RADIUS-Initiated Subscriber Secure Policy Traffic Mirroring

Published: 2012-02-13

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

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

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

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

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

Supported Platforms

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

- MX Series

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

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

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`

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

Convention	Description	Examples
Italic text like this	• Introduces important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; interface names; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub** <**default-metric** *metric*>**;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** (***string1*** **|** ***string2*** **|** ***string3***)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [** *community-ids* **]**

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

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can 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 (if applicable)

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/

- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

CHAPTER 1

Subscriber Secure Policy Traffic Mirroring

Subscriber Secure Policy Overview

Subscriber secure policy enables you to mirror traffic on a per-subscriber basis. You can mirror the content of subscriber traffic as well as monitor events related to the subscriber session that is being mirrored.

Subscriber secure policy mirroring can be based on information provided by either RADIUS or Dynamic Tasking Control Protocol (DTCP), and can mirror both IPv4 and IPv6 traffic. Configuration of subscriber secure policy mirroring is independent of the actual mirroring session—you can configure the mirroring parameters at any time. Also, you can use a single RADIUS or DTCP server to provision mirroring operations on multiple routers in a service provider's network. To provide security, the ability to configure, access, and view the subscriber secure policy components and configuration is restricted to authorized users.

After subscriber secure policy is triggered, both the subscriber ingress and egress traffic are mirrored. The original traffic is sent to its intended destination and the mirrored traffic is sent to a mediation device for analysis. The actual mirroring operation is transparent to subscribers whose traffic is being mirrored. A special UDP/IP header is prepended to each mirrored packet sent to the mediation device. The mediation device uses the header to differentiate multiple mirrored streams that arrive from different sources.

Subscriber Secure Policy for Subscribers on VLANs

Interface-based subscriber secure policy is supported on dynamic, authenticated VLAN interfaces and VLAN Demux interfaces. When you enable subscriber secure policy for these interfaces, traffic for all configured families (inet, inet6) including Layer 2 and Layer 3 control traffic is mirrored. The mirrored packets include Layer 2 encapsulations.

Reporting Mirroring-Related Events

Subscriber secure policy also supports the use of SNMPv3 traps to report events related to the mirroring operation to an external device. Type of information sent in traps include identifying information for subscribers, such as username or IP address, and subscriber session events, such as login or logout events or mirroring session activation or

deactivation. The traps map to messages defined in the *Lawfully Authorized Electronic Surveillance (LAES) for IP Network Access, American National Standard for Telecommunications*.

Related Documentation

- RADIUS-Initiated Subscriber Secure Policy Overview on page 5
- DTCP-Initiated Subscriber Secure Policy Overview
- Intercept-Related Events Transmitted to the Mediation Device on page 55

Subscriber Secure Policy Licensing Requirements

To enable and use subscriber secure policy, you must install and properly configure the Subscriber Secure Policy license.

Related Documentation

- For information about installing and managing Junos licenses, see “Installing and Managing Junos OS Licenses” in the *Junos OS Installation and Upgrade Guide*

CHAPTER 2

RADIUS-Initiated Subscriber Secure Policy Traffic Mirroring

RADIUS-Initiated Subscriber Secure Policy Overview

RADIUS-initiated mirroring creates secure policies based on RADIUS VSAs and uses RADIUS attributes to identify the subscriber whose traffic is to be mirrored. Mirroring is initiated without regard to the subscriber location, router, interface, or type of traffic.

The mirroring operation can be initiated by RADIUS messages as follows:

- Subscriber login—Mirroring starts when the subscriber logs in and the router receives the trigger in a RADIUS Access-Accept message. Using triggers in RADIUS Access-Accept messages enables you to mirror per-subscriber traffic without regard to how often the subscriber logs in or out, or which router or interface the subscriber uses.
- In-session—Mirroring starts when the router receives the trigger in a RADIUS change of authorization request (CoA-Request) message. Using triggers in CoA-Request messages enables you to immediately mirror traffic of a subscriber who is already logged in.

Related Documentation

- Subscriber Secure Policy Traffic Mirroring Architecture Using RADIUS on page 6
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 21

Subscriber Secure Policy Traffic Mirroring Architecture Using RADIUS

Figure 1 on page 6 shows the architecture of the RADIUS-initiated subscriber secure policy mirroring environment.

Figure 1: RADIUS-Initiated Subscriber Secure Policy Architecture

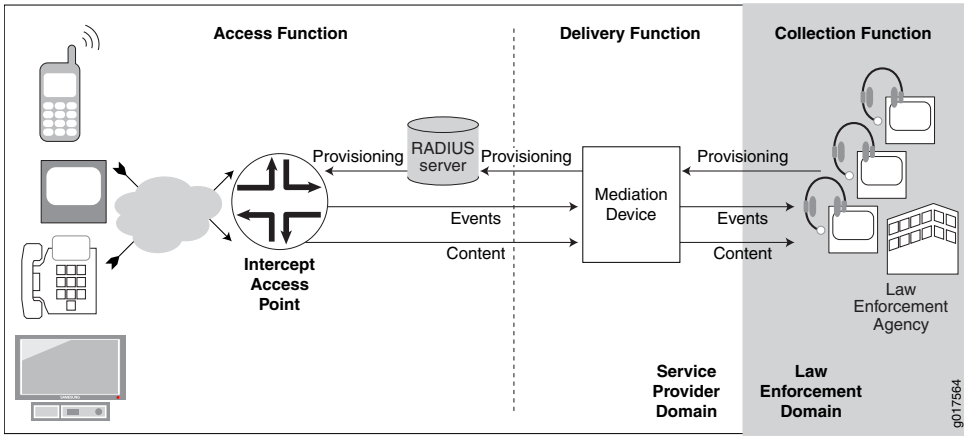


Table 3 on page 6 describes the functions and components of a RADIUS-initiated subscriber secure policy traffic mirroring environment.

Table 3: RADIUS-Initiated Subscriber Secure Policy Functions and Components

Function or Component	Description
Collection function	The collection function is responsible for collecting intercepted content and identifying information from the delivery function. The collection function is the responsibility of the law enforcement agency (LEA).
Delivery function	The delivery function delivers information that it receives from the access function to the collection function. The delivery function is performed by the mediation device.
Access function	The access function has access to the intercept target's traffic content and intercept-related events. It is responsible for collecting this information and sending it to the delivery function. The access function is the responsibility of intercept access points (IAPs).

Table 3: RADIUS-Initiated Subscriber Secure Policy Functions and Components *(continued)*

Function or Component	Description
Events	Intercept-related events, such as login or logout events or mirroring session activation or deactivation. The router sends the events to the mediation device in SNMP traps.
LEA	Law enforcement agency. The LEA provides intercept targets to the service provider who provisions the mediation device.
Mediation device	The mediation device receives provisioning information from the LEA, and it uses the information to send provisioning information to the RADIUS server. The mediation device also receives intercept-related events and intercepted content from the router, and delivers the events and intercepted content to the LEA.
RADIUS server	The RADIUS server receives provisioning information from the mediation device. It identifies subscribers whose traffic is to be mirrored, and triggers mirroring sessions on the IAP (the router) by including mirroring-related RADIUS attributes and VSAs in Access-Accept or CoA-Request messages that it sends to the IAP.
IAP	Intercept access point. In a subscriber access network the Juniper Networks router is the IAP. Using subscriber secure policies, the IAP intercepts traffic to and from the subscriber whose traffic is being mirrored. It encapsulates the intercepted content in a packet header and delivers it to the mediation device, while also sending the content to the intended destination. The IAP also sends intercept-related events to the mediation device using SNMP traps.

Related Documentation

- RADIUS-Initiated Subscriber Secure Policy Overview on page 5
- RADIUS-Initiated Traffic Mirroring Interfaces on page 8
- RADIUS-Initiated Traffic Mirroring Process at Subscriber Login on page 9
- RADIUS-Initiated Traffic Mirroring Process for Logged In Subscribers on page 10

RADIUS-Initiated Traffic Mirroring Interfaces

Figure 2 on page 8 shows the interfaces involved in RADIUS-initiated secure subscriber policy traffic mirroring.

