the traffic control level, in the traffic control mode of the specified level, use the following command:

- Disable the traffic control level: **disable**
- Enable the traffic control level: **no disable**

To enable/disable the root pipe, in the root pipe configuration mode of the specified root pipe, use the following command:

- Disable the root pipe: **disable**
- Enable the root pipe: **no disable**

To enable/disable the sub pipe, in the sub pipe configuration mode of the specified sub pipe, use the following command:

- Disable the sub pipe: **disable**
- Enable the sub pipe: **no disable**

Note: The disabled levels or pipes will not take effect during the iQoS process. The unavailable pipes will not take effect as well.

Enabling/Disabling NAT IP Matching

You can enable the NAT IP matching function in the traffic control mode of the specified level as needed. After it is enabled, system will use the IP addresses between the source NAT and the destination NAT as the matching items. If the matching is successful, system will limit the speed of these IP addresses. To enable the NAT IP matching, in the traffic control mode of the specified level, use the following command:

```
match-nat-ip enable
```

To disable the NAT IP matching, in the traffic control mode of the specified level, use the command **no match-nat-ip enable**.

Note: Before enabling NAT IP matching, you must config the NAT rules. Otherwise, the configuration will not take effect.

Creating a Root Pipe

In the traffic control mode, use the following command to create a root pipe and enter the root pipe configuration mode. If the name of the root pipe already exists, the system will enter the root pipe configuration mode directly.

```
root-pipe {pipe-name | default}
```

- **pipe-name** - Enter the name of the newly created root pipe.
- **default** - Enter the default pipe.

In the traffic control mode, use the following command to delete a root pipe:

```
no root-pipe pipe-name
```

Note:

- The name of the root pipe cannot exceed 63 characters.
- A root pipe can nest up to 3 level sub pipes.
- The default pipe cannot be deleted.

After entering the root pipe configuration mode, you can configure the following configurations:

- Enable/Disable the root pipe
- Configure the traffic matching conditions of the root pipe
- Create a traffic whit list of the root pipe
- Configure the traffic management action of the root pipe
- Configure the traffic control mode of the root pipe
- Specify a schedule for the root pipe
- Create a sub pipe

Creating a Sub Pipe

To create a sub pipe and enter the sub pipe configuration mode, use the following command in the pipe configuration mode. If the sub pipe name already exists, the system will enter the sub pipe configuration mode directly.

pipe *pipe-name*

- *pipe-name – Enter the name of the newly created sub pipe.*

In the pipe configuration mode, use the following command to delete the created sub pipe:

no pipe *pipe-name*

Note:

- The name of the pipe cannot exceed 63 characters.
- To delete the sub pipe, you need to execute the command **no pipe***pipe-name* in the pipe configuration mode of its parent pipe.

In the sub pipe configuration mode, you can configure the following options:

- Enable/Disable the sub pipe

- Configure the traffic matching conditions of the sub pipe
- Create a sub pipe

Configuring a Traffic Matching Condition

Before configuring a traffic matching condition, you need to first create a traffic matching condition and then enter the traffic matching condition configuration mode. If the ID already exists, the system will enter the traffic matching condition configuration mode directly. Without the ID specified, the system will create a traffic matching condition and enter its configuration mode. To create a traffic matching condition and enter its configuration mode, use the following command in the pipe configuration mode:

pipe-map *[id]*

- *id* - Enter the ID of the traffic matching condition.

Use the **no pipe-map** *[id]* command to delete the specified traffic matching condition.

After entering the traffic matching condition configuration mode, use the following command to configure the traffic matching condition:

- Specify the source zone name of the traffic: **src-zone** *src-zone*
- Delete the source zone name of the traffic: **no src-zone**
- Specify the destination zone name of the traffic: **dst-zone** *dst-zone*
- Delete the destination zone name of the traffic: **no dst-zone**
- Specify the source host name of the traffic: **src-host** *host-name*
- Delete the source host name of the traffic: **no src-host** *host-name*
- Specify the destination host name of the traffic: **dst-host** *host-name*
- Delete the destination host name of the traffic: **no dst-host** *host-name*
- Specify the source IP address of the traffic: **src-ip** {*ip/netmask* | *ip-address netmask*}
- Delete the source IP address of the traffic: **no src-ip** {*ip/netmask* | *ip-address netmask*}
- Specify the destination IP address of the traffic: **dst-ip** {*ip/netmask* | *ip-address netmask*}
- Delete the destination IP address of the traffic: **no dst-ip** {*ip/netmask* | *ip-address netmask*}
- Specify the source IP address range of the traffic: **src-range** *min-ip [max-ip]*
- Delete the source IP address range of the traffic: **no src-range** *min-ip [max-ip]*

- Specify the destination IP address range of the traffic: **dst-range** *min-ip [max-ip]*
- Delete the destination IP address range of the traffic: **no dst-range** *min-ip [max-ip]*
- Specify the ingress interface name of the traffic: **ingress-if** *interface-name*
- Delete the ingress interface name of the traffic: **no ingress-if** *interface-name*
- Specify the egress interface name of the traffic: **egress-if** *interface-name*
- Delete the egress interface name of the traffic: **no egress-if** *interface-name*
- Specify the source address entry of the traffic: **src-addr** *address-book*
- Delete the source address entry of the traffic: **no src-addr** *address-book*
- Specify the destination address entry of the traffic: **dst-addr** *address-book*
- Delete the destination address entry of the traffic: **no dst-addr** *address-book*
- Specify the user and its AAA server: **user** *AAA-server user-name*
- Delete the users and its AAA server: **no user** *AAA-server user-name*
- Specify the user group and its AAA server: **user-group** *AAA-server usergroup-name*
- Delete the users group and its AAA server: **no user-group** *AAA-server usergroup-name*
- Specify the application or application group, including pre-defined application and user-defined application: **application** *app-name*
- Delete the application or application group, including pre-defined application and user-defined application: **no application** *app-name*
- Specify the name of the service or service group: **service** *service-name*
- Delete the name of the service or service group: **no service** *service-name*
- Specify the ToS field: **tos** *tos-value*
- Delete the ToS field: **no tos** *tos-value*
- Specify the VLAN information: **vlan** *vlan-id*
- Delete the VLAN information: **no vlan** *vlan-id*
- Specify the URL category: **url-category** *category-name*
- Delete the URL category: **no url-category** *category-name*

Configuring a Traffic White List

After configuring a traffic white list, the system will not manage the traffic in the white list. You can specify a whit list for the root pipe or the default pipe.

Before configuring a white list, you need to first create a white list and then enter the white list configuration mode. If the specified ID already exists, the system will directly enter the white list configuration mode. If you do not specify an ID, the system will create a white list and enter its configuration mode. To create a white list and enter the white list configuration mode, in the pipe configuration mode, use the following command:

exception-map [*id*]

- *id* – Enter the ID of the white list.

Use the **no exception-map** [*id*] command to delete the specified white list.

After entering the white list configuration mode, use the following command to configure the white list:

- Specify the source zone name of the traffic: **src-zone***src-zone*
- Delete the source zone name of the traffic: **no src-zone**
- Specify the destination zone name of the traffic: **dst-zone***dst-zone*
- Delete the destination zone name of the traffic: **no dst-zone**
- Specify the ingress interface name of the traffic: **ingress-if** *interface-name*
- Delete the ingress interface name of the traffic: **no ingress-if** *interface-name*
- Specify the egress interface name of the traffic: **egress-if** *interface-name*
- Delete the egress interface name of the traffic: **no egress-if** *interface-name*
- Specify the source IP address of the traffic: **src-ip** {*ip/netmask* | *ip-address netmask*}
- Delete the source IP address of the traffic: **no src-ip** {*ip/netmask* | *ip-address netmask*}
- Specify the destination IP address of the traffic: **dst-ip** {*ip/netmask* | *ip-address netmask*}
- Delete the destination IP address of the traffic: **no dst-ip** {*ip/netmask* | *ip-address netmask*}
- Specify the user and its AAA server: **user** *AAA-server user-name*
- Delete the users and its AAA server: **no user** *AAA-server user-name*
- Specify the user group and its AAA server: **user-group** *AAA-server usergroup-name*

- Delete the users group and its AAA server: **no user-group** *AAA-server usergroup-name*
- Specify the application or application group, including pre-defined application and user-defined application: **application** *app-name*
- Delete the application or application group, including pre-defined application and user-defined application: **no application** *app-name*
- Specify the name of the service or service group: **service** *service-name*
- Delete the name of the service or service group: **no service** *service-name*
- Specify the ToS field: **tos** *tos-value*
- Delete the ToS field: **no tos** *tos-value*
- Specify the VLAN information: **vlan** *vlan-id*
- Delete the VLAN information: **no vlan** *vlan-id*
- Specify the URL category: **url-category** *category-name*
- Delete the URL category: **no url-category** *category-name*

Configuring Traffic Management Actions for a Root Pipe

To configure traffic management actions for a root pipe, in the root pipe configuration mode, use the following actions:

pipe-rule {forward | backward} bandwidth {Kbps | Mbps | Gbps *bandwidth-value* [per-ip-min *min-value*] [per-ip-max *max-value* [delay *delay-time*]] [per-ip-using {src-ip | dst-ip}] [tos-marking *tos-value*] [mode aggressive [strength-level *level-value*]] [priority *value*]

pipe-rule {forward | backward} bandwidth {Kbps | Mbps | Gbps} [per-user-min *min-value*] [per-user-max *max-value* [delay *delay-time*]] [tos-marking *tos-value*] [mode aggressive [strength-level *level-value*]] [priority *value*]

pipe-rule {forward | backward} bandwidth {Kbps | Mbps | Gbps} *bandwidth-value* average-using {src-ip | dst-ip | user} [tos-marking *tos-value*] [mode aggressive [strength-level *level-value*]] [priority *value*]

- **forward** – Specify the traffic control actions to the traffic that matches the traffic matching conditions and whose direction is from the source to the destination.
- **backward** -Specify the traffic control actions to the traffic that matches the traffic matching conditions and whose direction is from the destination to the source.

- **bandwidth** {**Kbps** | **Mbps** | **Gbps**} - Specify the minimum bandwidth of the pipe. When selecting Kbps, the bandwidth ranges from 32 to 100,000,000. When selecting Mbps, the bandwidth ranges from 1 to 100,000. When selecting Gbps, the bandwidth ranges from 1 to 100. Mbps and Gbps can be used when configuring a sub pipe.

- **per-ip-min** *min-value* - Specify the minimum bandwidth of each IP. The value ranges from 32Kbps to 1,000,000Kbps.

- **per-ip-max** *max-value* - Specify the maximum bandwidth of each IP. The value ranges from 32Kbps to 1,000,000Kbps.

- **per-ip-using** {**src-ip**|**dst-ip**} - Limit the bandwidth to each source IP address or destination IP address. This configuration can take effect after you have configured the per-ip-min min-value and per-ip-max max-value parameters.

- **per-user-min** *min-value* - Specify the minimum bandwidth of each user. When selecting **Kbps**, the value ranges from 32Kbps to 10,000,000Kbps. When selecting **Mbps**, the value ranges from 1Mbps to 10,000Mbps.

- **per-user-max** *max-value* - Specify the maximum bandwidth of each user. When selecting **Kbps**, the value ranges from 32Kbps to 10,000,000Kbps. When selecting **Mbps**, the value ranges from 1Mbps to 10,000Mbps.

- **delay** *delay-time* − Specify the delay time, whose value ranges from 1 second to 3600 seconds. The maximum bandwidth limit of each IP/ user is not effective within the delay time range.

- **tos-marking** *tos-value* - Specify the TOS filed.

- **mode aggressive** [**strength-level** *level-value*] - Enable the peer quench function. By default, this function is disabled. According to the distributed bandwidth by the user, the peer quench function makes the traffic that arrives at the device be the same as the distributed bandwidth as possible as it can, which reduces the missed packets of the device. When the peer quench function is enabled, the default value of strength-level is 1, whose value ranges from 1 to 8. A bigger value represents a higher strength-level and a lesser lost of packets.

- **priority** *value* - Specify the priority of the pipe. The value ranges from 0 to 7. The default value is 7. A smaller value represents a higher priority and the system will first arrange the traffic in a a pipe with a higher priority and will first borrow the idle bandwidth from other pipes with a lower priority.

- **average-using** {**src-ip** | **dst-ip** | **user**} - Allocate the bandwidth equally to each source IP address or each destination IP address in the pipe.

Use the no form of the above command to delete the traffic management actions of a specified direction.

Note:

- You cannot limit the bandwidth to each user and each IP address at the same time.
- You cannot enable the peer quench function in the positive and negative traffic management direction at the same time. The peer quench function only be supported in a end-pipe.

Configuring Traffic Management Actions for a Sub Pipe

To configure traffic management actions for a sub pipe, in the root pipe configuration mode, use the following actions:

pipe-rule {forward | backward} {min | reserve-bandwidth} {percent | Kbps | Mbps | Gbps} *value* max {percent | Kbps | Mbps | Gbps} *max-value* [per-ip-min *min-value*] [per-ip-max *max-value* [delay *delay-time*]] [per-ip-using {src-ip | dst-ip}] [tos-marking *tos-value*] [mode aggressive [strength-level *level-value*]] [priority *value*]

pipe-rule {forward | backward} {min | reserve-bandwidth} {percent | Kbps | Mbps | Gbps} *min-value* max {percent | Kbps | Mbps | Gbps} *max-value* [per-user-min *min-value*] [per-user-max *max-value* [delay *delay-time*]] [tos-marking *tos-value*] [mode aggressive [strength-level *level-value*]] [priority *value*]

- **forward** – Specify the traffic control actions to the traffic that matches the traffic matching conditions and whose direction is from the source to the destination.
- **backward** - Specify the traffic control actions to the traffic that matches the traffic matching conditions and whose direction is from the destination to the source.
- **{min | reserve-bandwidth} {percent | Kbps | Mbps | Gbps}** *value* - Specify the minimum bandwidth of the pipe, or set the reserved bandwidth of the pipe. `min` represents the minimum bandwidth and **reserve-bandwidth** represents the reserved bandwidth. When configuring the minimum bandwidth or the reserved bandwidth, **percent**represents that the minimum percentage of the parent pipe bandwidth. The value ranges from 1 to 100. When selecting **Kbps**, the value ranges from 32Kbps to 100,000,000Kbps. When selecting **Mbps** the value ranges from 1Mbps to 100,000Mbps. When selecting **Gbps**, the value ranges from 1Gbps to 100Gbps.
- **max {percent | Kbps | Mbps | Gbps}** *max-value* - Specify the maximum bandwidth of the pipe or the maximum percentage of its parent pipe. **percent**represents that the maximum percentage of the parent pipe bandwidth. The value ranges from 1 to 100. When selecting **Kbps**,

the value ranges from 32Kbps to 100,000,000Kbps. When selecting **Mbps**, the value ranges from 1Mbps to 100,000Mbps. When selecting **Gbps**, the value ranges from 1Gbps to 100Gbps.

- **per-ip-min** *min-value* - Specify the minimum bandwidth of each IP address. When selecting Kbps, the values ranges from 32Kbps to 10,000,000Kbps. When selecting Mbps, the value ranges from 1Mbps to 10,000Mbps.
- **per-ip-max** *max-value* - Specify the maximum bandwidth of each IP address. When selecting Kbps, the values ranges from 32Kbps to 10,000,000Kbps. When selecting Mbps, the value ranges from 1Mbps to 10,000Mbps.
- **per-ip-using** {**src-ip**|**dst-ip**} - Specify which kind of IP addresses will be controlled by the bandwidth limit you configured by the per-ip-max max-value and per-ip-min min-value commands. src-ip represents the source IP address, and dst-ip represents the destination IP address.
- **per-user-min** *min-value* - Specify the minimum bandwidth of each user. The values ranges from 32Kbps to 1,000,000Kbps.
- **per-user-max** *max-value* - Specify the maximum bandwidth of each user. The values ranges from 32Kbps to 1,000,000Kbps.
- **delay** *delay-time* – Specify the delay time, whose value ranges from 1 second to 3600 seconds. The maximum bandwidth limit of each IP/ user is not effective within the delay time range.
- **tos-marking** *tos-value* - Specify the TOS filed.
- **mode aggressive** [**strength-level** *level-value*] - Enable the peer quench function. By default, this function is disabled. According to the distributed bandwidth by the user, the peer quench function makes the traffic that arrives at the device be the same as the distributed bandwidth as possible as it can, which reduces the missed packets of the device. When the peer quench function is enabled, the default value of strength-level is 1, which value ranges from 1 to 8. A bigger value represents a higher strength-level and a lesser lost of packets.
- **priority** *value* - Specify the priority of the pipe. The value ranges from 0 to 7. The default value is 7. A smaller value represents a higher priority and the system will first arrange the traffic in a pipe with a higher priority and will first borrow the idle bandwidth from other pipes with a lower priority.

Note:

- You cannot limit the bandwidth to each user and each IP address at the same time.

- You cannot enable the peer quench function in the positive and negative traffic management direction at the same time. The peer quench function only be supported in a end-pipe.

Configuring a Traffic Control Mode for a Root Pipe

A root pipe has the following three traffic control modes:

- Shaping mode: After configuring this mode, the system can limit the data transmission rate and smoothly forward the traffic. This mode supports the bandwidth borrowing and priority schedule for the traffic within the root pipe.
- Policing mode: After configuring this mode, the system will drop the traffic that exceeds the bandwidth limit. This mode does not support the bandwidth borrowing and priority schedule, and cannot guarantee the minimum bandwidth.
- Monitoring mode: After configuring this mode, the system will monitor the matched traffic, generate the statistics, and will not control the traffic.

Bandwidth borrowing: All sub pipes in a root pipe can lend the idle bandwidth to the pipes that are lack of bandwidth. The prerequisite is the bandwidth of themselves are enough to forward their traffic.

Priority schedule: When there is traffic congestion, the system will arrange the traffic to enter the waiting queue. You can set the traffic to have higher priority and the system will deal with the traffic in order of precedence.

By default, a root pipe uses the policing mode. To configure the traffic control mode of a root pipe, use the following command in the root pipe configuration mode:

qos-mode {police | shape | stat}

- **police** – Use the policing mode.
- **shape** – Use the shaping mode.
- **stat** – Use the monitoring mode.

Configuring a Schedule for a Root Pipe

You can specify a schedule entry for a root pipe and this root pipe will take effect within the specified time. To specify a schedule for a root pipe, in the root pipe configuration mode, use the following command:

schedule *schedule-name*

- schedule-name – Specify the name of the schedule entry.

Use the **no schedule** *schedule-name* command to cancel the schedule configuration.

> Tip: For more information on creating a schedule, see "Configuring Schedule" in the "System Management".

Configuring a Schedule for a Sub Pipe

You can specify a schedule entry for a sub pipe and this sub pipe will take effect within the specified time. To specify a schedule for a sub pipe, in the sub pipe configuration mode, use the following command:

schedule *schedule-name*

- *schedule-name* – Specify the name of the schedule entry.

Use the **no schedule** *schedule-name* command to cancel the schedule configuration.

> Tip: For more information on creating a schedule, see "Configuring Schedule" in the "System Management".

Viewing Configurations of Traffic Control Levels and Pipes

To view the configurations of traffic control levels and pipes, use the following command in any mode:

show qos-engine {**first** | **second**} [**root-pipe** *pipe-name*]

- **first** – View the configurations of the first-level traffic control.
- **second** - View the configurations of the second-level traffic control.
- **root-pipe** *pipe-name* - View the configurations of the specified root pipe.

Load Balancing

This chapter introduces the following topics:

- server load balancing
- link load balancing

Server Load Balancing

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 perform the server load balance:

- Distribute the traffic to the specified port of each intranet server. This is applicable to the scenario that different intranet servers meanwhile and individually provide the same service via specified port.
- 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.

Adding/Deleting SLB Server Pool

A global SLB server pool is a database which stores the internal server IP ranges and the server names. The mapping between a server IP and the server name is called an SLB server pool entry.

The global SLB server pool includes SLB server pool entries. To add an entry into the global SLB server pool, under configuration mode, use the following command:

slb-server-pool *pool-name*

- *pool-name* - Specify a name for SLB server pool entry.

To delete an entry, use the command:

no slb-server-pool *pool-name*

Note: Before deleting an entry, make sure this entry has not binding with any other items.

Configuring Parameters for SLB Server Pool Entry

Parameters of an SLB Server Pool Entry includes IP range, port, weight, and maximum connections. There are two types of IP range in SLB server pool

- IP address/netmask, e.g. 10.100.2.0/24
- IP address range, e.g. 10.100.2.3 – 10.100.2.100

To add members and configure detailed parameters for an SLB server pool entry, under SLB server pool configuration mode, use the following command. You can add up to 256 members.

server {**ip** *ip/netmask* | **ip-range** *min-ip* [*max-ip*]} [**port** *port-num*]{**weight-per-server** *weight-num*} [**max-connection-per-server** *max-num*]

- **ip** *ip-address* – Specify IP address and netmaks.
- **ip-range** *start-ip* [*max-ip*] – Specify IP address range, *start-ip* is start IP address and *end-ip* is end IP address.
- **port** *port-num* – Specify port number.
- **weight-per-server** *weight-num* – Specify the weight in load balance. The range is from 1 to 255, and default value is 1.
- **max-connection-per-server** *max-num* – Specify the maximum connection number for a server. The range is from 1 to 1,000,000,000 and default value is 0, which mean no limit on maximum connection.

To delete an entry in SLB server pool, use the following command:

no server {**ip** *ip/netmask* | **ip-range** *min-ip* [*max-ip*]} [**port** *port-num*] {**weight-per-server***weight-num*} [**max-connection-per-server** *max-num*]

Assigning an Algorithm for SLB

The system supports three types of SLB algorithms: weighted hash algorithm, weighted round robin, and weighted least connection. By default, weight hash algorithm is used.

To apply an algorithm, under SLB server pool configuration mode, use the following command:

load-balance-algorithm {**weighted-hash** | **weighted-round-robin** [**sticky**] | **weighted-least-connection** [**sticky**]}

- **weighted-hash** - Specify weighted hash as SLB algorithm.
- **weighted-round-robin** - Specify weighted round robin as SLB algorithm.
- **weighted-least-connection** - Specify weighted least connection as SLB algorithm.
- **sticky** – If you use sticky, all sessions from the same source IP will be mapped to one server.

Adding/Deleting Track Rule for SLB

To add a track rule for SLB, under SLB server pool configuration mode, use the following command:

monitor{**track-ping** | {**track-tcp** |**track-udp** }[**port** *port-num*]} **interval** *interval-value* **threshold** *number* **weight** *weight-num*

- **track-ping** - Specify the track protocol type as PING.
- **track-tcp** - Specify the track protocol type as TCP.

- **track-udp** - Specify the track protocol type as UDP.
- **port** *port-num* - Specify the track port number. The range is from 0 to 65535.
  - When the members in the SLB server pool have the same IP address and different ports, you don’ t need to specify the port when configuring the track rule. The system will track each IP address and its port in the SLB server pool.
  - When there is a member whose port is not configured exists in the SLB sever pool, you must specify the port when configuring the track rule. The system will track the specified port of the IP addresses in the SLB server pool.
  - When the members in the SLB server pool are all configured with IP addresses and ports and these configured IP addresses are different from each other, you can select whether to specify the port when configuring the track rule. If specified, the system will track the specified port of these IP addresses. If not, the system will track the configured ports of the IP addresses of the members.
- **interval** *interval-value* - Specify the interval of track packets. The range is 1 to 255.
- **threshold** *number* - Specify the threshold which determines if track object files or not. If the system cannot get respond within the threshold packet number, the track object will be deemed as failure, i.e. the object cannot be reached. The range of threshold is 1 to 255. The default number is 3.
- **weight** *weight-num* - Specify the weight of the current track object. The weight determines if the whole track is failed or not when this object fails. The weight range is 1 to 255.

To delete an SLB track rule, use the no command below:

no monitor{**track-ping** | {**track-tcp** |**track-udp** }[**port** *port-num*]}

Configuring Threshold Value

When the weight sum of all track objects exceed the threshold, the server is deemed as failed. To specify the threshold, under SLB server pool configuration mode, use the following command:

monitor threshold *number*

- *number* - Specify threshold value. The range is from 1 to 255.

Binding SLB Server Pool Entry to DNAT Rule

SLB server pool entry can be bound to DNAT rule to achieve server load balancing.

To bind an SLB server pool entry to a DNAT rule, under VRouter configuration mode, use the following command:

dnatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] **trans-to** *trans-to-address* [**slb-server-pool** *pool-name*][**port** *port*] [**load-balance**] [**track-tcp** *port*] [**track-ping**] [**log**] [**group** *group-id*] [**description** *description*]

- **slb-server-pool** *pool-name* - Specify the name of SLB server pool entry.

Tip: For information about how to set up DNAT rules, see "Creating a DNAT Rule" in the "Firewall".

Viewing SLB Status

To view SLB server pool entry and track rule, under any mode, use the following command:

show slb-server-pool *pool-name*

- *pool-name* - Specify SLB server pool entry name.

To view SLB server, under any mode, use the following command:

show load-balance server

To view SLB DNAT:

show load-balance slb-server-pool *pool-name*

To view SLB DNAT rule, under any mode, use the following command:

show load-balance rule

Link Load Balancing

For the multiple ISP links, system uses the real-time link monitoring technology and dynamic link detection technology to reasonably distribute to different traffic links. It reduces the network delay, jitter and packet loss rate, so as to the network obtains a more balanced bandwidth utilization on each link.

You can enable the LLB(Link Load Balance) function in the outbound and inbound directions respectively. In the outbound and inbound directions, two different dynamic link detection techniques are used, real-time link monitoring technology and SmartDNS technology. Finally according to the detection results, automatic load balancing implementation flow.

Inbound LLB

After enabling LLB for inbound traffic, the system will resolve domains to different IPs based on the sources of DNS requests, and return IPs for different ISPs to the corresponding users who initiate the requests, thus reducing accesses 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.

Enabling SmartDNS

SmartDNS is enabled by default. To disable or enable the function, in the global configuration mode, use the following command:

llb inbound smartdns {disable | enable}

- **disable** – Disables SmartDNS.
- **enable** – Enables SmartDNS.

Configuring a SmartDNS Rule Table

The configuration of SmartDNS rule table includes creating a rule table, specifying the domain name, return IP and matching rule. The system resolves domains names into IPs of different ISP links based on the matching rule.

Creating a SmartDNS Rule Table

To create a SmartDNS rule table, in the global configuration mode, use the following command:

llb inbound smartdns *name*

- *name* – Creates a SmartDNS rule table, and enters SmartDNS rule table configuration mode. If the specified name already exists, the system will directly enters the SmartDNS rule table configuration mode. The system supports up to 2500 SmartDNS rule tables.

To delete the specified SmartDNS rule table, in the global configuration mode, use the following command:

no llb inbound smartdns *name*

Specifying the Domain Name

To specify the domain name that will be resolved smartly, in the SmartDNS rule table configuration mode, use the following command:

domain *domain-name*

- *domain-name* - Specifies the domain name that will be resolved smartly. The length is 1 to 255 characters.

Repeat the above command to add multiple domain names to the SmartDNS rule table. Each rule table supports up to 64 domain names (case insensitive).

To delete the specified domain name, in the SmartDNS rule table configuration mode, use the following command:

no domain *domain-name*

Specifying the Return IP

You can specify different return IPs for requests originating from different ISP links. The system determines the request sources based on the addresses in the ISP route (ISP static address). If the address of request source matches any entry of the above addresses, then the system will return the specified IP. In the SmartDNS rule table configuration mode, use the following command:

ip *ip-address* **isp** *isp-name* [**interface** *interface-name*] [**weight** *value*]

- *ip-address* - Specifies the return IP. You can configure up to 64 IPs for a domain name.
- **isp** *isp-name* - Specifies the ISP to which the request source address will be matched. If the source address matches any address entry of the ISP, the system will return the specified IP (**ip** *ip-address*). *isp-name* should be a predefined or user-defined ISP profile in the system. Each ISP can correspond to up to 16 IPs.
- **interface** *interface-name* - Specifies the inbound interface for the return IP address. System will judge whether the return IP address is valid according to the track result or the protocol status of the inbound interface. Only the valid IP address will be returned to the request source. When there's track object configured on the inbound interface, if the track status is successful, the return IP address is valid. Otherwise the IP address is invalid. When there's no track object configured on inbound interface, if the protocol state of the interface is UP, the return IP address is valid. Otherwise the IP address is invalid. If you don't specify the inbound interface for the return IP address, the return IP address is always valid.
- **weight** *value* – Specifies the weight of the return IP. The value range is 1 to 100. The default value is 1. In the SmartDNS rule table, one domain name might correspond to multiple IPs. The system will sort the IPs based on the weight and then return to the users.

To delete the specified return IP address, in the SmartDNS rule table configuration mode, use the following command:

no ip *ip-address*

Note:

- The ISP route being referenced by the SmartDNS rule table cannot be deleted. For more information about ISP route, see "ISP Route" in the "Route".
- Before completing the configuration of domain name, return IP, etc., the new SmartDNS rule table will be disabled.

Outbound LLB

By monitoring the delay, jitter, packet loss rate and bandwidth utilization of each link in real-time, the system can intelligently route and dynamically adjust the traffic load of each link. 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.

To create or configure an LLB profile, use the following command in the global configuration mode:

llb profile *llb-profile-name*

- *llb-profile-name* - Specifies the name of the LLB profile. After you execute this command, the system creates an LLB profile with the specified name and enters the LLB profile configuration mode. If the specified name already exists, the system will directly enter the LLB profile configuration mode.

To delete the specified LLB profile, in the global configuration mode, use the command: **no llb profile** *llb-profile-name*.

You can configure the related parameters as required. In LLB profile configuration mode, use the following command:

detect { **netmask** {*A.B.C.D* | *num*} | **threshold** *value*}

- **netmask** {*A.B.C.D* | *num*} - Specifies the destination IP segment of the detect task. The system carries out real-time monitoring of the traffic flow of the network segment, and adjusts the traffic load balance according to the monitoring and statistical results. The system supports two formats, A.B.C.D or num. The value of A.B.C.D ranges from 255.0.0.0 to 255.255.255.255, and the default value is 255.255.240.0; num ranges from 8 to 32 and defaults to 28.

- **threshold** *value* - Specifies the bandwidth utilization threshold of the interface. When the rate does not exceed the threshold by the interface bandwidth, the system will only analysis delay, jitter and packet loss rate to dynamically adjust the routing link; when the rate exceeds the threshold by the interface bandwidth, system will analysis of each link bandwidth utilization rate of the parameters at the same time to adjust the routing method. Value ranges from 0 to 100 (0% to 100%) and defaults to 60.

To configure the load balancing direction, use the following command:

bandwidth-balance-direction {**bidirection** | **downstream** | **upstream**}

- **bidirection** - The system will compare the maximum bandwidth utilization ratio with the bandwidth utilization threshold in the two directions of data flow into and out, and then adjust the routing method.
- **downstream** - The system will compare the bandwidth utilization of the data stream into the bandwidth utilization threshold, and then adjust the routing method.
- **upstream** - The system will compare the bandwidth utilization of the data stream out the bandwidth utilization threshold, and then adjust the routing method.

To configure the load balancing mode, use the following command:

mode {**compatibility** | **performance**}

- **compatibility** - Configure the load balancing mode to work in high compatibility mode. When the link load changes, the system does not switch the link frequently, but ensures that the service is as far as possible on the previous link, such as banking services.
- **performance** - Configure the load balancing mode for high-performance. In this mode, the system adjusts link to keep the link balance as fast as possible.

For more information about configuring load balancing, use the following command:

description *description*

- *description* – Configure Additional details of llb profile.

To cancel the configuration description, use the command: **no description**.

Configuring LLB Rule

LLB Profile and the route is bound to the formation of LLB rules, it can really take effect, currently support binding destination routing (DBR) and policy-based routing (PBR). To configure LLB rules, use the following command in global mode:

llb rule *rule-name* {**pbr** *pbr-name* **id** *match-id* | **dbr** [**vrouter** *vr-name*] {*A.B.C.D/M* | *A.B.C.D A.B.C.D* }} **profile** *profile-name*

- *rule-name* - Specify the name of llb rule.
- **pbr** *pbr-name* - Specify the name of PBR.
- **id** *match-id* - Specify the match id of PBR.
- **dbr vrouter** *vr-name* - Specify the vroute's name of DBR.
- *A.B.C.D/M* | *A.B.C.D A.B.C.D* - Specifies the Vrouter destination address. The device supports two modes, A.B.C.D / M or A.B.C.D A.B.C.D, for example, 1.1.1.0/24 or 1.1.1.0 255.255.255.0.
- **profile** *profile-name* - Specifies the bound LLB profile.

To delete the specified LLB rule, in the global configuration mode, use the command: **no llb rule** *llb-rule-name*.

Viewing LLB Configuration

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

show llb {**profile** [*profile-name*]| **rule** [*rule-name*]}

- **profile** [*profile-name*] – Shows the profile of outbound LLB.
- **rule** [*rule-name*] – Shows the rule of outbound LLB.

To view the configuration of inbound or the specified SmartDNS rule table, in any mode, use the following command:

show llb inbound [**smartdns** *name*]

- **inbound** - Show the configuration of inbound LLB.
- **smartdns** *name* - Specifies the name of SmartDNS rule table.

For example, to view the configuration of SmartDNS rule table named test, use the command **show llb inbound smartdns** *test*. Below is a return example:

```
hostname# show llb inbound smartdns test
domain:domain name; IP: ip address; ISP: isp name; IF: interface;
PROXY: proximity address book status; E: enable; D:disable
TRACK: track object name; W: ip weight; S:ip status;A:active; I: inactive
==============================================================
====================
--------------------------------------------------------------------------------
table name: test
table status: enable
domain count: 1
rule count: 1
domains: www.test.com;
ip addresses:
--------------------------------------------------------------------------------
IP ISP IF PROX TRACK W S
1.1.1.1 China-telecom ethernet0/1 E 1 I
==============================================================
==================
```

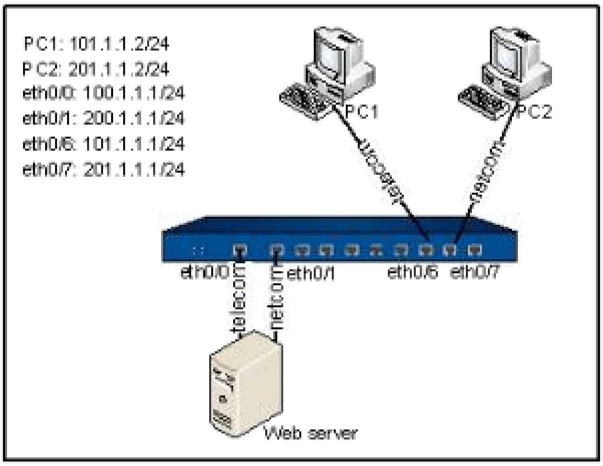
- For more information about the track object under TRACK, see "Configuring a Track Object" in the "System Management".
- The rule status displayed under S can be active or inactive, specifically relying on the configured interface and track object on the interface:
  - If only ISP (**isp** isp-name) is configured while interface (**interface** *interface-name*) is not configured, then the rule status will always be active;
  - If interface (**interface** *interface-name*) is configured but it is not configured with track object, then the rule status will be active when the protocol status of the interface is UP, and will be inactive when the protocol status is DOWN;
  - If interface (**interface** *interface-name*) is configured and it is configured with track object, then the rule status will be active when track succeeds, and will be inactive when track fails.

Example of Configuring LLB

This section describes an inbound LLB configuration example.

Requirement

Ethernet0/6 and ethernet0/7 are connected to telecom and netcom links respectively. With inbound LLB enabled, the device will return the IP address defined in the ISP static address named telecom after receiving a DNS request from netcom users, and will return the IP address defined in the ISP static address named telecom after receiving a DNS request from telecom users. The network topology is shown below:



Configuration Steps

Configurations of interfaces are omitted. Only the configurations of ISP information and inbound LLB are provided.

Step 1: Configure ISP information

```
hostname(config)# isp-network telecom

hostname(config-isp)# 101.1.1.0/24

hostname(config-isp)# exit

hostname(config)# isp-network netcom

hostname(config-isp)# 201.1.1.0/24

hostname(config-isp)# exit
```

Step 2: Enable SmartDNS and configure SmartDNS rules

```
hostname(config)# llb inbound smartdns enable

hostname(config)# llb inbound smartdns test
hostname(config-llb-smartdns)# domain www.test.com
hostname(config-llb-smartdns)# ip 100.1.1.2 isp telecom interface ethernet0/0 weight 10
hostname(config-llb-smartdns)# ip 200.1.1.2 isp netcom interface ethernet0/1 weight 10
hostname(config-llb-smartdns)# exit
```

Step 3: Confirm the above configurations have taken effect by command **show**

```
hostname(config)# show isp-network all
ISP telecom status: Active
Binding to nexthop: 0
Subnet(IP/Netmask): 1
101.1.1.0/24
ISP netcom status: Active
Binding to nexthop: 0
Subnet(IP/Netmask): 1
201.1.1.0/24
hostname(config)# show llb inbound smart test
domain:domain name; IP: ip address; ISP: isp name; IF: interface;
PROXY: proximity address book status; E: enable; D:disable
TRACK: track object name; W: ip weight; S:ip status;A:active;
I: inactive
==========================================================================
======
------------------------------------------------------------------------------
name: test
domain count: 1
rule count: 2
status: enable
domains: www.test.com;
ip addresses:
```

```
---------------------------------------------------------------------------
ID IP ISP IF PROX TRACK W S
1 100.1.1.2 telecom ethernet0/0 D 10 A
3 200.1.1.2 netcom ethernet0/1 D 10 A
================================================================
=======
```

When PC1 requests www.test.com, the device will return the IP address for telecom link (100.1.1.2); when PC2 requests www.test.com, the device will return the IP address for netcom link (200.1.1.2).

Session Limit

FS devices support the zone-based session limit function. You can limit the session number and control the new session ramp-up rate for the source IP address, destination address, specified IP address, protocol, application, role or user in the security zone, thereby to protect against DoS attacks and control the bandwidth of applications, such as IM or P2P.

Creating a Session Limit Rule

To create a session limit rule, in the security zone configuration mode, use the following command:

ad session-limit [**id** *id*] {{**src-ip** *address-entry* **dst-ip** *address-entry* | **ip** *address-entry* } [**protocol** *protocol-id*] [**application** *application-name*] [**role** *role-name* | **user** *aaa-server-name user-name* | **user-group** *aaa-server-name user-group-name*]} {**session** {**unlimit** | **max** *number* [**per-srcip** | **per-dstip** | **per-ip**] | **per-user**} | **ramp-rate max** *number*} [**schedule** *schedule-name*]

- **id** *id* - Specifies the ID of the session limit rule.
- **src-ip** *address-entry* - Limits the session number of the source IP address in the security zone. *address-entry* is the IP range of *src-ip*. This parameter should be an address entry defined in the address book.
- **dst-ip** *address-entry* - Limits the session number of the destination IP address in the security zone. *address-entry* is the IP range of *dst-ip*. This parameter should be an address entry defined in the address book.
- **ip** *address-entry* - Limits the session number of the specified IP address in the security zone. *address-entry* is the IP range of **ip**. This parameter should be an address entry defined in the address book.

- **protocol** *protocol-id* - Limits the session numbers of the specified protocol in the security zone.
- **application** *application-name* - Limits the session numbers of the specified application in the security zone.
- **role** *role-name* - Limits the session number of the specified role in the security zone.
- **user** *aaa-server-name user-name* - Limits the session number of the specified user in the security zone. *aaa-server-name* is the AAA server the user belongs to.
- **user-group** *aaa-server-name user-group-name* - Limits the session number of the specified user group in the security zone.*aaa-server-name* is the AAA server the user group belongs to.
- **session** {**unlimit** | **max** *number* [**per-srcip** | **per-dstip** | **per-ip**] | **per-user**} − Specifies the maximum session number for the IP address or role. **unlimit** indicates no session limit. **session max** *number* specifies the maximum session number for all the IP addresses defined in the address entry or all the users defined in the role; if **per-srcip, per-dstip, per-ip** or **per-user** is used, **session max** *number* specifies the maximum session number for each IP address or each user defined in the role. **per-srcip, per-dstip, per-ip** and **per-user** should be correspond to **src-ip, dst-ip, ip** and **role** respectively. For example, only when **src-ip** is specified can you choose **per-srcip**.
- **ramp-rate max** *number* - Specifies the maximum new sessions that can be established every 5 seconds for the IP address or role.
- **schedule** *schedule-name* - Specifies an schedule during which the session limit rule will take effect.

