BIG-IP Systems: Protecting against SYN Flood Attacks

Version 13.0

Table of Contents

Introduction to Protection Against SYN Flood Attacks

About SYN flood attacks

The BIG-IP® system includes features that help protect the system from a SYN flood attack. A *SYN flood* is a type of attack designed to exhaust all resources used to establish TCP connections. A SYN flood occurs when a client application intentionally fails to complete the initial handshake with the BIG-IP system, leaving the SYN queue to fill up with TCP half-open connections. As a result, the system no longer has the resources to process legitimate application traffic.

About SYN cookie protection

What are SYN Check activation and SYN cookie protection?

To protect against SYN flood attacks, the BIG-IP® system includes a feature known as *SYN Check*™. This feature globally monitors the system based on thresholds that you define, such as the number of TCP open-half connections on the system. When the system detects an attack, the BIG-IP system sends information about the flow to the requesting client, in the form of cookies.

SYN cookies help prevent the BIG-IP SYN queue from becoming full during a SYN flood attack, so that normal TCP communication can continue.

Scope of SYN cookie protection

Certain FPGA F5® platforms support both collaborative hardware and software SYN cookie protection, while other platforms support software SYN cookie protection only. When your platform uses software only for SYN cookie protection, the BIG-IP system implements SYN cookie protection per-virtual server. When your FPGA platform supports both hardware and software SYN cookie protection, you have the option of implementing SYN cookie protection per VLAN.

About thresholds

The BIG-IP system triggers SYN cookie protection based on thresholds that you configure. The system offers a per-virtual server threshold value, which is a number of TCP half-open connections. If any virtual server on the system experiences this number of half-open connections, the system triggers cookie protection for that virtual server. Additionally, the system offers a global threshold that applies system-wide. The system will trigger global cookie protection when the system experiences the configured number of TCP half-open connections in total. Additional thresholds exist for VLAN-based SYN cookie protection.

SYN Check activation vs. adaptive reaping

The SYN Check feature complements the existing adaptive reaper feature in the BIG-IP system. While the adaptive reaper handles established connection flooding, SYN Check prevents connection flooding altogether. That is, while the adaptive reaper must work overtime to flush connections, the SYN Check feature prevents the SYN queue from becoming full, thus allowing the target system to continue to establish TCP connections.

VLAN-based Hardware SYN Cookie Protection

Overview of VLAN-based hardware SYN cookie protection

What is VLAN-based hardware SYN cookie protection?

On certain F5® FPGA platforms, you can enable hardware SYN cookie protection per VLAN instead of per virtual server.

Configuring SYN cookie protection per VLAN avoids potential collisions within the FPGA programmable hardware. Such collisions can result in the BIG-IP® software handling all SYN cookie protection, causing performance degradation as CPU usage increases beyond normal levels.

Without collisions, hardware and software continue to work collaboratively to mitigate the attack, which ultimately prevents performance degradation on the system.

Configuration overview

If the BIG-IP hardware supports VLAN-based SYN cookie protection, you first configure the feature on one or more individual VLANs. Then you enable a global setting within BIG-IP Local Traffic Manager (LTM), **Hardware VLAN SYN Cookie Protection**. This global setting enables the feature on all VLANs on which you configured the feature.

In general, the global setting allows you to quickly and easily enable and disable the feature on all relevant VLANs, rather than you having to re-configure every VLAN when you want to enable or disable the feature for those VLANs.

When you disable the global **Hardware VLAN SYN Cookie Protection** setting, the system switches back to enabling SYN Check activation (with SYN cookie protection) on a per-virtual server basis.

Important: *On platforms on which the BIG-IP software works collaboratively with FPGA hardware to protect against SYN floods, enabling per-virtual SYN Check™ activation instead of VLAN-based hardware SYN cookie protection could result in performance degradation if FPGA collisions occur.*

About configuring hardware VLAN SYN cookie protection

To configure VLAN-based hardware SYN cookie protection, you must configure some settings on each VLAN that you want the BIG-IP® system to protect, and then globally enable the feature within BIG-IP® Local Traffic Manager™ (LTM).

Modifying a VLAN to configure global hardware SYN cookie protection

VLANs represent a logical collection of hosts that can share network resources, regardless of their physical location on the network. You can modify a VLAN to configure hardware SYN cookie protection for that VLAN. You configure hardware SYN cookie protection on a VLAN when you want to protect the VLAN from SYN flood attacks.

1. On the Main tab, click **Network** > **VLANs**.
   The VLAN List screen opens.
2. In the Name column, click the relevant VLAN name.
   The New VLAN screen opens.
3. From the **Configuration** list, select **Advanced**.

4. For the **Hardware SYN Cookie** setting, select or clear the check box.

   When you enable this setting, the BIG-IP system triggers hardware SYN cookie protection for this VLAN.

