Security Feature Guide for the OCX Series

Release
14.1X53-D20

Modified: 2015-08-12

Copyright © 2015, Juniper Networks, Inc.

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

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.

Security Feature Guide for the OCX Series
14.1X53-D20
Copyright © 2015, 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

Copyright © 2015, Juniper Networks, Inc.

Copyright © 2015, Juniper Networks, Inc.

Copyright © 2015, Juniper Networks, Inc.

Copyright © 2015, Juniper Networks, Inc.

List of Figures

Copyright © 2015, Juniper Networks, Inc.

Copyright © 2015, Juniper Networks, Inc.

List of Tables

Copyright © 2015, Juniper Networks, Inc.

Copyright © 2015, Juniper Networks, Inc.

About the Documentation

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.

Supported Platforms

For the features described in this document, the following platforms are supported:

- OCX1100

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.

Copyright © 2015, Juniper Networks, Inc.

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.xsl;
       }
     }
   }
   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.xsl; }
   ```

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

Copyright © 2015, Juniper Networks, Inc.

```
[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.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**

Copyright © 2015, Juniper Networks, Inc.

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

Convention	Description	Examples
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric** ***metric*****>;**
| (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.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.

Copyright © 2015, Juniper Networks, Inc.

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

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at https://www.juniper.net/cgi-bin/docbugreport/.
- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software 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 Partner Support Service 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/

Copyright © 2015, Juniper Networks, Inc.

- 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: http://kb.juniper.net/InfoCenter/
- 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.

Copyright © 2015, Juniper Networks, Inc.

PART 1

Firewall Filters

Copyright © 2015, Juniper Networks, Inc.

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 1

Using Firewall Filters

Overview of Firewall Filters

Firewall filters provide rules that define whether to accept or discard packets that are transiting an interface. If a packet is accepted, you can configure additional actions to perform on the packet, such as 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). You configure firewall filters to determine whether to accept or discard a packet before it enters or exits a Layer 3 (routed) interface.

An *ingress* firewall filter is applied to packets that are entering an interface, and an *egress* firewall filter is applied to packets that are exiting an interface .

NOTE: Firewall filters are sometimes called *access control lists* (ACLs).

Copyright © 2015, Juniper Networks, Inc.

Where You Can Apply Filters

You can apply a router firewall filter in both ingress and egress directions on IPv4 or IPv6 Layer 3 (routed) interfaces and a loopback interface, which filters traffic sent to the switch itself or generated by the switch.

You apply a filter to a loopback interface in the input direction to protect the switch from unwanted traffic. You also might want to apply a filter to a loopback interface in the output direction so that you can set the forwarding class and DSCP bit value for packets that originate on the switch itself. This feature gives you very fine control over the classification of CPU generated packets. For example, you might want to assign different DSCP values and forwarding classes to traffic generated by different routing protocols so the traffic for those protocols can be treated in a differentiated manner by other devices.

NOTE: If you apply ingress and egress filters to the same interface, the ingress filter is processed first.

To apply a firewall filter:

1. Configure the firewall filter.
2. Apply the firewall filter to a Layer 3 interface and specify the direction. If you specify the **input** direction, traffic is filtered on ingress. If you specify the **output** direction, traffic is filtered on egress.

NOTE: You can apply only one firewall filter to a Layer 3 interface for a given direction. For example, for a given family inet interface, you can apply one filter for input and one for output.

OCX switches support the maximum numbers of firewall filter terms per type of attachment point shown in Table 3 on page 4.

Table 3: Supported Firewall Filter Numbers

Filter Type	Maximum Number of Filters
Ingress	1536
Egress	1024

Firewall Filter Components

In a firewall filter, you first define the family address type (**inet** for IPv4 or **inet6** for IPv6) and then define one or more terms that specify the filtering criteria and the action to take if a match occurs.

Copyright © 2015, Juniper Networks, Inc.

Each term consists of the following components:

- Match conditions—Specify values that a packet must contain to be considered a match.
- Action—Specifies what to do if a packet matches the match conditions. A filter can accept, discard, or reject a matching packet and then perform additional actions, such as counting, classifying, and policing. If no action is specified for a term, the default is to accept the matching packet.

Firewall Filter Processing

If there are multiple terms in a filter, the order of the terms is important. If a packet matches the first term, the switch executes the action defined by that term, and no other terms are evaluated. If the switch does not find a match between the packet and the first term, it compares the packet to the next term. If no match occurs between the packet and the second term, the system continues to compare the packet to each successive term in the filter until a match is found. If the packet does not match any terms in the filter, the switch discards the packet by default.

Related Documentation

- Understanding Firewall Filter Planning on page 29
- *Understanding Firewall Filter Processing Points for Bridged and Routed Packets*
- Understanding How Firewall Filters Are Evaluated on page 5
- Understanding Firewall Filter Match Conditions on page 8
- Overview of Policers on page 41
- *Configuring Firewall Filters*

Understanding How Firewall Filters Are Evaluated

A firewall filter consists of one or more terms, and the order of the terms within a filter is important. Before you configure firewall filters, you should understand how switches evaluate the terms within a 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.
- If the packet does not match all the conditions, the switch discards it.

When a firewall filter consists of more than one term, the 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.

Copyright © 2015, Juniper Networks, Inc.

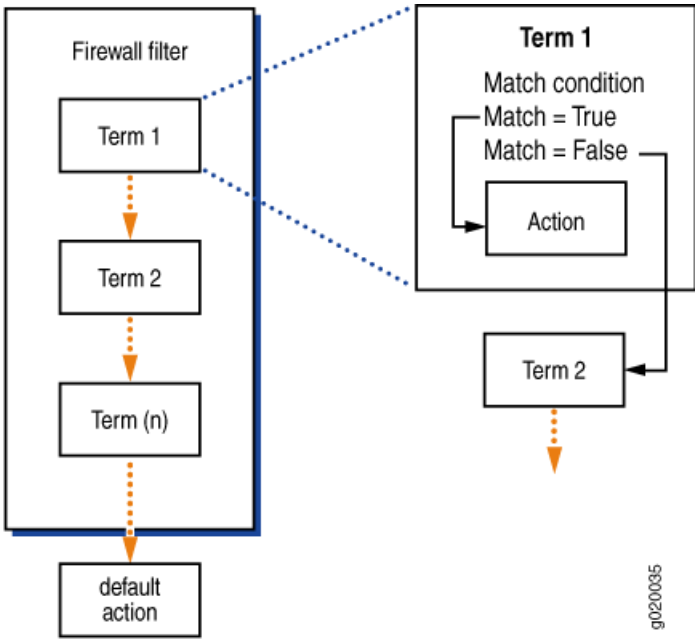
This process continues until the packet matches all the conditions in the **from** statement in one of the subsequent terms or there are no more terms in the filter.

4. If a packet passes through all the terms in the filter without a match, the switch discards it.

NOTE: The order of conditions in a **from** statement is not important because a packet must match all the conditions to be considered a match.

Figure 1 on page 6 shows how switches evaluate the terms within a firewall filter.

Figure 1: Evaluation of Terms Within a Firewall Filter



If you do not include a **from** statement in a term, all packets will match the term and be processed by the **then** statement. If a term does not contain a **then** statement or if an action has not been configured in the **then** statement, the term accepts any matching packets.

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, a packet that does not match any of the terms in a firewall filter is discarded. If you configure a filter that has no terms, all packets that pass through the filter are discarded.

Copyright © 2015, Juniper Networks, Inc.

NOTE: Firewall filtering is supported on packets that are at least 64 bytes long.

Related Documentation

- *Understanding Firewall Filter Match Conditions*
- Overview of Policers on page 41
- *Configuring Firewall Filters*

Understanding How Firewall Filters Control Packet Flows

A switch supports firewall filters that allow you to control flows of data packets and local packets. *Data packets* transit a switch as they are forwarded from a source to a destination. *Local packets* are destined for or sent by a Routing Engine (they do not transit a switch). Local packets usually contain routing protocol data, data for IP services such as Telnet or SSH, or data for administrative protocols such as the Internet Control Message Protocol (ICMP).

Firewall filters affect packet flows entering into or exiting from a switch as follows:

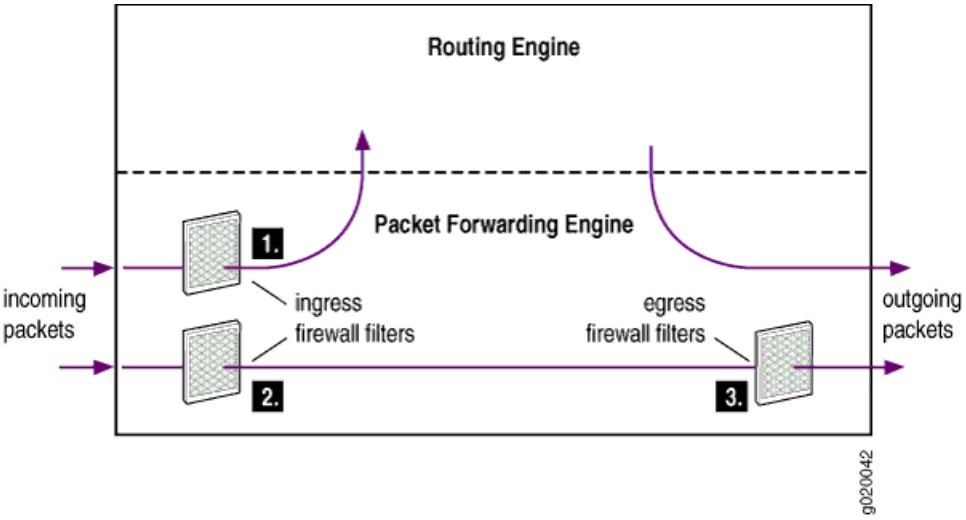
- Ingress firewall filters affect the flow of data packets that are received on switch interfaces. When a switch receives a data packet, the Packet Forwarding Engine in the system that contains the ingress interface determines where to forward the packet by looking in its Layer 2 or Layer 3 forwarding table for the best route to the destination. Data packets are forwarded to an egress interface. Locally destined packets are forwarded to the Routing Engine.
- Egress firewall filters affect data packets that are transiting a switch but do not affect packets sent by the Routing Engine. These filters are applied by the Packet Forwarding Engine in the system that contains the egress interface.

Figure 2 on page 8 illustrates the application of ingress and egress firewall filters to control the flow of packets through a switch:

1. Ingress firewall filter applied to locally destined packets that are received on switch interfaces and are destined for the Routing Engine.
2. Ingress firewall filter applied to data packets that are received on switch interfaces and will transit the switch.
3. Egress firewall filter applied to data packets that are transiting the switch.

Copyright © 2015, Juniper Networks, Inc.

Figure 2: Application of Firewall Filters to Control Packet Flow



Related Documentation

- *Understanding Firewall Filter Processing Points for Bridged and Routed Packets*
- Understanding How Firewall Filters Are Evaluated on page 5
- *Configuring Firewall Filters*

Understanding Firewall Filter Match Conditions

Before you define terms for firewall filters, you must understand how the conditions in a term are handled and how to specify interface, numeric, address, and bit-field filter match conditions to achieve the desired filter results.

- Filter Match Conditions on page 8
- Numeric Filter Match Conditions on page 9
- Interface Filter Match Conditions on page 9
- IP Address Filter Match Conditions on page 10
- Bit-Field Filter Match Conditions on page 10

Filter Match Conditions

In the **from** statement of a firewall filter term, you specify the conditions that the packet must match for the action in the **then** statement to be taken. All conditions must match for the action to be implemented. 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 multiple values for the same condition, a match on any one of those values matches that condition. For example, if you specify multiple IP source addresses using the **source-address** statement, a packet that contains any one of those IP source addresses matches the condition. In some cases you can specify multiple values for the same condition by enclosing the possible values in square brackets, as in:

```
[edit firewall family family-name filter filter-name term term-name from]
```


Copyright © 2015, Juniper Networks, Inc.

```
user@switch# set protocol (icmp | udp)
```

In other cases you must enter multiple statements, as in:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set source-address 10.1.1.1
user@switch# set source-address 10.1.1.2
```

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

NOTE: Unlike traditional Junos OS firewall filters, you cannot use except in a condition statement to negate the condition.

Numeric Filter Match Conditions

You can specify numeric filter match conditions that are identified by a numeric value, such as port and protocol numbers. For numeric filter match conditions, you specify the condition and a single value that a field in a packet must contain to be considered a 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, to match Telnet traffic:

  ```
  [edit firewall family family-name filter filter-name term term-name from]
  user@switch# set source-port 23
  ```

- 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, to match Telnet traffic:

  ```
  [edit firewall family family-name filter filter-name term term-name from]
  user@switch# set source-port telnet
  ```

- To specify multiple values for the same match condition in a filter term, enter each value in its own match statement. For example, a match occurs in the following term if the value of the source port in the packet is 22 or 23.

  ```
  [edit firewall family family-name filter filter-name term term-name from]
  user@switch# set source-port 22
  user@switch# set source-port 23
  ```

Interface Filter Match Conditions

You can specify an interface filter match condition to match an interface on which a packet is received or transmitted. In this example, the final character (**0**) specifies the logical unit. 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/*/6.0
user@switch# set interface ge-0/1/*0
user@switch# set interface ge-0/0/6.*
```

Note that you must specify a value or a wildcard for the logical unit.

Copyright © 2015, Juniper Networks, Inc.

IP Address Filter Match Conditions

You can specify an address filter match condition to match an IP source or destination address or prefix in a packet. Specify the address or prefix type and the address or prefix itself. For example:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set destination-address 10.2.1.0/24;
```

If you omit the 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 or prefix in a filter term, enter each address or prefix in its own match statement. For example, a match occurs in the following term if the source address of a packet matches either of the following prefixes:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set source-address 10.1.0.0/16
user@switch# set source-address 10.2.0.0/16
```

Bit-Field Filter Match Conditions

You can specify bit-field filter match conditions to match particular bits within certain fields in Ethernet frames and IP, TCP, UDP, and ICMP headers. You usually specify the field and the bit within the field that must be set in a packet to be considered a match.

In most cases you can use a keyword to specify the bit you want to match on. For example, to match on a TCP SYN packet you can enter **syn**, as in:

