WHITE PAPER

FortiGate DoS Protection

Block Malicious Traffic Before It Affects Critical Applications and Systems

Abstract: Denial of Service (DoS) attacks have been a part of the internet landscape for years. This white paper describes common DoS techniques, explains the technology integrated into every FortiGate consolidated security platform that helps in blocking DoS attacks, and offers suggestions on how to prevent an organization's network from being used to attack another organization.

Introduction

Denial of Service (DoS) attacks are nothing new—they have been part of the network security environment for years. There have been some high profile DoS attacks recently, many motivated by political or economic events. Whether wishing to conduct cyberwarfare or extract revenge over a corporation's actions, attackers today are deploying fundamentally the techniques as those employed over a decade ago. Recent changes in the threat landscape have made it likely that DoS attacks will continue to strike, and organizations need to deploy protection before they become a target.

During a DoS attack, an attacker floods a server with more traffic than it can accommodate. This deluge blocks legitimate users from accessing services and applications on the targeted server or network. The goal of the attack is not to penetrate a network and compromise a system, but overwhelm the network and prevent legitimate users from gaining access.

With the ascendance of Botnets and Crimeware-as-a-Service in the threat landscape, the ability to employ a botnet to launch a DoS attack is relatively simple. Those individuals wishing to launch a DoS attack can easily rent a Botnet and launch an attack against a target with little more than a credit card and cursory information about the target network.

The most common DoS attack is a distributed denial of service (DDoS) attack, in which an attacker directs a large number of computers to attempt to connect to the target system using standard access methods. The attack succeeds simply by denying others access to the target system.

DoS Attack Methods

Here are examples of several of the more common DoS attacks against which organizations need to protect themselves:

- **TCP SYN Floods**: A SYN packet is part of the well-known three-way handshake used to establish a connection using TCP:
    1. A client requests a connection with a server by sending a SYN packet
    2. The server responds with a SYN-ACK packet
    3. The client responds with an ACK packet, which establishes the connection between the two systems

  A SYN flood sends a succession of SYN requests to a target's system from hundreds or thousands of compromised systems, causing the target system to respond with SYN-ACKs. The target server consumes system resources while it waits for the ACKs from the requesting clients. The requestors never respond, and eventually the target of the attack stops answering requests for new connections, thus ignoring legitimate traffic.

- **UDP and ICMP Floods:** Unlike TCP, UDP is a connectionless protocol and does not set up a connection to transfer data. A UDP Flood occurs when multiple systems send a target server UDP packets to random ports.

  When it receives a UDP packet, the targeted system performs the following:

  1. Check for the application listening at that port;
  2. See that no application listens at that port;
  3. Reply with an ICMP Destination Unreachable packet.

  If the attacking systems generate a high quantity of UDP packets to ports on the targeted system, the targeted system will be unavailable to respond.

- **ICMP Sweep Attacks:** Also known as a Ping Sweep attack, an ICMP sweep attack sends multiple ICMP ECHO requests to a targeted host. As each ICMP packets solicits a reply from the targeted system, it prevents the targeted system from being able to receive legitimate traffic.

DoS Detection within FortiGate Platforms

FortiGate consolidated security platforms provide integrated DoS protection to reduce the effects of a DoS attack. The DoS Sensor included in the FortiOS operating system, uses network traffic anomaly detection to identify a DoS attack. It detects and drops DoS packets before requiring firewall policy look-ups or engaging any content scanning, thus avoiding any effect on processing-intensive protective services.

How DoS Protection Works

The DoS Sensor looks for specific traffic anomalies and identifies traffic that has the potential to cause a DoS attack. It can detect 12 types of network anomalies: TCP SYN floods, UDP and ICMP floods, UDP scans, TCP port scans, TCP, UDP, and ICMP source and destination session attacks, and ICMP sweep attacks. Denial of Service (DoS) policies, also known as anomaly thresholds, apply DoS sensors to network traffic based on the FortiGate interface it is entering, as well as the source and destination addresses.

As traffic enters the FortiGate interface, the DoS policy is applied first to determine whether the traffic is genuine or an attack (see figure 1). If it is genuine, the packets are forwarded to the normal firewall policies and applied as required. If the FortiGate unit determines the traffic is a DoS attack, the policy is applied as configured in the DoS sensor.

