

# Junos<sup>®</sup> OS for EX Series Ethernet Switches

## Routing Policy and Packet Filtering for EX Series Switches

Release  
**12.3**



---

Published: 2013-01-30

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

*Junos® OS for EX Series Ethernet Switches Routing Policy and Packet Filtering for EX Series Switches*

Release 12.3

Copyright © 2013, Juniper Networks, Inc.

All rights reserved.

The information in this document is current as of the date on the title page.

## YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

## END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

	About the Documentation . . . . .	xi
	Documentation and Release Notes . . . . .	xi
	Using the Examples in This Manual . . . . .	xi
	Merging a Full Example . . . . .	xii
	Merging a Snippet . . . . .	xii
	Documentation Conventions . . . . .	xiii
	Documentation Feedback . . . . .	xiv
	Requesting Technical Support . . . . .	xv
	Self-Help Online Tools and Resources . . . . .	xv
	Opening a Case with JTAC . . . . .	xvi
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Security Features Overview . . . . .</b>	<b>3</b>
	Security Features for EX Series Switches Overview . . . . .	3
<b>Chapter 2</b>	<b>Firewall Filters Overview . . . . .</b>	<b>7</b>
	Firewall Filters for EX Series Switches Overview . . . . .	7
	Firewall Filter Types . . . . .	8
	Firewall Filter Components . . . . .	9
	Firewall Filter Processing . . . . .	10
	Understanding Planning of Firewall Filters . . . . .	11
	Understanding Firewall Filter Processing Points for Bridged and Routed Packets on EX Series Switches . . . . .	13
	Understanding How Firewall Filters Control Packet Flows . . . . .	15
	Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches . . . . .	16
	Firewall Filter Elements . . . . .	17
	Match Conditions Supported on Switches . . . . .	17
	Actions for Firewall Filters . . . . .	24
	Action Modifiers for Firewall Filters . . . . .	24
	Support for Match Conditions and Actions for Loopback Firewall Filters on Switches . . . . .	26
	Platform Support for Firewall Filter Match Conditions, Actions, and Action Modifiers on EX Series Switches . . . . .	29
	Firewall Filter Types and Their Bind Points . . . . .	30
	Support for IPv4 and IPv6 Firewall Filters on Switches . . . . .	31
	Platform Support for Match Conditions for IPv4 Traffic . . . . .	31
	Platform Support for Match Conditions for IPv6 Traffic . . . . .	41
	Platform Support for Match Conditions for Non-IP Traffic . . . . .	47
	Platform Support for Actions for IPv4 Traffic . . . . .	48

	Platform Support for Actions for IPv6 Traffic . . . . .	50
	Platform Support for Action Modifiers for IPv4 Traffic . . . . .	52
	Platform Support for Action Modifiers for IPv6 Traffic . . . . .	56
	Understanding How Firewall Filters Are Evaluated . . . . .	60
	Understanding Firewall Filter Match Conditions . . . . .	62
	Filter Match Conditions . . . . .	62
	Numeric Filter Match Conditions . . . . .	62
	Interface Filter Match Conditions . . . . .	63
	IP Address Filter Match Conditions . . . . .	63
	MAC Address Filter Match Conditions . . . . .	64
	Bit-Field Filter Match Conditions . . . . .	64
	Understanding How Firewall Filters Test a Packet's Protocol . . . . .	66
	Understanding the Use of Policers in Firewall Filters . . . . .	66
	Policers Overview . . . . .	66
	Policer Types . . . . .	67
	Policer Actions . . . . .	68
	Policer Levels . . . . .	68
	Color Modes . . . . .	69
	Naming Conventions for Policers . . . . .	69
	Understanding Filter-Based Forwarding for EX Series Switches . . . . .	70
	Understanding Tricolor Marking Architecture . . . . .	70
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 3</b>	<b>Configuration Examples . . . . .</b>	<b>75</b>
	Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches . . . . .	75
	Example: Configuring a Firewall Filter on a Management Interface on an EX Series Switch . . . . .	93
	Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches . . . . .	96
	Example: Applying Firewall Filters to Multiple Suplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication . . . . .	100
<b>Chapter 4</b>	<b>Configuration Tasks . . . . .</b>	<b>107</b>
	Configuring Firewall Filters (CLI Procedure) . . . . .	107
	Configuring a Firewall Filter . . . . .	107
	Configuring a Term Specifically for IPv4 or IPv6 Traffic . . . . .	110
	Applying a Firewall Filter to a Port on a Switch . . . . .	111
	Applying a Firewall Filter to a Management Interface on a Switch . . . . .	112
	Applying a Firewall Filter to a VLAN on a Network . . . . .	113
	Applying a Firewall Filter to a Layer 3 (Routed) Interface . . . . .	114
	Configuring Firewall Filters (J-Web Procedure) . . . . .	115
	Configuring Policers to Control Traffic Rates (CLI Procedure) . . . . .	119
	Configuring Policers . . . . .	120
	Specifying Policers in a Firewall Filter Configuration . . . . .	121
	Applying a Firewall Filter That Is Configured with a Policers . . . . .	121
	Assigning Multifield Classifiers in Firewall Filters to Specify Packet-Forwarding Behavior (CLI Procedure) . . . . .	122
	Configuring Routing Policies (J-Web Procedure) . . . . .	123

	Configuring Tricolor Marking Policers . . . . .	128
	Configuring a Tricolor Marking Policer . . . . .	129
	Applying Tricolor Marking Policers to Firewall Filters . . . . .	129
<b>Chapter 5</b>	<b>Configuration Statements . . . . .</b>	<b>131</b>
	[edit firewall] Configuration Statement Hierarchy on EX Series Switches . . . . .	131
	Supported Statements in the [edit firewall] Hierarchy Level . . . . .	131
	Unsupported Statements in the [edit firewall] Hierarchy Level . . . . .	132
	Firewall Filter Configuration Statements Supported by Junos OS for EX Series	
	Switches . . . . .	133
	action (TCM Policers) . . . . .	136
	apply-path . . . . .	136
	as-path (Policy Options) . . . . .	137
	as-path-group . . . . .	138
	bandwidth-limit . . . . .	139
	burst-size-limit . . . . .	140
	color-aware . . . . .	141
	color-blind . . . . .	141
	committed-burst-size . . . . .	142
	committed-information-rate . . . . .	143
	community (Policy Options) . . . . .	144
	condition . . . . .	146
	counter . . . . .	147
	damping (Policy Options) . . . . .	148
	dynamic-db . . . . .	149
	excess-burst-size . . . . .	150
	family (Firewall Filter) . . . . .	151
	filter (Firewall Filters) . . . . .	152
	filter (VLANs) . . . . .	153
	filter-specific . . . . .	153
	firewall . . . . .	154
	from . . . . .	155
	if-exceeding . . . . .	156
	interface-specific . . . . .	157
	loss-priority high then discard (Three-Color Policer) . . . . .	157
	peak-burst-size . . . . .	158
	policer . . . . .	159
	policy-statement . . . . .	160
	prefix-list . . . . .	162
	routing-instance . . . . .	163
	single-rate . . . . .	164
	term . . . . .	165
	then (Firewall Filters) . . . . .	166
	then (Policer Action) . . . . .	167
	three-color-policer (Configuring) . . . . .	168
	two-rate . . . . .	169

<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 6</b>	<b>Routine Monitoring</b>	<b>173</b>
	Verifying That Firewall Filters Are Operational	173
	Verifying That Policers Are Operational	174
	Monitoring Firewall Filter Traffic	174
	Monitoring Traffic for All Firewall Filters and Policers That Are Configured on the Switch	175
	Monitoring Traffic for a Specific Firewall Filter	175
	Monitoring Traffic for a Specific Policer	175
<b>Chapter 7</b>	<b>Operational Commands</b>	<b>177</b>
	clear firewall	178
	show firewall	180
	show firewall log	187
	show policer	190
	show policy	192
	show policy conditions	194
	test policy	196
<b>Part 4</b>	<b>Troubleshooting</b>	
<b>Chapter 8</b>	<b>Troubleshooting Procedures</b>	<b>201</b>
	Troubleshooting Firewall Filters	201
	A Firewall Filter Configuration Returns a “No Space Available in TCAM” Message	201

# List of Figures

<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 2</b>	<b>Firewall Filters Overview</b> .....	<b>7</b>
	Figure 1: Firewall Filter Processing Points in the Packet Forwarding Path .....	14
	Figure 2: Application of Firewall Filters to Control Packet Flow .....	16
	Figure 3: Evaluation of Terms Within a Firewall Filter .....	61
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 3</b>	<b>Configuration Examples</b> .....	<b>75</b>
	Figure 4: Application of Port, VLAN, and Layer 3 Routed Firewall Filters .....	77
	Figure 5: SSH Connection From a Management PC to an EX Series Switch .....	94
	Figure 6: Conceptual Model: Dynamic Filter Updated for Each New User .....	102
	Figure 7: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server .....	103





# List of Tables

	<b>About the Documentation . . . . .</b>	<b>xi</b>
	Table 1: Notice Icons . . . . .	xiii
	Table 2: Text and Syntax Conventions . . . . .	xiii
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 2</b>	<b>Firewall Filters Overview . . . . .</b>	<b>7</b>
	Table 3: Elements of a Firewall Filter Configuration . . . . .	17
	Table 4: Firewall Filter Match Conditions Supported on EX Series Switches . . . . .	17
	Table 5: Actions for Firewall Filters . . . . .	24
	Table 6: Action Modifiers for Firewall Filters . . . . .	25
	Table 7: Match Conditions for Firewall Filters on Loopback Interfaces for IPv4 and IPv6 Traffic—Support per Switch . . . . .	27
	Table 8: Actions for Firewall Filters on Loopback Interfaces for IPv4 and IPv6 Traffic—Support per Switch . . . . .	28
	Table 9: Action Modifiers for Firewall Filters on Loopback Interfaces for IPv4 and IPv6 Traffic—Support per Switch . . . . .	29
	Table 10: Bind Points Associated with Firewall Filter Types . . . . .	30
	Table 11: Support for IPv4 and IPv6 Firewall Filters on Switches . . . . .	31
	Table 12: Firewall Filter Match Conditions Supported for IPv4 Traffic on Switches . . . . .	32
	Table 13: Firewall Filter Match Conditions Supported for IPv6 Traffic on Switches . . . . .	42
	Table 14: Firewall Filter Match Condition Supported for Non-IP Traffic on Switches . . . . .	48
	Table 15: Firewall Filter Actions Supported for IPv4 Traffic on Switches . . . . .	48
	Table 16: Firewall Filter Actions Supported for IPv6 Traffic on Switches . . . . .	50
	Table 17: Firewall Filter Action Modifiers Supported for IPv4 Traffic on Switches . . . . .	52
	Table 18: Firewall Filter Action Modifiers Supported for IPv6 Traffic on Switches . . . . .	57
	Table 19: Logical Operators for Matching Multiple Bit-Field Operators . . . . .	65
	Table 20: Policer Actions . . . . .	68
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 3</b>	<b>Configuration Examples . . . . .</b>	<b>75</b>
	Table 21: Configuration Components: Firewall Filters . . . . .	76
	Table 22: Configuration Components: VLANs . . . . .	78
	Table 23: Configuration Components: Switch Ports on a 48-Port All-PoE Switch . . . . .	78

<b>Chapter 4</b>	<b>Configuration Tasks . . . . .</b>	<b>107</b>
	Table 24: Create a New Filter . . . . .	116
	Table 25: Create a New Term . . . . .	116
	Table 26: Advanced Options for Terms . . . . .	117
	Table 27: Policies Global Configuration Parameters . . . . .	124
	Table 28: Terms Configuration Parameters . . . . .	125
<b>Chapter 5</b>	<b>Configuration Statements . . . . .</b>	<b>131</b>
	Table 29: Supported Options for Firewall Filter Statements . . . . .	133
	Table 30: Firewall Filter Statements That Are Not Supported by Junos OS for EX Series Switches . . . . .	134
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 7</b>	<b>Operational Commands . . . . .</b>	<b>177</b>
	Table 31: show firewall Output Fields . . . . .	181
	Table 32: show firewall log Output Fields . . . . .	187
	Table 33: show policer Output Fields . . . . .	190
	Table 34: show policy Output Fields . . . . .	192
	Table 35: show policy conditions Output Fields . . . . .	194

# About the Documentation

- Documentation and Release Notes on page xi
- Using the Examples in This Manual on page xi
- Documentation Conventions on page xiii
- Documentation Feedback on page xiv
- Requesting Technical Support on page xv

## Documentation and Release Notes

---

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

## Using the Examples in This Manual

---

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

## Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

## Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the CLI User Guide.

## Documentation Conventions

Table 1 on page xiii defines notice icons used in this guide.

Table 1: Notice Icons





Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xiii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> <b>show chassis alarms</b> No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces or emphasizes important new terms.</li> <li>Identifies book names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS System Basics Configuration Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name:  [edit] root@# <b>set system domain-name</b> <i>domain-name</i>
<b>Text like this</b>	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the [edit protocols ospf area area-id] hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>
< > (angle brackets)	Enclose optional keywords or variables.	<b>stub</b> <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	<b>broadcast</b>   <b>multicast</b>  ( <i>string1</i>   <i>string2</i>   <i>string3</i> )
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	<b>community name members</b> [ <i>community-ids</i> ]
Indentation and braces ( { } )	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
<b>J-Web GUI Conventions</b>		
<b>Bold text like this</b>	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> <li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul>
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at

<https://www.juniper.net/cgi-bin/docbugreport/> . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

## Requesting Technical Support

---

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

## Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.



## PART 1

# Overview

- [Security Features Overview on page 3](#)
- [Firewall Filters Overview on page 7](#)



## CHAPTER 1

# Security Features Overview

- [Security Features for EX Series Switches Overview on page 3](#)

## Security Features for EX Series Switches Overview

---

Juniper Networks Junos operating system (Junos OS) is a network operating system that has been hardened through the separation of control forwarding and services planes, with each function running in protected memory. The control-plane CPU is protected by rate limiting, routing policy, and firewall filters to ensure switch uptime even under severe attack. In addition, the switches fully integrate with the Juniper Networks Unified Access Control (UAC) product to provide both standards-based 802.1X port-level access and Layer 2 through Layer 4 policy enforcement based on user identity. Access port security features such as dynamic Address Resolution Protocol (ARP) inspection, DHCP snooping, and MAC limiting are controlled through a single Junos OS CLI command.

Juniper Networks EX Series Ethernet Switches provide the following hardware and software security features:

**Console Port**—Allows use of the console port to connect to the Routing Engine through an RJ-45 cable. You then use the command-line interface (CLI) to configure the switch.

**Out-of-Band Management**—A dedicated management Ethernet port on the rear panel allows out-of-band management.

**Software Images**—All Junos OS images are signed by Juniper Networks certificate authority (CA) with public key infrastructure (PKI).

**User Authentication, Authorization, and Accounting (AAA)**—Features include:

- User and group accounts with password encryption and authentication.
- Access privilege levels configurable for login classes and user templates.
- RADIUS authentication, TACACS+ authentication, or both, for authenticating users who attempt to access the switch.
- Auditing of configuration changes through system logging or RADIUS/TACACS+.

**802.1X Authentication**—Provides network access control. Supplicants (hosts) are authenticated when they initially connect to a LAN. Authenticating supplicants before they receive an IP address from a DHCP server prevents unauthorized supplicants from

gaining access to the LAN. EX Series switches support Extensible Authentication Protocol (EAP) methods, including EAP-MD5, EAP-TLS, EAP-TTLS, and EAP-PEAP.

**Port Security**—Access port security features include:

- DHCP snooping—Filters and blocks ingress DHCP server messages on untrusted ports; builds and maintains an IP-address/MAC-address binding database (called the DHCP snooping database).
- Dynamic ARP inspection (DAI)—Prevents ARP spoofing attacks. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made based on the results of those comparisons.
- MAC limiting—Protects against flooding of the Ethernet switching table.
- MAC move limiting—Detects MAC movement and MAC spoofing on access ports.
- Trusted DHCP server—With a DHCP server on a trusted port, protects against rogue DHCP servers sending leases.
- IP source guard—Mitigates the effects of IP address spoofing attacks on the Ethernet LAN. The source IP address in the packet sent from an untrusted access interface is validated against the source MAC address in the DHCP snooping database. The packet is allowed for further processing if the source IP address to source MAC address binding is valid; if the binding is not valid, the packet is discarded.
- DHCP option 82—Also known as the DHCP relay agent information option. Helps protect the EX Series switch against attacks such as spoofing (forging) of IP addresses and MAC addresses and DHCP IP address starvation. Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client.
- Unrestricted proxy ARP—The switch responds to all ARP messages with its own MAC address. Hosts that are connected to the switch's interfaces cannot communicate directly with other hosts. Instead, all communications between hosts go through the switch.
- Restricted proxy ARP—The switch does not respond to an ARP request if the physical networks of the source and target of the ARP request are the same. It does not matter whether the destination host has the same IP address as the incoming interface or a different (remote) IP address. An ARP request for a broadcast address elicits no reply.

**Device Security**—Storm control permits the switch to monitor unknown unicast and broadcast traffic and drop packets, or shut down, or temporarily disable the interface when a specified traffic level is exceeded, thus preventing packets from proliferating and degrading the LAN. You can enable storm control on access interfaces or trunk interfaces.

**Firewall Filters**—Allow auditing of various types of security violations, including attempts to access the switch from unauthorized locations. Firewall filters can detect such attempts and create audit log entries when they occur. The filters can also restrict access by limiting traffic to source and destination MAC addresses, specific protocols, or, in combination with policers, to specified data rates to prevent denial of service (DoS) attacks.

**Policers**—Provide rate-limiting capability to control the amount of traffic that enters an interface, which acts to counter DoS attacks.

**Encryption Standards**—Supported standards include:

- 128-, 192-, and 256-bit Advanced Encryption Standard (AES)
- 56-bit Data Encryption Standard (DES) and 168-bit 3DES

**Related  
Documentation**

- 802.1X for EX Series Switches Overview
- [Firewall Filters for EX Series Switches Overview on page 7](#)
- Port Security Overview
- Understanding Proxy ARP on EX Series Switches
- Understanding Storm Control on EX Series Switches
- [Understanding the Use of Policers in Firewall Filters on page 66](#)
- Understanding Centralized Network Access Control and EX Series Switches



## CHAPTER 2

# Firewall Filters Overview

- [Firewall Filters for EX Series Switches Overview on page 7](#)
- [Understanding Planning of Firewall Filters on page 11](#)
- [Understanding Firewall Filter Processing Points for Bridged and Routed Packets on EX Series Switches on page 13](#)
- [Understanding How Firewall Filters Control Packet Flows on page 15](#)
- [Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 16](#)
- [Support for Match Conditions and Actions for Loopback Firewall Filters on Switches on page 26](#)
- [Platform Support for Firewall Filter Match Conditions, Actions, and Action Modifiers on EX Series Switches on page 29](#)
- [Understanding How Firewall Filters Are Evaluated on page 60](#)
- [Understanding Firewall Filter Match Conditions on page 62](#)
- [Understanding How Firewall Filters Test a Packet's Protocol on page 66](#)
- [Understanding the Use of Policers in Firewall Filters on page 66](#)
- [Understanding Filter-Based Forwarding for EX Series Switches on page 70](#)
- [Understanding Tricolor Marking Architecture on page 70](#)

## Firewall Filters for EX Series Switches Overview

---

Firewall filters provide rules that define whether to permit, deny, or forward packets that are transiting an interface on a Juniper Networks EX Series Ethernet Switch from a source address to a destination address. You configure firewall filters to determine whether to permit, deny, or forward traffic before it enters or exits a port, VLAN, or Layer 3 (routed) interface to which the firewall filter is applied. To apply a firewall filter, you must first configure the filter and then apply it to an port, VLAN, or Layer 3 interface.

You can apply firewall filters to network interfaces, aggregated Ethernet interfaces (also known as link aggregation groups (LAGs)), loopback interfaces, management interfaces, virtual management Ethernet interfaces (VMEs), and routed VLAN interfaces (RVIs). For information on EX Series switches that support a firewall filter on these interfaces, see [EX Series Switch Software Features Overview](#).

An *ingress* firewall filter is a filter that is applied to packets that are entering a network. An *egress* firewall filter is a filter that is applied to packets that are exiting a network. You can configure firewall filters to subject packets to filtering, class-of-service (CoS) marking (grouping similar types of traffic together, and treating each type of traffic as a class with its own level of service priority), and traffic policing (controlling the maximum rate of traffic sent or received on an interface).

This topic describes:

- [Firewall Filter Types on page 8](#)
- [Firewall Filter Components on page 9](#)
- [Firewall Filter Processing on page 10](#)

## Firewall Filter Types

The following firewall filter types are supported for EX Series switches:

- Port (Layer 2) firewall filter—Port firewall filters apply to Layer 2 switch ports. You can apply port firewall filters in both ingress and egress directions on a physical port.
- VLAN firewall filter—VLAN firewall filters provide access control for packets that enter a VLAN, are bridged within a VLAN, or leave a VLAN. You can apply VLAN firewall filters in both ingress and egress directions on a VLAN. VLAN firewall filters are applied to all packets that are forwarded to or forwarded from the VLAN.
- Router (Layer 3) firewall filter—You can apply a router firewall filter in both ingress and egress directions on Layer 3 (routed) interfaces and routed VLAN interfaces (RVIs). You can apply a router firewall filter in the ingress direction on the loopback interface (**lo0**) also. Firewall filters configured on loopback interfaces are applied only to packets that are sent to the Routing Engine CPU for further processing.

You can apply port, VLAN, or router firewall filters to *both* IPv4 and IPv6 traffic on these switches:

- EX3200 switch
- EX4200 switch
- EX8200 switch

You can apply port, VLAN, or router firewall filters to *only* IPv4 traffic on these switches:

- EX2200 switch
- EX3300 switch
- EX4500 switch
- EX6200 switch

For information on firewall filters supported on different switches, see “[Platform Support for Firewall Filter Match Conditions, Actions, and Action Modifiers on EX Series Switches](#)” on page 29.



## Firewall Filter Components

In a firewall filter, you first define the family address type (**ethernet-switching**, **inet**, or **inet6**), and then you define one or more terms that specify the filtering criteria (specified as terms with match conditions) and the action (specified as actions or action modifiers) to take if a match occurs.

The maximum number of terms allowed per firewall filter for EX Series switches is:

- 512 for EX2200 switches
- 1,436 for EX3300 switches



**NOTE:** On EX3300 switches, if you add and delete filters with a large number of terms (on the order of 1000 or more) in the same commit operation, not all the filters are installed. You must add filters in one commit operation, and delete filters in a separate commit operation.

- 7,042 for EX3200 and EX4200 switches—as allocated by the dynamic allocation of ternary content addressable memory (TCAM) for firewall filters.
- 1,200 for EX4500 and EX4550 switches
- 1,400 for EX6200 switches
- 32,768 for EX8200 switches



**NOTE:** The on-demand dynamic allocation of the shared space TCAM in EX8200 switches is achieved by assigning free space blocks to firewall filters. Firewall filters are categorized into two different pools. Port and VLAN filters are pooled together (the memory threshold for this pool is 22K) while router firewall filters are pooled separately (the threshold for this pool is 32K). The assignment happens based on the filter pool type. Free space blocks can be shared only among the firewall filters belonging to the same filter pool type. An error message is generated when you try to configure a firewall filter beyond the TCAM threshold.

Each term consists of the following components:

- Match conditions—Specify the values or fields that the packet must contain. You can define various match conditions, including the IP source address field, IP destination address field, Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source port field, IP protocol field, Internet Control Message Protocol (ICMP) packet type, TCP flags, and interfaces.
- Action—Specifies what to do if a packet matches the match conditions. Possible actions are to accept or discard the packet or to send the packet to a specific virtual routing interface. In addition, packets can be counted to collect statistical information. If no action is specified for a term, the default action is to accept the packet.

- Action modifier—Specifies one or more actions for the switch if a packet matches the match conditions. You can specify action modifiers such as count, mirror, rate limit, and classify packets.

## Firewall Filter Processing

The order of the terms within a firewall filter configuration is important. Packets are tested against each term in the order in which the terms are listed in the firewall filter configuration. For information on how firewall filters process packets, see [“Understanding How Firewall Filters Are Evaluated” on page 60](#).

### Related Documentation

- [Understanding Planning of Firewall Filters on page 11](#)
- [Understanding Firewall Filter Processing Points for Bridged and Routed Packets on EX Series Switches on page 13](#)
- [Understanding How Firewall Filters Are Evaluated on page 60](#)
- [Understanding Firewall Filter Match Conditions on page 62](#)
- [Understanding the Use of Policers in Firewall Filters on page 66](#)
- [Understanding Filter-Based Forwarding for EX Series Switches on page 70](#)
- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)
- [Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches on page 96](#)

---

## Understanding Planning of Firewall Filters

---

Before you create a firewall filter and apply it to an interface, determine what you want the firewall filter to accomplish and how to use its match conditions and actions to achieve your goals. You must understand how packets are matched to match conditions, the default and configured actions of the firewall filter, and proper placement of the firewall filter.

You can configure and apply no more than one firewall filter per port, VLAN, or router interface, per direction. The following limits apply for the number of firewall filter terms allowed per filter on various switch models:

- On EX2200 switches, the number of terms per filter cannot exceed 512.
- On EX3300 switches, the number of terms per filter cannot exceed 1436.
- On EX3200 and EX4200 switches, the number of terms per filter cannot exceed 7042.
- On EX4500 and EX4550 switches, the number of terms per filter cannot exceed 1200.
- On EX6200 switches, the number of terms per filter cannot exceed 1400.
- On EX8200 switches, the number of terms per filter cannot exceed 32768.

In addition, try to be conservative in the number of terms (rules) that you include in each firewall filter because a large number of terms requires longer processing time during a commit and also can make firewall filter testing and troubleshooting more difficult. Similarly, applying firewall filters across many switch and router interfaces can make testing and troubleshooting the rules of those filters difficult.

Before you configure and apply firewall filters, answer the following questions for each of those firewall filters:

1. What is the purpose of the firewall filter?

For example, you can use a firewall filter to limit traffic to source and destination MAC addresses, specific protocols, or certain data rates or to prevent denial of service (DoS) attacks.

2. What are the appropriate match conditions?

- a. Determine the packet header fields that the packet must contain for a match. Possible fields include:

- Layer 2 header fields—Source and destination MAC addresses, dot1q tag, Ethernet type, and VLAN
- Layer 3 header fields—Source and destination IP addresses, protocols, and IP options (IP precedence, IP fragmentation flags, TTL type)
- TCP header fields—Source and destination ports and flags
- ICMP header fields—Packet type and code

b. Determine the port, VLAN, or router interface on which the packet was received.

3. What are the appropriate actions to take if a match occurs?

Possible actions to take if a match occurs are accept, discard, and forward to a routing instance.

4. What additional action modifiers might be required?

Determine whether additional actions are required if a packet matches a match condition; for example, you can specify an action modifier to count, analyze, or police packets.

5. On what interface should the firewall filter be applied?

Start with the following basic guidelines:

- If all the packets entering a port need to be exposed to filtering, then use port firewall filters.
- If all the packets that are bridged need filtering, then use VLAN firewall filters.
- If all the packets that are routed need filtering, then use router firewall filters.

Before you choose the interface on which to apply a firewall filter, understand how that placement can impact traffic flow to other interfaces. In general, apply a firewall filter that filters on source and destination IP addresses, IP protocols, or protocol information—such as ICMP message types, and TCP and UDP port numbers—nearest to the source devices. However, typically apply a firewall filter that filters only on a source IP address nearest to the destination devices. When applied too close to the source device, a firewall filter that filters only on a source IP address could potentially prevent that source device from accessing other services that are available on the network.



**NOTE:** Egress firewall filters do not affect the flow of locally generated control packets from the Routing Engine.

---

6. In which direction should the firewall filter be applied?

You can apply firewall filters to ports on the switch to filter packets that are entering a port. You can apply firewall filters to VLANs, and Layer 3 (routed) interfaces to filter packets that are entering or exiting a VLAN or routed interface. Typically, you configure different sets of actions for traffic entering an interface than you configure for traffic exiting an interface.

**Related  
Documentation**

- [Firewall Filters for EX Series Switches Overview on page 7](#)
- [Understanding the Use of Policers in Firewall Filters on page 66](#)
- [Understanding How Firewall Filters Are Evaluated on page 60](#)
- [Understanding Filter-Based Forwarding for EX Series Switches on page 70](#)

- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)
- [Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches on page 96](#)

## Understanding Firewall Filter Processing Points for Bridged and Routed Packets on EX Series Switches

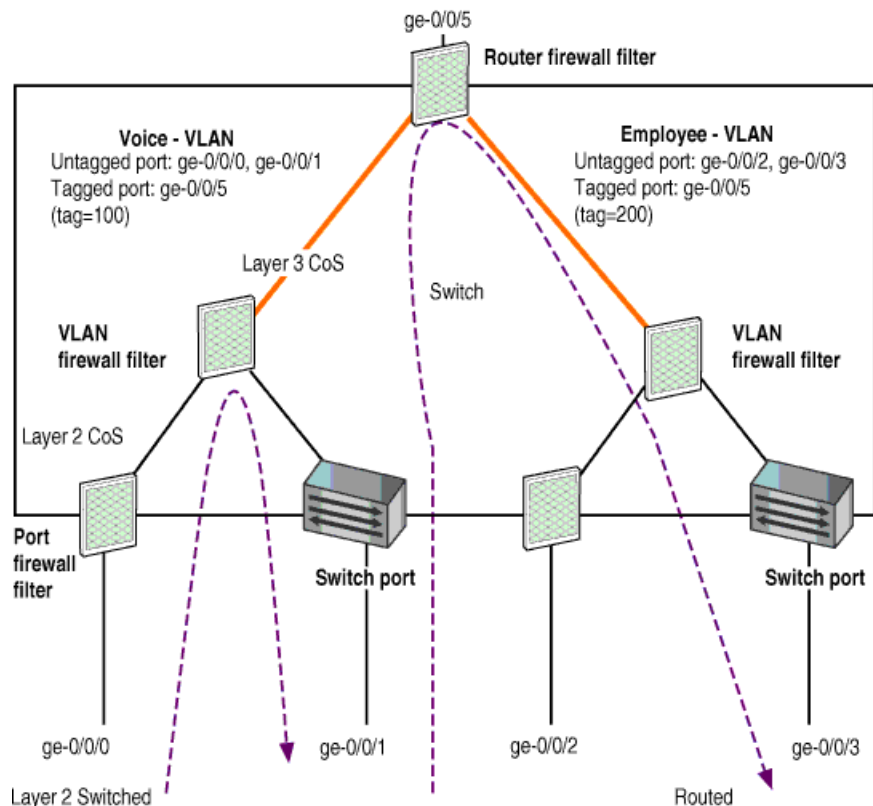
---

Juniper Networks EX Series Ethernet Switches are multilayered switches that provide Layer 2 switching and Layer 3 routing. You apply firewall filters at multiple processing points in the packet forwarding path on EX Series switches. At each processing point, the action to be taken on a packet is determined based on the results of the lookup in the switch's forwarding table. A table lookup determines which exit port on the switch to use to forward the packet.

For both bridged unicast packets and routed unicast packets, firewall filters are evaluated and applied hierarchically. First, a packet is checked against the port firewall filter, if present. If the packet is permitted, it is then checked against the VLAN firewall filter, if present. If the packet is permitted, it is then checked against the router firewall filter, if present. The packet must be permitted by the router firewall filter before it is processed.

[Figure 1 on page 14](#) shows the various firewall filter processing points in the packet forwarding path in a multilayered switching platform.

Figure 1: Firewall Filter Processing Points in the Packet Forwarding Path



g020007

For a multicast packet that results in replications, an egress firewall filter is applied to each copy of the packet based on its corresponding egress VLAN.

For Layer 2 (bridged) unicast packets, the following firewall filter processing points apply:

- Ingress port firewall filter
- Ingress VLAN firewall filter
- Egress port firewall filter
- Egress VLAN firewall filter

For Layer 3 (routed and multilayer-switched) unicast packets, the following firewall filter processing points apply:

- Ingress port firewall filter
- Ingress VLAN firewall filter (Layer 2 CoS)
- Ingress router firewall filter (Layer 3 CoS)
- Egress router firewall filter
- Egress VLAN firewall filter

- Related Documentation**
- [Firewall Filters for EX Series Switches Overview on page 7](#)
  - [Understanding How Firewall Filters Control Packet Flows on page 15](#)
  - [Understanding Bridging and VLANs on EX Series Switches](#)
  - [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)

---

## Understanding How Firewall Filters Control Packet Flows

Juniper Networks EX Series Ethernet Switches support firewall filters that allow you to control flows of data packets and local packets. *Data packets* are chunks of data that transit the switch as they are forwarded from a source to a destination. *Local packets* are chunks of data that are destined for or sent by the switch. Local packets usually contain routing protocol data, data for IP services such as Telnet or SSH, and data for administrative protocols such as the Internet Control Message Protocol (ICMP).

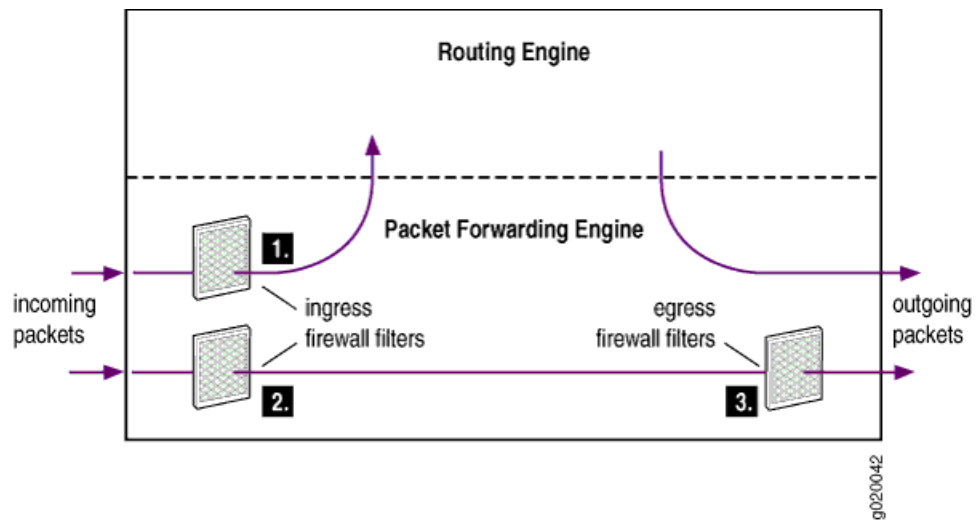
You create firewall filters to protect your switch from excessive traffic transiting the switch to a network destination or destined for the Routing Engine on the switch. Firewall filters that control local packets can also protect your switch from external incidents such as denial-of-service (DoS) attacks.

Firewall filters affect packet flows entering in to or exiting from the switch's interfaces:

- Ingress firewall filters affect the flow of data packets that are received by the switch's interfaces. The Packet Forwarding Engine handles this flow. When a switch receives a data packet on an interface, the switch determines where to forward the packet by looking in the forwarding table for the best route (Layer 2 switching, Layer 3 routing) to a destination. Data packets are forwarded to their destination through an outgoing interface. Locally destined packets are forwarded to the Routing Engine.
- Egress firewall filters affect the flow of data packets that are transmitted from the switch's interfaces but do not affect the flow of locally generated control packets from the Routing Engine. The Packet Forwarding Engine handles the flow of data packets that are transmitted from the switch, and egress firewall filters are applied here. The Packet Forwarding Engine also handles the flow of control packets from the Routing Engine.

[Figure 2 on page 16](#) illustrates the application of ingress and egress firewall filters to control the flow of packets through the switch.

Figure 2: Application of Firewall Filters to Control Packet Flow



1. Ingress firewall filter applied to control locally destined packets that are received on the switch's interfaces and are destined for the Routing Engine.
2. Ingress firewall filter applied to control incoming packets on the switch's interfaces.
3. Egress firewall filter applied to control packets that are transiting the switch's interfaces.

#### Related Documentation

- [Understanding Firewall Filter Processing Points for Bridged and Routed Packets on EX Series Switches on page 13](#)
- [Understanding How Firewall Filters Are Evaluated on page 60](#)

## Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches

When you define a firewall filter for an EX Series switch, you define filtering criteria (*terms*, with *match conditions*) for the packets and an *action* (and, optionally, an *action modifier*) for the switch to take if the packets match the filtering criteria. You can define a firewall filter to monitor IPv4, IPv6, or non-IP traffic.

This topic describes in detail the various match conditions, actions, and action modifiers that you can define in a firewall filter. For information about support for match conditions on various EX Series switches, see [“Platform Support for Firewall Filter Match Conditions, Actions, and Action Modifiers on EX Series Switches” on page 29](#).

This topic describes:

- [Firewall Filter Elements on page 17](#)
- [Match Conditions Supported on Switches on page 17](#)
- [Actions for Firewall Filters on page 24](#)
- [Action Modifiers for Firewall Filters on page 24](#)



## Firewall Filter Elements

A firewall filter configuration contains a term, a match condition, an action, and, optionally, an action modifier. [Table 3 on page 17](#) describes each element in a firewall filter configuration.

**Table 3: Elements of a Firewall Filter Configuration**

Element Name	Description
Term	Defines the filtering criteria for the packets. Each term in the firewall filter consists of match conditions and an action. You can define a single term or multiple terms in the firewall filter. If you define multiple terms, each term must have a unique name.
Match condition	Consists of a string (called a <i>match statement</i> ) that defines the match condition. Match conditions are the values or fields that a packet must contain. You can define a single match condition or multiple match conditions for a term. You can also opt not to define a match condition. If no match conditions are specified for a term, all packets are matched by default.
Action	Specifies the action that the switch takes if a packet matches all the criteria specified in the match conditions.
Action modifier	Specifies one or more actions that the switch takes if a packet matches the match conditions for the specific term.

## Match Conditions Supported on Switches

Based on the type of traffic that you want to monitor, you can configure a firewall filter to monitor IPv4, IPv6, or non-IP traffic. When you configure a firewall filter to monitor a particular type of traffic, ensure that you specify match conditions that are supported for that type of traffic. For information about match conditions supported for a specific type of traffic and switches on which they are supported, see [“Platform Support for Firewall Filter Match Conditions, Actions, and Action Modifiers on EX Series Switches” on page 29](#).

