Configuring Flow-Tap Service Support for Subscriber Secure Policy Mirroring

The RADIUS-initiated mirroring provided by the subscriber secure policy service runs on the flow-tap service infrastructure. This topic describes the steps to enable flow-tap support for subscriber secure policy mirroring.

NOTE: 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 flow-tap service to support subscriber secure policy mirroring:

1. Configure the standard flow-tap service.

   ```
   [edit services]
   user@host# set flow-tap interface sp-1/2/0.100
   ```

   See "Flow-Tap Configuration Guidelines" in the *JUNOS Services Interfaces Configuration Guide* for details on configuring the flow-tap service.

2. Allocate a pool of tunnel interfaces that the flow-tap service can use for subscriber secure policy mirroring. The intercept access point uses these interfaces to send mirrored traffic to the mediation device. The intercept access point equally distributes the mirrored traffic across the available tunnel interfaces.

   You can configure a maximum of 2048 mirrored subscriber sessions per chassis.

   ```
   [edit chassis]
   user@host#  set fpc 4 pic 1 tunnel-services bandwidth 1g
   ```

3. Configure the tunnel interfaces.

   ```
   [edit interfaces]
   user@host# set vt-4/1/10.0
   user@host# set vt-4/2/10.0
   ```

4. Assign the tunnel interfaces that the flow-tap service uses for RADIUS-initiated subscriber secure policy mirroring.

NOTE: If a currently used tunnel interface is deleted from the pool of interfaces, the subscriber secure policy service redistributes the active mirroring sessions 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 available interfaces—the new interface is used for new mirroring sessions or for existing sessions transferred from a failed interface.

```
[edit services]
user@host# set radius-flow-tap interfaces vt-4/1/10.0
user@host# set radius-flow-tap interfaces vt-4/2/10.0
```

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

   ```
   [edit services]
   user@host# set radius-flow-tap source-ipv4-address 192.168.100.33
   ```

6. (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, the 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]
   user@host# set radius-flow-tap forwarding-class best-effort
   ```

Related Topics

- Subscriber Secure Policy Overview
- Configuring Subscriber Secure Policy Mirroring Overview
- Guidelines for Configuring Subscriber Secure Policy Mirroring on the Flow-Tap Service

---

Published: 2009-07-16