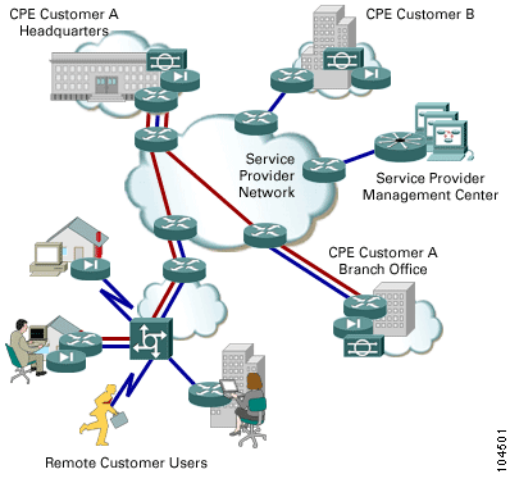
Remote Access VPN Services

This chapter contains the following sections:

Creating Remote Access VPN Services

Remote Access VPN tunnels are initiated by a VPN Client and terminated at the secure network edge, as illustrated in Figure 4-1. (The blue lines represent the Remote Access VPN tunnels.)

Figure 4-1 Remote Access VPNs



To begin the remote access provisioning process, the network administrator defines an encryption policy, a remote access VPN policy, and (optionally) configures a AAA server (pronounced “Triple A server”). The remote access policy is then applied to CPE devices in the network through deployment of a remote access service request that uses the remote access policy.

Note Before creating an ISC security policy or service request, it is necessary to populate the ISC repository with the target devices in your network, collect the initial device configuration files, designate customers and customer sites, and define each device as a CPE.

CPE devices are the devices at each end of the VPN tunnel. Creating CPE devices includes assigning each target device to a specific customer and customer site and marking the device interfaces. Specifically for security management, you must define at least one public and one private interface on each device.

For how-to information on populating your ISC repository and setting up CPE devices, refer to the *Cisco IP Solution Center Integrated VPN Management Suite Infrastructure Guide, 3.2*.

In the Remote Access VPN policy, the network administrator performs the following tasks:

- Configures the encryption policy (which contains IKE and IPsec proposal parameters) that defines the network layer encryption and authentication control.
- Specifies the IKE XAuth parameters for user authentication.
- Sets the Mode Configuration parameters for policy push and features such as dynamically assigned client IP addresses.
- Defines the remote access user group. (Because each remote access policy defines a user group, you can use multiple remote access policies in the same service request. This enables you to configure multiple user groups on the same CPE device.)
- Defines remote access parameters.

The group policy information is stored in a profile that can be used locally in the VPN device configuration. When the user or group information is stored on AAA servers, you must also configure access to the AAA servers and allow the VPN device to send requests to the AAA servers.

Once created, the remote access policies can also be applied to multiple service requests.

To define an remote access VPN service, use the following sections:

- Adding AAA Server Devices to Your Repository, page 4-2
- Creating Encryption Policies, page 4-5
- Creating Remote Access VPN Policies, page 4-5
- Creating Remote Access VPN Service Requests, page 4-25

