



Zone-Based Policy Firewall IPv6 Support

The zone-based policy firewall IPv6 support feature coexists with the zone-based policy firewall for IPv4 in order to support IPv6 traffic. The feature provides MIB support for TCP, UDP, ICMPv6, and FTP sessions. This document describes how to configure parameter-maps, and to create and use class maps, policy maps, zones and zone pairs.

- [Finding Feature Information, page 1](#)
- [Information About Zone-Based Policy Firewall IPv6 Support, page 1](#)
- [How to Configure Zone-Based Policy Firewall IPv6 Support, page 2](#)
- [Configuration Examples for Zone-Based Policy Firewall IPv6 Support, page 6](#)
- [Additional References for Zone-Based Policy Firewall IPv6 Support, page 7](#)
- [Feature Information for Zone-Based Policy Firewall IPv6 Support, page 8](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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.

Information About Zone-Based Policy Firewall IPv6 Support

Zone-Based Policy Firewall IPv6 Support

The zone-based policy firewall for IPv6 coexists with the zone-based policy firewall for IPv4 in order to support IPv6 traffic. The feature provides MIB support for TCP, UDP, ICMPv6, and FTP sessions.

How to Configure Zone-Based Policy Firewall IPv6 Support

Configuring an Inspect-Type Parameter Map

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `parameter-map type inspect {parameter-map-name | global | default}`
4. `sessions maximum sessions`
5. `ipv6 routing-enforcement-header loose`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	parameter-map type inspect {parameter-map-name global default} Example: Router(config)# parameter-map type inspect v6-param-map	Configures an inspect type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the inspect action, and places the router in parameter map configuration mode.
Step 4	sessions maximum sessions Example: Router(config-profile)# sessions maximum 10000	Sets the maximum number of allowed sessions that can exist on a zone pair.
Step 5	ipv6 routing-enforcement-header loose Example: Router(config-profile)# ipv6 routing-enforcement-header loose	Provides backward compatibility with legacy IPv6 inspection.

Creating and Using an Inspect-Type Class Map

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `class-map type inspect {match-any | match-all} class-map-name`
4. `match protocol tcp`
5. `match protocol udp`
6. `match protocol icmp`
7. `match protocol ftp`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p><code>configure terminal</code></p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p><code>class-map type inspect {match-any match-all} class-map-name</code></p> <p>Example:</p> <pre>Router(config-profile)# class-map type inspect match-any v6-class</pre>	<p>Create an inspect type class map, and places the router in lass-map configuration mode.</p>
Step 4	<p><code>match protocol tcp</code></p> <p>Example:</p> <pre>Router(config-cmap)# match protocol tcp</pre>	<p>Configures the match criterion for a class map based on TCP.</p>
Step 5	<p><code>match protocol udp</code></p> <p>Example:</p> <pre>Router(config-cmap)# match protocol udp</pre>	<p>Configures the match criterion for a class map based on UDP.</p>

	Command or Action	Purpose
Step 6	match protocol icmp Example: <pre>Router(config-cmap)# match protocol icmp</pre>	Configures the match criterion for a class map based on ICMP.
Step 7	match protocol ftp Example: <pre>Router(config-cmap)# match protocol ftp</pre>	Configures the match criterion for a class map based on FTP.

Creating and Using an Inspect-Type Policy 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 [*parameter-map-name*]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	policy-map type inspect <i>policy-map-name</i> Example: <pre>Router(config)# policy-map type inspect v6-policy</pre>	Creates an inspect-type policy map, and places the router in policy-map configuration mode.

	Command or Action	Purpose
Step 4	class type inspect <i>class-map-name</i> Example: <pre>Router(config-pmap)# class type inspect v6-class</pre>	Specifies the traffic (class) on which an action is to be performed.
Step 5	inspect [<i>parameter-map-name</i>] Example: <pre>Router(config-pmap)# inspect</pre>	Enables Cisco IOS stateful packet inspection.

Creating Security Zones and Zone Pairs

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **zone security** {*zone-name* | **default**}
4. **zone security** {*zone-name* | **default**}
5. **zone-pair security** *zone-pair-name* **source** {*source-zone-name* | **self** | **default**} **destination** {*destination-zone-name* | **self** | **default**}
6. **service-policy type inspect** *policy-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	zone security { <i>zone-name</i> default }	Creates a security zone.

	Command or Action	Purpose
	<p>Example:</p> <pre>Router(config)# zone security 1</pre>	<ul style="list-style-type: none"> • Cisco recommends that you create at least two security zones so that you can create a zone pair.
Step 4	<p>zone security {<i>zone-name</i> default}</p> <p>Example:</p> <pre>Router(config)# zone security 2</pre>	<p>Creates a security zone.</p> <ul style="list-style-type: none"> • Cisco recommends that you create at least two security zones so that you can create a zone pair.
Step 5	<p>zone-pair security <i>zone-pair-name</i> source {<i>source-zone-name</i> self default} destination {<i>destination-zone-name</i> self default}</p> <p>Example:</p> <pre>Router(config)# zone-pair security zp source z1 destination z2</pre>	<p>Creates a zone pair, and places the router in zone-pair configuration mode.</p>
Step 6	<p>service-policy type inspect <i>policy-map-name</i></p> <p>Example:</p> <pre>Router(config-sec-zone-pair)# service-policy type inspect v6-policy</pre>	<p>Attaches a firewall policy map to a zone pair.</p>

Configuration Examples for Zone-Based Policy Firewall IPv6 Support

Example: Configuring Cisco IOS Zone-Based Firewall for IPv6

```
parameter-map type inspect v6-param-map
sessions maximum 10000
ipv6 routing-header-enforcement loose
!
!
class-map type inspect match-any v6-class
match protocol tcp
match protocol udp
match protocol icmp
match protocol ftp
!
!
policy-map type inspect v6-policy
class type inspect v6-class
inspect
!
```

```

zone security z1
zone security z2
!
zone-pair security zp source z1 destination z2
service-policy type inspect v6-policy

```

Additional References for Zone-Based Policy Firewall IPv6 Support

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	<i>Cisco IOS IPv6 Command Reference</i>
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	<i>IPv6 RFCs</i>

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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 Zone-Based Policy Firewall IPv6 Support

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 Zone-Based Policy Firewall IPv6 Support

Feature Name	Releases	Feature Information
Zone-Based Policy Firewall IPv6 Support	15.1(2)T	Cisco zone-based firewall for IPv6 coexists with Cisco zone-based firewall for IPv4 in order to support IPv6 traffic.