



Auditing IPsec VPN Service Requests

When you initiate VPN Solutions Center service request audit, the audit tests each tunnel in the VPN. The service request is promoted to the Deployed state only when all the tunnels have passed the audit.

The elements that the VPN Solution Center audit checks are as follows: 1) Loopback interface, 2) GRE tunnel interface, 3) Crypto ACLs, 4) Transform sets, 5) Crypto maps (tunnel level auditing), 6) Crypto local identity, 7) IKE policy, 8) Preshared keys, 9) Routing protocols, and 10) Ingress traffic filters.

Generating a Service Request Audit

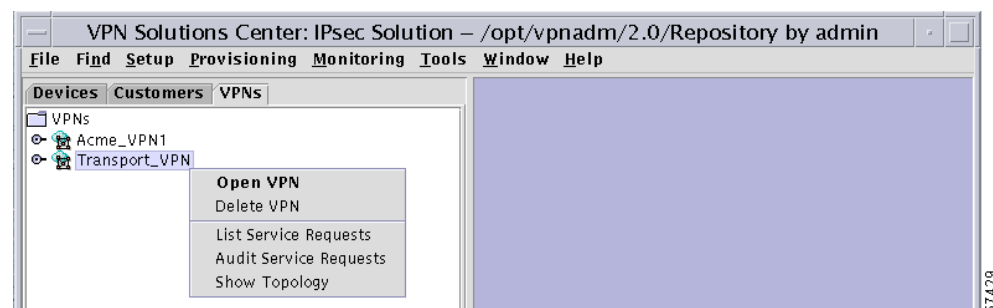
VPN Solutions Center software performs a basic audit each time you deploy a service request. You need only schedule the audit separately as described in this section if you want to run it more frequently or if you customized audits.

When a service request moves beyond the control of the Provisioning system, the *Auditor* for VPN Solutions Center takes control. The Auditor is a mechanism that monitors and reports the current state of a VPN service request over its lifetime. The lifetime of a VPN service request spans from the Requested state to the Closed state (see the “Service Request Description and State Transition Summary” section on page 6-6). The Auditor also provides the reasons why the service request is in its current state. The Auditor saves the state transition (if any) into the VPN Inventory Repository.

To audit the service requests for an IPsec VPN, 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 you want to audit.
- Step 3** Select the name of the VPN, then **right-click**. The menu shown in Figure 6-1 appears.

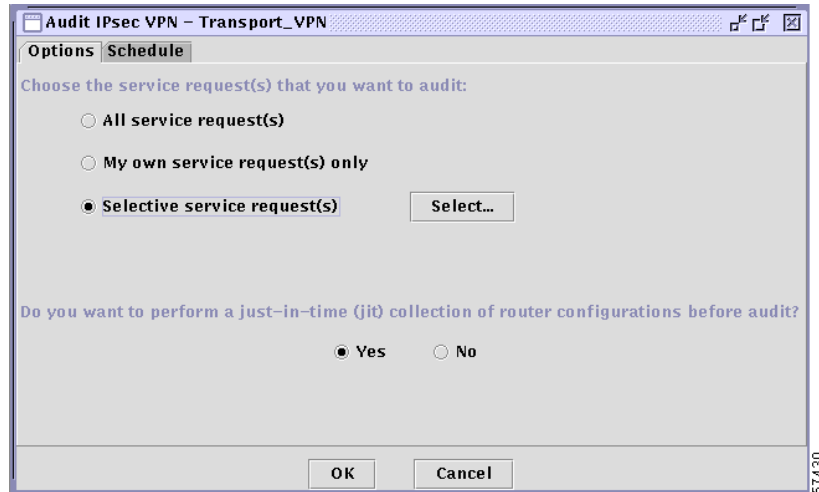
Figure 6-1 VPN Menu



Step 4 From the menu, choose **Audit Service Requests**.

The dialog box shown in Figure 6-2 appears.

Figure 6-2 Choosing Which Service Requests to Audit



Step 5 Choose which service requests you want to audit:

- All service requests for the selected VPN
- Your own service requests only
- Selected service requests

Step 6 If you want to audit only selected service requests, select the **Selective service requests** option, then click **Select**.

A table showing the service requests from which you can select is displayed (see Figure 6-3).

Figure 6-3 List of Service Requests to Choose From

SR ID	Customer Name	VPN Name	SR STATE
3	Transport-Inc	Transport_VPN	Pending
5	Transport-Inc	Transport_VPN	Deployed

- a. Select one or more service requests from the list.
- b. Click **OK**.

You return to the Audit Options dialog box shown in Figure 6-2.

Step 7 Select the appropriate response (**Yes** or **No**) to the just-in-time collection prompt:

Do you want to perform a just-in-time (jit) collection of router configurations before audit?

- a. If you want to collect the latest router configuration files from the routers effected by the selected service request before VPN Solutions Center runs the audit, accept the **Yes** option (the default).
- b. If you want VPN Solutions Center to use the router configuration files in the Repository (which may or may not be the most current versions) for the audit, select **No**.

Step 8 When the audit options are set to your satisfaction, click the **Schedule** tab.

The Audit Schedule dialog box appears (see Figure 6-4).