Note:Session limit function support IPv4 address and IPv6 address. If the IPv6 function for interface is enabled, you can configure the address of IPv6 type. The type of the source address entry and the destination address entry must keep same.

To delete the session limit rule, in the security zone configuration mode, use the following command:

no ad session-limit id *id*

- **id** *id* - The session limit rule ID of the security zone. To view the rule ID, use the command **show session-limit**.

With session limit configured, FSOS will drop the sessions that exceeds the maximum session number. To view the statistics on the dropped sessions, use the command **show session-limit**. To clear the statistics on the dropped sessions in the specified session limit rule, in any mode, use the following command:

clear session-limit id *id* **statistics**

- **id** *id* – Specifies the rule ID. The statistics on the dropped session in the specified session limit rule will be cleared.

Note: After Full-cone NAT is enabled on the device, the destination IP address in the session limit refers to the IP address before DNAT translation. For more information about Full-cone NAT, see "Full-cone NAT" in the "Firewall".

Viewing Session Limit

To view the configuration information of the session limit after configuring session limit, in any mode, use the following command:

show session-limit

Chapter 11 Threat Prevention

The chapter introduces the following topics:

- "Attack Defense" describes the common network attack concepts, how to configure Attack Defense, and examples of Attack Defense.
- "IPS" explains how to detect and protect mainstream application layer protocols (DNS, FTP, POP3, SMTP, TELNET, MYSQL, MSSQL, ORACLE, NETBIOS), against web-based attacks and common Trojan attacks.
- "Perimeter Traffic Filtering" describes how to filter the perimeter traffic based on known IP of black/white list, take block action on the malicious traffic that hits the blacklist, and how to update the IP reputation database.
- "Geolocation Information Database" describes how to update the geolocation information database.

Attack Defense

There are various inevitable attacks in networks, such as compromise or sabotage of servers, sensitive data theft, service intervention, or even direct network device sabotage that causes service anomaly or interruption. Security gates, as network security devices, must be designed with attack defense functions to detect various types of network attacks, and take appropriate actions to protect Intranet against malicious attacks, thus assuring the normal operation of the Intranet and systems. Devices provide attack defense functions based on security zones.

Common Network Attacks

This section describes some common network attacks. Devices can take appropriate actions against network attacks to assure the security of your network systems.

IP Address Spoofing

IP address spoofing is a technology used to gain unauthorized accesses to computers. An attacker sends packets with a forged IP address to a computer, and the packets are disguised as if they were from a real host. For applications that implement validation based on IP addresses, such an attack allows unauthorized users to gain access to the attacked system. The attacked system might be compromised even if the response packets cannot reach the attacker.

ARP Spoofing

LAN transmission network traffic based on MAC addresses. ARP spoofing attack is by filling in the wrong MAC address and IP address , to make a wrong corresponding relationship of the target host's ARP cache table. Follow-up will lead to the wrong destination host IP packets , and packet network unreasonable target resources are stolen.

Land Attack

In a land attack, the attacker carefully crafts a packet and sets its source and destination address to the address of the server that will be attacked. In such a condition the victim server will send a message to its own address, and this address will also return a response and establish a Null connection. Each of such connections will be maintained until timeout. Many servers will crash under Land attacks.

Smurf Attack

Smurf attacks consist of two types: basic attack and advanced attack. A basic Smurf attack is used to attack a network by setting the destination address of ICMP ECHO packets to the broadcast address of the attacked network. In such a condition all the hosts within the network will send their own response to the ICMP request, leading to network congestion. An advanced Smurf attack is mainly used to attack a target host by setting the source address of ICMP ECHO packets to the address of the attacked host, eventually leading to host crash. Theoretically, the more hosts in a network, the better the attacking effect will be.

Fraggle Attack

A fraggle attack is quite similar to a Smurf attack. The only difference is the attacking vector of fraggle is UDP packets.

Teardrop Attack

Teardrop attack is a denial of service attack. Is based on the method of attack morbid fragmented UDP packets, which works by sending multiple fragmented IP packets to the attacker is (IP fragmented packets include the fragmented packets belong to which the packet and the packet the location and other information) , some operating systems contain overlapping offset when received fragmented packets will forge a system crash , reboot and so on.

WinNuke Attack

A WinNuke attack sends OOB (out-of-band) packets to the NetBIOS port (139) of a Windows system, leading to NetBIOS fragment overlap and host crash. Another attacking vector is ICMP fragment. Generally an ICMP packet will not be fragmented; therefore many systems cannot properly process ICMP fragments. If your system receives any ICMP fragment, it's almost certain that the system is under attack.

SYN Flood

Due to resource limitations, a server will only permit a certain number of TCP connections. SYN Flood just makes use of this weakness. During the attack an attacker will craft a SYN packet, set its source address to a forged or non-existing address, and initiate a connection to a server. Typically the server should reply the SYN packet with SYN-ACK, while for such a carefully crafted SYN packet, the client will not send any ACK for the SYN-ACK packet, leading to a half-open connection. The attacker can send large amount of such packets to the attacked host and establish equally large number of half-open connections until timeout. As a result, resources will be exhausted and normal accesses will be blocked. In the environment of unlimited connections, SYN Flood will exhaust all the available memory and other resources of the system.

ICMP Flood and UDP Flood

An ICMP Flood/UDP Flood attack sends huge amount of ICMP messages (such as ping)/UDP packets to a target within a short period and requests for response. Due to the heavy load, the attacked target cannot complete its normal transmission task.

IP Address Sweep and Port Scan

This kind of attack makes a reconnaissance of the destination address and port via scanners, and determines the existence from the response. By IP address sweep or port scan, an attacker can determine which systems are alive and connected to the target network, and which ports are used by the hosts to provide services.

Ping of Death Attack

Ping of Death is designed to attack systems by some over-sized ICMP packets. The field length of an IP packet is 16 bits, which means the max length of an IP packet is 65535 bytes. For an ICMP response packet, if the data length is larger than 65507 bytes, the total length of ICMP data, IP header (20 bytes) and ICMP header (8 bytes) will be larger than 65535 bytes. Some routers or systems cannot properly process such a packet, and might result in crash, system down or reboot.

IP Fragment Attack

An attacker sends the victim an IP datagram with an offset smaller than 5 but greater than 0, which causes the victim to malfunction or crash.

IP Option Attack

An attacker sends IP datagrams in which the IP options are abnormal. This attack intends to probe the network topology. The target system will break down if it is incapable of processing error packets.

Huge ICMP Packet Attack

An attacker sends large ICMP packets to crash the victim. Large ICMP packets can cause memory allocation error and crash the protocol stack.

TCP Flag Attack

An attacker sends packets with defective TCP flags to probe the operating system of the target host. Different operating systems process unconventional TCP flags differently. The target system will break down if it processes this type of packets incorrectly.

DNS Query Flood Attack

The DNS server processes and replies all DNS queries that it receives. A DNS flood attacker sends a large number of forged DNS queries. This attack consumes the bandwidth and resources of the DNS server, which prevents the server from processing and replying legal DNS queries.

TCP Split Handshake Attack

When a client establishes TCP connection with a malicious TCP server, the TCP server responses with a fake SYN package and uses this fake one to initialize the TCP connection with the client. After establishing the TCP connection, the malicious TCP server switches its role and becomes the client side of the TCP connection. Thus, the malicious traffic might enter into the intranet.

Configuring Attack Defense

By default only part of the attack defense functions in the untrust zone of the device are enabled, including IP address spoofing attack defense, IP address sweep attack defense, port scan attack defense, ICMP Flood attack defense, SYN Flood attack defense, UDP flood attack defense, WinNuke attack defense, Ping of Death attack defense, Teardrop attack defense, IP Option attack defense, IP Fragment attack defense, IP Directed Broadcast attack defense and Land attack defense. To enable all the attack defense functions, in the security zone configuration mode, use the following command:

```
ad all
```

To disable all the attack defense functions in the security zone, in the security zone configuration mode, use the command **no ad all**.

You can configure the parameters of the above attack defense functions as needed. The attack defense configurations of FS devices include:

- Configuring IP address sweep attack defense
- Configuring port scan attack defense
- Configuring IP address spoofing attack defense

- Configuring SYN Flood attack defense
- Configuring SYN-Proxy
- Configuring ICMP Flood attack defense
- Configuring UDP Flood attack defense
- Configuring Large ICMP packet attack defense
- Configuring WinNuke attack defense
- Configuring Ping of Death attack defense
- Configuring Teardrop attack defense
- Configuring IP Option attack defense
- Configuring TCP option anomaly attack defense
- Configuring Land attack defense
- Configuring IP fragment attack defense
- Configuring Smurf and fraggle attack defense
- Configuring ARP spoofing attack defense
- Configuring DNS Query Flood attack defense
- Viewing the attack defense configurations of the security zone and statistics

Configuring IP Address Sweep Attack Defense

You can enable or disable IP address sweep attack defense for each security zone individually, and configure the time threshold and action for IP address sweep attacks. To configure the IP sweep scan attack defense for the specified security zone, in the security zone configuration mode, use the following command:

ad ip-sweep [**threshold** *value*| **action** {**alarm** | **drop**}]

- **ad ip-sweep** – Enables IP address sweep attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad ip-sweep**.
- **threshold** *value* – Specifies the time threshold for IP address sweep. If over 10 ICMP packets from one single source IP address are sent to different hosts within the period specified by the threshold, system will identify them as an IP address sweep attack. The value range is 1 to 5000 milliseconds. The default value is 1. To restore to the default value, use the command **no ad ip-sweep threshold**.

- **action** {**alarm** | **drop**} – Specifies the action for IP address sweep attacks. **alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Only permits 10 IMCP packets originating from one single source IP address while destined to different hosts to pass through during the specified period (**threshold** *value*), and also give an alarm. All the excessive packets of the same type will be dropped during this period. The default action is drop. To restore to the default action, use the command **no ad ip-sweep action**.

Configuring Port Scan Attack Defense

You can enable or disable port scan attack defense for each security zone individually, and configure the time threshold and action for the port scan attacks. To configure the port scan attack defense for the specified security zone, in the security zone configuration mode, use the following command:

ad port-scan [**threshold** *value* | **action** {**alarm** | **drop**}]

- **ad port-scan** – Enables port scan attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command**no ad port-scan**.

- **threshold** *value* – Specifies the time threshold for port scan. If over 10 TCP SYN packets are sent to different ports of one single destination address by the same source IP within the period specified by the threshold, system will identify them as a port scan attack. The value range is 1 to 5000 milliseconds. The default value is 1. To restore to the default value, in the security zone configuration mode, use the command **no ad port-scan threshold**.

- **action** {**alarm** | **drop**} – Specifies the action for port scan attacks. **alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Only permits 10 TCP SYN packets destined to different ports of one single destination address to pass through during the specified period (**threshold** *value*), and also gives an alarm. All the excessive packets of the same type will be dropped during this period. The default action is drop. To restore to the default action, use the command **no ad port-scan action**.

Configuring IP Address Spoofing Attack Defense

System can defend against Layer 3 IP address spoofing attacks. After enabling the Layer 3 IP address spoofing attack defense function, when a packet is passing through the device, system will trace out the source IP address, and take different actions based on the traceout results, including:

- If the security zone of the packet destined to the device (with this IP as its source address) is the same as the security zone of the packet originating from the device (with this IP as the destination address), then system will permit the packet to pass through. You can identify security zone of the packet originating from the device based on the traceout results.

- Vice versa, system will identify the packet as an abnormal packet, and give an alarm and drop the packet.

To enable Layer 3 IP address spoofing attack defense for a security zone, in the Layer 3 security zone configuration mode, use the following command:

ad ip-spoofing

To disable Layer 3 IP address spoofing attack defense for a security zone, in the Layer 3 security zone configuration mode, use the command **no ad ip-spoofing**.

Configuring SYN Flood Attack Defense

You can enable or disable SYN flood attack defense for each security zone individually, and configure the packet number threshold and actions for the SYN flood attacks. To configure SYN flood attack defense for the specified security zone, in the security zone configuration mode, use the following command:

ad syn-flood [**source-threshold** *number* | **destination-threshold** [**ip-based** | **port-based**] *number* | **destination** [**ip-based** | **port-based** [**address-book** *address-entry* | *A.B.C.D/M*] | **action** {**alarm** | **drop**}]

- **ad syn-flood** – Enables SYN flood attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad syn-flood**.
- **source-threshold** *number* – Specifies a threshold for outbound SYN packets (ignoring the destination IP address and port number). If the number of outbound SYN packets originating from one single source IP address per second exceeds the threshold, system will identify the traffic as a SYN flood. The value range is 0 to 50000. The default value is 1500. The value of 0 indicates the source threshold is void. To restore to the default value, use the command **no ad syn-flood source-threshold**.
- **destination-threshold** [**ip-based** | **port-based**] *number* – Specifies a threshold for inbound SYN packets destined to one single destination IP address (**ip-based**) or one single destination port of the IP address (**port-based**). If not specified, the system will use ip-based by default. If the number of inbound SYN packets destined to one single destination IP address or one single destination port per second exceeds the threshold, system will identify the traffic as a SYN flood. The value range is 0 to 50000. The default value is 1500. The value of 0 indicates the destination threshold is void. To restore to the default value, use the command **no ad syn-flood destination-threshold** [**ip-base** | **port-base**].
- **destination** [**ip-based** | **port-based** [**address-book** *address-entry* | *A.B.C.D/M*] – Enables **ip-based** or **port-based** SYN flood attack defense. If not specified, the system will use ip-based by default. To enable port-based SYN Flood attack defense for a specific segment, use

the parameter **address-book** *address-entry* | *A.B.C.D/M*. The SYN Flood attack defense for other segments will be based on the IP addresses. The value range of the destination IP mask is 24 to 32. To cancel the configuration, use the command **no ad syn-flood destination**.

- **action** {**alarm** | **drop**} – Specifies the action for SYN Flood attacks. **alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Only permits the specified number (**source-threshold** *number* | **destination-threshold** *number*) of SYN packets to pass through, and also give an alarm; if source threshold and destination threshold are also configured, system will first detect if the traffic is a destination SYN flood attack: if so, system will drop the packets and give an alarm, if not, system will continue to detect if the traffic is a source SYN attack; if so, system will drop the packets and give an alarm. The default action is drop. To restore to the default action, use the command**no ad syn-flood action**.

Configuring SYN-Proxy

SYN-Proxy is designed to defend against SYN flood attacks in combination with ad syn-flood. When both ad syn-flood and SYN proxy are enabled, SYN proxy will act on the packets that have already passed the detections of ad syn-flood.

The FS devices support SYN-Cookie, a stateless SYN-Proxy mechanism.

To configure the SYN-Proxy and the SYN-Cookie functions for the specified security zone, in the security zone configuration mode, use the following command:

ad syn-proxy [**min-proxy-rate** *number* | **max-proxy-rate** *number* | **proxy-timeout** number | cookie]

- **ad syn-proxy** – Enables SYN-Proxy for a security zone to defend against SYN Flood attacks. To disable the function, in the security zone configuration mode, use the command **no ad syn-proxy**.

- **min-proxy-rate** *number* – Specifies the minimum number for SYN packets that will trigger SYN proxy or SYN-Cookie (if enabled by cookie). If the number of inbound SYN packets destined to one single port of one single destination IP address per second exceeds the specified value, system will trigger SYN proxy or SYN-Cookie. The value range is 0 to 50000. The default value is 1000. To restore to the default value, use the command**no ad syn-proxy min-proxy-rate**.

- **max-proxy-rate** *number* – Specifies the maximum number for SYN packets that are permitted to pass through per second by SYN proxy or SYN-Cookie (if enabled by cookie). If the number of inbound SYN packets destined to one single port of one single destination IP address per second exceeds the specified value, system will only permit the specified number of SYN packets to pass through during the current and the next second. All the excessive packets of the same type will be dropped during this period. The value range is 1 to 1500000. The default value is 3000. To restore to the default value, use the command**no ad syn-proxy max-proxy-rate**.

- **proxy-timeout** *number* – Specifies the timeout for half-open connections. The half-open connections will be dropped after timeout. The value range is 1 to 180 seconds. The default value is 30. To restore to the default value, use the command **no ad syn-proxy proxy-timeout**.
- **cookie** – Enables SYN-Cookie (the prerequisite is SYN-Proxy is enabled). This function allows system to enhance its capacity of processing multiple SYN packets. Therefore, you are advised to expand the range between **min-proxy-rate** and **max-proxy-rate** appropriately. To disable SYN-Cookie, use the command**no ad syn-proxy cookie**.

Configuring ICMP Flood Attack Defense

You can enable or disable ICMP flood attack defense for each security zone individually, and configure the packet number threshold and actions for the ICMP flood attacks. To configure ICMP Flood attack defense of the specified security zone, in the security zone configuration mode, use the following command:

ad icmp-flood [**threshold** *number* | **action** {**alarm** | **drop**}]

- **ad icmp-flood** – Enables ICMP Flood attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad icmp-flood**.
- **threshold** *number* – Specifies a threshold for inbound ICMP packets. If the number of inbound ICMP packets destined to one single IP address per second exceeds the threshold, system will identify the traffic as an ICMP flood and take the specified action. The value range is 1 to 50000. The default value is 1500. To restore to the default value, use the command **no ad icmp-flood threshold**.
- **action** {**alarm** | **drop**} – Specifies the action for ICMP Flood attacks. **alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Only permits the specified number (**threshold** *number*) of IMCP packets to pass through during the current and the next second, and also gives an alarm. All the excessive packets of the same type will be dropped during this period. The default action is drop. To restore to the default action, use the command **no ad icmp-flood action**.

Configuring UDP Flood Attack Defense

You can enable or disable UDP flood attack defense for each security zone individually, and configure the packet number threshold and actions for the UDP Flood attacks. To configure UDP Flood attack defense of the specified security zone, in the security zone configuration mode, use the following command:

ad udp-flood [session-state-check] [source-threshold *number* | destination-threshold *number* | action {alarm | drop}]

- **ad udp-flood** – nables UDP Flood attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad udp-flood**.
- **session-state-check** – Enables the function of session state check. After the function is enabled, system will not check whether there is UDP Flood attack in the backward traffic of UDP packet of the identified sessions. To disable this function, use the command **no ad udp-flood session-state-check**.
- **source-threshold** *number* – Specifies a threshold for outbound UDP packets. If the number of outbound UDP packets originating from one single source IP address per second exceeds the threshold, system will identify the traffic as a UDP flood and take the specified action. The value range is 0 to 300000. The default value is 1500. To restore to the default value, use the command **no ad udp-flood source-threshold**.
- **destination-threshold** *number* – Specifies a threshold for inbound UDP packets. If the number of inbound UDP packets destined to one single port of one single destination IP address per second exceeds the threshold, system will identify the traffic as a UDP flood and take the specified action. The value range is 0 to 300000. The default value is 1500. To restore to the default value, use the command **no ad udp-flood destination-threshold**.
- **action** {**alarm** | **drop**} – Specifies an action for UDP flood attacks.**alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Only permits the specified number (**source-threshold** *number* | **destination-threshold** *number*) of UDP packets to pass through during the current and the next second, and also gives an alarm. All the excessive packets of the same type will be dropped during this period. The default action is drop. To restore to the default action, use the command **no ad udp-flood action**.

Configuring Large ICMP Packet Attack Defense

You can enable or disable large ICMP packet attack defense for each security zone individually, and configure the packet size threshold and actions for large ICMP packet attacks. To configure large ICMP packet attack defense for the specified security zone, in the security zone configuration mode, use the following command:

ad huge-icmp-pak [threshold *number* | action {alarm | drop}]

- **ad huge-icmp-pak** – Enables large ICMP packet attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad huge-icmp-pak**.

- **threshold** *number* – Specifies the size threshold for ICMP packets. If the size of any inbound ICMP packet is larger than the threshold, system will identify it as a large ICMP packet and take the specified action. The value range is 1 to 50000 bytes. The default value is 1024. To restore to the default value, use the command **no ad huge-icmp-pak threshold**.
- **action** {**alarm** | **drop**} – Specifies the action for large ICMP packet attacks. **alarm** – Gives an alarm but still allows the packet to pass through; **drop** – Gives an alarm and drop the packet. The default action is drop. To restore to the default action, use the command **no ad udp-flood action**.

Configuring WinNuke Attack Defense

With WinNuke attack defense enabled, system will drop the packets and give an alarm if any WinNuke attack has been detected. To enable WinNuke attack defense for the specified security zone, in the security zone configuration mode, use the following command:

```
ad winnuke
```

To disable the function, in the security zone configuration mode, use the command **no ad winnuke**.

Configuring Ping of Death Attack Defense

With Ping of Death attack defense enabled, system will drop the packets and give an alarm if any Ping of Death attack has been detected. To enable Ping of Death attack defense for the specified security zone, in the security zone configuration mode, use the following command:

```
ad ping-of-death
```

To disable the function, in the security zone configuration mode, use the command **no ad ping-of-death**.

Configuring Teardrop Attack Defense

With Teardrop attack defense enabled, system will drop the packets and give an alarm if any Teardrop attack has been detected. To enable Teardrop attack defense for the specified security zone, in the security zone configuration mode, use the following command:

```
ad tear-drop
```

To disable the function, in the security zone configuration mode, use the command **no ad tear-drop**.

Configuring IP Option Attack Defense

With IP Option attack defense enabled, system will drop the packets and give an alarm if any IP option attack has been detected. You can change the action for the attacks as needed. system will defend against the following types of IP options: Security, Loose Source Route, Record Route, Stream ID, Strict Source Route and Timestamp. To enable IP Option attack defense for the specified security zone, in the security zone configuration mode, use the following command:

```
ad ip-option [action {alarm | drop}]
```

- **ad ip-option** – Enables IP Option attack defense for the specified security zone. To disable the function, in the security zone configuration mode, use the command **no ad ip-option**.
- **action {alarm | drop}** – Specifies the action for IP Option attacks. **alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Gives an alarm and drops the packets. The default action is drop. To restore to the default action, use the command **no ad ip-option action**.

Configuring TCP Option Anomaly Attack Defense

With TCP option anomaly attack defense enabled, system will drop the packets and give an alarm if any TCP option anomaly attack has been detected. You can change the action for the attacks as needed. system identifies the following conditions as TCP option anomaly attack:

- SYN packets are fragmented
- TCP packets are only set with FIN flag
- TCP packets are not set with any flag
- TCP packets are set with both FIN and RST flag
- TCP packets are set with both SYN and URG flag
- TCP packets are set with both SYN and RST flag
- TCP packets are set with both SYN and FIN flag

To enable TCP option anomaly attack defense for the specified security zone, in the security zone configuration mode, use the following command:

```
ad tcp-anomaly [action {alarm | drop}]
```

- **ad tcp-anomaly** – Enables TCP option anomaly attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad tcp-anomaly**.
- **action {alarm | drop}** – Specifies the action for TCP option anomaly attacks. **alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Gives an alarm and drops the packets. The default action is drop. To restore to the default action, use the command **no ad tcp-anomaly action**.

Configuring Land Attack Defense

With Land attack defense enabled, system will drop the packets and give an alarm if any Land attack has been detected. You can change the action for the attacks as needed. To enable Land attack defense for the specified security zone, in the security zone configuration mode, use the following command:

```
ad land-attack [action {alarm | drop}]
```

- **ad land-attack** – Enables Land attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad land-attack**.
- **action** {**alarm** | **drop**} – Specifies the action for the Land attacks.**alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Gives an alarm and drops the packets. The default action is drop. To restore to the default action, use the command **no ad land-attack action**.

Configuring IP Fragment Attack Defense

When being transmitted among different networks, sometimes the packets need to be fragmented according to the MTU value. Attackers can modify the IP fragments and launch attacks by exploiting the vulnerabilities occurring during reassembling. The modified IP fragments destined to the victims might lead to improper reassembling, or even complete system crash.

system will drop the packets and give an alarm if any IP fragment attack has been detected. You can change the action for the attacks as needed. To enable IP fragment attack defense for the specified security zone, in the security zone configuration mode, use the following command:

```
ad ip-fragment [action {alarm | drop}]
```

- **ad ip-fragment** – Enables IP fragment attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad ip-fragment**.
- **action** {**alarm** | **drop**} – Specifies the action for IP fragment attacks. **alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Gives an alarm and drops the packets. The default action is drop. To restore to the default action, use the command **no ad ip-fragment action**.

Configuring Smurf and Fraggle Attack Defense

With Smurf and Fraggle attack defense enabled, system will drop the packets and give an alarm if any Smurf or Fraggle attack has been detected. You can change the action for the attacks as needed. To enable Smurf and Fraggle attack defense for the specified security zone, in the security zone configuration mode, use the following command:

```
ad ip-directed-broadcast [action {alarm | drop}]
```

- **ad ip-directed-broadcast** – Enables Smurf and Fraggle attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad ip-directed-broadcast**.
- **action** {**alarm** | **drop**} – Specifies the action for the Smurf and Fraggle attacks. **alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Gives an alarm and drops all the packets. The default action is drop. To restore to the default action, use the command **no ad ip-directed-broadcast action**.

Configuring ARP Spoofing Attack Defense

ARP spoofing attack defense can protect the Intranet against ARP spoofing attacks. To configure ARP spoofing attack defense of the specified security zone, in the security zone configuration mode, use the following command:

ad arp-spoofing {**reverse-query** | **ip-number-per-mac** *number* [**action** [**drop** | **alarm**]] | **gratuitous-arp-send-rate** *number*}

- **reverse-query** – Enables reverse query. When system receives an ARP request, it will log the IP address and reply with another ARP request; and then system will check if any packet with a different MAC address will be returned, or if the MAC address of the returned packet is the same as that of the ARP request packet. To disable the function, in the security zone configuration mode, use the command **no ad arp-spoofing reverse-query**.
- **ip-number-per-mac** *number* – Specifies whether system will check the IP number per MAC in ARP table. If the parameter is set to 0 (the default value), system will not check the IP number; if 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 action specified by **action** [**drop** | **alarm**]. The available actions include**drop**(give an alarm and drop the ARP packets) and**alarm**(give an alarm but still allow the packets to pass through). The value range is 0 to 1024. To restore to the default value, use the command **no ad arp-spoofing ip-number-per-mac**.
- **gratuitous-arp-send-rate***number* – Specifies if system will send gratuitous ARP packet(s). If the parameter is set to 0 (the default value), system will not send any gratuitous ARP packet; if set to a value other than 0, system will send gratuitous ARP packet(s), and the number sent per second is the specified parameter value. The value range is 0 to 10. To restore to the default value, use the command **no ad arp-spoofing gratuitous-arp-send-rate**.

Configuring DNS Query Flood Attack Defense

DNS (Domain Name System) is used to convert a domain name to an IP address, and resolve an IP address to a domain name. DNS is an application layer protocol, so it can be based on TCP or UDP. DNS Query Flood attacks are based on UDP.

The DNS Query Flood attacks are launched by sending a large number of domain name resolution requests to the target DNS server. Typically the requested domain name is randomly generated, or does not exist at all. When the DNS server being attacked receives the resolution requests, it will first look for the corresponding cache. If the cache is not found and the domain name can not be resolved directly by the server, the DNS server will send a recursive query request to its upper DNS server. The domain name resolution process will bring a heavy load to the DNS server. If the DNS requests per second exceed a certain number, the workload will lead to domain name resolution timeout on the DNS server. .

FS devices support DNS Query Flood attacks defense. You can enable or disable DNS Query Flood attack defense for each security zone individually, and configure the packet number threshold and the actions for DNS Query Flood attacks. To enable DNS Query Flood defense, in the security zone configuration mode, use the following command:

ad dns-query-flood [**recursion**] [**source-threshold** *number*] [**destination-threshold** *number* | **action** {**alarm** | **drop**}]

- **ad dns-query-flood** – Enables DNS Query Flood attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad dns-query-flood**.

- **recursion** – Only limits recursive DNS query packets. If this parameter is not specified, system will limit all the DNS query packets.

- **source-threshold** *number* – Specifies a threshold for outbound DNS query packets or recursive DNS query packets. If the number of outbound DNS query packets originating from one single IP address per second exceeds the threshold, system will identify the traffic as a DNS query flood and take the specified action. The value range is 0 to 300000. The default value is 1500. To restore to the default value, use the command **no ad dns-query-flood source-threshold**.

- **destination-threshold** *number* – Specifies a threshold for inbound DNS query packets or recursive DNS query packets. If the number of inbound DNS query packets destined to one single IP address per second exceeds the threshold, system will identify the traffic as a DNS query flood and take the specified action. The value range is 0 to 300000. The default value is 1500. To restore to the default value, use the command **no ad dns-query-flood destination-threshold**.

- **action** {**alarm** | **drop**} – Specifies the action for DNS Query Flood attacks. **alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Only permits the specified number (**threshold** *number*) of recursive DNS query packets to pass through during the current and next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period. The default action is drop. To restore to the default action, use the command **no ad dns-flood action**.

Note:DNS Query Flood attack defense is only applicable to UDP DNS query packets.

Configuring TCP Split Handshake Attack Defense

After enabling the TCP split handshake attack defense and this attack is detected, the device will drop the packet and give an alarm by default. You can change the defaul action. To configure the TCP split handshake attack defense, use the following command in the security zone configuration mode:

ad tcp-split-handshake [**action** {**alarm** | **drop**}]

- **ad tcp-split-handshake** – Enable the TCP split handshake attack defense for the security zone. To disable it, use the command **no ad tcp-split-handshake**.
- **action** {**alarm** | **drop**} – Specifies the action for the TCP split handshake attacks. **alarm**- Gives an alarm but still allows the packets to pass through; **drop**- Gives an alarm and drops all the packets. The default action is**drop**. To restore to the default action, use the command **no ad land-attack action**.

Configuring an Attack Defense Whitelist

With attack defense enabled, the system will check all the traffic in the zone. In practical scenario, possibly you do not want to check the traffic originating from certain hosts for test purpose. To solve this problem, you can add the addresses to an attack defense whitelist, so that the addresses can be exempted from the attack defense check.

To configure an attack defense whitelist, in the zone configuration mode, use the following command:

ad whitelist [**id** *id*] **ip** {*A.B.C.D/M* | *address-entry*}

- **id** – Specifies an ID for the whitelist rule. The value differs according to different models. If not specified, the system will assign an ID automatically for the rule.
- A.B.C.D/M – Specifies the IP address and network that will be added to the whitelist rule.
- *address-entry* – Specifies the address entry that will be added to the whitelist rule.

To delete the specified whitelist rule, in the zone configuration mode, use the following command:

no ad whitelist {**id** *id* | **ip** {*A.B.C.D/M* | *addr-book*}}

Viewing the Attack Defense Configuration and Statistics of the Security Zone

To view the attack defense configuration and statistics of the specified security zone, in any mode, use the following command:

show ad zone *zone-name* {**statistics** | **configuration** | **whitelist**}

- *zone-name* − Specifies the name of the security zone.
- **statistics** − Shows the attack defense statistics of the specified security zone.
- **configuration** − Shows the attack defense configurations of the specified security zone.
- **whitelist** − Shows the attack defense whitelist configurations of the specified security zone.

Examples of Configuring Attack Defense

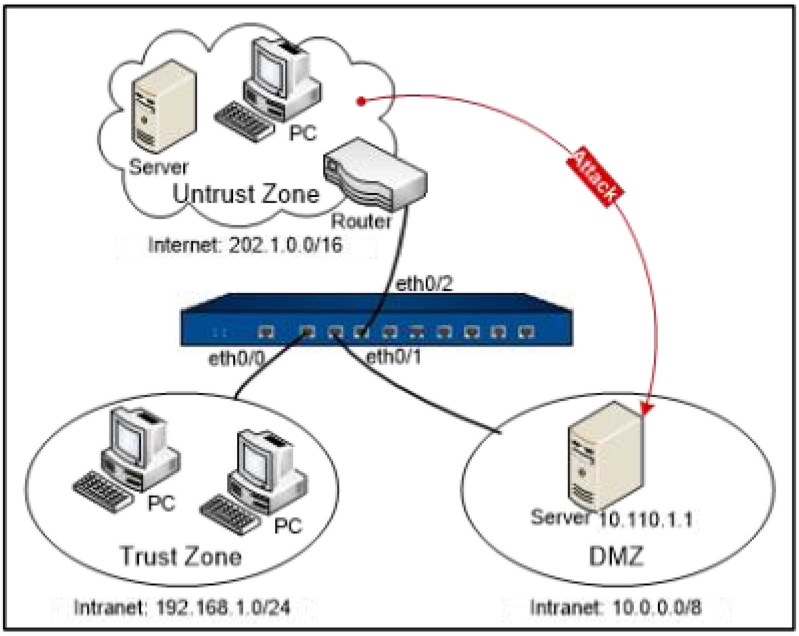
This section describes several attack defense configuration examples for your better understanding and helps you configure the attack defense function of the devices.

Example of Configuring Land Attack Defense

This section describes a Land attack defense configuration example.

Requirement

Device's ethernet 0/0 is bound to the trust zone, ethernet 0/2 is bound to the untrust zone, and ethernet 0/1 is bound to the DMZ zone. The goal is to protect the server in the DMZ zone against Land attacks. The network topology is shown below.



Configuration Steps

Step 1: Configure ethernet0/0.

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 2: Configure ethernet0/2.

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ip address 202.1.0.1/24
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Step 3: Configure ethernet0/1.

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone dmz
hostname(config-if-eth0/1)# ip address 10.0.0.1/8
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 4: Configure a policy rule.

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone dmz
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 5: Enable Land attack defense for the untrust zone.

```
hostname(config)# zone untrust
hostname(config-zone)# ad land-attack
hostname(config-if)# exit
hostname(config)#
```

Step 6: Test the Land attack defense configured for the server. Craft a packet with identical source and destination IP address, and send it to 10.110.1.1. The FS device will detect a Land attack, and then give an alarm and drop the packet.

Example of Configuring SYN Flood Attack Defense

This section describes a SYN Flood attack defense configuration example.

Requirement

Device's ethernet 0/0 is bound to the trust zone, ethernet 0/2 is bound to the untrust zone, and ethernet 0/1 is bound to the DMZ zone. The goal is to protect the server in the DMZ zone against SYN Flood attacks.

Configuration Steps

Step 1: Configure ethernet0/0:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 2: Configure ethernet0/2:

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ip address 202.1.0.1/24
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Step 3: Configure ethernet0/1:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone dmz
hostname(config-if-eth0/1)# ip address 10.0.0.1/8
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 4: Configure a policy rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone dmz
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 5: Enable SYN Flood attack defense for the untrust zone:

```
hostname(config)# zone untrust
hostname(config-zone)# ad syn-flood
hostname(config-if)# exit
hostname(config)#
```

Step 6: Test the SYN Flood attack defense configured for the server. Send over 1500 packets per second to 10.110.1.1. The FS device will detect a SYN Flood attack, and then give an alarm and drop the packets.

Example of Configuring IP Address Sweep Attack Defense

This section describes an IP address sweep attack defense configuration example.

Requirement

Device's ethernet 0/0 is bound to the trust zone, ethernet 0/2 is bound to the untrust zone, and ethernet 0/1 is bound to the DMZ zone. The goal is to protect the server in the DMZ zone against IP address sweep attacks.

Configuration Steps

Step 1: Configure ethernet0/0:

```
hostname(config)# interface ethernet0/0

hostname(config-if-eth0/0)# zone trust

hostname(config-if-eth0/0)# ip address 192.168.1.1/24

hostname(config-if-eth0/0)# exit

hostname(config)#
```

Step 2: Configure ethernet0/2:

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

hostname(config-if-eth0/2)# zone untrust

hostname(config-if-eth0/2)# ip address 202.1.0.1/24

hostname(config-if-eth0/2)# exit

hostname(config)#
```

Step 3: Configure ethernet0/1:

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

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

hostname(config-if-eth0/1)# ip address 10.0.0.1/8

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

hostname(config)#
```

Step 4: Configure a policy rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone dmz
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 5: Enable IP address sweep attack defense for the untrust zone:

```
hostname(config)# zone untrust
hostname(config-zone)# ad ip-sweep
hostname(config-if)# exit
hostname(config)#
```

Step 6: Test the IP address sweep attack defense configured for the server. Craft packets via smartbits and launch an IP address sweep attack against ethernet0/2. Send over 10 packets per millisecond to 202.1.0.1. The device will detect an IP address sweep attack, and then give an alarm and drop the packets.

Anti-Virus

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

System is designed with Anti-Virus that is controlled by licenses to provide AV solution featuring high speed, high performance and low delay. With this function configured in system, FS 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. FS device 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.

If IPv6 is enabled, Anti Virus function will detect files and protocols based on IPv6. How to enable IPv6, see IPv6.

Configuring Anti-Virus

To enable the anti-virus function on system, take the following steps:

1. Define an AV profile, and specify the file types, protocol types, the actions for the viruses, and the e-mail label function in the profile.
2. Bind the AV profile to an appropriate policy rule or security zone. To perform the Anti-Virus function on the HTTPS traffic, see Binding an AV Profile to a Policy Rule.

Note:You need to update the anti-virus signature database before enabling the function for the first time. For more information about how to update, see Updating AV Signature Database. To assure a proper connection to the default update server, you need to configure a DNS server for system before updating.

After installing the anti-virus license and rebooting the device, the anti-virus function will be enabled on the system, and the maximum number of concurrent connections will be reduced by half. To view the status of anti-virus, use the command show version. To enable or disable Anti-Virus, in any mode, use the following command:

```
exec av {enable | disable}
```

- **enable** – Enables Anti-Virus.
- **disable** – Disables Anti-Virus.

After executing the above commands, you need to reboot the system to make the modification take effect. After rebooting, system's maximum concurrent sessions will decrease by half if the function is enabled, and restore to normal if the function is disabled. When AV and multi-VR are enabled simultaneously, the maximum concurrent session will further decrease by 15% (with Multi-VR enabled, the maximum concurrent session will decrease by 15%). The formula is: actual maximum concurrent sessions = original maximum concurrent sessions*(1-0.15)*(1-0.5).

Creating an AV Profile

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

av-profile *av-profile-name*

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

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

Enabling Malicious Website Detection

System provides the malicious website detection function to protect against attacks from malicious websites if you click maliciously URLs accidentally. With this function enabled, System will detect Trojans, phishing and other malicious behaviors when you are trying to visit URLs, and process malicious URLs according to the actions specified by system.

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

```
anti-malicious-sites
```

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

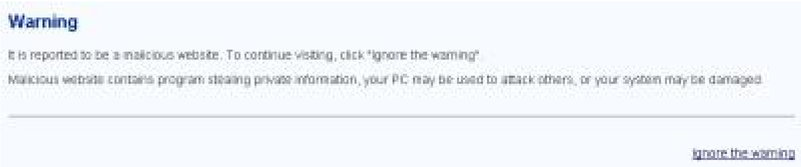
```
no anti-malicious-sites
```

Specifying Malicious Website Detection Action

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

```
anti-malicious-sites [action{ log-only | reset-conn | warning}| pacp]
```

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



Warning

It is reported to be a malicious website. To continue visiting, click "Ignore the warning"

Malicious website contains program stealing private information, your PC may be used to attack others, or your system may be damaged.

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

- pcap – Enable the Capture Packet function.

