

Subscriber Secure Policy Traffic Mirroring Architecture

This topic describes the subscriber secure policy architecture and includes a description of how mirrored traffic flows within the subscriber secure policy environment.

Figure 1 illustrates the subscriber secure policy mirroring environment. The Juniper Networks router, functioning as an intercept access point, is the center piece of the subscriber secure policy architecture. The figure indicates the sequence of events that are performed to configure mirroring operations and the traffic flow that occurs during mirroring. The tables after the figure describe the events indicated by the figure. Table 1 describes the configuration sequence. Table 2 and Table 3 describe the sequence of events that occur during mirroring operations.



NOTE: A special UDP/IP header is prepended to each mirrored packet sent to the mediation device. The prepended header is used as a demultiplexer, enabling the mediation device to differentiate the multiple mirrored streams that arrive from different sources.

Figure 1: Subscriber Secure Policy Architecture

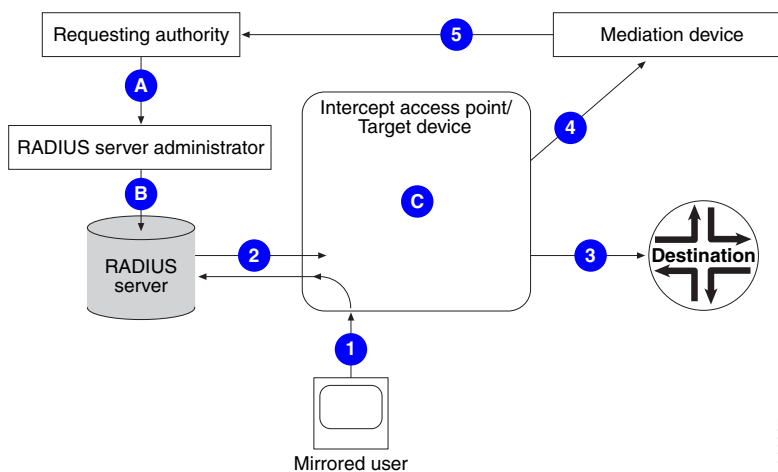


Table 1 lists the high-level steps that are required to configure the subscriber secure policy traffic mirroring environment.

Table 1: Subscriber Secure Policy Configuration Steps

Step	Description
A	An authorized individual or group requests traffic mirroring. This group also ensures that the mediation device is configured to receive and analyze mirrored traffic.
B	The RADIUS server administrator configures the subscriber RADIUS record to include the mirroring-related RADIUS attributes and VSAs.

Table 1: Subscriber Secure Policy Configuration Steps (continued)

Step	Description
C	The Juniper Networks router administrator configures the subscriber secure policy service on the router, including the flow-tap service configuration, RADIUS server information, and mediation device information.

Table 2 shows the process for a subscriber login mirroring operation, which is initiated when the mirrored subscriber logs in.

Table 2: RADIUS-Initiated Mirroring at Subscriber Login

Step	Description
1	The subscriber logs in, requesting authentication by the RADIUS server.
2	<ul style="list-style-type: none"> ■ The RADIUS server authenticates the subscriber and sends an Access-Accept message containing the mirroring-related RADIUS attributes and VSAs to the router (intercept access point). ■ The mirroring trigger in the RADIUS Access-Accept message initiates the mirroring operation. ■ The intercept access point creates the subscriber secure policy based on the mirroring VSAs and begins mirroring the subscriber's traffic.
3	The intercept access point sends the original subscriber traffic to its intended destination.
4	The intercept access point sends the mirrored subscriber traffic to the mediation device.
5	The mediation device provides information about the mirrored traffic to the requesting authority.

Table 3 shows the mirroring procedure for an in-session mirroring operation, in which the subscriber is already logged in.

Table 3: RADIUS-Initiated Mirroring for Current Subscriber

Step	Description
1	The subscriber logs in, requesting authentication by the RADIUS server. The RADIUS server authenticates the subscriber (no mirroring activity occurs).
2	<ul style="list-style-type: none"> ■ Subscriber-based mirroring is later requested by the requesting authority and then enabled on the RADIUS server. ■ The RADIUS server sends a CoA message containing the mirroring-related RADIUS attributes and VSAs to the router (intercept access point). ■ The mirroring trigger in the RADIUS CoA message initiates the mirroring operation. ■ The intercept access point creates the subscriber secure policy based on the mirroring VSAs and immediately begins mirroring subscriber traffic.

Table 3: RADIUS-Initiated Mirroring for Current Subscriber *(continued)*

Step	Description
3	The intercept access point sends the original subscriber traffic to its intended destination.
4	The intercept access point sends the mirrored subscriber traffic to the mediation device.
5	The mediation device provides information about the mirrored traffic to the requesting authority.

- Related Topics**
- Subscriber Secure Policy Overview
 - RADIUS Attributes Used for Subscriber Secure Policy
 - Configuring Subscriber Secure Policy Mirroring Overview

Published: 2009-07-16