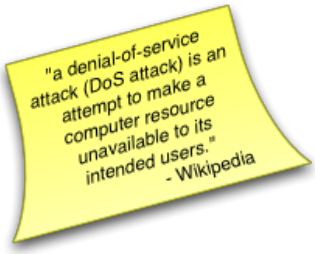
Layer 4 vs Layer 7 DoS Attack

Lori MacVittie, 2008-08-07

Not all DoS (Denial of Service) attacks are the same. While the end result is to consume as much - hopefully all - of a server or site's resources such that legitimate users are denied service (hence the name) there is a subtle difference in how these attacks are perpetrated that makes one easier to stop than the other.

SYN Flood

A Layer 4 DoS attack is often referred to as a SYN flood. It works at the transport protocol (TCP) layer. A TCP connection is established in what is known as a 3-way handshake. The client sends a SYN packet, the server responds with a SYN ACK, and the client responds to ***that*** with an ACK. After the "three-way handshake" is complete, the TCP connection is considered established. It is as this point that applications begin sending data using a Layer 7 or application layer protocol, such as HTTP.



A SYN flood uses the inherent patience of the TCP stack to overwhelm a server by sending a flood of SYN packets and then ignoring the SYN ACKs returned by the server. This causes the server to use up resources waiting a configured amount of time for the anticipated ACK that ***should*** come from a legitimate client. Because web and application servers are limited in the number of concurrent TCP connections they can have open, if an attacker sends enough SYN packets to a server it can easily chew through the allowed number of TCP connections, thus preventing legitimate requests from being answered by the server.

SYN floods are fairly easy for proxy-based application delivery and security products to detect. Because they proxy connections for the servers, and are generally hardware-based with a much higher TCP connection limit, the proxy-based solution can handle the high volume of connections without becoming overwhelmed. Because the proxy-based solution is usually terminating the TCP connection (i.e. it is the "endpoint" of the connection) it will not pass the connection to the server until it has completed the 3-way handshake. Thus, a SYN flood is stopped at the proxy and legitimate connections are passed on to the server with alacrity.

The attackers are generally stopped from flooding the network through the use of SYN cookies. SYN cookies utilize cryptographic hashing and are therefore computationally expensive, making it desirable to allow a proxy/delivery solution with hardware accelerated cryptographic capabilities handle this type of security measure. Servers can implement SYN cookies, but the additional burden placed on the server alleviates much of the gains achieved by preventing SYN floods and often results in available, but unacceptably slow performing servers and sites.

HTTP GET DoS

A Layer 7 DoS attack is a different beast and it's more difficult to detect. A Layer 7 DoS attack is often perpetrated through the use of HTTP GET. This means that the 3-way TCP handshake has been completed, thus fooling devices and solutions which are only examining layer 4 and TCP communications. The attacker ***looks*** like a legitimate connection, and is therefore passed on to the web or application server.

At that point the attacker begins requesting large numbers of files/objects using HTTP GET. They are generally legitimate requests, there are just a lot of them. So many, in fact, that the server quickly becomes focused on responding to those requests and has a hard time responding to new, legitimate requests.

When rate-limiting was used to stop this type of attack, the bad guys moved to using a distributed system of bots (zombies) to ensure that the requests (attack) was coming from myriad IP addresses and was therefore not only more difficult to detect, but more difficult to stop. The attacker uses malware and trojans to deposit a bot on servers and clients, and then remotely includes them in his attack by instructing the bots to request a list of objects from a specific site or server. The attacker might not use bots, but instead might gather enough evil friends to launch an attack against a site that has annoyed them for some reason.

Layer 7 DoS attacks are more difficult to detect because the TCP connection is valid and so are the requests. The trick is to realize when there are multiple clients requesting large numbers of objects at the same time and to recognize that it is, in fact, an attack. This is tricky because there may very well be legitimate requests mixed in with the attack, which means a "deny all" philosophy will result in the very situation the attackers are trying to force: a denial of service.

Defending against Layer 7 DoS attacks usually involves some sort of rate-shaping algorithm that watches clients and ensures that they request no more than a configurable number of objects per time period, usually measured in seconds or minutes. If the client requests more than the configurable number, the client's IP address is blacklisted for a specified time period and subsequent requests are denied until the address has been freed from the blacklist.

Because this can still affect legitimate users, layer 7 firewall (application firewall) vendors are working on ways to get smarter about stopping layer 7 DoS attacks without affecting legitimate clients. It is a subtle dance and requires a bit more understanding of the application and its flow, but if implemented correctly it can improve the ability of such devices to detect and prevent layer 7 DoS attacks from reaching web and application servers and taking a site down.

The goal of deploying an application firewall or proxy-based application delivery solution is to ensure the fast and secure delivery of an application. By preventing both layer 4 and layer 7 DoS attacks, such solutions allow servers to continue serving up applications without a degradation in performance caused by dealing with layer 4 or layer 7 attacks.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com