Hillstone Networks Inc.

StoneOS CLI User Guide

Threat Prevention

Version 5.5R5

Hillstone Networks Inc

Contact Information:

US Headquarters:

Hillstone Networks

292 Gibraltar Drive, Suite 105

Sunnyvale, CA 94089

Phone: 1-408-508-6750

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

About this Guide:

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

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

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

hs-doc@hillstonenet.com

TWNO: TW-CUG-UNI-TRT-5.5R5-EN-V1.1-Y17M11

Table of Contents

About This Guide

This document follows the conventions below:

Content

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

CLI

- Braces ({ }): indicate a required element.
- Square brackets ([ ]): indicate an optional element.
- Vertical bar (|): separates multiple mutually exclusive options.
- **`Bold`**: indicates an essential keyword in the command. You must enter this part correctly.
- *`Italic`*: indicates a user-specified parameter.
- The command examples may vary from different platforms.
- In the command examples, the hostname in the prompt is referred to as host-name.

WebUI

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

Command Line Interface

Overview

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

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

CLI Modes and Prompts

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

Execution Mode

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

```
hostname#
```

Global Configuration Mode

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

```
hostname(config)#
```

Sub-module Configuration Mode

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

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

Switching between CLI Modes

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

Table 1: CLI Mode Switching Commands

Mode	Command

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

CLI Error Message

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

Table 2: Error Messages and Description

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

Command Input

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

Command Short Form

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

Listing Available Commands

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

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

Completing Partial Commands

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

Using CLI

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

Previous Commands

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

Shortcut Keys

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

Table 3: Shortcut Key List

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.
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.

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

Filtering Output of Show Commands

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

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

CLI output filter syntax is shown as follows:

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

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

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

Table 4: Regular Expression and Meaning

Regular Expression	Meaning
. (period)	Represents any character.
* (star)	Indicates that there is zero or more of the preceding element.
+ (plus)	Indicates that there is one or more of the preceding element.
^ (caret)	Used at the beginning of an expression, denotes where a match should begin.
$ (dollar)	Used at the end of an expression, denotes that a term must be matched exactly up to the point of the $ character.
_(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 80 characters.

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

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

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

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

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

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

Specifying Connection Timeout

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

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

`console timeout` *`timeout-value`*

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

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

ssh timeout *timeout-value*

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

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

telnet timeout *timeout-value*

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

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

Redirecting the Output of Show Commands

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

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

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

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

- FTP - `ftp://[useranme: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.

Host Defense

With this function enabled, StoneOS can send gratuitous ARP packets for different hosts to protect them against ARP attacks. To configure the host defense function, in the global configuration mode, use the following command:

gratuitous-arp-send ip *ip-address* **mac** *mac-address* **switch-interface** *interface-name* **except-interface** *interface-name* **rate** *rate-value*

- **ip** *ip-address* - Specifies the IP address of the host that uses the device as a proxy.
- **mac** *mac-address* - Specifies the MAC address of the host that uses the device as a proxy.
- **switch-interface** *interface-name* - Specifies the interface that sends gratuitous ARP packets. It can be either a VSwitch or BGroup interface.
- **except-interface** *interface-name* - Specifies the excluded port, i.e., the port that does not send gratuitous ARP packets. Typically it is the port connected to the host that uses the device as a proxy.
- **rate** *rate-value* - Specifies a gratuitous ARP packet send rate. The value range is 1 to 10 packets/sec. The default value is 1.

Repeat the command to configure the gratuitous ARP packets for more hosts. You can configure the Hillstone device to send gratuitous ARP packets for up to 16 hosts.

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

no gratuitous-arp-send ip *ip-address* **switch-interface** *interface-name*

Host Blacklist

The host blacklist function of the Hillstone devices is designed to prevent users from accessing the network during the specified period. To enable the function, you need to add the MAC or IP address of the host to the blacklist, and then bind a schedule.

If the host IP address is added to the blacklist, while its IP is configured as an unrestricted IP and the unrestricted IP function is also enabled, the system will still block that host from accessing the network.

Adding a Blacklist Entry

To add the host to the blacklist, in the global configuration mode, use the following command:

host-blacklist {**mac** *mac-address* | **ip from** *ip-address* **to** *ip-address* **vrouter** *vrouter-name*} [**schedule** *schedule-name*] [**enable** | **disable**]

- *mac-address* - Specifies the MAC address of the host that will be added to the blacklist.
- *ip-address* - Specifies the IP address of the host to be added to the blacklist. Overlapped IP address range is not allowed.
- *vrouter-name* - Specifies the name of VRouter the IP address belongs to.
- *schedule-name* - Specifies the schedule that has been configured in the system. If this parameter is specified, the system will block the host from accessing the network during the specified period; if this parameter is not specified, the system will permanently block the host from accessing the network. For more information about how to create a schedule, see "Creating a Schedule" of "System Management".
- **enable** | **disable** - Enables or disables the host blacklist entry. By default, all the entries in the host blacklist are enabled.

For example, to add the host with the MAC address of 001c.f096.f1ea to the blacklist and bind the schedule named night to the blacklist so that the host cannot access the network during night, use the following commands:

```
hostname(config)# schedule night
hostname(config-schedule)# periodic daily 22:00 to 06:00
hostname(config-schedule)# exit
hostname(config)# host-blacklist mac 001c.f096.f1ea schedule night
```

Modifying a Schedule

To modify the schedule for the specified host blacklist entry, in the global configuration mode, use the following command:

host-blacklist {**mac** *mac-address* | **ip from** *ip-address* **to** *ip-address* **vrouter** *vrouter-name*} **schedule** *new-schedule-name*

- **schedule** *new-schedule-name* - Specifies the name of the new schedule.

For example, to modify the schedule for the host blacklist entry with MAC address 001c.f096.f1ea, and replace its existing schedule named schedule1 with the new schedule named schedule2, use the following commands:

```
hostname(config)# schedule schedule1
hostname(config-schedule)# periodic monday 9:00 to 18:00
hostname(config-schedule)# exit
hostname(config)# schedule schedule2
hostname(config-schedule)# absolute start 01/01/2009 9:00 end 05/01/2009 9:00
hostname(config-schedule)# exit
hostname(config)# host-blacklist mac 001c.f096.f1ea schedule schedule1
```

```
hostname(config)# host-blacklist mac 001c.f096.f1ea schedule
schedule2
```

Enabling or Disabling a Blacklist Entry

The created host blacklist entries can be identified by the MAC addresses or IDs. To enable or disable the specified host blacklist entry, in the global configuration mode, use the following command:

host-blacklist mac {*mac-address* | **id** *id-number* }{**enable** | **disable**}

The created host blacklist entries can be identified by the IP addresses or IDs. To enable or disable the specified host blacklist entry, in the global configuration mode, use the following command:

host-blacklist ip {**from** *ip-address* **to** *ip-address* **vrouter** *vrouter-name* | **id** *id-number*} {**enable** | **disable**}

For example, to disable the host blacklist entry identified by MAC address with the ID of 1, use the following command:

```
hostname(config)# host-blacklist mac id 1 disable
```

After disabling the entry, the entry is not deleted, and still exists in the blacklist. To enable the entry again, use the following command:

```
hostname(config)# host-blacklist mac id 1 enable
```

Viewing the Host Blacklist Content

To view the host blacklist content, in any mode, use the following commands:

- Show all the host blacklist entries identified by MAC address: **show host-blacklist mac**
- Show all the host blacklist entries identified by IP address: **show host-blacklist ip**

Deleting a Host Blacklist Entry

To delete the host blacklist entry identified by MAC address, in global configuration mode, use the following command:

no host-blacklist mac {*mac-address* | **id** *id-number*| **all**}

- *mac-address* - Deletes the host blacklist entry identified by the specified MAC address.
- **id** *id-number* - Deletes the host blacklist entry identified the specified ID number.
- **all** - Deletes all the host blacklist entries identified by all the MAC addresses.

To delete the host blacklist entry identified by IP address, in the global configuration mode, use the following command:

no host-blacklist ip {**from** *ip-address* **to** *ip-address* **vrouter** *vrouter-name* | **id** *id-number*| **vrouter** *vr-name*}

- **from** *ip-address* **to** *ip-address* **vrouter** *vr-name* - Deletes the host blacklist entry by identified by the IP address range of the specified VRouter.
- **id** *id-number* - Deletes the host blacklist identified by the ID number.
- **vrouter** *vrouter-name* - Deletes all the host blacklist entries identified by all the IP addresses of the specified VRouter.

Note: When you delete the VRouter by the command **no ip vrouter** *vrouter-name*, you'll also delete all the records related to this VRouter from the IP blacklist**.**

IP-MAC Binding

Hillstone devices support IP-MAC binding, MAC-port binding and IP-MAC-port binding to reinforce network security control. The bindings obtained from ARP/MAC learning and ARP scan are known as dynamic bindings, and those manually configured are known as static bindings. Besides, the Hillstone devices are also designed with the ARP inspection function.

WebUI: On the Navigation pane, click **Configure** > **Security** > **ARP Defense** to visit the ARP Defense page.

Static Binding

You can add static IP-MAC bindings and MAC-port bindings; you can also prevent the hosts that are enabled with dynamic ARP learning from accessing the Internet, and only allow the hosts with static IP-MAC bindings to access the Internet.

Adding a Static IP-MAC Binding

To add a static IP-MAC binding, in the global configuration mode, use the following command:

arp *ip-address mac-address* [**incompatible-auth-arp**] [**vrouter** *vrouter-name*]

- *ip-address* - Specifies the IP address for static binding.
- *mac-address* - Specifies the MAC address for static binding.
- **incompatible-auth-arp** - If this parameter is configured, ARP authentication will not be implemented on the IP address.
- **vrouter** *vrouter-name* - Adds the static IP-MAC binding to the specified VR. Parameter *vrouter-name* is used to specify the name of the VR. If the parameter is not specified, the static IP-MAC binding configured will belong to the default VR trust-vr.

To delete a static IP-MAC binding, in the global configuration mode, use the following command:

no arp {**all** | *ip-address*} [**vrouter** *vrouter-name*]

- **all** - Deletes all the static IP-MAC bindings in the system.
- *ip-address* - Deletes the static IP-MAC binding for the specified IP address in the system.
- **vrouter** *vrouter-name* - Deletes the static IP-MAC binding for the specified VR. Parameter *vrouter-name* is used to specify the name of the VR. If the parameter is not specified, the system will delete all the static IP-MAC bindings configured in the default VR or for the specified IP address.

Adding a Static IP-Port Binding

To add a static IP-port binding, in the global configuration mode, use the following command:

mac-address-static *mac-address* **interface** *interface-name*

- *mac-address* - Specifies the MAC address for static binding.
- **interface** *interface-name* - Specifies the interface for static binding.