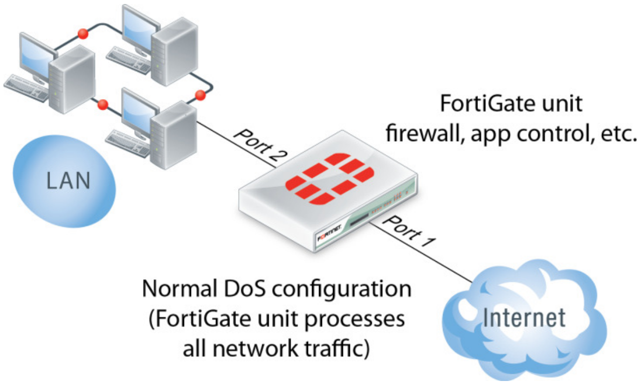

Figure 1: All FortiGate platforms include core security functions like application control, VPN, IPS, and web content filtering, as well as DoS protection.

When it identifies anomalous traffic, FortiOS can block the traffic when it reaches a user-configured threshold. It blocks only the traffic it identifies as part of a DoS attack, enabling it to continue to process legitimate traffic and maintain availability of essential services. To accelerate its ability to detect the threats and minimize any effect of a DoS attack on FortiGate system performance, FortiOS applies DoS protection as the first step in the traffic processing sequence (see Figure 2). This placement minimizes the effect of any DoS attack, as it eliminates the malicious packets before being processed by other FortiOS systems.

FortiOS DoS sensors apply the DoS protection by specifying the traffic anomalies and traffic thresholds to monitor. When the packet rate for an anomaly exceeds its threshold, the DoS protection system considers the packets to be part of an attack.

For example, in the event of TCP SYN Flood attack, FortiOS examine the SYN packet rate of new TCP connections, including retransmission, to one destination IP address. If this rate exceeds the configured threshold value (measured in packets per second), the FortiGate platform will block the traffic.

For UDP or ICMP Floods, FortiOS examines the packets per second volume of UDP or ICMP traffic to one destination IP address. If it exceeds the threshold values, the FortiGate platform will block the traffic. Likewise, for ICMP Sweep attacks, FortiOS looks at the number of ICMP packets originating from one source IP address. If that number exceeds the packets per second threshold, the FortiGate will block the traffic.

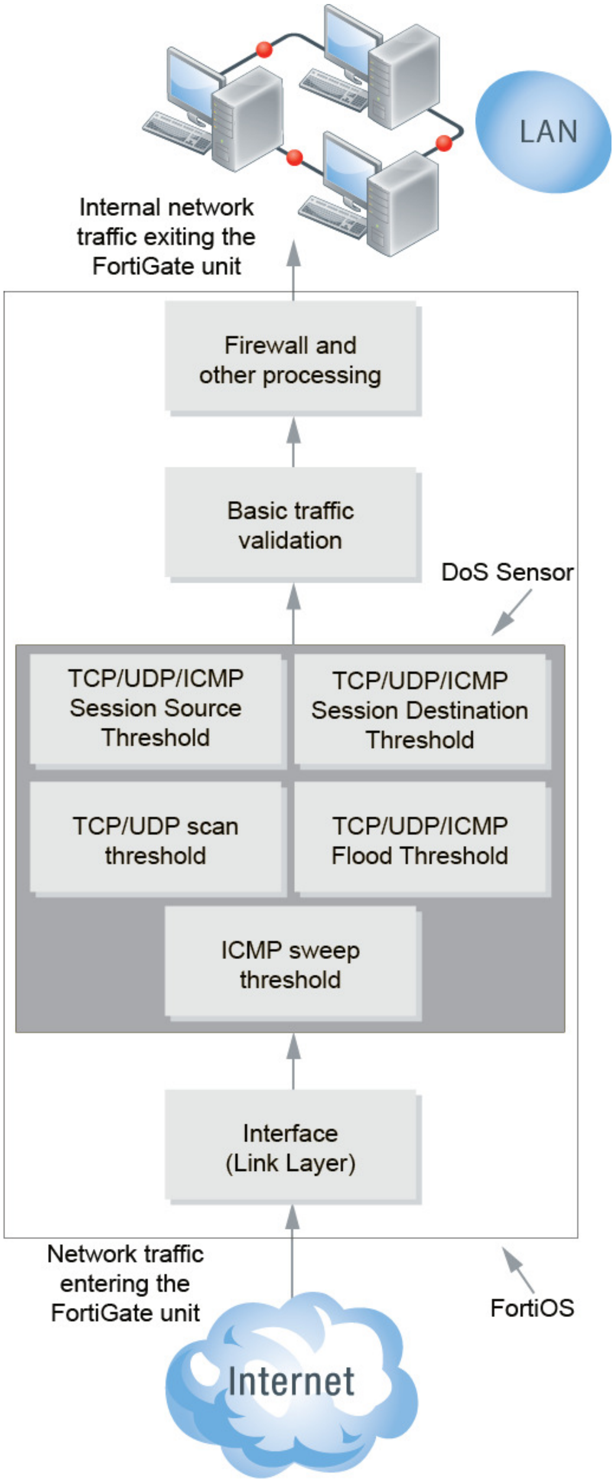
LAN
Internal network traffic exiting the FortiGate unit
Firewall and other processing
Basic traffic validation
DoS Sensor
TCP/UDP/ICMP Session Source Threshold
TCP/UDP/ICMP Session Destination Threshold
TCP/UDP scan threshold
TCP/UDP/ICMP Flood Threshold
ICMP sweep threshold
Interface (Link Layer)
Network traffic entering the FortiGate unit
FortiOS
Internet

