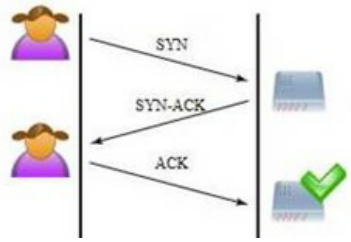
BIG-IP LTM SYN Check

John Wagnon, 2013-24-04

Denial of Service (DoS) attacks have been around for many years, but they are still frequently used today (ref: Iran's recent fascination with the US banking industry). These attacks are used against servers to disrupt legitimate communications between the server and the user. The following article discusses a common DoS attack (TCP SYN Flood) and how F5's BIG-IP LTM handles the problem.

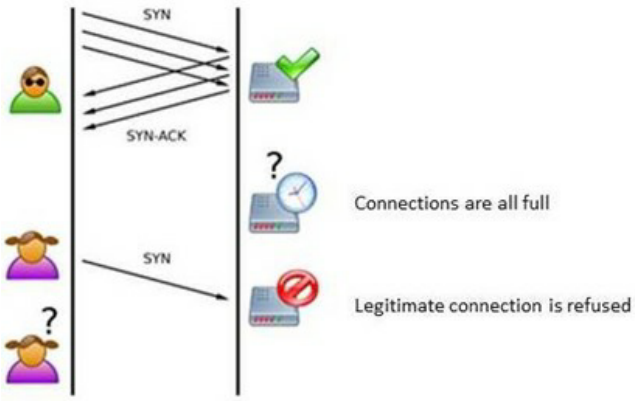
In a standard TCP connection, the user and the server engage in the all-important TCP 3-way handshake (SYN, SYN-ACK, ACK). When the final stage of the handshake takes place, the TCP connection is established, and the user and server suddenly find themselves deep in conversation…and life is good.