To delete a static IP-port binding, in the global configuration mode, use the following commands:

- Delete all the static MAC-port bindings in the system:

  no mac-address-static all

- Delete all the static MAC-port bindings for the specified interface:

  no mac-address-static interface *interface-name*

- Delete the specified static MAC-port binding:

  no mac**-address-static** *mac-address* {**interface** *interface*-**name** | **vid** *vlan-id*}

Only Allowing Hosts with Static IP-MAC Binding Accessing the Internet

By default, the system allows hosts with dynamic ARP learning enabled to access the Internet. To only allow the hosts with IP-MAC binding enabled to access the Internet, in the interface configuration mode, use the following command:

arp-disable-dynamic-entry

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

no arp-disable-dynamic-entry

Dynamic IP-MAC-Port Binding

Hillstone devices can obtain dynamic IP-MAC-port binding information from:

- ARP learning
- MAC learning

ARP Learning

Hillstone devices can obtain IP-MAC bindings in an Intranet from ARP learning, and add them to the ARP list. By default this function is enabled. Hillstone devices will always keep ARP learning on, and add the learned IP-MAC bindings to the ARP list. If any IP or MAC address changes during the learning process, Hillstone devices will add the updated IP-MAC binding to the ARP list. If this function is disabled, only IP addresses in the ARP list can access Internet.

To configure the ARP learning function, in the VSwitch or BGroup interface configuration mode, use the following commands:

- Enable ARP learning: **`arp-learning`**
- Disable ARP learning: **`no arp-learning`**

MAC Learning

Hillstone devices can obtain MAC-port bindings in an Intranet from MAC learning, and add them to the MAC list. By default this function is enabled. Hillstone devices will always keep MAC learning on, and add the learned MAC-port bindings to the MAC list. If any MAC address or port changes during the learning process, Hillstone devices will add the updated MAC-port binding to the MAC list.

To configure the MAC learning function, in the VSwitch or BGroup interface configuration mode, use the following commands:

- Enable MAC learning: **`mac-learning`**
- Disable MAC learning: **`no mac-learning`**

Viewing IP-MAC-Port Binding Information

To view the IP-MAC binding information (static and dynamic) and the MAC-port binding information (static and dynamic) in the system, use the following commands:

- IP-MAC binding information: **`show arp`** [**`vrouter`** *`vrouter-name`*]
- MAC-port binding information: **`show mac`**

Clearing ARP Binding Information

To clear the ARP binding information (static and dynamic), use the following command:

clear arp [**interface** *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*]

- **interface** *interface-name* - Clears the ARP binding information of the specified interface. Parameter *interface-name* is used to specify the interface name.
- *A.B.C.D* - Clears the ARP binding information of the specified IP address of the interface.
- **vrouter** *vrouter-name* - Clears the ARP binding information of the specified VRouter. Parameter *vrouter-name* is used to specify the VRouter name. If this parameter is not specified, the system will clear the ARP binding information of the default VRouter trust-vr.

Forcing Dynamic MAC-Port Binding

You can force to bind the dynamic MAC-Port binding information learned from the MAC learning function. To force to bind dynamic MAC-port binding, in any mode, use the following command:

exec mac-address dynamic-to-static

DHCP Snooping

DHCP (Dynamic Host Configuration Protocol) is designed to allocate appropriate IP addresses and related network parameters for sub networks automatically. DHCP snooping can create binding relationship between the MAC address of the DHCP client and the allocated IP address by analyzing the packets between the DHCP client and server. When ARP inspection is also enabled, StoneOS will check if an ARP packet passing through can be matched to any binding of the list. If not, the ARP packet will be dropped. In the network that allocates addresses via DHCP, you can prevent against ARP spoofing attacks by enabling ARP inspection and DHCP Snooping.

DHCP clients look for the server by broadcasting, and only accept the network configuration parameters provided by the first reachable server. Therefore, an unauthorized DHCP server in the network might lead to DHCP server spoofing attacks. Hillstone devices can prevent against DHCP server spoofing attacks by dropping DHCP response packets on related ports.

Besides, some malicious attackers send DHCP requests to a DHCP server in succession by forging different MAC addresses, and eventually result in IP address unavailability to legal users by exhausting all the IP address resources. This kind of attacks is commonly known as DHCP starvation. Hillstone devices can prevent against such attacks by dropping request packets on related ports, setting rate limit or enabling validity check.

Enabling/Disabling DHCP Snooping

The BGroup interface, VSwitch interface and VLAN interface of StoneOS all support DHCP snooping. By default, this function is disabled. To enable DHCP snooping for the

BGroup interface or VSwitch interface, in the VSwitch interface or BGroup interface configuration mode, use the following command:

dhcp-snooping

To disable the function, in the VSwitch interface or BGroup interface configuration mode, use the following command:

no dhcp-snooping

To enable DHCP snooping for the VLAN interface, in the global configuration mode, use the following command:

dhcp-snooping vlan *vlan-list*

- *vlan-list* - Specifies the VLAN ID that will be enabled with DHCP snooping. The value range is 1 to 4094, such as 1, 2-4, or 1, 2, 5. StoneOS reserves 32 VLAN IDs (from VLAN224 to VLAN255) for BGroup.

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

no dhcp-snooping vlan *vlan-list*

Configuring DHCP Snooping

You can configure the DHCP snooping function on the device, including the processing methods of DHCP request and response packets, and the validity check. By default, all the DHCP request and response packets are permitted, and the validity check is disabled. To enable the DHCP snooping function, in the Ethernet interface (physical interface of the BGroup, VSwitch or VLAN interface) configuration mode, use the following command:

dhcp-snooping {**deny-request**|**deny-response**|**validity-check**}

- **deny-request** - Drops all the request packets sent by the client to the server.
- **deny-response** - Drops all the response packets returned by the server to the client.
- **validity-check** - Checks if the client's MAC address of the DHCP packet is the same with the source MAC address of the Ethernet packet. If not, the packet will be dropped.

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

no dhcp-snooping {**deny-request**|**deny-response**|**validity-check**}

Configuring DHCP Packet Rate Limit

To configure the DHCP packet rate limit, in the Ethernet interface (physical interface of the BGroup, VSwitch or VLAN interface) configuration mode, use the following command:

dhcp-snooping rate-limit *number*

- *number* - Specifies the number of DHCP packets received per second on the interface. If the number exceeds the specified value, StoneOS will drop the excessive DHCP packets. The value range is 0 to 10000. The default value is 0, i.e., no rate limit.

To cancel the DHCP packet rate limit, in the Ethernet interface configuration mode, use the following command:

no dhcp-snooping rate-limit

Viewing DHCP Snooping Configuration Information

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

show dhcp-snooping configuration

DHCP Snooping List

With DHCP Snooping enabled, StoneOS will inspect all the DHCP packets passing through the interface, and create and maintain a DHCP Snooping list that contains IP-MAC binding information during the process of inspection. Besides, if the VSwitch, VLAN interface or any other Layer 3 physical interface is configured as a DHCP server, StoneOS will create IP-MAC binding information automatically and add it to the DHCP Snooping list even if DHCP Snooping is not enabled. The bindings in the list contain information like legal users' MAC addresses, IPs, interfaces, ports, lease time, etc. To view the DHCP snooping list, in any mode, use the following command:

show dhcp-snooping binding

To clear all or the specified DHCP snooping list entry, in any mode, use the following command:

clear dhcp-snooping binding [**interface** *interface-name* [*A.B.C.D*] | **vlan** *vlan-id* [*A.B.C.D*]]

- **clear dhcp-snooping binding** - Deletes all bindings in the DHCP snooping list.
- **interface** *interface-name* - Specifies the interface name to delete the bindings of the interface.
- **interface** *interface-name* [*A.B.C.D*] - Specifies the IP address under an interface to delete the bindings of the IP address.
- **vlan** *vlan-id* - Specifies the VLAN ID to delete the bindings of the VLAN.
- **vlan** *vlan-id* [*A.B.C.D*] - Specifies the IP address under a VLAN to remove the bindings of the IP address.

ARP Inspection

Hillstone devices support ARP Inspection for interfaces. With this function enabled, StoneOS will inspect all the ARP packets passing through the specified interfaces, and compare the IP addresses of the ARP packets with the static IP-MAC bindings in the ARP list and IP-MAC bindings in the DHCP Snooping list:

- If the IP address is in the ARP list and the MAC address is matched, the ARP packet will be forwarded;
- If the IP address is in the ARP list but the MAC address is not matched, the ARP packet will be dropped;
- If the IP address is not in the ARP list, continue to check if the IP address is in the DHCP snooping list;
- If the IP address is in the DHCP Snooping list and the MAC address is also matched, the ARP packet will be forwarded;
- If the IP address is in the DHCP snooping list but the MAC address is not matched, the ARP packet will be dropped;
- If the IP address is not in the DHCP snooping, the ARP packet will be dropped or forwarded according to the specific configuration.

Enabling/Disabling ARP Inspection

The BGroup, VSwitch and VLAN interface of StoneOS all support ARP inspection. By default, the function is disabled. To enable the function for BGroup or VSwitch interface, in the VSwitch or BGroup interface configuration mode, use the following command:

arp-inspection {**drop** | **forward**}

- **drop** - Drops the ARP packets whose IP address is not in the ARP table.
- **forward** - Forwards the ARP packets whose IP address is not in the ARP table.

To disable the function, in the VSwitch or BGroup interface configuration mode, use the following command:

no arp-inspection

To enable ARP Inspection for the VLAN interface, in the global configuration mode, use the following command:

arp-inspection vlan *vlan-list* {**drop** | **forward**}

- *vlan-list* - Specifies the VLAN ID that will be enabled with ARP Inspection. The value range is 1 to 4094, such as 1, 2-4, or 1, 2, 5. StoneOS reserves 32 VLAN IDs (from VLAN224 to VLAN255) for BGroup.

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

no arp-inspection vlan *vlan-list*

Configuring a Trusted Interface

You can configure a device interface (physical interface of the BGroup, VSwitch or VLAN interface) as the trusted interface. The packets passing through the trusted interface will not be checked by ARP inspection. By default, none of the device interfaces is the trusted interface. To configure a device interface as the trust interface, in the interface configuration mode, use the following command:

arp-inspection trust

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

no arp-inspection trust

Configuring an ARP Rate

To configure the ARP rate, in the interface configuration mode, use the following command:

arp-inspection rate-limit *number*

- *number* - Specifies the number of ARP packets received per second on the interface. If the number exceeds the specified value, StoneOS will drop the excessive ARP packets. The value range is 0 to 10000. The default value is 0, i.e., no rate limit.

To cancel the ARP rate, in the interface configuration mode, use the following command:

no arp-inspection rate-limit

Note: You can only configure ARP rate on physical interfaces that are bound to Layer 2 zones.

ARP Defense

Powered by the ARP learning, MAC learning, authenticated ARP and ARP inspection functions, StoneOS is capable of providing defense against ARP spoofing attacks. Besides, StoneOS can also gather statistics on the ARP spoofing attacks. To view the ARP spoofing attacks statistics, in any mode, use the following command:

show arp-spoofing-statistics [*number*]

- *number* - Shows the statistics of the top number records.

To clear the ARP spoofing attacks statistics, in the execution mode, use the following command:

clear arp-spoofing-statistics

Attack Defense

Overview

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. Hillstone devices provide attack defense functions based on security zones.

