

Chapter 24

Adding VPNs from JUNOS Routing Platforms

This chapter describes how to manage virtual private networks (VPNs) in the directory and contains the following sections:

- Overview of VPNs in the SRC Network on page 405
- Implementing a Routing Scheme for VPNs on page 406
- Configuring VPNs to Integrate into an SRC Network on page 406
- Modifying VPNs on page 408
- Adding Extranet Clients to VPNs on page 409
- Removing Extranet Clients on page 411
- Locating and Removing Inactive Subscriptions to a VPN on page 411
- Deleting VPNs from the Directory on page 412

Overview of VPNs in the SRC Network

For SRC configurations that support JUNOS routers, retailers and enterprises can support one or more VPNs. A VPN is an object in the directory that represents a virtual private network in an organization and has the object class `umcVpn`, which can be subordinate to the object classes `umcRetailer` and `umcEnterprise`.

For information about the object classes and their associated attributes, see the LDAP schema in the SRC software distribution in the folder *SDK/doc/ldap* or on the Juniper Networks Web site at

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

Implementing a Routing Scheme for VPNs

You must configure a routing scheme in the VPN that ensures that all members in the VPN can reach other and that does not require changes as members are added to and removed from the VPN. If a VPN is used as an intranet, you can achieve this goal by configuring static routes in the VPN or by configuring routing protocols appropriately.

If, however, the VPN is exported as an extranet, some members of the VPN may use private or conflicting address schemes. In addition, if the VPN has a large number of potential members, configuring static routing or routing protocols for all potential members may not be a manageable proposition. In these last two cases, we recommend that you use public addresses in the VPN and have VPN members implement NAT for traffic destined for the VPN (see *Overview of Services for Enterprise Manager Portal* on page 375).

VPNs use private IP addresses. If, however, enterprises that you administer export VPNs to extranet clients, you must ensure that the extranet clients can reach the IP addresses that the VPNs use. To implement an address scheme that allows all subscribers who have access to a VPN, we recommend that you implement NAT on the JUNOS routing platform. IT managers in the retailers and enterprises who own the VPNs can then map private IP addresses in the VPNs to public IP addresses, which extranet clients can reach.

Configuring VPNs to Integrate into an SRC Network

The administrator of a retailer can add and modify VPNs with an LDAP client, a data integrator, or SDX Admin. IT managers with the appropriate privileges can modify VPN properties through Enterprise Manager Portal.

For information about managing VPNs through Enterprise Manager Portal, see *Chapter 29, Managing Services with Enterprise Manager Portal*.

For information about managing VPNs from the SRC CLI, see *Chapter 23, Adding VPNs from JUNOS Routing Platforms with the SRC CLI*.

Adding VPNs with a Data Integrator

You can develop a data integrator that reads data from a storage medium, such as a database or a directory that does not use the SRC LDAP schema and that writes the data to the directory in a format that complies with the LDAP schema.

We provide a sample data integrator, VPN Directory Updater, which reads data about VPNs from a database and writes the data to a directory. If you want to use this data integrator, you need to understand how it works, and customize it for your specific application.

For information about data integrators and VPN Directory Updater, see *SRC-PE Integration Guide, Chapter 9, Integrating Data with the LDAP Directory*.

Adding VPNs with SDX Admin

To use SDX Admin add a VPN:

1. In the navigation pane, right-click the retailer or enterprise to which you want to add the new VPN, and select **New > VPN**.

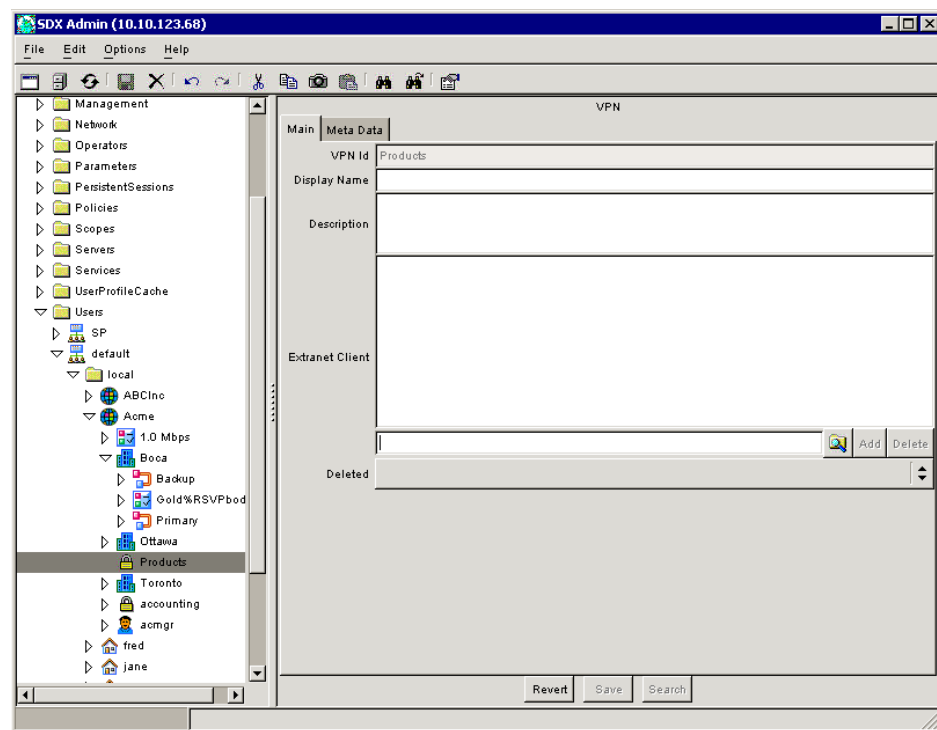
The New VPN dialog box appears.

