防止攻击配置

目 录

第 1 章　防攻击介绍

1.1　Filter概述

为保证网络带宽的合理利用，确保网络用户以及设备自身的正常工作，我司以太网交换机系列产品提供了防攻击功能（Filter），用于对恶意流量进行检测和抑制。

Filter 能够识别交换机端口上接收的报文，并按照报文类型进行统计。针对目前常见的攻击形式，Filter 可以统计出一段时间内某个主机发送的 ARP、 IGMP 或者 IP 报文的数目，一旦数目超限，设备便不再转发该主机的报文。

Filter 通过阻塞源地址的方式限制来自特定主机的报文。对于 ARP 攻击，Filter 阻塞源 MAC 地址；而对于 IP 类型的攻击，比如 Ping 扫描和 TCP/UDP 端口扫描，Filter 会阻塞源 IP 地址。

1.2　Filter的模式

Filter 的模式决定了交换机如何限制已经确定的攻击源，有两种模式可以选择：

- 源地址定时阻塞（Raw）：

Raw 模式下，从确定攻击源时开始，交换机会在预先设定的阻塞时间（**block-time**）内丢弃来自攻击源的报文。超过阻塞时间之后，自动解除对攻击源地址的限制，并启动新一轮统计。

Raw 模式严格按照源地址阻塞报文。比如，在攻击源的 MAC 地址被阻塞之后，所有源 MAC 地址等于该地址的报文，无论 ARP、ICMP、DHCP 或其它类型，都会被丢弃。

- 源地址阻塞加轮询，或称混合模式（Hybrid）

阻塞攻击源之后，交换机继续对来自攻击源的报文进行计数，并在预先设定的轮询时间（**Polling Interval**）到达时检查这段时间攻击源发送的报文是否仍然超过限制，若超过限制，说明攻击源仍然存在，则保持阻塞状态，若没有超过限制，说明攻击可能已经停止，此时便解除阻塞。在混合模式下，可以对初次确定攻击源时的报文限制数目和轮询检查时的报文限制数目分别进行配置。

为了实现对攻击报文的持续统计，混合模式在阻塞源地址的同时会匹配报文类型。比如，一台主机因发起 ARP 攻击而被阻塞了 MAC 地址，除非该主机也被识别为存在 IP 攻击，否则来自该主机的 IP 报文仍然会被交换机转发。

请根据应用环境选择 Filter 的模式。如果希望对攻击源进行严格的控制，并相对减轻交换机 CPU 的负担，请使用 Raw 模式；如果希望灵活的控制攻击源，并在攻击停止后尽快恢复主机的通信，请使用混合模式。需要注意的是，混合模式交换机能够支持的 Filter 数目是有限的，在数目不足的情况下，会自动使用 Raw 模式阻塞攻击源。

第 2 章　防止攻击配置

2.1　防止攻击的配置任务列表

当某台主机在任意指定时间间隔内发送的 IGMP, ARP 或者 IP 报文数量超过门限时，就认为它对网络造成了攻击。

Filter 支持选择需要统计的报文类型（ARP，IGMP，IP 等）、应用防攻击功能的端口和攻击检测参数。用户需要进行的配置任务有：

- 配置攻击检测参数
- 配置攻击检测类型
- 启用防止攻击功能
- 查看当前防止攻击功能的工作情况

2.2　防止攻击配置

2.2.1　配置攻击检测参数

在交换机全局配置模式下，通过下面的命令配置 Filter 的检测参数。

命令	目的
Switch# **config**	进入全局配置模式。
Switch_config# **filter period** *time*	配置攻击检测周期为time，单位为秒。
Switch_config# **filter threshold** **[arp | bpdu | dhcp | igmp | ip | icmp]** *value*	配置各种报文类型的攻击检测门限为value个报文。
Switch_config# **filter block-time** *time*	配置Raw模式下对攻击源地址进行阻塞的时间，以秒为单位。
Switch_config# **filter polling period** *time*	配置Hybrid模式下轮询检查攻击源的周期，单位秒。
Switch_config# **filter polling threshold** **[arp | bpdu | dhcp | igmp | ip | icmp]** *value*	配置Hybrid模式轮询检查时的攻击报文门限值。
Switch_config# **filter polling auto-fit**	配置Hybrid模式轮询检查的**period**和**threshold**参数自动适应攻击源检测的对应参数。