Common Network Attacks

This section describes some common network attacks. Hillstone 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 Hillstone 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
- Limiting the number of IP connections
- Viewing the attack defense configurations of the security zone and statistics

WebUI: To configure Attack Defense via WebUI, take the following steps:

1. On the Navigation pane, click **Configure** > **Security** > **Attack Defense** to visit the Attack Defense page.
2. Select a security zone for attack defense from the **Zone** drop-down list.
3. To enable all the attack defense functions for the security zone, select the **Enable all** checkbox, and also select an action from the **Action** drop-down list. To enable an individual defense function, select its corresponding checkbox.
4. Configure parameters for the selected functions.
5. Click **OK** to save the changes.

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, StoneOS 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, StoneOS 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

StoneOS 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, StoneOS 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 StoneOS 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, StoneOS 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, StoneOS will identify the traffic as a SYN flood. The value range is 0 to 50000. The default value is 1500. The value of 0 indicates the 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, StoneOS will identify the traffic as a SYN flood. The value range is 0 to 50000. The default value is 1500. The value of 0 indicates the 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, StoneOS will first detect if the traffic is a destination SYN flood attack: if so, StoneOS will drop the packets and give an alarm, if not, StoneOS will continue

to detect if the traffic is a source SYN attack; if so, StoneOS will drop the packets and give an alarm. The default action is **drop**. To restore to the default action, use the command **no ad syn-flood action**.

Configuring SYN-Proxy

SYN-Proxy is designed to defend against SYN flood attacks in combination with **ad syn-flood**. When both **ad syn-flood** and SYN proxy are enabled, SYN proxy will act on the packets that have already passed the detections of **ad syn-flood**.

The Hillstone devices support SYN-Cookie, a stateless SYN-Proxy mechanism.

To configure the SYN-Proxy and the SYN-Cookie functions for the specified security zone, in the security zone configuration mode, use the following command:

ad syn-proxy [**min-proxy-rate** *number* | **max-proxy-rate** *number* | **proxy-timeout** *number* | **cookie**]

- **ad syn-proxy** - Enables SYN-Proxy for a security zone to defend against SYN Flood attacks. To disable the function, in the security zone configuration mode, use the command **no ad syn-proxy**.
- **min-proxy-rate number** - Specifies the minimum number for SYN packets that will trigger SYN proxy or SYN-Cookie (if enabled by **cookie**). If the number of inbound SYN packets destined to one single port of one single destination IP address per second exceeds the specified value, StoneOS 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, StoneOS will only permit the specified number of SYN packets to pass through during the current and the next second. All the excessive packets of the same type will be dropped during this period. The value range is 1 to 1500000. The default value is 3000. 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 StoneOS 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, StoneOS 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 [**source-threshold** *number* | **destination-threshold** *number* | **action** {**alarm** | **drop**}]

- **ad udp-flood** - Enables 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**.
- **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, StoneOS 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, StoneOS

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, StoneOS 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, StoneOS 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, StoneOS 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, StoneOS 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, StoneOS 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. StoneOS 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, StoneOS 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. StoneOS 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, StoneOS 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.

StoneOS 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, StoneOS 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 StoneOS receives an ARP request, it will log the IP address and reply with another ARP request; and then StoneOS will check if any packet with a different MAC address will be returned, or if the MAC address of the returned packet is the same as that of the ARP 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 StoneOS will check the IP number per MAC in ARP table. If the parameter is set to 0 (the default value), StoneOS will not check the IP number; if set to a value other than 0, StoneOS will check the IP number, and if the IP number per MAC is larger than the parameter value, StoneOS 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 StoneOS will send gratuitous ARP packet(s). If the parameter is set to 0 (the default value), StoneOS will not send any gratuitous ARP packet; if set to a value other than 0, StoneOS will send gratuitous ARP packet(s), and the number sent per second is the specified parameter value. The value range is 0 to 10. To restore to the default value, use the command **no ad arp-spoofing gratuitous-arp-send-rate**.

Configuring DNS Query Flood Attack Defense

DNS (Domain Name System) is used to convert a domain name to an IP address, and resolve an IP address to a domain name. DNS is an application layer protocol, so it can be based on TCP or UDP. DNS Query Flood attacks are based on UDP.

The DNS Query Flood attacks are launched by sending a large number of domain name resolution requests to the target DNS server. Typically the requested domain name is randomly generated, or does not exist at all. When the DNS server being attacked receives the resolution requests, it will first look for the corresponding cache. If the cache is not found and the domain name can not be resolved directly by the server, the DNS server will send a recursive query request to its upper DNS server. The domain name resolution process will bring a heavy load to the DNS server. If the DNS requests per second exceed a certain number, the workload will lead to domain name resolution timeout on the DNS server. .

Hillstone devices support DNS Query Flood attacks defense. You can enable or disable DNS Query Flood attack defense for each security zone individually, and configure the packet number threshold and the actions for DNS Query Flood attacks. To enable DNS Query Flood defense, in the security zone configuration mode, use the following command:

ad dns-query-flood [**recursion**] [**source-threshold** *number*] [**destination-threshold** *number* | **action** {**alarm** | **drop**}]

- **ad dns-query-flood** - Enables DNS Query Flood attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad dns-query-flood**.
- **recursion** - Only limits recursive DNS query packets. If this parameter is not specified, StoneOS 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, StoneOS 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, StoneOS 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 tcp-split-handshake 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*}}

Configuring Session Limit

Hillstone devices support the zone-based session limit function. You can limit the session number and control the new session ramp-up rate for the source IP address, destination address, specified IP address or service 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* } [**application** *application-name*] [**service** *servicename*] [**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.
- **service** *servicename* - Limits the session number of the specified service 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 session ramp-up rate for the IP address or role.
- **schedule** *schedule-name* - Specifies an schedule during which the session limit rule will take effect.

Note: The type of the source address entry and the destination address entry must keep same.

To delete the session limit rule, in the security zone configuration mode, use the following command:

no ad session-limit id *id*

- **id** *id* - The session limit rule ID of the security zone. To view the rule ID, use the command **show session-limit**.

With session limit configured, StoneOS will drop the sessions that exceeds the maximum session number. To view the statistics on the dropped sessions, use the

command show session-limit. To clear the statistics on the dropped sessions in the specified session limit rule, in any mode, use the following command:

clear session-limit id *id* **statistics**

- **id** *id* - Specifies the rule ID. The statistics on the dropped session in the specified session limit rule will be cleared.

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-core NAT" of "Firewall".

WebUI: To create a zone-based session limit rule via WebUI, take the following steps:

1. On the Navigation pane, click **Configure** > **Content** > **Session Limit** to visit the Session Limit page.
2. Click **New**. In the Session Limit Configuration dialog, select the zone you need from the **Zone** drop-down list, and configure session limit conditions.
3. Click **OK** to save your settings.

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

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 Hillstone devices.

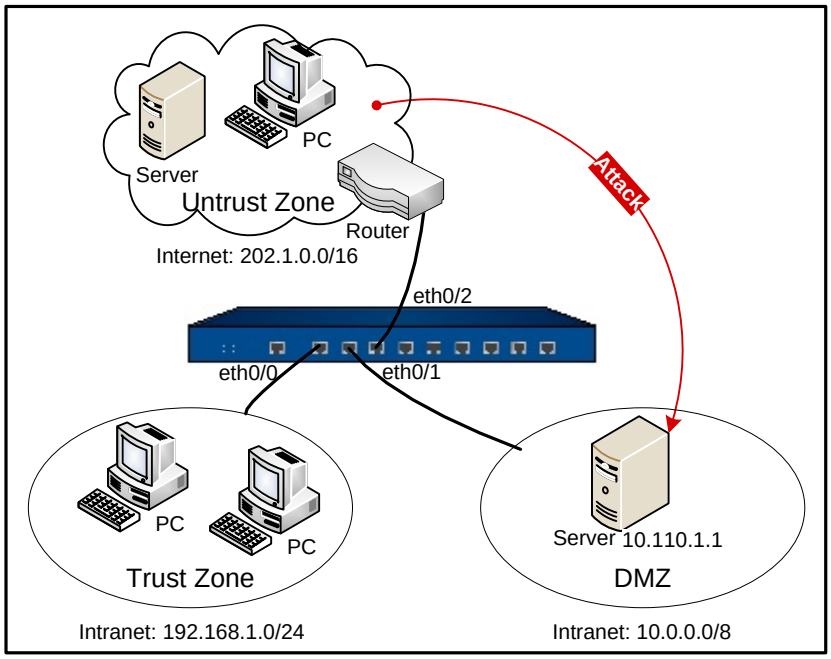
Example of Configuring Land Attack Defense

This section describes a Land attack defense configuration example.

Requirement

Hillstone 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.

Figure 1: Attack Defense Network Topology



Configuration Steps

Step 1: Configure ethernet0/0:

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

Step 2: Configure ethernet0/2:

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ip address 202.1.0.1/24
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Step 3: Configure ethernet0/1:

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

```
hostname(config-if-eth0/1)# zone dmz
hostname(config-if-eth0/1)# ip address 10.0.0.1/8
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 4: Configure a policy rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone dmz
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 5: Enable Land attack defense for the untrust zone:

```
hostname(config)# zone untrust
hostname(config-zone)# ad land-attack
hostname(config-if)# exit
hostname(config)#
```

Step 6: Test the Land attack defense configured for the server. Craft a packet with identical source and destination IP address, and send it to 10.110.1.1. The Hillstone device will detect a Land attack, and then give an alarm and drop the packet.

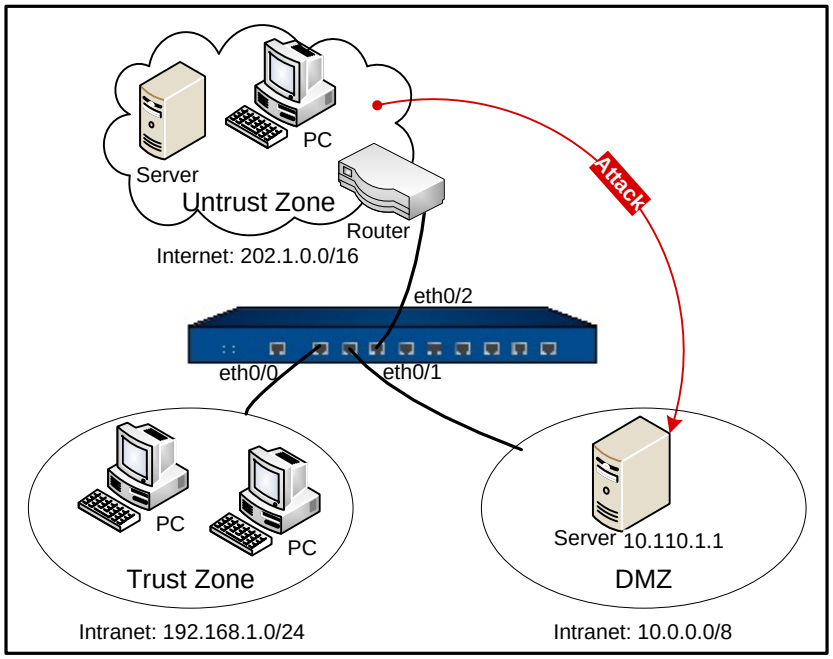
Example of Configuring SYN Flood Attack Defense

This section describes a SYN Flood attack defense configuration example.

Requirement

Hillstone 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.

Figure 2: Attack Defence Network Topology



Configuration Steps

Step 1: Configure ethernet0/0:

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

Step 2: Configure ethernet0/2:

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ip address 202.1.0.1/24
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Step 3: Configure ethernet0/1:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone dmz
hostname(config-if-eth0/1)# ip address 10.0.0.1/8
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 4: Configure a policy rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
```

```
hostname(config-policy-rule)# dst-zone dmz
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 5: Enable SYN Flood attack defense for the untrust zone:

```
hostname(config)# zone untrust
hostname(config-zone)# ad syn-flood
hostname(config-if)# exit
hostname(config)#
```

Step 6: Test the SYN Flood attack defense configured for the server. Send over 1500 packets per second to 10.110.1.1. The Hillstone device will detect a SYN Flood attack, and then give an alarm and drop the packets.

Example of Configuring IP Address Sweep Attack Defense

This section describes an IP address sweep attack defense configuration example.

Requirement

Hillstone 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 Hillstone device will detect an IP address sweep attack, and then give an alarm and drop the packets.

Anti-Virus

Overview

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 StoneOS, Hillstone devices can detect various threats including worms, Trojans, malware, malicious websites, etc., and proceed with the configured actions.

Anti Virus function can detect the common file types and protocol types which are most likely to carry the virus and protect. Hillstone 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 funtion will detect files and protocols based on IPv6. How to enable IPv6, see StoneOS_CLI_User_Guide_IPv6.

Configuring Anti-Virus

To enable the anti-virus function on StoneOS, 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 StoneOS 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).

WebUI: On the Navigation pane, click **Configure** > **Security** > **Anti-Virus** to visit the Anti-Virus page.

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

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

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

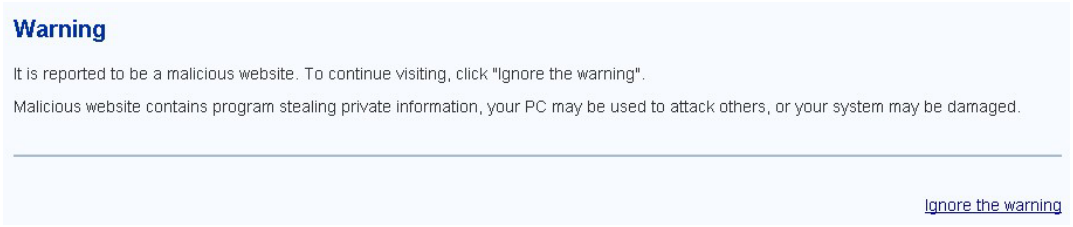
Specifying Malicious Website Detection Action

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**} –pecifies 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.

    Figure 3: Malicious Website Warning Page

    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.

Figure 4: Virus Warning Page

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.

Figure 5: Malicious Website Download Warning 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.

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, StoneOS 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 }
```

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 in **Table 5**; otherwise information related to the virus will be displayed in the Email, including the filename, path, result and action, as shown in **Table 6**.

Table 5: Scan Result - No Virus Found

Body
No virus found. Checked by Hillstone AntiVirus

Table 6: Scan Result - Virus Found

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 Hillstone 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 Hillstone AntiVirus". To

configure an Email signature, in the AV profile configuration mode, use the following command:

mail-sig *signature-string*

- *signature-string* - Configures the signature of the labeled Email.

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

no mail-sig

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
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.

For more information about SSL proxy, see the SSL Proxy chapter in **StoneOS_CLI_User_Guide_Network_Behavior_Control**.

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 StoneOS 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
```

Updating AV Signature Database

By default StoneOS updates the AV signature database everyday automatically. You can change the update configuration as needed. The configurations of updating AV signature database include:

- Configuring an AV signature update mode
- Configuring an update 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

StoneOS 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

StoneOS provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers to download the latest AV signatures as needed. To configure the update the server, in the global configuration mode, use the following command:

av signature update {server1 | server2 | server3} {*ip-address* | *domain-name*}

- **server1** | **server2** | **server3** - Specifies the update server you want to configure. The default value of **server1** is update1.hillstonenet.com, and the default value of **server2** is update2.hillstonenet.com.
- *ip-address* | *domain-name* - Specifies the name of the update server. It can be an *ip-address*, or a *domain-name*, for example, update1.hillstonenet.com.

To cancel the specified update the server, in the global configuration mode, use the following command:

no 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}** command.

Specifying an Update Schedule

By default, StoneOS 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, StoneOS 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
```

Configuration Example

Before enabling anti-virus, make sure your Hillstone device has already been installed with a corresponding anti-virus license.

This section describes an anti-virus configuration example. Hillstone devices with this example configured can:

- Scan Emails and its attachments, and display the anti-virus result in the Emails. The Emails are transferred over SMTP and POP3, and the attachments may contain .exe and .jpeg files.
- Scan compressed files. RAR-compressed files contain .jpeg files, and all the compressed files are transferred over FTP.

Configuration Steps

Step 1: Configure the AV profile, and specify the protocol types and file types:

```
hostname(config)# av-profile Email-scan
hostname(config-av-profile)# protocol-type smtp action fill-magic
hostname(config-av-profile)# protocol-type pop3 action fill-magic
hostname(config-av-profile)# protocol-type ftp action fill-magic
hostname(config-av-profile)# file-type pe
hostname(config-av-profile)# file-type jpeg
hostname(config-av-profile)# file-type mail
hostname(config-av-profile)# label-mail
hostname(config-av-profile)# mail-sig "Checked by Mail AntiVirus"
hostname(config-av-profile)# exit
hostname(config)#
```

Step 2: Create a policy rule, and reference the AV Profile to the rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
```

```
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# av Email-scan
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 3: View the anti-virus status by command **show version**. If the function is disabled, use following command to enable it and reboot the system to make it take effect:

```
hostname(config)# exec av enable
```

Sandbox

Overview

A sandbox executes a suspicious file in a virtual environment, collects the actions of this file, analyzes the collected data, and verifies the legality of the file.

The Sandbox function of the system uses the cloud sandbox technology. The suspicious file will be uploaded to the cloud side and the cloud sandbox will collect the actions of this file, analyze the collected data, verify the legality of the file, and give the analyze result to the system.

The Sandbox function contains the following parts:

- Collect and upload the suspicious file: The Sandbox function parses the traffic, extracts the suspicious file from the traffic.

  If there is no analyze result about this file in the local database, system will upload this file to the cloud intelligence server, and the cloud server intelligence will upload the suspicious file to the cloud sandbox for analysis.If this file has been identified as an illegal file in the local database of the Sandbox function, the system will generate corresponding threat logs and cloudsandbox logs. Additionally, you can specify the criteria of the suspicious files by configuring a sandbox profile.

- Check the analyze result returned from the cloud sandbox and take actions: The Sandbox function checks the analyze result of the suspicious file returned from the cloud sandbox, verifies the legality of the file, saves the result to the local database. If this suspicious is identified as an illegal file, the system will generate threat logs and cloudsandbox logs. This part is completed by the Sandbox function automatically.

- Maintain the local database of the Sandbox function: Record the information of the uploaded files, including uploaded time, analyze result. This part is completed by the Sandbox function automatically.

The Sandbox function is controlled by license. To use the Sandbox function, install the Cloud sandbox license.

Preparation for Configuring Sandbox

Before enabling the Sandbox function, make the following preparations:

- Make sure your system version supports the Sandbox function.The current device is connected to the Cloud Intelligence platform.

- Import the Cloud sandbox license and reboot. The Sandbox function will be enabled after the rebooting.

Except M8860/M8260/M7860/M7360/M7260, if the Sandbox function is enabled, the max amount of concurrent sessions will decrease by half.

To view the status of the Sandbox function, use the command **show version**. To enable or disable the Sandbox function, in any mode, use the following command:

exec sandbox {**enable** | **disable**}

- **enable** - Enables the Sandbox function.
- **disable** - Disables the Sandbox function.

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 Sandbox 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).

Configuring Sandbox

The system supports the policy-based Sandbox. To realize the policy-based Sandbox:

1. Enable Sandbox function.
2. Define a sandbox profile, and configure white list settings and file filter settings.
3. Bind the sandbox profile to an appropriate policy rule.

A sandbox profile contains the files types that device scaned, the protocols types that device scaned, and the white list settings.

- **File Type**: Support to detect PE, APK, JAR, MS-Office, PDF, SWF, RAR and ZIP file.
- **Protocol Type**: Support to detect HTTP, FTP, POP3, SMTP and IMAP4 protocol.
- **White list**: A white list includes domain names that are safe. When a file extracted from the traffic is from a domain name in the white list, this file will not be marked as a suspicious file and it will not be upload to the cloud sandbox.

There are three built-in sandbox rules with the files and protocols type configured, white list enabled and file filter configured. The three default sandbox rules includes predef_low, predef_middle and predef_high.

- **predef_low**: A loose sandbox detection rule, whose file type is PE and protocol types are HTTP/FTP/POP3/SMTP/IMAP4, with white list and file filter enabled.
- **predef_middle**: A middle-level sandbox detection rule, whose file types are PE/APK/JAR/MS-Office/PDF and protocol types are HTTP/FTP/POP3/SMTP/IMAP4, with white list and file filter enabled.

- **predef_high**: A strict sandbox detection rule, whose file types are PE/APK/JAR/MS-Office/PDF/SWF/RAR/ZIP and protocol types are HTTP/FTP/POP3/SMTP/IMAP4, with white list and file filter enabled.

Creating a Sandbox Profile

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

sandbox-profile *sandbox-profile-name*

- *sandbox-profile-name* - Specifies the sandbox profile name and enters the sandbox profile configuration mode. If the specified name exists, then the system will directly enter the sandbox profile configuration mode.

To delete the specified sandbox profile, in the global configuration mode, use the command **no sandbox-profile** *sandbox-profile-name*.

Enabling White List

The white list includes domain names that are safe. When a file extracted from the HTTP traffic is from a domain name in the white list, this file will not be marked as a suspicious file and it will not be upload to the cloud sandbox. To enable the white list function, in the sandbox profile configuration mode, use the following command:

whitelist enable

To disable this function, use **whitelist disable**.

Configuring Certificate Verification

System supports to enable the verification for the trusted certification. After enabling, system will not detect the PE file whose certification is trusted.

To enable the certificate verification, in the sandbox profile configuration mode, use the following command:

certificate-validation enable

To disable this function, use **no certificate-validation enable**.

Configuring File Filter

The file filter marks the file as a suspicious file if it satisfies the criteria configured in the file filter settings. The analyze result from the cloud sandbox determines whether this suspicious file is legal or not.

You can set the following criteria:

Mark the file of the specified file type as a suspicious file. The system can mark the PE, APK, JAR, MS-Office, PDF, SWF, RAR and ZIP file as a suspicious file now. Use the following command in the sandbox profile to specify the file type:

file-type {pe | apk | jar | swf | ms-office | pdf | rar | zip} max-file-size *size*

- **pe** – Mark the PE file as a suspicious file.
- **apk** – Mark the APK file as a suspicious file.
- **jar** – Mark the JAR file as a suspicious file.
- **swf** – Mark the SWF file as a suspicious file.
- **ms-office** – Mark the MS-Office file as a suspicious file.
- **pdf** – Mark the PDF file as a suspicious file.
- **rar** – Mark the RAR file as a suspicious file.
- **zip** – Mark the ZIP file as a suspicious file.
- **size** – Specify the file size. The range varies from 1 to 6. The unit is MB. Mark the file that is small than the specified file size as a suspicious file.

