



JunosE™ Software for E Series™ Broadband Services Routers

Policy Management

Release

13.2.x



Published: 2012-07-02

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Copyright © 2012, Juniper Networks, Inc. All rights reserved.

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

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

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

JunosE™ Software for E Series™ Broadband Services Routers Policy Management
Release 13.2.x
Copyright © 2012, Juniper Networks, Inc.
All rights reserved.

Revision History
July 2012—FRS JunosE 13.2.x

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.

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

END USER LICENSE AGREEMENT

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

Table of Contents

	About the Documentation	vii
	E Series and JunosE Documentation and Release Notes	vii
	Audience	vii
	E Series and JunosE Text and Syntax Conventions	vii
	Obtaining Documentation	ix
	Documentation Feedback	ix
	Requesting Technical Support	ix
	Self-Help Online Tools and Resources	x
	Opening a Case with JTAC	x
Part 1	Overview	
Chapter 1	How Policy Management Works	3
	Policy Management Overview	3
	Description of a Policy	5
	Policy References	5
Chapter 2	Hardware Requirements	7
	Policy Platform Considerations	7
Part 2	Configuration	
Chapter 3	Configuration Overview	11
	Policy Management Configuration Tasks	11
Part 3	Administration	
Chapter 4	Monitoring Overview	15
	Monitoring Policy Management Overview	15
	Setting a Statistics Baseline for Policies	15
Part 4	Index	
	Index	19

List of Tables

About the Documentation	vii
Table 1: Notice Icons	viii
Table 2: Text and Syntax Conventions	viii

About the Documentation

- E Series and JunosE Documentation and Release Notes on page vii
- Audience on page vii
- E Series and JunosE Text and Syntax Conventions on page vii
- Obtaining Documentation on page ix
- Documentation Feedback on page ix
- Requesting Technical Support on page ix

E Series and JunosE Documentation and Release Notes

For a list of related JunosE documentation, see
<http://www.juniper.net/techpubs/software/index.html>.

If the information in the latest release notes differs from the information in the documentation, follow the *JunosE 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/>.

Audience

This guide is intended for experienced system and network specialists working with Juniper Networks E Series Broadband Services Routers in an Internet access environment.

E Series and JunosE Text and Syntax Conventions

Table 1 on page viii defines notice icons used in this documentation.

Table 1: Notice Icons

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

[Table 2 on page viii](#) defines text and syntax conventions that we use throughout the E Series and JunosE documentation.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents commands and keywords in text.	<ul style="list-style-type: none"> Issue the clock source command. Specify the keyword exp-msg.
Bold text like this	Represents text that the user must type.	host1(config)#traffic class low-loss1
Fixed-width text like this	Represents information as displayed on your terminal's screen.	host1#show ip ospf 2 Routing Process OSPF 2 with Router ID 5.5.0.250 Router is an Area Border Router (ABR)
<i>Italic text like this</i>	<ul style="list-style-type: none"> Emphasizes words. Identifies variables. Identifies chapter, appendix, and book names. 	<ul style="list-style-type: none"> There are two levels of access: <i>user</i> and <i>privileged</i>. <i>clusterId</i>, <i>ipAddress</i>. <i>Appendix A, System Specifications</i>
Plus sign (+) linking key names	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
Syntax Conventions in the Command Reference Guide		
Plain text like this	Represents keywords.	terminal length
<i>Italic text like this</i>	Represents variables.	<i>mask</i> , <i>accessListName</i>

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

Convention	Description	Examples
(pipe symbol)	Represents a choice to select one keyword or variable to the left or to the right of this symbol. (The keyword or variable can be either optional or required.)	diagnostic line
[] (brackets)	Represent optional keywords or variables.	[internal external]
[]* (brackets and asterisk)	Represent optional keywords or variables that can be entered more than once.	[level1 level2 l1]*
{ } (braces)	Represent required keywords or variables.	{ permit deny } { in out } { clusterId ipAddress }

Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documentation, see the Technical Documentation page on the Juniper Networks Web site at <http://www.juniper.net/>.

