CHAPTER 5

Defining VPNs and Provisioning Service Requests

The focus of the VPN Solutions Center: IPsec Solution product is the service provided for a customer on the link between the customer's edge device routers in their IPsec VPN. This chapter describes how to modify and delete service requests. This chapter also tells you how to check on a service request's status and find out what went wrong if a service fails.

The main topics presented in this chapter are as follows:

Service Request Description and State Transition Summary

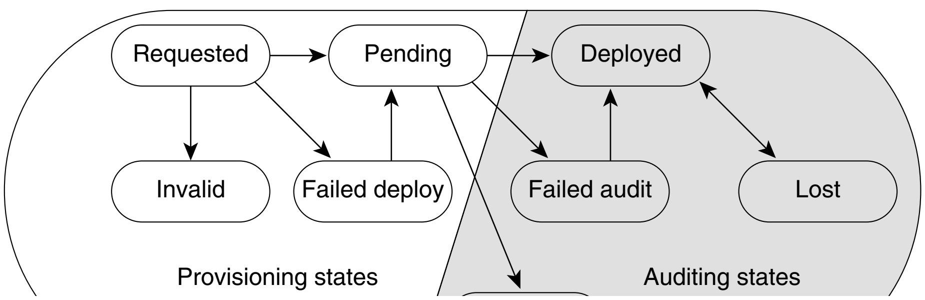
The service model is the centerpiece of service provisioning. With the service model, the VPNSC: IPsec Solution software can capture the specified VPN service provisioning request, analyze the validity of the request, and audit the provisioning results.

The service provider operators take all service request information from their customers. VPNSC: IPsec Solution can assist the operator in making entries because the product has customer information such as the VPN information, the list of the assigned edge routers, and so forth.

The VPN Console steps the operator through the process and simplifies the task of provisioning the edge routers by automating most of the tasks required to set up an IPsec VPN.

Figure 5-1 shows a high-level diagram of the relationships and movement among VPN Solutions Center service request states.

Figure 5-1 Service Request States: Movement and Relationships



The sections below describe each of the service request states and their transition sequences.

Definitions of VPN Solutions Center Service Request States

Table 5-1 describes each VPN Solutions Center service request state. They are listed in alphabetical order.

Table 5-1 Summary of VPN Solutions Center Service Request States

Service Request Type	Description
Closed	A service request moves to Closed if the service request should no longer be used during the provisioning or auditing process. A service request moves to the Closed state only upon a successful audit of a remove request. VPNSC: IPsec Solution does not remove a service request from the database to allow for extended auditing. Only a specific administrator action results in service requests being removed.
Deployed	A service request moves to Deployed if the configuration IOS commands have been verified as found in the router configuration file. Deployed indicates that the configuration file has been downloaded to the router.

Table 5-1 Summary of VPN Solutions Center Service Request States (continued)

Service Request Type	Description
Failed Audit	This state indicates that the service request has not yet successfully passed an audit, and therefore has not yet moved to the Deployed state. The Failed Audit state is initiated from the Pending state. Once a service request is deployed successfully, it cannot reenter the Failed Audit state (except when the service request is redeployed).
Failed Deploy	After provisioning occurred, the service request failed to download the configuration updates to the router. A service request moves to Failed Deploy if the Telnet Gateway Server (TGS) detected an error during the deployment process. If TGS is not being used to download configuration updates, and VPNSC is simply exporting configuration updates to a directory, there is no way to distinguish between a service request in the Failed Deploy and Pending states. The cause for a Failed Deploy status is that TGS reports that either the upload of the initial configuration file from the routers failed or the download of the configuration update to the routers failed (due to lost connection, faulty password, etc.). If the configuration updates are exported to a directory, the service request cannot move into a Failed Deploy state.
Invalid	Indicates that the service request information is incorrect in some way. A service request moves to Invalid if the request was either internally inconsistent or not consistent with the rest of the existing network/router configurations (for example, no more interfaces were available on the router). The Provisioning Driver cannot generate configuration updates to service this request.
Lost	A service request moves to Lost when the Auditor cannot find a configuration-level verification of intent in the router configuration files. The service request was deployed, but now some or all router configuration information is missing. A service request can move to the Lost state *only* when the service request had been Deployed.
Pending	A service request moves to Pending when the Provisioning Driver determines that the request looks consistent and was able to generate the required configuration updates for this request. Pending indicates that the service request has generated the configuration updates and the configuration updates are successfully downloaded to the routers. The Auditor regards pending service requests as new requests and begins the audit. If the service has been freshly provisioned and not yet audited, it is not an error (pending audit). However, if an audit is done and the service is still pending, it is in an error state.
Requested	If the service is newly entered and not yet deployed, it is not an error. However, if a Deploy is done and it remains Requested, the service is in an error state.

Service Request State Transition Sequences

Table 5-2 on page 5-4 and Table 5-3 on page 5-5 show the state transition sequences for VPN Solutions Center service requests. The beginning state of a service request is listed in the first column; the states that service requests can transition to are displayed in the heading row.

For example, to use Table 5-2 to trace the state of a Pending service request to Deployed, find "**Pending**" in the leftmost Service Request States column and move to your right until you find "**Deployed**" in the heading. You can see that for a service request to move from Pending to Deployed, a successful configuration audit must take place.

Table 5-2 shows the service request transitions from **Requested** to **Lost**.

Table 5-2 State Transition Paths for VPNSC Service Requests (Part 1)

SERVICE REQUEST STATES	Requested	Pending	Failed Audit	Deployed	Lost
Requested	No transition to Requested	Successful service request deployment	No transition to Failed Audit	No transition to Deployed	No transition to Lost
Pending	No transition to Requested	—Successful service request redeployment —Audit with error	Audit is not successful	Successful configuration audit	No transition to Lost
Failed Audit	No transition to Requested	Successful service request redeployment	No transition to Failed Audit	Successful configuration audit	No transition to Lost
Deployed	No transition to Requested	Successful service request redeployment	No transition to Failed Audit	Successful configuration audit	Audit found error
Lost	No transition to Requested	Successful service request redeployment	No transition to Failed Audit	Successful configuration audit	Audit found error
Invalid	No transition to Requested	Successful service request redeployment	Redeployment caused service request error	No transition to Deployed	No transition to Lost
Failed Deploy	No transition to Requested	Successful service request redeployment	Redeployment service request failed. configuration update cannot be downloaded.	No transition to Deployed	No transition to Lost
Closed	No transition to Requested	No transition to Pending	No transition to Failed Audit	No transition to Deployed	No transition to Lost

Table 5-3 shows the service request transitions from **Invalid** to **Closed**.