Figure 2: FortiGate DoS protection detects and eliminates malicious traffic before it can affect network performance or block access to critical systems

Flexibility and Granular Control

Administrators can configure thresholds in each DoS sensor, along with the action to take when the traffic volume exceeds the threshold. They add DoS sensors to DoS policies (which are similar to firewall policies) which match traffic according to source interface, source and destination address, and service.

Administrators can then apply DoS policies to all traffic or just to traffic to or from specific IP addresses. They can also customize individual thresholds in each sensor to fine tune DoS performance for the traffic being analyzed by the sensor. The FortiOS DoS protection blocks the attack traffic that exceeds the threshold, allowing the server to continue to process legitimate traffic, causing the attack to fail.

In-Band or Out-of-Band

Administrators also have the option of deploying DoS protection in-line or in Out-of-Band mode (also called sniffer-mode or one-arm mode). As shown in Figure 3, out-of-band mode allows organizations to detect and log the anomalous traffic but not block it.

Although blocking DoS traffic provides the best protection for networks, monitoring potentially malicious traffic before enabling blocking can provide very useful information about attacks targeting systems on its network, and the effect on traffic flow once the organization enables blocking via DoS policies.

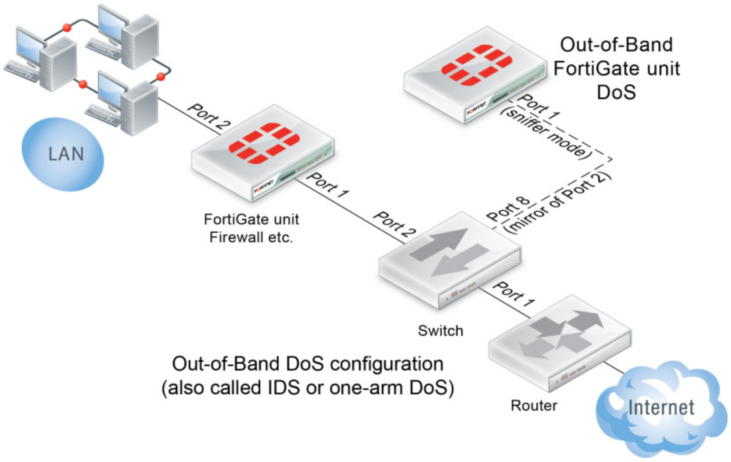

Figure 3: Out-of-Band DoS enables organizations to understand the effect of DoS protection on legitimate traffic and fine tune the thresholds settings before enabling blocking

Adding DoS Protection to a Network

Most commonly, organizations enable DoS protection as follows:

1. On a FortiGate unit that connects a private or DMZ network to the Internet
2. On a FortiWiFi unit that connects a wireless LAN to an internal network and to the Internet

As all traffic from the Internet or from the wireless LAN passes through the FortiGate or FortiWiFi device, it is an ideal location for DoS protection (See Figure 4). Every FortiGate consolidate security platform includes an integrated wireless controller, enabling organizations to apply a single set of security policies to both wired and wireless traffic.

As described above, organizations can also add DoS protection in Out-of-Band in sniffer mode, also called one-arm mode. In this mode, DoS protection operates as a traditional 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 for analysis. If it detects a DoS attack, FortiOS records log messages and sends alerts to system administrators. Since its out-of-band, IDS scanning does not affect network performance.