To download complete sets of technical documentation to create your own documentation CD-ROMs or DVD-ROMs, see the Portable Libraries page at

<http://www.juniper.net/techpubs/resources/index.html>

Copies of the Management Information Bases (MIBs) for a particular software release are available for download in the software image bundle from the Juniper Networks Web site at <http://www.juniper.net/>.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation to better meet your needs. Send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

- [How Policy Management Works on page 3](#)
- [Hardware Requirements on page 7](#)

CHAPTER 1

How Policy Management Works

- [Policy Management Overview on page 3](#)
- [Description of a Policy on page 5](#)
- [Policy References on page 5](#)

Policy Management Overview

This chapter introduces policy-based routing management on E Series routers. Policy management enables you to configure, manage, and monitor policies that selectively cause packets to take different paths without requiring a routing table lookup. The JunosE Software's packet-mirroring feature uses secure policies.

Policy management enables network service providers to configure services that customize the treatment of individual packet flows received on a subscriber's interface. The main tool for implementing policy management is a policy list. A policy list is a set of rules, each of which specifies a policy action. A rule is a policy action optionally combined with a classification.

Packets are sorted at ingress or egress into packet flows based on attributes defined in classifier control lists (CLACLs). You can apply policy lists to packets arriving and leaving an interface. You can use policy management on ATM, Frame Relay, generic routing encapsulation (GRE), IP, IPv6, Layer 2 Tunneling Protocol (L2TP), Multiprotocol Label Switching (MPLS), and virtual local area network (VLAN) traffic.

Policy management provides:

- **Policy routing**—Predefines a classified packet flow to a destination port or IP address. The router does not perform a routing table lookup on the packet. This provides superior performance for real-time applications.
- **Bandwidth management**—Rate-limits a classified packet flow at ingress to enforce ingress data rates below the physical line rate of a port. A rate-limit profile with a policy rate-limit profile rule provides this capability. You can construct policies to provide rate limiting for individual packet flows or for the aggregate of multiple packet flows. Juniper Networks E Series Broadband Services Router rate limits are calculated based on the layer 2 packet size. To configure rate limiting, you first create a rate-limit profile, which is a set of bandwidth attributes and associated actions. You next create a policy list with a rule that has rate limit as the action and associate a rate-limit profile with this rule. You can configure rate-limit profiles to provide a variety of services, including

tiered bandwidth service where traffic conforming to configured bandwidth levels is treated differently than traffic that exceeds the configured values, and a hard-limit service where a fixed bandwidth limit is applied to a traffic flow. Finally, you can configure rate-limit profiles to provide a TCP-friendly rate-limiting service that works in conjunction with TCP's native flow-control functionality.

- **Security**—Provides a level of network security by using policy rules that selectively forward or filter packet flows. You can use a filter rule to stop a denial-of-service attack. You can use secure policies to mirror packets and send them to an analyzer.
- **RADIUS policy support**—Enables you to create and attach a policy to an interface through RADIUS.
- **Packet tagging**—Enables the traffic-class rule in policies to tag a packet flow so that the Quality of Service (QoS) application can provide traffic-class queuing. Policies can perform both in-band and out-of-band packet tagging.
- **Packet forwarding**—Allows forwarding of packets in a packet flow.
- **Packet filtering**—Drops packets in a packet flow.
- **Packet mirroring**—Uses secure policies to mirror packets and send them to an analyzer.
- **Packet logging**—Logs packets in a packet flow.

Policy management gives you the CLI tools to build databases, which can then be drawn from to implement a policy. Each database contains global traffic specifications. When building a policy, you specify input from one or more of these databases and then attach the policy to an interface. By combining the information from the various databases into policies, you can deploy a wide variety of services.



NOTE: When applying policies to interfaces that are managed by the SRC, avoid using any other policy management tools, such as CLI, RADIUS, CoA, or Service Manager. SRC is not compatible with other types of policy management tools. When policies are applied to the interface before SRC management begins, such as at access-accept time, these policies are properly replaced. However, if other policy managers change existing policies while SRC management is active, problems can occur. The precedence of each source when modifying configurations is:

- If you have a pre-configured policy through CLI as part of subscriber PVC/VLAN provisioning, SRC overwrites the policy when the SRC manages the interface
 - If you have a policy in the Access-Accept, SRC overwrites the policy when the SRC manages the interface
-

**Related
Documentation**

- [Description of a Policy on page 5](#)
- [Monitoring Policy Management Overview on page 15](#)
- [Policy Management Configuration Tasks on page 11](#)

Description of a Policy

A policy is a condition and an action that is attached to an interface. The condition and action cause the router to handle the packets passing through the interface in a certain way. A policy can be attached to IP interfaces and certain layer 2 interfaces such as Frame Relay, L2TP, MPLS, and VLAN interfaces. The policies do not need to be the same in both directions.