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

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

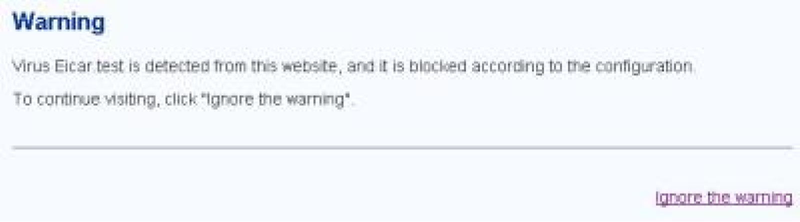
Specifying a Protocol Type

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

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

- ftp – Scans the files transferred over FTP.
- http – Scans the files transferred over HTTP.
- imap4 – Scans the files transferred over IMAP4.
- pop3 – Scans the Emails transferred over POP3.
- smtp – Scans the Emails transferred over SMTP.
- pcap – Capture the packet for protocol scanning.
- action {fill-magic | log-only | reset-conn | warning} – Specifies the action for the viruses.
  - fill-magic – Processes the virus file by filling magic words, i.e., fills the file with the magic words (Virus is found, cleaned) from the beginning to the ending part of the infected section.
  - log-only – Generates logs. This is the default action for FTP, IMAP4, POP3 and SMTP.
  - reset-conn – Resets the connection if any virus has been detected.

- **warning** – Pops up a warning page to prompt that a virus or malicious website download has been detected. There are two kinds of pages: the virus warning page , and malicious website warning page (the malicious website detection is enabled), as shown below. This option is only effective to the messages transferred over HTTP, and is also the default action if any virus or malicious website download has been detected.

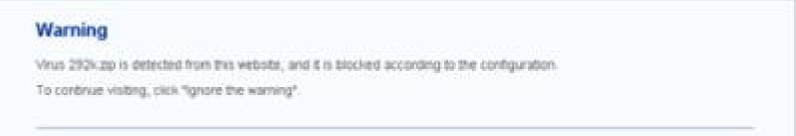
  

  Warning

  Virus Eicar.test is detected from this website, and it is blocked according to the configuration.

  To continue visiting, click "Ignore the warning".

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

  Warning

  Virus 292k.zip is detected from this website, and it is blocked according to the configuration.

  To continue visiting, click "Ignore the warning".

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

Repeat the above command to specify more protocol types.

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

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

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

Specifying a File Type

To specify a file type, in the AV Profile configuration mode, use the following command:

file-type {bzip2 | gzip | html | jpeg | mail | pe | rar | riff | tar | zip | elf | pdf | office | raw-data | others }

- **bzip2** – Scans BZIP2 compressed files.
- **gzip** – Scans GZIP compressed files.
- **html** – Scans HTML files.
- **jpeg** – Scans JPEG files.
- **mail** – Scans mail files.

- pe – Scans PE files. PE (Portable Executable) is an executable file format supported by Win32 environment. This file format can be used across Win32 platforms. Even if Windows is running on a non-Intel CPU, the PE loader of any Win32 platform can identify and use the file format. Besides, system also supports packed PE files. The supported packing types include ASPack 2.12, UPack 0.399, UPX (all versions), and FSG v1.3, 1.31, 1.33, 2.0.
- rar – Scans RAR compressed files.
- riff – Scans RIFF files. RIFF (Resource Interchange File Format) is a class of multimedia file formats designed by Microsoft for Windows, mainly consisting of WAV and AVI types.
- tar – Scans TAR compressed files.
- zip – Scans ZIP compressed files.
- elf – Scans the ELF files.
- pdf – Scans the PDF files.
- office – Scans the Office files.
- raw-data – Scans the txt file and unrecognized file.
- others – Scans the other file.

Repeat the above command to specify more protocol types.

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

no file-type { bzip2 | gzip | html | jpeg | mail | pe | rar | riff | tar | zip | elf | pdf | office | raw-data | others }

Label Email

If an Email transferred over SMTP is scanned, you can enable label Email to scan the Email and its attachment(s). The scanning results will be included in the mail body, and sent with the Email. If no virus has been detected, the message of "No virus found" will be labeled, as shown below:

Body
No virus found. Checked by FS AntiVirus

Otherwise information related to the virus will be displayed in the Email, including the filename, path, result and action, as shown below:

Body
Here are the AntiVirus scanning results: Body: Found virus: virusname1, action: log; Attachment1.zip/virustest1.exe: Found virus: virusname2, action: log; Attachment2.tar/subfolder/file1.doc: Found virus: virusname3, action: log; Checked by FS AntiVirus

Note:The Email will display the scan information of up to 3 virus file (including the message body and attachments). You can view all the scan information in the log.

Enabling/Disabling Label Email

By default the label Email function is disabled. To enable the function, in the AV Profile configuration mode, use the following command:

label-mail

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

no label-mail

Configuring Email Signature

After enabling the label Email function, you can customize your own Email signature. By default, the signature of the labeled Email is "Checked by FS AntiVirus". To configure an Email signature, in the AV profile configuration mode, use the following command:

mail-sig *signature-string*

- *signature-string* – Configures the signature of the labeled Email.

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

no mail-sig

Binding an AV Profile to a Security Zone

If the AV profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration. If the policy rule is bound with an AV Profile, and the destination zone of the policy rule is also bound with an AV profile, then the AV profile bound to the policy rule will be valid, while the AV profile bound to the security zone will be void.

To bind the AV profile to a security zone, in the security zone configuration mode, use the following command:

av enable *av-profile-name*

- *av-profile-name* – Specifies the name of the AV profile that will be bound to the security zone. One security zone can only be bound with one AV profile.

To cancel the binding, in the security zone configuration mode, use the following command:

no av enable

To view the binding between the security zones and AV Profiles, use the command **show av zone-binding**.

Binding an AV Profile to a Policy Rule

If the AV profile is bound to a policy rule, the system will detect the traffic matched to the specified policy rule based on the profile configuration. To bind the AV profile to a policy rule, in the policy rule configuration mode, use the following command:

av {*av-profile-name* | **no-av**}

- *av-profile-name* – Specifies the name of the AV profile that will be bound to the policy rule.
- **no-av** – Specifies the predefined AV profile named no-av, which means the anti-virus is disabled. If this profile is bound to any policy rule, even if there are other matched AV profiles, the system still will not detect the traffic.

To cancel the binding, in the policy rule configuration mode, use the following command:**no av**

To perform the Anti-Virus function on the HTTPS traffic, you need to enable the SSL proxy function for the above specified security policy rule. The system will decrypt the HTTPS traffic according to the SSL proxy profile and then perform the Anti-Virus function on the decrypted traffic. According to the various configurations of the security policy rule, the system will perform the following actions:

Policy Rule Configurations	Actions

Policy Rule Configurations	Actions
SSL proxy enabled Anti-Virus disabled	The system decrypts the HTTPS traffic according to the SSL proxy profile but it does not perform the Anti-Virus function on the decrypted traffic.
SSL proxy enabled Anti-Virus enabled	The 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	The system performs the Anti-Virus function on the HTTP traffic according to the Anti-Virus profile. The HTTPS traffic will not be decrypted and the system will transfer it.

If the destination zone or the source zone specified in the security policy rule are configured with Anti-Virus as well, the system will perform the following actions:

Policy Rule Configurations	Zone Configurations	Actions
SSL proxy enabled Anti-Virus disabled	Anti-Virus enabled	The system decrypts the HTTPS traffic according to the SSL proxy profile and performs the Anti-Virus function on the decrypted traffic according to the Anti-Virus rule of the zone.
SSL proxy enabled Anti-Virus enabled	Anti-Virus enabled	The system decrypts the HTTPS traffic according to the SSL proxy profile and performs the Anti-Virus function on the decrypted traffic according to the Anti-Virus rule of the policy rule.
SSL proxy disabled Anti-Virus enabled	Anti-Virus enabled	The system performs the Anti-Virus function on the HTTP traffic according to the Anti-Virus rule of the policy rule. The HTTPS traffic will not be decrypted and the system will transfer it.

Tip: For more information about SSL proxy, see the SSL Proxy chapter.

Viewing AV Profile Information

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

```
show av-profile
```

Specifying the Maximum Decompression Layer

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

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

- *number* – Specifies the decompression layer. The value range is 1 to 5. The default value is 1.
- **log-only** | **reset-conn** – Specifies the action for the compressed files that exceed the maximum decompression layer. The available options include(**log-only**)and(**reset-conn**). The default action is **log-only**.

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

```
no av max-decompression-recursion
```

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

Updating AV Signature Database

By default system updates the AV signature database everyday automatically. You can change the update configuration as needed. The configurations of updating AV signature database include:

- Configuring an AV Signature Update Mode
- Configure an Update Server
- Specifying a HTTP Proxy Server
- Specifying an Update Schedule
- Updating Now
- Importing an AV Signature File
- Viewing AV Signature Information

- Viewing AV Signature Update Information

Configuring an AV Signature Update Mode

System supports both manual and automatic update modes. To configure an AV signature update mode, in the global configuration mode, use the following command:

```
av signature update mode {auto | manual}
```

- **auto** – Specifies the automatic AV signature update mode. This is the default mode.
- **manual** – Specifies the manual AV signature update mode.

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

```
no av signature update mode
```

Configure an Update Server

System provides two default update servers: Update1.fw1.fs.com and Update2.fw2.fs.com. You can also configure another up to three update servers to download the latest AV signatures as needed. To configure the update the server, in the global configuration mode, use the following command:

```
av signature update {server1 | server2 | server3} {ip-address | domain-name}
```

- **server1** | **server2** | **server3** – Specifies the update server you want to configure. The default value of **server1** is Update1.fw1.fs.com, and the default value of **server2** is Update2.fw2.fs.com.
- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an *ip-address*or a *domain-name*, for example, Update1.fw1.fs.com.

To cancel the specified update the server, in the global configuration mode, use the following command:

```
no av signature update {server1 | server2 | server3}
```

Specifying a HTTP Proxy Server

When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update automatically and normally.

To specify the HTTP proxy server for the Antivirus signature database updating, use the following command in the global configuration mode:

```
av signature update proxy-server {main | backup} ip-address port-number
```

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

To cancel the proxy server configurations, use the **no av signature update proxy-server** {**main** | **backup**}.

Specifying an Update Schedule

By default, system automatically updates the AV signature database every day. To reduce the update server' s workload, the time of daily update is random. To specify the schedule and specific time for the update, in the global configuration mode, use the following command:

av signature update schedule {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**}} [*HH:MM*]

- **daily** – Updates the database every day.
- **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} – Updates the database every week. Parameter **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**is used to specify the specific date in a week.
- *HH:MM* – Specifies the time of update, for example, 09:00.

Updating Now

For both manual and automatic update modes, you can update the AV signature database immediately as needed. To update the AV signature database now, in any mode, use the following command:

exec av signature update

- **exec av signature update** – Only updates the incremental part between the current AV signature database and the latest AV signature database released by the update server.

Importing an AV Signature File

In some cases, your device may be unable to connect to the update server to update the AV signature database. To solve this problem, system provides the AV signature file import function, i.e., importing the AV signature files to the device from an FTP, TFTP server or USB disk, so that the device can update the AV signature database locally. To import the AV signature file, in the execution mode, use the following command:

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

- *ip-address* – Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP server.
- **vrouter** *vr-name* – Specifies the VRouter of the FTP or TFTP server.
- *file-name* – Specifies the name of the AV signature file that be imported.

Viewing AV Signature Information

You can view the AV signature database information of the device as needed, including the AV signature database version, release dates, and the number of the AV signatures. To view AV signature database information, in any mode, use the following command:

show av signature info

Viewing AV Signature Update Information

You can view the AV signature update information of the device as needed, including the update server information, update mode, update frequency and time, as well as the status of the AV signature database update. To view the AV signature update information, in any mode, use the following command:

show av signature update

Examples of Configuring Anti-Virus

Before enabling anti-virus, make sure your device has already been installed with a corresponding anti-virus license.

This section describes an anti-virus configuration example. Devices with this example configured can:

- Scan Emails and its attachments, and display the anti-virus result in the Emails. The Emails are transferred over SMTP and POP3, and the attachments may contain .exe and .jpeg files.
- Scan compressed files. RAR-compressed files contain .jpeg files, and all the compressed files are transferred over FTP.

Configuration Steps

Step 1: Configure the AV profile, and specify the protocol types and file types:

```
hostname(config)# av-profile email-scan
hostname(config-av-profile)# protocol-type smtp action fill-magic
hostname(config-av-profile)# protocol-type pop3 action fill-magic
hostname(config-av-profile)# protocol-type ftp action fill-magic
hostname(config-av-profile)# file-type pe
hostname(config-av-profile)# file-type jpeg
hostname(config-av-profile)# file-type mail
hostname(config-av-profile)# label-mail
hostname(config-av-profile)# mail-sig “Checked by Mail AntiVirus”
hostname(config-av-profile)# exit
hostname(config)#
```

Step 2: Create a policy rule, and reference the AV Profile to the rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# av email-scan
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 3: View the anti-virus status by command show version. If the function is disabled, use following command to enable it and reboot the system to make it take effect:

```
hostname(config)# exec av enable
```

IPS

IPS (Intrusion Prevention System) is designed to monitor various network attacks in real time and take appropriate actions (like block) against the attacks according to your configuration. FSOS supports license-controlled IPS, i.e., the IPS function will not work unless an IPS license has been installed on a FSOS that supports IPS.

The IPS on FSOS 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, FSOS will update the signature database automatically everyday to assure its integrity and accuracy.

IPS Detection and Submission Procedure

The protocol detection procedure of IPS consists of two stages: protocol parsing and signature matching.

- Protocol parsing: IPS analyzes the protocol part of the traffic. If the analyze results shows the protocol part contains abnormal contents, the system will process the traffic according to the action configuration. And it can generate logs for the administrator if any anomaly has been detected. Each Threat log contains "Threat ID", the signature ID in the signature database. You can view detailed information in Threat log details.

- Signature matching: IPS abstracts the interested protocol elements of the traffic for signature matching. If the elements are matched to the items in the signature database, the system will process the traffic according to the action configuration and it can generate logs for the administrator. Each Threat log contains "Threat ID", the signature ID in the signature database. You can view detailed information about the error according to the ID.

Signatures

The IPS signatures are categorized by protocols, and identified by a unique signature ID. The signature ID consists of two parts: protocol ID (1st bit or 1st and 2nd bit) and attacking signature ID (the last 5 bits). For example, in ID 605001, "6" identifies a Telnet protocol, and "00120" is the attacking signature ID. 1st bit in signature ID identify protocol anomaly signatures, 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

ID	Protocol	ID	Protocol	ID	Protocol	ID	Protocol
5	SMTP	11	SUNRPC	17	Oracle	-	-
6	Telnet	12	NNTP	18	MSRPC	-	-

In the above table, other-TCP identifies all the TCP protocols other than the standard TCP protocols listed in the table, and other-UDP identifies all the UDP protocols other than the standard UDP protocols listed in the table.

Updating IPS Signature Database

By default FSOS updates the IPS signature database everyday automatically. You can change the update configuration as needed. FS devices provide two default update servers: Update1.fw1.fs.com and Update2.fw2.fs.com. FSOS supports auto update and local update. Non-root VSYS does not support this feature. For more information about the signature database configurations, please refer to the table below.

Configuration	CLI
To configure an update mode (auto by default)	In the global configuration mode, use the following command: • Specifying the update mode: **ips signature update mode {auto | manual}** • Restoring to the default: **no ips signature update mode**
To configure an update server	In the global configuration mode, use the following command: • Specifying the update server: **ips signature update** {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} • Canceling the server: **no ips signature update** {**server1** | **server2** | **server3**}
To configure an update schedule	In the global configuration mode, use the following command to make the IPS signature database update daily or weekly: **ips signature update schedule** {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**}} [*HH:MM*] In the global configuration mode, use the following command to make the IPS signature database update hourly: **ips signature update schedule hourly** *minute*

Configuration	CLI
	• *minute* – Specifies the minute that the update starts.
To update now	In the execution mode, use the following command: **exec ips signature update**
To update locally	In the execution mode, use the following command: **import ips signature from** {**ftp server** *ip-address* [**user** *user-name* **password** *password* | **vrouter** *vr-name*] | **tftp server** *ip-address* [**vrouter** *vr-name*]} *file-name*
To view signature statistics	**show ips signature info**
To view signature database configurations	**show ips signature update**

Specifing the HTTP Proxy Server

When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update automatically and normally.

To specify the HTTP proxy server for the IPS signature database updating, use the following command in the global configuration mode:

ips signature update proxy-server {**main** | **backup**} *ip-address port-number*

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

To cancel the proxy server configurations, use the command **no ips signature update proxy-server** {**main** | **backup**}.

IPS Working Modes

System supports two IPS working modes: log only mode and IPS mode. In log only mode, system only generates protocol anomaly alarms and attacking behavior logs, but will not block attackers or reset connections; while in IPS mode, system not only generates protocol anomaly alarms and attacking behavior logs, but also blocks attackers or resets connections. By default, system works in IPS mode.

To switch to the IPS mode, in the global configuration mode, use the command **ips mode {ips-logonly | ips}**.

Configuring IPS

Before enabling IPS, make the following preparations:

1. Make sure your FSOS version supports IPS.
2. Import an IPS license and reboot. The IPS will be enabled after the rebooting.

The configuration of IPS includes the following contents:

- Signature set configurations: IPS abstracts the interested protocol elements of the traffic for signature matching. If the elements are matched to the items in the signature database, the system will process the traffic according to the action configuration.
- Protocol configurations: IPS abstracts the interested protocol elements of the traffic for signature matching. If the elements are matched to the items in the signature database, the system will process the traffic according to the action configuration.
- IPS profile: contains signature set configurations, protocol configurations, and packet capture configurations. You can bind an IPS profile to different directions of the security zone (inbound, outbound, bi-direction) to apply the IPS function to the specified direction, or bind an IPS profile to a policy rule to apply the IPS function to the traffic that matches the specified policy rule.

If a policy rule is bound with an IPS profile and the source and destination security zone are also bound with an IPS Profile, the priority of the IPS detection will be: IPS profile for the policy rule > IPS profile for the destination zone > IPS profile for the source zone.

With IPS configured, FSOS will generate an Threat log if any intrusion has been detected. Each Threat log contains a signature ID. You can view detailed information about the signature according to the ID in IPS online help pages. To view Threat logs, use the command **show logging ips**.

Configuration Suggestions

All the IPS rules configured for different attacks and intrusions will eventually affect the final actions. When determining the final action, the system will follow the principles below:

- The IPS working mode has the highest priority. When the working mode is set to log only, no matter what action is specified in other related configurations, the final action will always be log only.
- If you create several signature sets and some of them contain a particular signature. If the actions of these signature sets are different and the attack matches this particular signature , the system will adopt the following rules:
  - Always perform the stricter action on the attack. The signature set with stricter action will be matched. The strict level is: Block IP > Block Service > Rest > Log Only. If one signature set is Block IP with 15s and the other is Block Service with 30s, the final action will be Block IP with 30s
  - If one signature set is configured with Capture Packet, the system will capture the packets.
  - The action of the signature set created by Search Condition has high priority than the action of the signature set created by Filter.
- For the IPS Profile that is bound to a security zone or policy rule, you can modify the signature sets for the IPS Profile, or a specific signature and its corresponding action. If any IPS profile has been modified, the system will process the related sessions following the principles below:
  - If the IPS profile reference has been changes, the modification will not take effect on the existing sessions immediately. For example, if the IPS profile bound to the trust zone is IPS-pro1 and then is replaced by IPS-pro2, the existing session will continue to use IPS-pro1, and only new sessions will use IPS-pro2. To make the IPS profile reference take effect on the existing sessions immediately, use the command **clear session**.
  - If the signature set of the referenced IPS profile has been changed, the modification will take effect on the existing sessions immediately.

Performing IPS Detection on HTTPS Traffic

To perform the IPS detection on the HTTPS traffic, you need to enable the SSL proxy function for the security policy rule that the HTTPS traffic is matched. The system will decrypt the HTTPS traffic that matches the security policy rule according to the SSL proxy profile and then perform the IPS detection on the decrypted traffic.

According to the various configurations of the security policy rule, the system will perform the following actions:

Policy Rule Configurations	Actions
SSL proxy enabled IPS disabled	The system decrypts the HTTPS traffic according to the SSL proxy profile but it does not perform the IPS detection on the decrypted traffic.
SSL proxy enabled IPS enabled	The system decrypts the HTTPS traffic according to the SSL proxy profile and performs the IPS detection on the decrypted traffic.
SSL proxy disabled IPS enabled	The system performs the IPS detection on the HTTP traffic according to the IPS profile. The HTTPS traffic will not be decrypted and the system will transfer it.

If the destination zone or the source zone specified in the security policy rule are configured with IPS as well, the system will perform the following actions:

Policy Rule Configurations	Zone Configurations	Actions
SSL proxy enabled IPS disabled	IPS enabled	The system decrypts the HTTPS traffic according to the SSL proxy profile and performs the IPS detection on the decrypted traffic according to the IPS profile of the zone.
SSL proxy enabled IPS enabled	IPS enabled	The system decrypts the HTTPS traffic according to the SSL proxy profile and performs the IPS detection on the decrypted traffic according to the IPS profile of the policy rule.
SSL proxy disabled IPS enabled	IPS enabled	The system performs the IPS detection on the HTTP traffic according to the IPS profile of the policy rule. The HTTPS traffic will not be decrypted and the system will transfer it.

Tip: For more information about SSL proxy, see the SSL Proxy chapter.

IPS Commands

action

When the traffic matches the signatures configured by filter rule and/or search rule, specify the corresponding actions.

Command:

action {block-service *timeout*| block-ip *timeout* | log-only | reset}

Description:

action {**block-service***timeout*| **block-ip***timeout* | **log-only** | **reset**} - **block-service**Block the service of the attacker and specify a block duration. **block-ip**Block the IP address of the attacker and specify a block duration. **log-only**Record a log. **reset**Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

log-only。

Mode:

Filter rule configuration mode;

Search rule configuration mode.

Guidance:

None

Example:

```
hostname(config)# ips profile test
hostname(config-ips-profile)# filter-class 1
hostname(config-ips-filter-class)# action log-only
```

affected-software

Configure the affected-software parameter to include signatures, related to the specified software, in the filter rule.

Command:

affected-software {Apache | IE | Firefox | …}

no affected-software {Apache | IE | Firefox | …}

Description:

Apache | **IE** | **Firefox** | … − Enter the name of the software. You can press the Tab key after the**affected-software**parameter to see the entire software list.

Default values:

None

Mode:

Filter rule configuration mode;

Guidance:

None

Example:

```
hostname(config)# ips profile test
hostname(config-ips-profile)# filter-class 1
hostname(config-ips-filter-class)# affected-software Apache
```

attack-type

Configure the attack-type parameter to include signatures, related to the specified attack type, in the filter rule.

Command:

```
attack-type {Access-Control | SPAM | Mail | …}
no attack-type {Access-Control | SPAM | Mail | …}
```

Description:

Access-Control | SPAM | Mail | … - Enter the name of the attack type. You can press the Tab key after the **attack-type**parameter to see the entire attack type list.

Default values:

None

Mode:

Filter rule configuration mode;

Guidance:

None

Example:

```
hostname(config)# ips profile test
hostname(config-ips-profile)# filter-class 1
hostname(config-ips-filter-class)# attack-type WEB-PHP
```

banner-protect enable

Enable the function that protects the banner information of FTP/Web/POP3/SMTP servers and set the new banner information to replace the original one. Use the no form of the command to disable the function.

Command:

banner-protect enable replace-with *string*

no banner-protect enable

Description:

string - Specifies the banner information.

Default values:

None

Mode:

protocol configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset test template ftp
hostname(config-ftp-sigset)# banner-protect enable replace-with vsftp2.0
```

brute-force auth

Enable the brute force function and configure the corresponding settings. Use the no form to disable this function.

Command:

brute-force auth *times* **block** {**ip** | **service**} *timeout*

no brute-force auth

Description:

times - Specifies the allowed failed times of authentication/login in one minute. The value ranges from 1 to 100000.

ip | service - Blocks the IP of the attacker or the service that exceeds the allowed failed times of authentication/login.

timeout - Specifies the period (in seconds) of blocking the IP of the attacker or the service. The value ranges from 60 to 3600.

Default values:

None

Mode:

protocol configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset test1 template telnet
hostname(config-telnet-sigset)# brute-force auth 10 block service 120
```

brute-force lookup

Enable the brute lookup function and configure the corresponding settings. Use the no form to disable this function.

Command:

brute-force lookup *times* **block** {**ip** | **service**} *timeout*

no brute-force lookup

Description:

times - Specifies the allowed times of lookup in one minute. The value ranges from 1 to 100000.

ip | **service** - Blocks the IP of the attacker or the service that exceeds the allowed times of lookup.

timeout - Specifies the period (in seconds) of blocking the IP of the attacker or the server. The value ranges from 60 to 3600.

Default values:

None

Mode:

protocol configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset msrpc-cus template msrpc**

hostname(config-msrpc-sigset)# **brute-force lookup 20 block service 120**

bulletin-board

Configure the bulletion-board parameter to include signatures, related to the specified bulletin board, in the filter rule.

Command:

bulletin-board {CVE | BID | OSVDB | …}

no bulletin-board {CVE | BID | OSVDB | …}

Description:

CVE | BID | OSVDB | … Enter the name of the bulletin board. You can press the Tab key after the **bulletin-board**parameter to see the entire bulletion board list.

Default values:

None

Mode:

Filter rule configuration mode;

Guidance:

None

Example:

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

hostname(config-ips-profile)# **filter-class 1**

hostname(config-ips-filter-class)# **bulletin-board CVE**

command-injection-check

Enable the function of detecting the HTTP protocol command injection attack. Use the no form to disable this function.

Command:

command-injection-check enable

no command-injection-check enable

Description:

None

Default values:

None

Mode:

protocol configuration mode

Guidance:

None.

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# command-injection-check enable
```

cc-url

Configure the URL path for the CC URL constraint. After the configuration, the system will make statistics on the frequency of the HTTP requests that access the path. If the frequency exceeds the threshold, the system will block the source IP of the request and the IP will not be able to access the Web server. Use the no form to delete the url configuration.

Command:

cc-url *url_string*

no cc-url *url_string*

Description:

url_string - Specifies the URL path of CC URL constraint. System will check the frequency of the HTTP requests that access the specified paths, including the whole or part of the paths. For example, if the configuration is /home/ab, system will check and calculate the HTTP requests like /home/ab/login and /home/abc/login. If the frequency of requests exceeds the threshold, system will block the source IP of the request and deny its access to the web server. URL path does not support the path format which contains the host name or domain name, for example: the configuration should be / home / login.html, instead of www.baidu.com/home/login.html, while www.baidu.com should be configured in the domain name settings of the Web server. System allows up to 32 URL paths configuration. The length range of each path is 1 to 255 characters.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# domain www.abc.com
hostname(config-web-server)# cc-url /home/login.php
```

cc-url-limit

Configure t threshold value of visiting frequency of URL path and the time to block IP for the CC URL constraint. After the configuration, the system will make statistics on the frequency of the HTTP requests that access the path. If the frequency exceeds the threshold, the system will block the source IP of the request and the IP will not be able to access the Web server. The system will release the blocked IP and the IP can revisit the Web server after the blocking time.Use the no form to delete the domain name configuration.

Command:

cc-url-limit threshold *value* **action block-ip** *block-ip_time*

no cc-url-limit

Description:

value-Specifies the maximum number of times a single source IP accesses the URL path per minute. When the frequency of a source IP address exceeds this threshold, the system will block the flow of the IP. The value ranges from 1 to 65535 times per minute.

block-ip_time - Specifies the time to block IP. The default is 60 seconds, in the range of 60 to 3600 seconds. Over this time, the system will release the blocked IP, this IP can re-visit the Web server.

Default values:

value − 1 times per minute.

block-ip_time − 60 seconds

Mode:

Web server configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# domain www.abc.com
hostname(config-web-server)# cc-url /home/login.php
hostname(config-web-server)# cc-url-limit threshold 1500 action block-ip 100
```

deny-method

Specify the HTTP method that is refused by the system. Use the no form to allow the specified HTTP method.

Command:

deny-method {**connect** | **delete** | **get** | **head** | **options** | **post** | **put** | **trace** | **webdav**}

no deny-method {**connect** | **delete** | **get** | **head** | **options** | **post** | **put** | **trace** | **webdav**}

Description:

connect | **delete** | **get** | **head** | **options** | **post** | **put** | **trace** | **webdav** - Specifies the refused/allowed HTTP method.

Default values:

All methods are allowed by default.

Mode:

protocol configuration mode

Guidance:

When the system discovers the requested method is not allowed, it will disconnect the connection.

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# deny-method post
```

domain

Configure the domain name for the Web server. Use the no form to delete the domain name configuration.

Command:

domain *domain_name*

no domain *domain_name*

Description:

domain_name -Specifies the domain name of the Web server. You can specify up to 255 characters.

Default values:

None

Mode:

Web server configuration mode

Guidance:

Cannot configure the domain name for the default Web server.

You can configure up to 5 domain names for each Web server.

The domain name of the Web server follows the longest match principle as shown below:

```
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# domain abc.com
hostname(config-web-server)# exit
hostname(config-http-sigset)# web-server web_server2
hostname(config-web-server)# domain email.abc.com
```

With the above configurations, the traffic that accesses the news.abc.com will be matched to the web_server1, the traffic that accesses the www.email.abc.com will be matched to the web_server2, and the traffic that accesses the www.abc.com.cn will be matched to the default Web server.

Example:

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# domain www.abc.com
```

dst-ip

Configure the destination IP address for the IPS white list. Use the no form to delete the IP address.

Command:

dst-ip *A.B.C.D* | *A.B.C.D/M*

no dst-ip

Description:

A.B.C.D | *A.B.C.D/M*-Specifies the destination address IP address for the IPS white list to match.

Default values:

None

Mode:

IPS white list configuration mode

Guidance:

None

Example:

```
hostname(config)# ips whitelist white1
hostname(config-ips-whitelist)# dst-ip 10.1.1.2
```

enable

Enable the Web server. Use the no form to disable the Web server.

Command:

enable

no enable

Description:

None

Default values:

Enable the Web server.

Mode:

Web server configuration mode

Guidance:

The default Web server is enabled by default and it cannot be disabled

Example:

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# enable
```

exec block-ip add

Add an IP address that will be able to be blocked.

Command:

exec block-ip add {**ip** *ipv4-address* |**ipv6** *ipv6-address*} [**vrouter** *vr-name*] **timeout** *timeout*

Description:

ip *ipv4-address* | **ipv6** *ipv6-address* - Add a specified IP address that will be able to be blocked.

timeout *timeout* -Specifies the period (in seconds) of blocking the IP of the attacker. The value ranges from 60 to 3600. Once the time expired, the IP address will automatically be deleted from the blocked IP list.

vr-name -Specifies the VR where the IP address locates.

Default values:

vr-name – trust-vr

Mode:

execution mode

Guidance:

Non-root VSYS does not support this command.

Example:

```
hostname# exec block-ip add ipv4 100.10.10.1 timeout 60
```

exec block-ip remove

Delete the IP address that are blocked from the blocked IP list.

Command:

exec block-ip remove {**all** | **ipv4** *ipv4-address* |**ipv6** *ipv6-address* } [**vrouter** *vr-name*]}

Description:

all - Deletes all blocked IP addresses.

ipv4 *ipv4-address*|**ipv6** *ipv6-address* - Deletes the specified blocked IP address.

vr-name - Specifies the VR where the IP address locates.

Default values:

vr-name – trust-vr

Mode:

execution mode

Guidance:

Non-root VSYS does not support this command.

Example:

hostname# **exec block-ip remove ipv4 100.10.10.1**

exec block-service add

Add a service item that will be able to be blocked.

Command:

exec block-service add {**src-ipv4** *src-ipv4-address* **dst-ipv4** *dst-ipv4-address*|**src-ipv6** *src-ipv6-address* **dst-ipv6** *dst-ipv6-address*} [**vrouter** *vr-name*] **dst-port** *port-number* **proto** *protocol*

Description:

src-ipv4 *src-ipv4-address* - Specifies the source IPv4 address of the service.

dst-ipv4 *dst- ipv4-address* - Specifies the destination IPv4 address of the service.

src-ipv6 *src-ipv6-address* - Specifies the source IPv6 address of the service.

dst-ipv6 *dst-ipv6-address* - Specifies the destination IPv6 address of the service.

vrouter *vr-name* - Specifies the name of the VRouter.

dst-port *port-number* - Specifies the destination port of the service. The value ranges from 1 to 65535.

proto *protocol* - Specifies the protocol of the service. The value ranges from 1 to 255.

Default values:

vr-name – trust-vr

Mode:

execution mode

Guidance:

Non-root VSYS does not support this command.

Example:

hostname# **exec block-service add src-ipv4** 100.10.10.1 **dst-ipv4** 100.20.10.4 **dst-port** 1025 **proto** 23

exec block-service remove

Delete the service items that are blocked.

Command:

exec block-service remove {**all** | {**src-ipv4** *src-ipv4-address* **dst-ipv4** *dst-ipv4-address*|**src-ipv6** *src-ipv6-address* **dst-ipv6** *dst-ipv6-address*} [**vrouter** *vr-name*] **dst-port** *port-number* **proto** *protocol*}

Description:

all - Deletes all blocked services.

src-ipv4 *src-ipv4-address* **dst- ipv4** *dst- ipv4-address* - Specifies the source IPv4 address and destination IPv4 address of the service.

src-ipv6 *src-ipv6-address* **dst-ipv6** *dst-ipv6-address* - Specifies the source IPv6 address of the service.

vrouter *vr-name* - Specifies the name of the VRouter.

dst-port *port-number* - Specifies the destination port of the service. The value ranges from 1 to 65535.

proto *protocol* - Specifies the protocol of the service. The value ranges from 1 to 255.

Default values:

vr-name – trust-vr

Mode:

execution mode

Guidance:

Non-root VSYS does not support this command.

Example:

```
hostname# exec block-service remove all
```

exec ips

Enable/disable the IPS function.

Command:

Enable the function: **exec ips enable**

Disable the function: **exec ips disable**

Description:

None

Default values:

None

Mode:

execution mode

Guidance:

- This command is valid for the platforms with the IPS license installed.
- After executing the **exec ips enable**command, you must restart the device to enable the IPS function.
- After enabling the IPS function, the maximum number of concurrent sessions decreases. After executing the**exec ips disable**command, the IPS function will be disabled immediately but the maximum number of concurrent sessions will remain the same. After the device reboots, the maximum number of concurrent session will be restored to the original value.
- Non-root VSYS does not support this command.

Example:

```
hostname# exec ips enable
```

external-link

Configure the URL of external link. The URL must be an absolute path, which indicates that you must enter the protocol, i.e. http://, https:// or ftp://. For example, http://www.abc.com/script represents that all files located under this path can be referenced by the Web server. Use the no form to delete the specified URL of the external link.

Command:

external-link *url*

no external-link *url*

Description:

url - Specifies the URL of external link.

Default values:

None

Mode:

Web server configuration mode

Guidance:

For each Web server, you can configure up to 32 URLs of external link.

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server www.abc.com
hostname(config-web-server)# external-link http://www.abc.com/script
```

external-link-check

Enable the function of external link check to control the referenced actions performed by the Web server. Use the no form to disable this function.

Command:

```
external-link-check enable action {reset | log}
no external-link-check enable
```

Description:

reset | log - Specifies the actions performed to the behavior of Web site external link.

- reset - If discovering the behavior of Web site external link, reset the connection (TCP) or send the packets (UDP) to notify the unreachable destination and generate the logs.
- log - If discovering the behavior of Web site external link, only generate the logs.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None.

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server www.abc.com
hostname(config-http-web-server)# external-link-check enable action reset
```

filter-class

When configuring a signature set, you can create a filter rule. And in this filter rule, you can specify the desired signatures by using filter conditions. Use the following command to create a filter rule and enter into the filter rule configuration mode. Use the no form to delete this rule.

Command:

filter-class id [**name** *name*]

no filter-class id

Description:

id - Specifies the ID of the filter rule.

name *name*- Specifies the name of the filter rule.

Default values:

None

Mode:

IPS Profile configuration mode.

Guidance:

None

Example:

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

hostname(config-http-sigset)# **filter-class 1 name test2**

http-request-flood auth

Configure the authentication method for the HTTP request flood protection. The system judge whether the source IP address of the HTTP request is valid or not by authentication, thus identifying the attack traffic and executing the protection. If it is failed to authenticate a certain source IP address, the system will block the HTTP request generated by the source IP address. Use the no form to cancel the configurations.

Command:

http-request-flood auth {**auto-js-cookie** | **auto-redirect** | **manual-CAPTCHA** | **manual-confirm**} [**crawlers-friendly**]

no http-request-flood auth

Description:

auto-js-cookie | **auto-redirect** | **manual-CAPTCHA** | **manual-confirm**

Specifies the authentication method:

- **auto-js-cookie** – Automatic (JS Cookie). This authentication method is automatically completed by the Web browser.

- **auto-redirect** – Automatic (Redirect). This authentication method is automatically completed by the Web browser.
- **manual-CAPTCHA** – Manual (Access confirmation). When using this authentication method, the user that initiates the HTTP requests must click the OK button to complete the authentication.
- **manual-confirm** – Manual (Verification code). When using this authentication method, the user that initiates the requests must enter the verification code to complete the authentication.

crawlers-friendly - With this parameter entered, the system will not authenticate the crawlers.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# http-request-flood auth auto-js-cookie
```

http-request-flood enable

Enable the HTTP request flood protection function and set the request threshold. When the HTTP request rate reaches the configured threshold, the system concludes that the HTTP request flood happens and it enable the HTTP request flood protection function. Use the no form to disable the function.

Command:

http-request-flood enable [**threshold request** *value*]

no http-request-flood enable

Description:

threshold request *value* - Specifies the request threshold. The value ranges from 0 to 1000000 per second.

Default values:

The default value is 1500 per second.

Mode:

Web server configuration mode

Guidance:

None

Example:

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

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)# **http-request-flood enable**

http-request-flood proxy-limit

Configure the proxy rate limit. After configuring the proxy rate limit, the system checks whether each source IP belongs to the proxy server. If it belongs to the server, the system limits the proxy rate based on the proxy rate limit. Use the no form to cancel the proxy rate limit.

Command:

http-request-flood proxy-limit threshold *value* {**blockip timeout** *value* | **reset**} [**nolog**]

no http-request-flood proxy-limit

Description:

threshold *value* - Specifies the threshold for the request rate. If the received request rate exceeds the configured threshold and the http request flood protection is enabled, the system will perform the corresponding limitations. The value ranges from 0 to 1000000.

blockip timeout *value* | **reset** - Specifies the limitations that the system performed to the request rate that exceeds the configured threshold.

- **blockip timeout** *value* – Block the source IP address from which the received request rate exceeds the configured threshold. Use the value parameter to specify the period of blocking. The value ranges from 60 to 3600.
- **reset** – Reset the requests that exceed the configured threshold.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# http-request-flood proxy-limit threshold 10000 reset nolog
```

http-request-flood request-limit

Configure the access rate limit. After configuring the access rate limit, the system limits the access rate for each source IP address. Use the no form to cancel the access rate limit.

Command:

http-request-flood request-limit threshold *value* {**blockip timeout** *value* | **reset**} [**nolog**]

no http-request-flood request-limit

Description:

threshold *value* - Specifies the threshold for the access rate. If the received request rate exceeds the configured threshold and the http request flood protection is enabled, the system will perform the corresponding limitations. The value ranges from 0 to 1000000.

blockip timeout *value* | **reset** - Specifies the limitations that the system performed to the request rate that exceeds the configured threshold.

- **blockip timeout** *value* – Block the source IP address from which the received request rate exceeds the configured threshold. Use the value parameter to specify the period of blocking. The value ranges from 60 to 3600.
- **reset** – Reset the requests that exceed the configured threshold.

nolog - Do not record logs.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# http-request-flood request-limit threshold 10000 blockip timeout 60
```

http-request-flood statistics

Enable the URL request statistics function. Use the no form to cancel the URL request statistics function.

Command:

http-request-flood statistics enable

no http-request-flood statistics enable

Description:

None

Default values:

None

Mode:

Web server configuration mode

Guidance:

Only after executing the **http-request-flood statistics enable**command, the **show ips sigset** *sigset-name* **web-server** *server-name* **http-request-flood req-stat top**command can take effect.

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# http-request-flood statistics enable
```

http-request-flood white-list

Configure the white list for the HTTP request flood protection function. The system will not check the source IP addresses that are added to the white list. Use the no form to cancel the white list configurations.

