JunosE™ Software for E Series™ Broadband Services Routers

Packet Mirroring

Release
14.3.x

Published: 2013-07-15

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

JunosE™ Software for E Series™ Broadband Services Routers Packet Mirroring
Release 14.3.x

Revision History
July 2013—FRS JunosE 14.3.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

List of Figures

List of Tables

About the Documentation

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 xiv 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 xiv 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.	• 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)`

Italic text like this	• Emphasizes words. • Identifies variables. • Identifies chapter, appendix, and book names.	• There are two levels of access: *user* and *privileged*. • *clusterId, ipAddress.* • *Appendix A, System Specifications*
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
Italic text like this	Represents variables.	*mask*, *accessListName*

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 athttp://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

CHAPTER 1

How Packet Mirroring Works

Packet Mirroring Overview

Packet mirroring enables you to automatically send a copy of a packet to an external host for analysis. Packet mirroring has many uses, including traffic debugging and troubleshooting user networking problems.

The JunosE Software provides two methods that you can use to configure and manage your packet-mirroring environment—CLI-based and RADIUS-based.

- CLI-based packet mirroring—An authorized operator uses the router's CLI commands to configure and manage packet mirroring. You can mirror traffic related to a specific IP, IPv6, or L2TP interface or traffic related to a particular user. You also use CLI commands to create secure policies that identify the traffic to be mirrored and specify how the mirrored traffic is treated.
- RADIUS-based packet mirroring—A RADIUS administrator uses RADIUS attributes to configure packet mirroring of a particular user's traffic. The router creates dynamic secure policies for the mirroring operation.

In both the CLI-based and the RADIUS-based packet mirroring methods, the original traffic is sent to its intended destination and the mirrored traffic is sent to an analyzer (the mediation device). The mirroring operations are transparent to the user whose traffic is being mirrored.

NOTE: Packet mirroring operations require some system resources. To avoid performance degradation, limit the amount of mirrored traffic to a maximum of 5 percent of the E Series router's total traffic.

Packet mirroring is supported on ASIC-based modules. See *ERX Module Guide*, *Appendix A*, *Module Protocol Support* for information about modules supported on ERX routers. See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about modules supported on the E120 and E320 Broadband Services Routers.

Related Documentation

- CLI-Based Packet Mirroring Overview on page 17
- Comparing CLI-Based Mirroring and RADIUS-Based Mirroring on page 4
- Monitoring Packet Mirroring Overview on page 57
- Packet-Mirroring Terms on page 13
- RADIUS-Based Mirroring Overview on page 23

Comparing CLI-Based Mirroring and RADIUS-Based Mirroring

This section compares the characteristics of CLI-based and RADIUS-based mirroring techniques. You can use CLI-based mirroring for both interface-specific and user-specific mirroring; RADIUS-based mirroring is used for user-specific mirroring. This section highlights differences in configuration, security, and application of the CLI-based and RADIUS-based mirroring methods.

Configuration

This section describes differences in the configuration processes for CLI-based and RADIUS-based mirroring:

- CLI-based packet mirroring—You use CLI commands to configure and manage packet mirroring of specific interfaces and users. For interface-specific mirroring, you enable the static configuration after the IP interface is created. The interface method mirrors only the traffic on the specific interface.

  In user-specific mirroring, authentication, authorization, and accounting (AAA) uses RADIUS attributes as triggers to identify the user whose traffic is to be mirrored. The mirroring session starts when the user logs in. If the user is already logged in, AAA immediately starts the mirroring session when you enable packet mirroring.

- RADIUS-based packet mirroring—This dynamic method uses RADIUS and vendor-specific attributes (VSAs), rather than CLI commands, to identify a user whose traffic is to be mirrored and to trigger the mirroring session. A RADIUS administrator configures and enables the mirroring separate from the user's session. You can use a single RADIUS server to provision packet-mirroring operations on multiple E Series routers in a service provider's network.

  There are two variations of RADIUS-based packet mirroring. For both types, the mirroring feature is initiated without regard to the user location, router, interface, or type of traffic.

- User-initiated mirroring—If the user is not currently logged in, the mirroring session starts when the user logs in and is authenticated by RADIUS. The user's Acct-Session-Id is the identification trigger.
- RADIUS-initiated mirroring—If the user is already logged in, the JunosE RADIUS dynamic-request server uses RADIUS-initiated change-of-authorization (COA) messages to immediately start the mirroring session when the packet mirroring is enabled.

Security

The following list highlights security features provided by CLI-based and RADIUS-based mirroring:

- CLI-based packet mirroring—All packet mirroring commands are hidden by default. You must execute the **mirror-enable** command to make the mirroring commands visible. You can optionally configure authorization methods to control access to the **mirror-enable** command, which makes the packet mirroring commands available only to authorized users. The **mirror-enable** command is in privilege level 12 by default and the mirroring commands are in privilege level 13 by default. You can change the privilege levels of these commands; however, we recommend that you always put the **mirror-enable** command at a different privilege level than the mirroring commands.
- RADIUS-based packet mirroring—Access to RADIUS-based mirroring functionality is unrestricted. However, the display of mirroring functionality is restricted to privilege level 13 users by default. In addition, the user must execute the **mirror-enable** command to make the packet mirroring-related **show** commands visible.

  RADIUS-based mirroring uses dynamically created secure policies based on certain RADIUS VSAs. You attach the secure policies to the interface used by the mirrored user. The packet-mirroring VSAs that the RADIUS server sends to the E Series router are MD5 salt-encrypted.

Application

The following list compares the different types of packet-mirroring methods:

- CLI-based packet mirroring—Is useful when organizations want to provide separation between the typical network operations personnel and the mirroring operations personnel. For example, if security is essential, you might perform the entire packet-mirroring configuration on the analyzer device, separate from the normal network operations role. This way, only the authorized personnel on the analyzer device are aware of the mirroring operation. If this level of security is not required, authorized network operations personnel can perform the configuration and management on the router as usual.
  - CLI-based interface-specific mirroring—Can be useful in small networks with few E Series routers and in static environments where a user typically logs in to the same router through the same interface.
  - CLI-based user-specific mirroring—Is useful in B-RAS environments, in which users log in and log out frequently.

- RADIUS-based user-specific mirroring—Is triggered when needed, either when the specified user logs in (user-initiated) or when the user is already logged in and RADIUS-based mirroring is enabled or modified (RADIUS-initiated). RADIUS-based mirroring also provides an excellent solution for B-RAS networks, for example to troubleshoot traffic problems related to mobile users.

CLI-based user-specific and RADIUS-based user-specific mirroring are also useful to mirror L2TP traffic at the L2TP access concentrator (LAC). If the L2TP network server (LNS) and the LAC belong to different service providers, mirroring at the LAC enables mirroring to take place close to the user's domain.

Related Documentation

- CLI-Based Packet Mirroring Overview on page 17
- RADIUS-Based Mirroring Overview on page 23
- Packet Mirroring Overview on page 3

Avoiding Conflicts Between Multiple Packet Mirroring Configurations

The JunosE Software gives you a great deal of flexibility in creating your packet mirroring environment by supporting both the CLI-based and the RADIUS-based configuration methods. However, a conflict might occur when you use both methods. For example, a given subscriber might be targeted by both a CLI-based configuration and a RADIUS-based configuration. The rival configurations might use the same trigger to identify the subscriber, or they might use different triggers.

The configuration method that is applied to the subscriber depends on several variables: the trigger, when the packet mirroring configuration is created, and when the subscriber logs in. The following considerations apply to multiple packet mirroring configurations.

- CLI-based and RADIUS COA (RADIUS-initiated mirroring) configurations identify targeted subscribers according to the following configured criteria in the order given:
  1. Account session ID
  2. Calling station ID
  3. IP address associated with the virtual router where the subscriber logs in
  4. Username associated with the virtual router where the subscriber logs in
  5. NAS port ID
- A RADIUS log-in configuration always implicitly uses the Acct-Session-ID to identify the subscriber. This trigger has the highest priority of the five possible identification methods. For this reason, when a subscriber logs in, an existing RADIUS login configuration always takes effect over other packet mirroring configurations.
- A RADIUS COA configuration affects only subscribers that are currently logged in. It does not create persistent rules. Subscribers that log in after the COA request goes out are not mirrored by the configuration.

  If a subscriber that is mirrored by a RADIUS COA configuration subsequently logs out and then logs back in, that subscriber is no longer mirrored by the configuration.

However, that subscriber might now be mirrored by an existing RADIUS login or CLI-based configuration.

- A CLI-based configuration creates persistent rules. The configuration affects subscribers that are logged in when the configuration is created, and subscribers that log in thereafter.
- You can create a new configuration or modify an existing configuration to override a configuration that is currently mirroring subscribers. You must use the same subscriber selection criteria that were used by the current configuration. The overriding configuration can be either CLI-based or a RADIUS COA configuration; it does not have to match the configuration source used by the current configuration.
- When a CLI-based or RADIUS COA configuration identifies a targeted subscriber group, all members of the group are examined to determine whether any of these members is already mirrored using a different identification method. If that is the case, none of the group members is mirrored by the new configuration.
- Deletion of a CLI rule has no effect on subscribers that are currently being mirrored. They continue to be mirrored as before the deletion. These subscribers are not reevaluated against any remaining identification criteria when a CLI rule is deleted.
- When mirroring is disabled by RADIUS COA, subscribers that were being mirrored are not evaluated against an existing CLI configuration.
- When you create a CLI-based mirror rule, any previously configured secure policy that is attached to an interface and that is currently mirroring the subscriber traffic is overwritten. This secure policy attachment might be statically or dynamically attached to that subscriber interface. Also, the previously configured settings associated with the static secure policy that is attached to the subscriber interface are removed.

Consider the following scenarios.

Scenario 1: When Configurations Use the Same Identification Criteria

1. Currently logged-in subscribers are not being mirrored. These subscribers include 20 subscribers with the username joe@example.com. Their subscriber access is through virtual router boston1.
2. You create a RADIUS COA (RADIUS-initiated) configuration that targets subscribers that match joe@example.com logging in through virtual router boston1.
3. Mirroring begins for all 20 of these subscribers.
4. Ten more subscribers with the username joe@example.com log in through VR boston1. None of these new subscribers is mirrored because the RADIUS COA configuration makes no persistent rules.
5. You create a CLI configuration to mirror subscribers with username joe@example.com logging in through VR boston1.
6. All 30 of these subscribers are now mirrored. The CLI configuration expands the RADIUS COA configuration because both configurations use the same identification

criteria. The original mirrored users continue to be mirrored based on the COA configuration; the new users are mirrored based on the CLI configuration.

7. You delete the CLI configuration while the subscribers are still logged in and being mirrored. The deletion has no effect on these subscribers; mirroring continues as before the deletion.

Scenario 2: When Configurations Use Different Identification Criteria

1. Currently logged-in subscribers are not being mirrored. These subscribers include 20 subscribers with the username joe@example.com. Their subscriber access is through virtual router boston1.

   The subscribers have been assigned IP addresses 10.1.1.1 through 10.1.1.20.

2. You create a RADIUS COA (RADIUS-initiated) configuration that targets the subscriber that matches IP address 10.1.1.5 and VR boston1.
3. This subscriber is mirrored.
4. You create a CLI configuration to mirror subscribers with username joe@example.com logging in through VR boston1.
5. No additional subscribers are mirrored because one subscriber that matches that group (username and VR) is already being mirrored by another identification criterion (IP address and VR).

Related Documentation

- Comparing CLI-Based Mirroring and RADIUS-Based Mirroring on page 4
- Using Multiple Triggers for CLI-Based Packet Mirroring on page 35

Understanding the Prepended Header During a Packet Mirroring Session

During a packet mirroring session, the router prepends a special UDP/IP header to each mirrored packet that is sent to the analyzer interface. This prepended header is created by the policy-mirroring action, and is used for demultiplexing at the analyzer to sort through the multiple mirrored streams that arrive from different sources.

All mirrored L2TP session packets are prepended with a UDP/IP header. However, for IP traffic mirroring, the prepend header is optional; the header is added if the mirroring-related VSAs (VSAs 26-59 and 26-61) are both included in the RADIUS message. For CLI-based mirroring, the **analyzer-udp-port** keyword of the **mirror analyzer-ip-address** command creates the same information contained in the two VSAs. If you do not include the VSAs or the **analyzer-udp-port** keyword, an IP mirroring action is indicated, and the prepend header is not used.

NOTE: For IP mirroring, you must include both VSA 26-59 and VSA 26-61, or you must omit both of these VSAs. If you use only one of these VSAs, the configuration fails.

Figure 1 on page 9 shows the structure of the prepended header. The values in parentheses indicate the fixed value for individual fields. For fields that do not have a

fixed value listed, the value is dynamically created for each mirrored packet. Table 3 on page 9 lists the fields in the prepended header and indicates the values and field length.