Figure 6-4 Scheduling the Audit

Audit IPsec VPN - Transport_VPN

Options | **Schedule**

Enter an Unique Task Name:

Schedule List

Schedule	Status
Multiple runs - Every 1 day(s) at 16:15	Active

Schedule Information

Frequency: ☐ Once
☐ Hourly
☒ **Daily**
☐ Weekly
☐ Monthly
☐ Yearly

Start Time: MM dd yyyy HH mm
02 06 2001 16 15

Every: 1 day(s)

End Time: End On
MM dd yyyy HH mm
02 12 2001 16 15

Set Defaults

OK Cancel

- Step 9** Complete the fields in the dialog box to schedule the audit as needed.
- From the *Frequency* list, choose the desired frequency: **Once**, **Hourly**, **Daily**, **Weekly**, **Monthly**, or **Yearly**.
 - Set the *Start Time*: **Now** or **Later**.
 - If you choose **Later**, specify the date and time to start and end the audit.
 - If you choose anything other than **Once**, specify how often the audit should run from the **Every** drop-down list.
- Step 10** When you have scheduled the audit to your satisfaction, click **Add**.
- The audit is added to the Schedule List, displayed in the upper area of the dialog box (as shown in Figure 6-4).
- Step 11** Click **OK**.
- You return to the VPN Console.

Viewing Audit Reports

To view audit reports, 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 6-5).

Figure 6-5 All IPsec Service Requests Report

SR ID	State	Customer	VPN	Routing Protocol	Policy	Tunnels	Created At	Last State Change
1	Failed Au...	Acme_Inc	Acme_VPN1	No Routing	Gold	2	2000/10/24 Tue 16:20:31 P...	2000/10/24 Tue 16:20:31 P...
3	Requested	Transport-l...	Transport_V...	OSPF Routing	Transport_G...	1	2001/01/15 Mon 15:40:28 P...	2001/01/15 Mon 15:40:28 P...
5	Deployed	Transport-l...	Transport_V...	No Routing	Transport_G...	1	2001/01/22 Mon 15:21:03 P...	2001/01/22 Mon 15:21:03 P...

Note

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

- Step 2

Select the service request for which you want audit information.
- Step 3

Click the **Tunnel List Report** button (at the bottom of the All IPsec Service Requests Report window).
The Tunnel List Report appears.
- Step 4

Click the **Tunnel Details** button (at the bottom of the Tunnel List Report).
The Tunnel Details Report appears (see Figure 6-6).

Figure 6-6 Tunnel Details Report

Item	Value
Tunnel ID	6
Operation Type	Add
Primary Endpoint #1	
Secured Interface Address	192.168.129.194/30
Secured Tunnel Endpoint	FastEthernet0.1
Edge Device Name	brussels_2
Edge Device Network	widgets_net
Endpoint Role	Spoke
State	Failed Deploy
Is this Endpoint Dynamic Crypto?	No
Number of secondary endpoint(s) for this primary endpoint	0
Primary Endpoint #2	
Secured Interface Address	101.101.101.12/32
Secured Tunnel Endpoint	Loopback1
Edge Device Name	london_2
Edge Device Network	widgets_net
Endpoint Role	Hub
State	Failed Deploy
Is this Endpoint Dynamic Crypto?	No
Number of secondary endpoint(s) for this primary endpoint	0

Filter: 22/22 Displayed Advanced Filter

Audit Detail

Step 5 To view the Audit Details Report (see Figure 6-7), click the **Audit Detail** button (at the bottom of the Tunnel Details Report).

Figure 6-7 Audit Details Report

Audit Details
!!! Audit Info for Primary Endpoint #1 !!!
Audit Time: 2001/01/26 Fri 20:00:51 PST
Audit Details:
crypto map on interface FastEthernet0.1: no error
crypto map entry(name=VPNSEC_CME, peerlist=101.101.101.12) No Error
transform set(name=VPNSEC_TS_1) : no error
access list VPNSEC_ACL_1: no error
ip address mismatch in interface Tunnel0
access group (Ingress) on interface FastEthernet0.1: no error
access list VPNSEC_INGRESS_ACL_FastEthernet0.1: no error
static route to 0.0.0.0/0 via FastEthernet0.1: no error
pre-shared key for peer 101.101.101.12: no error
ike policy(encryption=3des, hash=md5, authentication=pre-share, group=2, lifetime=86400) : no error
global parameters: no error
static route to 10.1.1.0/30 via Tunnel0: no error
static route to 10.1.1.0/30 via Null0: no error
!!! Audit Info for Primary Endpoint #2 !!!

Filter: 42/42 Displayed Advanced Filter

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

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

Service Request Description and State Transition Summary

The service model is the centerpiece of service provisioning. With the service model, the VPN Solutions Center: 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. VPN Solutions Center: 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.

Definitions of VPN Solutions Center Service Request States

Table 6-1 describes each VPN Solutions Center service request state. They are listed in alphabetical order.

Table 6-1 Summary of VPN Solutions Center Service Request States

Service Request Type	Description
<i>Closed</i>	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.
<i>Deployed</i>	A service request moves to Deployed if the configuration update commands have been verified as found in the router configuration file. Deployed indicates that the configuration file has been downloaded to the router, and the intent of the request has been verified at the configuration level.
<i>Failed Audit</i>	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. It indicates that the configuration update has been successfully downloaded to the router. Once a service request is deployed successfully, it cannot reenter the Failed Audit state (except when the service request is redeployed).
<i>Failed Deploy</i>	<p>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.</p> <p>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.).</p> <p>If the configuration updates are exported to a directory, the service request cannot move into a Failed Deploy state.</p>

Table 6-1 Summary of VPN Solutions Center Service Request States (continued)

Service Request Type	Description
<i>Invalid</i>	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.
<i>Lost</i>	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 <i>only</i> when the service request had been Deployed.
<i>Pending</i>	<p>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.</p> <p>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.</p>
<i>Requested</i>	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 6-2 and Table 6-3 on page 6-9 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 6-2 on page 6-8 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 routing audit must take place.

Table 6-2 shows the service request transitions from **Requested** to **Lost**.

Table 6-2 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 6-3 shows the service request transitions from **Invalid** to **Closed**.

Table 6-3 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

