Contents

1 Configuring DoS Protection...

1.1 Introduction...1

1.1.1 Overview...1

1.1.2 Principles...1

1.2 Configuration Task Summary...3

1.3 Configuring the Function of Denying Land Attacks...3

1.3.1 Overview...3

1.3.2 Procedure...3

1.4 Configuring the Function of Denying Invalid TCP Packets...4

1.4.1 Overview...4

1.4.2 Procedure...4

1.5 Configuring the Function of Denying Invalid L4 Ports...4

1.5.1 Overview...4

1.5.2 Procedure...4

1.6 Configuring the Function of Denying ICMP Flood Packets...4

1.6.1 Overview...4

1.6.2 Restrictions and Guidelines...4

1.6.3 Procedure...5

1.7 Configuring the Function of Denying SYN Flood Packets...5

1.7.1 Overview...5

1.7.2 Restrictions and Guidelines...5

1.7.3 Procedure...5

1.8 Configuring Attack Packet Statistics.....5

1.8.1 Overview.....5

1.8.2 Restrictions and Guidelines.....5

1.8.3 Procedure.....6

1.9 Monitoring.....6

1 Configuring DoS Protection

1.1 Introduction

1.1.1 Overview

Denial-of-service (DoS) attacks aim to put computers or networks out of service.

DoS attacks are diversified in types and can be implemented in many ways but have one common purpose, that is, prevent victim hosts or networks from receiving, processing, or responding to external requests in time. In particular, in an L2 network, DoS attack packets can be spread in the entire broadcast domain. If hackers maliciously initiate DoS attacks, some operating systems (OSs) may collapse. Orion products support the following anti-DoS attack functions:

- Denying land attacks
- Denying invalid Transmission Control Protocol (TCP) packets
- Denying invalid L4 ports
- Denying null scan attacks
- Denying Internet Control Message Protocol (ICMP) flood packets
- Denying TCP synchronization (SYN) flood packets

1.1.2 Principles

1. Denying Land Attacks

In a land attack, the attacker sets the source and destination IP addresses in an SYN packet to the same address of the target host. Consequently, the attacked host will be trapped in an infinite loop or even collapse when attempting to set up a TCP connection with itself.

When the function of denying land attacks is enabled, the device checks packets based on characteristics of land packets (that is, SYN packets with the same source and destination IP addresses), and discards invalid packets.

2. Denying Invalid TCP Packets

There are several flag fields in the TCP packet header:

- SYN: Connection establishment flag. A TCP SYN packet sets this flag to **1** to request establishment of a connection.
- ACK: Acknowledgment flag. In a TCP connection, this field must be available in every packet (except the first packet, that is, the TCP SYN packet) as the acknowledgment of the previous packet.
- FIN: Finish flag. When a host receives the TCP packet with the FIN flag, the host disconnects the TCP connection.
- RST: Reset flag. When the IP protocol stack receives a TCP packet that contains a non-existent destination port, it responds with a packet carrying the RST flag.

- PSH: This flag notifies the protocol stack to submit TCP data to the upper-layer program for processing as soon as possible.

In invalid TCP packets, flag fields are set improperly to consume processing resources of hosts or even collapse the system. The following lists several common methods for setting flag fields in invalid TCP packets:

- TCP packets with both the SYN and FIN flags

  Normally, a TCP packet cannot contain both the SYN and FIN flags. In addition, RFC does not stipulate how the IP protocol stack should process such invalid packets containing both the SYN and FIN flags. The protocol stack of each OS may process such packets in different ways. Attackers can use this feature to send packets containing both the SYN and FIN flags to identify the OS type and initiate attacks on this OS.

- TCP packets without any flag

  Normally, a TCP packet contains at least one of the five flags, including SYN, FIN, ACK, RST, and PSH. The first TCP packet (TCP SYN packet) must contain the SYN flag, and the subsequent packets contain the ACK flag. Based on such assumptions, some protocol stacks do not specify the method for processing TCP packets without any flag and may collapse if such TCP packets are received. Attackers use this feature to initiate attacks on target hosts.

- TCP packets with the FIN flag but without the ACK flag

  Normally, except the first packet (TCP SYN packet), all other packets, including the packets with the FIN flag, contain the ACK flag. Some attackers may send TCP packets with the FIN flag but without the ACK flag to the target hosts, causing breakdown of the target hosts.

- TCP packets with the SYN flag and the source port ID set to a value between 0 and 1023

  Port IDs 0 to 1023 are known port IDs allocated by the Internet Assigned Numbers Authority (IANA). In most systems, these port IDs can be used only by the system (or root) processes or programs run by privileged users. These ports (0–1023) cannot be used as the source ports in the first TCP packets (with the SYN flag) sent by clients.

  When the function of denying invalid TCP packets is enabled, the device checks packets based on characteristics of invalid TCP packets and discards invalid TCP packets.

3. Denying Invalid L4 Ports

Attackers send packets in which the IP address and L4 port ID are the same as those of the target host to the target host. As a result, the target host sends TCP connection setup requests to itself. Under such attacks, resources of the target host will soon be exhausted and the system will collapse.

When the function of denying invalid L4 ports is enabled, the device checks the L4 source port ID and destination port ID in the packets. If they are the same, the device discards the packets.