2. Enter the names of the routing instances, as defined on the JUNOS routing platform, that implement the VPN in the network, and click **OK**.

For more information about routing instances and JUNOS routing platforms, see the JUNOS Internet Software documentation.

An object for the new VPN appears in the navigation pane, and the Main tab of the VPN pane appears.

Figure 29: VPN Pane



3. Edit or accept the default values for the VPN fields.

See *VPN Fields* on page 408.

4. Click **Save**.

VPN Fields

In SDX Admin, you can modify the following fields in the content pane for a VPN (*retailername* = <retailer name>, *o* = *Users*, *o* = *umc* or *enterprisename* = <enterprise name>, *ou* = <foldername>, *retailername* = <retailer name>, *o* = *Users*, *o* = *umc*).

Display Name

- Name of the VPN that appears in other SRC components, such as the Enterprise Manager Portal.
- Value—Text string
- Default—No value
- Example—Products VPN

Description

- Description of the VPN.
- Value—Text string
- Default—No value
- Example—VPN for sales representatives

Extranet Client

- Extranet client for this VPN.
- Value—Retailer or enterprise
- Default—No value
- Guidelines —For information about completing this field, see *Adding Extranet Clients to VPNs* on page 409.

Deleted

- Availability of this entry to other SRC components connected to the directory.
- Value—Blank or True or False
 - Blank—Other SRC components can access this entry in the directory.
 - True—Other SRC components cannot use this entry in the directory, although the object still exists.
 - False—Other SRC components can access this entry in the directory.
- Default—Blank

Modifying VPNs

IT managers with the appropriate permissions can display names and modify the descriptions of VPNs through the Enterprise Manager portal. Service providers can modify VPNs with an LDAP client or SDX Admin.

Adding Extranet Clients to VPNs

Retailers and enterprises can be extranet clients. Service providers can add extranet clients to VPNs with an LDAP client or SDX Admin. IT managers add extranet clients to their VPNs through Enterprise Manager Portal.

For information about adding extranet clients through Enterprise Manager Portal, see *Chapter 29, Managing Services with Enterprise Manager Portal*.

Two LDAP attributes specify information about extranet clients:

- The object classes `umcRetailer` and `umcEnterprise` have an LDAP attribute called `ImportedExtranet` that defines the DNSs of the imported VPNs.
- The object class `umcVPN` has an attribute called `extranetClient` that defines the DNSs of extranet clients of the VPN.

To use SDX Admin to add an extranet client:

1. In the navigation pane, select the VPN you want to export to the extranet client.

The VPN pane appears (see Figure 29 on page 407).

2. Click the magnifying glass below the Extranet Client field.

The Select Object dialog box appears and displays a list of subscribers.

3. Navigate to the retailer or enterprise who will be the extranet client.

- To navigate to a subordinate subscriber, double-click on a subscriber in the list.
- To navigate to a subscriber at a higher level in the directory, use the menu at the top of the Select Object dialog box.
- To select multiple options, shift-click or control-click the subscribers.

4. Click **OK**.

The extranet clients appear in the VPN pane.

5. Click **Add**.

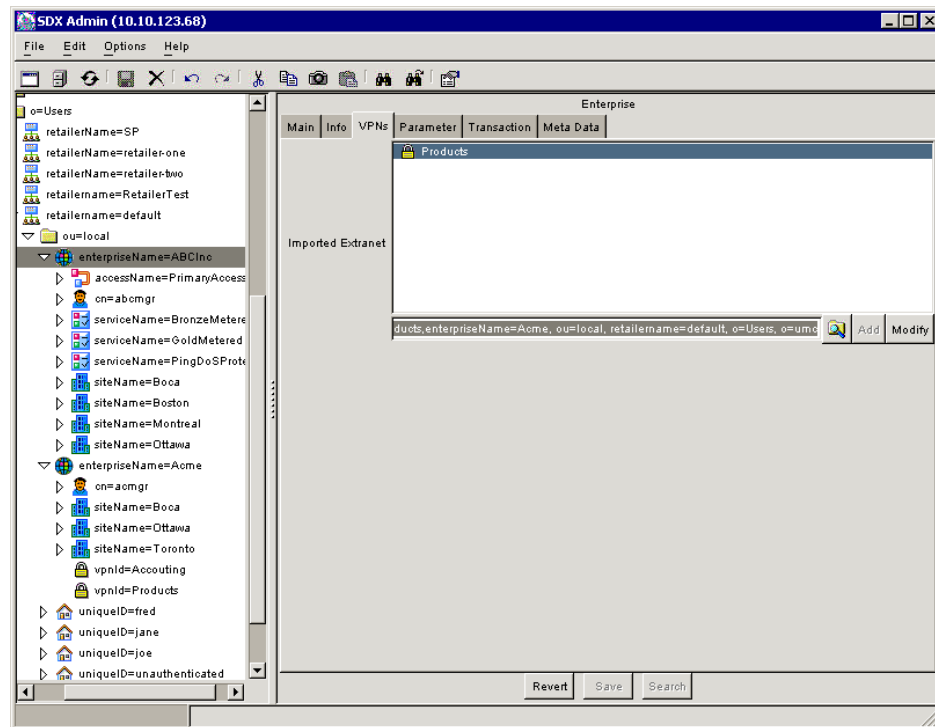
The extranet clients appear in the Extranet Client field of the VPN pane.

