Configurable Number of Simultaneous Packets per Flow

In zone-based policy firewalls, the number of simultaneous packets per flow is restricted to 25 and packets that exceed the limit are dropped. The dropping of packets when the limit is reached impacts the performance of networks. The Configurable Number of Simultaneous Packets per Flow feature allows you to configure the number of simultaneous packets per flow from 25 to 100.

This modules provides an overview of the feature and explains how to configure it.

- Restrictions for Configurable Number of Simultaneous Packets per Flow, on page 1
- Information About Configurable Number of Simultaneous Packets per Flow, on page 2
- How to Configure the Number of Simultaneous Packets per Flow, on page 2
- Configuration Examples for Configurable Number of Simultaneous Packets per Flow, on page 7
- Additional References for Configurable Number of Simultaneous Packets per Flow, on page 8
- Feature Information for Configurable Number of Simultaneous Packets per Flow, on page 9

Restrictions for Configurable Number of Simultaneous Packets per Flow

- When the TCP window scale option is configured, the firewall cannot simultaneously fit too many TCP packets per flow, and packets that exceed the configured limit are dropped. The maximum window size that can be used, if the TCP window scale option is enabled, is 1 GB.

  The standard TCP window size is between 2 and 65,535 bytes. If the TCP payload size is smaller than 655 bytes, 100 simultaneous packets cannot contain all TCP packets that belong to a single TCP window, and this can result in packet drops. We recommend that you increase the TCP payload size or reduce the TCP window size to avoid packet drops.

- The total available threads in each platform varies according to the enabled license levels. If the configured number of simultaneous packets per flow is bigger than the available hardware thread number, the configuration of simultaneous packets is not effective.

Information About Configurable Number of Simultaneous Packets per Flow

Overview of Configurable Number of Simultaneous Packets per Flow

The Configurable Number of Simultaneous Packets per Flow feature allows you to increase the number of simultaneous packets per flow that can enter a network. You can increase the number of simultaneous packets per flow from 25 to 100. The default is 25 simultaneous packets.

In multithreaded environments, the zone-based policy firewall may simultaneously receive multiple packets for a single traffic flow. During packet processing, the firewall uses two types of locks: flow lock and software lock. The flow lock ensures that packets that belong to the same flow are processed in the correct order. Normal software locks are used when multiple power processing element (PPE) threads try to read or write critical sections or common data structure (for example, memory).

If the number of simultaneous packets per flow is too large, the time taken by a thread to request and acquire a lock may be too long. This latency adversely affects time-critical infrastructure such as resource reuse and heat-beat processing. To control latency, the number of simultaneous packets was restricted to 25, and packets that exceeded 25 were dropped.

However, the dropping of packets drastically impacts system performance of a system. To minimize packet dropping, the Configurable Number of Simultaneous Packets per Flow feature was introduced. You can configure the number of simultaneous packets per flow from 25 to 100.

To change the number of simultaneous packets per flow, you must configure either the **parameter-map type inspect** *parameter-map-name* command or the **parameter-map type inspect global** command, followed by the **session packet** command. The limit configured under the **parameter-map type inspect** *parameter-map-name* command takes precedence over the limit configured under the **parameter-map type inspect global** command.

The firewall considers Session Initiation Protocol (SIP) trunk traffic as a single session. However, the SIP trunk traffic contains a large number of application-layer gateway (ALG) flows of different users. When the throughput of the SIP trunk traffic is high compared to other traffic, the simultaneous packet limit causes packets to drop and users may experience call drops.