Table 5-3 State Transition Paths for VPNSC Service Requests (Part 2)

Service Request States	Invalid	Failed Deploy	Closed
Requested	Deploy Service Request error	Deployment failed	No transition to Closed
Pending	Redeployment caused service request error	Redeployment service request failed. Configuration update cannot be downloaded.	Removal of the service request is successful
Failed Audit	Redeployment caused service request error	Redeployment service request failed. Configuration update cannot be downloaded.	No transition to Closed
Deployed	Redeployment caused service request error	Redeployment service request failed. Configuration update cannot be downloaded.	No transition to Closed
Lost	Redeployment caused service request error	Redeployment service request failed. Configuration update cannot be downloaded.	No transition to Closed
Invalid	Redeployment caused service request error	Redeployment service request failed. Configuration update cannot be downloaded.	No transition to Closed
Failed Deploy	Redeploy service request error	Redeployment service request failed. Configuration update cannot be downloaded.	No transition to Closed
Closed	No transition to Invalid	No transition to Failed Deploy	No transition to Closed

Overview of Service Request Definition Process

Provisioning an IPsec VPN provides a method to build a service for site-to-site connectivity between a customer edge devices. It includes the following steps in the VPN Solutions Center software:

1. Creating an IPsec VPN
2. Defining the VPN
3. Initiating a service request for the VPN
4. Deploying the service request

Creating a New IPsec VPN and Provisioning a Service Request

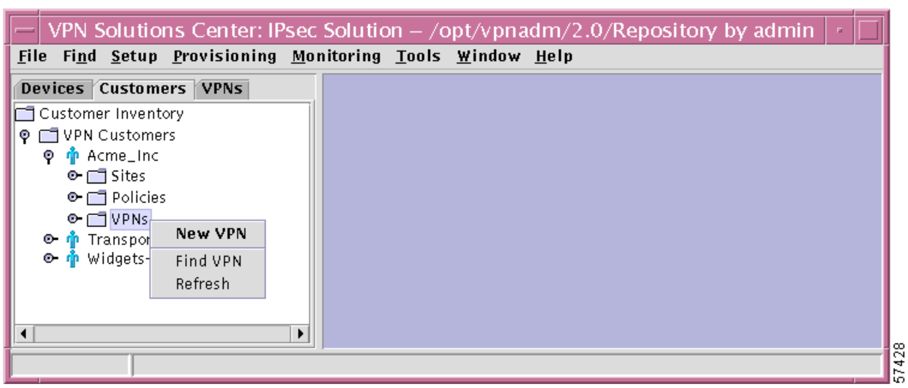
To create a new IPsec VPN and provision a service request for that VPN, follow these steps:

Step 1 In the VPN Console hierarchy pane, choose the **Customers** tab.

Step 2 From the Customers tab, expand the VPN Customers hierarchy for the desired Customer until you can see the VPNs folder.

Step 3 Select the **VPNs** folder, then **right-click**. The Customer VPN menu appears (see Figure 5-2).

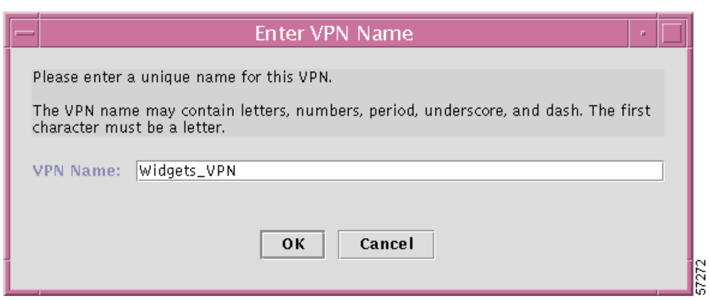
Figure 5-2 Customer VPN Menu



Step 4 From the VPN menu, choose **New VPN**.

The Enter VPN Name dialog box appears (see Figure 5-3).

Figure 5-3 Entering the VPN Name



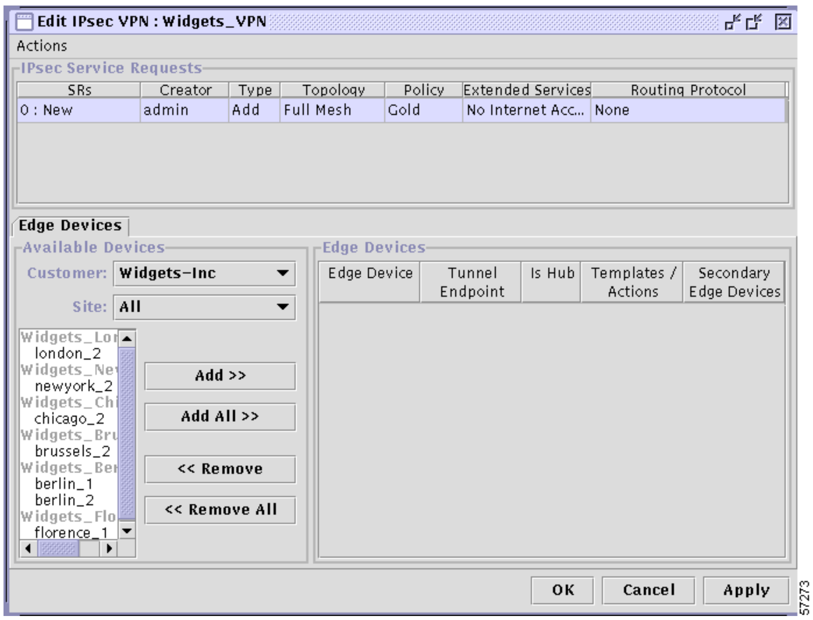
Step 5 Enter the VPN name, then click **OK**.

The first character in the VPN name must be a letter. The VPN name can contain letters, numbers, and these punctuation characters: period, underscore, and dash. The VPN name cannot exceed 63 characters.

Defining a Service Request for the VPN

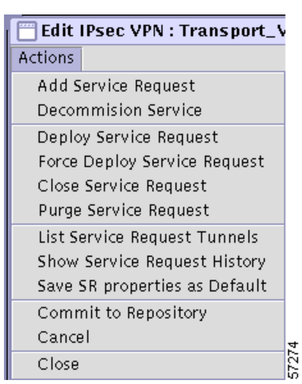
The Edit IPsec VPN dialog box appears (see Figure 5-4).

Figure 5-4 Edit IPsec VPN Dialog Box



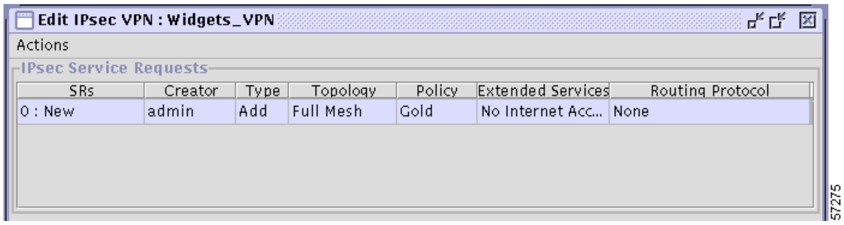
Step 1 From the Edit IPsec VPN dialog box, choose **Actions > Add Service Request**.

Figure 5-5 VPN Actions Menu



A new line is displayed in the IPsec Service Requests panel showing the default values for the new service request (see Figure 5-6).

Figure 5-6 Initial Service Request Settings



Step 2 Modify the following fields to define the service request:

To modify a field, double-click the field and choose the pertinent value from the list.

a. Topology

Choose from *Full Mesh* or *Hub & Spoke*.

b. Policy

Choose the appropriate policy name from the list to associate the correct policy with the new service request.

c. Extended Services

- *No Internet Access*

  This option indicates that the service request provides VPN service only (that is, only secure traffic is allowed between VPN sites). *No Internet Access* is the default setting.

