

Chapter 4

Overview of IDP Integration

This chapter provides overview information about integration of Juniper Networks Intrusion Detection and Prevention (IDP) system with the SRC software. Topics include:

- Overview of IDP Integration on page 43
- Before You Integrate IDP into an SRC Environment on page 44
- Example: Integrating IDP into an SRC Environment on page 45
- Directing Subscriber Traffic to IDP for Monitoring on page 47
- Integrating IDP into an SRC Environment on page 49

Overview of IDP Integration

IDP monitors network traffic to detect potentially detrimental traffic and responds to problem incidents to prevent damage to the network. By integrating IDP into an SRC-managed environment, you can use SRC extensions that support IDP to:

- Monitor subscriber traffic.
- Take actions for subscribers who are sending or receiving traffic that behaves in a detrimental manner on the network by:
 - Redirecting a subscriber's Web requests to a Web page that provides information about the nature of the problem traffic
 - Sending e-mail to a subscriber to provide information about the problem
 - Applying policies to the subscriber interface to manage subscriber traffic, such as applying policies that reduce the amount of bandwidth available to the subscriber to limit traffic sent to and received from the subscriber

You can deploy IDP in a network to monitor all traffic, or you can configure the SRC software to direct subsets of subscriber traffic to IDP for monitoring.

The Surveillance Director is the component that manages the process of selecting subscriber traffic to be monitored and activating SRC services to direct specified traffic to an IDP sensor (IDP hardware appliances that run the IDP sensor software). It divides subscribers into groups, then directs traffic for one group at a time through IDP. This means that IDP monitors different groups of traffic at different times, and that traffic for SRC-managed subscribers is periodically monitored. The Surveillance Director relies on SRC services to policy-route traffic from JUNOS routers or to mirror traffic from JUNOS routing platforms to the IDP sensor.

Before You Integrate IDP into an SRC Environment

Integrating IDP into an SRC-managed environment requires:

- The UMCidp package installed with your SRC application library software.
- SRC-managed JUNOS routers or SRC-managed JUNOS routers and JUNOS routing platforms in the network.



NOTE: If you want to integrate IDP into an SRC-managed network that manages enterprise subscribers from a JUNOS routing platform as a subscriber access router, contact Juniper Networks Professional Services for assistance.

- Subscriber IP addresses assigned from an IP pool that is defined in the virtual router entry in the directory

Typically, IP addresses are assigned from an IP pool for residential subscribers. For enterprise subscribers or for subscribers who use a static IP address, make sure that the IP addresses are allocated from the IP pool that is defined in the virtual router entry in the directory.

- Working knowledge of aggregate services. See *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.
- Working knowledge of the IDP software, including IDP Manager, and familiarity with IDP documentation. See

<http://www.juniper.net/techpubs/software/management/idp/>

Before you extend IDP traffic monitoring to SRC subscriber traffic, you typically:

- Install the IDP sensors. The sensors monitor network traffic to detect suspicious or anomalous traffic and respond as configured.
- We recommend that IDP sensors, or sensor clusters, be one hop from all the routers in the network for which the sensor monitors traffic. (Recommended) Deploy IDP as an active gateway. In instances in which traffic is copied to an IDP sensor, ensure that IDP routes the traffic to a null interface so that the traffic is not forwarded.
- Configure IDP rules for the type of traffic incidents to report.

Example: Integrating IDP into an SRC Environment

The SRC application library provides a robust sample implementation for integrating IDP into an SRC-managed network. It illustrates configurations for a network that contains only JUNOSe routers, and for a network that contains JUNOSe routers as subscriber access routers with JUNOS routing platforms as core routers.

You can also customize the sample data and applications to integrate IDP into your network, or you can use the samples as a guide to create your own implementation.

For a full configuration example, see the *IDP.xml* file in the SAE folder in SDX Configuration Editor.

Sample Network Topologies

Figure 7 shows the network topology that serves as the basis for the configuration in the sample data for a network that contains only JUNOSe routers.