Figure 1: Prepended Header

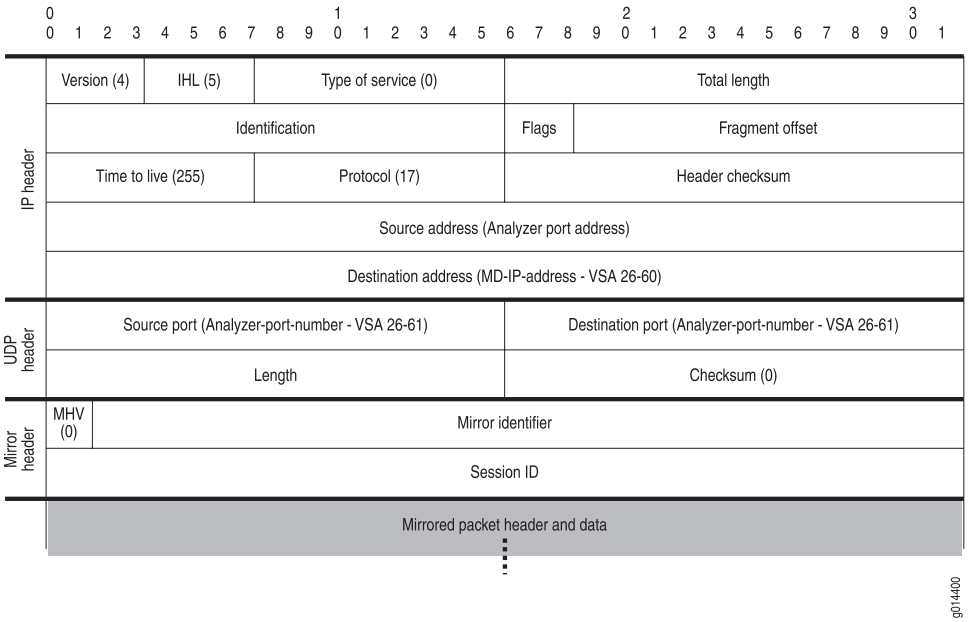


Table 3: Prepended Header Field Descriptions

Field	Value	Length (Bits)
IP Header		
Version	4	4
IHL	5	4
Type of Service	0	8
Total Length	Dynamically computed	16
Identification	Dynamically computed	16
Flags	Dynamically computed	3
Fragment Offset	Dynamically computed	13
Time to Live	255	8
Protocol	17	8
Header Checksum	Dynamically computed	16

Table 3: Prepended Header Field Descriptions *(continued)*

Field	Value	Length (Bits)
Source Address	Analyzer interface IP address	32
Destination Address	VSA 26-60	32
UDP Header		
Source Port	VSA 26-61	16
Destination Port	VSA 26-61	16
Length	Dynamically computed	16
Checksum	0	16
Mirror Header		
MHV (mirror header value)	0	2
Mirror Identifier	See "Format of the Mirror Header Attributes" on page 10 for details	30
Session-ID	See "Format of the Mirror Header Attributes" on page 10 for details	32

Format of the Mirror Header Attributes

The mirror header values are determined by the value that you configure in VSA 26-59. VSA 26-59 is declared as a hexadecimal string that can be either 8 bytes or 4 bytes long. The 8-byte format enables you to further specify the value that is used for the Session-ID field. If you use the 4-byte format, the router automatically determines the Session-ID field. The value in the 2-bit version field specifies the format that is used—0 indicates the 8-byte format, and 1 indicates the 4-byte format.

8-Byte Format

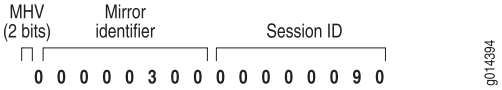
The 8-byte format of VSA 26-59 enables you to manually specify the Session-ID value in addition to the Mirror Identifier value. To use the 8-byte format, you configure the first two most significant bits of the first word of the VSA to a value of 0, which indicates two words in the VSA. The remaining 30 bits of the first word form the Mirror Identifier value, and the second word is the Session-ID field. You cannot change the order of these two words.

For example, a value of 0000030000000090 in VSA 26-59 configures the following fields in the mirror header, as shown in Figure 2 on page 11:

- MHV = 0

- Mirror Identifier = 0x300
- Session-ID = 0x90

Figure 2: 8-Byte Format of VSA 26-59



4-Byte Format

To use the 4-byte format of VSA 26-59, you configure the first two most significant bits of the VSA to a value of 1, which indicates a single word in the VSA. The remaining 30 bits of the word form the Mirror Identifier value. The router then creates the Session-ID value based on the least significant 32 bits of the Acct-Session-ID (RADIUS attribute 44).

For example, a value of 40000010 for VSA 26-59 configures the following fields in the mirror header, as shown in Figure 3 on page 11:

- MHV = 1
- Mirror Identifier = 0x10

Figure 3: 4-Byte Format of VSA 26-59

Related Documentation

- Configuring RADIUS-Based Packet Mirroring on page 41
- Packet Mirroring Overview on page 3
- RADIUS-Based Mirroring Sequence of Events on page 43

Optimizing Packet Mirroring Performance

Packet mirroring operations require some system resources. As a general rule, to avoid performance degradation, limit the amount of mirrored traffic to a maximum of 5 percent of the E Series router's total traffic.

For many packet mirroring environments, using the 5-percent guideline is sufficient. However, if you want to more closely manage packet mirroring's use of your router's resources, this section provides guidelines and equations to help you determine your packet mirroring requirements.

The guidelines for packet mirroring requirements use the following assumptions for a specific line module:

- A = Total input traffic at the line module
- B = Total output traffic at the line module

- X = Amount of traffic mirrored at input in the line module
- Y = Amount of traffic mirrored at output in the line module

Determine Traffic Loads

Using the previous assumptions, you can determine traffic loads for a given line module:

- A = Load at ingress side of the line module
- (B + X) = Load at egress side of the line module
- (A + 2X + Y) = Load at ingress to fabric from the line module

Establish Resource Guidelines

Next, using the traffic loads that you determined for the line module, you can establish guidelines for the amount of packet mirroring traffic for your router.

If you exceed these guidelines, regular (non-packet mirroring) packets from all subscribers, including nonmirrored subscribers, will be dropped. If the fabric bandwidth is not exceeded, then the performance penalties are contained within the slot where the packet mirroring activity occurs. However, if the fabric bandwidth is exceeded, traffic from other line modules might also be dropped.

- (A + 2X + Y) must be less than the maximum fabric bandwidth supported from this line module.
- (2X + Y) must be less than 100Mbps (the enforced queue limit).

  The 100 Mbps limit does not apply to the following line modules:

  - GE-2 line module (Juniper Networks ERX310 and ERX1440 Broadband Services Routers)
  - GE-HDE line module (ERX310 and ERX1440 router)
  - OC48 Frame APS I/O module (ERX1440 router only)
  - ES2 4G LM (E120 router and E320 Broadband Services Routers)
  - ES2 10G LM (E120/E320)
- (B + X) must be less than the maximum supported egress bandwidth.
- The number of mirrored interfaces per line module must be less than 1023 (the configuration enforced for secure policy attachments).
- The number of interfaces mirrored per chassis must be less than 2400 (the configuration enforced for secure policy attachments).

NOTE: **Packet mirroring can also affect the forwarding controller's packet handling performance.**

Related Documentation

- Packet Mirroring Overview on page 3

Logging Packet Mirroring Information

The JunosE Software's packet mirroring feature provides two secure methods of capturing and displaying packet mirroring-related information. Both methods ensure security by requiring the **mirror-enable** command to be enabled.

- Secure logging—Captures packet mirroring information to a local secure log on the router.
- SNMP secure packet mirroring traps—Captures and reports packet mirroring information to an external device; you can then use the privileged **show mirror trap** and **show snmp traps** CLI commands to view secure trap configuration information.

  SNMP agent also implements a secure audit logging facility for the debugging of packet mirroring traps and packet Mirror-MIB accesses. When secure audit logging is enabled, SNMP agent logs reported mirror traps and packet Mirror-MIB get/set operations to local volatile memory on the router.

By default, the JunosE Software captures packet mirroring-related activity to a secure local mirror log. No action is required on your part to enable or disable the logging process; however, only authorized users can access the secure log.

The secure logging feature includes the **clear mirror log** and **show mirror log** commands. The **mirror-enable** command must be enabled to make the commands visible in the CLI.

Related Documentation

- Packet Mirroring Overview on page 3
- *clear mirror log*
- *show mirror log*

Packet-Mirroring Terms

Table 4 on page 13 defines terms used in this discussion of packet mirroring.

Table 4: Packet-Mirroring Terminology

Term	Meaning
Analyzer device	Device that receives the mirrored traffic from the E Series router. Also called the mediation device.
Analyzer interface	IP interface in analyzer mode on the E Series router that is used to direct mirrored traffic to the analyzer device.
CLI access class	Security level that grants access to specific CLI commands.
Mediation device	Device that receives the mirrored traffic from the E Series router. Also called the analyzer device.

Table 4: Packet-Mirroring Terminology *(continued)*

Term	Meaning
Mirrored interface	Statically or dynamically configured interface on which traffic is being mirrored.
Mirrored user	User whose traffic is being mirrored.
Requesting authority	Group that is authorized to request or conduct packet mirroring.
Salt encryption	Random string of data used to modify a password hash.
Secure policy	Policies created with a mirror action and that contain information about where to forward mirrored traffic.
Trigger	RADIUS attribute that identifies a user whose traffic is to be mirrored. Packet mirroring starts when a trigger is detected. An E Series router supports a maximum of 100 mirror trigger rules.

Related Documentation

- CLI-Based Packet Mirroring Overview on page 17
- Packet Mirroring Overview on page 3
- Packet Mirroring Platform Considerations on page 14
- Packet Mirroring References on page 15
- RADIUS-Based Mirroring Overview on page 23

Packet Mirroring Platform Considerations

For information about modules that support packet mirroring on ERX14xx models, ERX7xx models, and the ERX310 Broadband Services Router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support packet mirroring.

For detailed information about the modules that support packet mirroring on the E120 and E320 Broadband Services Router:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the protocols and applications that support packet mirroring.

Related Documentation

- Packet Mirroring References on page 15

Packet Mirroring References

For more information about RADIUS-based packet mirroring, consult the following resources:

- RFC 3576—Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS) (July 2003)
- Lawfully Authorized Electronic Surveillance (LAES) for IP Network Access, American National Standard for Telecommunications, version PTSC-LAES-2006-084R6

Related Documentation

- Packet Mirroring Platform Considerations on page 14

CHAPTER 2

How CLI-Based Packet Mirroring Works

CLI-Based Packet Mirroring Overview

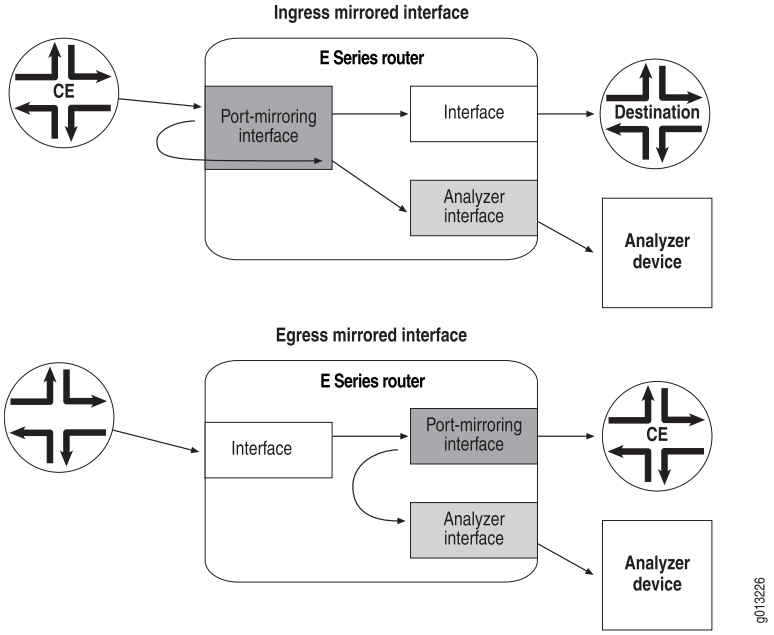
The JunosE Software enables you to use CLI commands to configure and manage packet mirroring on specific static IP interfaces, or for a specific user. You use CLI commands to create a secure policy that specifies the analyzer device and how the mirrored traffic is treated.

When you mirror an interface, you can replicate ingress and egress traffic on the interface (traffic entering or exiting the E Series router through that interface). When you mirror a user, you can replicate all traffic to or from the user.

In both interface-specific and user-specific mirroring, the original traffic is forwarded to its intended destination as usual, while the replicated copy of the traffic is forwarded to an analyzer interface on the E Series router. The analyzer interface then directs the mirrored traffic to the specified analyzer device for analysis.

Figure 4 on page 18 shows the traffic flow for ingress and egress IP interface mirroring.

Figure 4: CLI-Based Interface Mirroring



Related Documentation

- CLI-Based Packet Mirroring Sequence of Events on page 29
- Comparing CLI-Based Mirroring and RADIUS-Based Mirroring on page 4
- Configuring CLI-Based Packet Mirroring on page 27
- Monitoring CLI-Based Packet Mirroring on page 59
- Packet Mirroring Overview on page 3
- Reloading a CLI-Based Packet-Mirroring Configuration on page 32

Using SNMP Secure Packet Mirroring Traps

SNMP secure packet mirroring traps enable you to capture and report packet mirroring information to an external device; you can then view the secure information on the remote device. The secure packet mirroring traps feature is an extension of the router's standard SNMP implementation, and is only available to SNMPv3 users who are authorized to use packet mirroring.

You can also log mirror traps to local volatile memory for debugging purposes by enabling the SNMP secure log feature. See "Capturing SNMP Secure Audit Logs" on page 39 for details of secure audit logging. Normal console and syslog audit logs for packet mirroring traps and packet Mirror-MIB accesses are suppressed due to security concerns.

NOTE: **The contents of secure logs are not preserved across a reboot.**

The **mirror-enable** command must be enabled to make packet mirroring-related commands, command options, and **show** command output visible.

NOTE: You must use the CLI to configure the secure packet mirroring trap category to allow transmission of secure packet mirroring traps through the router—you cannot use SNMP to configure the secure packet mirroring trap category. However, after you have configured the secure packet mirroring trap category using the CLI, you can then use SNMP (juniPacketMirrorMIB.mi2) to enable and disable secure packet mirroring traps.

Table 5 on page 19 indicates the events that trigger secure packet-mirroring traps and lists the information sent in the trap for each event.