Caution If you enable the *No Internet Access* option, any existing ingress ACL on the router's secure (egress) interface is overwritten by the VPN Solutions Center ingress ACL, which prevents clear traffic being exchanged between VPN sites.

- *Internet Access*

  This option indicates that the service request provides both VPN service and Internet service.

- *Ignore*

  This option indicates that the service request provides both VPN service and Internet service. If you enable the *Ignore* option, VPN Solutions Center does not generate its own ingress ACL. Any existing access control lists on the interface are left intact. The service provider is free to associate any ingress ACL on the router's secured (egress) interface.

  If there is no existing ingress ACL associated with the secured interface, the *Ignore* option serves the same function as the *Internet Access* option.

Removing devices that are part of a deployed service request does not remove the entire access list that was created by VPN Solutions Center. To remove the access lists that are left out, use the Template Manager or manually remove the left out access list from each removed device.

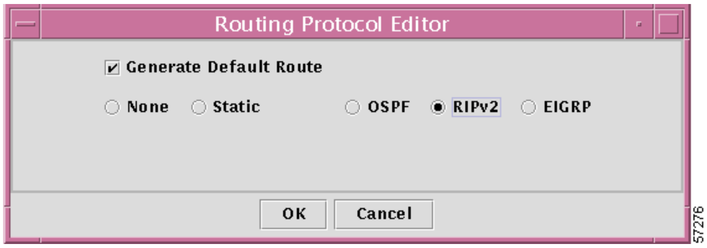
If there is no access list present on the secured interface before deployment and you want extended service specified as **Internet Access**, for better performance, specify the **Ignore** option instead of **Internet Access**. With Internet Access specified, VPN Solutions Center adds an access list or appends "`IP permit any any` " to the existing access list applied to the secured interface.

d. Routing Protocol

This field provides for exchanging Customer site IP addresses across the current VPN. The default routing protocol setting is **None**, which indicates that Customer site IP addresses are not exchanged.

To set the Routing Protocol options, click the **Routing Protocol** field. The Routing Protocol Editor dialog box appears (see Figure 5-7).

Figure 5-7 Setting the Routing Protocol Options



Step 3 To exchange Customer IP addresses, set the values in the Routing Protocol Editor as necessary for the current VPN, then click **OK**.

a. *Generate Default Route*. When this is enabled, VPN Solutions Center generates a default route for the VPN (regardless of which routing protocol is specified, including *None*).

If you disable the *Generate Default Route* option, VPN Solutions Center does not generate a default route for the VPN.

b. Routing protocols: *Static*, *OSPF*, *RIPv2*, and *EIGRP*. When you specify any routing protocol from this dialog box, VPN Solutions Center employs generic routing encapsulation (GRE) tunnels in concert with IPsec in Transport mode.

None. If you specify the *None* option, VPN Solutions Center employs IPsec in Tunnel mode (for more information, see the "Transport Mode and Tunnel Mode" section on page 1-8).

GRE Tunnel Limitation When Using Static Routes

When a service provider uses a Generic Routing Encapsulation (GRE) tunnel provisioned with static routes between two edge device routers—and a secondary device is also configured with a parallel GRE tunnel also using static routes—a limitation in GRE tunnel technology can cause the following problem.

If the tunnel between the primary device and the peer device is down for any reason, the peer device is not notified of the tunnel failure. Its corresponding route remains in the peer devices's routing table, even though the route is no longer in service. As a result, viable traffic continues to be sent along an invalid route (the failed static route from the primary device to the peer device). It is likely that these packets will be lost. The secondary GRE tunnel is never activated.

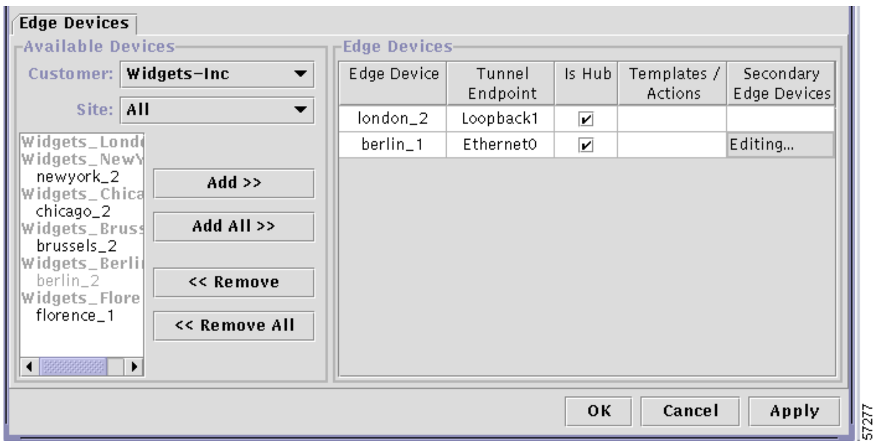
The only remedy is to manually remove the invalid static route.

Associating the Edge Devices with the Service Request

In this procedure, you associate the edge devices (that is, the sites) with the new service request. You can filter edge devices by Customer or site.

Step 1 From the Edit IPsec VPN dialog box, go to the **Edge Devices** tab (see Figure 5-8).

Figure 5-8 Defining the Edge Devices in the Service Request



Step 2 In the Available Devices Customer drop-down menu, choose the appropriate Customer.

Step 3 In the Available Devices Site drop-down menu, choose a particular site or choose **All** to see all the devices for all the Customer sites.

Step 4 From the list of available edge device routers, specify those devices that participate in this service request.

- To specify a single device at a time, select the device name in the list and click **Add**.

  The device name is displayed in the Edge Devices panel, which shows additional information, such as the name of the secured interface, whether the device is a hub, and so on.

- To specify all the devices in the Available Devices list, click **Add All**.

  All the device names are displayed in the Edge Devices panel.

Step 5 When satisfied with the settings, proceed to assigning secondary edge devices or templates as described in the following sections.

If you have no additional information to specify, click **Apply** to activate the service request. Proceed to the "Deploying Service Requests" section on page 5-15.

The service request is now activated. In the IPsec Service Requests panel, the service request is assigned a number and its initial state (usually Requested) is displayed (see Figure 5-8).

Integrating a Template with a Service Request

VPN Solutions Center provides a way to integrate a template with VPNSC configlets. For a given router, you specify the following:

- Edge device router
- Template name
- Template data file name
- Whether the Template configuration file should be appended or prepended to the VPNSC configlet
- Whether the Template configuration file is active or inactive for downloading to the edge device

The template data files are tightly linked with its corresponding template. You can use a data file and its associated template to create a template configuration file. The template configuration file is merged with (either appended to or prepended to) the VPNSC configlet. VPN Solutions Center downloads the combined VPNSC configlet and template configuration file to the edge device router.

You can also download a template configuration file to a router. For details, see the "Provisioning a Template Configuration File Directly to a Router" section on page 8-22.

You can apply the same template to multiple edge devices, assigning the appropriate template data file for each device. Each template data file includes the specific data for a particular device (for example, the management IP address or host name of each device).

