Nested Class Map Support for Zone-Based Policy Firewall

The Nested Class Map Support for Zone-Based Policy Firewall feature provides the Cisco IOS XE firewall the functionality to configure multiple traffic classes (which are also called nested class maps or hierarchical class maps) as a single traffic class. When packets meet more than one match criterion, you can configure multiple class maps that can be associated with a single traffic policy. The Cisco IOS XE firewall supports up to three levels of class map hierarchy.

Prerequisites for Nested Class Map Support for Zone-Based Policy Firewall

Before configuring nested class maps, you should be familiar with the modular Quality of Service (QoS) CLI (MQC).

Information About Nested Class Map Support for Zone-Based Policy Firewall

Nested Class Maps

In Cisco IOS XE Release 3.5S and later releases, you can configure multiple traffic classes (which are also called nested class maps or hierarchical class maps) as a single traffic class. When packets meet more than one match criterion, you can configure multiple class maps that can be associated with a single traffic policy. The nesting of class maps can be achieved by configuring the **match class-map** command. The only method

of combining the match-any and match-all characteristics within a single traffic class is by using the **class-map** command.

match-all and match-any Keywords of the class-map Command

To create a traffic class, you must configure the **class-map** command with the **match-all** and **match-any** keywords. You need to specify the **match-all** and **match-any** keywords only if more than one match criterion is configured in the traffic class. The following rules apply to the **match-all** and **match-any** keywords:

- Use the **match-all** keyword when all match criteria in the traffic class must be met to place a packet in the specified traffic class.
- Use the **match-any** keyword when only one of the match criterion in the traffic class must be met to place a packet in the specified traffic class.
- If you do not specify the **match-all** keyword or the **match-any** keyword, the traffic class behaves in a manner that is consistent with the **match-all** keyword.

Your zone-based policy firewall configuration supports nested class maps if the following criteria are met:

- Individual class maps in a hierarchy include multiple **match class-map** command references.
- Individual class maps in a hierarchy include match rules other than the **match class-map** command.

How to Configure Nested Class Map Support for Zone-Based Policy Firewall

Configuring a Two-Layer Nested Class Map

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **class-map match-any** *class-map-name*
7. **match protocol** *protocol-name*
8. **exit**
9. **class-map match-any** *class-map-name*
10. **match class-map** *class-map-name*
11. **match class-map** *class-map-name*
12. **end**

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	**class-map match-any** *class-map-name* **Example:** `Router(config)# class-map match-any child1`	Creates a Layer 3 or Layer 4 class map and enters class map configuration mode.
Step 4	**match protocol** *protocol-name* **Example:** `Router(config-cmap)# match protocol tcp`	Configures the match criteria for a class map on the basis of a specified protocol.
Step 5	**exit** **Example:** `Router(config-cmap)# exit`	Exits class map configuration mode and enters global configuration mode.
Step 6	**class-map match-any** *class-map-name* **Example:** `Router(config)# class-map match-any child2`	Creates a Layer 3 or Layer 4 class map and enters class map configuration mode.
Step 7	**match protocol** *protocol-name* **Example:** `Router(config-cmap)# match protocol udp`	Configures the match criteria for a class map on the basis of a specified protocol.
Step 8	**exit** **Example:** `Router(config-cmap)# exit`	Exits class map configuration mode and enters global configuration mode.
Step 9	**class-map match-any** *class-map-name* **Example:** `Router(config)# class-map match-any parent`	Creates a Layer 3 or Layer 4 class map and enters class map configuration mode.
Step 10	**match class-map** *class-map-name* **Example:** `Router(config-cmap)# match class-map child1`	Configures a traffic class as a classification policy.

	Command or Action	Purpose
Step 11	**match class-map** *class-map-name* **Example:** `Router(config-cmap)# match class-map child2`	Configures a traffic class as a classification policy.
Step 12	**end** **Example:** `Router(config-cmap)# end`	Exits class map configuration mode and enters privileged EXEC mode.

Configuring a Policy Map for a Nested Class Map

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class-type inspect** *class-map-name*
5. **inspect**
6. **end**

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	**policy-map type inspect** *policy-map-name* **Example:** `Router(config)# policy-map type inspect pmap`	Creates a Layer 3 or Layer 4 inspect type policy map and enters policy map configuration mode.
Step 4	**class-type inspect** *class-map-name* **Example:** `Router(config-pmap)# class-type inspect parent`	Specifies the traffic (class) on which an action is to be performed and enters policy-map class configuration mode.
Step 5	**inspect** **Example:**	Enables Cisco IOS XE stateful packet inspection.