Table 5: Packet-Mirroring SNMP Traps

Trap Information Sent	Event That Triggers the Trap			
	A secure policy failed during COA-based or RADIUS-initiated packet mirroring	A secure policy failed during CLI trigger or CLI-based packet mirroring	An interface with secure policies attached is deleted	An analyzer is unreachable
Analyzer address	–	–	–	✓
Application name	✓	✓	–	–
Configuration source	✓	✓	✓	–
Date and time of event	–	✓	✓	✓
Error cause	✓	✓	–	–
Error string	✓	✓	–	–
Mirror ID	✓	–	✓	–
Mirroring direction	–	–	✓	–
Secure policy name	–	✓	✓	–
Secure policy UID	–	✓	✓	–
Session ID	✓	–	✓	–
Trigger event	✓	✓	✓	–
Trigger type	✓	✓	✓	–
Username	✓	–	–	–

Table 5: Packet-Mirroring SNMP Traps *(continued)*

Trap Information Sent	Event That Triggers the Trap			
	A secure policy failed during COA-based or RADIUS-initiated packet mirroring	A secure policy failed during CLI trigger or CLI-based packet mirroring	An interface with secure policies attached is deleted	An analyzer is unreachable
Virtual router (0 for L2TP)	✓	✓	✓	✓

Additional Packet-Mirroring Traps for CALEA Compliance

You can use the packet-mirroring traps shown in Table 6 on page 20 to help support compliance with the Communications Assistance for Law Enforcement Act (CALEA), which defines electronic surveillance guidelines for telecommunications companies. For example, a third-party vendor of mediation devices might receive packet mirroring traps from the router and convert the traps to messages that comply with CALEA, such as Lawfully Authorized Electronic Surveillance (LAES) for IP Network Access, American Nation Standard For Telecommunications messages. Individual traps might map to multiple LAES messages to provide additional compliance-related information.

Table 6: Packet-Mirroring Traps for CALEA Compliance

Trap	Description
juniPacketMirrorSessionStart	A grant has been issued to a mirrored subscriber.
juniPacketMirrorSessionEnd	A mirrored session has been terminated; includes the termination reason.
juniPacketMirrorInterfaceSessionActivated	A secure policy has been attached to an existing interface or to an existing session.
juniPacketMirrorInterfaceSessionDeactivated	A secure policy has been detached from an interface, not including interface or session termination.
juniPacketMirrorSessionReject	A deny has been issued because the potential mirrored user was not allowed on the network for some reason. However, the user would have been mirrored if access to the network had been allowed.
juniPacketMirrorSessionFailed	The user session was terminated before the secure policy was attached. For example, no resources were available to create the interface. The termination reason is included.

Packet Mirroring Trap Severity Levels

Table 7 on page 21 lists the default severity levels for packet mirroring traps. See the *JunosE System Basics Configuration Guide* for descriptions of the severity levels.

Table 7: Packet Mirroring Trap Severity Levels

Trap	Default Severity Level
juniPacketMirrorAnalyzerUnreachable	Warning
juniPacketMirrorCliTriggerBasedMirroringFailure	Error
juniPacketMirrorInterfaceDeleted	Notice
juniPacketMirrorInterfaceSessionActivated	Info
juniPacketMirrorInterfaceSessionDeactivated	Info
juniPacketMirrorRadiusBasedMirroringFailure	Error
juniPacketMirrorSessionEnd	Info
juniPacketMirrorSessionFailed	Info
juniPacketMirrorSessionStart	Info
juniPacketMirrorSessionReject	Info

See Configuring SNMP in *JunosE System Basics Configuration Guide* for information about JunosE Software SNMP support.

Related Documentation

- Configuring SNMP Secure Packet Mirroring Traps on page 38
- Monitoring SNMP Secure Packet Mirroring Traps on page 69
- *mirror trap-enable*
- *snmp-server clear secure-log*
- *snmp-server enable traps*
- *snmp-server host*
- *snmp-server secure-log*
- *show mirror trap*
- *show snmp secure-log*

CHAPTER 3

How RADIUS-Based Packet Mirroring Works

RADIUS-Based Mirroring Overview

RADIUS-based packet mirroring enables you to mirror traffic related to a specific user, without regard to how often the user logs in or out, or which E Series router or interface the user uses. RADIUS-based mirroring is particularly appropriate for large networks, because you can use a single RADIUS server to provision mirroring on multiple E Series routers in a service provider's network. RADIUS-based mirroring is useful when debugging network problems related to mobile users, who do not always log in to a particular router.

You configure RADIUS-based mirroring independent of the actual mirroring session—you can configure the mirroring parameters at any time. RADIUS-based mirroring uses RADIUS and VSAs, rather than CLI commands, to specify the user whose traffic is to be mirrored. The VSAs specify attributes that are carried in Access-Accept messages and change-of-authorization messages from the RADIUS dynamic-request server to the E Series router.

NOTE: **You cannot use RADIUS-based packet mirroring to mirror static interfaces, which might not be authenticated through RADIUS. To mirror static interfaces, you must use CLI-based mirroring.**

Related Documentation

- Comparing CLI-Based Mirroring and RADIUS-Based Mirroring on page 4
- Configuring RADIUS-Based Packet Mirroring on page 41
- Packet Mirroring Overview on page 3
- RADIUS-Based Mirroring Sequence of Events on page 43
- RADIUS Attributes Used for Packet Mirroring on page 44

PART 2

Configuration

CHAPTER 4

Configuration Tasks for CLI-Based Packet Mirroring

Configuring CLI-Based Packet Mirroring

To configure the CLI-based packet-mirroring environment, you must coordinate the mirroring operations of two devices in the network: the E Series router and the analyzer device. The configuration of the analyzer device is mentioned in this section for reference only. The actual configuration procedures depend on the policies and guidelines established by the responsible organizations.

The **secure ip policy** and **secure ipv6 policy** commands are visible only to authorized users; the **mirror-enable** command must be enabled before using **secure ip policy** or **secure ipv6 policy** command. If you enter the **secure ip policy** or **secure ipv6 policy** command and the policy list does not exist, the router creates a policy list with a default mirror rule that disables mirroring. If you attach this policy list to an interface, there is no packet mirroring. When you use this command to create a secure policy list, statistics-related keywords are not supported.

The **secure ip classifier-list** command creates or modifies a secure IP classifier control list, which can then be included in a secure policy list.

The **secure ipv6 classifier-list** command creates or modifies a secure IPv6 classifier control list, which can then be included in a secure policy list.

NOTE: Do not use the asterisk (*) for the name of a classifier list. The asterisk is used as a wildcard for the **classifier-group** command.

Except for the following considerations, secure IP classifier lists are created and function the same as standard IP classifier lists—see *Classifier Control Lists Overview* for information:

- The **secure ip classifier-list** and **secure ipv6 classifier-list** commands are visible only to authorized users—the **mirror-enable** command must be enabled before using this command.
- Secure IP classifier lists and secure IPv6 classifier lists are the only types of classifier lists allowed in secure policy lists
- Secure IP classifier lists and secure IPv6 classifier lists cannot be used in non-secure policy lists.
- You can associate secure IP and secure IPv6 policy classifier lists with all secure IP and secure IPv6 policies dynamically created by RADIUS. This allows you to selectively identify and drop high load traffic, such as video.

The **secure ip policy-list**, **secure ipv6 policy-list**, and **secure l2tp policy-list** commands create or modify a secure IP, IPv6, or L2TP policy list. These commands are visible only to authorized users—the **mirror-enable** command must be enabled before using this command. These commands enter Policy List Configuration mode, enabling you to specify the parameters of the secure policy list. If you enter Policy List Configuration mode and then type **exit** without specifying any parameters, the router creates a policy list with a mirror disable rule. Attaching this policy list to an interface results in no packet mirroring.

Secure IP classifier lists are the only type of classifier lists allowed in secure IP policy lists. Secure L2TP policies do not support classification. Therefore, the only classifier group you can use for secure L2TP policies is **classifier-group ***. You cannot delete a secure policy list that is currently attached to an interface.

Related Documentation

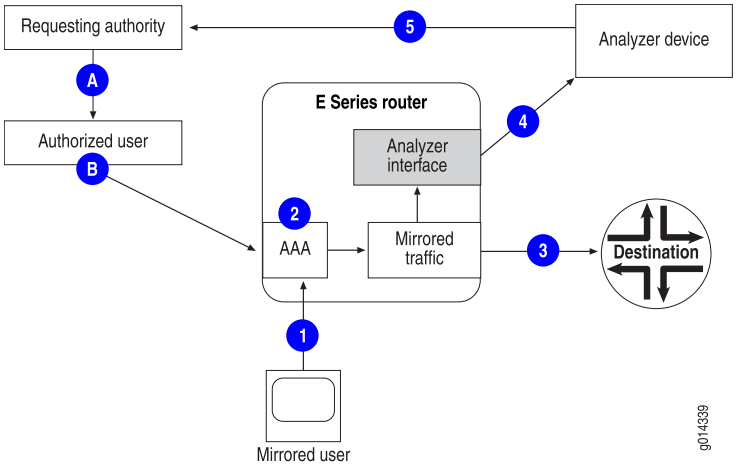
- Enabling and Securing CLI-Based Packet Mirroring on page 31
- CLI-Based Packet Mirroring Sequence of Events on page 29
- Reloading a CLI-Based Packet-Mirroring Configuration on page 32
- *classifier-group*
- *ip analyzer*
- *ip mirror*
- *ip policy*

- *mirror*
- *mirror analyzer-ip-address*
- *mirror disable*
- *mirror disable*
- *secure ip classifier-list*
- *secure ipv6 classifier-list*
- *secure ip policy-list*
- *secure ipv6 policy-list*
- *secure l2tp policy-list*

CLI-Based Packet Mirroring Sequence of Events

Figure 5 on page 29 shows the sequence of events that take place during CLI-based mirroring. The tables after the figure describe the events indicated by the numbers and letters in the figure. Table 8 on page 29 describes the configuration process; Table 9 on page 30 describes the flow of traffic during a mirroring operation that is initiated when the user logs in; and Table 10 on page 30 describes the flow of traffic when mirroring a user who is already logged in or when mirroring a static interface.

Figure 5: CLI-Based Packet Mirroring



To create a CLI-based packet mirroring environment, you must complete the processes listed in Table 8 on page 29.

Table 8: Setting Up the CLI-Based Packet-Mirroring Environment

Process	Description
A	The authorized individual requests packet mirroring of a user's or interface's traffic and configures the analyzer device to receive mirrored traffic.

Table 8: Setting Up the CLI-Based Packet-Mirroring Environment *(continued)*

Process	Description
B	An individual who is authorized to use the packet mirroring CLI commands configures the packet mirroring environment, including the secure policy, analyzer interface connection to the analyzer device, and the interface or trigger information.

Table 9 on page 30 indicates the sequence of steps for a packet-mirroring operation that takes place when a user starts a new session.

Table 9: CLI-Based User-Specific Mirroring During Session Start

Step	Description
1	The user logs in to an E Series router, requesting authentication by AAA.
2	AAA authenticates the user, and the router starts mirroring the user's traffic.
3	The router sends the user's original traffic to the intended destination.
4	The router sends the mirrored traffic to the analyzer device.
5	The analyzer device provides information to the requesting individual.

Table 10 on page 30 indicates the sequence of steps for a packet-mirroring operation that is configured for an interface or for a user who is already logged in.

Table 10: CLI-Based Mirroring of Currently Running Session

Step	Description
1	For user-specific mirroring, the user logs in to the E Series router; no mirroring action is configured.
2	• CLI-based packet mirroring is configured and enabled on the router. • For interface-specific mirroring, the router starts mirroring all traffic for the interface. • For user-specific mirroring, AAA verifies that the mirrored user is already logged in, then starts mirroring all subsequent traffic to or from the user.
3	The router sends the original traffic to its intended destination.
4	The router sends mirrored traffic to the analyzer device.
5	The analyzer device provides information for the requesting individual.

Related Documentation

- Enabling and Securing CLI-Based Packet Mirroring on page 31
- Configuring CLI-Based Packet Mirroring on page 27
- Reloading a CLI-Based Packet-Mirroring Configuration on page 32

Enabling and Securing CLI-Based Packet Mirroring

The JunosE Software enables you to create a secure environment for your packet-mirroring operation by restricting access to the packet mirroring CLI commands and information. For example, when dealing with a critical diagnostic or troubleshooting procedure, you might want the packet-mirroring feature to be available and visible to a subset of your network operations group. Or, if you are monitoring confidential traffic from a particular user, you might want the configuration and results of the mirroring operation to be available only to a unique group, such as the management group of the analyzer device.

By default, the packet mirroring configuration commands are hidden from all users. You must use the **mirror-enable** command to make the commands visible, which then enables you to configure the packet-mirroring environment. The command applies only to the current CLI session. When you log out of the current session and then log in again, the packet mirroring commands are no longer visible,

NOTE: The **no mirror-enable** command makes the packet mirroring commands no longer visible. However, any active mirroring sessions are unaffected and traffic continues to be mirrored.

To create a secure packet-mirroring environment, you use a combination of the JunosE Software authorization methods and the **mirror-enable** command. You configure the authorization method to control who can use the **mirror-enable** command. Authorized users can then issue the **mirror-enable** command, making the packet mirroring commands visible. However, the commands are still hidden from unauthorized users.
Table 11 on page 31 lists the commands whose visibility is controlled by the **mirror-enable** command.

