# Introduction to Attack Defense

There are various inevitable attacks in networks, such as compromise or sabotage of servers, sensitive data theft, service intervention, or even direct network device sabotage that causes service anomaly or interruption. Security gates, belonging to a category of network security devices, must be designed with attack defense functions to detect various types of network attacks, and take appropriate actions to protect Intranet against malicious attacks, thus assuring the normal operation of the Intranet and systems.

System provides attack defense functions based on security zones, and can take appropriate actions against network attacks to assure the security of your network systems.

## IP Address Spoofing

IP address spoofing is a technology used to gain unauthorized accesses to computers. An attacker sends packets with a forged IP address to a computer, and the packets are disguised as if they were from a real host. For applications that implement validation based on IP addresses, such an attack allows unauthorized users to gain access to the attacked system. The attacked system might be compromised even if the response packets cannot reach the attacker.

## Land Attack

During a Land attack, an attacker will carefully craft a packet and set its source and destination address to the address of the server that will be attacked. In such a condition the attacked server will send a message to its own address, and this address will also return a response and establish a Null connection. Each of such connections will be maintained until timeout. Many servers will crash under Land attacks.

## Smurf Attack

Smurf attacks consist of two types: basic attack and advanced attack. A basic Smurf attack is used to attack a network by setting the destination address of ICMP ECHO packets to the broadcast address of the attacked network. In such a condition all the hosts within the network will send their own response to the ICMP request, leading to network congestion. An advanced Smurf attack is mainly used to attack a target host by setting the source address of ICMP ECHO packets to the address of the attacked host, eventually leading to host crash. Theoretically, the more hosts in a network, the better the attacking effect will be.

## Fraggle Attack

A fraggle attack is basically the same with a smurf attack. The only difference is the attacking vector of fraggle is UDP packets.

## WinNuke Attack

A WinNuke attack sends OOB (out-of-band) packets to the NetBIOS port (139) of a Windows system, leading to NetBIOS fragment overlap and host crash. Another attacking vector is ICMP fragment. Generally an ICMP packet will not be fragmented; so many systems cannot properly process ICMP fragments. If your system receives any ICMP fragment, it's almost certain that the system is under attack.

## SYN Flood

Due to resource limitations, a server will only permit a certain number of TCP connections. SYN Flood just makes use of this weakness. During the attack an attacker will craft a SYN packet, set its source address to a forged or non-existing address, and initiate a connection to a server. Typically the server should reply the SYN packet with SYN-ACK, while for such a carefully crafted SYN packet, the client will not send any ACK for the SYN-ACK packet, leading to a half-open connection. The attacker can send large amount of such packets to the attacked host and establish equally large number of half-open connections until timeout. As a result, resources will be exhausted and normal accesses will be blocked. In the environment of unlimited connections, SYN Flood will exhaust all the available memory and other resources of the system.

## ICMP Flood and UDP Flood

An ICMP Flood/UDP Flood attack sends huge amount of ICMP messages (such as ping)/UDP packets to a target within a short period and requests for response. Due to the heavy load, the attacked target cannot complete its normal transmission task.

## IP Address Sweep and Port Scan

This kind of attack makes a reconnaissance of the destination address and port via scanners, and determines the existence from the response. By IP address sweep or port scan, an attacker can determine which systems are alive and connected to the target network, and which ports are used by the hosts to provide services.

## Ping of Death Attack

Ping of Death is designed to attack systems by some over-sized ICMP packets. The field length of an IP packet is 16 bits, which means the max length of an IP packet is 65535 bytes. For an ICMP response packet, if the data length is larger than 65507 bytes, the total length of ICMP data, IP header (20 bytes) and ICMP header (8 bytes) will be larger than 65535 bytes. Some routers or systems cannot properly process such a packet, and might result in crash, system down or reboot.

**Related Topics**:

- Configuring Attack Defense