	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。

2.2.2 配置攻击检测类型

在全局和端口配置模式下，使用下面的命令配置攻击检测类型。

命令	目的
Switch# **config**	进入全局配置模式。
Switch_config# **filter dhcp**	全局启动DHCP报文攻击检测。
Switch_config# **filter icmp**	启动ICMP报文攻击检测。
Switch_config# **filter igmp**	启动IGMP报文攻击检测。
Switch_config# **filter ip source-ip**	全局启动IP攻击检测。
Switch_config# **interface intf-name**	进入端口配置模式。
Switch_config_intf# **filter arp**	启动端口的ARP报文攻击检测。
Switch_config_intf# **filter bpdu**	启动端口的BPDU报文攻击检测。
Switch_config_intf# **filter dhcp**	启动端口的DHCP报文攻击检测。
Switch_config_intf# **filter icmp**	启动端口的ICMP报文攻击检测。
Switch_config_intf# **filter ip source-ip**	启动端口的IP报文攻击检测。

说明：
ARP 攻击将一个“主机 MAC 地址+来源端口”二元组作为一个攻击源。也就是说，对于相同的 MAC 地址但从不同端口来的报文，计数不会被累加。而 IGMP 和 IP 攻击都将“主机 IP+来源端口”作为攻击源。

请注意：
1、 防止 IGMP 攻击和防止 IP 攻击功能不能同时启动。
2、IP、ICMP 和 DHCP 报文攻击检测需要同时在全局和端口模式配置之后才生效。

2.2.3 启用防止攻击功能

当防攻击的全部参数配置完毕后，就可以启动防止攻击功能了。需要指出的是，防止攻击功能是需要消耗少量处理器资源的。

命令	目的
Switch_config# **filter enable**	启用防止攻击功能
Switch_config# **filter mode** [**raw** | **hybrid**]	配置Filter的模式，Raw或者Hybrid。

使用 **no filter enable** 命令，关闭攻击检测功能，并且解除所有被阻塞的攻击源。

2.2.4 查看当前防止攻击功能的工作情况

当您启用防止攻击功能后，可以通过下面命令查看该功能的工作情况。

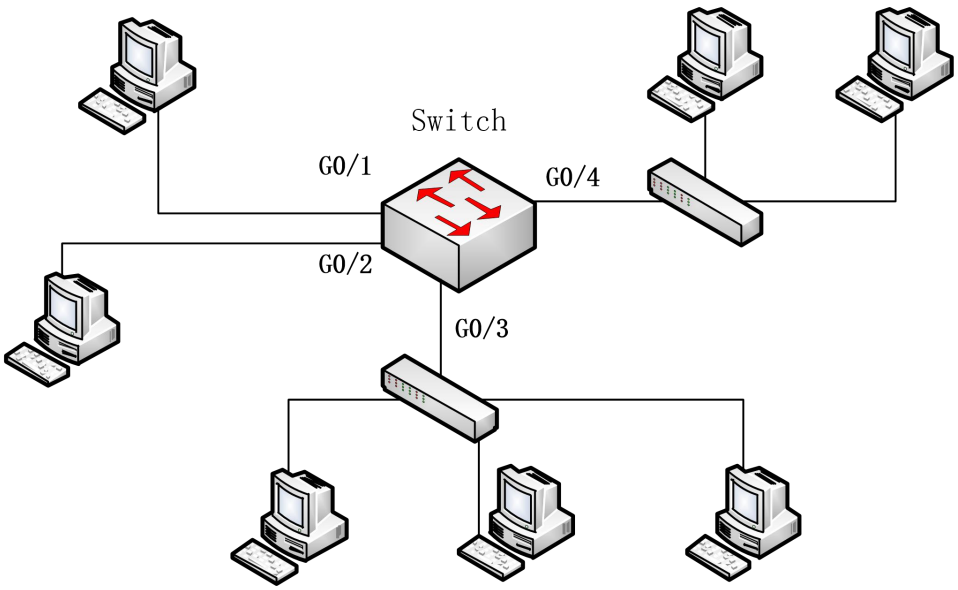
命令	目的
show filter	查看Filter的参数设置、被阻塞的攻击源以及正在统计的报文条目。
show filter summary	查看Filter的参数设置和摘要信息。