Figure 2: RADIUS-Initiated Traffic Mirroring Interfaces

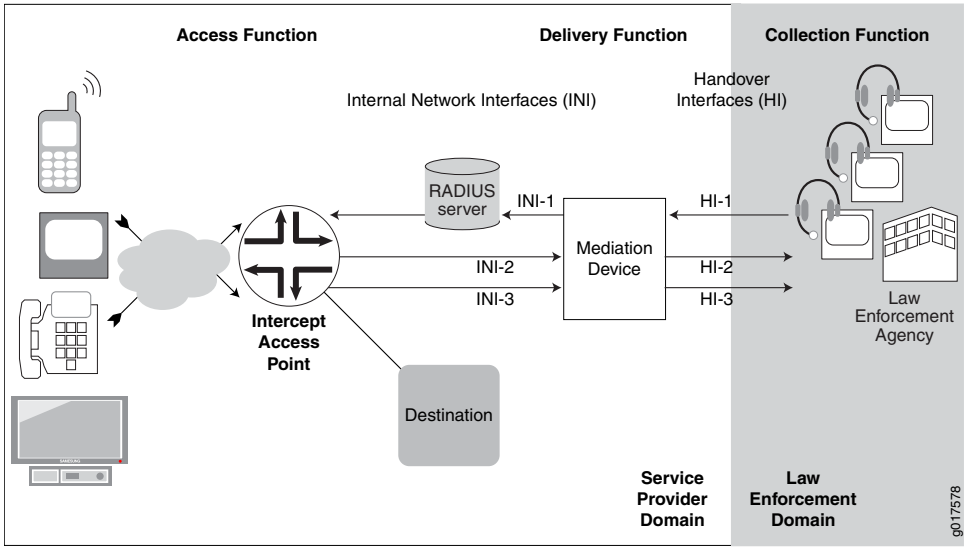


Table 4 on page 8 describes the interfaces involved in RADIUS-initiated secure subscriber policy traffic mirroring.

Table 4: RADIUS-Initiated Traffic Mirroring Interfaces

Interface	Description
HI-1	Handover Interface 1—Administrative interface between the LEA and the service provider mediation device. The LEA sends provisioning information to the mediation device on this interface.
HI-2	Handover Interface 2—Intercept-related information interface between the LEA and the mediation device that is used to deliver intercept-related events to the LEA. These events can be subscriber session events such as login, logout, and authentication.
HI-3	Handover Interface 3—Intercepted content Interface between the mediation device and LEA that is used to deliver intercepted content to the LEA.
INI-1	Internal network Interface 1—Interface used to send intercept provisioning information from the mediation device to the RADIUS server.
INI-2	Internal network interface 2—Interface used to send intercept-related events from the router to the mediation device. This information is sent in SNMP traps.
INI-3	Internal network interface 3—Interface used to send intercepted content from the router to the mediation device.

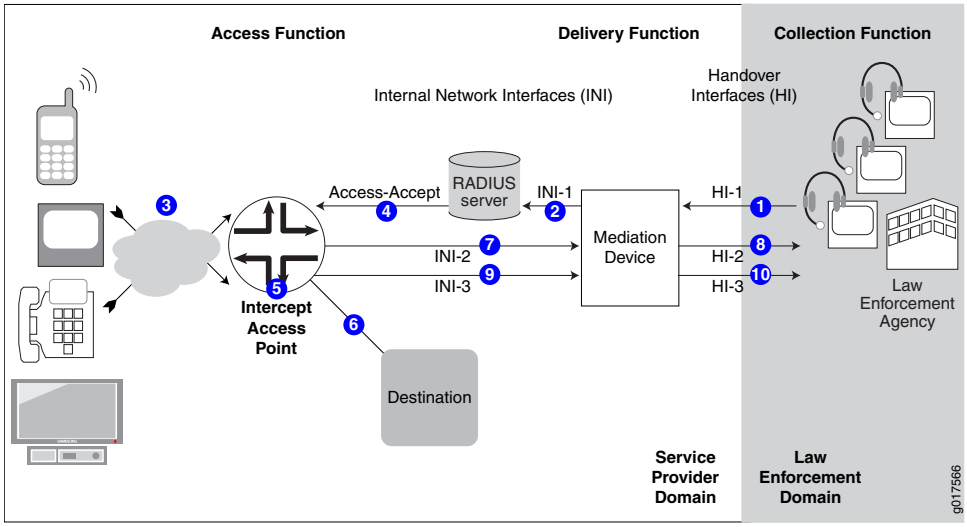
Related Documentation

- Subscriber Secure Policy Traffic Mirroring Architecture Using RADIUS on page 6
- RADIUS-Initiated Traffic Mirroring Process at Subscriber Login on page 9
- RADIUS-Initiated Traffic Mirroring Process for Logged In Subscribers on page 10

RADIUS-Initiated Traffic Mirroring Process at Subscriber Login

Figure 3 on page 9 shows the process for a RADIUS-initiated subscriber mirroring operation that is initiated when the mirrored subscriber logs in.

Figure 3: RADIUS-Initiated Subscriber Secure Policy Model at Login



1—The LEA sends provisioning information for a subscriber whose traffic is to be mirrored over the HI-1 interface to the mediation device.	6—The IAP sends the original subscriber traffic to its intended destination.
2—The mediation device sends the provisioning information over the INI-1 interface to the RADIUS server.	7—As subscriber-related events occur, the IAP sends the events in SNMP traps over the INI-2 interface to the mediation device.
3—The subscriber logs in, requesting authentication by the RADIUS server.	8—The mediation device provides the events over the HI-2 interface to the LEA.
4—The RADIUS server authenticates the subscriber and sends an Access-Accept message containing mirroring-related RADIUS attributes in Juniper VSAs to the IAP (the router).	9—The IAP encapsulates the mirrored content in a packet header and sends it over the INI-3 interface to the mediation device. The IAP uses the destination IP address of the mediation device that it received in the Access-Accept messaged from the RADIUS server.
5—The IAP creates a subscriber secure policy based on the mirroring VSAs and begins mirroring the subscriber's traffic.	10—The mediation device sends mirrored content over the HI-3 interface to the LEA.

Related Documentation

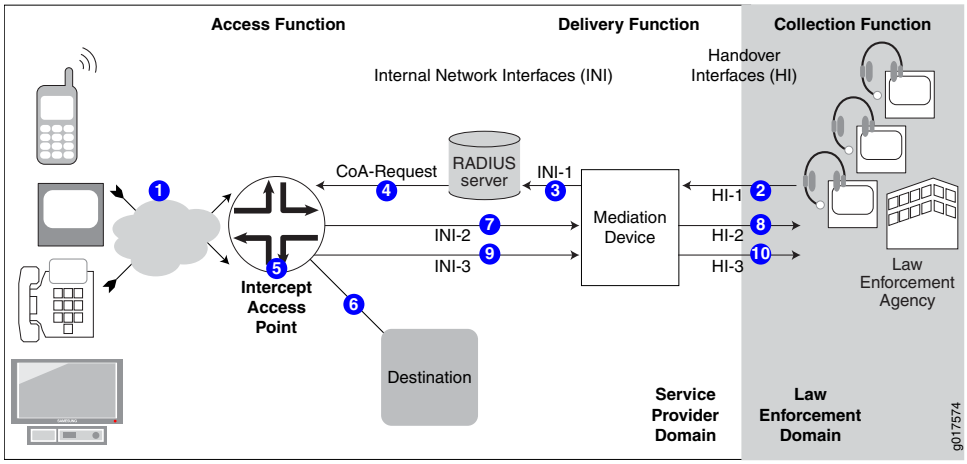
- Subscriber Secure Policy Traffic Mirroring Architecture Using RADIUS on page 6
- RADIUS-Initiated Traffic Mirroring Interfaces on page 8

- RADIUS-Initiated Traffic Mirroring Process for Logged In Subscribers on page 10
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 21

RADIUS-Initiated Traffic Mirroring Process for Logged In Subscribers

Figure 4 on page 10 shows the process for a RADIUS-initiated subscriber mirroring operation that is initiated after the subscriber has logged in.

Figure 4: RADIUS-Initiated Subscriber Secure Policy Model After Login



1—The subscriber logs in, requesting authentication by the RADIUS server. The RADIUS server authenticates the subscriber (no mirroring activity occurs).	6—The IAP sends the original subscriber traffic to its intended destination.
2—The LEA sends provisioning information for a subscriber whose traffic is to be mirrored over the HI-1 interface to the mediation device.	7—As subscriber-related events occur, the IAP sends the events in SNMP traps over the INI-2 interface to the mediation device.
3—The mediation device sends the provisioning information over the INI-1 interface to the RADIUS server.	8—The mediation device provides events over the HI-2 interface to the LEA.
4—The RADIUS server sends a CoA message containing the mirroring-related RADIUS attributes and VSAs to the IAP (the router).	9—The IAP encapsulates the mirrored subscriber content in a packet header and sends it to the mediation device over the INI-3 interface. The IAP uses the destination IP address that it received in the Access-Accept messaged from the RADIUS server.
5—The RADIUS CoA message initiates the mirroring operation. The IAP creates the subscriber secure policy based on the mirroring VSAs and immediately begins mirroring subscriber traffic.	10—The mediation device sends mirrored content over the HI-3 interface to the LEA.

Related Documentation

- Subscriber Secure Policy Traffic Mirroring Architecture Using RADIUS on page 6
- RADIUS-Initiated Traffic Mirroring Interfaces on page 8

- RADIUS-Initiated Traffic Mirroring Process at Subscriber Login on page 9
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 21

Subscriber Secure Policy Support for IPv4 Multicast Traffic

IP multicast traffic is used for applications such as audio or video streaming, IPTV, video conferencing, or online gaming. Multicast traffic is sent to multiple subscribers who have joined a multicast group.

