IP-Attack Prevention Configuration

Table of Contents

Chapter 1 IP-Attack Prevention Configuration

1.1 Overview

To ensure the reasonable use of network bandwidth, the company's switches provide the IP-Attack Prevention function to prevent malicious IP traffic from occupying the network bandwidth. For the common attacks at present, communication restrictions are imposed on hosts that send a large number of ICMP, IGMP or IP packets over a period of time, and no network services are provided to these hosts. This configuration can prevent the problem of network congestion caused by malicious packets occupying a large amount of network bandwidth.

1.2 IP-Attack Prevention Configuration Task List

When the number of IGMP, ICMP, or IP packets sent by a host within any specified time interval exceeds the threshold, we assume that an attack occurs on the network.

You can choose the anti-attack types (ICMP, IGMP or IP), the application ports and attack detection parameters. The configuration tasks inlclude:

- Configure IP-Attack Prevention type
- Configure IP attack detection parameters

1.3 IP-Attack Prevention Configuration

1.3.1 Configuring IP attack detection parameters

Command	Purpose
ip verify log-enable	Enable/disable attack detection system log
ip verify filter *time*	When the attack source is identified, stop service for them. The adjustment unit is seconds, the default time is 180 seconds

1.3.2 Configuring the IP attack detection type

Command	Purpose
ip verify icmp ping-flood *value*	Limit ping packet reception. **value** means the detection threshold.
ip verify icmp ping-sweep *time*	Limit ping scanning. **time** means detection period, unit is second.
ip verify tcp syn-flood *value*	Restrict tcp syn packet reception. **value** means the detection threshold.

ip verify tcp syn-sweep *time*	Limit tcp syn port scanning. **time** means detection period, unit is second.
ip verify tcp fin-scan *time*	Limit tcp stealth fin scanning. **time** means detection period, unit is second.
ip verify tcp rst-flood *value*	Limit tcp rst packet reception. **value** means the detection threshold.
ip verify udp udp-flood *value*	Limit udp packet reception. **value** means the detection threshold.
ip verify udp udp-sweep *time*	Limit udp scanning. **time** means detection period, unit is second.
ip verify attack Xmas-Tree *time*	Filter Xmas-Tree scanning attacks. **time** means detection period, unit is second.
ip verify attack Null-scan *time*	Filter Null scanning attacks. **time** means detection period, unit is second.
ip verify attack Land	Filter Land attacks.
ip verify attack Smurf	Filter Smurf attacks.
ip verify attack WinNuke	Filter WinNuke attacks.
ip verify attack TearDrop	Filter TearDrop attacks.
ip verify attack Fraggle	Filter Fraggle attacks.

1.3.3 Enabling IP-Attack Prevention function

When all the parameters for anti-attack are configured, the anti-attack function can be activated. It should be noted that the attack prevention function takes up a small amount of processor space.

Command	Purpose
ip verify enable	Enable/disable attack detection.

With no form of this command is used, the attack detection is disabled, and all blocked attack sources are unblocked.

1.4 Examples of IP-Attack Prevention Configuration

To enable the port scanning anti-attack, you can configure as follows. When any host scans the port more than one scanning unit in any 15 seconds, it is considered as an attack and block network service for 10 minutes.

ip verify icmp ping-sweep 15

ip verify tcp syn-sweep 15

ip verify udp udp-sweep 15

ip verify enable

ip verify log-enable

ip verify filter 600

Chapter 2 IP Attacks Prevention against Direct Network Segment Scanning

2.1 Overview

To prevent malicious attacks from sending a large number of scan packets to the directly connected route, the switch creates a software cache for unreachable addresses of the directly connected route to increase CPU utilization. The function of IP attacks prevention against direct network segment scanning can deal with attacks to reduce the CPU utilization.

2.2 Configuration task list of IP Attacks Prevention against Direct Network Segment Scanning

When the number of incomplete arps on a switch vlan exceeds a certain number, we think the switch has received an attack from direct network segment scanning.

When the number of unreachable IP packets within any specified time interval exceeds the threshold, we assume that an attack occurs, then record and print to prompt the user.

The user can select the function mode and attack detection parameters of the anti-direct network segment scanning attack. The configuration tasks include:

- Configure detection parameters of IP attacks prevention against direct network segment scanning
- Configure detection types of IP anti-direct network segment scanning detection types

Note:

The **ip verify ip-sweep action rate-limit-attacker** command will override the **ip verify ip-sweep action rate-limit** command, otherwise you need to configure **no ip verify ip-sweep action rate-limit-attacker** first to configure **ip verify ip- sweep action rate-limit**. Time and packet parameters are inherited when overwriting.

2.3 Configuring IP Attacks Prevention against Direct Network Segment Scanning

2.3.1 Configuring detection parameters of IP attacks prevention against direct network segment scanning

Command	Purpose
ip verify filter *time*	When the attack source is identified, stop service for

	the attack source. The adjustment unit is seconds, the default time is 180 seconds.

2.3.2 Configure detection types of IP anti-direct network segment scanning detection types

Command	Purpose
ip verify ip-sweep action rate-limit	Limit the number of IP packets
ip verify ip-sweep action rate-limit *time packets*	Limit the number of ip packets, configure the limited time period and the maximum number of ip packets allowed in this period.
ip verify ip-sweep action rate-limit-attacker	Only limit the number of packets defined as attacker's ip packets.
ip verify ip-sweep action rate-limit-attacker *time packets*	Limit the number of packets defined as attacker's ip packets. Configure the limited time period and the maximum number of ip packets allowed for the source address in the period.
ip verify ip-sweep action no-cache	Prohibit the creation of cache for unknown hosts directly connected to the network segment.

2.3.3 Enable IP Attacks Prevention against Direct Network Segment Scanning

When all the parameters are configured, you can enable the IP attacks prevention against direct network segment scanning. It should be noted that the attack prevention function takes up a small amount of processor space.

Command	Purpose
ip verify ip-sweep detect unknown-host	Enable/disable the anti-attack function for IP scanning of unknown hosts on the directly connected network.

With no form of this command is used, the attack detection is disabled, and all blocked attack sources are unblocked.

2.4 Examples of IP Attacks Prevention against Direct Network Segment Scanning

To enable the IP attacks prevention against direct network segment scanning, you can configure as follows. That is, the detected attacker is only allowed to forward 200 IP packets every two seconds and the cache of unknown direct network segment hosts is prevented. In addition, the entire test result is reset every 10 minutes,

ip verify filter 600

ip verify ip-sweep detect unknown-host

ip verify ip-sweep action no-cache

ip verify ip-sweep action rate-limit 2 200

2.5 Detection Results of IP Attacks Prevention against Direct Network Segment Scanning

Jan 1 00:07:14 Unknown-host (connected network sweep) attack detected

Jan 1 00:07:14 Action rate-limit-attacker is being used.

Jan 1 00:07:14 Action no-cache is being used.

Jan 1 00:07:14 Connected network sweep attacker 100.1.1.2 detected, VLAN 100, port g2/1

Jan 1 00:07:14 [SLOT 2]Connected network sweep attacker 100.1.1.2 detected, VLAN 100, port g2/1

When the anti-direct network segment scanning attack and rate-limit-attacker and action no-cache defense methods are enabled, an attacker's IP network segment scanning attack with port vlan 100, physical port g2/1, and IP address 100.1.1.2 is received, please deal with it as soon as possible.