

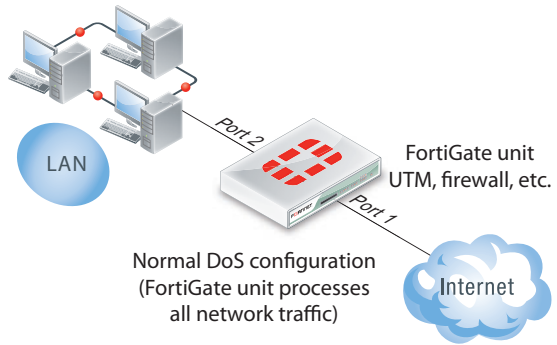


Denial of Service (DoS) Protection

FortiOS DoS protection analyzes network traffic for network-based denial of service attacks and takes action to prevent attacks from affecting network performance

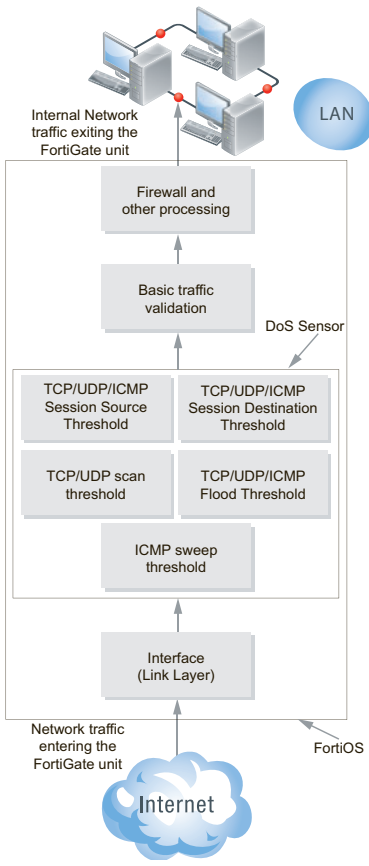
Denial of Service

A denial of service is the result of an attacker sending an abnormally large amount of network traffic to a target system. During a DoS attack, a server can be flooded with far more traffic than it can handle. This traffic flood slows down the server, effectively blocking legitimate users. The most common example of a DoS attack is a distributed denial of service (DDoS) attack, in which an attacker directs a large number of computers to attempt apparently normal access of the target system using standard access methods. If enough access attempts are made, the server is overwhelmed and unable to service genuine users. The attacker does not gain access to the target system, but the target server is not accessible to anyone else.



FortiOS DoS protection, a complement to signature-based IPS protection, helps to prevent these types of attacks. FortiOS DoS uses network traffic anomaly detection to protect a network when the network traffic, in the form of DoS attacks, is used as a weapon.

DoS Protection in FortiOS



FortiOS DoS protection identifies traffic that has the potential to cause a DoS attack by looking for specific traffic anomalies. Traffic anomalies that can cause DoS attacks include TCP syn floods, UDP and ICMP floods, TCP port scans, TCP, UDP, and ICMP session attacks, and ICMP sweep attacks. When anomalous traffic is identified, FortiOS can block the traffic when it reaches a configured threshold. Only the traffic identified as part of a DoS attack is blocked; connections from legitimate users are identified and processed normally.

FortiOS DoS protection can also operate in out-of-band mode (also called sniffer mode or one-arm mode) similar to an intrusion detection system (IDS), detecting attacks and logging them but not blocking them. Blocking offending traffic provides the most protection, but monitoring potentially offending traffic can provide useful information about attacks or potential attacks affecting traffic flow.

To minimize the affect of a DoS attack on FortiOS system performance, FortiOS applies DoS protection very early in its traffic processing sequence. In fact, DoS protection is the first step for packets after they are received by a FortiGate interface. This means that potential DoS attacks are detected and blocked before the packets are possessed by other FortiOS systems.

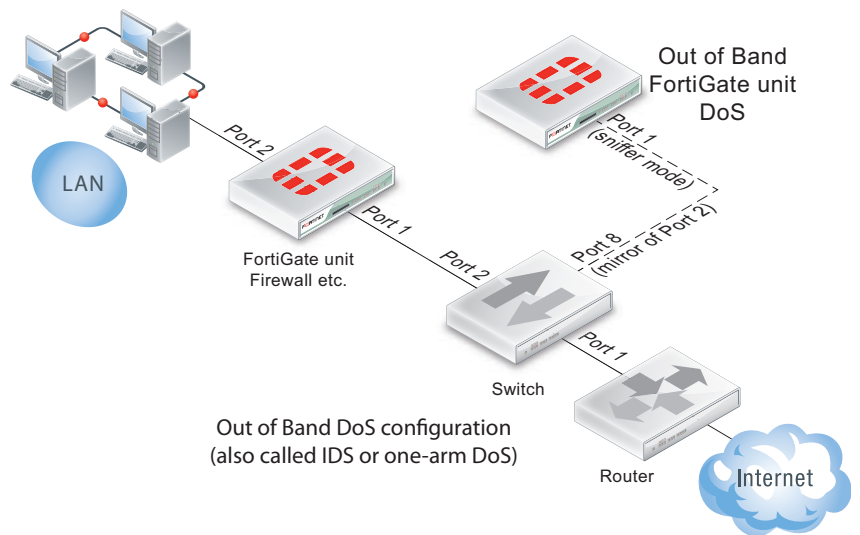
DoS sensor

FortiOS DoS sensors protect networks against DoS attacks by limiting anomalous traffic to thresholds that can be customized for any traffic flow on any network. FortiOS DoS protection keeps the FortiGate unit and the networks, including the network servers that it is protecting, operating while under attack.

