DoS Attack Prevention Configuration

Table of Contents

Chapter 1 DoS Attack Prevention Configuration

1.1 DoS Attack Overview

1.1.1 Concept of DoS Attack

The DoS attack is also called the service rejection attack. Common DoS attacks include network bandwidth attacks and connectivity attacks. DoS attack is a frequent network attack mode triggered by hackers. Its ultimate purpose is to break down networks to stop providing legal users with normal network services.

DoS attack prevention requires a switch to provide many attack prevention methods to stop such attacks as Pingflood, SYNflood, Landattack, Teardrop, and illegal-flags-contained TCP. When a switch is under attack, it needs to judge which attack type it is and handles these attack packets specially, for example, sending them to CPU and drop them.

1.1.2 DoS Attack Type

Hackers will make different types of DoS attack packets to attack the servers. The following are common DoS attack packets:

1. Ping of Death

Ping of Death is the abnormal Ping packet, which claims its size exceeds the ICMP threshold and causes the breakdown of the TCP/IP stack and finally the breakdown of the receiving host.

2. TearDrop

TearDrop uses the information, which is contained in the packet header in the trusted IP fragment in the TCP/IP stack, to realize the attack. IP fragment contains the information that indicates which part of the original packet is contained, and some TCP/IP stacks will break down when they receive the fake fragment that contains the overlapping offset.

3. SYN Flood

A standard TCP connection needs to experience three hand-shake processes. A client sends the SYN message to a server, the server returns the SYN-ACK message, and the client sends the ACK message to the server after receiving the SYN-ACK message. In this way, a TCP connection is established. SYN flood triggers the DoS attack when the TCP protocol stack initializes the hand-shake procedure between two hosts.

4. Land Attack

The attacker makes a special SYN message (the source address and the destination address are the same service address). The SYN message causes the server to send the SYN-ACK message

to the sever itself, hence this address also sends the ACK message and creates a null link. Each of this kinds of links will keep until the timeout time, so the server will break down. Landattack can be classified into IPland and MACland.

1.2 DoS Attack Prevention Configuration Task List

As to global DoS attack prevention configuration, you configure related sub-functions and then the switch drops corresponding DoS attack packets. Hence, the bandwidth of the switch is guaranteed not to be used up.

DoS attack prevention configuration tasks are shown below:

Configuring Global DoS Attack Prevention

Displaying All DoS Attack Prevention Configuration

1.3 DoS Attack Prevention Configuration Tasks

1.3.1 Configuring Global DoS Attack Prevention

Configuring global DoS attack prevention means configuring DoS attack prevention sub-functions in global mode and each sub-function can prevent a different type of DoS attack packets. The DoS IP sub-function can prevent the LAND attacks, while the DoS ICMP sub-function can prevent Ping of Death. You can set the corresponding sub-function according to actual requirements.

Configure the DoS attack prevention function in EXEC mode.

Command	Purpose
config	Enters the global configuration mode.
[**no**] **dos enable {all | icmp** ***icmp-value*** **| ip | ipv4firstfrag | l4port | mac | tcpflags | tcpfrag** ***tcpfrag-value***}	Configures **all** to prevent all types of DoS attack packets. Configures **icmp** to prevent the ICMP packets, among which the **icmp-value** means the maximum length of the ICMP packet. Configures **ip** to prevent those IP packets whose source IPs are the same as the destination IPs. Configures **ipv4firstfrag** to check the first fragment of the IP packet. Configures **l4port** to prevent those TCP/UDP packets whose source port IDs are destination port IDs. Configures **mac** to prevent those packets whose source MACs are destination MACs. Configures **tcpflags** to prevent those TCP packets containing illegal TCP flags.

	Configures **tcpfrag** to prevent those TCP packets whose minimum TCP header is **tcpfrag-value**.
exit	Goes back to the EXEC mode.
write	Saves the settings.

1.3.2 Displaying All DoS Attack Prevention Configurations

You can display the Dos attack prevention configurations through the **show** command.

Run the following command in EXEC mode to display the configured DoS attack prevention functions.

Command	Purpose
show dos	Displays Dos attack prevention configuration.

1.4 DoS Attack Prevention Configuration Example

The following example shows how to configure to prevent the attacks of TCP packets, which have illegal flags, and then displays user's configuration.

```
config

dos enable tcpflags

show dos
```

The following example shows how to prevent the attacks of IP packets whose source IPs are destination IPs in global mode.

```
config

dos enable ip
```

The following example shows how to prevent in global mode the attacks of ICMP packets whose maximum length is more than 255.

```
config

dos enable icmp 255
```