Figure 7: Sample Network Topology with a JUNOSe Router

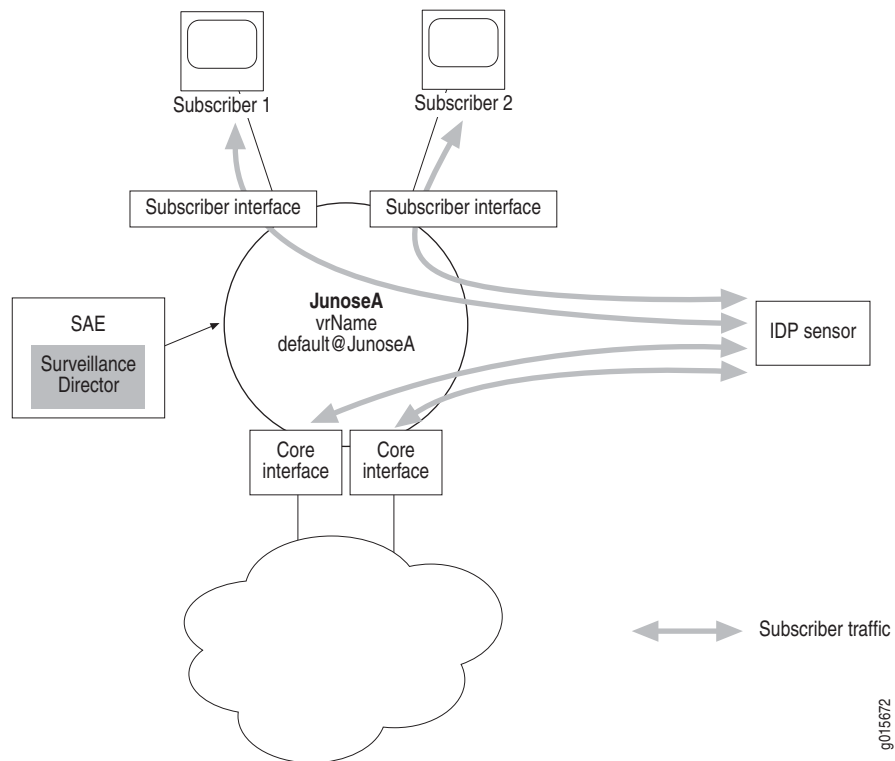
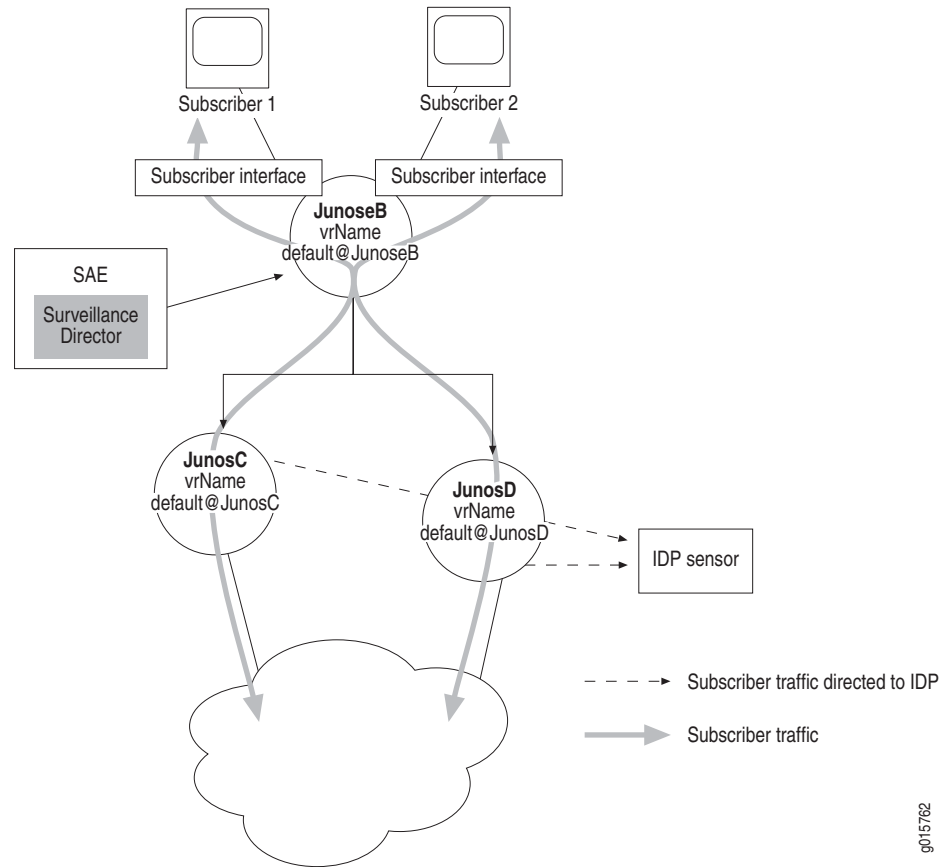