Table 11: Commands Made Visible by the mirror-enable Command

• ip policy { secure-input | secure-output }	• secure ipv6 policy-list
• show ip interface (packet mirroring information)	• ipv6 policy { secure-input | secure-output }
• clear mirror log	• show ipv6 interface (packet mirroring information)
• mirror acct-session-id	• show mirror log
• mirror agent-circuit-id	• show mirror rules
• mirror agent-remote-id	• show mirror trap
• mirror analyzer-ip-address	• show mirror subscribers
• mirror calling-station-id	• show secure classifier-list
• mirror dhcp-option-82	• show secure policy-list

Table 11: Commands Made Visible by the mirror-enable Command *(continued)*

• mirror disable	• show snmp secure-log
• mirror ip-address	• show snmp trap (packet mirroring information)
• mirror nas-port-id	• snmp-server clear secure-log
• mirror trap-enable	• snmp-server secure-log
• mirror username	• snmp-server enable traps (packetMirror keyword)
• secure ip classifier-list	• snmp-server host (packetMirror keyword)
• secure ip policy-list	• secure ipv6 classifier-list
• secure l2tp policy-list	

To provide increased security, the **mirror-enable** command must be the only command at its access level (level 12 by default) and it also must be at a different privilege level than the other packet mirroring commands (level 13 by default) and other regular JunosE CLI commands. This separation enables you to control authorization to the **mirror-enable** command and to limit the visibility of packet mirroring commands. For example, if you are using TACACS+, the **mirror-enable** command is the only packet mirroring command that is sent to the TACACS+ server. You can also use TACACS+ to prevent unauthorized individuals from modifying the configuration of analyzed ports.

See *Chapter 7, Passwords and Security* in *JunosE System Basics Configuration Guide* for more information about access levels and *Chapter 9, Configuring TACACS+* in *JunosE Broadband Access Configuration Guide* for information about TACACS+ authorization.

Related Documentation

- CLI-Based Packet Mirroring Overview on page 17
- CLI-Based Packet Mirroring Sequence of Events on page 29
- Configuring CLI-Based Packet Mirroring on page 27
- Reloading a CLI-Based Packet-Mirroring Configuration on page 32

Reloading a CLI-Based Packet-Mirroring Configuration

You can reload your packet mirroring configuration as part of a configuration file (.cnf) reload operation or when you run a script file (.scr) that you have saved from the **show configuration** command display. When you reload a .cnf file, the packet-mirroring configuration is restored—no additional steps are required.

For a .scr file operation, the **mirror-enable** command must be enabled both before saving the scr. file from the **show configuration** display and also before you run the script to reload the packet-mirroring configuration. If the **mirror-enable** command is not enabled, the .scr file operation for the packet-mirroring configuration fails.

Related Documentation

- Enabling and Securing CLI-Based Packet Mirroring on page 31
- CLI-Based Packet Mirroring Overview on page 17
- CLI-Based Packet Mirroring Sequence of Events on page 29
- Configuring CLI-Based Packet Mirroring on page 27
- *mirror-enable*
- *show configuration*

Using TACACS+ and Vty Access Lists to Secure Packet Mirroring

This procedure uses TACACS+ and vty access lists to manage the users who have access to the **mirror-enable** command. An authorized user who issues the **mirror-enable** command then gains access to the packet mirroring CLI commands and information.

This technique enables you to restrict the visibility and use of packet mirroring commands to a controlled, authorized group of users.

1. Configure TACACS+ authorization for the access level of the **mirror-enable** command (level 12 by default).

   Configure the router either to allow or disallow authorization when the TACACS+ servers are not available.

2. Configure all vty lines and the console to use the TACACS+ authorization configuration from Step 1 for access level 12 commands.

This procedure ensures that packet mirroring commands are never sent out of the E Series router—only the **mirror-enable** command is sent. The packet mirroring configuration and all information about mirrored interfaces and subscribers are available only to users who are authorized for the packet mirroring CLI commands on the router.

Related Documentation

- CLI-Based Packet Mirroring Overview on page 17
- Configuring CLI-Based Packet Mirroring on page 27
- Using Vty Access Lists to Secure Packet Mirroring on page 33
- *mirror-enable*

Using Vty Access Lists to Secure Packet Mirroring

In this procedure, TACACS+ authorization is not used. However, you can still use vty access lists to control access to the **mirror-enable** command, which enables you to create isolation between the authorized packet mirroring users and unauthorized network operators.

1. Configure TACACS+ authorization for the **mirror-enable** command privilege level. Specify that authorization is denied if TACACS+ is not available. Because TACACS+ is not being used, authorization always fails.

2. Configure the *majority* of the vty lines and the console to use the authorization configuration from Step 1. (Users who use Telnet on these lines are denied access to the **mirror-enable** command.)
3. On the remaining vty lines (without the TACACS+ authorization) create an access list that contains the IP addresses of the users that you want to grant access to these vty lines—these users are granted access to the **mirror-enable** command, and therefore, the packet-mirroring feature.

This configuration grants access to the packet mirroring CLI commands to the users from the specified IP addresses. The packet mirroring commands remain hidden for all other users.

Related Documentation

- CLI-Based Packet Mirroring Overview on page 17
- Configuring CLI-Based Packet Mirroring on page 27
- Using TACACS+ and Vty Access Lists to Secure Packet Mirroring on page 33
- *mirror-enable*

Configuring Triggers for CLI-Based Mirroring

In user-specific packet mirroring, you use triggers to identify the user whose traffic you want to mirror and to start the mirroring session. The triggers are similar to the RADIUS attributes used in RADIUS-based mirroring. However, for CLI-based mirroring, AAA can use any supported authentication method, including RADIUS.

NOTE: An E Series router supports a maximum of 100 mirror trigger rules.

Attributes associated with users are examined in the following order of priority to find a match. When a match is found, examination stops.

1. Account session ID
2. Calling station ID
3. Username and virtual router ID
4. IP address and virtual router ID
5. Nas-Port-Id

You specify the triggers with the **mirror** command, except that the virtual router associated with username or IP address is taken from the VR context from which you issue the command.

The following considerations apply to trigger rules:

- A new trigger rule is not applied to matching connected subscribers if any of the subscribers is mirrored by another rule.

- CLI-initiated mirroring per account session ID creates a rule that continues to exist after the subscriber logs out.
- RADIUS COA messages affect only currently connected subscribers; they do not create persistent rules.

Related Documentation

- Configuring CLI-Based Packet Mirroring on page 27
- Example: Configuring CLI-Based Interface-Specific Packet Mirroring on page 51
- Example: Configuring CLI-Based User-Specific Packet Mirroring on page 52

Using Multiple Triggers for CLI-Based Packet Mirroring

When you configure CLI-based packet mirroring, you can create multiple mirroring rules for a particular subscriber. For example. you might create two rules; one rule that uses IP address as the trigger that identifies the user and a second rule with the subscriber's username as the trigger. You can also configure RADIUS-based mirroring to use multiple methods to identify subscribers

To avoid conflicts between multiple mirroring rules, both CLI-based and RADIUS-based mirroring operations assign a precedence to the subscriber identification triggers. Subscriber information is examined for configured triggers according to the order of precedence.

The following list indicates the order of precedence for the subscriber identification triggers; Acct-Session-Id has the highest precedence. The keywords for the **mirror** and **mirror disable** command are listed below with their associated RADIUS attributes.

1. **acct-session-id**—Acct-Session-Id, RADIUS attribute [44]
2. **calling-station-id**—Calling-Station-Id, RADIUS attribute [31]
3. **ip-address**—Framed-IP-Address, RADIUS attribute [8]; associated with the virtual router where the subscriber logs in, RADIUS VSA [26-1]
4. **username**—User-Name, RADIUS attribute [1]; associated with the virtual router where the subscriber logs in, RADIUS VSA [26-1]
5. **nas-port-id**—NAS-Port-Id, RADIUS attribute [87]
6. **dhcp-option-82**—DHCP-Option-82, RADIUS attribute [26–159], Vendor ID 4874
7. **agent-circuit-id**—Agent-Circuit-ID, RADIUS attribute [26–1], Vendor ID 3561
8. **agent-remote-id**—Agent-Remote-ID, RADIUS attribute [26–2], Vendor ID 3561

For example, suppose you create the following three rules to trigger a packet mirroring session.

```
host1(config)#mirror ip-address 192.168.105.25 ip secure-policy-list securePolicyIp4
host1(config)#mirror username jwbooth@isptheatre.com ip secure-policy-list
  securePolicyIp15
host1(config)#mirror acct-session-id atm 2/1.2:0.42:0001048579 ip secure-policy-list
  securePolicyIp10
```

Regardless of the order in which you configure the rules, the subscriber information is first examined to determine whether the Acct-Session-Id matches the rule. If it does, no further examination takes place and the subscriber's traffic is mirrored,

If the Acct-Session-Id does not match, then the subscriber information is next examined to determine whether the Calling-Station-Id matches the rule. This process continues for all configured rules.

If none of the trigger rules are matched, then that subscriber's traffic is not mirrored.

If the packet mirroring request is a RADIUS-initiated session (a RADIUS-based packet mirroring session for a subscriber who is already logged in), the router verifies the validity of all of the mirroring rules related to the particular subscriber. If any of the rules fail (for example, the identification fields do not match), the packet mirroring request is denied.

The calling-station-id trigger is externally visible only for tunneled users (if there are no RADIUS overrides). If a case-sensitive user name does not match a subscriber's name or if the dynamic IP interface UID does not exist, the subscriber is disregarded.

Related Documentation

- Avoiding Conflicts Between Multiple Packet Mirroring Configurations on page 6
- Configuring Triggers for CLI-Based Mirroring on page 34

Configuring the Analyzer Device

The analyzer device must be configured to receive the mirrored traffic from the E Series router's analyzer interface. You can use the **default** keyword with the **interface** command to configure an interface as the virtual router's default analyzer interface; it is then used when an analyzer interface is not explicitly specified in the **ip mirror** command. You cannot configure multiaccess interfaces, such as IP over Ethernet, as default analyzer interfaces.

You can configure any type of IP interface on the E Series router as an analyzer interface, except for special interfaces such as SRP interfaces, null interfaces, and loopback interfaces. An interface cannot be both an analyzer interface and a mirrored interface at the same time. A single analyzer interface can serve multiple mirrored sessions. Analyzer interfaces drop all nonmirrored traffic.

You can configure IP or GRE analyzer interfaces to enable traffic to flow between tunnel endpoints that are local to the router. The tunnel can be located on a shared tunnel server port or line module. For a complete list of the line modules and I/O modules available for ERX14xx models, ERX7xx models, and the ERX310 Broadband Services Router, see *ERX Module Guide*. For more information about line modules and IOAs available with the E120 and E320 Broadband Services Routers, see *E120 and E320 Module Guide*.

Shared tunnel server on the ES2 10G ADV LM supports GRE tunnels for tunneling the mirrored data packets. The mirrored data is forwarded to the analyzer device using the GRE analyzer interface. Use the **ip analyzer** command to configure the GRE tunnel interface to act as a GRE analyzer tunnel interface. The ES2 10G ADV LM does not support non-analyzer tunnel interfaces. Also, when you configure a GRE interface for checksum calculations, use of sequence numbers, session keys, and other optional parameters, the

ES2 10G ADV LM does not support those GRE interfaces. However, if you have configured a non-analyzer tunnel interface or a GRE interface with optional parameters, these interfaces remain non-operational. The GRE analyzer interface forwards mirrored traffic and drops all non-mirrored traffic.

Also, placement of GRE tunnels on the supported locations is no longer synchronous with the tunnel configuration. So, you can configure tunnel servers when the chassis does not support the required resources such as shared tunnel server ports or tunnel server modules. However, the tunnels configured are non-operational. The tunnels become operational when the required resources are added to the chassis.

NOTE: If a chassis has shared or dedicated tunnel server on the ES2 4G LM and shared tunnel server on the ES2 10G ADV LM, the GRE non-analyzer tunnel interfaces are available on the ES2 4G LM. Only GRE analyzer interfaces with no optional configurations are available on the ES2 10G ADV LM shared tunnel server.

Policies are not supported on analyzer interfaces. When you configure an analyzer interface, existing policies are disabled, and no new policies are accepted.

Related Documentation

- CLI-Based Packet Mirroring Sequence of Events on page 29
- Configuring CLI-Based Packet Mirroring on page 27
- Resolving and Tracking the Analyzer Device's Address on page 37
- *ip analyzer*
- *ip mirror*

Resolving and Tracking the Analyzer Device's Address

During the packet mirroring configuration process, you specify the IP address of the analyzer device to which the mirrored traffic is sent. For CLI-based packet mirroring, you use the **mirror analyzer-ip-address** command to specify the IP address. For RADIUS-based packet mirroring, the RADIUS attribute Med-IP-Address [26-60] is the address of the analyzer device.

After configuration is complete, the router performs a route lookup to resolve the analyzer device's address and to ensure that traffic can be forwarded to the analyzer device for analysis. However, the analyzer device is considered unreachable if the router's analyzer interface is not in analyzer mode, is not yet created, or if the routes to the analyzer device are absent

If the analyzer device is unreachable, then the mirror action in the secure policy is disabled, and no packets are mirrored. The **show secure policy-list** command output indicates that the mirror action is disabled and the analyzer device is unreachable.

The router tracks the analyzer device's IP address for any route changes within the router. This tracking ability provides a degree of failure recovery by enabling you to configure multiple analyzer interfaces to serve as redundant ports to reach the analyzer device.

Related Documentation

- Configuring the Analyzer Device on page 36
- *mirror analyzer-ip-address*
- *show secure policy-list*

Configuring the E Series Router to Support CLI-Based Mirroring

To configure the router to support CLI-based packet mirroring:

1. Configure the analyzer interface, the route to the analyzer device, and any static ARP entries.
2. Allow authorized users to have access to the **mirror-enable** command. The users can then make the packet mirroring CLI commands visible and perform the following steps.
3. Configure the secure policy that forwards the mirrored traffic to the analyzer device.
4. (Optional) For increased security, create an IPSec tunnel between the analyzer interface and the analyzer device.
5. For interface-specific mirroring, attach the secure policy to the interface.
6. For user-specific mirroring, configure the trigger that identifies the user.

