

防止攻击配置

目 录

第 1 章 防止攻击配置	1
1.1 概述	1
1.2 防止攻击的配置任务列表	1
1.3 防止攻击配置	1
1.3.1 配置攻击检测参数	1
1.3.2 配置攻击检测类型	1
1.3.3 启用防止攻击功能	2
1.3.4 查看当前防止攻击功能的工作情况	2
1.4 防止攻击配置举例	2

第1章 防止攻击配置

1.1 概述

为保证网络带宽的合理利用，本公司 6508 交换机提供了防止恶意流量大量占用网络带宽的功能。针对目前最常见的攻击形式，对一段时间内大量发送 ARP, IGMP 或者 IP 报文的主机进行通信限制，不对这些主机提供任何网络服务。使用该功能可以防止恶意报文大量占用网络带宽导致网络 congestion 的问题。

1.2 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，我们就认为它对网络造成了攻击。

用户可以选择防止攻击的类型（ARP, IGMP 或者 IP）、应用防攻击功能的端口和攻击检测参数。因此用户需要进行的配置任务有：

- 配置防止攻击类型
- 配置攻击检测参数

1.3 防止攻击配置

1.3.1 配置攻击检测参数

命令	目的
filter period time	配置攻击检测周期为time，单位为秒
filter threshold value	配置攻击检测门限为value个报文
filter block-time time	当时别出攻击源后，对攻击源进行停止服务的时间，以秒为单位

1.3.2 配置攻击检测类型

命令	目的
filter igmp	允许igmp攻击的检测
filter ip source-ip	允许基于源IP地址的IP攻击检测
interface f x/y	进入槽x端口y的端口配置模式，
filter arp	允许arp攻击的检测

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。

需要注意的是，防止 IGMP 攻击和防止 IP 攻击功能不能同时启动。

1.3.3 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
filter enable	启用防止攻击功能

使用该命令的 no 形式时，关闭攻击检测功能，并且所有被阻塞的攻击源被解除阻塞。

1.3.4 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，可以通过命令查看该功能的工作情况。

命令	目的
show filter	查看防止攻击功能的工作情况

1.4 防止攻击配置举例

用户希望打开防止 IGMP 攻击功能，并在端口 1/2 上打开防止 ARP 攻击功能，要求任何主机在任何 15 秒内发送超过 1200 个报文时就认为是攻击，对攻击源阻塞网络服务 10 分钟，则应该如下配置：

```
filter period 15
filter threshold 1200
filter block-time 600
interface f1/2
filter arp
exit
filter enable
```