Configuring Dos Defend

CHAPTERS

This guide applies to:

T1500G-8T v2 or above, T1500G-10PS v2 or above, T1500G-10MPS v2 or above, T1500-28PCT v3 or above, T1600G-18TS v2 or above, T1600G-28PS v3 or above, T1600G-28TS v3 or above, T1600G-52TS v3 or above, T1600G-52PS v3 or above, T1700X-16TS v3 or above, T1700G-28TQ v3 or above, T2500G-10TS v2 or above, T2600G-18TS v2 or above, T2600G-28TS v3 or above, T2600G-28MPS v3 or above, T2600G-28SQ v1 or above, T2600G-52TS v3 or above.

1 Overview

The DoS (Denial of Service) defend feature provides protection against DoS attacks. DoS attacks occupy the network bandwidth maliciously by sending numerous service requests to the hosts. It results in an abnormal service or breakdown of the network.

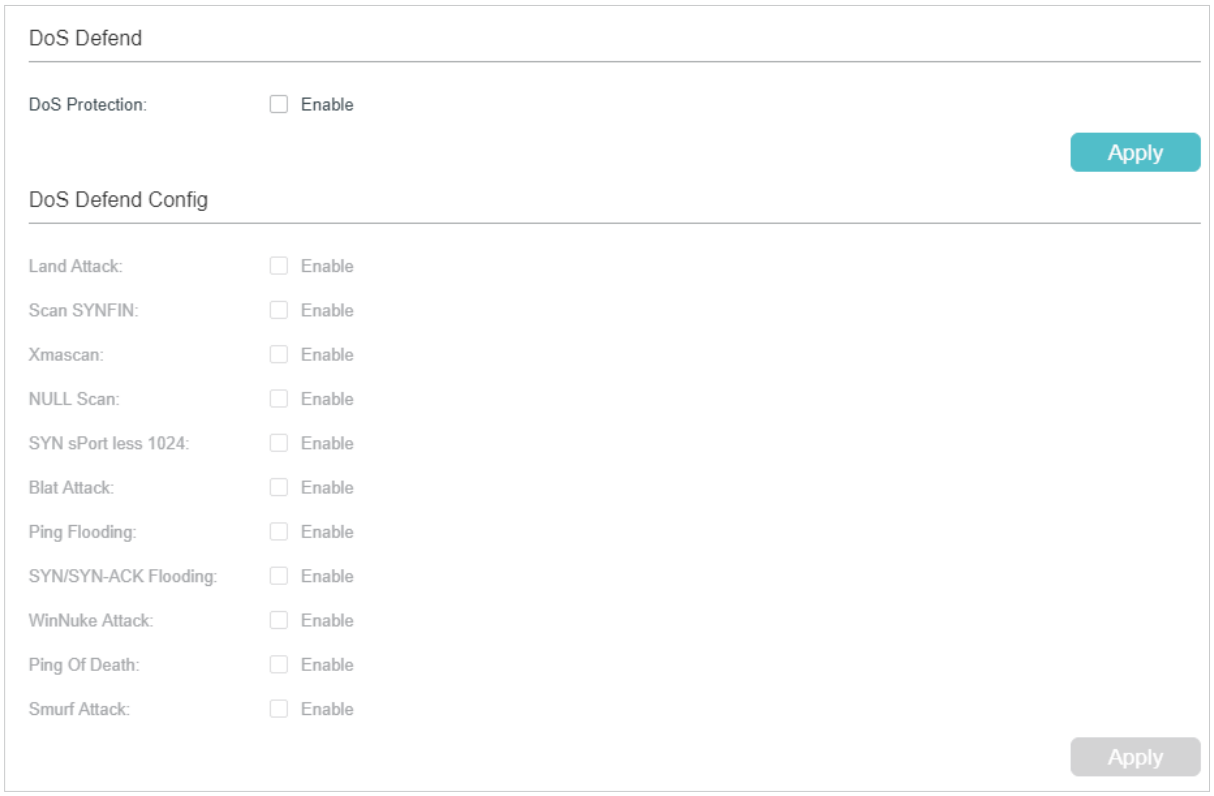
With DoS Defend feature, the switch can analyze the specific fields of the IP packets, distinguish the malicious DoS attack packets and discard them directly. Also, DoS Defend feature can limit the transmission rate of legal packets. When the number of legal packets exceeds the threshold value and may incur a breakdown of the network, the switch will discard the packets.

2 DoS Defend Configuration

2.1 Using the GUI

Choose the menu **SECURITY > DoS Defend** to load the following page.

Figure 2-1 DoS Defend



Follow these steps to configure DoS Defend:

1) In the **DoS Defend** section, enable DoS Protection and click **Apply**.
2) In the **DoS Defend Config** section, select one or more defend types according to your needs and click **Apply**. The following table introduces each type of DoS attack.

Land Attack	The attacker sends a specific fake SYN (synchronous) packet to the destination host. Because both of the source IP address and the destination IP address of the SYN packet are set to be the IP address of the host, the host will be trapped in an endless circle of building the initial connection.
Scan SYNFIN	The attacker sends the packet with its SYN field and the FIN field set to 1. The SYN field is used to request initial connection whereas the FIN field is used to request disconnection. Therefore, the packet of this type is illegal.
Xmascan	The attacker sends the illegal packet with its TCP index, FIN, URG and PSH field set to 1.