Related Documentation

- CLI-Based Packet Mirroring Sequence of Events on page 29
- Configuring CLI-Based Packet Mirroring on page 27
- *mirror-enable*

Configuring SNMP Secure Packet Mirroring Traps

To configure SNMP secure traps support, perform the following tasks on your E Series router:

1. Enable packet mirroring support.
2. Configure the packet mirroring application to generate traps.
3. (Optional) Verify the packet mirroring trap configuration.
4. (Optional) Configure the SNMP server to support secure logs.
5. Configure the SNMP server to generate packet mirroring traps.
6. Configure the SNMPv3 user for whom packet mirroring traps are generated.
7. Configure the SNMP server to report packet mirroring traps to a remote host.
8. (Optional) Verify the SNMP server packet mirroring configuration.

The following example illustrates the procedure to configure SNMP secure packet mirroring traps support:

```
host1#mirror-enable
host1#configure terminal
host1(config)#mirror trap-enable
host1(config)#show mirror trap
Traps are enabled
host1(config)#snmp-server secure-log
host1(config)#snmp-server user fredMirrorUser group mirror authentication md5
  fred-md5password privacy des fred-despassword
host1(config)#snmp-server enable traps packetMirror trapFilters notice
host1(config)#snmp-server host 192.168.57.103 version 3 fredMirrorUser  cliSecurityAlert
  packetMirror trapFilters notice
host1(config)#show snmp trap

Enabled Categories: CliSecurity, PacketMirror, Sonet
SNMP authentication failure trap is disabled
Trap Source: FastEthernet 6/0, Trap Source Address:192.168.120.78
Trap Proxy: enabled
Global Trap Severity Level: 6 - informational
Address          Security String                   Ver  Port   Trap Categories
---------------  --------------------------------  ---  -----  ----------------
192.168.1.1      host1                             v1   162    Cli
192.168.57.103   fredMirrorUser                    v3   162    CliPacketMirror
192.168.57.162   host2                             v3   162    Sonet
Address         TrapSeverityFilter  Ping    Maximum    Queue    Queue Full
                                   TimeOut QueueSize DrainRate discrd methd
--------------- ------------------ ------- --------- --------- -------------
192.168.1.1     5 - notice         1       32        0         dropLastIn
192.168.57.103  5 - notice         1       32        0         dropLastIn
192.168.57.162  2 - critical       1       32        0         dropLastIn
```

See Configuring SNMP in *JunosE System Basics Configuration Guide* for information about JunosE Software SNMP support.

Related Documentation

- Using SNMP Secure Packet Mirroring Traps on page 18
- Monitoring SNMP Secure Packet Mirroring Traps on page 69
- *mirror trap-enable*
- *snmp-server clear secure-log*
- *snmp-server enable traps*
- *snmp-server host*
- *snmp-server secure-log*
- *show mirror trap*
- *show snmp secure-log*

Capturing SNMP Secure Audit Logs

SNMP secure audit logging enables administrators to collect the SNMP audit logs for mirror traps and Mirror-MIB get/set operations with the protection of the mirror enabling

feature. Secure audit logging facilitates the debugging of issues related to SNMP packet mirror traps.

All normal SNMP console and syslog audit logs (including snmpTrap, snmpPduAudit, and snmpSetPduAudit) for secure traps and Mirror-MIB are suppressed due to security concerns. When you have issued the **mirror enable** command, you can issue the **snmp secure-log** command to capture secure audit logs. Configuration, storage, and display of the SNMP secure logging is on global basis rather than a per-VR basis.

The SNMP agent captures and stores the audit logs for secure traps. The SNMP agent also captures PDU audit logs for Mirror-MIB operations. Configure the snmpTrap, snmpPduAudit, and snmpSetPduAudit logs at the proper severity level to capture the secure audit logs.

You can use the **show snmp secure-log** command to display the captured secure logs. Secure logs are stored in a string format similar to SNMP trap audit logs. You can use the **snmp-server clear secure-log** command to reset the secure logs.

The secure log data is not persistent. Secure audit logs are not available after a warm or cold restart of the SNMP agent, because the SNMP agent does not store the secure logs in NVS. The SNMP agent can store a maximum of 100 secure logs before overwriting the logs.

The secure log configuration is persistent. The configuration is available after a warm restart operation because it is stored in the nonvolatile memory. Based on the configuration, data is logged for the packet mirrors that are automatically applied during subscriber login for the newly attached secure policy after the restart operation.

To enhance security, you can configure and display the secure audit logs only through the CLI. You cannot use SNMP to configure and display the logs. Secure trap logs are not populated in the notification logs MIB. From the perspective of the notification log MIB, secure traps do not exist.

Related Documentation

- Monitoring SNMP Secure Audit Logs on page 71
- *snmp-server clear secure-log*
- *snmp-server secure-log*
- *show snmp secure-log*
- *show snmp trap*

CHAPTER 5

Configuration Tasks for RADIUS-Based Packet Mirroring

Configuring RADIUS-Based Packet Mirroring

To configure the RADIUS-based packet mirroring environment, you must coordinate the mirroring operations of three devices in the network: the RADIUS server, the E Series router, and the analyzer device. The configuration of the RADIUS server and the analyzer device is described in this section for reference only. The actual configuration procedures depend on the policies and guidelines established by the responsible organizations.

Configuring the RADIUS Server

Table 17 on page 46 lists the VSAs that are included for both types of RADIUS-based mirroring—user-initiated (when the user logs in to start a new session), and RADIUS-initiated (when the user is already logged in).

Disabling RADIUS-Based Mirroring

To disable mirroring, you include the RADIUS attribute (for example, Acct-Session-ID) and set the Mirror-Action attribute to 0 in the mirrored user's RADIUS record.

You can also use the **mirror disable** CLI commands to disable RADIUS-based mirroring. You must use the version of the **mirror disable** command that corresponds to the RADIUS attribute that was used to identify the user. For example, if you used the RADIUS Calling-Station-ID attribute to create the mirroring session, you must use the **mirror disable calling-station-id** command to disable the session.

NOTE: All RADIUS-based mirroring sessions that start when a user logs in are considered to use the Acct-Session-ID attribute. Therefore, you must use the **mirror disable acct-session-id** command to disable these sessions. For RADIUS-based sessions of a user that is already logged in, you use the **mirror disable** command with the same keyword you used to configure the session.

Configuring the Analyzer Device

The analyzer device must be configured to receive the mirrored traffic from the E Series router's analyzer interface. The analyzer interface directs mirrored traffic to the specified analyzer device for analysis. You can configure the interface as the virtual router's default analyzer interface. You cannot configure multiaccess interfaces, such as IP over Ethernet, as default analyzer interfaces.

When mirroring an IP interface, the analyzer interface must reside in the same virtual router as the mirrored interface. When mirroring an L2TP interface, the analyzer interface must reside in the default virtual router.

NOTE: You must configure a static route to reach the analyzer device through the analyzer interface. If the analyzer interface is an IP over Ethernet interface, you must also configure a static Address Resolution Protocol (ARP) entry to reach the analyzer device.

You can configure any type of IP interface on the E Series router as an analyzer interface, except for special interfaces such as SRP interfaces, null interfaces, and loopback interfaces. An interface cannot be both an analyzer interface and a mirrored interface at the same time. A single analyzer interface can support multiple mirrored interfaces. The receive side of the analyzer interface is disabled. All traffic attempting to access the router through an analyzer interface is dropped. Analyzer interfaces drop all nonmirrored traffic. Policies are not supported. When you configure an analyzer interface, existing policies are disabled, and no new policies are accepted.

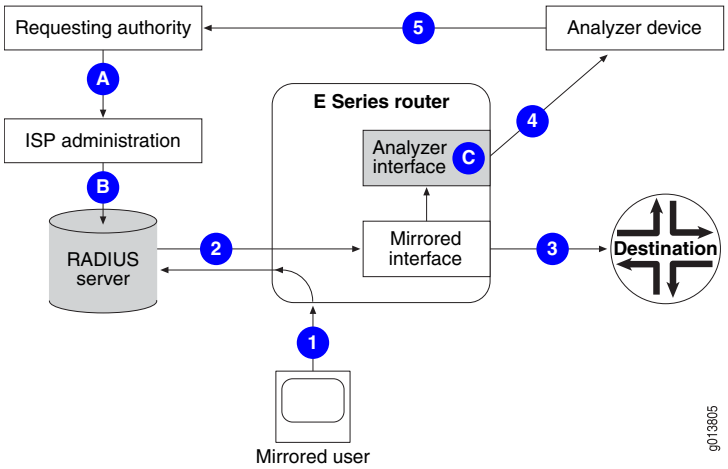
Related Documentation

- RADIUS-Based Mirroring Overview on page 23
- RADIUS-Based Mirroring Sequence of Events on page 43
- *authorization change*
- *ip analyzer*
- *key*
- *mirror disable*
- *radius dynamic-request server*
- *udp-port*

RADIUS-Based Mirroring Sequence of Events

Figure 6 on page 43 shows the sequence of events that take place during RADIUS-based mirroring. The tables after the figure describe the events indicated by the numbers and letters in the figure. Table 12 on page 43 describes the configuration process; Table 13 on page 43 describes the flow of traffic during a mirroring operation that is initiated when the user logs in; and Table 14 on page 44 describes the flow of traffic when mirroring a user who is already logged in.

Figure 6: RADIUS-Based Packet Mirroring



To create a RADIUS-based packet-mirroring environment, you must complete the processes listed in Table 12 on page 43.

Table 12: Setting Up the RADIUS-Based Packet-Mirroring Environment

Process	Description
A	The authorized individual requests packet mirroring of the user's traffic and configures the analyzer device to receive mirrored traffic.
B	The ISP administration configures VSAs in the user's RADIUS record.
C	The E Series router administrator configures RADIUS server information and the analyzer interface connection to the analyzer device.

Table 13 on page 43 indicates the sequence of steps for a packet mirroring operation that takes place when a user starts a new session.

Table 13: RADIUS-Based Mirroring During Session Start (User-Initiated)

Step	Description
1	A user logs in to an E Series router, requesting authentication by the RADIUS server. Attributes in the logon request are examined to determine whether any match a configured trigger. The first match starts the packet mirroring session for the user.

Table 13: RADIUS-Based Mirroring During Session Start (User-Initiated) *(continued)*

Step	Description
2	• The RADIUS server authenticates the user and sends packet mirroring VSAs and any other configured VSAs to the router. • The router creates a secure policy based on the VSAs and starts mirroring the user's traffic.
3	The router sends the user's original traffic to its intended destination.
4	The router sends the mirrored traffic to analyzer device.
5	The analyzer device provides information for the requesting individual.

Table 14 on page 44 indicates the sequence of steps for a packet mirroring operation that is configured for a currently running session.

Table 14: RADIUS-Based Mirroring of Currently Running Session (RADIUS-Initiated)

Step	Description
1	A user logs in to the E Series router; no mirroring action is configured.
2	• Packet mirroring is enabled on the RADIUS server. • Authenticated users are examined to determine whether any match a configured trigger. The first match determines the router to which to send change-of-authorization messages. • The RADIUS server sends change-of-authorization messages containing packet mirroring VSAs to the router. • The router creates a secure policy based on the VSAs and starts mirroring the user's traffic.
3	The router sends the user's original traffic to its intended destination.
4	The router sends mirrored traffic to the analyzer device.
5	The analyzer device provides information for the requesting individual.

Related Documentation

- Configuring RADIUS-Based Packet Mirroring on page 41
- RADIUS-Based Mirroring Overview on page 23

RADIUS Attributes Used for Packet Mirroring

Table 15 on page 45 and Table 16 on page 45 list the packet mirroring triggers. The triggers are RADIUS attributes that identify a user whose traffic is to be mirrored. A packet mirroring session starts when the router receives a RADIUS packet that contains mirroring attributes and then applies the mirroring configuration to the appropriate interface. For example,

packet mirroring starts when a logon request occurs that contains a specified User-Name attribute.

The triggers also enable RADIUS-initiated mirroring to start when the user is already logged in.

Table 15: RADIUS Attributes Used as Packet Mirroring Triggers (Vendor ID 4874)

Standard Number	Attribute Name	Order of Preference
[1]	User-Name	4
[8]	Framed-IP-Address	3
[26-1]	Virtual-Router	Used with Framed-IP-Address and User-Name
[31]	Calling-Station-ID	2
[44]	Acct-Session-ID	1
[87]	Nas-Port-ID	5
[26–159]	DHCP- Option-82	6

Table 16: RADIUS Attributes Used as Packet Mirroring Triggers (Vendor ID 3561)

Standard Number	Attribute Name	Order of Preference
[26-1]	Agent-Circuit-ID	7
[26-2]	Agent-Remote-ID	8

You add the trigger to the RADIUS record of the user whose traffic will be mirrored. In addition, you must include the RADIUS VSAs listed in Table 17 on page 46 in the mirrored user's RADIUS record.

NOTE: For IP mirroring, you must include both VSA 26-59 and VSA 26-61, or you must omit both of these VSAs. If you use only one of these VSAs, the configuration fails.

Table 17: RADIUS-Based Mirroring Attributes

Standard Number	Attribute Name	Setting
[26-58]	LI-Action	0 = disable mirroring 1 = enable mirroring 2 = no action
[26-59]	Med-Dev-Handle	String (not null-terminated)
[26-60]	Med-IP-Address	IP address of analyzer device
[26-61]	Med-Port-Number	UDP port number of monitoring application in analyzer device

An LI-Action setting of 2 specifies that the router does not perform any packet mirroring–related configuration. This setting can provide additional security by confusing unauthorized users who attempt to access packet mirroring communication between the router and the RADIUS server.

Related Documentation

- RADIUS-Based Mirroring Overview on page 23
- RADIUS-Based Mirroring Sequence of Events on page 43

RADIUS-Based Packet Mirroring Dynamically Created Secure Policies

RADIUS-based packet mirroring uses dynamically created secure policies, which are based on the RADIUS VSAs that an authorized RADIUS administrator creates. A policy is created when the packet mirroring action is initiated at the RADIUS server, and then applied to the interface that is dynamically created for the user. When the mirroring operation is disabled, the secure policy is deleted.