Command:

http-request-flood white-list *address_entry* no http-request-flood white-list

Description:

address_entry - Specifies the address entry that will not be checked.

Default values:

None

Mode:

Web server configuration mode

Guidance:

- The address entry cannot be domain names and IPv6 addresses
- If the traffic of the source IP addresses in the white list exceeds the request threshold, the HTTP request flood protection function will be enabled

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# http-request-flood white-list addr1
```

http-request-flood x-forward-for

Configure the value of the x-forward-for field of HTTP for HTTP request flood protection. After the configuration, the system will make a statistics of the access frequency of the above field. When the number of HTTP connecting request per second towards this URL reaches the threshold and this lasts 20 seconds, the system will treat it as a HTTP request flood attack.Use the no form to cancel the value configuration of the x-forward-for field.

Command:

http-request-flood x-forward-for {**first** | **last** | **all**}

no http-request-flood x-forward-for

Description:

first | **last** | **all** - Specifies the value of the x-forward-for field of HTTP for HTTP request flood protection. **first** is the first value of the x-forwarded-for field, and **last**is the last value of the x-forwarded-for field, and **all**is the all value of the x-forwarded-for field.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# http-request-flood x-forward-for first
```

http-request-flood x-real-ip

Enable the x-real-for field statistics for HTTP request flood protection. When enabled, the system calculates the value of the x-real-for field.Use the no form to cancel the configuration.

Command:

```
http-request-flood x-real-ip enable
no http-request-flood x-real-ip
```

Description:

None

Default values:

None

Mode:

Web server configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# http-request-flood x-real-ip enable
```

iframe-check

Enable the function of hides iframe check and configure the function. Through the iframe check, the system recognizes whether there is a hidden iframe HTML page, so as to log or reset the connection. Use the no form to disable this function.

Command:

iframe-check enable action {**log** | **reset**}

no iframe-check enable

Description:

reset | **log** - Specify the action for the HTTP request that hides iframe behavior.

- **reset** – If discovering the behavior of hides iframe, reset the connection (TCP) or send the packets (UDP) to notify the unreachable destination and generate the logs.
- **log** – If discovering the behavior of hides iframe, only generate the logs.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None.

Example:

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# iframe-check enable action log
```

iframe width

Configure the limits of height and width for the iframe check function. Then System will check the iframe of HTML page according to the given height and width. When one value of the height or width in HTML page is less than or equal to the given value, system will identify the happening of hidden iframe attack. and then log or reset the connection. Use the no form to cancel the configurations.

Command:

iframe width *width_value* **height** *height_value* no iframe

Description:

width *width_value* - Specifies the height value for the iframe, range from 0 to 4096.

height *height_value* - Specifies the width value of the iframe, range from 0 to 4096.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None.

Example:

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# iframe width 0 height 1
```

ips enable

Enable the IPS function for a certain security zone and specify the IPS Profile to be used. Use the no form to disable the IPS function.

Command:

ips enable {**no-ips** | **predef_default** | **predef_loose** | *profile-name*} {**egress** | **ingress** | **bidirectional**}

no ips enable

Description:

profile-name - Specifies a IPS profile for the current security zone.

egress - Performs the IPS check for the egress traffic of the current security zone.

ingress - Performs the IPS check for the ingress traffic of the current security zone.

bidirectional - Performs the IPS check for both the ingress and egress traffic of the current security zone.

Default values:

None

Mode:

security zone configuration mode

Guidance:

- If the policy rule has been bound with an IPS Profile and the source and destination security zones have been bound with an IPS Profile simultaneously, the system will perform the IPS check according to the following order of priority: IPS Profile bound to the policy rule, IPS Profile bound to the destination security zone, IPS Profile bound to the source security zone.
- For each security zone, you can only bind one IPS Profile with it.

Example:

```
hostname(config)# zone trust
hostname(config-zone-trust)# ips enable test bidirectional
```

ips log aggregation

System can merge IPS logs which have the same protocol ID, the same VSYS ID, the same Signature ID, the same log ID, and the same merging type.Thus it can help reduce logs and avoid to receive redundant logs.

Command:

ips log aggregation {**by-src** | **by-dst** | **by-src-dst**}

Description:

by-src - Merge the IPS logs with the same Source IP.

by-dst - Merge the IPS logs with the same Destination IP.

by-src-dst - Merge the IPS logs with the same Source IP and the same Destination IP.

Default values:

Disabled

Mode:

global configuration mode

Guidance:

- Only support to merge IPS logs.
- Non-root VSYS does not support this command.

Example:

```
hostname(config)# ips log aggregation by-src
```

ips mode

Specify the IPS work mode. The system supports the IPS online emulation mode and IPS mode.

Command:

ips mode {**ips** | **ips-logonly**}

Description:

ips - Uses the IPS mode. Besides providing the warnings and logs for the abnormal protocols and network attacks, the system can perform the block or reset operation to the discovered attacks.

ips-logonly - Uses the IPS online emulation mode. The system provides the warnings and logs for the abnormal protocols and network attacks, and cannot perform the block or reset operation to the discovered attacks.

Default values:

IPS mode

Mode:

global configuration mode

Guidance:

Non-root VSYS does not support this command.

Example:

```
hostname(config)# ips mode ips-logonly
```

ips profile

Create a IPS profile and enter the IPS Profile configuration mode. If the specified name already exists, the system will enter the IPS Profile configuration mode directly. Use the no form to delete the specified IPS Profile.

Command:

ips profile {**no-ips** | **predef_default** | **predef_loose** | *profile-name*}

no ips profile *profile-name*

Description:

profile-name - Specifies the name of the IPS Profile.

Default values:

None

Mode:

global configuration mode

Guidance:

Non-root VSYS also supports predefined IPS Profiles.

Example:

```
hostname(config)# ips profile test
hostname(config-ips-profile)#
```

ips signature

Disable a certain signature. Use the no form to re-enable this signature.

Command:

ips signature id disable

no ips signature id disable

Description:

id - Specifies the ID of the enabled/disabled signature.

Default values:

None

Mode:

global configuration mode

Guidance:

- When a certain signature is disabled, it is the disabled status in the signature set as well.
- Non-root VSYS does not support this command.

Example:

```
hostname(config)# ips signature 160009 disable
```

ips sigset

Use the existing pre-defined protocol as a template and create a user-defined protocol based on this template. Enter the protocol configuration mode. If the specified name already exists, the system will enter the protocol configuration mode directly. Use the no form to delete the specified protocol.

Command:

ips sigset *sigset-name* [**template** {**dhcp** | **dns** | **finger** | **ftp** | **http** | **imap** | **ldap** | **msrpc** | **mssql** | **mysql** | **netbios** | **nntp** | **oracle** | **other-tcp** | **other-udp** | **pop3** | **smtp** | **snmp** | **sunrpc** | **telnet** | **tftp** | **voip**}]

no ips sigset *sigset-name*

Description:

sigset-name - Specifies the name of the protocol.

dhcp | dns … | voip - Selects a predefined protocol as the template.

Default values:

None

Mode:

global configuration mode

Guidance:

- The predefined protocol cannot be deleted and edited.
- The user-defined protocol cannot have the same name as the predefined protocol.
- Cannot create signature set based on the user-defined signature set.
- Protocols of the same type cannot be added to one IPS Profile. For example, two protocols created based on the HTTP template cannot be added to one IPS Profile.

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)#
```

ips whitelist

Configure the white list for IPS. The system will release data packets that match the IPS whitelist, no longer detect and defend, thereby reducing the rate of false reports of threats. IPS whitelist matching criteria include source address, destination address, signature ID, and VRouter. The user needs to configure at least one condition; when the user configure multiple conditions, the data packets need to meet all the conditions and then the system will release. Use the no form to delete the specified white list.

Command:

ips whitelist *list-name*

no ips whitelist *list-name*

Description:

list-name- Specifies the name of IPS whitelist. The length of it ranges from 1 to 255.

Default values:

None

Mode:

global configuration mode

Guidance:

None

Example:

```
hostname(config)# ips whitelist white1
hostname(config-ips-whitelist)#
```

issue-date

Configure the issue-date parameter to include signatures, issued in the specified year, in the filter rule.

Command:

issue-date *year*

no issue-date *year*

Description:

year - Enter the year when the vulnerability was issued. The range varies from 2000 to 2004.

Default values:

None

Mode:

Filter rule configuration mode;

Guidance:

None

Example:

```
hostname(config)# ips profile test
hostname(config-ips-profile)# filter-class 1
hostname(config-ips-filter-class)# issue-date 2006
```

max-arg-length

Specify the maximum length for the POP3 client command parameters and the action performed when discovering this kind of anomaly. Use the no form to restore the length setting to the default value.

Command:

max-arg-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-arg-length (Restore the length to the default value)

Description:

length - Specifies the maximum length for the POP3 client command parameters (in byte).

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service**- Block the service of the attacker and specify a block duration. **block-ip**- Block the IP address of the attacker and specify a block duration. **log-only**- Record a log. **reset**- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 40 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset pop3-cus template pop3
hostname(config-pop3-sigset)# max-arg-length 30 action log-only
```

max-bind-length

Specify the allowed maximum length for the MSRPC binding packet and the action performed when discovering this kind of anomaly . Use the no form to restore the length setting to the default value.

Command:

max-bind-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-bind-length- Restore the length to the default value.

Description:

length - Specifies the maximum length for the binding packet (in byte). The value ranges from 16 to 65535.

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service** -Block the service of the attacker and specify a block duration. **block-ip**- - Block the IP address of the attacker and specify a block duration. **log-only**- Record a log. **reset**- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 2048 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset msrpc-cus template msrpc
hostname(config-msrpc-sigset)# max-bind-length 3000 action log-only
```

max-black-list

Specify the maximum number of URLs that a Web server black list can contain. When a user accesses a statistic page, the system will add the URL of this page to the black list if the system discovers that the contents in this page violate the external link check and the uploading path check. When a user accesses this statistic page again, the URL will hit the black list, thus, improving the processing speed of the system. Use the no form to cancel the above setting.

Command:

max-black-list *size*

no max-black-list

Description:

size - Specifies the maximum length of URLs that a Web server black list can contain.

Default values:

0

Mode:

Web server configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server www.abc.com
hostname(config-http-web-server)# max-black-list 4096
```

max-cmd-line-length

Specify the maximum length of the FTP command line/POP3 client command line/SMTP client command line and the action performed when discovering this kind of anomaly . When calculating the length, both the line feed and carriage return are calculated. Use the no form to restore the length setting to the default value.

Command:

max-cmd-line-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-cmd-line-length- Restore the length to the default value.

Description:

length - Specifies the maximum length of the command line (in byte). The maximum length of FTP command line ranges from 5 to 1024. The maximum length of POP/SMTP client command line ranges from 64 to 1024.

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service** - Block the service of the attacker and specify a block duration. **block-ip**- Block the IP address of the attacker and specify a block duration. **log-only**- Record a log. **reset**- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 512 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset test1 template ftp
hostname(config-ftp-sigset)# max-cmd-line-length 80 action log-only
```

max-content-filename-length

Specify the allowed maximum length of the attachment name of SMTP emails and the action performed when discovering this kind of anomaly. Use the no form to restore the length setting to the default value.

Command:

max-content-filename-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-content-filename-length- Restore the length to the default value.

Description:

length - Specifies the maximum length of the attachment name of SMTP emails (in byte). The value ranges from 64 to 1024.

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service** -Block the service of the attacker and specify a block duration. **block-ip**-Block the IP address of the attacker and specify a block duration. **log-only**Record a log.**reset**Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 128 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset smtp-cus template smtp
hostname(config-smtp-sigset)# max-content-filename-length 512 action log-only
```

max-content-type-length

Specify the allowed maximum length of the SMTP Content-Type value and the action performed when discovering this kind of anomaly. Use the no form to restore the length setting to the default value.

Command:

max-content-type-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-content-type-length- Restore the length to the default value.

Description:

length - Specifies the maximum length of the SMTP Content-Type value (in byte). The value ranges from 64 to 1024.

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service** - Block the service of the attacker and specify a block duration. **block-ip**- Block the IP address of the attacker and specify a block duration. **log-only**- Record a log.**reset**Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 128 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset smtp-cus template smtp
hostname(config-smtp-sigset)# max-content-type-length 256 action log-only
```

max-failure

For each POP3/SMTP session, specify the allowed maximum number of times of errors returned from POP3/SMTP server and the action performed when discovering this kind of anomaly. Use the no form to restore the setting to the default value.

Command:

max-failure *times* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-failure- Restore the number of times to the default value.

Description:

times - For each POP3 session, specifies the allowed maximum number of times of errors returned from the POP3 server. The value ranges from 0 to 512.

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service**- Block the service of the attacker and specify a block duration. **block-ip**- Block the IP address of the attacker and specify a block duration. **log-only**- Record a log. **reset**- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

times － 0 (no limitation)

Mode:

protocol configuration mode

Guidance:

For each POP3/SMTP session, specifying the allowed maximum number of times of errors returned from POP3/SMTP server can prevent the invalid attempts effectively.

Example:

```
hostname(config)# ips sigset pop3-cus template pop3
hostname(config-pop3-sigset)# max-failure 8 action log-only
```

max-input-length

Specify the allowed maximum length of Telnet username and the action performed when discovering this kind of anomaly. Use the no form to restore the setting to the default value.

Command:

max-input-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-input-length- Restore the number of times to the default value

Description:

length - Specifies the maximum length of Telnet username and password (in byte). The value ranges from 6 to 1024.

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service** - Block the service of the attacker and specify a block duration. **block-ip**- Block the IP address of the attacker and specify a block duration. **log-only**- Record a log. **reset**- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 128 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset telnet-cus template telnet
hostname(config-telnet-sigset)# max-input-length 30 action log-only
```

max-path-length

Specify the allowed maximum length of two SMTP client commands, i.e. reverse-path and forward path and the action performed when discovering this kind of anomaly. Use the no form to restore the setting to the default value.

Command:

max-path-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | reset}

no max-path-length- Restore the length setting to the default value

Description:

length - Specifies the maximum length of two SMTP client commands, i.e. reverse-path and forward path (in byte). The value ranges from 16 to 512, including punctuation marks.

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service** - Block the service of the attacker and specify a block duration. **block-ip**- - Block the IP address of the attacker and specify a block duration. **log-only**- Record a log. **reset**- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 256 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset smtp-cus template smtp
hostname(config-smtp-sigset)# max-path-length 128 action log-only
```

max-reply-line-length

Specify the allowed maximum length of SMTP server responses and the action performed when discovering this kind of anomaly. When calculating the length, both the carriage return and line feed are calculated. Use the no form to restore the setting to the default value.

Command:

max-reply-line-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-reply-line-length- Restore the length setting to the default value

Description:

length - Specifies the maximum length of SMTP server responses (in byte). The value ranges from 64 to 1024.

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service**- Block the service of the attacker and specify a block duration. **block-ip**- - Block the IP address of the attacker and specify a block duration. **log-only**- Record a log. **reset**- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 512 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset smtp-cus template smtp
hostname(config-smtp-sigset)# max-reply-line-length 1024 action log-only
```

max-request-length

Specify the allowed maximum length of MSRPC request packets and the action performed when discovering this kind of anomaly. Use the no form to restore the setting to the default value.

Command:

max-request-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-request-length- Restore the length setting to the default value

Description:

length - Specifies the maximum length of MSRPC request packets (in byte). The value ranges from 16 to 65535.

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}- **block-service**- Block the service of the attacker and specify a block duration. **block-ip**- - Block the IP address of the attacker and specify a block duration. **log-only**- Record a log. **reset**- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 65535 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset msrpc-cus template msrpc
hostname(config-msrpc-sigset)# max-request-length 60000 action log-only
```

max-rsp-line-length

Specify the allowed maximum length of FTP responses and the action performed when discovering this kind of anomaly. Use the no form to restore the setting to the default value.

Command:

max-rsp-line-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-rsp-line-length- Restore the length setting to the default value.

Description:

length - Specifies the maximum length of FTP responses (in byte). The value ranges from 5 to 1024.

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service**- Block the service of the attacker and specify a block duration. **block-ip**- Block the IP address of the attacker and specify a block duration. **log-only**- Record a log. **reset**- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 512 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset test1 template ftp
hostname(config-ftp-sigset)# max-rsp-line-length 100 action log-only
```

max-scan-bytes

Specify the maximum length of scanning. Use the no form to restore the setting to the default value.

Command:

max-scan-bytes *length*

no max-scan-bytes

Description:

length - Specifies the maximum length of scanning (in byte).

Default values:

length － 4096

Mode:

protocol configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset test1 template other-tcp
hostname(config-other-tcp-sigset)# max-rsp-line-length 1000
```

max-text-line-length

Specify the allowed maximum length of the email text in SMTP client and the action performed when discovering this kind of anomaly. When calculating the length, both the carriage return and line feed are calculated. Use the no form to restore the setting to the default value.

Command:

max-text-line-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-text-line-length- Restore the length setting to the default value

Description:

length - Specifies the allowed maximum length of the email text in SMTP client (in byte). The value ranges from 64 to 2048.

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service**- Block the service of the attacker and specify a block duration. **block-ip**- Block the IP address of the attacker and specify a block duration. **log-only**- Record a log. **reset**- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length － 1000 byte

Mode:

protocol configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset smtp-cus template smtp
hostname(config-smtp-sigset)# max-text-line-length 1024 action log-only
```

max-uri-length

Specify the allowed maximum length of the HTTP URL and the action performed when discovering this kind of anomaly. Use the no form to restore the setting to the default value.

Command:

max-uri-length *length* **action** {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**}

no max-uri-length- Restore the length setting to the default value

Description:

length - Specifies the allowed maximum length of URL (in byte). The value ranges from 64 to 4096.

action {**block-service** *timeout*| **block-ip** *timeout* | **log-only** | **reset**} - **block-service**- Block the service of the attacker and specify a block duration. **block-ip**- Block the IP address of the attacker and specify a block duration. **log-only**- Record a log. **reset**- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 4096 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# max-uri-length 1000 action log-only
```

max-white-list

Specify the maximum number of URLs that a Web server white list can contain. When a user accesses a statistic page, the system will add the URL of this page to the white list if the system discovers that the contents in this page do not violate the external link check and the uploading path check. When a user accesses this statistic page again, the URL will hit the white list, thus, improving the processing speed of the system. Use the no form to cancel the above setting.

Command:

max-white-list *size*

no max- white-list

Description:

length- Specify the maximum number of URLs that a Web server white list can contain. The value ranges from 0 to 4096.

Default values:

0

Mode:

Web server configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server www.abc.com
hostname(config-http-web-server)# max-white-list 4096
```

pcap

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

Command:

pcap enable

pcap disable

Description:

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

disable -Do not capture the abnormal packets.

Default values:

disable。

Mode:

Filter rule configuration mode;

search rule configuration mode.

Guidance:

None

Example:

```
hostname(config)# ips profile test
hostname(config-ips-profile)# pcap enable
```

protocol-check

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

Command:

protocol-check disable

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

Description:

enable -Enable the protocol legality check.

block-service - Block the service of the attacker and specify a block duration.

block-ip -Block the IP address of the attacker and specify a block duration.

log-only- Record a log.

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

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

Default values:

The system disables the protocol legality check.

Mode:

protocol configuration mode.

Guidance:

None

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# protocol-check strict
hostname(config-http-sigset)# protocol-check enable action log-only
```

protocol

Configure the protocol parameter to include signatures, related to the specified protocol, in the filter rule.

Command:

```
protocol {DNS | FTP | HTTP | …}
no protocol { DNS | FTP | HTTP | …}
```

Description:

DNS | FTP | HTTP | … - Enter the protocol name. You can press the Tab key after the **protocol**parameter to see the entire protocol list.

Default values:

None

Mode:

Filter rule configuration mode;

Guidance:

None

Example:

```
hostname(config)# ips profile test
hostname(config-ips-profile)# filter-class 1
hostname(config-ips-filter-class)# protocol Telnet
```

referer-white-list

Configure the exception URL for the Web server. Once configured, the URL can refer to the Web site, and the other unadded cannot reference the Web site. Use the no form to delete the URL.

Command:

referrer-white-list *url_string*

no referrer-white-list *url_string*

Description:

url_string - Specifies the exception URL for Web server. The length of URL is in the range of 1-255 characters.

Default values:

None

Mode:

Web server configuration mode

Guidance:

You can configure up to 32 URL paths.

Example:

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# referrer-white-list www.abc.com
```

referer-white-list-check

Enable the referer checking function and configure it. After the configuration, the system can reset the connection or record log for the HTTP Request of the hotlinking and CSRF (Cross Site Request Forgery) attack. Use the no form to disable the function.

Command:

referrer-white-list-check enable action {**log** | **reset**}

no referrer-white-list-check enable

Description:

reset | log Specifies the action for the hotlinking and CSRF attack check for HTTP protocol:

- **reset**: If discovering the hotlinking and CSRF attack, the system resets the connection (TCP) or sends the packets (UDP) to notify the unreachable destination and generate the logs.
- **log**: If discovering the hotlinking and CSRF attack, the system only generates the logs.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# referrer-white-list-check enable action log
```

response-bypass

Specify does not scan the HTTP server data packets.

Command:

response-bypass

no response-bypass

Description:

None

Default values:

None

Mode:

protocol configuration mode

Guidance:

Only for HTTP protocol

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# response-bypass
```

search-class

When configuring a signature set, you can create a search rule. And in this search rule, you can specify the desired signatures by using search conditions. Use the following command to create a search rule and enter into the search rule configuration mode. Use the no form to delete this rule.

Command:

search-class *id* **name** *name*

no search-class *id*

Description:

id -Specifies the ID of the search rule.

name *name* -Specifies the name of the search rule.

Default values:

None

Mode:

IPS Profile configuration mode.

Guidance:

None

Example:

```
hostname(config)# ips profile test
hostname(config-ips-profile)# search-class 1 name test1
```

search-condition

When using a search condition to search signatures, you can specify the information of the signature. The system will perform the fuzzy searching among the following fields: signature ID, signature name, CVE-ID, and signature description:

Command:

search-condition *description*

no search-condition *description*

Description:

description - Enter the information of the desired signatures.

Default values:

None

Mode:

Search rule configuration mode.

Guidance:

None

Example:

```
hostname(config)# ips profile test
hostname(config-ips-profile)# search-class 1
hostname(config-ips-filter-class)# search-condition DNS
```

severity

Configure the severity parameter to include signatures, related to the specified severity, in the filter rule.

Command:

severity {Low | Medium | High}

no severity {Low | Medium | High}

Description:

Low | Medium | High - Enter the severity.

Default values:

None

Mode:

Filter rule configuration mode;

Guidance:

None

Example:

```
hostname(config)# ips profile test
hostname(config-ips-profile)# filter-class 1
hostname(config-ips-filter-class)# severity Low
```

signature id

Configure the signature id parameter to include signatures, related to the specified id, in the search rule.

Command:

signature id *id*

no signature id *id*

Description:

id - Enter the signature ID.

Default values:

None

Mode:

search rule configuration mode

Guidance:

None

Example:

```
hostname(config)# ips profile test
hostname(config-ips-profile)# search-class 1
hostname(config-ips-filter-class)# signature id 105001
```

signature-id

Configure the signature ID for the IPS white list. Use the no form to delete the signature ID.

Command:

signature-id *id*

no signature-id *id*

Description:

id - Specifies the signature ID for the IPS white list to match.

Default values:

None

Mode:

IPS white list configuration mode

Guidance:

None

Example:

```
hostname(config)# ips whitelist white1
hostname(config-ips-whitelist)# signature-id 105002
```

sigset

Add the protocol configurations to the IPS Profile. Use the no form to delete the protocol configuration from the IPS Profile.

Command:

sigset *user-defined-profile*

no sigset *user-defined-profile*

Description:

user-defined-profile - Adds the user-defined signature set to the IPS Profile.

Default values:

None

Mode:

IPS Profile configuration mode

Guidance:

None

Example:

```
hostname(config)# ips profile ips-profile1
hostname(config-profile)# sigset test
```

src-ip

Configure the source IP address for the IPS white list. Use the no form to delete the IP address.

Command:

src-ip *A.B.C.D* | *A.B.C.D/M*

no src-ip

Description:

A.B.C.D | *A.B.C.D/M* - Specifies the source IP address for the IPS white list to match.

Default values:

None

Mode:

IPS white list configuration mode

Guidance:

None

Example:

```
hostname(config)# ips whitelist white1
hostname(config-ips-whitelist)# src-ip 10.1.1.1
```

system

Configure the system parameter to include signatures, related to the specified system, in the filter rule.

Command:

system {Windows | Linux | FreeBSD | …}

no system { Windows | Linux | FreeBSD | …}

Description:

Windows | Linux | FreeBSD | … - Enter the OS name. You can press the Tab key after the **system**parameter to see the entire system list.

Default values:

None

Mode:

Filter rule configuration mode;

Guidance:

None

Example:

```
hostname(config)# ips profile test
hostname(config-ips-profile)# filter-class 1
hostname(config-ips-filter-class)# system Linux
```

sql-injection

Disable the SQL injection check. Use the no form to enable the SQL injection check.

Command:

sql-injection {cookie | cookie2 | post | referer | uri} disable

no sql-injection {cookie | cookie2 | post | referer | uri} disable

Description:

{cookie | cookie2 | post | referer | uri} disable - Disables the specified SQL injection check, namely HTTP Cookie, HTTP Cookie2, HTTP Post, HTTP Refer, or HTTP URI.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# sql-injection cookie disable
```

sql-injection-check

Enable the SQL injection check for HTTP protocol.

Command:

sql-injection-check enable [**sensitive** {**low** | **medium** | **high**}] [**action** {**reset** | **log**}] [**block** {**ip** | **service**} **timeout**] [**noblock**]

sql-injection-check disable

Description:

sensitive {low | medium | high} -Specifies the sensitivity level for the SQL injection check for HTTP protocol,**high**, **medium** or **low**. The higher sensitivity level you specify, the lower missing report ratio has.

reset | **log** -Specifies the action for the SQL injection check for HTTP protocol:

- **reset** – If discovering the SQL injection attack, the system resets the connection (TCP) or sends the packets (UDP) to notify the unreachable destination and generate the logs.
- **log** – If discovering the SQL injection, the system only generates the logs.

ip | **service** - Blocks the IP (ip)_of the SQL injection attacker or the service (service).

timeout - Specifies the period (in seconds) of blocking the IP of the attacker or the service. The value ranges from 60 to 3600.

noblock - Do not bock the IP of the attacker or the service.

Default values:

By default, the sensitivity level is low.

Mode:

Web server configuration mode

Guidance:

The severity level of the SQL injection attack is critical. Without configuring actions, the system will only generate logs when discovering SQL injection attack.

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server www.abc.com
hostname(config-web-server)# sql-injection-check enable
```

vr

Configure the VRouter for the IPS white list. Use the no form to delete the IP address.

Command:

vr *vr-name*

no vr

Description:

vr-name - Specifies the VRouter for the IPS white list to match.

Default values:

None

Mode:

IPS white list configuration mode

Guidance:

None

Example:

```
hostname(config)# ips whitelist white1
hostname(config-ips-whitelist)# src-ip 10.1.1.1
hostname(config-ips-whitelist)# vr trust-vr
```

web-acl

Configure the Web site path and specify the attributes. Use the no form to disable the function.

Command:

web-acl *url* {**static** | **deny**}

no web-acl *url*

Description:

url- Specifies Web site path.

static | **deny** - Specifies the attributes of Web site path:

- **static**- With this attribute specified, the resources in this Web site path can only be accessed as static resources (pictures and text). Otherwise, the system will perform the actions based on the configurations of the uploading path check function (**web-acl-check enable action** {**reset** | **log**}).
- **deny**- With this attribute specified, the resources in this Web site path cannot be accessed.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server www.abc.com
hostname(config-http-web-server)# web-acl www.eee.com deny
```

web-acl-check

Enable the uploading path check function to prevent the attacker from uploading malicious codes to the Web server. Use the no form to disable the function.

Command:

web-acl-check enable action {**reset** | **log**}

no web-acl-check enable

Description:

reset | **log** - Specifies the control action for the Web site uploading behavior:

- **reset**- If discovering the Web site uploading behavior, the system resets the connection (TCP) or sends the packets (UDP) to notify the unreachable destination and generate the logs.
- **log** – If discovering the Web site uploading behavior, the system only generates the logs.

Default values:

None

Mode:

Web server configuration mode

Guidance:

The severity level of the Web site uploading behavior is warnings.

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server www.abc.com
hostname(config-http-web-server)# web-acl-check enable action reset
```

web-server

Create a Web server and enters the Web server configuration mode. If the name already exists, the system will enter the Web server configuration mode directly. Use the no form to delete the Web server.

Command:

web-server {**default** | *server_name*}

no web-server *server_name*

Description:

default - Configure the default Web server. When creating a HTTP signature set, the system will create a default Web server.

server_name - Specifies the name for the created Web server. You can specify up to 21 characters.

Default values:

None

Mode:

protocol configuration mode

Guidance:

- The default Web server cannot be deleted or edited.
- You can configure up to 32 Web servers (excluding the default Web server) for each signature set.

Example:

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)#
```

xss-injection

Disable the XSS injection check. Use the no form to enable the XSS injection check.

Command:

```
xss-check {cookie | cookie2 | post | referer | uri} disable
no xss-injection {cookie | cookie2 | post | referer | uri} disable
```

Description:

{cookie | cookie2 | post | referer | uri} disable - Disables the specified XSS injection check, namely HTTP Cookie, HTTP Cookie2, HTTP Post, HTTP Refer, or HTTP URI.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# xss-injection uri disable
```

xss-check enable

Enable the XSS injection check for HTTP protocol.

Command:

xss-check enable [sensitive {low | medium | high}] [action {log | reset}] [block {ip | service} *timeout*] **[noblock]**

xss-check disable

Description:

sensitive {**low** | **medium** | **high**} - Specifies the sensitivity level for the XSS injection check for HTTP protocol **high**, **medium**or **low**. The higher sensitivity level you specify, the lower missing report ratio has.

reset | **log** - Specifies the action for the XSS injection check for HTTP protocol:

- **reset**- If discovering the XSS injection attack, the system resets the connection (TCP) or sends the packets (UDP) to notify the unreachable destination and generate the logs.
- **log** – If discovering the XSS injection, the system only generates the logs.

ip | **service** - Blocks the IP (**ip**) of the XSS injection attacker or the service (**service**).

timeout - Specifies the period (in seconds) of blocking the IP of the attacker or the service. The value ranges from 60 to 3600.

noblock - Do not block the IP of the attacker or the service.

Default values:

None

Mode:

Web server configuration mode

Guidance:

The severity level of the XSS injection attack is Critical. If you configure no action, the system will only record the logs.

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)# web-server www.abc.com
hostname(config-web-server)# xss-check enable
```

show ips

Display the configurations about IPS.

Command:

show ips configuration – Shows all information of IPS configurations.(Non-root VSYS does not support this command)

show ips profile [*profile-name*] [**signature-class** *signature-class-id*]- Shows all information of IPS Profile.

show ips sigset [*sigset-name*] – Shows all information of IPS protocol configurations.

show ips sigset *sigset-name* **web-server** *server-name* **http-request-flood auth-ck** – Shows the corresponding information of the authentication of HTTP request flood protection.

show ips sigset *sigset-name* **web-server** *server-name* **http-request-flood ip-top** {**max-rate** | **total**} – For HTTP request flood protection, shows the maximum rate ranking of the source IP addresses and the total number ranking.

show ips sigset *sigset-name* **web-server** *server-name* **http-request-flood req-stat** {**overview** {**by-day** | **by-hour** | **by-minute** | **by-second**} | **protect** {**by-day** | **by-hour** | **by-minute** | **by-second**} | **top**} – For HTTP request flood protection, shows the overview, protection information, and requested URL ranking.

show ips status – Shows the status of IPS.

show ips zone-binding – Shows the binding between the security zones and IPS Profiles.

Description:

sigset-name - Specifies the name of the protocol that you want to display.

profile-name - Specifies the name of the IPS profile that you want to display.

signature-class-id - Specifies the ID of the search rule or filter rule that you want to display.

web-server *server-name* - Specifies the name of the Web server that you want to display.

ip-top {**max-rate** | **total**} - Shows the maximum rate ranking of source IP addresses and the total number ranking.

req-stat {**overview** {**by-day** | **by-hour** | **by-minute** | **by-second**} - Shows the overview of the packets, including request numbers, request numbers of different methods (GET and POST), response numbers, response numbers of different status number (4XX and 5XX). You can show the information by days, hours, minutes, or seconds.

protect {**by-day** | **by-hour** | **by-minute** | **by-second**} - Shows the protection information of the packets, including request numbers, response numbers, and other information.

top - Shows the requested URL ranking.

Default values:

None

Mode:

any mode

Guidance:

After executing the **http-request-flood statistics enable**command, the **show ips sigset** *sigset-name* **web-server** *server-name* **http-request-flood req-stat top**command can take effect.

Example:

```
hostname(config)# show ips sigset

Total count: 53

==============================================================

IPS signature set dhcp

Default actions:

Attack-level Action Block Seconds

INFO log noblock 0

WARNING log noblock 0

CRITICAL log noblock 0

Max scan bytes per direction: 0(Unlimited)

Used by 1 IPS profiles:

test

--------------------------------------------------------
```

Perimeter Traffic Filtering

Overview

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.

You need to update the IP reputation database before enabling the IP Reputation function for the first time. For more information about how to update, see Updating IP Reputation Database.

Configuring Perimeter Traffic Filtering

To enable the Perimeter Traffic Filtering function on system, take the following steps:

1. Make sure your FSOS version supports Perimeter Traffic Filtering.

2. Import a TP license and reboot. The Perimeter Traffic Filtering will be enabled after the rebooting.

Enabling/Disabling Perimeter Traffic Filtering

To enable the perimeter traffic filtering based on zone and enter the perimeter traffic filtering configuration mode, in zone configuration mode, use the following command:

perimeter-traffic-filtering

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

no perimeter-traffic-filtering

Enabling/Disabling Perimeter Traffic Filtering Based on Risk IP List

For three types of risk IP list (IP Reputation list, User-defined black/white list and Third-party risk IP list), you can enable the perimeter traffic filtering based on different black/white list and specifies an action for the malicious traffic that hits the blacklist. In the perimeter traffic filtering configuration mode, use the following command:

- IP Reputation list: **ip-reputation category** {**bot** | **brute-forcer** | **compromised** | **ddos-attacker** | **proxy** | **scanner** | **spam** | **tornode**} {**drop** | **log-only** | **block-ip** *timeout*}
  - **bot | brute-forcer | compromised |ddos-attacker | proxy | scanner | spam | tornode** – Specify IP reputation categories, including Botnet, Brute-forcer, Compromised, ddos-attacker , Proxy, Scanner, Spam, Tor nodes.
  - **drop** – Drop packets if the malicious traffic hits the IP Reputation list.
  - **log-only** – Only generates logs if the malicious traffic hits the IP Reputation list.
  - **block-ip** *timeout* - Block the IP address and specify a block duration if the malicious traffic hits the IP Reputation list.
- • User-defined black/white list: **user-define [drop | log-only]**
  - **drop** – Drop packets if the malicious traffic hits the user-defined black/white list.
  - **log-only** – Only generates logs if the malicious traffic hits the user-defined black/white list.

To disable the perimeter traffic filtering based on different black/white list, in the perimeter traffic filtering configuration mode, use the following command:

- IP Reputation list: **no ip-reputation category** {**bot** | **brute-forcer** | **compromised** | **ddos-attacker** | **proxy** | **scanner** | **spam** | **tornode**}
- User-defined black/white list: **no user-define**

Configuring User-defined Black/White List

To enter the black/white list configuration mode, in the global configuration mode, use the following command:

perimeter-traffic-filtering

Add a IP entry to the user-defined black/white list, in black/white list configuration mode, use the following command:

userdefined-iplist [**id** *id*] **ip** *ip-address*

- **id** *id* – Specify the black/white list entry ID. If this parameter is not specified, the system will specifiy ID for list entry automatically.
- **ip** *ip-address* – Specify the IP address for the user-defined black/white list.

To delete the IP entry in the user-defined black/white list, in the black/white list configuration mode, use the following command:

no userdefined-iplist id *id*

Viewing User-defined Black/White List Information

To view the User-defined black/white list information, in any mode, use the following command:

show perimeter-traffic-filtering userdefined

Viewing the Hit Count of Black/White List

To view the hit count of black/white list, in any mode, use the following command:

show perimeter-traffic-filtering hit-count

Viewing the Specific IP Hit Count of Black/White List

To view the specific IP hit count of black/white list, in any mode, use the following command:

show perimeter-traffic-filtering ip *ip-address*

Updating IP Reputation Database

By default FSOS updates the IP reputation database everyday automatically. You can change the update configuration as needed. The configurations of updating IP reputation database include:

- Configuring an IP reputation update mode
- Configuring an update server
- Specifying an update schedule
- Updating now
- Importing an IP reputation file
- Viewing IP reputation information
- Viewing IP reputation update information

Configuring an IP Reputation Update Mode

System supports both manual and automatic update modes. To configure an IP reputation update mode, in the global configuration mode, use the following command:

ip-reputation update mode {**auto** | **manual**}

- **auto** – Specifies the automatic IP reputation update mode. This is the default mode.
- **manual** – Specifies the manual IP reputation update mode.

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

no ip-reputation update mode

Configure an Update Server

System provides two default update servers: https://Update1.fw1.fs.com and https://Update2.fw2.fs.com. You can also configure another up to three update servers to download the latest IP reputation as needed. To configure the update the server, in the global configuration mode, use the following command:

ip-reputation update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*}

- **server1** | **server2** | **server3** – Specifies the update server you want to configure. The default value of **server1**is https://Update1.fw1.fs.com , and the default value of **server2**is https://Update2.fw2.fs.com.

- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an *ip-address*s, or a *domain-name*, for example, Update1.fw1.fs.com.

To cancel the specified update the server, in the global configuration mode, use the following command:

no ip-reputation signature update {**server1** | **server2** | **server3**}

Specifying a HTTP Proxy Server

When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update automatically and normally.

To specify the HTTP proxy server for the IP reputation signature database updating, use the following command in the global configuration mode:

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

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

To cancel the proxy server configurations, use the **no perimeter-traffic-filter update proxy-server** {**main** | **backup**}command.

Specifying an Update Schedule

By default, system automatically updates the IP reputation database every day. To reduce the update server's workload, the time of daily update is random. To specify the schedule and specific time for the update, in the global configuration mode, use the following command:

ip-reputation update schedule {**daily** [*HH:MM*] | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} | **hourly** *minute* }

- **daily** [*HH:MM*] – Updates the database every day *HH:MM* is used to specify the time of update, for example, 09:00.
- **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} – Updates the database every week. Parameter **mon | tue | wed | thu | fri | sat | sun**is used to specify the specific date in a week.
- **hourly** *minute* – Updates the database every three hours. This option is the default update schedule *minute*is used to specify the specific minute in one hour.

Updating Now

For both manual and automatic update modes, you can update the IP reputation database immediately as needed. To update the IP reputation database now, in any mode, use the following command:

exec ip-reputation update

- **exec av signature update** – Only updates the incremental part between the current IP reputation database and the latest IP reputation database released by the update server.

Importing an IP Reputation File

In some cases, your device may be unable to connect to the update server to update the IP reputation database. To solve this problem, system provides the IP reputation file import function, i.e., importing the IP reputation files to the device from an FTP, TFTP server or USB disk, so that the device can update the IP reputation database locally. To import the IP reputation file, in the execution mode, use the following command:

import ip-reputation from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *ip-address* – Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP server.
- **vrouter** *vr-name* – Specifies the VRouter of the FTP or TFTP server.
- *file-name* – Specifies the name of the IP reputation file that be imported.