To integrate a VPN Solutions Center template with a service request, follow these steps:

Step 1 In the VPN Console hierarchy pane, choose the **VPNs** tab.

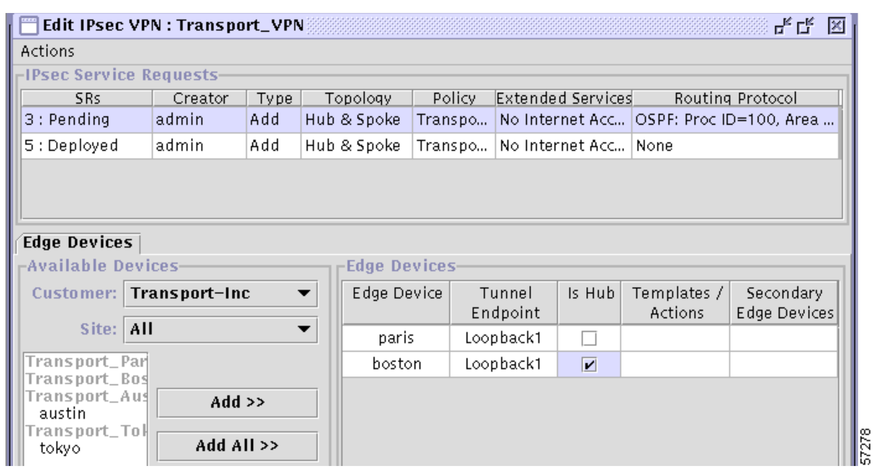
Step 2 Expand the hierarchy so you can see the list of VPNs that are currently defined.

Step 3 Select the pertinent VPN name, then **right-click**.

Step 4 From the menu, choose **Open VPN**.

The Edit IPsec VPN dialog box appears (see Figure 5-9).

Figure 5-9 Edit IPsec VPN Dialog Box



The lower right side of this dialog box is the Edge Devices area. Notice the *Templates/Actions* column.

Step 5 **Double-click** the *Templates/Actions* cell for the edge device of interest.

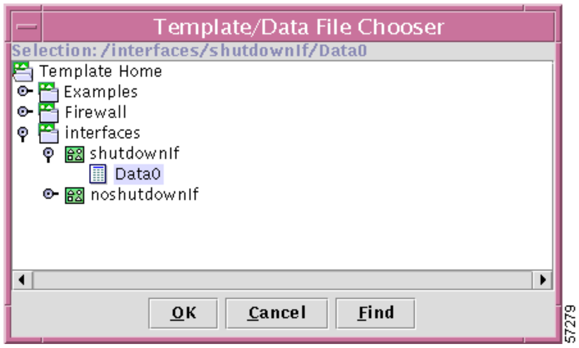
The Add/Remove Templates dialog box appears.

Selecting a Data File From the Template/Data File Chooser

Step 6 In the Add/Remove Template dialog box, click **Add**.

The Template/Data File Chooser dialog box appears (see Figure 5-10).

Figure 5-10 The Template/Data File Chooser Dialog Box



Step 7 Expand the Template Home hierarchy until you can see the pertinent template name and its data files.

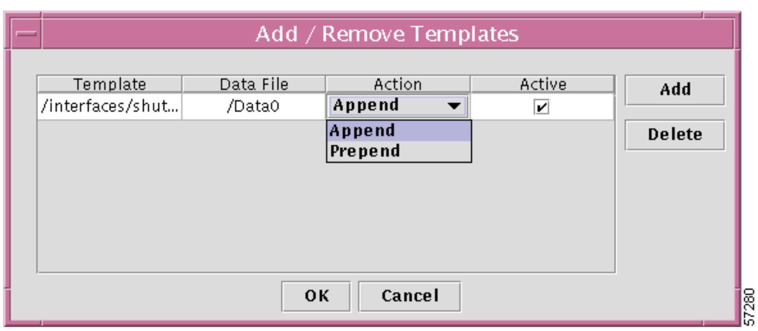
The template data files are tightly associated with its corresponding template. You can use a data file and its associated template to create a template configuration file. The template configuration file is merged with (either appended to or prepended to) the VPNSC configlet. VPN Solutions Center downloads the combined configlet to the edge device router.

Step 8 Select the data file of interest, then click **OK**.

You return to the Add/Remove Templates dialog box (see Figure 5-11).

Determining the Placement and Active Status of the Data File

Figure 5-11 Add/Remove Templates Dialog Box



The **Action** column in the Add/Remove Templates dialog box lets you specify where the template configuration file is placed in the VPNSC configlet—either prepended or appended.

The **Active** column lets you determine whether you want the template configuration file to be merged with the VPNSC configlet and downloaded to the target router.

Step 9 To specify the placement of the template configuration file, click the *Action* field for the appropriate template, then choose **Append** or **Prepend**.

- If you choose **Append**, the template configuration file is appended to (that is, placed at the end of) the VPNSC configlet prior to being downloaded to the target router.
- If you choose **Prepend**, the template configuration file is prepended to (that is, placed at the beginning of) the VPNSC configlet prior to being downloaded to the target router.

Step 10 Specify the Active status of the template configuration file.

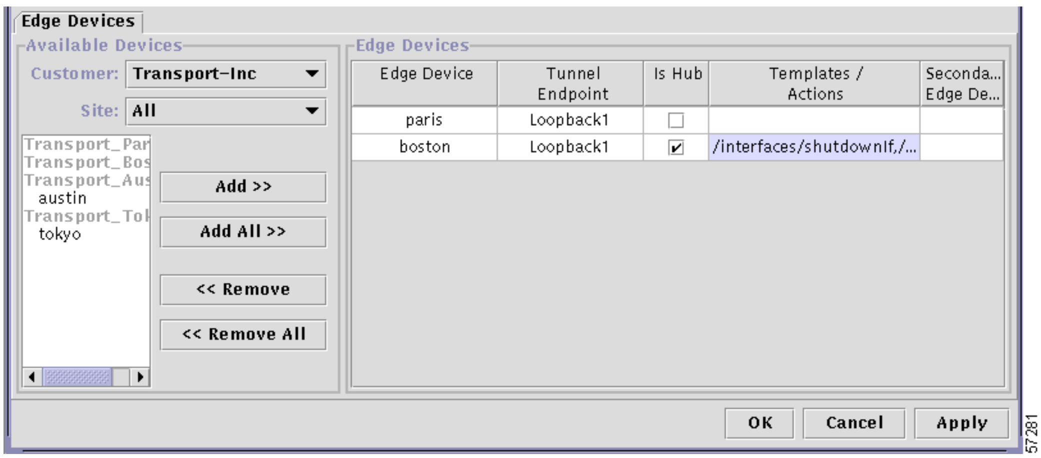
- If you set the Active checkbox as checked, the template configuration file is merged with the VPNSC configlet and downloaded to the target router.
- If you uncheck the Active checkbox, the template configuration file is not merged at this time with the VPNSC configlet.

Step 11 To designate additional templates for the selected service request, click **Add**, then repeat Step 5 through Step 10 as described in this procedure.

Step 12 When the Add Templates fields are set to your satisfaction, click **OK**.