The E Series router creates a name for the dynamically created policies—the name consists of the string spl followed by a hexadecimal integer, such as spl_88000008. The name is displayed by the **show secure policy-list** command.

Related Documentation

- RADIUS-Based Mirroring Overview on page 23
- RADIUS-Based Mirroring Sequence of Events on page 43
- *show secure policy-list*

RADIUS-Based Packet Mirroring MLPPP Sessions

When you use RADIUS-based packet mirroring on MLPPP traffic, RADIUS authentication and authorization is performed on the individual links. The mirroring-related VSAs are returned with the RADIUS response. For user-initiated mirroring, which starts when the user logs in, a RADIUS response is returned for each successful authentication/authorization. For RADIUS-initiated mirroring of a user who is already logged in, a single RADIUS request is sent for each link.

- If you are mirroring an L2TP session, the packet-mirroring operation is enabled or disabled on a single link that is uniquely identified by the trigger you use (the RADIUS attributes for Acct-Session-ID or User-Name). For tunneled MLPPP, the individual links in the MLPPP bundle are mirrored separately. The packet-mirroring configuration fails if you use the Acct-Multi-Session-ID attribute (RADIUS attribute 50) for the configuration.
- If you are mirroring an IP session, the packet-mirroring operation is enabled or disabled on the MLPPP bundle as a whole. We recommend that you use the Account-Session-ID RADIUS attribute rather than the User-Name attribute as the trigger. Using the Account-Session-ID attribute is more efficient because the JunosE Software creates one secure policy that packet mirroring uses for all links in the MLPPP bundle. If you use the User-Name attribute, a secure policy is created for the first link, then removed and re-created for every other link.

Related Documentation

- Configuring RADIUS-Based Packet Mirroring on page 41
- RADIUS-Based Mirroring Overview on page 23
- RADIUS-Based Mirroring Sequence of Events on page 43

Configuring Router to Start Mirroring When User Logs On

To configure the router to support user-initiated mirroring, which starts when the user logs in:

1. Configure RADIUS server authentication information in the router. See *JunosE Broadband Access Configuration Guide* for information.
2. Configure the analyzer interface to send the mirrored traffic to the analyzer device.

   ```
   host1(config)#interface fastEthernet 4/0
   host1(config-if)#ip analyzer
   ```

   Alternatively, for increased security, create the analyzer interface at one end of an IPSec tunnel to the analyzer device.

   ```
   host1(config)# interface tunnel ipsec:mirror3 transport-virtual-router default
   host1(config-if)#ip analyzer
   host1(config-if)#exit
   host1(config)#ip route 192.168.99.2 255.255.255.255 tunnel ipsec:mirror3
   ```

Related Documentation

- Configuring RADIUS-Based Packet Mirroring on page 41
- Configuring Router to Mirror Users Already Logged In on page 48
- RADIUS-Based Mirroring Sequence of Events on page 43
- *interface fastEthernet*
- *interface tunnel*
- *ip analyzer*

Configuring Router to Mirror Users Already Logged In

When a mirroring operation is initiated for a user who is already logged in (RADIUS-initiated mirroring), the RADIUS server uses change-of-authorization messages and passes the required RADIUS attributes and the identifier of the currently running session to the E Series router. The router uses this information to create the secure policy and attaches it to the interface that is created for the user. The E Series router must be configured to accept change-of-authorization messages from the RADIUS server.

1. Specify the RADIUS dynamic-request server that sends change-of-authorization messages to the router, and enter RADIUS configuration mode.

   host1(config)#radius dynamic-request server 192.168.11.0

2. Specify the UDP port used to communicate with the RADIUS server.

   host1(config-radius)#udp-port 3799

3. Create the key used to communicate with the RADIUS server.

   host1(config-radius)#key mysecret

4. Configure the router to receive change-of-authorization messages from the RADIUS server.

   host1(config-radius)#authorization change
   host1(config-radius)#exit
   host1(config)#exit

5. Verify your RADIUS-initiated mirroring configuration.

   host1#show radius dynamic-request servers

```
                RADIUS Request Configuration
                ----------------------------
                                          Change
                 Udp                        Of
 IP Address      Port   Disconnect   Authorization   Secret
-------------    ----   ----------   -------------   ------
 10.10.3.4       3799   enabled      enabled         mysecret
```

6. Configure the analyzer interface to send the mirrored traffic to the analyzer device.

   host1(config)#interface fastEthernet 4/0
   host1(config-if)#ip analyzer

   Alternatively, for increased security, create the analyzer interface at one end of an IPSec tunnel to the analyzer device.

   host1(config)# interface tunnel ipsec:mirror3 transport-virtual-router default
   host1(config-if)#ip analyzer
   host1(config-if)#exit
   host1(config)#ip route 192.168.99.2 255.255.255.255 tunnel ipsec:mirror3

Related Documentation

- Configuring RADIUS-Based Packet Mirroring on page 41
- Configuring Router to Start Mirroring When User Logs On on page 47
- *interface fastEthernet*

- *interface tunnel*
- *ip analyzer*
- *radius dynamic-request server*
- *udp-port*

CHAPTER 6

Examples

Example: Configuring CLI-Based Interface-Specific Packet Mirroring

This example shows the configuration of a CLI-based packet mirroring session for a particular static IP interface. The configuration results in all traffic through the interface being replicated and the replicated traffic then sent through an IPSec tunnel to the analyzer device.

1. Enable the visibility and use of the packet mirroring CLI commands.

   host1#mirror-enable

2. Configure the analyzer interface and a route to reach the analyzer device at 192.168.125.29.

   NOTE: If the analyzer interface is Ethernet-based, you must configure a static ARP entry for the analyzer device.

   host1(config)#virtual-router vr1
   host1:vr1(config)#interface tunnel ipsec:Diag transport-virtual-router default
   host1:vr1(config-if)#ip analyzer
   host1:vr1(config-if)#exit
   host1:vr1(config)#ip route 192.168.125.29 255.255.255.255 tunnel ipsec:Diag

3. Configure the secure IP policy that forwards the mirrored traffic to the analyzer device at 192.168.125.29.

   In this example, the configured mirror rule does not include the **analyzer-udp-port** keyword. Therefore, the rule sets the mirror header to **disable**, which means that the mirror header is not prepended to the mirrored packets. See "Understanding the Prepended Header During a Packet Mirroring Session" on page 8 for information about the prepended mirror header. The **classifier-group** command uses a previously configured classifier list, secClassA.

   host1:vr1(config)#secure ip policy-list secureIpPolicy1
   host1:vr1(config-policy-list)#classifier-group secClassA

```
host1:vr1(config-policy-list-classifier-group)#mirror analyzer-ip-address 192.168.125.29
  analyzer-virtual-router vr1
```

4. Attach the secure policy to the interfaces whose traffic you want to mirror. This example mirrors input traffic at interface ATM 5/0.1 and output traffic at interface ATM 5/0.2.

```
host1:vr1(config)#interface atm 5/0.1
host1:vr1(config-if)#ip policy secure-input secureIpPolicy1

host1:vr1(config)#interface atm 5/0.2
host1:vr1(config-if)#ip policy secure-output secureIpPolicy1
```

5. Verify the secure policy configuration.

```
host1# show secure policy-list name secureIpPolicy1
                                    Policy Table
                                    ------ -----
Secure IP Policy secureIpPolicy1
 Administrative state: enable
 Reference count:      2
 Classifier control list: secClassA
  mirror analyzer-ip-address 192.168.125.29 analyzer-virtual-router vr1
 Referenced by interface(s):
  ATM5/0.1  secure-input policy, virtual-router vr1
  ATM5/0.2  secure-output policy, virtual-router vr1
```

Related Documentation

- Configuring CLI-Based Packet Mirroring on page 27
- Configuring Triggers for CLI-Based Mirroring on page 34
- Example: Configuring CLI-Based User-Specific Packet Mirroring on page 52

Example: Configuring CLI-Based User-Specific Packet Mirroring

This example shows the configuration of a CLI-based packet mirroring session for subscribers. . The mirroring session replicates all traffic associated with each user, and then sends the replicated traffic to the analyzer device.

1. Enable the visibility and use of the packet mirroring CLI commands.

```
host1#mirror-enable
```

2. Create the analyzer interface and the route to the analyzer device.

   - For L2TP subscribers:

```
host1(config)# interface tunnel ipsec:mirror3 transport-virtual-router default
host1(config-if)#ip analyzer
host1(config-if)#exit
host1(config)#ip route 192.168.99.2 255.255.255.255 tunnel ipsec:mirror3
```

   - For DHCP and PPP subscribers:

```
host1(config)# interface atm 4/0.1
host1(config-if)#ip address 19.0.0.2 255.255.255.0
host1(config-if)#ip analyzer
host1(config-if)#exit
```

```
host1(config)#ip route 19.0.0.2 255.255.255.255 101.101.101.2
```

3. Configure the secure policy that forwards the mirrored traffic to the analyzer device. The **classifier-group** command uses the default classifier list, which is indicated by the asterisk character (*).

   - For L2TP subscribers:

     ```
     host1(config)#secure l2tp policy-list l2tp_toMirrorHQ
     host1(config-policy-list)#classifier-group *
     host1(config-policy-list-classifier-group)#mirror analyzer-ip-address 192.168.99.2
       analyzer-virtual-router default analyzer-udp-port 6500 mirror-identifier 1
       session-identifier 1
     ```

   - For DHCP and PPP subscribers:

     ```
     host1(config)#secure ip policy-list secure-ipv4-policy
     host1(config-policy-list)#classifier-group *
     host1(config-policy-list-classifier-group)#mirror analyzer-ip-address 19.0.0.2
       analyzer-virtual-router default analyzer-udp-port 2500 mirror-identifier 1
       session-identifier 1
     ```

4. Configure packet mirroring for the subscriber and associate the secure policy with the user.

   - For L2TP subscribers:

     ```
     host1(config)#virtual-router lac
     host1:lac(config)#mirror username jwbooth@isptheatre.com l2tp secure-policy-list
       l2tp_toMirrorHQ
     ```

   - For DHCP and PPP subscribers:

     ```
     host1(config)#mirror dhcp-option-82 agent-circuit-id "x:12000004:circuit id:45"
       agent-remote-id "y:12000004:remote id:89" ip secure-policy-list
       secure-ipv4-policy
     host1(config)#mirror agent-circuit-id "x:12000001:pppoe agent circuit id:47" ip
       secure-policy-list secure-ipv4-policy
     host1(config)#mirror agent-remote-id hex
       79:3a:02:00:00:02:3a:72:65:6d:6f:74:65:20:69:64:3a:35 ip secure-policy-list
       secure-ipv4-policy
     ```

   Now, when the subscriber logs in , the packet mirroring session starts and the subscriber's replicated traffic is sent to the remote analyzer device.

5. Verify the packet-mirroring configuration.

```
host1# show mirror subscribers
Subscriber ID                                          ID         Secure
  Secure         Mirrored
                                                     Method       Policy Type
  Policy List    Sessions
------------------                                 ----------   -----------
----------------  --------
lac:jwbooth@isptheatre.com                           username         l2tp
 l2tp_toMirrorHQ    1
x:12000004:circuit id:45.y:12000004:remote id:89     dhcp-option-82   IP
 secure-ipv4-policy 1
x:12000001:pppoe agent circuit id:47                 agent-circuit-id IP
 secure-ipv4-policy 1
```

```
79:3a:02:00:00:02:3a:72:65:6d:6f:74:65:20:69:64:3a:35 agent-remote-id  IP
 secure-ipv4-policy 1
```

6. Verify the configuration of the secure policy.

```
host1# show secure policy-list
                                    Policy Table
                                    ------ -----
Secure L2TP Policy l2tp_toMirrorHQ
 Administrative state: enable
 Reference count:      2
 Classifier control list: *
  mirror analyzer-ip-address 192.168.99.2 analyzer-virtual-router default
analyzer-udp-port 6500 mirror-id 1 session-id 1
 Referenced by interface(s):
  TUNNEL l2tp:5/1/5  secure-input policy
  TUNNEL l2tp:5/1/5  secure-output policy

Secure IP Policy secure-ipv4-policy
  Administrative state: enable
  Reference count:      6
  Classifier control list: *
mirror analyzer-ip-address 19.0.0.2 analyzer-virtual-router default
analyzer-udp-port 2500 mirror-identifier 1 session-identifier 1
Referenced by interface(s):
 ip100.1.1.3  secure-input policy, statistics disabled, virtual-router default

 ip100.1.1.3  secure-output policy, statistics disabled, virtual-router default
```

Related Documentation

- Configuring CLI-Based Packet Mirroring on page 27
- Configuring Triggers for CLI-Based Mirroring on page 34
- Example: Configuring CLI-Based Interface-Specific Packet Mirroring on page 51

PART 3

Administration

CHAPTER 7

Monitoring Tasks

Monitoring Packet Mirroring Overview

This topic describes the commands you can use to view your CLI-based and RADIUS-based packet mirroring environments.

Use the **baseline radius dynamic-request** command in RADIUS-based packet mirroring to set a statistics baseline for packet mirroring–related RADIUS statistics. The E Series router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline when you retrieve baseline-relative statistics. Use the **delta** keyword with the **show radius statistics** command to show baselined statistics.

Related Documentation

- Packet Mirroring Overview on page 3
- *baseline radius dynamic-request*
- *clear mirror log*

CHAPTER 8

Monitoring Tasks for CLI-Based Packet Mirroring

Monitoring CLI-Based Packet Mirroring

Purpose Display brief or default (normal) information about your CLI-based packet mirroring environment, including interface analyzer information. To display secure packet mirroring information you must enable the **mirror-enable** command before using this command. This command displays a maximum of two secure policy attachments and statistics, if configured.

