Anti-Attack Configuration Commands
Table of Contents

Chapter 1 Anti-Attack Configuration Commands .............................................................................................................1
  1.1 Anti-Attack Configuration Commands .............................................................................................................1
    1.1.1 filter period time ...........................................................................................................................................1
    1.1.2 filter threshold value ...................................................................................................................................2
    1.1.3 filter block-time value ..................................................................................................................................3
    1.1.4 filter igmp .....................................................................................................................................................3
    1.1.5 filter arp ......................................................................................................................................................3
    1.1.6 filter enable ................................................................................................................................................4
    1.1.7 show filter ....................................................................................................................................................4
Chapter 1 Anti-Attack Configuration Commands

1.1 Anti-Attack Configuration Commands

1.1.1 filter period *time*

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

<table>
<thead>
<tr>
<th>parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>time</td>
<td>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.</td>
</tr>
</tbody>
</table>

default

10 seconds

Command mode

Global configuration mode

example

Switch_config#filter period 15

Related commands

1.1.2 filter threshold *value*

To configure the filter threshold value, use the filter threshold value command.

<table>
<thead>
<tr>
<th>parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>It is considered as attack when the receiving packets exceed the filter threshold value.</td>
</tr>
</tbody>
</table>
default

1000

command mode

global configuration mode

eample

Switch_config#filter threshold 1500

Related commands

filter period time

1.1.3 filter block-time value

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

default

300 seconds

command mode

global configuration mode

eample

Switch_config#filter block-time 600

Related commands

filter period time

filter threshold value
1.1.4 filter igmp

To filter IGMP attack, use the filter igmp command.

Parameter

none

Command mode

Global configuration mode

Example

Switch_config#filter igmp

Related commands

filter enable

1.1.5 filter arp

To filter ARP attack, use the filter arp command.

Parameter

none

Command mode

Physical interface configuration mode

Example

Switch_config_f0/1#filter arp

Related commands

filter enable

1.1.6 filter enable

To enable filter feature, use the filter enable command.
parameter

none

Command mode

Global configuration mode

example

Switch_config#filter enable

Related commands

filter igmp
filter arp

1.1.7  show filter

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

parameter

none

command mode

non-user mode

Switch#show fil
Filter threshold: 1000 packet in any 10 seconds
Filters blocked:
Address         seconds     source interface
00a0.0c13.647d    27.0      FastEthernet1/2

Filters counting:
Address         seconds     count    source interface
00a0.0c43.647d     1.84     371       FastEthernet1/2

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.