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

You can also enter **0x02** because the SYN bit is the third least-significant bit of the 8-bit tcp-flags field:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-flags 0x02
```

To match multiple bit-field values, use the logical operators, which are described in Table 4 on page 10. The operators are listed in order from highest precedence to lowest precedence. Operations are evaluated from left to right.

Table 4: Actions for Firewall Filters

Logical Operators	Description
!	Negation
&	Logical AND
|	Logical OR

Copyright © 2015, Juniper Networks, Inc.

If you use a logical operator, enclose the values in quotation marks and do not include any spaces. For example, the following statement matches the second packet of a TCP handshake:

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

To negate a match, precede the value with an exclamation point. For example, the following statement matches only the initial packet of a TCP handshake:

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

You can use text synonyms to specify some common bit-field matches. For example, the following statement also matches the initial packet of a TCP handshake:

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

Related Documentation

- Understanding How a Firewall Filter Tests a Protocol on page 29
- Firewall Filter Match Conditions and Actions on page 11
- *Configuring Firewall Filters*

Firewall Filter Match Conditions and Actions

Each term in a firewall filter consists of *match conditions* and an *action*. Match conditions are the fields and values that a packet must contain to be considered a match. You can define single or multiple match conditions in *match statements*. You can also include no match statement, in which case the term matches all packets.

When a packet matches a filter, a switch takes the action specified in the term. In addition, you can specify action modifiers to count, mirror, rate-limit, and classify packets. If no match conditions are specified for the term, the switch accepts the packet by default.

This topic describes the various match conditions, actions, and action modifiers that you can define in a firewall filter.

- Table 5 on page 12 describes the match conditions you can specify when configuring a firewall filter. Some of the numeric range and bit-field match conditions allow you to specify a text synonym. To see a list of all the synonyms for a match condition, type **?** at the appropriate place in a statement.
- Table 6 on page 25 shows the actions that you can specify in a term.
- Table 7 on page 26 shows the action modifiers you can use to count, mirror, rate-limit, and classify packets.

NOTE: On switches that do not support Layer 2 features (such as the OCX1100), you can use only those match conditions that are valid for IPv4 and IPv6 interfaces.

Copyright © 2015, Juniper Networks, Inc.

Table 5: Supported Match Conditions for Firewall Filters

Match Condition	Description	Direction and Interface
arp-type	ARP request packet or ARP reply packet.	Egress and ingress ports.
destination-address *ip-address*	IP destination address field, which is the address of the final destination node.	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces, and IPv6 (inet6) interfaces.
destination-mac-address *mac-address*	Destination media access control (MAC) address of the packet.	Ingress ports, VLANs and IPv4 (inet) interfaces. Egress ports and VLANs.

Copyright © 2015, Juniper Networks, Inc.

Table 5: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
destination-port *value*	TCP or UDP destination port field. Typically, you specify this match in conjunction with the **protocol** match statement. For the following well-known ports you can specify text synonyms (the port numbers are also listed): **afs (1483)**, **bgp (179)**, **biff (512)**, **bootpc (68)**, **bootps (67)**, **cmd (514)**, **cvspserver (2401)**, **dhcp (67)**, **domain (53)**, **eklogin (2105)**, **ekshell (2106)**, **exec (512)**, **finger (79)**, **ftp (21)**, **ftp-data (20)**, **http (80)**, **https (443)**, **ident (113)**, **imap (143)**, **kerberos-sec (88)**, **klogin (543)**, **kpasswd (761)**, **krb-prop (754)**, **krbupdate (760)**, **kshell (544)**, **ldap (389)**, **login (513)**, **mobileip-agent (434)**, **mobilip-mn (435)**, **msdp (639)**, **netbios-dgm (138)**, **netbios-ns (137)**, **netbios-ssn (139)**, **nfsd (2049)**, **nntp (119)**, **ntalk (518)**, **ntp (123)**, **pop3 (110)**, **pptp (1723)**, **printer (515)**, **radacct (1813)**,**radius (1812)**, **rip (520)**, **rkinit (2108)**, **smtp (25)**, **snmp (161)**, **snmptrap (162)**, **snpp (444)**, **socks (1080)**, **ssh (22)**, **sunrpc (111)**, **syslog (514)**, **tacacs-ds (65)**, **talk (517)**, **telnet (23)**, **tftp (69)**, **timed (525)**, **who (513)**, **xdmcp (177)**, **zephyr-clt (2103)**, **zephyr-hm (2104)**	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.
destination-port range-optimize *range*	Match a range of TCP or UDP port ranges while using the available memory more efficiently. Using this condition allows you to configure more firewall filters than if you configure individual destination ports. (Not supported with filter-based forwarding.)	Egress and ingress IPv4 (inet) interfaces.

Copyright © 2015, Juniper Networks, Inc.

Table 5: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
destination-prefix-list *prefix-list*	IP destination prefix list field. You can define a list of IP address prefixes under a prefix-list alias for frequent use. Define this list at the **[edit policy-options]** hierarchy level.	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces and IPv6 (inet6) interfaces.
dot1q-tag *number*	802.1Q VLAN ID field in the Ethernet frame. The tag values can be 1–4094.	Ingress ports and VLANs. Egress ports and VLANs (*Number* must be the VLAN ID of the VLAN you want to match).
dot1q-user-priority *number*	802.1Q priority field in the Ethernet frame (used for class-of-service priorities). 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): • **best-effort (0)**—Best effort • **background (1)**—Background • **standard (2)**—Standard or spare • **excellent-load (3)**—Excellent load • **controlled-load (4)**—Controlled load • **video (5)**—Video • **voice (6)**—Voice • **network-control (7)**—Network control reserved traffic	Ingress ports and VLANs. Egress ports and VLANs.
dscp *value*	Differentiated Services code point (DSCP). The DiffServ protocol uses the type-of-service (ToS) byte in the IP header. The most-significant 6 bits of this byte form the DSCP. You can specify DSCP in hexadecimal, binary, or decimal form. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): • **be**—best effort (default) • **ef (46)**—as defined in RFC 3246, *An Expedited Forwarding PHB*. • **af11 (10)**, **af12 (12)**, **af13 (14)**; **af21 (18)**, **af22 (20)**, **af23 (22)**; **af31 (26)**, **af32 (28)**, **af33 (30)**; **af41 (34)**, **af42 (36)**, **af43 (38)** These four classes, with three drop precedences in each class, for a total of 12 code points, are defined in RFC 2597, *Assured Forwarding PHB*. • **cs0**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **cs5**	Ingress ports, VLANs, and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.

Copyright © 2015, Juniper Networks, Inc.

Table 5: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
ether-type *value*	Ethernet type field of a packet. The EtherType value specifies what protocol is being transported in the Ethernet frame. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): • **aarp (0x80F3)**—EtherType value AARP • **appletalk (0x809B)**—EtherType value AppleTalk • **arp (0x0806)**—EtherType value ARP • **fcoe (0x8906)**—EtherType value FCoE • **fip (0x8914)**—EtherType value FIP • **ipv4 (0x0800)**—EtherType value IPv4 • **ipv6 (0x08DD)**—EtherType value IPv6 • **mpls-multicast (0x8848)**—EtherType value MPLS multicast • **mpls-unicast (0x8847)**—EtherType value MPLS unicast • **oam (0x88A8)**—EtherType value OAM • **ppp (0x880B)**—EtherType value PPP • **pppoe-discovery (0x8863)**—EtherType value PPPoE Discovery Stage • **pppoe-session (0x8864)**—EtherType value PPPoE Session Stage • **sna (0x80D5)**—EtherType value SNA	Ingress ports and VLANs. Egress ports and VLANs.
exp	Match on MPLS EXP bits.	Ingress MPLS interfaces. Egress MPLS interfaces.
fragment-flags *value*	IP fragmentation flags. In place of the numeric value, you can specify one of the following text synonyms (the hexadecimal values are also listed): • **is-fragment** • **dont-fragment (0x4000)** • **more-fragments (0x2000)** • **reserved (0x8000)**	Ingress ports and VLANs.

Copyright © 2015, Juniper Networks, Inc.

Table 5: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
from-fabric	(QFabric systems only) Traffic flows forwarded from a QFabric system Interconnect device egress interface to a Node device ingress interface. In one "from" filter term, use one or more of the following match conditions to identify a flow of traffic: • Client-side MAC address (for example, an FCF MAC address for FCoE traffic) (**destination-mac-address** ***mac-address***) or **source-mac-address** ***mac-address***) • Server-side MAC address (for example, an ENode MAC address for FCoE traffic) (**destination-mac-address** ***mac-address***) or **source-mac-address** ***mac-address***) • EtherType (**ether-type** ***value*****)** NOTE: If you remap an FCoE flow using EtherType as the match condition, you need to include two terms in the filter in each direction of flow to identify the traffic, one term to identify FCoE traffic (EtherType 0x8906), and one term to identify FIP traffic (EtherType 0x8914). • VLAN (**vlan (*vlan-name* | *vlan-id*)** • .1q user priority (**dot1q-user-priority**) In the same "from" filter term, use the "from-fabric" match condition to match traffic flowing from the Interconnect device to the Node device. In the "then" statement of the filter term, remap the identified traffic flow from the forwarding class used on the Interconnect device back into its original forwarding class, by specifying the original forwarding class and loss priority as action modifiers. This programs the QFabric system to use the original forwarding class for the flow when the flow is forwarded out of the QFabric system, not the temporarily remapped forwarding class the flow uses as it crosses the Interconnect device. The "to-fabric" match condition, which you configure using a different term in the same filter, maps the flow from the original forwarding class into a new forwarding class at the Node device egress, before the traffic crosses the Interconnect device. The "to-fabric" and the "from-fabric" match conditions combine to enable you to avoid traffic flow fate sharing as the traffic crosses the Interconnect device. The to-fabric match condition allows you to separate the flow into multiple forwarding classes as it crosses the Interconnect device, and the from-fabric match condition brings the traffic back together into the same forwarding class before the traffic leaves the QFabric system.	VLANs. Filter applies to traffic forwarded from an Interconnect device to a Node device.

Copyright © 2015, Juniper Networks, Inc.

Table 5: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
icmp-code *value*	ICMP code field. Because the meaning of the value depends upon the associated **icmp-type**, you must specify a value for **icmp-type** along with a value for **icmp-code**. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed). The keywords are grouped by the ICMP type with which they are associated: • *IPv4:* parameter-problem—**ip-header-bad (0)**, **required-option-missing (1)** • *IPv6:* parameter-problem—**ip6-header-bad (0)**, **unrecognized-next-header (1)**, **unrecognized-option (2)** • **redirect**—**redirect-for-network (0)**, **redirect-for-host (1)**, **redirect-for-tos-and-net (2)**, **redirect-for-tos-and-host (3)** • **time-exceeded**—**ttl-eq-zero-during-reassembly (1)**, **ttl-eq-zero-during-transit (0)** • *IPv4:* unreachable—**network-unreachable (0)**, **host-unreachable (1)**, **protocol-unreachable (2)**, **port-unreachable (3)**, **fragmentation-needed (4)**, **source-route-failed (5)**, **destination-network-unknown (6)**, **destination-host-unknown (7)**, **source-host-isolated (8)**, **destination-network-prohibited (9)**, **destination-host-prohibited (10)**, **network-unreachable-for-TOS (11)**, **host-unreachable-for-TOS (12)**, **communication-prohibited-by-filtering (13)**, **host-precedence-violation (14)**, **precedence-cutoff-in-effect (15)** • *IPv6:* unreachable—**address-unreachable (3)**, **administratively-prohibited (1)**, **no-route-to-destination (0)**, **port-unreachable (4)**	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.
hop-limit*value*	Match the the specified hop limit or set of hop limits. Specify a single value or a range of values from 0 through 255.	Ingress and egress IPv6 (inet6) interfaces.

Copyright © 2015, Juniper Networks, Inc.

Table 5: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
icmp-type *value*	ICMP message type field. Typically, you specify this match in conjunction with the **protocol** match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): *IPv4:* **echo-reply (0)**, **destination unreachable (3)**, **source-quench (4)**, **redirect (5)**, **echo-request (8)**, **IPv4 (inet)-advertisement (9)**, **IPv4 (inet)-solicit (10)**, **time-exceeded (11)**, **parameter-problem (12)**, **timestamp (13)**, **timestamp-reply (14)**, **info-request (15)**, **info-reply (16)**, **mask-request (17)**, **mask-reply (18)** *IPv6:* **destination-unreachable (1)**, **packet-too-big (2)**, **time-exceeded (3)**, **parameter-problem (4)**, **echo-request (128)**, **echo-reply (129)**, **membership-query (130)**, **membership-report (131)**, **membership-termination (132)**, **router-solicit (133)**, **router-advertisement (134)**, **neighbor-solicit (135)**, **neighbor-advertisement (136)**, **redirect (137)**, **router-renumbering (138)**, **node-information-request (139)**, **node-information-reply (140)** See also **icmp-code** *variable*.	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.
interface *interface-name*	Interface on which the packet is received, including the logical unit. You can include the wildcard character (*) as part of an interface name or logical unit. NOTE: An interface from which a packet is sent cannot be used as a match condition.	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces and IPv6 (inet6) interfaces.
ip-destination-address *address*	IPv4 address that is the final destination node address for the packet.	Ingress ports and VLANs.
ip6-destination-address *address*	IPv6 address that is the final destination node address for the packet.	Ingress ports and VLANs. (You cannot simultaneously apply a filter with this match criterion to a Layer 2 port and VLAN that includes that port.)
ip-options	Specify **any** to create a match if anything is specified in the options field in the IP header.	Ingress ports, VLANs, and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.
ip-precedence *ip-precedence-field*	IP precedence field. In place of the numeric field value, you can specify one of the following text synonyms (the field values are also listed): **critical-ecp** (0xa0), **flash** (0x60), **flash-override** (0x80), **immediate** (0x40), **internet-control** (0xc0), **net-control** (0xe0), **priority** (0x20), or **routine** (0x00).	Ingress ports, VLANs, and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.

Copyright © 2015, Juniper Networks, Inc.

Table 5: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
ip-protocol *number*	IP protocol field.	Ingress ports, VLANs, and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.
ip-source-address *address*	IPv4 address of the source node sending the packet.	Ingress ports and VLANs.
ip6-source-address *address*	IPv6 address of the source node sending the packet.	Ingress ports and VLANs. (You cannot simultaneously apply a filter with this match criterion to a Layer 2 port and VLAN that includes that port.)
ip-version *address*	IP version of the packet. Use this condition to match IPv4 or IPv6 header fields in traffic that arrives on a Layer 2 port or VLAN interface.	Ingress ports and VLANs.
is-fragment	Using this condition causes a match if the More Fragments flag is enabled in the IP header or if the fragment offset is not zero.	Ingress ports, VLANs, and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.
l2-encap-type llc-non-snap	Match on logical link control (LLC) layer packets for non-Subnet Access Protocol (SNAP) Ethernet Encapsulation type.	Ingress ports and VLANs. Egress ports and VLANs.
label	Match on MPLS label bits.	Ingress MPLS interfaces. Egress MPLS interfaces.
learn-vlan-id *number*	Matches the ID of a normal VLAN or the ID of the outer (service) VLAN (for Q-in-Q VLANs). The acceptable values are 1-4095.	Ingress ports and VLANs. Egress ports and VLANs.
next-header	IPv4 or IPv6 protocol value. In place of the numeric value, you can specify one of the following text synonyms (the numeric values are also listed): **hop-by-hop (0)**,**icmp (1)**, **icmp6 (58)**, **igmp (2)**, **ipip (4)**, **tcp (6)**, **egp (8)**, **udp (17)**, **ipv6 (41)**, **routing (43)**, **fragment (44)**,**rsvp (46)**, **gre (47)**, **esp (50)**, **ah (51)**, **icmp6 (58)**, **no-next-header (59)**, **dstopts (60)**, **ospf (89)**, **pim (103)**, **vrrp (112)**, **sctp (132)**	Ingress ports, VLANs, and IPv6 (inet6) interfaces. Egress IPv6 (inet6) interfaces.
packet-length	Packet length in bytes. You must enter a value between 0 and 65535.	Ingress ports, VLANs, IPv4 (inet), and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.

Copyright © 2015, Juniper Networks, Inc.

Table 5: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
payload-protocol	IPv4 or IPv6 protocol value. In place of the numeric value, you can specify one of the following text synonyms (the numeric values are also listed): **hop-by-hop (0),icmp (1), icmp6 (58), igmp (2), ipip (4), tcp (6), egp (8), udp (17), ipv6 (41), routing (43), fragment (44),rsvp (46), gre (47), esp (50), ah (51), icmp6 (58), no-next-header (59), dstopts (60), ospf (89), pim (103), vrrp (112), sctp (132)**	Ingress ports, VLANs, and IPv6 (inet6) interfaces. Egress IPv6 (inet6) interfaces.
precedence *value*	IP precedence bits in the type-of-service (ToS) byte in the IP header. (This byte can also used for the DiffServ DSCP.) In place of the numeric value, you can specify one of the following text synonyms (the numeric values are also listed): • **routine (0)** • **priority (1)** • **immediate (2)** • **flash (3)** • **flash-override (4)** • **critical-ecp (5)** • **internet-control (6)** • **net-control (7)**	Ingress ports, VLANs, and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.
protocol *type*	IPv4 or IPv6 protocol value. In place of the numeric value, you can specify one of the following text synonyms (the numeric values are also listed): **hop-by-hop (0),icmp (1), icmp6, igmp (2), ipip (4), tcp (6), egp (8), udp (17), ipv6 (41), routing (43), fragment (44),rsvp (46), gre (47), esp (50), ah (51), icmp6 (58), no-next-header (59), dstopts (60), ospf (89), pim (103), vrrp (112), sctp (132)**	Ingress ports, VLANs and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.

Copyright © 2015, Juniper Networks, Inc.

Table 5: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
rat-type *tech-type-value*	Match the radio-access technology (RAT) type specified in the 8-bit Tech-Type field of Proxy Mobile IPv4 (PMIPv4) access technology type extension. The technology type specifies the access technology through which the mobile device is connected to the access network. Specify a single value, a range of values, or a set of values. You can specify a technology type as a numeric value from 0 through 255 or as a system keyword. • Numeric value 1 matches IEEE 802.3. • Numeric value 2 matches IEEE 802.11a/b/g. • Numeric value 3 matches IEEE 802.16e • Numeric value 4 matches IEEE 802.16m. • Text string **eutran** matches 4G. • Text string **geran** matches 2G. • Text string **utran** matches 3G. •	Egress and ingress IPv4 (inet) interfaces.
sample	Sample the packet traffic. Apply this option only if you have enabled traffic sampling.	Egress and ingress IPv4 (inet) interfaces.
source-address *ip-address*	IP source address field, which is the address of the node that sent the packet.	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.
source-mac-address *mac-address*	Source media access control (MAC) address of the packet.	Ingress ports and VLANs. Egress ports and VLANs.
source-port *value*	TCP or UDP source port. Typically, you specify this match in conjunction with the **protocol** match statement. In place of the numeric field, you can specify one of the text synonyms listed under **destination-port**.	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.
source-port range-optimize *range*	Match a range of TCP or UDP port ranges while using the available memory more efficiently. Using this condition allows you to configure more firewall filters than if you configure individual source ports. (Not supported with filter-based forwarding.)	Egress and ingress IPv4 (inet) interfaces.
source-prefix-list *prefix-list*	IP source prefix list. You can define a list of IP address prefixes under a prefix-list alias for frequent use. Define this list at the **[edit policy-options]** hierarchy level.	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.

Copyright © 2015, Juniper Networks, Inc.

Table 5: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
tcp-established	Match packets of an established TCP connection. This condition matches packets other than those used to set up a TCP connection—that is, three-way handshake packets are not matched. When you specify **tcp-established**, a switch does not implicitly verify that the protocol is TCP. You must also specify the **protocol tcp** match condition.	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.
tcp-flags *value*	One or more TCP flags: • **ack (0x10)** • **fin (0x01)** • **push (0x08)** • **rst (0x04)** • **syn (0x02)** • **urgent (0x20)**	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.
tcp-initial	Match the first TCP packet of a connection. A match occurs when the TCP flag **SYN** is set and the TCP flag **ACK** is not set. When you specify **tcp-initial**, a switch does not implicitly verify that the protocol is TCP. You must also specify the **protocol tcp** match condition.	Ingress ports, VLANs, IPv4 (inet) interfaces, and IPv6 (inet6) interfaces. Egress IPv4 (inet) interfaces.

Copyright © 2015, Juniper Networks, Inc.

Table 5: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
to-fabric <except>		VLANs. Filter applies to traffic forwarded from a Node device to the Interconnect device.

Copyright © 2015, Juniper Networks, Inc.

Table 5: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
	(QFabric systems only) Traffic flows forwarded from a QFabric system Node device egress interface to an Interconnect device ingress interface. In one "from" filter term, use one or more of the following match conditions to identify a flow of traffic: • Client-side MAC address (for example, an FCF MAC address for FCoE traffic) (**destination-mac-address** ***mac-address***) or **source-mac-address** ***mac-address***) • Server-side MAC address (for example, an ENode MAC address for FCoE traffic) (**destination-mac-address** ***mac-address***) or **source-mac-address** ***mac-address***) • EtherType (**ether-type** ***value*****)** NOTE: If you remap an FCoE flow using EtherType as the match condition, you need to include two terms in the filter in each direction of flow to identify the traffic, one term to identify FCoE traffic (EtherType 0x8906), and one term to identify FIP traffic (EtherType 0x8914). • VLAN (**vlan (*vlan-name* | *vlan-id*)** • .1q user priority (**dot1q-user-priority**) In the same "from" filter term, use the "to-fabric" match condition to match traffic flowing from the Node device to the Interconnect device. In the "then" statement of the filter term, remap the identified traffic flow from its current forwarding class into another forwarding class (default or user-defined) and loss priority by specifying the forwarding class and loss priority as action modifiers. The QFabric system uses the remapped forwarding class to transport the flow across the Interconnect device. The "from-fabric" match condition, which you configure using a different term in the same filter, maps the flow back to the original forwarding class after the flow traverses the Interconnect device, when the flow enters the Node device from which the traffic will egress from the QFabric system. The "to-fabric" and the "from-fabric" match conditions combine to enable you to avoid traffic flow fate sharing as the traffic crosses the Interconnect device. The to-fabric match condition allows you to separate the flow into multiple forwarding classes as it crosses the Interconnect device, and the from-fabric match condition brings the traffic back together into the same forwarding class before the traffic leaves the QFabric system. The **except**option matches traffic that is locally	

Copyright © 2015, Juniper Networks, Inc.

Table 5: Supported Match Conditions for Firewall Filters *(continued)*

Match Condition	Description	Direction and Interface
	switched—that is, traffic that enters and exits the same QFabric system Node device and does not cross the Interconnect device. If traffic identified by the match conditions contains some flows that are locally switched, the "except" option remaps the forwarding class for the locally switched traffic and does *not* remap the forwarding class for remotely switched traffic.	
traffic-class	8-bit field that specifies the class-of-service (CoS) priority of the packet. The traffic-class field is used to specify a DiffServ code point (DSCP) value. This field was previously used as the type-of-service (ToS) field in IPv4, and, the semantics of this field (for example, DSCP) are identical to those of IPv4. You can specify one of the following text synonyms (the field values are also listed): **af11 (10)**, **af12 (12)**, **af13 (14)**, **af21 (18)**, **af22 (20)**, **af23 (22)**, **af31 (26)**, **af32 (28)**, **af33 (30)**, **af41 (34)**, **af42 (36)**, **af43 (38)**, **cs0 (0)**, **cs1 (8)**, **cs2 (16)**, **cs3 (24)**, **cs4 (32)**, **cs5 (40)**, **cs6 (48)**, **cs7 (56)**, **ef (46)**	Ingress ports, VLANs, and IPv6 (inet6) interfaces. Egress IPv6 (inet6) interfaces.
ttl *value*	IP Time-to-live (TTL) field in decimal. The value can be 1-255.	Ingress IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.
user-vlan-1p-priority *value*	Match on the IEEE 802.1p priority bits in the inner (customer) VLAN tag in a Q-in-Q VLAN. Specify a single value or multiple values from **0-7**.	Ingress ports, VLANs, and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.
user-vlan-id *number*	Matches the ID of the inner (customer) VLAN in a Q-in-Q VLAN. The acceptable values are 1-4095.	Ingress ports, VLANs, and IPv4 (inet) interfaces. Egress IPv4 (inet) interfaces.
vlan (*vlan-name* **|** *vlan-id* **)**	VLAN names or ID.	Ingress ports and VLANs. Egress ports and VLANs.

Use **then** statements to define actions that should occur if a packet matches all conditions in a **from** statement. Table 6 on page 25 shows the actions that you can specify in a term. (If you do not include a **then** statement, the system accepts packets that match the filter.)

Table 6: Actions for Firewall Filters

Action	Description
accept	Accept a packet. This is the default action for packets that match a term.

Copyright © 2015, Juniper Networks, Inc.

Table 6: Actions for Firewall Filters *(continued)*

Action	Description
discard	Discard a packet silently without sending an Internet Control Message Protocol (ICMP) message.
reject *message-type*	Discard a packet and send a "destination unreachable" ICMPv4 message (type 3). To log rejected packets, configure the **syslog** action modifier. You can specify one of the following message types: **administratively-prohibited (default), bad-host-tos, bad-network-tos, host-prohibited, host-unknown, host-unreachable, network-prohibited, network-unknown, network-unreachable, port-unreachable, precedence-cutoff, precedence-violation, protocol-unreachable, source-host-isolated, source-route-failed,** or **tcp-reset**. If you specify **tcp-reset**, the system sends a TCP reset if the packet is a TCP packet; otherwise nothing is sent. If you do not specify a message type, the ICMP notification "destination unreachable" is sent with the default message "communication administratively filtered." NOTE: The **reject** action is supported on ingress interfaces only.
routing-instance *instance-name*	Forward matched packets to a virtual routing instance.
vlan *VLAN-name*	Forward matched packets to a specific VLAN. NOTE: The **vlan** action is supported on ingress interfaces only. NOTE: This action is not supported on OCX series switches.

You can also specify the action modifiers listed in Table 7 on page 26 to count, mirror, rate-limit, and classify packets.

Table 7: Action Modifiers for Firewall Filters

Action Modifier	Description
analyzer *analyzer-name*	(Non-ELS platforms) Mirror traffic (copy packets) to an analyzer configured at the **[edit ethernet-switching-options analyzer]** hierarchy level. You can specify port mirroring for ingress port, VLAN, and IPv4 (inet) firewall filters only.
count *counter-name*	Count the number of packets that match the term.
decapsulate [gre | *routing-instance***]**	De-encapsulate GRE packets or forward de-encapsulated GRE packets to the specified routing instance

Copyright © 2015, Juniper Networks, Inc.

Table 7: Action Modifiers for Firewall Filters *(continued)*

Action Modifier	Description
dscp *value*	Differentiated Services code point (DSCP). The DiffServ protocol uses the type-of-service (ToS) byte in the IP header. The most-significant 6 bits of this byte form the DSCP. You can specify DSCP in hexadecimal, binary, or decimal form. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): • **be**—best effort (default) • **ef (46)**—as defined in RFC 3246, *An Expedited Forwarding PHB*. • **af11 (10)**, **af12 (12)**, **af13 (14)**; **af21 (18)**, **af22 (20)**, **af23 (22)**; **af31 (26)**, **af32 (28)**, **af33 (30)**; **af41 (34)**, **af42 (36)**, **af43 (38)** These four classes, with three drop precedences in each class, for a total of 12 code points, are defined in RFC 2597, *Assured Forwarding PHB*. • **cs0**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **cs5**
forwarding-class *class*	Classify the packet in one of the following default forwarding classes, or in a user-defined forwarding class: • **best-effort** • **fcoe** • **mcast** • **network-control** • **no-loss** NOTE: To configure a forwarding class, you must also configure loss priority.
interface	Switch the traffic to the specified interface without performing a lookup on it. This action is valid only when the filter is applied on ingress.
log	Log the packet's header information in the Routing Engine. To view this information, enter the **show firewall log** operational mode command. NOTE: The **log** action modifier is supported on ingress interfaces only.
loss-priority (low | medium-low | medium-high | high)	Set the packet loss priority (PLP). NOTE: The **loss-priority** action modifier is supported on ingress interfaces only. NOTE: The **loss-priority** action modifier is not supported in combination with the **policer** action.

Copyright © 2015, Juniper Networks, Inc.

Table 7: Action Modifiers for Firewall Filters *(continued)*

Action Modifier	Description
policer *policer-name*	Send packets to a policer (for the purpose of applying rate limiting). You can specify a policer for ingress port, VLAN, IPv4 (inet), IPv6 (inet6), and MPLS filters. NOTE: The **policer** action modifier is not supported in combination with the **loss-priority** action.
port-mirror	(ELS platforms) Mirror traffic (copy packets) to an output interface configured in a port-mirroring instance at the **[edit forwarding-options port-mirroring]** hierarchy level. You can specify port mirroring for ingress port, VLAN, and IPv4 (inet) firewall filters only.
port-mirror-instance *port-mirror-instance-name*	(ELS platforms) Mirror traffic to a port-mirroring instance configured at the **[edit forwarding-options port-mirroring]** hierarchy level. You can specify port mirroring for ingress port, VLAN, and IPv4 (inet) firewall filters only. NOTE: This action modifier is not supported on OCX series switches.
syslog	Log an alert for this packet. NOTE: The **syslog** action modifier is supported on ingress interfaces only.
three-color-policer *three-color-policer-name*	Send packets to a three-color policer (for the purpose of applying rate limiting). You can specify a three-color policer for ingress and egress port, VLAN, IPv4 (inet), IPv6 (inet6), and MPLS filters. NOTE: The **policer** action modifier is not supported in combination with the **loss-priority** action.

Related Documentation

- Understanding How Firewall Filters Are Evaluated on page 5
- Understanding How a Firewall Filter Tests a Protocol on page 29
- Overview of Policers on page 41
- *Understanding Port Mirroring*
- *Configuring Firewall Filters*

Copyright © 2015, Juniper Networks, Inc.

Understanding How a Firewall Filter Tests a Protocol

When examining match conditions in a firewall filter, a switch tests only the fields that you specify. It does not implicitly test any fields that you do not explicitly configure. For example, if you specify a match condition of **source-port ssh**, there is no implied test to determine if the protocol is TCP. In this case, the switch considers any packet that has a value of **22** (decimal) in the 2-byte field that follows a *presumed* IP header to be a match. To ensure that the term matches on TCP packets, you also specify an **ip-protocol tcp** match condition.

For the following match conditions, you should explicitly specify the protocol match condition in the same term:

- **destination-port**—Specify protocol **tcp** or protocol **udp**.
- **icmp-code**—Specify protocol **icmp** and **icmp-type**.
- **icmp-type**—Specify protocol **icmp** or protocol **icmp6**.
- **source-port**—Specify protocol **tcp** or protocol **udp**.
- **tcp-flags**—Specify protocol **tcp**.

Related Documentation

- *Understanding Firewall Filter Match Conditions*
- *Configuring Firewall Filters*

Understanding Firewall Filter Planning

Before you create a firewall filter and apply it, determine what you want the filter to accomplish and how to use its match conditions and actions to achieve your goals. It is important that you understand how packets are matched, the default and configured actions of the firewall filter, and where to apply the firewall filter.

You can apply no more than one firewall filter per router interface per direction (input and output). For example, for a given interface you can apply at most one filter in the input direction and one filter in the output direction. You should 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 operation and can make testing and troubleshooting more difficult.

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

1. What is the purpose of the filter?

   For example, the system can drop packets based on header information, rate-limit traffic, classify packets into forwarding classes, log and count packets, or prevent denial-of-service attacks.

2. What are the appropriate match conditions? Determine the packet header fields that the packet must contain for a match. Possible fields include:

Copyright © 2015, Juniper Networks, Inc.

- Layer 3 header fields—Source and destination IP addresses, protocols, and IP options (IP precedence, IP fragmentation flags, or TTL type).
- TCP header fields—Source and destination ports and flags.
- ICMP header fields—Packet type and code.

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

   The system can accept, discard, or reject packets.

4. What additional action modifiers might be required?

   For example, you can configure the system to mirror (copy) packets to a specified port, count matching packets, apply traffic management, or police packets.

5. On what Layer 3 interface should the firewall filter be applied?

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

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

   You typically configure different actions for traffic entering an interface than you configure for traffic exiting an interface.

7. How many filters should I create?

Related Documentation

- Overview of Policers on page 41
- Understanding How Firewall Filters Are Evaluated on page 5
- *Configuring Firewall Filters*

Configuring Firewall Filters

You can configure firewall filters in a switch to control traffic that enters or exits Layer 3 (routed) interfaces. To use a firewall filter, you must configure the filter and then apply it to a Layer 3 interface.

- Configuring a Firewall Filter on page 31
- Applying a Firewall Filter to a Layer 3 (Routed) Interface on page 32

Copyright © 2015, Juniper Networks, Inc.

Configuring a Firewall Filter

To configure a firewall filter:

1. Configure the family address type, filter name, term name, and at least one match condition—for example, match on packets that contain a specific source address:

   ```
   [edit]
   user@switch# set firewall family (inet | inet6) filter ingress-port-filter term t1 from
   source-address 192.0.2.14
   ```

   Specify the family address type **inet** for IPv4 or **inet6** for IPv6.

   The filter and term names can contain letters, numbers, and hyphens (-) and can be up to 64 characters long. Each filter name must be unique. A filter can contain one or more terms, and each term name must be unique within a filter.

2. Configure additional match conditions. For example, match on packets that contain a specific source port:

   ```
   [edit firewall family inet filter ingress-port-filter term t1 from]
   user@switch# set 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, it cannot be empty. If you omit the **from** statement, all packets are considered to match.