Secure subscriber policy allows for the mirroring of IPv4 multicast traffic sent to a specific subscriber. If multiple subscribers whose traffic requires mirroring join the same multicast session, the subscriber secure policy feature mirrors each subscriber's traffic and forwards it separately to the mediation device with the proper prepended header.

Mirroring of multicast traffic is supported only for subscribers in the default logical system.

You can enable and disable the mirroring of multicast traffic on a per-chassis basis. You cannot enable or disable it on a per-subscriber basis.

Triggering the Mirroring of IPv4 Multicast Traffic

Multicast traffic being sent towards a subscriber does not contain much of the identifying information used to trigger mirroring of a subscriber's unicast traffic. For example, the multicast packet contains the multicast group address in the destination address of the packet instead of the subscriber's IP address. It also does not contain the user name or MAC address of the subscriber, and does not include information obtained by RADIUS or DHCP. Therefore, methods of identifying multicast traffic that is received by a subscriber are not the same as methods of identifying a subscriber's unicast traffic or multicast traffic that is sent by a subscriber.

To join a multicast group, a subscriber sends an IGMP join request, and it receives a reply. The reply contains the multicast groups to which the subscriber is registered. Triggering the mirroring of multicast traffic is based on the sending of the IGMP join request and the information in the IGMP reply. If the subscriber's unicast traffic is already being mirrored either through DTCP-initiated or RADIUS-initiated traffic mirroring, and the subscriber sends an IGMP join request, mirroring of multicast traffic sent to the subscriber is initiated. The traffic being mirrored is based on the groups contained in the IGMP reply.

Related Documentation

- Enabling Subscriber Secure Policy Mirroring for IPv4 Multicast Traffic on page 28

RADIUS Attributes Used for Subscriber Secure Policy

Table 5 on page 12 lists the RADIUS VSAs that are associated with subscriber secure policy. If these VSAs are present in the RADIUS Access-Accept message for a subscriber, the action specified in the LI-Action attribute takes effect.

Some mirroring VSAs that the RADIUS server sends to the router are salt-encrypted. Salt encryption is a random string of data used to modify a password hash.

Table 5: RADIUS-Based Mirroring Attributes

Attribute Number	Attribute Name	Description	Value
[26-58]	LI-Action	Traffic mirroring action	• 0 = stop mirroring • 1 = start mirroring • 2 = no action
[26-59]	Med-Dev-Handle	Identifier that associates mirrored traffic with a specific subscriber Med-Dev-Handle includes: • Intercept-Identifier • Acct-Session-ID (optional)	Salt-encrypted string
[26-60]	Med-Ip-Address	IP address of mediation device to which mirrored traffic is forwarded	Salt-encrypted IP address
[26-61]	Med-Port-Number	UDP port in the mediation device to which mirrored traffic is forwarded	Salt-encrypted integer

If a subscriber is already logged in, Table 6 on page 12 lists the RADIUS attributes that can be present in RADIUS CoA messages to identify the subscriber whose traffic is to have a mirroring action applied (activation or deactivation).

Table 6: RADIUS Attributes Used in CoA Messages to Identify Subscribers for Traffic Mirroring

Attribute Number	Attribute Name
[1]	User-Name
[44]	Acct-Session-ID

Triggering Subscriber Secure Policy for Subscribers on Dynamic Authenticated VLANs

BEST PRACTICE: When you have DHCPv4/DHCPv6 subscribers over VLANs, two sessions are created for each subscriber—one for the Layer 2 VLAN, and one for DHCP. In this case, we recommend that you use one trigger that matches both the DHCP and the VLAN session.

If authentication is performed on both the VLAN session and the DHCP session, we recommend that you use a separate, unique username for the VLAN and DHCP sessions to allow RADIUS to distinguish on which of the sessions to trigger subscriber secure policy traffic mirroring. Otherwise, when the DHCP session is authenticated and activated, traffic mirroring fails.

Related Documentation

- RADIUS-Initiated Subscriber Secure Policy Overview on page 5
- Subscriber Secure Policy Traffic Mirroring Architecture Using RADIUS on page 6

Using the Packet Header to Track Subscribers on the Mediation Device

When the router sends mirrored traffic to the mediation device, it encapsulates it in a packet header. Figure 5 on page 13 is the mirrored packet header and payload that the router sends to the mediation device.

Figure 5: Mirrored Packet Header and Payload

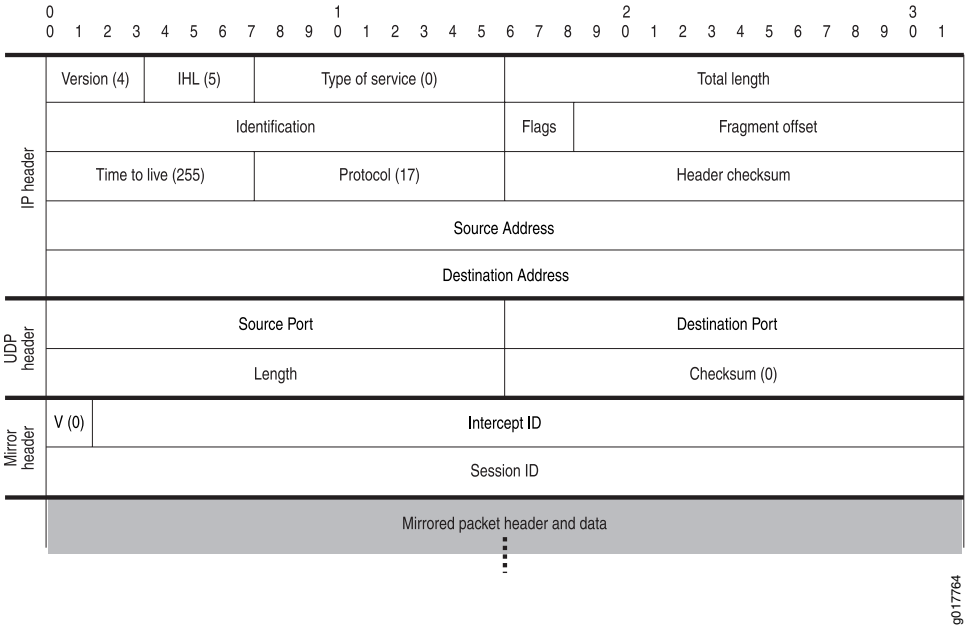


Table 7 on page 14 describes the fields in the packet header of mirrored packets.

Table 7: Mirrored Packet Header and Payload 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
Source Address	IP address of the router interface that sends mirrored traffic to the mediation device	32
Destination Address	IP address of the mediation device to which mirrored traffic is forwarded (VSA 26-60)	32
UDP Header		
Source Port	UDP port number on the router from which mirrored traffic is sent to the mediation device	16
Destination Port	UDP port on the mediation device to which mirrored traffic is forwarded (VSA 26-61)	16
Length	Dynamically computed	16
Checksum	0	16
Mirror Header		

Table 7: Mirrored Packet Header and Payload Field Descriptions *(continued)*

Field	Value	Length (Bits)
V (mirror header value)	0	2
Intercept ID	See "Format of the Mirror Header Values Used to Track Subscribers and Subscriber Sessions" on page 16 for details	30
Session-ID	See "Format of the Mirror Header Values Used to Track Subscribers and Subscriber Sessions" on page 16 for details	32

Format of the Mirror Header Values Used to Track Subscribers and Subscriber Sessions

The packet header includes mirror header attributes that the mediation device can use to track subscribers and subscriber sessions. The router creates values for these attributes based on information that it receives from RADIUS. There are three mirror header attributes in the packet header:

- V (mirror header value)—Used by the router to specify how the values of the Session ID and Intercept ID are determined. The value received from RADIUS can be a 0 or a 1. However, the value is always 0 in the packet header sent to the mediation device.
- Session ID—Used by the mediation device to identify the session of the mirrored subscriber. The value is assigned to a subscriber session by the Junos OS. The Session ID changes with each new session for a subscriber.
- Intercept ID—Used along with the Session ID by the mediation device to track a subscriber across multiple login and logout events. The value is assigned to a subscriber whose traffic is being intercepted. The Intercept ID is constant; it does not change as a subscriber logs in and logs out of sessions.

The values of the Intercept ID and the Session ID are determined by the value that the router receives in VSA 26-59. VSA 26-59 is declared as a hexadecimal string that can be either 4 bytes or 8 bytes long. The mirror header value specifies whether a 4-byte value or an 8-byte value is used to form the Intercept ID and the Session ID.

4-Byte Format

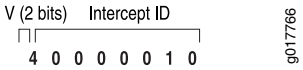
The 4-byte format allows you to manually specify the Intercept ID. The Session ID value is automatically created based on the least significant 32 bits of the Acct-Session-ID (RADIUS attribute 44).

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 Intercept ID value.