You return to the Edit IPsec VPN dialog box, where the *Templates/Actions* field now displays the name of the assigned templates and data files for the designated edge devices (see Figure 5-12).

Figure 5-12 Template Applied to Device



Step 13 If you have no additional information to specify, click **Apply** to activate the service request. Proceed to the "Deploying Service Requests" section on page 5-15.

The service request is now activated. In the IPsec Service Requests panel, the service request is assigned a number and its initial state (usually *Requested*) is displayed. The following message is displayed:

All modified SRs successfully updated.

Assigning a Secondary Edge Device

VPN Solutions Center provides a way to assign a *secondary edge device* in the same site as the primary device. A secondary edge device is a device that can be brought up automatically either for loadsharing or in the event that the primary edge device goes down.

- Assigning a secondary edge device for loadsharing is available for all the routing protocol options (**Static** route, **OSPF**, **RIPv2**, and **EIGRP**), except **None**.

  The Administrative Distance value for configuring load sharing for the primary device and the specified secondary device is **1**.

- Assigning a secondary edge device in the event that the primary edge device goes down is supported for the **None** and **Static** options only.

  The Administrative Distance value for assigning a secondary device is **10** (which the default).

To assign a secondary edge device, follow these steps:

Step 1 If the Edit IPsec VPN dialog box is not already displayed, bring it up by choosing the **Customers** tab from the VPN Console.

Step 2 Expand the VPN Customers hierarchy until you can see the **VPNs** folder and the VPNs defined in that folder for the pertinent Customer.

Step 3 Select the VPN name and **right-click**.

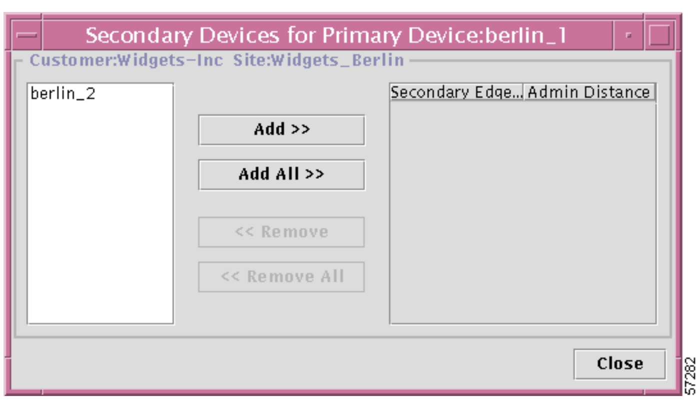
Step 4 Choose **Open VPN** from the menu.

The Edit IPsec VPN dialog box is displayed (see Figure 5-4 on page 5-7). The Secondary Edge Devices column is on the far right in the Edge Devices area of the dialog box.

Step 5 Place your cursor in the Secondary Edge Device field for the edge device you want to assign a secondary edge device to, then **double-click**.

The Secondary Devices for Primary Device dialog box appears (see Figure 5-13).

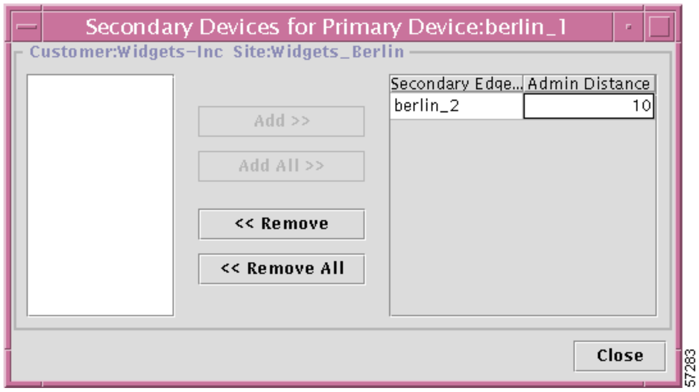
Figure 5-13 Secondary Devices for Primary Device Dialog Box



Step 6 Select the device name of the device to be assigned as a secondary device, then click **Add**.

The device is now added to list of secondary edge devices for that site (see Figure 5-14).

Figure 5-14 Secondary Edge Device Added



Step 7 Set the Administrative Distance to determine the function of the secondary device.

The default Admin Distance is set to **10**, which defines the specified device as the device to come up in the event that the primary device goes down.

a. To set the function so that the device will come up if the primary device goes down, leave the default value of **10**.

b. To set the function so that the device will share the load with the primary device, change the Administrative Distance value to **1**.

Step 8 When satisfied with the secondary device settings, click **Close**.

The specified device is now configured in the VPN Solutions Center software as the secondary edge device in that site.

Step 9 If you have no additional information to specify, click **Apply** to activate the service request. Proceed to the "Deploying Service Requests" section on page 5-15.

The service request is now activated. In the IPsec Service Requests panel, the service request is assigned a number and its initial state (usually *Requested*) is displayed. The following message is displayed:

All modified SRs successfully updated.

Deploying Service Requests

When the VPN is defined and the service requests for that VPN are activated, you can then deploy the service requests. To deploy service requests, follow these steps:

Step 1 In the VPN Console hierarchy pane, choose the **VPNs** tab.

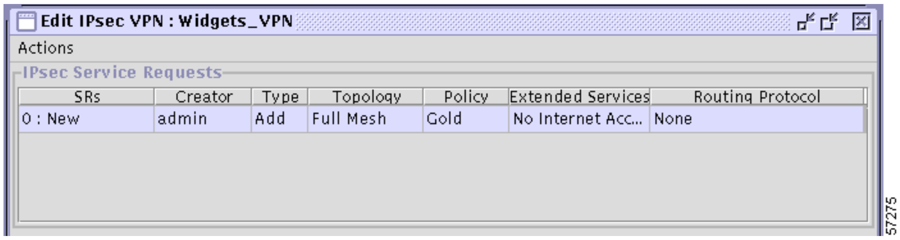
Step 2 Select the name of the VPN that the service request is for, then **right-click**.

The VPN menu is displayed.

Step 3 From the VPN menu, choose **Open VPN**.

The Edit IPsec VPN dialog box appears. The upper area of this dialog box is the IPsec Service Requests area (see Figure 5-15).

Figure 5-15 Selecting the Service Request You Want to Deploy



Step 4 Select the service request that you want to deploy.

Step 5 Choose **Actions** > **Deploy Service Request**.

