

Configuring Firewall Resource Management

The Firewall Resource Management feature limits the number of VPN Routing and Forwarding (VRF) and global firewall sessions that are configured on a router.

- Restrictions for Configuring Firewall Resource Management, on page 1
- Information About Configuring Firewall Resource Management, on page 1
- How to Configure Firewall Resource Management, on page 3
- Configuration Examples for Firewall Resource Management, on page 5
- Additional References, on page 6
- Feature Information for Configuring Firewall Resource Management, on page 6

Restrictions for Configuring Firewall Resource Management

- After you configure the global-level or VRF-level session limit and reconfigure the session limit, if the global-level or VRF-level session limit is below the initially configured session count, no new session is added; however, no current session is dropped.

Information About Configuring Firewall Resource Management

Firewall Resource Management

Resource Management limits the level of usage of shared resources on a device. Shared resources on a device include:

- Bandwidth
- Connection states
- Memory usage (per table)
- Number of sessions or calls
- Packets per second
- Ternary content addressable memory (TCAM) entries

The Firewall Resource Management feature extends the zone-based firewall resource management from the class level to the VRF level and the global level. Class-level resource management provides resource protection for firewall sessions at a class level. For example, parameters such as the maximum session limit, the session rate limit, and the incomplete session limit protect firewall resources (for example, chunk memory) and keep these resources from being used up by a single class.

When virtual routing and forwarding (VRF) instances share the same policy, a firewall session setup request from one VRF instance can make the total session count reach the maximum limit. When one VRF consumes the maximum amount of resources on a device, it becomes difficult for other VRF instances to share device resources. To limit the number of VRF firewall sessions, you can use the Firewall Resource Management feature.

At the global level, the Firewall Resource Management feature helps limit the usage of resources at the global routing domain by firewall sessions.

VRF-Aware Cisco IOS XE Firewall

The VRF-Aware Cisco IOS XE Firewall applies the Cisco IOS XE Firewall functionality to VPN Routing and Forwarding (VRF) interfaces when the firewall is configured on a service provider (SP) or large enterprise edge routers. SPs provide managed services to small and medium business markets.

The VRF-Aware Cisco IOS XE Firewall supports VRF-lite (also known as Multi-VRF CE) and Application Inspection and Control (AIC) for various protocols.

The VRF-aware firewall supports VRF-lite (also known as Multi-VRF CE) and Application Inspection and Control (AIC) for various protocols.



Note Cisco IOS XE Releases do not support Context-Based Access Control (CBAC) firewalls.

Firewall Sessions

Session Definition

At the virtual routing and forwarding (VRF) level, the Firewall Resource Management feature tracks the firewall session count for each VRF instance. At the global level, the firewall resource management tracks the total firewall session count at the global routing domain and not at the device level. In both the VRF and global levels, session count is the sum of opened sessions, half-opened sessions, and sessions in the imprecise firewall session database. A TCP session that has not yet reached the established state is called a half-opened session.

A firewall has two session databases: the session database and the imprecise session database. The session database contains sessions with 5-tuple (source IP address, destination IP address, source port, destination port, and protocol). A tuple is an ordered list of elements. The imprecise session database contains sessions with fewer than 5-tuple (missing IP addresses, port numbers, and so on).

The following rules apply to the configuration of a session limit:

- The class-level session limit can exceed the global limit.
- The class-level session limit can exceed its associated VRF session maximum.

- The sum of the VRF limit, including the global context, can be greater than the hardcoded session limit.

Session Rate

The session rate is the rate at which sessions are established at any given time interval. You can define maximum and minimum session rate limits. When the session rate exceeds the maximum specified rate, the firewall starts rejecting new session setup requests.

From the resource management perspective, setting the maximum and minimum session rate limit helps protect Cisco Packet Processor from being overwhelmed when numerous firewall session setup requests are received.

Incomplete or Half-Opened Sessions

Incomplete sessions are half-opened sessions. Any resource used by an incomplete session is counted, and any growth in the number of incomplete sessions is limited by setting the maximum session limit.