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

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

4. In each firewall filter term, specify the actions to take if the packet matches all the conditions in that term. You can specify an action and action modifiers:

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

     ```
     [edit firewall family inet filter ingress-port-filter term t1 then]
     user@switch# set discard
     ```

     You can specify no more than one action (**accept**, **discard**, **reject**, **routing-instance**, or **vlan**) per term.

   - To specify action modifiers, for example, to count and classify packets to a forwarding class. For example:

     ```
     [edit firewall family inet filter ingress-port-filter term t1 then]
     user@switch# set count counter-one
     user@switch# set loss-priority high
     ```

   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 should always explicitly configure an action in the **then** statement. You can include no more than one action statement, 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.

Copyright © 2015, Juniper Networks, Inc.

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

NOTE: For the complete list of match conditions, actions, and action modifiers, see "Firewall Filter Match Conditions and Actions" on page 11. Note that on the OCX1100 switch you can use only those match conditions that are valid for IPv4 and IPv6 interfaces.

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

To apply a firewall filter to a Layer 3 interface:

1. Provide a meaningful description of the firewall filter in the configuration of the interface to which the filter will be applied:

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

2. You can apply firewall filters to filter packets that enter or exit a Layer 3 interface:

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

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

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

     ```
     [edit]
     user@switch# set interfaces xe-0/0/2 unit 0 family inet filter output egress-router-filter
     ```

NOTE: You can apply only one filter to an interface for a given direction (ingress or egress).

Related Documentation

- Overview of Firewall Filters on page 3
- Firewall Filter Match Conditions and Actions on page 11
- Verifying That Firewall Filters Are Operational on page 36
- Monitoring Firewall Filter Traffic on page 35
- *Configuring Port Mirroring*

Copyright © 2015, Juniper Networks, Inc.

Applying Firewall Filters to Interfaces

For a firewall filter to work, you must apply it to at least one Layer 3 interface. To do this, include the **filter** statement when configuring a logical interface at the **[edit interfaces]** hierarchy level:

```
[edit interfaces]
user@switch# set interface-name unit logical-unit-number family (inet | inet6) filter (input | output) filter-name
```

In the **input** statement, specify a firewall filter to be evaluated when packets are received on the interface. Input filters applied to a loopback interface affect only traffic destined for the Routing Engine.

In the **output** statement, specify a filter to be evaluated when packets exit the interface.

NOTE: When you create a loopback interface, it is important to apply an ingress filter to it so the Routing Engine is protected. We recommend that when you apply a filter to the loopback interface lo0, you include the apply-groups statement. Doing so ensures that the filter is automatically inherited on every loopback interface, including lo0 and other loopback interfaces.

Related Documentation

- *Configuring Firewall Filters*

Configuring a Firewall Filter to De-Encapsulate GRE Traffic on a QFX5100 or OCX Switch

Generic routing encapsulation (GRE) provides a private, secure path for transporting packets through a network by encapsulating (or tunneling) the packets. GRE tunneling is performed by tunnel endpoints that encapsulate or de-encapsulate traffic.

You can use a firewall filter to de-encapsulate GRE traffic on a QFX5100 or OCX switch. This feature provides significant benefits in terms of scalability, performance, and flexibility because you don't need to create a tunnel interface to perform the de-encapsulation. For example, you can terminate many tunnels from multiple source IP addresses with one firewall term.

NOTE: QFX5100 and OCX switches support as many as 512 GRE tunnels, including tunnels created with a firewall filter. That is, you can create a total of 512 GRE tunnels, regardless of which method you use.

This topic describes:

Copyright © 2015, Juniper Networks, Inc.

Configuring a Filter to De-Encapsulate GRE Traffic

To configure a firewall filter to de-encapsulate GRE traffic:

1. Create an IPv4 firewall filter and (optionally) specify a source address for the tunnel:

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

   You must create an IPv4 filter by using **family inet** because the outer header of a GRE packet must be IPv4. If you specify a source address, it should be an address on a device that will encapsulate traffic into GRE packets.

   NOTE: To terminate many tunnels from multiple source IP addresses with one firewall term, do not configure a source address. In this case, the filter will de-encapsulate any GRE packets received by the interface that you apply the filter to.

2. Specify a destination address for the tunnel:

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

   This should be an address on an interface of the switch on which you want the tunnel or tunnels to terminate and the GRE packets to be de-encapsulated. You should also configure this address as a tunnel endpoint on all the tunnel source routers that you want to form tunnels with the switch.

3. Specify that the filter should match and accept GRE traffic:

   ```
   [edit ]
   user@switch# set firewall family inet filter filter-name term term-name from protocol
     gre
   ```

4. Specify that the filter should de-encapsulate GRE traffic:

   ```
   [edit ]
   user@switch# set firewall family inet filter filter-name term term-name then decapsulate
     gre
   ```

   Based on the configuration you have performed so far, the switch forwards the de-encapsulated packets by comparing the inner header to the default routing table (**inet0**). If you want the switch to use a virtual routing instance to forward the de-encapsulated packets, perform the following steps:

5. Specify the name of the virtual routing instance:

   ```
   [edit ]
   user@switch# set firewall family inet filter filter-name term term-name then decapsulate
     routing-instance instance-name
   ```

6. Specify that the virtual routing instance is a virtual router:

   ```
   [edit ]
   ```


Copyright © 2015, Juniper Networks, Inc.

```
user@switch# set routing-instances instance-name instance-type virtual-router
```

7. Specify the interfaces that belong to the virtual router:

```
[edit ]
user@switch# set routing-instances instance-name interface interface-name
```

Applying the Filter to an Interface

After you create the firewall filter, you must also apply it to an interface that will receive GRE traffic. Be sure to apply it in the input direction. For example, enter

```
[edit ]
user@switch# set interfaces interface-name unit logical-unit-number family inet filter
  input filter-name
```

Because the outer header of a GRE packet must be IPv4, you must apply the filter to an IPv4 interface and specify **family inet**.

Related Documentation

- *Understanding Generic Routing Encapsulation*
- *Configuring Generic Routing Encapsulation Tunneling*
- *Configuring Firewall Filters*

Monitoring Firewall Filter Traffic

You can use operational mode commands to monitor firewall filter traffic.

- Monitoring Traffic for All Firewall Filters and Policers That Are Configured on page 35
- Monitoring Traffic for a Specific Firewall Filter on page 36
- Monitoring Traffic for a Specific Policer on page 36

Monitoring Traffic for All Firewall Filters and Policers That Are Configured

Purpose 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 **show firewall** operational mode command:

```
user@switch> show firewall
Filter: egress-vlan-watch-employee
Counters:
Name                                                Bytes              Packets
counter-employee-web                                 3348                   27
Filter: ingress-port-limit-tcp-icmp
Counters:
Name                                                Bytes              Packets
icmp-counter                                          560                   10
Policers:
Name                                               Packets
icmp-connection-policer                                 10
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, counters, and policers that are configured. 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.

Monitoring Traffic for a Specific Firewall Filter

Purpose Monitor the number of packets and bytes that matched a firewall filter and monitor the number of packets that exceeded policer rate limits.

Action Use the **show firewall filter *filter-name*** operational mode command:

```
user@switch> show firewall filter ingress-port-limit-tcp-icmp
Filter: ingress-port-limit-tcp-icmp
Counters:
Name                                                Bytes              Packets
icmp-counter                                          560                   10
```

Meaning The **show firewall filter *filter-name*** command limits the display information to the counters and policers that are defined for the specified filter.

Monitoring Traffic for a Specific Policer

Purpose Monitor the number of packets that exceeded the rate limits of a policer:

Action Use the **show firewall policer *policer-name*** operational mode command:

```
user@switch> show firewall policer icmp-connection-policer
Filter: ingress-port-limit-tcp-icmp
Policers:
Name                                                Packets
icmp-connection-policer                                  10
```

Meaning The **show firewall policer *policer-name*** command displays the number of packets that exceeded the rate limits for the specified policer.

Related Documentation

- *Configuring Firewall Filters*
- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59
- Verifying That Firewall Filters Are Operational on page 36

Verifying That Firewall Filters Are Operational

Purpose Verify that firewall filters are working properly.

Action Use the **show firewall** operational mode command to verify that the firewall filters are working properly:

```
user@switch> show firewall
```


Copyright © 2015, Juniper Networks, Inc.

```
Filter: egress-vlan-watch-employee
Counters:
Name                                                Bytes              Packets
counter-employee-web                                    0                    0
Filter: ingress-port-limit-tcp-icmp
Counters:
Name                                                Bytes              Packets
icmp-counter                                          560                   10
Policers:
Name                                              Packets
icmp-connection-policer                              10
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, counters, and policers that are configured. 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. In the above example, the **icmp-counter** in the filter **ingress-port-limit-tcp-icmp** shows that the filter matched 10 packets. 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. The policer **icmp-connection-policer** shows that 10 ICMP packets were policed.

Related Documentation

- *Configuring Firewall Filters*
- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59
- Monitoring Firewall Filter Traffic on page 35

Copyright © 2015, Juniper Networks, Inc.

Copyright © 2015, Juniper Networks, Inc.

PART 2

Policers

Copyright © 2015, Juniper Networks, Inc.

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 2

Using Policers

Overview of Policers

A switch polices traffic by limiting the input or output transmission rate of a class of traffic according to user-defined criteria. Policing (or rate-limiting) traffic allows you to control the maximum rate of traffic sent or received on an interface and to provide multiple priority levels or classes of service.