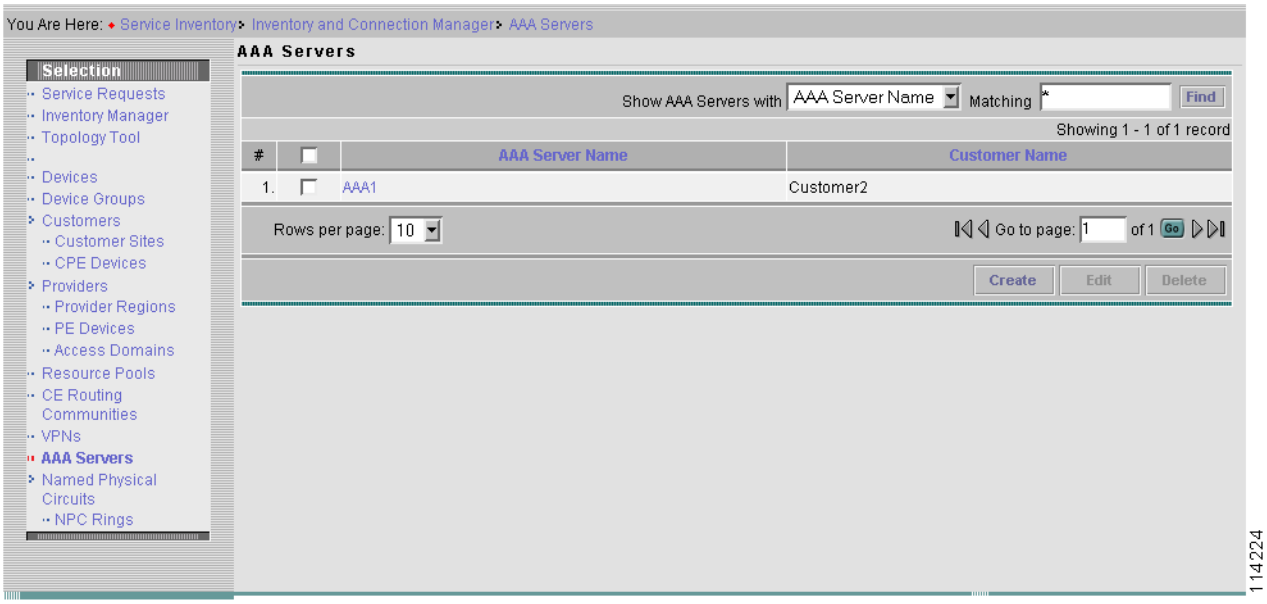
Adding AAA Server Devices to Your Repository

A AAA server (pronounced “Triple A” server) is required when the user authentication method is external or the group policy information is stored on an external AAA server. If user profiles or group attributes are to be obtained from a AAA Server (as opposed to having them stored on the CPE device itself), then a AAA Server entry must be created and added to your ISC repository.

To create a AAA server entry in ISC, perform the following steps:

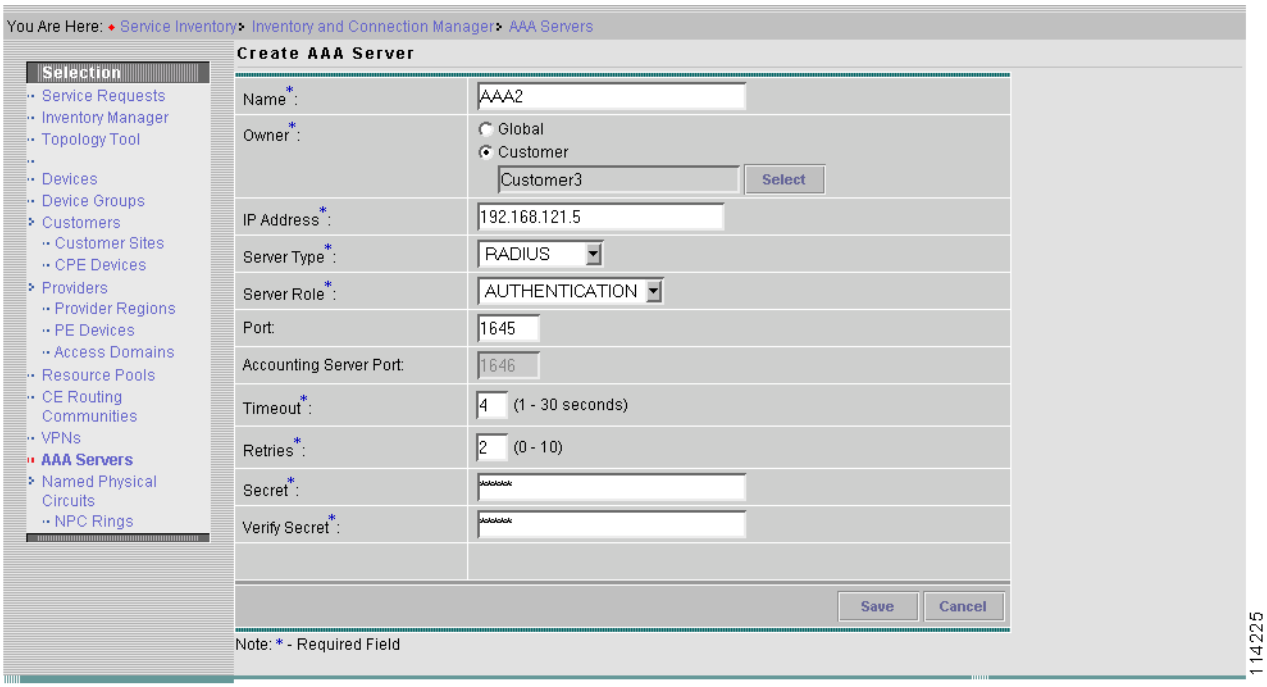
Step 1 Click **Home** > **Service Inventory** > **Inventory and Connection Manager** > **AAA Servers**. The AAA Servers page appears as shown in Figure 4-2.