Action To display the default (normal) format for a specific interface, which is used as the default analyzer interface:

```
host1#show ip interface atm 5/0.1
ATM5/0.1 line protocol Atm1483 is up, ip is analyzer (default)
  Network Protocols: IP
  Internet address is 10.10.3.4/255.255.255.0
  Broadcast address is 255.255.255.255
  Operational MTU = 0  Administrative MTU = 0
  Operational speed = 100000000  Administrative speed = 0
  Discontinuity Time = 0
  Router advertisement = disabled
  Proxy Arp = disabled
  Administrative debounce-time = disabled
  Operational debounce-time    = disabled
```

```
  Access routing = disabled
  Multipath mode = hashed

  In Received Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Packets 0, Bytes 0
  In Policed Packets 0, Bytes 0
  In Error Packets 0
  In Invalid Source Address Packets 0
  In Discarded Packets 0
  Out Forwarded Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Routed Packets 0, Bytes 0
  Out Scheduler Dropped Packets 0, Bytes 0
  Out Policed Packets 0, Bytes 0
  Out Discarded Packets 0
```

To display the format for a specific interface, showing secure policy attachments:

```
host1#show ip interface atm 4/1.1
ATM5/0.1 line protocol Atm1483 is up
  Network Protocols: IP
  Internet address is 10.10.7.14/255.255.255.0
  Broadcast address is 255.255.255.255
  Operational MTU = 0  Administrative MTU = 0
  Operational speed = 100000000  Administrative speed = 0
  Discontinuity Time = 0
  Router advertisement = disabled
  Proxy Arp = disabled
  Administrative debounce-time = disabled
  Operational debounce-time    = disabled
  Access routing = disabled
  Multipath mode = hashed

  In Received Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Packets 0, Bytes 0
  In Policed Packets 0, Bytes 0
  In Error Packets 0
  In Invalid Source Address Packets 0
  In Discarded Packets 0
  Out Forwarded Packets 0, Bytes 0
    Unicast Packets 0, Bytes 0
    Multicast Routed Packets 0, Bytes 0
  Out Scheduler Dropped Packets 0, Bytes 0
  Out Policed Packets 0, Bytes 0
  Out Discarded Packets 0

  IP policy secure-input ipSecureIn
    classifier-group secClassA entry 1
      0 packets, 0 bytes
      mirror analyzer-ip-address 10.10.3.14, analyzer-virtual-router default
    classifier-group secClassB entry 2
      0 packets, 0 bytes
      mirror analyzer-ip-address 10.10.3.14, analyzer-virtual-router vr200
  IP policy secure-output ipSecureOut
    classifier-group secClassC entry 1
      0 packets, 0 bytes
      mirror analyzer-ip-address 10.10.7.104, analyzer-virtual-router vr300
```

Meaning Table 18 on page 61 lists the secure packet mirroring-related fields.

Table 18: show ip interface Output Fields

Field Name	Field Description
IP Policy	Type (secure-input, secure-output) and name of the secure policy
classifier-group	Name of a CLACL attached to the interface and number of entry
packets	Number of packets classified by the CLACL
bytes	Number of bytes classified by the CLACL
mirror analyzer-ip-address	IP address of analyzer device
analyzer-virtual-router	Name of analyzer interface virtual router

Related Documentation

- Configuring CLI-Based Packet Mirroring on page 27
- *show ip interface*

Monitoring the Packet Mirroring Configuration of IP Interfaces

Purpose Display CLI-based packet mirroring configuration information for a specific interface or for all interfaces on which mirroring is enabled.

NOTE: This command is deprecated and might be removed completely in a future release. The function provided by this command has been replaced by the **show secure policy-list** command.

Action To display information about a specific interface or for all interfaces:

```
host1#show ip mirror interface atm 5/0.1

    Interface          Analyzer Port      Analyzer next-hop
------------------- ------------------- --------------------
ATM5/0.1            FastEthernet3/0       192.168.1.1
```

Meaning Table 19 on page 61 lists the **show ip mirror interface** command output fields.

Table 19: show ip mirror interface Output Fields

Field Name	Field Description
Interface	Interface being mirrored
Analyzer Port	Interface to which the mirrored traffic is sent, and that then sends the traffic to the analyzer device

Table 19: show ip mirror interface Output Fields *(continued)*

Field Name	Field Description
Analyzer next-hop	IP address of the next hop to the analyzer device; displayed when the analyzer interface is a shared medium

Related Documentation

- Configuring CLI-Based Packet Mirroring on page 27
- *show ip mirror interface*

Monitoring Failure Messages for Secure Policies

Purpose Display failure messages and information for secure policies. This command and the output are visible only to authorized users—the **mirror-enable** command must be enabled before using this command. All normal E Series system log messages are suppressed for packet mirroring-related policy operations.

Action To display information for secure policies:

```
host1#show mirror log

 Time             Mirror-ID   Session-ID   User       Error Status
-----------     ------------ ---------- ------------ --------------
TUE SEP 15         8976        1923    123@abc.com  no secure policies available

2009 18:35:43 UTC
```

Meaning Table 20 on page 62 lists the **show mirror log** command output fields.

Table 20: show mirror log Output Fields

Field Name	Field Description
Time	Day, date, and time of failure
Mirror-ID	Unique identifier of the mirrored session
Session-ID	Unique identifier of the user session
User	User login name
Error Status	Description of error condition

Related Documentation

- Configuring CLI-Based Packet Mirroring on page 27
- *show mirror log*

Monitoring Packet Mirroring Triggers

Purpose Display CLI-based packet mirroring information about all packet mirroring triggers (active and inactive) that are configured on the router. This command and the output are visible only to authorized users—the **mirror-enable** command must be enabled before using this command.

Action To display information about all packet mirroring triggers:

```
host1# show mirror rules
 Mirror Trigger Rules : 11 Total
Subscriber ID                                          ID            Secure      Secure      Sessions
                                                      Method         Policy Type Policy List Mirrored
------------------                                ------------------  ----------- ----------  --------
default:1.2.3.4                                     IP address       IP          spl_88000001  0
52:11:02:0F:12:4F:87:3A:72:65:6D:6F:74:65:00:69:64 dhcp-option-82    IP          spl_88000002  1
01:0D:61:74:6D:20:34:2F:32:3A:30:2E:31:30:35       agent-circuit-id IPV6        spl_88000003  1
02:0F:67:68:69:31:40:64:6F:6D:61:69:6E:2E:63:6F:6D agent-remote-id  IPV6        spl_88000004  1
52:10:01:0E:12:4F:87:3A:61:67:65:6E:74:00:69:64    dhcp-option-82   IP        op82hex_policy  1
01:0D:61:74:6D:20:34:2F:32:3A:30:2E:31:30:31       agent-circuit-id IPV6      cidhex_policy   1
02:0E:61:62:63:40:64:6F:6D:61:69:6E:2E:63:6F:6D    agent-remote-id  IPV6      ridhex_policy   1
01:0E:63:69:64:40:64:6F:6D:61:69:6E:2E:63:6F:6D    agent-remote-id  L2TP      l2tphex_pol     1
atm 4/1:0.101.abc@domain.com                       dhcp-option-82   IP        op82string_plcy 0
atm 4/2:0.101                                      agent-circuit-id IP        cidstring_plcy  0
user@juniper.com                                   agent-remote-id  IP        ridstring_plcy  0
```

Meaning Table 21 on page 63 lists **show mirror rules** command output fields.

Table 21: show mirror rules Output Fields

Field Name	Field Description
Subscriber ID	Identification of the subscriber
ID Method	Method used to identify the subscriber
Secure Policy Type	Type of secure policy; IP, IPv6, or L2TP
Secure Policy List	Name of secure policy list used for packet mirroring
Sessions Mirrored	Number of sessions currently being mirrored

Related Documentation

- Configuring Triggers for CLI-Based Mirroring on page 34
- Using Multiple Triggers for CLI-Based Packet Mirroring on page 35
- *show mirror rules*

Monitoring Packet Mirroring Subscriber Information

Purpose Display CLI-based packet mirroring information about the subscribers for whom packet mirroring is currently active. This command and the output are visible only to authorized users—the **mirror-enable** command must be enabled before using this command.

Action To display information about subscribers for whom packet mirroring is active:

```
host1# show mirror subscribers
                          Mirror Subscribers:  7 Total

Subscriber ID                                        ID            Secure   Secure        Mirrored
                                                    Method        PolicyType Policy Name    Sessions
------------------                                 ---------------  --------- -------------- --------
52:10:01:0E:12:4F:87:3A:61:67:65:6E:74:00:69:64    dhcp-option-82    IP       op82hex_pol     1
01:0D:61:74:6D:20:34:2F:32:3A:30:2E:31:30:31       agent-circuit-id IPV6      cidhex_poli     1
02:0E:61:62:63:40:64:6F:6D:61:69:6E:2E:63:6F:6D    agent-remote-id  IPV6      ridhex_poli     1
52:11:02:0F:12:4F:87:3A:72:65:6D:6F:74:65:00:69:64 dhcp-option-82   IP        spl_88000002    1
01:0D:61:74:6D:20:34:2F:32:3A:30:2E:31:30:35       agent-circuit-id IPV6      spl_88000003    1
02:0E:61:62:63:40:64:6F:6D:61:69:6E:2E:63:6F:6E    agent-remote-id  IPV6      spl_88000004    1
01:0E:63:69:64:40:64:6F:6D:61:69:6E:2E:63:6F:6D    agent-remote-id  L2TP      l2tphex_pol     1
```

Meaning Table 22 on page 64 lists **show mirror subscribers** command output fields.

Table 22: show mirror subscribers Output Fields

Field Name	Field Description
Subscriber ID	Subscriber being mirrored
Subscriber ID Method	Method used to identify the subscriber
Secure Policy Type	Type of secure policy; IP, IPv6, or L2TP
Secure Policy List	Name of secure policy list used for packet mirroring
Sessions Mirrored	Number of sessions being mirrored

Related Documentation

- Configuring CLI-Based Packet Mirroring on page 27
- Example: Configuring CLI-Based User-Specific Packet Mirroring on page 52
- *show mirror subscribers*

Monitoring Secure CLACL Configurations

Purpose Display information about only secure CLACL configurations. This command and the output are visible only to authorized users—the **mirror-enable** command must be enabled before using this command. Use the **brief** or **detail** keywords with the **show secure classifier-list** command to display different levels of information.

Action To display a list of secure CLACLs

```
host1#show secure classifier-list

                        Classifier Control List Table
                        ---------- ------- ---- -----
Secure IP secClassA.1 ip any any
Secure IP secClassB.1 ip any not 10.10.10.1 255.255.255.255
Secure IP secClass25.1 user-packet-class 8 source-route-class 100 ip
192.168.44.103 255.255.255.255 any
```

Displays details of each secure CLACL

```
host1#show secure classifier-list secClass25 detailed

                        Classifier Control List Table
                        ---------- ------- ---- -----
Secure IP Classifier Control List secClass25
   Reference count:      0
   Entry count:          1

   Classifier-List secClass25 Entry 1
      User Packet Class:          8
      Source Route Class:         100
      Protocol:                   ip
      Not Protocol:               false
      Source IP Address:          192.168.44.103
      Source IP WildcardMask:     255.255.255.255
      Not Source Ip Address:      false
      Destination IP Address:     0.0.0.0
      Destination IP WildcardMask:255.255.255.255
      Not Destination Ip Address: false
```

Meaning Table 23 on page 65 lists **show secure classifier-list** command output fields.

Table 23: show secure classifier-list Output Fields

Field Name	Field Description
Reference count	Number of times the CLACL is referenced by policies
Entry count	Number of entries in the classifier list
Classifier-List	Name of the classifier list
Entry	Entry number of the classifier list rule
Color	Packet color to match: green, yellow, or red
Protocol	Protocol type
Not Protocol	If true, matches any protocol except the preceding protocol; if false, matches the preceding protocol
Source IP Address	Address of the network or host from which the packet is sent
Source IP WildcardMask	Mask that indicates addresses to be matched when specific bits are set

Table 23: show secure classifier-list Output Fields *(continued)*

Field Name	Field Description
Not Source Ip Address	If true, matches any source IP address and mask except the preceding source IP address and mask; if false, matches the preceding source IP address and mask
Destination IP Address	Number of the network or host from which the packet is sent
Destination IP WildcardMask	Mask that indicates addresses to be matched when specific bits are set
Not Destination Ip Address	If true, matches any destination IP address and mask except the preceding destination IP address and mask; if false, matches the preceding destination IP address and mask
Traffic Class	Name of the traffic class to match
User Packet Class	User packet value to match
DS Field	DS field value to match
TOS Byte	ToS value to match
Precedence	Precedence value to match
User Priority bits	User priority bits value to match
Traffic Class Field	Traffic class field value to match
EXP Bits	MPLS EXP bit value to match
EXP Mask	Mask applied to EXP bits before matching
DE Bit	Frame Relay DE bit value to match5.2.0b1 ID-1381
Destination Route Class	Route class used to classify packets based on the packet's destination address
Source Route Class	Route class used to classify packets based on the packet's source address
Local	If true, matches packets destined to a local interface; if false, matches packets that are traversing the router

Related Documentation

- Configuring CLI-Based Packet Mirroring on page 27
- *show secure classifier-list*

Monitoring Secure Policy Lists

Purpose Display information about only secure policy lists. This command and the output are visible only to authorized users—the **mirror-enable** command must be enabled before using this command. Use the **name** keyword to display information for a specific secure policy list.

