

Configuring Firewall TCP SYN Cookie

The Firewall TCP SYN Cookie feature protects your firewall from TCP SYN-flooding attacks. TCP SYN-flooding attacks are a type of denial-of-service (DoS) attack. Usually, TCP synchronization (SYN) packets are sent to a targeted end host or a range of subnet addresses behind the firewall. These TCP SYN packets have spoofed source IP addresses. A spoofing attack is when a person or a program pretends to be another by falsifying data and thereby gaining an illegitimate advantage. TCP SYN-flooding can take up all resources on a firewall or an end host, thereby causing DoS to legitimate traffic. To prevent TCP SYN-flooding on a firewall and the end hosts behind the firewall, you must configure the Firewall TCP SYN Cookie feature.

- Restrictions for Configuring Firewall TCP SYN Cookie, on page 1
- Information About Configuring Firewall TCP SYN Cookie, on page 1
- How to Configure Firewall TCP SYN Cookie, on page 2
- Configuration Examples for Firewall TCP SYN Cookie, on page 7
- Additional References for Firewall TCP SYN Cookie, on page 8
- Feature Information for Configuring Firewall TCP SYN Cookie, on page 9

Restrictions for Configuring Firewall TCP SYN Cookie

- Because a default zone does not support zone type parameter map, you cannot configure the Firewall TCP SYN Cookie feature for a default zone.
- The Firewall TCP SYN Cookie feature does not support per-subscriber firewall.

Information About Configuring Firewall TCP SYN Cookie

TCP SYN Flood Attacks

The Firewall TCP SYN Cookie feature implements software to protect the firewall from TCP SYN-flooding attacks, which are a type of DoS attack.

A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a website, accessing e-mail, using FTP service, and so on.

SYN flood attacks are divided into two types:

- Host flood—SYN flood packets are sent to a single host aiming to utilize all resources on that host.
- Firewall session table flood—SYN flood packets are sent to a range of addresses behind the firewall, with the aim of exhausting the session table resources on the firewall and thereby denying resources to the legitimate traffic going through the firewall.

The Firewall TCP SYN Cookie feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. The firewall intercepts TCP SYN packets that are sent from clients to servers. When the TCP SYN cookie is triggered, it acts on all SYN packets that are destined to the configured VPN Routing and Forwarding (VRF) or zone. The TCP SYN cookie establishes a connection with the client on behalf of the destination server and another connection with the server on behalf of the client and knits together the two half-connections transparently. Thus, connection attempts from unreachable hosts will never reach the server. The TCP SYN cookie intercepts and forwards packets throughout the duration of the connection.

The Firewall TCP SYN Cookie feature provides session table SYN flood protection for the global routing domain and for the VRF domain. Because the firewall saves sessions in a global table, you can configure a limit to the number of TCP half-opened sessions. A TCP half-opened session is a session that has not reached the established state. In a VRF-aware firewall, you can configure a limit to the number of TCP half-opened sessions for each VRF. At both the global level and at the VRF level, when the configured limit is reached, the TCP SYN cookie verifies the source of the half-opened sessions before creating more sessions.

How to Configure Firewall TCP SYN Cookie

Configuring Firewall Host Protection

TCP SYN packets are sent to a single host with the aim of taking over all resources on the host. You can configure host protection only for the source zone. Configuring protection on the destination zone will not protect the destination zone from TCP SYN attacks.

Perform this task to configure the firewall host protection.

Note You can specify the **show** commands in any order.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-zone** *zone-pmap-name*
4. **tcp syn-flood rate per-destination** *maximum-rate*
5. **max-destination** *limit*
6. **exit**
7. **zone security** *zone-name*
8. **protection** *parameter-map-name*
9. **exit**
10. **show parameter-map type inspect-zone** *zone-pmap-name*

11. **show zone security**
12. **show policy-firewall stats zone** *zone-name*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type inspect-zone** *zone-pmap-name* **Example:** `Router(config)# parameter-map type inspect-zone zone-pmap`	Configures an inspect zone type parameter map and enters profile configuration mode.
Step 4	**tcp syn-flood rate per-destination** *maximum-rate* **Example:** `Router(config-profile)# tcp syn-flood rate per-destination 400`	Configures the number of SYN flood packets per second for each destination address. • If the rate of SYN packets sent to a particular destination address exceeds the per-destination limit, the firewall starts processing SYN cookies for SYN packets that are routed to the destination address.
Step 5	**max-destination** *limit* **Example:** `Router(config-profile)# max-destination 10000`	Configures the maximum number of destinations that the firewall can track for a zone. • The firewall drops the SYN packets if the maximum destination crosses the limit that is configured by using the *limit* argument.
Step 6	**exit** **Example:** `Router(config-profile)# exit`	Exits profile configuration mode and enters global configuration mode.
Step 7	**zone security** *zone-name* **Example:** `Router(config)# zone security secure-zone`	Configures a security zone and enters security zone configuration mode.

	Command or Action	Purpose
Step 8	**protection** *parameter-map-name* **Example:** `Router(config-sec-zone)# protection zone-pmap`	Configures protection for the specified zone using the parameter map.
Step 9	**exit** **Example:** `Router(config-sec-zone)# exit`	Exits security zone configuration and enters privileged EXEC mode.
Step 10	**show parameter-map type inspect-zone** *zone-pmap-name* **Example:** `Router# show parameter-map type inspect-zone zone-pmap`	(Optional) Displays details about the inspect zone type parameter map.
Step 11	**show zone security** **Example:** `Router# show zone security`	(Optional) Displays zone security information.
Step 12	**show policy-firewall stats zone** *zone-name* **Example:** `Router# show policy-firewall stats zone secure-zone`	(Optional) Displays how many SYN packets exceeded the packet limit and were processed by SYN cookies.