For example, a value of 40000010 for VSA 26-59 configures the following fields in the mirror header, as shown in Figure 6 on page 16:

- V = 1
- Intercept ID = 0x10

Figure 6: 4-Byte Format of VSA 26-59



8-Byte Format

The 8-byte format of VSA 26-59 enables you to manually specify the both the Session-ID value and the Intercept ID 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 Intercept ID 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 7 on page 17:

- V = 0
- Intercept-ID = 0x300
- Session-ID = 0x90

Figure 7: 8-Byte Format of VSA 26-59

Related Documentation

- RADIUS-Initiated Subscriber Secure Policy Overview on page 5
- Subscriber Secure Policy Traffic Mirroring Architecture Using RADIUS on page 6

Subscriber Secure Policy and L2TP LAC Subscribers

RADIUS-initiated per-subscriber traffic mirroring can be applied to subscribers whose traffic is tunneled with L2TP. Both subscriber ingress traffic (from the subscriber into the tunnel) and subscriber egress traffic (from the tunnel to the subscriber) are mirrored at the subscriber-facing ingress interface on the LAC. The ingress traffic is mirrored after PPPoE decapsulation and before L2TP encapsulation. The egress traffic is mirrored after L2TP decapsulation. The mirrored packet includes the complete HDLC frame sent to the LNS rather than only the IP datagram.

Related Documentation

- Subscriber Secure Policy Overview on page 3
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 21
- RADIUS Attributes Used for Subscriber Secure Policy on page 12

PART 2

Configuration

CHAPTER 3

Configuration Overview and Guidelines

Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview

Before you configure subscriber secure policy traffic mirroring, note the following:

- Subscriber secure policy mirroring runs on the radius-flow-tap service infrastructure. To configure the subscriber secure policy service, you must have the same privileges that are required to configure the radius-flow-tap service.
- The subscriber secure policy feature requires some system resources while mirroring, encrypting, and sending traffic to the mediation device. For example, you might elect to use a 10-Gigabit Ethernet interface for the tunnel to the mediation device if you expect the amount of traffic you plan to mirror to approach 1 Gbps of actual user data.

To configure the subscriber secure policy service:

1. Configure tunnel interfaces (vt interfaces) that are used to send mirrored content to the mediation device.

   See "Configuring Tunnel Interfaces for Subscriber Secure Policy Mirroring" on page 25.

2. Configure radius-flow-tap service support for secure subscriber policy. This support includes optional forwarding-class information that the subscriber secure policy service uses to send mirrored traffic to the content destination device.

   See "Configuring Support for Subscriber Secure Policy Mirroring" on page 26.

3. Configure an access profile that specifies the RADIUS-related support for subscriber secure policy on the router, including a list of one or more RADIUS authentication servers. The router uses the list of specified servers for both authentication and dynamic request operations. You must also configure the RADIUS dynamic request feature, which provides the CoA message support used in-session traffic mirroring.

   See "Configuring RADIUS Server Support for Subscriber Secure Policy Mirroring" on page 27.

4. Ensure that the following support is also configured:

   - The RADIUS record of the mirrored subscriber must include the RADIUS attributes and VSAs required for subscriber secure policy mirroring. See "RADIUS Attributes Used for Subscriber Secure Policy" on page 12 for descriptions of the supported attributes used in RADIUS Accept-Accept and CoA messages.
   - The mediation device must be configured to accept the mirrored content.

5. (Optional) Enable the mirroring of IPv4 multicast traffic on the router.

   See "Enabling Subscriber Secure Policy Mirroring for IPv4 Multicast Traffic" on page 28.

6. (Optional) Configure SNMPv3 trap support to report mirroring-related events to the mediation device.

   See "Configuring SNMPv3 Traps for Subscriber Secure Policy Mirroring" on page 57.

To terminate an active subscriber mirroring session at any time.

See "Terminating RADIUS-Initiated Subscriber Traffic Mirroring" on page 59.

Related Documentation

- RADIUS Attributes Used for Subscriber Secure Policy on page 12
- Guidelines for Configuring Subscriber Secure Policy Mirroring on page 22
- Intercept-Related Events Transmitted to the Mediation Device on page 55
- Terminating RADIUS-Initiated Subscriber Traffic Mirroring on page 59

Guidelines for Configuring Subscriber Secure Policy Mirroring

The subscriber secure policy service uses the radius-flow-tap service infrastructure.

When configuring subscriber secure policy mirroring, consider the following guidelines regarding the relationship between subscriber secure policy service and the radius-flow-tap service:

- The radius-flow-tap service **[edit services radius-flow-tap]** and the flow-tap service **[edit services flow-tap]** cannot run simultaneously on the router. Therefore, flow-tap and subscriber secure policy mirroring cannot run simultaneously on the same router.
- You can configure one instance of the radius-flow-tap service on the router. Subscriber secure policy RADIUS-initiated mirroring and DTCP-initiated mirroring use the radius-flow-tap service.
- If you delete the radius-flow-tap service all subscriber secure policy mirroring stops.

Related Documentation

- Subscriber Secure Policy Overview on page 3
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 21
- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview
- Configuring Support for Subscriber Secure Policy Mirroring on page 26

Considerations When Using RADIUS Attributes for Subscriber Secure Policy

When using RADIUS attributes and VSAs for the subscriber secure policy service, keep the following considerations in mind:

- A dynamic profile must exist for a subscriber whose traffic is to be mirrored. Otherwise, the subscriber is unable to log in when the mirroring-related VSAs are received in RADIUS Accept-Accept or CoA-Request messages. See Dynamic Profiles Overview for information about dynamic profiles.
- VSA 26-60 must always be present in the RADIUS Access-Accept or CoA-Request message, or the instantiation of the mirroring session fails. The presence of VSA 26-60 triggers the prepending operation—all mirrored packets must be prepended with both the UDP/IP header and the MD header.
- VSA 26–58 (LI-Action) specifies the action taken by the router. The action differs if the VSA is received in an Access-Accept message or a CoA message, as indicated in Table 8 on page 23.

Table 8: LI-Action VSA Action

LI-Action Value	Access-Accept Message Action	CoA Message Action
0	Prevents subscriber from logging in	Immediately stops mirroring subscriber traffic; subscriber remains logged in
1	Starts mirroring subscriber traffic when subscriber logs in	Immediately starts mirroring subscriber traffic
2	No action	No action

- A VSA 26–58 value of 2 specifies that the router does not perform any traffic mirroring-related action. This setting can provide additional security by confusing unauthorized users who attempt to access traffic mirroring communication between the router and the RADIUS server.

Related Documentation

- RADIUS Attributes Used for Subscriber Secure Policy on page 12

CHAPTER 4

Configuration Tasks

Configuring Tunnel Interfaces for Subscriber Secure Policy Mirroring

The router, acting as the IAP, uses tunnel interfaces (vt interfaces) to send mirrored traffic to the mediation device. The IAP equally distributes the mirrored traffic across the available tunnel interfaces.

Because the MX Series 3D Universal Edge Routers do not support Tunnel Services PICs, you create a pool tunnel interfaces on MX Series routers at the **[edit chassis]** hierarchy level.

You can configure up to 2048 mirrored subscriber sessions per chassis.

To configure a pool of tunnel interfaces for use by subscriber secure policy mirroring:

1. Access the chassis configuration, and specify the slot number of the DPC, MPC, or MIC.
   - On the MX80 router, the range is 0 through 1.
   - On other MX Series routers, if two System Control Boards (SCBs), are installed, the range is 0 through 11. If three SCBs are installed, the range is 0 through 5 and 7 through 11.

     ```
     [edit chassis]
     user@host# edit fpc 1
     ```
2. Configure the PIC number of the FPC.
   - On MX80 routers, if the FPC is 0, the PIC number can only be 0. If the FPC is 1, the PIC range is 0 through 3.
   - For all other MX Series routers, the range is 0 through 3.

     ```
     [edit chassis fpc 1]
     user@host# edit pic 1
     ```

3. Specify that the FPC and PIC are to be used for tunnel interfaces.

   ```
   [edit chassis fpc 1 pic 1]
   user@host# edit tunnel-services
   ```

4. Specify the amount of bandwidth to reserve for tunnel traffic on each Packet Forwarding Engine.

   - 1g indicates that 1 Gbps of bandwidth is reserved for tunnel traffic.
   - 10g indicates that 10 Gbps of bandwidth is reserved for tunnel traffic.

   If you specify a bandwidth that is not compatible, tunnel services are not activated. For example, you cannot specify a bandwidth of 1 Gbps for a Packet Forwarding Engine on a 10-Gigabit Ethernet 4-port DPC.

   ```
   [edit chassis fpc 1 pic 1 tunnel-services]
   user@host#
   user@host# set bandwidth 1g
   ```

5. Configure the tunnel interfaces, including the family.

   To configure subscriber secure policy mirroring for IPv6 traffic, configure the tunnel interfaces for both the **inet** and **inet6** families.