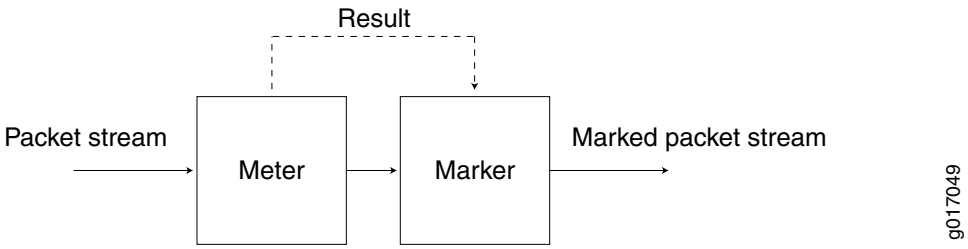
Copyright © 2015, Juniper Networks, Inc.

Policer Overview

You use policers to apply limits to traffic flow and set consequences for packets that exceed these limits—usually applying a higher loss priority—so that if packets encounter downstream congestion, they can be discarded first. Policers apply only to unicast packets.

Policers provide two functions: metering and marking. A policer meters (measures) each packet against traffic rates and burst sizes that you configure. It then passes the packet and the metering result to the marker, which assigns a packet loss priority that corresponds to the metering result. Figure 3 on page 42 illustrates this process.

Figure 3: Flow of Tricolor Marking Policer Operation



After you name and configure a policer, you use it by specifying it as an action in one or more firewall filters.

Policer Types

A switch supports three types of policers:

- Single-rate two-color marker—A two-color policer (or “policer” when used without qualification) 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 with a specified PLP or simply discard them.

  You can specify this type of policer in an ingress or egress firewall.

  NOTE: **A two-color policer is most useful for metering traffic at the port (physical interface) level.**

- Single-rate three-color marker—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 one rate—the configured committed information rate (CIR) as well as the committed burst size (CBS) and the excess burst size (EBS). The CIR specifies the average rate at which bits are admitted to the switch. The CBS specifies the usual burst size in bytes and the EBS specifies the maximum burst size in bytes. The EBS must be greater than or equal to the CBS, and neither can be 0.

Copyright © 2015, Juniper Networks, Inc.

You can specify this type of policer in an ingress or egress firewall.

NOTE: A single-rate three-color marker (TCM) is most useful when a service is structured according to packet length and not peak arrival rate.

- Two-rate three-color marker—This type of policer is defined in RFC 2698, *A Two Rate Three Color Marker*, as part of an assured forwarding per-hop-behavior classification system for a Differentiated Services environment. This type of policer meters traffic based on two rates—the CIR and peak information rate (PIR) along with their associated burst sizes, the CBS and peak burst size (PBS). The PIR specifies the maximum rate at which bits are admitted to the network and must be greater than or equal to the CIR.

  You can specify this type of policer in an ingress or egress firewall.

  NOTE: A two-rate three-color policer is most useful when a service is structured according to arrival rates and not necessarily packet length.

See Table 8 on page 43 for information about how metering results are applied for each of these policer types.

Policer Actions

Policer actions are implicit or explicit and vary by policer type. *Implicit* means that Junos OS assigns the loss priority automatically. Table 8 on page 43 describes the policer actions.

Table 8: Policer Actions

Policer	Marking	Implicit Action	Configurable Action
Single-rate two-color	Green (conforming)	Assign low loss priority	None
	Red (nonconforming)	None	Discard
Single-rate three-color	Green (conforming)	Assign low loss priority	None
	Yellow (above the CIR and CBS)	Assign medium-high loss priority	None
	Red (above the EBS)	Assign high loss priority	Discard

Copyright © 2015, Juniper Networks, Inc.

Table 8: Policer Actions *(continued)*

Policer	Marking	Implicit Action	Configurable Action
Two-rate three-color	Green (conforming)	Assign low loss priority	None
	Yellow (above the CIR and CBS)	Assign medium-high loss priority	None
	Red (above the PIR and PBS)	Assign high loss priority	Discard

NOTE: If you specify a policer in an egress firewall filter, the only supported action is **discard**.

Policer Colors

Single-rate and two-rate three-color policers can operate in two modes:

- Color-blind—In color-blind mode, the three-color policer assumes that all packets examined have not 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 assumes that all packets examined have been previously marked or metered. 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 cannot decrease it. For example, if a color-aware three-color policer meters a packet with a medium PLP marking, it can raise the PLP level to high but cannot reduce the PLP level to low.

Filter-Specific Policers

You can configure policers 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. However, the behavior of a filter-specific policer is affected by how the firewall filter terms that reference the policer are stored in TCAM. If you create a filter-specific policer and reference it in multiple firewall filter terms, the policer allows more traffic than expected if the terms are stored in different TCAM slices. For example, if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms that are stored in three separate memory slices, the total bandwidth allowed by the filter is 3 Gbps, not 1 Gbps.

To prevent this unexpected behavior from occurring, use the information about TCAM slices presented in *Planning the Number of Firewall Filters to Create* to organize your configuration file so that all the firewall filter terms that reference a given filter-specific policer are stored in the same TCAM slice.

Copyright © 2015, Juniper Networks, Inc.

Suggested Naming Convention for Policers

We recommend that you use the naming convention ***policertypeTCM#-color type*** when configuring three-color policers and ***policer#*** when configuring two-color policers. TCM stands for three-color marker. Because policers can be numerous and must be applied correctly to work, a simple naming convention makes it easier to apply the policers properly. For example, the first single-rate, color-aware three-color policer configured would be named **srTCM1-ca**. The second two-rate, color-blind three-color configured would be named **trTCM2-cb**. The elements of this naming convention are explained below:

- sr (single-rate)
- tr (two-rate)
- TCM (tricolor marking)
- 1 or 2 (number of marker)
- ca (color-aware)
- cb (color-blind)

Policer Counters

Each policer that you configure includes an implicit counter that counts the number of packets that exceed the rate limits that are specified for the policer. If you use the same policer in multiple terms—either within the same filter or in different filters—the implicit counter counts all the packets that are policed in all of these terms. If you want to obtain separate packet counts for each term, use these options:

- Configure a unique policer for each term.
- Configure only one policer, but use a unique, explicit counter in each term.

Policer Algorithms

Policing uses the *token-bucket algorithm*, which enforces a limit on average bandwidth while allowing bursts up to a specified maximum value. It offers more flexibility than the *leaky bucket algorithm* in allowing a certain amount of bursty traffic before it starts discarding packets.

How Many Policers Are Supported?

QFX5100 switches support 1535 ingress policers and 1024 egress policers (assuming one policer per firewall filter term).

QFX3500 and QFX3600 standalone switches and QFabric Node devices support the following numbers of policers (assuming one policer per firewall filter term):

- Two-color policers used in ingress firewall filters: 767
- Three-color policers used in ingress firewall filters: 767

Copyright © 2015, Juniper Networks, Inc.

- Two-color policers used in egress firewall filters: 1022
- Three-color policers used in egress firewall filters: 512

Policers Can Limit Egress Firewall Filters

The number of egress policers that you configure can affect the total number of allowed egress firewall filters. Every policer has two implicit counters that consume two entries in a 1024-entry TCAM that is used for counters, including counters that are configured as action modifiers in firewall filter terms. (Policers consume two entries because one is used for green packets and one is used for nongreen packets regardless of policer type.) If the TCAM becomes full, you cannot commit any more egress firewall filters that have terms with counters. For example, if you configure and commit 512 egress policers (two-color, three-color, or a combination of both policer types), all of the memory entries for counters are used up. If later in your configuration file you insert additional egress firewall filters with terms that also include counters, *none* of the terms in those filters are committed because there is no available memory space for the counters.

Here are some additional examples:

- Assume that you configure egress filters that include a total of 512 policers and no counters. Later in your configuration file you include another egress filter with 10 terms, 1 of which has a counter action modifier. None of the terms in this filter are committed because there is not enough TCAM space for the counter.
- Assume that you configure egress filters that include a total of 500 policers, so 1000 TCAM entries are occupied. Later in your configuration file you include the following two egress filters:
  - Filter A with 20 terms and 20 counters. All the terms in this filter are committed because there is enough TCAM space for all the counters.
  - Filter B comes after Filter A and has five terms and five counters. *None* of the terms in this filter are committed because there is not enough memory space for *all* the counters. (Five TCAM entries are required but only four are available.)

You can prevent this problem by ensuring that egress firewall filter terms with counter actions are placed earlier in your configuration file than terms that include policers. In this circumstance, Junos OS commits policers even if there is not enough TCAM space for the implicit counters. For example, assume the following:

- You have 1024 egress firewall filter terms with counter actions.
- Later in your configuration file you have an egress filter with 10 terms. None of the terms have counters but one has a policer action modifier.

You can successfully commit the filter with 10 terms even though there is not enough TCAM space for the implicit counters of the policer. The policer is committed without the counters.

Related Documentation

- Understanding Color-Blind Mode for Single-Rate Tricolor Marking on page 47
- Understanding Color-Blind Mode for Two-Rate Tricolor Marking on page 49

Copyright © 2015, Juniper Networks, Inc.

- Understanding Color-Aware Mode for Single-Rate Tricolor Marking on page 48
- Understanding Color-Aware Mode for Two-Rate Tricolor Marking on page 50
- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59

Understanding Policers with Link Aggregation Groups

If you apply a policer to a link aggregation group (LAG) on a standalone switch or QFabric node, the policer applies to all the interfaces in the LAG in aggregate. For example, if you configure a policer to rate-limit at 1 Gbps and apply the policer (by using a firewall filter) to a LAG that has two member interfaces on a single switch or node, the total allowed throughput for both members is 1 Gbps.

If you apply a policer to a LAG that has members on different nodes in a QFabric network Node group or redundant server Node group, the configured rate applies to the interface on each node. For example, if you configure a policer to rate-limit at 1 Gbps and apply the policer to a LAG that has one member on server node A and one member on server node B, the allowed throughput for each member is 1 Gbps, for a total allowed throughput of 2 Gbps.

Related Documentation

- Overview of Policers on page 41
- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59

Understanding Color-Blind Mode for Single-Rate Tricolor Marking

With the color-blind mode of single-rate tricolor marking, all packets are evaluated against the CBS. If a packet exceeds the CBS, it is evaluated against the EBS. In color-blind mode, the policer supports three loss priorities only: low, medium-high, and high.

Packets that exceed the CBS but are below the EBS are marked yellow (medium-high). Packets that exceed the EBS are marked red (high), as shown in Table 9 on page 47.

Table 9: Color-Blind Mode TCM Color-to-PLP Mapping

Color	PLP	Meaning
Green	**low**	Conforming.
Yellow	**medium-high**	Packet exceeds the CIR and CBS but does not exceed the EBS.
Red	**high**	Packet exceeds the EBS.

Related Documentation

- Overview of Policers on page 41
- Configuring Color-Blind Egress Policers for Medium-Low PLP on page 58

Copyright © 2015, Juniper Networks, Inc.

Understanding Color-Aware Mode for Single-Rate Tricolor Marking

In color-aware mode, the treatment the packet receives depends on its classification. Marking can increase a preassigned PLP but cannot decrease it.

Summary of PLP Changes

Table 10 on page 48 shows how a packet's incoming priority can be modified with single-rate marking.

Table 10: Color-Aware Mode Single-Rate PLP Mapping

Incoming PLP	Packet Metered Against	Possible Cases	Outgoing PLP
low	CIR, CBS, and EBS	Conforming	**low**
		Packet exceeds the CIR and CBS but does not exceed the EBS.	**medium-high**
		Packet exceeds the EBS.	**high**
medium-low	EBS only	Packet does not exceed the EBS.	**medium-low**
		Packet exceeds the EBS.	**high**
medium-high	EBS only	Packet does not exceed the EBS.	**medium-high**
		Packet exceeds the EBS.	**high**
high	Not metered by the policer.	All cases.	**high**

The following sections describe single-rate color-aware PLP mapping in more detail.

Effect on Green Packets (Low PLP)

Packets belonging to the green class have already been marked by a classifier with low PLP. The marking policer can leave the PLP unchanged or increase it to medium-high or high, so these packets are therefore metered against both the CBS and the EBS. For example, if a behavior aggregate or multifield classifier marks a packet with low PLP and the two-rate TCM policer is in color-aware mode, the output loss priority is as follows:

- If the rate of traffic flow is less than the CIR, packets remain marked as low PLP.
- If bursts exceed the CBS but not the EBS, some of the packets are marked as medium-high PLP, and some of the packets remain marked as low PLP.
- If bursts exceed the EBS, some of the packets are marked as high PLP, and some of the packets remain marked as low PLP.

Copyright © 2015, Juniper Networks, Inc.

Effect on Yellow Packets (Medium PLP)

Packets belonging to the yellow class have already been marked by a classifier with medium-low or medium-high PLP. The marking policer can leave the PLP unchanged or increase it to high, so these packets are therefore metered against the EBS only. For example, if a behavior aggregate or multifield classifier marks a packet with medium-low PLP and the two-rate TCM policer is in color-aware mode, the output loss priority is as follows:

- If the rate of traffic flow is less than the CBS, the packets remain marked as medium-low PLP.
- If the rate of traffic flow is greater than the CBS but less than the EBS, the packets remain marked as medium-low PLP.
- If the rate of traffic flow is greater than the EBS, some of the packets are marked as high PLP and some remain marked as medium-low PLP.

If a BA or multifield classifier marks a packet with medium-high PLP and the two-rate TCM policer is in color-aware mode, the policer assigns output loss priority as follows:

- If the rate of traffic flow is less than the CBS, the packets remain marked as medium-high PLP.
- If the rate of traffic flow is greater than the CBS but less than the EBS, the packets remain marked as medium-high PLP.
- If the rate of traffic flow is greater than the EBS, some of the packets are marked as high PLP and some remain marked as medium-high PLP.

Effect on Red Packets (High PLP)

Packets belonging to the red class have already been marked by a classifier with high PLP. Because the policer cannot decrease the PLP, it does not change it, and these packets are not metered against the CBS or the EBS.

Related Documentation

- Overview of Policers on page 41
- Configuring Color-Blind Egress Policers for Medium-Low PLP on page 58

Understanding Color-Blind Mode for Two-Rate Tricolor Marking

With the color-blind mode of two-rate tricolor marking, all packets are evaluated against the committed information rate (CIR). If a packet exceeds the CIR, it is evaluated against the peak information rate (PIR). Packets that exceed the CIR but are below the PIR are marked yellow (medium-high). Packets that exceed the PIR are marked red (high).

Table 11: Color-Blind Mode TCM Color-to-PLP Mapping

Color	PLP	Meaning
Green	**low**	Packet does not exceed the CIR.

Copyright © 2015, Juniper Networks, Inc.

Table 11: Color-Blind Mode TCM Color-to-PLP Mapping *(continued)*

Color	PLP	Meaning
Yellow	**medium-high**	Packet exceeds the CIR but does not exceed the PIR.
Red	**high**	Packet exceeds the PIR.

Related Documentation

- Overview of Policers on page 41
- Configuring Color-Blind Egress Policers for Medium-Low PLP on page 58

Understanding Color-Aware Mode for Two-Rate Tricolor Marking

In color-aware mode, the treatment the packet receives depends on its classification. Marking can increase the preassigned PLP but cannot decrease it

Summary of PLP Changes

Table 12 on page 50 shows how a packet's incoming priority can be modified with two-rate marking.

Table 12: Color-Aware Mode Two-Rate PLP Mapping

Incoming PLP	Packet Metered Against	Possible Cases	Outgoing PLP
low	CIR and PIR	Packet does not exceed the CIR.	**low**
		Packet exceeds the CIR but not the PIR.	**medium-high**
		Packet exceeds the PIR.	**high**
medium-low	PIR only	Packet does not exceed the PIR.	**medium-low**
		Packet exceeds the PIR.	**high**
medium-high	PIR only	Packet does not exceed the PIR.	**medium-high**
		Packet exceeds the PIR.	**high**
high	Not metered by the policer.	All cases.	**high**

The following sections describe color-aware two-rate PLP mapping in more detail.

Effect on Green Packets (Low PLP)

Packets belonging to the green class have already been marked by a classifier with low PLP. The marking policer can leave the packet's PLP unchanged or increase the PLP to medium-high or high. These packets are therefore metered against both the CIR and the

Copyright © 2015, Juniper Networks, Inc.

PIR. For example, if a behavior aggregate or multifield classifier marks a packet with low PLP and the two-rate TCM policer is in color-aware mode, the output loss priority is as follows:

- If the rate of traffic flow is less than the CIR, the packets remain marked as low PLP.
- If the rate of traffic flow is greater than the CIR but less than the PIR, some of the packets are marked as medium-high PLP and some of the packets remain marked as low PLP.
- If the rate of traffic flow is greater than the PIR, some of the packets are marked as high PLP and some of the packets remain marked as low PLP.

Effect on Yellow Packets (Medium PLP)

Packets belonging to the yellow class have already been marked by a classifier with medium-low or medium-high PLP. The marking policer can leave the PLP unchanged or increase it to high. These packets are therefore metered against the PIR only. For example, if a behavior aggregate (BA) or multifield classifier marks a packet with medium-low PLP and the two-rate TCM policer is in color-aware mode, the policer assigns output loss priority as follows:

- If the rate of traffic flow is less than the CIR, the packets remain marked as medium-low PLP.
- If the rate of traffic flow is greater than the CIR but less than the PIR, the packets remain marked as medium-low PLP.
- If the rate of traffic flow is greater than the PIR, some of the packets are marked as high PLP and some of the packets remain marked as medium-low PLP.

If a BA or multifield classifier marks a packet with medium-high PLP and the two-rate TCM policer is in color-aware mode, the policer assigns output loss priority as follows:

- If the rate of traffic flow is less than the CIR, the packets remain marked as medium-high PLP.
- If the rate of traffic flow is greater than the CIR but less than the PIR, the packets remain marked as medium-high PLP.
- If the rate of traffic flow is greater than the PIR, some of the packets are marked as high PLP and some of the packets remain marked as medium-high PLP.

Effect on Red Packets (High PLP)

Packets belonging to the red class have already been marked by a classifier with high PLP. Because the policer cannot decrease the PLP, it does not change it, and these packets are not metered against the CIR or the PIR.

Related Documentation

- Overview of Policers on page 41
- Configuring Color-Blind Egress Policers for Medium-Low PLP on page 58

Copyright © 2015, Juniper Networks, Inc.

Example: Using Two-Color Policers and Prefix Lists

If you provide specific amounts of bandwidth to internal or external customers, you can use policing to make sure that customers do not consume more bandwidth than they should receive. For example, you might connect many customers to one 10-Gbps interface and want to ensure that none of them congest the interface by using more bandwidth than they have been allotted.