NULL Scan	The attacker sends the illegal packet with its TCP index and all the control fields set to 0. During the TCP connection and data transmission, the packets with all control fields set to 0 are considered illegal.
SYN sPort less 1024	The attacker sends the illegal packet with its TCP SYN field set to 1 and source port smaller than 1024.
Blat Attack	The attacker sends the illegal packet with the same source port and destination port on Layer 4 and with its URG field set to 1. Similar to the Land Attack, the system performance of the attacked host is reduced because the Host circularly attempts to build a connection with the attacker.
Ping Flooding	The attacker floods the destination system with Ping packets, creating a broadcast storm that makes it impossible for the system to respond to legal communication.
SYN/SYN-ACK Flooding	The attacker uses a fake IP address to send TCP request packets to the server. Upon receiving the request packets, the server responds with SYN-ACK packets. Since the IP address is fake, no response will be returned. The server will keep on sending SYN-ACK packets. If the attacker sends overflowing fake request packets, the network resource will be occupied maliciously and the requests of the legal clients will be denied.
WinNuke Attack	Because the Operation System with bugs cannot correctly process the URG (Urgent Pointer) of TCP packets, the attacker sends this type of packets to the TCP port139 (NetBIOS) of the host with the Operation System bugs, which will cause the host with a blue screen.
Ping of Death	**Note**: Only T1500&T1500G&T1600G series switch supports this feature. Ping of Death attack means that the attacker sends abnormal ping packets larger than 65535 bytes to cause system crash on the target computer.
Smurf Attack	**Note**: Only T1500&T1500G&T1600G series switch supports this feature. Smurf attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic.

3) Click **Apply**.

2.2 Using the CLI

Follow these steps to configure DoS Defend:

Step 1	**configure** Enter global configuration mode.

Step 2	**ip dos-prevent** Globally enable the DoS defend feature.
Step 3	**ip dos-prevent type {** land | scan-synfin | xma-scan | null-scan | port-less-1024 | blat | ping-flood | syn-flood | win-nuke **}** Configure one or more defend types according to your needs. The types of DoS attack are introduced as follows. land: The attacker sends a specific fake SYN (synchronous) packet to the destination host. Because both the source IP address and the destination IP address of the SYN packet are set to be the IP address of the host, the host will be trapped in an endless circle of building the initial connection. scan-synfin: The attacker sends the packet with its SYN field and the FIN field set to 1. The SYN field is used to request initial connection whereas the FIN field is used to request disconnection. Therefore, a packet of this type is illegal. xma-scan: The attacker sends the illegal packet with its TCP index, FIN, URG and PSH field set to 1. null-scan: The attacker sends the illegal packet with its TCP index and all the control fields set to 0. During the TCP connection and data transmission, the packets with all the control fields set to 0 are considered as the illegal packets. port-less-1024: The attacker sends the illegal packet with its TCP SYN field set to 1 and source port smaller than 1024. blat: The attacker sends the illegal packet with the same source port and destination port on Layer 4 and with its URG field set to 1. Similar to the Land Attack, the system performance of the attacked host is reduced because the Host circularly attempts to build a connection with the attacker. ping-flood: The attacker floods the destination system with Ping packets, creating a broadcast storm that makes it impossible for system to respond to legal communication. syn-flood: The attacker uses a fake IP address to send TCP request packets to the server. Upon receiving the request packets, the server responds with SYN-ACK packets. Since the IP address is fake, no response will be returned. The server will keep on sending SYN-ACK packets. If the attacker sends overflowing fake request packets, the network resource will be occupied maliciously and the requests of the legal clients will be denied. win-nuke: An Operation System with bugs cannot process the URG (Urgent Pointer) of TCP packets. If the attacker sends TCP packets to port139 (NetBIOS) of the host with Operation System bugs, it will cause blue screen. ping-of-death: Ping of Death attack means that the attacker sends abnormal ping packets larger than 65535 bytes to cause system crash on the target computer. **Note**: Only T1500&T1500G&T1600G series switch supports this feature. smurf: Smurf attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. **Note**: Only T1500&T1500G&T1600G series switch supports this feature.

Step 4	**show ip dos-prevent** Verify the DoS Defend configuration.
Step 5	**end** Return to privileged EXEC mode.
Step 6	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable the DoS Defend type named land:

Switch#configure

Switch(config)#ip dos-prevent

Switch(config)#ip dos-prevent type land

Switch(config)#show ip dos-prevent

DoS Prevention State: Enabled

Type	Status
----	------
Land Attack	Enabled
Scan SYNFIN	Disabled
Xmascan	Disabled
NULL Scan	Disabled
SYN sPort less 1024	Disabled
Blat Attack	Disabled
Ping Flooding	Disabled
SYN/SYN-ACK Flooding	Disabled
WinNuke Attack	Disabled

Switch(config)#end

Switch#copy running-config startup-config

3 Appendix: Default Parameters

Default settings of Network Security are listed in the following tables.

Table 3-1 DoS Defend

Parameter	Default Setting
DoS Defend	Disabled