   ```
   [edit interfaces]
   user@host# set vt-1/1/0 unit 0 family inet
   user@host# set vt-1/1/0 unit 0 family inet6
   ```

Related Documentation

- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 21
- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview

Configuring Support for Subscriber Secure Policy Mirroring

Subscriber secure policy runs on the radius-flow-tap service. This topic describes the steps to configure radius-flow-tap support for RADIUS-initiated and DTCP-initiated subscriber secure policy mirroring.

To configure the radius-flow-tap service to support subscriber secure policy mirroring:

1. Configure the flow-tap service used for subscriber secure policy mirroring.

   ```
   [edit services]
   user@host# edit radius-flow-tap
   ```

2. Assign the tunnel interfaces that the radius-flow-tap service uses.

   ```
   [edit services radius-flow-tap]
   user@host# set interfaces vt-1/1/0.0
   ```

   If a currently used tunnel interface is deleted from the pool of interfaces, the active mirroring sessions are redistributed from the deleted interface to other tunnel interfaces in the pool. Also, when a new tunnel interface is added into the pool, the service adds the new interface to the list of interfaces available for new mirroring sessions or for existing sessions transferred from a failed interface.

3. Specify the source IP address that the radius-flow-tap service uses for mirroring. This address is used in the IP header prepended to mirrored packets that are sent to the content destination device.

   ```
   [edit services radius-flow-tap]
   user@host# set source-ipv4-address ipv4-address
   ```

4. (Optional) Specify the forwarding class that is applied to the mirrored packets sent to the mediation device.

   If you do not specify a forwarding class, mirrored packets inherit the forwarding class from the original packet (which is the forwarding class set by default classification that CoS applies to the packet on the ingress interface).

   ```
   [edit services radius-flow-tap]
   user@host# set forwarding-class class-name
   ```

Related Documentation

- Subscriber Secure Policy Overview on page 3
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 21
- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview
- Guidelines for Configuring Subscriber Secure Policy Mirroring on page 22

Configuring RADIUS Server Support for Subscriber Secure Policy Mirroring

This topic describes how to configure support for the RADIUS server that initiates subscriber-based traffic mirroring. You create an access profile to specify the RADIUS server support.

To configure the router's interaction with the RADIUS server in support of subscriber secure policy mirroring:

1. Create the access profile and assign a name.

   ```
   [edit access]
   user@host# edit profile profile-name
   ```

2. Specify RADIUS as the authentication method.

   ```
   [edit access profile profile-name]
   user@host# set authentication-order radius
   ```

3. Specify the IP address of the RADIUS server that performs authentication. This server also performs dynamic request (CoA) functions.

   ```
   [edit access profile profile-name]
   user@host# set radius authentication-server ip-address
   ```

4. Specify the secret to use when communicating with the RADIUS server.

   ```
   [edit access profile profile-name]
   user@host# set radius-server server-address secret password
   ```

5. Specify other optional RADIUS configuration settings as needed, such as accounting support.

Related Documentation

- Subscriber Secure Policy Overview on page 3
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 21
- RADIUS Attributes Used for Subscriber Secure Policy on page 12

Enabling Subscriber Secure Policy Mirroring for IPv4 Multicast Traffic

This topic describes the steps to enable subscriber secure policy mirroring of IPv4 multicast traffic. You can enable and disable IPv4 multicast intercept on a per chassis basis.

To configure the radius-flow-tap service to support subscriber secure policy mirroring:

1. Configure the flow-tap service used for subscriber secure policy mirroring.

   ```
   [edit services]
   user@host# edit radius-flow-tap
   ```

2. Enable the interception of multicast traffic.

   ```
   [edit services radius-flow-tap]
   user@host# set multicast-interception
   ```

Related Documentation

- Subscriber Secure Policy Support for IPv4 Multicast Traffic on page 11
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 21
- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview

CHAPTER 5

Configuration Statements

[edit services radius-flow-tap] Hierarchy Level

```
services {
  radius-flow-tap {
    forwarding-class class-name;
    interfaces interface-name;
    multicast-interception;
    source-ipv4-address ipv4-address;
  )
}
```

Related Documentation

- Subscriber Secure Policy Overview on page 3
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 21

authentication (Login)

Syntax

```
authentication {
  (encrypted-password "password" | plain-text-password);
  load-key-file URL filename;
  ssh-dsa "public-key";
  ssh-rsa "public-key";
}
```

Hierarchy Level [edit system login user *username*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Authentication methods that a user can use to log in to the router or switch. You can assign multiple authentication methods to a single user.

Options

encrypted-password "*password*"—Message Digest 5 (MD5) or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password for each user.

You cannot configure a blank password for **encrypted-password** using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

load-key-file *URL filename*—Load previously-generated RSA (SSH version 1 and SSH version 2) and DSA (SSH version 2) public keys from a named file at a specified URL location. The file contains one or more SSH keys.

plain-text-password—When using this option, the command-line interface (CLI) prompts you for the password and then encrypts it.

ssh-dsa "*public-key*"—SSH version 2 authentication. Specify the SSH public key. You can specify one or more public keys for each user.

ssh-rsa "*public-key*"—SSH version 1 and SSH version 2 authentication. Specify the SSH public key. You can specify one or more public keys for each user.

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

Related Documentation

- Configuring Junos OS User Accounts
- root-authentication

authentication-order

Syntax authentication-order [*authentication-methods*];

Hierarchy Level [edit access profile *profile-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
none option introduced in Junos OS Release 11.2.

Description Set the order in which the Junos OS tries different authentication methods when verifying that a client can access the router or switch. For each login attempt, the software tries the authentication methods in order, from first to last.

Default password

Options *authentication-methods*

- **none**—Grants authentication without examining the client credentials. Can be used, for example, when the Diameter function Gx-Plus is employed for notification during subscriber provisioning.
- **password**—Verify the client using the information configured at the **[edit access profile *profile-name* client *client-name*]** hierarchy level.
- **radius**—Verify the client using RADIUS authentication services.

NOTE: For subscriber access management, you must always specify the radius method. Subscriber access management does not support the password option (the default), and authentication fails when no method is specified.

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

Related Documentation

- Example: Configuring CHAP Authentication with RADIUS
- Specifying the Authentication and Accounting Methods for Subscriber Access
- Configuring Access Profiles for L2TP or PPP Parameters

authentication-server

Syntax authentication-server [*ip-address*];

Hierarchy Level [edit access profile *profile-name* radius]

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify a list of the RADIUS authentication servers used to authenticate DHCP, L2TP, and PPP clients. The servers in the list are also used as RADIUS dynamic-request servers, from which the router accepts and processes RADIUS disconnect requests, CoA requests, and dynamic service activations and deactivations.

Options ***ip-address***—IPv4 address.

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

Related Documentation

- Configuring RADIUS Server Parameters for Subscriber Access

bandwidth

Syntax bandwidth *bandwidth-value*;

Hierarchy Level [edit chassis fpc *slot-number* pic *number* tunnel-services]

Release Information Statement introduced in Junos OS Release 8.2.

Description (MX Series 3D Universal Edge Routers and T4000 Core Routers only) Specify the amount of bandwidth in gigabits per second to reserve for tunnel services.

Options *bandwidth-value*—Define the amount of bandwidth in gigabits per second to reserve for tunnel services. On MX Series routers, the bandwidth values can be **1g**, **10g**, **20g**, or **40g**. On T4000 routers, the bandwidth values are multiples of **10g** up to **100g**.

NOTE: If you specify a bandwidth that is not compatible with the type of DPCs or MPCs and their respective Packet Forwarding Engine, tunnel services are not activated. For example, you cannot specify 1 gigabit per second bandwidth for a Packet Forwarding Engine on a 10-Gigabit Ethernet 4-port DPC or 16x10GE 3D MPC.

NOTE: Bandwidth rates of 20 gigabits per second and 40 gigabits per second require use of an MX Series router with the 100-Gigabit Ethernet MPC and the 100-Gigabit CFP MIC.

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

Related Documentation

- Example: Configuring Tunnel Interfaces on a Gigabit Ethernet 40-Port DPC
- Example: Configuring Tunnel Interfaces on a 10-Gigabit Ethernet 4-Port DPC
- Example: Configuring Tunnel Interfaces on a 100-Gigabit Ethernet MPC
- tunnel-services on page 49
- [edit chassis] Hierarchy Level

class (Defining Login Classes)

Syntax

```
class class-name {
  allow-commands "regular-expression";
  ( allow-configuration | allow-configuration-regexps) “regular expression 1” “regular
    expression 2”;
  deny-commands "regular-expression";
  ( deny-configuration | deny-configuration-regexps ) “regular expression 1” “regular expression
    2 ”;
  idle-timeout minutes;
  permissions [ permissions ];
}
```

Hierarchy Level [edit system login]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Define a login class.

Options ***class-name***—A name you choose for the login class.

The remaining statements are explained separately.

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

Related Documentation

- Defining Junos OS Login Classes
- user on page 51

class (Assigning a Class to an Individual User)

Syntax

```
class class-name;
```

Hierarchy Level [edit system login user *username*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure a user’s login class. You must configure one class for each user.