Action To display information about secure policy lists:

```
host1#show secure policy-list

                                Policy Table
                                ------ -----
Secure IP Policy secureIpPolicy
   Administrative state: enable
   Reference count:      2
   Classifier control list: secClassA
      mirror analyzer-ip-address 192.168.1.1 analyzer-virtual-router default
analyzer-udp-port 3000 mirror-id 6789 session-id 6543

   Referenced by interface(s):
      ATM5/0.1  secure-input policy, statistics disabled, virtual-router default

     ATM5/0.1  secure-output policy, statistics disabled, virtual-router default


Secure IPv6 Policy secure-ipv6-pol3
   Administrative state: enable
   Reference count:      2
   Classifier control list: *
      Mirror analyzer-ip-address 190.168.1.1 analyzer-virtual-router default
analyzer-udp-port 3000 mirror-id 6789 session-id 6543

   Referenced by interface(s):
      GigabitEthernet1/0/2.1.2  secure-input policy, statistics disabled,
virtual-router default
      GigabitEthernet1/0/2.1.2  secure-output policy, statistics disabled,
virtual-router default

   Referenced by merged policies:
      None

L2TP Secure Policy secureL2tpPolicy
   Administrative state: enable
   Reference count:      2
   Classifier control list: *
      mirror analyzer-ip-address 192.168.2.1 analyzer-virtual-router default
analyzer-udp-port 3000 mirror-id 6789 session-id 6543 (unreachable)

   Referenced by interface(s):
      TUNNEL l2tp:1/msn.pwh.com/1  secure-input policy, statistics disabled
      TUNNEL l2tp:1/msn.pwh.com/1  secure-output policy, statistics disabled
```

Meaning Table 24 on page 68 lists **show secure policy-list** command output fields.

Table 24: show secure policy-list Output Fields

Field Name	Field Description
Policy	Type (IP, IPv6, or L2TP) and name of the policy list
Administrative state	Status of administrative state, enable or disable; set to enable when the policy list is created
Reference count	Number of attachments to interfaces or profiles
Classifier control list	Name of the classifier control list
Mirror analyzer-ip-address	IP address of analyzer device
Analyzer-virtual-router	Analyzer interface virtual router
Analyzer-udp-port	UDP port used to communicate with analyzer device
Mirror-id	Unique identifier of the mirrored session
Session-id	Unique identifier of the user session
Referenced by interface(s)	List of interfaces to which the policy is attached; indicates whether the attachment is at secure input or secure output of interface
Referenced by profile(s)	Not currently supported: always null
Statistics	Not currently supported: always disabled

Related Documentation

- Configuring CLI-Based Packet Mirroring on page 27
- *show secure policy-list*

Monitoring Information for Secure Policies

Purpose Display failure messages and information for secure policies. This command and the output are visible only to authorized users—the **mirror-enable** command must be enabled before using this command. All normal E Series system log messages are suppressed for packet mirroring-related policy operations.

Action To display information for secure policies:

```
host1# show mirror log
  Time            Mirror-ID      Session-ID   User           Error Status
-----------     -------------- ---------- --------------  --------------
TUE SEP 15         8976           1923       123@abc.com  no secure policies available
2009 18:35:43 UTC
```

Meaning Table 25 on page 69 lists the **show mirror log** command output fields.

Table 25: show mirror log Output Fields

Field Name	Field Description
Time	Day, date, and time of failure
Mirror-ID	Unique identifier of the mirrored session
Session-ID	Unique identifier of the user session
User	User login name
Error Status	Description of the error condition

Related Documentation

- Configuring CLI-Based Packet Mirroring on page 27
- *clear mirror log*
- *show mirror log*

Monitoring SNMP Secure Packet Mirroring Traps

Purpose Display configuration information about SNMP traps and trap destinations. The PacketMirror trap category is displayed only when the **mirror enable** command has been configured. The Secure Trap Logging status is displayed only when the **mirror enable** command has been issued and secure audit logs have been configured. Text in bold indicates secure packet mirroring trap configuration information.

Action To display secure packet mirroring traps:

```
host1# show snmp trap
Enabled Categories: CliSecurity,  PacketMirror , Sonet
SNMP authentication failure trap is disabled
Trap Source: FastEthernet 6/0, Trap Source Address:192.168.120.78
Trap Proxy: enabled
Secure Trap Logging is enabled
Global Trap Severity Level: 6 - informational
Address          Security String                  Ver  Port   Trap Categories
---------------  -------------------------------  ---  -----  ----------------
10.1.1.1         host1                            v1     162  Cli
10.12.12.12      secureHost                       v3     162  CliOspf PacketMirror Sonet
192.168.57.162   host2                            v3     162  Sonet
Address         TrapSeverityFilter  Ping    Maximum    Queue    Queue Full
                                    TimeOut QueueSize DrainRate discrd methd
--------------- ------------------ ------- --------- --------- -------------
10.1.1.1        5 - notice         1       32          0         dropLastIn
10.12.12.12     2 - critical       1       32          0         dropLastIn
192.168.57.162  2 - critical       1       32          0         dropLastIn
```

Meaning Table 26 on page 70 lists the **show snmp trap** command output fields.

Table 26: show snmp trap Output Fields

Field Name	Field Description
Enabled Categories	Trap categories that are enabled on the router
SNMP authentication failure trap	Enabled or disabled
Trap Source	Interface whose IP address is used as the source address for all SNMP traps
Trap Source Address	IP address used as the source address for all SNMP traps
Trap Proxy	Enabled or disabled
Secure Trap Logging	Enabled or disabled
Global Trap Severity Level	Global severity level filter; if a trap does not meet this severity level, it is discarded
Address	IP address of the trap recipient
Security String	Name of the SNMP community
Ver	SNMP version (v1 or v2) of the SNMP trap packet
Port	UDP port on which the trap recipient accepts traps
Trap Categories	Types of traps that the trap recipient can receive
TrapSeverityFilter	Severity level filter for this SNMP host
Ping TimeOut	Configured ping timeout in minutes
Maximum QueueSize	Maximum number of traps to be kept in the trap queue
Queue DrainRate	Maximum number of traps per second to be sent to the host
Queue Full discrd methd	Method used to discard traps when the queue is full:
dropFirstIn	Oldest trap in the queue is dropped
dropLastIn	Most recent trap is dropped

NOTE: Secure packet-mirroring trap configuration information appears in the Enabled Categories and Trap Categories fields only if the **mirror-enable** command is enabled.

Related Documentation

- Configuring SNMP Secure Packet Mirroring Traps on page 38
- *mirror trap-enable*
- *snmp-server enable traps*
- *snmp-server host*
- *snmp-server secure-log*
- *show mirror trap*
- *show snmp trap*

Monitoring SNMP Secure Audit Logs

Purpose Display output when the secure audit log data is available.

NOTE: The secure audit log data is not preserved across the reboot because secure logs are not stored in the nonvolatile memory. Only the **snmp-server secure-log** command configuration is stored in the nonvolatile memory.

Action To display the contents of the SNMP secure audit log:

```
host1# show snmp secure-log
Agent's Context    LogData
---------------    ------------------------------------------------------------
SnmpRouterAgent1   SNMP Trap, SNMPVer= 3, src=10.27.120.117, dest=10.1.1.1,
reqId=3, errSts=0, errIndx=0, msgID=2, msgMaxSize=1500, msgFlags=0,
msgSecurityModel=3,
contextEngineID=80:00:13:0a:05:00:90:1a:41:45:51:80:00:00:01 ,
securityName=jbond, engineBoots=0, engineTime=0, varCnt=13, Vars:
1.3.6.1.2.1.1.3.0 [1259], 1.3.6.1.6.3.1.1.4.1.0
1],3.6.1.4.1.4874.2.2.77.3.0.3], 1.3.6.1.4.1.4874.2.2.77.3.1.13 [?^K^B
1.3.6.1.4.1.4874.2.2.77.3.1.5 [0], 1.3.6.1.4.1.4874.2.2.77.3.1.4 [0],
1.3.6.1.4.1.4874.2.2.77.3.1.3 [f], 1.3.6.1.4.1.4874.2.2.77.3.1.14 [1],
1.3.6.1.4.1.4874.2.2.77.3.1.1 [1], 1.3.6.1.4.1.4874.2.2.77.3.1.2 [1],
1.3.6.1.4.1.4874.2.2.77.3.1.11 [f], 1.3.6.1.4.1.4874.2.2.77.3.1.12 [1],
1.3.6.1.4.1.4874.2.2.77.3.1.15 [0], 1.3.6.1.4.1.4874.2.2.16.1.3.5.0 [5],
SnmpRouterAgent44   SNMP Trap, SNMPVer= 3, src=10.27.120.117, dest=10.1.1.1,
reqId=5, errSts=0, errIndx=0, msgID=4, msgMaxSize=1500, msgFlags=0,
msgSecurityModel=3,
contextEngineID=80:00:13:0a:05:00:90:1a:41:45:51:80:00:00:01 ,
securityName=jbond, engineBoots=0, engineTime=0, varCnt=14, Vars:
1.3.6.1.2.1.1.3.0 [1259], 1.3.6.1.6.3.1.1.4.1.0
1],3.6.1.4.1.4874.2.2.77.3.0.1], 1.3.6.1.4.1.4874.2.2.77.3.1.13 [?^K^B
1.3.6.1.4.1.4874.2.2.77.3.1.5 [0], 1.3.6.1.4.1.4874.2.2.77.3.1.4 [0],
1.3.6.1.4.1.4874.2.2.77.3.1.3 [f], 1.3.6.1.4.1.4874.2.2.77.3.1.14 [1],
1.3.6.1.4.1.4874.2.2.77.3.1.10 [f], 1.3.6.1.4.1.4874.2.2.77.3.1.1 [1],
1.3.6.1.4.1.4874.2.2.77.3.1.2 [1], 1.3.6.1.4.1.4874.2.2.77.3.1.6 [0],
1.3.6.1.4.1.4874.2.2.77.3.1.8 [0], 1.3.6.1.4.1.4874.2.2.77.3.1.7 [f],
1.3.6.1.4.1.4874.2.2.16.1.3.5.0 [3],
SnmpRouterAgent22   SNMP Trap, SNMPVer= 3, src=10.27.120.117, dest=10.1.1.1,
reqId=8, errSts=0, errIndx=0, msgID=7, msgMaxSize=1500, msgFlags=3,
msgSecurityModel=3,
contextEngineID=80:00:13:0a:05:00:90:1a:41:45:51:80:00:00:01 ,
```

```
securityName=jbond, engineBoots=1, engineTime=8602, varCnt=6, Vars:
1.3.6.1.2.1.1.3.0 [1259], 1.3.6.1.6.3.1.1.4.1.0
1],3.6.1.4.1.4874.2.2.77.3.0.4], 1.3.6.1.4.1.4874.2.2.77.3.1.13 [?^K^B
1.3.6.1.4.1.4874.2.2.77.3.1.9 [192.168.7.120], 1.3.6.1.4.1.4874.2.2.77.3.1.14
[1], 1.3.6.1.4.1.4874.2.2.16.1.3.5.0 [4],
```

Meaning Table 27 on page 72 lists the **show snmp secure-log** command output fields.

Table 27: show snmp secure-log Output Fields

Field Name	Field Description
Agent's Context	Owner of the secure log entry
LogData	Contents of the secure audit log

Related Documentation

- Capturing SNMP Secure Audit Logs on page 39
- *snmp-server clear secure-log*
- *show snmp secure-log*

CHAPTER 9

Monitoring Tasks for RADIUS-Based Packet Mirroring

Monitoring RADIUS Dynamic-Request Server Information

Purpose Display RADIUS dynamic-request server configuration information and statistics.

Action To display RADIUS dynamic-request server configuration information:

```
host1#show radius dynamic-request servers

                RADIUS Request Configuration
                        ----------------------------
                                          Change
                 Udp                        Of
 IP Address      Port   Disconnect   Authorization   Secret
-------------    ----   ----------   -------------   ------
192.168.2.3      1700   disabled     disabled        <NULL>
10.10.120.104    1700   disabled     disabled        mysecret
```

```
host1#show radius dynamic-request statistics

RADIUS Request Statistics
       -------------------------
          Statistic             10.10.3.4
-----------------------------   -------
UDP Port                        1700
Disconnect Requests             0
Disconnect Accepts              0
Disconnect Rejects              0
Disconnect No Session ID        0
Disconnect Bad Authenticators   0
Disconnect Packets Dropped      0
CoA Requests                    0
CoA Accepts                     0
CoA Rejects                     0
CoA No Session ID               0
CoA Bad Authenticators          0
CoA Packets Dropped             0
No Secret                       0
Unknown Request                 0

Invalid Addresses Received  :0
```

Meaning Table 28 on page 74 lists **show radius dynamic-request statistics** command output fields.

Table 28: show radius dynamic-request statistics Output Fields

Field Name	Field Description
IP Address	IP address of the RADIUS server
Udp Port	Port on which the router listens for RADIUS server
Disconnect	Status of RADIUS-initiated disconnect feature, enabled or disabled
Change of Authorization	Status of change of authorization feature, enabled or disabled
Secret	Secret (key) used to connect to RADIUS server
Disconnect or CoA Requests	Number of RADIUS-initiated disconnect or CoA requests received
Disconnect or CoA Accepts	Number of RADIUS-initiated disconnect or CoA requests accepted
Disconnect or CoA Rejects	Number of RADIUS-initiated disconnect or CoA requests rejected
Disconnect or CoA No Session ID	Number of RADIUS-initiated disconnect or CoA messages rejected because the request did not include a session ID attribute
Disconnect or CoA Bad Authenticators	Number of RADIUS-initiated disconnect or CoA messages rejected because the calculated authenticator in the authenticator field of the request did not match
Disconnect or CoA Packets Dropped	Number of RADIUS-initiated disconnect or CoA packets dropped because of queue overflow
No Secret	Number of messages rejected because a secret was not present in the authenticator field
Unknown Request	Number of packets received with an invalid RADIUS code for RADIUS disconnect or change of authorization
Invalid Addresses Received	Number of invalid addresses received

Related Documentation

- Configuring RADIUS-Based Packet Mirroring on page 41
- *show radius servers*
- *show radius statistics*

PART 4

Index

Index

T