[Table 4 on page 17](#) describes all the match conditions that are supported for firewall filters on EX Series Switches.

**Table 4: Firewall Filter Match Conditions Supported on EX Series Switches**

Match Condition	Description
<b>destination-address</b> <i>ip-address</i>	IP destination address field, which is the address of the final destination node.
<b>destination-mac-address</b> <i>mac-address</i>	Destination media access control (MAC) address of the packet.  You can define a destination MAC address with a prefix, such as <b>destination-mac-address 00:01:02:03:04:05/24</b> . If no prefix is specified, the default value 48 is used.

Table 4: Firewall Filter Match Conditions Supported on EX Series Switches (*continued*)

Match Condition	Description
<b>destination-port</b> <i>number</i>	<p>TCP or UDP destination port field. Typically, you specify this match condition in conjunction with the <b>protocol</b> match condition to determine which protocol is used on the port. For <i>number</i>, you can specify one of the following text synonyms (the port numbers are also listed):</p> <p><b>afs</b> (1483), <b>bgp</b> (179), <b>biff</b> (512), <b>bootpc</b> (68), <b>bootps</b> (67),</p> <p><b>cmd</b> (514), <b>cvspserver</b> (2401),</p> <p><b>dhcp</b> (67), <b>domain</b> (53),</p> <p><b>eklogin</b> (2105), <b>ekshell</b> (2106), <b>exec</b> (512),</p> <p><b>finger</b> (79), <b>ftp</b> (21), <b>ftp-data</b> (20),</p> <p><b>http</b> (80), <b>https</b> (443),</p> <p><b>ident</b> (113), <b>imap</b> (143),</p> <p><b>kerberos-sec</b> (88), <b>klogin</b> (543), <b>kpasswd</b> (761), <b>krb-prop</b> (754), <b>krbupdate</b> (760), <b>kshell</b> (544),</p> <p><b>ldap</b> (389), <b>login</b> (513),</p> <p><b>mobileip-agent</b> (434), <b>mobileip-mn</b> (435), <b>msdp</b> (639),</p> <p><b>netbios-dgm</b> (138), <b>netbios-ns</b> (137), <b>netbios-ssn</b> (139), <b>nfsd</b> (2049), <b>nntp</b> (119), <b>ntalk</b> (518), <b>ntp</b> (123),</p> <p><b>pop3</b> (110), <b>pptp</b> (1723), <b>printer</b> (515),</p> <p><b>radacct</b> (1813), <b>radius</b> (1812), <b>rip</b> (520), <b>rkinit</b> (2108),</p> <p><b>smtp</b> (25), <b>snmp</b> (161), <b>snmptrap</b> (162), <b>snpp</b> (444), <b>socks</b> (1080), <b>ssh</b> (22), <b>sunrpc</b> (111), <b>syslog</b> (514),</p> <p><b>tacacs-ds</b> (65), <b>talk</b> (517), <b>telnet</b> (23), <b>tftp</b> (69), <b>timed</b> (525),</p> <p><b>who</b> (513),</p> <p><b>xdmcp</b> (177),</p> <p><b>zephyr-clt</b> (2103), <b>zephyr-hm</b> (2104)</p>
<b>destination-prefix-list</b> <i>prefix-list</i>	<p>IP destination prefix list field.</p> <p>You can define a list of IP address prefixes under a prefix-list alias for frequent use. You define this match condition at the <b>[edit policy-options]</b> hierarchy level.</p>
<b>dot1q-tag</b> <i>number</i>	<p>The tag field in the Ethernet header. The tag values range from 1 through 4095. The <b>dot1q-tag</b> match condition and the <b>vlan</b> match condition are mutually exclusive.</p>

Table 4: Firewall Filter Match Conditions Supported on EX Series Switches (*continued*)

Match Condition	Description
<b>dot1q-user-priority <i>number</i></b>	<p>User-priority field of the tagged Ethernet packet. User-priority values can range from 0 through 7.</p> <p>For <i>number</i>, you can specify one of the following text synonyms (the field values are also listed):</p> <ul style="list-style-type: none"> <li>• <b>background (1)</b>—Background</li> <li>• <b>best-effort (0)</b>—Best effort</li> <li>• <b>controlled-load (4)</b>—Controlled load</li> <li>• <b>excellent-load (3)</b>—Excellent load</li> <li>• <b>network-control (7)</b>—Network control reserved traffic</li> <li>• <b>standard (2)</b>—Standard or spare</li> <li>• <b>video (5)</b>—Video</li> <li>• <b>voice (6)</b>—Voice</li> </ul>
<b>dscp <i>number</i></b>	<p>Specifies the Differentiated Services code point (DSCP). The DiffServ protocol uses the type-of-service (ToS) byte in the IP header. The most significant six bits of this byte form the DSCP.</p> <p>You can specify DSCP in hexadecimal, binary, or decimal form.</p> <p>For <i>number</i>, you can specify one of the following text synonyms (the field values are also listed):</p> <ul style="list-style-type: none"> <li>• <b>ef (46)</b>—as defined in <a href="#">RFC 2598</a>, <i>An Expedited Forwarding PHB</i>.</li> <li>• <b>af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38)</b></li> </ul> <p>These four classes, with three drop precedences in each class, are defined for 12 code points in <a href="#">RFC 2597</a>, <i>Assured Forwarding PHB Group</i>.</p>

Table 4: Firewall Filter Match Conditions Supported on EX Series Switches (*continued*)

Match Condition	Description
<b>ether-type <i>value</i></b>	<p>Ethernet type field of a packet. The <i>value</i> specifies what protocol is being transported in the Ethernet frame. For <i>value</i>, you can specify one of the following text synonyms:</p> <ul style="list-style-type: none"> <li>• <b>aarp</b>—EtherType value AARP (0x80F3)</li> <li>• <b>appletalk</b>—EtherType value AppleTalk (0x809B)</li> <li>• <b>arp</b>—EtherType value ARP (0x0806)</li> <li>• <b>ipv4</b>—EtherType value IPv4 (0x0800)</li> <li>• <b>ipv6</b>—EtherType value IPv6 (0x08DD)</li> <li>• <b>mpls multicast</b>—EtherType value MPLS multicast (0x8848)</li> <li>• <b>mpls unicast</b>—EtherType value MPLS unicast (0x8847)</li> <li>• <b>oam</b>—EtherType value OAM (0x88A8)</li> <li>• <b>ppp</b>—EtherType value PPP (0x880B)</li> <li>• <b>pppoe-discovery</b>—EtherType value PPPoE Discovery Stage (0x8863)</li> <li>• <b>pppoe-session</b>—EtherType value PPPoE Session Stage (0x8864)</li> <li>• <b>sna</b>—EtherType value SNA (0x80D5)</li> </ul> <p><b>NOTE:</b> The following match conditions are not supported when <b>ether-type</b> is set to <b>ipv6</b>:</p> <ul style="list-style-type: none"> <li>• <b>dscp</b></li> <li>• <b>fragment-flags</b></li> <li>• <b>is-fragment</b></li> <li>• <b>precedence</b></li> <li>• <b>protocol</b></li> </ul>
<b>fragment-flags <i>fragment-flags</i></b>	<p>IP fragmentation flags, specified in symbolic or hexadecimal formats. You can specify one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>dont-fragment</b> (0x4000)</li> <li>• <b>more-fragments</b> (0x2000)</li> <li>• <b>reserved</b> (0x8000)</li> </ul>

Table 4: Firewall Filter Match Conditions Supported on EX Series Switches (*continued*)

Match Condition	Description
<b>icmp-code</b> <i>number</i>	<p>ICMP code field. This value or option provides more specific information than <b>icmp-type</b>. Because the value's meaning depends upon the associated <b>icmp-type</b>, you must specify <b>icmp-type</b> along with <b>icmp-code</b>. For <i>number</i>, you can specify one of the following text synonyms (the field values are also listed). The options are grouped by the ICMP type with which they are associated:</p> <ul style="list-style-type: none"> <li>parameter-problem—ip-header-bad (0), required-option-missing (1)</li> <li>redirect—redirect-for-host (1), redirect-for-network (0), redirect-for-tos-and-host (3), redirect-for-tos-and-net (2)</li> <li>time-exceeded—ttl-eq-zero-during-reassembly (1), ttl-eq-zero-during-transit (0)</li> <li>unreachable—communication-prohibited-by-filtering (13), destination-host-prohibited (10), destination-host-unknown (7), destination-network-prohibited (9), destination-network-unknown (6), fragmentation-needed (4), host-precedence-violation (14), host-unreachable (1), host-unreachable-for-TOS (12), network-unreachable (0), network-unreachable-for-TOS (11), port-unreachable (3), precedence-cutoff-in-effect (15), protocol-unreachable (2), source-host-isolated (8), source-route-failed (5)</li> </ul>
<b>icmp-type</b> <i>number</i>	<p>ICMP packet type field. Typically, you specify this match condition in conjunction with the <b>protocol</b> match condition to determine which protocol is being used on the port. For <i>number</i>, you can specify one of the following text synonyms (the field values are also listed):</p> <p>echo-reply (0), echo-request (8), info-reply (16), info-request (15), mask-request (17), mask-reply (18), parameter-problem (12), redirect (5), router-advertisement (9), router-solicit (10), source-quench (4), time-exceeded (11), timestamp (13), timestamp-reply (14), unreachable (3)</p>
<b>interface</b> <i>interface-name</i>	<p>Interface on which the packet is received. You can specify the wildcard character (*) as part of an interface name.</p> <p><b>NOTE:</b> The <b>interface</b> match condition is not supported for egress traffic on an EX8200 Virtual Chassis.</p>
<b>ip-options</b>	Presence of the options field in the IP header.

Table 4: Firewall Filter Match Conditions Supported on EX Series Switches (*continued*)

Match Condition	Description
<b>ip-version</b> <i>version match_condition(s)</i>	<p>Version of the IP protocol for port and VLAN firewall filters. The value for <i>version</i> can be <b>ipv4</b> or <b>ipv6</b>.</p> <p>For <i>match_condition(s)</i>, you can specify one or more of the following match conditions:</p> <ul style="list-style-type: none"> <li>• <b>destination-address</b></li> <li>• <b>destination-port</b></li> <li>• <b>destination-prefix-list</b></li> <li>• <b>dscp</b></li> <li>• <b>fragment-flags</b></li> <li>• <b>icmp-code</b></li> <li>• <b>icmp-type</b></li> <li>• <b>is-fragment</b></li> <li>• <b>precedence</b></li> <li>• <b>protocol</b></li> <li>• <b>source-address</b></li> <li>• <b>source-port</b></li> <li>• <b>source-prefix-list</b></li> <li>• <b>tcp-established</b></li> <li>• <b>tcp-flags</b></li> <li>• <b>tcp-initial</b></li> </ul>
<b>is-fragment</b>	<p>If the packet is a trailing fragment, this match condition does not match the first fragment of a fragmented packet. Use two terms to match both first and trailing fragments.</p>
<b>l2-encap-type llc-non-snap</b>	<p>Match on logical link control (LLC) layer packets for non-Subnet Access Protocol (SNAP) Ethernet Encapsulation type.</p>
<b>next-header bytes</b>	<p>8-bit protocol field that identifies the type of header immediately following the IPv6 header. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed):</p> <p><b>ah (51), dstops (60), egp (8), esp (50), fragment (44), gre (47), hop-by-hop (0), icmp (1), icmp6 (1), igmp (2), ipip (4), ipv6 (41), no-next-header (59), ospf (89), pim (103), routing (43), rsvp (46), sctp (132), tcp (6), udp (17), vrrp (112)</b></p>
<b>packet-length bytes</b>	<p>Length of the received packet, in bytes.</p> <p>The length refers only to the IP packet, including the packet header, and does not include any Layer 2 encapsulation overhead.</p>
<b>precedence precedence</b>	<p>IP precedence. For <i>precedence</i>, you can specify one of the following text synonyms (the field values are also listed):</p> <p><b>critical-ecp (5), flash (3), flash-override (4), immediate (2), internet-control (6), net-control (7), priority (1), routine (0)</b></p>

Table 4: Firewall Filter Match Conditions Supported on EX Series Switches (*continued*)

Match Condition	Description
<b>protocol</b> <i>list of protocol</i>	<p>IPv4 protocol value. For <i>protocols</i>, you can specify one of the following text synonyms:</p> <p><b>egp (8), esp (50), gre (47), icmp (1), igmp (2), ipip (4), ospf (89), pim (103), rsvp (46), tcp (6), udp (17)</b></p>
<b>source-address</b> <i>ip-address</i>	<p>IP source address field, which is the address of the source node sending the packet. For IPv6, the source-address field is 128 bits in length. The filter description syntax supports the text representations for IPv6 addresses that are described in <a href="#">RFC 2373</a>, <i>IP Version 6 Addressing Architecture</i>.</p>
<b>source-mac-address</b> <i>mac-address</i>	<p>Source MAC address.</p> <p>You can define a source MAC address with a prefix, such as <b>source-mac-address 00:01:02:03:04:05/24</b>. If no prefix is specified, the default value 48 is used.</p>
<b>source-port</b> <i>number</i>	<p>TCP or UDP <b>source-port</b> field. Typically, you specify this match in conjunction with the <b>protocol</b> match condition to determine which protocol is being used on the port. For <i>number</i>, you can specify one of the text synonyms listed under <b>destination-port</b>.</p>
<b>source-prefix-list</b> <i>prefix-list</i>	<p>IP source prefix list field.</p> <p>You can define a list of IP address prefixes under a prefix-list alias for frequent use. You define this match condition at the <b>[edit policy-options]</b> hierarchy level.</p>
<b>tcp-established</b>	<p>TCP packets of an established TCP connection. This condition matches packets other than the first packet of a connection. <b>tcp-established</b> is a synonym for the bit names "(ack rst)".</p> <p><b>tcp-established</b> does not implicitly check whether the protocol is TCP. To do so, specify the <b>next-header tcp</b> match condition.</p>
<b>tcp-flags</b> ( <i>flags tcp-initial</i> )	<p>One or more TCP flags:</p> <ul style="list-style-type: none"> <li>bit-name—<b>fin, syn, rst, push, ack, urgent</b></li> <li>logical operators—<b>&amp;</b> (logical AND), <b> </b> (logical OR), <b>!</b> (negation)</li> <li>numerical value—0x01 through 0x20</li> <li>text synonym—<b>tcp-initial</b></li> </ul> <p>To specify multiple flags, use logical operators.</p>
<b>tcp-initial</b>	<p>Matches the first TCP packet of a connection. <b>tcp-initial</b> is a synonym for the bit names "(syn&amp;!ack)".</p> <p><b>tcp-initial</b> does not implicitly check whether the protocol is TCP. To do so, specify the <b>protocol tcp</b> match condition.</p>
<b>traffic-class</b> <i>number</i>	<p>Specifies the DSCP code point for a packet.</p>
<b>ttl</b> <i>value</i>	<p>TTL type to match. The value ranges from 1 through 255.</p>

Table 4: Firewall Filter Match Conditions Supported on EX Series Switches (*continued*)

Match Condition	Description
<b>vlan</b> ( <i>vlan-name</i>   <i>vlan-id</i> )	The VLAN that is associated with the packet. For <i>vlan-id</i> , you can specify either the VLAN ID or a VLAN range. The <b>vlan</b> match condition and the <b>dot1q-tag</b> match condition are mutually exclusive.

## Actions for Firewall Filters

You can define an action for the switch to take if a packet matches the filtering criteria defined in a match condition. [Table 5 on page 24](#) describes the actions supported in a firewall filter configuration.

Table 5: Actions for Firewall Filters

Action	Description
<b>accept</b>	Accept a packet.
<b>discard</b>	Discard a packet silently without sending an Internet Control Message Protocol (ICMP) message.
<b>reject</b> <i>message-type</i>	<p>Discard a packet, and send the ICMPv4 message (type 3) <b>destination unreachable</b>. You can log the rejected packets if you configure the <b>syslog</b> action modifier.</p> <p>You can specify one of the following message codes: <b>administratively-prohibited</b> (default), <b>bad-host-tos</b>, <b>bad-network-tos</b>, <b>host-prohibited</b>, <b>host-unknown</b>, <b>host-unreachable</b>, <b>network-prohibited</b>, <b>network-unknown</b>, <b>network-unreachable</b>, <b>port-unreachable</b>, <b>precedence-cutoff</b>, <b>precedence-violation</b>, <b>protocol-unreachable</b>, <b>source-host-isolated</b>, <b>source-route-failed</b>, <b>tcp-reset</b>.</p> <p>If you specify <b>tcp-reset</b>, a TCP reset is returned if the packet is a TCP packet. Otherwise nothing is returned.</p> <p>If you do not specify a message type, the ICMP notification <b>destination unreachable</b> is sent with the default message <b>communication administratively filtered</b>.</p>
<b>routing-instance</b> <i>routing-instance-name</i>	<p>Forward matched packets to a virtual routing instance.</p> <p><b>NOTE:</b> EX4200 switches do not support firewall-filter-based redirection to the default routing instance.</p>
<b>vlan</b> <i>vlan-name</i>	<p>Forward matched packets to a specific VLAN. Ensure that you specify the VLAN name or VLAN ID and not a VLAN range, because the <b>vlan</b> action does not support the <i>vlan-range</i> option.</p> <p><b>NOTE:</b> If you have defined a VLAN that is enabled for dot1q tunneling, then that particular VLAN is not supported as an action (using the <b>vlan</b> <i>vlan-name</i> action) for an ingress VLAN firewall filter.</p>

## Action Modifiers for Firewall Filters

In addition to the actions described in [Table 5 on page 24](#), you can define action modifiers in a firewall filter configuration for a switch if packets match the filtering criteria defined



in the match condition. [Table 6 on page 25](#) describes the action modifiers supported in a firewall filter configuration.

**Table 6: Action Modifiers for Firewall Filters**

Action Modifier	Description
<b>analyzer</b> <i>analyzer-name</i>	<p>Mirror port traffic to a specified destination port or VLAN that is connected to a protocol analyzer application. Mirroring copies all packets seen on one switch port to a network monitoring connection on another switch port. The analyzer name must be configured under <code>[edit ethernet-switching-options analyzer]</code>.</p> <p><b>NOTE:</b> <b>analyzer</b> is not a supported action modifier for a management interface.</p> <p><b>NOTE:</b> On EX4500 switches, you can configure only one analyzer and include it in a firewall filter. If you configure multiple analyzers, you cannot include any one of those analyzers in a firewall filter.</p>
<b>dscp</b> <i>number</i>	<p>Change the DSCP value for matched packets to the DSCP value specified with this action modifier. <i>number</i> specifies the Differentiated Services code point (DSCP). The DiffServ protocol uses the type-of-service (ToS) byte in the IP header. The most significant six bits of this byte form the DSCP.</p> <p>You can specify DSCP in hexadecimal, binary, or decimal form.</p> <p>For <i>number</i>, you can specify one of the following text synonyms (the field values are also listed):</p> <ul style="list-style-type: none"> <li><b>ef (46)</b>—as defined in <a href="#">RFC 2598</a>, <i>An Expedited Forwarding PHB</i>.</li> <li><b>af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38)</b></li> </ul> <p>These four classes, with three drop precedences in each class, are defined for 12 code points in <a href="#">RFC 2597</a>, <i>Assured Forwarding PHB Group</i>.</p>
<b>count</b> <i>counter-name</i>	<p>Count the number of packets that pass this filter, term, or policer. A policer enables you to specify rate limits on traffic that enters an interface on a switch.</p>
<b>forwarding-class</b> <i>class</i>	<p>Classify the packet in one of the following forwarding classes:</p> <ul style="list-style-type: none"> <li><b>assured-forwarding</b></li> <li><b>best-effort</b></li> <li><b>expedited-forwarding</b></li> <li><b>network-control</b></li> </ul>
<b>interface</b> <i>interface-name</i>	<p>Forward the traffic to the specified interface bypassing the switching lookup.</p>
<b>log</b>	<p>Log the packet's header information in the Routing Engine. To view this information, issue the <b>show firewall log</b> command in the CLI.</p> <p><b>NOTE:</b> If the <b>log</b> or the <b>syslog</b> action modifier is configured along with a <b>vlan</b> action or an <b>interface</b> action modifier, the events might not be logged. However, the redirect interface functionality works as expected.</p>
<b>loss-priority</b> (high   low)	<p>Set the packet loss priority (PLP).</p>

Table 6: Action Modifiers for Firewall Filters (*continued*)

Action Modifier	Description
<b>policer</b> <i>policer-name</i>	<p>Apply rate limits to the traffic.</p> <p>You can specify a policer in a firewall filter only for ingress traffic on a port, VLAN, and router.</p> <p><b>NOTE:</b> A counter for a policer is not supported on EX8200 switches.</p>
<b>syslog</b>	<p>Log an alert for this packet. You can specify that the log be sent to a server for storage and analysis.</p> <p><b>NOTE:</b> If the <b>log</b> or the <b>syslog</b> action modifier is configured along with a <b>vlan</b> action or an <b>interface</b> action modifier, the events might not be logged. However, the redirect interface functionality works as expected.</p>
<b>three-color-policer</b>	Apply a three-color policer.

#### Related Documentation

- [Platform Support for Firewall Filter Match Conditions, Actions, and Action Modifiers on EX Series Switches on page 29](#)
- [Understanding Firewall Filter Match Conditions on page 62](#)
- [Firewall Filter Configuration Statements Supported by Junos OS for EX Series Switches on page 133](#)
- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)
- [Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches on page 96](#)

## Support for Match Conditions and Actions for Loopback Firewall Filters on Switches

On EX Series Ethernet switches, a loopback interface is a gateway for all the control traffic that enters the Routing Engine of the switch. If you want to monitor this control traffic, you must configure a firewall filter on the loopback interface (lo0). Loopback firewall filters are applied only to packets that are sent to the Routing Engine CPU for further processing. Therefore, you can apply a firewall filter only in the ingress direction on the loopback interface.

Each term in a firewall filter consists of *match conditions* and an *action*. Match conditions are the values or fields that a packet must contain. You can define multiple, single, or no match conditions. If no match conditions are specified for the term, all packets are matched by default. The string that defines a match condition is called a *match statement*. The action is the action that the switch takes if a packet matches the match conditions for the specific term. Action modifiers are optional and specify one or more actions that the switch takes if a packet matches the match conditions for the specific term.

The following tables list match conditions, actions, and action modifiers that are supported for a firewall filter configured on a loopback interface on a switch:

- [Table 7 on page 27](#)
- [Table 8 on page 28](#)
- [Table 9 on page 29](#)

For information on match conditions, actions, and action modifiers supported for a firewall filter configured on a network interface, see [“Platform Support for Firewall Filter Match Conditions, Actions, and Action Modifiers on EX Series Switches”](#) on page 29.

**Table 7: Match Conditions for Firewall Filters on Loopback Interfaces for IPv4 and IPv6 Traffic—Support per Switch**

Match Condition	EX2200	EX3200, EX4200	EX3300	EX4500	EX6200	EX8200
Match conditions for IPv4 traffic:						
destination-address	✓	✓	✓	✓	✓	✓
destination-port	✓	✓	✓	✓	✓	✓
destination-prefix-list	✓	✓	✓	✓	✓	✓
dscp	✓	✓	✓	✓	✓	✓
icmp-code	✓	✓	✓	✓	✓	✓
icmp-type	✓	✓	✓	✓	✓	✓
interface	✓	✓	✓	✓	✓	✓
is-fragment	✓	✓	✓	✓	—	—
packet-length	—	—	—	—	—	✓
precedence	✓	✓	✓	✓	✓	✓
protocol	✓	✓	✓	✓	✓	✓
source-address	✓	✓	✓	✓	✓	✓
source-port	✓	✓	✓	✓	✓	✓
source-prefix-list	✓	✓	✓	✓	✓	✓
Match conditions for IPv6 traffic:						
destination-address	—	✓	—	✓	—	✓
destination-port	—	✓	—	✓	—	✓

Table 7: Match Conditions for Firewall Filters on Loopback Interfaces for IPv4 and IPv6 Traffic—Support per Switch (*continued*)

Match Condition	EX2200	EX3200, EX4200	EX3300	EX4500	EX6200	EX8200
destination-prefix-list	–	✓	–	–	–	✓
icmp-code	–	✓	–	✓	–	✓
icmp-type	–	✓	–	✓	–	✓
interface	–	✓	–	–	–	✓
next-header	–	✓	–	✓	–	✓
packet-length	–	–	–	–	–	✓
source-address	–	✓	–	✓	–	✓
source-port	–	✓	–	✓	–	✓
source-prefix-list	–	✓	–	–	–	✓
tcp-established	–	✓	–	–	–	–
tcp-flags	–	✓	–	–	–	–
tcp-initial	–	✓	–	–	–	–
traffic-class	–	✓	–	✓	–	✓

Table 8: Actions for Firewall Filters on Loopback Interfaces for IPv4 and IPv6 Traffic—Support per Switch

Match Condition	EX2200	EX3200, EX4200	EX3300	EX4500	EX6200	EX8200
Actions for IPv4 traffic:						
accept	✓	✓	✓	✓	✓	✓
discard	✓	✓	✓	✓	✓	✓
Actions for IPv6 traffic:						
accept	–	✓	–	✓	–	✓
discard	–	✓	–	✓	–	✓

**Table 9: Action Modifiers for Firewall Filters on Loopback Interfaces for IPv4 and IPv6 Traffic—Support per Switch**

Match Condition	EX2200	EX3200, EX4200	EX3300	EX4500	EX6200	EX8200
Action modifiers for IPv4 traffic:						
count	–	✓	–	–	✓	–
forwarding-class	✓	✓	✓	✓	–	✓
loss-priority	✓	✓	✓	✓	–	✓
Action modifiers for IPv6 traffic:						
count	–	✓	–	✓	–	–
forwarding-class	–	✓	–	✓	–	✓
loss-priority	–	✓	–	✓	–	✓



**NOTE:** On EX8200 switches, if an implicit or explicit discard action is configured on a loopback interface for IPv4 traffic, next hop resolve packets are accepted and allowed to pass through the switch. However, for IPv6 traffic, you must explicitly configure a rule to allow the neighbor discovery IPv6 resolve packets to pass through the switch.

**Related Documentation**

- [Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 16](#)
- [Platform Support for Firewall Filter Match Conditions, Actions, and Action Modifiers on EX Series Switches on page 29](#)
- [Understanding Firewall Filter Match Conditions on page 62](#)
- [Understanding How Firewall Filters Are Evaluated on page 60](#)
- [Understanding How Firewall Filters Test a Packet's Protocol on page 66](#)
- [Understanding the Use of Policers in Firewall Filters on page 66](#)

## Platform Support for Firewall Filter Match Conditions, Actions, and Action Modifiers on EX Series Switches

After you define a firewall filter on an EX Series switch, you must associate the filter to a bind point so that the filter can filter the packets that enter or exit the bind point. Port firewall filters, VLAN firewall filters, and Layer 3 (or router) firewall filters are the different types of firewall filters you can apply on a switch, depending on the bind points the filters are associated with. While a port firewall filter applies to Layer 2 interfaces, a VLAN

firewall filter applies to packets that enter or leave a VLAN and also to packets that are bridged within a VLAN. A Layer 3 firewall filter applies to Layer 3 (routed) interfaces and routed VLAN interfaces (RVIs).



**NOTE:** If you want to control the traffic that enters the Routing Engine of the switch, you must configure a firewall filter on the loopback interface (lo0) of the switch. For information about match conditions, actions, and action modifiers supported on the loopback interface of a switch, see [“Support for Match Conditions and Actions for Loopback Firewall Filters on Switches”](#) on page 26.

This topic describes the supported switches and bind points for match conditions, actions, and action modifiers for firewall filters supported on EX Series switches. For descriptions of the match conditions, actions, and action modifiers, see [“Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches”](#) on page 16.

This topic describes:

- [Firewall Filter Types and Their Bind Points](#) on page 30
- [Support for IPv4 and IPv6 Firewall Filters on Switches](#) on page 31
- [Platform Support for Match Conditions for IPv4 Traffic](#) on page 31
- [Platform Support for Match Conditions for IPv6 Traffic](#) on page 41
- [Platform Support for Match Conditions for Non-IP Traffic](#) on page 47
- [Platform Support for Actions for IPv4 Traffic](#) on page 48
- [Platform Support for Actions for IPv6 Traffic](#) on page 50
- [Platform Support for Action Modifiers for IPv4 Traffic](#) on page 52
- [Platform Support for Action Modifiers for IPv6 Traffic](#) on page 56

## Firewall Filter Types and Their Bind Points

You can apply a firewall filter at specific bind points to filter IPv4, IPv6, or non-IP traffic. See the remaining sections in this topic for information about support on individual switches for different traffic types.

[Table 10 on page 30](#) lists the firewall filter types and their associated bind points that are supported on the switches.

**Table 10: Bind Points Associated with Firewall Filter Types**

Bind Points	Firewall Filter Type
Ports (Layer 2 interfaces)	Port firewall filter
VLANs	VLAN firewall filter
Layer 3 interfaces (Layer 3 (routed) interfaces or routed VLAN interfaces (RVIs))	Router firewall filter

## Support for IPv4 and IPv6 Firewall Filters on Switches

You can apply a port, VLAN, or router firewall filter to filter IPv4 traffic on all EX Series switches. You can apply port, VLAN, and router firewall filters for IPv6 traffic on EX3200, EX4200, and EX8200 switches and only router firewall filters for IPv6 traffic on EX2200, EX3300, and EX4500 switches.

[Table 11 on page 31](#) briefly summarizes the support for IPv4 and IPv6 firewall filters on different switches. The support for port, VLAN, and router firewall filters on different switches is further discussed in the subsequent sections in this topic.

**Table 11: Support for IPv4 and IPv6 Firewall Filters on Switches**

Switch	Support for IPv4 Firewall Filter	Support for IPv6 Firewall Filter
EX2200	Yes	Yes
EX3200 and EX4200	Yes	Yes
EX3300	Yes	Yes
EX4500	Yes	Yes
EX6200	Yes	No
EX8200	Yes	Yes

## Platform Support for Match Conditions for IPv4 Traffic

You can define port, VLAN, and router firewall filters for ingress and egress IPv4 traffic on all EX Series switches. [Table 12 on page 32](#) summarizes the support for match conditions on different bind points for ingress and egress IPv4 traffic on different switches.

Table 12: Firewall Filter Match Conditions Supported for IPv4 Traffic on Switches

Match Condition	Switch	Supported Bind Points	
		Ingress	Egress
<b>destination-address</b> <i>ip-address</i>	EX2200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>destination-mac-address</b> <i>mac-address</i>	EX2200	Ports and VLANs	Ports and VLANs
	EX3200 and EX4200	Ports and VLANs	Ports and VLANs
	EX3300	Ports and VLANs	Ports and VLANs
	EX4500	Ports and VLANs	Ports and VLANs
	EX6200	Ports and VLANs	Ports and VLANs
	EX8200	Ports and VLANs	Ports and VLANs
<b>destination-port number</b>	EX2200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces



Table 12: Firewall Filter Match Conditions Supported for IPv4 Traffic on Switches (*continued*)

Match Condition	Switch	Supported Bind Points	
		Ingress	Egress
<b>destination-prefix-list</b> <i>prefix-list</i>	EX2200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>dot1q-tag number</b>	EX2200	Ports and VLANs	Ports and VLANs
	EX3200 and EX4200	Ports and VLANs	Ports and VLANs
	EX3300	Ports and VLANs	Ports and VLANs
	EX4500	Ports and VLANs	Ports and VLANs
	EX6200	Ports and VLANs	Ports and VLANs
	EX8200	Ports and VLANs	Not supported
<b>dot1q-user-priority number</b>	EX2200	Ports and VLANs	Ports and VLANs
	EX3200 and EX4200	Ports and VLANs	Ports and VLANs
	EX3300	Ports and VLANs	Ports and VLANs
	EX4500	Ports and VLANs	Ports and VLANs
	EX6200	Ports and VLANs	Ports and VLANs
	EX8200	Ports and VLANs	Ports and VLANs

Table 12: Firewall Filter Match Conditions Supported for IPv4 Traffic on Switches (*continued*)

Match Condition	Switch	Supported Bind Points	
		Ingress	Egress
<b>dscp number</b>	EX2200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>ether-type value</b>	EX2200	Ports and VLANs	Ports and VLANs
	EX3200 and EX4200	Ports and VLANs	Ports and VLANs
	EX3300	Ports and VLANs	Ports and VLANs
	EX4500	Ports and VLANs	Ports and VLANs
	EX6200	Ports and VLANs	Ports and VLANs
	EX8200	Ports and VLANs	Not supported
<b>fragment-flags</b> <i>fragment-flags</i>	EX2200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX3300	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX4500	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX6200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX8200	Ports, VLANs, and Layer 3 interfaces	Not supported

Table 12: Firewall Filter Match Conditions Supported for IPv4 Traffic on Switches (*continued*)

Match Condition	Switch	Supported Bind Points	
		Ingress	Egress
<b>icmp-code <i>number</i></b>	EX2200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports and Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>icmp-type <i>number</i></b>	EX2200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces

Table 12: Firewall Filter Match Conditions Supported for IPv4 Traffic on Switches (*continued*)

Match Condition	Switch	Supported Bind Points	
		Ingress	Egress
<b>interface</b> <i>interface-name</i>	EX2200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>ip-options</b>	EX2200	Layer 3 interfaces	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports and VLANs
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports and VLANs
	EX4500	Layer 3 interfaces	Not supported
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Layer 3 interfaces	Not supported
<b>ip-version</b> <i>version match_condition(s)</i>	EX2200	Ports and VLANs	Ports and VLANs
	EX3200 and EX4200	Ports and VLANs	Ports and VLANs
	EX3300	Ports and VLANs	Ports and VLANs
	EX4500	Ports and VLANs	Ports and VLANs
	EX6200	Ports and VLANs	Ports and VLANs
	EX8200	Ports and VLANs	Ports and VLANs

Table 12: Firewall Filter Match Conditions Supported for IPv4 Traffic on Switches (*continued*)

Match Condition	Switch	Supported Bind Points	
		Ingress	Egress
<b>is-fragment</b>	EX2200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Not supported
<b>precedence <i>precedence</i></b>	EX2200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces

Table 12: Firewall Filter Match Conditions Supported for IPv4 Traffic on Switches (*continued*)

Match Condition	Switch	Supported Bind Points	
		Ingress	Egress
<b>protocol</b> <i>list of protocols</i>	EX2200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>source-address</b> <b>ip-address</b>	EX2200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>source-mac-address</b> <b>mac-address</b>	EX2200	Ports and VLANs	Ports and VLANs
	EX3200 and EX4200	Ports and VLANs	Ports and VLANs
	EX3300	Ports and VLANs	Ports and VLANs
	EX4500	Ports and VLANs	Ports and VLANs
	EX6200	Ports and VLANs	Ports and VLANs
	EX8200	Ports and VLANs	Ports and VLANs

Table 12: Firewall Filter Match Conditions Supported for IPv4 Traffic on Switches (*continued*)

Match Condition	Switch	Supported Bind Points	
		Ingress	Egress
<b>source-port</b> <i>number</i>	EX2200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>source-prefix-list</b> <i>prefix-list</i>	EX2200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces

Table 12: Firewall Filter Match Conditions Supported for IPv4 Traffic on Switches (*continued*)

Match Condition	Switch	Supported Bind Points	
		Ingress	Egress
<b>tcp-established</b>	EX2200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>tcp-flags (<i>flags tcp-initial</i>)</b>	EX2200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces



Table 12: Firewall Filter Match Conditions Supported for IPv4 Traffic on Switches (*continued*)

Match Condition	Switch	Supported Bind Points	
		Ingress	Egress
<b>tcp-initial</b>	EX2200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>ttl value</b>	EX2200	Layer 3 interfaces	Not supported
	EX3200 and EX4200	Layer 3 interfaces	Not supported
	EX3300	Layer 3 interfaces	Not supported
	EX4500	Layer 3 interfaces	Not supported
	EX6200	Layer 3 interfaces	Not supported
	EX8200	Layer 3 interfaces	Not supported
<b>vlan (vlan-name   vlan-id)</b>	EX2200	Ports and VLANs	Ports and VLANs
	EX3200 and EX4200	Ports and VLANs	Ports and VLANs
	EX3300	Ports and VLANs	Ports and VLANs
	EX4500	Ports and VLANs	Ports
	EX6200	Ports and VLANs	Ports and VLANs
	EX8200	Ports and VLANs	Ports and VLANs

### Platform Support for Match Conditions for IPv6 Traffic

You can define port, VLAN, and router firewall filters for ingress and egress IPv6 traffic on EX3200, EX4200, and EX8200 switches, and router firewall filters for ingress and

egress IPv6 traffic on EX2200, EX3300, and EX4500 switches. [Table 13 on page 42](#) summarizes support for match conditions on different bind points for ingress and egress IPv6 traffic on different switches.

**Table 13: Firewall Filter Match Conditions Supported for IPv6 Traffic on Switches**

Match Condition	Switch	Supported Bind Points	
		Ingress	Egress
<b>destination-address</b> <i>ip-address</i>	EX2200	Layer 3 interfaces	Layer 3 interfaces
	EX3200 and EX4200	Layer 3 interfaces	Layer 3 (routed) interfaces only
	EX3300	Layer 3 interfaces	Layer 3 interfaces
	EX4500	Layer 3 interfaces	Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Layer 3 interfaces
<b>destination-mac-address</b> <i>mac-address</i>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Ports and VLANs	Ports and VLANs
	EX3300	Not supported	Not supported
	EX4500	Not supported	Not supported
	EX8200	Ports and VLANs	Ports and VLANs
<b>destination-port</b> <i>number</i>	EX2200	Layer 3 interfaces	Layer 3 interfaces
	EX3200 and EX4200	Layer 3 interfaces	Layer 3 interfaces
	EX3300	Layer 3 interfaces	Layer 3 interfaces
	EX4500	Layer 3 interfaces	Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces

Table 13: Firewall Filter Match Conditions Supported for IPv6 Traffic on Switches (*continued*)

Match Condition	Switch	Supported Bind Points	
		Ingress	Egress
<b>destination-prefix-list</b> <i>prefix-list</i>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Layer 3 interfaces	Layer 3 (routed) interfaces only
	EX3300	Not supported	Not supported
	EX4500	Not supported	Not supported
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>dot1q-tag number</b>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Ports and VLANs	Ports and VLANs
	EX3300	Not supported	Not supported
	EX4500	Not supported	Not supported
	EX8200	Ports and VLANs	Not supported
<b>dot1q-user-priority number</b>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Ports and VLANs	Ports and VLANs
	EX3300	Not supported	Not supported
	EX4500	Not supported	Not supported
	EX8200	Ports and VLANs	Ports and VLANs
<b>ether-type (ipv6) value</b>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Ports and VLANs	Ports and VLANs
	EX3300	Not supported	Not supported
	EX4500	Not supported	Not supported
	EX8200	Ports and VLANs	Ports and VLANs.