Options ***class-name***—One of the classes defined at the **[edit system login class]** hierarchy level.

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

Related Documentation

- Configuring Junos OS User Accounts

connection-limit

Syntax connection-limit *limit*;

Hierarchy Level [edit system services finger],
[edit system services ftp],
[edit system services ssh],
[edit system services telnet],
[edit system services xnm-clear-text],
[edit system services xnm-ssl]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the maximum number of connections sessions for each type of system services (finger, ftp, ssh, telnet, xnm-clear-text, or xnm-ssl) per protocol (either IPv6 or IPv4).

Options ***limit***—(Optional) Maximum number of established connections per protocol (either IPv6 or IPv4).

Range: 1 through 250

Default: 75

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

Related Documentation

- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications
- Configuring DTCP-over-SSH Service for the Flow-Tap Application
- Configuring Finger Service for Remote Access to the Router
- Configuring FTP Service for Remote Access to the Router or Switch
- Configuring SSH Service for Remote Access to the Router or Switch
- Configuring Telnet Service for Remote Access to a Router or Switch

flow-tap-dtcp

Syntax

```
flow-tap-dtcp {
  ssh {
    connection-limit limit;
    rate-limit limit;
  }
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced in Junos OS Release 8.1.

Description Configure Dynamic Tasking Control Protocol (DTCP) sessions to run over SSH in support of the flow-tap application.

Options

connection-limit *limit*—(Optional) Maximum number of connections allowed.

Range: 1 through 250

Default: 75

rate-limit *limit*—(Optional) Maximum number of connection attempts allowed per minute.

Range: 1 through 250

Default: 150

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

Related Documentation

- Configuring DTCP-over-SSH Service for the Flow-Tap Application

forwarding-class (Subscriber Secure Policy)

Syntax forwarding-class *class-name*;

Hierarchy Level [edit services radius-flow-tap]

Release Information Statement introduced in Junos OS Release 9.4.

Description Specify forwarding class that is applied to mirrored packets sent to a mediation device.

Options ***class-name***—Name of the forwarding class.

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

Related Documentation

- Subscriber Secure Policy Overview on page 3
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 21

fpc (MX Series 3D Universal Edge Routers)

Syntax

```
fpc slot-number {
  pic number {
    inline-services {
      bandwidth (1g | 10g);
    }
    port-mirror-instance port-mirroring-instance-name-pic-level;
    tunnel-services {
      bandwidth (1g | 10g)
    }
  }
  port-mirror-instance port-mirroring-instance-name-fpc-level;
}
```

Hierarchy Level [edit chassis]

Release Information Statement introduced in Junos OS Release 8.2.
port-mirror-instance option introduced in Junos OS Release 9.3.

Description Configure properties for the DPC or MPC and corresponding Packet Forwarding Engines to create tunnel interfaces.

(MX Series Virtual Chassis only) To configure properties for MPCs in a member router in an MX Series Virtual Chassis configuration, you must specify the router's Virtual Chassis member number *before* the **fpc** statement. Specify the member number in the form **member *member-id***, where ***member-id*** is 0 or 1. If you do not specify the member number before the **fpc** statement, the commit operation fails and the software displays an error message indicating that the **fpc** statement must include the member number for routers in Virtual Chassis mode.

Options

fpc *slot-number*—Specify the slot number of the DPC.

Range: 0 through 11

pic *number*—Specify the number of the Packet Forwarding Engine. Each DPC includes four Packet Forwarding Engines.

Range: 0 through 4

port-mirror-instance *port-mirroring-instance-name-fpc-level*—Associate a port-mirroring instance with the DPC and its corresponding PICs. The port-mirroring instance is configured under the **[edit forwarding-options port-mirroring]** hierarchy level.

The remaining statements are explained separately.

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

Related Documentation

- Configuring Port-Mirroring Instances on MX Series 3D Universal Edge Routers
- Enabling Inline Service Interfaces

interfaces (Subscriber Secure Policy)

Syntax interfaces *interface-name*;

Hierarchy Level [edit services radius-flow-tap]

Release Information Statement introduced in Junos OS Release 9.4.

Description Specify tunnel interfaces that are used to send mirrored packets to a mediation device.

Options ***interface-name***—Name of the interface.

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

Related Documentation

- Subscriber Secure Policy Overview on page 3
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 21

login

Syntax

```
login {
  announcement text;
  class class-name {
    allow-commands "regular-expression";
    ( allow-configuration | allow-configuration-regexps) “regular expression 1” “regular
      expression 2”;
    deny-commands "regular-expression";
    ( deny-configuration | deny-configuration-regexps )  “regular expression 1” “regular
      expression 2 ”;
    idle-timeout minutes;
    login-tip;
    permissions [ permissions ];
  }
  message text;
  password {
    change-type (set-transitions | character-set);
    format (md5 | sha1 | des);
    maximum-length length;
    minimum-changes number;
    minimum-length length;
  }
  retry-options {
    backoff-threshold number;
    backoff-factor seconds;
    minimum-time seconds;
    tries-before-disconnect number;
  }
  user username {
    full-name complete-name;
    uid uid-value;
    class class-name;
    authentication authentication;
    (encrypted-password "password" | plain-text-password);
    ssh-rsa "public-key";
    ssh-dsa "public-key";
  }
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure user access to the router or switch.

Options The remaining statements are explained separately.

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

Related Documentation
- Defining Junos OS Login Classes

multicast-interception (Subscriber Secure Policy)

Syntax multicast-interception;

Hierarchy Level [edit services radius-flow-tap]

Release Information Statement introduced in Junos OS Release 11.4.

Description Enables subscriber secure policy to mirror IPv4 multicast traffic sent to subscribers. It enables the mirroring of multicast traffic for all subscribers on the chassis.

Mirroring of multicast traffic is supported only for subscribers in the default logical system.

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

Related Documentation
- Subscriber Secure Policy Overview on page 3
- Subscriber Secure Policy Support for IPv4 Multicast Traffic on page 11
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 21
- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview

permissions

Syntax permissions [*permissions*];

Hierarchy Level [edit system login class]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the login access privileges to be provided on the router or switch.

Options ***permissions***—Privilege type. For a list of permission flag types, see Understanding Junos OS Access Privilege Levels.

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

Related Documentation
- Configuring Access Privilege Levels
- user on page 51

profile

Syntax

```
profile profile-name {
  accounting {
    accounting-stop-on-access-deny;
    accounting-stop-on-failure;
    coa-immediate-update;
    coa-no-override service-class-attribute;
    duplication;
    immediate-update;
    order [ accounting-method ];
    statistics (time | volume-time);
    update-interval minutes;
    }
  authentication-order [ authentication-methods ];
  client client-name {
    chap-secret chap-secret;
    group-profile profile-name;
    ike {
      allowed-proxy-pair {
        remote remote-proxy-address local local-proxy-address;
      }
      pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
      ike-policy policy-name;
      interface-id string-value;
    }
    l2tp {
      aaa-access-profile profile-name;
      interface-id interface-id;
      lcp-renegotiation;
      local-chap;
      maximum-sessions-per-tunnel number;
      multilink {
        drop-timeout milliseconds;
        fragment-threshold bytes;
      }
      ppp-authentication (chap | pap);
      ppp-profile profile-name;
      shared-secret shared-secret;
    }
    pap-password pap-password;
    ppp {
      cell-overhead;
      encapsulation-overhead bytes;
      framed-ip-address ip-address;
      framed-pool framed-pool;
      idle-timeout seconds;
      interface-id interface-id;
      keepalive seconds;
      primary-dns primary-dns;
      primary-wins primary-wins;
      secondary-dns secondary-dns;
      secondary-wins secondary-wins;
    }
```

```
    user-group-profile profile-name;
}
radius {
    accounting-server [ ip-address ];
    authentication-server [ ip-address ];
    options {
        accounting-session-id-format (decimal | description);
        client-accounting-algorithm (direct | round-robin);
        client-authentication-algorithm (direct | round-robin);
        coa-dynamic-variable-validation;
        ethernet-port-type-virtual;
        interface-description-format {
            exclude-adapter;
            exclude-sub-interface;
        }
        juniper-dsl-attributes;
        nas-identifier identifier-value;
        nas-port-extended-format {
            adapter-width width;
            port-width width;
            slot-width width;
            stacked-vlan-width width;
            vlan-width width;
        }
        nas-port-id-delimiter delimiter-character;
        nas-port-id-format {
            agent-circuit-id;
            agent-remote-id;
            interface-description;
            nas-identifier;
        }
        nas-port-type {
            ethernet {
                port-type;
            }
        }
        revert-interval interval;
        vlan-nas-port-stacked-format;
    }
    attributes {
        exclude {
            ...
        }
        ignore {
            framed-ip-netmask;
            input-filter;
            logical-system:routing-instance;
            output-filter;
        }
    }
}
radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry attempts;
    routing-instance routing-instance-name;
```

```
    secret password;
    max-outstanding-requests value;
    source-address source-address;
    timeout seconds;
  }
  service {
    accounting-order (activation-protocol | radius);
  }
  session-options {
    client-group [ group-names ];
    client-idle-timeout minutes;
    client-session-timeoutminutes;
  }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure PPP CHAP, or a profile and its subscriber access, L2TP, or PPP properties.

Options *profile-name*—Name of the profile.

For CHAP, the name serves as the mapping between peer identifiers and CHAP secret keys. This entity is queried for the secret key whenever a CHAP challenge or response is received.

The remaining statements are explained separately.

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

Related Documentation

- Configuring the PPP Authentication Protocol
- Configuring Access Profiles for L2TP or PPP Parameters
- Configuring L2TP Properties for a Client-Specific Profile
- Configuring an L2TP LNS with Inline Service Interfaces
- Configuring PPP Properties for a Client-Specific Profile
- Configuring Service Accounting with JSRC
- AAA Service Framework Overview
- show network-access aaa statistics
- clear network-access aaa statistics

radius (Access Profile)

Syntax

