DoS防攻击配置

目 录

第 1 章　DoS 防攻击配置

1.1　DoS攻击概述

1.1.1　DoS 攻击概念

DoS 攻击也即拒绝服务攻击。最常见的 DoS 攻击有计算机网络带宽攻击和联通性攻击。DoS 攻击是一种最常见的攻击计算机网络的黑客方式。它的最终目的就是让计算机网络陷入瘫痪而无法为合法客户提供正常的网络请求服务。

DoS 防攻击需要交换机提供包括 Pingflood、SYNflood、Landattack、Teardrop、带非法 Flags 的 TCP 攻击在内的诸多攻击的防御手段。交换机在收到攻击时，需要判断这些攻击属于何种攻击类型，并对攻击报文进行特定的处理，如发往 CPU 并丢弃。

1.1.2　DoS 攻击类型

黑客会通过构造各种不同的 DoS 攻击报文来攻击服务器。最常见的 DoS 攻击报文有：

1. Ping of Death

Ping of Death 造畸形的 Ping 包，声称自己的大小已经超过 ICMP 大小上限，导致 TCP/IP 协议栈崩溃，最终导致接收方宕机。

2. TearDrop

TearDrop 用在 TCP/IP 协议栈中信任 IP 碎片中的包的标题头所包含的信息来实现自己的攻击。IP 分段含有指示该分段所包含的是原包的哪一段的信息，即 offset 位，某些 TCP/IP 协议栈在收到含有重叠偏移的伪造分段时将崩溃。

3. SYN Flood

对于标准的 TCP 连接，需要进行三次握手过程，首先请求方向服务器发送一个 SYN 信息，然后服务方回复一个 SYN-ACK，请求方收到后再向服务方发送一个 ACK 信息，这样一个 TCP 连接就建立了。SYN 泛洪攻击是专门针对 TCP 协议栈在两台主机间初始化连接握手的过程进行 DoS 攻击，它在请求方收到 SYN-ACK 信息后，请求方通过源地址欺骗等手段，使得服务方收不到 ACK 回应，于是服务方就会在一定时间内处于等待 ACK 信息阶段。如果攻击者连续发送此类连接请求，这样该服务器的 TCP 连接队列就会很快被阻塞，网络带宽迅速减小，系统将无法提供正常的服务。

4. Land Attack

攻击者通过构造一个特殊的 SYN 包（源地址和目的地址同为一个服务地址），这样将会导致服务器向自己发送 SYN-ACK 信息，结果这个地址又 发送 ACK 信息并创建一个空链接，每个这样的连接都会保持到超时，这样服务器会崩溃。Landattack 又可以分为 IPland 和 MACland。

1.2 DoS防攻击配置任务列表

基于全局的 dos 防攻击配置，用户配置相应的子功能后，交换机能丢弃相应的 dos 攻击报文，从而保证交换机的网络带宽不被消耗殆尽。

DoS 防攻击配置任务有：

- 配置全局 DoS 防攻击功能
- 显示配置的 DoS 防攻击功能

1.3 DoS防攻击配置任务

1.3.1 配置全局 DOS 防攻击功能

配置全局 DoS 防攻击功能是指在全局状态下配置 DoS 防攻击子功能，每一项子功能能抵御不同类型的 DoS 攻击报文。dos 的 IP 子功能可以抵御 Land 攻击，dos 的 icmp 子功能能抵御死亡之 Ping 的攻击等。用户可以视情况配置对应的子功能。

进入特权模式下按下列步骤配置 dos 防攻击功能。

命令	目的
config	进入全局配置模式。
[**no**] **dos enable {all | icmp *icmp-value* | ip | ipv4firstfrag | l4port | mac | tcpflags | tcpfrag *tcpfrag-value*}**	配置all可以抵御各种类型的DoS攻击报文 配置icmp抵御icmp报文，*icmp-value*是最大的icmp报文长度 配置ip可以抵御源、目的IP相等的IP报文 配置ipv4firstfrag用于检测IP报文的第一个分片 配置l4port用于抵御源、目的端口号相等的TCP/UDP报文 配置mac用于抵御源、目的mac相等的报文攻击 配置tcpflags用于抵御带非法tcpflags的TCP报文 配置tcpfrag用于抵御检测TCP分包，

	*tcpfrag-value*为最小的TCP头部长度
exit	退回到管理配置模式。
write	保存配置。

1.3.2 显示配置的 DOS 防攻击功能

可以通过 show 命令来显示用户配置的 DoS 防攻击功能。

进入特权模式下使用下列命令显示用户配置的 DoS 防攻击功能。

命令	目的
show dos	显示用户配置的DoS防攻击功能

1.4 DoS防攻击配置示例

在全局状态下配置抵御带非法 flag 的 TCP 报文攻击，并显示用户配置。

config

dos enable tcpflags

show dos

在全局状态下配置抵御源、目的 IP 地址相等的 IP 报文攻击。

config

dos enable ip

在全局状态下配置抵御最大长度超过 255 的 ICMP 报文攻击。

config

dos enable icmp 255