6. Click **Save** in the VPN pane.

7. In the navigation pane, highlight the subscriber for whom you want to import the VPN.

The subscriber's pane appears.

8. Click the **VPNs** tab for this subscriber.

Figure 30: Enterprise Pane

9. Click the magnifying glass below the Imported Extranet field.

The Select Object dialog box appears and displays a list of subscribers.

10. Navigate to the VPN you want to import.

- To navigate to a subordinate VPN, double-click on a subscriber in the list.
- To navigate to a VPN at a higher level in the directory, use the menu at the top of the Select Object dialog box.
- To select multiple options, shift-click or control-click the subscribers.

11. Click **OK**.

The VPN appears in the subscriber's pane.

12. Click **Add**.

The VPN appears in the Extranet Client field of the subscriber's pane.

13. Click **Save** in the subscriber's pane.

Removing Extranet Clients

Service providers can remove extranet clients to VPNs with an LDAP client or SDX Admin. IT managers can remove extranet clients through Enterprise Manager Portal.

For information about removing extranet clients with Enterprise Manager Portal, see *Chapter 29, Managing Services with Enterprise Manager Portal*.

To use SDX Admin to remove an extranet client:

1. In the navigation pane, select the subscriber who is the extranet client.
2. Click the VPN tab for this subscriber.

The subscriber's pane appears (for example, see Figure 30 on page 410).

3. Right-click the VPN in the Imported Extranet field, and select **Delete**.
4. Click **Save** in the subscriber's pane.
5. In the navigation pane, select the VPN.

The VPN pane (see Figure 29 on page 407) appears.

6. Right-click the extranet client in the Extranet Client field, and select **Delete**.
7. Click **Save** in the VPNs pane.

Locating and Removing Inactive Subscriptions to a VPN

When an IT manager cancels the export of a VPN, the Enterprise Manager Portal automatically deactivates any active subscriptions to that VPN for the associated extranet client. If an IT manager cancels the export of a VPN at the same time that the extranet client activates a subscription to this VPN, there is a remote possibility that the Enterprise Manager portal will maintain the active subscription.

We recommend that you periodically check for and deactivate these types of invalid subscriptions to prevent this type of invalid subscription. We provide a data integrator, VPN Subscription Deactivator, for this purpose. This data integrator works with the Enterprise Service Portal audit plug-in. For more information on data integrators and VPN Subscription Deactivator, see *SRC-PE Integration Guide, Chapter 9, Integrating Data with the LDAP Directory*.

To use this data integrator:

1. Install and configure the Enterprise Service Portal audit plug-in with the Enterprise Manager portal (see *Chapter 27, Installing and Configuring Enterprise Service Portals*).
2. Install the Data Integration package (see *SRC-PE Getting Started Guide, Chapter 28, Installing the SRC Software on a Solaris Platform*).
3. Run the script `/opt/UMC/datint/etc/vpndatamgt` with the check option, or configure a utility, such as a crontab file, to run this script at a defined time (see *SRC-PE Integration Guide, Chapter 9, Integrating Data with the LDAP Directory*).

Deleting VPNs from the Directory

Service providers can delete VPNs in the directory.

To delete VPNs:

1. Delete subscriptions to BoD services associated with the VPN.

Subscriptions to BoD services associated with a particular VPN all contain the substitution

`bodVpnName=<vpnID>`

where `<vpnID>` is the DN of the VPN to be deleted.

You can delete subscriptions with the specified substitution through an LDAP client. You can also delete individual subscriptions with SDX Admin (see *Modifying and Deleting Subscribers and Subscriptions* on page 271), although this solution is not practical for large numbers of subscribers. As a third option, you can develop a data integrator to delete the subscriptions (see *SRC-PE Integration Guide, Chapter 9, Integrating Data with the LDAP Directory*).

2. Remove all extranet clients (see *Removing Extranet Clients* on page 411).
3. Delete the VPN object from the directory.

For information about deleting entries with SDX Admin, see *SRC-PE Getting Started Guide, Chapter 38, Using SDX Admin*.

If you also want to delete the VPNs from the JUNOS routing platform, delete the routing instances that implement the VPN in the network. For complete information about configuring JUNOS routing platforms, see the JUNOS Internet Software documentation.