

防攻击配置命令

目 录

第 1 章 防攻击配置命令	1
1.1 防攻击配置命令	1
1.1.1 filter period <i>time</i>	1
1.1.2 filter threshold <i>value</i>	1
1.1.3 filter block-time <i>value</i>	2
1.1.4 filter igmp	3
1.1.5 file ip source-ip	3
1.1.6 filter arp	3
1.1.7 filter enable	4
1.1.8 show filter	4

第1章 防攻击配置命令

1.1 防攻击配置命令

1.1.1 filter period *time*

配置攻击检测周期。

参数

参数	参数说明
<i>time</i>	防攻击的检测周期，以秒为单位。攻击源在任何 <code>time</code> 时间长度内发送超过指定数量的报文则认为是攻击

缺省

`time` 缺省为 10 秒

命令模式

全局配置态

示例

```
Switch_config#filter period 15
```

相关命令

filter threshold *value*

1.1.2 filter threshold *value*

配置攻击检测周期收到多少报文时认为是攻击

参数

参数	参数说明
<i>value</i>	防攻击的检测在任意一个周期内收到 <code>value</code> 个报文时认为是攻击

缺省

value 缺省为 1000 个报文

命令模式

全局配置态

示例

Switch_config#filter threshold 1500

相关命令

filter period time

1.1.3 filter block-time *value*

配置检测到攻击后，阻塞攻击源的时间。

参数

参数	参数说明
<i>value</i>	检测到攻击后，阻塞攻击源的时间，单位为秒

缺省

value 缺省为 300 秒

命令模式

全局配置态

示例

Switch_config#filter block-time 600

相关命令

filter period time

filter threshold value

1.1.4 filter igmp

允许对 IGMP 攻击进行检测

参数

无

命令模式

全局配置态

示例

```
Switch_config#filter igmp
```

相关命令

filter enable

1.1.5 file ip source-ip

允许对 IP 攻击进行检测

参数

无

命令模式

全局配置态

示例

```
switch_config#filter ip source-ip
```

相关命令

filter enable

1.1.6 filter arp

允许对 ARP 攻击进行检测

参数

无

命令模式

物理接口配置态

示例

Switch_config_f0/1#filter arp

相关命令

filter enable

1.1.7 filter enable

打开攻击检测功能

参数

无

命令模式

全局配置态

示例

Switch_config#filter enable

相关命令

filter igmp

filter arp

1.1.8 show filter

显示当前交换机防攻击功能的工作状态

参数

无

命令模式

非用户态

示例

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:表示已经被阻塞的攻击源的 MAC 地址、已阻塞时间和来源端口。

Filters counting:表示正在检测的可能是攻击源的 MAC 地址、当前已经记录的时间长度、在该时间内收到的报文数量和来源端口。