Figure 4-2 The AAA Servers Page



Step 2 Click **Create**. The Create AAA Server page appears as shown in Figure 4-3.

Figure 4-3 The Create AAA Server Page



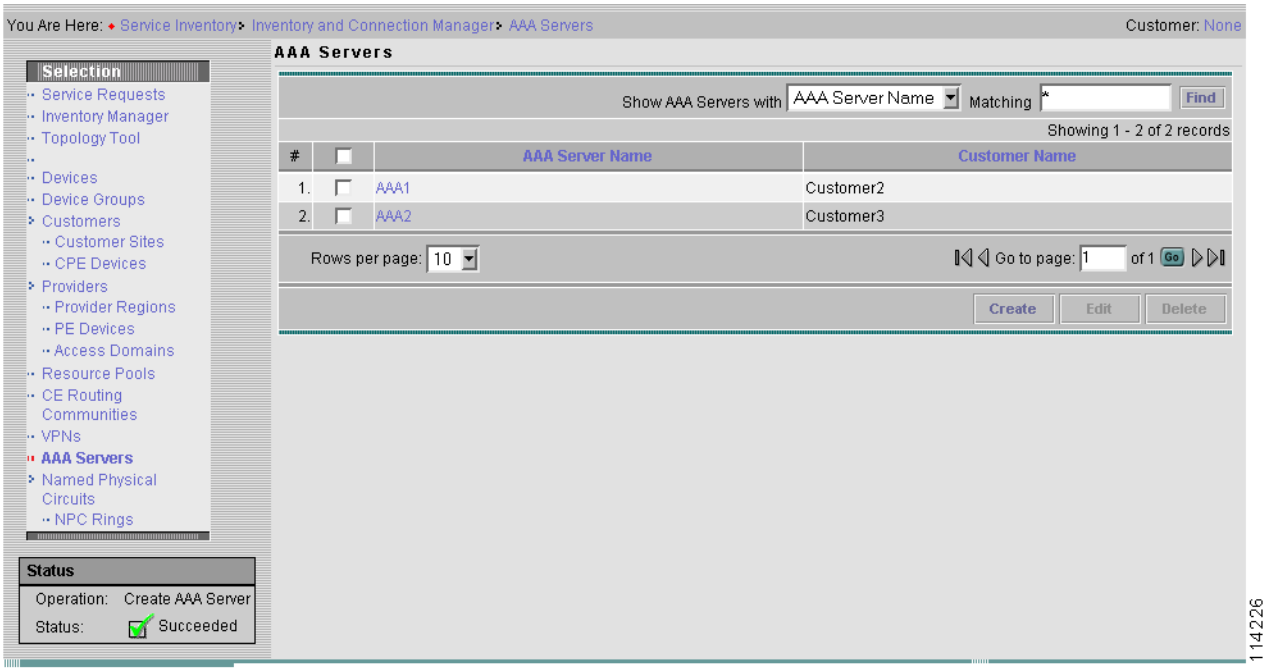
Step 3 Follow the instructions in Table 4-1 to enter the AAA server attributes.