	Command or Action	Purpose
	`Router(config-pmap-c)# inspect`	
Step 6	**end** **Example:** `Router(config-pmap-c)# end`	Exits policy-map class configuration mode and enters privileged EXEC mode.

Attaching a Policy Map to a Zone Pair

SUMMARY STEPS

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

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	**zone security** *zone-name* **Example:** `Router(config)# zone security source-zone`	Creates a security zone to which interfaces can be assigned and enters security zone configuration mode.
Step 4	**exit** **Example:** `Router(config-sec-zone)# exit`	Exits security zone configuration mode and enters global configuration mode.

	Command or Action	Purpose
Step 5	**zone security** *zone-name* **Example:** `Router(config)# zone security destination-zone`	Creates a security zone to which interfaces can be assigned and enters security zone configuration mode.
Step 6	**exit** **Example:** `Router(config-sec-zone)# exit`	Exits security zone configuration mode and enters global configuration mode.
Step 7	**zone-pair security** *zone-pair-name* [**source** *zone-name* **destination** [*zone-name*]] **Example:** `Router(config)# zone-pair security secure-zone source source-zone destination destination-zone`	Creates a zone pair and enters security zone pair configuration mode. • To apply a policy, you must configure a zone pair.
Step 8	**service-policy type inspect** *policy-map-name* **Example:** `Router(config-sec-zone-pair)# service-policy type inspect pmap`	Attaches a firewall policy map to the destination zone pair. **Note** If a policy is not configured between a pair of zones, traffic is dropped by default.
Step 9	**exit** **Example:** `Router(config-sec-zone-pair)# exit`	Exits security zone pair configuration mode and enters global configuration mode.
Step 10	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/0/1`	Configures an interface and enters interface configuration mode.
Step 11	**zone-member security** *zone-name* **Example:** `Router(config-if)# zone-member security source-zone`	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 router or initiated by the router) is dropped by default. To let traffic through the interface, you must make the zone part of a zone pair to which you apply a policy. If the policy permits traffic, traffic can flow through that interface.
Step 12	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and enters privileged EXEC mode.

Configuration Examples for Nested Class Map Support for Zone-Based Policy Firewall

Example: Configuring a Two-Layer Nested Class Map

```
Router# configure terminal
Router(config)# class-map match-any child1
Router(config-cmap)# match protocol tcp
Router(config-cmap)# exit
Router(config)# class-map match-any child2
Router(config-cmap)# match protocol udp
Router(config-cmap)# exit
Router(config)# class-map match-any parent
Router(config-cmap)# match class-map child1
Router(config-cmap)# match class-map child2
Router(config-cmap)# end
```

Example: Configuring a Policy Map for a Nested Class Map

```
Router# configure terminal
Router(config)# policy-map type inspect pmap
Router(config-pmap)# class-type inspect parent
Router(config-pmap-c)# inspect
Router(config-pmap-c)# end
```

Example: Attaching a Policy Map to a Zone Pair

```
Router# configure terminal
Router(config)# zone security source-zone
Router(config-sec-zone)# exit
Router(config)# zone security destination-zone
Router(config-sec-zone)# exit
Router(config)# zone-pair security secure-zone source source-zone destination destination-zone
Router(config-sec-zone-pair)# service-policy type inspect pmap
Router(config-sec-zone-pair)# exit
Router(config)# interface gigabitethernet 0/0/1
Router(config-if)# zone-member security source-zone
Router(config-if)# end
```

Additional References for Nested Class Map Support for Zone-Based Policy Firewall

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security 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
Zone-based policy firewall	*Zone-Based Policy Firewall*

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 Nested Class Map Support for Zone-Based Policy Firewall

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 Nested Class Map Support for Zone-Based Policy Firewall

Feature Name	Releases	Feature Information
Nested Class Map Support for Zone-Based Policy Firewall	Cisco IOS XE Release 3.5S	The Nested Class Map Support for Zone-Based Policy Firewall feature provides the Cisco IOS XE firewall the functionality to configure multiple traffic classes (which are also called nested class maps or hierarchical class maps) as a single traffic class. When packets meet more than one match criterion, you can configure multiple class maps that can be associated with a single traffic policy.