Table 13: Firewall Filter Match Conditions Supported for IPv6 Traffic on Switches (*continued*)

Match Condition	Switch	Supported Bind Points	
		Ingress	Egress
<b>icmp-code</b> <i>number</i>	EX2200	Layer 3 interfaces	Layer 3 interfaces
	EX3200 and EX4200	Layer 3 interfaces	Layer 3 interfaces
	EX3300	Layer 3 interfaces	Layer 3 interfaces
	EX4500	Layer 3 interfaces	Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>icmp-type</b> <i>number</i>	EX2200	Layer 3 interfaces	Layer 3 interfaces
	EX3200 and EX4200	Layer 3 interfaces	Layer 3 interfaces
	EX3300	Layer 3 interfaces	Layer 3 interfaces
	EX4500	Layer 3 interfaces	Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>interface</b> <i>interface-name</i>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Not supported	Layer 3 interfaces
	EX4500	Not supported	Not supported
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>ip-version</b> <i>version</i> <i>match_condition(s)</i>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Not supported	Not supported
	EX3300	Not supported	Not supported
	EX4500	Not supported	Not supported
	EX8200	Ports and VLANs	Ports and VLANs

Table 13: Firewall Filter Match Conditions Supported for IPv6 Traffic on Switches (*continued*)

Match Condition	Switch	Supported Bind Points	
		Ingress	Egress
<b>next-header bytes</b>	EX2200	Layer 3 interfaces	Layer 3 interfaces
	EX3200 and EX4200	Layer 3 interfaces	Layer 3 interfaces
	EX3300	Layer 3 interfaces	Layer 3 interfaces
	EX4500	Layer 3 interfaces	Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>packet-length bytes</b>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Not supported	Not supported
	EX3300	Not supported	Not supported
	EX4500	Not supported	Not supported
	EX8200	Layer 3 interfaces	Not supported
<b>source-address ip-address</b>	EX2200	Layer 3 interfaces	Layer 3 interfaces
	EX3200 and EX4200	Layer 3 interfaces	Layer 3 interfaces
	EX3300	Layer 3 interfaces	Layer 3 interfaces
	EX4500	Layer 3 interfaces	Layer 3 interfaces
	EX8200	Ports, VLANs, Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>source-mac-address mac-address</b>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Ports and VLANs	Ports and VLANs
	EX3300	Not supported	Not supported
	EX4500	Not supported	Not supported
	EX8200	Ports and VLANs	Ports and VLANs

Table 13: Firewall Filter Match Conditions Supported for IPv6 Traffic on Switches (*continued*)

Match Condition	Switch	Supported Bind Points	
		Ingress	Egress
<b>source-port <i>number</i></b>	EX2200	Layer 3 interfaces	Layer 3 interfaces
	EX3200 and EX4200	Layer 3 interfaces	Layer 3 interfaces
	EX3300	Layer 3 interfaces	Layer 3 interfaces
	EX4500	Layer 3 interfaces	Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>source-prefix-list <i>prefix-list</i></b>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Layer 3 interfaces	Layer 3 interfaces
	EX3300	Not supported	Not supported
	EX4500	Not supported	Not supported
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>tcp-established</b>	EX2200	Layer 3 interfaces	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Layer 3 interfaces	Not supported
	EX4500	Layer 3 interfaces	Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>tcp-flags (<i>flags</i> tcp-initial)</b>	EX2200	Layer 3 interfaces	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Layer 3 interfaces	Not supported
	EX4500	Layer 3 interfaces	Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces

Table 13: Firewall Filter Match Conditions Supported for IPv6 Traffic on Switches (*continued*)

Match Condition	Switch	Supported Bind Points	
		Ingress	Egress
<b>tcp-initial</b>	EX2200	Layer 3 interfaces	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Layer 3 interfaces	Not supported
	EX4500	Layer 3 interfaces	Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>traffic-class <i>number</i></b>	EX2200	Not supported	Layer 3 interfaces
	EX3200 and EX4200	Layer 3 interfaces	Layer 3 interfaces
	EX3300	Not supported	Layer 3 interfaces
	EX4500	Layer 3 interfaces	Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>vlan (<i>vlan-id</i>   <i>vlan-name</i>)</b>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Ports and VLANs	Ports and VLANs
	EX3300	Not supported	Not supported
	EX4500	Not supported	Not supported
	EX8200	Ports and VLANs	Not supported

### Platform Support for Match Conditions for Non-IP Traffic

You can define port, VLAN, and router firewall filters for ingress and egress non-IP traffic on all EX Series switches. [Table 14 on page 48](#) summarizes support for match conditions on different bind points for ingress and egress non-IP traffic on different switches.

Table 14: Firewall Filter Match Condition Supported for Non-IP Traffic on Switches

Match Condition	Switch	Supported Bind Points	
		Ingress	Egress
<b>l2-encap-type llc-non-snap</b>	EX2200	Ports and VLANs	Ports and VLANs
	EX3200 and EX4200	Ports and VLANs	Ports and VLANs
	EX3300	Ports and VLANs	Ports and VLANs
	EX4500	Ports and VLANs	Ports and VLANs
	EX6200	Ports and VLANs	Ports and VLANs
	EX8200	Ports and VLANs	Ports and VLANs

### Platform Support for Actions for IPv4 Traffic

Table 15 on page 48 summarizes the support for actions on different bind points for ingress and egress IPv4 traffic on different switches.

Table 15: Firewall Filter Actions Supported for IPv4 Traffic on Switches

Action	Switch	Supported Bind Points	
		Ingress	Egress
<b>accept</b>	EX2200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces



Table 15: Firewall Filter Actions Supported for IPv4 Traffic on Switches (*continued*)

Action	Switch	Supported Bind Points	
		Ingress	Egress
<b>discard</b>	EX2200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>reject <i>message-type</i></b>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Layer 3 interfaces	Not supported
	EX3300	Layer 3 interfaces	Not supported
	EX4500	Not supported	Not supported
	EX6200	Layer 3 interfaces	Not supported
	EX8200	Layer 3 interfaces	Not supported
<b>routing-instance <i>routing-instance-name</i></b>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Layer 3 interfaces	Not supported
	EX3300	Not supported	Not supported
	EX4500	Not supported	Not supported
	EX6200	Layer 3 interfaces	Not supported
	EX8200	Layer 3 interfaces	Not supported

Table 15: Firewall Filter Actions Supported for IPv4 Traffic on Switches (*continued*)

Action	Switch	Supported Bind Points	
		Ingress	Egress
vlan <i>vlan-name</i>	EX2200	Ports and VLANs	Not supported
	EX3200 and EX4200	Ports and VLANs	Not supported
	EX3300	Ports and VLANs	Ports and VLANs
	EX4500	Ports and VLANs	Ports
	EX6200	Ports and VLANs	Ports and VLANs
	EX8200	Ports and VLANs	Not supported
NOTE: Supported only when used in conjunction with the <b>interface</b> action modifier. On EX8200 Virtual Chassis, the <b>vlan</b> action is supported only for VLANs.			

## Platform Support for Actions for IPv6 Traffic

Table 16 on page 50 summarizes the support for actions on different bind points for ingress and egress IPv6 traffic.

Table 16: Firewall Filter Actions Supported for IPv6 Traffic on Switches

Action	Switch	Supported Bind Points	
		Ingress	Egress
accept	EX2200	Layer 3 interfaces	Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Layer 3 interfaces	Layer 3 interfaces
	EX4500	Layer 3 interfaces	Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces

Table 16: Firewall Filter Actions Supported for IPv6 Traffic on Switches (*continued*)

Action	Switch	Supported Bind Points	
		Ingress	Egress
<b>discard</b>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Layer 3 interfaces	Layer 3 interfaces
	EX4500	Layer 3 interfaces	Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
<b>reject message-type</b>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Layer 3 interfaces	Not supported
	EX3300	Not supported	Not supported
	EX4500	Not supported	Not supported
	EX8200	Layer 3 interfaces	Not supported
<b>routing-instance routing-instance-name</b>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Layer 3 interfaces	Not supported
	EX3300	Layer 3 interfaces	Not supported
	EX4500	Not supported	Not supported
	EX8200	Layer 3 interfaces	Not supported

Table 16: Firewall Filter Actions Supported for IPv6 Traffic on Switches (*continued*)

Action	Switch	Supported Bind Points	
		Ingress	Egress
vlan <i>vlan-name</i>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Ports and VLANs	Not supported
	EX3300	Not supported	Not supported
	EX4500	Not supported	Not supported
	EX8200	Ports and VLANs	Not supported
NOTE: Supported only when used in conjunction with the <b>interface</b> action modifier. On EX8200 Virtual Chassis, the <b>vlan</b> action is supported only for VLANs.			

### Platform Support for Action Modifiers for IPv4 Traffic

Table 17 on page 52 summarizes support for action modifiers on different bind points for ingress and egress IPv4 traffic on different switches.

Table 17: Firewall Filter Action Modifiers Supported for IPv4 Traffic on Switches

Action Modifier	Switch	Supported Bind Points	
		Ingress	Egress
analyzer	EX2200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX3300	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX4500	Ports, VLANs, and Layer 3 interfaces	Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX8200	Ports, VLANs, and Layer 3 interfaces	Not supported

Table 17: Firewall Filter Action Modifiers Supported for IPv4 Traffic on Switches (*continued*)

Action Modifier	Switch	Supported Bind Points	
		Ingress	Egress
<b>dscp</b>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Not supported	Not supported
	EX3300	Not supported	Not supported
	EX4500	Not supported	Not supported
	EX6200	Not supported	Not supported
	EX8200	Layer 3 interfaces	Not supported
<b>count</b>	EX2200	VLANs and Layer 3 interfaces ( <b>me0</b> interfaces only)	Layer 3 interfaces ( <b>me0</b> interfaces only)
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	VLANs and Layer 3 interfaces ( <b>me0</b> and <b>vme0</b> interfaces only)	Layer 3 interfaces ( <b>me0</b> and <b>vme0</b> interfaces only)
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Not supported
<b>forwarding-class class</b>	EX2200	Ports, VLANs, and Layer 3 interfaces	Ports and Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports and Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports and Layer 3 interfaces

Table 17: Firewall Filter Action Modifiers Supported for IPv4 Traffic on Switches (*continued*)

Action Modifier	Switch	Supported Bind Points	
		Ingress	Egress
<b>interface</b> <i>interface-name</i>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Ports and VLANs	Not supported
	EX3300	Not supported	Not supported
	EX4500	Ports and VLANs	Not supported
	EX6200	Ports and VLANs	Not supported
	EX8200	Ports and VLANs  <small>NOTE: On EX8200 Virtual Chassis, the <b>interface</b> action modifier is supported only for VLANs.</small>	Not supported
<b>log</b>	EX2200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX3300	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX4500	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX6200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX8200	Ports, VLANs, and Layer 3 interfaces	Not supported

Table 17: Firewall Filter Action Modifiers Supported for IPv4 Traffic on Switches (*continued*)

Action Modifier	Switch	Supported Bind Points	
		Ingress	Egress
<b>loss-priority (high   low)</b>	EX2200	Ports, VLANs, and Layer 3 interfaces	Ports and Layer 3 interfaces
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports and Layer 3 interfaces
	EX3300	Ports, VLANs, and Layer 3 interfaces	Ports and Layer 3 interfaces
	EX4500	Ports, VLANs, and Layer 3 interfaces	Ports and Layer 3 interfaces
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports and Layer 3 interfaces
<b>policer <i>policer-name</i></b>	EX2200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX3300	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX4500	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX6200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX8200	Ports, VLANs, and Layer 3 interfaces	Not supported

Table 17: Firewall Filter Action Modifiers Supported for IPv4 Traffic on Switches (*continued*)

Action Modifier	Switch	Supported Bind Points	
		Ingress	Egress
<b>syslog</b>	EX2200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX3300	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX4500	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX6200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX8200	Ports, VLANs, and Layer 3 interfaces	Not supported
<b>three-color-policer</b>	EX2200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX3300	Not supported	Not supported
	EX4500	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX6200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX8200	Not supported	Not supported

### Platform Support for Action Modifiers for IPv6 Traffic

Table 18 on page 57 summarizes support for action modifiers on different bind points for ingress and egress IPv6 traffic.



Table 18: Firewall Filter Action Modifiers Supported for IPv6 Traffic on Switches

Action Modifier	Switch	Supported Bind Points	
		Ingress	Egress
<b>analyzer</b>	EX2200	Layer 3 interfaces	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX3300	Layer 3 interfaces	Not supported
	EX4500	Layer 3 interfaces	Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Not supported
<b>dscp</b>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Not supported	Not supported
	EX3300	Not supported	Not supported
	EX4500	Not supported	Not supported
	EX8200	Layer 3 interfaces	Not supported
<b>count</b>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports, VLANs, and Layer 3 interfaces
	EX3300	Layer 3 interfaces ( <b>me0</b> and <b>vme0</b> interfaces only)	Layer 3 interfaces ( <b>me0</b> and <b>vme0</b> interfaces only)
	EX4500	Layer 3 interfaces	Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Not supported
<b>forwarding-class</b> <i>class</i>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports and Layer 3 interfaces
	EX3300	Layer 3 interfaces	Layer 3 interfaces
	EX4500	Layer 3 interfaces	Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports and Layer 3 interfaces

Table 18: Firewall Filter Action Modifiers Supported for IPv6 Traffic on Switches (*continued*)

Action Modifier	Switch	Supported Bind Points	
		Ingress	Egress
<b>interface</b> <i>interface-name</i>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Ports and VLANs	Not supported
	EX3300	Not supported	Not supported
	EX4500	Not supported	Not supported
	EX8200	Ports and VLANs  <small>NOTE: On EX8200 Virtual Chassis, the <b>interface</b> action modifier is supported only for VLANs.</small>	Not supported
<b>log</b>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX3300	Layer 3 interfaces	Layer 3 interfaces
	EX4500	Not supported	Not supported
	EX8200	Ports, VLANs, and Layer 3 interfaces	Not supported
<b>loss-priority (high   low)</b>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Ports and Layer 3 interfaces
	EX3300	Layer 3 interfaces	Layer 3 interfaces
	EX4500	Layer 3 interfaces	Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Ports and Layer 3 interfaces

Table 18: Firewall Filter Action Modifiers Supported for IPv6 Traffic on Switches (*continued*)

Action Modifier	Switch	Supported Bind Points	
		Ingress	Egress
<b>policer</b> <i>policer-name</i>	EX2200	Layer 3 interfaces	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX3300	Layer 3 interfaces	Not supported
	EX4500	Layer 3 interfaces	Layer 3 interfaces
	EX8200	Ports, VLANs, and Layer 3 interfaces	Not supported
<b>syslog</b>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Ports, VLANs, and Layer 3 interfaces	Not supported
	EX3300	Not supported	Not supported
	EX4500	Not supported	Not supported
	EX8200	Ports, VLANs, and Layer 3 interfaces	Not supported
<b>three-color-policer</b>	EX2200	Not supported	Not supported
	EX3200 and EX4200	Not Supported	Not Supported
	EX3300	Not supported	Not supported
	EX4500	Not supported	Not supported
	EX8200	Not Supported	Not Supported

**Related Documentation**

- [Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 16](#)
- [Support for Match Conditions and Actions for Loopback Firewall Filters on Switches on page 26](#)
- [Understanding Firewall Filter Match Conditions on page 62](#)
- [Firewall Filter Configuration Statements Supported by Junos OS for EX Series Switches on page 133](#)
- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)

- [Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches on page 96](#)

## Understanding How Firewall Filters Are Evaluated

---

A firewall filter consists of one or more terms, and the order of the terms within a firewall filter is important. Before you configure firewall filters, you should understand how Juniper Networks EX Series Ethernet Switches evaluate the terms within a firewall filter and how packets are evaluated against the terms.

When a firewall filter consists of a single term, the filter is evaluated as follows:

- If the packet matches all the conditions, the action in the **then** statement is taken.
- If the packet matches all the conditions, and no action is specified in the **then** statement, the default action **accept** is taken.

When a firewall filter consists of more than one term, the firewall filter is evaluated sequentially:

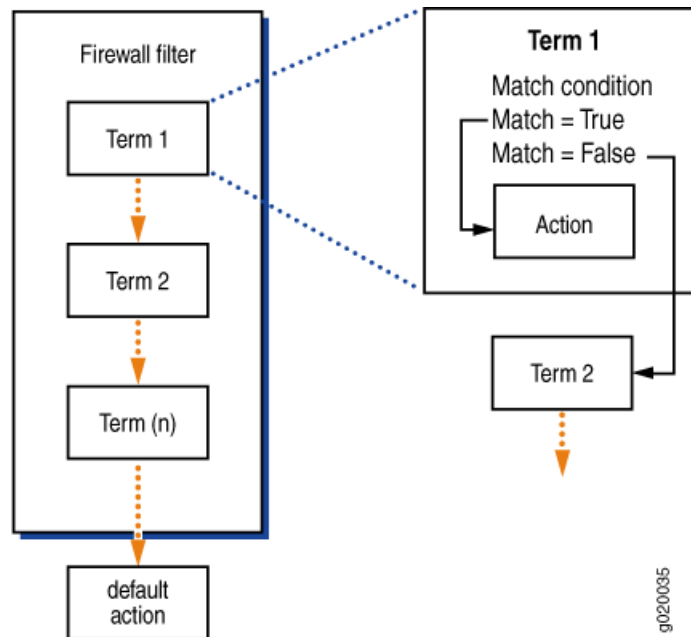
1. The packet is evaluated against the conditions in the **from** statement in the first term.
2. If the packet matches all the conditions in the term, the action in the **then** statement is taken and the evaluation ends. Subsequent terms in the filter are not evaluated.
3. If the packet does not match all the conditions in the term, the packet is evaluated against the conditions in the **from** statement in the second term.

This process continues until either the packet matches the conditions in the **from** statement in one of the subsequent terms or there are no more terms in the filter.

4. If a packet passes through all the terms in the filter without a match, the packet is discarded.

[Figure 3 on page 61](#) shows how an EX Series switch evaluates the terms within a firewall filter.

Figure 3: Evaluation of Terms Within a Firewall Filter



If a term does not contain a **from** statement, the packet is considered to match and the action in the **then** statement of the term is taken.

If a term does not contain a **then** statement, or if an action has not been configured in the **then** statement, and the packet matches the conditions in the **from** statement of the term, the packet is accepted.

Every firewall filter contains an implicit **deny** statement at the end of the filter, which is equivalent to the following explicit filter term:

```
term implicit-rule {
  then discard;
}
```

Consequently, if a packet passes through all the terms in a filter without matching any conditions, the packet is discarded. If you configure a firewall filter that has no terms, all packets that pass through the filter are discarded.



**NOTE:** Firewall filtering is supported on packets that are at least 48 bytes long.

#### Related Documentation

- [Firewall Filters for EX Series Switches Overview on page 7](#)
- [Understanding Firewall Filter Match Conditions on page 62](#)
- [Understanding the Use of Policers in Firewall Filters on page 66](#)
- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)

## Understanding Firewall Filter Match Conditions

---

Before you define terms for firewall filters, you must understand how the match conditions that you specify in a term are handled and how to specify various types of match conditions to achieve the desired filtering results. A match condition consists of a string (called a match statement) that defines the match condition. Match conditions are the values or fields that a packet must contain.

This topic describes:

- [Filter Match Conditions on page 62](#)
- [Numeric Filter Match Conditions on page 62](#)
- [Interface Filter Match Conditions on page 63](#)
- [IP Address Filter Match Conditions on page 63](#)
- [MAC Address Filter Match Conditions on page 64](#)
- [Bit-Field Filter Match Conditions on page 64](#)

### Filter Match Conditions

In the **from** statement of a firewall filter term, you specify the packet conditions that trigger the action in one of the **then** statements: **then** with various options, **then interface** or **then vlan**. All conditions in the **from** statement must match for the action to be taken. The order in which you specify match conditions is not important, because a packet must match all the conditions in a term for a match to occur.

If you specify no match conditions in a term, that term matches all packets.

An individual condition in a **from** statement cannot contain a list of values. For example, you cannot specify numeric ranges or multiple source or destination addresses.

Individual conditions in a **from** statement cannot be negated. A negated condition is an explicit mismatch.

### Numeric Filter Match Conditions

Numeric filter conditions match packet fields that are identified by a numeric value, such as port and protocol numbers. For numeric filter match conditions, you specify a keyword that identifies the condition and a single value that a field in a packet must match.

You can specify the numeric value in one of the following ways:

- Single number—A match occurs if the value of the field matches the number. For example:  
`source-port 25;`
- Text synonym for a single number— A match occurs if the value of the field matches the number that corresponds to the synonym. For example:  
`source-port http;`

To specify more than one value in a filter term, you enter each value in its own match statement, which is a string that defines a match condition. For example, a match occurs in the following term if the value of **vlan** is 10 or 30.

```
[edit firewall family family-name filter filter-name term term-name from]
vlan 10;
vlan 30;
```

The following restrictions apply to numeric filter match conditions:

- You cannot specify a range of values.
- You cannot specify a list of comma-separated values.
- You cannot exclude a specific value in a numeric filter match condition. For example, you cannot specify a condition that would match only if the match condition was not equal to a given value.

## Interface Filter Match Conditions

Interface filter match conditions can match interface name values in a packet. For interface filter match conditions, you specify the name of the interface, for example:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set interface ge-0/0/1
```

Port and VLAN interfaces do not use logical unit numbers. However, a firewall filter that is applied to a router interface can specify the logical unit number in the interface filter match condition, for example:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set interface ge-0/1/0.0
```

You can include the **\*** wildcard as part of the interface name, for example:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set interface ge-0/*/1
user@switch# set interface ge-0/1/*
user@switch# set interface ge-*
```

## IP Address Filter Match Conditions

Address filter match conditions can match prefix values in a packet, such as IP source and destination prefixes. For address filter match conditions, you specify a keyword that identifies the field and one prefix of that type that a packet must match.

You specify the address as a single prefix. A match occurs if the value of the field matches the prefix. For example:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set destination-address 10.2.1.0/28;
```

Each prefix contains an implicit **0/0** except statement, which means that any prefix that does not match the prefix that is specified is explicitly considered not to match.

To specify the address prefix, use the notation **prefix/prefix-length**. If you omit **prefix-length**, it defaults to **/32**. For example:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set destination-address 10
```

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# show destination-address
10.0.0.0/32;
```

To specify more than one IP address in a filter term, you enter each address in its own match statement. For example, a match occurs in the following term if the value of the **source-address** field matches either of the following source-address prefixes:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set source-address 10.0.0.0/8
user@switch# set source-address 10.1.0.0/16
```

## MAC Address Filter Match Conditions

MAC address filter match conditions can match source and destination MAC address values in a packet. For MAC address filter match conditions, you specify a keyword that identifies the field and one value of that type that a packet must match.

You can specify the MAC address as six hexadecimal bytes in the following formats:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set destination-mac-address 0011.2233.4455
```

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set destination-mac-address 00:11:22:33:44:55
```

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set destination-mac-address 001122334455
```

To specify more than one MAC address in a filter term, you enter each MAC address in its own match statement. For example, a match occurs in the following term if the value of the **source-mac-address** field matches either of the following addresses.

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set source-mac-address 00:11:22:33:44:55
user@switch# set source-mac-address 00:11:22:33:20:15
```

## Bit-Field Filter Match Conditions

Bit-field filter conditions match packet fields if particular bits in those fields are or are not set. You can match the IP options, TCP flags, and IP fragmentation fields. For bit-field filter match conditions, you specify a keyword that identifies the field and tests to determine that the option is present in the field.

To specify the bit-field value to match, enclose the value in double quotation marks. For example, a match occurs if the **RST** bit in the TCP flags field is set:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-flags "rst"
```

Typically, you specify the bits to be tested by using keywords. Bit-field match keywords always map to a single bit value. You also can specify bit fields as hexadecimal or decimal numbers.

To match multiple bit-field values, use the logical operators, which are described in [Table 19 on page 65](#). The operators are listed in order from highest precedence to lowest precedence. Operations are left-associative.



Table 19: Logical Operators for Matching Multiple Bit-Field Operators

Logical Operators	Description
!	Negation.
&	Logical AND.
	Logical OR.

To negate a match, precede the value with an exclamation point. For example, a match occurs only if the RST bit in the TCP flags field is not set:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-flags "!rst"
```

In the following example of a logical AND operation, a match occurs if the packet is the initial packet on a TCP session:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-flags "syn&!ack"
```

In the following example of a logical OR operation, a match occurs if the packet is not the initial packet on a TCP session:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-flags "syn|ack"
```

For a logical OR operation, you can specify a maximum of two match conditions in a single term. If you need to match more than two bit-field values in a logical OR operation, configure the same match condition in consecutive terms with additional bit-field values. In the following example, the two terms configured match the SYN, ACK, FIN, or RST bit in the TCP flags field:

```
[edit firewall family family-name filter filter-name term term-name1 from]
user@switch# set tcp-flags "syn|ack"
[edit firewall family family-name filter filter-name term term-name2 from]
user@switch# set tcp-flags "fin|rst"
```

You can use text synonyms to specify some common bit-field matches. You specify these matches as a single keyword. In the following example of a text synonym, a match occurs if the packet is the initial packet on a TCP session:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-flags tcp-initial
```

#### Related Documentation

- [Firewall Filters for EX Series Switches Overview on page 7](#)
- [Understanding How Firewall Filters Test a Packet's Protocol on page 66](#)
- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)
- [Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches on page 96](#)
- [Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 16](#)

## Understanding How Firewall Filters Test a Packet's Protocol

---

When examining match conditions, Juniper Networks Junos operating system (Junos OS) for Juniper Networks EX Series Ethernet Switches tests only the field that is specified. The software does not implicitly test the IP header to determine whether a packet is an IP packet. Therefore, in some cases, you must specify **protocol** field match conditions in conjunction with other match conditions to ensure that the filters are performing the expected matches.

If you specify a protocol match condition or a match of the ICMP type or TCP flags field, there is no implied protocol match. For the following match conditions, you must explicitly specify the protocol match condition in the same term:

- **destination-port**—Specify the match **protocol tcp** or **protocol udp**.
- **source-port**—Specify the match **protocol tcp** or **protocol udp**.

If you do not specify the protocol when using the preceding fields, design your filters carefully to ensure that they perform the expected matches. For example, if you specify a match of **destination-port ssh**, the switch deterministically matches any packets that have a value of **22** in the two-byte field that is two bytes beyond the end of the IP header without ever checking the IP protocol field.

### Related Documentation

- [Firewall Filters for EX Series Switches Overview on page 7](#)
- [Understanding Firewall Filter Match Conditions on page 62](#)
- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)

## Understanding the Use of Policers in Firewall Filters

---

Policing, or rate limiting, is an important component of firewall filters that lets you control the amount of traffic that enters an interface on Juniper Networks EX Series Ethernet Switches. You can achieve policing by including policers in firewall filter configurations.

This topic describes:

- [Policers Overview on page 66](#)
- [Policer Types on page 67](#)
- [Policer Actions on page 68](#)
- [Policer Levels on page 68](#)
- [Color Modes on page 69](#)
- [Naming Conventions for Policers on page 69](#)

### Policers Overview

You can use policers to specify rate limits on traffic. A firewall filter configured with a policer permits only traffic within a specified set of rate limits, thereby providing protection

from denial-of-service (DoS) attacks. Traffic that exceeds the rate limits specified by the policer is either discarded immediately or is marked as lower priority than traffic that is within the rate limits. The switch discards the lower-priority traffic when there is traffic congestion.

A policer applies two types of rate limits on traffic:

- Bandwidth—The number of bits per second permitted, on average.
- Maximum burst size—The maximum size permitted for bursts of data that exceed the given bandwidth limit.

Policing uses an algorithm to enforce a limit on average bandwidth while allowing bursts up to a specified maximum value. You can define specific classes of traffic on an interface and apply a set of rate limits to each class. After you name and configure a policer, it is stored as a template. You can then use the policer in a firewall filter configuration.

On all EX Series switches except Juniper Networks EX8200 Ethernet Switches, each policer that you configure includes an implicit counter that counts the number of packets that exceed the rate limit specified for the policer. Each EX8200 switch contains three global management counters. You must assign ingress policers to these global management counters to obtain policer statistics. You can assign any number of ingress policers to each global management counter. The policer statistics for each global management counter are the aggregate of the policer statistics for all policers associated with that global management counter.

To get filter-specific packet counts, you must configure a different policer for each firewall filter. Policers give term-specific counts by default.

## Policer Types

Switches support three types of policers:

- Single-rate two-color—A two-color policer (sometimes called simply “policer”) meters the traffic stream and classifies packets into two categories of packet loss priority (PLP) according to a configured bandwidth and burst-size limit. You can mark packets that exceed the bandwidth and burst-size limit or simply discard them. A two-color policer is most useful for metering traffic at the port (physical interface) level.
- Single-rate three-color—This type of policer is defined in RFC 2697, *A Single Rate Three Color Marker*, as part of an assured forwarding (AF) per-hop-behavior (PHB) classification system for a Differentiated Services (DiffServ) environment. This type of policer meters traffic based on the configured committed information rate (CIR), committed burst size (CBS), and the excess burst size (EBS). Traffic is marked as belonging to one of three categories (green, yellow, or red) based on whether the packets are arriving at rates that are below the CBS (green), exceed the CBS but not the EBS (yellow), or exceed the EBS (red). A single-rate three-color policer is most useful when a service is structured according to packet size and not according to peak arrival rate.
- Two-rate three-color—This type of policer is defined in RFC 2698, *A Two Rate Three Color Marker*, as part of an assured forwarding (AF) per-hop-behavior (PHB) classification system for a Differentiated Services (DiffServ) environment. This type

of policer meters traffic based on the configured CIR and the peak information rate (PIR), along with their associated burst sizes; the CBS, and the peak burst size (PBS). Traffic is marked as belonging to one of three categories (green, yellow, or red) based on packets arriving at rates that are below the CIR (green), exceed the CIR but not the PIR (yellow), or exceed the PIR (red). A two-rate three-color policer is most useful when a service is structured according to arrival rates and not to packet size.

## Policer Actions

Policer actions can be implicit or explicit and vary by policer type. The term implicit means that Junos OS assigns a loss-priority value automatically; explicit means that you configure the action. [Table 20 on page 68](#) lists policer actions.

**Table 20: Policer Actions**

Policer	Marking	Implicit Action	Configurable Action
Single-rate two-color	Green (Conforming)	Assign low loss priority	None
	Red (Nonconforming)	None	Assign low or high loss priority, assign a forwarding class, or discard
	Yellow	Not supported	Not supported
Single-rate three-color	Green (Conforming)	Assign low loss priority	None
	Red (Above the EBS)	Assign high loss priority	Discard
	Yellow (Exceeds the CBS but not the EBS)	Assign high loss priority <b>NOTE:</b> Not supported on EX8200 switches	None <b>NOTE:</b> Not supported on EX8200 switches
Two-rate three-color	Green (Conforming)	Assign low loss priority	None
	Red (Above the PIR)	Assign high loss priority	Discard
	Yellow (Exceeds the CIR but not the PIR)	Assign high loss priority <b>NOTE:</b> Not supported on EX8200 switches	None <b>NOTE:</b> Not supported on EX8200 switches

## Policer Levels

You can configure policers at the queue level, logical interface level, or Layer 2 (MAC) level. Only a single policer is applied to a packet at the egress queue. The search for policers occurs in this order:

- Queue level
- Logical interface level

- Layer 2 (MAC) level

## Color Modes

Tricolor marking (TCM) policers are not bound by a green-yellow-red coloring convention. Packets are marked with low or high PLP bit configurations based on color. Therefore, both three-color policer types (single-rate and two-rate) extend the functionality of class-of-service (CoS) traffic policing by providing three levels of drop precedence (loss priority) instead of the two normally available in policers. Both single-rate and two-rate three-color policer types can operate in two modes:

- Color-blind—In color-blind mode, the three-color policer operates without reference to whether the examined packets have been previously marked or metered. In other words, the three-color policer is *blind* to any previous coloring a packet might have had.
- Color-aware—In color-aware mode, the three-color policer operates with reference to any previous marking or metering of the examined packets. In other words, the three-color policer is *aware* of the previous coloring a packet might have had. In color-aware mode, the three-color policer can increase the PLP of a packet but can never decrease it. For example, if a color-aware three-color policer meters a packet with a low PLP marking, it can raise the PLP level to high. But it cannot reduce a high PLP level to low.

## Naming Conventions for Policers

We recommend you use the naming convention *rate-TCMnumber-colortype* when configuring three-color policers. TCM stands for tricolor marking. Because policers can be numerous and must be applied correctly to work, observing a simple naming convention makes it easier to apply the policers properly.

For example, if you configure a single-rate, three-color, color-aware policer, name it srTCM1-ca. If you configure a two-rate, three-color, color-blind policer, name it trTCM2-cb.

### Related Documentation

- [Firewall Filters for EX Series Switches Overview on page 7](#)
- [Understanding Tricolor Marking Architecture on page 70](#)
- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)
- [Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 16](#)

## Understanding Filter-Based Forwarding for EX Series Switches

---

Administrators of Juniper Networks EX Series Ethernet Switches can use firewall filters in conjunction with virtual routing instances to specify different routes for packets to travel in their networks. To set up this feature, which is called filter-based forwarding, you specify a filter and match criteria and then specify the virtual routing instance to send packets to.

You might want to use filter-based forwarding to route specific types of traffic through a firewall or security device before the traffic continues on its path. You can also use filter-based forwarding to give certain types of traffic preferential treatment or to improve load balancing of switch traffic.

### Related Documentation

- [Understanding Virtual Routing Instances on EX Series Switches](#)
- [Firewall Filters for EX Series Switches Overview on page 7](#)
- [Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches on page 96](#)

## Understanding Tricolor Marking Architecture

---

Tricolor marking (TCM) policers provide two functions: metering and marking. A policer meters each packet and passes the packet and the metering result to the marker.

The meter operates in two modes. In the color-blind mode, the meter treats the packet stream as uncolored. Any preset loss priorities are ignored. In the color-aware mode, the meter inspects the packet loss priority (PLP) field, which has been set by an upstream device as high or low; in other words, the PLP field has already been set by a behavior aggregate (BA) or multifield (MF) classifier. The marker changes the PLP of each incoming IP packet according to the results of the meter.

Single-rate TCM is so called because traffic is policed according to one rate—the committed burst rate (CBR)—and two burst sizes: the committed burst size (CBS) and the excess burst size (EBS). The configured information rate (CIR) specifies the average rate at which bits are admitted to the network. The CBS specifies the usual burst size in bytes and the EBS specifies the maximum burst size in bytes for packets that are admitted to the network. The EBS is greater than or equal to the CBS, and neither can be 0. As each packet enters the network, its bytes are counted. Packets that do not exceed the CBS are marked low PLP. Packets that exceed the peak information rate (PIR) are marked high PLP.

Two-rate TCM is so called because traffic is policed according to two rates: the CIR and the PIR. The PIR is greater than or equal to the CIR. The CIR specifies the average rate at which bits are admitted to the network, and the PIR specifies the maximum rate at which bits are admitted to the network. As each packet enters the network, its bits are counted. Bits in packets that do not exceed the CIR have their packets marked low PLP. Bits in packets that exceed the PIR have their packets marked high PLP.

- Related Documentation**
- [Understanding the Use of Policers in Firewall Filters on page 66](#)
  - [Configuring Tricolor Marking Policers on page 128](#)





## PART 2

# Configuration

- [Configuration Examples on page 75](#)
- [Configuration Tasks on page 107](#)
- [Configuration Statements on page 131](#)



## CHAPTER 3

# Configuration Examples

- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)
- [Example: Configuring a Firewall Filter on a Management Interface on an EX Series Switch on page 93](#)
- [Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches on page 96](#)
- [Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication on page 100](#)

### Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches

---

This example shows how to configure and apply firewall filters to control traffic that is entering or exiting a port on the switch, a VLAN on the network, and a Layer 3 interface on the switch. Firewall filters define the rules that determine whether to forward or deny packets at specific processing points in the packet flow.

- [Requirements on page 75](#)
- [Overview on page 76](#)
- [Configuring an Ingress Port Firewall Filter to Prioritize Voice Traffic and Rate-Limit TCP and ICMP Traffic on page 79](#)
- [Configuring a VLAN Ingress Firewall Filter to Prevent Rogue Devices from Disrupting VoIP Traffic on page 84](#)
- [Configuring a VLAN Firewall Filter to Count, Monitor, and Analyze Egress Traffic on the Employee VLAN on page 86](#)
- [Configuring a VLAN Firewall Filter to Restrict Guest-to-Employee Traffic and Peer-to-Peer Applications on the Guest VLAN on page 88](#)
- [Configuring a Router Firewall Filter to Give Priority to Egress Traffic Destined for the Corporate Subnet on page 90](#)
- [Verification on page 91](#)

### Requirements

This example uses the following software and hardware components:

- Junos OS Release 9.0 or later for EX Series switches.
- Two Juniper Networks EX3200-48T switches: one to be used as an access switch, the other to be used as a distribution switch
- One Juniper Networks EX-UM-4SFP uplink module
- One Juniper Networks J-series router

Before you configure and apply the firewall filters in this example, be sure you have:

- An understanding of firewall filter concepts, policers, and CoS
- Installed the uplink module in the distribution switch. See [Installing an Uplink Module in an EX3200 Switch](#).

