DoS-Attack Prevention Configuration Commands

Table of Contents

Chapter 1 DoS-Attack Prevention Configuration Commands

1.1. DoS-Attack Prevention Configuration Commands

DoS-Attack Prevention Configuration Commands include:

- dos enable
- show dos

1.1.1. dos enable

Syntax

dos enable {all / icmp *icmp-value* **| ip | l4port | mac | tcpflags | tcpfrag** *tcpfrag-value* **| tcpsmurf | icmpsmurf | ipsmurf }**

no dos enable { **all / icmp** *icmp-value* **| ip | l4port | mac | tcpflags | tcpfrag** *tcpfrag-value* **| tcpsmurf | icmpsmurf | ipsmurf** }

Parameters

Parameters	Description
all	Enables to prevent all kinds of DoS attacks.
icmp *icmp-value*	Enables detection ICMP packet *icmp-value* is the maximum length of the ICMP packet. The ICMP packet and ICMPv6 packet whose length is larger than *icmp-value* will be dropped.
ip	Prevents those DoS attack packets whose source IP addresses are equal to the destination IP addresses.
l4port	Starts to check the L4 packets whose source port is equal to the destination port.
mac	Prevents those packets whose source MACs equal to destination MACs.
tcpflags	Starts to check the TCP packets with illegal flags.
tcpfrag *tcpfrag-value*	Starts to check the DoS attack packet of TCP fragment. Here, the tcpfrag-value parameter means the minimum TCP header, whose default value is 20.
tcpsmurf	Prevents those TCP packets whose destination addresses equal to broadcast addresses.
icmpsmurf	Prevents those ICMP packets whose destination addresses equal to broadcast addresses.
ipsmurf	Prevents those ICMP packets whose destination addresses equal to broadcast addresses.

Default Value

DoS attack prevention is disabled by default.

Usage Guidelines

DoS attack prevention is configured in global mode.

The DoS IP sub-function can drop those IP packets whose source IPs are equal to the destination IPs. Prevents LAND attack.

The DoS ICMP sub-function can drop the following two kinds of packets: 1. ICMP ping packets whose size is larger than icmp-value;   2. ICMP packets, ICMPv6 packets. Prevents PING attack.

The DoS l4port sun-function can drop those TCP/UDP packets whose source port is equal to the destination port.

TheDoS mac sub-function can check packet MAC address and prevents those packets whose source MAC addresses equal to destination MAC address.

The DoS tcpflags sub-function can drop the following 4 kinds of TCP packets: 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.

The DoS tcpfrag sub-function can drop the following two kinds of TCP packets: 1. The TCP header is smaller than the first TCP fragment of tcpfrag-value; 2. TCP fragments whose offset values are 1. Prevents tear drop attack.

The DoS tcpsmurf sub-function can prevent tcpmurf attack and those TCP packets whose destination addresses are broadcast addresses.

The DoS icmpsmurf sub-function can prevent icmpsmurf attack and those ICMP packets whose destination addresses are broadcast addresses.

The DoS icmpsmurf sub-function can prevent icmpsmurf attack and those IP packets whose destination addresses are broadcast addresses.

Example

The following example shows how to set the global DoS attack prevention function to prevent those IP packets whose source IPs are destination IP addresses.

Switch_config#dos enable ip

The following example shows how to detect illegal TCPflag packets.

Switch_config#dos enable tcpflags

1.1.2. show dos

Syntax

To show all DoS attack prevention functions that users have set, run this command.

show dos

Parameters

None

Default Value

None

Usage Guidelines

EXEC mode

Example

The following example shows how to display all DoS attack prevention functions.

Switch_config#dos enable all
Switch_config#show dos

dos enable icmp

dos enable ip

dos enable l4port

dos enable mac

dos enable tcpflags

dos enable tcpfrag

dos enable tcpsmurf

dos enable icmpsmurf

dos enable ipsmurf

Switch_config#

The following example shows how to set dos enable ip to display the sub-function that users have set.

Switch_config#dos enable ip

Switch_config#show dos

dos enable ip