Subscriber Secure Policy Overview

Subscriber secure policy provides RADIUS-initiated traffic mirroring on a per-subscriber basis. RADIUS-initiated mirroring creates secure policies based on certain RADIUS VSAs and uses RADIUS attributes to identify the subscriber whose traffic is to be mirrored. The traffic mirroring operation is triggered by the attributes received in RADIUS messages. Both the subscriber's 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.

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

- Subscriber log in—The mirroring operation starts when the subscriber logs in and the trigger is received 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—The mirroring operation starts when the trigger is received in a RADIUS Change-of-Authorization-Request (CoA-Request) message. Using triggers in CoA messages enables you to immediately mirror traffic of a subscriber who is already logged in.

Configuration of RADIUS-based mirroring is independent of the actual mirroring session—you can configure the mirroring parameters at any time. Also, you can use a single RADIUS 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. The actual mirroring operation is transparent to subscribers whose traffic is being mirrored.

Traffic mirroring has many uses, such as debugging network problems, troubleshooting specific user issues, and lawful intercept. For example, you might use RADIUS-based mirroring when debugging network problems related to mobile users, who do not always log in to the same router. RADIUS-based mirroring is particularly useful for large networks, in which you can use a single RADIUS server to provision the mirroring operation.

Subscriber Secure Policy Terms

Table 1 defines terms that are used in the discussion of subscriber secure policy.

Table 1: Subscriber Secure Policy Terms

Term	Definition
Flow-tap service	The application that extends the Dynamic Tasking Control Protocol (DTCP) for active traffic monitoring. The subscriber secure policy service runs on top of the flow-tap service.

Table 1: Subscriber Secure Policy Terms *(continued)*

Term	Definition
Intercept access point	Device that requests and configures the subscriber secure policy service. The Juniper Networks router performs this function.
Mediation device	Location to which the mirrored traffic is sent. Also called an analyzer device.
Mirrored subscriber	Subscriber whose traffic is mirrored.
Mirror trigger	RADIUS attribute that identifies a subscriber whose traffic is to be mirrored. Mirroring starts when the trigger is detected.
Requesting authority	Authorized group that requests or conducts traffic mirroring.
Salt encryption	Random string of data used to modify a password hash. The mirroring VSAs sent to the router by the RADIUS server are Salt-encrypted.
Target system	The system on which the subscriber secure policy service (and flow-tap service) is configured.

Related Topics

- Subscriber Secure Policy Traffic Mirroring Architecture
- RADIUS Attributes Used for Subscriber Secure Policy
- Configuring Subscriber Secure Policy Mirroring Overview
- Subscriber Secure Policy Licensing Requirements