How to Configure the Number of Simultaneous Packets per Flow

Configuring Class Maps and Policy Maps for Simultaneous Packets per Flow

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect** {**match-any** | **match-all**} *class-map-name*
4. **match protocol** *protocol-name*

5. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **inspect**
9. **exit**
10. **class class-default**
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode. • Enter your password if prompted.
Step 3	**class-map type inspect** {**match-any** | **match-all**} *class-map-name* **Example:** `Device(config)# class-map type inspect match-any cmap-protocols`	Creates an inspect-type class map and enters class map configuration mode.
Step 4	**match protocol** *protocol-name* **Example:** `Device(config-cmap)# match protocol tcp`	Configures the match criteria for a class map on the basis of a specified protocol.
Step 5	**exit** **Example:** `Device(config-cmap)# exit`	Exits class map configuration mode and returns to global configuration mode.
Step 6	**policy-map type inspect** *policy-map-name* **Example:** `Device(config)# policy-map type inspect policy1`	Creates an inspect-type policy map and enters policy map configuration mode.
Step 7	**class type inspect** *class-map-name* **Example:** `Device(config-pmap)# class type inspect cmap-protocols`	Specifies the traffic class on which an action is to be performed and enters policy-map class configuration mode.
Step 8	**inspect** **Example:** `Device(config-pmap-c)# inspect`	Enables stateful packet inspection.

	Command or Action	Purpose
Step 9	**exit** **Example:** `Device(config-pmap-c)# exit`	Exits policy-map class configuration mode and returns to policy map configuration mode.
Step 10	**class class-default** **Example:** `Device(config-pmap)# class class-default`	Configures or modifies a policy for the default class.
Step 11	**end** **Example:** `Device(config-pmap)# end`	Exits policy map configuration mode and returns to privileged EXEC mode.

Configuring the Number of Simultaneous Packets per Flow

You can configure the number of simultaneous packets per flow after configuring either the **parameter-map type inspect** command or the **parameter-map type inspect global** command. The number of simultaneous packets per flow configured under the **parameter-map type inspect** command overwrites the number configured under the **parameter-map type inspect global** command.

You must configure the **session packet** command to configure the number of simultaneous packets per flow.

Note You must configure either Steps 3 and 4 or Steps 6 and 7.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** *parameter-map-name*
4. **session packet** *number-of-simultaneous-packets*
5. **exit**
6. **parameter-map type inspect global**
7. **session packet** *number-of-simultaneous-packets*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:**	Enters global configuration mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**parameter-map type inspect** *parameter-map-name* **Example:** `Device(config)# parameter-map type inspect param1`	(Optional) Defines an inspect type parameter map, which configures connection thresholds, timeouts, and other parameters pertaining to the inspect action; and enters parameter-map type inspect configuration mode.
Step 4	**session packet** *number-of-simultaneous-packets* **Example:** `Device(config-profile)# session packet 55`	(Optional) Configures the number of simultaneous traffic packets that can be configured per session. • Valid values for the *number-of-simultaneous-packets* argument are 25 to 55.
Step 5	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and returns to global configuration mode.
Step 6	**parameter-map type inspect global** **Example:** `Device(config)# parameter-map type inspect global`	(Optional) Defines a global inspect parameter map and enters parameter-map type inspect configuration mode.
Step 7	**session packet** *number-of-simultaneous-packets* **Example:** `Device(config-profile)# session packet 35`	(Optional) Configures the number of simultaneous traffic packets that can be configured per session. • Valid values for the *number-of-simultaneous-packets* argument are 25 to 55.
Step 8	**end** **Example:** `Device(config-profile)# end`	Exits parameter-map type inspect configuration mode and returns to privileged EXEC mode.

Configuring Zones for Simultaneous Packets per Flow

This task shows how to configure security zones, a zone pair, and assign interfaces as zone members.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **zone security** *security-zone*
4. **exit**
5. **zone security** *security-zone*
6. **exit**
7. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **zone-member security** *zone-name*

12. **exit**
13. **interface** *type number*
14. **zone-member security** *zone-name*
15. **end**