第 3 章　防止攻击配置举例

请注意：
本章描述的示例仅作为配置 Filter 功能的参考，相关参数值的选取，请结合实际网络的情况而定。

3.1　使用Filter ARP保护局域网

如下图所示，在交换机 Switch 上配置 Filter 防止 ARP 攻击。



配置 Filter 的参数，判断攻击源的标准为主机 10 秒钟发送超过 100 个 ARP 报文：

```
Switch# config
Switch_config# filter period 10
Switch_config# filter threshold arp 100
```

配置四个端口的 ARP 攻击检测：

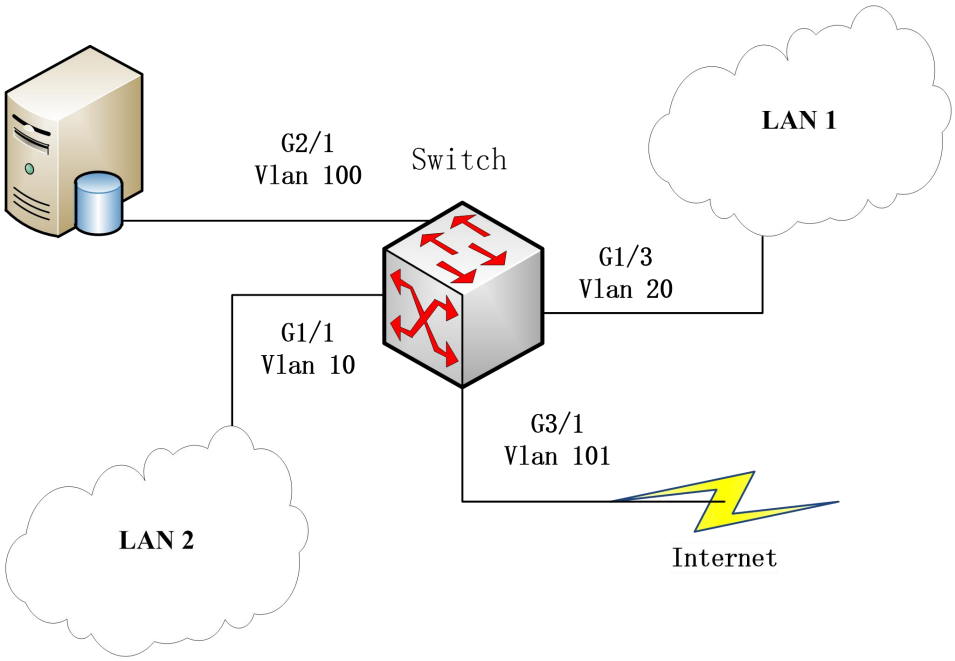
```
Switch_config# interface range g0/1 – 4
Switch_config_intf# filter arp
```

配置使用 Raw 模式，然后启动 Filter：

```
Switch_config_intf# exit
Switch_config# filter mode raw
Switch_config# filter enable
```

3.2 使用Filter IP保护三层网络

如下图所示，交换机 Switch 连接多个局域网、服务器，并连接到互联网。通过配置防 IP 报文攻击，可以有效阻断跨子网的 IP 扫描，并可阻止 BitTorrent 等工具在短时间里发起大量的网络连接。



配置 Filter 参数，判断攻击源的标准为 1 分钟 300 个 IP 报文：

```
Switch# config
Switch_config# filter period 60
Switch_config# filter threshold ip 300
```

在全局模式和端口模式下启动 IP 报文检测，注意连接服务器和外网的端口无需配置：

```
Switch_config# filter ip source-ip
Switch_config# interface g1/1
Switch_config_g1/1# filter ip source-ip
Switch_config_g1/1# interface g1/3
Switch_config_g1/3# filter ip source-ip
Switch_config_g1/3# exit
Switch_config#
```

启动 Filter：

```
Switch_config# filter enable
```