   Enabling this setting causes additional settings to appear. These settings appear on specific BIG-IP platforms only.
5. For the **Syncache Threshold** setting, retain the default value or change it to suit your needs.

   The **Syncache Threshold** value represents the number of outstanding SYN flood packets on the VLAN that will trigger the hardware SYN cookie protection feature.

   When the **Hardware SYN Cookie** setting is enabled, the BIG-IP system triggers SYN cookie protection in either of these cases, whichever occurs first:

   - The number of TCP half-open connections defined in the LTM® setting **Global SYN Check Threshold** is reached.
   - The number of SYN flood packets defined in this **Syncache Threshold** setting is reached.
6. For the **SYN Flood Rate Limit** setting, retain the default value or change it to suit your needs.

   The **SYN Flood Rate Limit** value represents the maximum number of SYN flood packets per second received on this VLAN before the BIG-IP system triggers hardware SYN cookie protection for the VLAN.
7. Click **Update**.

Hardware SYN cookie protection is now enabled on this VLAN whenever the global **Hardware VLAN SYN Cookie Protection** setting is enabled within BIG-IP® Local Traffic Manager™ (LTM).

Enabling global hardware VLAN SYN cookie protection settings

Before starting this task, make sure you have configured SYN cookie protection on at least one BIG-IP® VLAN.

You can use the Configuration utility to globally enable the hardware VLAN-based SYN cookie feature on all VLANs configured for SYN cookie protection.

1. On the Main tab, click **System** > **Configuration** > **Local Traffic** > **General**

   This shows the settings that you can set globally for BIG-IP® Local Traffic Manager ™(LTM).
2. In the Properties area of the screen, for the **Hardware VLAN SYN Cookie Protection** setting, make sure that the check box is selected.
3. Click **Update**.

About configuring hardware SYN cookies using tmsh

To configure VLAN-based hardware SYN cookie protection, you use the TMOS Shell (`tmsh`) to configure some settings on each VLAN that you want the BIG-IP® system to protect. You then globally enable the feature within BIG-IP Local Traffic Manager™ (LTM).

Modifying a VLAN to configure global hardware SYN cookie protection using tmsh

You can use the TMOS Shell (`tmsh`) to configure the global hardware VLAN SYN cookie settings on a VLAN.

1. Open the TMOS Shell (`tmsh`).

   ```
   tmsh
   ```
2. Change to the network module.

`net`

The system prompt updates with the module name: `user@bigip01(Active)(/Common)(tmos.net)#` `user@bigiq01(Active)(/Common)(tmos.net)#`

3. View all existing properties for a specified VLAN.
   `list vlan <name> all-properties`
4. Enable or disable hardware SYN cookie protection on a specified VLAN.
   `modify vlan <name> [disabled | enabled]`
5. Configure the number of outstanding SYN packets on the VLAN required to trigger hardware VLAN SYN cookie protection.
   `modify vlan <name> syncache-threshold <number>`

   The default value is 6000 packets.
6. Configure a maximum number of SYN flood packets per second to be received on the VLAN before hardware SYN cookie protection is triggered.
   `modify vlan <name> syn-flood-rate-limit <number>`

   The default value is 1000 packets per second.

Enabling global hardware VLAN SYN cookie protection using tmsh

Before starting this task, make sure you have configured SYN cookie protection on at least one BIG-IP® VLAN.

You can use the TMOS Shell (`tmsh`) to globally enable or disable the hardware VLAN-based SYN cookie feature on your system.

1. Open the TMOS Shell (`tmsh`).
   `tmsh`
2. Configure whether to enable global hardware SYN cookies on VLANs.
   `modify connection vlan-syn-cookie [disabled | enabled]`

Platform support for hardware SYN cookies

This table lists the platforms that support hardware SYN cookie protection.

Platform name	Platform ID
BIG-IP® 5000 Series	C109
BIG-IP 7000 Series	D110
BIG-IP 10000 Series	D113
BIG-IP 12000 Series	D111
BIG-IP i5000 Series	C119
BIG-IP i7000 Series	C118
BIG-IP i10000 Series	C116
VIPRION® B2100 Blade	A109
VIPRION B2150 Blade	A113
VIPRION B2250 Blade	A112
VIPRION B4300 Blade	A108
VIPRION B4340N Blade	A110

Platform name	Platform ID
VIPRION B4450 Blade	A114

Legal Notices

Legal notices

Publication Date

This document was published on February 28, 2017.

Publication Number

MAN-0660-00

Copyright

Trademarks

For a current list of F5 trademarks and service marks, see *http://www.f5.com/about/guidelines-policies/trademarks*.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by one or more patents indicated at: *https://f5.com/about-us/policies/patents*.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Index

F

H

S

V