Table 4-1 Create AAA Server Fields

Field Name	Type	Instructions
Name	text box	Enter a name for the AAA server.
Owner	**Select** button	Specify whether the policy is global by clicking **Global**, or customer owned by clicking **Customer**. If you select **Customer**, you are required to specify the owner. Choose the customer with which you want to associate the AAA server. To do this, click **Customer** > **Select**. The Customer for IPsec Policy dialog box appears. Click the button next to the customer you want to select and click **Select** (to choose that customer), or click **Cancel** to exit the dialog box without saving changes. Both return you to the main page.
IP Address	text box	Enter the IP address of the AAA server.
Server Type	drop-down list	Click the drop-down list and select the type of the AAA server. The type can be **RADIUS**, **NTDOMAIN**, **SDI**, or **TACACS+**. The **NTDOMAIN** and **SDI** options are supported for the VPN 3000 only.
Server Role	drop-down list	Click the drop-down list and select the server role for this AAA server: • **AUTHENTICATION** – Use as an authentication server only. • **ACCOUNTING** – Use as an accounting server only. • **BOTH** – Use as an authentication and accounting server.
Port	text box	Enter the authentication port number if the AAA server acts as an authentication server. The default authentication port is 1645 for a RADIUS server.
Accounting Server Port	text box	Enter the accounting port number if the AAA server acts as an accounting server. The default accounting port is 1646 for a RADIUS server.
Timeout	text box	Enter the timeout in seconds for how long to wait after sending a query to the server and receiving no response before trying again. The default is 4 seconds.
Retries	text box	Enter the number of times to retry sending a query to the server after the timeout period. The default is 2.
Secret	text box	Enter the AAA server secret (also called the shared secret). The field displays only asterisks.
Verify Secret	text box	Retype the AAA server secret. It must match what you entered in the **Secret** field exactly.

Step 4 Click **Save** when done. The AAA Servers page appears with the newly created AAA server displayed in the AAA server list, as shown in Figure 4-4.

Figure 4-4 The AAA Servers Page After Adding A New Server



Creating Encryption Policies

The encryption policy defines the security parameters for protecting data traveling through the VPN tunnels. It consists of one or more IKE proposals, one or more IPsec proposals, and global attributes. For example, the IKE proposal portion of the encryption policy could consist of selecting the 3DES, SHA, certificates, and Diffie-Hellman Group 2 options, and the IPsec proposal portion of the encryption policy could consist of selecting the ESP-AES, ESP-SHA, no authentication header (AH), no compression, and no PFS options.

You must have an encryption policy for your remote access policy. However, the same encryption policy defined for a site-to-site VPN policy may also be used for a remote access policy. So, if you have already created an encryption policy in ISC that you would like to use, proceed to the "Creating Remote Access VPN Policies" section on page 4-5. Otherwise, follow the instructions in "Creating an Encryption Policy" section on page 3-5 and create an encryption policy before continuing.