You could accomplish this by creating a two-color policer similar to the following for each customer:

```
firewall {
    policer Limit-Customer-1 {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 150m;
        }
        then discard;
    }
```

Creating a policer for each customer is clearly not a scalable solution, however. As an alternative, you can create prefix lists that group classes of customers and then create policers for each prefix list. For example, you could create prefix lists such as **Class-A-Customer-Prefixes**, **Class-B-Customer-Prefixes**, and **Class-C-Customer-Prefixes** (at the **[edit policy-options]** hierarchy level) and create the following corresponding policers:

```
firewall {
    policer Class-A {
        if-exceeding {
            bandwidth-limit 100m;
            burst-size-limit 150m;
        }
        then discard;
    }
    policer Class-B {
        if-exceeding {
            bandwidth-limit 75m;
            burst-size-limit 100m;
        }
        then discard;
    }
    policer Class-C {
        if-exceeding {
            bandwidth-limit 50m;
            burst-size-limit 75m;
        }
        then discard;
    }
}
```

You must create filter terms that specify the prefix lists in their **from** statements and the corresponding policers in their **then** statements similar to the following:

Copyright © 2015, Juniper Networks, Inc.

```
firewall
  family inet {
    filter Class-A-Customers {
      term term-1 {
        from {
          destination-prefix-list {
            Class-A-Customer-Prefixes;
          }
        }
        then policer Class-A;
      }
    }
    filter Class-B-Customers {
      term term-1 {
        from {
          destination-prefix-list {
            Class-B-Customer-Prefixes;
          }
        }
        then policer Class-B;
      }
    }
    filter Class-C-Customers {
      term term-1 {
        from {
          destination-prefix-list {
            Class-C-Customer-Prefixes;
          }
        }
        then policer Class-C;
      }
    }
  }
```

Here are the steps to create this firewall configuration:

1. Create the first policer:

```
[edit firewall]
user@switch# set policer Class-A if-exceeding bandwidth-limit 100m burst-size-limit 150m
user@switch# set policer Class-A then discard
```

2. Create the second policer:

```
[edit firewall]
user@switch# set policer Class-B if-exceeding bandwidth-limit 75m burst-size-limit 100m
user@switch# set policer Class-B then discard
```

3. Create the third policer:

```
[edit firewall]
user@switch# set policer Class-C if-exceeding bandwidth-limit 50m burst-size-limit 75m
user@switch# set policer Class-C then discard
```

4. Create a filter for class A customers:

```
[edit firewall]
user@switch# edit family inet filter Class-A-Customers
```

5. Configure the filter to send packets matching the **Class-A-Customer-Prefixes** prefix list to the **Class-A** policer:

Copyright © 2015, Juniper Networks, Inc.

```
[edit firewall family inet filter Class-A-Customers]
user@switch# set term term-1 from source-prefix-list Class-A-Customers
user@switch# set term term-1 then policer Class-A
```

6. Create a filter for class B customers:

```
[edit firewall]
user@switch# edit family inet filter Class-B-Customers
```

7. Configure the filter to send packets matching the **Class-B-Customer-Prefixes** prefix list to the **Class-B** policer:

```
[edit firewall family inet filter Class-B-Customers]
user@switch# set term term-1 from source-prefix-list Class-B-Customers
user@switch# set term term-1 then policer Class-B
```

8. Create a filter for class C customers:

```
[edit firewall]
user@switch# edit family inet filter Class-C-Customers
```

9. Configure the filter to send packets matching the **Class-C-Customer-Prefixes** prefix list to the **Class-C** policer:

```
[edit firewall family inet filter Class-C-Customers]
user@switch# set term term-1 from source-prefix-list Class-C-Customers
user@switch# set term term-1 then policer Class-C
```

10. Apply the filters you created to the appropriate interfaces in the output direction.

NOTE: Note that the implicit deny statement in this filter will block traffic from any source that does not match one of the prefix lists. If you want the filter to allow this traffic, you must include an explicit term for this purpose.

Related Documentation

- Overview of Policers on page 41
- Applying Firewall Filters to Interfaces on page 33
- *prefix-list*

Example: Using Policers to Manage Oversubscription

You might want to use a policer when an interface is oversubscribed and you want to control what will happen if congestion occurs. For example, you might have servers connected to a switch as listed in Table 13 on page 54.

Table 13: Servers Connected to Switch

Server Type	Connection	IP Address
Network application server	1-gigabit interface	10.0.0.1
Authentication server	1-gigabit interface	10.0.0.2
Database server	10-gigabit interface	10.0.0.3

Copyright © 2015, Juniper Networks, Inc.

In this example, users access services provided by the network application server, which requests information from the database server as appropriate. When it receives a request from a user, the network application server first contacts the authentication server to verify the user's credentials. When a user is authenticated and the network application server provides the requested service, all the packets sent from the database server to the application server must transit the 1-Gigabit Ethernet interface connected to the application server twice—once on ingress to the application server and again on egress to the user.

The sequence of events for a user session is as follows:

1. A user connects to the application server and requests a service.
2. The application server requests the user's credentials and relays them to the authentication server.
3. If the authentication server verifies the credentials, the application server initiates the requested service.
4. The application server requests the files necessary to meet the user's request from the database server.
5. The database server sends the requested files to the application server.
6. The application server includes the requested files in its response to the user.

Traffic from the database server to the application server might congest the 1-gigabit interface to which that the application server is connected. This congestion might prevent the server from responding to requests from users and creating new sessions for them. You can use policing to make sure that this does not occur.

To create this firewall configuration, perform the following steps on the database server:

1. Create a policer to drop traffic from the database server to the application server if it exceeds certain limits:

   ```
   [edit firewall]
   user@switch# set policer Database-Egress-Policer if-exceeding bandwidth-limit 400
   burst-size-limit 500m
   user@switch# set policer Database-Egress-Policer then discard
   ```

2. Create a filter to examine traffic from the database server to the application server:

   ```
   [edit firewall]
   user@switch# edit family inet filter Database-Egress-Filter
   ```

3. Configure the filter to apply the policer to traffic egressing the database server and destined for the application server:

   ```
   [edit firewall family inet filter Database-Egress-Filter]
   user@switch# set term term-1 from destination-address 10.0.0.1
   user@switch# set term term-1 then policer Database-Egress-Policer
   ```

4. If required, configure a term to allow traffic from the database server to other destinations (otherwise the traffic will be dropped by the implicit deny statement):

   ```
   [edit firewall family inet filter Database-Egress-Filter]
   user@switch# set term term-2 then accept
   ```

Copyright © 2015, Juniper Networks, Inc.

Note that omitting a **from** statement causes the term to match all packets, which is the desired behavior.

5. Install the egress filter as an output filter on the database server interface that is connected the application server:

```
[edit interfaces]
user@switch# set xe-0/0/3 unit 0 family inet filter output Database-Egress-Filter
```

Here is how the final configuration would appear:

```
firewall {
  policer Database-Egress-Policer {
    if-exceeding {
      bandwidth-limit 400;
      burst-size-limit 500m;
    }
    then discard;
  }
  family inet {
    filter Database-Egress-Filter {
      term term-1 {
        from {
          destination-address {
            10.0.0.1/24;
          }
        }
        then policer Database-Egress-Policer;
      }
      term term-2 {  # If required, include this term so that traffic from the database server
        to other destinations is allowed.
        then accept;
      }
    }
  }
]
```

Related Documentation

- Overview of Policers on page 41

Copyright © 2015, Juniper Networks, Inc.

Assigning Forwarding Classes and Loss Priority

You can configure firewall filters to assign packet loss priority (PLP) and forwarding classes so that if congestion occurs, the marked packets can be dropped according to the priority you set. The valid match conditions are one or more of the six packet header fields: destination address, source address, IP protocol, source port, destination port, and DSCP. In other words, you can set the forwarding class and the PLP for each packet entering or an interface with a specific destination address, source address, IP protocol, source port, destination port, or DSCP.

NOTE: **Junos OS assigns forwarding classes and PLP on ingress only. Do not use a filter that assigns forwarding classes or PLP as an egress filter.**

When tricolor marking is enabled, a switch supports four PLP designations: **low**, **medium-low**, **medium-high**, and **high**. You can also specify any of the forwarding classes listed in Table 14 on page 57

Table 14: Unicast Forwarding Classes

Unicast Forwarding Class	For CoS Traffic Type
be	Best-effort traffic
no-loss	Guaranteed delivery for TCP traffic
fcoe	Guaranteed delivery for Fibre Channel over Ethernet (FCoE) traffic
nc	Network-control traffic

To assign forwarding classes in firewall filters:

1. Configure the family address type and filter name:

   ```
   [edit]
   user@switch# edit firewall family inetfilter ingress-filter
   ```

2. Configure the terms of the filter as appropriate, including the **forwarding-class** and **loss-priority** action modifiers. For example, each of the following terms in the filter examines various packet header fields and assigns the appropriate forwarding class and packet loss priority:

   - The term **corp-traffic** matches all IPv4 packets with a **10.1.1.0/24** source address and assigns the packets to forwarding class **no-loss** with a loss priority of **low**:

     ```
     [edit firewall family inet filter ingress-filter]
     user@switch# set term corp-traffic from source-address 10.1.1.0/24;
     user@switch# set term corp-traffic then forwarding-class no-loss
     user@switch# set term corp-traffic then loss-priority low
     ```

   - The term **data-traffic** matches all IPv4 packets with a **10.1.2.0/24** source address and assigns the packets to forwarding class **be** (best effort) with a loss priority of **medium-high**:

Copyright © 2015, Juniper Networks, Inc.

```
[edit firewall family inet filter ingress-filter]
user@switch# set term data-traffic from source-address 10.1.2.0/24;
user@switch# set term data-traffic then forwarding-class be
user@switch# set term data-traffic then loss-priority medium-high
```

- The last term **accept-traffic** matches any packets that did not match on any of the preceding terms and assigns the packets to forwarding class **be** with a loss priority of **high**:

```
[edit firewall family inet filter ingress-filter]
user@switch# set term accept-traffic then forwarding-class be
user@switch# set term accept-traffic then loss-priority high
```

3. Apply the filter **ingress-filter** to a Layer 3 interface. For information about applying the filter, see *Configuring Firewall Filters*. (Assigning forwarding classes and PLP is supported only on ingress filters.)

Related Documentation

- *Configuring Firewall Filters*
- Verifying That Firewall Filters Are Operational on page 36
- Monitoring Firewall Filter Traffic on page 35
- Overview of Policers on page 41
- *Understanding CoS Classifiers*
- *Understanding CoS Forwarding Classes*

Configuring Color-Blind Egress Policers for Medium-Low PLP

If you use color-blind mode and want to configure an egress policer that marks packets to have medium-low PLP, you must configure a single-rate two-color policer at the **[edit firewall policer *policer-name*]** hierarchy level, because color-blind mode does not support medium-low priority. For example:

1. Specify the name of the policer, the bandwidth limit in bits per second (bps) to control the traffic rate on an interface, and the maximum allowed burst size to control the amount of traffic bursting:

```
[edit]
user@switch# set firewall policer policer-name if-exceeding bandwidth-limit bytes
burst-size-limit bytes
```

2. Specify medium-low loss priority for matching packets:

```
[edit]
user@switch# set firewall policer policer-name then loss-priority medium-low;
```

3. Apply the filter to a port, VLAN, or Layer 3 interface.

Related Documentation

- Overview of Policers on page 41
- Understanding Color-Blind Mode for Single-Rate Tricolor Marking on page 47
- Understanding Color-Blind Mode for Two-Rate Tricolor Marking on page 49
- *Configuring Firewall Filters*
- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59

Copyright © 2015, Juniper Networks, Inc.

Configuring Two-Color and Three-Color Policers to Control Traffic Rates

You can rate-limit traffic 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.

NOTE: **You can include two-color policer actions on ingress firewall filters only. You can include three-color policer actions on ingress and egress filters.**

Configuring Two-Color Policers

To configure a two-color policer:

1. Specify the name of the policer, the bandwidth limit to control the traffic rate on an interface, and the maximum allowed burst size to control the amount of traffic bursting:

   ```
   [edit firewall]
   user@switch# set policer policer-name <filter-specific> if-exceeding bandwidth-limit bps
   burst-size-limit bytes
   ```

   The policer name can contain letters, numbers, and hyphens (-) and can have as many as 64 characters.

   The range for the bandwidth limit is 32000 (32k) through 102,300,000,000 (102300m) bps.

   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 and divide the result by 8:

   maximum burst size = (interface bandwidth) X (allowable time for burst) / (8 bits/byte)

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

2. Specify the policer action to discard or assign a loss priority to packets that exceed the rate limits:

   ```
   [edit firewall policer policer-name]
   ```

Copyright © 2015, Juniper Networks, Inc.

```
user@switch# set then (discard | loss-priority low | loss-priority high)
```

Configuring Three-Color Policers

To configure a three-color 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 whether the three-color policer should be single-rate or two-rate and whether it should be color-aware or color-blind:

   ```
   [edit firewall three-color-policer policer-name]
   user@switch# set (single-rate | two-rate) (color-aware | color-blind)
   ```
3. For single-rate three-color policers, configure the CIR, CBS, and 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 two-rate three-color policers, configure the CIR, CBS, PIR, and 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
   ```

Specifying Policers in a Firewall Filter Configuration

To use a two-color policer, configure a filter term that includes the action **policer**:

```
[edit firewall family family-name]
user@switch# set filter filter-name term name then name
```

For example, the following commands apply a two-color policer to all packets sent from 192.0.2.0/24.

```
[edit firewall family family-name]
user@switch# set filter limit—hosts term term1 from source-address 192.0.2.0/24
user@switch# set filter limit—hosts term term1 then policer policer1
```

To use a three-color policer, configure a filter term that includes the action **three-color-policer**:

```
[edit firewall family name]
user@switch# set filter name term name from match-condition
user@switch# set filter name term name then three-color-policer (single-rate | two-rate) name
```

For example, the following commands apply a single-rate three-color policer to all packets received or sent by interface **ge-0/0/6** (depending on whether the filter is an ingress or egress filter).

```
[edit firewall family name]
user@switch# set filter srTCM term term-one from interface ge-0/0/6
user@switch# set filter srTCM term term-one then three-color-policer single-rate srTCM1-ca
```

You must specify whether the three-color policer is single-rate or two-rate, and this must match the policer itself. Otherwise, the configuration listing includes an error message indicating that the three-color policer you referenced in the filter does not exist.

Copyright © 2015, Juniper Networks, Inc.

Applying a Firewall Filter That Includes a Policer

A firewall filter that includes one or more policer action modifiers must be applied to a port, VLAN, or Layer 3 interface like any other filter. For information about applying firewall filters, see *Configuring Firewall Filters*.

NOTE: You can include two-color policer actions on ingress firewall filters only. You can include three-color policer actions on ingress and egress filters.

Related Documentation

- *Configuring Firewall Filters*
- Overview of Policers on page 41
- Verifying That Two-Color Policers Are Operational on page 61
- Verifying That Three-Color Policers Are Operational on page 61
- Configuring Color-Blind Egress Policers for Medium-Low PLP on page 58

Verifying That Three-Color Policers Are Operational

Purpose Verify that three-color policers in firewall filter configurations are working properly.

Action Use the following operational mode commands to verify that a three-color policer is working properly:

- **show class-of-service forwarding-table classifiers**
- **show interfaces** ***interface-name*** **extensive**
- **show interfaces queue** ***interface-name***

Related Documentation

- Overview of Policers on page 41
- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59

Verifying That Two-Color Policers Are Operational

Purpose Verify that two-color policers in firewall filter configurations are working properly.

Action Use the **show firewall policer** operational mode command to verify that the policers are working properly:

```
user@switch> show firewall policer
Filter: egress-vlan-watch-employee
Filter: ingress-port-filter
Filter: ingress-port-limit-tcp-icmp
Policers:
Name                                                Packets
icmp-connection-policer                                  10
tcp-connection-policer                                  539
```

Copyright © 2015, Juniper Networks, Inc.

```
Filter: ingress-vlan-rogue-block
Filter: ingress-vlan-limit-guest
```

Meaning The **show firewall policer** command displays the names of all firewall filters and policers that are configured. 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.

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59
- *Configuring Firewall Filters*
- Monitoring Firewall Filter Traffic on page 35

Troubleshooting Policer Configuration

Incomplete Count of Packet Drops

Problem **Description:** Under certain circumstances, Junos OS might display a misleading number of packets dropped by an ingress policer.

If packets are dropped because of ingress admission control, policer statistics might not show the number of packet drops you would expect by calculating the difference between ingress and egress packet counts. This might happen if you apply an ingress policer to multiple interfaces, and the aggregate ingress rate of those interfaces exceeds the line rate of a common egress interface. In this case, packets might be dropped from the ingress buffer. These drops are not included in the count of packets dropped by the policer, which causes policer statistics to underreport the total number of drops.

Solution This is expected behavior.

Counter Reset When Editing Filter

Problem **Description:** If you edit a firewall filter term, the value of any counter associated with any term in the same filter is set to 0, including the implicit counter for any policer referenced by the filter. Consider the following examples:

- Assume that your filter has **term1**, **term2**, and **term3**, and each term has a counter that has already counted matching packets. If you edit any of the terms in any way, the counters for all the terms are reset to 0.
- Assume that your filter has **term1** and **term2**. Also assume that **term2** has a **policer** action modifier and the implicit counter of the policer has already counted 1000 matching packets. If you edit **term1** or **term2** in any way, the counter for the policer referenced by **term2** is reset to 0.

Copyright © 2015, Juniper Networks, Inc.

Solution This is expected behavior.

Invalid Statistics for Policer

Problem **Description:** If you apply a single-rate two-color policer in more than 128 terms in a firewall filter, the output of the **show firewall** command displays incorrect data for the policer.

Solution This is expected behavior.

Policers Can Limit Egress Filters

Problem **Description:** The number of egress policers that you configure can affect the total number of allowed egress firewall filters. Every policer has two implicit counters that consume two entries in a 1024-entry TCAM that is used for counters, including counters that are configured as action modifiers in firewall filter terms. (Policers consume two entries because one is used for green packets and one is used for nongreen packets regardless of policer type.) If the TCAM becomes full, you cannot commit any more egress firewall filters that have terms with counters. For example, if you configure and commit 512 egress policers (two-color, three-color, or a combination of both policer types), all of the memory entries for counters are used up. If later in your configuration file you insert additional egress firewall filters with terms that also include counters, *none* of the terms in those filters are committed because there is no available memory space for the counters.

Here are some additional examples:

- Assume that you configure egress filters that include a total of 512 policers and no counters. Later in your configuration file you include another egress filter with 10 terms, 1 of which has a counter action modifier. None of the terms in this filter are committed because there is not enough TCAM space for the counter.
- Assume that you configure egress filters that include a total of 500 policers, so 1000 TCAM entries are occupied. Later in your configuration file you include the following two egress filters:
  - Filter A with 20 terms and 20 counters. All the terms in this filter are committed because there is enough TCAM space for all the counters.
  - Filter B comes after Filter A and has five terms and five counters. *None* of the terms in this filter are committed because there is not enough memory space for *all* the counters. (Five TCAM entries are required but only four are available.)

Solution You can prevent this problem by ensuring that egress firewall filter terms with counter actions are placed earlier in your configuration file than terms that include policers. In this circumstance, Junos OS commits policers even if there is not enough TCAM space for the implicit counters. For example, assume the following:

- You have 1024 egress firewall filter terms with counter actions.

Copyright © 2015, Juniper Networks, Inc.

- Later in your configuration file you have an egress filter with 10 terms. None of the terms have counters but one has a policer action modifier.

You can successfully commit the filter with 10 terms even though there is not enough TCAM space for the implicit counters of the policer. The policer is committed without the counters.

Copyright © 2015, Juniper Networks, Inc.

PART 3

Using Port Security

Copyright © 2015, Juniper Networks, Inc.

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 3

Port Security

Understanding Trusted DHCP Servers for Port Security

Any interface on the switching device that connects to a DHCP server can be configured as a trusted port. Configuring a DHCP server on a trusted port protects against rogue DHCP servers sending leases.

Ensure that the DHCP server interface is physically secure—that is, that access to the server is monitored and controlled at the site—before you configure the port as trusted.

Related Documentation

- *Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks*
- *Enabling a Trusted DHCP Server (CLI Procedure)*

Verifying That a Trusted DHCP Server Is Working Correctly

Purpose Verify that a DHCP trusted server is working on the switch. See what happens when the DHCP server is trusted and then untrusted.

Copyright © 2015, Juniper Networks, Inc.

Action Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.

Display the DHCP snooping information when the interface on which the DHCP server connects to the switch is trusted. The following output results when requests are sent from the MAC addresses and the server has provided the IP addresses and leases:

```
user@switch> show dhcp snooping binding
DHCP Snooping Information:
MAC Address         IP Address    Lease    Type     VLAN          Interface
-----------------   ----------    -----    ----     ----          ---------
00:05:85:3A:82:77    192.0.2.17    600    dynamic  employee-vlan   ge-0/0/1.0
00:05:85:3A:82:79    192.0.2.18    653    dynamic  employee-vlan   ge-0/0/1.0
00:05:85:3A:82:80    192.0.2.19    720    dynamic  employee-vlan   ge-0/0/2.0
00:05:85:3A:82:81    192.0.2.20    932    dynamic  employee-vlan   ge-0/0/2.0
00:05:85:3A:82:83    192.0.2.21   1230    dynamic  employee-vlan   ge-0/0/2.0
00:05:85:27:32:88    192.0.2.22   3200    dynamic  employee-vlan   ge-0/0/2.0
```

Meaning When the interface on which the DHCP server connects to the switch has been set to trusted, the output (see preceding sample) shows, for each MAC address, the assigned IP address and lease time—that is, the time, in seconds, remaining before the lease expires.

If the DHCP server had been configured as untrusted, no entries would be added to the DHCP snooping database and nothing would be shown in the output of the **show dhcp snooping binding** command.

Related Documentation

- *Enabling a Trusted DHCP Server (CLI Procedure)*
- *Enabling a Trusted Port for DHCP*
- *Example: Configuring Basic Port Security Features*
- *Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks*
- *Monitoring Port Security*
- *Troubleshooting Port Security*

Copyright © 2015, Juniper Networks, Inc.

Understanding DHCP Option 82 for Port Security

You can use DHCP option 82, also known as the DHCP relay agent information option, to help protect the switch against attacks such as spoofing (forging) of IP addresses and MAC addresses, and DHCP IP address starvation. Hosts on untrusted access interfaces on Ethernet LAN switches send requests for IP addresses in order to access the Internet. The switch forwards or relays these requests to DHCP servers, and the servers send offers for IP address leases in response. Attackers can use these messages to perpetrate address spoofing and 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. The Juniper Networks Junos operating system (Junos OS) implementation of DHCP option 82 supports RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046.

This topic covers:

DHCP Option 82 Processing

If DHCP option 82 is enabled on the switch, then when a DHCP client that is connected to the switch on an untrusted interface sends a DHCP request, the switch inserts information about the client's network location into the packet header of that request. The switch then sends the request to the DHCP server. The DHCP server reads the option 82 information in the packet header and uses it to implement the IP address or another parameter for the client. See "Suboption Components of Option 82" on page 70 for details about option 82 information.

You can enable DHCP option 82 on a single VLAN or on all VLANs on the switch. You can also configure it on Layer 3 interfaces (in routed VLAN interfaces, or RVIs) when the switch is functioning as a relay agent.

When option 82 is enabled on the switch, then this sequence of events occurs when a DHCP client sends a DHCP request:

1. The switch receives the request and inserts the option 82 information in the packet header.
2. The switch forwards or relays the request to the DHCP server.
3. The server uses the DHCP option 82 information to formulate its reply and sends a response back to the switch. It does not alter the option 82 information.
4. The switch strips the option 82 information from the response packet.
5. The switch forwards the response packet to the client.

Copyright © 2015, Juniper Networks, Inc.

NOTE: To use the DHCP option 82 feature, you must ensure that the DHCP server is configured to accept option 82. If it is not configured to accept option 82, then when it receives requests containing option 82 information, it does not use the information in setting parameters and it does not echo the information in its response message.

Suboption Components of Option 82

When configuring DHCP option 82, you can use the following suboptions:

- circuit ID—Identifies the circuit (interface and/or VLAN) on the switch on which the request was received. The circuit ID contains the interface name and/or VLAN name, with the two elements separated by a colon—for example, **xe-0/0/10:vlan1**. If the request packet is received on a Layer 3 interface, the circuit ID is just the interface name—for example, **xe-0/0/10**.

  Use the **prefix** option to add an optional prefix to the circuit ID. If you enable the **prefix** option, the hostname for the switch is used as the prefix; for example, **switch1:xe-0/0/10:vlan1**..

  You can also specify that the interface description be used rather than the interface name and that the VLAN ID be used rather than the VLAN name.

- remote ID—Identifies the host. By default, the remote ID is the MAC address of the switch. You can specify that the remote ID be the hostname of the switch, the interface description, or a character string of your choice. You can also add an optional prefix to the remote ID.

- vendor ID—Identifies the vendor of the host. If you specify the **vendor-id** option but do not enter a value, the default value **Juniper** is used. To specify a value, you type a character string.

Configurations That Support Option 82

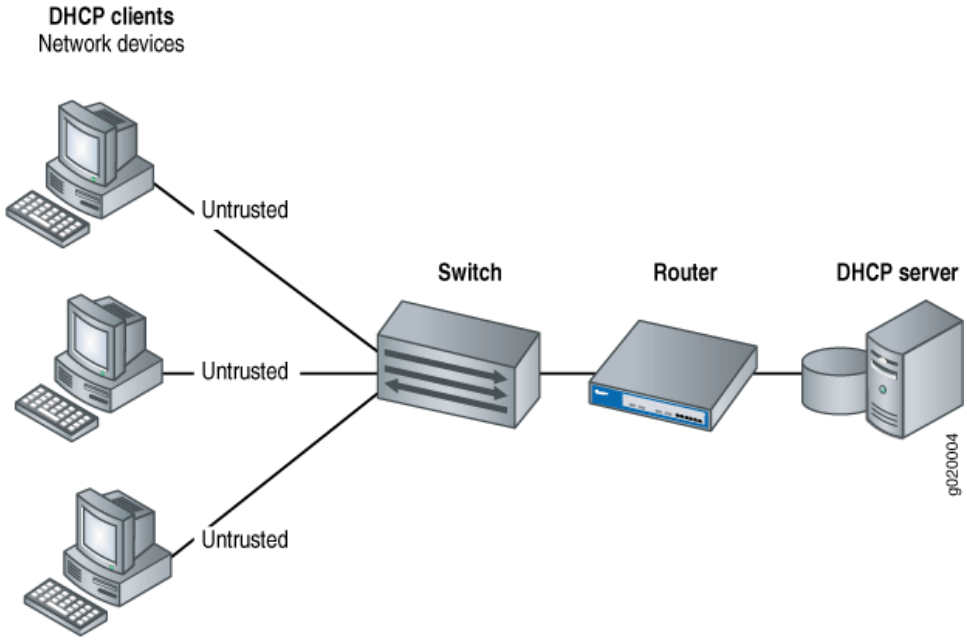
You can use option 82 with the following configurations:

- The DHCP client and the DHCP server are on the same VLAN. In this case the switch forwards the requests from the clients on untrusted access interfaces to the server on a trusted interface. For this configuration, you set DHCP option 82 at the **[edit ethernet-switching-options secure-access-port vlan]** hierarchy level.

- The DHCP client or the DHCP server is connected to the switch through a Layer 3 interface and the switch is configured to relay DHCP requests. Figure 4 on page 71 illustrates a scenario for the switch-as-relay-agent; in this instance, the switch relays requests through a router to the server.

 Copyright © 2015, Juniper Networks, Inc.

Figure 4: Switch Relays DHCP Requests to Server



For the configuration shown in Figure 4 on page 71, you set DHCP option 82 at the **[edit forwarding-options helpers bootp]** hierarchy level.

Related Documentation

- *Overview of Access Port Protection*
- *DHCP and BOOTP Relay Overview*
- *dhcp-option82*
- *Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server*
- *Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server*
- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- *Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure)*

Copyright © 2015, Juniper Networks, Inc.

Copyright © 2015, Juniper Networks, Inc.

PART 4

Using Device Security

Copyright © 2015, Juniper Networks, Inc.

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 4

Device Security

Understanding Unicast RPF

Unicast reverse-path forwarding (RPF) helps protect the switch against denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks by verifying the unicast source address of each packet that arrives on an ingress interface where unicast RPF is enabled. It also helps ensure that traffic arriving on ingress interfaces comes from a network source that the receiving interface can reach.

When you enable unicast RPF, the switch forwards a packet only if the receiving interface is the best return path to the packet's unicast source address. This is known as strict mode unicast RPF.

NOTE: On Juniper Networks EX3200, EX4200, and EX4300 Ethernet Switches, the switch applies unicast RPF *globally* to all interfaces when unicast RPF is configured on any interface. For additional information, see "Limitations of the Unicast RPF Implementation on EX3200, EX4200, and EX4300 Switches" on page 78.

This topic covers:

Copyright © 2015, Juniper Networks, Inc.

Unicast RPF for Switches Overview

Unicast RPF functions as an ingress filter that reduces the forwarding of IP packets that might be spoofing an address. By default, unicast RPF is disabled on the switch interfaces.

The type of unicast RPF provided on the switches—that is, strict mode unicast RPF is especially useful on untrusted interfaces. An untrusted interface is an interface where untrusted users or processes can place packets on the network segment.

The switch supports only the active paths method of determining the best return path back to a unicast source address. The active paths method looks up the best reverse path entry in the forwarding table. It does not consider alternate routes specified using routing-protocol-specific methods when determining the best return path.

If the forwarding table lists the receiving interface as the interface to use to forward the packet back to its unicast source, it is the best return path interface.

Use strict mode unicast RPF only on symmetrically routed interfaces. (For information about symmetrically routed interfaces, see "When to Enable Unicast RPF" on page 77.)

For more information about strict unicast RPF, see RFC 3704, *Ingress Filtering for Multihomed Networks* at http://www.ietf.org/rfc/rfc3704.txt.

Unicast RPF Implementation

This section includes:

Unicast RPF Packet Filtering

When you enable unicast RPF on the switch, the switch handles traffic in the following manner:

- If the switch receives a packet on the interface that is the best return path to the unicast source address of that packet, the switch forwards the packet.
- If the best return path from the switch to the packet's unicast source address is not the receiving interface, the switch discards the packet.
- If the switch receives a packet that has a source IP address that does not have a routing entry in the forwarding table, the switch discards the packet.

Bootstrap Protocol (BOOTP) and DHCP Requests

Bootstrap protocol (BOOTP) and DHCP request packets are sent with a broadcast MAC address and therefore the switch does not perform unicast RPF checks on them. The switch forwards all BOOTP packets and DHCP request packets without performing unicast RPF checks.

Copyright © 2015, Juniper Networks, Inc.

Default Route Handling

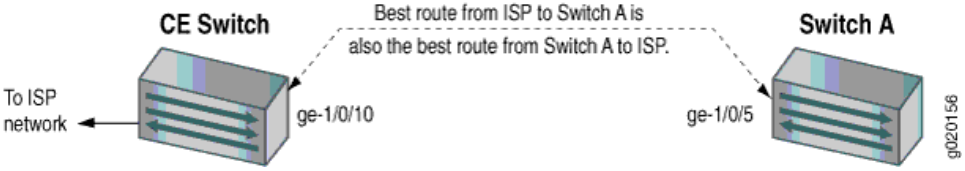
If the best return path to the source is the default route (**0.0.0.0**) and the default route points to **reject**, the switch discards the packets. If the default route points to a valid network interface, the switch performs a normal unicast RPF check on the packets.

When to Enable Unicast RPF

Enable unicast RPF when you want to ensure that traffic arriving on a network interface comes from a source that resides on a network that that interface can reach. You can enable unicast RPF on untrusted interfaces to filter spoofed packets. For example, a common application for unicast RPF is to help defend an enterprise network from DoS/DDoS attacks coming from the Internet.

Enable unicast RPF only on symmetrically routed interfaces. A symmetrically routed interface uses the same route in both directions between the source and the destination, as shown in Figure 5 on page 77. Symmetrical routing means that if an interface receives a packet, the switch uses the same interface to send a reply to the packet source (the receiving interface matches the forwarding-table entry for the best return path to the source).

Figure 5: Symmetrically Routed Interfaces



Enabling unicast RPF on asymmetrically routed interfaces (where different interfaces receive a packet and reply to its source) results in packets from legitimate sources being filtered (discarded) because the best return path is not the same interface that received the packet.

The following switch interfaces are most likely to be symmetrically routed and thus are candidates for unicast RPF enabling:

- The service provider edge to a customer
- The customer edge to a service provider
- A single access point out of the network (usually on the network perimeter)
- A terminal network that has only one link

NOTE: Because unicast RPF is enabled globally on EX3200, EX4200, and EX4300 switches, ensure that *all* interfaces are symmetrically routed before you enable unicast RPF on these switches. Enabling unicast RPF on asymmetrically routed interfaces results in packets from legitimate sources being filtered.

Copyright © 2015, Juniper Networks, Inc.

TIP: Enabling unicast RPF as close as possible to the traffic source stops spoofed traffic before it can proliferate or reach interfaces that do not have unicast RPF enabled.

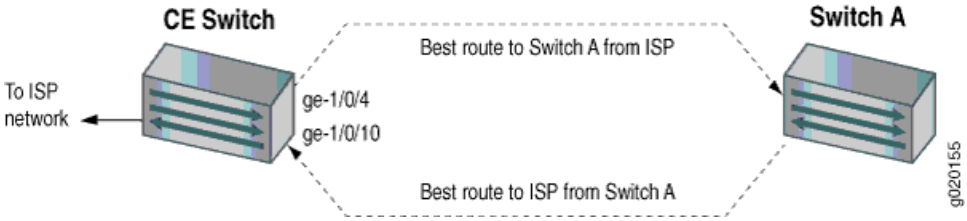
When Not to Enable Unicast RPF

Typically, you will not enable unicast RPF if:

- Switch interfaces are multihomed.
- Switch interfaces are trusted interfaces.
- BGP is carrying prefixes and some of those prefixes are not advertised or are not accepted by the ISP under its policy. (The effect in this case is the same as filtering an interface by using an incomplete access list.)
- Switch interfaces face the network core. Core-facing interfaces are usually asymmetrically routed.

An asymmetrically routed interface uses different paths to send and receive packets between the source and the destination, as shown in Figure 6 on page 78. This means that if an interface receives a packet, that interface does not match the forwarding table entry as the best return path back to the source. If the receiving interface is not the best return path to the source of a packet, unicast RPF causes the switch to discard the packet even though it comes from a valid source.

Figure 6: Asymmetrically Routed Interfaces



NOTE: Do not enable unicast RPF on EX3200, EX4200, and EX4300 switches if any switch interfaces are asymmetrically routed, because unicast RPF is enabled globally on all interfaces of these switches. All switch interfaces must be symmetrically routed for you to enable unicast RPF without the risk of the switch discarding traffic that you want to forward.

Limitations of the Unicast RPF Implementation on EX3200, EX4200, and EX4300 Switches

On EX3200, EX4200, and EX4300 switches, the switch implements unicast RPF on a global basis. You cannot enable unicast RPF on a per-interface basis. Unicast RPF is globally disabled by default.

Copyright © 2015, Juniper Networks, Inc.

- When you enable unicast RPF on any interface, it is automatically enabled on all switch interfaces, including link aggregation groups (LAGs), integrated routing and bridging (IRB) interfaces, and routed VLAN interfaces (RVIs).
- When you disable unicast RPF on the interface (or interfaces) on which you enabled unicast RPF, it is automatically disabled on all switch interfaces.

NOTE: **You must explicitly disable unicast RPF on every interface on which it was explicitly enabled or unicast RPF remains enabled on all switch interfaces.**

QFX switches, OCX switches, and EX3200 and EX4200 switches do not perform unicast RPF filtering on equal-cost multipath (ECMP) traffic. The unicast RPF check examines only one best return path to the packet source, but ECMP traffic employs an address block consisting of multiple paths. Using unicast RPF to filter ECMP traffic on these switches can result in the switch discarding packets that you want to forward because the unicast RPF filter does not examine the entire ECMP address block.

Related Documentation

- *Example: Configuring Unicast RPF on an EX Series Switch*
- Configuring Unicast RPF (CLI Procedure) on page 79
- Disabling Unicast RPF (CLI Procedure) on page 81

Configuring Unicast RPF (CLI Procedure)

Unicast reverse-path forwarding (RPF) can help protect your LAN from denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks on untrusted interfaces. Enabling unicast RPF on the switch interfaces filters traffic with source addresses that do not use the incoming interface as the best return path back to the source. When a packet comes into an interface, if that interface is not the best return path to the source, the switch discards the packet. If the incoming interface is the best return path to the source, the switch forwards the packet.

NOTE: **On EX3200, EX4200, and EX4300 switches, you can enable unicast RPF only globally—that is, on all switch interfaces. You cannot enable unicast RPF on a per-interface basis.**

Before you begin:

- On an EX8200, EX6200, QFX Series switch, or OCX Series switch, ensure that the selected switch interface is symmetrically routed before you enable unicast RPF. A symmetrically routed interface is an interface that uses the same route in both directions between the source and the destination. Do not enable unicast RPF on asymmetrically routed interfaces. An asymmetrically routed interface uses different paths to send and receive packets between the source and the destination.

Copyright © 2015, Juniper Networks, Inc.

- On an EX3200, EX4200, or EX4300 switch, ensure that *all* switch interfaces are symmetrically routed before you enable unicast RPF on an interface. When you enable unicast RPF on any interface, it is enabled globally on all switch interfaces. Do not enable unicast RPF on asymmetrically routed interfaces. An asymmetrically routed interface uses different paths to send and receive packets between the source and the destination.

To enable unicast RPF, configure it explicitly on a selected customer-edge interface:

```
[edit interfaces]
user@switch# set ge-1/0/10 unit 0 family inet rpf-check
```

BEST PRACTICE: On EX3200, EX4200, and EX4300 switches, unicast RPF is enabled globally on *all* switch interfaces, regardless of whether you configure it explicitly on only one interface or only on some interfaces.

On EX3200, EX4200, and EX4300 switches, we recommend that you enable unicast RPF explicitly on either all interfaces or only one interface. To avoid possible confusion, do not enable it on only some interfaces:

- Enabling unicast RPF explicitly on only one interface makes it easier if you choose to disable it in the future because you must explicitly disable unicast RPF on every interface on which you explicitly enabled it. If you explicitly enable unicast RPF on two interfaces and you disable it on only one interface, unicast RPF is still implicitly enabled globally on the switch. The drawback of this approach is that the switch displays the flag that indicates that unicast RPF is enabled only on interfaces on which unicast RPF is explicitly enabled, so even though unicast RPF is enabled on all interfaces, this status is not displayed.
- Enabling unicast RPF explicitly on all interfaces makes it easier to know whether unicast RPF is enabled on the switch because every interface shows the correct status. (Only interfaces on which you explicitly enable unicast RPF display the flag that indicates that unicast RPF is enabled.) The drawback of this approach is that if you want to disable unicast RPF, you must explicitly disable it on every interface. If unicast RPF is enabled on any interface, it is implicitly enabled on all interfaces.

Related Documentation

- *Example: Configuring Unicast RPF on an EX Series Switch*
- Verifying Unicast RPF Status on page 81
- Disabling Unicast RPF (CLI Procedure) on page 81
- *Troubleshooting Unicast RPF*
- Understanding Unicast RPF on page 75

Copyright © 2015, Juniper Networks, Inc.

Disabling Unicast RPF (CLI Procedure)

Unicast reverse-path forwarding (RPF) can help protect your LAN from denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks on untrusted interfaces. Unicast RPF filters traffic with source addresses that do not use the incoming interface as the best return path back to the source. If the network configuration changes so that an interface that has unicast RPF enabled becomes a trusted interface or becomes asymmetrically routed (the interface that receives a packet is not the best return path to the packet's source), disable unicast RPF.

To disable unicast RPF on an EX3200, EX4200, or EX4300 switch, you must delete it from every interface on which you explicitly configured it. If you do not disable unicast RPF on every interface on which you explicitly enabled it, it remains implicitly enabled on all interfaces. If you attempt to delete unicast RPF from an interface on which it was not explicitly enabled, the **warning: statement not found** message appears. If you do not disable unicast RPF on every interface on which you explicitly enabled it, unicast RPF remains implicitly enabled on all interfaces of the EX3200, EX4200, or EX4300 switch.

On EX8200, EX6200, QFX Series switches, and OCX Series switches, the switch does not apply unicast RPF to an interface unless you explicitly enable that interface for unicast RPF.

To disable unicast RPF, delete its configuration from the interface:

```
[edit interfaces]
user@switch# delete ge-1/0/10 unit 0 family inet rpf-check
```

NOTE: On EX3200, EX4200, and EX4300 switches, if you do not disable unicast RPF on every interface on which you explicitly enabled it, unicast RPF remains implicitly enabled on all interfaces.

Related Documentation

- *Example: Configuring Unicast RPF on an EX Series Switch*
- Verifying Unicast RPF Status on page 81
- Configuring Unicast RPF (CLI Procedure) on page 79
- Understanding Unicast RPF on page 75

Verifying Unicast RPF Status

Purpose Verify that unicast reverse-path forwarding (RPF) is enabled and is working on the interface.

Action Use one of the **show interfaces *interface-name*** commands with either the **extensive** or **detail** options to verify that unicast RPF is enabled and working on the switch. The following example displays output from the **show interfaces ge- extensive** command.

```
user@switch> show interfaces ge-1/0/10 extensive
```

Copyright © 2015, Juniper Networks, Inc.

```
Physical interface: ge-1/0/10, Enabled, Physical link is Down
  Interface index: 139, SNMP ifIndex: 58, Generation: 140
  Link-level type: Ethernet, MTU: 1514, Speed: Auto, MAC-REWRITE Error: None,
  Loopback: Disabled, Source filtering: Disabled, Flow control: Enabled,
  Auto-negotiation: Enabled, Remote fault: Online
  Device flags   : Present Running
  Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: 00:19:e2:50:95:ab, Hardware address: 00:19:e2:50:95:ab
  Last flapped   : Never
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :                    0                    0 bps
   Output bytes  :                    0                    0 bps
   Input  packets:                    0                    0 pps
   Output packets:                    0                    0 pps
   IPv6 transit statistics:
    Input  bytes  :                   0
    Output bytes  :                   0
    Input  packets:                   0
    Output packets:                   0
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0,
    L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
    FIFO errors: 0, Resource errors: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,

    FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
  Egress queues: 8 supported, 4 in use
  Queue counters:       Queued packets  Transmitted packets      Dropped packets

    0 best-effort                   0                    0                    0

    1 assured-forw                  0                    0                    0

    5 expedited-fo                  0                    0                    0

    7 network-cont                  0                    0                    0

  Active alarms  : LINK
  Active defects : LINK
  MAC statistics:                      Receive         Transmit
    Total octets                             0                0
    Total packets                            0                0
    Unicast packets                          0                0
    Broadcast packets                        0                0
    Multicast packets                        0                0
    CRC/Align errors                         0                0
    FIFO errors                              0                0
    MAC control frames                       0                0
    MAC pause frames                         0                0
    Oversized frames                         0
    Jabber frames                            0
    Fragment frames                          0
    VLAN tagged frames                       0
    Code violations                          0
  Filter statistics:
    Input packet count                       0
```


Copyright © 2015, Juniper Networks, Inc.

```
  Input packet rejects                    0
  Input DA rejects                        0
  Input SA rejects                        0
  Output packet count                                    0
  Output packet pad count                                0
  Output packet error count                              0
  CAM destination filters: 0, CAM source filters: 0
Autonegotiation information:
  Negotiation status: Incomplete
Packet Forwarding Engine configuration:
  Destination slot: 1

Logical interface ge-1/0/10.0 (Index 69) (SNMP ifIndex 59) (Generation 135)
  Flags: Device-Down SNMP-Traps 0x0 Encapsulation: ENET2
  Traffic statistics:
   Input  bytes  :                  0
   Output bytes  :                  0
   Input  packets:                  0
   Output packets:                  0
   IPv6 transit statistics:
    Input  bytes  :                 0
    Output bytes  :                 0
    Input  packets:                 0
    Output packets:                 0
  Local statistics:
   Input  bytes  :                  0
   Output bytes  :                  0
   Input  packets:                  0
   Output packets:                  0
  Transit statistics:
   Input  bytes  :                  0                    0 bps
   Output bytes  :                  0                    0 bps
   Input  packets:                  0                    0 pps
   Output packets:                  0                    0 pps
   IPv6 transit statistics:
    Input  bytes  :                 0
    Output bytes  :                 0
    Input  packets:                 0
    Output packets:                 0
      Protocol inet, Generation: 144, Route table: 0
    Flags: uRPF
    Addresses, Flags: Is-Preferred Is-Primary
```

Meaning The **show interfaces ge-1/0/10 extensive** command (and the **show interfaces ge-1/0/10 detail** command) displays in-depth information about the interface. The **Flags:** output field near the bottom of the display reports the unicast RPF status. If unicast RPF has not been enabled, the **uRPF** flag is not displayed.

On EX3200, EX4200, and EX4300 switches, unicast RPF is implicitly enabled on *all* switch interfaces, including aggregated Ethernet interfaces (also referred to as link aggregation groups or LAGs), integrated routing and bridging (IRB) interfaces, and routed VLAN interfaces (RVIs) when you enable unicast RPF on a single interface. However, the unicast RPF status is shown as enabled only on interfaces for which you have explicitly configured unicast RPF. Thus, the **uRPF** flag is not displayed on interfaces for which you have not explicitly configured unicast RPF even though unicast RPF is implicitly enabled on all interfaces on EX3200 and EX4200 switches.

Copyright © 2015, Juniper Networks, Inc.

Related Documentation

- *show interfaces xe-*
- *Example: Configuring Unicast RPF on an EX Series Switch*
- Configuring Unicast RPF (CLI Procedure) on page 79
- Disabling Unicast RPF (CLI Procedure) on page 81
- *Troubleshooting Unicast RPF*

Copyright © 2015, Juniper Networks, Inc.

PART 5

Configuration Statements and Operational Commands

Copyright © 2015, Juniper Networks, Inc.

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 5

Configuration Statements for Firewall Filters

Copyright © 2015, Juniper Networks, Inc.

family

Syntax

```
family family-name {
  filter filter-name {
    interface-specific;
    term term-name {
      from {
        match-conditions;
      }
      then {
        action;
        action-modifiers;
      }
    }
  }
}
```

Hierarchy Level [edit firewall]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure the fields a firewall filter can match on.

Options *family-name*—Type of addressing protocol:

- **ethernet-switching**—Filter Layer 2 Ethernet packets and Layer 3 (IP) packets (allows some Layer 3 filtering). Not supported on OCX series switches.
- **inet**—Filter Layer 3 IPv4 packets (provides additional Layer 3 filter options).
- **inet6**—Filter Layer 3 IPv6 packets (provides additional Layer 3 filter options).
- **mpls**—Filter multiprotocol label switched packets. Not supported on OCX series switches.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Firewall Filter Match Conditions and Actions on page 11
- *Configuring Firewall Filters*
- *Overview of Firewall Filters*

Copyright © 2015, Juniper Networks, Inc.

filter

Syntax

```
filter filter-name {
  interface-specific;
  term term-name {
    from {
      match-conditions;
    }
    then {
      action;
      action-modifiers;
    }
  }
}
```

Hierarchy Level [edit firewall family *family-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure firewall filters.

Options ***filter-name***—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.

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

- Firewall Filter Match Conditions and Actions on page 11
- *Configuring Firewall Filters*
- *Overview of Firewall Filters*

Copyright © 2015, Juniper Networks, Inc.

filter (Layer 3 Interfaces)

Syntax filter (input | output) *filter-name*;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family-name*]

Release Information Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Apply a firewall filter to traffic transiting a Layer 3 interface.

Default All incoming traffic is accepted unmodified on the Layer 3 interface, and all outgoing traffic is sent unmodified from the Layer 3 interface.

Options ***filter-name***—Name of a firewall filter defined at the **[edit firewall family *family-name* filter]** hierarchy level.

input—Apply a firewall filter to traffic entering the Layer 3 interface.

output—Apply a firewall filter to traffic exiting the Layer 3 interface.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Firewall Filters on page 30
- Overview of Firewall Filters on page 3

Copyright © 2015, Juniper Networks, Inc.

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 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure firewall filters and policers.

Copyright © 2015, Juniper Networks, Inc.

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
- Firewall Filter Match Conditions and Actions on page 11
- *Configuring Firewall Filters*
- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59
- *Overview of Firewall Filters*

from

Syntax
```
from {
  match-conditions;
}
```

Hierarchy Level
[edit **firewall family** *family-name* **filter** *filter-name* **term** *term-name*]

Release Information
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Match packet fields to values specified in a match condition. If the **from** statement is not included in a firewall filter configuration, all packets are considered to match and the actions and action modifiers in the **then** statement are implemented.

Options
match-conditions—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 **then** statement to be implemented.

Required Privilege Level
firewall—To view this statement in the configuration.
firewall-control—To add this statement to the configuration.

Related Documentation
- Firewall Filter Match Conditions and Actions on page 11
- *Configuring Firewall Filters*
- *Understanding Firewall Filter Match Conditions*

Copyright © 2015, Juniper Networks, Inc.

interface-specific

Syntax interface-specific;

Hierarchy Level [edit firewall family *family-name* filter *filter-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure separate counters for each interface to which a filter is applied.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Firewall Filter Match Conditions and Actions on page 11
- *Configuring Firewall Filters*
- *Overview of Firewall Filters*

Copyright © 2015, Juniper Networks, Inc.

term

Syntax

```
term term-name {
  from {
    match-conditions;
  }
  then {
    action;
    action-modifiers;
  }
}
```

Hierarchy Level [edit firewall family *family-name* filter *filter-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Define a firewall filter term.

Options *term-name*—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.

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

- Firewall Filter Match Conditions and Actions on page 11
- *Configuring Firewall Filters*
- *Overview of Firewall Filters*

Copyright © 2015, Juniper Networks, Inc.

then (Filters)

Syntax

```
then {
  action;
  action-modifiers;
}
```

Hierarchy Level [edit firewall family *family-name* filter *filter-name* term *term-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure a firewall filter action.

Options

action—Actions to accept, discard, or forward packets that match all conditions specified in a filter term.

action-modifiers—Additional actions to analyze, classify, count, or police packets that match all conditions specified in a filter term.

Required Privilege Level firewall—To view this statement in the configuration.
firewall-control—To add this statement to the configuration.

Related Documentation

- Firewall Filter Match Conditions and Actions on page 11
- *Configuring Firewall Filters*
- *Understanding Firewall Filter Match Conditions*

Copyright © 2015, Juniper Networks, Inc.

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 6

Configuration Statements for Policers

Copyright © 2015, Juniper Networks, Inc.

action

Syntax

```
action {
  loss-priority high then discard;
}
```

Hierarchy Level [edit firewall three-color-policer *name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Discard traffic on a logical interface using tricolor marking policing.

Options The statements are explained separately.

Required Privilege Level firewall—To view this statement in the configuration.
firewall-control—To add this statement to the configuration.

bandwidth-limit

Syntax bandwidth-limit *bps*;

Hierarchy Level [edit firewall policer *policer-name* if-exceeding]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify the traffic rate in bits per second.

Options *bps*—Traffic rate in bits per second. Specify *bps* as a decimal value or as a decimal number followed by one of the abbreviation **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

Range: 32000 bps (32 Kbps) through 10,000,000,000 bps (10 Gbps)

Required Privilege Level firewall—To view this statement in the configuration.
firewall-control—To add this statement to the configuration.

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59
- Overview of Policers on page 41

Copyright © 2015, Juniper Networks, Inc.

burst-size-limit

Syntax burst-size-limit *bytes*;

Hierarchy Level [edit firewall policer *policer-name* if-exceeding]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify the maximum allowed burst size to control the amount of traffic bursting.

Options ***bytes***—Decimal value or a decimal number followed by k (thousand), m (million), or g (giga).
Range: 1 through 2,147,450,880 bytes (2147 MB)

Required Privilege Level firewall—To view this statement in the configuration.
firewall-control—To add this statement to the configuration.

Related Documentation
- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59
- Overview of Policers on page 41

Copyright © 2015, Juniper Networks, Inc.

color-aware

Syntax color-aware;

Hierarchy Level [edit firewall three-color-policer *policer-name* single-rate],
[edit firewall three-color-policer *policer-name* two-rate]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure the way preclassified packets are metered. In color-aware mode, the switch can assign a higher packet-loss priority, but cannot assign a lower packet loss priority (PLP). For example, suppose an upstream device assigns medium-high PLP to a packet because the packet exceeded its committed information rate (CIR). The switch cannot change the PLP to low even if the packet conforms to the configured CIR of the appropriate interface. On the other hand, if an upstream device assigns low PLP to a packet but the packet exceeds the CIR and committed burst size (CBS) of the switch interface, the switch can increase the PLP to medium-high.

Default If you omit the **color-aware** statement, the default behavior is color-aware mode.

Required Privilege Level firewall—To view this statement in the configuration.
firewall-control—To add this statement to the configuration.

Related Documentation

- Overview of Policers on page 41
- Understanding Color-Aware Mode for Single-Rate Tricolor Marking on page 48
- Understanding Color-Aware Mode for Two-Rate Tricolor Marking on page 50
- color-blind on page 101

Copyright © 2015, Juniper Networks, Inc.

color-blind

Syntax color-blind;

Hierarchy Level [edit firewall three-color-policer *policer-name* single-rate],
[edit firewall three-color-policer *policer-name* two-rate]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure the way preclassified packets are metered. In color-blind mode, the switch ignores any preclassification of packets and can assign a higher or lower packet loss priority (PLP). For example, suppose an upstream device assigns medium-high PLP to a packet because the packet exceeded the CIR on the upstream device. The switch can change the PLP to low if the packet conforms to the CIR of the appropriate interface.

Default If you omit the **color-blind** statement, the default behavior is color-aware mode.

Required Privilege Level firewall—To view this statement in the configuration.
firewall-control—To add this statement to the configuration.

Related Documentation

- Overview of Policers on page 41
- Understanding Color-Blind Mode for Single-Rate Tricolor Marking on page 47
- Understanding Color-Blind Mode for Two-Rate Tricolor Marking on page 49
- Configuring Color-Blind Egress Policers for Medium-Low PLP on page 58
- color-aware on page 100

Copyright © 2015, Juniper Networks, Inc.

committed-burst-size

Syntax committed-burst-size *bytes*;

Hierarchy Level [edit firewall three-color-policer *policer-name* single-rate],
[edit firewall three-color-policer *policer-name* two-rate]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure the maximum number of bytes allowed for incoming traffic to burst above the committed information rate and still be marked with low packet loss priority (green).

NOTE: When you include the committed-burst-size statement in the configuration, you must also include the committed-information-rate statement at the same hierarchy level.

Options *bytes*—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 **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

Range: 512 bytes through 268435456 bytes (268 MB)

Required Privilege Level firewall—To view this statement in the configuration.
firewall-control—To add this statement to the configuration.

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59
- Overview of Policers on page 41

Copyright © 2015, Juniper Networks, Inc.

committed-information-rate

Syntax committed-information-rate *bits-per-second*;

Hierarchy Level [edit firewall three-color-policer *policer-name* single-rate],
[edit firewall three-color-policer *policer-name* two-rate]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure the guaranteed bandwidth under normal line conditions and the average rate up to which packets are marked with low packet loss priority (green).

NOTE: When you include the **committed-information-rate** statement in the configuration, you must also include the **committed-burst-size** statement at the same hierarchy level.

Options ***bits-per-second***—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 **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

Range: 32,000 bps through 10,000,000,000 bps (10 gbps)

Required Privilege Level firewall—To view this statement in the configuration.
firewall-control—To add this statement to the configuration.

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59
- Overview of Policers on page 41

Copyright © 2015, Juniper Networks, Inc.

excess-burst-size

Syntax excess-burst-size *bytes*;

Hierarchy Level [edit firewall three-color-policer *policer-name* single-rate]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure the maximum number of bytes allowed for incoming traffic 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).

NOTE: When you include the **excess-burst-size** statement in the configuration, you must also include the **committed-burst-size** and **committed-information-rate** statements at the same hierarchy level.

Options ***bytes***—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 **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

Range: 512 bytes through 268435456 bytes (268 MB)

Required Privilege Level firewall—To view this statement in the configuration.
firewall-control—To add this statement to the configuration.

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59
- Overview of Policers on page 41

Copyright © 2015, Juniper Networks, Inc.

filter-specific

Syntax filter-specific;

Hierarchy Level [edit firewall policer *policer-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description 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. If you use a filter-specific policer in multiple terms, both of the following are true:

- Traffic is policed at the aggregate rate. For example, if you create a policer that has a bandwidth limit of 100 Mbps and use the policer in two terms, the total allowed bandwidth for both terms is 100 Mbps—not 100 Mbps for each term.
- The implicit counter counts all the packets are that matched by any of the terms. For example, if you reference the same filter-specific policer in term1 and term2, and term1 matches 1000 packets and term2 matches 500 packets, the implicit counter shows 1500 matches for the policer.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration

Related Documentation
- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59
- Overview of Policers on page 41

Copyright © 2015, Juniper Networks, Inc.

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 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure firewall filters and policers.

Copyright © 2015, Juniper Networks, Inc.

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
- Firewall Filter Match Conditions and Actions on page 11
- *Configuring Firewall Filters*
- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59
- *Overview of Firewall Filters*

if-exceeding

Syntax
```
if-exceeding {
  bandwidth-limit bps;
  burst-size-limit bytes;
}
```

Hierarchy Level
[edit firewall policer *policer-name*]

Release Information
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
Configure policer rate limits.

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 Two-Color and Three-Color Policers to Control Traffic Rates on page 59
- Overview of Policers on page 41

Copyright © 2015, Juniper Networks, Inc.

loss-priority high then discard (Three-Color Policer)

Syntax loss-priority high then discard;

Hierarchy Level [edit firewall three-color-policer *policer-name* action]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description For packets with high loss priority, discard the packets. The loss priority setting is not configurable. Include this statement if you do not want the switch to forward packets that have high packet-loss priority.

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.

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.

Required Privilege Level firewall—To view this statement in the configuration.
firewall-control—To add this statement to the configuration.

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59
- Overview of Policers on page 41

Copyright © 2015, Juniper Networks, Inc.

peak-burst-size

Syntax peak-burst-size *bytes*;

Hierarchy Level [edit firewall three-color-policer *policer-name* two-rate]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description 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).

NOTE: When you include the **peak-burst-size** statement in the configuration, you must also include the **committed-burst-size** and **peak-information-rate** statements at the same hierarchy level.

Options *bytes*—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 **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

Range: 1500 bytes through 100,000,000,000 bytes (100 GB)

Required Privilege Level firewall—To view this statement in the configuration.
firewall-control—To add this statement to the configuration.

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59
- Overview of Policers on page 41

Copyright © 2015, Juniper Networks, Inc.

peak-information-rate

Syntax peak-information-rate *bits-per-second*;

Hierarchy Level [edit firewall three-color-policer *policer-name* two-rate]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure the maximum achievable rate. Packets that exceed the committed information rate (CIR) but are below the peak information rate (PIR) are marked with medium-high packet loss priority (yellow). Packets that exceed the PIR are marked with high packet loss priority (red). You can configure a discard action for packets that exceed the PIR.

NOTE: When you include the **peak-information-rate** statement in the configuration, you must also include the **committed-information-rate** and **peak-burst-size** statements at the same hierarchy level.

Options *bits-per-second*—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 **k** (1000), **m** (1,000,000), or **g** (1,000,000,000).

Range: 32,000 bps through 10,000,000,000 bps (10 gbps)

Required Privilege Level firewall—To view this statement in the configuration.
firewall-control—To add this statement to the configuration.

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59
- Overview of Policers on page 41

Copyright © 2015, Juniper Networks, Inc.

policer

Syntax