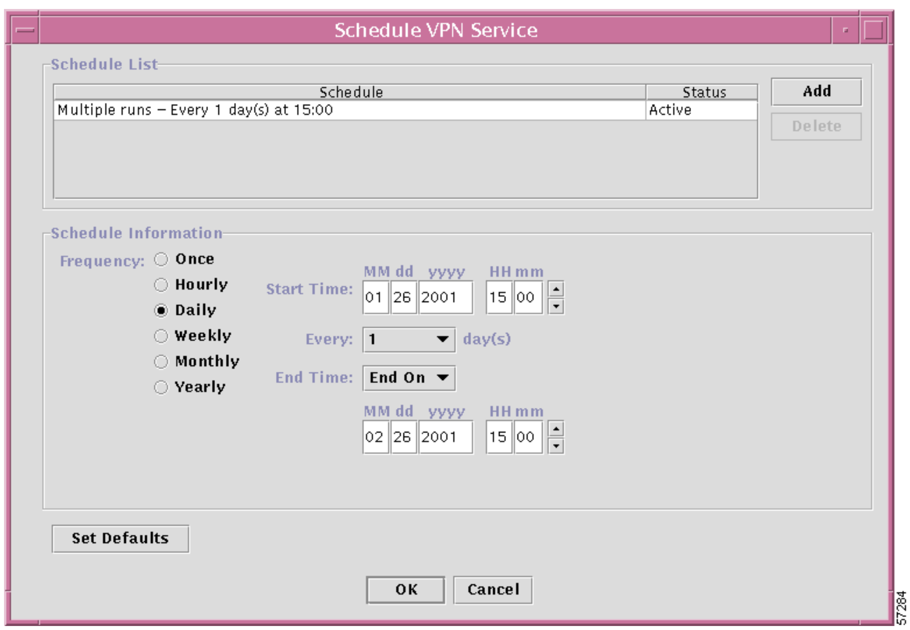
A dialog box appears, giving you the choice to proceed with the deployment or cancel the operation.

This deployment operation both deploys and audits the selected service request. To view the results, you can bring up the Task Logs by choosing **Tools** > **Task Logs**.

Step 6 If you wish to proceed with the deployment and audit operation, click **Yes**.

The Schedule VPN Service dialog box appears (see Figure 5-16).

Figure 5-16 Schedule VPN Service Dialog Box



Step 7 Complete the fields in the dialog box to schedule the service request as needed.

- **a.** From the *Frequency* list, choose the desired frequency: **Once**, **Hourly**, **Daily**, **Weekly**, **Monthly**, or **Yearly**.
- **b.** Set the *Start Time*: **Now** or **Later**.
- **c.** If you choose **Later**, specify the date and time to start and end the service.
- **d.** If you choose anything other than **Once**, specify how often the service should run from the **Every** drop-down list.

Step 8 When you have scheduled the service request to your satisfaction, click **Add**.

The service is added to the Schedule List, displayed in the upper area of the dialog box (as shown in Figure 5-16).

Step 9 Click **OK**.

You return to the VPN Console. At the bottom of the screen, the following message appears:

All selected SRs successfully scheduled for deployment.

Note You can also deploy a service request from the All IPsec Service Requests Report. To do so, select the pertinent service request from the list, then click the **Deploy Service Request** button at the bottom of the report and follow the deployment wizard.

Task Log Error and Warning Messages

If you deploy an invalid service request, VPN Solutions Center generates task logs that say the task completed successfully, but it includes an error message and a warning message. In the task logs, the terms “error” and “warning” are pertinent to the system, not the user.

“*Error*” indicates that the current process encountered a system error and it cannot run further. Such errors include: database errors, invalid command line parameters, invalid VPN Solutions Center configuration files, disk full, and so on.

“*Warning*” indicates that the current process did run successfully, but the results are not the expected results.

Redeploying After Changing a Deployed Service Request

When you deploy a service request and then change a provisioning key in the *csm.properties* file or reconfigure the tunnels on the devices, you can make the change take effect for one or more service requests even if the current service request is already deployed. To do so, follow these steps:

Step 1 In the VPN Console hierarchy pane, choose the **VPNs** tab.

Step 2 Select the name of the VPN that the service request is for, then **right-click**.

The VPN menu is displayed.

Step 3 From the VPN menu, choose **Open VPN**.

The Edit IPsec VPN dialog box appears. The upper area of this dialog box is the IPsec Service Requests area (see Figure 5-15 on page 5-16).

Step 4 Select the service request that you want to deploy.

Step 5 From the Edit IPsec VPN dialog box, choose **Actions** > **Force Deploy Service Request**.

A dialog box appears, giving you the choice to proceed with the deployment or cancel the operation.

This deployment operation both deploys and audits the selected service request. To view the results, you can bring up the Task Logs by choosing **Tools** > **Task Logs**.

Step 6 If you wish to proceed with the deployment and audit operation, click **Yes**.

The Schedule VPN Service dialog box appears (see Figure 5-16 on page 5-16).

Step 7 Complete the fields in the dialog box to schedule the service request as needed.

a. From the *Frequency* list, choose the desired frequency: **Once**, **Hourly**, **Daily**, **Weekly**, **Monthly**, or **Yearly**.

b. Set the *Start Time*: **Now** or **Later**.

c. If you choose **Later**, specify the date and time to start and end the service.

d. If you choose anything other than **Once**, specify how often the service should run from the **Every** drop-down list.

Step 8 When you have scheduled the service request to your satisfaction, click **Add**.

The service is added to the Schedule List, displayed in the upper area of the dialog box.

Step 9 Click **OK**.

Getting Detailed Information on Service Requests

VPN Solutions Center provides a wealth of detailed information about each VPN and service request, such as:

- Tunnel List report
- Tunnel Details report
- Audit Details report
- History report

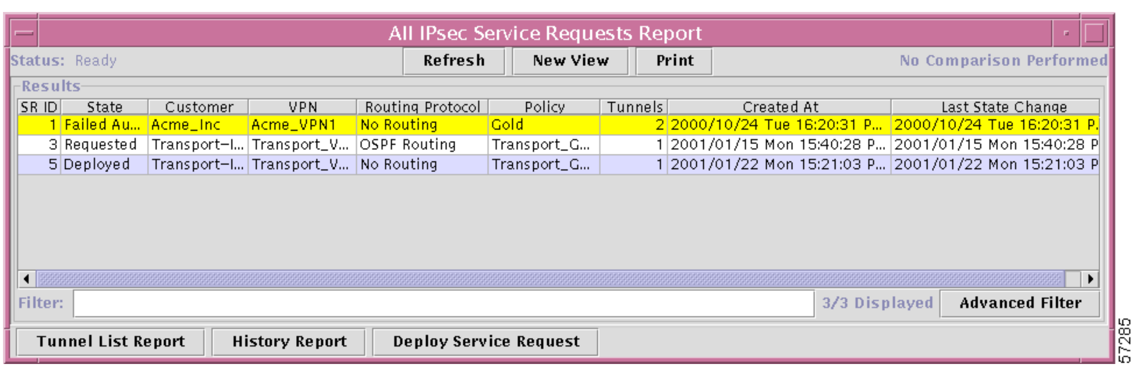
You can also deploy a service request from the All IPsec Service Requests Report. To do so, select the pertinent service request from the list, then click the **Deploy Service Request** button at the bottom of the report.

To view information on a service request, follow these steps:

Step 1 From the VPN Console menu bar, choose **Provisioning** > **List All Service Requests**.

The All IPsec Service Requests Report appears (see Figure 5-17).