## Overview

This configuration example show how to configure and apply firewall filters to provide rules to evaluate the contents of packets and determine when to discard, forward, classify, count, and analyze packets that are destined for or originating from the EX Series switches that handle all **voice-vlan**, **employee-vlan**, and **guest-vlan** traffic. [Table 21 on page 76](#) shows the firewall filters that are configured for the EX Series switches in this example.

**Table 21: Configuration Components: Firewall Filters**

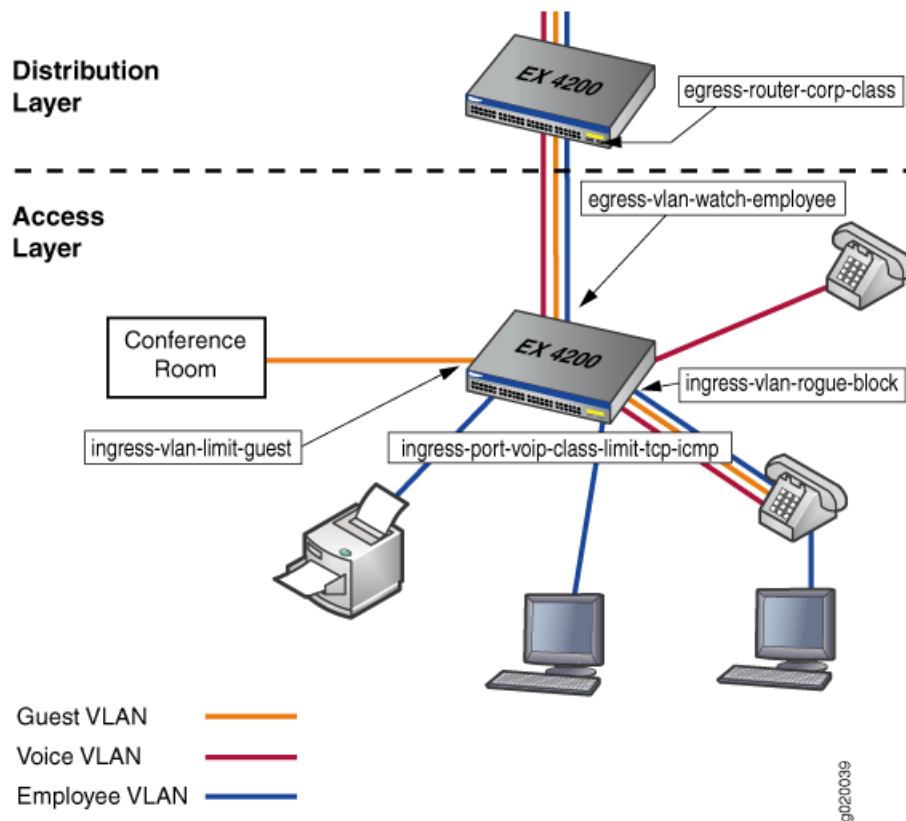
Component	Purpose/Description
Port firewall filter, <b>ingress-port-voip-class-limit-tcp-icmp</b>	<p>This firewall filter performs two functions:</p> <ul style="list-style-type: none"> <li>• Assigns priority queueing to packets with a source MAC address that matches the phone MAC addresses. The forwarding class <b>expedited-forwarding</b> provides low loss, low delay, low jitter, assured bandwidth, and end-to-end service for all <b>voice-vlan</b> traffic.</li> <li>• Performs rate limiting on packets that enter the ports for <b>employee-vlan</b>. The traffic rate for TCP and ICMP packets is limited to 1 Mbps with a burst size up to 30,000 bytes.</li> </ul> <p>This firewall filter is applied to port interfaces on the access switch.</p>
VLAN firewall filter, <b>ingress-vlan-rogue-block</b>	<p>Prevents rogue devices from using HTTP sessions to mimic the gatekeeper device that manages call registration, admission, and call status for VoIP calls. Only TCP or UDP ports should be used; and only the gatekeeper uses HTTP. That is, all <b>voice-vlan</b> traffic on TCP ports should be destined for the gatekeeper device. This firewall filter applies to all phones on <b>voice-vlan</b>, including communication between any two phones on the VLAN and all communication between the gatekeeper device and VLAN phones.</p> <p>This firewall filter is applied to VLAN interfaces on the access switch.</p>
VLAN firewall filter, <b>egress-vlan-watch-employee</b>	<p>Accepts <b>employee-vlan</b> traffic destined for the corporate subnet, but does not monitor this traffic. Employee traffic destined for the Web is counted and analyzed.</p> <p>This firewall filter is applied to vlan interfaces on the access switch.</p>

Table 21: Configuration Components: Firewall Filters (*continued*)

Component	Purpose/Description
VLAN firewall filter, <b>ingress-vlan-limit-guest</b>	Prevents guests (non-employees) from talking with employees or employee hosts on <b>employee-vlan</b> . Also prevents guests from using peer-to-peer applications on <b>guest-vlan</b> , but allows guests to access the Web.  This firewall filter is applied to VLAN interfaces on the access switch.
Router firewall filter, <b>egress-router-corp-class</b>	Prioritizes <b>employee-vlan</b> traffic, giving highest forwarding-class priority to employee traffic destined for the corporate subnet.  This firewall filter is applied to a routed port (Layer 3 uplink module) on the distribution switch.

Figure 4 on page 77 shows the application of port, VLAN, and Layer 3 routed firewall filters on the switch.

Figure 4: Application of Port, VLAN, and Layer 3 Routed Firewall Filters



### Network Topology

The topology for this configuration example consists of one EX-3200-48T switch at the access layer, and one EX-3200-48T switch at the distribution layer. The distribution switch's uplink module is configured to support a Layer 3 connection to a J-series router.

The EX Series switches are configured to support VLAN membership. [Table 22 on page 78](#) shows the VLAN configuration components for the VLANs.

**Table 22: Configuration Components: VLANs**

VLAN Name	VLAN ID	VLAN Subnet and Available IP Addresses	VLAN Description
voice-vlan	10	192.0.2.0/28 192.0.2.1 through 192.0.2.14  192.0.2.15 is subnet's broadcast address	Voice VLAN used for employee VoIP traffic
employee-vlan	20	192.0.2.16/28 192.0.2.17 through 192.0.2.30 192.0.2.31 is subnet's broadcast address	VLAN standalone PCs, PCs connected to the network through the hub in VoIP telephones, wireless access points, and printers. This VLAN completely includes the voice VLAN. Two VLANs ( <b>voice-vlan</b> and <b>employee-vlan</b> ) must be configured on the ports that connect to the telephones.
guest-vlan	30	192.0.2.32/28 192.0.2.33 through 192.0.2.46 192.0.2.47 is subnet's broadcast address	VLAN for guests' data devices (PCs). The scenario assumes that the corporation has an area open to visitors, either in the lobby or in a conference room, that has a hub to which visitors can plug in their PCs to connect to the Web and to their company's VPN.
camera-vlan	40	192.0.2.48/28 192.0.2.49 through 192.0.2.62 192.0.2.63 is subnet's broadcast address	VLAN for the corporate security cameras.

Ports on the EX Series switches support Power over Ethernet (PoE) to provide both network connectivity and power for VoIP telephones connecting to the ports. [Table 23 on page 78](#) shows the switch ports that are assigned to the VLANs and the IP and MAC addresses for devices connected to the switch ports:

**Table 23: Configuration Components: Switch Ports on a 48-Port All-PoE Switch**

Switch and Port Number	VLAN Membership	IP and MAC Addresses	Port Devices
ge-0/0/0, ge-0/0/1	voice-vlan, employee-vlan	IP addresses: 192.0.2.1 through 192.0.2.2  MAC addresses: 00.05.85.00.00.01, 00.05.85.00–00.02	Two VoIP telephones, each connected to one PC.

Table 23: Configuration Components: Switch Ports on a 48-Port All-PoE Switch (*continued*)

Switch and Port Number	VLAN Membership	IP and MAC Addresses	Port Devices
ge-0/0/2, ge-0/0/3	employee-vlan	192.0.2.17 through 192.0.2.18	Printer, wireless access points
ge-0/0/4, ge-0/0/5	guest-vlan	192.0.2.34 through 192.0.2.35	Two hubs into which visitors can plug in their PCs. Hubs are located in an area open to visitors, such as a lobby or conference room
ge-0/0/6, ge-0/0/7	camera-vlan	192.0.2.49 through 192.0.2.50	Two security cameras
ge-0/0/9	voice-vlan	IP address: 192.0.2.14 MAC address: 00.05.85.00.00.0E	Gatekeeper device. The gatekeeper manages call registration, admission, and call status for VoIP phones.
ge-0/1/0		IP address: 192.0.2.65	Layer 3 connection to a router; note that this is a port on the switch's uplink module

### Configuring an Ingress Port Firewall Filter to Prioritize Voice Traffic and Rate-Limit TCP and ICMP Traffic

To configure and apply firewall filters for port, VLAN, and router interfaces, perform these tasks:

#### CLI Quick Configuration

To quickly configure and apply a port firewall filter to prioritize voice traffic and rate-limit packets that are destined for the **employee-vlan** subnet, copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall policer tcp-connection-policer if-exceeding burst-size-limit 30k bandwidth-limit 1m
set firewall policer tcp-connection-policer then discard
set firewall policer icmp-connection-policer if-exceeding burst-size-limit 30k bandwidth-limit 1m
set firewall policer icmp-connection-policer then discard
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term voip-high
from source-mac-address 00.05.85.00.00.01
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term voip-high
from source-mac-address 00.05.85.00.00.02
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term voip-high
from protocol udp
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term voip-high
then forwarding-class expedited-forwarding
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term voip-high
then loss-priority low
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term
network-control from precedence net-control
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term
network-control then forwarding-class network-control
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term
network-control then loss-priority low
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term
tcp-connection from destination-address 192.0.2.16/28
```

```

set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term
tcp-connection from protocol tcp
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term
tcp-connection then policer tcp-connection-policer
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term
tcp-connection then count tcp-counter
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term
tcp-connection then forwarding-class best-effort
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term
tcp-connection then loss-priority high
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term
icmp-connection from destination-address 192.0.2.16/28
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term
icmp-connection from protocol icmp
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term
icmp-connection then policer icmp-connection-policer
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term
icmp-connection then count icmp-counter
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term
icmp-connection then forwarding-class best-effort
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term
icmp-connection then loss-priority high
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term best-effort
then forwarding-class best-effort
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term best-effort
then loss-priority high
set interfaces ge-0/0/0 description "voice priority and tcp and icmp traffic rate-limiting filter at
ingress port"
set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input
ingress-port-voip-class-limit-tcp-icmp
set interfaces ge-0/0/1 description "voice priority and tcp and icmp traffic rate-limiting filter at
ingress port"
set interfaces ge-0/0/1 unit 0 family ethernet-switching filter input
ingress-port-voip-class-limit-tcp-icmp
set class-of-service schedulers voice-high buffer-size percent 15
set class-of-service schedulers voice-high priority high
set class-of-service schedulers net-control buffer-size percent 10
set class-of-service schedulers net-control priority high
set class-of-service schedulers best-effort buffer-size percent 75
set class-of-service schedulers best-effort priority low
set class-of-service scheduler-maps ethernet-diffsrv-cos-map forwarding-class
expedited-forwarding scheduler voice-high
set class-of-service scheduler-maps ethernet-diffsrv-cos-map forwarding-class network-control
scheduler net-control
set class-of-service scheduler-maps ethernet-diffsrv-cos-map forwarding-class best-effort
scheduler best-effort

```

**Step-by-Step Procedure** To configure and apply a port firewall filter to prioritize voice traffic and rate-limit packets that are destined for the `employee-vlan` subnet:

1. Define the policers `tcp-connection-policer` and `icmp-connection-policer`:
 

```

[edit]
user@switch# set firewall policer tcp-connection-policer if-exceeding burst-size-limit 30k
bandwidth-limit 1m
user@switch# set firewall policer tcp-connection-policer then discard
user@switch# set firewall policer icmp-connection-policer if-exceeding burst-size-limit
30k bandwidth-limit 1m
user@switch# set firewall policer icmp-connection-policer then discard

```
2. Define the firewall filter `ingress-port-voip-class-limit-tcp-icmp`:



- ```
[edit firewall]
user@switch# set family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp
```
3. Define the term **voip-high**:
 

```
[edit firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp ]
user@switch# set term voip-high from source-mac-address 00.05.85.00.00.01
user@switch# set term voip-high from source-mac-address 00.05.85.00.00.02
user@switch# set term voip-high from protocol udp
user@switch# set term voip-high then forwarding-class expedited-forwarding
user@switch# set term voip-high then loss-priority low
```
  4. Define the term **network-control**:
 

```
[edit firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp ]
user@switch# set term network-control from precedence net-control
user@switch# set term network-control then forwarding-class network-control
user@switch# set term network-control then loss-priority low
```
  5. Define the term **tcp-connection** to configure rate limits for TCP traffic:
 

```
[edit firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp]
user@switch# set term tcp-connection from destination-address 192.0.2.16/28
user@switch# set term tcp-connection from protocol tcp
user@switch# set term tcp-connection then policer tcp-connection-policer
user@switch# set term tcp-connection then count tcp-counter
user@switch# set term tcp-connection then forwarding-class best-effort
user@switch# set term tcp-connection then loss-priority high
```
  6. Define the term **icmp-connection** to configure rate limits for ICMP traffic:
 

```
[edit firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp]
user@switch# set term icmp-connection from destination-address 192.0.2.16/28
user@switch# set term icmp-connection from protocol icmp
user@switch# set term icmp-connection then policer icmp-policer
user@switch# set term icmp-connection then count icmp-counter
user@switch# set term icmp-connection then forwarding-class best-effort
user@switch# set term icmp-connection then loss-priority high
```
  7. Define the term **best-effort** with no match conditions for an implicit match on all packets that did not match any other term in the firewall filter:
 

```
[edit firewall family ethernet-switching filter
ingress-port-voip-class-limit-tcp-icmp]
user@switch# set term best-effort then forwarding-class best-effort
user@switch# set term best-effort then loss-priority high
```
  8. Apply the firewall filter **ingress-port-voip-class-limit-tcp-icmp** as an input filter to the port interfaces for **employee-vlan** :
 

```
[edit interfaces]
user@switch# set ge-0/0/0 description "voice priority and tcp and icmp traffic rate-limiting
filter at ingress port"
user@switch# set ge-0/0/0 unit 0 family ethernet-switching filter input
ingress-port-voip-class-limit-tcp-icmp
user@switch# set ge-0/0/1 description "voice priority and tcp and icmp traffic rate-limiting
filter at ingress port"
user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter input
ingress-port-voip-class-limit-tcp-icmp
```
  9. Configure the parameters that are desired for the different schedulers.



**NOTE:** When you configure parameters for the schedulers, define the numbers to match your network traffic patterns.

- ```
[edit class-of-service]
user@switch# set schedulers voice-high buffer-size percent 15
user@switch# set schedulers voice-high priority high
user@switch# set schedulers network-control buffer-size percent 10
user@switch# set schedulers network-control priority high
user@switch# set schedulers best-effort buffer-size percent 75
user@switch# set schedulers best-effort priority low
```
10. Assign the forwarding classes to schedulers with a scheduler map:
- ```
[edit class-of-service]
user@switch# set scheduler-maps ethernet-diffsrv-cos-map
user@switch# set scheduler-maps ethernet-diffsrv-cos-map forwarding-class
expedited-forwarding scheduler voice-high
user@switch# set scheduler-maps ethernet-diffsrv-cos-map forwarding-class
network-control scheduler net-control
user@switch# set scheduler-maps ethernet-diffsrv-cos-map forwarding-class best-effort
scheduler best-effort
```
11. Associate the scheduler map with the outgoing interface:
- ```
[edit class-of-service]
user@switch# set interfaces ge-0/1/0 scheduler-map ethernet-diffsrv-cos-map
```

**Results** Display the results of the configuration:

```
user@switch# show
firewall {
  policer tcp-connection-policer {
    if-exceeding {
      bandwidth-limit 1m;
      burst-size-limit 30k;
    }
    then {
      discard;
    }
  }
  policer icmp-connection-policer {
    if-exceeding {
      bandwidth-limit 1m;
      burst-size-limit 30k;
    }
    then {
      discard;
    }
  }
}
family ethernet-switching {
  filter ingress-port-voip-class-limit-tcp-icmp {
    term voip-high {
      from {
        destination-mac-address 00.05.85.00.00.01;
        destination-mac-address 00.05.85.00.00.02;
        protocol udp;
      }
    }
  }
}
```

```

    }
    then {
        forwarding-class expedited-forwarding;
        loss-priority low;
    }
}
term network-control {
    from {
        precedence net-control ;
    }
    then {
        forwarding-class network-control;
        loss-priority low;
    }
}
term tcp-connection {
    from {
        destination-address 192.0.2.16/28;
        protocol tcp;
    }
    then {
        policer tcp-connection-policer;
        count tcp-counter;
        forwarding-class best-effort;
        loss-priority high;
    }
}
term icmp-connection
    from {
        protocol icmp;
    }
    then {
        policer icmp-connection-policer;
        count icmp-counter;
        forwarding-class best-effort;
        loss-priority high;
    }
}
term best-effort {
    then {
        forwarding-class best-effort;
        loss-priority high;
    }
}
}
}
}
interfaces {
    ge-0/0/0 {
        description "voice priority and tcp and icmp traffic rate-limiting filter at ingress port";
        unit 0 {
            family ethernet-switching {
                filter {
                    input ingress-port-voip-class-limit-tcp-icmp;
                }
            }
        }
    }
}

```

```
    }
  }
  ge-0/0/1 {
    description "voice priority and tcp and icmp traffic rate-limiting filter at ingress port";
    unit 0 {
      family ethernet-switching {
        filter {
          input ingress-port-voip-class-limit-tcp-icmp;
        }
      }
    }
  }
}
scheduler-maps {
  ethernet-diffsrv-cos-map {
    forwarding-class expedited-forwarding scheduler voice-high;
    forwarding-class network-control scheduler net-control;
    forwarding-class best-effort scheduler best-effort;
  }
}
interfaces {
  ge-0/1/0 {
    scheduler-map ethernet-diffsrv-cos-map;
  }
}
```

## Configuring a VLAN Ingress Firewall Filter to Prevent Rogue Devices from Disrupting VoIP Traffic

To configure and apply firewall filters for port, VLAN, and router interfaces, perform these tasks:

### CLI Quick Configuration

To quickly configure a VLAN firewall filter on **voice-vlan** to prevent rogue devices from using HTTP sessions to mimic the gatekeeper device that manages VoIP traffic, copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family ethernet-switching filter ingress-vlan-rogue-block term to-gatekeeper from destination-address 192.0.2.14
set firewall family ethernet-switching filter ingress-vlan-rogue-block term to-gatekeeper from destination-port 80
set firewall family ethernet-switching filter ingress-vlan-rogue-block term to-gatekeeper then accept
set firewall family ethernet-switching filter ingress-vlan-rogue-block term from-gatekeeper from source-address 192.0.2.14
set firewall family ethernet-switching filter ingress-vlan-rogue-block term from-gatekeeper from source-port 80
set firewall family ethernet-switching filter ingress-vlan-rogue-block term from-gatekeeper then accept
set firewall family ethernet-switching filter ingress-vlan-rogue-block term not-gatekeeper from destination-port 80
set firewall family ethernet-switching filter ingress-vlan-rogue-block term not-gatekeeper then count rogue-counter
set firewall family ethernet-switching filter ingress-vlan-rogue-block term not-gatekeeper then discard
set vlans voice-vlan description "block rogue devices on voice-vlan"
set vlans voice-vlan filter input ingress-vlan-rogue-block
```

**Step-by-Step Procedure** To configure and apply a VLAN firewall filter on **voice-vlan** to prevent rogue devices from using HTTP to mimic the gatekeeper device that manages VoIP traffic:

1. Define the firewall filter **ingress-vlan-rogue-block** to specify filter matching on the traffic you want to permit and restrict:  

```
[edit firewall]
user@switch# set family ethernet-switching filter ingress-vlan-rogue-block
```
2. Define the term **to-gatekeeper** to accept packets that match the destination IP address of the gatekeeper:  

```
[edit firewall family ethernet-switching filter ingress-vlan-rogue-block]
user@switch# set term to-gatekeeper from destination-address 192.0.2.14
user@switch# set term to-gatekeeper from destination-port 80
user@switch# set term to-gatekeeper then accept
```
3. Define the term **from-gatekeeper** to accept packets that match the source IP address of the gatekeeper:  

```
[edit firewall family ethernet-switching filter ingress-vlan-rogue-block]
user@switch# set term from-gatekeeper from source-address 192.0.2.14
user@switch# set term from-gatekeeper from source-port 80
user@switch# set term from-gatekeeper then accept
```
4. Define the term **not-gatekeeper** to ensure all **voice-vlan** traffic on TCP ports is destined for the gatekeeper device:  

```
[edit firewall family ethernet-switching filter ingress-vlan-rogue-block]
user@switch# set term not-gatekeeper from destination-port 80
user@switch# set term not-gatekeeper then count rogue-counter
user@switch# set term not-gatekeeper then discard
```
5. Apply the firewall filter **ingress-vlan-rogue-block** as an input filter to the VLAN interface for the VoIP telephones:  

```
[edit]
user@switch# set vlans voice-vlan description "block rogue devices on voice-vlan"
user@switch# set vlans voice-vlan filter input ingress-vlan-rogue-block
```

**Results** Display the results of the configuration:

```
user@switch# show
firewall {
  family ethernet-switching {
    filter ingress-vlan-rogue-block {
      term to-gatekeeper {
        from {
          destination-address 192.0.2.14/32
          destination-port 80;
        }
        then {
          accept;
        }
      }
      term from-gatekeeper {
        from {
          source-address 192.0.2.14/32
          source-port 80;
        }
        then {
          accept;
        }
      }
    }
  }
}
```

```
    }  
  }  
  term not-gatekeeper {  
    from {  
      destination-port 80;  
    }  
    then {  
      count rogue-counter;  
      discard;  
    }  
  }  
}  
vpls {  
  voice-vlan {  
    description "block rogue devices on voice-vlan";  
    filter {  
      input ingress-vlan-rogue-block;  
    }  
  }  
}
```

## Configuring a VLAN Firewall Filter to Count, Monitor, and Analyze Egress Traffic on the Employee VLAN

To configure and apply firewall filters for port, VLAN, and router interfaces, perform these tasks:

**CLI Quick Configuration** A firewall filter is configured and applied to VLAN interfaces to filter **employee-vlan** egress traffic. Employee traffic destined for the corporate subnet is accepted but not monitored. Employee traffic destined for the Web is counted and analyzed.

To quickly configure and apply a VLAN firewall filter, copy the following commands and paste them into the switch terminal window:

```
[edit]  
set firewall family ethernet-switching filter egress-vlan-watch-employee term employee-to-corp  
from destination-address 192.0.2.16/28  
set firewall family ethernet-switching filter egress-vlan-watch-employee term employee-to-corp  
then accept  
set firewall family ethernet-switching filter egress-vlan-watch-employee term employee-to-web  
from destination-port 80  
set firewall family ethernet-switching filter egress-vlan-watch-employee term employee-to-web  
then count employee-web-counter  
set firewall family ethernet-switching filter egress-vlan-watch-employee term employee-to-web  
then analyzer employee-monitor  
set vlans employee-vlan description "filter at egress VLAN to count and analyze employee to  
Web traffic"  
set vlans employee-vlan filter output egress-vlan-watch-employee
```

**Step-by-Step Procedure** To configure and apply an egress port firewall filter to count and analyze **employee-vlan** traffic that is destined for the Web:

1. Define the firewall filter **egress-vlan-watch-employee**:

```
[edit firewall]
user@switch# set family ethernet-switching filter egress-vlan-watch-employee
```

2. Define the term **employee-to-corp** to accept but not monitor all **employee-vlan** traffic destined for the corporate subnet:

```
[edit firewall family ethernet-switching filter egress-vlan-watch-employee]
user@switch# set term employee-to-corp from destination-address 192.0.2.16/28
user@switch# set term employee-to-corp then accept
```

3. Define the term **employee-to-web** to count and monitor all **employee-vlan** traffic destined for the Web:

```
[edit firewall family ethernet-switching filter egress-vlan-watch-employee]
user@switch# set term employee-to-web from destination-port 80
user@switch# set term employee-to-web then count employee-web-counter
user@switch# set term employee-to-web then analyzer employee-monitor
```



**NOTE:** See Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches for information about configuring the **employee-monitor** analyzer.

4. Apply the firewall filter **egress-vlan-watch-employee** as an output filter to the port interfaces for the VoIP telephones:

```
[edit]
user@switch# set vlans employee-vlan description "filter at egress VLAN to count and
analyze employee to Web traffic"
user@switch# set vlans employee-vlan filter output egress-vlan-watch-employee
```

**Results** Display the results of the configuration:

```
user@switch# show
firewall {
  family ethernet-switching {
    filter egress-vlan-watch-employee {
      term employee-to-corp {
        from {
          destination-address 192.0.2.16/28
        }
        then {
          accept;
        }
      }
      term employee-to-web {
        from {
          destination-port 80;
        }
        then {
          count employee-web-counter;
          analyzer employee-monitor;
        }
      }
    }
  }
}
```

```

    }
  }
}
vlands {
  employee-vlan {
    description "filter at egress VLAN to count and analyze employee to Web traffic";
    filter {
      output egress-vlan-watch-employee;
    }
  }
}
}

```

## Configuring a VLAN Firewall Filter to Restrict Guest-to-Employee Traffic and Peer-to-Peer Applications on the Guest VLAN

To configure and apply firewall filters for port, VLAN, and router interfaces, perform these tasks:

### CLI Quick Configuration

In the following example, the first filter term permits guests to talk with other guests but not employees on **employee-vlan**. The second filter term allows guests Web access but prevents them from using peer-to-peer applications on **guest-vlan**.

To quickly configure a VLAN firewall filter to restrict guest-to-employee traffic, blocking guests from talking with employees or employee hosts on **employee-vlan** or attempting to use peer-to-peer applications on **guest-vlan**, copy the following commands and paste them into the switch terminal window:

```

[edit]
set firewall family ethernet-switching filter ingress-vlan-limit-guest term guest-to-guest from
destination-address 192.0.2.33/28
set firewall family ethernet-switching filter ingress-vlan-limit-guest term guest-to-guest then
accept
set firewall family ethernet-switching filter ingress-vlan-limit-guest term
no-guest-employee-no-peer-to-peer from destination-mac-address 00:05:85:00:00:DF
set firewall family ethernet-switching filter ingress-vlan-limit-guest term
no-guest-employee-no-peer-to-peer then accept
set vlans guest-vlan description "restrict guest-to-employee traffic and peer-to-peer applications
on guest VLAN"
set vlans guest-vlan filter input ingress-vlan-limit-guest

```

### Step-by-Step Procedure

To configure and apply a VLAN firewall filter to restrict guest-to-employee traffic and peer-to-peer applications on **guest-vlan**:

1. Define the firewall filter **ingress-vlan-limit-guest**:

```

[edit firewall]
set firewall family ethernet-switching filter ingress-vlan-limit-guest

```

2. Define the term **guest-to-guest** to permit guests on the **guest-vlan** to talk with other guests but not employees on the **employee-vlan**:

```

[edit firewall family ethernet-switching filter ingress-vlan-limit-guest]
user@switch# set term guest-to-guest from destination-address 192.0.2.33/28
user@switch# set term guest-to-guest then accept

```

3. Define the term **no-guest-employee-no-peer-to-peer** to allow guests on **guest-vlan** Web access but prevent them from using peer-to-peer applications on the **guest-vlan**.





**NOTE:** The destination-mac-address is the default gateway, which for any host in a VLAN is the next-hop router.

- ```
[edit firewall family ethernet-switching filter ingress-vlan-limit-guest]
user@switch# set term no-guest-employee-no-peer-to-peer from destination-mac-address
00.05.85.00.00.DF
user@switch# set term no-guest-employee-no-peer-to-peer then accept
```
4. Apply the firewall filter **ingress-vlan-limit-guest** as an input filter to the interface for **guest-vlan** :
- ```
[edit]
user@switch# set vlans guest-vlan description "restrict guest-to-employee traffic and
peer-to-peer applications on guest VLAN"
user@switch# set vlans guest-vlan filter input ingress-vlan-limit-guest
```

**Results** Display the results of the configuration:

```
user@switch# show
firewall {
  family ethernet-switching {
    filter ingress-vlan-limit-guest {
      term guest-to-guest {
        from {
          destination-address 192.0.2.33/28;
        }
        then {
          accept;
        }
      }
      term no-guest-employee-no-peer-to-peer {
        from {
          destination-mac-address 00.05.85.00.00.DF;
        }
        then {
          accept;
        }
      }
    }
  }
}
vlans {
  guest-vlan {
    description "restrict guest-to-employee traffic and peer-to-peer applications on
    guest VLAN";
    filter {
      input ingress-vlan-limit-guest;
    }
  }
}
```

## Configuring a Router Firewall Filter to Give Priority to Egress Traffic Destined for the Corporate Subnet

To configure and apply firewall filters for port, VLAN, and router interfaces, perform these tasks:

### CLI Quick Configuration

To quickly configure a firewall filter for a routed port (Layer 3 uplink module) to filter **employee-vlan** traffic, giving highest forwarding-class priority to traffic destined for the corporate subnet, copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family inet filter egress-router-corp-class term corp-expedite from destination-address 192.0.2.16/28
set firewall family inet filter egress-router-corp-class term corp-expedite then forwarding-class expedited-forwarding
set firewall family inet filter egress-router-corp-class term corp-expedite then loss-priority low
set firewall family inet filter egress-router-corp-class term not-to-corp then accept
set interfaces ge-0/1/0 description "filter at egress router to expedite destined for corporate network"
set ge-0/1/0 unit 0 family inet address 103.104.105.1
set interfaces ge-0/1/0 unit 0 family inet filter output egress-router-corp-class
```

### Step-by-Step Procedure

To configure and apply a firewall filter to a routed port (Layer 3 uplink module) to give highest priority to **employee-vlan** traffic destined for the corporate subnet:

1. Define the firewall filter **egress-router-corp-class**:

```
[edit]
user@switch# set firewall family inet filter egress-router-corp-class
```

2. Define the term **corp-expedite**:

```
[edit firewall]
user@switch# set family inet filter egress-router-corp-class term corp-expedite from destination-address 192.0.2.16/28
user@switch# set family inet filter egress-router-corp-class term corp-expedite then forwarding-class expedited-forwarding
user@switch# set family inet filter egress-router-corp-class term corp-expedite then loss-priority low
```

3. Define the term **not-to-corp**:

```
[edit firewall]
user@switch# set family inet filter egress-router-corp-class term not-to-corp then accept
```

4. Apply the firewall filter **egress-router-corp-class** as an output filter for the port on the switch's uplink module, which provides a Layer 3 connection to a router:

```
[edit interfaces]
user@switch# set ge-0/1/0 description "filter at egress router to expedite employee traffic destined for corporate network"
user@switch# set ge-0/1/0 unit 0 family inet address 103.104.105.1
user@switch# set ge-0/1/0 unit 0 family inet filter output egress-router-corp-class
```

**Results** Display the results of the configuration:

```
user@switch# show
firewall {
  family inet {
    filter egress-router-corp-class {
```

```

term corp-expedite {
  from {
    destination-address 192.0.2.16/28;
  }
  then {
    forwarding-class expedited-forwarding;
    loss-priority low;
  }
}
term not-to-corp {
  then {
    accept;
  }
}
}
}
}
interfaces {
  ge-0/1/0 {
    unit 0 {
      description "filter at egress router interface to expedite employee traffic destined
for corporate network";
      family inet {
        source-address 103.104.105.1
        filter {
          output egress-router-corp-class;
        }
      }
    }
  }
}
}

```

## Verification

To confirm that the firewall filters are working properly, perform the following tasks:

- [Verifying that Firewall Filters and Policers are Operational on page 91](#)
- [Verifying that Schedulers and Scheduler-Maps are Operational on page 92](#)

### Verifying that Firewall Filters and Policers are Operational

**Purpose** Verify the operational state of the firewall filters and policers that are configured on the switch.

**Action** Use the operational mode command:

```

user@switch> show firewall
Filter: ingress-port-voip-class-limit-tcp-icmp
Counters:
Name                               Packets
icmp-counter                        0
tcp-counter                         0
Policers:
Name                               Packets
icmp-connection-policer            0
tcp-connection-policer             0

```

Filter: ingress-vlan-rogue-block

Filter: egress-vlan-watch-employee

Counters:

Name	Packets
employee-web-counter	0

**Meaning** The **show firewall** command displays the names of the firewall filters, policers, and counters that are configured on the switch. The output fields show byte and packet counts for all configured counters and the packet count for all policers.

### Verifying that Schedulers and Scheduler-Maps are Operational

**Purpose** Verify that schedulers and scheduler-maps are operational on the switch.

**Action** Use the operational mode command:

```
user@switch> show class-of-service scheduler-map
```

Scheduler map: default, Index: 2

Scheduler: default-be, Forwarding class: best-effort, Index: 20  
Transmit rate: 95 percent, Rate Limit: none, Buffer size: 95 percent,  
Priority: low

Drop profiles:

Loss priority	Protocol	Index	Name
Low	non-TCP	1	default-drop-profile
Low	TCP	1	default-drop-profile
High	non-TCP	1	default-drop-profile
High	TCP	1	default-drop-profile

Scheduler: default-nc, Forwarding class: network-control, Index: 22  
Transmit rate: 5 percent, Rate Limit: none, Buffer size: 5 percent,  
Priority: low

Drop profiles:

Loss priority	Protocol	Index	Name
Low	non-TCP	1	default-drop-profile
Low	TCP	1	default-drop-profile
High	non-TCP	1	default-drop-profile
High	TCP	1	default-drop-profile

Scheduler map: ethernet-diffsrv-cos-map, Index: 21657

Scheduler: best-effort, Forwarding class: best-effort, Index: 61257  
Transmit rate: remainder, Rate Limit: none, Buffer size: 75 percent,  
Priority: low

Drop profiles:

Loss priority	Protocol	Index	Name
Low	non-TCP	1	<default-drop-profile>
Low	TCP	1	<default-drop-profile>
High	non-TCP	1	<default-drop-profile>
High	TCP	1	<default-drop-profile>

Scheduler: voice-high, Forwarding class: expedited-forwarding, Index: 3123  
Transmit rate: remainder, Rate Limit: none, Buffer size: 15 percent,  
Priority: high

Drop profiles:

Loss priority	Protocol	Index	Name
Low	non-TCP	1	<default-drop-profile>

Low	TCP	1	<default-drop-profile>
High	non-TCP	1	<default-drop-profile>
High	TCP	1	<default-drop-profile>

Scheduler: net-control, Forwarding class: network-control, Index: 2451  
 Transmit rate: remainder, Rate Limit: none, Buffer size: 10 percent,  
 Priority: high  
 Drop profiles:

Loss priority	Protocol	Index	Name
Low	non-TCP	1	<default-drop-profile>
Low	TCP	1	<default-drop-profile>
High	non-TCP	1	<default-drop-profile>
High	TCP	1	<default-drop-profile>

**Meaning** Displays statistics about the configured schedulers and schedulers-maps.

- Related Documentation**
- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches](#)
  - [Example: Configuring CoS on EX Series Switches](#)
  - [Configuring Firewall Filters \(CLI Procedure\) on page 107](#)
  - [Configuring Firewall Filters \(J-Web Procedure\) on page 115](#)
  - [Configuring Policers to Control Traffic Rates \(CLI Procedure\) on page 119](#)
  - [Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 16](#)
  - [\[edit firewall\] Configuration Statement Hierarchy on EX Series Switches on page 131](#)

## Example: Configuring a Firewall Filter on a Management Interface on an EX Series Switch

You can configure a firewall filter on a management interface on an EX Series switch to filter ingress or egress traffic on the management interface on the switch. You can use utilities such as SSH or Telnet to connect to the management interface over the network and then use management protocols such as SNMP to gather statistical data from the switch.

This example discusses how to configure a firewall filter on a management interface to filter SSH packets egressing from an EX Series switch:

- [Requirements on page 93](#)
- [Overview and Topology on page 94](#)
- [Configuration on page 94](#)
- [Verification on page 95](#)

### Requirements

This example uses the following hardware and software components:

- One EX Series switch and one management PC

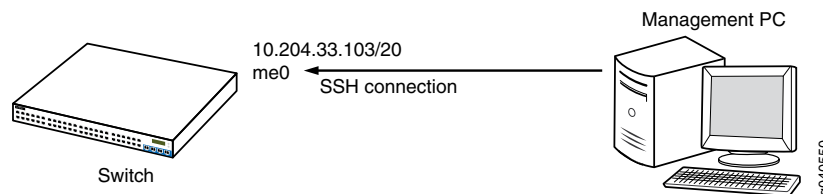
- Junos OS Release 10.4 or later for EX Series switches

## Overview and Topology

In this example, a management PC establishes an SSH connection with the management interface on a switch to remotely manage the switch. The IP address configured for the management interface is 10.204.33.103/20. A firewall filter is configured on the management interface to count the number of packets egressing from a source SSH port on the management interface. When the management PC establishes the SSH session with the management interface, the management interface returns SSH packets to the management PC to confirm that the session is established. These SSH packets are filtered based on the match condition specified in the firewall filter before they are forwarded to the management PC. As these packets are generated from the source SSH port on the management interface, they fulfill the match condition specified for the management interface. The number of matched SSH packets provides a count of the number of packets that have traversed the management interface. A system administrator can use this information to monitor the management traffic and take any action if required.

Figure 5 on page 94 shows the topology for this example in which a management PC establishes an SSH connection with the switch.

Figure 5: SSH Connection From a Management PC to an EX Series Switch



## Configuration

To configure a firewall filter on a management interface, perform these tasks:

### CLI Quick Configuration

To quickly create and configure a firewall filter on the management interface to filter SSH packets egressing from the management interface, copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family inet filter mgmt_fil1 term t1 from source-port ssh
set firewall family inet filter mgmt_fil1 term t1 then count c1
set firewall family inet filter mgmt_fil1 term t2 then accept
set interfaces me0 unit 0 family inet filter output mgmt_fil1
```

### Step-by-Step Procedure

To configure a firewall filter on the management interface to filter SSH packets:

1. Configure the firewall filter that matches SSH packets from the source port:

```
[edit]
user@switch# set firewall family inet filter (Firewall Filters) mgmt_fil1 term t1 from
source-port ssh
user@switch# set firewall family inet filter mgmt_fil1 term t1 then count c1
user@switch# set firewall family inet filter mgmt_fil1 term t2 then accept
```

These statements set a counter **c1** to count the number of SSH packets that egress from the source SSH interface on the management interface.