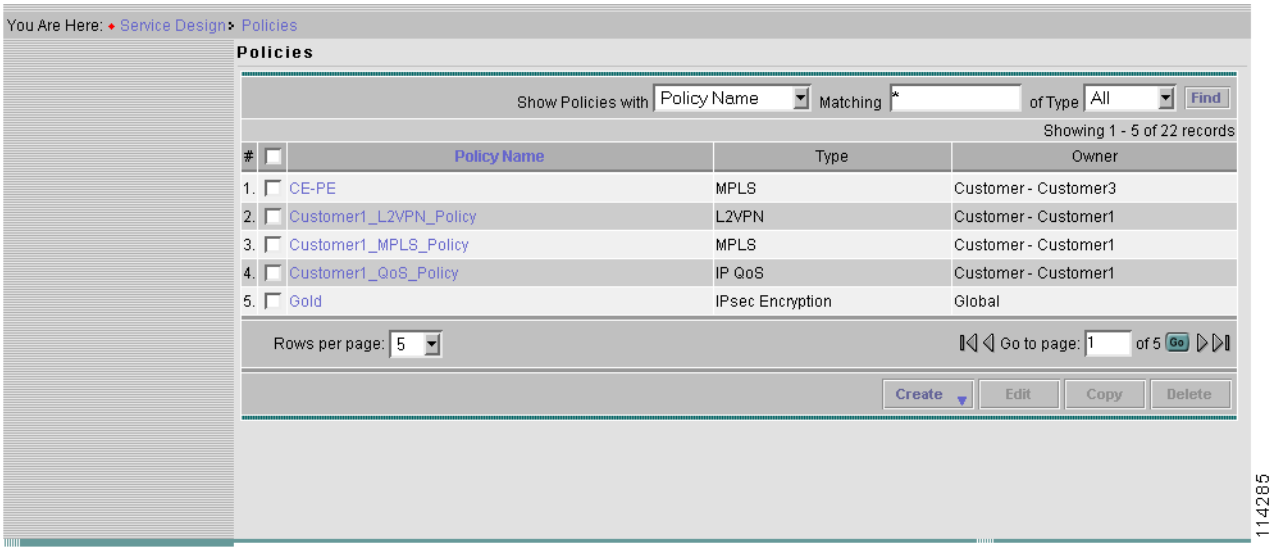
Creating Remote Access VPN Policies

The remote access VPN policy defines the characteristics of the IPsec tunnel between the customer site and the remote user. Its attributes include the VPN group name and password, IP address pools, and split tunneling subnets. Additionally, the policy defines what VPN features are enabled and which are not. For example, the policy enables (or disables) reverse route injection and NAT transparency.

To create a remote access VPN policy, perform the following steps:

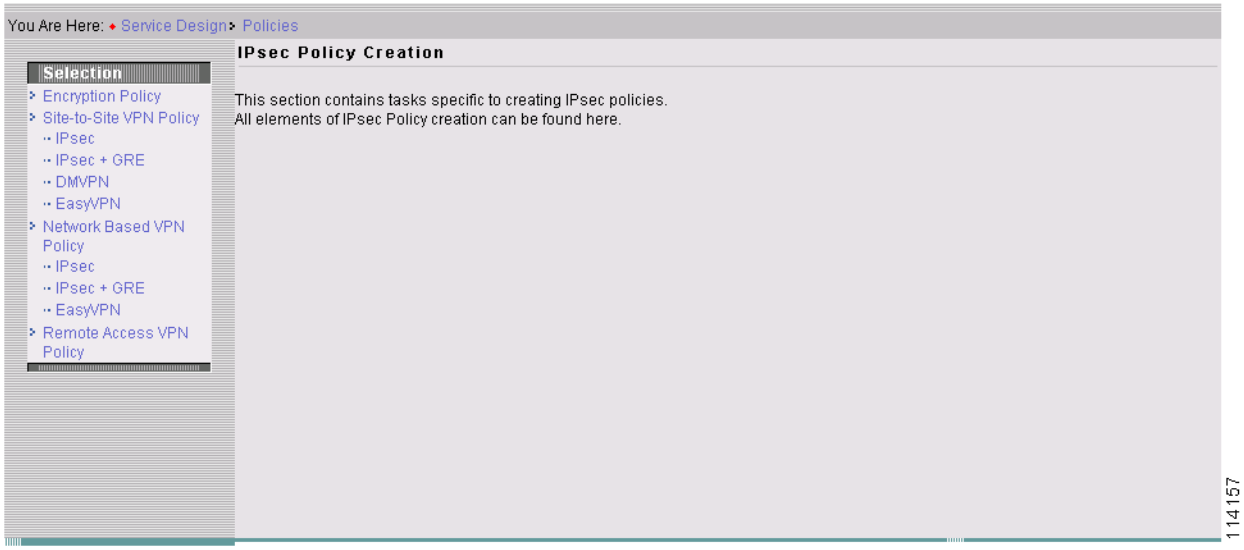
Step 1 Click **Service Design > Policies**. The Policies page appears as shown in Figure 4-5, with previously created policies displayed.

Figure 4-5 The Policies Page



Step 2 Click **Create > IPsec Policy**. The IPsec Policy Creation page appears as shown in Figure 4-6.