Packets are sorted at ingress or egress into packet flows based on attributes defined in classifier control lists. Policy lists contain rules that associate actions with these CLACLs. A rule is a policy action optionally combined with a classification.

When packets arrive on an interface, you can have a policy evaluate a condition before the normal route lookup; this kind of policy is known as an input policy. You can also have conditions evaluated after a route lookup; this kind of policy is known as a secondary input policy. You can use secondary input policies to defeat denial-of-service attacks directed at a router's local interface or to protect a router from being overwhelmed by legitimate local traffic. If you have a policy applied to packets before they leave an interface, this is known as an output policy.

Classification is the process of taking a single data stream in and sorting it into multiple output substreams. The classifier engine on an E Series router is a combination of PowerPC processors, working with a Field Programmable Gate Array (FPGA) for a hardware assist.

In the Differentiated Services (DiffServ) architecture, two basic types of classifiers exist. The first classifier type is a multifield (MF) classifier, which examines multiple fields in the IP datagram header to determine the service class to which a packet belongs. The second type of classifier is a behavior aggregate (BA) classifier, which examines a single field in an IP datagram header and assigns the packet to a service class based on what it finds.

There are two categories of hardware classifiers, depending on the type of line module being used. ES2 4G LM, ES2 10G Uplink LM, ES2 10G LM, OC48/STM16, GE-2, and GE-HDE line modules support content-addressable memory (CAM) hardware classifiers—all other line modules support FPGA hardware classifiers.

The maximum number of policies that you can attach to interfaces on an E Series router depends on the classifier entries that make up the policy and the number of attachment resources available on the interface. JunosE Software allocates interface attachment resources when you attach policies to interfaces. E Series routers support software and hardware classifiers. A policy can be made up of any combination of software and hardware classifiers.

Related Documentation

- [Policy Management Overview on page 3](#)

Policy References

For more information about policy management, see the following resources:

- RFC 2474—Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (December 1998)
- RFC 2475—An Architecture for Differentiated Services (December 1998)
- RFC 2697—A Single Rate Three Color Marker (September 1999)
- RFC 2698—A Two Rate Three Color Marker (September 1999)
- RFC 3198—Terminology for Policy-Based Management (November 2001)

CHAPTER 2

Hardware Requirements

- [Policy Platform Considerations on page 7](#)

Policy Platform Considerations

Policy services are supported on all E Series routers.

For information about the modules supported on E Series routers:

- See the *ERX Module Guide* for modules supported on ERX7xx models, ERX14xx models, and the Juniper Networks ERX310 Broadband Services Router.
- See the *E120 and E320 Module Guide* for modules supported on the Juniper Networks E120 and E320 Broadband Services Routers.

PART 2

Configuration

- [Configuration Overview on page 11](#)

CHAPTER 3

Configuration Overview

- [Policy Management Configuration Tasks on page 11](#)

Policy Management Configuration Tasks

Perform the required tasks and also any optional tasks that you need for your policy management configuration:

1. Create a CLACL (optional).
See [Classifier Control Lists Overview](#)
2. Create a rate-limit profile (optional).
See [Creating Rate-Limit Profiles](#)
3. Create a policy list.
See [Policy Lists Overview](#)
4. Create a classifier group.
See [Classifier Groups and Policy Rules Overview](#)
5. Create one or more policy rules within the classifier group.
See [Rate Limits for Interfaces Overview](#)
6. Apply a policy list to an interface or profile.
See [Classifier Groups and Policy Rules Overview](#)

Related Documentation

- [Policy Management Overview on page 3](#)
- [Description of a Policy on page 5](#)
- [Monitoring Policy Management Overview on page 15](#)