Figure 5-17 All IPsec Service Requests Report



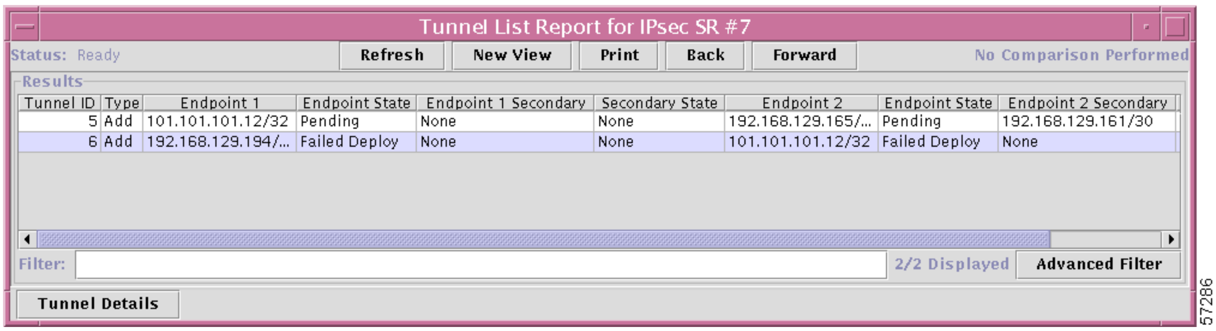
Note Service requests that report a problem in deployment are displayed in yellow.

Step 2 Select the service request that you want information on.

The Tunnel List Report

Step 3 To view the Tunnel List Report (see Figure 5-18), click the **Tunnel List Report** button (at the bottom of the All IPsec Service Requests Report window).

Figure 5-18 Tunnel List Report



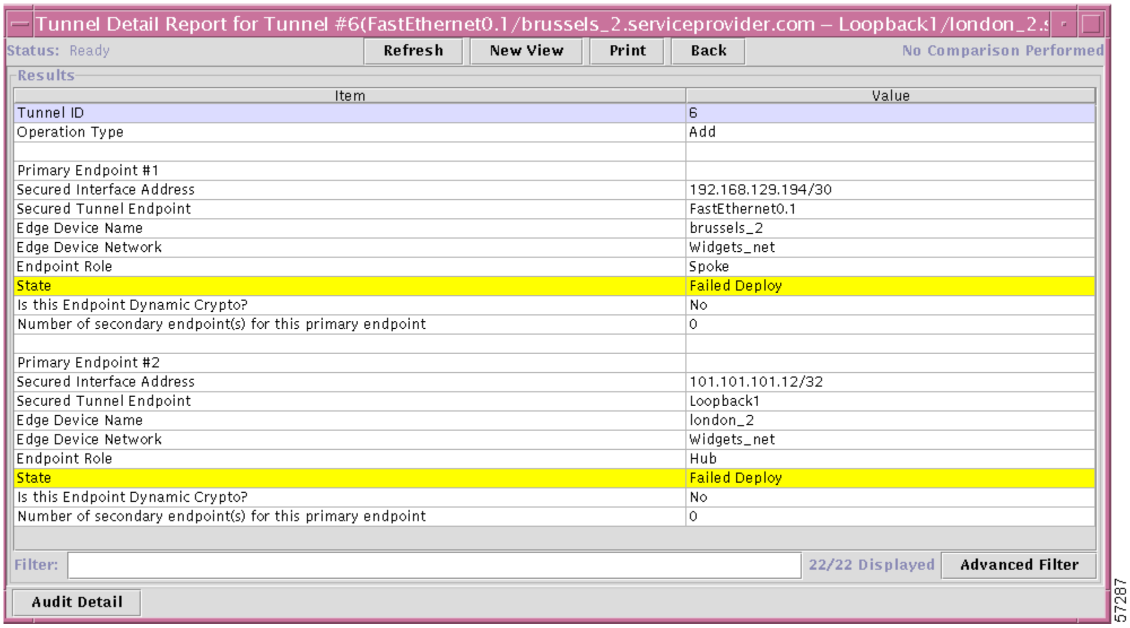
To return to the previous window, click **Back**.

Tunnel Details Report

Step 4 To view the Tunnel Details report, click the **Tunnel Details** button at the bottom of the Tunnel List Report.

The Tunnel Detail Report provides a great deal of information on each tunnel endpoint (see Figure 5-19). If a deployment problem exists, the State is displayed in yellow.

Figure 5-19 Tunnel Details Report



The title bar for the Tunnel Detail Report displays the following information:

- Tunnel number
- Type of interface for each tunnel endpoint
- Name of the router at each tunnel endpoint

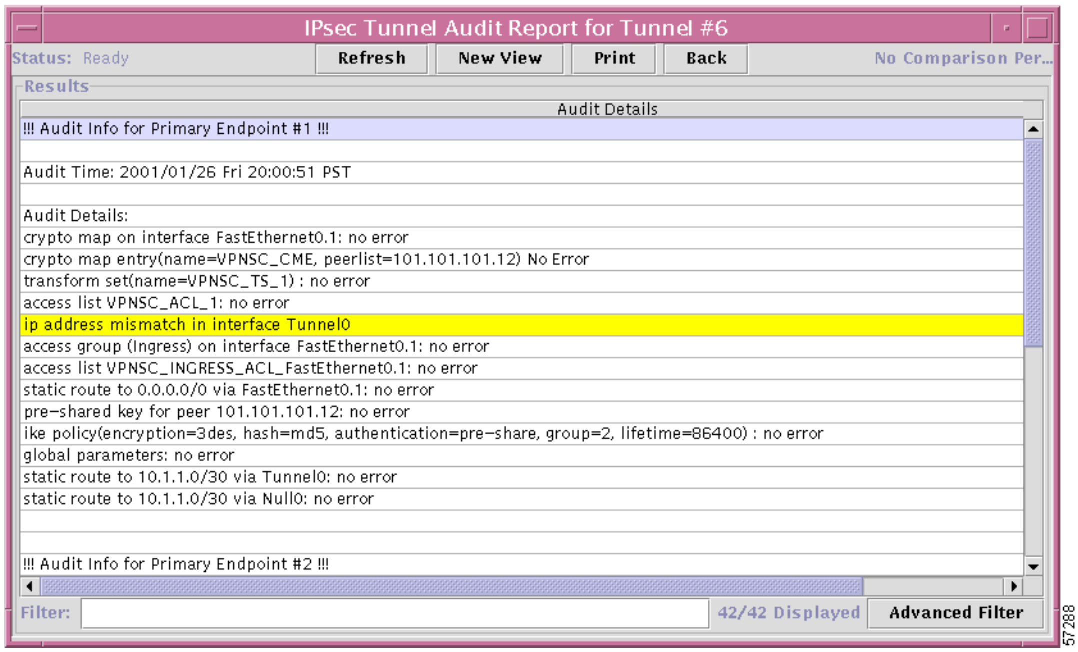
  For example, Figure 5-19 shows that the tunnel is between the *brussels_2* and *london_2* edge device routers. The interface on brussels_2 is a FastEthernet0 interface; the interface on london_2 is loopback0 interface.

To return to the previous window, click **Back**.

Audit Details Report

Step 5 To view the Audit Details Report (see Figure 5-20), click the **Audit Detail** button at the bottom of the Tunnel Details Report.

Figure 5-20 IPsec Tunnel Audit Details Report



The IPsec Tunnel Audit Details Report highlights in yellow problems found in the audit.

To return to the previous window, click **Back**.