To cancel the file type setting, use **no file-type {pe | apk | jar | swf | ms-office | pdf | rar | zip}**. If no file type is specified, the Sandbox function will mark no file as a suspicious one.

Specifies the protocol to scan and directions of the detection. The system can scan the HTTP, FTP, POP3, SMTP and IMAP4 traffic now. Use the following command in the sandbox profile to specify the protocol:

protocol {http | ftp | imap4 | pop3 | smtp} direction {download | upload | both}

- **http | ftp | imap4 | pop3 | smtp** - Specifies the protocol to scan.
- **download | upload | both** - Specifies the direction of the detection. Upload means direction from client to server.Download means direction from server to client.

If no protocol is specified, the Sandbox function will not scan the network traffic.

In the sandbox profile, use **no protocol {http | ftp | imap4 | pop3 | smtp}** to delete the protocol specifications.

Specifying Actions for a Sandbox Profile

When system identifies the suspicious files as malicious files, it will deal with them with set actions. To specify the actions, in the Sandbox Profile configuration mode, use the following command:

action {**reset** | **log-only**}

- **reset** – Specifies the actions as reseting connections. After detecting the malicious files, system will reset connection of malicious link and record threat logs and cloud sandbox logs.

- **log-only** – Specifies the actions as recording logs. After detecting the malicious files, system will release traffic and record logs (threat logs and cloud sandbox logs) only.

Binding a Sandbox Profile to a Policy Rule

If the sandbox profile is bound to a policy rule, the system will detect the traffic matched to the specified policy rule based on the profile configuration. To bind the sandbox profile to a policy rule, in the policy rule configuration mode, use the following command:

sandbox {*sandbox-profile-name* | **predef_low** | **predef_middle** | **predef_high**}

- *sandbox-profile-name* - Specifies the name of the sandbox profile that will be bound to the policy rule.
- **predef_low** | **predef_middle** | **predef_high** - Bind the predef_low/ predef_middle/predef_high sandbox profile.

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

no sandbox

Enabling Benign File

If you enable the Benign File function, system will record cloudsandbox logs of the file when it marks it as a benign file. By default, system will not record logs for the benign files.

To enable the Benign File function, in the global configuration mode, use the following command:

sandbox benign-file report enable

In the global configuration mode, use **no sandbox benign-file report enable** command to disable the Benign File function.

the Greyware File function

If you enable Greyware File function, system will record cloudsandbox logs of the file when it marks it as a greyware file. A greyware file is the one system cannot judge it is a benign file or a malicious file. By default, system will not record logs for the greyware files.

To enable the Greyware File function, in the global configuration mode, use the following command:

sandbox greyware report enable

In the global configuration mode, use **no sandbox greyware report enable** command to disable the Greyware File function.

Adding Items to the Trust List

The local sandbox finds suspicious files and reports to cloud. After verifying the file is malicious, the cloud will send the synchronous threat information to other devices, which has connected to the cloud and enabled Sandbox function. After the device receiving the synchronous threat information and matching the threat, the threat item will be listed in the threat list and system will block it with the set actions.

You can add the sandbox threat items to the trust list. Once the item in the trust list is matched, the corresponding traffic will be released and not controlled by the actions of sandbox rule

To add or remove a sandbox threat item, in any mode, use the following command:

exec sandbox-threat *value* **{trust | untrust}**

- *value* – Specifies the name of the sandbox threat item.
- **trust** – Add the sandbox threat item to the trust list.
- **untrust** – Remove the sandbox threat item from the trust list.

Viewing Sandbox Information

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

show sandbox-profile [*sandbox-profile-name***]**

To view the sandbox status and statistic information, in any mode, use the following command:

show sandbox status

To view the sandbox threat items in the treat list, in any mode, use the following command:

show sandbox threat-entry info

Updating Sandbox Whitelist Database

By default StoneOS updates the sandbox whitelist database everyday automatically. You can change the update configuration as needed. The configurations of updating sandbox whitelist database include:

- Configuring a sandbox whitelist update mode
- Configuring an update server
- Specifying a HTTP proxy server
- Specifying an update schedule
- Updating now
- Importing a sandbox whitelist file

- Viewing sandbox whitelist information
- Viewing sandbox whitelist update information

Configuring a Sandbox Whitelist Update Mode

StoneOS supports both manual and automatic update modes. To configure a sandbox whitelist update mode, in the global configuration mode, use the following command:

sandbox whitelist update mode {auto | manual}

- **auto** - Specifies the automatic sandbox whitelist update mode. This is the default mode.
- **manual** - Specifies the manual sandbox whitelist update mode.

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

no sandbox whitelist update mode

Configure an Update Server

StoneOS provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers to download the latest sandbox whitelist as needed. To configure the update the server, in the global configuration mode, use the following command:

sandbox whitelist update {server1 | server2 | server3} {*ip-address* | *domain-name*}

- **server1** | **server2** | **server3** - Specifies the update server you want to configure. The default value of **server1** is update1.hillstonenet.com, and the default value of **server2** is update2.hillstonenet.com.
- *ip-address* | *domain-name* - Specifies the name of the update server. It can be an *ip-address*, or a *domain-name*, for example, update1.hillstonenet.com.

To cancel the specified update the server, in the global configuration mode, use the following command:

no sandbox whitelist update {**server1** | **server2** | **server3**}

Specifying a HTTP Proxy Server

When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update automatically and normally.

To specify the HTTP proxy server for the sandbox whitelist signature database updating, use the following command in the global configuration mode:

sandbox whitelist update proxy-server {main | backup} *ip-address port-number*

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

To cancel the proxy server configurations, use the **no sandbox whitelist update proxy-server {main | backup}** command.

Specifying an Update Schedule

By default, StoneOS automatically updates the sandbox whitelist database every day. To reduce the update server's workload, the time of daily update is random. To specify the schedule and specific time for the update, in the global configuration mode, use the following command:

sandbox whitelist update schedule {daily | weekly {mon | tue | wed | thu | fri | sat | sun}} [*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 sandbox whitelist database immediately as needed. To update the sandbox whitelist database now, in any mode, use the following command:

exec sandbox whitelist update

- **exec sandbox whitelist update** - Only updates the incremental part between the current sandbox whitelist database and the latest sandbox whitelist database released by the update server.

Importing a Sandbox Whitelist File

In some cases, your device may be unable to connect to the update server to update the sandbox whitelist database. To solve this problem, StoneOS provides the sandbox whitelist file import function, i.e., importing the sandbox whitelist files to the device from an FTP, TFTP server or USB disk, so that the device can update the sandbox whitelist database locally. To import the sandbox whitelist file, in the execution mode, use the following command:

import sandbox whitelist from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *ip-address* - Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* **password** *password* - Specifies the username and password of the FTP server.
- **vrouter** *vr-name* –Specifies the VRouter of the FTP or TFTP server.
- ***file****-name* - Specifies the name of the sandbox whitelist file that be imported.

Viewing Sandbox Whitelist Information

You can view the sandbox whitelist database information of the device as needed, including the sandbox whitelist database version, and release dates. To view sandbox whitelist database information, in any mode, use the following command:

show sandbox whitelist info

Viewing Sandbox Whitelist Update Information

You can view the sandbox whitelist update information of the device as needed, including the update server information, update mode, update frequency and time, as well as the status of the sandbox whitelist database update. To view the sandbox whitelist update information, in any mode, use the following command:

show sandbox whitelist update

IPS

Overview

IPS (Intrusion Prevention System) is designed to monitor various network attacks in real time and take appropriate actions (like block) against the attacks according to your configuration. StoneOS supports license-controlled IPS, i.e., the IPS function will not work unless an IPS license or TP license has been installed on a StoneOS that supports IPS.

The IPS on StoneOS can implement a complete state-based detection which significantly reduces the false positive rate. Even if the device is enabled with multiple application layer detections, enabling IPS will not cause any noticeable performance degradation. Besides, StoneOS will update the signature database automatically everyday to assure its integrity and accuracy.

IPS Detection and Submission Procedure

The protocol detection procedure of IPS consists of two stages: protocol parsing and signature matching.

- Protocol parsing: IPS analyzes the protocol part of the traffic. If the analyze results shows the protocol part contains abnormal contents, the system will process the traffic according to the action configuration. And it can generate logs for the administrator if any anomaly has been detected. Each Threat log contains "Threat ID", the signature ID in the signature database. You can view detailed information in Threat log details.
- Signature matching: IPS abstracts the interested protocol elements of the traffic for signature matching. If the elements are matched to the items in the signature database, the system will process the traffic according to the action configuration and it can generate logs for the administrator. Each Threat log contains "Threat ID", the signature ID in the signature database. You can view detailed information about the error according to the ID.

Signatures

The IPS signatures are categorized by protocols, and identified by a unique signature ID. The signature ID consists of two parts: protocol ID (1st bit or 1st and 2nd bit) and attacking signature ID (the last 5 bits). For example, in ID 605001, "6" identifies a Telnet protocol, and "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:

Table 7: ID-protocol mappings

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	My SQL	21	LDAP
4	POP3	10	Finger	16	MSSQL	22	VoIP
5	SMTP	11	SUNRPC	17	Oracle	-	-
6	Telnet	12	NNTP	18	MSRPC	-	-

In the above table, other-TCP identifies all the TCP protocols other than the standard TCP protocols listed in the table, and other-UDP identifies all the UDP protocols other than the standard UDP protocols listed in the table.

Updating IPS Signature Database

By default StoneOS updates the IPS signature database everyday automatically. You can change the update configuration as needed. Hillstone devices provide two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. StoneOS supports auto update and local update. Non-root VSYS does not support this feature. For more information about the signature database configurations, please refer to the table below.

Table 8: Signature Database Configurations

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* ♦ *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*] | **usb0** | **usb1**} *file-name*
To view signature statistics	**show ips signature info**
To view signature database configurations	**show ips signature update**

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 **no ips signature update proxy-server {main | backup}** command.

IPS Working Modes

StoneOS supports two IPS working modes: log only mode and IPS mode. In log only mode, StoneOS only generates protocol anomaly alarms and attacking behavior logs, but will not block attackers or reset connections; while in IPS mode, StoneOS not only generates protocol anomaly alarms and attacking behavior logs, but also blocks attackers or resets connections. By default, StoneOS works in IPS mode.

To switch to the IPS mode, in the global configuration mode, use the command **ips mode** {**ips-logonly** | **ips**}.

Configuring IPS

Before enabling IPS, make the following preparations:

1. Make sure your StoneOS version supports IPS.
2. Import an IPS license or TP license and reboot. The IPS will be enabled after the rebooting.