4. Denying Null Scan Attacks

Attackers send TCP packets without any flag to the target host IP address. Some OSs proactively respond with RST packets. In this case, attackers can obtain enabled ports. By sending TCP packets without any flag in the data packet header, attackers can generate invalid data packets based on RFC 793 to initiate null scan attacks. The expected behavior in RFC 793 is that TCP packets with incorrect state are sent to enabled ports of the destination host, which will be discarded by the destination host, and TCP packets with the status flag are sent to disabled ports of the destination host, and the destination host will response with RST packets. Attackers may send data packets of some types that violate rules (non-synchronized TCP connection or TCB disallowed) to scan disabled ports and use RST data packets to detect disabled ports.

The new RFC standard can filter out all TCP packets without a flag. Denying null scan attacks is to discard TCP packets without any TCP flag. This effectively prevents attackers from obtaining the disabling status of ports through null scan and initiating subsequent attacks.

5. Denying ICMP Flood Packets

ICMP flood is a distributed denial-of-service (DDoS) attack, which sends many ping packets to the target host in a short period of time to consume resources of the host. After resources of the host are used up, the host will collapse or cannot provide services.

6. Denying SYN Flood Packets

SYN flood is the commonest DDoS attack and also a typical DoS attack in networks. By exploiting TCP implementation defects, it sends many attack packets with forged source addresses to network service ports, which may cause the half-open connection queue of the target server being occupied and prevent other legitimate users from accessing the server.

1.2 Configuration Task Summary

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring the Function of Denying Land Attacks
- Configuring the Function of Denying Invalid TCP Packets
- Configuring the Function of Denying Invalid L4 Ports
- Ошибка: источник перекрёстной ссылки не найден
- Configuring the Function of Denying ICMP Flood Packets
- Configuring the Function of Denying SYN Flood Packets
- Configuring Attack Packet Statistics

1.3 Configuring the Function of Denying Land Attacks

1.3.1 Overview

If the function of denying land attacks is enabled, the device checks packets based on characteristics of land packets (that is, SYN packets with the same source and destination IP addresses), and discards invalid packets.

1.3.2 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable the function of denying land attacks.

ip deny land

The function of denying land attacks is disabled by default.

1.4 Configuring the Function of Denying Invalid TCP Packets

1.4.1 Overview

When the function of denying invalid TCP packets is enabled, the device checks packets based on characteristics of invalid TCP packets and discards invalid TCP packets.

1.4.2 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable the function of denying invalid TCP packets.

ip deny invalid-tcp

The function of denying invalid TCP packets is disabled by default.

1.5 Configuring the Function of Denying Invalid L4 Ports

1.5.1 Overview

When the function of denying invalid L4 ports is enabled, the device checks the L4 source port ID and destination port ID in the packets. If they are the same, the device discards the packets.

1.5.2 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable the function of denying invalid L4 ports.

ip deny invalid-l4port

The function of denying invalid L4 ports is disabled by default.

1.6 Configuring the Function of Denying ICMP Flood Packets

1.6.1 Overview

After the function of denying ICMP flood packets is enabled, the device will limit the rate of ICMP packets entering the network and prevent resources of the internal server being excessively consumed by ICMP attack packets.

1.6.2 Restrictions and Guidelines

- Typically, this function is configured on devices connected to the server.
- After this function is enabled, only the rate of bypassing ICMP packets is limited, and ICMP packets sent

from the local device to the CPU are not affected.

1.6.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable the function of denying ICMP flood packets.

ip defense icmp-flood *rate-limit*

The function of denying ICMP flood packets is disabled by default.

1.7 Configuring the Function of Denying SYN Flood Packets

1.7.1 Overview

After the function of denying SYN flood packets is enabled, the device will limit the rate of SYN packets entering the network and prevent resources of the internal server being excessively consumed by SYN attack packets.

1.7.2 Restrictions and Guidelines

- Typically, this function is configured on devices connected to the server.
- After this function is enabled, only the rate of bypassing TCP SYN packets is limited, and TCP SYN packets sent from the local device to the CPU are not affected.

1.7.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable the function of denying TCP SYN flood packets.

ip defense syn-flood *rate-limit*

The function of denying TCP SYN flood packets is disabled by default.

1.8 Configuring Attack Packet Statistics

1.8.1 Overview

After the attack packet statistics function is enabled, statistics are collected for null scan packets entering the network and bypassing ICMP/SYN flood packets, and interfaces are provided to display permitted and discarded packets on the forwarding plane.

1.8.2 Restrictions and Guidelines

- Typically, this function is configured on devices connected to the server.

- Enabling this function will occupy many underlying hardware resources. Therefore, this function is disabled by default.
- The device discards null scan attack packets directly. Therefore, only the count of discarded packets will be updated.
- The function can collect statistics of null scan packets and bypass ICMP/SYN flood packets only.

1.8.3 Procedure

(1)Enter the privileged EXEC mode.

```
enable
```

(2)Enter the global configuration mode.

```
configure terminal
```

(3)Enable the function of collecting statistics of null scan packets and ICMP/SYN flood packets.

```
ip ddos counter enable
```

The function of collecting statistics of null scan packets and ICMP/SYN flood packets is disabled by default.

1.9 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1Monitoring

Command	Purpose
show ip defense icmp-flood	Displays the status of the function of denying ICMP flood packets.
show ip defense syn-flood	Displays the status of the function of denying TCP SYN flood packets.
show ip deny land	Displays the status of the function of denying land attacks.
show ip deny invalid-tcp	Displays the status of the function of denying invalid TCP packets.
show ip deny invalid-l4port	Displays the status of the function of denying invalid L4 ports.
show ip deny	Displays the status of all anti-DoS attack functions.