Configuring Firewall Session Table Protection

TCP SYN packets are sent to a range of addresses behind the firewall aiming to exhaust the session table resources on the firewall, thereby denying resources to the legitimate traffic going through the firewall. You can configure firewall session table protection either for the global routing domain or for the VRF domain.

Configuring Firewall Session Table Protection for Global Routing Domain

Perform this task to configure firewall session table protection for global routing domains.

Note A global parameter map takes effect on the global routing domain and not at the router level.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect global**

4. **tcp syn-flood limit** *number*
5. **end**
6. **show policy-firewall stats vrf global**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type inspect global** **Example:** `Router(config)# parameter-map type inspect global`	Configures a global parameter map and enters profile configuration mode.
Step 4	**tcp syn-flood limit** *number* **Example:** `Router(config-profile)# tcp syn-flood limit 500`	Limits the number of TCP half-open sessions that triggers SYN cookie processing for new SYN packets.
Step 5	**end** **Example:** `Router(config-profile)# end`	Exits profile configuration mode and enters privileged EXEC mode.
Step 6	**show policy-firewall stats vrf global** **Example:** `Router# show policy-firewall stats vrf global`	(Optional) Displays the status of the global VRF firewall policy. • The command output also displays how many TCP half-open sessions are present.

Configuring Firewall Session Table Protection for VRF Domain

Perform this task to configure the firewall session table protection for VRF domains.

Note You can specify the **show** commands in any order.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-vrf** *vrf-pmap-name*
4. **tcp syn-flood limit** *number*
5. **exit**
6. **parameter-map type inspect global**
7. **vrf** *vrf-name* **inspect** *parameter-map-name*
8. **end**
9. **show parameter-map type inspect-vrf**
10. **show policy-firewall stats vrf** *vrf-name*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type inspect-vrf** *vrf-pmap-name* **Example:** `Router(config)# parameter-map type inspect-vrf vrf-pmap`	Configures an inspect-VRF type parameter map and enters profile configuration mode.
Step 4	**tcp syn-flood limit** *number* **Example:** `Router(config-profile)# tcp syn-flood limit 200`	Limits the number of TCP half-open sessions that triggers SYN cookie processing for new SYN packets.
Step 5	**exit** **Example:** `Router(config-profile)# exit`	Exits profile configuration mode and enters global configuration mode.
Step 6	**parameter-map type inspect global** **Example:** `Router(config)# parameter-map type inspect global`	Binds the inspect-VRF type parameter map to a VRF and enters profile configuration mode.

	Command or Action	Purpose
Step 7	**vrf** *vrf-name* **inspect** *parameter-map-name* **Example:** `Router(config-profile)# vrf vrf1 inspect vrf-pmap`	Binds the parameter map to the VRF.
Step 8	**end** **Example:** `Router(config-profile)# end`	Exits profile configuration mode and enters privileged EXEC mode.
Step 9	**show parameter-map type inspect-vrf** **Example:** `Router# show parameter-map type inspect-vrf`	(Optional) Displays information about inspect VRF type parameter map.
Step 10	**show policy-firewall stats vrf** *vrf-name* **Example:** `Router# show policy-firewall stats vrf vrf-pmap`	(Optional) Displays the status of the VRF firewall policy. • The command output also displays how many TCP half-open sessions are present.

Configuration Examples for Firewall TCP SYN Cookie

Example Configuring Firewall Host Protection

The following example shows how to configure the firewall host protection:

```
Router(config)# parameter-map type inspect-zone zone-pmap
Router(config-profile)# tcp syn-flood rate per-destination 400
Router(config-profile)# max-destination 10000
Router(config-profile)# exit
Router(config)# zone security secure-zone
Router(config-sec-zone)# protection zone-pmap
```

Example Configuring Firewall Session Table Protection

Global Parameter Map

The following example shows how to configure firewall session table protection for global routing domains:

```
Router# configure terminal
Router(config)# parameter-map type inspect global
Router(config-profile)# tcp syn-flood limit 500
Router(config-profile)# end
```

Inspect-VRF Type Parameter Map

The following example shows how to configure firewall session table protection for VRF domains:

```
Router# configure terminal
Router(config)# parameter-map type inspect-vrf vrf-pmap
Router(config-profile)# tcp syn-flood limit 200
Router(config-profile)# exit
Router(config)# parameter-map type inspect global
Router(config-profile)# vrf vrf1 inspect vrf-pmap
Router(config-profile)# end
```

Additional References for Firewall TCP SYN Cookie

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Security Command Reference: Commands A to C • Security Command Reference: Commands D to L • Security Command Reference: Commands M to R • Security Command Reference: Commands S to Z

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring Firewall TCP SYN Cookie

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Configuring Firewall TCP SYN Cookie

Feature Name	Releases	Feature Information
Firewall TCP SYN Cookie	Cisco IOS XE Release 3.3S	The Firewall TCP SYN Cookie feature protects your firewall from TCP SYN-flooding attacks. TCP SYN-flooding attacks are a type of DoS attack. Usually, TCP SYN packets are sent to a targeted end host or a range of subnet addresses behind the firewall. These TCP SYN packets have spoofed source IP addresses. A spoofing attack is when a person or a program pretends to be another by falsifying data and thereby gaining an illegitimate advantage. The TCP SYN-flooding can take up all the resource on a firewall or an end host, thereby causing DoS to legitimate traffic. To prevent TCP SYN-flooding on a firewall and the end hosts behind the firewall, you must configure the Firewall TCP SYN Cookie feature. The following commands were introduced or modified: **parameter-map type inspect-vrf**, **parameter-map type inspect-zone**, **parameter-map type inspect global**, **show policy-firewall stats**, **tcp syn-flood rate per-destination**, **tcp syn-flood limit**.