The configuration of IPS includes the following contents:

- Signature set configurations: IPS abstracts the interested protocol elements of the traffic for signature matching. If the elements are matched to the items in the signature database, the system will process the traffic according to the action configuration.
- Protocol configurations: IPS abstracts the interested protocol elements of the traffic for signature matching. If the elements are matched to the items in the signature database, the system will process the traffic according to the action configuration.
- IPS profile: contains signature set configurations, protocol configurations, and packet capture configurations. You can bind an IPS profile to different directions of the security zone (inbound, outbound, bi-direction) to apply the IPS function to the specified direction, or bind an IPS profile to a policy rule to apply the IPS function to the traffic that matches the specified policy rule.

If a policy rule is bound with an IPS profile and the source and destination security zone are also bound with an IPS Profile, the priority of the IPS detection will be: IPS profile for the policy rule > IPS profile for the destination zone > IPS profile for the source zone.

With IPS configured, StoneOS will generate an Threat log if any intrusion has been detected. Each Threat log contains a signature ID. You can view detailed information about the signature according to the ID in IPS online help pages. To view Threat logs, use the command **`show logging ips`**.

Configuration Suggestions

All the IPS rules configured for different attacks and intrusions will eventually affect the final actions. When determining the final action, the system will follow the principles below:

- The IPS working mode has the highest priority. When the working mode is set to log only, no matter what action is specified in other related configurations, the final action will always be log only.
- If you create several signature sets and some of them contain a particular signature. If the actions of these signature sets are different and the attack matches this particular signature , the system will adopt the following rules:
    - Always perform the stricter action on the attack. The signature set with stricter action will be matched. The strict level is: Block IP > Block

Service > Rest > Log Only. 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.

For more information about SSL proxy, see the SSL Proxy chapter in **StoneOS_CLI_User_Guide_Network_Behavior_Control**.

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
```

cc-url

Configure the URL path for the CC URL constraint. After the configuration, the system will make statistics on the frequency of the HTTP requests that access the path. If the frequency exceeds the threshold, the system will block the source IP of the request and the IP will not be able to access the Web server. Use the **no** form to delete the url configuration.

Command:

cc-url *url_string*

no cc-url *url_string*

Description:

url_string	Specifies the URL path of CC URL constraint. System will check the frequency of the HTTP requests that access the specified paths, includingthe whole or part of the paths. For example, if the configuration is /home/ab, system will check and calculate the HTTP requests like /home/ab/login and /home/abc/login. If the frequency of requests exceeds the threshold, system will block the source IP of the request and deny its access to the web server. URL path does not support the path format which contains the host name or domain name, for example: the configuration should be / home / login.html, instead of www.baidu.com/home/login.html, while www.baidu.com should be configured in the domain name settings of the Web server. System allows up to 32 URL paths configuration. The length range of each path is 1 to 255 characters.

Default values:

None

Mode:

Web server configuration mode

Guidance:

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
```

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
```

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 *A.B.C.D* [**vrouter** *vr-name*] **timeout** *timeout*

Description:

ip *A.B.C.D*	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:

The default value of the **vr-name** parameter is **trust-vr**.

Mode:

execution mode

Guidance:

Non-root VSYS does not support this command.

Example:

```
hostname# exec block-ip add ip 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** | **ip** *ip-address* [**vrouter** *vr-name*]}

Description:

all	Deletes all blocked IP addresses.
ip *ip-address*	Deletes the specified blocked IP address.
vr-name	Specifies the VR where the IP address locates.

Default values:

The default value of the **vr-name** parameter is **trust-vr**.

Mode:

execution mode

Guidance:

Non-root VSYS does not support this command.

Example:

```
hostname# exec block-ip remove ip 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-ip *src-ip-address* **dst-ip** *dst-ip-address* [**vrouter** *vr-name*] **dst-port** *port-number* **proto** *protocol*

Description:

src-ip *src-ip-address* **dst-ip** *dst-ip-address* [**vrouter** *vr-name*] **dst-port** *port-number* **proto** *protocol*	Add a specified service that will be able to be blocked. • **src-ip** *src-ip-address* – Specifies the source IP address of the service. • **dst-ip** *dst-ip-address* – Specifies the destination IP 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 to65535. • **proto** *protocol* – Specifies the protocol of the service. The value ranges from 1 to 255.

Default values:

The default value of the **vr-name** parameter is **trust-vr**.

Mode:

execution mode

Guidance:

Non-root VSYS does not support this command.

Example:

```
hostname# exec block-service add src-ip 100.10.10.1 dst-ip
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-ip** *src-ip-address* **dst-ip** *dst-ip-address* [**vrouter** *vr-name*] **dst-port** *port-number* **proto** *protocol*}

Description:

all	Deletes all blocked services.
src-ip *src-ip-address* **dst-ip** *dst-ip-address* [**vrouter** *vr-name*] **dst-port** *port-number* **proto** *protocol*	Deletes the specified blocked service item. • **src-ip** *src-ip-address* – Specifies the source IP address of the service. • **dst-ip** *dst-ip-address* – Specifies the destination IP 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 to65535. • **proto** *protocol* – Specifies the protocol of the service. The value ranges from 1 to 255.

Default values:

The default value of the **vr-name** parameter is **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
```

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 *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 disable

Disable the IPS function. Use the **no** form to enable the IPS function.

Command:

```
ips log disable
no ips log disable
```

Description:

None

Default values:

Enable

Mode:

security zone configuration mode

Guidance:

Since the IPS function occupies memory, you can disable the IPS logs under the circumstances so that the system can work normally.

Example:

```
hostname(config)# ips log disable
```

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 *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 white-list

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-pop3-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* |	**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** -

log-only | reset}	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 – 512 byte

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-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 byte

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.
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.
**pcap {disable	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 FTP
```

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 tht exception URL for Web server. The length of URL is in the range of 1-255 characters.

Default values:

None

Mode:

Web server configuration mode

Guidance:

You can configure up to 32 URL paths.

Example:

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# 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:

log | reset	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-http-sigset)# search-class 1 name test2
```

search-condition

When using a search condtion to search signatures, you can specify the information of the signature. The system will perform the fuzzy searching among the following fields: signature ID, signature name, CVE-ID, and signature description:

Command:

search-condition *description*

no search-condition *description*

Description:

description	Enter the information of the desired signatures.

Default values:

None

Mode:

Search rule configuration mode.

Guidance:

None

Example:

```
hostname(config)# ips profile test
hostname(config-ips-profile)# search-class 1
hostname(config-ips-filter-class)# search-condition DNS
```

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 *number*

no signature id *number*

Description:

id	Enter the signature ID.

Default values:

None

Mode:

search rule configuration mode

Guidance:

None

Example:

```
hostname(config)# ips profile test
hostname(config-ips-profile)# search-class 1
hostname(config-ips-filter-class)# signature id 105001
```

signature-id

Configure the signature ID for the IPS white list. Use the **no** form to delete the signature ID.

Command:

signature-id *id*

no signature-id *id*

Description:

id	Specifies the signature ID for the IPS white list to match.

Default values:

None

Mode:

IPS white list configuration mode

Guidance:

None

Example:

```
hostname(config)# ips whitelist white1
hostname(config-ips-whitelist)# signature-id 105002
```

sigset

Add the protocol configurations to the IPS Profile. Use the **no** form to delete the protocol congurations from the IPS Profile.

Command:

sigset *user-defined-profile*

no sigset *user-defined-profile*

Description:

user-defined-profile	Adds the user-defined signature set to the IPS Profile.

Default values:

None

Mode:

IPS Profile configuration mode

Guidance:

None

Example:

```
hostname(config)# ips profile ips-profile1
hostname(config-profile)# sigset test
```

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 web_server1
hostname(config-web-server)# sql-injection cookie disable
```

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

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

Abnormal Behavior Detection

Overview

There are various threat attacks in networks, such as Web server attacks ,DoS attacks, application layer attacks , port/server scan attacks , amplification attacks, SSL attacks etc. These threats have demonstrated a wide variety of abnormal behavior. System provide abnormal behavior detection function based on security zones. This function inspects the sessions of the detected object in multiple factors. When one detected object has multiple abnormal parameters, the system will analyze the relationship among the abnormal parameters to see whether an abnormal behavior formed. If there is an abnormal behavior, the system will send the alarm message and generate the threat logs.

The followings are the concept description of the Abnormal Behavior Detection:

- Detected object: The object that is configured with the risk object function. Three types of detected object are supported: subnet , server and host.When the object type is configured with host, for each host which is identified host name, to establish a data model.
- Parameter: The basic statistical factor of a session, for example, the received bytes of inbound sessions per second. The statistical values of the parameters are used by the system to judge whether the detected object is abnormal or not.
- Baseline: The baseline is the benchmark for the parameters. Value of the baseline is calculated by the system according to the historical data.
- Abnormal behavior model database: The abnormal behavior model database includes the abnormal information of the traffic, which are detecting rules, description of the abnormalities, the reason for the abnormalities, and the suggestions. The information in the database helps you analyze and resolve the abnormal problems. By default, System will update the database at the certain time everyday, and you can modify the update the updating settings according to your own requirements. For more information about how to update, see Updating Abnormal Behavior Model Database. To assure a proper connection to the default update server, you need to configure a DNS server for StoneOS before updating.

Configuring Abnormal Behavior Detection

To enable the abnormal behavior detection function on StoneOS, take the following steps:

1. Make sure your StoneOS version supports abnormal behavior detection.
2. Import a StoneShield license and reboot. The abnormal behavior detection will be enabled after the rebooting.

Enabling/Disabling Abnormal Behavior Detection

To enable the zone-based abnormal behavior detection function, in the zone configuration mode, use the following command. By default, the abnormal behavior detection function will detect the entire network covered by this security zone.

anomaly-detection [host-enable [advanced-protection] [ddos-protection]] | [forensic]

- **host-enable** – Enable the Host Defender function for the specific zone, for each host which is identified host name, establish a data model for each host which is identified host name, analyze the network behavior of host, and define the corresponding signature dimension for different network behavior, and then detect the abnormal behavior of the host based on the signature dimension, to find the more hidden threat attack. When enabling the Host Defender function, both the DDoS protection function and the abnormal behavior detection of the HTTP factor are not enabled by default. To enable the abnormal behavior detection of the HTTP factor, use the **advanced-protection** parameter. To enable the DDoS protection, use the **ddos-protection** parameter.
- **forensic** – Capture packets. If this parameter is specified, the system will save the evidence messages.

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

no anomaly-detection [host-enable [advanced-protection] [ddos-protection]] | [forensic]

Configuring Detected Object

The configuration of detected object includes:

- Creating a detected object
- Modifying/deleting the descriptions of a detected object
- Configuring the zone of detected object
- Configuring the IP address of detected object
- Specifying an Exclude Schedule
- Re-establishing the Object Data Model
- Renaming a detected object
- Enabling/Disabling Web Server Advanced Protection

Creating a Detected Object

To configure a detected object, in the global configuration mode, use the following command:

anomaly-detection object name *object-name* **type** {**subnet | server** }

- *object-name* –Specify the name of the detected object and enters the detected object configuration mode.. If the specified name exists, then the system will directly enter the detected object configuration mode.
- **type** {**subnet | server** } – Specify the type of the detected object.
  - **subnet** – Specify the type of the detected object is subnet.
  - **server** –Specify the type of the detected object is server.

To delete the deceted object, in the global configuration mode, use the following command:

no anomaly-detection object name *object-name*

Modifying/Deleting the Descriptions of a Detected Object

In the detected object configuration mode, use the following command to modify the description of a detected object.

description *description*

- *description* –Specify the description for the detected object if necessary.