Figure 8 shows the network topology that serves as the basis for the configuration in the sample data for a network that contains JUNOSE routers and JUNOS routing platforms.

Figure 8: Sample Network Topology with a JUNOSE Router and JUNOS Routing Platforms



g015762

Components in Sample Data

The sample implementation includes:

- Policies, services, router definitions, and SAE configurations in the sample data. Sample entries for IDP integration have the prefix IDP

For information about installing sample data, see *Chapter 1, Installing the Sample SRC Applications*.

- IDP captive portal application (a Web page that receives redirected HTTP requests in response to a problem detected by IDP) with policies and services to limit bandwidth and direct Web requests to the sample portal
- IDP E-Mailer application
- Script to enable subscriber actions from IDP Manager

You can use the sample data and applications to create a demonstration implementation. The IDP router definitions, identified as IDP <routername> in the sample data, can be configured to act as simulated routers for a demonstration environment. For information about setting up a simulated router, see *SRC-PE Monitoring and Troubleshooting Guide, Chapter 6, Configuring a Simulated Router Driver for Testing with the SRC CLI*.

The sample data uses the following terminology:

- Subscriber-facing router—Subscriber access router
- Core-facing router—Router that transmits subscriber traffic to the network core

Directing Subscriber Traffic to IDP for Monitoring

You can direct all traffic to IDP by placing an IDP sensor in the network paths through which all incoming and outgoing subscriber traffic passes. In this case, you do not need to configure the SRC software to direct subscriber traffic to an IDP sensor.

If you do plan to direct subsets of subscriber traffic to an IDP sensor, how you do so depends on your network configuration. Table 7 lists ways in which you route subscriber traffic to an IDP sensor.

Table 7: Network Configuration and Forwarding Method

For This Network Configuration	Use This Method to Forward Subscriber Traffic
JUNOSe routers as subscriber access routers No JUNOS routing platforms as core routers	Policy-based routing from the JUNOSe router
JUNOSe routers as subscriber access routers and JUNOS routing platforms as core routers	Mirroring from the JUNOS routing platform



NOTE: Use mirroring from JUNOS routing platform(s) if you are sure that most, or all, of the subscriber traffic traverses those routers. When you mirror traffic to IDP, IDP monitors only the subscriber traffic that traverses a JUNOS routing platform.

For policy-based routing from JUNOSe routers, a service is activated on subscriber interfaces for each subscriber IP address, and on each core interface. For mirroring on JUNOS routing platforms, a service is activated only one time for a router or for a set of routers. If your configuration includes a JUNOS routing platform, we recommend that you use mirroring to direct subscriber traffic to IDP.

Surveillance Director

The Surveillance Director manages how to direct subscriber traffic to an IDP sensor. It queries the directory for IP pools associated with specified virtual routers and generates classless interdomain routing (CIDR) subnets that include only the set of IP addresses that are assigned to subscribers. You can configure the number of IP addresses to be included in a CIDR subnet. The Surveillance Director uses CIDR subnets because routers can efficiently handle these subnets to match policy rules.

