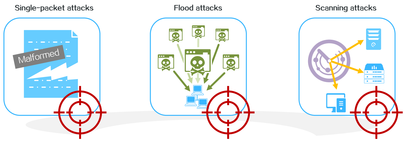
Technical Introduction

Attack detection and prevention

Overview

As an important network security feature, attack detection and prevention enables a device to detect attacks by inspecting arriving packets, and to take prevention actions to protect a private network.

Attack detection and prevention can effectively defense single-packet attacks, flood attacks, and scanning attacks.



Single-packet attacks are also known as malformed packet attacks. An attacker typically launches single-packet attacks by sending protocol-incompliant packets to a device, which causes the target system to malfunction or crash.

An attacker launches a flood attack by sending a large number of forged requests to the victim in a short period of time. The victim is too busy responding to these forged requests to provide services for legal users, and a DoS attack occurs.

Attackers use scanning tools to probe a network, find vulnerable hosts, and discover services that are running on the hosts. Attackers can use the information to launch attacks.

Benefits

Simple configuration

Configuration parameters are included in an attack prevention strategy to facilitate user configuration and management.

Intelligent threshold learning

According to the real-time network traffic, the attack prevention threshold can be adjusted adaptively to improve attack detection accuracy.

Statistics display

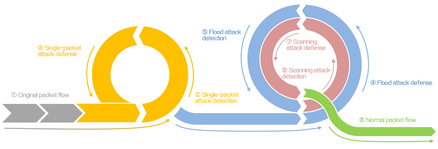
Various types of attack prevention data statistics can be collected for users to know attack prevention status in real time.

Various attack defense

Single-packet attacks, flood attacks, and scanning attacks can be effectively defended.

Process

Single-packet attack defense, flood attack defense, and scanning attack defense each have its own detection and defense processes, as shown in the following figure.



Mechanism

Single-packet attack detection

Typically, packets sent by a single-packet attacker have fixed signatures. The device can identify the attack packets if the packets match the signatures.

Single-packet attack prevention

The device drops single-packet attack packets and generates single-packet attack logs.

The device can detect and prevent single-packet attacks of the following types:

ICMP redirect, ICMP unreachable, ICMP type, ICMPv6 type, Land, Large ICMP, Large ICMPv6, IP option, IP option abnormal, Fragment, Impossible, Tiny fragment, Smurf, TCP Flag, Traceroute, Winnuke, UDP Bomb, UDP Snork, UDP Fraggle, Teardrop, Ping of death, and IPv6 ext-header.

Flood attack detection

The device determines that a flood attack occurs when the rate of packets originated from or destined for an IP address reaches the threshold and the attack ends when the packet rate drops below the threshold.

Flood attack prevention

The device drops the packets or perform client verification, and generates flood attack logs.

Tips: Client verification is a proactive prevention feature. Based on the Connect-Challenge-Respond mechanism, the device initiatively verifies the validity of the packet source and drops packets from illegal clients.

The device can detect and prevent flood attacks of the following types:

SYN flood attack, ACK flood attack, SYN-ACK flood attack, FIN flood attack, RST flood attack, UDP flood attack, ICMP flood attack, ICMPv6 flood attack, DNS flood attack, DNS reply flood attack, HTTP flood attack, and SIP flood attack.

Scanning attack detection

The device monitors the rate of connections to the target system initiated by network users. If the device detects that the change frequency of the destination IP or the destination port of a client exceeds the threshold, it determines that the client launches a scanning attack.

Scanning attack prevention

The device drops scanning attack packets or blocks the packet source, and generates scanning attack logs.

Tips: If the device blocks a packet source, it drops subsequent packets from the source.

The device can detect and prevent IP sweep attack and port scanning attack.

Application scenarios

Device self-protection

Apply attack and protection on the device to protect the device against various cyber attacks targeting on the device itself.

Internal server protection

Apply attack and protection on interfaces or security zones on the device to protect internal servers and hosts from various cyber attacks.