Viewing IP Reputation Information

You can view the IP reputation database information of the device as needed, including the IP reputation database version, release dates, and the number of the IP reputation. To view IP reputation database information, in any mode, use the following command:

show ip-reputation info

Viewing IP Reputation Update Information

You can view the IP reputation update information of the device as needed, including the update server information, update mode, update frequency and time, as well as the status of the IP reputation database update. To view the IP reputation update information, in any mode, use the following command:

show ip-reputation update

Geolocation Information Database

Overview

System can display the incoming threat map via WebUI. You can view the selected threat or risky host region. You need to update the geolocation information database before use this function for the first time.

> Note:Only support to update the geolocation information database via CLI currently.

Updating Geolocation Information Database

By default FSOS updates the geolocation information database everyday automatically. You can change the update configuration as needed. The configurations of updating geolocation information database include:

- Configuring a geolocation information database update mode
- Configuring an update server
- Specifying an update schedule
- Updating now
- Importing a geolocation information database file
- Viewing geolocation information database information
- Viewing geolocation information database update information

Configuring a Geolocation Information Database Update Mode

System supports both manual and automatic update modes. To configure a geolocation information database update mode, in the global configuration mode, use the following command:

```
geolocation-IP-signature update mode {auto | manual}
```

- **auto** – Specifies the automatic geolocation information database update mode. This is the default mode.
- **manual** – Specifies the manual geolocation information database update mode.

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

```
no geolocation-IP-signature update mode
```

Configure an Update Server

System provides two default update servers: Update1.fw1.fs.com and Update2.fw2.fs.com. You can also configure another up to three update servers to download the latest geolocation informations as needed. To configure the update the server, in the global configuration mode, use the following command:

geolocation-IP-signature update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*}

- **server1** | **server2** | **server3** – Specifies the update server you want to configure. The default value of **server1**is Update1.fw1.fs.com, and the default value of **server2**is Update2.fw2.fs.com.
- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an *ip-address*, or a *domain-name*, for example, Update1.fw1.fs.com.

To cancel the specified update the server, in the global configuration mode, use the following command:

no geolocation-IP-signature update {**server1** | **server2** | **server3**}

Specifying a HTTP Proxy Server

When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update automatically and normally.

To specify the HTTP proxy server for the geolocation information database updating, use the following command in the global configuration mode:

geolocation-ip-signature update proxy-server {**main** | **backup**} *ip-address port-number*

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

To cancel the proxy server configurations, use the **no geolocation-ip-signature update proxy-server** {**main** | **backup**} command.

Specifying an Update Schedule

By default, system automatically updates the geolocation information database every day. To reduce the update server's workload, the time of daily update is random. To specify the schedule and specific time for the update, in the global configuration mode, use the following command:

geolocation-IP-signature update schedule {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**}} [*HH:MM*]

- **daily** – Updates the database every day.
- **weekly {mon | tue | wed | thu | fri | sat | sun}** – Updates the database every week. Parameter **mon | tue | wed | thu | fri | sat | sun**is used to specify the specific date in a week.
- *HH:MM* – Specifies the time of update, for example, 09:00.

Updating Now

For both manual and automatic update modes, you can update the geolocation information database immediately as needed. To update the geolocation information database now, in any mode, use the following command:

exec geolocation-IP-signature update [full]

- **exec geolocation-IP-signature update** – Only updates the incremental part between the current geolocation information database and the latest geolocation information database released by the update server.
- **full** – Force to upgrade the current geolocation information database

Importing a Geolocation Information Database File

In some cases, your device may be unable to connect to the update server to update the geolocation information database. To solve this problem, FSOS provides the geolocation information database file import function, i.e., importing the geolocation information database files to the device from an FTP, TFTP server or USB disk, so that the device can update the geolocation information database locally. To import the geolocation information database file, in the execution mode, use the following command:

import geolocation-IP-signature from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *ip-address* – Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP server.
- **vrouter** *vr-name* – Specifies the VRouter of the FTP or TFTP server.
- *file-name* – Specifies the name of the geolocation information database file that be imported.

Viewing Geolocation Information Database Information

You can view the geolocation information database information of the device as needed, including the geolocation information database version, release dates, and the number of the geolocation information. To view geolocation information database information, in any mode, use the following command:

```
show geolocation-IP-signature info
```

Viewing Geolocation Information Database Update Information

You can view the geolocation information database update information of the device as needed, including the update server information, update mode, update frequency and time, as well as the status of the geolocation information database update. To view the geolocation information database update information, in any mode, use the following command:

```
show geolocation-IP-signature update
```

Chapter 12 Data Security & URL Filtering

The chapter introduces the following topics:

- "Data Security" describes the data security functions included in the system, including content filtering, file filtering, online behavior auditing, and log management.
- "Object Configuration" describes the public Data Security configurations that are used for configuring Data Security rules.
- "URL Filtering" explains how to configure the URL filtering function to control the access to some websites.
- "SSL Proxy" describes how to configure the SSL proxy function in two typical scenarios to decrypt HTTPS traffic.

Data Security

Overview

The booming and popularization of Internet bring significant convenience to people's work and life. However, problems caused by access to Internet, like bandwidth misuse, low efficiency, information leakage, legal risks, security potentials, etc., are also becoming increasingly prominent. For example, in some enterprises, online chatting and Internet forum browsing during the office hours, or disclose some confidential information to the public in emails; in some public places like net bar, netizens randomly visit illegal websites, post irresponsible topics, or even get involved in illegal network movement.

To solve the above problems, system provides the Data Security function to control and audit network behaviors, and check the transmitted files, effectively optimizing the utilization of Internet resources.

Introduction to Data Security

The Data Security function of FSOS allows you to flexibly configure control rules for different users, network behaviors and schedules, check the transmitted files, in order to perform comprehensive control and audit (by behavior logs) on users' network behavior.

FSOS Data Security includes the following features. The main functions and description is listed in the table below.

- Content filter
  - Web Content
  - Web posting

  - Email filter
  - HTTP/FTP control
- Network Behavior Record
  - IM
  - Web Surfing Record
- File filter
- Log management

Function		Description
Content Filter	URL keyword	Controls the network behavior of visiting the webpages (including the webpages encrypted by HTTPS) that contain certain keywords, and log the actions.
	Web posting	Controls the network behavior of posting on websites (including the webpages encrypted by HTTPS) and posting specific keywords, and logs the posting.
	Email filter	Controls and audit SMTP 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.
	HTTP/FTP control	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;
Network Behavior Record	IM	Audits the QQ, wechat and sinaweibo user behaviors.
	Web Surfing Record	Log the access behaviors.

Function	Description
File filter	Checks the files transported through HTTP, FTP, SMTP, POP3 protocols and control them according to the file filter rules.
Log	Rich Data Security log export and storage solution.

Content Filter

Security includes the following features.

- Web Content
- Web posting
- Email filter
- HTTP/FTP control

Web Content

The web content function is designed to control the network behavior of visiting the webpages that contain certain keywords, and log the actions. For example, you can configure to block the access to webpage that contains the keyword "gamble", and record the access action and content in the log.

Configuring Web Content via CLI

The Web content function is mainly implemented by binding a profile to a policy rule. Once the Web content profile is bound to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration.

To configure Web content via CLI, take the following steps:

1. Create a Web content profile, and specify the keyword category, action and control range in the profile. You can also configure to exclude HTML tags from the Web content.
2. Bind the Web content profile to an appropriate policy rule or a zone.

Creating a Web Content Profile

You need to specify the keyword category, action and control range in the Web content profile. To create a Web content profile, in the global configuration mode, use the following command:

contentfilter-profile *profile-name*

- *profile-name* - Specifies the name of the Web content profile, and enter the configuration mode of the Web content profile. If the specified name exists, the system will directly enter the Web content profile configuration mode. To delete the specified Web content profile, in the global configuration mode, use the command **no contentfilter-profile** *profile-name*.

Specifying the Keyword Category and Action

To specify the keyword category that will be filtered and the corresponding action, in the Web content profile configuration mode, use the following command:

keyword-category {*keyword-category-name* | **other**} [**block**] [**log**]

- *keyword-category-name* / **other** – Specifies the keyword category that will be filtered. For more information about how to create a keyword category, see Keyword Category.
- **block** – Blocks access to the website that contains the specified keyword.
- **log** – Logs access to the website that contains the specified keyword.

Repeat the command to add more keyword categories and actions.

To cancel the specified the keyword category and action, in the Web content profile configuration mode, use the command **no keyword-category** *keyword-category-name*.

Specifying the Control Range

The system will only control the keyword within the specified websites. To specify the control range, in the Web content profile configuration mode, use the following command:

url-category {**all** | *url-category-name*}

- **all** | *url-category-name* – Specifies the URL category that will be controlled. It can be all the URL categories (**all**) or a specific URL category (*url-category-name*). For more information about how to create a URL category, see Specifying a HTTP Proxy Server.

Repeat the command to add more URL categories.

To cancel the specified URL category, in the Web content configuration mode, use the command **no url-category** {**all** | **url-category-name**}.

Excluding HTML Tags

By default the system with Web content enabled will not only filter the content displayed in the webpage, but also filter the codes in the HTML tag. To exclude the HTML tags from the filtering, in the Web content profile configuration mode, use the following command:

exclude-html-tag

To restore to the default value, in the Web content profile configuration mode, use the following command:

no exclude-html-tag

> Note:This function only takes effect when the HTML content type is set to text/html, i.e., content="text/html".

Binding the Web Content Profile to a Policy Rule

After binding the Web content profile to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration. To bind the Web content profile to a policy rule, enter the policy rule configuration mode in two steps. First, in the global configuration mode, use the following command to enter the policy configuration mode:

policy-global

Then, in the policy configuration mode, use the following command to enter the policy rule configuration mode:

rule [**id** *id-number*]

To bind the Web content profile to a policy rule, in the policy rule configuration mode, use the following command:

contentfilter *profile-name*

- *profile-name* - Specifies the name of Web content profile that will be bound.

Binding the Web Content Profile to a Security Zone

If the Web content profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration. If the policy rule is bound with a Web content profile, and the destination zone of the policy rule is also bound with a Web content profile, then the Web content profile bound to the policy rule will be valid.

To bind the Web content profile to a security zone, in the security zone configuration mode, use the following command:

contentfilter enable *profile-name*

- *profile-name* − Specifies the name of the Web content profile that will be bound to the security zone. One security zone can only be bound with one Web content profile.

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

no contentfilter enable

Viewing Web Content Profile Information

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

show contentfilter-profile [*profile-name*]

- *profile-name* – Shows the specified Web content profile information. If this parameter is not specified, the command will show the information of all the Web content profiles.

Web Posting

The web posting function is designed to control the network behavior of posting on websites and posting specific keywords, and can log the posting action and posted content. For example, forbid the users to post information containing the keyword X, and record the action log.

Configuring Web Posting via CLI

The Web posting can be configured via CLI by binding a profile to a policy rule. Once the Web posting profile is bound to a policy rule, the system will process the matching traffic according to the profile configuration.

To configure Web posting via CLI, take the following steps:

1. Create a Web posting profile, and specify the control type, action and control range in the profile.
2. Bind the Web posting profile to an appropriate policy rule or a zone.

Creating a Web Posting Profile

You need to specify control type, action and control range in the Web posting profile. To create a Web posting profile, in the global configuration mode, use the following command:

webpost-profile *profile-name*

- *profile-name* - Specifies the name of the Web posting profile, and enter the configuration mode of the Web posting profile. If the specified name exists, the system will directly enter the Web posting profile configuration mode.

Specifying the Control Type and Action of Web Posting

You can control all the posting information, or only control the posting information with specific keyword.

To control all the posting information and specify the action, in the Web posting profile configuration mode, use the following command:

webpost all [**block**] [**log**]

- **block** – Blocks all the posting actions.
- **log** – Logs all the posting actions.

To cancel the specified control type, in the Web posting profile configuration mode, use the command **no webpost all**.

To control the posting information with specific keyword and specify the action, in the Web posting profile configuration mode, use the following command:

keyword-category {*keyword-category-name* | **other** } [**block**] [**log**]

- *keyword-category-name* | **other** – Specifies the keyword category that will be filtered. For more information about how to create a keyword category, see Keyword Category.
- **block** – Blocks postings that contain the specified keywords.
- **log** – Logs postings that contain the specified keywords.

Repeat the command to specify more keyword categories and actions.

To cancel the specified keyword category and action, in the Web posting profile configuration mode, use the command **no keyword-category** *keyword-category-name*.

Specifying the Control Range

The system will only control the postings within the specified websites. To specify the control range, in the Web posting profile configuration mode, use the following command:

url-category {**all** | *url-category-name*}

- **all** | *url-category-name* – Specifies the URL category that will be controlled. It can be all the URL categories (**all**) or a specific URL category (*url-category-name*. For more information about how to create a URL category, see Specifying a HTTP Proxy Server.

Repeat the command to add more URL categories.

To cancel the specified URL category, in the Web posting profile configuration mode, use the command **no url-category** {**all** | *url-category-name*}.

Binding the Web Posting Profile to a Policy Rule

After binding the Web posting profile to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration. To bind the Web posting profile to a policy rule, enter the policy rule configuration mode in two steps. First, in the global configuration mode, use the following command to enter the policy configuration mode:

policy-global

Then, in the policy configuration mode, use the following command to enter the policy rule configuration mode:

rule [**id** *id-number*]

To bind the Web posting profile to a policy rule, in the policy rule configuration mode, use the following command:

webpost *profile-name*

- *profile-name* - Specifies the name of Web posting profile that will be bound.

Binding the Web Posting Profile to a Security Zone

If the Web posting profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration. If the policy rule is bound with a Web posting profile, and the destination zone of the policy rule is also bound with a Web posting profile, then the Web posting profile bound to the policy rule will be valid.

To bind the Web posting profile to a security zone, in the security zone configuration mode, use the following command:

webpost enable *profile-name*

- *profile-name* – Specifies the name of the Web posting profile that will be bound to the security zone. One security zone can only be bound with one Web posting profile.

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

no webpost enable

Viewing Web Posting Profile Information

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

show webpost-profile [*profile-name*]

- *profile-name* – Shows the specified Web posting profile information. If this parameter is not specified, the command will show the information of all the Web posting profiles.

Email Filter

The email filter function is designed to control the email sending actions according to the sender, receiver, email content and attachment, and record the sending log messages and content. Both the SMTP emails can be controlled.

Configuring Email Filter via CLI

The email filter can be configured via CLI by binding a profile to a policy rule. Once the email filter profile is bound to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration.

To configure email filter via CLI, take the following steps:

1. Create an email filter profile, and specify the control type, action, controlled mailbox and mailbox exception in the profile.
2. Bind the email filter profile to an appropriate policy rule or a zone.

Creating a Mail Filter Profile

You need to specify control type, action, controlled mailbox and mailbox exception in the email filter profile. To create an email filter profile, in the global configuration mode, use the following command:

mail-profile *profile-name*

- *profile-name* - Specifies the name of the email filter profile, and enter the configuration mode of the email filter profile. If the specified name exists, the system will directly enter the email filter profile configuration mode.

To delete the specified email filter profile, in the global configuration mode, use the command **no mail-profile** *profile-name*.

Specifying the Control Type

By default the email filter rule is applied to all the supported mailboxes. To specify the control type, in the email filter profile configuration mode, use the following command:

mail control smtp

- **smtp** - Specifies the email type that will be controlled. It can be SMTP mails (**smtp**).

To cancel the specified control type, in the email filter profile configuration mode, use the command **no mail control smtp**.

Controlling All the Emails and Specifying the Action

To control all the emails and specify the action, in the email filter profile configuration mode, use the following command:

mail any [**log**]

- **log** – Logs all the behaviors of sending emails.

To cancel the specified action, in the email filter profile configuration mode, use the command **no mail any**.

Specifying the Sender/Recipient and Action

To specify the sender/recipient that will be controlled and the corresponding action, in the email filter profile configuration mode, use the following command:

mail {**sender** | **recipient**} *email-address* [**block**] [**log**]

- **sender** | **recipient** – Specifies to control the sender or recipient.
- *email-address* – Specifies the email address of the sender or recipient.
- **block** – Blocks the emails that contain the specified sender or recipient.
- **log** – Logs the behaviors of sending emails that contain the specified sender or recipient.

Repeat the command to specify more senders/recipients and the corresponding actions.

To cancel the specified sender/recipient and action, in the email filter profile configuration mode, use the command **no {sender | recipient} email-address**.

Specifying the Keyword Category and Action

To control the email that contains the specified keyword category and the corresponding action, in the email filter profile configuration mode, use the following command:

keyword-category {*keyword-category-name* | **other** } [**block**] [**log**]

- *keyword-category-name* | **other** – Specifies the keyword category that will be filtered. For more information about how to create a keyword category, see Keyword Category.
- **block** – Blocks the emails that contain the specified keyword(s).
- **log** – Logs the behaviors of sending emails that contain the specified keyword(s).

Repeat the command to specify more keyword categories and actions.

To cancel the specified keyword category and the corresponding action, in the email filter profile configuration mode, use the command **no keyword-category** *keyword-category-name*.

Specifying the Control Type

To specify the control type, in the email filter profile configuration mode, use the following command:

```
mail enable {sender | recipient | attach | keyword-category}
```

- **sender | recipient | attach | keyword-category** – Specifies to control the **sender**, **recipient**, **attach**, **keyword-category**.

To disable the specified control type, in the email filter profile configuration mode, use the command **no mail enable** {**sender** | **recipient** | **attach** | **keyword-category**}.

Specifying the Action for other emails

Other emails refer to the emails that do not match any of the specified conditions (including sender, recipient, keyword category and attachment). To specify the action for other emails, in the email filter profile configuration mode, use the following command:

```
mail others [block] [log]
```

- **block** – Blocks other emails.
- **log** – Logs the behaviors of sending other emails.

To cancel the specified action for other emails, in the email filter profile configuration mode, use the command **no mail others**.

Specifying the Account Exception

The account exception, either a sender or a recipient account, is not controlled by the email filter rule. To specify an account exception, in the email filter profile configuration mode, use the following command:

mail whitelist *mail-address*

- *mail-address* – Specifies the email address of the exception account.

Repeat the command to specify more account exceptions.

To remove the specified account from the whitelist, in the email filter profile configuration mode, use the command **no mail whitelist** *mail-address*.

Binding the Email Filter Profile to a Policy Rule

After binding the email filter profile to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration. To bind the email filter profile to a policy rule, enter the policy rule configuration mode in two steps. First, in the global configuration mode, use the following command to enter the policy configuration mode:

policy-global

Then, in the policy configuration mode, use the following command to enter the policy rule configuration mode:

rule [**id** *id-number*]

To bind the email filter profile to a policy rule, in the policy rule configuration mode, use the following command:

mail *profile-name*

- *profile-name* - Specifies the name of email filter profile that will be bound.

Binding the Email Filter Profile to a Security Zone

If the email filter profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration. If the policy rule is bound with a email filter profile, and the destination zone of the policy rule is also bound with a email filter profile, then the email filter profile bound to the policy rule will be valid.

To bind the email filter profile to a security zone, in the security zone configuration mode, use the following command:

mail enable *profile-name*

- *profile-name* – Specifies the name of the email filter profile that will be bound to the security zone. One security zone can only be bound with one email filter profile.

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

no mail enable

Viewing Email Filter Profile Information

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

show mail-profile [*profile-name*]

- *profile-name* – Shows the specified email filter profile information. If this parameter is not specified, the command will show the information of all the email filter profiles.

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

show mail-object [**mail-profile** *profile-name*]

- **mail-profile** *profile-name* – Shows the control type information of the specified email filter profile. If this parameter is not specified, the command will show all the control type information.

HTTP/FTP Control

The HTTP/FTP control function is designed to control and audit (record log messages) the actions of HTTP and FTP applications, including:

- Control and audit the FTP methods, including Login, Get, and Put;
- Control and audit the HTTP methods, including Connect, Get, Put, Head, Options, Post, and Trace;

Configuring HTTP/FTP Control via CLI

The HTTP/FTP control function is mainly implemented by binding a profile to a policy rule. Once the HTTP/FTP control profile is bound to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration.

To configure HTTP/FTP control via CLI, take the following steps:

1. Create an HTTP/FTP control profile, and specify the FTP method, HTTP method or HTTP download that will be controlled and action in the profile.
2. Bind the HTTP/FTP control profile to an appropriate policy rule or a zone.

Creating an HTTP/FTP Control Profile

You need to specify the FTP method, HTTP method or HTTP download that will be controlled and action in the HTTP/FTP control profile. To create an HTTP/FTP control profile, in the global configuration mode, use the following command:

behavior-profile *profile-name*

- *profile-name* - Specifies the name of the HTTP/FTP control profile, and enter the configuration mode of the HTTP/FTP control profile. If the specified name exists, the system will directly enter the HTTP/FTP control profile configuration mode.

To delete the specified HTTP/FTP control profile, in the global configuration mode, use the command **no behavior-profile** *profile-name*.

Controlling FTP Methods

To configure the action for the FTP method, in the HTTP/FTP control profile configuration mode, use the following command:

ftp {**login** [*user-name*] | **get** [*file-name*] | **put** [*file-name*]} {**block** | **permit**} [**log**]

- **login** [*user-name*] − Controls FTP login method. To control the login method of the specified user, use parameter *user-name*.
- **get** [*file-name*] − Controls FTP Get method. To control the Get method to the specified file, use parameter *file-name*.
- **put** [*file-name*] − Controls FTP Put method. To control the Put method to the specified file, use parameter *file-name*.
- **block | permit** − Specifies the action. It can be **block**or **permit**.
- **log** − Logs the FTP method.

To cancel the specified action for the FTP method, in the HTTP/FTP control profile configuration mode, use the following command:

no ftp {**login** [*user-name*] | **get** [*file-name*] | **put** [*file-name*]}

Controlling HTTP Methods

To configure the action for the HTTP method, in the HTTP/FTP control profile configuration mode, use the following command:

http {**connect** | **delete** [*host*] | **get** [*host*] | **head** [*host*] | **options** [*host*] | **post** [*host*] | **put** [*host*] | **trace** [*host*]} {**block** | **permit**} [**log**]

- **connect** | **delete** [*host*] | **get** [*host*] | **head** [*host*] | **options** [*host*] | **post** [*host*] | **put** [*host*] | **trace** [*host*] − Controls the specified HTTP method. To control the HTTP method to the specified host, use parameter host.
- **block | permit** − Specifies the action. It can be block or permit.
- **log** − Logs the HTTP method.

To cancel the specified action for the HTTP method, in the HTTP/FTP control profile configuration mode, use the following command:

no http {**connect** | **delete** [*host*] | **get** [*host*] | **head** [*host*] | **options** [*host*] | **post** [*host*] | **put** [*host*] | **trace** [*host*]}

Binding the HTTP/FTP Control Profile to a Policy Rule

After binding the HTTP/FTP control profile to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration. To bind the HTTP/FTP control profile to a policy rule, enter the policy rule configuration mode in two steps. First, in the global configuration mode, use the following command to enter the policy configuration mode:

policy-global

Then, in the policy configuration mode, use the following command to enter the policy rule configuration mode:

rule [**id** *id-number*]

To bind the HTTP/FTP control profile to a policy rule, in the policy rule configuration mode, use the following command:

behavior *profile-name*

- *profile-name* - Specifies the name of HTTP/FTP control profile that will be bound.

Binding the HTTP/FTP Control Profile to a Security Zone

If the HTTP/FTP control profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration. If the policy rule is bound with a HTTP/FTP control profile, and the destination zone of the policy rule is also bound with a HTTP/FTP control profile, then the HTTP/FTP control profile bound to the policy rule will be valid.

To bind the HTTP/FTP control profile to a security zone, in the security zone configuration mode, use the following command:

behavior enable *profile-name*

- *profile-name* – Specifies the name of the HTTP/FTP control profile that will be bound to the security zone. One security zone can only be bound with one HTTP/FTP control profile.

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

no behavior enable

Viewing HTTP/FTP Control Profile Information

To view the HTTP/FTP control profile information, in any mode, use the following command:

show behavior-profile [*profile-name*]

- *profile-name* – Shows the specified HTTP/FTP control profile information. If this parameter is not specified, the command will show the information of all the HTTP/FTP control profiles.

To view the object information in the HTTP/FTP control profile, in any mode, use the following command:

show behavior-object [**behavior-profile** *profile-name*]

- **behavior-profile** *profile-name* – Shows the object information of the specified HTTP/FTP control profile. If this parameter is not specified, the command will show the object information of all the HTTP/FTP control profiles.

File Filter

The file filter function checks the files transported through HTTP, FTP, SMTP, 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, and POP3.
- Support file type filter conditions.
- Support block, log, and permit actions.

The filter conditions supported by each protocol area shown below:

	HTTP		FTP	SMTP	POP3
	GET	POST			
File type	√	√	√	√	√

Configuring File Filtering

After bind the file filter profile to a policy rule, the system will process the traffic that matches the rule according to the profile.

To configure file filter via CLI, take the following steps:

1. Create a file filter profile, and configure the file filter rule.

2. Specify the protocol to be checked, the filter condition, and the actions in the file filter rule.

3. Bind the file filter profile to an appropriate policy rule.

Creating a File Filter Profile

To create a file filter profile, in the global configuration mode, use the following command:

dlp-profile *profile-name*

- *profile-name* - Specifies the name of the file filter profile, and enter the configuration mode of the file filter profile. If the specified name exists, the system will directly enter the file filter profile configuration mode.

To delete the file filter profile, use the**no dlp-profile** *profile-name* command.

Creating a File Filter Rule

Use the file filter rule to specify the protocol that you want to check, the filter conditions, and the actions. To create a filter rule, in the file filter profile configuration mode, use the following command:

filter id *id-number*

- **id** *id-number* – Specifies the ID of the created file filter rule, and enter the configuration mode of the file filter rule. If the specified ID exists, the system will directly enter the file filter rule configuration mode. The ID value ranges from 1 to 3.

If one filter rule 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; if the file rules that the file matches to have no block action configured, then the system will permit this file and log this file.

Use the **no filter id** *id-number*to delete the specified filter id.

Specifying the Protocol

The file filter function will check the files transported through the protocols you specified. To specify the protocol, in the file filter rule, use the following command:

protocol-type { all | http-get | http-post | ftp | smtp | pop3 }

- **all | http-get | http-post | ftp | smtp | pop3** – Specifies the protocols. **all**represents to check the files transported through the GET and POST methods of HTTP, FTP, SMTP and POP3. **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.

ftprepresents to check the files transported through FTP. smtprepresents to check the files transported through SMTP. pop3represents to check the files transported through POP3.

To cancel the settings, use the no protocol-typecommand.

Specifying the File Type

When the transmitted file is a particular type, the system will trigger the actions. The file filter function can identify the following file types:

7Z, AI, APK, ASF, AVI, BAT, BMP, CAB, CATPART, CDR, CIN, CLASS, CMD, CPL, DLL, DOC, DOCX, DPX, DSN, DWF, DWG, DXF, EDIT, EMF, EPS, EPUB, EXE, EXR, FLA, FLV, GDS, GIF, GZ, HLP, HTA, HTML, IFF, ISO, JAR, JPG, KEY, LNK, LZH, MA, MB, MDB, MDI, MIF, MKV, MOV, MP3, MP4, MPEG, MPKG, MSI, NUMBERS, OCX, PAGES, PBM, PCL, PDF, PGP, PIF, PL, PNG, PPT, PPTX, PSD, RAR, REG, RLA, RMVB, RPF, RTF, SGI, SH, SHK, STP, SVG, SWF, TAR, TDB, TIF, TORRENT, TXT, VBE, WAV, WEBM, WMA, WMF, WMV, WRI, WSF, XLS, XLSX, XML, XPM, ZIP, UNKNOWN

To specify the file type, in the file filter rule configuration mode, use the following command:

file-type *type*

- *type* - Specify the file type. The type names are described above. You can specify one type once and repeat this command to specify multiple types. To control the file type that not supported, you can use the UNKNOWN type.

Use the no file-type *type*command to cancel the settings.

Specifying the Action

Specify the action to control the files that matches the filter conditions. To specify the action, in the file filter rule configuration mode, use the following command:

action { log | block }

- block – block represents to block the uploading or downloading of the file that matches the filter conditions.
- log – Permit the transporting of the file that matches the filter conditions with logs.

Use the no actioncommand to cancel the settings.

Binding the File Filter Profile to a Policy Rule

After binding the file filter profile to a policy rule, the system will process the traffic that matches the rule according to the profile. To bind the file filter profile to a policy rule, enter the policy rule configuration mode in two steps.

In the global configuration mode, use the following command to enter the policy configuration mode:

policy-global

Then, in the policy configuration mode, use the following command to enter the policy rule configuration mode:

rule [**id** *id-number*]

To bind the file filter profile to a policy rule, in the policy rule configuration mode, use the following command:

dlp-profile *profile-name*

- *profile-name* - Specifies the name of file filter profile that will be bound.

To cancel the binding, use the **no dlp-profile**command.

Viewing File Filter Profile

To view the file filter profile, in any mode, use the following command:

show dlp-profile *profile-name*

- *profile-name* – Shows the specified file filter profile.

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 via CLI

The Network behavior record can be configured via CLI by binding a profile to a policy rule. Once the Network behavior record profile is bound to a policy rule, the system will process the matching traffic according to the profile configuration.

To configure Network behavior record via CLI, take the following steps:

1. Create a Network behavior record profile, and specify the IM application type, timeout and record log messages for the access actions in the profile.
2. Bind the Network behavior record profile to an appropriate policy rule or a zone.

Creating a Network Behavior Record Profile

You need to specify the the IM application type, timeout and record log messages for the access actions in the network behavior record profile. To create a NBR profile, in the global configuration mode, use the following command:

nbr-profile *profile-name*

- *profile-name* - Specifies the name of the NBR profile, and enter the configuration mode of the NBR profile. If the specified name exists, the system will directly enter the NBR profile configuration mode.

To delete the specified NBR profile, in the global configuration mode, use the command **no nbr-profile** *profile-name*.

IM Audit

The system can identify the UID (unique identification) from the IM applications traffic, as well as the related IP address, MAC address, and occurred time. Then it records the corresponding logs in IM logs.

To enable this function, in the NBR configuration mode, use the following command:

im {qq | wechat | sinaweibo} log enable

- **qq** - Specifies the audits of QQ.
- **wechat** - Specifies the audits of WeChat.
- **sinaweibo** - Specifies the audits of sina Weibo.

To disable this function, in the NBR configuration mode, user the **no im** {**qq** | **wechat** | **sinaweibo**} **log enable**command.

Note:To configuring the IM auditing function, you need to use the **application-identify**command to enable the application identification function of the zone bound by the rule.

Configuring Timeout Value

During the timeout period, the IM user traffic of the same UID will not trigger the new logs and after the timeout reaches, it will trigger new logs. To configure the timeout value, in the NBR configuration mode, use the command below:

im {qq | wechat | sinaweibo} timeout *value*

- **qq** | **wechat** | **sinaweibo** – Specifies the IM user type.
- **value** – Specifies the timeout value. The unit is minute. The default value is 20.

In the NBR configuration mode, use **no im** {**qq** | **wechat** | **sinaweibo**} **timeout**command to restore to the default value.

Recording Web Surfing Log

In the NBR profile configuration mode, you can use the following command to enable the system to record the web surfing log:

web-surfing-record method [get | get-post [post-content] | post [post-content]]

- **get** - Records the web surfing log using the GET method.
- **get-post** - Records the web surfing log using the GET and POST methods.
- **post** - Records the web surfing log using the POST method.
- **post-content** – Records the POST content.

In the NBR profile configuration mode, use the following command:

no web-surfing-record

Binding the NBR Profile to a Policy Rule

After binding the NBR profile to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration. To bind the NBR profile to a policy rule, enter the policy rule configuration mode in two steps. First, in the global configuration mode, use the following command to enter the policy configuration mode:

policy-global

Then, in the policy configuration mode, use the following command to enter the policy rule configuration mode:

rule [**id** *id-number*]

To bind the NBR profile to a policy rule, in the policy rule configuration mode, use the following command:

nbr *profile-name*

- *profile-name* - Specifies the name of NBR profile that will be bound.

After the binding, you need to modify the priority of the policy rule to assure the traffic matching to this rule is prioritized. After then, you need to specify the user, destination zone and schedule of the rule. You can also enable or disable the rule. For more information, see the "Policy" .

Binding the NBR Profile to a Security Zone

If the NBR profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration. If the policy rule is bound with a NBR profile, and the destination zone of the policy rule is also bound with a NBR profile, then the NBR profile bound to the policy rule will be valid.

To bind the NBR profile to a security zone, in the security zone configuration mode, use the following command:

nbr enable *profile-name*

- *profile-name* – Specifies the name of the NBR profile that will be bound to the security zone. One security zone can only be bound with one NBR profile.

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

no nbr enable

Viewing NBR Profile Information

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

show nbr-profile [*profile-name*]

- *profile-name* – Shows the specified NBR profile information. If this parameter is not specified, the command will show the information of all the NBR control profiles.

Log Management

The Data Security logs (File Filter logs, Content Filter logs, Network Behavior Record logs) of system provide comprehensive records of users' network behaviors, including visiting URLs, sending emails, content of the emails and the attachments, Web postings, IM and chatting content, and FTP/HTTP methods, etc.

Log Severity and Format

The Data Security logs belong to the severity of Information.

To facilitate the access and analysis of the Data Security logs, FSOS logs follow a fixed pattern of information layout, i.e. **date/time, severity level@module: descriptions**. See the example below.

2017-06-17 11:34:27, WEBPOST: IP 100.100.10.55 (-) vrouter trust-vr, url, content_type content_type, action action, reason, rule rule, character set character-set, content

Output Destinations

Log files can be sent to the following destinations. You can specify one of them at your own choice:

- Console - Console port of the device.
- Buffer - Memory buffer.
- Syslog Server - Sends logs to a UNIX or Windows Syslog Server.

Configuring Log

The configurations of Data Security logs include enabling/disabling Data Security log, specifying the output destination, exporting and clearing logs. For more information about the configurations, see the table below.

Configuration	CLI
To enable/disable the log function	In the global configuration mode, use the following command: • Enable: **logging data-security [dlp | cf | nbr] on** • Disable:**no logging data-security[dlp | cf | nbr] on**
To record the login/logout log messages of IM	In the NBR profile configuration mode, use the following command: • To record the login/logout log messages of QQ, WeChat, and sinaWeibo:**im {qq | wechat | sinaweibo}**

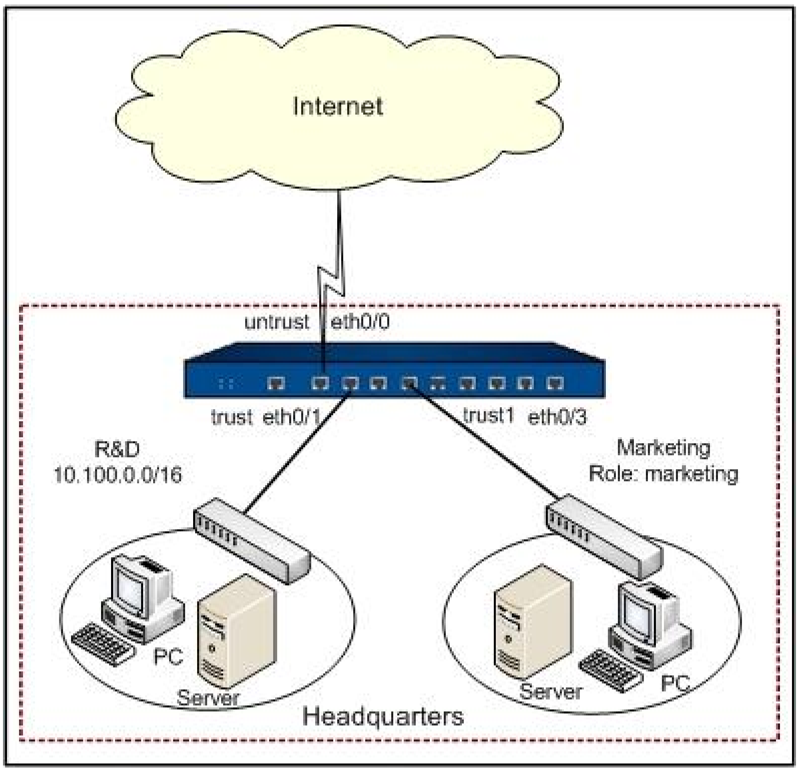
Configuration	CLI
	log enable • To disable the recording of the login/logout log messages of QQ, WeChat, and sinaWeibo:**no im {qq | wechat | sinaweibo} log enable**
To specify the output destination	In the global configuration mode, use the following command: • To Console or syslog server:**logging data-security [dlp | cf | nbr] to {console | syslog[binary-format [distributed [src-ip-hash | round-robin]] | custom-format] }** • To buffer:**logging data-security [dlp | cf | nbr] to buffer** [**size** *buffer-size*]
To view the data security logs	**show logging data-security [dlp | cf | nbr]**
To clear data security logs	**clear logging data-security [dlp | cf | nbr]**

Data Security Configuration Examples

This section describes five Data Security configuration examples, including:

- Example 1: URL filter
- Example 2: Web content
- Example 3: Web posting
- Example 4: Mail filter
- Example 5: Network behavior record

The network topology is shown in the figure below. FS device works as the gateway of an enterprise. Ethernet0/0 connects to Internet and belongs to the untrust zone; ethernet0/1 connects to the Intranet of R&D Department and belongs to the trust zone; ethernet0/3 connects to the Intranet of Marketing Department and belongs to the trust1 zone.



Tip:

- Do not use CLI and WebUI to configure Data security at the same time. Choose only one method.
- For more information about how to configure the interface, security zone and log, see other related chapters. This section only describes Data security configuration.

Example1: URL Filter Configuration

The goal is to configure a URL filter rule that forbids the members in the R&D department (the network segment is 10.100.0.0/16) to access the news websites (except for www.abc.com) and an entertainment websites www.bcd.com during office hours (09:00 to 18:00, Monday to Friday), also forbids searching the keyword ef, and logs the access and search attempts.

Preparations

Before configuring the URL filter function, finish the following preparations first:

1. Install the URL service license and reboot the device.
2. Update the predefined URL database.

Configuration Steps on CLI

Step 1: Configure a schedule:

```
hostname(config)# schedule workday
hostname(config-schedule)# periodic weekdays 09:00 to 18:00
hostname(config-schedule)# exit
hostname(config)#
```

Step 2: Configure the user-defined URL category named bcd that contains www.bcd.com:

```
hostname(config)# url-category bcd
hostname(config)# url www.bcd.com url-category bcd
```

Step 3: Configure the keyword category named url-keyword:

```
hostname(config)# category url-keyword
hostname(config)# keyword ef simple category url-keyword
```

Step 4: Configure the URL filter profile named urlcontrol:

```
hostname(config)# url-profile urlcontrol
hostname(config-url-profile)# url-category News block log
hostname(config-url-profile)# keyword-category url-keyword block log
hostname(config-url-profile)# exit
hostname(config)#
```

Step 5: Bind the URL filter profile to a policy rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# url urlcontrol
hostname(config-policy-rule)# src-ip 10.100.0.0/16
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# schedule workday
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 6: Configure a bypass domain that excludes www.abc.com from control:

```
hostname(config)# address abc
hostname(config-addr)# host www.abc.com
hostname(config-addr)# exit
hostname(config)# policy-global
hostname(config-policy)# rule from any to abc service any permit
hostname(config-policy)# exit
hostname(config)#
```

After the configuration, modify the priority of the policy rule to assure the traffic matching to the configured rule is prioritized. When the rule takes effect, during the office hours, the member in the R&D department cannot access the news websites (except for www.abc.com) and www.bcd.com, and cannot search the keyword ef. The system will log the access and search attempts.

Example 2: Web Content Configuration

The goal of Exmaple 2 is to configure a Web content rule that forbids the members in the R&D department to access the web pages containing the keywords X and Y (except for the member a. The network segment of the R&D department is 10.100.0.0/16), and logs the access attempts.