```
radius {
    accounting-server [ ip-address ];
    attributes {
        exclude
            ...
        }
        ignore {
            framed-ip-netmask;
            input-filter;
            logical-system-routing-instance;
            output-filter;
        }
    }
    authentication-server [ ip-address ];
    options {
        accounting-session-id-format (decimal | description);
        client-accounting-algorithm (direct | round-robin);
        client-authentication-algorithm (direct | round-robin);
        coa-dynamic-variable-validation;
        ethernet-port-type-virtual;
        interface-description-format {
            exclude-adapter;
            exclude-sub-interface;
        }
        juniper-dsl-attributes;
        nas-identifier identifier-value;
        nas-port-extended-format {
            adapter-width width;
            port-width width;
            slot-width width;
            stacked-vlan-width width;
            vlan-width width;
        }
        nas-port-id-delimiter delimiter-character;
        nas-port-id-format {
            agent-circuit-id;
            agent-remote-id;
            interface-description;
            nas-identifier;
        }
        nas-port-type {
            ethernet {
                port-type;
            }
        }
        revert-interval interval;
        vlan-nas-port-stacked-format;
    }
}
```

Hierarchy Level [edit access profile *profile-name*]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the RADIUS parameters that the router uses for AAA authentication and accounting for subscribers.

The remaining statements are explained separately.

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

Related Documentation
- Configuring RADIUS Server Parameters for Subscriber Access
- RADIUS Server Options for Subscriber Access

radius-flow-tap

Syntax

```
radius-flow-tap {
  forwarding-class class-name;
  interfaces interface-name;
  multicast-interception;
  source-ipv4-address ipv4-address;
)
```

Hierarchy Level [edit services]

Release Information Statement introduced in Junos OS Release 9.4.

Description Assign parameters that are used with subscriber secure policy mirroring.

The remaining statements are explained separately.

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

Related Documentation
- Subscriber Secure Policy Overview on page 3
- Configuring Support for Subscriber Secure Policy Mirroring on page 26

radius-server

Syntax

```
radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry attempts;
    routing-instance routing-instance-name;
    secret password;
    max-outstanding-requests value;
    source-address source-address;
    timeout seconds;
}
```

Hierarchy Level

[edit access],
[edit access profile *profile-name*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure RADIUS for subscriber access management, L2TP, or PPP.

To configure multiple RADIUS servers, include multiple **radius-server** statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

Options

server-address—Address of the RADIUS authentication server.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Configuring RADIUS Authentication for L2TP
- Configuring the PPP Authentication Protocol
- Configuring RADIUS Authentication
- Configuring Authentication and Accounting Parameters for Subscriber Access
- show network-access aaa statistics
- clear network-access aaa statistics

rate-limit

Syntax rate-limit *limit*;

Hierarchy Level [edit system services finger],
[edit system services ftp],
[edit system services ssh],
[edit system services telnet],
[edit system services xnm-clear-text],
[edit system services xnm-ssl]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the maximum number of connections attempts per protocol (either IPv6 or IPv4) on an access service.

Default **150** connections

Options **rate-limit *limit***—(Optional) Maximum number of connection attempts allowed per minute, per IP protocol (either IPv4 or IPv6).

Range: **1** through **250**

Default: **150**

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

Related Documentation
- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications

source-ipv4-address

Syntax source-ipv4-address *ipv4-address*;

Hierarchy Level [edit services radius-flow-tap]

Release Information Statement introduced in Junos OS Release 9.4.

Description Specify the source IP address used in the IP header that is prepended to mirrored packets sent to a mediation device.

Options ***ipv4-address***—IPv4 address.

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

Related Documentation
- Subscriber Secure Policy Overview on page 3
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 21

ssh

Syntax

```
ssh {
  connection-limit limit;
  protocol-version [v1 v2];
  rate-limit limit;
  root-login (allow | deny | deny-password);
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Allow SSH requests from remote systems to the local router or switch.

The remaining statements are explained separately.

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

Related Documentation

- Configuring SSH Service for Remote Access to the Router or Switch

tunnel-services

Syntax

```
tunnel-services {
  bandwidth (1g | 10g | 20g | 40g);
  tunnel-only;
}
```

Hierarchy Level [edit chassis fpc *slot-number* pic *number*]

Release Information Statement introduced in Junos OS Release 8.2.

Description For MX Series 3D Universal Edge Routers, configure the amount of bandwidth for tunnel services.

For M7i, M10i, M120, M320, T Series and TX Matrix routers with IQ2 PICs and IQ2E PICs, configure support for per unit scheduling for GRE tunnels. Use the **tunnel-services** statement to specify that the IQ2 or IQ2E PIC will work both as a regular PIC and as a tunnel PIC. For M7i, M10i, M120, M320, T Series and TX Matrix routers with IQ2 PICs and IQ2E PICs, you can use the **tunnel-only** option to specify that an IQ2 or IQ2E PIC work in tunnel mode only.

NOTE: **Bandwidth rates of 20 gigabits per second and 40 gigabits per second require use of an MX Series router with the 100-Gigabit Ethernet Modular Port Concentrator (MPC) and the 100-Gigabit CFP MIC.**

Options **tunnel–only** (Optional)—For M7i, M10i, M120, M320, T Series and TX Matrix routers with IQ2 PICs and IQ2E PICs, specify that an IQ2 or IQ2E PIC work in tunnel mode only.

The remaining statements are explained separately.

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

Related Documentation

- Example: Configuring Tunnel Interfaces on a Gigabit Ethernet 40-Port DPC
- Example: Configuring Tunnel Interfaces on a 10-Gigabit Ethernet 4-Port DPC
- Example: Configuring Tunnel Interfaces on a 100-Gigabit Ethernet MPC
- bandwidth on page 33
- [edit chassis] Hierarchy Level

uid

Syntax uid *uid-value*;

Hierarchy Level [edit system login user]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Numeric identifier associated with the user account name, either assigned by an administrator or assigned automatically when you commit the user configuration. It is used by applications that request numeric identifiers, such as some RADIUS queries or secure applications such as flow-tap monitoring.

Options ***uid-value***—Number associated with the login account. This value must be unique on the router or switch.

Range: 100 through 64000

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

Related Documentation

- Configuring Junos OS User Accounts

user (Access)

Syntax

```
user username {
  authentication {
  class class-name;
  (encrypted-password "password" | plain-text-password);
  full-name complete-name;
  load-key-file URL filename;
  ssh-dsa “public-key” <from hostname>;
  ssh-rsa “public-key” <from hostname>;
  uid uid-value;
  }
}
```

Hierarchy Level [edit system login]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure access permission for individual users.

Options The remaining statements are explained separately.

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

Related Documentation

- Configuring Junos OS User Accounts
- class on page 34

PART 3

Administration

CHAPTER 6

Reporting Intercept Related Information for Subscriber Secure Policy

Intercept-Related Events Transmitted to the Mediation Device

You can use SNMPv3 traps to report intercept-related events to the mediation device. These events include identifying information for subscribers, such as username or IP address, and subscriber session events, such as login or logout events or mirroring session activation or deactivation. The router sends the events to the mediation device in SNMP traps. Using SNMPv3 provides secure traps that are visible only to authorized individuals on the intended secure mediation device. The traps help support compliance with the Communications Assistance for Law Enforcement Act (CALEA), which defines electronic surveillance guidelines for telecommunications companies.

The supported SNMPv3 traps map to messages defined by the *Lawfully Authorized Electronic Surveillance (LAES) for IP Network Access, American Nation Standard For Telecommunications*. "SNMP Traps for Subscriber Secure Policy LAES Compliance" on page 55 describes the supported SNMPv3 traps and their related LAES messages.