TCP 3-Way Handshake

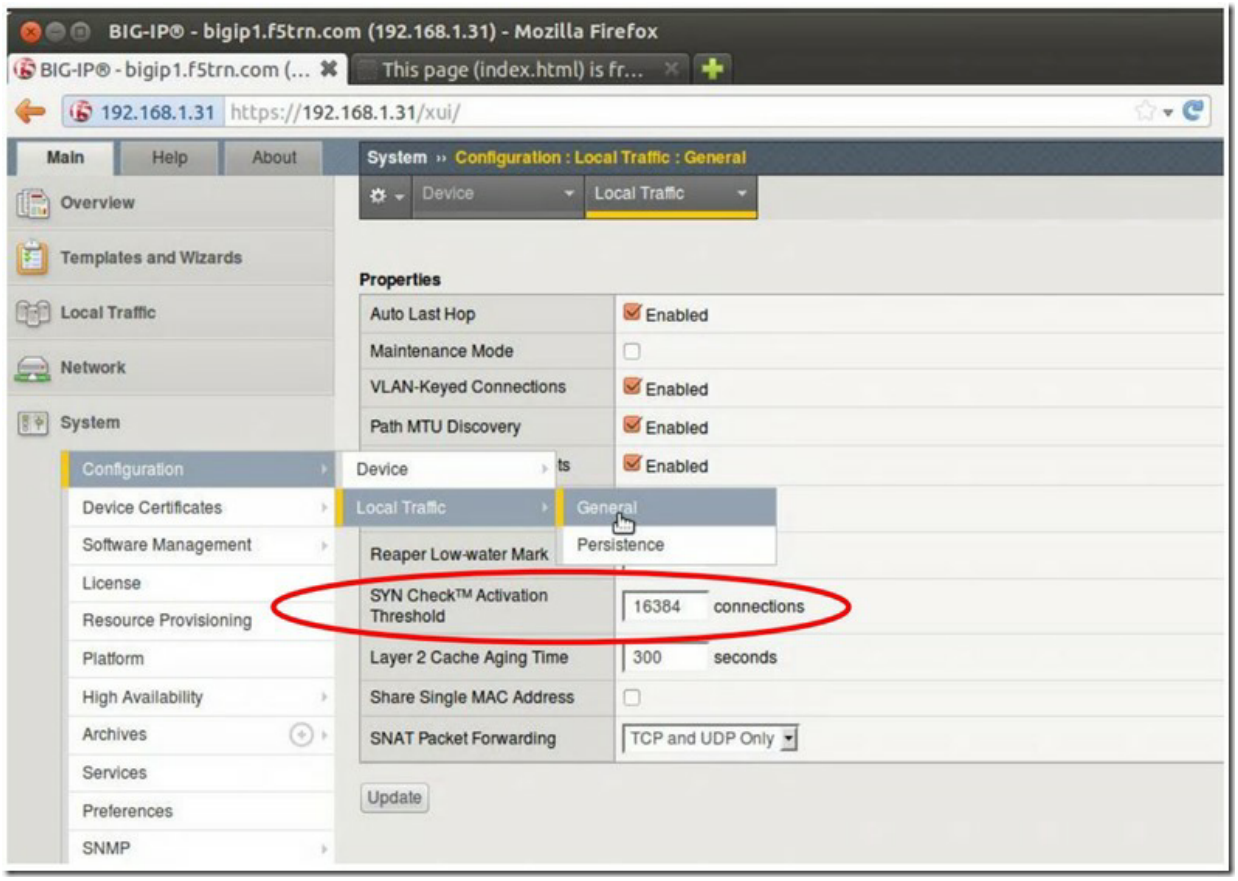


Well, not all users behave correctly. Some bad guys feel it necessary to send the SYN message and never respond again. In this case the user sends the SYN message, the server does its job and replies with a SYN-ACK, but the user never calls back to finalize the connection with the last part of the handshake (ACK). Sometimes network congestion is to blame for the delayed arrival of the final ACK, so the server will typically wait a predetermined amount of time for the ACK to arrive. The bad guys will take advantage of this and send multiple SYN messages in a short period of time. The server then responds with SYN-ACK replies, but the bad guy never sends the final ACKs. This creates what is called a "Half-Open" connection (these are fairly common in Distributed Denial of Service (DDoS) attacks). The server is limited on the number of concurrent TCP connections it can handle, so if all those connections are used up with Half-Open connections, it allows no room for legitimate users to connect. The following picture shows a SYN Flood Attack that results in Half-Open connections and a Denial of Service for a legitimate user.

SYN Flood Attack



The BIG-IP LTM is designed to handle these types of attacks. Specifically, the SYN Check™ Activation Threshold limits the number of TCP connections that are allowed before the BIG-IP activates the SYN Cookies authentication method for new TCP connections. The SYN Check™ Activation Threshold is set in the Configuration Utility by navigating to **System -> Configuration -> Local Traffic -> General** and entering the maximum number of concurrent TCP connections allowed (shown below).



You can also set the activation threshold using the following command line:

```
tmsh modify /sys db connection.syncookies.threshold value <threshold number of connections>
```

For example:

```
tmsh modify /sys db connection.syncookies.threshold value 16384
```

Here's how the SYN Cookies authentication method works…

1. A user sends a TCP SYN to the LTM virtual server
2. BIP-IP sends a SYN-ACK back to the user but discards the SYN queue entry
3. BIG-IP receives an ACK from the user and reconstructs the SYN queue entry by decoding data from the TCP sequence number

The BIG-IP SYN queue is the list of connections in the connection table that are in the SYN-RECEIVED state. Connections in the SYN-RECEIVED state are considered Half-Open and are waiting for an ACK from the user. When the maximum number of connections is established, the SYN queue is full and other legitimate connections are not allowed. BIG-IP's SYN Check alleviates this problem by sending cookies to the requesting users, thus eliminating the need to keep the SYN-RECEIVED state of each connection. Because the SYN-RECEIVED state is not kept, the SYN queue will never get full, and TCP traffic will not be affected. When the BIG-IP validates the user's ACK, the session is added to the connection table and the BIG-IP establishes a connection to the pool member. It's possible to activate SYN Check for all connections; however, latency can become a problem as the user must send back the SYN cookie, incremented by 1, as the acknowledgement number in the ACK flag. So, it's recommended to set the SYN Check™ Activation Threshold at a number considerably higher than 0.

For more information, read this AskF5 article: http://support.f5.com/kb/en-us/solutions/public/7000/800/sol7847.html?sr=28954937

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