



August 2003

NetScaler SYN Flood Protection

INTRODUCTION

NetScaler's unique SYN flood protection system, released in May, 2000 is based on an enhanced version of the TCP/IP SYN cookie (see below) approach. This method of protection is more efficient and more effective than standard SYN cookie implementations for several reasons which are examined below.

Syn Flood Description

Traditionally, the key reason that SYN floods have been so effective is that it was easy to fool a server into allocating resources for a connection attempt. Since the source-IP of these connection attempts is almost always forged, the server does not know where the attack is really coming from, and also would be responding with SYN acknowledgements to another location that would also become a victim.

SYN cookies were introduced in September of 1996 by D.J. Bernstein. He pointed out that this protection could be implemented with no changes to the TCP/IP protocol (<http://cr.yip.to/syncookies.html>). The basic idea was to use cryptographic techniques to provide an entry ticket of sorts for new connections. When a connection request was made, the SYN cookie would be formulated and sent back to the requestor. The information in this SYN cookie would be used in the final acknowledgement to prove that the client was legitimate, and to allocate resources for that connection.

SYN cookies have been effective at stopping small-scale SYN floods. The problem is that it's still too easy to overwhelm systems even if they are using SYN cookies, and even standard SYN cookie-protected servers can be victimized by forged connections.

NETSCALER UNIQUE SYN FLOOD PROTECTION

Resource Allocation

Firstly, and most importantly, the NetScaler never makes any resource allocation for a connection until the client has fully completed the three-way TCP/IP handshake. This is fundamentally important for withstanding massive floods of SYN packets. By refusing to allocate any resources whatsoever until a connection is completed, NetScaler avoids any server resource limitation issues during these attacks.

Furthermore, the NetScaler never cause any resources on a server to be allocated to a connection until the client has sent a valid request. This ensures that the server is only handling fully completed and legitimate clients. In fact, the server never knows about the client until a valid request has been made.

TCP/IP Efficiency

Standard SYN cookies limit connections to the use of only eight Maximum Segment Size (MSS) values for all clients, which on the surface may not seem to be of great concern, but it will affect the overall efficiency of all connections made to a server. When the MSS can be negotiated to the most optimal value for each client (commonly between 64 and 1460) each connection will transmit fewer packets for the same data stream. This translates into higher throughput and higher performance. With only eight out of 1396 MSS values available, most clients will have to opt for a lower than optimal MSS value, meaning it will take more packets to send the same amount of data. This translates into minimized capacity because of the higher number of packets being processed, and slower performance for users.

Non-Forgeable Connections

Normal SYN cookies contain encoded information that makes it near impossible to request a connection to a host from a forged (spoofed) originating address. In this scenario, the attacker must guess a valid TCP sequence number used by that server to connect to some other legitimate host. The cryptographic protection in the standard SYN cookie makes this attack possible with as few as one million guesses, which is not impossible for a determined attacker.

NetScaler uses an enhanced SYN cookie protection scheme that is fully compatible with the TCP/IP protocol, but have rendered the "forged connection" technique obsolete. Each new connection is unrelated to previous connections, and knowing a valid sequence number used for a previous connection will not enable an attacker to forge a connection.

High-Speed Packet Engine

The SYN cookie mechanism is effective at stopping small-scale attacks, but when the attack escalates, the server cannot keep up. Even routers and firewalls will fail long before reaching wire speed when faced with a SYN flood attack. This is because the processing required to keep up with the SYN flood simply creates another kind of DoS condition, known as CPU overload.

The NetScaler 9000 Series is designed to process TCP/IP at wire speed. This allows us to implement a further enhanced set of TCP/IP processing, even at gigabit speeds. The NetScaler has successfully demonstrated the blocking of a SYN flood attack approaching one million packets per second, far more than any other network device in this category.

SUMMARY

The NetScaler 9000 Series provides superior attack protection from SYN floods by implementing an enhanced SYN cookie mechanism that operates at wire-speed, making the NetScaler a perfect choice for providing superior DoS attack protection such as GET floods, SYN-ACK floods and surges mixed with legitimate traffic. While using SYN cookies on FreeBSD and Linux can withstand small floods of SYN traffic, they cannot withstand the larger more threatening attacks that are coming from distributed DoS clients. Furthermore, standard SYN cookie implementations offer no protection from a growing list of other DoS attacks that NetScaler can mitigate, while continuing to service legitimate traffic ensuring users are not effected during attack conditions.

NetScaler, the NetScaler logo and Request Switching are trademarks of NetScaler, Inc. All other products are trademarks of their respective holders and should be treated as such.