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

To configure filter period for attack, use the filter period command.

filter period *time*

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

no filter period

Parameter

Parameter	Description
time	The filter period for attack in seconds. It is considered as attack when the attack source sends packets above the specified number in any filter period time. Value range: 1-600s.

Default

10 seconds

Command Mode

Global configuration mode

Example

Switch_config# filter period 15

Related Command

filter threshold

1.1.2 filter threshold

Syntax

To configure the filter threshold value, use the filter threshold value command. Vary your configuration in terms of the packet type.

filter threshold *type value*

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

no filter threshold *type*

Parameter

Parameter	Description
type	Packet type, including ARP, BPDU, DHCP, IGMP, ICMP, IP.
value	It is considered as attack when the receiving packets excddes the filter threshold value. Value range: 5-2000.

Default

1000

Command Mode

Global configuration mode

Example

Switch_config# filter threshold ip 1500

Related Command

filter period

1.1.3 filter block-time

Syntax

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

filter block-time *value*

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

no filter block-time

Parameter

Parameter	Description
Value	Time to block attack source in seconds. Value range: 1-86400.

Default

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

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

filter polling period *time*

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

no filter polling period

Parameter

Parameter	Description

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

Default

10s

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

To configure the filter polling threshold in the hybrid mode, run the following command.

filter polling thredhold *type value*

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

no filter polling threshold *type*

Parameter

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

Default

750 packets

Command Mode

Global configuration mode

Example

Switch_config# filter polling threshold ip 1500

Related Commands

filter polling period

filter polling auto-fit

1.1.6 filter polling auto-fit

Syntax

To configure auto-fit the polling detect period and thereshold, 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.

filter polling auto-fit

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

no filter polling auto-fit

Parameter

None

Command Mode

Global configuration mode

Example

Switch_config# filter polling auto-fit

Related Commands

filter polling period

filter polling threshold

1.1.7 filter igmp

Syntax

To enable IGMP attack detection, run the following command.

filter igmp

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

no filter igmp

Parameter

None

Command mode

Global configuration mode

Example

Switch_config# filter igmp

Related command

filter enable

1.1.8 filter ip source-ip

Syntax

To enable IP attack detection, run the following command.

filter ip source-ip

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

no filter ip source-ip

Parameter

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

To enable ICMP attack detection, run the following command.

filter icmp

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

no filter icmp

Parameter

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 icmpv6

Syntax

To enable ICMPv6 attack detection, run the following command.

filter icmpv6

To disable ICMPv6 attack detection, run the no form of the previous command.

no filter icmpv6

Parameter

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 icmpv6
Switch_config# interface g0/1
switch_config_g0/1# filter icmpv6
```

Related command

filter enable

1.1.11 filter dhcp

Syntax

To enable DHCP attack detection, run the following command.

filter dhcp

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

no filter dhcp

Parameter

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 Commands

filter enable

1.1.12 filter arp

Syntax

To fliter ARP attack, use the filter arp command.

filter arp

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

no filter arp

Parameter

None

Command Mode

Physical interface configuration

Example

Switch_config_g0/1# filter arp

Related Command

filter enable

1.1.13 filter bpdu

Syntax

To enable BPDU attack detection, run the following command.

filter bpdu

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

no filter bpdu

Parameter

None

Command Mode

Physical interface configuration

Example

Switch_config_g0/1# filter bpdu

Related Commands

filter enable

1.1.14 filter mode

Syntax

To configure the filter mode, run the following command.

filter mode [raw | hybrid]

Parameter

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

Default

Hybrid mode

Command Mode

Global configuration mode

Example

Switch_config# filter mode raw

Related Command

filter enable

1.1.15 filter enable

Syntax

To enable filter feature, use the filter enable command.

filter enable

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

no filter enable

Parameter

None

Command Mode

Global configuration mode

Example

Switch_config# filter enable

Related Command

None

1.1.16 filter shutdown-action

Syntax

To configure to shut down the port when an attack source is detected in raw mode, run the following command.

filter shutdown-action

To configure not to shut down the port when an attack source is detected in raw mode,, use the no form of the previous command.

no filter shutdown-action

Parameter

None

Command mode

Global configuration mode

Example

Switch_config# filter shutdown-action

Related command

None

1.1.17 show filter

Syntax

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

show filter

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

show filter summary

Parameter

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.