Preparations

Before configuring the Web content function, finish the following preparations first:

1. Install the URL service license and reboot the device.
2. Update the predefined URL database.

Configuration Steps on CLI

Step 1: Configure the keyword category named web-keyword:

```
hostname(config)# contentfilter
hostname(config-contentfilter)# category web-keyword
hostname(config-contentfilter)# keyword X simple category stock-keyword
hostname(config-contentfilter)# keyword Y simple category stock-keyword
hostname(config-contentfilter)# exit
hostname(config)#
```

Step 2: Configure the Web content profile named webkeyword-control:

```
hostname(config)# contentfilter-profile webkeyword-control
hostname(config-contentfilter-profile)# keyword-category web-keyword block log
hostname(config-contentfilter-profile)# exit
hostname(config)#
```

Step 3: Bind the Web content profile to a policy rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule id 2
hostname(config-policy-rule)# contentfilter webkeyword-control
hostname(config-policy-rule)# src-ip 10.100.0.0/16
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 4: Set the user exception that excludes member a from control:

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user a
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)# policy-global
hostname(config-policy)# rule from any to any from-zone trust to-zone untrust service any
permit
Rule id 3 is created
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# user local a
hostname(config-policy-rule)# exit
hostname(config)#
```

After the configuration, modify the priority of the policy rule to assure the traffic matching to the configured rule is prioritized. When the rule takes effect, the members in the R&D department cannot access web pages containing the keyword X or Y. And also, the system will log the access attempts.

Example 3: Web Posting Configuration

The goal is to configure a Web posting rule that logs the actions of posting information with keyword X on the website www.abc.com.

Preparations

Before configuring the Web posting function, finish the following preparations first:

1. Install the URL service license and reboot the device.
2. Update the predefined URL database.

Configuration Steps on CLI

Step 1: Configure the keyword category named reactionary-keyword:

```
hostname(config)# contentfilter
hostname(config-contentfilter)# category reactionary-keyword
hostname(config-contentfilter)# keyword X simple categoryreactionary-keyword
hostname(config-contentfilter)# exit
hostname(config)#
```

Step 2: Configure the use-defined URL category named abc that contains www.abc.com:

```
hostname(config)# url-category abc
hostname(config)# url www.abc.com url-category abc
```

Step 3: Configure the Web posting profile named webpost-control:

```
hostname(config)# webpost-profile webpost-control
hostname(config-webpost-profile)# keyword-category reactionary-keyword log
hostname(config-webpost-profile)# url-category abc
hostname(config-webpost-profile)# exit
hostname(config)#
```

Step 4: Bind the Web posting profile to a policy rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# webpost webpost-control
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# exit
hostname(config)#
```

After the configuration, modify the priority of the policy rule to assure the traffic matching to the configured rule is prioritized. When the rule takes effect, the system will record log messages when someone is posting information with keyword X in the website www.abc.com.

Example 4: Email Filter Configuration

The goal is to forbid the employees to send emails through QQ mailbox, and record log messages when any is sending emails through other mailboxes.

Configuration Steps on CLI

Step 1: Configure the Email filter profile named mailfilter:

```
hostname(config)# mail-profile mailfilter
hostname(config-mail-profile)# mail sender *@qq.com block
hostname(config-mail-profile)# mail others log
hostname(config-mail-profile)# mail control all
hostname(config-mail-profile)# exit
hostname(config)#
```

Step 2: Bind the Email filter profile to a policy rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule id 4
hostname(config-policy-rule)# mail mailfilter
hostname(config-policy-rule)# dst-zone untrust

hostname(config-policy-rule)# exit

hostname(config)#
```

After the configuration, modify the priority of the policy rule to assure the traffic matching to the configured rule is prioritized. When the rule takes effect, the employees cannot send emails through QQ mailbox, and all the sending actions through other mailboxes will be logged.

Example 5: Network Behavior Record Configuration

The goal is to configure a network behavior record rule that records the WeChat login/logout log messages of the Marketing department members (the role is marketing).

Configuration Steps on CLI

Step 1: Configure the user, role, and role mapping rule (take user1 as the example):

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

hostname(config-aaa-server)# user-group usergroup1

hostname(config-user-group)# exit

hostname(config-aaa-server)# user user1

hostname(config-user)# password 123456

hostname(config-user)# group usergroup1

hostname(config-user)# exit

hostname(config-aaa-server)# exit

hostname(config)# role marketing

hostname(config)# role-mapping-rule role-mapping1

hostname(config-role-mapping)# match user-group usergroup1 role marketing

hostname(config-role-mapping)# exit

hostname(config)#
```

Step 2: Configure the role mapping rule for the local AAA server:

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

hostname(config-aaa-server)# role-mapping-rule role-mapping1
hostname(config-aaa-server)# exit

hostname(config)#
```

Step 3: Configure interfaces and zones:

```
hostname(config)# internet ethernet0/3

hostname(config-if-eth0/3)# zone trust1

hostname(config-if-eth0/3)# ip address 192.168.1.1/16

hostname(config-if-eth0/3)# exit

hostname(config)# interface ethernet0/0

hostname(config-if-eth0/0)# zone untrust

hostname(config-if-eth0/0)# ip address 66.1.200.1/16

hostname(config-if-eth0/0)# exit

hostname(config)#
```

Step 4: Configure WebAuth and DNS policy:

```
hostname(config)# webauth

hostname(config-webauth)# enable

hostname(config-webauth)# protocal http

hostname(config-webauth)# exit

hostname(config)# policy-global

hostname(config-policy)# rule from any to any service any webauth local

Rule id 1 is created

hostname(config-policy)# rule id 1

hostname(config-policy-rule)# src-ip 192.168.1.1/16

hostname(config-policy-rule)# src-zone trust1

hostname(config-policy-rule)# dst-zone untrust

hostname(config-policy-rule)# role unknown

hostname(config-policy-rule)# exit

hostname(config-policy)# rule from any to any service dns permit
```

```
Rule id 2 is created
hostname(config-policy)# rule id 2
hostname(config-policy-rule)# src-zone trust1
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 5: Configure the policy rule:

```
hostname(config-policy)# rule from any to any service any permit
Rule id 3 is created
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# src-zone trust1
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# role marketing
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 6: Configure the NBR profile named marketim:

```
hostname(config)# nbr-profile marketim
hostname(config-nbr-profile)# im wechat log enable
hostname(config-nbr-profile)# exit
hostname(config)#
```

Step 7: Control the NBR rule named imcontrol:

```
hostname(config)# policy-global
hostname(config-policy)# rule id 4
hostname(config-policy-rule)# im marketim
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# role marketing
hostname(config-policy-rule)# exit
hostname(config)#
```

After the configuration, modify the priority of the policy rule to assure the traffic matching to the configured rule is prioritized. When the rule takes effect, the system will log the WeChat login/logout actions of the Marketing department members.

Object Configuration

Objects mean the items referenced during Content Filter profiles and URL Filtering profiles configurations.

- Predefined URL database
- User-defined URL database
- URL lookup
- Keyword category
- Warning page
- Bypass domain
- User exception

Predefined URL Database

System ships with a license controlled predefined URL database. The predefined URL database will not take effect on the supported platforms until a URL license is installed.

Predefined URL database provides URL categories for the configurations of URL filter, web content, and web posting. The predefined URL database is divided into 39 categories, with a total number of URLs up to 20 million.

Updating the Predefined URL Database

By default, the system updates the predefined URL database every day. You can change the update parameters according to your own requirements. FS provides two default URL database update servers: Update1.fw1.fs.com and Update2.fw2.fs.com. You can update your URL database online or manually. For more information about how to configure the predefined URL database, see the following table:

Configuration	CLI

Configuration	CLI
To specify the update mode	In the global configuration mode, use the following command: **url-db update mode** {**auto** | **manual**}
To configure the update server	In the global configuration mode, use the following command: **url-db update** {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter** *vrouter-name*]
To specify the update schedule	In the global configuration mode, use the following command: **url-db update schedule** {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**}} [*HH:MM*]
To update now	In the execution mode, use the following command: **exec url-db update**
To update manually	In the execution mode, use the following command: **import url-db from** {**ftp server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} *file-name* **Note**: Non-root VSYS does not support this command.
To view URL DB info	**show url-db info**
To view URL DB update configuration	**show url-db update**
To view URL statistics	**show statistics-set** *name* [{**current** | **history** | **history-max**} [**sort-by** {**up** | **down** | **item**}]]

Specifying a HTTP Proxy Server

When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update automatically and normally.

To specify the HTTP proxy server for the URL category signature database updating, use the following command in the global configuration mode:

url-db update proxy-server {**main** | **backup**} *ip-address port-number*

- **main** | **backup** − Use the **main**parameter to specify the main proxy server and use the **backup**parameter to specify the backup proxy server.
- *ip-address port-number* − Specify the IP address and the port number of the proxy server.

To cancel the proxy server configurations, use the**no url-db update proxy-server** {**main** | **backup**}command.

User-defined URL Database

Besides categories in predefined URL database, you can also customize user-defined URL categories. User-defined URL database provides URL categories for the configurations of URL filter, web content, and web posting.

System provides three predefined URL categories: custom1, custom2, custom3. You can import your own URL lists into one of the predefined URL category.

For more information about user-defined URL database, see the table below:

Configuration	CLI
To create a URL category	In the global configuration mode, use the following command: **url-category** *category-name*
To add a URL entry	In the global configuration mode, use the following command: **url** *url* **url-category** *category-name*
Enable/Disable the function that the user-defined URL database supports the domain name of the HTTPS protocol	To enable this function, use the following command in the global configuration mode: **url-db-https-enable** To disable this function, use the following command in the global configuration mode: **no url-db-https-enable**
To view the status of this function, use the command in any mode:	**show url-db-https**
Import User-defined URL	**import url-file** {**custom1** | **custom2** | **custom3**} **from ftp server** *IP* [**vrouter** *vrouter-name*] [**user** *username* **password** *password*] *file-name*

Configuration	CLI
	import url-file {**custom1** | custom2 | custom3} from tftp server IP [vrouter vrouter-name] file-name **Note:** The URL file directory is /flash/urldb/url_file. The file should be less than 1 M, and has at most 1000 URLs. Wildcard is supported to use once in the URL file, which should be located at the start of the address. Non-root VSYS does not support this function.
Clear User-defined URL	**exec url-file** {**custom1** | **custom2** | **custom3**} **clear**
To view URL category info	**show url-category**
To view all the user-defined URLs	**show url**

URL Lookup

You can inquire a URL to view the details by URL lookup, including the URL category and the category type. For more information about how to inquire a URL, see the table below:

Configuration	CLI
To inquire a URL	**show url** *url-string*

Configuring a URL Inquiry Server

URL inquiry server can classify an uncategorized URL (an uncatergorized URL is an address that is neither in predefined URL database nor in user-defined URL database) you have accessed, and then add it to the URL database during database updating. FS provides two default URL inquiry servers: url1.fw1.fs.com and url2.fw2.fs.com. By default, the URL inquiry servers are enabled. For more information about how to configure the URL inquiry server, see the table below:

Configuration	CLI
To enable/disable a URL inquiry server	Enable: in the global configuration mode, use the following command: **url-db-query** {**server1** | **server2**} **enable** Disable: in the global configuration mode, use the following command: **no url-db-query** {**server1** | **server2**} **enable**

Configuration	CLI
To configure a URL inquiry server	In the global configuration mode, use the following command: **url-db-query** {**server1** | **server2**} {*ip-address* | *domain-name*} [**vrouter** *vrouter-name*] [**port** *port*] [**encrypt-type** *BCAP*]
To view the URL inquiry server info	**show url-db-query** [**server1** | **server2**]

Keyword Category

Keyword categories referenced by URL filter, web content, web posting, and email filter can be customized. For more information about how to customize a keyword category, see the table below:

Configuration	CLI
To create a keyword category	In the global configuration mode, use the following command: **category** *category-name*
To add a keyword entry	In the global configuration mode, use the following command: **keyword** *keyword* {**regexp** | **simple**} **category** *category-name* [**confidence** *value*]
To commit the changes to keywords (number increase/decrease, content changes)	In the execution mode, use the following command: **exec contentfilter apply**
Show the keyword category	In any mode, use the following command: **show category** *category-name*
Show the keyword entry	In any mode, use the following command: **keyword keyword** {**regexp** | **simple**} **category** *category-name* [**confidence** *value*]

Keyword Matching Rules

System will scan traffic according to the configured keywords and calculate the trust value for the hit keywords. The calculating method is: adding up the results of times * trust value of each keyword that belongs to the category. The system will perform the following actions according to the added up value:

- If the sum is larger than or equal to the category threshold (100), the configured category action will be triggered;
- If more than one category action can be triggered and there is a block action configured, the final action is to block;
- If more than one category action can be triggered and all the configured actions are permit, the final action is to permit.

For example, a web content rule contains two keyword categories C1 with action block and C2 with action permit. Both of C1 and C2 contain the same keywords K1 and K2. Trust values of K1 and K2 in C1 are 20 and 40. Trust values of K1 and K2 in C2 are 30 and 80.

If the system detects one occurrence of K1 and K2 each on a web page, then C1 trust value is 20*1+40*1=60<100, and C2 trust value is 30*1+80*1=110>100. As a result, the C2 action is triggered and the web page access is permitted.

If the system detects three occurrences of K1 and 1 occurrence of K2 on a web page, then C1 trust value is 20*3+40*1=100, and C2 trust value C2 is 30*3+80*1=170>100. Conditions for both C1 and C2 are satisfied, but the block action for C1 is triggered, so the web page access is denied.

Tip:

- The keyword category threshold is 100.
- To implement network behavior control accurately and effectively, you are recommended to configure multiple keywords. E.g., if only web game is configured to block accesses to web game websites, lots of other websites will be blocked together. However, if you configure web game, experience value, and equipment as the keywords, and give proper trust values to these keywords, the control accuracy will be improved. And if you can collect all the game related terms and assign a proper trust value to each term, the control will be implemented completely and precisely.

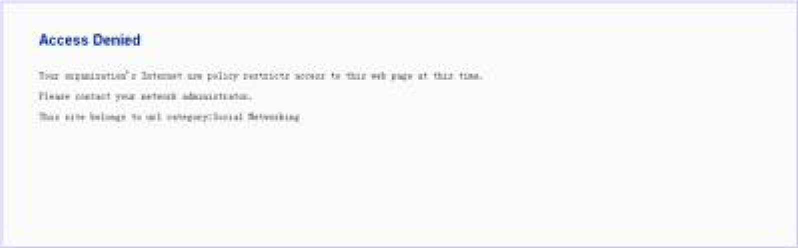
Warning Page

The warning page shows the user block information and user audit information.

Configuring Block Warning

If the network behavior is blocked by the Data Security function (URL filter, web content, web post, email filter, HTTP/FTP control), the access to the Internet will be denied. The information of Access Denied will be displayed in your browser, and some web surfing rules will be shown to you on the warning page at the same time. You can also define the displayed information by yourself. According to the different network behaviors, the default block warning page includes the following three situations:

- Visiting a certain type of URL:



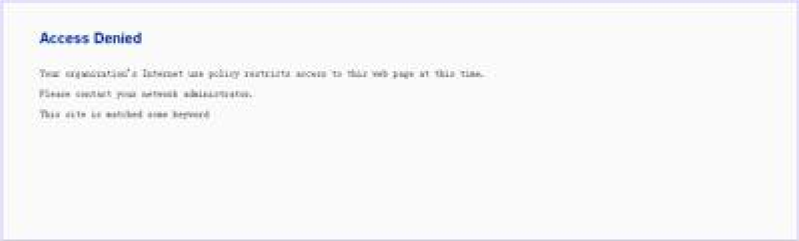
Access Denied

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:



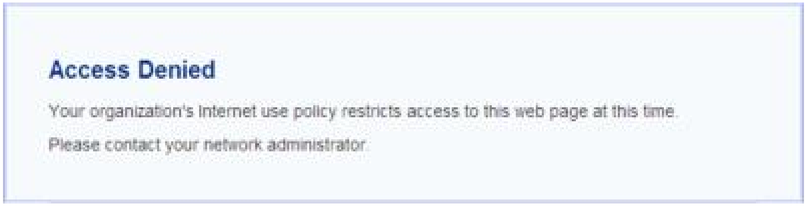
Access Denied

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

- Posting information to a certain type of website or posting a certain type of keywords; HTTP actions of Connect, Get, Put, Head, Options, Post, and Trace; downloading HTTP binary files, such as .bat, .com; downloading ActiveX and Java Applets.



Access Denied

Your organization's Internet use policy restricts access to this web page at this time.

Please contact your network administrator.

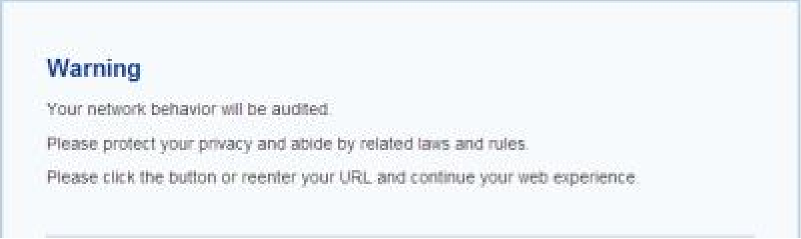
By default the block warning function is enabled. For more information about the configuration of the function, see the table below:

Configuration	CLI
To enable/disable block warning	Enable: In the global configuration mode, use the following command: **block-notification** Disable: In the global configuration mode, use the following command: **no block-notification**
Customize the block warning information or restore the block warning information to the default one	To customize the block warning information, use the following command in the global configuration mode: **customize-block-notification title** *title-name* **body** *string* To restore the block warning information to the default one, use the following command in the global configuration mode: **no customize-block-notification**

Configuration	CLI
To view the status of block warning	show block-notification
To view the user-defined block warning information	show customize-block-notification Tips: • If you have customized your own block warning information, the customized information will display. • If you do not use the customized information, the default block information will display.

Configuring Audit Warning

After enabling the audit warning function, when your network behavior matches the configured Data Security rule, your HTTP request will be redirected to a warning page, on which the audit and privacy protection information is displayed. For example, if a keyword rule is configured to monitor HTTPS access to websites that contain the specified keyword, then after enabling the audit warning function, when you’ re accessing a website that contains the keyword over HTTPS, a warning page will be displayed in your Web browser, as shown in the figure 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.

Audit warning is disabled by default. For more information about the configurations of the function, see the table below:

Configuration	CLI
To enable/disable audit warning	Enable: In the global configuration mode, use the following command: nbc-user-notification Disable: In the global configuration mode, use the following command: no nbc-user-notification
Customize the audit	To customize the audit warning information, use the following

Configuration	CLI
warning information or restore the audit warning information to default	command in the global configuration mode: **customize-audit-notification title title-name body string** To restore the audit warning information to default, use the following command in the global configuration mode: **no customize-audit-notification**
To view the user-defined audit warning information	**show customize-audit-notification** • If you have customized your own audit warning information, the customized information will be displayed. If you do not use the customized information, the default audit information will be displayed.

After enabling audit warning, if your network behavior originating from one single source IP is matched to any configured network behavior control rule, you will be prompted with the audit warning page every 24 hours when visiting the web page.

Bypass Domain

Regardless of the Data Security configurations (URL filter, keyword filter, web posting control, email filter, and HTTP/FTP control), requests to the specified bypass domains will be allowed unconditionally. To add a bypass domain via WebUI, take the following steps:

1. Select **Object > Data Security >Content Filter > Web Content/Web Posting/Email Filter/HTTP/FTP Control**.
2. At the top-right corner, Select **Configuration > Bypass Domain**. The Bypass Domain dialog appears.
3. Click **Add**. The domain name will be added to the system and displayed in the bypass domain list. Repeat Step 3 to add more bypass domains.
4. Click **OK** to save your settings.

Note:

- Bypass domains must be precisely matched
- Bypass domains are effective to the entire system.

User Exception

The user exception function is used to specify the users who will not be controlled by Data Security, including URL filter, Web content, Web posting control, email filter, IM control, and HTTP/FTP control. The system supports the following types of user exception: IP, IP range, role, user, user group, and address entry.

To configure user exception via WebUI, take the following steps:

1. Select **Object** > **Data Security** > **Content Filter** > **Web Content/Web Posting/Email Filter/HTTP/FTP Control**.
2. At the top-right corner, Select **Configuration** > **User Exception**. The User Exception dialog appears.
3. Select the type of the user from the Type drop-down list.
4. Configure the corresponding options.
5. Click **Add**. The user will be added to the system and displayed in the user exception list.
6. Click **OK** to save the settings.

Note:User exceptions are effective to the entire system.

URL Filtering

URL filtering is designed to control the access to some websites. This function helps you control the network behaviors in the following aspects:

- Access control to certain category of websites, such as gambling and pornographic websites;
- Access control to certain category of websites during the specified period. For example, forbid to access IM websites during the office hours;
- Access control to the website whose URL contains the specified keywords. For example, forbid to access the URL that contains the keyword of game.

Configuring URL Filter via CLI

The URL filtering configurations are based on security zones or policies. If IPv6 is enabled, you can configure URL and keyword for both IPv4 and IPv6 address.

To configure URL filtering via CLI, take the following steps:

1. Create a URL filtering profile, and specify the URL category, URL keyword category and action in the profile.

2. Bind the URL filtering profile to a security zone or policy rule.

Creating a URL Filter Profile

You need to specify the control type of the URL filtering profile. The control types are URL category, URL keyword category, and Web surfing record. URL category controls the access to some certain category of website; URL keyword category controls the access to the website who's URL contains the specific keywords; Web surfing record logs the GET and POST methods of HTTP, and the posted content. You can select only one control type for each URL filtering profile. There is a default URL filtering profile named no-url. It can not be edited and deleted. After you bind it to a policy, URL filtering is disabled. To create a URL filtering profile, in the global configuration mode, use the following command:

url-profile *profile-name*

- *profile-name* - Specifies the name of the URL filtering profile, and enter the configuration mode of the URL filtering profile. If the specified name exists, the system will directly enter the URL filtering profile configuration mode. You can configure same URL profile name in different VSYSs.

To delete the specified URL filtering profile, in the global configuration mode, use the command **no url-profile** *profile-name*.

Specifying the URL Category and Action

To specify the URL category that will be filtered and the corresponding action, in the URL filtering profile configuration mode, use the following command:

url-category {**all** | *url-category-name*} [**block**] [**log**]

- **all** | *url-category-name* – Specifies the URL category that will be filtered. It can be all the URL categories (**all**) or a specific URL category (*url-category-name*）). You can not specify URL category of other VSYSs. For more information about how to create a URL category, see Specifying a HTTP Proxy Server.

- **block** – Blocks access to the corresponding URL category.

- **log** – Logs access to the corresponding URL category.

Repeat the command to specify more URL categories and the corresponding actions.

To cancel the specified URL category and action, in the URL filtering profile configuration mode, use the command **no url-category** {**all** | *url-category-name*}.

Inspecting SSL Negotiation Packets

For HTTPS traffic, the system can acquire the domain name of the site which you want to access from the SSL negotiation packets after this feature is configured. Then, the system will perform URL filtering in accordance with the domain name. This feature is only applicable to the URL filtering profile whose control type is URL category. If SSL proxy is configured at the same time, SSL negotiation packets inspection method will be preferred for URL filtering. To configure the SSL negotiation packets inspection, in the URL filtering profile configuration mode, use the following command:

ssl-inspection

In the URL filtering profile configuration mode, use**no ssl-inspection**to cancel the SSL negotiation packets inspection.

Specifying the URL Keyword and Action

To specify the URL keyword that will be filtered and the corresponding action, in the URL filtering profile configuration mode, use the following command:

keyword-category {*keyword-category-name* | **other**} [**block**] [**log**]

- *keyword-category-name* | **other** – Specifies the URL keyword that will be filtered. The URL keyword can be a specific keyword category (*keyword-category-name*) or all the other URL keyword categories that are not listed (**other**). For more information about how to create a keyword category, see Keyword Category.
- **block** – Blocks the access to the website whose URL contains the specified keyword.
- **log** – Logs the access to the website whose URL contains the specified keyword.

Repeat the command to specify more URL keywords and the corresponding actions.

To cancel the specified URL keyword and action, in the URL filtering profile configuration mode, use the command **no keyword-category** {*keyword-category-name* | **other**}.

Binding the URL Filtering Profile to a Security Zone

If the URL filtering profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration. If the policy rule is bound with an URL filtering Profile, and the destination zone of the policy rule is also bound with an URL filtering profile, then the URL filtering profile bound to the policy rule will be valid.

To bind the URL filtering profile to a security zone, in the security zone configuration mode, use the following command:

url enable *url-profile-name*

- *url-profile-name* – Specifies the name of the URL filtering profile that will be bound to the security zone. One security zone can only be bound with one URL filtering profile.

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

no url enable

Binding the URL Filtering Profile to a Policy Rule

After binding the URL filtering profile to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration. To bind the URL filtering profile to a policy rule, enter the policy rule configuration mode in two steps. First, in the global configuration mode, use the following command to enter the policy configuration mode:

policy-global

Then, in the policy configuration mode, use the following command to enter the policy rule configuration mode:

rule [**id** *id-number*]

To bind the URL filtering profile to a policy rule, in the policy rule configuration mode, use the following command:

url *profile-name*

- *profile-name* - Specifies the name of URL filtering profile that will be bound.

Note:Only after canceling the binding can you delete the URL filtering profile.

After the binding, you need to modify the priority of the policy rule to assure the traffic matching to this rule is prioritized. Then, you need to specify the user, destination zone and schedule of the rule. You can also enable or disable the rule.

To perform the URL filtering function on the HTTPS traffic, you need to enable the SSL proxy function for the above specified security policy rule. The system will decrypt the HTTPS traffic according to the SSL proxy profile and then perform the URL filtering function on the decrypted traffic. According to the various configurations of the security policy rule, the system will perform the following actions:

Policy Rule Configurations	Actions

Policy Rule Configurations	Actions
SSL proxy enabled URL filtering disabled	The system decrypts the HTTPS traffic according to the SSL proxy profile but it does not perform the URL filtering function on the decrypted traffic.
SSL proxy enabled URL filtering enabled	The system decrypts the HTTPS traffic according to the SSL proxy profile and performs the URL filtering function on the decrypted traffic.
SSL proxy disabled URL filtering enabled	The system performs the URL filtering function on the HTTP traffic according to the URL filtering profile. The HTTPS traffic will not be decrypted and the 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 profile is the Web surfing record, the system will not record the GET and POST methods and the posted contents via HTTPS.

If the zone which the security policy rule binds with is also configured with URL filtering, the system will perform the following actions:

Policy Rule Configurations	Zone Configurations	Actions
SSL proxy enabled URL filtering disabled	URL filtering enabled	The system decrypts the HTTPS traffic according to the SSL proxy profile and performs the URL filtering function on the decrypted traffic according to the URL filtering rule of the zone.
SSL proxy enabled URL filtering enabled	URL filtering enabled	The system decrypts the HTTPS traffic according to the SSL proxy profile and performs the URL filtering function on the decrypted traffic according to the URL filtering rule of the policy rule.
SSL proxy disabled URL filtering enabled	URL filtering enabled	The system performs the URL filtering function on the HTTP traffic according to the URL filtering rule of the policy rule. The HTTPS traffic will not be decrypted and the system will transfer it.

Viewing URL Filtering Profile Information

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

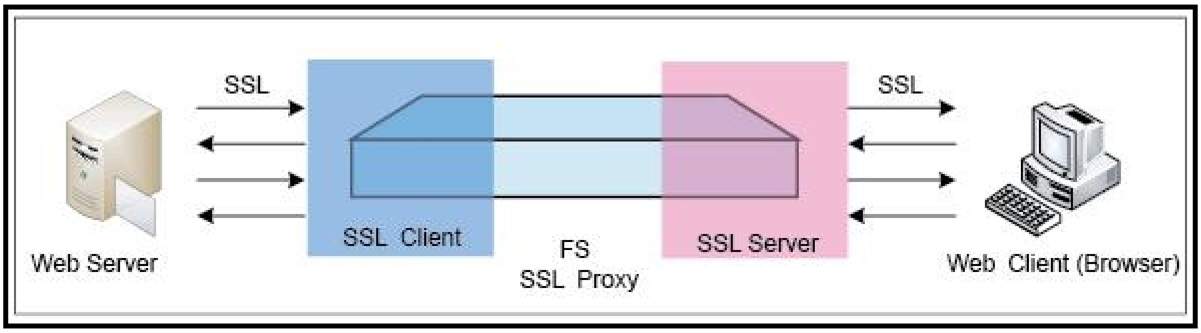
show url-profile [*profile-name*]

- *profile-name* – Shows the specified URL filtering profile information. If this parameter is not specified, the command will show the information of all the URL filtering profiles.

SSL Proxy

To assure the security of sensitive data when being transmitting over networks, more and more websites adopt SSL encryption to protect their information. The device provides the SSL proxy function to decrypt HTTPS traffic. The SSL proxy function works in the following two scenarios:

The first scenario, the device works as the gateway of Web clients. The SSL proxy function replaces the certificates of encrypted websites with the SSL proxy certificate to get the encrypted information and send the SSL proxy certificate to the client’ s Web browser. During the process, the device acts as an SSL client and SSL server to establish connections to the Web server and Web browser respectively. The SSL proxy certificate is generated by using the device's local certificate and re-signing the website certificate. The process is described as below:



The second scenario, the device works as the gateway of Web servers. The device with SSL proxy enabled can work as the SSL server, use the certificate of the Web server to establish the SSL connection with Web clients (Web browsers), and send the decrypted traffic to the internal Web server.

Work Mode

There are three work modes. For the first scenario, the SSL proxy function can work in the "Client Inspection - Proxy" mode ; for the second scenario, the SSL proxy function can work in the "Server Inspection - Offload" mode .

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 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 traffic can be blocked or bypassed according to the action you specified.

- If the action is Block, the HTTPS traffic will be blocked by the device.
- If the action is Bypass, the HTTPS 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 traffic will be bypassed.

The device will decrypte the HTTPS traffic that are not blocked or bypassed.

When the SSL proxy function works in the "Server Inspection - Offload" mode, it will proxy the SSL connections initialized by Web clients, decrypt the HTTPS traffic, and send the HTTPS traffic as plaintext to the Web server.

You can integrate SSL proxy function with the followings:

- Integrate with the application identification function. Devices can decrypte the HTTPS traffic encrypted using SSL by the applications and identify the application. After the application identification, you can configure the policy rule, QoS, session limit, policy-based route.
- Integrate with the Web content function, Web post function, and email filter function. Devices can audit the actions that access the HTTPS website.
- Integrate with AV, IPS, and URL. Devices can perform the AV protection, IPS protection, and URL filtering on the decrypted HTTPS traffic.

Working as Gateway of Web Clients

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, the system will use the SSL proxy profile to deal with the traffic that matches the policy rule. To implement SSL proxy, take the following steps:

1. Configure the corresponding parameters of SSL negotiation, including the following items: specify the PKI trust domain of the device certificates, obtain the CN value of the subject field from the website certificate and import a device certificate to the Web browser.
2. Configure 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 traffic when its SSL negotiation matches the item in the checklist, enable the aduite warning page, and so on.
3. Bind a SSL proxy profile to a proper policy rule. The device will decrypte the HTTPS traffic that matches the policy rule and is not blocked or bypassed by the device.

Configuring SSL Proxy Parameters

Configuring SSL proxy parameters includes the following items:

- Specify the PKI trust domain of the device certificate
- Obtain the CN value of the website certificate
- Import a device certificate to a Web browser

Specifying the PKI Trust Domain of Device Certificate

By default, the device will use the PKI trust domain of trust_domain_ssl_proxy_2048 to re-sign the Web server certificate, i.e. SSL proxy certificate. You can change the PKI trust domain by using the following command in the global configuration mode:

sslproxy trust-domain *trust-domain-name*

- *trust-domain-name* – Select a trust domain. You can select trust_domain_ssl_proxy or trust_domain_ssl_proxy_2048. The trust domain of trust_domain_ssl_proxy uses RSA and the modulus is 1024; the trust domain of trust_domain_ssl_proxy_2048 uses RSA and the modulus is 2048.

To restore the trust domain settings to the default one, use the **no sslproxy trust-domain**.

Specifying Key Pair Modulus Size

Specify the key pair modulus size of the private/public keys that are associated with the SSL proxy certificate. The generated private key is stored by the device and the public key is stored in the SSL proxy certificate. By default, the system uses key modulus size of 2048 bits. You can change it to 1024 bits by using the following command in the SSL proxy profile configuration mode:

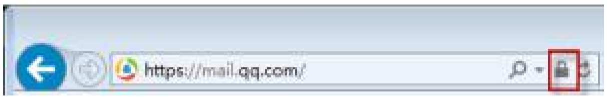
cert-key-modulus 1024

To use the modules size of 2048 bits, use the**no cert-key-nodulus**command in the SSL proxy profile configuration mode.

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, click **View certificates**.
4. In the Details tab, click **Subject**. You can view the CN value in the text box.

Importing a Device Certificate to a Web Browser

In the proxy process, the SSL proxy certificate will be used to replace the website certificate. However, there is no SSL proxy certificate's root certificate in the client browser, and the client cannot visit the proxy website properly. To address this problem, you have to import the root certificate (certificate of the device) to the browser. To import a device to the client browser, take the following steps:

1. Export the device certificate to your local PC. Use the following command:

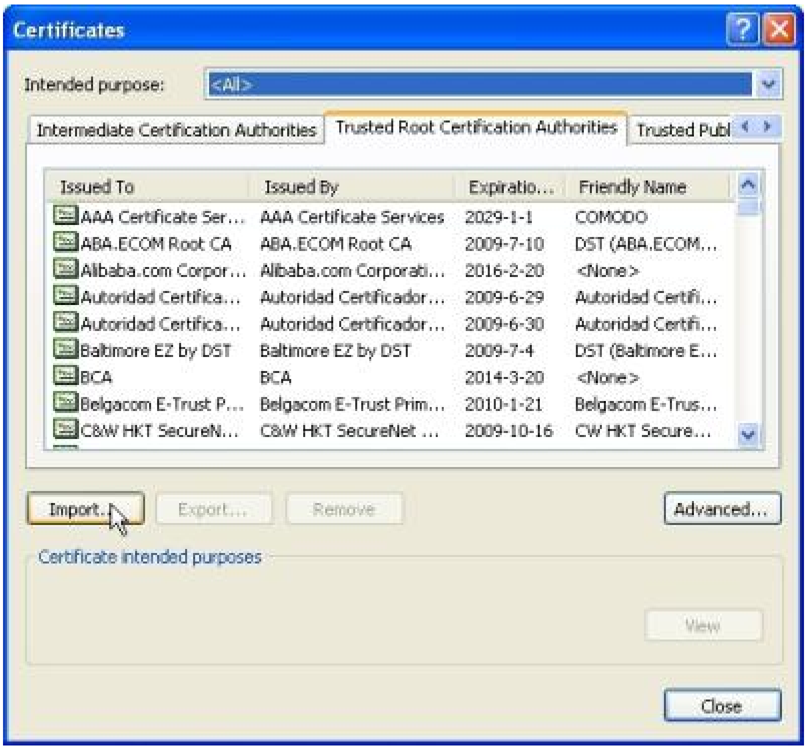
CLI:

export pki *trust-domain-name* {**cacert** | **cert** | **pkcs12** *password* | **pkcs12-der** *password*} **to** {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** i*p-address* | **usb0** | **usb1**} [*file-name*]

Example:

```
hostname# export pki trust_domain_ssl_proxy cacert to tftp server 10.10.10.1
Export ok, target filename 1252639478
hostname#
```

2. Import the certificate (before importing the certificate, change the extension name of the certificate to .crt) to the web browser (take Internet Explore as the example). Start IE, from the toolbar, select **Tools > Internet Options**. On the Content tab, click **Certificates**. In the Certificates dialog, click the **Trusted Root Certification Authorities** tab, and then click **Import**, as shown in the figure below. Import the certificate as prompted by the Certificate Import Wizard.



Intended purpose: <All>

Intermediate Certification Authorities | Trusted Root Certification Authorities | Trusted Publ

Issued To	Issued By	Expiratio...	Friendly Name
AAA Certificate Ser...	AAA Certificate Services	2029-1-1	COMODO
ABA.ECOM Root CA	ABA.ECOM Root CA	2009-7-10	DST (ABA.ECOM...
Alibaba.com Corpor...	Alibaba.com Corporati...	2016-2-20	<None>
Autoridad Certifica...	Autoridad Certificador...	2009-6-29	Autoridad Certifi...
Autoridad Certifica...	Autoridad Certificador...	2009-6-30	Autoridad Certifi...
Baltimore EZ by DST	Baltimore EZ by DST	2009-7-4	DST (Baltimore E...
BCA	BCA	2014-3-20	<None>
Belgacom E-Trust P...	Belgacom E-Trust Prim...	2010-1-21	Belgacom E-Trus...
C&W HKT SecureN...	C&W HKT SecureNet ...	2009-10-16	CW HKT Secure...

If the encryption standard you select in step 1 is pkcs12 or pkcs12-der, you need to enter the certificate password in the pop-up window when importing the certificate to the web browser. The password is the one that you specified in the **pkcs12** *password* | **pkcs12-der** *password*command.

Configuring 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 traffic when its SSL negotiation matches the item in the checklist, enable the aduite warning page, and so on. The system supports up to 32 SSL proxy profiles and each profile supports up to 10,000 statistic website entries. To create a SSL proxy profile, use the following command in the global configuration mode:

sslproxy-profile *profile-name*

- *profile-name* - Specify the name of the SSL proxy profile and enter the SSL proxy profile configuration mode. If the name already exists, the system will enter the SSL proxy profile configuration mode directly.

To delete a SSL proxy profile, use the **no sslproxy-profile** *profile-name*.

Choosing a Work Mode

When the device works as the gateway of Web clients, the SSL proxy function can work in the Client Inspection - Proxy mode.

In the SSL Profile configuration mode, use the following command to choose the work mode:

```
modeclient-inspection proxy
```

Setting the Website List

Set the website list based on the work mode. When the SSL proxy is in the Client Inspection - Proxy 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, specify the CN value of the subject field of the website certificate. In the SSL proxy profile configuration mode, use the following command to add the CN value to the website list:

cert-subject-name *value*

- *value* – Enters the CN value of the subject filed of the website certificate.

To delete a certain CN value from the list, use the **no cert-subject-name** *value*command.

Setting the URL Whitelist

When the SSL proxy is in the Client Inspection - Proxy mode, you can specify URL categories (predefined URL categories or user-defined URL categories) as needed, set the URL websites that will not be proxied by the SSL proxy function. By default, the predefined URL categories "Health & Medicine" and "Finance" have been added to the URL whitelist.

To set the URL whitelist, in the SSL proxy profile configuration mode, use the following command:

url-category*category-name*

- *category-name* - Specifies the name of the URL category that needs to be added to the URL whitelist. Up to 8 URL categories can be added.

To delete a URL category from the URL whitelist, use the **no url-category***category-name*command.

Note:To ensure that the URL whitelist works, please upgrade the predefined URL database before configuring this function.

Configuring the Actions to the HTTPS Traffic

Before performing the SSL proxy process, the device will chek the parameters of the SSL negotiation. When a parameter matches an item in the checklist, the corresponding HTTPS traffic can be blocked or bypassed according to the action you specified.

- If the action is Block, the HTTPS traffic will be blocked and cannot display in the Web browser.

- If the action is Bypass, the HTTPS traffic will not be decrypted. Meanwhile, the device will dynamically add the IP address and port number of the Website to the bypass list. When connecting to the Websites that are dynamically added to the bypass list, the first connection will be disconnected. Uses need to re-connect to the Websites and the content will be displayed.

The device will decrypt the HTTPS traffic that are not blocked or bypassed.

Notice the following items during the configurations:

- When the parameters match multiple items in the checklist and you configure difference actions to different items, the Block action will take effect. THe corresponding HTTPS traffic will be blocked.
- If the HTTPS traffic is not bypassed or blocked after the SSL negotiation check, the system will decrypt the HTTPS traffic.

Checking Whether the SSL Server Verifies the Client Certificate

Check whether the SSL server verifies the client certificate. When the server verifies the client certificate, the system can block or bypass the HTTPS traffic. By default, the system bypass the HTTPS traffic and the traffic will not be decrypted. To bypass the traffic, use the following command in the SSL proxy profile configuration mode:

verify-client bypass

To restore the setting to the default one, use the **no verify-client**command.

Checking Whether the SSL Server Certificate is Overdue

Check whether the SSL server certificate is overdue. When the SSL server certificate is overdue, the system can block or bypass the HTTPS traffic. Use the following command in the SSL proxy profile configuration mode to specify the action:

expired-cert {block | bypass}

- **block | bypass** – Use the block parameter to block the HTTPS traffic. Use the bypass parameter to bypass the HTTPS traffic and the system will not decrypt the HTTPS traffic. By default, the system will decrypt the traffic no matter the SSL server certificate is overdue or not.

To restore the value to the default one, use **no expired-cert**command.

Checking the SSL Protocol Version

Check the SSL protocol version used by the server. When the SSL server uses the specified version of SSL protocol, the system can block its HTTPS traffic. Use the following command in the SSL proxy profile mode to check the SSL protocol version and specify the Block action:

```
ssl-version {sslv3 | tlsv1.0 | tlsv 1.1} {block}
```

- **sslv3 | tlsv1.0 | tlsv 1.1** – Specify a SSL protocol version whose HTTPS traffic you want to block.
- **block** - When the SSL server uses the specified version of SSL protocol, use the block parameter to block its HTTPS traffic. The HTTPS traffic based on the supported SSL protocol versions will be allowed to pass by default.

To restore the setting to the default one, use the **no ssl-version**command.

When SSL server uses the SSL protocol version which is not supported in system, system will block the HTTPS traffic by default. To bypass the HTTPS traffic, in the SSL proxy profile configuration mode, use the following command. When the HTTPS traffic is bypassed, it will not be decrypted:

unsupported-ssl-version bypass

To restore the setting to the default value, use the **no unsupported-ssl-version**command.

Checking the Encryption Algorithm

Check the encryption algorithm used by the SSL server. When the SSL server uses the specified encryption algorithm, the system can block its HTTPS traffic. In the SSL proxy profile configuration mode, use the following command to check the encryption algorithm and specify the Block action:

```
cipher {des | 3des | rc2 | rc4} {block}
```

- **des | 3des | rc2 | rc4** – Specify the encryption algorithm used by the SSL server.
- **block** - When the SSL server uses the specified encryption algorithm, use the block parameter to block its HTTPS traffic. The HTTPS traffic based on the supported encryption algorithms will be allowed to pass by default.

To restore the setting to the default one, use the **no cipher**command.

When SSL server uses the encryption algorithm which is not supported in system, system will block the HTTPS traffic by default. To bypass the HTTPS traffic, in the SSL proxy profile configuration mode, use the following command. When the HTTPS traffic is bypassed, it will not be decrypted:

unsupported-cipher bypass

To restore the setting to the default one, use the **no unsupported-cipher**command.

Checking the Unkown Failure

When SSL negotiation fails and the cause of failure can’ t be confirmed, the system can block or bypass the HTTPS traffic. By default, system block the HTTPS traffic. To bypass the HTTPS traffic, in the SSL proxy profile configuration mode, use the following command. When the HTTPS traffic is bypassed, it will not be decrypted:

unknown-failure bypass

To restore the setting to the default value, use the **no unknown-failure**command.

Verifying the Web Server Certificate

Network will become unsafe when users access the untrusted web server. In order to block the traffic that accesses the untrusted server, system supports to use the root certificate list to verify the server certificate. In the SSL proxy profile configuration mode, use the following command:

untrusted-server-cert block

By default, system will perform proxy when users access the untrusted server. To restore to default, in the SSL proxy profile configuration mode, use **no untrusted-server-cert**command.

Enable Warning Page

When the HTTPS traffic is decrypted by the SSL proxy function, the request to a HTTPS website will be redirected to a warning page of SSL proxy. In this page, the system notifies the users that their accesses to HTTPS websites are being monitored and asks the uses to protect their privacy.

In the SSL proxy profile configuration mode, use the following command to enable/disable the warning page:

Enable the warning page: **no ssl-notification-disable**

Disable the warning page: **ssl-notification-disable**

After enabling the warning page, if your HTTPS access behavior originating from one single source IP is matched to any configured policy rule and SSL proxy profile, you will be prompted with the warning page every 30 minutes when visiting the website over HTTPS.

You can clear the SSL proxy warning history. After that, even that you have received the warning page before, you will be prompted immediately when you visit the website over HTTPS again. To clear the SSL proxy audit warning history, in any mode, use the following command:

clear sslproxy notification

Configuring the Description

To add the description to a SSL proxy profile, in the SSL proxy profile configuration mode, use the following command:

description *description*

- *description* – Enters the description.

Use **no description**to delete the description.

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, the system will use the SSL proxy profile to deal with the traffic that matches the policy rule. To implement SSL proxy, take the following steps:

1. Configure a SSL proxy profile, including the following items: choose the work mode, specify the trust domain of the Web server certificate and the HTTP port number of the Web server.
2. Bind a SSL proxy profile to a proper policy rule. The device will decrypte 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 create a SSL proxy profile, use the following command in the global configuration mode:

sslproxy-profile *profile-name*

- *profile-name* - Specify the name of the SSL proxy profile and enter the SSL proxy profile configuration mode. If the name already exists, the system will enter the SSL proxy profile configuration mode directly.

To delete a SSL proxy profile, use the **no sslproxy-profile** *profile-name*command.

Choosing a Work Mode

When the device works as the gateway of Web servers, the SSL proxy function can work in the "Server Inspection - Offload" mode .

- When the SSL proxy function works in the "Server Inspection - Offload" mode, it will proxy the SSL connections initialized by Web clients, decrypt the HTTPS traffic, and send the HTTPS traffic as plaintext to the Web server.

In in the SSL Profile configuration mode, use the following command to specify the work mode:

mode server-inspection offload

- offload - Specify the SSL proxy working mode as "Server Inspection - Offload" mode.

Specifying Trust Domain

Since the device will work as the SSL server and use the certificate of the Web server to establish the SSL connection with Web clients (Web browsers), you need to import the certificate and the key pair into a trust domain in the device.

After you complete the importing, specify the trust domain used by this SSL Profile. In the SSL Profile configuration mode, use the following command to specify the trust domain:

ssl-offload server-trust-domain *trust-domain-name*

- *trust-domain-name* – Specifies the trust domain name that will be used by this SSL Profile.

To cancel the setting, use the no ssl-offload server-trust-domaincommand.

Specifying HTTP Port Number

To specify the HTTP port number of the Web server, in the SSL Profile configuration mode, use the following command:

server-port *port*

- *port* – Specifies the port number. In Server Inspection - Offload Mode, the default port number is 80.

Use the no server-portcommand to cancel the setting.

Enable Warning Page

When the HTTPS traffic is decrypted by the SSL proxy function, the request to a HTTPS website will be redirected to a warning page of SSL proxy. In this page, the system notifies the users that their accesses to HTTPS websites are being monitored and asks the uses to protect their privacy.

In the SSL proxy profile configuration mode, use the following command to enable/disable the warning page:

Enable the warning page: **no ssl-notification-disable**

Disable the warning page: **ssl-notification-disable**

After enabling the warning page, if your HTTPS access behavior originating from one single source IP is matched to any configured policy rule and SSL proxy profile, you will be prompted with the warning page every 30 minutes when visiting the website over HTTPS.

You can clear the SSL proxy warning history. After that, even that you have received the warning page before, you will be prompted immediately when you visit the website over HTTPS again. To clear the SSL proxy audit warning history, in any mode, use the following command:

clear sslproxy notification

Configuring the Description

To add the description to a SSL proxy profile, in the SSL proxy profile configuration mode, use the following command:

description *description*

- *description* − Enters the description.

Use **no description**to delete the description.

Binding the SSL Proxy Profile to a Policy Rule

After binding the SSL proxy profile to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration. To bind the SSL proxy profile to a policy rule, enter the policy rule configuration mode in two steps. First, in the global configuration mode, use the following command to enter the policy configuration mode:

policy-global

Then, in the policy configuration mode, use the following command to enter the policy rule configuration mode:

rule [**id** *id-number*]

To bind the SSL proxy profile to a policy rule, in the policy rule configuration mode, use the following command:

sslproxy *profile-name*

- *profile-name* - Specifies the name of profile that is bound to the SSL proxy.

After the binding, you need to modify the priority of the policy rule to assure the traffic matching to this rule is prioritized. After then, you need to specify the user, destination zone and schedule of the rule. You can also enable or disable the rule. For more information, see the “Policy” .

Viewing SSL Proxy Information

To view the SSL proxy information, use the following commands:

- View the trusted SSL certificates: **show sslproxy trustca** [*file-name*]
- View the certificates in the dynamic bypass list:**show tcproxy exempt**
- View the SSL proxy state, including the SSL proxy work mode, statistics, and the PKI domain of the SSL proxy certificate: **show sslproxy state**
- View the SSL profile information: **show sslproxy-profile** [*profile-name*]

Chapter 13 Monitor

The chapter introduces the following topics:

- "Monitor" describes how to configure all monitoring statistics function for the system.
- "Logs" introduces all the log functions of the system and how to output various log information of the device.
- "Diagnostic Tool" describes all troubleshooting commands.
- "NetFlow" describes how to configure the NetFlow function to perform statistics and analysis on network traffic.

Monitor

Overview

Monitor include:

- User Monitor: Monitor based on user, Gathers statistics on the data and traffic passing through user, usergroup, address Book.
- Application Monitor: Monitor based on application, Gathers statistics on the data and traffic passing through application, application-group.
- Threat Monitor: Monitor based on threat, Gathers statistics on the threats.
- iQoS Monitor: Monitor based on iQoS, Gathers statistics on the pipes.
- Service/Network Node Monitor: Monitor based on service/network node, Gathers statistics on the packet loss rate and latency of service/network nodes.
- Device Monitor: Monitor based on devices. Gathers statistics on the total traffic, interface traffic, zone, Online IP , new/concurrent sessions, NATand hardware status.
- URL Hit: Monitor based on URL. Gathers statistics on user/IPs, URLs and URL categories.
- Application Block: Gathers statistics on the applications and user/IPs.
- Keyword Block: Gathers statistics on the Web keyword, Web keywords, email keywords, posting keywords and users/IPs.
- Authentication User: Gathers statistics on the authenticated users.

- User-defined Monitor: Gathers statistics on the data passing through the FS device.

If IPv6 is enabled, system will count the total traffic/sessions/AD/URLs/applications of IPv4 and IPv6 address. Only User Monitor/Application Monitor/Cloud Application Monitor/Device Monitor/URL Hit/Application Block/User-defined Monitor support IPv6 address.

> Tip: It is strongly recommended to use WebUI to configuring and view the monitor results, because it can render the data information more vividly. CLI is not recommended.

User Monitor

Gathers statistics on the data and traffic passing through user, usergroup, address Book. If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

Configuring Monitor Address Book

The monitor address is a database that stores the user's address which is used for the statistics. In the global configuration mode, use the following command:

statistics address *address-entry-name*

- *address-entry-name* – Specifies the name of the address entry.

To disable address-based statistics, in the global configuration mode, use the following command:

no statistics address *address-entry-name*

Viewing Address Book Statistical Information

To view the statistical information on the traffic from or to the specified address, in any mode, use the following command:

show statistics address [*address-entry-name*] [**current** | **lasthour** | **lastday** | **lastmonth**]

- *address-entry-name* – Specifies the name of the address entry. If this parameter is not specified, the command will show traffic statistics of all the address entries being referenced by the statistics function (by command statistics address address-entry-name).
- **current** – Shows the real-time traffic statistics of the specified address entry
- **lasthour** – Shows the traffic statistics of the specified address entry per 30 seconds for the last 60 minutes.
- **lastday** – Shows the traffic statistics of the specified address entry per 10 minutes for the last 24 hours.

Viewing Monitor Address Entry Information

In any mode, use the following command:

show monitor-address

Viewing the Stat-set for User Monitor

The predefined stat-set for user monitor includes:

Type	Name	Description
User Monitor	predef_user_bw	Statistics on the traffic of all the users
	predef_user_sess	Statistics on the sessions of all the users
	predef_user_app_bw	Statistics on the traffic of all the users' applications
	predef_exstat_exstat_ip_bw	Statistics on the user traffic of the selected address book
	predef_exstat_exstat_ip_sess	Statistics on the user sessions of the selected address book
	predef_exstat_exstat_app_bw	Statistics on the app traffic of the selected address book
	predef_exstat_exstat_app_sess	Statistics on the app sessions of the selected address book

To view the predefined stat-set information for user monitor, see Viewing Stat-set Information.

Tip: Non-root VSYS also supports user monitor, but does not support address book statistics.

Application Monitor

Application-based statistics allows you to gather statistics on the traffic of the specified application in real time, or per 30 seconds, per 10 minutes and per 24 hours in the last 60 minutes, 24 hours and 30 days respectively. If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

Configuring Monitor Application Group

To configure the monitor application group, in the global configuration mode, use the following command:

statistics application-group *application-group-name*

- *application-group-name* – Specifies the name of the application group.

To delete monitor application group, in the global configuration mode, use the following command:

no statistics application-group *application-group-name*

Viewing Application-based Statistical Information

To view the statistical information on the traffic of the specified application, in any mode, use the following command:

show statistics application-group [*application-group-name*] [**current** | **lasthour** | **lastday** | **lastmonth**]

- *application-group-name* – Specifies the name of the application group. If this parameter is not specified, the command will show traffic statistics of all the application groups being referenced by the statistics function (by command statistics servgroup servicegroup).
- **current** – Shows the real-time traffic statistics of the specified application group.
- **lasthour** – Shows the traffic statistics of the specified application group per 30 seconds for the last 60 minutes.
- **lastday** – Shows the traffic statistics of the specified application group per 10 minutes for the last 24 hours.
- **lastmonth** – Shows the traffic statistics of the specified application group per 24 hours for the last 30 days.

Viewing the Stat-set for Application Monitor

The predefined stat-set for application monitor includes:

Type	Name	Description
application monitor	predef_app_bw	Statistics on the traffic of all the applications
	predef_app_sess	Statistics on the sessions of all the applications
	predef_exstat_exstat_ip_bw	Statistics on the user traffic of the selected application group
	predef_exstat_exstat_ip_sess	Statistics on the user sessions of the selected application group
	predef_exstat_exstat_app_bw	Statistics on the app traffic of the selected application group.

Type	Name	Description
	predef_exstat_exstat_app_sess	Statistics on the app sessions of the selected application group.

To view the predefined stat-set information for application monitor, see Viewing Viewing Stat-set Information.

> Tip: Non-root VSYS also supports application monitor, but does not support to monitor application group.

Threat Monitor

Viewing the Stat-set for Threat Monitor

The predefined stat-set for threat monitor includes:

Type	Name	Description
threat monitor	predef_ip_dip_threat	Statistics on the all the threats

To view the predefined stat-set information for threat monitor, see Viewing Stat-set Information.

iQoS Monitor

Only supports to use WebUI to viewing the iQoS monitor information, see FSOS_WebUI_User_Guide.

Device Monitor

Non-root VSYS also supports device monitor, but doesn't support hardware status. If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address. The commands of device monitor:

Viewing Interface-based Statistical Information

To view the statistical information on the traffic passing through the specified interface, in any command mode, use the following command:

show statistics interface-counter interface *interface-name* {**second** | **minute** | **hour**}

- *interface-name* – Specifies the name of the interface.
- **second** – Shows the traffic statistics of the specified interface per 5 seconds for the last 60 seconds.
- **minute** – Shows the traffic statistics of the specified interface per minute for the last 60 minutes.

- **hour** – Shows the traffic statistics of the specified interface per hour for the last 24 hours.

Viewing the Stat-set for Device Monitor

The predefined stat-set for device monitor includes:

Type	Name	Description
Device Monitor	predef_zone_ bw	Statistics on the traffic of all the security zones
	predef_if_bw	Statistics on the traffic of all the interfaces
	predef_zone_sess	Statistics on the sessions of all the security zones
	predef_if_sess	Statistics on the sessions of all the interfaces

To view the predefined stat-set information for device monitor, see Viewing Stat-set Information.

URL Hit

The predefined stat-set for URL hit includes:

Type	Name	Description
URL Hit	predef_url_hit	Statistics on the URL hits
	predef_user_url	Statistics on the URLs accessed by the users
	predef_url_cat_hit	Statistics on the URL category hits
	predef_user_url_cat_hit	Statistics on the URL categories accessed by the users

If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

To view the predefined stat-set information for URL hit, see Viewing Stat-set Information.

Tip: Non-root VSYS also supports URL hit in NSG series platforms.

Link State Monitor

Link state monitoring can calculate the sampling traffic information of the specific interface in the link, including latency, packet loss rate, jitter, bandwidth utilization, so as to realize the monitoring and display of the overall status of the link. System also supports for link detection to calculate the traffic information of the specific destination IP address in the link, including latency, and jitter.

Enabling/Disabling Link User Experience Monitor

To enable the link user experience monitor, first enter the link monitor configuration mode, and then specify the binding interface. In the global configuration mode, use the following command to specify the binding interface:

link-perf-monitor interface *interface-name*

- *interface-name* – Specify the interface name.

To delete the interface, use the **no link-perf-monitor interface** *interface-name*command in the link monitor configuration mode.

To enable the link user experience monitor for interface, in the link monitor configuration mode, use the following command:

monitor on

To disable this function for the specified interface, use the **no monitor on** command in the link monitor configuration mode.

Enabling/Disabling Application Switch for Interface

After enabling the application switch, you can see details of the specific application in this interface. By default, the application switch is disabled. To enable the application switch, in the link monitor configuration mode, use the following command:

application on

To disable this function for the specified interface, use the **no application on**command in the link state monitor configuration mode.

Specify the Description of Interface

To specify the description for the binding interface, in the link monitor configuration mode, use the following command:

description *string*

- *string* - Specify the description for the binding interface.

To delete the description, use the **no description** in the link monitor configuration mode.

Viewing Link Configuration Information

To view link state monitor configuration information, in any mode, use the following command:

show link-perf-monitor information

Viewing Statistics Information of Link User Experience

To view statistics information of link user experience, in any mode, use the following command:

show link-perf-monitor statistics [**interface** *interface-name* [**application** *application-name*][**history** {**minute** | **hour** | **day** | **month**}]]

- **interface** *interface-name* – View the link user experience monitoring statistics according to the specified interface.
- **application** *application-name* – View the link user experience monitoring statistics according to the specified application. If not specified, the system will display the statistics information according to the specified interface.
- **history** {**minute** | **hour** | **day** | **month**} – View the history statistics information.

Configuring the Link Detection Destination

System supports for link detection to calculate the traffic information of the specific destination IP address in the link, including latency, and jitter.

To configure the detection destination, first enter the link detection monitor configuration mode, and then specify the destination IP address. In the global configuration mode, use the following command to specify the destination IP address:

link-detect-object

To configure the link detection destination of IPv4, in the link detection monitor configuration mode, use the following command:

ip *A.B.C.D* **protocol** {**tcp** [**port** *port-number*] | **icmp**} [**interval** *value*] [**description** *description*]

- *A.B.C.D*- Specify the IP address of detection destination.
- **tcp** [**port** *port-number*]- Specify the protocol type as TCP and specify the port number.
- **icmp**- Specify the protocol type as ICMP.
- **interval** *value*- Specifies the interval time of the detection packet. The value range is 1 to 5 seconds, the default value is 1.
- **description** *description*-Specify the description for the detection destination.

To delete the detection destination, use the **no ip** *A.B.C.D* in the link detection monitor configuration mode.

To configure the link detection destination of IPv6, in the link detection monitor configuration mode, use the following command:

ipv6 *X:X:X:X::X* **protocol** {**tcp** [**port** *port-number*] | **icmpv6**} [**interval** *value*] [**description** *description*]

- *X:X:X:X::X*- Specify the IPv6 address of detection destination.
- **tcp** [**port** *port-number*]- Specify the protocol type as TCP and specify the port number.
- **icmpv6**- Specify the protocol type as ICMPv6.
- **interval** *value*- Specifies the interval time of the detection packet. The value range is 1 to 5 seconds, the default value is 1.
- **description** *description*- Specify the description for the detection destination.

To delete the detection destination, use the **no ipv6** *X:X:X:X::X* in the link detection monitor configuration mode.

Viewing Link Detection Monitor Configuration Information

To view link detection monitor configuration information, in any mode, use the following command:

show link-detect-object {**all** | *A.B.C.D* | *X:X:X:X::X*}

- **all** – Display the link detection monitor configuration information of all the destination IP address.
- *A.B.C.D* | *X:X:X:X::X* - Display the link detection monitor configuration information of the specified destination IP address.

Application Block

The predefined stat-set for Application Block includes:

Type	Name	Description
Application Block	predef_app_block	Statistics on the application blocks
	predef_user_app_block	Statistics on the application blocks of all the users
	predef_user_app_app_block	Statistics on the application blocks of the specified user

If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

To view the predefined stat-set information for Application Block, see Viewing Stat-set Information.

Tip: Non-root VSYS also supports application block in NSG series platforms.

Keyword Block

The predefined stat-set for Keyword Block includes:

Type	Name	Description
Keyword Block	predef_kw_block	Statistics on the webpage/E-mail/Web posting keyword blocks
	predef_user_kw_block	Statistics on the keyword blocks of all the users
	predef_user_kw_kw_block	Statistics on the keyword blocks of the specified user

To view the predefined stat-set information for Keyword Block, see Viewing Stat-set Information.

Tip: Non-root VSYS also supports keyword block in NSG series platforms.

Authentication User

The commands of authentication User:

show auth-user

View the online authuser information.

Command:

show auth-user [**username** *user-name* **interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

username *user-name* -View the online user of specific username information .

web-auth -View the online WebAuth user information.

scvpn -View online users of all SCVPN instances.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user scvpn**

show auth-user agent

View the information of the online agent users.

Command:

show auth-user agent [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

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

vrouter *vrouter-name* -Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

```
hostname# show auth-user agent interface ethernet0/0
```

show auth-user dot1x

View the information of the online 802.1x users.

Command:

show auth-user dot1x [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

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

vrouter *vrouter-name* -Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

```
hostname# show auth-user dot1x
```

show auth-user interface

View the online users information that use specific interface as authentication ingress interface.

Command:

show auth-user interface *interface-name*

Description:

interface-name -Specifies the interface name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

```
hostname# show auth-user interface ethernet1/1
```

show auth-user ip

View the online user of specific IP information .

Command:

show auth-user agent [**ip** *ip-address*]

Description:

ip-address -Specifies the IP address.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

```
hostname# show auth-user ip 10.180.32.1
```

show auth-user l2tp

To view all the clients of the L2TP instance.

Command:

show auth-user l2tp [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

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

vrouter *vrouter-name* -Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

```
hostname# show auth-user l2tp interface ethernet0/1
```

show auth-user mac

View the online user of specific MAC address.

Command:

show auth-user mac *mac-address*

Description:

mac-address -Specifies the MAC address.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

```
hostname# show auth-user mac 0050.569d.0b7e
```

show auth-user radius-snooping

To view the information of the online users.

Command:

show auth-user radius-snooping [**interface** *interface-name* | **vrouter** *vrouter-name* | **slot** *slot-no*]

Description:

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

vrouter *vrouter-name* - Specifies the interface VRouter name.

slot *slot-no* - Specifies the number.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user radius-snooping**

show auth-user static

View the static auth-user, include IP or MAC binding users.

Command:

show auth-user {**static** | **mac** *mac-address* | **ip** *ip-address* } [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

mac *mac-address* -Specifies the MAC address for binding.

ip *ip-address* -Specifies the IP address for binding.

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

vrouter *vrouter-name* - Specifies the VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

```
hostname# show auth-user static
```

show auth-user scvpn

View online users of all SCVPN instances.

Command:

show auth-user scvpn [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

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

vrouter *vrouter-name* - Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

```
hostname# show auth-user scvpn
```

show auth-user ad-scripting

View the information of the online sso-agent users.

Command:

show auth-user ad-scripting [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

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

vrouter *vrouter-name*- Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user ad-scripting**

show auth-user ad-polling

View the information of the online users.

Command:

show auth-user ad-polling [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

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

vrouter *vrouter-name* - Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user ad-polling**

show auth-user sso-radius

View the information of the online users.

Command:

show auth-user sso-radius [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

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

vrouter *vrouter-name*- Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user sso-radius**

show auth-user sso-monitor

View the information of the online users.

Command:

show auth-user sso-monitor [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

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

vrouter *vrouter-name* - Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user sso-monitor**

show auth-user webauth-ntlm

View the information of the online users.

Command:

show auth-user webauth-ntlm [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

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

vrouter *vrouter-name* - Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

```
hostname# show auth-user webauth-ntlm
```

show auth-user xauth

View the information of the online XAUTH users.

Command:

show auth-user xauth [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

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

vrouter *vrouter-name* - Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

```
hostname# show auth-user xauth
```

show auth-user webauth

View the online WebAuth user information.

Command:

show auth-user webauth [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

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

vrouter *vrouter-name* - Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

```
hostname# show auth-user webauth
```

show auth-user vrouter

View the user of specific VRouter.

Command:

show auth-user vrouter

Description:

None

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