2. Set the firewall filter for the management interface:

```
[edit]
user@switch# set interfaces me0 unit 0 family inet filter output mgmt_fil1
```



**NOTE:** You can also set the firewall filter for a VME interface.

**Results** Check the results of the configuration:

```
[edit]
user@switch# show
interfaces {
  me0 {
    unit 0 {
      family inet {
        filter {
          output mgmt_fil1;
        }
        address 10.93.54.6/24;
      }
    }
  }
}

firewall {
  family inet {
    filter mgmt_fil1 {
      term t1 {
        from {
          source-port ssh;
        }
        then count c1;
      }
      term t2 {
        then accept;
      }
    }
  }
}
```

## Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying That the Firewall Filter Is Configured on a Management Interface on page 95](#)

### Verifying That the Firewall Filter Is Configured on a Management Interface

**Purpose** Verify that the firewall filter has been enabled on the management interface on the switch.

- Action** 1. Verify that the firewall filter is applied to the management interface:

```
[edit]
user@switch# show interfaces me0
unit 0 {
    family inet {
        filter {
            output mgmt_filt1;
        }
        address 10.204.33.103/20;
    }
}
```

2. Check the counter value that is associated with the firewall filter:

```
user@switch> show firewall
Filter: mgmt_filt1
Counters:
Name                               Bytes      Packets
c1                                 0           0
```

3. From the management PC, establish a secure shell session with the switch:

```
[user@management-pc ~]$ ssh user@10.204.33.103
```

4. Check counter values after SSH packets are generated from the switch in response to the secure shell session request by the management PC:

```
user@switch> show firewall
Filter: mgmt_filt1
Counters:
Name                               Bytes      Packets
c1                                 3533       23
```

**Meaning** The output indicates that the firewall filter has been applied to the management interface and the counter value indicates that 23 SSH packets were generated from the switch.

**Related Documentation**

- [Configuring Firewall Filters \(CLI Procedure\) on page 107](#)
- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)

---

## Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches

---

Administrators can configure filter-based forwarding on an EX Series switch by using a firewall filter to forward matched traffic to a specific virtual routing instance.

This example describes how to set up filter-based forwarding:

- [Requirements on page 97](#)
- [Overview and Topology on page 97](#)
- [Configuration on page 97](#)
- [Verification on page 99](#)



## Requirements

This example uses the following software and hardware components:

- One EX Series switch
- Junos OS Release 9.4 or later for EX Series switches

## Overview and Topology

In this example, traffic from one application server that is destined for a different application server is matched by a firewall filter based on the IP address. Any matching packets are routed to a particular virtual routing instance that first sends all traffic to a security device, then forwards it to the designated destination address.

## Configuration

To configure filter-based forwarding:

### CLI Quick Configuration

To quickly create and configure filter-based forwarding, copy the following commands and paste them into the switch terminal window:

```
[edit]
set interfaces ge-0/0/0 unit 0 family inet address 10.1.0.1/24
set interfaces ge-0/0/3 unit 0 family inet address 10.1.3.1/24
set firewall family inet filter fil term t1 from source-address 1.1.1.1/32
set firewall family inet filter fil term t1 from protocol tcp
set interfaces ge-0/0/0 unit 0 family inet filter input fil
set routing-instances vrf01 instance-type virtual-router
set routing-instances vrf01 interface ge-0/0/1.0
set routing-instances vrf01 interface ge-0/0/3.0
set routing-instances vrf01 routing-options static route 12.34.56.0/24 next-hop 10.1.3.254
set firewall family inet filter fil term t1 then routing-instance vrf01
```

### Step-by-Step Procedure

To configure filter-based forwarding:

1. Create interfaces to the application servers:

```
[edit]
user@switch# set interfaces ge-0/0/0 unit 0 family inet address 10.1.0.1/24
user@switch# set interfaces ge-0/0/3 unit 0 family inet address 10.1.3.1/24
```

2. Create a firewall filter that matches the correct source address:

```
[edit]
user@switch# set firewall family inet filter fil term t1 from source-address 1.1.1.1/32
user@switch# set firewall family inet filter fil term t1 from protocol tcp
```

3. Associate the filter with the source application server's interface:

```
[edit]
user@switch# set interfaces ge-0/0/0 unit 0 family inet filter input fil
```

4. Create a virtual router:

```
[edit]
user@switch# set routing-instances vrf01 instance-type virtual-router
```

5. Associate the interfaces with the virtual router:

```
[edit]
user@switch# set routing-instances vrf01 interface ge-0/0/1.0
user@switch# set routing-instances vrf01 interface ge-0/0/3.0
```

6. Configure the routing information for the virtual routing instance:

```
[edit]
user@switch# set routing-instances vrf01 routing-options static route 12.34.56.0/24
next-hop 10.1.3.254
```

7. Set the filter to forward packets to the virtual router you created:

```
[edit]
user@switch# set firewall family inet filter fil term t1 then routing-instance vrf01
```

---

## Results

Check the results of the configuration:

```
user@switch> show configuration
interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet {
        filter {
          input fil;
        }
        address 10.1.0.1/24;
      }
    }
  }
  ge-0/0/3 {
    unit 0 {
      family inet {
        address 10.1.3.1/24;
      }
    }
  }
}
firewall {
  family inet {
    filter fil {
      term t1 {
        from {
          source-address {
            1.1.1.1/32;
          }
          protocol tcp;
        }
        then {
          routing-instance vrf01;
        }
      }
    }
  }
}
routing-instances {
  vrf01 {
    instance-type virtual-router;
    interface ge-0/0/1.0;
    interface ge-0/0/3.0;
    routing-options {
```

```

static {
    route 12.34.56.0/24 next-hop 10.1.3.254;
}
}
}
}

```

## Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying That Filter-Based Forwarding Was Configured on page 99](#)

### Verifying That Filter-Based Forwarding Was Configured

**Purpose** Verify that filter-based forwarding was properly enabled on the switch.

**Action** 1. Use the **show interfaces filters** command:

```

user@switch> show interfaces filters ge-0/0/0.0
Interface      Admin Link Proto Input Filter      Output Filter
ge-0/0/0.0     up    down inet  fil

```

2. Use the **show route forwarding-table** command:

```

user@switch> show route forwarding-table

Routing table: default.inet
Internet:
Destination      Type RtRef Next hop      Type Index NhRef Netif
default          user  1 0:12:f2:21:cf:0 ucst  331  4 me0.0
default          perm  0                rjct  36   3
0.0.0.0/32       perm  0                dscd  34   1
10.1.0.0/24      ifdn  0                rslv  613  1 ge-0/0/0.0
10.1.0.0/32      iddn  0 10.1.0.0        recv  611  1 ge-0/0/0.0
10.1.0.1/32      user  0                rjct  36   3
10.1.0.1/32      intf  0 10.1.0.1        locl  612  2
10.1.0.1/32      iddn  0 10.1.0.1        locl  612  2
10.1.0.255/32    iddn  0 10.1.0.255      bcst  610  1 ge-0/0/0.0
10.1.1.0/26      ifdn  0                rslv  583  1 vlan.0
10.1.1.0/32      iddn  0 10.1.1.0        recv  581  1 vlan.0
10.1.1.1/32      user  0                rjct  36   3
10.1.1.1/32      intf  0 10.1.1.1        locl  582  2
10.1.1.1/32      iddn  0 10.1.1.1        locl  582  2
10.1.1.63/32     iddn  0 10.1.1.63       bcst  580  1 vlan.0
255.255.255.255/32 perm  0                bcst  32   1

```

```

Routing table: vrf01.inet
Internet:
Destination      Type RtRef Next hop      Type Index NhRef Netif
default          perm  0                rjct  559  2
0.0.0.0/32       perm  0                dscd  545  1
10.1.3.0/24      ifdn  0                rslv  617  1 ge-0/0/3.0
10.1.3.0/32      iddn  0 10.1.3.0        recv  615  1 ge-0/0/3.0
10.1.3.1/32      user  0                rjct  559  2
10.1.3.1/32      intf  0 10.1.3.1        locl  616  2
10.1.3.1/32      iddn  0 10.1.3.1        locl  616  2
10.1.3.255/32    iddn  0 10.1.3.255      bcst  614  1 ge-0/0/3.0
224.0.0.0/4      perm  0                mdsc  546  1
224.0.0.1/32     perm  0 224.0.0.1       mcst  529  1

```

```
255.255.255.255/32 perm 0 bcst 543 1

Routing table: default.iso
ISO:
Destination      Type RtRef Next hop      Type Index NhRef Netif
default          perm  0                rjct  60  1

Routing table: vrf01.iso
ISO:
Destination      Type RtRef Next hop      Type Index NhRef Netif
default          perm  0                rjct 600  1
```

**Meaning** The output indicates that the filter was created on the interface and that the virtual routing instance is forwarding matching traffic to the correct IP address.

- Related Documentation**
- [Configuring Firewall Filters \(CLI Procedure\) on page 107](#)
  - [Configuring Static Routing \(CLI Procedure\)](#)
  - [Configuring Static Routing \(J-Web Procedure\)](#)
  - [Understanding Filter-Based Forwarding for EX Series Switches on page 70](#)

---

## Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication

---

On EX Series switches, firewall filters that you apply to interfaces enabled for 802.1X or MAC RADIUS authentication are dynamically combined with the per-user policies sent to the switch from the RADIUS server. The switch uses internal logic to dynamically combine the interface firewall filter with the user policies from the RADIUS server and create an individualized policy for each of the multiple users or nonresponsive hosts that are authenticated on the interface.

This example describes how dynamic firewall filters are created for multiple supplicants on an 802.1X-enabled interface (the same principles shown in this example apply to interfaces enabled for MAC RADIUS authentication):

- [Requirements on page 100](#)
- [Overview and Topology on page 101](#)
- [Configuration on page 103](#)
- [Verification on page 105](#)

### Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.5 or later for EX Series switches
- One EX Series switch

- One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you apply firewall filters to an interface for use with multiple supplicants, be sure you have:

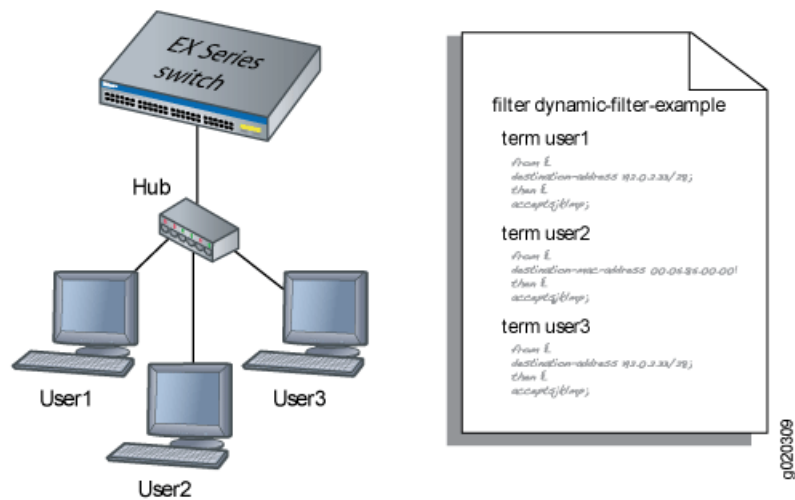
- Set up a connection between the switch and the RADIUS server. See Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch.
- Configured 802.1X authentication on the switch, with the authentication mode for interface **ge-0/0/2** set to **multiple**. See Configuring 802.1X Interface Settings (CLI Procedure) and Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX Series Switch.
- Configured users on the RADIUS authentication server.

## Overview and Topology

When the 802.1X configuration on an interface is set to multiple supplicant mode, the system dynamically combines interface firewall filter with the user policies sent to the switch from the RADIUS server during authentication and creates separate terms for each user. Because there are separate terms for each user authenticated on the interface, you can, as shown in this example, use counters to view the activities of individual users that are authenticated on the same interface.

When a new user (or a nonresponsive host) is authenticated on an interface, the system adds a term to the firewall filter associated with the interface, and the term (policy) for each user is associated with the MAC address of the user. The term for each user is based on the user-specific filters set on the RADIUS server and the filters configured on the interface. For example, as shown in [Figure 6 on page 102](#), when User1 is authenticated by the EX Series switch, the system creates the firewall filter **dynamic-filter-example**. When User2 is authenticated, another term is added to the firewall filter, and so on.

Figure 6: Conceptual Model: Dynamic Filter Updated for Each New User



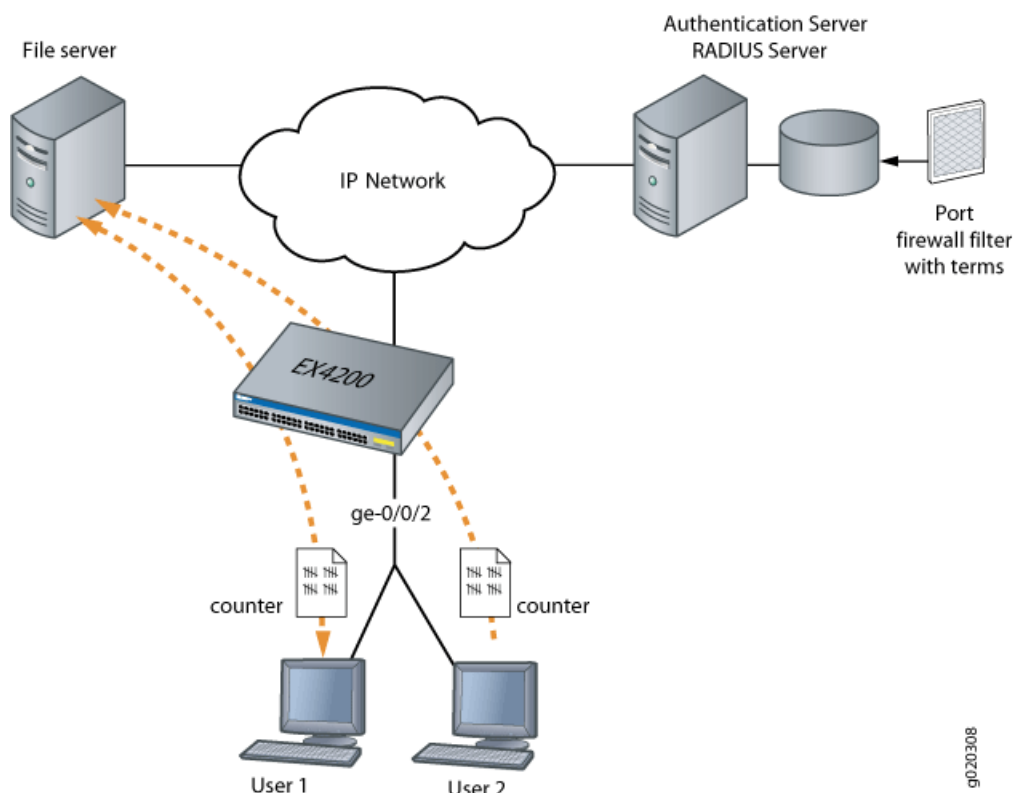
This is a conceptual model of the internal process—you cannot access or view the dynamic filter.



**NOTE:** If the firewall filter on the interface is modified after the user (or nonresponsive host) is authenticated, the modifications are not reflected in the dynamic filter unless the user is reauthenticated.

In this example, you configure a firewall filter to count the requests made by each endpoint authenticated on interface **ge-0/0/2** to the file server, which is located on subnet **192.0.2.16/28**, and set policer definitions to rate limit the traffic. [Figure 7 on page 103](#) shows the network topology for this example.

Figure 7: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server



## Configuration

To configure firewall filters for multiple supplicants on 802.1X-enabled interfaces:

- [Configuring Firewall Filters on Interfaces with Multiple Supplicants on page 103](#)

### Configuring Firewall Filters on Interfaces with Multiple Supplicants

#### CLI Quick Configuration

To quickly configure firewall filters for multiple supplicants on an 802.1X-enabled interface copy the following commands and paste them into the switch terminal window:

```
[edit]
set protocols dot1x authenticator interface ge-0/0/2 supplicant multiple
set firewall family ethernet-switching filter filter1 term term1 from destination-address 192.0.2.16/28
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1k
set firewall family ethernet-switching filter filter1 term term1 then count counter1
set firewall family ethernet-switching filter filter1 term term2 then policer p1
```

#### Step-by-Step Procedure

To configure firewall filters on an interface enabled for multiple supplicants:

1. Configure interface **ge-0/0/2** for multiple supplicant mode authentication:
 

```
[edit protocols dot1x]
user@switch# set authenticator interface ge-0/0/2 supplicant multiple
```
2. Set policer definition:

```
user@switch# show policer p1 |display set
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1k
set firewall policer p1 then discard
```

3. Configure a firewall filter to count packets from each user and a policer that limits the traffic rate. As each new user is authenticated on the multiple supplicant interface, this filter term will be included in the dynamically created term for the user:

```
[edit firewall family ethernet-switching]
user@switch# set filter filter1 term term1 from destination-address 192.0.2.16/28
user@switch# set filter filter1 term term1 then count counter1
user@switch# set filter filter1 term term2 then policer p1
```

**Results** Check the results of the configuration:

```
user@switch> show configuration
```

```
firewall {
  family ethernet-switching {
    filter filter1 {
      term term1 {
        from {
          destination-address {
            192.0.2.16/28;
          }
        }
        then count counter1;
      }
      term term2 {
        from {
          destination-address {
            192.0.2.16/28;
          }
        }
        then policer p1;
      }
    }
  }
}
policer p1 {
  if-exceeding {
    bandwidth-limit 1m;
    burst-size-limit 1k;
  }
  then discard;
}
protocols {
  dot1x {
    authenticator
    interface ge-0/0/2 {
      supplicant multiple;
    }
  }
}
```



## Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying Firewall Filters on Interfaces with Multiple Supplicants on page 105](#)

### Verifying Firewall Filters on Interfaces with Multiple Supplicants

<b>Purpose</b>	Verify that firewall filters are functioning on the interface with multiple supplicants.
<b>Action</b>	<ol style="list-style-type: none"> <li>1. Check the results with one user authenticated on the interface. In this case, the user is authenticated on <b>ge-0/0/2</b>:           <pre>user@switch&gt; show dot1x firewall Filter: dot1x_ge-0/0/2 Counters counter1_dot1x_ge-0/0/2_user1 100</pre> </li> <li>2. When a second user, User2, is authenticated on the same interface, <b>ge-0/0/2</b>, you can verify that the filter includes the results for both of the users authenticated on the interface:           <pre>user@switch&gt; show dot1x firewall Filter: dot1x-filter-ge-0/0/0 Counters counter1_dot1x_ge-0/0/2_user1 100 counter1_dot1x_ge-0/0/2_user2 400</pre> </li> </ol>
<b>Meaning</b>	The results displayed by the <b>show dot1x firewall</b> command output reflect the dynamic filter created with the authentication of each new user. User1 accessed the file server located at the specified destination address 100 times, while User2 accessed the same file server 400 times.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on an EX Series Switch</a></li> <li>• <a href="#">Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75</a></li> <li>• <a href="#">Filtering 802.1X Supplicants Using RADIUS Server Attributes</a></li> </ul>



## CHAPTER 4

# Configuration Tasks

- [Configuring Firewall Filters \(CLI Procedure\) on page 107](#)
- [Configuring Firewall Filters \(J-Web Procedure\) on page 115](#)
- [Configuring Policers to Control Traffic Rates \(CLI Procedure\) on page 119](#)
- [Assigning Multifield Classifiers in Firewall Filters to Specify Packet-Forwarding Behavior \(CLI Procedure\) on page 122](#)
- [Configuring Routing Policies \(J-Web Procedure\) on page 123](#)
- [Configuring Tricolor Marking Policers on page 128](#)

### Configuring Firewall Filters (CLI Procedure)

---

You configure firewall filters on EX Series switches to control traffic that enters ports on the switch or enters and exits VLANs on the network and Layer 3 (routed) interfaces. To configure a firewall filter you must configure the filter and then apply it to a port, VLAN, or Layer 3 interface.

This topic describes:

- [Configuring a Firewall Filter on page 107](#)
- [Configuring a Term Specifically for IPv4 or IPv6 Traffic on page 110](#)
- [Applying a Firewall Filter to a Port on a Switch on page 111](#)
- [Applying a Firewall Filter to a Management Interface on a Switch on page 112](#)
- [Applying a Firewall Filter to a VLAN on a Network on page 113](#)
- [Applying a Firewall Filter to a Layer 3 \(Routed\) Interface on page 114](#)

### Configuring a Firewall Filter

Before you can apply a firewall filter to a port, VLAN, or Layer 3 interface, you must configure a firewall filter with the required details, such as type of family for the firewall filter, firewall filter name, and match conditions. A match condition in the firewall filter configuration can contain multiple terms that define the criteria for the match condition. For each term, you must specify an action to be performed if a packet matches the conditions in the term. For information on different match conditions and actions, see [“Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches” on page 16](#).

To configure a firewall filter:

1. Configure the family address type for the firewall filter:

- For a firewall filter that is applied to a port or VLAN, specify the family address type **ethernet-switching** to filter Layer 2 (Ethernet) packets and Layer 3 (IP) packets, for example:

```
[edit firewall]
user@switch# set family ethernet-switching
```

- For a firewall filter that is applied to a Layer 3 (routed) interface:

- To filter IPv4 packets, specify the family address type **inet**, for example:

```
[edit firewall]
user@switch# set family inet
```

- To filter IPv6 packets, specify the family address type **inet6**, for example:

```
[edit firewall]
user@switch# set family inet6
```



**NOTE:** You can configure firewall filters for both IPv4 and IPv6 traffic on the same Layer 3 interface.

---

2. Specify the filter name:

```
[edit firewall family ethernet-switching]
user@switch# set filter ingress-port-filter
```

The filter name can contain letters, numbers, and hyphens (-) and can have a maximum of 64 characters. Each filter name must be unique.

3. If you want to apply a firewall filter to multiple interfaces and name individual firewall counters specific to each interface, configure the **interface-specific** option:

```
[edit firewall family ethernet-switching filter ingress-port-filter]
user@switch# set interface-specific
```

4. Specify a term name:

```
[edit firewall family ethernet-switching filter ingress-port-filter]
user@switch# set term term-one
```

The term name can contain letters, numbers, and hyphens (-) and can have a maximum of 64 characters.

A firewall filter can contain one or more terms. Each term name must be unique within a filter.

**NOTE:**

The maximum number of terms allowed per firewall filter for EX Series switches is:

- 512 for EX2200 switches
- 1,436 for EX3300 switches



**NOTE:** On EX3300 switches, if you add and delete filters with a large number of terms (on the order of 1000 or more) in the same commit operation, not all the filters are installed. You must add filters in one commit operation, and delete filters in a separate commit operation.

- 7,168 for EX3200 and EX4200 switches
- 1,200 for EX4500 and EX4550 switches
- 1,400 for EX6200 switches
- 32,768 for EX8200 switches

If you attempt to configure a firewall filter that exceeds these limits, the switch returns an error message when you commit the configuration.

5. In each firewall filter term, specify the match conditions to use to match components of a packet.

To specify match conditions to match on packets that contain a specific source address and source port—for example:

```
[edit firewall family ethernet-switching filter ingress-port-filter term
term-one]
user@switch# set from source-address 192.0.2.14
user@switch# set from source-port 80
```

You can specify one or more match conditions in a single **from** statement. For a match to occur, the packet must match all the conditions in the term.

The **from** statement is optional, but if included in a term, the **from** statement cannot be empty. If you omit the **from** statement, all packets are considered to match.

6. In each firewall filter term, specify the action to take if the packet matches all the conditions in that term.

You can specify an action and/or action modifiers:

- To specify a filter action, for example, to discard packets that match the conditions of the filter term:

```
[edit firewall family ethernet-switching filter ingress-port-filter term
term-one]
user@switch# set then discard
```

You can specify no more than one action per filter term.

- To specify an action modifier, for example, to count and classify packets in a forwarding class:

```
[edit firewall family ethernet-switching filter ingress-port-filter term  
term-one]  
user@switch# set then count counter-one  
user@switch# set then forwarding-class expedited-forwarding
```

In a **then** statement, you can specify the following action modifiers:

- **analyzer *analyzer-name***—Mirror port traffic to a specified destination port or VLAN that is connected to a protocol analyzer application. An **analyzer** must be configured under the **ethernet-switching** family address type. See Configuring Port Mirroring to Analyze Traffic (CLI Procedure).
- **count *counter-name***—Count the number of packets that pass this filter term.



**NOTE:** We recommend that you configure a counter for each term in a firewall filter, so that you can monitor the number of packets that match the conditions specified in each filter term.

- **forwarding-class *class***—Classify packets in a forwarding class.
- **loss-priority *priority***—Set the priority for dropping a packet.
- **policer *policer-name***—Apply rate limiting to the traffic.
- **interface *interface-name***—Forward the traffic to the specified interface, bypassing the switching lookup.
- **log**—Log the packet's header information in the Routing Engine.

If you omit the **then** statement or do not specify an action, packets that match all the conditions in the **from** statement are accepted. However, you must always explicitly configure an action and/or action modifier in the **then** statement. You can include no more than one action, but you can use any combination of action modifiers. For an action or action modifier to take effect, all conditions in the **from** statement must match.



**NOTE:** Implicit discard is also applicable to a firewall filter applied to the loopback interface, lo0.

On Juniper Networks EX8200 Ethernet Switches, if an implicit or explicit discard action is configured on a loopback interface for IPv4 traffic, next hop resolve packets are accepted and allowed to pass through the switch. However, for IPv6 traffic, you must explicitly configure a rule to allow the next hop IPv6 resolve packets to pass through the switch.

---

## Configuring a Term Specifically for IPv4 or IPv6 Traffic

To configure a term in a firewall filter configuration specifically for IPv4 traffic:

1. Verify that neither **ether-type ipv6** nor **ip-version ipv6** is specified in the term in the configuration. By default, a configuration that does not contain either **ether-type ipv6** or **ip-version ipv6** in a term applies to IPv4 traffic.
2. (Optional) Perform one of these tasks:
  - Define **ether-type ipv4** in a term in the configuration.
  - Define **ip-version ipv4** in a term in the configuration.
  - Define both **ether-type ipv4** and **ip-version ipv4** in a term in the configuration.
  - Verify that neither **ether-type ipv6** nor **ip-version ipv6** is specified in a term in the configuration—by default, a configuration that does not contain either **ether-type ipv6** or **ip-version ipv6** in a term applies to IPv4 traffic if it does not contain **ether-type ipv6** or **ip-version ipv6**.
3. Ensure that other match conditions in the term are valid for IPv4 traffic.

To configure a term in a firewall filter configuration specifically for IPv6 traffic:

1. Perform one of these tasks:
  - Define **ether-type ipv6** in a term in the configuration.
  - Define **ip-version ipv6** in a term in the configuration.
  - Define both **ether-type ipv6** and **ip-version ipv4** in a term in the configuration.



**NOTE:** By default, a configuration that does not contain either **ether-type ipv6** or **ip-version ipv6** in a term applies to IPv4 traffic.

2. Ensure that other match conditions in the term are valid for IPv6 traffic.



**NOTE:** If the term contains either of the match conditions **ether-type ipv6** or **ip-version ipv6**, with no other IPv6 match condition specified, all IPv6 traffic is matched.



**NOTE:** To configure a firewall filter for both IPv4 and IPv6 traffic, you must include two separate terms, one for IPv4 traffic and the other for IPv6 traffic.

## Applying a Firewall Filter to a Port on a Switch

You can apply a firewall filter to a port on a switch to filter ingress or egress traffic on the switch. When you configure the firewall filter, you can specify any match condition, action, and action modifiers specified in [“Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches” on page 16](#). The action specified in the match condition indicates the action for the matched packets in the ingress or egress traffic.

To apply a firewall filter to a port to filter ingress or egress traffic:



**NOTE:** For applying a firewall filter to a management interface, see [“Applying a Firewall Filter to a Management Interface on a Switch” on page 112](#)

1. Specify the interface name and provide a meaningful description of the firewall filter and the interface to which the filter is applied:

```
[edit interfaces]
user@switch# set ge-0/0/1 description "filter to limit tcp traffic filter at trunk port for
employee-vlan and voice-vlan applied on the interface"
```



**NOTE:** Providing the description is optional.

2. Specify the unit number and family address type for the interface:

```
[edit interfaces]
user@switch# set ge-0/0/1 unit 0 family ethernet-switching
```

For firewall filters that are applied to ports, the family address type must be **ethernet-switching**.

3. To apply a firewall filter to filter packets that are entering a port:

```
[edit interfaces]
user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter input ingress-port-filter
```

To apply a firewall filter to filter packets that are exiting a port:

```
[edit interfaces]
user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter output egress-port-filter
```



**NOTE:** You can apply no more than one firewall filter per port, per direction.

## Applying a Firewall Filter to a Management Interface on a Switch

You can configure and apply a firewall filter to a management interface to control traffic that is entering or exiting the interface on a switch. You can use utilities such as SSH or Telnet to connect to the management interface over the network and then use management protocols such as SNMP to gather statistical data from the switch. Similar to configuring a firewall filter on other types of interfaces, you can configure a firewall filter on a management interface using any match condition, action, and action modifier specified in [“Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches” on page 16](#) except for the following action modifiers:

- **loss-priority**
- **forwarding-class**

You can apply a firewall filter to the management Ethernet interface on any EX Series switch. You can also apply a firewall filter to the virtual management Ethernet (VME) interface on the EX4200 switch. For more information on the management Ethernet interface and the VME interface, see [EX Series Switches Interfaces Overview](#).



To apply a firewall filter on the management interface to filter ingress or egress traffic:

1. Specify the interface name and provide a meaningful description of the firewall filter and the interface to which the filter is applied:

```
[edit interfaces]
user@switch# set me0 description "filter to limit tcp traffic filter at management interface"
```



**NOTE:** Providing the description is optional.

2. Specify the unit number and family address type for the management interface:

```
[edit interfaces]
user@switch# set me0 unit 0 family inet
```



**NOTE:** For firewall filters that are applied to management interfaces, the family address type can be either `inet` or `inet6`.

3. To apply a firewall filter to filter packets that are entering a management interface:

```
[edit interfaces]
user@switch# set me0 unit 0 family inet filter input ingress-port-filter
```

To apply a firewall filter to filter packets that are exiting a management interface:

```
[edit interfaces]
user@switch# set me0 unit 0 family inet filter output egress-port-filter
```



**NOTE:** You can apply no more than one firewall filter per management interface, per direction.

## Applying a Firewall Filter to a VLAN on a Network

You can apply a firewall filter to a VLAN on a network to filter ingress or egress traffic on the network. To apply a firewall filter to a VLAN, specify the VLAN name and ID, and then apply the firewall filter to the VLAN. When you configure the firewall filter, you can specify any match condition, action, and action modifiers specified in [“Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches” on page 16](#). The action specified in the match condition indicates the action for the matched packets in the ingress or egress traffic.

To apply a firewall filter to a VLAN:

1. Specify the VLAN name and VLAN ID and provide a meaningful description of the firewall filter and the VLAN to which the filter is applied:

```
[edit vlans]
user@switch# set employee-vlan vlan-id (802.1Q Tagging) 20 vlan-description "filter to rate limit traffic applied on employee-vlan"
```



**NOTE:** Providing the description is optional.

2. Apply firewall filters to filter packets that are entering or exiting the VLAN:

- To apply a firewall filter to filter packets that are entering the VLAN:

```
[edit vlans]
user@switch# set employee-vlan vlan-id 20 filter input ingress-vlan-filter
```

- To apply a firewall filter to filter packets that are exiting the VLAN:

```
[edit vlans]
user@switch# set employee-vlan vlan-id 20 filter output egress-vlan-filter
```



**NOTE:** You can apply no more than one firewall filter per VLAN, per direction.

## Applying a Firewall Filter to a Layer 3 (Routed) Interface

You can apply a firewall filter to a Layer 3 (routed) interface to filter ingress or egress traffic on the switch. When you configure the firewall filter, you can specify any match condition, action, and action modifiers specified in [“Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches”](#) on page 16. The action specified in the match condition indicates the action for the matched packets in the ingress or egress traffic.

To apply a firewall filter to a Layer 3 interface on a switch:

1. Specify the interface name and provide a meaningful description of the firewall filter and the interface to which the filter is applied:

```
[edit interfaces]
user@switch# set ge-0/1/0 description "filter to count and monitor employee-vlan traffic
applied on layer 3 interface"
```



**NOTE:** Providing the description is optional.

2. Specify the unit number, family address type, and address for the interface:

```
[edit interfaces]
user@switch# set ge-0/1/0 unit 0 family inet address 10.10.10.1/24
```

For firewall filters applied to Layer 3 interfaces, the family address type must be **inet** (for IPv4 traffic) or **inet6** (for IPv6 traffic).

3. You can apply firewall filters to filter packets that are entering or exiting a Layer 3 (routed) interface:

- To apply a firewall filter to filter packets that are entering a Layer 3 interface:

```
[edit interfaces]
user@switch# set ge-0/1/0 unit 0 family inet address 10.10.10.1/24 filter input
ingress-router-filter
```

- To apply a firewall filter to filter packets that are exiting a Layer 3 interface:

```
[edit interfaces]
user@switch# set ge-0/1/0 unit 0 family inet address 10.10.10.1/24 filter output
egress-router-filter
```



**NOTE:** You can apply no more than one firewall filter per Layer 3 interface, per direction.

#### Related Documentation

- [Configuring Firewall Filters \(J-Web Procedure\) on page 115](#)
- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)
- [Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches on page 96](#)
- [Example: Configuring a Firewall Filter on a Management Interface on an EX Series Switch on page 93](#)
- [Verifying That Firewall Filters Are Operational on page 173](#)
- [Monitoring Firewall Filter Traffic on page 174](#)
- [Configuring Policers to Control Traffic Rates \(CLI Procedure\) on page 119](#)

## Configuring Firewall Filters (J-Web Procedure)

You configure firewall filters on EX Series switches to control traffic that enters ports on the switch or enters and exits VLANs on the network and Layer 3 (routed) interfaces. To configure a firewall filter you must configure the filter and then apply it to a port, VLAN, or Layer 3 interface.

To configure firewall filter settings using the J-Web interface:

1. Select **Configure > Security > Filters**.

The Firewall Filter Configuration page displays a list of all configured port/VLAN or router filters and the ports or VLANs associated with a particular filter.



**NOTE:** After you make changes to the configuration in this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options > Commit**. See [Using the Commit Options to Commit Configuration Changes](#) for details about all commit options.

2. Click one:

- **Add**—Select this option to create a new filter. Enter information as specified in [Table 24 on page 116](#).
- **Edit**—Select this option to edit an existing filter. Enter information as specified in [Table 24 on page 116](#).
- **Delete**—Select this option to delete a filter.
- **Term Up**—Select this option to move a term up in the filter term list.
- **Term Down**—Select this option to move a term down in the filter term list.

**Table 24: Create a New Filter**

Field	Function	Your Action
Filter tab		
Filter type	Specifies the filter type: port/VLAN firewall filter or router firewall filter.	Select the filter type.
Filter name	Specifies the name for the filter.	Enter a name.
Select terms to be part of the filter	Specifies the terms to be associated with the filter. Add new terms or edit existing terms.	Click <b>Add</b> to add new terms. Enter information as specified in <a href="#">Table 25 on page 116</a> and <a href="#">Table 26 on page 117</a> .
Association tab		
Port Associations	Specifies the ports with which the filter is associated.  <b>NOTE:</b> For a port/VLAN filter type, only Ingress direction is supported for port association.	<ol style="list-style-type: none"> <li>1. Click <b>Add</b>.</li> <li>2. Select the direction: Ingress or Egress.</li> <li>3. Select the ports. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the available ports from the list.</li> <li>4. Click <b>OK</b>.</li> </ol>
VLAN Associations	Specifies the VLANs with which the filter is associated.  <b>NOTE:</b> Because router firewall filters can be associated with ports only, this section is not displayed for a router firewall filter.	<ol style="list-style-type: none"> <li>1. Click <b>Add</b>.</li> <li>2. Select the direction: Ingress or Egress.</li> <li>3. Select the VLANs.</li> <li>4. Click <b>OK</b>.</li> </ol>

**Table 25: Create a New Term**

Field	Function	Your Action
Term Name	Specifies the name of the term.	Enter a name.
Protocols	Specifies the protocols to be associated with the term.	<ol style="list-style-type: none"> <li>1. Click <b>Add</b>.</li> <li>2. Select the protocols.</li> <li>3. Click <b>OK</b>.</li> </ol>

Table 25: Create a New Term (*continued*)

Field	Function	Your Action
Source	Specifies the source IP address, MAC address, and available ports.  <b>NOTE:</b> MAC address is specified only for port/VLAN filters.	To specify the IP address, click <b>Add &gt; IP</b> and enter the IP address.  To specify the MAC address, click <b>Add &gt; MAC</b> and enter the MAC address.  To specify the ports (interfaces), click <b>Add &gt; Ports</b> and enter the port number.  To delete the IP address, MAC address, or port details, select it and click <b>Remove</b> .
Destination	Specifies the destination IP address, MAC address, and available ports.  <b>NOTE:</b> MAC address is specified only for port/VLAN filters.	To specify the IP address, click <b>Add &gt; IP</b> and enter the IP address.  To specify the MAC address, click <b>Add &gt; MAC</b> and enter the MAC address.  To specify the ports (interfaces), click <b>Add &gt; Ports</b> and enter the port number.  To delete the IP address, MAC address, or port details, select it and click <b>Remove</b> .
Action	Specifies the packet action for the term.	Select one: <ul style="list-style-type: none"> <li>• Accept</li> <li>• Discard</li> </ul>
More	Specifies advanced configuration options for the filter.	Select the match conditions as specified in <a href="#">Table 26 on page 117</a> .  Select the packet action for the term as specified in <a href="#">Table 26 on page 117</a> .