History Report

Step 6 To view the History Report for a selected service:

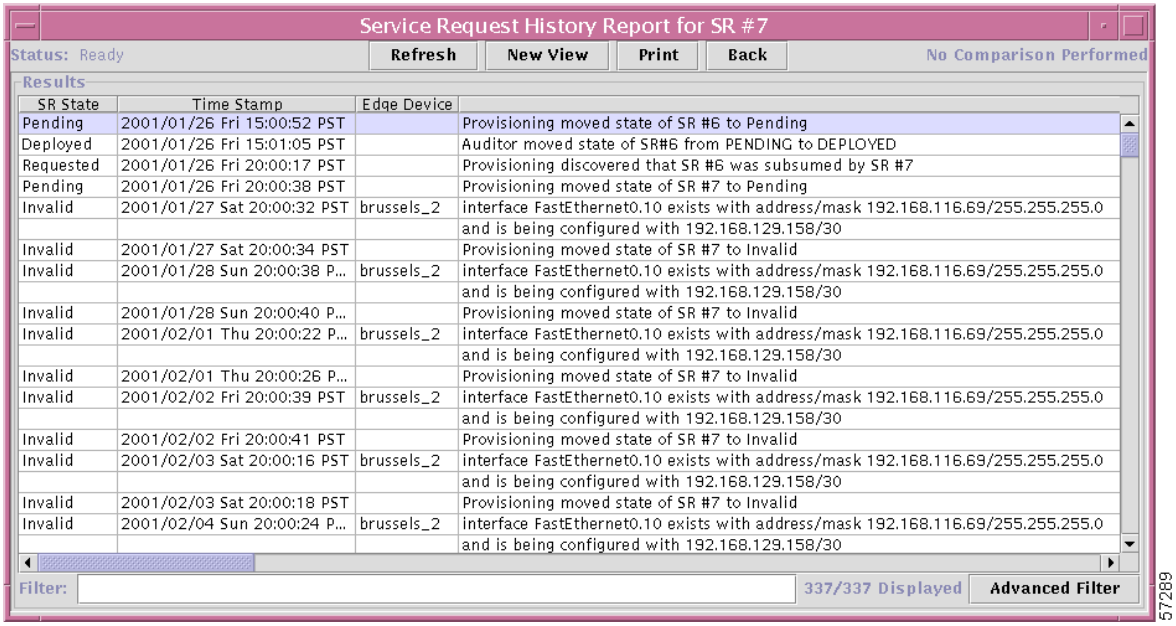
a. Bring up or return to the All IPsec Service Requests window (see Figure 5-17 on page 5-18).

b. Select the service request of interest.

c. Click the **History Report** button.

The History Report for the selected service appears (see Figure 5-21).

Figure 5-21 History Report



To return to the previous window, click **Back**.

Closing Service Requests Manually

When you manually close a service request, VPN Solutions Center changes the state of the service to Closed in the Repository. VPNSC does not make any modifications to the router's configuration file when you close a service request. You cannot purge a service request from the Repository until it is closed.

To close a service request, follow these steps:

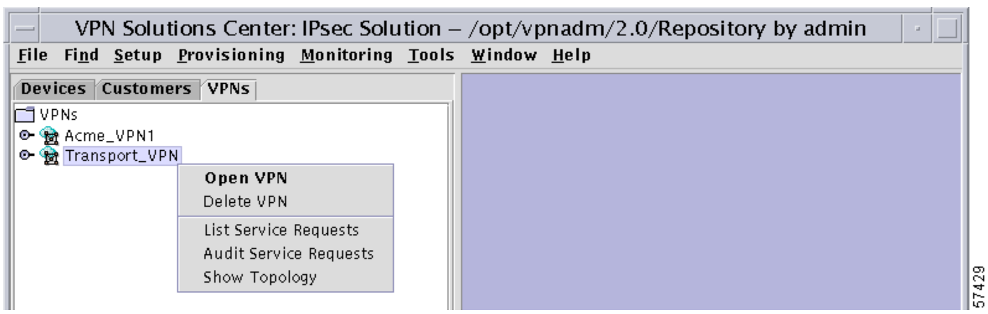
Step 1 From the VPN Console hierarchy pane, choose the **VPNs** tab.

Step 2 From the VPNs tab, expand the VPN hierarchy until you can see the VPN with the service of interest.

Step 3 Select the name of the VPN, then **right-click**.

The menu shown in Figure 5-22 appears.

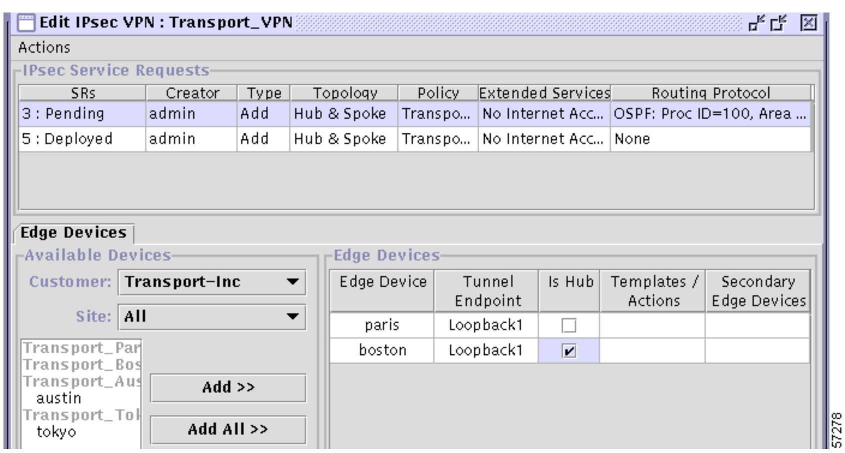
Figure 5-22 VPN Menu



Step 4 From the menu, choose **Open VPN**.

The Edit IPsec VPN dialog box appears (see Figure 5-23).

Figure 5-23 Edit IPsec VPN Dialog Box



Step 5 From the IPsec Service Requests area, select the one or more service requests you want to close.

Step 6 Choose **Actions** > **Close Service Request**.

You receive the following confirmation prompt:

Are you sure you want to close the selected service request(s)?

Step 7 To close the selected service requests, click **Yes**.

To cancel the close operation, click **No**.

In the IPsec Service Requests area, the request is now displayed as "Closed." VPN Solutions Center changes the state of the selected services to Closed in the Repository.

Removing Service Requests From the Repository

To save disk space and remove extraneous entries in service request reports, you may choose to remove invalid or failed service requests from the Repository. VPN Solutions Center only removes service requests that are in the Closed state.

To remove service requests from the Repository, follow these steps:

Step 1 Ensure that the service requests you want to remove are in the Closed state. If they are not closed, close the service requests as described in the previous section.

Step 2 From the VPN Console menu bar, choose **Provisioning** > **Purge Closed Requests from Database**.

You receive the following confirmation prompt:

All closed service requests will be removed from the database. (There follows additional information on how to close a service request).

Do you want to purge closed service requests now?

Step 3 To proceed with the service request removal operation, click **Yes**.

To cancel the operation, click **No**.

You receive the following message:

All Closed Requests Purged.

Step 4 Click **OK**.

The entries for the removed service requests in the Edit IPsec VPN dialog box and in service request reports are also removed.