Firewall Resource Management Sessions

The following rules apply to firewall resource management sessions:

- By default, the session limit for opened and half-opened sessions is unlimited.
- Opened or half-opened sessions are limited by parameters and counted separately.
- Opened or half-opened session count includes Internet Control Message Protocol (ICMP), TCP, or UDP sessions.
- You can limit the number and rate of opened sessions.
- You can only limit the number of half-opened sessions.

How to Configure Firewall Resource Management

Configuring Firewall Resource Management



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-vrf** *vrf-pmap-name*
4. **session total** *number*
5. **tcp syn-flood limit** *number*
6. **exit**
7. **parameter-map type inspect-global**
8. **vrf** *vrf-name* **inspect** *parameter-map-name*

9. **exit**
10. **parameter-map type inspect-vrf vrf-default**
11. **session total** *number*
12. **tcp syn-flood limit** *number*
13. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type inspect-vrf** *vrf-pmap-name* **Example:** `Device(config)# parameter-map type inspect-vrf vrf1-pmap`	Configures an inspect VRF-type parameter map and enters parameter-map type inspect configuration mode.
Step 4	**session total** *number* **Example:** `Device(config-profile)# session total 1000`	Configures the total number of sessions.
Step 5	**tcp syn-flood limit** *number* **Example:** `Device(config-profile)# tcp syn-flood limit 2000`	Limits the number of TCP half-opened sessions that trigger synchronization (SYN) cookie processing for new SYN packets.
Step 6	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and enters global configuration mode.
Step 7	**parameter-map type inspect-global** **Example:** `Device(config)# parameter-map type inspect-global`	Configures a global parameter map and enters parameter-map type inspect configuration mode.
Step 8	**vrf** *vrf-name* **inspect** *parameter-map-name* **Example:** `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	Binds a VRF to the parameter map.
Step 9	**exit** **Example:**	Exits parameter-map type inspect configuration mode and enters global configuration mode.

	Command or Action	Purpose
	`Device(config-profile)# exit`	
Step 10	**parameter-map type inspect-vrf vrf-default** **Example:** `Device(config)# parameter-map type inspect-vrf vrf-default`	Configures a default inspect VRF-type parameter map.
Step 11	**session total** *number* **Example:** `Device(config-profile)# session total 6000`	Configures the total number of sessions. • You can configure the **session total** command for an inspect VRF-type parameter map and for a global parameter map. When you configure the **session total** command for an inspect VRF-type parameter map, the sessions are associated with an inspect VRF-type parameter map. The **session total** command is applied to the global routing domain when it is configured for a global parameter-map.
Step 12	**tcp syn-flood limit** *number* **Example:** `Device(config-profile)# tcp syn-flood limit 7000`	Limits the number of TCP half-opened sessions that trigger SYN cookie processing for new SYN packets.
Step 13	**end** **Example:** `Device(config-profile)# end`	Exits parameter-map type inspect configuration mode and enters privileged EXEC mode.

Configuration Examples for Firewall Resource Management

Example: Configuring Firewall Resource Management

```
Device# configure terminal
Device(config)# parameter-map type inspect-vrf vrf1-pmap
Device(config-profile)# session total 1000
Device(config-profile)# tcp syn-flood limit 2000
Device(config-profile)# exit
Device(config)# parameter-map type inspect-global
Device(config-profile)# vrf vrf1 inspect pmap1
Device(config-profile)# exit
Device(config)# parameter-map type inspect-vrf vrf-default
Device(config-profile)# session total 6000
Device(config-profile)# tcp syn-flood limit 7000
Device(config-profile)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands 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
VRF-aware firewall	"VRF-Aware Cisco IOS XE Firewall" module
Zone-based policy firewall	" Zone-Based Policy Firewall" module

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 Resource Management

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 Resource Management

Feature Name	Releases	Feature Information
Firewall Resource Management	Cisco IOS XE Release 3.3S	The Firewall Resource Management feature limits the number of VPN Routing and Forwarding (VRF) and global firewall sessions that are configured on a router. The following commands were introduced or modified: **parameter-map type inspect-vrf**.