Table 26: Advanced Options for Terms

Table	Function	Your Action
ICMP Type	Specifies the ICMP packet type field. Typically, you specify this match condition in conjunction with the protocol match condition to determine which protocol is being used on the port.	Select the option from the list.
ICMP Code	Specifies more specific information than ICMP type. Because the value's meaning depends upon the associated ICMP type, you must specify <b>icmp-type</b> along with <b>icmp-code</b> . The keywords are grouped by the ICMP type with which they are associated.	Select a value from the list.
DSCP	Specifies the Differentiated Services code point (DSCP). The DiffServ protocol uses the type-of-service (ToS) byte in the IP header. The most significant six bits of this byte form the DSCP.	Select the DSCP number from the list.

Table 26: Advanced Options for Terms (*continued*)

Table	Function	Your Action
Precedence	Specifies IP precedence.  <b>NOTE:</b> IP precedence and DSCP number cannot be specified together for the same term.	Select the option from the list.
IP Options	Specifies the presence of the options field in the IP header.	Select the option from the list.
Interface	Specifies the interface on which the packet is received.	Select the interface from the list.
Ether type	Specifies the Ethernet type field of a packet.  <b>NOTE:</b> This option is not applicable for a routing filter.	Select a value from the list.
Dot1q user priority	Specifies the user-priority field of the tagged Ethernet packet. User-priority values can be 0–7.  In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed) <ul style="list-style-type: none"> <li>background (1)—Background</li> <li>best-effort (0)—Best effort</li> <li>controlled-load (4)—Controlled load</li> <li>excellent-load (3)—Excellent load</li> <li>network-control (7)—Network control reserved traffic</li> <li>standard (2)—Standard or Spare</li> <li>video (5)—Video</li> <li>voice (6)—Voice</li> </ul> <b>NOTE:</b> This option is not applicable for a routing filter.	Select a value from the list.
VLAN	Specifies the VLAN to be associated with the packet.  <b>NOTE:</b> This option is not applicable for a routing filter.	Select the VLAN from the list.
TCP Flags	Specifies one or more TCP flags.  <b>NOTE:</b> TCP flags are supported on ingress ports, VLANs, and router interfaces.	Select the option <b>TCP Initial</b> or enter a combination of TCP flags.
Fragmentation Flags	Specifies the IP fragmentation flags.  <b>NOTE:</b> Fragmentation flags are supported on ingress ports, VLANs, and router interfaces.	Select either the option <b>is-fragment</b> or enter a combination of fragment action flags.
Dot1q tag	Specifies the value for tag field in the Ethernet header. Values can be from 1 through 4095.  <b>NOTE:</b> This option is not applicable for a routing filter.	Enter the value.
Action		

Table 26: Advanced Options for Terms (*continued*)

Table	Function	Your Action
Counter name	Specifies the count of the number of packets that pass this filter, term, or policer.	Enter a value.
Forwarding class	Classifies the packet into one of the following forwarding classes: <ul style="list-style-type: none"> <li>assured-forwarding</li> <li>best-effort</li> <li>expedited-forwarding</li> <li>network-control</li> <li>user-defined</li> </ul>	Select the option from the list.
Loss priority	Specifies the packet loss priority.  <b>NOTE:</b> Forwarding class and loss priority should be specified together for the same term.	Enter the value.
Analyzer	Specifies whether to perform port-mirroring on packets. Port-mirroring copies all packets entering one switch port to a network monitoring connection on another switch port.	Select the analyzer (port mirroring configuration) from the list.

- Related Documentation**
- [Configuring Firewall Filters \(CLI Procedure\) on page 107](#)
  - [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)
  - [Verifying That Firewall Filters Are Operational on page 173](#)
  - [Firewall Filters for EX Series Switches Overview on page 7](#)
  - [Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 16](#)

## Configuring Policers to Control Traffic Rates (CLI Procedure)

You can configure policers to rate limit traffic on EX Series switches. After you configure a policer, you can include it in an ingress firewall filter configuration.

When you configure a firewall filter, you can specify a policer action for any term or terms within the filter. All traffic that matches a term that contains a policer action goes through the policer that the term references. Each policer that you configure includes an implicit counter. To get term-specific packet counts, you must configure a separate policer for each filter term that requires policing.



**NOTE:** On all EX Series switches except EX8200 switches, each policer that you configure includes an implicit counter. To ensure term-specific packet counts, configure a policer for each term in the filter that requires policing. For EX8200 switches, configure a policer and associate it with a global management counter using the **counter** option.

The following policer limits apply on a switch:

- A maximum of 512 policers can be configured for port firewall filters.
- A maximum of 512 policers can be configured for VLAN and Layer 3 firewall filters.

If the number of policers in the firewall filter configuration exceeds these limits, the switch returns the following message when you commit the configuration:

Cannot assign policers: Max policer limit reached

This topic includes these tasks:

1. [Configuring Policers on page 120](#)
2. [Specifying Policers in a Firewall Filter Configuration on page 121](#)
3. [Applying a Firewall Filter That Is Configured with a Policar on page 121](#)

## Configuring Policers

To configure a policer:

1. Specify the name of the policer:

```
[edit firewall]
user@switch# set policer policer-one
```

The policer name can include letters, numbers, and hyphens (-) and can contain up to 64 characters.

2. Specify the **filter-specific** statement to configure a policer to act as a filter-specific policer; else proceed to step 3:

```
[edit firewall]
user@switch# set policer policer-one filter-specific
```

If you do not specify the **filter-specific** statement, the policer acts as a term-specific policer by default.

3. Configure rate limiting for the policer:

- a. Specify the bandwidth limit in bits per second (bps) to control the traffic rate on an interface:

```
[edit firewall policer policer-one]
user@switch# set if-exceeding bandwidth-limit 300k
```

The range for the bandwidth limit is 1k through 102.3g bps.

- b. Specify the burst-size limit (the maximum allowed burst size in bytes) to control the amount of traffic bursting:

```
[edit firewall policer policer-one]
```



```
user@switch# set if-exceeding burst-size-limit 500k
```

To determine the value for the burst-size limit, multiply the bandwidth of the interface on which the filter is applied by the amount of time to allow a burst of traffic at that bandwidth to occur:

burst size = (bandwidth) \* (allowable time for burst traffic)

The range for the burst-size limit is 1 through 2,147,450,880 bytes.

- Specify the policer action **discard** to discard packets that exceed the rate limits:

```
[edit firewall policer]
user@switch# set policer-one then (Policer Action) discard
```

Discard is the only supported policer action.

- On EX8200 switches, you must assign a global management counter to the policer to obtain policer statistics:

```
[edit firewall policer]
user@switch# set policer-one counter counter-id 0
```

In this sample statement, the global management counter ID is 0. You can assign any number of policers to the global management counter. The policer statistics displayed for each counter are the collective statistics of all policers assigned to that counter.

## Specifying Policers in a Firewall Filter Configuration

To reference a policer for a single firewall, configure a filter term that includes the policer action:

```
[edit firewall family ethernet-switching]
user@switch# set filter limit-hosts term term-one from source-address 192.0.2.16/28
users@witch# set filter limit-hosts term term-one then policer policer-one
```

## Applying a Firewall Filter That Is Configured with a Policer

A firewall filter that is configured with one or more policer actions, like any other firewall filter, must be applied to a port, VLAN, or Layer 3 interface. For information about applying firewall filters, see the sections on applying firewall filters in “[Configuring Firewall Filters \(CLI Procedure\)](#)” on page 107.

### Related Documentation

- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)
- [Configuring Firewall Filters \(CLI Procedure\) on page 107](#)
- [Configuring Firewall Filters \(J-Web Procedure\) on page 115](#)
- [Verifying That Policers Are Operational on page 174](#)
- [Understanding the Use of Policers in Firewall Filters on page 66](#)

## Assigning Multifield Classifiers in Firewall Filters to Specify Packet-Forwarding Behavior (CLI Procedure)

You can configure firewall filters with multifield classifiers to classify packets transiting a port, VLAN, or Layer 3 interface on an EX Series switch.

You specify multifield classifiers in a firewall filter configuration to set the forwarding class and packet loss priority (PLP) for incoming or outgoing packets. By default, the data traffic that is not classified is assigned to the **best-effort** class associated with queue 0.

You can specify any of the following default forwarding classes:

Forwarding class	Queue
best-effort	0
assured-forwarding	1
expedited-forwarding	5
network-control	7

To assign multifield classifiers in firewall filters:

1. Configure the family name and filter name for the filter at the **[edit firewall]** hierarchy level, for example:

```
[edit firewall]
user@switch# set family ethernet-switching
user@switch# set family ethernet-switching filter ingress-filter
```

2. Configure the terms of the filter, including the **forwarding-class** and **loss-priority** action modifiers as appropriate. When you specify a forwarding class you must also specify the packet loss priority. For example, each of the following terms examines different packet header fields and assigns an appropriate classifier and the packet loss priority:

- The term **voice-traffic** matches packets on the **voice-vlan** and assigns the forwarding class **expedited-forwarding** and packet loss priority **low**:

```
[edit firewall family ethernet-switching filter ingress-filter]
user@switch# set term voice-traffic from vlan-id voice-vlan
user@switch# set term voice-traffic then forwarding-class expedited-forwarding
user@switch# set term voice-traffic then loss-priority low
```

- The term **data-traffic** matches packets on **employee-vlan** and assigns the forwarding class **assured-forwarding** and packet loss priority **low**:

```
[edit firewall family ethernet-switching filter ingress-filter]
user@switch# set term data-traffic from vlan-id employee-vlan
user@switch# set term data-traffic then forwarding-class assured-forwarding
user@switch# set term data-traffic then loss-priority low
```

- Because loss of network-generated packets can jeopardize proper network operation, delay is preferable to discard of packets. The following term,

**network-traffic**, assigns the forwarding class **network-control** and packet loss priority **low**:

```
[edit firewall family ethernet-switching filter ingress-filter]
user@switch# set term network-traffic from precedence net-control
user@switch# set term network-traffic then forwarding-class network
user@switch# set term network-traffic then loss-priority low
```

- The last term **accept-traffic** matches any packets that did not match on any of the preceding terms and assigns the forwarding class **best-effort** and packet loss priority **low**:

```
[edit firewall family ethernet-switching filter ingress-filter]
user@switch# set term accept-traffic from precedence net-control
user@switch# set term accept-traffic then forwarding-class best-effort
user@switch# set term accept-traffic then loss-priority low
```

3. Apply the filter **ingress-filter** to a port, VLAN or Layer 3 interface. For information about applying the filter, see [“Configuring Firewall Filters \(CLI Procedure\)” on page 107](#).

#### Related Documentation

- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)
- [Verifying That Firewall Filters Are Operational on page 173](#)
- [Monitoring Firewall Filter Traffic on page 174](#)
- [Defining CoS Classifiers \(CLI Procedure\)](#)
- [Defining CoS Classifiers \(J-Web Procedure\)](#)
- [Configuring Firewall Filters \(CLI Procedure\) on page 107](#)
- [Configuring Firewall Filters \(J-Web Procedure\) on page 115](#)

## Configuring Routing Policies (J-Web Procedure)

All routing protocols use the Junos OS routing table to store the routes that they learn and to determine which routes are advertised in the protocol packets. Routing policy allows you to control which routes the routing protocols store in and retrieve from the routing table on the routing device.

To configure routing policies for an EX Series switch using the J-Web interface:

1. Select **Configure > Routing > Policies**.



**NOTE:** After you make changes to the configuration in this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options > Commit**. See [Using the Commit Options to Commit Configuration Changes](#) for details about all commit options.

2. Click one:

- **Global Options**—Configures global options for policies. Enter information into the configuration page as described in [Table 27 on page 124](#).
- **Add**—Configures a new policy. Select **New** and specify a policy name. To add terms, enter information into the configuration page as described in [Table 28 on page 125](#). Select **Clone** to create a copy of an existing policy.
- **Edit**—Edits an existing policy. To modify an existing term, enter information into the configuration page as described in [Table 28 on page 125](#).
- **Term Up**—Moves a term up in the list.
- **Term Down**—Moves a term down in the list.
- **Delete**—Deletes the selected policy.
- **Test Policy**—Tests the policy. Use this option to check whether the policy produces the results that you expect.

Table 27: Policies Global Configuration Parameters

Field	Function	Your Action
Prefix List	Specifies a list of IPv4 address prefixes for use in a routing policy statement.	<p>To add a prefix list:</p> <ol style="list-style-type: none"> <li>1. Click <b>Add</b>.</li> <li>2. Enter a name for the prefix list.</li> <li>3. To add an IP address, click <b>Add</b>.</li> <li>4. Enter the IP address and the subnet mask and click <b>OK</b>.</li> <li>5. Click <b>OK</b>.</li> </ol> <p>To edit a prefix list, click <b>Edit</b>. Edit the settings and click <b>OK</b>.</p> <p>To delete a prefix list, select it and click <b>Delete</b>.</p>
BGP Community	Specifies a BGP community.	<p>To add a BGP community:</p> <ol style="list-style-type: none"> <li>1. Click <b>Add</b>.</li> <li>2. Enter a name for the community.</li> <li>3. To add a community, click <b>Add</b>.</li> <li>4. Enter the community ID and click <b>OK</b>.</li> <li>5. Click <b>OK</b>.</li> </ol> <p>To edit a BGP community, click <b>Edit</b>. Edit the settings and click <b>OK</b>.</p> <p>To delete a BGP community, select it and click <b>Delete</b>.</p>

Table 27: Policies Global Configuration Parameters (*continued*)

Field	Function	Your Action
AS Path	Specifies an AS path. This is applicable to BGP only.	<p>To add an AS path:</p> <ol style="list-style-type: none"> <li>1. Click <b>Add</b>.</li> <li>2. Enter the AS path name.</li> <li>3. Enter the regular expression and click <b>OK</b>.</li> <li>4. Click <b>OK</b>.</li> </ol> <p>To edit an AS path, click <b>Edit</b>. Edit the settings and click <b>OK</b>.</p> <p>To delete an AS path, select it and click <b>Delete</b>.</p>

Table 28: Terms Configuration Parameters

Field	Function	Your Action
Term Name	Specifies a term name.	Type or select and edit the name.
<b>Source tab</b>		
Family	Specifies an address family protocol.	Select a value from the list.
Routing Instance	Specifies a routing instance.	Select a value from the list.
RIB	Specifies the name of a routing table.	Select a value from the list
Preference	Specifies the individual preference value for the route.	Type or select and edit the value.
Metric	Specifies a metric value. You can specify up to four metric values.	Type or select and edit the value.
Interface	Specifies a name or IP address of one or more routing device interfaces. Do not use this qualifier with protocols that are not interface-specific, such as internal BGP (IBGP).	<p>To add an interface, select <b>Add &gt; Interface</b>. Select the interface from the list. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list.</p> <p>To add an address, select <b>Add &gt; Address</b>. Select the address from the list.</p> <p>To remove an interface, select it and click <b>Remove</b>.</p>
Prefix List	Specifies a named list of IP addresses. You can specify an exact match with incoming routes.	<p>Click <b>Add</b>. Select the prefix list from the list and click <b>OK</b>.</p> <p>To remove a prefix list, select it and click <b>Remove</b>.</p>
Protocol	Specifies the name of the protocol from which the route was learned or to which the route is being advertised.	<p>Click <b>Add</b> and select the protocol from the list.</p> <p>To remove a protocol, select it and click <b>Remove</b>.</p>

Table 28: Terms Configuration Parameters (*continued*)

Field	Function	Your Action
Policy	Specifies the name of a policy to evaluate as a subroutine.	Click <b>Add</b> . Select the policy from the list.  To remove a policy, select it and click <b>Remove</b> .
More	Specifies advanced configuration options for policies.	Click <b>More</b> for advanced configuration.
OSPF Area ID	Specifies the area identifier.	Type the IP address.
BGP Origin	Specifies the origin of the AS path information.	Select a value from the list.
Local Preference	Specifies the BGP local preference.	Type a value.
Route	Specifies the type of route.	Select <b>External</b> .  Select the OSPF type from the list.
AS Path	Specifies the name of an AS path regular expression.	Click <b>Add</b> . Select the AS path from the list.
Community	Specifies the name of one or more communities.	Click <b>Add</b> . Select the community from the list.
<b>Destination tab</b>		
Family	Specifies an address family protocol.	Select a value from the list.
Routing Instance	Specifies a routing instance.	Select a value from the list.
RIB	Specifies the name of a routing table.	Select a value from the list.
Preference	Specifies the individual preference value for the route.	Type a value.
Metric	Specifies a metric value.	Type a value.
Interface	Specifies a name or IP address of one or more routing device interfaces. Do not use this qualifier with protocols that are not interface-specific, such as internal BGP (IBGP).	To add an interface, select <b>Add &gt; Interface</b> . Select the interface from the list. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list.  To add an address, select <b>Add &gt; Address</b> . Select the address from the list.  To delete an interface, select it and click <b>Remove</b> .
Protocol	Specifies the name of the protocol from which the route was learned or to which the route is being advertised.	Click <b>Add</b> and select the protocol from the list.  To delete a protocol, select it and click <b>Remove</b> .

Table 28: Terms Configuration Parameters (*continued*)

Field	Function	Your Action
<b>Action tab</b>		
Action	Specifies the action to take if the conditions match.	Select a value from the list.
Default Action	Specifies that any action that is intrinsic to the protocol is overridden. This action is also nonterminating, so that various policy terms can be evaluated before the policy is terminated.	Select a value from the list.
Next	Specifies the default control action if a match occurs, and there are no further terms in the current routing policy.	Select a value from the list.
Priority	Specifies a priority for prefixes included in an OSPF import policy. Prefixes learned through OSPF are installed in the routing table based on the priority assigned to the prefixes.	Select a value from the list.
BGP Origin	Specifies the BGP origin attribute.	Select a value from the list.
AS Path Prepend	Affixes an AS number at the beginning of the AS path. The AS numbers are added after the local AS number has been added to the path. This action adds an AS number to AS sequences only, not to AS sets. If the existing AS path begins with a confederation sequence or set, the affixed AS number is placed within a confederation sequence. Otherwise, the affixed AS number is placed with a nonconfederation sequence.	Enter a value.
AS Path Expand	Extracts the last AS number in the existing AS path and affixes that AS number to the beginning of the AS path $n$ times, where $n$ is a number from 1 through 32. The AS number is added before the local AS number has been added to the path. This action adds AS numbers to AS sequences only, not to AS sets. If the existing AS path begins with a confederation sequence or set, the affixed AS numbers are placed within a confederation sequence. Otherwise, the affixed AS numbers are placed within a nonconfederation sequence. This option is typically used in non-IBGP export policies.	Select the type and type a value.
Load Balance Per Packet	Specifies that all next-hop addresses in the forwarding table must be installed and have the forwarding table perform per-packet load balancing. This policy action allows you to optimize VPLS traffic flows across multiple paths.	Select the check box to enable the option.
Tag	Specifies the tag value. The tag action sets the 32-bit tag field in OSPF external link-state advertisement (LSA) packets.	Select the action and type a value.
Metric	Changes the metric (MED) value by the specified negative or positive offset. This action is useful only in an external BGP (EBGP) export policy.	Select the action and type a value.
Route	Specifies whether the route is external.	Select the <b>External</b> check box to enable the option, and select the OSPF type.

Table 28: Terms Configuration Parameters (*continued*)

Field	Function	Your Action
Preference	Specifies the preference value.	Select the preference action and type a value.
Local Preference	Specifies the BGP local preference attribute.	Select the action and type a value.
Class of Service	Specifies and applies the class-of-service parameters to routes installed into the routing table. <ul style="list-style-type: none"> <li>Source class The value entered here maintains the packet counts for a route passing through your network, based on the source address.</li> <li>Destination class The value entered here maintains packet counts for a route passing through your network, based on the destination address in the packet.</li> <li>Forwarding class</li> </ul>	Type the source class. Type the destination class. Type the forwarding class.

**Related Documentation**

- Configuring BGP Sessions (J-Web Procedure)
- Configuring an OSPF Network (J-Web Procedure)
- Configuring a RIP Network (J-Web Procedure)
- Configuring Static Routing (J-Web Procedure)
- Layer 3 Protocols Supported on EX Series Switches

## Configuring Tricolor Marking Policers

You can rate-limit traffic on EX Series switches by configuring a policer and specifying it as an action modifier for a term in a firewall filter. By default, if you specify the same policer in multiple terms, Junos OS creates a separate policer instance for each term and applies rate limiting separately for each instance. For example, if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms, each policer instance enforces a 1-Gbps limit. In this case, the total bandwidth allowed by the filter is 3 Gbps.

You can also configure a policer to be filter-specific, which means that Junos OS creates only one policer instance regardless of how many times the policer is referenced. When you do this, rate limiting is applied in aggregate, so if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms, the total bandwidth allowed by the filter is 1 Gbps.

This topic describes how to configure single-rate and two-rate tricolor marking (TCM) policers, also known as single-rate and two-rate three-color policers. If you want to



configure a single-rate two-color policer (also known just as a "policer"), see ["Configuring Policers to Control Traffic Rates \(CLI Procedure\)" on page 119](#).

This topic includes:

- [Configuring a Tricolor Marking Policer on page 129](#)
- [Applying Tricolor Marking Policers to Firewall Filters on page 129](#)

## Configuring a Tricolor Marking Policer

A tricolor marking policer polices traffic on the basis of metering rates, including the configured information rate (CIR), the peak information rate (PIR), their associated burst sizes, and any policing actions configured for the traffic. With tri-color marking, you can configure traffic policing according to two separate modes—color-blind and color-aware. In color-blind mode, the current packet loss priority (PLP) value is ignored. In color-aware mode, the current PLP values are considered by the policer, and the policer can increase those values but cannot decrease them.

To configure a tricolor marking (TCM) policer:

1. Specify the name of the policer and (optionally) whether to automatically discard packets with high loss priority (PLP):

```
[edit firewall]
user@switch# set three-color-policer policer-name
user@switch# set three-color-policer policer-name action loss-priority high then discard
```

2. Specify the policer as either single-rate or two-rate and as color-aware or color-blind:

```
[edit firewall three-color-policer policer-name]
user@switch# set rate mode
```

For example:

```
[edit firewall three-color-policer srTCM1a]
user@switch# set single-rate color-aware
[edit firewall three-color-policer trTCM2-cb]
user@switch# set two-rate color-blind
```

3. For a single-rate TCM policer, configure the CIR, committed burst size (CBS), and excess burst size (EBS):

```
[edit firewall three-color-policer policer-name single-rate]
user@switch# set committed-information-rate bps
user@switch# set committed-burst-size bytes
user@switch# set excess-burst-size bytes
```

4. For a two-rate TCM policer, configure the CIR, CBS, PIR, and peak burst size (PBS):

```
[edit firewall three-color-policer policer-name single-rate]
user@switch# set committed-information-rate bps
user@switch# set committed-burst-size bytes
user@switch# set peak-information-rate bps
user@switch# set peak-burst-size bytes
```

## Applying Tricolor Marking Policers to Firewall Filters

To rate-limit traffic by applying a tricolor marking (TCM) policer to a firewall filter:

```
[edit firewall family family filter filter-name term term-name then]
user@switch# set three-color-policer rate stTCM1-ca
```

For example:

```
[edit firewall family inet filter test1 term term1 then]
user@switch# set three-color-policer single-rate policer1
```

You must include either the **single-rate** statement or the **two-rate** statement in the reference to the policer in the firewall filter configuration, and this statement must match the configured TCM policer. Otherwise, an error message appears in the configuration listing.

For example, if you configure **srTCM1-ca** as a single-rate TCM policer and try to apply it as a two-rate policer, the following message appears:

```
[edit firewall]
user@switch# show three-color-policer srTCM1-ca
single-rate {
  color-aware;
  ...
}
user@switch# show filter TESTER
term A {
  then {
    three-color-policer {
      ##
      ## Warning: Referenced two-rate policer does not exist
      ##
      two-rate srTCM;
    }
  }
}
```

**Related  
Documentation**

- [Understanding Tricolor Marking Architecture on page 70](#)
- [Understanding the Use of Policers in Firewall Filters on page 66](#)

## CHAPTER 5

# Configuration Statements

- [\[edit firewall\] Configuration Statement Hierarchy on EX Series Switches on page 131](#)
- [Firewall Filter Configuration Statements Supported by Junos OS for EX Series Switches on page 133](#)

### [\[edit firewall\] Configuration Statement Hierarchy on EX Series Switches](#)

---

This topic lists supported and unsupported configuration statements in the **[edit firewall]** hierarchy level on EX Series switches.

- *Supported* statements are those that you can use to configure some aspect of a software feature on the switch.
- *Unsupported* statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.
- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see EX Series Switch Software Features Overview.

This topic lists:

- [Supported Statements in the \[edit firewall\] Hierarchy Level on page 131](#)
- [Unsupported Statements in the \[edit firewall\] Hierarchy Level on page 132](#)

### Supported Statements in the [edit firewall] Hierarchy Level

The following hierarchy shows the **[edit firewall]** configuration statements supported on EX Series switches:

```
firewall {  
  family family-name {  
    filter filter-name {  
      interface-specific;  
    term term-name {  
      from {  
        match-conditions;  
      }  
      then {  
        action;  
        action-modifiers;  
      }  
    }  
  }  
}
```

```
    }  
  }  
}  
} policer policer-name {  
  filter-specific;  
  if-exceeding {  
    bandwidth-limit bps;  
    burst-size-limit bytes;  
  }  
  then {  
    policer-action;  
  }  
}  
}  
three-color-policer policer-name {  
  action {  
    loss-priority high then discard;  
  }  
  filter-specific;  
  single-rate {  
    (color-aware | color-blind);  
    committed-burst-size bytes;  
    committed-information-rate bps;  
    excess-burst-size bytes;  
  }  
  two-rate {  
    (color-aware | color-blind);  
    committed-burst-size bytes;  
    committed-information-rate bps;  
    peak-information-rate bps;  
    peak-burst-size bytes;  
  }  
}
```

## Unsupported Statements in the [edit firewall] Hierarchy Level

All statements in the [edit firewall] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented.

### Related Documentation

- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)
- [Configuring Firewall Filters \(CLI Procedure\) on page 107](#)
- [Configuring Policers to Control Traffic Rates \(CLI Procedure\) on page 119](#)
- [Firewall Filter Configuration Statements Supported by Junos OS for EX Series Switches on page 133](#)
- [Firewall Filters for EX Series Switches Overview on page 7](#)

## Firewall Filter Configuration Statements Supported by Junos OS for EX Series Switches

You configure firewall filters to filter packets based on their components and to perform an action on packets that match the filter.

Table 29 on page 133 lists the options that are supported for the firewall statement in Junos OS for EX Series switches.

**Table 29: Supported Options for Firewall Filter Statements**

Statement and Option	Description
<code>family <i>family-name</i> {</code> <code>}</code>	The <b><i>family-name</i></b> option specifies the version or type of addressing protocol: <ul style="list-style-type: none"> <li>• <b>any</b>—Filter packets based on protocol-independent match conditions.</li> <li>• <b>ethernet-switching</b>—Filter Layer 2 (Ethernet) packets and Layer 3 (IP) packets</li> <li>• <b>inet</b>—Filter IPv4 packets</li> <li>• <b>inet6</b>—Filter IPv6 packets</li> </ul>
<code>filter <i>filter-name</i> {</code> <code>}</code>	The <b><i>filter-name</i></b> option identifies the filter. The name can contain letters, numbers, and hyphens (-) and can be up to 64 characters long. To include spaces in the name, enclose the name in quotation marks (" ").
<code>interface-specific</code>	The <b>interface-specific</b> statement configures unique names for individual firewall counters specific to each interface.
<code>term <i>term-name</i> {</code> <code>}</code>	The <b><i>term-name</i></b> option identifies the term. The name can contain letters, numbers, and hyphens (-) and can be up to 64 characters long. To include spaces in the name, enclose the entire name in quotation marks (" "). Each term name must be unique within a filter.
<code>from {</code> <i>match-conditions</i> ; <code>}</code>	The <b>from</b> statement is optional. If you omit it, all packets are considered to match.
<code>then {</code> <i>action</i> ; <i>action-modifiers</i> ; <code>}</code>	For information about the <b><i>action</i></b> and <b><i>action-modifiers</i></b> options, see <a href="#">“Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches” on page 16</a> .
<code>policer <i>policer-name</i> {</code> <code>}</code>	The <b><i>policer-name</i></b> option identifies the policer. The name can contain letters, numbers, and hyphens (-) and can be up to 64 characters long. To include spaces in the name, enclose the name in quotation marks (" ").
<code>filter-specific</code>	The <b>filter-specific</b> statement configures policers and counters for a specific filter name.

Table 29: Supported Options for Firewall Filter Statements (*continued*)

Statement and Option	Description
<pre>if-exceeding {   bandwidth-limit <i>bps</i>   burst-size-limit <i>bytes</i> }</pre>	<p>The <b>bandwidth-limit <i>bps</i></b> option specifies the traffic rate in bits per second (bps).</p> <p>You can specify <b><i>bps</i></b> as a decimal value or as a decimal number followed by one of the following abbreviations:</p> <ul style="list-style-type: none"> <li>• k (thousand)</li> <li>• m (million)</li> <li>• g (billion, which is also called a thousand million)</li> </ul> <p><b>Range:</b> 1000 (1k) through 102,300,000,000 (102.3g) bps</p> <p>The <b>burst-size-limit <i>bytes</i></b> option specifies the maximum allowed burst size to control the amount of traffic bursting. To determine the value for the burst-size limit, you can multiply the bandwidth of the interface on which the filter is applied by the amount of time (in seconds) to allow a burst of traffic at that bandwidth to occur:</p> <p>burst size = bandwidth * allowable time for burst traffic</p> <p>You can specify a decimal value or a decimal number followed by k (thousand) or m (million).</p> <p><b>Range:</b> 1 through 2,147,450,880 bytes</p>
<pre>then {   <i>policer-action</i> }</pre>	<p>Use the <b><i>policer-action</i></b> option to specify <b>discard</b> to discard traffic that exceeds the rate limits.</p>

Junos OS for EX Series switches does not support some of the firewall filter statements that are supported by other Junos OS packages. [Table 30 on page 134](#) shows the firewall filter statements that are not supported by Junos OS for EX Series switches.

Table 30: Firewall Filter Statements That Are Not Supported by Junos OS for EX Series Switches

Statements Not Supported	Statement Hierarchy Level
<ul style="list-style-type: none"> <li>• interface-set <i>interface-set-name</i> {   }</li> <li>• load-balance-group <i>group-name</i> {   }</li> <li>• three-color-policer <i>name</i> {   }</li> <li>• logical-interface-policer;</li> <li>• single-rate {   }</li> <li>• two-rate {   }</li> </ul>	[edit firewall]

Table 30: Firewall Filter Statements That Are Not Supported by Junos OS for EX Series Switches (*continued*)

Statements Not Supported	Statement Hierarchy Level
<ul style="list-style-type: none"> <li>• <code>prefix-action <i>name</i> {</code>   <code>}</code></li> <li>• <code>prefix-policer {</code>   <code>}</code></li> <li>• <code>service-filter <i>filter-name</i> {</code>   <code>}</code></li> <li>• <code>simple-filter <i>simple-filter-name</i> {</code>   <code>}</code></li> </ul>	[edit firewall family <i>family-name</i> ]
<ul style="list-style-type: none"> <li>• <code>accounting-profile <i>name</i>;</code></li> </ul>	[edit firewall family <i>family-name</i> filter <i>filter-name</i> ]
<ul style="list-style-type: none"> <li>• <code>logical-bandwidth-policer;</code></li> <li>• <code>logical-interface-policer;</code></li> </ul>	[edit firewall policer <i>policer-name</i> ]
<code>bandwidth-percent <i>number</i>;</code>	[edit firewall policer <i>policer-name</i> if-exceeding]

**Related  
Documentation**

- [Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 16](#)
- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)
- [Configuring Firewall Filters \(CLI Procedure\) on page 107](#)
- [Configuring Policers to Control Traffic Rates \(CLI Procedure\) on page 119](#)
- [Firewall Filters for EX Series Switches Overview on page 7](#)

## action (TCM Policers)

---

<b>Syntax</b>	<code>action {     loss-priority high then discard; }</code>
<b>Hierarchy Level</b>	[edit <code>firewall three-color-policer name</code> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2 for EX Series switches.
<b>Description</b>	Discard traffic on a logical interface using tricolor marking policing.  The remaining statement is explained separately.
<b>Required Privilege Level</b>	firewall—To view this statement in the configuration. firewall-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Tricolor Marking Policers on page 128</a></li></ul>

## apply-path

---

<b>Syntax</b>	<code>apply-path path;</code>
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> policy-options <code>prefix-list name</code> ], [edit policy-options <code>prefix-list name</code> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Expand a prefix list to include all prefixes pointed to by a defined path.
<b>Options</b>	<b>path</b> —String of elements composed of identifiers or configuration keywords that points to a set of prefixes. You can include wildcards (enclosed in angle brackets) to match more than one identifier. You cannot add a path element, including wildcards, after a leaf statement. Path elements, including wildcards, can only be used after a container statement.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Prefix Lists</a></li></ul>



## as-path (Policy Options)

<b>Syntax</b>	<code>as-path name regular-expression;</code>
<b>Hierarchy Level</b>	[edit dynamic policy-options], [edit logical-systems <i>logical-system-name</i> policy-options], [edit policy-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Support for configuration in the dynamic database introduced in Junos OS Release 9.5. Support for configuration in the dynamic database introduced in Junos OS Release 9.5 for EX Series switches.
<b>Description</b>	Define an autonomous system (AS) path regular expression for use in a routing policy match condition.
<b>Options</b>	<p><b>name</b>—Name that identifies the regular expression. The name can contain letters, numbers, and hyphens (-) and can be up to 65,536 characters long. To include spaces in the name, enclose it in quotation marks (" ").</p> <p><b>regular-expression</b>—One or more regular expressions used to match the AS path.</p>
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring AS Path Regular Expressions to Use as Routing Policy Match Conditions</li> <li>Configuring Routing Policies and Policy Objects in the Dynamic Database</li> <li><a href="#">dynamic-db on page 149</a></li> </ul>

## as-path-group

---

<b>Syntax</b>	<pre>as-path-group <i>group-name</i> {     as-path <i>name</i> <i>regular-expression</i>; }</pre>
<b>Hierarchy Level</b>	[edit dynamic policy-options], [edit logical-systems <i>logical-system-name</i> policy-options], [edit policy-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Support for dynamic database configuration introduced in Junos OS Release 9.5. Support for dynamic database configuration introduced in Junos OS Release 9.5 for EX Series switches.
<b>Description</b>	Define a group containing multiple AS path regular expressions for use in a routing policy match condition.
<b>Options</b>	<p><b><i>group-name</i></b>—Name that identifies the AS path group. One or more AS path regular expressions must be listed below the <b>as-path-group</b> hierarchy.</p> <p><b><i>name</i></b>—Name that identifies the regular expression. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters long. To include spaces in the name, enclose it in quotation marks (" ").</p> <p><b><i>regular-expression</i></b>—One or more regular expressions used to match the AS path.</p>
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring AS Path Regular Expressions to Use as Routing Policy Match Conditions</li><li>• Configuring Routing Policies and Policy Objects in the Dynamic Database</li><li>• <a href="#">dynamic-db on page 149</a></li></ul>

## bandwidth-limit

<b>Syntax</b>	<code>bandwidth-limit <i>bps</i>;</code>
<b>Hierarchy Level</b>	[edit <code>firewall policer <i>policer-name</i> if-exceeding</code> ] [edit logical-systems <code><i>logical-system-name</i> firewall policer <i>policer-name</i> if-exceeding</code> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Logical systems support introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the traffic rate in bits per second.
<b>Options</b>	<p><b><i>bps</i></b> —Traffic rate to be specified in bits per second. Specify <b><i>bps</i></b> as a decimal value or as a decimal number followed by one of the following abbreviations:</p> <ul style="list-style-type: none"> <li>• k (thousand)</li> <li>• m (million)</li> <li>• g (billion, which is also called a thousand million)</li> </ul> <p><b>Range:</b></p> <ul style="list-style-type: none"> <li>• 1000 (1k) through 102,300,000,000 (102.3g) bps (EX Series switches)</li> <li>• 8000 (8k) through 40,000,000,000 (40g) bps (routers)</li> </ul>
<b>Required Privilege Level</b>	<p>firewall—To view this statement in the configuration.</p> <p>firewall-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75</a></li> <li>• <a href="#">Configuring Policers to Control Traffic Rates (CLI Procedure) on page 119</a></li> <li>• <a href="#">Understanding the Use of Policers in Firewall Filters on page 66</a></li> <li>• <a href="#">Basic Single-Rate Two-Color Policers</a></li> </ul>

## burst-size-limit

---

<b>Syntax</b>	<code>burst-size-limit bytes;</code>
<b>Hierarchy Level</b>	[edit <a href="#">firewall policer policer-name if-exceeding</a> ] [edit logical-systems <i>logical-system-name</i> firewall policer <i>policer-name</i> if-exceeding]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Logical systems support introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the maximum allowed burst size to control the amount of traffic bursting.
<b>Options</b>	<b>bytes</b> —Decimal value or a decimal number followed by k (thousand) or m (million). <b>Range:</b> <ul style="list-style-type: none"><li>• 1 through 2,147,450,880 bytes (EX Series switches)</li><li>• 1500 through 1,00,000,000,000 bytes (routers)</li></ul>
<b>Required Privilege Level</b>	firewall—To view this statement in the configuration. firewall-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75</a></li><li>• <a href="#">Configuring Policers to Control Traffic Rates (CLI Procedure) on page 119</a></li><li>• <a href="#">Understanding the Use of Policers in Firewall Filters on page 66</a></li><li>• <a href="#">Basic Single-Rate Two-Color Policers</a></li></ul>