For each CIDR subnet, the Surveillance Director activates a specified aggregate service, and then the aggregate service activates its fragment services to route traffic to an IDP sensor. The configuration for the fragment services determines whether it policy-routes or mirrors traffic.

Table 8 describes the types of fragment services to configure in an aggregate service, and shows where the fragment services are activated. For general information about aggregate services and fragment services, see *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.

Table 8: Types of Fragment Services in an Aggregate Service

Fragment Services	Policy	Where Fragment Service Is Activated
Policy-Based Routing		
Subscriber-interface fragment	Routes traffic sent by a subscriber to an IDP sensor	JUNOSe routers
Core-interface fragment	Routes traffic destined for a subscriber to an IDP sensor	JUNOSe routers
Mirroring		
Router (forwarding)-interface fragment	Mirrors traffic to an IDP sensor	JUNOS routing platforms that transmit subscriber traffic

Traffic for one group of CIDR subnets at a time is sent to an IDP sensor for monitoring. You can configure the length of the interval during which to monitor traffic from CIDR subnet; all traffic for subscribers with IP addresses within the CIDR subnet is monitored during a specified monitoring interval.

The Surveillance Director provides subscriber IDs in the form of a distinguished name (DN) to locate the subscriber session in which to activate a service. The DN is used to locate the SAE that manages the subscriber session in which the aggregate service is activated.

Router and Interface Subscriber Sessions

In addition to the typical subscriber sessions used to activate services, the services to support IDP integration require special subscriber sessions to host:

- An aggregate service
- Core interface fragment services if traffic is policy-routed to an IDP sensor
- Router fragment services if traffic is mirrored to an IDP sensor

Subscriber Session to Host an Aggregate Service

On a JUNOSe router, a router subscriber session hosts an aggregate service. In these cases, a subscriber profile must have a name in the form `<vrName> @ <routerName>`. The `<vrName>` and `<routerName>` must correspond to virtual router names and routers names of objects under `o = Networks`, `o = umc` in the directory.

Subscriber Session to Host a Core Interface Fragment Service

On a JUNOSe router, a subscriber session is needed to activate a core interface fragment service that policy-routes traffic to the IDP sensor. All core routing interfaces use a single shared subscriber object in the directory.

Subscriber Session to Host a Router Interface Fragment Service

On a JUNOS routing platform, a router subscriber session is used to activate the fragment service that mirrors traffic to the IDP sensor. We recommend that the router subscriber profile have a name in the form `<vrName> @ <routerName>`. The router subscriber session must be associated with the forwarding interface that the SRC software creates.

Integrating IDP into an SRC Environment

How you integrate IDP into your SRC environment depends on whether or not you direct all traffic to an IDP sensor. If you direct all traffic to an IDP sensor by placing an IDP sensor in the network paths through which all incoming and outgoing subscriber traffic passes, you do not need to configure services and subscriptions to director traffic to a sensor, and do not need to monitor subsets of traffic. In this case, you can skip Steps 1 and 2 in the following procedure.

To integrate IDP into an SRC environment:

1. Configure services to direct traffic to IDP.
See Chapter 5, Configuring Services and Subscriptions to Integrate IDP.
2. Configure Surveillance Director to monitor groups of subscriber traffic.
See Chapter 7, Monitoring Subsets of Subscriber Traffic.
3. Configure actions to be taken for traffic that IDP identifies as malicious.
See Chapter 8, Defining Actions to Be Taken for Subscriber Traffic.

4. (Optional) Create an application, such as one to send e-mail notification to a subscriber about problem traffic that have sent or received.

We provide a sample application to send an e-mail notification to a subscriber about the problem. See *Chapter 6, Sending E-Mail to Subscribers*.

5. Create an SRC script for IDP Manager to complete the IDP integration with the SRC software.

See *Chapter 9, Enabling SRC Actions from IDP Manager*.