In the detected object configuration mode, use the following command to delete the description of a detected object.

no description

Configuring the Zone of Detected Object

In the detected object configuration mode, use the following command to specify the zone of detected object.

zone *zone*

- *zone* – Specify the zone of detected object.

In the detected object configuration mode, use the following command to delete the specified zone.

no zone

Configuring the IP address of Detected Object

To specify the IP address/netmask of the subnet, and specify the IP address of the server, in the detected object configuration mode, use the following command:

ip {*A.B.C.D* | *A.B.C.D/M*}

In the detected object configuration mode, use the following command to delete the IP of the detected objec.

no ip

Specifying an Exclude Schedule

Specify a schedule for the detected object. The anomalies occurring in the schedule will be ignored by the system. In the detected object configuration mode, use the following command:

schedule *schedule-name*

- *schedule-name* – Specify the name of schedule. For more information about how to configure a schedule, see "Configuring Schedule" of "System Management".

To delete the exclude schedule , In the detected object configuration mode, use the following command:

no schedule *schedule-name*

Re-establishing the Object Data Model

If you want to re-establish the object data model, in the detected object configuration mode, use the following command:

reset

Renaming a Detected Object

To rename a detected object, in the detected object configuration mode, use the following command:

rename *new-name*

- *new-name* – Specifies the new name for the detected object.

Enabling/Disabling Web Server Advanced Protection

Web Server Advanced Protection function to detect HTTP protocol type of Web server attacks, and find the abnormal behavior immediately and correctly. When the server type is selected, enable this function, can detect the following types of attacks and behavior:

- Web Vulnerability Scan: A web vulnerability scanner is a program which communicates with a web application through the web front-end in order to identify potential security vulnerabilities in the web application and architectural weaknesses.
- Http-based DoS Attack: Denial of service (DoS) usually refers to an attack that attempts to make a computer resource unavailable to its intended users by flooding a network or server with requests and data. As the name suggests, Http-Based DoS Attack is based on http protocol.
- Web Spider : A Web spider is an internet bot that systematically browses the World Wide Web, typically for the purpose of Web indexing. Web search engines and some other sites use web spider to update their web content or indexes of

others sites' web content. Web spider s can copy all the pages they visit for later processing by a search engine that indexes the downloaded pages so that users can search them much more quickly.

To enable the function, in the detected object configuration mode, use the following command:

```
mark-webserver
```

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

```
no mark-webserver
```

DNS Mapping

DNS as the domain name resolution protocol,is designed to resolve fixed domain names to IP addresses.Due to the use of domain name is convenient, and is widely used, so the attacker will take different means to use the domain name to generate attack. For example, A IP address can correspond to multiple domain name, the server according to the Host field of HTTP packet to find the Goal URL, the malware will use this feature by modifying the Host field to disguise the domain name, and generate the abnormal behavior. DGA, is the domain generation algorithm, this algorithm will generate a large number of pseudo random domain name, and will be used by malware. ISP DNS hijack, add some of the malicious domain name used by the malicious software to its blacklist.

To solve these problem, DNS domain name analysis can be used as an important basis to determine the malicious behavior. System will monitor the DNS response packets after the abnormal behavior detection function function is enabled, and establish the DNS mapping list, The DNS mapping list is used to store domain names and IP addresses, the pseudo random domain name generated by DGA algorithm, and the black and white domain name updated from the cloud. The device can detect the malware and abnormal behavior attack according the DNS mapping, and generate the threat logs.

Viewing the Entry of DNS Mapping

To view the number of domain name entries in DNS mapping, in any mode,use the following commands:

```
show dns-mapping
```

Viewing Detected Object Configuration Information

To view the detected object configuration information, in any mode,use the following commands:

```
show anomaly-detection object [name object-name]
```

Viewing Detection Status of Dos Attacks

To view the detection status of DOS attacks, in any mode,use the following commands:

show anomaly-detection ddos status

Updating Abnormal Behavior Model Database

By default StoneOS updates the abnormal behavior model database everyday automatically. You can change the update configuration as needed. The configurations of updating abnormal behavior model database include:

- Configuring an abnormal behavior model update mode
- Specifying an automatic update period
- Updating now
- Importing an abnormal behavior model file
- Viewing abnormal behavior model update information

Configuring an Abnormal Behavior Model Update Mode

StoneOS supports both manual and automatic (periodicity) update modes. To configure an abnormal behavior model update mode, in the global configuration mode, use the following command:

cloud abnormal-behavior-detection mode {**1** | **2**}

- **1** – **manual**, Specifies the manual update mode.
- **2** – **period**, Specifies the automatic (periodicity) update mode.

Specifying an Automatic Update Period

To specify an automatic update period, in the global configuration mode, use the following command:

cloud abnormal-behavior-detection period *period*

- *period* - Specifies the automatic update period, the range is 600 to 86400 seconds.

Updating Now

For both manual and automatic update modes, you can update the abnormal behavior model database immediately as needed. To update the abnormal behavior model database now, in any mode, use the following command:

exec cloud abnormal-behavior-detection update

- **exec cloud abnormal-behavior-detection update** –Only updates the incremental part between the current abnormal behavior model database and the latest abnormal behavior model database released by the update server.

Importing an Abnormal Behavior model File

In some cases, your device may be unable to connect to the update server to update the abnormal behavior model database. To solve this problem, StoneOS provides the abnormal behavior model file import function, i.e., importing the abnormal behavior model files to the device from an FTP, TFTP server or USB disk, so that the device can update the Abnormal Behavior model database locally. To import the abnormal behavior model file, in the execution mode, use the following command:

import cloud abnormal-behavior-detection from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *ip-address* –Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* **password** *password* –Specifies the username and password of the FTP server.
- **vrouter** *vr-name* –Specifies the username and password of the FTP server.
- *file-name* –Specifies the name of the abnormal behavior model file that be imported.

Viewing Abnormal Behavior Model Update Information

To view the abnormal behavior model update information, in any mode, use the following command:

show cloud abnormal-behavior-detection update

Advanced Threat Detection

Overview

Advanced Threat Detection , is on the basis of learning advanced threat detection signatures, to analysis the suspicious traffic of host, detect malicious behavior to identify APT (Advanced Persistent Threat) attack and generate the threat logs.

You need to update the malware behavior model database before enabling the function for the first time. For more information about how to update, see Updating Malware Behavior Model Database.

Configuring Advance Threat Detection

To enable the advance threat detection function on StoneOS, take the following steps:

1. Make sure your StoneOS version supports advance threat detection.
2. Import a StoneShield license and reboot. The advance threat detection will be enabled after the rebooting.

To configure the advance threat detection based on zone, in zone configuration mode, use the following command:

malware-detection [forensic]

- **malware-detection** –Enabling the advance threat detection for specific zone.
- **forensic** – Capture packets. If this parameter is specified , the system will save the evidence messages, and support to download it.

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

no malware-detection [forensic]

Updating Malware Behavior Model Database

By default StoneOS updates the malware behavior model database everyday automatically. You can change the update configuration as needed. The configurations of updating malware behavior model database include:

- Configuring a malware behavior model update mode
- Specifying a automatic update period
- Updating now
- Importing a malware behavior model file
- Viewing malware behavior model update information

Configuring a Malware Behavior Model Update Mode

StoneOS supports both manual and automatic (periodicity) update modes. To configure a malware behavior model update mode, in the global configuration mode, use the following command:

cloud advanced-threat-detection mode {**1** | **2**}

- **1** – **manual**, Specifies the manual update mode.
- **2** – **period**, Specifies the automatic (periodicity) update mode.

Specifying an Automatic Update Period

To specify an automatic update period, in the global configuration mode, use the following command:

cloud advanced-threat-detection period *period*

- *period* - Specifies the automatic update period, the range is 600 to 86400 seconds.

Updating Now

For both manual and automatic update modes, you can update the malware behavior model database immediately as needed. To update the malware behavior model database now, in any mode, use the following command:

exec cloud advanced-threat-detection update

- **exec cloud advanced-threat-detection update** –Only updates the incremental part between the current malware behavior model database and the latest malware behavior model database released by the update server.

Importing a Malware Behavior Model File

In some cases, your device may be unable to connect to the update server to update the malware behavior model database. To solve this problem, StoneOS provides the malware behavior model file import function, i.e., importing the malware behavior model files to the device from an FTP, TFTP server or USB disk, so that the device can update the malware behavior model database locally. To import the malware behavior model file, in the execution mode, use the following command:

import cloud advanced-threat-detection from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *ip-address* –Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* **password** *password* –Specifies the username and password of the FTP server.

- **vrouter** *vr-name* –Specifies the username and password of the FTP server.
- *file-name* –Specifies the name of the malware behavior model file that be imported.

Viewing Malware Behavior Model Update Information

To view the malware behavior model update information, in any mode, use the following command:

```
show advanced-threat-detection update
```

Perimeter Traffic Filtering

Overview

Perimeter Traffic Filtering can filter the perimeter traffic based on known IP of black/white list, and take block action on the malicious traffic that hits the blacklist.

Black/White list includes the following three types:

- Predefined black list: Retrieve the IP of black/white 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.
- Third-party black list: Make a linkage with trend of TDA, to get blacklist from the trend TDA devices regularly.

You need to update the IP reputation database before enabling the 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 StoneOS, take the following steps:

1. Make sure your StoneOS 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 Black/White List

For three types of black/white list (Predefined black list, User-defined black/white list and Third-party black 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:

- Predefined black list: **pre-define [drop | log-only]**
  - **drop** – Drop packets if the malicious traffic hits the predefined black list.
  - **log-only** – Only generates logs if the malicious traffic hits the predefined black 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.
- Third-party black list: **trend-micro [drop | log-only]**
  - **drop** – Drop packets if the malicious traffic hits the third-party black list.
  - **log-only** – Only generates logs if the malicious traffic hits the third-party black list.

To disable the perimeter traffic filtering based on different black/white list, in the perimeter traffic filtering configuration mode, use the following command:

- Predefined black list: **no pre-define**
- User-defined black/white list: **no user-define**
- Third-party black list: **no trend-micro**

Configuring User-defined Black/White List

To enter the black/white list configuration mode, in the global configuration mode, use the following command:

reputation

Add a IP entry to the user-defined black/white list, in black/white list configuration mode, use the following command:

iplist [id *id***] ip** *ip-address* **reputation-index {0 | 100}**

- **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.
- **reputation-index {0 | 100}** –Add the IP address to the blacklist or whitelist
  - **0** –Add the IP address to the blacklist。

- **100** –Add the IP address to the whitelist。

To delete the IP entry in the user-defined black/white list, in the black/white list configuration mode, use the following command:

no iplist id

Configuring Third-party Black List

Make a linkage with trend of TDA, to get blacklisted from the trend TDA devices regularly. The configurations of third-party black list include:

- Entering the third-party black list configuration mode
- Enabling/Disabling linkage with trend of TDA
- Configuring TDA device address
- Configuring the linkage request cycle
- Enabling/Disabling the linkage with sandbox

Entering the Third-Party Black List Configuration Mode

To Enter the third-party black list configuration mode, in the global configuration mode, use the following command:

third-party trendmicro

Enabling/Disabling Linkage with Trend of TDA

To enable/disable the linkage with trend of TDA, in the third-party black list configuration mode, use the following command:

global-blacklist {enable | disable}

- **enable** –Enable the linkage with trend of TDA.
- **disable** –Disable the linkage with trend of TDA.