PART 3

Administration

- [Monitoring Overview on page 15](#)

CHAPTER 4

Monitoring Overview

- [Monitoring Policy Management Overview on page 15](#)
- [Setting a Statistics Baseline for Policies on page 15](#)

Monitoring Policy Management Overview

You can set a statistics baseline and use the **show** command to display your policy configuration and monitor policy statistics. When you set baseline statistics, you can retrieve statistics beginning at the time when the baselining is set. The policy log rule provides a way to monitor a packet flow by capturing a sample of the packets that satisfy the classification of the rule in the system log. See *JunosE System Event Logging Reference Guide* for information about logging.



NOTE: You can use the output filtering feature of the **show** command to include or exclude lines of output based on a text string you specify. See *Chapter 2, Command-Line Interface in JunosE System Basics Configuration Guide* for details.

Related Documentation

- [Policy Management Configuration Tasks on page 11](#)
- [Policy Management Overview on page 3](#)

Setting a Statistics Baseline for Policies

Purpose You can set a baseline for policy statistics by using the **baseline interface** command and the **atm policy**, **frame-relay policy**, **gre-tunnel policy**, **ip policy**, **ipv6 policy**, **l2tp policy**, **mpls policy**, and **vlan policy** commands. If you do not enable baselining, **show** command output fields for baseline counters display the contents of the regular statistics counters.

If you enable statistics, you can enable or disable baselining of the statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline when baseline-relative statistics are retrieved. Unlike other baseline statistics, policy baseline statistics are not stored in nonvolatile storage (NVS).

If you issue the **baseline interface** command for an interface without first enabling policy statistics baselining on that interface, a warning message indicates that policy baseline statistics are not enabled.

Enable a baseline for the statistics for the attachment of a policy list with statistics enabled to the ingress of an interface.

Action Enable baseline counters.

```
host1(config)#interface atm 12/0.1
host1(config-subif)#ip policy input routeForXYZCorp statistics enabled baseline enabled
```

Run the **show ip interface** command with the **delta** keyword to show baseline counters:

```
host1#show ip interface atm 12/0.1 delta
atm12/0.1 is up, line protocol is up
  Network Protocols: IP
    Internet address is 200.200.1.1/255.255.255.0
    Broadcast address is 255.255.255.255
    Operational MTU = 9180   Administrative MTU = 0
    Operational speed = 155520000   Administrative speed = 0
    Discontinuity Time = 1251181
    Router advertisement = disabled
    Administrative debounce-time = disabled
    Operational debounce-time = disabled
    Access routing = disabled
    Multipath mode = hashed

  In Received Packets 5, Bytes 540
  In Policed Packets 0, Bytes 0
  In Error Packets 0
  In Invalid Source Address Packets 0
  In Discarded Packets 0
  Out Forwarded Packets 5, Bytes 540
  Out Scheduler Drops Packets 0, Bytes 0
  Out Policed Packets 5, Bytes 540
  Out Discarded Packets 0

  IP Policy input routeForXYZCorp
    classifier-group *
      filter
        5 Packets  540 Bytes dropped
```

Related Documentation

- atm policy
- frame-relay policy
- gre-tunnel policy
- ip policy
- ipv6 policy
- l2tp policy
- mpls policy
- vlan policy

PART 4

Index

- [Index on page 19](#)

Index

C

classifier	
CAM hardware.....	5
FPGA hardware.....	5
conventions	
notice icons.....	vii
text and syntax.....	viii
customer support.....	ix
contacting JTAC.....	ix

D

documentation set	
comments on.....	ix

M

manuals	
comments on.....	ix

N

notice icons.....	vii
-------------------	-----

P

policy management	
bandwidth management.....	3
baselining statistics.....	15
overview.....	3
packet logging.....	4
packet mirroring.....	3
packet tagging.....	3
policy routing.....	3
QoS classification and marking.....	3
RADIUS support.....	3
resources.....	5
security.....	3
policy management configuration tasks.....	11

S

support, technical	See technical support
--------------------	-----------------------

T

technical support	
contacting JTAC.....	ix
text and syntax conventions.....	viii