DETAILED STEPS

	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	**zone security** *security-zone* **Example:** `Device(config)# zone security z1`	Creates a security zone to which interfaces can be assigned and enters security zone configuration mode. • You need two security zones to create a zone pair: a source zone and a destination zone.
Step 4	**exit** **Example:** `Device(config-sec-zone)# exit`	Exits security zone configuration mode and returns to global configuration mode.
Step 5	**zone security** *security-zone* **Example:** `Device(config)# zone security z2`	Creates a security zone to which interfaces can be assigned and enters security zone configuration mode. • You need two security zones to create a zone pair: a source zone and a destination zone.
Step 6	**exit** **Example:** `Device(config-sec-zone)# exit`	Exits security zone configuration mode and returns to global configuration mode.
Step 7	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* **Example:** `Device(config)# zone-pair security zp-security source z1 destination z2`	Creates a zone pair and enters security zone pair configuration mode.
Step 8	**service-policy type inspect** *policy-map-name* **Example:** `Device(config-sec-zone-pair)# service-policy type inspect policy1`	Attaches a firewall policy map to the destination zone pair. • If a policy is not configured between a pair of zones, traffic is dropped by default.
Step 9	**exit** **Example:**	Exits security zone pair configuration mode and returns to global configuration mode.

	Command or Action	Purpose
	`Device(config-sec-zone-pair)# exit`	
Step 10	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Configures an interface and enters interface configuration mode.
Step 11	**zone-member security** *zone-name* **Example:** `Device(config-if)# zone-member security z1`	Assigns an interface to a specified security zone. • When you make an interface a member of a security zone, all traffic into and out of that interface (except traffic bound for the device or initiated by the device) is dropped by default. To let traffic through the interface, you must make the zone a part of a zone pair to which you apply a policy. If the policy permits traffic, traffic can flow through that interface.
Step 12	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 13	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/3`	Configures an interface and enters interface configuration mode.
Step 14	**zone-member security** *zone-name* **Example:** `Device(config-if)# zone-member security z2`	Assigns an interface to a specified security zone.
Step 15	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for Configurable Number of Simultaneous Packets per Flow

Example: Configuring Class Maps and Policy Maps for Simultaneous Packets per Flow

```
Device# configure terminal
Device(config)# class-map type inspect match-any cmap-protocols
Device(config-cmap)# match protocol tcp
Device(config-cmap)# exit
Device(config)# policy-map type inspect policy1
Device(config-pmap)# class type inspect cmap-protocols
```

```
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap)# end
```

Example: Configuring the Number of Simultaneous Packets per Flow

You can configure the number of simultaneous packets per flow after configuring either the **parameter-map type inspect** command or the **parameter-map type inspect global** command. The number of simultaneous packets per flow configured under the **parameter-map type inspect** command overwrites the number configured under the **parameter-map type inspect global** command.

```
Device# configure terminal
Device(config)# parameter-map type inspect param1
Device(config-profile)# session packet 55
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# session packet 35
Device(config-profile)# end
```

Example: Configuring Zones for Simultaneous Packets per Flow

```
Device# configure terminal
Device(config)# zone security z1
Device(config-sec-zone)# exit
Device(config)# zone security z2
Device(config-sec-zone)# exit
Device(config)# zone-pair security zp-security source z1 destination z2
Device(config-sec-zone-pair)# service-policy type inspect policy1
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# zone-member security z1
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/0/3
Device(config-if)# zone-member security z2
Device(config-if)# end
```

Additional References for Configurable Number of Simultaneous Packets per Flow

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
Firewall commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Configurable Number of Simultaneous Packets per Flow

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 Configurable Number of Simultaneous Packets per Flow

Feature Name	Releases	Feature Information
Configurable Number of Simultaneous Packets per Flow	Cisco IOS XE Release 3.11S	In zone-based policy firewalls, the number of simultaneous packets per flow was restricted to 25, and packets that exceeded the limit were dropped. The dropping of packets when the number is reached impacts network performance. The Configurable Number of Simultaneous Packets per Flow feature allows you to configure the number of simultaneous packets per flow from 25 to 100. In Cisco IOS XE Release 3.11S, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers, the Cisco 4400 Series Integrated Services Routers, and the Cisco Cloud Services Routers 1000V Series. The following commands were introduced or modified: **session packet**, **show parameter-map type inspect**, **show platform hardware qfp feature firewall datapath scb**, **show platform hardware qfp feature firewall zone-pair**, and **show platform software firewall parameter-map**.