```
policer policer-name {
  filter-specific;
  if-exceeding {
    bandwidth-limit bps;
    burst-size-limit bytes;
  }
  then {
    policer-action;
  }
}
```

Hierarchy Level [edit firewall]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure policer rate limits and actions. To activate a policer, you must include the **policer** action modifier in the **then** statement in a firewall filter term.

Each policer that you configure includes an implicit counter that counts the number of packets that exceed the rate limits that are specified for the policer. If you use the same policer in multiple terms—either within the same filter or across filters—the policer's implicit counter is used to count packets that are policed in all of these terms. If you want to obtain separate packet counts for each term, use these approaches:

- Configure a unique policer for each term.
- Configure only one policer, but use a unique, explicit counter in each term.

Options *policer-name*—Name that identifies the policer. The name can contain letters, numbers, hyphens (-), and can be up to 64 characters long.

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 Two-Color and Three-Color Policers to Control Traffic Rates on page 59
- *Configuring Firewall Filters*
- Overview of Policers on page 41

Copyright © 2015, Juniper Networks, Inc.

single-rate

Syntax

```
single-rate {
  (color-aware | color-blind);
  committed-information-rate bps;
  committed-burst-size bytes;
  excess-burst-size bytes;
}
```

Hierarchy Level [edit firewall three-color-policer *policer-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description 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).

Packets that conform to the CIR or the CBS are assigned low loss priority (green). Packets that exceed the CIR and the CBS but are within the EBS are assigned medium-high loss priority (yellow). Packets that exceed the EBS are assigned high loss priority (red).

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.

The remaining statements are explained separately.

Options ***policer-name***—Name of the three-color policer. Use this name when you apply the policer to an interface.

Required Privilege Level firewall—To view this statement in the configuration.
firewall-control—To add this statement to the configuration.

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59
- Overview of Policers on page 41

Copyright © 2015, Juniper Networks, Inc.

then (Policers)

Syntax

```
then {
  policer-action;
}
```

Hierarchy Level [edit firewall policer *policer-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure a policer action.

Options ***policer-action***—Allowed policer actions are **discard**, **loss-priority high**, and **loss-priority low**. **discard** causes the system to drop traffic that exceeds the rate limits defined by the policer. Use **loss-priority high** to allow the system to forward matching traffic in some cases.

NOTE: If you specify a policer in an egress firewall filter, the only supported action is **discard**.

Required Privilege Level firewall—To view this statement in the configuration.
firewall-control—To add this statement to the configuration.

Related Documentation

- Configuring Two-Color and Three-Color Policers to Control Traffic Rates on page 59
- *Configuring Firewall Filters*
- Overview of Policers on page 41

Copyright © 2015, Juniper Networks, Inc.

three-color-policer

Syntax

```
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 firewall],
[edit logical-systems *logical-system-name* firewall]

Release Information

Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure a three-color policer.

Options

policer-name—Name of the three-color policer. Use 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 Two-Color and Three-Color Policers to Control Traffic Rates on page 59
- Overview of Policers on page 41

Copyright © 2015, Juniper Networks, Inc.

two-rate

Syntax

```
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 firewall three-color-policer *policer-name*]

Release Information Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description 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).

Packets that conform to the CIR or the CBS are assigned low loss priority (green). Packets that exceed the CIR and the CBS but are within the PIR or the PBS are assigned medium-high loss priority (yellow). Packets that exceed the PIR and the PBS are assigned high loss priority (red).

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.

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.

Copyright © 2015, Juniper Networks, Inc.

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 7

Configuration Statements for Port Security

Copyright © 2015, Juniper Networks, Inc.

circuit-id

Syntax

```
circuit-id {
  prefix {
    host-name;
    logical-system-name;
    routing-instance-name;
  }
  use-interface-description (device | logical);
  use-vlan-id;
}
```

Hierarchy Level

- For platforms with Enhanced Layer 2 Software (ELS):

  [edit vlans *vlan-name* forwarding-options dhcp-security option-82]

- For platforms without ELS:

  [edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*) dhcp-option82],
  [edit forwarding-options helpers bootp dhcp-option82] ,
  [edit forwarding-options helpers bootp interface *interface-name* dhcp-option82]

- For MX Series platforms:

  [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security option-82]

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Hierarchy level **[edit vlans *vlan-name* forwarding-options dhcp-security]** introduced in Junos OS Release 13.2X50-D10. (See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)
Statement introduced in Junos OS Release 14.1 for the MX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure the **circuit-id** suboption (suboption 1) of DHCP option 82 (the DHCP relay agent information option) in DHCP packets destined for a DHCP server. This suboption identifies the circuit (the interface, the VLAN, or both) on which the DHCP request arrived.

The remaining statements are explained separately.

Default

If DCHP option 82 is enabled on the switch, the circuit ID is supplied by default in the format ***interface-name*:*vlan-name*** or, on a Layer 3 interface, just ***interface-name***.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Setting Up DHCP Option 82 on an MX Series Router (CLI Procedure)*
- *Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server*
- *Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server*

Copyright © 2015, Juniper Networks, Inc.

- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- *Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*
- RFC 3046, *DHCP Relay Agent Information Option*, at http://tools.ietf.org/html/rfc3046

Copyright © 2015, Juniper Networks, Inc.

vendor-id

Syntax vendor-id <*string*>;

For Platforms with Enhanced Layer 2 Software (ELS) [edit vlans *vlan-name* forwarding-options dhcp-security option-82]

For Platforms Without ELS [edit ethernet-switching-options secure-access-port vlan (all | *vlan-name*) dhcp-option82],
[edit forwarding-options helpers bootp dhcp-option82],
[edit forwarding-options helpers bootp interface *interface-name* dhcp-option82]

For MX Series Platforms [edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security option-82]

Release Information Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Hierarchy level **[edit vlans *vlan-name* forwarding-options dhcp-security]** introduced in Junos OS Release 13.2X50-D10. (See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)
Hierarchy level **[edit bridge-domains *bridge-domain-name* forwarding-options dhcp-security]** introduced in Junos OS Release 14.1 for the MX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Insert a vendor ID in the DHCP option 82 information in a DHCP request packet header before forwarding or relaying the request to a DHCP server.

Default If **vendor-id** is not explicitly configured for DHCP option 82, then no vendor ID is set.

Options ***string***—(Optional) A single string that designates the vendor ID.

Range: 1–255 characters

Default: If you specify **vendor-id** with no ***string*** value, then the default vendor ID **Juniper Networks** is configured.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Setting Up DHCP Option 82 on an MX Series Router (CLI Procedure)*
- *Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server*
- *Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server*
- *Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)*

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 8

Configuration Statement for Device Security

rpf-check

Syntax rpf-check;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family inet],
[edit interfaces *interface-name* unit *logical-unit-number* family inet6]

Release Information Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description On EX3200 and EX4200 switches, enable a reverse-path forwarding (RPF) check on unicast traffic (except ECMP packets) on all ingress interfaces.

On EX4300 switches, enable a reverse-path forwarding (RPF) check on unicast traffic, including ECMP packets, on all ingress interfaces.

On EX8200 and EX6200 switches, enable an RPF check on unicast traffic, including ECMP packets, on the selected ingress interfaces.

On QFX Series switches, enable an RPF check on unicast traffic (except ECMP packets) on the selected ingress interfaces.

Default Unicast RPF is disabled on all interfaces.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring Unicast RPF on an EX Series Switch*
- Configuring Unicast RPF (CLI Procedure) on page 79
- Disabling Unicast RPF (CLI Procedure) on page 81
- Understanding Unicast RPF on page 75

Copyright © 2015, Juniper Networks, Inc.

Copyright © 2015, Juniper Networks, Inc.

CHAPTER 9

Firewall Filters Monitoring Commands

- clear firewall
- show firewall
- show firewall policer
- show interfaces filters

Copyright © 2015, Juniper Networks, Inc.

clear firewall

Syntax clear firewall (all | counter *counter-name* | filter *filter-name*)

Release Information Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Clear statistics provided by firewall filters.

When you clear the counters of a filter, this not only impacts the counters shown by the CLI, but also the ones tracked by SNMP 2.

Options **all**—Clear the packet and byte counts for all firewall filter counters and clear the packet counts for all policer counters.

counter *counter-name*—Clear the packet and byte counts for the specified firewall filter counter.

filter *filter-name*—Clear the packet and byte counts for the specified firewall filter.

Required Privilege Level clear

Related Documentation

- Verifying That Firewall Filters Are Operational on page 36
- Verifying That Two-Color Policers Are Operational on page 61
- *Overview of Firewall Filters*
- Overview of Policers on page 41

Sample Output

clear firewall all

```
user@switch> clear firewall all
```

clear firewall counter

```
user@switch> clear firewall counter port-filter-counter
```

clear firewall filter

```
user@switch> clear firewall filter ingress-port-filter
```


Copyright © 2015, Juniper Networks, Inc.

show firewall

Syntax

show firewall
<counter *counter-name*>
<filter *filter-name*>
<log <detail | interface *interface-name*>>
<terse>

Release Information

Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Display statistics about configured firewall filters.

Options

counter *counter-name*—(Optional) Display statistics about a particular firewall filter counter.

filter *filter-name*—(Optional) Display statistics about a particular firewall filter.

log—(Optional) Display log entries for all firewall filter activity.

terse—(Optional) Display firewall filter names only.

Required Privilege Level

view

Related Documentation

- Verifying That Firewall Filters Are Operational on page 36
- Verifying That Two-Color Policers Are Operational on page 61
- *Overview of Firewall Filters*
- Overview of Policers on page 41

List of Sample Output

show firewall on page 126
show firewall filter filter-name on page 127
show firewall counter counter-name on page 127
show firewall log on page 127
show firewall log detail on page 127

Output Fields

Table 15 on page 125 lists the output fields for the **show firewall** command. Output fields are listed in the approximate order in which they appear.

Table 15: show firewall Output Fields

Field Name	Field Description	Level of Output
Filter	Name of the filter that is configured at the **[edit firewall family *family-name* filter]** hierarchy level.	All levels

Copyright © 2015, Juniper Networks, Inc.

Table 15: show firewall Output Fields *(continued)*

Field Name	Field Description	Level of Output
Counters	Display filter counter information: • Name—Name of a filter counter that has been configured with the **count** firewall filter action modifier. • Bytes—Number of bytes that match the filter term where the **count** action modifier was specified. • Packets—Number of packets that matched the filter term where the **count** action modifier was specified.	All levels
Policers	Display policer information: • Name—Name of the policer that is configured at the **[edit firewall policer]** hierarchy level. • Packets—Number of packets that matched the filter term where the **policer** action modifier was specified. This is the number of packets that exceeded the rate limits that the policer specifies.	All levels
Action	Filter action: • **A**—Accept • **D**—Discard	All levels
Interface	Interface on which the firewall filter is applied.	All levels
Protocol	Name of the packet protocol.	All levels
Packet Length	Length of the packet.	All levels
Src Addr	Source address of the packet.	All levels
Dest Addr	Destination address of the packet.	All levels

Sample Output

show firewall

```
user@switch> show firewall
Filter: egress-vlan-watch-employee
Counters:
Name                                                Bytes              Packets
counter-employee-web                                    0                    0
Filter: ingress-port-limit-tcp-icmp
Counters:
Name                                                Bytes              Packets
icmp-counter                                          560                   10
Policers:
Name                                               Packets
icmp-connection-policer                                10
tcp-connection-policer                                  0
Filter: ingress-vlan-rogue-block
Filter: ingress-vlan-limit-guest
```


Copyright © 2015, Juniper Networks, Inc.

show firewall filter filter-name

```
user@switch> show firewall filter ingress-port-limit-tcp-icmp
Filter: ingress-port-limit-tcp-icmp
Counters:
Name                                                Bytes              Packets
icmp-counter                                          560                   10
Policers:
Name                                               Packets
icmp-connection-policer                                 10
tcp-connection-policer                                   0
```

show firewall counter counter-name

```
user@switch> show firewall counter icmp-counter
Filter: ingress-port-voip-class-filter
Counters:
Name                                                Bytes              Packets
icmp-counter                                          560                   10
```

show firewall log

```
user@switch> show firewall log
Log :

Time      Filter    Action Interface     Protocol        Src Addr
          Dest Addr
08:00:53  pfe       R      ge-1/0/6.0    ICMP            192.168.3.5
         192.168.3.4
08:00:52  pfe       R      ge-1/0/6.0    ICMP            192.168.3.5
         192.168.3.4
08:00:51  pfe       R      ge-1/0/6.0    ICMP            192.168.3.5
         192.168.3.4
08:00:50  pfe       R      ge-1/0/6.0    ICMP            192.168.3.5
         192.168.3.4
08:00:49  pfe       R      ge-1/0/6.0    ICMP            192.168.3.5
         192.168.3.4
08:00:48  pfe       R      ge-1/0/6.0    ICMP            192.168.3.5
         192.168.3.4
08:00:47  pfe       R      ge-1/0/6.0    ICMP            192.168.3.5
         192.168.3.4
```

show firewall log detail

```
user@switch> show firewall log detail
Log :

Time of Log: 2010-10-13 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: 2010-10-13 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: 2010-10-13 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: 2010-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of
```

Copyright © 2015, Juniper Networks, Inc.

```
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: 2010-10-13 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: 2010-10-13 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
```


Copyright © 2015, Juniper Networks, Inc.

show firewall policer

Syntax show firewall policer
<*policer-name*>

Release Information Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Display statistics about configured policers.

Options **none**—Display the count of policed packets for all configured policers.

policer-name—(Optional) Display the count of policed packets for the specified policer.

Required Privilege Level view

Related Documentation
- Verifying That Firewall Filters Are Operational on page 36
- Verifying That Two-Color Policers Are Operational on page 61
- *Overview of Firewall Filters*
- Overview of Policers on page 41

List of Sample Output
show firewall policer on page 129
show firewall policer policer-name on page 130

Output Fields Table 16 on page 129 lists the output fields for the **show firewall policer** command. Output fields are listed in the approximate order in which they appear.

Table 16: show firewall policer Output Fields

Field Name	Field Description	Level of Output
Filter	Name of the filter that is configured at the **[edit firewall family *family-name* filter]** hierarchy level.	All levels
Policers	Display policer information: • Filter—Name of filter that specifies the **policer** action modifier. • Name—Name of policer. • Packets—Number of packets that matched the filter term in which the **policer** action modifier is specified. This is the number of packets that exceed the rate limits that the policer specifies.	All levels

Sample Output

show firewall policer

```
user@switch> show firewall policer
Filter: egress-vlan-filter
Filter: ingress-port-filter
```

Copyright © 2015, Juniper Networks, Inc.

```
Policers:
Name                                                Packets
icmp-connection-policer                                   0
tcp-connection-policer                                    0
Filter: ingress-vlan-rogue-block
```

show firewall policer policer-name

```
user@switch> show firewall policer tcp-connection-policer
Filter: ingress-port-filter
Policers:
Name                                                Packets
tcp-connection-policer                                    0
```


Copyright © 2015, Juniper Networks, Inc.

show interfaces filters

Syntax show interfaces filters
<interface-name>

Release Information Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Display firewall filters that are configured on each interface in a switch.

Options **none**—Display firewall filter information about all interfaces.

interface-name—(Optional) Display firewall filter information about a particular interface.

Required Privilege Level view

Related Documentation
- show firewall on page 125

List of Sample Output show interfaces filters on page 131
show interfaces filters interface-name on page 132

Output Fields Table 17 on page 131 lists the output fields for the **show interfaces filters** command. Output fields are listed in the approximate order in which they appear.

Table 17: show interfaces filters Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the physical interface.	All levels
Admin	Interface state: **up** or **down**.	All levels
Link	Link state: **up** or **down**.	All levels
Proto	Protocol that is configured on the interface.	All levels
Input Filter	Name of the firewall filter to be evaluated when packets are received on the interface.	All levels
Output Filter	Name of the firewall filter to be evaluated when packets are transmitted on the interface.	All levels

Sample Output

show interfaces filters

```
user@switch> show interfaces filters
Interface       Admin Link Proto Input Filter        Output Filter
ge-0/0/6        up    up
ge-0/0/6.0      up    up   inet
```

Copyright © 2015, Juniper Networks, Inc.

```
ge-0/0/7        up    down
ge-0/0/8        up    down
ge-0/0/9        up    down
ge-0/0/10       up    down
ge-0/0/10.0     up    down
```

show interfaces filters interface-name

```
user@switch> show interfaces filters ge-0/0/6
Interface       Admin Link Proto Input Filter         Output Filter
ge-0/0/6        up    up
ge-0/0/6.0      up    up inet
```


Copyright © 2015, Juniper Networks, Inc.