DoS sensors can contain a variety of different attack patterns, providing a greater range of detection for DoS attacks.

DoS sensors specify the traffic anomalies to look for, including the threshold at which each should be considered an attack. When the packet rate for an anomaly exceeds its threshold, the FortiOS DoS protection system considers the packets to be part of an attack. FortiOS DoS protection then blocks all packets causing the attack or, if configured, only blocks the packets that exceed the threshold.

The thresholds are set in the DoS sensor along with the action to take when a threshold is exceeded. DoS sensors are added to DoS policies matching traffic according to source interface, source and destination address, and service. DoS policies can be used to apply DoS protection to all traffic or just traffic to or from specific IP addresses. The thresholds can be customized in each sensor to fine tune DoS performance for the traffic being analyzed by the sensor.



DoS policies

DoS policies are configured to keep track of certain traffic patterns and attributes and will stop traffic that displays those attributes. DoS policies are also known as anomaly thresholds, and are used to apply DoS sensors to network traffic based on the FortiGate interface it is entering, as well as the source and destination addresses.

DoS policies affect only incoming traffic on a single interface and you can limit a DoS policy even further by specifying source address, destination address, and service.

The FortiGate unit processes DoS policies first, before any other firewall policies, but in their own respective order. Since DoS policies are processed first, this provides a very efficient defence that uses few resources.

Out-of-band sniffer mode

Most commonly, DoS protection is enabled on a FortiGate unit that connects a private network or DMZ network to the Internet or a FortiWiFi unit that connects a wireless LAN to an internal network and to the Internet. All traffic from the Internet or from the wireless LAN passes through the FortiGate or FortiWiFi unit where DoS protection can be applied.

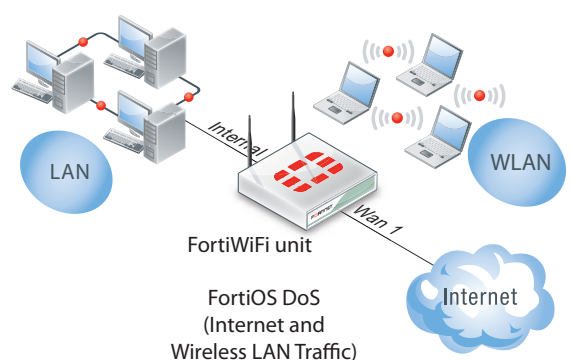
DoS protection can also be deployed out-of-band in sniffer mode, also called one-arm mode. In this mode, DoS protection operates as an Intrusion Detection System (IDS), detecting attacks and reporting them but not taking any action against them. In sniffer mode, the FortiGate unit does not process network traffic. Instead a FortiGate interface operates in sniffer mode and is connected to a spanning or mirrored port of a switch that processes all of the traffic to be analyzed.

The spanning or mirrored switch port sends a copy of the switch traffic to the FortiGate interface operating in sniffer mode where it is analyzed. If a DoS attack is detected, FortiOS records log messages and sends alerts to system administrators. Since its out-of-band, IDS scanning does not affect network performance and network traffic is not affected if the IDS fails or goes offline.

DoS syn proxy: hardware acceleration

Fortinet Security Processing (SP) modules such as the CE4, XE2, and FE8 include a proxy-like function for TCP syn flood protection. The proxy offloads detection and blocking of TCP syn flood attacks to the SP module. The result is an improvement in TCP syn flood protection performance and capacity as well as an overall system performance improvement because TCP syn flood protection is offloaded to the SP module.

The SP module with proxy enabled increases a FortiGate unit's capacity to protect against TCP syn flood attacks while minimizing the effect of the attack on overall FortiGate unit and network performance.



Typically, a TCP syn flood attack involves multiple infected computers on the Internet simultaneously attempting to connect to a target server. These attacking computers request a connection, but then do not respond to the reply, leaving the partially open connection to time out on the server. This time out can take minutes. In the meantime, more and more connections are started and left incomplete. Normally, an unprotected server can keep track of a large, but limited number, of connections. But, as the number of open connections increases, the server may not be able to service new ones. As long as the attack continues, the target server can be so busy that it remains inaccessible. Even as the incomplete connections begin to time-out, the attacking computers open new connections and leave them incomplete, continuing the attack.

