防止攻击配置命令

目 录

第 1 章　防止攻击配置命令

1.1　防止攻击配置命令

1.1.1　filter period

filter period *time*

配置攻击检测周期。

no filter period

恢复攻击检测周期为缺省值。

参数

参数	参数说明
time	防攻击的检测周期，以秒为单位。攻击源在任何time时间长度内发送超过指定数量的报文则认为是攻击。 范围：1-600秒。

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

1.1.2　filter threshold

filter threshold *type value*

配置检测周期收到多少报文时认为是攻击。可对不同的报文类型区别设置。

no filter threshold *type*

恢复某一类报文的检测门限为缺省值。

参数

参数	参数说明
type	报文类型，包括：ARP, BPDU, DHCP, IGMP, ICMP, IP。
value	防攻击的检测在任意一个周期内收到value个报文时认为是攻击。 范围：5-2000.

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 ip 1500

相关命令

filter period

1.1.3 filter block-time

filter block-time *value*

配置 Raw 模式下检测到攻击后，阻塞攻击源的时间。

no filter block-time

恢复阻塞攻击源的时间为缺省值。

参数

参数	参数说明
value	检测到攻击后，阻塞攻击源的时间，单位为秒。 范围：1-86400.

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

filter threshold

1.1.4 filter polling period

filter polling period *time*

配置混合模式（Hybrid）下对攻击源轮询检测的周期。

no filter polling period

恢复混合模式（Hybrid）下对攻击源轮询检测的周期为缺省值。

参数

参数	参数说明
time	阻塞攻击源后，轮询检测的周期，单位秒。 范围：1-600.

缺省

time 缺省为 10 秒

命令模式

全局配置态

示例

Switch_config# filter polling period 20

相关命令

filter polling threshold

filter polling auto-fit

1.1.5 filter polling threshold

filter polling thredhold *type value*

配置混合模式下，一次轮询检测周期收到多少个攻击报文认为攻击源仍然存在。可对不同的报文类型区别设置。

no filter polling threshold *type*

恢复轮训检测的报文门限为缺省值。

参数

参数	参数说明
type	报文类型，包括：ARP, BPDU, DHCP, IGMP, ICMP, IP。
value	在任意一个轮询周期内收到value个报文时认为攻击源仍然存在。 范围：1-2000.

缺省

value 缺省为 750 个报文

命令模式

全局配置态

示例

Switch_config# filter polling threshold ip 1500

相关命令

filter polling period

filter polling auto-fit

1.1.6 filter polling auto-fit

filter polling auto-fit

配置轮询检测的 period 和 threshold 参数在攻击源检测的参数变化时自动更新。该命令缺省有效，轮询的周期等于攻击检测周期，轮询的报文门限值等于攻击检测报文门限值的四分之三。

no filter polling auto-fit

取消轮询检测参数的自动更新。

参数

无

命令模式

全局配置态

示例

Switch_config# filter polling auto-fit

相关命令

filter polling period

filter polling threshold

1.1.7 filter igmp

filter igmp

允许对 IGMP 攻击进行检测。

no filter igmp

关闭对 IGMP 攻击的检测。

参数

无

命令模式

全局配置态

示例

Switch_config# filter igmp

相关命令

filter enable

1.1.8 filter ip source-ip

filter ip source-ip

允许对 IP 攻击进行检测

no filter ip source-ip

关闭对 IP 攻击的检测。

参数

无

命令模式

全局配置态和物理端口配置态。

在全局和物理端口都配置时该功能生效。

示例

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

相关命令

filter enable

1.1.9 filter icmp

filter icmp

允许对 ICMP 攻击进行检测。

no filter icmp

关闭对 ICMP 攻击的检测。

参数

无

命令模式

全局配置态和物理端口配置态。

在全局和物理端口都配置时该功能生效。

示例

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

相关命令

filter enable

1.1.10 filter dhcp

filter dhcp

允许对 DHCP 攻击进行检测。

no filter dhcp

关闭对 DHCP 攻击的检测。

参数

无

命令模式

全局配置态和物理端口配置态。

在全局和物理端口都配置时该功能生效。

示例

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

相关命令

filter enable

1.1.11 filter arp

filter arp

允许对 ARP 攻击进行检测。

no filter arp

关闭对 ARP 攻击的检测。

参数

无

命令模式

物理接口配置态

示例

Switch_config_g0/1# filter arp

相关命令

filter enable

1.1.12 filter bpdu

filter bpdu

允许对 BPDU 攻击进行检测。

no filter bpdu

关闭对 BPDU 攻击的检测。

参数

无

命令模式

物理接口配置态

示例

Switch_config_g0/1# filter bpdu

相关命令

filter enable

1.1.13 filter mode

filter mode [raw | hybrid]

配置 Filter 的模式。

参数

参数	参数说明
raw	配置Filter为Raw模式。
hybrid	配置Filter为Hybrid模式。

缺省

Filter 缺省为 Hybrid 模式。

命令模式

全局配置态

示例

Switch_config# filter mode raw

相关命令

filter enable

1.1.14 filter enable

filter enable

全局打开攻击检测功能。

no filter enable

全局关闭攻击检测，所有已阻塞的攻击源将会被解除阻塞。

参数

无

命令模式

全局配置态

示例

Switch_config# filter enable

相关命令

无

1.1.15 show filter

show filter

显示当前交换机防攻击功能的工作状态

show filter summary

显示防攻击功能当前的参数配置以及统计信息。

参数

无

命令模式

非用户态

示例

```
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: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。