Configuring Subscriber Secure Policy Mirroring Overview

You can configure subscriber secure policy mirroring to mirror the traffic of a particular subscriber.

NOTE: Subscriber secure policy RADIUS-initiated mirroring runs on the flow-tap service infrastructure. To configure the subscriber secure policy service, you must have the same privileges that are required to configure the flow-tap service.

To configure the subscriber secure policy service:

1. Configure the flow-tap service.

   See the *JUNOS Services Interfaces Configuration Guide* for information about configuring the flow-tap service.

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

   See Configuring Flow-Tap Service Support for Subscriber Secure Policy Mirroring.

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.

   See Using RADIUS Dynamic Requests for Subscriber Access Management.

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 for descriptions of the supported attributes used in RADIUS Accept-Accept and CoA messages.
   - The content destination device must be configured to accept the mirrored data from the mediation device.

   The descriptions of these configurations are beyond the scope of this document.

5. You can terminate an active subscriber mirroring session at any time. See Terminating Subscriber Secure Policy Mirroring Sessions.

NOTE: The subscriber secure policy feature requires some system resources while mirroring, encrypting, and sending traffic to the mediation device. We recommend that you consider this requirement when you configure subscriber secure policy. For example, you might elect to use a 10-Gigabit Ethernet interface for the tunnel and mediation device if you expect the amount of traffic you plan to mirror to approach 1 Gps of actual user data.

Related Topics

- RADIUS Attributes Used for Subscriber Secure Policy
- Terminating Subscriber Secure Policy Mirroring Sessions

Published: 2009-07-16