```
hostname# show auth-user vrouter trust-vr
```

User-defined Monitor

The stat-set of FSOS allows you to gather statistics on the data passing through the device. With this function configured, you can view the real-time or periodical statistical information based on data types or grouping methods. All the statistical information can be filtered as needed to help you have a more detailed and accurate understanding of the resource allocation and network security status of system.

If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

User-defined monitor statistics include:

- Creating a stat-set
- Configuring the type of statistical data
- Configuring a data grouping method
- Configure a filter

Creating a Stat-set

To create a stat-set, in the global configuration mode, use the following command:

statistics-set *name*

- *name* – Specifies the name of the stat-set. The length is 1 to 31 characters.

After executing the above command, the system will create a stat-set with the specified name, and enter the configuration mode; if the name of the stat-set exists, the system will directly enter the stat-set configuration mode.

To delete the specified stat-set, in the global configuration mode, use the following command:

no statistics-set *name*

Configuring the Type of Statistical Data

The type of statistical data of stat-sets includes bandwidth, session, new session ramp-up rate, attack rate, virus number, intrusion count, URL hit, keyword block and application block. To configure the type of statistical data, in the stat-set configuration mode, use the following command:

target-data {bandwidth | session | rampup-rate | url-hit| application-block| attack-rate } [record-history] [root-vsys-only]

- **bandwidth | session | rampup-rate | url-hit | application-block | attack-rate** – Specifies the type of statistical data of stat-sets. It can be bandwidth, session, new session ramp-up rate, attack rate, virus number, intrusion count, URL hit or application block and AD attack count.
- **record-history** – Monitors data of the last 24 hours.
- **root-vsys-only** – Just monitors data of root VSYS. If this parameter is not configured, data of all VSYSs will be statistical.

To remove the configurations that specify the type of statistical data of the stat-set, in the stat-set configuration mode, use the following command:

no target-data

Note:When configuring a stat-set, keep in mind that:

- The URL hit statistics are only available to users who have a URL license.
- Non-root VSYS only supports types including bandwidth, session, new session ramp-up rate and URL hit
- If you specified the root-vsys-only parameter, data grouping method cannot be configured to VSYS.

Configuring a Data Grouping Method

The data grouping methods of statistical set include IP, interface, security zone, application, user, URL, URL category and VSYS type. The actual options may vary from different date types. Non-root VSYS also supports grouping methods including IP, interface, security zone, application, user, URL and URL category.

To configure a data grouping method, in the stat-set configuration mode, use the following command:

group-by {[**ip** [**directional**] [**initiator** | **responder** | **belong-to-zone** *zone-name* | **not-belong-to-zone** *zone-name* | **belong-to-interface** *interface-name* | **not-belong-to-interface** *interface-name*]] | **interface** [**directional**] | **zone** [**directional**] | **application** | **user** [**directional**] | **url** | **url-category** | **vsys**}

- **ip** − Specifies IP address as the data grouping method for the stat-set. You can use **initiator** | **responder** | **belong-to-zone** *zone-name* | **not-belong-to-zone** *zone-name* | **belong-to-interface** *interface-name* | **not-belong-to-interface** *interface-name*parameters to specify the IP range for the statistics. It can be the IP that initiates the session (**initiator**), the IP that receives the session (**responder**), the IP that belongs to a specific security zone (**belong-to-zone** *zone-name*), the IP that does not belong to a specific security zone (**not-belong-to-zone** *zone-name*), the IP that belongs to a specific interface (**belong-to-interface** *interface-name*), or the IP that does not belong to a specific interface (**not-belong-to-interface** *interface-name*).
- **directional** − Specifies the statistical results for both directions, i.e., when the data is grouped by IP, interface or security zone, the inbound and outbound traffic, the number of received and sent sessions, the ramp-up rate of new received and sent sessions will be gathered for the statistics respectively; if this option is not configured, the default statistics result is non-directional, i.e., when the data is grouped by IP, interface or security zone, all the traffic, sessions and ramp-up rate of news sessions will be gathered for the statistics.
- **interface** − Specifies interface as the data grouping method for the stat-set.

- **zone** – Specifies security zone as the data grouping method for the stat-set.
- **application** – Specifies application as the data grouping method for the stat-set. In such a case the type of statistical data should not be AD attack rate, URL hit count and keyword block count.
- **user** – Specifies user as the data grouping method for the stat-set.
- **url** – Specifies URL as the data grouping method for the stat-set.
- **url-category** – Specifies URL category as the data grouping method for the stat-set.
- **vsys** – Specifies VSYS as the data grouping method for the stat-set.

To cancel of the configurations that specify the data grouping method of the stat-set, in the stat-set configuration mode, use the following command:

no group-by

The following table lists statistical information based on IP type:

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
No direction	Initiator	Statistics on the traffic of the initiator's IP	Statistics on the session number of the initiator's IP	Statistics on the new sessions of the initiator's IP	Statistics on the URL hit count of the specified IPs	Statistics on the keyword block count of the specified IPs	Statistics on the application block count of the specified IPs
	Responder	Statistics on the traffic of the responder's IP	Statistics on the session number of the responder's IP	Statistics on the new sessions of the responder's IP			
	Belong to zone	Statistics on the traffic of an IP that	Statistics on the session number of an IP that	Statistics on the new sessions of an IP that			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
		belongs to a specific security zone	belongs to a specific security zone	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 zone	Statistics on the new sessions of an IP that does not belong to a specific security zone			
	Belong to interface	Statistics on the traffic of an IP that belongs to a specific interface	Statistics on the session number of an IP that belongs to a specific interface	Statistics on the new sessions of an IP that belongs to a specific interface			
	Not belong to interface	Statistics on the traffic of 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 interface	Statistics on the new sessions of an IP that does not belong to a specific interface			
Bi-directional	Initiator	Statistics on the inbound and	Statistics on the number of received and sent sessions	Statistics on the new received and sent sessions			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
		outbound traffic of the initiator's IP	of the initiator's IP	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			
	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			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
	Not belong to zone	Statistics on the inbound and outbound traffic of an IP that does not belong to a specific security zone	Statistics on the number of received and sent sessions of an IP that does not belong to a specific security zone	Statistics on the new received and sent sessions of an IP that does not belong to a specific security zone			
	Belong to interface	Statistics on the inbound and outbound traffic of an IP that belongs to a specific interface	Statistics on the number of received and sent sessions of an IP that belongs to a specific interface	Statistics on the new received and sent sessions of an IP that belongs to a specific interface			
	Not belong to interface	Statistics on the inbound and 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 the traffic of the specified interfaces	Statistics on the session number of the specified interfaces	Statistics on the new sessions of the specified interfaces	Statistics on the URL hit count of the specified interfaces	N/A	N/A
	Bi-directional	Statistics on the inbound and outbound traffic of the specified	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			

Group by	Direction	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
		interfaces					
Application	N/A	Statistics on the traffic of the specified applications	Statistics on the session number of the specified applications	Statistics on the new sessions of the specified applications	N/A	N/A	Statistics on the block count of the specified applications
User	No direction	Statistics on the traffic of the specified users	Statistics on the session number of the specified users	Statistics on the new sessions of the specified 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					
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	N/A	N/A

Group by	Direction	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
					hit count of the specified URL categories		
VSYS	N/A	Statistics on the traffic of the specified VSYSs	Statistics on the session number of the specified VSYSs	Statistics on the new sessions of the specified VSYSs	Statistics on the URL hit count of the specified VSYSs	N/A	N/A

Configuring a Filter

You can configure a filtering condition for the stat-set to gather statistics on the specified condition, such as statistics on the session number of the specified security zone, or the traffic of the specified IP.

Type	Description
filter zone	Data is filtered by security zone.
filter zone zone-name ingress	Data is filtered by ingress security zone.
filter zone zone-name egress	Data is filtered by egress security zone.
filter interface	Data is filtered by interface.
filter interface if-name ingress	Data is filtered by ingress interface.
filter interface if-name egress	Data is filtered by egress interface.
filter application	Data is filtered by application.
filter ip	Data is filtered by address entry.
filter ip add-entry source	Data is filtered by source address (address entry).
filter ip add-entry destination	Data is filtered by destination address (address entry).

Type	Description
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.

To configure a filter, in the stat-set configuration mode, use the following command:

filter {**ip** {*A.B.C.D/M* | *address-entry*} [**source** | **destination**] | **interface** *name* [**ingress** | **egress**] | **zone** *name* [**ingress** | **egress**] | **application** *name* | **user** *user-name aaa-server-name* | **user-group** *user-group-name aaa-server-name*}

- **ip** {*A.B.C.D/M* | *address-entry*} – Specifies an IP as the filter. The IP can be an IP address range (for example, 10.101.0.1, 255.255.255.0 or 10.101.0.1/24) or an address entry defined in the system address book. If IPv6 is enabled, system will support to monitor items of IPv6 address.
  - **source|destination** – Specifies a source IP address or destination IP address as the filter.
- **interface** *name* – Specifies an interface as the filter.
  - **ingress | egress** – Specifies an ingress interface or egress interface as the filter.
- **zone** *name* – Specifies a security zone as the filter.
  - **ingress** | **egress** – Specifies an ingress or egress of a security zone as the filter.
- **application** *name* – Specifies an application as the filter.
- **user** *user-name aaa-server-name* – Specifies a user as the filter.
- **user-group** *user-group-name aaa-server-name* – pacifies a user group as the filter.

Repeat the command to configure multiple filters. The system supports up to 32 filters for each stat-set. If multiple filters configured for the same stat-set belong to the same type, then the logical relationship among these conditions will be OR; if they belong to different types, the logical relationship among these conditions will be AND.

To delete the specified type of filters, in the stat-set configuration mode, use the following command:

no filter {**ip** {*A.B.C.D/M* | *address-entry* } [**source** | **destination**] | **interface** *name* [**ingress** | **egress**] | **zone** *name* [**ingress** | **egress**] | **application** *name* | **user** *user-name aaa-server-name* | **user-group** *user-group-name aaa-server-name*}

To delete all types of filters, in the stat-set configuration mode, use the following command:

no filter all

Enabling/Disabling Stat-set

By default all the predefined stat-set for user monitor, application monitor, device monitor are disabled except for the stat-set of bandwidth.

To enable or disable a stat-set, in the stat-set configuration mode, use the following commands.

- Enable: **active**
- Disable: **no active**

Tip: After the above command is executed in the root VSYS, specified predefined stat-set of all VSYSs will be enabled or disabled（except that the non-root VSYS does not support this predefined stat-set）. You can not enable or disable their own predefined stat-set in non-root VSYSs.

Viewing Stat-set Information

To view the configuration information of the predefined and user-defined stat-set, in any mode, use the following command:

show statistics-set *name* [{**current** | **history** | **history-max**} [**sort-by** {**up** | **down** | **item**}]]

- **show statistics-set** – Shows the configuration information of all the stat-sets in the system.
- *name* – Specifies the name of the stat-set to show the configuration information of the stat-set.
- **current** | **history** | **history-max** – Shows specific statistics of the specified stat-set, including:
    - **current** – Shows the current statistics of the specifies stat-set.
    - **history** – Shows historic statistics of the specified stat-set. The system samples data every five minutes.
    - **history-max** – Shows historic maximum statistics of the specified stat-set. This parameter is only applicable to stat-set of session type.

- sort-by {up | down | item} – Specifies the sorting method for the statistics of the specified stat-set (in a descending order of the file size).
    - up - Sorted by outbound data.
    - down – Sorted by inbound data (only when the Group by is configured with Bi-directional parameters).
    - item - Sorted by Group by objects.

Logs

Overview

Devices are designed with the log function. System records and outputs various system logs, including event logs, threat logs, configuration logs, operation logs, network logs, data security logs (file filter logs, content filter logs, network behavior record logs), traffic logs and debug logs.

- Event logs - Event logs are divided into eight severity levels: errors, warnings, notification, informational, emergencies, alerts, critical and debugging. For more information about log severity, see Log Severity.
- Configuration logs - Configuration logs describe the changes of configurations, e.g. configurations on interfaces.
- Operation logs - Logs related with clear command, exec command and some corresponding WebUI operations, such as the delete operation of NBT cache.
- Network logs - Network logs record operations of network services, e.g. PPPoE and DDNS.
- Threat logs - Threat logs related to behaviors threatening the protected system, e.g. attack defense and application security.
- File filter logs – Logs related with file filter function.
- Content filter logs – Logs related with content filter function, e.g. 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.
- Traffic logs - Traffic logs consist of session logs, NAT logs, and web surfing logs
    - Session logs - Session logs, e.g. session protocols, source and destination IP addresses and ports.

- NAT logs - NAT logs, including NAT type, source and destination IP addresses and ports.
- URL logs - logs about network surfing, e.g. Internet visiting time, web pages visiting history, URL faltering logs.

- Debug logs - Debug logs record the system debugging information.

The log function of FSOS is a tool to show device operation status, providing evidence for you to analyze the network and protect against network attacks.

Log Severity

Event logs categorize system events by severities. The eight severities are described as follows:

Severity	No.	Description	Log Definition
Emergencies	0	Identifies invalid system events.	LOG_EMERG
Alerts	1	Identifies problems which need immediate attention, e.g., the device is being attacked.	LOG_ALERT
Critical	2	Identifies urgent problems, such as hardware failure.	LOG_CRIT
Errors	3	Generates messages for system errors.	LOG_ERR
Warnings	4	Generates messages for warning.	LOG_WARNING
Notifications	5	Generates messages for notice and special attention.	LOG_NOTICE
Informational	6	Generates informational messages.	LOG_INFO
Debugging	7	Generates all debugging messages, including daily operation messages.	LOG_DEBUG

Log Output

Log messages can be sent to the following destinations. You can specify one of them at your own choice:

- Console - The console port of the device. You can close this destination via CLI.
- Remote - Includes Telnet and SSH.
- Buffer - Memory buffer.

- File - By default, FSOS creates a file to record log messages. You can also specify a file in a USB destination to output log messages.
- Syslog Server - Sends logs to a UNIX or Windows Syslog Server.
- Email - Sends logs to a specified email account.
- Localdb - Sends logs to the local database of the device.

Event logs can be sent to all the above destinations except for Localdb; threat logs can be sent to all the above destinations except for Localdb; traffic logs can be sent to console, buffer, syslog server, and file; network and debug logs can only be sent to console, buffer and syslog server.

Log Format

To facilitate the access and analysis of the system logs, FSOS logs follow a fixed pattern of information layout, i.e. **date/time, severity level@module: descriptions**. See the example below:

2018-02-05 01:51:21, WARNING@LOGIN: Admin user "admin" logged in through console from localhost.

Configuring System Logs

You can configure the following log options via CLI:

- Enabling and disabling the log function
- Sending and filtering event logs
- Sending threat logs
- Sending configuration, debug and network logs
- Sending traffic logs
- Sending data security logs (file filter logs, content filter logs, network behavior record logs)
- Configuring a Syslog Server
- Specifying a facility
- Displaying hostname/username in the traffic logs
- Configuring an email address
- Configuring a SMTP instance
- Viewing log configurations

- Viewing logs
- Exporting logs
- Clearing logs

Enabling/Disabling the Log Function

By default, the traffic logs are disabled (enabling the above logs will affect system performance). To enable or disable a system log, in the global configuration mode, use the following command:

- Enable:**logging** {**event** | **configuration** | **operation** | **network** | **traffic** {**session** | **nat** | **urlfilter**} | **debug** | **threat**| **email** | **data-security [dlp** | **cf** | **nbr]**} **on**
- Disable: **no logging** {**event** | **configuration** | **operation** | **network** | **traffic** {**session** | **nat** | **urlfilter**} | **debug** | **threat**| **email** | **data-security [dlp** | **cf** | **nbr]**} **on**

Sending and Filtering Event Logs

You can specify the output destination for the event logs as needed, and filter the output logs based on the severity.

To send event logs to the console, remote terminal, syslog server, mobile phone, hard-disk card or enable email notification, and filter the output logs, in the global configuration mode, use the following command:

logging event to {**console** | **remote** | **syslog** | **email** } [**severity** *severity-level*]

- **console** – Sends the event logs to the console.
- **remote** – Sends the event logs to the remote terminal.
- **syslog** – Sends the event logs to the Syslog Server.
- **email** – Enables email notification.
- **severity** *severity-level* – Specifies the severity of the output event logs to filter the logs. Only the logs of the specified severity or higher severities will be sent, i.e., the number should be equal to or smaller than the specified number. For example, if the specified severity is Notifications, then system will only send event logs of Notifications, Warnings and Errors severities.

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

no logging event to {**console** | **remote** | **syslog** |**email** }

To send the event logs to the memory buffer and filter the logs, in the global configuration mode, use the following command:

logging event to buffer [**severity** *severity-level*] [**size** *buffer-size*]

- **severity** *severity-level* – Specifies the severity of the output event logs to filter the logs. Only the logs of the specified severity or higher severities will be sent, i.e., the number should be equal to or smaller than the specified number. For example, if the specified severity is Notifications, then system will only send event logs of Notifications, Warnings and Errors severities.
- **size** *buffer-size* – Specifies the buffer size. The value range is 4096 to 10485764 bytes. The default value is 1048576.

To disable the function, in the global configuration mode, use the command **no logging event to buffer**.

To write the event logs to a file and filter the logs, in the global configuration mode, use the following command:

logging event to file [**severity** *severity-level*] [**name** [**usb0** | **usb1**] *file-name*] [**size** *file-size*]

- **severity** *severity-level* – Specifies the severity of the output event logs to filter the logs. Only the logs of the specified severity or higher severities will be sent, i.e., the number should be equal to or smaller than the specified number. For example, if the specified severity is Notifications, then system will only write event logs of Notifications, Warnings and Errors severities.
- **name** [**usb0** | **usb1**] *file-name* – Specifies the USB disk and file that are used to save the logs.
- **size** *file-size* – Specifies the size of the file (on the USB disk or Flash disk) to which the logs are written to. The value range is 4096 to 10485764 bytes. The default value is 1048576.

To disable the function, in the global configuration mode, use the command **no logging event to file**.

Sending Threat Logs

You can specify the output destination for the threat logs as needed. To send threat logs to the console, remote terminal, syslog server, hard-disk or enable email notification, in the global configuration mode, use the following command:

logging threat to {**console** | **remote** | **syslog** [**custom-format** [**distributed** [**round-robin** | **src-ip-hash**]]]| **email** | **localdb** [**size** *size*][**location** *storage-name*][**storage** {**automatically-overwrite** | **stop-overwrite**}}

- **console** − Sends the threat logs to the console.
- **remote** − Sends the threat logs to the remote terminal.
- **syslog** − Sends the threat logs to the Syslog Server.
- **custom-format** − Sends the log messages in plaintext. By default, the system sends the log messages in plaintext.
- **distributed** − Sends the log messages to multiple syslog servers in the distribution mode.
- **src-ip-hash** | **round-robin** − Specifies the server selection algorithm.**src-ip-hash**indicates the source-hashing algorithm and **round-robin**indicates the round-robin scheduling algorithm. The round-robin scheduling algorithm is the default algorithm.
- **email** − Enables email notification.
- **localdb** − Sends the logs to the local database(hard-disk card). Only several platforms support the parameters.
  - **size** − Enter a number as the percentage of a storage the logs will take. Value range is 1 to 90, and the default is 30. For example, if you enter 30, the event logs will take at most 30% of the total disk size.
  - **location** − Specifies the location that stores the threat logs.
  - **storage** {**automatically-overwrite** | **stop-overwrite**} − If **automatically-overwrite**is selected, the logs which exceed the disk space will overwrite the old logs automatically. If **stop-overwrite**is selected, system will stop storing new logs when the logs exceed the disk space.

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

no logging threat to {**console** | **remote** | **syslog** [**custom-format** [**distributed** [**round-robin** | **src-ip-hash**]]] | **email**| **localdb** }

To send the threat logs to the memory buffer, in the global configuration mode, use the following command:

logging threat to buffer [**severity** *severity-level*] [**size** *buffer-size*]

- **severity** *severity-level* − Specifies the severity of the output threat logs to filter the logs. Only the logs of the specified severity or higher severities will be sent, i.e., the number should be equal to or smaller than the specified number. For example, if the specified severity is Notifications, then system will only send event logs of Notifications, Warnings and Errors severities.

- **size** *buffer-size* – Specifies the buffer size. The value range is 4096 to 1048576 bytes. The default value is 1048576.

To disable the function, in the global configuration mode, use the command **no logging threat to buffer**.

To write the threat logs to a file, in the global configuration mode, use the following command:

logging threat to file [**severity** *severity-level*] [**name** [**usb0** | **usb1**] file-name] [size file-size]

- **severity** *severity-level* – Specifies the severity of the output threat logs to filter the logs. Only the logs of the specified severity or higher severities will be sent, i.e., the number should be equal to or smaller than the specified number. For example, if the specified severity is Notifications, then system will only send event logs of Notifications, Warnings and Errors severities.
- **name** [**usb0** | **usb1**] *file-name* – Specifies the USB disk and file that are used to save the logs.
- **size** *file-size* – Specifies the size of the file (on the USB disk or Flash disk) to which the logs are written to. The value range is 4096 to 1048576 bytes. The default value is 1048576.

To disable the function, in the global configuration mode, use the command **no logging threat to file**.

Sending Configuration/ Operation/Debug/Network Logs

You can specify the output destination for the configuration, debug and network logs as needed.

To send configuration, operation, debug or network logs to the console, syslog server, memory buffer , file or local database, in the global configuration mode, use the following command:

logging {**configuration** | **network**} **to** {**console** | **syslog** | **localdb** [**size** *size*][**location** *storage-name*][**storage** {**automatically-overwrite** | **stop-overwrite**}}

- **configuration** | **network** – Specifies the type of the logs that will be sent. The available options include configuration and network.
- **console** – Sends the logs to console.
- **syslog** - Sends the logs to syslog server.
- **localdb** – Sends the logs to the local database(hard-disk card). Only several platforms support the parameters.
  - **size** – Enter a number as the percentage of a storage the logs will take. Value range is 1 to 30, and the default is 10. For example, if you enter 30, the event logs will take at most 30% of the total disk size.

- **location** – Specifies the location that stores the configuration and network logs.
- **storage** {**automatically-overwrite** | **stop-overwrite**} – If **automatically-overwrite**is selected, the logs which exceed the disk space will overwrite the old logs automatically. If **stop-overwrite**is selected, system will stop storing new logs when the logs exceed the disk space.

logging [**debug** | **operation**]**to** {**console** | **syslog**}

- **console** – Sends the debug and operation logs to console.
- **syslog** - Sends the logs to syslog server.

To disable the function, in the global configuration mode, use the command **no logging** {**configuration**| **operation** | **debug** | **network**} **to** {**console** | **syslog** | **localdb**}

To write the configuration , operation or network logs to a file, in the global configuration mode, use the following command:

logging {**configuration** | **operation** | **network**} **to file** [**name** [**usb0** | **usb1**] *file-name*] [**size** *file-size*]

- **configuration | operation | network** – Specifies the log type.
- **name** [**usb0** | **usb1**] *file-name* – Specifies the USB disk and file that are used to save the logs.
- **size** *file-size* – Specifies the size of the file (on the USB disk or Flash disk) to which the logs are written to. The value range is 4096 to 1048576 bytes. The default value is 1048576.

To disable the function, in the global configuration mode, use the command **no logging** {**configuration** | **operation** | **network**} **to file**.

To send configuration, operation, debug or network logs to the memory buffer, in the global configuration mode, use the following command:

logging {**configuration** | **operation** | **debug** | **network**} **to buffer** [**size** *buffer-size*]

- **configuration** | **operation** | **debug** | **network** – Specifies the type of the logs that will be sent. The available options include configuration, debug and network.
- **size** *buffer-size* - Specifies the buffer size. The value range is 4096 to 524288 bytes. The default value is 1048576.

To disable the function, in the global configuration mode, use the command **no logging** {**configuration** | **operation** | **traffic** | **debug** | **network**} **to buffer**.

Sending Traffic Logs

Traffic logs consist of session logs, NAT logs, and web surfing logs. You can send traffic logs to the console, syslog server, memory buffer. You can select the output destination according to your requirements.

To send the traffic logs to the console , buffer or syslog server, use the following command in the global configuration mode:

logging traffic {**session** | **nat** | **urlfilter**} **to** {**console** | **syslog** | **buffer** [**size** *buffer-size*]}

- **session** | **nat** | **urlfilter** – Specifies the log type that you want to output.
- **console** | **syslog** | **buffer** – Specifies the output destination. You can output the logs to the console ,buffer or syslog server.
- **size** *buffer-size* - Specifies the buffer size. The value range is 4096 to 524288 bytes. The default value is 1048576.

In the global configuration mode, use the following command to disable the output function: **no logging traffic** {**session** | **nat** | **urlfilter**} **to** {**console** | **syslog** | **buffer** }.

Sending Data Security Logs

You can specify the output destination for the data security logs (file filter logs, content filter logs, network behavior record logs) as needed. To send data security logs (file filter logs, content filter logs, network behavior record logs)to the console, remote terminal, syslog server, local database, or enable email notification, in the global configuration mode, use the following command:

logging data-security [**dlp** | **cf** | **nbr**] **to** {**console** | **syslog**[**binary-format** [**distributed** [**src-ip-hash** | **round-robin**]] | **custom-format**]] }

- **console** – Sends the data security logs to the console.
- **syslog** – Sends the data security logs to the Syslog Server.
- **binary-format** – Sends the logs in binary format.
- **distributed** – Sends the logs to multiple servers in the distribution mode.
- **src-ip-hash | round-robin** – Specifies the server selection algorithm.**src-ip-hash**indicates the source-hashing algorithm and**round-robin**indicates the round-robin scheduling algorithm. The round-robin scheduling algorithm is the default algorithm.
- **custom-format** – Sends the logs in plaintext. By default, the system sends the logs in plaintext.

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

no logging data-security [**dlp** | **cf** | **nbr**] **to** {**console** | **syslog** }

To send the data security logs (file filter logs, content filter logs, network behavior record logs) to the memory buffer, in the global configuration mode, use the following command:

logging data-security [**dlp** | **cf** | **nbr**] **to buffer** [**size** *buffer-size*]

- **size** *buffer-size* – Specifies the buffer size. The value range is 4096 to 524288 bytes. The default value is 524288.

To disable the function, in the global configuration mode, use the command **no logging data-security** [**dlp** | **cf** | **nbr**] **to buffer**.

Configuring the Output Log Format

FSOS logs follow a fixed pattern of information layout. By default, the logs sent to the Syslog Server does not display the year, the hostname and the log severity, you can configure the output log format as needed. In the global configuration mode, use the following command:

- Display the four digit year:**logging syslog 4digit-year-timestamp**
- Display the hostname and the log severity:**logging syslog additional-information**

To cancel displaying of four digit year /hostname/ log severity, in the the global configuration mode, use the following command:

- Cancel display the four digit year:**no logging syslog 4digit-year-timestamp**
- Cancel display the hostname and the log severity: **no logging syslog additional-information**

Configuring a Syslog Server

To send logs to a Syslog Server, you need to configure the IP address or host name of the Syslog Server, or configure the VRouter and UDP/TCP port number of the Syslog Server as needed. To configure a Syslog Server, in the global configuration mode, use the following command:

logging syslog {*ip-address* | *hostname*} {**tcp** *port-number* | **udp** *port-number* | **secure-tcp** *port-number* [**server-cert-check-disable**]| **vrouter** *vr-name* {**tcp** *port-number* | **udp** *port-number* | **secure-tcp** *port-number* [**server-cert-check-disable**]} | **source-interface** *interface-name* {**tcp** *port-number* | **udp** *port-number* | **secure-tcp** *port-number* [**server-cert-check-disable**]}} [**type** *log-type*]

- *ip-address* | *hostname* – Specifies the IP address or host name of the Syslog Server.

- **tcp** *port-number* | **udp** *port-number* | **secure-tcp** *port-number* [**server-cert-check-disable**] – Specifies the protocol type and port number. If "Secure-TCP" protocol is selected, you can type **server-cert-check-disable**， and system can transfer logs normally and do not need any certifications.
- **vrouter** *vr-name* – Specifies the name of the VRouter.
- **source-interface** *interface-name* - Specifies the source interface on which logs are sent. The system will use the IP address of the interface as the source IP and send logs to the syslog server. If this interface is configured with a management IP address, the management IP address will be priorized.
- **type** *log-type* – Specifies the log type. If this parameter is configured, only the specified log type will be sent to the syslog server.

To delete the Syslog Server configuration, in the global configuration mode, use the following command:

no logging syslog {*ip-address* | *hostname*} {**tcp** *port-number* | **udp** *port-number* | **secure-tcp** *port-number* [**server-cert-check-disable**]| **vrouter** *vr-name* {**tcp** *port-number* | **udp** *port-number* | **secure-tcp** *port-number* [**server-cert-check-disable**]} | **source-interface** *interface-name* {**tcp** *port-number* | **udp** *port-number* | **secure-tcp** *port-number* [**server-cert-check-disable**]}} [**type** *log-type*]

Specifying a Facility

To send the log information to a UNIX Syslog Server, you need to specify a facility for the Syslog Server. To specify a facility, in global configuration mode, use the following command:

logging facility local*x*

- **local***x* – Specifies the facility. The value range of x is 0 to 7. The default value is 7.

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

Displaying Hostname/Username in the Traffic Logs

Traffic logs consist of session logs, NAT logs, and web surfing logs. By default the hostname and username are not displayed in the traffic logs. To display the hostname or username in the traffic logs, in the global configuration mode, use the following command:

- Display the hostname of the session logs, NAT logs, and web surfing logs: **logging content hostname**
- Display the username of the session logs: **logging session content username**

After executing the above commands, the hostname and username will be displayed in the traffic logs.

> Note: The NetBIOS name resolution function is the prerequisite of displaying hostname in the traffic logs. For detailed configuration procedure, see Configuring NetBIOS Name Resolution.

To cancel the displaying of hostname/username, in the global configuration mode, use the following commands:

- no logging {session | nat | urlfilter} content hostname
- no logging session content username

Configuring an Email Address

To enable the email notification function, you need to configure an email address to receive the log messages. To configure the email address, in the global configuration mode, use the following command:

logging email to *email-address* **smtp** *smtp-instance*

- *email-address* – Specifies the email address that is used to receive the log messages.
- **smtp** *smtp-instance* – Specifies the SMTP instance of the email address (must be a valid SMTP instance in the system).

To delete the configuration of email address, in the global configuration mode, use the following command:

no logging email to *email-address*

Configuring a SMTP Instance

To configure a SMTP instance, in global configuration mode, use the following command:

smtp name *smtp-name* **server** {*ip-address* | *hostname*} {**from** *email-addr* | **vrouter** *vr-name* **from** *email-addr* }[**username** *user-name* **password** *password*]

- *smtp-name* – Specifies the name of the SMTP instance.
- *ip-address* / *hostname* – Specifies the IP address or hostname of the SMTP server.
- *email-addr* – Specifies the sender's address.
- **vrouter** *vr-name* – Specifies the VRouter of the SMTP server.
- **username** *user-name* **password** *password* – Specifies the username and password of the sender account.

To delete the specified SMTP instance, in the global configuration mode, use the command **no smtp name** *smtp-name*.

Configuring PBR Log Function

After you enable PBR log, the system will generate PBR logs once PBR policy rule is matched by traffic.

Enabling PBR Log Function

You can enable PBR log function basing on PBR policy rules. By default, this feature is disabled. To enable or disable PBR log function, in the PBR policy rule configuration mode, use the following command:

- To enable: **log enable**
- To disable: **no log enable**

To display the PBR logs in output destination, in the global configuration mode, use the following command:

logging traffic pbr on

In the global configuration mode, use the **no logging traffic pbr on**command

to cancel the settings.

> Tip: If you have configured prioritized destination routing (DBR) lookup, even if PBR policy rule is matched by traffic, the system will not generate PBR logs.

Sending PBR Logs

You can send PBR traffic logs to the console, syslog server and memory buffer. You can select the output destination according to your requirements.

To send PBR traffic logs to the console, syslog server or memory buffer, in the global configuration mode, use the following command:

logging traffic pbr to {**console** | **syslog** | **buffer** [**size** *buffer-size*]}

- **console** | **syslog** | **buffer** – Specify the output destination. You can output the logs to the console, syslog server or buffer.
- **size** *buffer-size* - Specify the buffer size. The value range is 4096 to 2097152 bytes. The default value is 1048576.

In the global configuration mode, use the **no logging traffic pbr to** {**console** | **syslog** | **buffer**}command to disable the corresponding output function.

Tip: Currently, the system does not output:

- PBR logs of binary format.
- PBR logs for IPv6.

Displaying Hostname/Username in PBR Logs

By default, the hostname and username are not displayed in the PBR traffic logs. To display the hostname or username in PBR logs, in the global configuration mode, use the following command:

logging pbr content {**hostname** | **username**}

In the global configuration mode, use the **no logging pbr content** {**hostname** | **username**}command to cancel the display of hostname/username.

Viewing PBR Logs

To view all the PBR logs, in any mode, use the following commands:

show logging traffic pbr

Viewing Log Configurations

To view the log configurations, in any mode, use the following commands:

- Show the system log configuration:**show logging**
- Show the syslog server configuration:**show logging syslog**
- Show the email address configuration:**show logging email**
- Show the log statistics:**show logging statistics**
- Show the SMTP server configuration: **show smtp**
- Show if the hostname and username are displayed in the traffic logs: **show logging content**

Viewing Logs

To view the specified type of logs, in any mode, use the following commands:

- Show the event logs:
  show logging event [**severity** *severity-level*]
- Show the debug, network or threat logs:
  show logging {**debug** [**slot** *slot-number*] [**cpu** *cpu-number*] | **network** | **threat** }

- Show the configuration logs:

show logging configuration

- Show the operation logs:

show logging [**operation**]

- Show the data security logs (file filter logs, content filter logs, network behavior record logs):

show logging data-security [**dlp** | **cf** | **nbr**]

- Show all the traffic logs:

show logging traffic

- Show the traffic logs (session log part):

show logging traffic *session* **filter-session** [**src-ip** *A.B.C.D* | **src-port** *port-num* | **dst-ip** *A.B.C.D* | **dst-port** *port-num* | **protocol** {**icmp** | **tcp** | **udp** | **others**} | **policy-id policy-id** | **action** {**policy-deny** | **session-start** | **session-end** | **policy-default**}]

- Show the traffic logs (NAT log part):

show logging traffic *nat* **filter-nat** [**src-ip** *A.B.C.D* | **src-port** *port-num* | **dst-ip** *A.B.C.D* | **dst-port** *port-num* | **protocol** {**icmp** | **tcp** | **udp** | **others**} | **trans-src-ip** *A.B.C.D* | **trans-src-port** *port-num* | **trans-dst-ip** *A.B.C.D* | **trans-dst-port** *port-num* | **snat-rule-id** *rule-id* | **dnat-rule-id** *rule-id*]

- Show the traffic logs (URL log part):

show logging traffic urlfilter

Exporting Logs

You can export the event logs and threat logs to the specified FTP server, TFTP server or USB disk.

To export the event logs or threat logs to the specified FTP server, in the execution mode, use the following command:

export log {**event** | **threat** } **to ftp server** *ip-address* **user** *user-name* **password** *password* [*file-name*]

- **event** | **threat** - Specifies the log type that will be exported.
- *ip-address* - Specifies the IP address of the FTP server.
- **user** *user-name* **password** *password* - Specifies the username and password of the FTP server.
- *file-name* - Specifies the name of the file to which the event logs will be exported.

To export the event logs or threat logs to the specified TFTP server, in the execution mode, use the following command:

export log {event | threat } to tftp server *ip-address* [*file-name*]

To export the event logs or threat logs to the specified USB disk, in the execution mode, use the following command:

export log {event | threat } to {usb0 | usb1} [*file-name*]

Clearing Logs

To clear the specified logs in the system, in the execution mode, use the following command:

clear logging { configuration | operation | debug | event | network | threat | traffic {session | nat | urlfilter} | data-security [dlp | cf | nbr]}

- configuration -Clears all the configuration logs information in the system.
- operation -Clears all the operation logs information in the system.
- debug – Clears all the debug logs information in the system.
- event – Clears all the event logs information in the system.
- network – Clears all the network logs information in the system.
- threat – Clears all the threat logs information in the system.
- traffic {session | nat | urlfilter} – Clears the specified traffic logs information in the system.
- data-security [dlp | cf | nbr] – Clears all the data security logs information in the system. File filter logs (dlp), Content filter logs (cf), Network behavior record logs (nbr) .

Note:This command cannot clear the following important event log information:

- Restart: system restart, module restart.
- Hardware exception: fan, power, etc.
- Configurations for deleting or rolling back.
- Swithing between master device and backup device.

Sending Traffic Logs to Syslog Servers

When there are lots of log messages generated by FS devices, a single Syslog server may fail to deal with all the messages. To address this problem, FS devices support the distributed sending function. With this function configured, FS devices can send the log messages to multiple Syslog servers according to a certain algorithm to reduce the pressure to a single Syslog server.

Only the traffic and data security log messages can be sent in the distributed way. And only the threat logs can be sent in plaintext and in the distributed way.

To configure the distributed sending function, in the global configuration mode, use the following command:

logging {**traffic** {**session** | **nat** | **urlfilter**} | **data-security** [**dlp** | **cf** | **nbr**]} **to syslog** [**binary-format** [**distributed** [**src-ip-hash** | **round-robin**]] | **custom-format**]

- **traffic** {**session** | **nat** | **urlfilter**} | **data-security** [**dlp** | **cf** | **nbr**] – Specifies the log type that will be sent.
- **syslog** – Sends the logs to Syslog servers.
- **binary-format** – Sends the traffic logs in the binary format.
- **distributed** – Sends the traffic logs to multiple Syslog servers according to the algorithm specified.
- **src-ip-hash** | **round-robin** – Specifies the algorithm used to choose Syslog servers. **src-ip-hash**, choose the Syslog server according to the source IP address; **round-robin**, choose the Syslog server by the round-robin algorithm, and this is the default algorithm used by the system.
- **custom-format** – Sends logs in the plaintext format. By default, the system will send the traffic logs in the plaintext format.

To remove the traffic log sending configuration, in the global configuration mode, use the following command:

no logging {**traffic** {**session** | **nat** | **urlfilter**} | **data-security** [**dlp** | **cf** | **nbr**]} **to syslog**

To send the threat logs in the plaintext format and in the distributed way, use the following command in the global configuration mode:

logging threat to syslog [**custom-format** [**distributed** [**src-ip-hash** | **round-robin**]]]

- **custom-format** – Sends the logs in the plaintext format. By default, the system sends the logs in the plaintext format.
- **syslog** – Sends the logs to the syslog server.

- **distributed** – Sends the logs to the syslog server in the distributed way.
- **src-ip-hash** | **round-robin** – Specifies the server selection algorithm.**src-ip-hash**indicates the source-hashing algorithm and **round-robin**indicates the round-robin scheduling algorithm. The round-robin scheduling algorithm is the default algorithm.

In the global configuration mode, use the following command to cancel the output of the threat logs:

no logging threat to syslog

Example of Configuring Logs

This section describes two typical CLI log configuration examples: sending event logs to the console and sending event logs to the Syslog server.

Example 1: Sending Event Logs to the Console

Step 1: Enable the event log function:

```
hostname# configure
hostname(config)# logging event on
```

Step 2: Send the event logs to the console; set the severity to Debugging:

```
hostname(config)# logging event to console severity debugging
```

Example 2: Sending Event Logs to the Syslog Server

Step 1: Enable the event log function. The workstation with IP address of 202.38.1.10 is used as the Syslog Server of UDP type; set the severity to Informational:

```
hostname(config)# logging event on
hostname(config)# logging syslog 202.38.1.10 udp 514 type event
hostname(config)# logging event to syslog severity informational
```

Step 2: Power on the Syslog Server.

Example 3: Sending Traffic Logs to a Local File

Step 1:Configure a track object. Track the syslog server whose IP address is 202.38.1.10.

```
hostname(config)# track abc
hostname(config-trackip)# threshold 3
hostname(config-trackip)# ip 202.38.1.10 interface ethernet0/1 interval 2
```

Step 2: Enable the function of sending traffic logs to the syslog server. The IP address of the syslog server is 202.38.1.10. The name of the VRouter is trust-vr, the type is UDP, the port number is 514, and the log type is traffic (NAT logs).

```
hostname(config)# logging traffic nat on

hostname(config)# logging syslog 202.38.1.10 vrouter "trust-vr" udp 514 type traffic nat

hostname(config)# logging traffic nat to syslog
```

Step 3: Power on the syslog server.

Step 4: Configure the settings to send the traffic logs to a local file. The folder name is aa.

```
hostname(config)# logging traffic nat to file name usb0 aa
```

Step 5: Enable the track function for the syslog server and set the maximum rate of sending traffic logs to a file as 600 entries per second.

```
hostname(config)# logging traffic nat to syslog track abc local-backup rate-limit 600
```

Diagnostic Tool

Introduction

System supports the following diagnostic methods:

- Packet Capture Tool: Users can capture packets in the system by Packets Capture Tools. After capturing the packets, you can export them to your local disk and then analyze them by third-party tools.
- Packet Path Detection: Based on the packet process flow, the packet path detection function detects the packets and shows the detection processes and results to users by chart and description. This function can detect the following packet sources: emulation packet, online packet, and imported packet (system provides the Packet Capture Tool for you that can help you capture the packets).

The detectable packets from different packet sources have different detection measures. The system supports the following measures:

- Emulation packet detection: Emulate a packet and detects the process flow in the system of this packet.
- Online packet detection: Perform a real-time detection of the process flow of the packets in the system.
- Imported packet detection: Import the existing packets and detects the process flow in the system of the packets.

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

Using WebUI to configure the diagnostic tool is strongly recommended.

Commands

exec troubleshooting packet-trace (imported detection)

Begin or stop imported packet path detection.

Command:

Begin imported packet path detection: **exec troubleshooting packet-trace filter** *name* **start**

Stop imported packet path detection: **exec troubleshooting packet-trace stop**

Description:

filter *name* - Specifies the name of the imported packet.

Default values:

None

Mode:

Any mode

Guidance:

N/A

Example:

```
hostname# exec troubleshooting packet-trace filter test1 start
```

```
hostname# exec troubleshooting packet-trace stop
```

exec troubleshooting packet-trace emulation-template(emulation detection)

Begin emulation packet path detection.

Command:

exec troubleshooting packet-trace emulation-template *name* **start**

Description:

template *name*- Specifies the name of the emulation packet.

Default values:

None

Mode:

Any mode

Guidance:

N/A

Example:

```
hostname# exec troubleshooting packet-trace emulation-templatetest start
```

export packet-capture-file

Export the file which is captured by Packet Capture Tool.

Command:

export packet-capture-file to {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address*} [**vrouter** *vr-name*] [*file-name*]

Description:

ftp server *ip-address* [**user** *user-name* **password** *password*] -Export the specified file to FTP server.

- *ip-address* - Specifies the FTP IP address.
- **user** *user-name* **password** *password* – Specifies the username and password for the FTP user. If not specified, system will use anonymous to login.

tftp server *ip-address* -Export the specified file to TFTP server.

vrouter *vr-name* -Specifies the VR name.

file-name -Specifies the file name you exported.

Default values:

vrouter *vr-name* - trust-vr;

file-name – pktdump.pcap。

Mode:

Executive mode

Guidance:

N/A

Example:

```
hostname# export packet-capture-file to tftp server 10.1.1.1
```

export troubleshooting packet-trace packet-capture-file

Export the file captured by online packet path detection.

Command:

export troubleshooting packet-trace packet-capture-file to {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address*} [**vrouter** *vr-name*] [*file-name*]

Description:

ftp server *ip-address* [**user** *user-name* **password** *password*] -Export the specified file to FTP server.

- *ip-address* - Specifies the FTP IP address.
- **user** *user-name* **password** *password* – Specifies the username and password for the FTP user. If not specified, system will use anonymous to login.

tftp server *ip-address* -Export the specified file to TFTP server.

vrouter *vr-name* -Specifies the VR name.

file-name- Specifies the file name you exported.

Default values:

vrouter *vr-name* - trust-vr;

file-name – ts_pktdump.pcap。

Mode:

Executive mode

Guidance:

N/A

Example:

```
hostname# export troubleshooting packet-trace packet-capture-file to tftp server 10.1.1.1
```

export troubleshooting packet-trace emulation-template

Export the file captured by emulation packet path detection.

Command:

export troubleshooting packet-trace emulation-template *name* **to** {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address*} [**vrouter** *vr-name*] [*file-name*]

Description:

ftp server *ip-address* [**user** *user-name* **password** *password*] -Export the specified file to FTP server.

- *ip-address* -Specifies the FTP IP address.
- **user** *user-name* **password** *password* – Specifies the username and password for the FTP user. If not specified, system will use anonymous to login.

tftp server *ip-address* - Export the specified file to TFTP server.

vrouter *vr-name* -Specifies the VR name.

file-name -Specifies the file name you exported.

Default values:

vrouter *vr-name* - trust-vr。

Mode:

Executive mode

Guidance:

N/A

Example:

hostname# **export troubleshooting packet-trace emulation-template temp1 to tftp server 10.1.1.1**

import troubleshooting packet-trace

Import a file for packet path detection.

Command:

import troubleshooting packet-trace replay-file from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address*} [**vrouter** *vr-name*] *file-name*

Description:

ftp server *ip-address* [**user** *user-name* **password** *password*] -Import the specified file from FTP server.

- *ip-address* - Specifies the FTP IP address.

- **user** *user-name* **password** *password* – Specifies the username and password for the FTP user. If not specified, system will use anonymous to login.

tftp server *ip-address* -Import the specified file from TFTP server.

vrouter *vr-name* -Specifies the VR name.

file-name -Specifies the file name you imported.

Default values:

vrouter *vr-name* - trust-vr。

Mode:

Executive mode

Guidance:

N/A

Example:

hostname# **import troubleshooting packet-trace replay-file from ftp server 10.1.1.1 user user1 password password1 test.pcap**

packet-capture filter

Specify the packets capture entry.

Command:

packet-capture filter *name* {[[**src-ip** *ip-address*] | [**user** *aaa-server user-name*] | [**user-group** *aaa-server user-name*]] [**src-port** *port-num*] [[**dst-ip** *ip-address*] | [**url** *url*]] [**dst-port** *port-num*] [**proto** {**tcp** | **udp** | **icmp** | *proto-num*}] [**application** *app-name*]} [**max-size** *file-size*] [**description** *description*]

no packet-capture filter *name*

Description:

filter *name* -Enter the name of the packets capture entry.

src-ip *ip-address* -Specifies the source IP address of the packet.

user *aaa-server user-name* -Specifies the user of the packet.

user-group *aaa-server user-name* -Specifies the user group of the packet.

dst-ip *ip-address* -Specifies the destination IP address of the packet.

url *url*-Specifies the URL of the packet.

application *app-name* -Specifies the application type of the packet.

proto {**tcp** | **udp** | **icmp** | *proto-num*} -Specifies the protocol type or the protocol number of the packet.

src-port *port-num* -Specifies the source port of the packet.

dst-port *port-num* -Specifies the destination port of the packet.

max-size *file-size* - Specifies the maximum size of the captured packet file. When the file size reaches the maximum size, the system stops the capturing. The range of the value is from 2M to 20M. The default value is 10M.

description *description* -Specifies the entry description.

Default values:

max-size *file-size* – 10 M。

Mode:

Global configuration mode

Guidance:

The system allows you to create at most 5 packets capture entries.

Example:

hostname(config)# **packet-capture filter filter1 src-ip 192.168.0.1 application http max-size 20 description test**

troubleshooting packet-trace filter (online detection)

Configure online detection.

Command:

troubleshooting packet-trace filter *name* **type live-traffic** {[[**src-ip** *ip-address*] | [**user** *aaa-server user-name*] | [**user-group** *aaa-server user-name*]] [**src-port** *port-num*] [[**dst-ip** *ip-address*] | [**url** *url*]] [**dst-port** *port-num*] [**proto** {**tcp** | **udp** | **icmp** | *proto-num*}] [**application** *app-name*] [**ingress-interface** *interface-name*]} [**description** *description*]

no troubleshooting packet-trace filter *name*

Description:

filter *name* -Specifies the name of the online packet.

src-ip *ip-address* -Specifies the source IP address of the online packet.

user *aaa-server user-name* -Specifies the user of the online packet.

user-group *aaa-server user-name* -Specifies user group of the online packet.

src-port *port-num* -Specifies the source port of the online packet.

dst-ip *ip-address* -Specifies the destination IP address of the online packet.

url *url* -Specifies the URL of the online packet.

dst-port *port-num* -Specifies the destination port of the online packet.

proto {**tcp** | **udp** | **icmp** | *proto-num*} -Specifies the protocol type or the protocol number of the packet.

application *app-name* -Specifies the application type of the online packet.

ingress-interface *interface-name* -Specifies the ingress interface of the online packet.

description *description*- Specifies the description.

Default values:

None

Mode:

Global configuration mode

Guidance:

The system allows you to create at most 5 packets capture entries.

Example:

```
hostname(config)# troubleshooting packet-trace filter test type live-traffic dst-ip 10.1.1.1
application http ingress-interface ethernet0/0
```

troubleshooting packet-trace emulation-template

Configure emulation detection.

Command:

troubleshooting packet-trace emulation-template *name* **type** {**tcp** | **udp**} **src-ip** *ip-address* **src-port** *port-num* **dst-ip** *ip-address* **dst-port** *port-num* **ingress-interface** *interface-name* [**description** *description*]

troubleshooting packet-trace template *name* **type icmp src-ip** *ip-address* **dst-ip** *ip-address* **type** *type-value* **code** *code-value* **ingress-interface** *interface-name* [**description** *description*]

no troubleshooting packet-trace template *name*

Description:

template *name* -Specifies the name of the emulation packet.

type {**tcp** | **udp**} /**type icmp** -Specifies the protocol type of the emulation packet.

src-ip *ip-address* -Specifies the source IP address of the emulation packet.

dst-ip *ip-address*- Specifies the source port of the emulation packet, only when the protocol type is specified as TCP/UDP.

src-port *port-num* -Specifies the destination port of the emulation packet, only when the protocol type is specified as TCP/UDP.

dst-port *port-num* -Specifies the destination IP address of the emulation packet.

type *type-value* **code** *code-value* -Specifies the ICMP type value and code value only when the protocol type is specified as ICMP.

ingress-interface *interface-name* -Specifies the ingress interface of the emulation packet.

description *description* -Specifies the description.

Default values:

None

Mode:

Global configuration mode

Guidance:

The system allows you to create at most 20 emulation packets.

Example:

```
hostname(config)# troubleshooting packet-trace emulation-template temp1 type udp src-ip 10.0.0.1 src-port 10 dst-ip 192.168.0.1 dst-port 100 ingress-interface ethernet0/0
```

NetFlow

Overview

NetFlow is a data exchange method, which records the source /destination address and port numbers of data packets in the network. It is an important method for network traffic statistics and analysis.

FS NetFlow supports the NetFlow Version 9. With this function configured, the device can collect user's ingress traffic according to the NetFlow profile, and send it to the server with NetFlow data analysis tool, so as to detect, monitor and charge traffic.

Configuring NetFlow

The NetFlow configurations are based on interfaces.

To configure the interface-based NetFlow, take the following steps:

1. Enable NetFlow function.
2. Create a NetFlow profile, and then specify the active timeout value, template refresh rate and configure the NetFlow server in the profile.
3. Bind the NetFlow Profile to an interface.

Enabling NetFlow

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

netflow enable

To disable the NetFlow function, in the global configuration mode, use the following command: **no netflow enable**.

Creating a NetFlow Profile

NetFlow profile configurations contains the active timeout value, the template refresh rate, and the NetFlow server settings.

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

netflow-profile *netflow-profile-name*

- *netflow-profile-name* - Specifies the NetFlow profile name and enters the NetFlow profile configuration mode. If the specified name exists, system will directly enter the NetFlow profile configuration mode.

To delete the specified NetFlow profile, in the global configuration mode, use the command **no netflow-profile** *netflow-profile-name*.

Configuring the Template Refresh Rate

You can configure the NetFlow template refresh rate by time or number of packets, after which system will refreshes the NetFlow profile. In the NetFlow profile configuration mode, use the following command:

- Time: **template-refresh-minute** *refresh-value*
  refresh-value -Specifies the time after which system refreshes the NetFlow profile. The range is 1 to 3600 minutes. The default value is 30 minutes.
- Packets: **template-refresh-packet** *packet-value*
  packet-value - Specifies the number of packets. When the number of NetFlow packets exceeds the specified value, system will refreshes the NetFlow profile. The range is 1 to 600. The default value is 20.

Configuring the Active Timeout Value

The active timeout value is the time after which the device will send the collected NetFlow traffic information to the specified server once. In the NetFlow profile configuration mode, use the following command:

active-timeout *timeout-value*

- *timeout-value* − Specifies the active timeout value. The range is 1 to 60 minutes. The default value is 5 minutes.

To restore to the default value, in the NetFlow profile configuration mode, use the following command: **no active-timeout**.

Configuring the NetFlow Server

To configure the NetFlow server for data analysis, in the NetFlow profile configuration mode, use the following command:

server *name* [**ip** *ip-address* | **port** *port-number*]

- *name* − Specifies the server name, the range is 1 to 32 characters.
- **ip** *ip-address* − Specifies the IP address of NetFlow server.
- **port** *port-number* − Specifies the port number of NetFlow server. The range is 1 to 65535. The default value is 9996.

To delete the specified server, in the NetFlow profile configuration mode, use the following command: **no server** *name*.

Note:You can add up to 2 NetFlow servers.

Containing the Enterprise Field

You can specify whether the collected NetFlow traffic information contains the enterprise field.

To specify that the collected NetFlow traffic contains enterprise field, in the NetFlow profile configuration mode, use the following command：

export-enterprise-fields

To specify that the collected NetFlow traffic does not contains enterprise field, in the NetFlow profile configuration mode, use the following command: **no export-enterprise-fields**.

Specifying the Source Interface

To specify the source interface for sending NetFlow traffic information, in the NetFlow profile configuration mode, use the following command:

source interface *interface-name* **address** *interface-address*

- *interface-name* – Specifies the source interface name.
- *interface-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.

To delete the source interface configurations, in the NetFlow profile configuration mode, use the following command: **no source**.

Binding a NetFlow Profile to an Interface

If the NetFlow profile is bound to an interface, the device will collect user's ingress traffic information according to the NetFlow profile. To bind a NetFlow profile to an interface, in the interface configuration mode, use the following command:

netflow-profile *netflow-profile-name*

- *netflow-profile-name* – Specifies the name of the NetFlow profile that will be bound to the interface.

To remove the binding, in the interface configuration mode, use the following command: **no netflow-profile**

Viewing NetFlow Information

To view the configurations of NetFlow profile, in any mode, use the following command:

show netflow-profile [*netflow-profile-name*]

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

show netflow [**generic**] | [**slot** *slot-no*]

- **generic** – Shows the general NetFlow statistic information.
- **slot** *slot-no* – Shows the NetFlow statistic information of the specified slot..

https://www.fs.com

The information in this document is subject to change without notice. FS has made all efforts to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty.