DoS防攻击配置命令

目 录

1. DoS 防攻击配置命令

1.1. DoS防攻击配置命令

DoS 防攻击配置命令有：

- dos enable
- show dos

1.1.1. dos enable

命令描述

dos enable {all | icmp *icmp-value* **| ip | ipv4firstfrag | l4port | mac | tcpflags | tcpfrag** *tcpfrag-value***}**

no dos enable {**all | icmp | ip | ipv4firstfrag | l4port | mac | tcpflags | tcpfrag**}

参数

参数	参数说明
all	开启抵御所有类型的dos攻击报文
icmp *icmp-value*	开启抵御icmp类型的dos攻击报文，*icmp-value为最大的icmp报文长度*，缺省值为512
ip	抵御源IP地址与目的IP地址相等的dos攻击报文
ipv4firstfrag	开启检测ip报文的第一个分包
l4port	开启检测源端口等于目的端口的四层报文
mac	开启检测源、目的mac相等的报文
tcpflags	开启检测带非法的flag的tcp报文
tcpfrag *tcpfrag-value*	开启检测tcp分包的dos攻击报文，*tcpfrag-value为最小的tcp头部*，缺省值为20

缺省

缺省为 DoS 防攻击功能关闭

说明

DoS 防攻击功能配置模式是全局配置。

dos 的 ip 子功能能丢弃源 IP 地址等于目的 IP 地址的 IP 报文。

dos 的 icmp 子功能能丢弃报文：1.大小大于 *icmp-value* 的 ICMPv4、ICMPv6 ping 包 2.分包的 ICMP 报文。

dos 的 l4port 子功能能丢弃源端口号等于目的端口号的 TCP/UDP 报文。

dos 的 mac 子功能丢弃源、目的 mac 相等的报文。

dos 的 tcpflags 子功能能丢弃以下四类 TCP 报文：1.TCP SYN flag = 1 & source port<1024；2.TCP control flags = 0 & sequence = 0；3.TCP FIN URG PSH =1 & sequence = 0；4.TCP FIN SYN =1。

dos 的 tcpfrag 子功能丢弃以下两类 TCP 报文：1.TCP 头部小于 *tcpfrag-value* 的第一个 TCP 分包；2.offset 值为 1 的 TCP 分包。

示例

设置全局的 dos 防攻击子功能，抵御源、目的 IP 地址相等的 IP 报文

Switch_config#dos enable ip

配置全局状态下的 dos 防攻击子功能，抵御最大 icmp 长度大于 255 的攻击报文。

Switch_config#dos enable icmp 255

1.1.2. show dos

命令描述

show dos

显示用户配置的所有 dos 防攻击子功能。

参数

无

缺省

无

说明

管理模式

示例

显示所有的 dos 防攻击子功能。

```
Switch_config#dos enable all
Switch_config#show dos
dos enable ip
dos enable ipv4firstfrag
dos enable tcpflags
dos enable l4port
dos enable mac
dos enable tcpfrag
dos enable icmp
Switch_config#
```

用户配置 dos enable icmp，显示用户配置的子功能

```
Switch_config#dos enable icmp
Switch_config#show dos
dos enable icmp
```

用户配置 dos enable icmp 255，显示用户配置的子功能

```
Switch_config#dos enable icmp 255
Switch_config#show dos
dos enable icmp 255
```