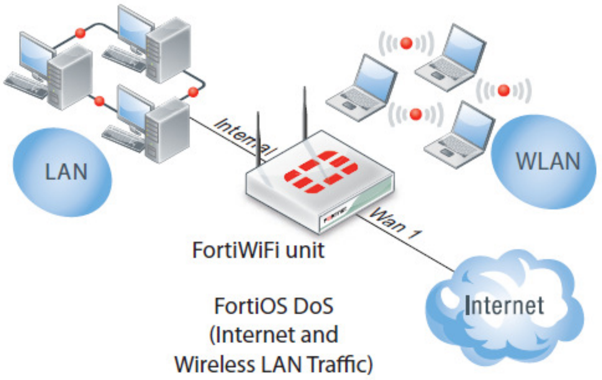

Figure 4: Every FortiGate and FortiWiFi consolidated security platform includes DoS protection, enabling comprehensive protection of LANs and WLANs from a single device

Hardware Acceleration Boosts Protection

Fortinet's Security Processing (SP) modules such as the CE4, FE8, XE2, and XG2, include a proxy-like function for TCP SYN flood protection. The proxy offloads detection and blocking of TCP SYN flood attacks to the to the SP module, to take advantage of Fortinet's custom FortiASIC technology.

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. The result is an improvement in TCP SYN flood protection performance and capacity, as well as an overall system performance improvement because of the offloading of TCPSYN flood protection to the SP module.

FortiGate units with network acceleration hardware, whether built-in or installed in the form of an add-on module, offer a third action for the TCP SYN Flood threshold. Instead of Block and Pass, organizations can choose to Proxy the incomplete connections that exceed the threshold value.

Best Practices

The systems generating the DoS attacks today are likely compromised by bots or other malicious code that allows remote access by an attacker. In addition to the steps outlined above to protect its network from DoS attacks, there are several actions an organization can take to reduce the risk of its systems being compromised and used as a launching pad for attacks. Fortinet's FortiGate consolidated security platforms plus its wide range of specialized security solutions deliver the functionality necessary to deploy the following security best practices:

- **Ingress and egress filtering on the firewall**
  Ingress filtering controls the incoming traffic and protects the network from being attacked. Egress filtering can help contain the botnet activity and keep it from affecting other areas by detecting and blocking the bots' attempt to connect to their command and control server. In addition, Web filtering can block users from visiting malicious sites where their systems would become compromised. *FortiGate platforms include ingress/egress filtering.*

- **Antispam filtering**
  The vast majority of bots are distributed via email, making it essential to deploy antispam technologies to block the malware from making a beachhead in a network. *FortiGate platforms include antispam filtering. FortiMail provides advanced messaging security, including antispam filtering.*

- **Enforce security measures on all systems**
  Having proper system protection is one of the most effective measures against the propagation of the malicious software that turns systems into bots. Endpoint protection can prevent the installation of malicious code on systems. Network Access Control (NAC) can also enforce system hygiene requirements before allowing a system to connect to the network. *Fortinet offers FortiClient endpoint protection for PCs and notebooks, and FortiGate includes key NAC functionality.*

- **Audit Network on a regular basis**
  Regular network audits and vulnerability scans provide essential data regarding systems and applications that may reside on a network without the IT department's knowledge, as well as systems that need patches. These audits and scans identity potential weaknesses in a network, providing the necessary action to plug those holes before the next attack. *FortiAnalyzer, FortiScan and FortiGate platforms can perform vulnerability management scanning to increase an organization's visibility of network status.*

- **Install IPS on the gateway**
  IPS can detect anomalous traffic, enabling an organization to block abnormal network activity and limit the damage from the attack. Implementing IPS at the edge of the network adds an essential layer of protection to the network. An integrated IPS/Firewall gateway reduces the complexity at the edge and provides a single management interface to deploy multiple layers of protection. *FortiGate platforms include IPS functionality*.

Conclusion

The effects of DoS attacks can range from minor annoyance to significant loss of revenue and unavailability of critical business systems. With the ready availability of botnets for rental, anyone with a grudge and a credit card can launch a DoS attack. Organizations need to have DoS protection in place before the attacks occur, to ensure continued availability of core systems and data. Fortinet's wide range of security solutions enables organizations of all sizes to deploy DoS protection quickly and easily, minimizing their exposure to these attacks.

Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and the market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2009 Fortune Global 100. Fortinet's flagship FortiGate product delivers ASIC-accelerated performance and integrates multiple layers of security designed to help protect against application and network threats. Fortinet's broad product line goes beyond UTM to help secure the extended enterprise – from endpoints, to the perimeter and the core, including databases and applications. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

FORTINET

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE
Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE
Fortinet Incorporated
300 Beach Road #20-01, The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784