## color-aware

---

<b>Syntax</b>	color-aware;
<b>Hierarchy Level</b>	[edit <b>firewall three-color-policer</b> <i>policer-name</i> single-rate] [edit <b>firewall three-color-policer</b> <i>policer-name</i> two-rate]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2 for EX Series switches.
<b>Description</b>	Configure the way preclassified packets are metered. In color-aware mode, the local switch can assign a higher packet loss priority but cannot assign a lower packet loss priority.
<b>Default</b>	If you omit the <b>color-aware</b> statement, the default behavior is color-aware mode.
<b>Required Privilege Level</b>	firewall—To view this statement in the configuration. firewall-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Tricolor Marking Policers on page 128</a></li> </ul>


## color-blind

---


<b>Syntax</b>	color-blind;
<b>Hierarchy Level</b>	[edit <b>firewall three-color-policer</b> <i>policer-name</i> single-rate] [edit <b>firewall three-color-policer</b> <i>policer-name</i> two-rate]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2 for EX Series switches.
<b>Description</b>	Configure the way preclassified packets are metered. In color-blind mode, the local switch ignores the preclassification of packets and can assign a higher or lower packet loss priority.
<b>Default</b>	If you omit the <b>color-blind</b> statement, the default behavior is color-aware mode.
<b>Required Privilege Level</b>	firewall—To view this statement in the configuration. firewall-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Tricolor Marking Policers on page 128</a></li> </ul>

## committed-burst-size

---

<b>Syntax</b>	<code>committed-burst-size bytes;</code>
<b>Hierarchy Level</b>	[edit <a href="#">firewall three-color-policer policer-name</a> single-rate], [edit <a href="#">firewall three-color-policer policer-name</a> two-rate]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2 for EX Series switches.
<b>Description</b>	Configure the maximum number of bytes allowed for incoming packets to burst above the committed information rate (CIR) and still be marked with low packet loss priority (green).
	<div> <b>NOTE:</b> When you include the <code>committed-burst-size</code> statement in the configuration, you must also include the <code>committed-information-rate</code> statement at the same hierarchy level.</div>
<b>Options</b>	<b>bytes</b> —Number of bytes. You can specify a value in bytes either as a complete decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000). <b>Range:</b> 1500 through 100,000,000,000 bytes
<b>Required Privilege Level</b>	<code>firewall</code> —To view this statement in the configuration. <code>firewall-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Tricolor Marking Policers on page 128</a></li></ul>

## committed-information-rate

<b>Syntax</b>	<code>committed-information-rate <i>bps</i>;</code>
<b>Hierarchy Level</b>	[edit <code>firewall three-color-policer <i>policer-name</i> single-rate</code> ], [edit <code>firewall three-color-policer <i>policer-name</i> two-rate</code> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2 for EX Series switches.
<b>Description</b>	Configure the guaranteed bandwidth under normal line conditions and the average rate up to which packets are marked with low packet loss priority (green).
	<div>  <p><b>NOTE:</b> When you include the <code>committed-information-rate</code> statement in the configuration, you must also include the <code>committed-burst-size</code> statement at the same hierarchy level.</p> </div>
<b>Options</b>	<p><b><i>bps</i></b>—Number of bits per second. You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000).</p> <p><b>Range:</b> 32,000 through 40,000,000,000 bps</p>
<b>Required Privilege</b>	firewall—To view this statement in the configuration.
<b>Level</b>	firewall-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Tricolor Marking Policers on page 128</a></li> </ul>

## community (Policy Options)

---

<b>Syntax</b>	<pre>community <i>name</i> {     invert-match;     members [ <i>community-ids</i> ]; }</pre>
<b>Hierarchy Level</b>	[edit dynamic policy-options], [edit logical-systems <i>logical-system-name</i> policy-options], [edit policy-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Support for configuration in the dynamic database introduced in Junos OS Release 9.5. Support for configuration in the dynamic database introduced in Junos OS Release 9.5 for EX Series switches.
<b>Description</b>	Define a community or extended community for use in a routing policy match condition.
<b>Options</b>	<p><b><i>name</i></b>—Name that identifies the regular expression. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters. To include spaces in the name, enclose it in quotation marks (" ").</p> <p><b><i>invert-match</i></b>—Invert the results of the community expression matching.</p> <p><b><i>members community-ids</i></b>—One or more community members. If you specify more than one member, you must enclose all members in brackets.</p> <p>The format for <b><i>community-ids</i></b> is:</p> <p style="padding-left: 40px;"><b><i>as-number:community-value</i></b></p> <p><b><i>as-number</i></b> is the AS number and can be a value in the range from 0 through 65,535. <b><i>community-value</i></b> is the community identifier and can be a number in the range from 0 through 65,535.</p> <p>You also can specify <b><i>community-ids</i></b> for communities as one of the following well-known community names, which are defined in RFC 1997, <i>BGP Communities Attribute</i>:</p> <ul style="list-style-type: none"><li>• <b><i>no-export</i></b>—Routes containing this community name are not advertised outside a BGP confederation boundary.</li><li>• <b><i>no-advertise</i></b>—Routes containing this community name are not advertised to other BGP peers.</li><li>• <b><i>no-export-subconfed</i></b>—Routes containing this community name are not advertised to external BGP peers, including peers in other members' ASs inside a BGP confederation.</li></ul> <p>You can explicitly exclude BGP community information with a static route using the <b><i>none</i></b> option. Include <b><i>none</i></b> when configuring an individual route in the <b><i>route</i></b> portion of the <b><i>static</i></b> statement to override a <b><i>community</i></b> option specified in the <b><i>defaults</i></b> portion of the statement.</p>



The format for extended **community-ids** is the following:

**type:administrator:assigned-number**

**type** is the type of extended community and can be either a **bandwidth**, **target**, **origin**, **domain-id**, **src-as**, or **rt-import** community or a 16-bit number that identifies a specific BGP extended community. The **target** community identifies the destination to which the route is going. The **origin** community identifies where the route originated. The **domain-id** community identifies the OSPF domain from which the route originated. The **src-as** community identifies the autonomous system from which the route originated. The **rt-import** community identifies the route to install in the routing table.



**NOTE:** For **src-as**, you can specify only an AS number and not an IP address. For **rt-import**, you can specify only an IP address and not an AS number.

**administrator** is the administrator. It is either an AS number or an IPv4 address prefix, depending on the type of extended community.

**assigned-number** identifies the local provider.

The format for linking a bandwidth with an AS number is:

**bandwidth:as-number:bandwidth**

**as-number** specifies the AS number and **bandwidth** specifies the bandwidth in bytes per second.



**NOTE:** In Junos OS Release 9.1 and later, you can specify 4-byte AS numbers as defined in RFC 4893, *BGP Support for Four-octet AS Number Space*, as well as the 2-byte AS numbers that are supported in earlier releases of the Junos OS. In plain-number format, you can configure a value in the range from 1 through 4,294,967,295. To configure a target or origin extended community that includes a 4-byte AS number in the plain-number format, append the letter “L” to the end of number. For example, a target community with the 4-byte AS number 334,324 and an assigned number of 132 is represented as **target:334324L:132**.

In Junos OS Release 9.2 and later, you can also use AS-dot notation when defining a 4-byte AS number for the target and origin extended communities. Specify two integers joined by a period: *16-bit high-order value in decimal.16-bit low-order value in decimal*. For example, the 4-byte AS number represented in plain-number format as 65546 is represented in AS-dot notation as 1.10.

<b>Required Privilege</b>	routing—To view this statement in the configuration.
<b>Level</b>	routing-control—To add this statement to the configuration.

- Related Documentation**
- Understanding BGP Communities and Extended Communities as Routing Policy Match Conditions
  - Defining BGP Communities and Extended Communities for Use in Routing Policy Match Conditions
  - Configuring Routing Policies and Policy Objects in the Dynamic Database
  - [dynamic-db on page 149](#)

---

## condition

---

<b>Syntax</b>	<code>condition <i>condition-name</i> {     if-route-exists <i>address</i> table <i>table-name</i>; }</code>
<b>Hierarchy Level</b>	[edit dynamic policy-options], [edit logical-systems <i>logical-system-name</i> policy-options], [edit policy-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0. Statement introduced in Junos OS Release 9.0 for EX Series switches. Support for configuration in the dynamic database introduced in Junos OS Release 9.5. Support for configuration in the dynamic database introduced in Junos OS Release 9.5 for EX Series switches.
<b>Description</b>	Define a policy condition based on the existence of routes in specific tables for use in BGP export policies.
<b>Options</b>	<b>if-route-exists <i>address</i></b> —Specify the address of the route in question.  <b>table <i>table-name</i></b> —Specify a routing table.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Routing Policy Match Conditions Based on Routing Table Entries</li><li>• Configuring Routing Policies and Policy Objects in the Dynamic Database</li><li>• <a href="#">dynamic-db on page 149</a></li></ul>

---



## counter

---

<b>Syntax</b>	<pre>counter {   counter-id <i>counter-index</i>; }</pre>
<b>Hierarchy Level</b>	[edit <b>firewall</b> <b>policer</b> <i>policer-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 12.2 for EX Series switches.
<b>Description</b>	(On EX8200 switches only) Configure a policer counter.
<b>Options</b>	<b>counter-id</b> <i>counter-index</i> —Global management counter ID. <b>Range:</b> 0 through 2
<b>Required Privilege Level</b>	firewall—To view this statement in the configuration. firewall-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Policers to Control Traffic Rates (CLI Procedure) on page 119</a></li><li>• <a href="#">Configuring Firewall Filters (CLI Procedure) on page 107</a></li><li>• <a href="#">Configuring Firewall Filters (J-Web Procedure) on page 115</a></li><li>• <a href="#">Understanding the Use of Policers in Firewall Filters on page 66</a></li></ul>

## damping (Policy Options)

---

Syntax	<pre>damping <i>name</i> {     disable;     half-life <i>minutes</i>;     max-suppress <i>minutes</i>;     reuse <i>number</i>;     suppress <i>number</i>; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> policy-options], [edit policy-options]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Define route flap damping properties to set on BGP routes.
Options	<p><b>disable</b>—Disable damping on a per-prefix basis. Any damping state that is present in the routing table for a prefix is deleted if damping is disabled.</p> <p><b>half-life <i>minutes</i></b>—Decay half-life. <i>minutes</i> is the interval after which the accumulated figure-of-merit value is reduced by half if the route remains stable. <b>Range:</b> 1 through 45 <b>Default:</b> 15 minutes</p> <p> <b>NOTE:</b> For the half-life, configure a value that is less than the max-suppress. If you do not, the configuration is rejected.</p> <p><b>max-suppress <i>minutes</i></b>—Maximum hold-down time. <i>minutes</i> is the maximum time that a route can be suppressed no matter how unstable it has been. <b>Range:</b> 1 through 720 <b>Default:</b> 60 minutes</p> <p> <b>NOTE:</b> For the max-suppress, configure a value that is greater than the half-life. If you do not, the configuration is rejected.</p> <p><b><i>name</i></b>—Name that identifies the set of damping parameters. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters long. To include spaces in the name, enclose it in quotation marks (" ").</p> <p><b>reuse <i>number</i></b>—Reuse threshold. <i>number</i> is the figure-of-merit value below which a suppressed route can be used again. <b>Range:</b> 1 through 20,000 <b>Default:</b> 750 (unitless)</p>

**suppress *number***—Cutoff (suppression) threshold. *number* is the figure-of-merit value above which a route is suppressed for use or inclusion in advertisements.

**Range:** 1 through 20,000

**Default:** 3000 (unitless)

**Required Privilege Level** routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**

- Configuring BGP Flap Damping Parameters

## dynamic-db

**Syntax** dynamic-db;

**Hierarchy Level** [edit logical-systems *logical-system-name* policy-options **as-path** *path-name*],  
[edit logical-systems *logical-system-name* policy-options **as-path-group** *group-name*],  
[edit logical-systems *logical-system-name* policy-options **community** *community-name*],  
[edit logical-systems *logical-system-name* policy-options **condition** *condition-name*],  
[edit logical-systems *logical-system-name* policy-options **policy-statement** *policy-statement-name*],  
[edit logical-systems *logical-system-name* policy-options **prefix-list** *prefix-list-name*],  
[edit policy-options **as-path** *path-name*],  
[edit policy-options **as-path-group** *group-name*],  
[edit policy-options **community** *community-name*],  
[edit policy-options **condition** *condition-name*],  
[edit policy-options **policy-statement** *policy-statement-name*],  
[edit policy-options **prefix-list** *prefix-list-name*]

**Release Information** Statement introduced in Junos OS Release 9.5.  
Statement introduced in Junos OS Release 9.5 for EX Series switches.

**Description** Define routing policies and policy objects that reference policies configured in the dynamic database at the **[edit dynamic]** hierarchy level.


**Required Privilege Level** routing—To view this statement in the configuration.  
routing-control-level—To add this statement to the configuration.

**Related Documentation**

- Configuring Routing Policies Based on Dynamic Database Configuration

## excess-burst-size

---

<b>Syntax</b>	<code>excess-burst-size bytes;</code>
<b>Hierarchy Level</b>	[edit <a href="#">firewall three-color-policer</a> <i>policer-name</i> single-rate]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2 for EX Series switches.
<b>Description</b>	Configure the maximum number of bytes allowed for incoming packets to burst above the committed information rate and still be marked with medium-high packet loss priority (yellow). Packets that exceed the excess burst size (EBS) are marked with high packet loss priority (red).
	<div> <b>NOTE:</b> When you include the <code>excess-burst-size</code> statement in the configuration, you must also include the <code>committed-burst-size</code> and <code>committed-information-rate</code> statements at the same hierarchy level.</div>
<b>Options</b>	<p><b>bytes</b>—Number of bytes. You can specify a value in bytes either as a complete decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000).</p> <p><b>Range:</b> 1500 through 100,000,000,000 bytes</p>
<b>Required Privilege Level</b>	<p><code>firewall</code>—To view this statement in the configuration.</p> <p><code>firewall-control</code>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Tricolor Marking Policers on page 128</a></li></ul>

## family (Firewall Filter)

<b>Syntax</b>	<pre> family <i>family-name</i> {     filter <i>filter-name</i> {         interface-specific;         term <i>term-name</i> {             from {                 match-conditions;             }             then {                 action;                 action-modifiers;             }         }     } } </pre>
<b>Hierarchy Level</b>	[edit <a href="#">firewall</a> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0 for EX Series switches. Option <a href="#">interface-specific</a> introduced in Junos OS Release 9.5 for EX Series switches.
<b>Description</b>	Configure a firewall filter for IP version 4 or IP version 6.
<b>Options</b>	<p><i>family-name</i>—Version or type of addressing protocol:</p> <ul style="list-style-type: none"> <li>• <b>any</b>—Filter packets based on protocol-independent match conditions.</li> <li>• <b>ethernet-switching</b>—Filter Layer 2 (Ethernet) packets and Layer 3 (IP) packets.</li> <li>• <b>inet</b>—Filter IPv4 packets.</li> <li>• <b>inet6</b>—Filter IPv6 packets.</li> </ul> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 16</a></li> <li>• <a href="#">Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75</a></li> <li>• <a href="#">Configuring Firewall Filters (CLI Procedure) on page 107</a></li> <li>• <a href="#">Configuring Firewall Filters (J-Web Procedure) on page 115</a></li> <li>• <a href="#">Firewall Filters for EX Series Switches Overview on page 7</a></li> </ul>

## filter (Firewall Filters)

---

<b>Syntax</b>	<pre>filter <i>filter-name</i> {     <i>interface-specific</i>;     term <i>term-name</i> {         from {             <i>match-conditions</i>;         }         then {             <i>action</i>;             <i>action-modifiers</i>;         }     } }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">firewall family</a> <i>family-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0 for EX Series switches. Option <a href="#">interface-specific</a> introduced in Junos OS Release 9.5 for EX Series switches.
<b>Description</b>	Configure firewall filters.
<b>Options</b>	<p><b><i>filter-name</i></b>—Name that identifies the filter. The name can contain letters, numbers, and hyphens (-), and can be up to 64 characters long. To include spaces in the name, enclose it in quotation marks.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>firewall—To view this statement in the configuration.</p> <p>firewall-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 16</a></li><li>• <a href="#">Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75</a></li><li>• <a href="#">Configuring Firewall Filters (CLI Procedure) on page 107</a></li><li>• <a href="#">Configuring Firewall Filters (J-Web Procedure) on page 115</a></li><li>• <a href="#">Firewall Filters for EX Series Switches Overview on page 7</a></li></ul>



## filter (VLANs)

---

<b>Syntax</b>	<code>filter (input   output) <i>filter-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit vlans <i>vlan-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Apply a firewall filter to traffic coming into or exiting from the VLAN.
<b>Default</b>	All incoming traffic is accepted unmodified to the VLAN, and all outgoing traffic is sent unmodified from the VLAN.
<b>Options</b>	<p><b><i>filter-name</i></b> —Name of a firewall filter defined in a <b>filter</b> statement.</p> <ul style="list-style-type: none"> <li><b>input</b>—Apply a firewall filter to VLAN ingress traffic.</li> <li><b>output</b>—Apply a firewall filter to VLAN egress traffic.</li> </ul>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75</a></li> <li><a href="#">Configuring Firewall Filters (CLI Procedure) on page 107</a></li> <li><a href="#">Configuring Firewall Filters (J-Web Procedure) on page 115</a></li> <li><a href="#">Firewall Filters for EX Series Switches Overview on page 7</a></li> </ul>

## filter-specific

---

<b>Syntax</b>	<code>filter-specific;</code>
<b>Hierarchy Level</b>	<code>[edit <b>firewall policer</b> <i>policer-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 for EX Series switches.
<b>Description</b>	Configure a policer to act as a filter-specific policer. If you do not specify the <b>filter-specific</b> statement, the policer acts as a term-specific policer by default.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75</a></li> <li><a href="#">Configuring Policers to Control Traffic Rates (CLI Procedure) on page 119</a></li> <li><a href="#">Understanding the Use of Policers in Firewall Filters on page 66</a></li> </ul>

## firewall

```
Syntax  firewall {
        family family-name {
            filter filter-name {
                interface-specific;
                term term-name {
                    from {
                        match-conditions;
                    }
                    then {
                        action;
                        action-modifiers;
                    }
                }
            }
        }
        policer policer-name {
            filter-specific;
            if-exceeding {
                bandwidth-limit bps;
                burst-size-limit bytes;
            }
            then {
                policer-action;
            }
        }
    }

three-color-policer policer-name {
    action {
        loss-priority high then discard;
    }
    single-rate {
        (color-aware | color-blind);
        committed-information-rate bps;
        committed-burst-size bytes;
        excess-burst-size bytes;
    }
    two-rate {
        (color-aware | color-blind);
        committed-information-rate bps;
        committed-burst-size bytes;
        peak-information-rate bps;
        peak-burst-size bytes;
    }
}
```

Hierarchy Level [edit]

**Release Information** Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Options **interface-specific** and **filter-specific** introduced in Junos OS Release 9.5 for EX Series switches.

<b>Description</b>	Configure firewall filters and policers.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	firewall—To view this statement in the configuration. firewall-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 16</a></li> <li>• <a href="#">Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75</a></li> <li>• <a href="#">Configuring Firewall Filters (CLI Procedure) on page 107</a></li> <li>• <a href="#">Configuring Policers to Control Traffic Rates (CLI Procedure) on page 119</a></li> <li>• <a href="#">Firewall Filters for EX Series Switches Overview on page 7</a></li> </ul>

---

## from

---

<b>Syntax</b>	<pre>from {     match-conditions; }</pre>
<b>Hierarchy Level</b>	[edit <b>firewall</b> <b>family</b> <i>family-name</i> <b>filter</b> <i>filter-name</i> <b>term</b> <i>term-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Match packet fields to values specified in a match condition. If the <b>from</b> statement is not included in a firewall filter configuration, all packets are considered to match and the actions and action modifiers in the <b>then</b> statement are taken.
<b>Options</b>	<b>match-conditions</b> —Conditions that define the values or fields that the incoming or outgoing packets must contain for a match. You can specify one or more match conditions. If you specify more than one, they all must match for a match to occur and for the action in the <b>then</b> statement to be taken.
<b>Required Privilege Level</b>	firewall—To view this statement in the configuration. firewall-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 16</a></li> <li>• <a href="#">Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75</a></li> <li>• <a href="#">Configuring Firewall Filters (CLI Procedure) on page 107</a></li> <li>• <a href="#">Configuring Firewall Filters (J-Web Procedure) on page 115</a></li> <li>• <a href="#">Understanding Firewall Filter Match Conditions on page 62</a></li> </ul>

## if-exceeding

---

<b>Syntax</b>	<pre>if-exceeding {     bandwidth-limit <i>bps</i>;     bandwidth-percent <i>percent</i>     burst-size-limit <i>bytes</i>; }</pre>
<b>Hierarchy Level</b>	<pre>[edit <b>firewall</b> <b>policer</b> <i>policer-name</i>] [edit logical-systems logical-system-name firewall policer <i>policer-name</i>]</pre>
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Logical systems support introduced in Junos OS Release 9.3.</p>
<b>Description</b>	<p>Configure policer rate limits.</p> <p>The <b>bandwidth-percent</b> statement is supported on routers only.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>firewall—To view this statement in the configuration.</p> <p>firewall-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75</a></li><li>• <a href="#">Configuring Policers to Control Traffic Rates (CLI Procedure) on page 119</a></li><li>• <a href="#">Understanding the Use of Policers in Firewall Filters on page 66</a></li><li>• <a href="#">Basic Single-Rate Two-Color Policers</a></li></ul>

## interface-specific

---

<b>Syntax</b>	interface-specific;
<b>Hierarchy Level</b>	[edit <b>firewall family</b> <i>family-name</i> <b>filter</b> <i>filter-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5 for EX Series switches.
<b>Description</b>	Configure firewall counters that are interface-specific. You can configure an interface-specific firewall filter only on a port or a Layer 3 interface as an interface-specific firewall filter is not supported for a VLAN.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 16</a></li> <li>• <a href="#">Configuring Firewall Filters (CLI Procedure) on page 107</a></li> <li>• <a href="#">Configuring Firewall Filters (J-Web Procedure) on page 115</a></li> <li>• <a href="#">Firewall Filters for EX Series Switches Overview on page 7</a></li> </ul>


## loss-priority high then discard (Three-Color Policer)

---

<b>Syntax</b>	loss-priority high then discard;
<b>Hierarchy Level</b>	[edit firewall <b>three-color-policer</b> <i>policer-name</i> <b>action</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2 for EX Series switches.
<b>Description</b>	<p>For packets with high loss priority, discard the packets. The loss priority setting is implicit and cannot be configured. Include this statement if you do not want the local switch to forward packets that have high packet loss priority.</p> <p>For single-rate three-color policers, Junos OS assigns high loss priority to packets that exceed the committed information rate and the excess burst size.</p> <p>For two-rate three-color policers, Junos OS assigns high loss priority to packets that exceed the peak information rate and the peak burst size.</p>
<b>Required Privilege Level</b>	firewall—To view this statement in the configuration. firewall-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Tricolor Marking Policers on page 128</a></li> </ul>

## peak-burst-size

---

<b>Syntax</b>	<code>peak-burst-size bytes;</code>
<b>Hierarchy Level</b>	[edit <a href="#">firewall three-color-policer</a> <i>policer-name</i> two-rate]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2 for EX Series switches.
<b>Description</b>	Configure the maximum number of bytes allowed for incoming packets to burst above the peak information rate (PIR) and still be marked with medium-high packet loss priority (yellow). Packets that exceed the peak burst size (PBS) are marked with high packet loss priority (red).
	<div> <b>NOTE:</b> When you include the <code>peak-burst-size</code> statement in the configuration, you must also include the <code>committed-burst-size</code> and <code>peak-information-rate</code> statements at the same hierarchy level.</div>
<b>Options</b>	<p><b>bytes</b>—Number of bytes. You can specify a value in bytes either as a complete decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000).</p> <p><b>Range:</b> 1500 through 100,000,000,000 bytes</p>
<b>Required Privilege Level</b>	<p><code>firewall</code>—To view this statement in the configuration.</p> <p><code>firewall-control</code>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Tricolor Marking Policers on page 128</a></li></ul>

## policer

<b>Syntax</b>	<pre> policer <i>policer-name</i> {     counter {         counter-id <i>counter-index</i>;     }     filter-specific;     if-exceeding {         bandwidth-limit <i>bps</i>;         bandwidth-percent <i>percent</i>         burst-size-limit <i>bytes</i>;     }     then {         <i>policer-action</i>;     } } </pre>
<b>Hierarchy Level</b>	[edit <a href="#">firewall</a> ], [edit logical-systems <i>logical-system-name</i> <a href="#">firewall</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Logical systems support introduced in Junos OS Release 9.3.
<b>Description</b>	Configure policer rate limits and actions. To activate a policer, you must include the <b>policer</b> action modifier in the <b>then</b> statement in a firewall filter term. Except for EX8200 switches, each policer that you configure includes an implicit counter. To obtain term-specific packet counts, configure a policer for each term in the filter that requires policing. For EX8200 switches, configure a policer and associate it with a global management counter using the <a href="#">counter</a> option.
<b>Options</b>	<p><b><i>policer-name</i></b>—Name that identifies the policer. The name can include letters, numbers, hyphens (-), and can contain up to 64 characters.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	firewall—To view this statement in the configuration. firewall-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75</a></li> <li>• <a href="#">Example: Configuring CoS on EX Series Switches</a></li> <li>• <a href="#">Configuring Policers to Control Traffic Rates (CLI Procedure) on page 119</a></li> <li>• <a href="#">Configuring MPLS on Provider Edge Switches Using Circuit Cross-Connect (CLI Procedure)</a></li> <li>• <a href="#">Configuring MPLS on Provider Edge Switches Using IP Over MPLS (CLI Procedure)</a></li> <li>• <a href="#">Understanding the Use of Policers in Firewall Filters on page 66</a></li> <li>• <a href="#">Basic Single-Rate Two-Color Policers</a></li> </ul>

## policy-statement

<b>Syntax</b>	<pre> policy-statement <i>policy-name</i> {   term <i>term-name</i> {     from {       family <i>family-name</i>;       match-conditions;       policy <i>subroutine-policy-name</i>;       prefix-list <i>prefix-list-name</i>;       prefix-list-filter <i>prefix-list-name</i> match-type &lt;actions&gt;;       route-filter <i>destination-prefix</i> match-type &lt;actions&gt;;       source-address-filter <i>source-prefix</i> match-type &lt;actions&gt;;     }     to {       match-conditions;       policy <i>subroutine-policy-name</i>;     }     then <i>actions</i>;   } } </pre>
<b>Hierarchy Level</b>	<p>[edit dynamic policy-options],  [edit logical-systems <i>logical-system-name</i> policy-options],  [edit policy-options]</p>
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.  Statement introduced in Junos OS Release 9.0 for EX Series switches.  Support for configuration in the dynamic database introduced in Junos OS Release 9.5.  Support for configuration in the dynamic database introduced in Junos OS Release 9.5 for EX Series switches.  <b>inet-mdt</b> option introduced in Junos OS Release 10.0R2.  Statement introduced in Junos OS Release 11.3 for the QFX Series.  <b>route-target</b> option introduced in Junos OS Release 12.2.</p>
<b>Description</b>	<p>Define a routing policy, including subroutine policies.</p> <p>To list the routing policies under the <b>[edit policy-options]</b> hierarchy level by <b>policy-statement <i>policy-name</i></b> in alphabetical order, enter the <b>show policy-options</b> configuration command.</p>
<b>Options</b>	<p><b>actions</b>—(Optional) One or more actions to take if the conditions match. The actions are described in Configuring Flow Control Actions.</p> <p><b>family <i>family-name</i></b>—(Optional) Specify an address family protocol. Specify <b>inet</b> for IPv4. Specify <b>inet6</b> for 128-bit IPv6, and to enable interpretation of IPv6 router filter addresses. For IS-IS traffic, specify <b>iso</b>. For IPv4 multicast VPN traffic, specify <b>inet-mvpn</b>. For IPv6 multicast VPN traffic, specify <b>inet6-mvpn</b>. For multicast-distribution-tree (MDT) IPv4 traffic, specify <b>inet-mdt</b>. For BGP route target VPN traffic, specify <b>route-target</b>.</p>





**NOTE:** When **family** is not specified, the routing device or routing instance uses the address family or families carried by BGP. If multiprotocol BGP (MP-BGP) is enabled, the policy defaults to the protocol family or families carried in the network layer reachability information (NLRI) as configured in the family statement for BGP. If MP-BGP is not enabled, the policy uses the default BGP address family unicast IPv4.

**from**—(Optional) Match a route based on its source address.

**match-conditions**—(Optional in **from** statement; required in **to** statement) One or more conditions to use to make a match. The qualifiers are described in Configuring Match Conditions in Routing Policy Terms.

**policy subroutine-policy-name**—Use another policy as a match condition within this policy. The name identifying the subroutine policy can contain letters, numbers, and hyphens (-) and can be up to 255 characters long. To include spaces in the name, enclose it in quotation marks (" "). Policy names cannot take the form `__.*-internal__`, as this form is reserved. For information about how to configure subroutines, see Configuring Subroutines in Routing Policy Match Conditions.

**policy-name**—Name that identifies the policy. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters long. To include spaces in the name, enclose it in quotation marks (" ").

**prefix-list prefix-list-name** —Name of a list of IPv4 or IPv6 prefixes.

**prefix-list-filter prefix-list-name**—Name of a prefix list to evaluate using qualifiers; **match-type** is the type of match (see Configuring Prefix List Filters), and **actions** is the action to take if the prefixes match.

**route-filter destination-prefix match-type <actions>**—(Optional) List of routes on which to perform an immediate match; **destination-prefix** is the IPv4 or IPv6 route prefix to match, **match-type** is the type of match (see Configuring Route Lists), and **actions** is the action to take if the **destination-prefix** matches.

**source-address-filter source-prefix match-type <actions>**—(Optional) Unicast source addresses in multiprotocol BGP (MBGP) and Multicast Source Discovery Protocol (MSDP) environments on which to perform an immediate match. **source-prefix** is the IPv4 or IPv6 route prefix to match, **match-type** is the type of match (see Configuring Route Lists), and **actions** is the action to take if the **source-prefix** matches.

**term term-name**—Name that identifies the term.

**to**—(Optional) Match a route based on its destination address or the protocols into which the route is being advertised.

**then**—(Optional) Actions to take on matching routes. The actions are described in Configuring Flow Control Actions and Configuring Actions That Manipulate Route Characteristics.

<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Defining Routing Policies</li><li>Configuring Routing Policies and Policy Objects in the Dynamic Database</li><li><a href="#">dynamic-db on page 149</a></li></ul>

---

## prefix-list

---

<b>Syntax</b>	<pre>prefix-list <i>name</i> {     <i>ip-addresses</i>;     apply-path <i>path</i>; }</pre>
<b>Hierarchy Level</b>	[edit dynamic policy-options], [edit logical-systems <i>logical-system-name</i> policy-options], [edit policy-options]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Support for configuration in the dynamic database introduced in Junos OS Release 9.5. Support for configuration in the dynamic database introduced in Junos OS Release 9.5 for EX Series switches. Support for the <b>vpls</b> protocol family introduced in Junos OS Release 10.2.
<b>Description</b>	Define a list of IPv4 or IPv6 address prefixes for use in a routing policy statement or firewall filter statement.  You can configure up to 85,325 prefixes in each prefix list. To configure more than 85,325 prefixes, configure multiple prefix lists and apply them to multiple firewall filter terms.
<b>Options</b>	<b><i>name</i></b> —Name that identifies the list of IPv4 or IPv6 address prefixes.  <b><i>ip-addresses</i></b> —List of IPv4 or IPv6 address prefixes, one IP address per line in the configuration.  The remaining statement is explained separately.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Prefix Lists for Use in Routing Policy Match Conditions</li><li>Firewall Filter Match Conditions Based on Address Fields</li><li>Example: Configuring a Filter to Limit TCP Access to a Port Based On a Prefix List</li></ul>

## routing-instance

---

<b>Syntax</b>	<code>routing-instance <i>routing-instance-name</i>;</code>
<b>Hierarchy Level</b>	[edit <code>firewall</code> family inet <code>filter filter-name</code> <code>term term-name</code> <code>then</code> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4 for EX Series switches.
<b>Description</b>	Specify a specific virtual routing instance to which the switch sends matched packets.
<b>Options</b>	<i>routing-instance-name</i> —Name of a virtual routing instance.
<b>Required Privilege Level</b>	<code>firewall</code> —To view this statement in the configuration. <code>firewall-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches on page 96</a></li><li>• <a href="#">Configuring Virtual Routing Instances (CLI Procedure)</a></li><li>• <a href="#">Understanding Filter-Based Forwarding for EX Series Switches on page 70</a></li></ul>

## single-rate

---

<b>Syntax</b>	<pre>single-rate {   (color-aware   color-blind);   committed-burst-size bytes;   committed-information-rate bps;   excess-burst-size bytes; }</pre>
<b>Hierarchy Level</b>	[edit <a href="#">firewall three-color-policer</a> <i>policer-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2 for EX Series switches.
<b>Description</b>	<p>Configure a single-rate three-color policer in which marking is based on the committed information rate (CIR), committed burst size (CBS), and excess burst size (EBS).</p> <p>Packets that conform to the CIR or the CBS are assigned low loss priority (green). Packets that exceed the CIR and the CBS but do not exceed the EBS are assigned medium-high loss priority (yellow). Packets that exceed the EBS are assigned high loss priority (red).</p> <p>Green and yellow packets are always forwarded; this action is not configurable. You can configure red packets to be discarded. By default, red packets are forwarded.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>firewall—To view this statement in the configuration.</p> <p>firewall-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Tricolor Marking Policers on page 128</a></li></ul>

## term

---

<b>Syntax</b>	<pre>term <i>term-name</i> {     from {         <i>match-conditions</i>;     }     then {         <i>action</i>;         <i>action-modifiers</i>;     } }</pre>
<b>Hierarchy Level</b>	[edit <b>firewall family</b> <i>family-name</i> <b>filter</b> <i>filter-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Define a firewall filter term.
<b>Options</b>	<p><b><i>term-name</i></b>—Name that identifies the term. The name can contain letters, numbers, and hyphens (-), and can be up to 64 characters long. To include spaces in the name, enclose it in quotation marks.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>firewall—To view this statement in the configuration.</p> <p>firewall-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 16</a></li> <li>• <a href="#">Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75</a></li> <li>• <a href="#">Configuring Firewall Filters (CLI Procedure) on page 107</a></li> <li>• <a href="#">Configuring Firewall Filters (J-Web Procedure) on page 115</a></li> <li>• <a href="#">Firewall Filters for EX Series Switches Overview on page 7</a></li> </ul>

## then (Firewall Filters)

---

<b>Syntax</b>	<pre>then {     action;     action-modifiers; }</pre>
<b>Hierarchy Level</b>	[edit <b>firewall family</b> <i>family-name</i> <b>filter</b> <i>filter-name</i> <b>term</b> <i>term-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Configure a filter action.
<b>Options</b>	<p><b>action</b>—Action to accept, discard, or forward packets that match all match conditions specified in a filter term.</p> <p><b>action-modifiers</b>—Additional actions to analyze, classify, count, or police packets that match all conditions specified in a filter term.</p>
<b>Required Privilege Level</b>	<p>firewall—To view this statement in the configuration.</p> <p>firewall-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 16</a></li><li>• <a href="#">Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75</a></li><li>• <a href="#">Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches on page 96</a></li><li>• <a href="#">Configuring Firewall Filters (CLI Procedure) on page 107</a></li><li>• <a href="#">Configuring Firewall Filters (J-Web Procedure) on page 115</a></li><li>• <a href="#">Understanding Firewall Filter Match Conditions on page 62</a></li></ul>

## then (Policer Action)

---

<b>Syntax</b>	<pre>then {     <i>policer-action</i>; }</pre>
<b>Hierarchy Level</b>	<pre>[edit <b>firewall</b> <b>policer</b> <i>policer-name</i>] [edit logical-systems <i>logical-system-name</i> firewall policer <i>policer-name</i>]</pre>
<b>Release Information</b>	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
<b>Description</b>	Configure a policer action.
<b>Options</b>	<p><b><i>policer-action</i></b>—Actions to take are:</p> <ul style="list-style-type: none"> <li>• <b>discard</b>—Discard traffic that exceeds the rate limits defined by the policer.</li> <li>• <b>forwarding-class <i>class-name</i></b>—For routers only, classify traffic that exceeds the rate limits defined by the policer.</li> <li>• <b>loss-priority</b>—Set the loss priority for traffic that exceeds the rate limits defined by the policer.</li> </ul>
<b>Required Privilege Level</b>	<p><b>firewall</b>—To view this statement in the configuration.</p> <p><b>firewall -control</b>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75</a></li> <li>• <a href="#">Configuring Policers to Control Traffic Rates (CLI Procedure) on page 119</a></li> <li>• <a href="#">Configuring Firewall Filters (CLI Procedure) on page 107</a></li> <li>• <a href="#">Configuring Firewall Filters (J-Web Procedure) on page 115</a></li> <li>• <a href="#">Understanding the Use of Policers in Firewall Filters on page 66</a></li> <li>• <a href="#">Example: Configuring CoS for a PBB Network on MX Series Routers</a></li> <li>• <a href="#">Basic Single-Rate Two-Color Policers</a></li> </ul>

## three-color-policer (Configuring)

---

**Syntax**    `three-color-policer policer-name {  
                  action {  
                    loss-priority high then discard;  
                  }  
                  single-rate {  
                    (color-aware | color-blind);  
                    committed-burst-size bytes;  
                    committed-information-rate bps;  
                    excess-burst-size bytes;  
                  }  
                  two-rate {  
                    (color-aware | color-blind);  
                    committed-burst-size bytes;  
                    committed-information-rate bps;  
                    peak-burst-size bytes;  
                    peak-information-rate bps;  
                  }  
                }`

**Hierarchy Level**    [edit [firewall](#)]

**Release Information**    Statement introduced in Junos OS Release 11.2 for EX Series switches.

**Description**    Configure a three-color policer.

**Options**    *policer-name*—Name of the three-color policer. Reference this name when you apply the policer to an interface.

The remaining statements are explained separately.

**Required Privilege Level**    firewall—To view this statement in the configuration.  
                                  firewall-control—To add this statement to the configuration.

