

## Overview of Configuring and Deploying the SRC-TMP

---

The SRC-TMP provided with the SRC software is designed to be used with the threat mitigation implementation in the sample data.

### ***Using the NIC Resolver for the SRC-TMP***

The Threat Mitigation Application pushes policies to the interfaces from which the problem traffic enters the network. To do so, the SRC-TMP must be able to map from a given attack source IP address to the SAEs managing the interfaces on the routers where that traffic enters the network. The Threat Mitigation Application uses the network information collector (NIC) to perform this mapping. Each service activation interface uses a different NIC configuration.

For information about the NIC configuration for each interface, see:

- JUNOS provider edge interface—“Configuring the NIC for Provider Edge Interfaces” on page 1
- JUNOS forwarding interface—“Configuring the NIC for Forwarding Interfaces” on page 1
- JUNOS subscriber interface—“Configuring the NIC for Subscriber Interfaces” on page 2

For more information about configuring the service activation interface, see *Configuring the Threat Mitigation Application*.

### ***Configuring the NIC for Provider Edge Interfaces***

To configure the NIC to map the source IP address for a given attack to the SAEs managing the JUNOS subscriber-facing interfaces, use the `OnePopStaticRouteIp` configuration scenario and restart the NIC host. The `OnePopStaticRouteIp` configuration scenario resolves an assigned IP address for a subscriber whose traffic enters the network through an interface on a JUNOS routing platform to a reference for the SAE that manages the interface. The realm for this configuration accommodates the situation in which the network publisher component gathers interface information for the JUNOS routing platforms. The resolution process takes a subscriber’s IP address as a key and returns a reference to the SAE that manages the interface. For information about the NIC, see *Locating Subscriber Management Information*.

For information about associating an existing address pool with an interface, see *Updating Information About Address Pools*.

### ***Configuring the NIC for Forwarding Interfaces***

To configure the NIC to map the source IP address for a given attack to the SAEs managing the JUNOS forwarding interfaces, use the `OnePop` configuration scenario and restart the NIC host. The realm for the `OnePop` configuration scenario accommodates the situation in which IP address pools are configured locally on each VR. The resolution process takes a subscriber’s IP address as the key and returns a

reference to the SAE managing this subscriber as the value. For information about configuring the NIC, see [Configuring the NIC \(SRC CLI\)](#).

## **Configuring the NIC for Subscriber Interfaces**

To configure the NIC to map the source IP address for a given attack to the SAEs managing the JUNOS subscriber interfaces, use the OnePopAllRealms configuration scenario and restart the NIC host. The realm for the OnePopAllRealms configuration scenario accommodates the situations in which IP address pools are configured locally on each VR or IP address pools are shared by VRs in the same POP. The resolution process takes a subscriber's IP address as the key and returns a reference to the SAE managing this subscriber as the value. For information about configuring the NIC, see [Configuring the NIC \(SRC CLI\)](#).

If the IP address pools are shared across multiple VRs, you must also configure an external plug-in for the SAE plug-in agent in the NIC host as follows:

```
Plugin.nic.objectref=corbaname::<host>:<port>/NameService#nicsae/saePort
```

- <host > is the name or IP address of the COS name server
- <port > is the TCP port

For information about configuring the SAE for external plug-ins, see [Configuring the SAE for External Plug-Ins](#).

### **Related Topics**

- [Overview of the SRC-TMP](#)
- [Accessing the SRC-TMP](#)
- [Deploying the Threat Mitigation Application](#)