Anti-Attack Configuration Commands

Table of contents

CHAPTER 1 ANTI-ATTACK CONFIGURATION COMMANDS

1.1. Anti-Attack Configuration Commands

1.1.1. filter period

Syntax

filter period time

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

no filter period

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

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

Syntax

filter threshold type value

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

no filter threshold type

To resume to the default value, use the no form of the previous command.

Parameters

Parameters	Description
type	Packet type, including ARP, BPDU, DHCP, IGMP, ICMPv6, 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

Syntax

filter block-time value

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

no filter block-time

To resume to the default value, use the no form of this command.

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

Syntax

filter polling period time

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

no filter polling period

To resume to the default value, use the no form of the previous command.

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

Related Command

filter polling threshold

filter polling auto-fit

1.1.5. filter polling threshold

Syntax

filter polling thredhold type value

To configure the filter polling threshold in the hybrid mode, run the following command. Vary your configuration in terms of the packet type.

no filter polling threshold type

To resume to the default value, use the no form of the previous command.

Parameters

Parameters	**Description**
type	Packet type, including ARP, BPDU, DHCP, IGMP, ICMP, ICMPv6,IP.
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

Syntax

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 detection period and the polling packet threshold equals to 3/4 of the attack detection packet threshold

no filter polling auto-fit

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

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

Syntax

filter igmp

To enable detect ICMP attack, run the previous command.

no filter igmp

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

Parameters

None

Command Mode

Global configuration mode

Example

Switch_config# filter igmp

Related Command

filter enable

1.1.8. filter ip source-ip

Syntax

filter ip source-ip

To enable IP attack detection, run this command.

no filter ip source-ip

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

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

Syntax

filter icmp

To enable ICMP attack detection, run the previous command.

no filter icmp

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

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

Syntax

filter dhcp

To enable ICMP attack detection, run the previous command.

no filter dhcp

To disable DHCP attack detection, run the previous command.

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

Related Command

filter enable

1.1.11. filter arp

Syntax

filter arp

To enable the ARP attack detection, run this command.

no filter arp

To disable ARP attack detection, run the no form of the previous command.

Parameters

None

Command Mode

Physical interface configuration mode

Example

Switch_config_g0/1# filter arp

Related Command

filter enable

1.1.12. filter bpdu

Syntax

filter bpdu

To enable the BPDU attack detection, run this command.

no filter bpdu

To disable BPDU attack detection, run this command.

Parameters

None

Command Mode

Physical interface configuration mode

Example

Switch_config_g0/1# filter bpdu

Related Command

filter enable

1.1.13. filter mode

Syntax

filter mode [raw | hybrid]

To configure the filter mode, run the following command.

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

Syntax

filter enable

To enable the attack detection function, run this command in global mode.

no filter enable

To resume to the default setting, run the no form of the previous command.

Parameters

None

Command Mode

Global configuration mode

Example

```
Switch_config# filter enable
```

Related Command

None

1.1.15. show filter

Syntax

show filter

To display the working state of the attack-proof function of the current switch, run this command.

show filter summary

To display working state of the anti-attack feature of the current switch, use the show filter command.

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.