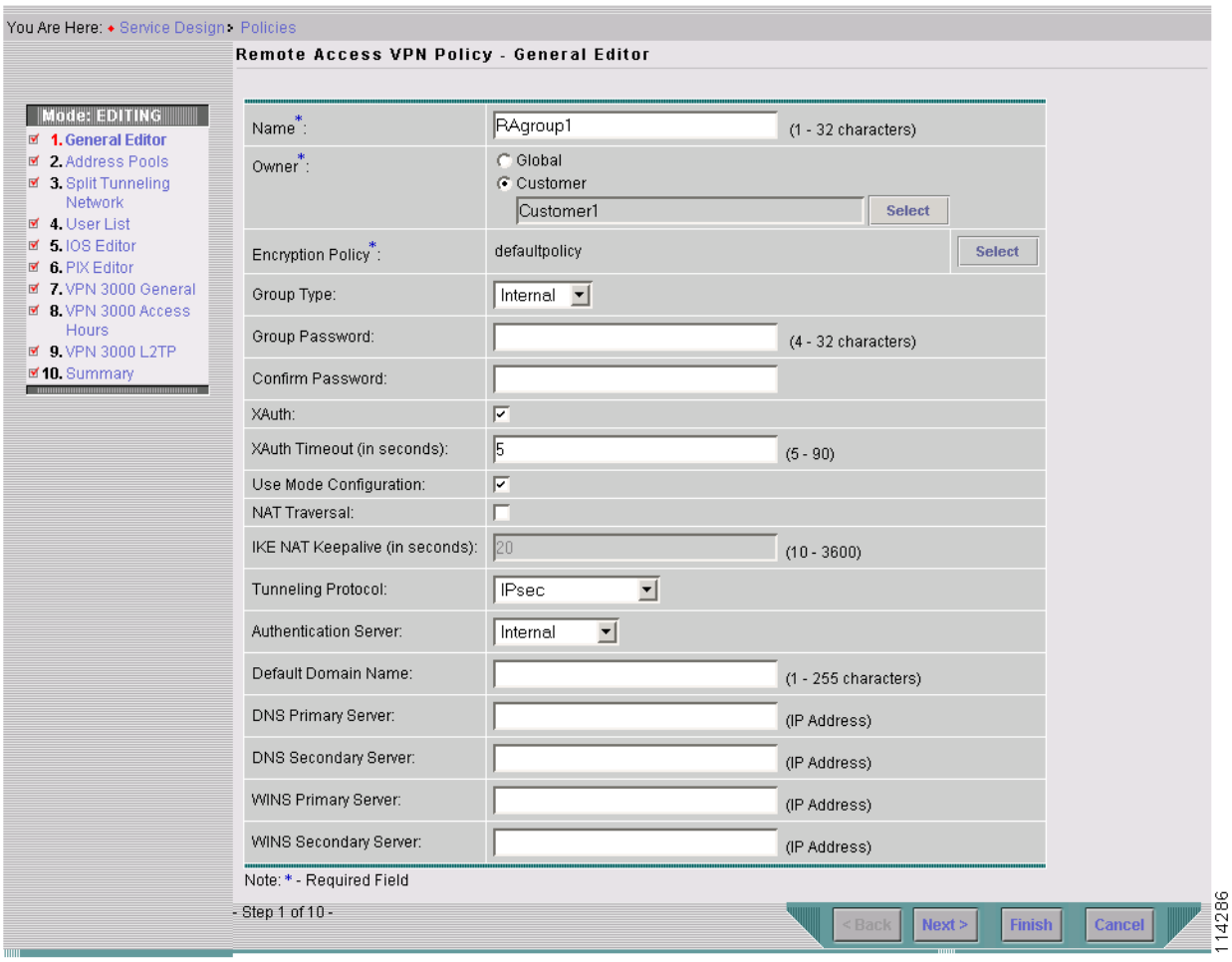
Figure 4-6 The IPsec Policy Creation Page



Step 3 Click **Remote Access VPN Policy**.

Step 4 The Remote Access VPN Policy – General Editor page appears as shown in Figure 4-7. Look at the list of steps in the table of contents (TOC) on the left of the page. These are the steps for creating a remote access VPN policy.

Figure 4-7 The Remote Access VPN Policy – General Editor Page



Step 5 Follow the instructions in Table 4-2 to enter values for the Remote Access VPN Policy – General Editor.

