Anti-Attack Configuration Commands

Table of Contents

Chapter 1 Anti-Attack Configuration Commands

1.1 Anti-Attack Configuration Commands

1.1.1 filter period

To configure the attack checkup period, run the following command.

filter period *time*

To configure the attack checkup period, run the following command. **no filter period**

Parameters

Parameters	Description
time	Stands for the attack-proof checkup period whose unit is second. If the number of packets transmitted by the attack source exceeds the designated number in the checkup period, the attack source is thought to trigger attacks. Value range: 1-600 second(s)

Default Value

The default time is 10 seconds.

Command Mode

Global configuration mode

Example

Switch_config# filter period 15

Related Command

filter threshold

1.1.2 filter threshold

To configure the threshold value which is exceeded before the system thinks an attack, run the following command. Vary your configuration in terms of the packet type.

To return to the default setting, use the no form of this command.

filter threshold *type value* **no filter threshold** *type*

Parameters

Parameters	Description
type	Packet type, including ARP, BPDU, DHCP, IGMP and ICMP.
value	Stands for the number of the packets received in an attack-proof checkup period before the system thinks it as an attack. Value range: 5-2000

Default Value

The default value is 1000 packets.

Command Mode

Global configuration mode

Example

Switch_config# filter threshold ip 1500

Related Command

filter period

1.1.3 filter block-time

To configure the time to block attack resource, use the filter block-time value command.

To return to the default setting, use the no form of this command.

filter block-time *value* **no filter block-time**

Parameters

Parameters	Description
value	Stands for the time of blocking the attack source after the attack is detected. Its unit is second. Value range: 1-86400

Default Value

The default value is 300 seconds.

Command Mode

Global configuration mode

Example

Switch_config# filter block-time 600

Related Command

filter period filter threshold

1.1.4 filter polling period

To configure the period of the attack source polling check in the hybrid mode, run the following command.

To return to the default setting, use the no form of this command.

filter polling period *time* **no filter polling period**

Parameters

Parameters	Description
time	The period of the polling attack after blocking the attack source. Unit: second Value range: 1-600

Default Value

The default time is 10 seconds.

Command Mode

Global configuration mode

Example

Switch_config# filter polling period 20

filter polling threshold filter polling auto-fit

1.1.5 filter polling threshold

To configure the filter polling threshold in the hybrid mode, run the following command. Vary your configuration in terms of the packet type. To return to the default setting, use the no form of this command. **filter polling thredhold** *type value* **no filter polling threshold** *type*

Parameters

Parameters	Description
type	Packet type, including ARP, BPDU, DHCP, IGMP and ICMP.
value	The attack source is taken as existed if 1-2000 packets are received within any polling period. Value range: 1-2000

Default Value

The default value is 750 packets.

Command Mode

Global configuration mode

Example

Switch_config# filter polling threshold ip 1500

Related Command

filter polling period filter polling auto-fit

1.1.6 filter polling auto-fit

To configure auto-fit the polling detect period and threshold, run the following command. The command is efficient by default. The polling period equals with the attack filter period and the polling packet threshold equals to 3/4 of the attack filter packet threshold. To resume to the default setting, use the no form of this command.

filter polling auto-fit no filter polling auto-fit

Parameters

None

Command Mode

Global configuration mode

Example

Switch_config# filter polling auto-fit

Related Command

filter polling period filter polling threshold

1.1.7 filter igmp

To enable detect ICMP attack, run the following command. To disable ICMP attack detection, run the no form of this command.

filter igmp no filter igmp

Parameters

None

Command Mode

Global configuration mode

Example

Switch_config# filter igmp

filter enable

1.1.8 filter ip source-ip

To enable IP attack detection, run this command. To disable IP attack detection, run the no form of this command.

filter ip source-ip no filter ip source-ip

Parameters

None

Command Mode

Global configuration mode and physical port configuration mode.

The command is efficient when both the global port and the physical port are configured.

Example

Switch_config# filter ip source-ip Switch_config# interface g0/1 switch_config_g0/1# filter ip source-ip

Related Command

filter enable

1.1.9 filter icmp

To enable ICMP attack detection, run the following command. To disable ICMP attack detection, run the no form of the following command.

filter icmp no filter icmp

Parameters

None

Command Mode

Global configuration mode and physical port configuration mode.

The command is efficient when both the global port and the physical port are configured.

Example

Switch_config# filter icmp Switch_config# interface g0/1 switch_config_g0/1# filter icmp

Related Command

filter enable

1.1.10 filter dhcp

To enable ICMP attack detection, run the following command. To disable DHCP attack detection, run the no form of this command.

filter dhcp no filter dhcp

Parameters

None

Command Mode

Global configuration mode and physical port configuration mode.

The command is efficient when both the global port and the physical port are configured.

Example

Switch_config# filter dhcp Switch_config# interface g0/1 switch_config_g0/1# filter dhcp

filter enable

1.1.11 filter arp

To enable the ARP attack detection, run this command. To disable ARP attack detection, run the no form of the following command.

filter arp no filter arp

Parameters

None

Command Mode

Physical interface configuration mode

Example

Switch_config_g0/1# filter arp

Related Command

filter enable

1.1.12 filter bpdu

To enable the BPDU attack detection, run this command. To disable BPDU attack detection, run this command.

filter bpdu no filter bpdu

Parameters

None

Command Mode

Physical interface configuration mode

Example

Switch_config_g0/1# filter bpdu

Related Command

filter enable

1.1.13 filter mode

To configure the filter mode, run the following command. **filter mode [raw | hybrid]**

Parameters

Parameters	Description
raw	To configure Filter as Raw mode.
hybrid	To configure Filter as Hybrid mode.

Default Value

Hybrid mode

Command Mode

Global configuration mode

Example

Switch_config# filter mode raw

Related Command

filter enable

1.1.14 filter enable

To enable the attack detection function, run this command in global mode. To return to the default setting, use the no form of this command.

filter enable no filter enable Parameters

None

Command Mode

Global configuration mode

Example

Switch_config# filter enable

Related Command

None

1.1.15 show filter

To display the working state of the attack-proof function of the current switch, run this command. To display working state of the anti-attack feature of the current switch, use the show filter command. **show filter show filter summary**

Parameters

None

Command Mode

Non-user mode

Example

Switch#show filter

Filter period 600 seconds, polling interval 600 seconds Filter thresholds:

Filter type(major code) Minor code Threshold Polling arp A 5 3 bpdu B

1000 750 dhcp D 1000 750 ip I 1000 750 icmp I

1000 750 igmp I 1000 750 Filters blocked:

Cause Address Seconds Discard Rate Polling Interface arp 0000.abcd.1234 7.41 0 0/0 592.59 G0/1

Filters counting:

Cause Address Seconds Count Interface arp 0000.abcd.1234 15.59 1 G0/1

Filters blocked:indicates MAC address of the blocked attack source, blocked time and source interface.

Filters counting:indicates MAC address of the attack source, counting time, the number of the receiving packets and the source interface.