**Related Documentation**    • [Configuring Tricolor Marking Policers on page 128](#)



## two-rate

---

<b>Syntax</b>	<pre>two-rate {   (color-aware   color-blind);   committed-burst-size bytes;   committed-information-rate bps;   peak-burst-size bytes;   peak-information-rate bps; }</pre>
<b>Hierarchy Level</b>	[edit <b>firewall three-color-policer</b> <i>policer-name</i> ],
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2 for EX Series switches.
<b>Description</b>	<p>Configure a two-rate three-color policer in which marking is based on the committed information rate (CIR), committed burst size (CBS), peak information rate (PIR), and peak burst size (PBS).</p> <p>Packets that conform to the CIR or the CBS are assigned low loss priority (green). Packets that exceed the PIR and the PBS are assigned high loss priority (red).</p> <p>Green packets are always forwarded; this action is not configurable. You can configure red packets to be discarded. By default, red packets are forwarded.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	firewall—To view this statement in the configuration. firewall-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring Tricolor Marking Policers on page 128</a></li> </ul>



## PART 3

# Administration

- [Routine Monitoring on page 173](#)
- [Operational Commands on page 177](#)



## CHAPTER 6

# Routine Monitoring

- [Verifying That Firewall Filters Are Operational on page 173](#)
- [Verifying That Policers Are Operational on page 174](#)
- [Monitoring Firewall Filter Traffic on page 174](#)

### Verifying That Firewall Filters Are Operational

---

**Purpose** After you configure and apply firewall filters to ports, VLANs, or Layer 3 interfaces, you can perform the following task to verify that the firewall filters configured on EX Series switches are working properly.

**Action** Use the operational mode command to verify that the firewall filters on the switch are working properly:

```
user@switch> show firewall
Filter: egress-vlan-watch-employee
Counters:
Name                                     Bytes      Packets
counter-employee-web                     0           0
Filter: ingress-port-voip-class-limit-tcp-icmp
Counters:
Name                                     Bytes      Packets
icmp-counter                             0           0
Policies:
Name                                     Packets
icmp-connection-policer                  0
tcp-connection-policer                   0
Filter: ingress-vlan-rogue-block
Filter: ingress-vlan-limit-guest
```

**Meaning** The **show firewall** command displays the names of all firewall filters, policers, and counters that are configured on the switch. For each counter that is specified in a filter configuration, the output field shows the byte count and packet count for the term in which the counter is specified. For each policer that is specified in a filter configuration, the output field shows the packet count for packets that exceed the specified rate limits.

- Related Documentation**
- [Configuring Firewall Filters \(CLI Procedure\) on page 107](#)
  - [Configuring Firewall Filters \(J-Web Procedure\) on page 115](#)
  - [Configuring Policers to Control Traffic Rates \(CLI Procedure\) on page 119](#)

- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)
- [Monitoring Firewall Filter Traffic on page 174](#)

---

## Verifying That Policers Are Operational

---

<b>Purpose</b>	After you configure policers and include them in firewall filter configurations, you can perform the following tasks to verify that the policers configured on EX Series switches are working properly.
<b>Action</b>	<p>Use the operational mode command to verify that the policers on the switch are working properly:</p> <pre>user@switch&gt; show policer Filter: egress-vlan-watch-employee Filter: ingress-port-filter Filter: ingress-port-voip-class-limit-tcp-icmp Policers: Name                                     Packets icmp-connection-policer                  0 tcp-connection-policer                   0 Filter: ingress-vlan-rogue-block Filter: ingress-vlan-limit-guest</pre>
<b>Meaning</b>	The <b>show policer</b> command displays the names of all firewall filters and policers that are configured on the switch. For each policer that is specified in a filter configuration, the output field shows the current packet count for all packets that exceed the specified rate limits.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Policers to Control Traffic Rates (CLI Procedure) on page 119</a></li><li>• <a href="#">Configuring Firewall Filters (CLI Procedure) on page 107</a></li><li>• <a href="#">Configuring Firewall Filters (J-Web Procedure) on page 115</a></li><li>• <a href="#">Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75</a></li><li>• <a href="#">Monitoring Firewall Filter Traffic on page 174</a></li></ul>

---

## Monitoring Firewall Filter Traffic

---

You can monitor firewall filter traffic on EX Series switches.

- [Monitoring Traffic for All Firewall Filters and Policers That Are Configured on the Switch on page 175](#)
- [Monitoring Traffic for a Specific Firewall Filter on page 175](#)
- [Monitoring Traffic for a Specific Policer on page 175](#)

## Monitoring Traffic for All Firewall Filters and Policers That Are Configured on the Switch

**Purpose** Perform the following task to monitor the number of packets and bytes that matched the firewall filters and monitor the number of packets that exceeded policer rate limits:

**Action** Use the operational mode command:

```
user@switch> show firewall
Filter: egress-vlan-watch-employee
Counters:
Name                               Bytes      Packets
counter-employee-web              3348        27
Filter: ingress-port-voip-class-limit-tcp-icmp
Counters:
Name                               Bytes      Packets
icmp-counter                      4100        49
Policers:
Name                               Packets
icmp-connection-policer           0
tcp-connection-policer            0
Filter: ingress-vlan-rogue-block
Filter: ingress-vlan-limit-guest
```

**Meaning** The **show firewall** command displays the names of all firewall filters, policers, and counters that are configured on the switch. The output fields show byte and packet counts for counters and packet count for policers.

## Monitoring Traffic for a Specific Firewall Filter

**Purpose** Perform the following task to monitor the number of packets and bytes that matched a firewall filter and monitor the number of packets that exceeded the policer rate limits.

**Action** Use the operational mode command:

```
user@switch> show firewall filter ingress-vlan-rogue-block
Filter: ingress-vlan-rogue-block
Counters:
Name                               Bytes      Packets
rogue-counter                      2308        20
```

**Meaning** The **show firewall filter *filter-name*** command displays the name of the firewall filter, the packet and byte count for all counters configured with the filter, and the packet count for all policers configured with the filter.

## Monitoring Traffic for a Specific Policer

**Purpose** Perform the following task to monitor the number of packets that exceeded policer rate limits:

**Action** Use the operational mode command:

```
user@switch> show policer tcp-connection-policer
```

```
Filter: ingress-port-voip-class-limit-tcp-icmp
Policers:
Name                                     Packets
tcp-connection-policer                  0
```

**Meaning** The `show policer policer-name` command displays the name of the firewall filter that specifies the policer-action and displays the number of packets that exceeded rate limits for the specified filter.


- Related Documentation**
- [Configuring Firewall Filters \(CLI Procedure\) on page 107](#)
  - [Configuring Firewall Filters \(J-Web Procedure\) on page 115](#)
  - [Configuring Policers to Control Traffic Rates \(CLI Procedure\) on page 119](#)
  - [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)
  - [Verifying That Firewall Filters Are Operational on page 173](#)



## CHAPTER 7

# Operational Commands

## clear firewall

<b>Syntax</b>	clear firewall (all   counter <i>counter-name</i>   filter <i>filter-name</i>   logical-system <i>logical-system-name</i> )
<b>Syntax (EX Series Switches)</b>	clear firewall (all   counter <i>counter-name</i>   filter <i>filter-name</i>   policer counter (all   counter-id <i>counter-index</i> ))
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. <b>logical-system</b> option introduced in Junos OS Release 9.3.
<b>Description</b>	Clear statistics about configured firewall filters.  When you clear the counters of a filter, this impacts not only the counters shown by the CLI, but also the ones tracked by SNMP2.
	<div>  <p><b>NOTE:</b> The clear firewall command cannot be used to clear the Routing Engine filter counters on a backup Routing Engine that is enabled for graceful Routing Engine switchover (GRES).</p> </div> <p>If you clear statistics for firewall filters that are applied to Trio-based DPCs and that also use the <b>prefix-action</b> action on matched packets, wait at least 5 seconds before you enter the <b>show firewall prefix-action-stats</b> command. A 5-second pause between issuing the <b>clear firewall</b> and <b>show firewall prefix-action-stats</b> commands avoids a possible timeout of the <b>show firewall prefix-action-stats</b> command.</p>
<b>Options</b>	<p><b>all</b>—Clear the packet and byte counts for all filters. On EX Series switches, this option also clears the packet counts for all policer counters.</p> <p><b>counter <i>counter-name</i></b>—Clear the packet and byte counts for a filter counter that has been configured with the counter firewall filter action.</p> <p><b>filter <i>filter-name</i></b>—Clear the packet and byte counts for the specified firewall filter.</p> <p><b>logical-system <i>logical-system-name</i></b>—Clear the packet and byte counts for the specified logical system.</p> <p><b>policer counter (all   counter-id <i>counter-index</i>)</b>—(EX8200 switches only) Clear all policer counters using the <b>policer counter all</b> command, or clear a specific policer counter using the <b>policer counter counter-id <i>counter-index</i></b> command. The value of <i>counter-index</i> can be 0, 1, or 2.</p>
<b>Required Privilege Level</b>	clear
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">show firewall on page 180</a></li> </ul>

**List of Sample Output**

- [clear firewall all on page 179](#)
- [clear firewall \(counter counter-name\) on page 179](#)
- [clear firewall \(filter filter-name\) on page 179](#)
- [clear firewall \(policer counter all\) \(EX8200 Switch\) on page 179](#)
- [clear firewall \(policer counter counter-id counter-index\) \(EX8200 Switch\) on page 179](#)

## Sample Output

**clear firewall all**                      user@host> clear firewall all

**clear firewall (counter  
counter-name)**                      user@host> clear firewall counter port-filter-counter

**clear firewall (filter  
filter-name)**                      user@host> clear firewall filter ingress-port-filter

**clear firewall (policer  
counter all) (EX8200  
Switch)**                      user@switch> clear firewall policer counter all

**clear firewall (policer  
counter counter-id  
counter-index)  
(EX8200 Switch)**                      user@switch> clear firewall policer counter counter-id 0

## show firewall

---

<b>Syntax</b>	<code>show firewall</code> <code>&lt;counter <i>counter-name</i>&gt;</code> <code>&lt;filter <i>filter-name</i>&gt;</code> <code>&lt;log&gt;</code> <code>&lt;logical-system (all   <i>logical-system-name</i>)&gt;</code> <code>&lt;terse&gt;</code>
<b>Syntax (EX Series Switches)</b>	<code>show firewall</code> <code>&lt;counter <i>counter-name</i>&gt;</code> <code>&lt;detail&gt;</code> <code>&lt;filter <i>filter-name</i>&gt;</code> <code>&lt;log &lt;(detail   interface <i>interface-name</i>)&gt;&gt;</code> <code>&lt;policer counters &lt;(detail   counter-id <i>counter-index</i> &lt;detail&gt;)&gt;&gt;</code> <code>&lt;terse&gt;</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. <b>logical-system</b> option introduced in Junos OS Release 9.3. <b>terse</b> option introduced in Junos OS Release 9.4. <b>policer counters</b> option introduced in Junos OS Release 12.2 for EX Series switches. <b>detail</b> option introduced in Junos OS Release 12.3.
<b>Description</b>	Display statistics about configured firewall filters.
<b>Options</b>	<p><b>none</b>—(Optional) Display statistics about all configured firewall filters and counters. For EX Series switches, this command also displays statistics about all configured policers.</p> <p><b>counter <i>counter-name</i></b>—(Optional) Name of a filter counter.</p> <p><b>detail</b>—(EX Series switches only) (Optional) Display firewall filter statistics with enhanced policer.</p> <p><b>filter <i>filter-name</i></b>—(Optional) Name of a configured filter.</p> <p><b>logical-system (all   <i>logical-system-name</i>)</b>—(Optional) Perform this operation on all logical systems or on a particular logical system.</p> <p><b>log</b>—(Optional) Display log entries for firewall filters.</p> <p><b>log &lt;(detail   interface <i>interface-name</i>)&gt;</b>—(EX Series switches only) (Optional) Display detailed log entries of firewall activity or log information about a specific interface.</p> <p><b>policer counters &lt;(detail   counter-id <i>counter-index</i> &lt;detail&gt;)&gt;</b>—(EX8200 switches only) (Optional) Display policer counter statistics in brief or in detail.</p> <p><b>terse</b>—(Optional) Display firewall filter names only.</p>
<b>Required Privilege Level</b>	view

- Related Documentation**
- [clear firewall on page 178](#)
  - [show firewall log on page 187](#)
  - [Verifying That Firewall Filters Are Operational on page 173](#)
  - [Verifying That Policers Are Operational on page 174](#)

- List of Sample Output**
- [show firewall filter \(MX Series\) on page 183](#)
  - [show firewall filter \(non MX Series Router\) on page 183](#)
  - [show firewall filter \(Hierarchical Policier, MX Series with MPC\) on page 183](#)
  - [show firewall filter \(Dynamic Input Filter\) on page 183](#)
  - [show firewall \(Logical Systems\) on page 183](#)
  - [show firewall \(counter counter-name\) on page 184](#)
  - [show firewall log on page 184](#)
  - [show firewall policer counters \(EX8200 Switch\) on page 184](#)
  - [show firewall policer counters \(detail\) \(EX8200 Switch\) on page 185](#)
  - [show firewall policer counters \(counter-id counter-index\) \(EX8200 Switch\) on page 185](#)
  - [show firewall policer counters \(counter-id counter-index detail\) \(EX8200 Switch\) on page 185](#)
  - [show firewall detail on page 186](#)

- Output Fields** [Table 31 on page 181](#) lists the output fields for the **show firewall** command. Output fields are listed in the approximate order in which they appear.

Table 31: show firewall Output Fields

Field Name	Field Description
<b>Filter</b>	<p>Name of a filter that has been configured with the <b>filter</b> statement at the <b>[edit firewall]</b> hierarchy level.</p> <p>Except on EX Series switches:</p> <ul style="list-style-type: none"> <li>• When an interface-specific filter is displayed, the name of the filter is followed by the full interface name and by either <b>-i</b> for an input filter or <b>-o</b> for an output filter.</li> <li>• When dynamic filters are displayed, the name of the filter is followed by the full interface name and by either <b>-in</b> for an input filter or <b>-out</b> for an output filter. When a logical system-specific filter is displayed, the name of the filter is prefixed with two underscore (__) characters and the name of the logical system (for example, <b>__ls1/filter1</b>).</li> </ul>
<b>Counters</b>	<p>Display filter counter information:</p> <ul style="list-style-type: none"> <li>• <b>Name</b>—Name of a filter counter that has been configured with the <b>counter</b> firewall filter action.</li> <li>• <b>Bytes</b>—Number of bytes that match the filter term under which the <b>counter</b> action is specified.</li> <li>• <b>Packets</b>—Number of packets that matched the filter term under which the <b>counter</b> action is specified.</li> </ul>

Table 31: show firewall Output Fields (*continued*)

Field Name	Field Description
<b>Policers</b>	<p>Display policer information:</p> <ul style="list-style-type: none"> <li>• <b>Name</b>—Name of policer.</li> <li>• <b>Bytes</b>—(For two-color policers on MX Series routers, and for hierarchical policers on interfaces hosted on MICs and MPCs in MX Series routers) Number of bytes that match the filter term under which the policer action is specified. This is only the number out-of-specification (out-of-spec) byte counts, not all the bytes in all packets policed by the policer. For other platforms, this field is blank.</li> <li>• <b>Packets</b>—Number of packets that matched the filter term under which the policer action is specified. This is only the number of out-of-specification (out-of-spec) packet counts, not all packets policed by the policer.</li> </ul>
<b>Policer Counter Index</b>	(EX8200 switch only) Global management counter ID. The counter ID value ( <i>counter-index</i> ) can be 0, 1, or 2.
<b>Green</b>	(EX8200 switch only) Number of packets within the limits. The number of packets is smaller than the committed information rate (CIR).
<b>Yellow</b>	(EX8200 switch only) Number of packets partially within the limits. The number of packets is greater than the CIR, but the burst size is within the excess burst size (EBS) limit.
<b>Discard</b>	(EX8200 switch only) Number of discarded packets.
<b>Bytes</b>	(EX8200 switch only) Number of green, yellow, red, or discarded packets in bytes.
<b>Packets</b>	(EX8200 switch only) Number of green, yellow, red, or discarded packets.
<b>Filter name</b>	(EX8200 switch only) Name of the filter with a term associated to a policer.
<b>Term name</b>	(EX8200 switch only) Name of the term associated with a policer.
<b>Policer name</b>	(EX8200 switch only) Name of the policer that is associated with a global management counter.

## Sample Output

### show firewall filter (MX Series)

```
user@host> show firewall filter test
Filter: test
Counters:
Name                               Bytes          Packets
Counter-1                          0              0
Counter-2                          0              0
Policers:
Name                               Bytes          Packets
Policer-1                         2770           70
```

### show firewall filter (non MX Series Router)

```
user@host> show firewall filter test
Filter: test
Counters:
Name                               Bytes          Packets
Counter-1                          0              0
Counter-2                          0              0
Policers:
Name                               Bytes          Packets
Policer-1                         70
```

### show firewall filter (Hierarchical Policer, MX Series with MPC)

```
user@host> show firewall filter
FL_V4_PHY-HP-EF-AWARE-Gold=400k-MCAST=200k-Total=1M-ds-10/0/0:2:1-i

Filter: FL_V4_PHY-HP-EF-AWARE-Gold=400k-MCAST=200k-Total=1M-ds-10/0/0:2:1-i
Counters:
Name                               Bytes          Packets
AF1x_counter-ds-10/0/0:2:1-i      0              0
AF2x_counter-ds-10/0/0:2:1-i      25529445976    24500428
AF3x_counter-ds-10/0/0:2:1-i      2182022        39482
AF4x_counter-ds-10/0/0:2:1-i      0              0
BE_counter-ds-10/0/0:2:1-i        0              0
EF_counter-ds-10/0/0:2:1-i        14817044120    12265765
STD_counter-ds-10/0/0:2:1-i       0              0
Policers:
Name                               Bytes          Packets
POL_CE-PE_M=200k-filter-ds-10/0/0:2:1-i 5948099658     5708349
POL_CE-PE_G=400K_R=1M-filter-ds-10/0/0:2:1-i ??????????    3572794
???????????????????????????????????????? ??????????    ????????
```

### show firewall filter (Dynamic Input Filter)

```
user@host> show firewall filter dfwd-ge-5/0/0.1-in
Filter: dfwd-ge-5/0/0.1-in
Counters:
Name                               Bytes          Packets
c1-ge-5/0/0.1-in                  0              0
```

### show firewall (Logical Systems)

```
user@host> show firewall

Filter: __lr1/test
Counters:
Name                               Bytes          Packets
icmp                              420            5
Filter: __default_bpdu_filter__
```

```

Filter: __lr1/inet_filter1
Counters:
Name                               Bytes      Packets
inet_tcp_count                     0           0
inet_udp_count                     0           0
Filter: __lr1/inet_filter2
Counters:
Name                               Bytes      Packets
inet_icmp_count                    0           0
inet_pim_count                     0           0
Filter: __lr2/inet_filter1
Counters:
Name                               Bytes      Packets
inet_tcp_count                     0           0
inet_udp_count                     0           0

```

#### show firewall (counter counter-name)

```

user@host> show firewall counter icmp-counter
Filter: ingress-port-voip-class-filter
Counters:
Name                               Bytes      Packets
icmp-counter                       0           0

```

#### show firewall log

```

user@host> show firewall log
Log :

Time      Filter  Action Interface  Protocol  Src Addr
Dest Addr
08:00:53  pfe      R      ge-1/0/1.0    ICMP      192.168.3.5
192.168.3.4
08:00:52  pfe      R      ge-1/0/1.0    ICMP      192.168.3.5
192.168.3.4
08:00:51  pfe      R      ge-1/0/1.0    ICMP      192.168.3.5
192.168.3.4
08:00:50  pfe      R      ge-1/0/1.0    ICMP      192.168.3.5
192.168.3.4
08:00:49  pfe      R      ge-1/0/1.0    ICMP      192.168.3.5
192.168.3.4
08:00:48  pfe      R      ge-1/0/1.0    ICMP      192.168.3.5
192.168.3.4
08:00:47  pfe      R      ge-1/0/1.0    ICMP      192.168.3.5
192.168.3.4

```

#### show firewall policer counters (EX8200 Switch)

```

user@switch> show firewall policer counters
Policer Counter Index 0:
Bytes      Packets
Green:      73      15914
Yellow:      9      1962
Discard:    119     25942

Policer Counter Index 1:
Bytes      Packets
Green:      0       0
Yellow:      0       0
Discard:      0       0

Policer Counter Index 2:
Bytes      Packets

```



Green:	0	0
Yellow:	0	0
Discard:	0	0

**show firewall policer  
counters (detail)  
(EX8200 Switch)**

user@switch> **show firewall policer counters detail**

Policer Counter Index 0:

	Bytes	Packets
Green:	73	15914
Yellow:	9	1962
Discard:	119	25942

Filter name	Term name	Policer name
myfilter	polcr-term-1	myfilter-polcr-1
inet-filter-ae	ae-snmp	policer-1
inet-filter-ae	ae-ssh	policer-2

Policer Counter Index 1:

	Bytes	Packets
Green:	0	0
Yellow:	0	0
Discard:	0	0

Filter name	Term name	Policer name
-------------	-----------	--------------

Policer Counter Index 2:

	Bytes	Packets
Green:	0	0
Yellow:	0	0
Discard:	0	0

Filter name	Term name	Policer name
-------------	-----------	--------------

**show firewall policer  
counters (counter-id  
counter-index)  
(EX8200 Switch)**

user@switch> **show firewall policer counters counter-id 0**

Policer Counter Index 0:

	Bytes	Packets
Green:	73	15914
Yellow:	9	1962
Discard:	119	25942

**show firewall policer  
counters (counter-id**

user@switch> **show firewall policer counters counter-id 0 detail**

Policer Counter Index 0:

Bytes	Packets
-------	---------

**counter-index detail**  
**(EX8200 Switch)**

Green:	73	15914
Yellow:	9	1962
Discard:	119	25942

Filter name	Term name	Policer name
myfilter	polcr-term-1	myfilter-polcr-1
inet-filter-ae	ae-snmp	policer-1
inet-filter-ae	ae-ssh	policer-2

**show firewall detail**

```
user@host> show firewall detail
Filter: __default_bpdu_filter__

Filter: foo
Counters:
Name                               Bytes          Packets
c1                                  17652140       160474
Policers:
Name                               Bytes          Packets
P1-t1
  OOS                               0              18286
  Offered                           0 18446744073709376546
  Transmitted                       0 18446744073709358260
```

## show firewall log

<b>Syntax</b>	show firewall log <detail> <interface <i>interface-name</i> > <logical-system ( <i>logical-system-name</i>   all)>
<b>Syntax (EX Series Switches)</b>	show firewall log <detail> <interface <i>interface-name</i> >
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. <b>logical-system</b> option introduced in Junos OS Release 9.3.
<b>Description</b>	Display log information about firewall filters.
<b>Options</b>	<p><b>none</b>—Display log information about firewall filters.</p> <p><b>detail</b>—(Optional) Display detailed information.</p> <p><b>interface <i>interface-name</i></b>—(Optional) Display log information about a specific interface.</p> <p><b>logical-system (<i>logical-system-name</i>   all)</b>—(Optional) Perform this operation on all logical systems or on a particular system.</p>
<b>Required Privilege Level</b>	view
<b>List of Sample Output</b>	<a href="#">show firewall log on page 189</a> <a href="#">show firewall log detail on page 189</a>
<b>Output Fields</b>	Table 32 on page 187 lists the output fields for the <b>show firewall log</b> command. Output fields are listed in the approximate order in which they appear.

**Table 32: show firewall log Output Fields**

Field Name	Field Description
<b>Time of Log</b>	Time that the event occurred.
<b>Filter</b>	<p>Name of a filter that has been configured with the <b>filter</b> statement at the <b>[edit firewall]</b> hierarchy level.</p> <ul style="list-style-type: none"> <li>A hyphen (-) indicates that the packet was handled by the Packet Forwarding Engine.</li> <li>A space (no hyphen) indicates the packet was handled by the Routing Engine.</li> <li>The notation <b>pfe</b> indicates packets logged by the Packet Forwarding Engine hardware filters.</li> </ul>

Table 32: show firewall log Output Fields (*continued*)

Field Name	Field Description
Filter Action	Filter action: <ul style="list-style-type: none"><li>• A—Accept</li><li>• D—Discard</li><li>• R—Reject</li></ul>
Name of Interface	Ingress interface for the packet.
Name of protocol	Packet's protocol name: <b>egp</b> , <b>gre</b> , <b>icmp</b> , <b>ipip</b> , <b>ospf</b> , <b>pim</b> , <b>rsvp</b> , <b>tcp</b> , or <b>udp</b> .
Packet length	Length of the packet.
Source address	Packet's source address.
Destination address	Packet's destination address and port.

## Sample Output

### show firewall log

```
user@host>show firewall log
```

Time	Filter	Action	Interface	Protocol	Src Addr	Dest Addr
13:10:12	pfe	D	rlsq0.902	ICMP	180.1.177.2	180.1.177.1
13:10:11	pfe	D	rlsq0.902	ICMP	180.1.177.2	180.1.177.1

### show firewall log detail

```
user@host> show firewall log detail
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0Name of protocol: TCP, Packet Length: 50824, Source address:
172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0
Name of protocol: TCP, Packet Length: 1020, Source address: 172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 172.17.22.108:829,
Destination address: 192.168.70.66:513
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 172.17.22.108:829,
Destination address: 192.168.70.66:513
....
```

## show policer

<b>Syntax</b>	<b>show policer</b> <b>&lt;policer-name&gt;</b>
<b>Release Information</b>	Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Display statistics about configured policers.
<b>Options</b>	<b>none</b> —Display the count of policed packets for all configured policers in the system. <b>policer-name</b> —(Optional) Display the count of policed packets for the specified policer.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75</a></li> <li>• <a href="#">Verifying That Firewall Filters Are Operational on page 173</a></li> <li>• <a href="#">Verifying That Policers Are Operational on page 174</a></li> <li>• <a href="#">Firewall Filters for EX Series Switches Overview on page 7</a></li> <li>• <a href="#">Understanding the Use of Policers in Firewall Filters on page 66</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show policer on page 191</a> <a href="#">show policer (policer-name) on page 191</a>
<b>Output Fields</b>	<a href="#">Table 33 on page 190</a> lists the output fields for the <b>show policer</b> command. Output fields are listed in the approximate order in which they appear.

**Table 33: show policer Output Fields**

Field Name	Field Description	Level of Output
<b>Filter</b>	Name of filter that is configured with the <b>filter</b> statement at the <b>[edit firewall]</b> hierarchy level.	All levels
<b>Policers</b>	Display policer information: <ul style="list-style-type: none"> <li>• <b>Filter</b>—Name of filter that specifies the policer action.</li> <li>• <b>Name</b>—Name of policer.</li> <li>• <b>Packets</b>—Number of packets that matched the filter term where the policer action is specified. This is the number of packets that exceed the rate limits that the policer specifies.</li> </ul>	All levels

## Sample Output

`show policer`

```
user@host> show policer
Filter: egress-vlan-filter
Filter: ingress-port-filter
Policers:
Name                                     Packets
icmp-connection-policer                 0
tcp-connection-policer                  0
Filter: ingress-vlan-rogue-block
```

`show policer`  
`(policer-name)`

```
user@host> show policer tcp-connection-policer
Filter: ingress-port-filter
Policers:
Name                                     Packets
tcp-connection-policer                  0
```

## show policy

<b>Syntax</b>	show policy <logical-system (all   <i>logical-system-name</i> )> < <i>policy-name</i> >
<b>Syntax (EX Series Switches)</b>	show policy < <i>policy-name</i> >
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Display information about configured routing policies.
<b>Options</b>	<p><b>none</b>—List the names of all configured routing policies.</p> <p><b>logical-system (all   <i>logical-system-name</i>)</b>—(Optional) Perform this operation on all logical systems or on a particular logical system.</p> <p><b><i>policy-name</i></b>—(Optional) Show the contents of the specified policy.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>show policy damping</li> </ul>
<b>List of Sample Output</b>	<a href="#">show policy on page 193</a> <a href="#">show policy policy-name on page 193</a> <a href="#">show policy (Multicast Scoping) on page 193</a>
<b>Output Fields</b>	Table 34 on page 192 lists the output fields for the <b>show policy</b> command. Output fields are listed in the approximate order in which they appear.

**Table 34: show policy Output Fields**

Field Name	Field Description
<i>policy-name</i>	Name of the policy listed.
<i>term</i>	Policy term listed.
<i>from</i>	Match condition for the policy.
<i>then</i>	Action for the policy.



## Sample Output

**show policy**

```
user@host> show policy
Configured policies:
__vrf-export-red-internal__
__vrf-import-red-internal__
red-export
all_routes
```

**show policy  
policy-name**

```
user@host> show policy test-statics
Policy test-statics:
  from
    3.0.0.0/8  accept
    3.1.0.0/16  accept
  then reject
```

**show policy (Multicast  
Scoping)**

```
user@host> show policy test-statics
Policy test-statics:
  from
    multicast-scoping == 8
```

## show policy conditions

<b>Syntax</b>	<pre>show policy conditions &lt;condition-name&gt; &lt;detail&gt; &lt;dynamic&gt; &lt;logical-system (all   logical-system-name)&gt;</pre>
<b>Syntax (EX Series Switches)</b>	<pre>show policy conditions &lt;condition-name&gt; &lt;detail&gt; &lt;dynamic&gt;</pre>
<b>Release Information</b>	<p>Command introduced in Junos OS Release 9.0.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p>
<b>Description</b>	<p>Display all the configured conditions as well as the routing tables with which the configuration manager is interacting. If the <b>detail</b> keyword is included, the output also displays dependent routes for each condition.</p>
<b>Options</b>	<p><b>none</b>—Display all configured conditions and associated routing tables.</p> <p><b>condition-name</b>—(Optional) Display information about the specified condition only.</p> <p><b>detail</b>—(Optional) Display the specified level of output.</p> <p><b>dynamic</b>—(Optional) Display information about the conditions in the dynamic database.</p> <p><b>logical-system (all   logical-system-name)</b>—(Optional) Perform this operation on all logical systems or on a particular logical system.</p>
<b>Required Privilege Level</b>	view
<b>List of Sample Output</b>	<a href="#">show policy conditions detail on page 195</a>
<b>Output Fields</b>	<p><a href="#">Table 35 on page 194</a> lists the output fields for the <b>show policy conditions</b> command. Output fields are listed in the approximate order in which they appear.</p>

**Table 35: show policy conditions Output Fields**

Field Name	Field Description	Level of Output
<b>Condition</b>	Name of configured condition.	All levels
<b>event</b>	Condition type. If the <b>if-route-exists</b> option is configured, the event type is: <b>Existence of a route in a specific routing table.</b>	All levels
<b>Dependent routes</b>	List of routes dependent on the condition, along with the latest generation number.	<b>detail</b>
<b>Condition tables</b>	List of routing tables associated with the condition, along with the latest generation number and number of dependencies.	All levels

Table 35: show policy conditions Output Fields (*continued*)

Field Name	Field Description	Level of Output
If-route-exists conditions	List of conditions configured to look for a route in the specified table.	All levels

## Sample Output

```
show policy conditions detail user@host> show policy conditions detail
Configured conditions:
Condition cond1, event: Existence of a route in a specific routing table
Dependent routes:
  4.4.4.4/32, generation 3
  6.6.6.6/32, generation 3
  10.10.10.10/32, generation 3

Condition cond2, event: Existence of a route in a specific routing table
Dependent routes:
None

Condition tables:
Table inet.0, generation 4, dependencies 3, If-route-exists conditions: cond1
(static) cond2 (static)
```

## test policy

---

<b>Syntax</b>	<code>test policy <i>policy-name</i> <i>prefix</i></code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Test a policy configuration to determine which prefixes match routes in the routing table.
<b>Options</b>	<i>policy-name</i> —Name of a policy. <i>prefix</i> —Destination prefix to match.
<b>Additional Information</b>	All prefixes in the default unicast routing table (inet.0) that match prefixes that are the same as or longer than the specific prefix are processed by the <b>from</b> clause in the specified policy. All prefixes accepted by the policy are displayed. The <b>test policy</b> command evaluates a policy differently from the BGP import process. When testing a policy that contains an <b>interface</b> match condition in the <b>from</b> clause, the <b>test policy</b> command uses the match condition. In contrast, BGP does not use the <b>interface</b> match condition when evaluating the policy against routes learned from internal BGP (IBGP) or external BGP (EGBP) multihop peers.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• show policy damping</li></ul>
<b>List of Sample Output</b>	<a href="#">test policy on page 197</a>
<b>Output Fields</b>	For information about output fields, see the output field tables for the show route command, the show route detail command, the show route extensive command, or the show route terse command.

## Sample Output

### test policy

```
user@host> test policy test-statics 3.0.0.1/8
inet.0: 44 destinations, 44 routes (44 active, 0 holddown, 0 hidden)
Prefixes passing policy:

3.0.0.0/8      *[BGP/170] 16:22:46, localpref 100, from 10.255.255.41
               AS Path: 50888 I
               > to 10.11.4.32 via en0.2, label-switched-path l2
3.3.3.1/32     *[IS-IS/18] 2d 00:21:46, metric 0, tag 2
               > to 10.0.4.7 via fxp0.0
3.3.3.2/32     *[IS-IS/18] 2d 00:21:46, metric 0, tag 2
               > to 10.0.4.7 via fxp0.0
3.3.3.3/32     *[IS-IS/18] 2d 00:21:46, metric 0, tag 2
               > to 10.0.4.7 via fxp0.0
3.3.3.4/32     *[IS-IS/18] 2d 00:21:46, metric 0, tag 2
               > to 10.0.4.7 via fxp0.0
Policy test-statics: 5 prefixes accepted, 0 prefixes rejected
```



## PART 4

# Troubleshooting

- [Troubleshooting Procedures on page 201](#)





## CHAPTER 8

# Troubleshooting Procedures

- [Troubleshooting Firewall Filters on page 201](#)

## Troubleshooting Firewall Filters

---

Troubleshooting issues with firewall filters on EX Series switches:

1. [A Firewall Filter Configuration Returns a “No Space Available in TCAM” Message on page 201](#)

### A Firewall Filter Configuration Returns a “No Space Available in TCAM” Message

**Problem** When a firewall filter configuration exceeds the amount of available ternary content addressable memory (TCAM) space, the switch returns the following system log (**syslogd**) message:

```
No space available in tcam.  
Rules for filter filter-name will not be installed.
```

The switch returns this error message during the commit operation in the following instances:

- If the firewall filter that you have applied to a port, VLAN, or Layer 3 interface requires more than the amount of available TCAM space.
- If you delete and add large firewall filters in the same commit operation. In this case, the large firewall filter might not be deleted from the TCAM space, because of which there will be no TCAM space freed up for the new firewall filter to be added to it. In addition to the **syslogd** message, the following error message is displayed in the CLI:

```
fpc<device-id> dfw_grph_merge_dfw_bind: rules for filter filter-name will not  
be installed
```

However, in both these instances, the commit operation for the firewall filter configuration is completed in the CLI.

**Solution** When a firewall filter configuration exceeds the amount of available TCAM table space, you must configure a new firewall filter with fewer filter terms or, if you had deleted and created a firewall filter with a large number of terms (on the order of 1000 or more), you must delete and add the large firewall filters in separate commit operations.

The first procedure (set of steps) in this Solution section tells you how to delete a firewall filter and its bind point and associate a new firewall filter with that existing bind point.

The second procedure in this Solution section tells you how to create a new firewall filter with fewer terms (without deleting the bind point) and bind the new firewall filter with the existing bind point, when you want to create a firewall filter with fewer terms. Do not use the second procedure if you need to replace one large firewall filter with another large firewall filter—you must delete the original large firewall filter and commit that delete operation, and then add the new large firewall filter.

To delete the firewall filter and its bind point and apply a new firewall filter to the same bind point:

1. Delete the firewall filter configuration and its bind points to ports, VLANs, or Layer 3 interfaces—for example:

```
[edit]
user@switch# delete firewall family ethernet-switching filter mini-filter-ingress-vlan
user@switch# delete vlans voice-vlan description "filter to block rogue devices on voice-vlan"
user@switch# delete vlans voice-vlan filter input mini-filter-ingress-vlan
```

2. Commit the operation:

```
[edit]
user@switch# commit
```



**NOTE:** Use separate commit operations for deleting and adding large firewall filters.

3. Configure a firewall filter with fewer terms (if the error message appeared when you tried to create a new filter) or configure a large filter (if the error message appeared when you tried to delete and add large firewall filters)—for example:

```
[edit]
user@switch# set firewall family ethernet-switching filter new-filter-ingress-vlan ...
```



**NOTE:** See [“Firewall Filters for EX Series Switches Overview”](#) on page 7 to ascertain the maximum number of terms allowed for various firewall filters on EX Series switches.

4. Apply (bind) the new firewall filter to a port, VLAN , or Layer 3 interface—for example:

```
[edit]
user@switch# set vlans voice-vlan description "filter to block rogue devices on voice-vlan"
user@switch# set vlans voice-vlan filter input new-filter-ingress-vlan
```

5. Commit the operation:

```
[edit]
user@switch# commit
```

To create a new firewall filter and attach it to the existing bind point:

1. Configure a firewall filter with fewer terms than the original filter:

```
[edit]
user@switch# set firewall family ethernet-switching filter new-filter-ingress-vlan...
```

2. Apply the firewall filter to the port, VLAN, or Layer 3 interfaces to overwrite the bind points of the original filter—for example:

```
[edit]
user@switch# set vlans voice-vlan description "smaller filter to block rogue devices on voice-vlan"
user@switch# set vlans voice-vlan filter input new-filter-ingress-vlan
```

As a bind point can be attached to only one firewall filter, this configuration detaches the bind point from the previous firewall filter that contained many terms and attaches the bind point to the new firewall filter.

3. Commit the operation:

```
[edit]
user@switch# commit
```

#### Related Documentation

- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 75](#)
- [Verifying That Firewall Filters Are Operational on page 173](#)
- [Configuring Firewall Filters \(CLI Procedure\) on page 107](#)
- [Configuring Firewall Filters \(J-Web Procedure\) on page 115](#)