Table 4-2 Remote Access VPN Policy – General Editor Fields

Field Name	Type	Instructions
Name	text box	Enter a name for the policy. However, the name cannot contain spaces because it is used as the VPN group name.
Owner	radio button and **Select** button	Click **Customer > Select** and choose the customer for which the remote access VPN is intended. When you click **Customer > Select**, the Customer for IPsec Policy dialog box appears. Click the button next to the customer you want to select and click **Select** (to choose that customer), or click **Cancel** to exit the dialog box without saving changes. Both return you to the main page. Do not select **Global**. It is important to associate remote access policies with a specific customer because many remote access VPN parameters are customer-specific.
Encryption Policy	**Select** button	Choose the name of an encryption policy you created in previous steps by clicking **Select**. The encryption policy specifies the IKE and IPsec proposal parameters for the IPsec VPN and determines the level of encryption used in the IPsec VPN tunnels.
Group Type	drop-down list	Select the policy type. An internal group is configured on the VPN device while an external group is configured on an external AAA server. • **Internal** – Group attributes are on the target device. If the user profiles and group attributes are maintained on the CPE device itself, select **Internal**. • **External** – Group attributes are obtained from a AAA Server. If the user profiles and group attributes are maintained on a AAA Server, select **External**.
Group Password	text box	Required when you select **Internal** for the **Group Type** field. Enter the password (IKE preshared key) for the group. The policy name and password are very important because they are the group name and password that remote users must use when connecting through the Cisco VPN Client.
Confirm Password	text box	Re-enter the group password to verify it.
XAuth	checkbox	Check to enable IKE Extended Authentication (XAuth).
XAuth Timeout	text box	Enter the idle timeout value for XAuth. The range is from 5 to 90 seconds. The default value is 5 seconds.
Use Mode Configuration	checkbox	Mode Configuration is also known as the ISAKMP Configuration Method or Configuration Transaction. Specifically, when enabled, this option exchanges configuration parameters with the client while negotiating Security Associations (SAs). Check the **Mode Configuration** checkbox to use Mode Configuration with the IPsec clients in this group. You must enable **Mode Configuration** for IPsec clients because IPsec uses Mode Configuration to pass all configuration parameters to the client. Otherwise, these parameters are not passed to the client. Also, you must check this box to use split tunneling. Uncheck the box if you are using **L2TP over IPsec** as your tunneling protocol. **Note** The Cisco VPN Client supports Mode Configuration, but other IPsec clients may not. For example, the Microsoft Windows 2000 IPsec client does not support Mode Configuration. (The Windows 2000 client uses the PPP layer above L2TP to receive its IP address from the VPN Concentrator.) If you are using other client software packages, check for compatibility in the documentation for your client software before using this option.

Table 4-2 Remote Access VPN Policy – General Editor Fields (continued)

Field Name	Type	Instructions
NAT Traversal	checkbox	Also called NAT transparency. NAT traversal enables IPsec VPN tunnels to span multiple Network Address Translation (NAT) and Port Address Translation (PAT) domains. Without NAT traversal, IPsec VPN tunnels cannot span NAT or PAT domains due to incompatibilities between IPsec packet header requirements and address translation mechanisms. When **ON**, this option allows IPsec traffic to travel through a NAT or PAT point in the network. Requires Cisco IOS Software Release 12.2(13)T or above.
IKE NAT Keepalive (in seconds)	text box	Available only when **NAT Traversal** is enabled. The default value is 20 seconds and the range is from 10 to 3600 seconds.
Tunneling Protocol	drop-down list	Select the tunneling protocol with which this group can connect. Select **IPSec** or **L2TP over IPsec**. The **L2TP over IPsec** option is supported for the VPN 3000 only. Consequently, if you select **L2TP over IPsec**, only VPN 3000 devices will be available for use in any **IPsec RA** service request that uses this remote access policy.
Authentication Server	drop-down list	Select the authentication method for members of this user group. (The name of the Remote Access Policy becomes the user group name.) The following options are supported: • **None** – Select this option if you selected **L2TP over IPsec** as the tunnelling protocol option. If you select this option, remote users will not be authenticated by an authentication server. This option is supported for the VPN 3000 only. • **RADIUS** – Authenticate users using Remote Authentication Dial In User Service (RADIUS). The RADIUS specification is described in RFC 2865. • **Internal** – Authenticate users against a database internal to the device. • **NT Domain** – Authenticate users using an external Windows NT Domain system. • **SDI** – Authenticate users using Security Dynamics International (SDI) authentication. • **TACACS+** – Authenticate users using Terminal Access Controller Access Control System Plus (TACACS+).
Default Domain Name	text box	Enter the default domain name given to users of this group.
DNS Primary Server	text box	Enter the IP address of the primary Domain Name System (DNS) server. This option is for use with all authentication methods.
DNS Secondary Server	text box	Enter the IP address of the secondary DNS server. This option is for use with all authentication methods.
WINS Primary Server	text box	Enter the IP address of the primary Windows Internet Name System (WINS) server. This option is for use with all authentication methods.
WINS Secondary Server	text box	Enter the IP address of the secondary WINS server. This option is for use with all authentication methods.