Related Documentation

- Subscriber Secure Policy Overview on page 3
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 21
- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview
- SNMP Traps for Subscriber Secure Policy LAES Compliance on page 55
- Example: SNMPv3 Traps Configuration for Subscriber Secure Policy Mirroring on page 61

SNMP Traps for Subscriber Secure Policy LAES Compliance

Table 9 on page 56 describes the SNMPv3 traps that subscriber secure policy mirroring uses to provide information that maps to messages defined in the *Lawfully Authorized Electronic Surveillance (LAES) for IP Network Access, American National Standard for Telecommunications*. These messages enable subscriber secure policy to comply with

the *Communications Assistance for Law Enforcement Act* (CALEA). The Juniper Packet Mirroring MIB, **jnx-js-packet-mirror.mib**, provides the SNMP trap.

Table 9: Subscriber Secure Policy SNMPv3 Traps for LAES Messages

SNMPv3 Trap	LAES Message	Description
jnxPacketMirrorLiSubscriberLoggedIn	• **access-attempt** (implied) • **access-session-accept** • **packet-data-session-start**	A subscriber, who is identified to have a mirrored service that is activated at login, has successfully logged in.
jnxPacketMirrorSessionLiSubscriberLogInFailed	• **access-attempt** (implied) • **access-failed** (all termination reasons except authentication-reject) • **access-reject** (termination reason is authentication-reject)	A subscriber, who is identified to have a mirrored service that is activated at login, has failed to log in.
jnxPacketMirrorInterfaceLiSubscriberLoggedOut	• **access-session-end** • **packet-data-session-end**	A subscriber, who had an active mirrored service, has logged out.
jnxPacketMirrorInterfaceLiServiceActivated	• **packet-data-session-already-established**	A mirrored session has been activated.
jnxPacketMirrorSessionLiServiceActivationFailed	–	A mirrored session for a subscriber has failed.
jnxPacketMirrorSessionLiServiceDeactivated	–	A mirrored session for an established subscriber has been deactivated.
jnxPacketMirrorMirroringFailure	–	A mirrored service request failed due to an invalid value in the request. Note: This trap is not related to LAES messages.
jnxPacketMirrorTriggerType	–	The type of trigger that caused the mirroring session to be activated.
jnxPacketMirrorCallingStationIdentifier	–	The calling station ID of the subscriber whose traffic is currently being mirrored.
jnxPacketMirrorNasIdentifier	–	The NAS ID of the session in which traffic is being mirrored.
jnxPacketMirrorTargetIPv6Address	–	The IPv6 address of the subscriber interface that is being mirrored.

Related Documentation

- Intercept-Related Events Transmitted to the Mediation Device on page 55
- Example: SNMPv3 Traps Configuration for Subscriber Secure Policy Mirroring on page 61

Configuring SNMPv3 Traps for Subscriber Secure Policy Mirroring

This topic provides an overview of the SNMPv3 configuration process as it pertains to subscriber secure policy. The steps are described in detail in Chapter 7, "Configuring SNMPv3" in the *Junos OS Network Management Configuration Guide*.

To configure SNMPv3 trap support for subscriber secure policy and to send the trap information to the mediation device:

1. Configure the MIB view.

   See Configuring MIB Views.

2. Configure the trap notification and trap notification filter. See the following topics:
   - Configuring the SNMPv3 Trap Notification
   - Configuring the Trap Notification Filter
3. Configure the target device. The target device is the mediation device that receives the trap information.

   See Configuring SNMPv3 Traps on a Device Running Junos OS.

4. Configure the SNMPv3 user, authentication method and password, and privacy method and password. See the following topics:
   - Creating SNMPv3 Users
   - Configuring the SNMPv3 Authentication Type
   - Configuring the Encryption Type
5. Configure user access privileges to management information.

   See Defining Access Privileges for an SNMP Group.

Related Documentation

- Intercept-Related Events Transmitted to the Mediation Device on page 55
- SNMP Traps for Subscriber Secure Policy LAES Compliance on page 55
- Example: SNMPv3 Traps Configuration for Subscriber Secure Policy Mirroring on page 61
- For information about SNMPv3, see the *Junos OS Network Management Configuration Guide*

CHAPTER 7

Terminating Subscriber Secure Policy Traffic Mirroring Sessions

Terminating RADIUS-Initiated Subscriber Traffic Mirroring

You can terminate RADIUS-initiated traffic mirroring sessions by the following action:

- RADIUS CoA message receipt—Terminated upon receipt of a CoA message with the VSA 26-58 (LI-Action) value of 0. The RADIUS administrator configures the LI-Action of 0 in the mirrored subscriber's RADIUS record.

Related Documentation

- RADIUS-Initiated Subscriber Secure Policy Overview on page 5
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 21

CHAPTER 8

Example

Example: SNMPv3 Traps Configuration for Subscriber Secure Policy Mirroring

This example shows an SNMP configuration that provides SNMPv3 trap support.

Configure the SNMPv3 trap support at the **[edit snmp]** hierarchy level.

```
[edit snmp]
view system {
   oid 1.3.6.1.2.1.1 include;
}
view all {
   oid .1 include;
}
v3 {
   notify n1 {
      type trap;
      tag mediation8;
   }
   notify-filter nf1 {
      oid .1 include;
   }
   target-address london-1 {
      address 172.19.87.240; # Address of the mediation device receiving the traps
      port 162;
      tag-list mediation-8;
      target-parameters tp1 {
         parameters {
            message-processing-model v3;
            security-model usm;
            security-level authentication;
            security-name mediation-device1; # Name of the mediation device
         }
         notify-filter nf1;
      }
   }
   usm {
      local-engine {
         user mediation-device1 { # Name of the mediation device
            authentication-md5 {
```

```
            authentication-key
            "yourAuthenticationKey"
          }
          privacy-des {
            privacy-password "yourPrivacyPassword"
          }
        }
      }
    }
    vacm {
      access {
        group london-10 {
          default-context-prefix {
            security-model usm {
              security-level privacy {
                read-view system;
                notify-view all;
              }
            }
          }
        }
      }
      security-to-group {
        security-model usm {
          security-name mediation-device1 { # Name of the mediation device
            group london-10;
          }
        }
      }
    }
  }
```

Related Documentation

- Subscriber Secure Policy Overview on page 3
- Configuring SNMPv3 Traps for Subscriber Secure Policy Mirroring on page 57
- For information about SNMPv3, see the *Junos OS Network Management Configuration Guide*

PART 4

Troubleshooting

CHAPTER 9

Acquiring Troubleshooting Information

Collecting Subscriber Access Logs Before Contacting Juniper Technical Support

Problem When you experience a subscriber access problem in your network, we recommend that you collect certain logs before you contact Juniper Technical Support. This topic shows you the most useful logs for a variety of network implementations. In addition to the relevant log information, you must also collect standard troubleshooting information and send it to Juniper Technical Support in your request for assistance.

Solution To collect standard troubleshooting information:

- Redirect the command output to a file.

  user@host> **request support information | save rsi-1**

To configure logging to assist Juniper Technical Support:

1. Review the following blocks of statements to determine which apply to your configuration.
2. Copy the relevant statements into a text file and modify the log filenames as you want.
3. Copy the statements from the text file and paste them into the CLI on your router to configure logging.
4. Commit the logging configuration to begin collecting information.

NOTE: The maximum file size for DHCP local server and DHCP relay log files is 1 GB. The maximum number of log files for DHCP local server and DHCP relay is 1000.

BEST PRACTICE: Enable these logs only to collect information when troubleshooting specific problems. Enabling these logs during normal operations can result in reduced system performance.

```
[edit]
set system syslog archive size 100m files 25

set system auto-configuration traceoptions file filename
set system auto-configuration traceoptions file filename size 100m files 25

set protocols ppp-service traceoptions file filename size 100m files 25
set protocols ppp-service traceoptions level all
set protocols ppp-service traceoptions flag all

set protocols ppp traceoptions file filename size 100m files 25
set protocols ppp traceoptions level all
set protocols ppp traceoptions flag all
set protocols ppp monitor-session all

set interfaces pp0 traceoptions flag all

set demux traceoptions file filename size 100m files 25
set demux traceoptions level all
set demux traceoptions flag all

set system processes dhcp-service traceoptions file filename
set system processes dhcp-service traceoptions file size 100m
set system processes dhcp-service traceoptions file files 25
set system processes dhcp-service traceoptions flag all

set class-of-service traceoptions file filename
set class-of-service traceoptions file size 100m
set class-of-service traceoptions flag all
set class-of-service traceoptions file files 25

set routing-options traceoptions file filename
set routing-options traceoptions file size 100m
set routing-options traceoptions flag all
set routing-options traceoptions file files 25

set interfaces traceoptions file filename
set interfaces traceoptions file size 100m
set interfaces traceoptions flag all
set interfaces traceoptions file files 25

set system processes general-authentication-service traceoptions file filename
set system processes general-authentication-service traceoptions file size 100m
set system processes general-authentication-service traceoptions flag all
set system processes general-authentication-service traceoptions file files 25
```

PART 5

Index

Index

T

U