Configuring TDA Device Address

To configure the TDA device address and port, in the third-party black list configuration mode, use the following command:

query-server ip *ip-address* [**port** *port-number*]

- *ip-address* –Specify the address for the TDA device.
- **port** *port-number* –Specify the port number for the TDA device. The value range is 1 to 65535.

To restore to the default value (ip: 0.0.0.0, port: 443), in the third-party black list configuration mode, use the following command:

no query-server

Configuring the Linkage Request Cycle

To configure the linkage request cycle, in the third-party black list configuration mode, use the following command:

query-cycle *cycle*

- *cycle* –Specify the Linkage request period for getting the blacklisted from the TDA devices. The value range is 1 to 60 minutes, the default value is 30 minutes.

To restore to the default value, in the third-party black list configuration mode, use the following command:

no query-cycle

Enabling/Disabling the Linkage with Sandbox

To enable/disable the linkage with sandbox for getting the blacklist of the TDA device sandbox. in the global configuration mode, use the following command:

sandbox-blacklist {enable | disable}

- **enable** –Enable the linkage with sandbox.
- **disable** –Disable the linkage with sandbox.

Viewing User-defined Black/White List Information

To view the User-defined black/white list information, in any mode, use the following command:

show reputation 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 reputation blacklist [third-party]

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 reputation ip *ip-address*

Viewing TDA Configuration Information

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

```
show third-party trendmicro configuration
```

Viewing the Information getting from TDA

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

```
show third-party trendmicro statistics
```

Updating IP Reputation Database

By default StoneOS updates the IP reputation database everyday automatically. You can change the update configuration as needed. The configurations of updating IP reputation database include:

- 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

StoneOS supports both manual and automatic update modes. To configure an IP reputation update mode, in the global configuration mode, use the following command:

```
perimeter-traffic-filter 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 perimeter-traffic-filter update mode
```

Configure an Update Server

StoneOS provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers to download the latest IP reputation as needed. To configure the update the server, in the global configuration mode, use the following command:

perimeter-traffic-filter 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.hillstonenet.com, and the default value of **server2** is update2.hillstonenet.com.
- *ip-address* | *domain-name* - Specifies the name of the update server. It can be an *ip-address*, or a *domain-name*, for example, update1.hillstonenet.com.

To cancel the specified update the server, in the global configuration mode, use the following command:

no perimeter-traffic-filter 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:

perimeter-traffic-filter 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, StoneOS 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:

perimeter-traffic-filter update schedule {daily | weekly {mon | tue | wed | thu | fri | sat | sun} | three-hours } [*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.
- **three-hours** – Updates the database every three hours. This option is the default update schedule.
- *HH:MM* - Specifies the time of update, for example, 09:00.

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 perimeter-traffic-filter update

- **exec perimeter-traffic-filter 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, StoneOS 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 perimeter-traffic-filter 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 perimeter-traffic-filter 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 perimeter-traffic-filter update
```

Mitigation

Overview

The system can identify the potential risks and network attacks dynamically, and take action on the risk that hits the mitigation rules.

Mitigation Rule

Tack auto mitigation action on the risk that hits the mitigation rules.

Mitigation rules includes the following two types:

- Predefined rule: this rule is retrieved from the Mitigation signature database. The predefined rules may vary by different mitigation signature databases. About updating the signature database, see Updating Mitigation Rule Database.
- User-defined rule: According to user needs, specify the trigger condition and action.

Notes:

- Mitigation rules only for the threat types of Scan，Dos and Spam.
- Predefined rule can not be edited or deleted.

The configurations of auto mitigation rule include:

- Enabling/Disabling auto mitigation
- Configuring the mitigation rule
- Viewing the status of auto mitigation

Enabling/Disabling Auto Mitigation

After enabling auto mitigation , mitigation rules (user-defined rule and predefined rule) to be able to take effect.

To enable/disable auto mitigation, in global command mode, use the following command:

`mitigation-status {enable | disable}`

- **`enable`** –Enable the auto mitigation.
- **`disable`** – Disable the auto mitigation.

Configuring the Mitigation Rule

Only supports to use WebUI to configuring the mitigation rule, see *StoneOS_WebUI_User_Guide.*

Viewing the Status of Auto Mitigation

To view the status of auto mitigation, in any mode, use the following command:

show mitigation-status

Updating Mitigation Rule Database

By default StoneOS updates the mitigation rule database everyday automatically. You can change the update configuration as needed. The configurations of updating malware behavior model database include:

- Configuring a mitigation rule update mode
- Specifying a automatic update period
- Updating now
- Importing a mitigation rule file
- Viewing mitigation rule update information

Configuring a Mitigation Rule Update Mode

StoneOS supports both manual and automatic (periodicity) update modes. To configure a mitigation rule update mode, in the global configuration mode, use the following command:

cloud mitigation mode {**1** | **2**}

- **1** – **manual**, Specifies the manual update mode.
- **2** – **period**, Specifies the automatic (periodicity) update mode.

Specifying an Automatic Update Period

To specify an automatic update period, in the global configuration mode, use the following command:

cloud mitigation period *period*

- *period* - Specifies the automatic update period, the range is 600 to 86400 seconds.

Updating Now

For both manual and automatic update modes, you can update the mitigation rule database immediately as needed. To update the mitigation rule database now, in any mode, use the following command:

exec cloud mitigation update

- **exec cloud mitigation update** –Only updates the incremental part between the current mitigation rule database and the latest mitigation rule database released by the update server.

Importing a Mitigation Rule File

In some cases, your device may be unable to connect to the update server to update the mitigation rule database. To solve this problem, StoneOS provides the malware behavior model file import function, i.e., importing the mitigation rule files to the device from an FTP, TFTP server or USB disk, so that the device can update the A mitigation rule database locally. To import the mitigation rule file, in the execution mode, use the following command:

import cloud mitigation from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *ip-address* –Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* **password** *password* –Specifies the username and password of the FTP server.
- **vrouter** *vr-name* –Specifies the username and password of the FTP server.
- *file-name* –Specifies the name of the mitigation rule file that be imported.

Viewing Mitigation Rule Update Information

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

show mitigation update

Critical Assets

Critical assets refer to IT assets owned by a company that are essential to its ability to operate and make profit. Those assets include key servers, networking devices, data storage server etc. Since critical assets are essential for business day-to-day operations, they are grown to targets of cyber-attacks. Therefore, the critical assets in a company need to be secured and protected with even stronger defense mechanisms comparing with other individual host machines.

After configuring critical asset object, the system will automatically enable the advanced threat detection and abnormal behavior detection functions in the select security zone, protect the priority and resource for critical asset monitoring, and display the related threat and traffic of the critical asset in the Critical Assets page in iCenter.

Configuring critical assets includes the following items:

- Specifying the name of the critical asset
- Specifying the IP address of the critical asset
- Speicifying the security zone of the critical asset
- View the critical asset configurations

Specifying Critical Asset Name

To specify the critical asset name, in the global configuration mode, use the following command:

critical-asset name *name*

- *name* – Specify the critical asset name and enter into the critical asset object configuration mode. If the name already exists, the system will enter into the critical asset object configuration mode directly.

To delete a critical asset, use the **no critical-asset name** *name* command.

Specifying Critial Asset IP Address

To specify the critical asset IP address, in the critical asset object configuration mode, use the following command:

ip *ip-address*

- *ip-address* – Specify the IP address of the critical asset.

To cancel the IP setting, use the **no ip** command.

Specifying Critial Asset Zone

To specify the security zone where the critical asset locates, in the critical asset object configuration mode, use the following command:

zone *zone-name*

- *zone-name* – Specify the security zone where the critical asset locates. The system will automatically enable the advanced threat detection and abnormal behavior detection functions of this security zone.

To cancel the security zone setting, use the **no zone** command.

Viewing Critical Asset Object Configurations

Use the **show critical-asset object** command to view the critical asset object configurations.

Correlation Analysis

System provides the correlation analysis engine and this engine makes the correlation analysis of the threat events generated by each modules of threat prevention. According to the defined correlation analysis rules, this engine analyzes the happened threat events, try to find the correlation of these threat events and the threats that crosss hosts, and discover the potential threats with high severity. You view the correlation analysis results in WebUI > iCenter > Threat.

Updating Correlation Analysis Engine/Rules

The updating of correlation analysis engine/rule is merged into the updating of abnormal behavior model database. For information of updating abnormal behavior model database, see the Updating Abnormal Behavior Model Database section.

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 StoneOS updates the geolocation information database everyday automatically. You can change the update configuration as needed. The configurations of updating geolocation information database include:

- Configuring a geolocation information database update mode
- Configuring an update 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

StoneOS 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

StoneOS provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers to download the latest geolocation informations as needed. To configure the update the server, in the global configuration mode, use the following command:

geolocation-IP-signature update {server1 | server2 | server3} {*ip-address* | *domain-name*}

- **server1** | **server2** | **server3** - Specifies the update server you want to configure. The default value of **server1** is update1.hillstonenet.com, and the default value of **server2** is update2.hillstonenet.com.
- *ip-address* | *domain-name* - Specifies the name of the update server. It can be an *ip-address*, or a *domain-name*, for example, update1.hillstonenet.com.

To cancel the specified update the server, in the global configuration mode, use the following command:

no geolocation-IP-signature update {**server1** | **server2** | **server3**}

Specifying a HTTP Proxy Server

When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update automatically and normally.

To specify the HTTP proxy server for the geolocation information database updating, use the following command in the global configuration mode:

geolocation-ip-signature update proxy-server {main | backup} *ip-address port-number*

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

To cancel the proxy server configurations, use the **no geolocation-ip-signature update proxy-server {main | backup}** command.

Specifying an Update Schedule

By default, StoneOS 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

- **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.

Importing a Geolocation Information Database File

In some cases, your device may be unable to connect to the update server to update the geolocation information database. To solve this problem, StoneOS provides the geolocation information database file import function, i.e., importing the geolocation information database files to the device from an FTP, TFTP server or USB disk, so that the device can update the geolocation information database locally. To import the geolocation information database file, in the execution mode, use the following command:

import geolocation-IP-signature from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *ip-address* - Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* **password** *password* - Specifies the username and password of the FTP server.
- **vrouter** *vr-name* –Specifies the VRouter of the FTP or TFTP server.
- ***file****-name* - Specifies the name of the geolocation information database file that be imported.

Viewing Geolocation Information Database Information

You can view the geolocation information database information of the device as needed, including the geolocation information database version, release dates, and the number of the geolocation informations. To view geolocation information database information, in any mode, use the following command:

```
show geolocation-IP-signature info
```

Viewing Geolocation Information Database Update Information

You can view the geolocation information database update information of the device as needed, including the update server information, update mode, update frequency and time, as well as the status of the geolocation information database update. To view the geolocation information database update information, in any mode, use the following command:

```
show geolocation-IP-signature update
```