Step 6 Click **Next** to continue to the Address Pools page as described in the "Defining Address Pools" section on page 4-10.

Note You can click **Finish** on any of the Remote Access VPN Policy pages. When you click **Finish**, the unedited policy parameters take the default settings provided by ISC, and ISC saves the policy to your repository.

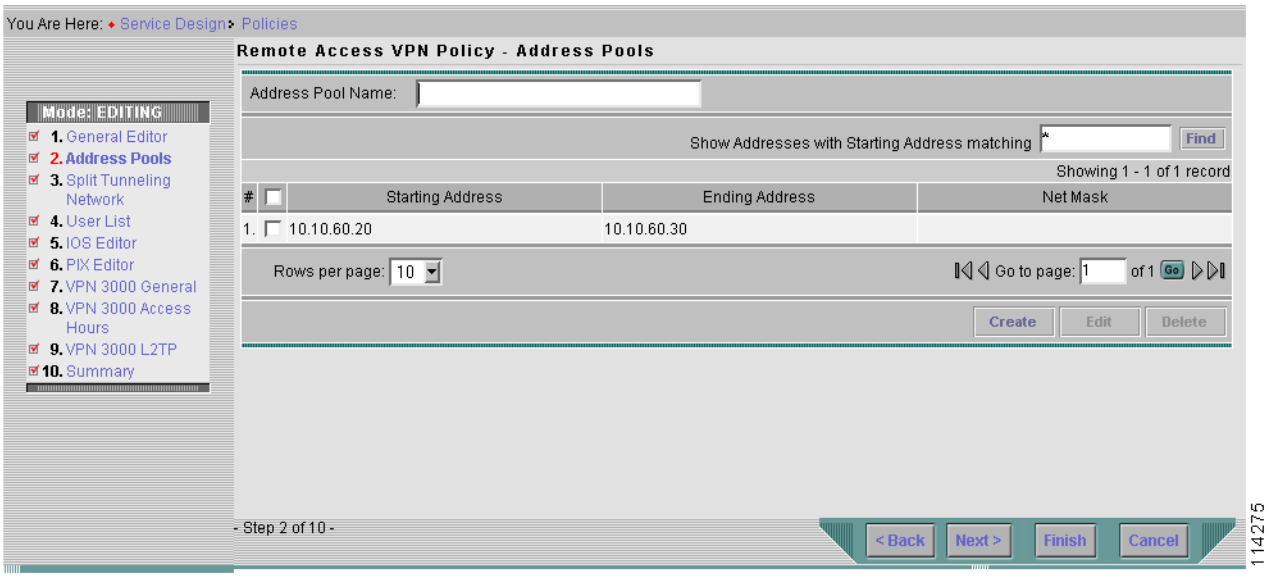
Defining Address Pools

In this section, you create the IP address pools that remote clients use to establish IPsec tunnels to the private site. Remote clients are assigned an inside IP address from these pools.

Step 1 From the Remote Access VPN Policy – General Editor page click **Address Pools**. The Remote Access VPN Policy – Address Pools page appears as shown in Figure 4-8.

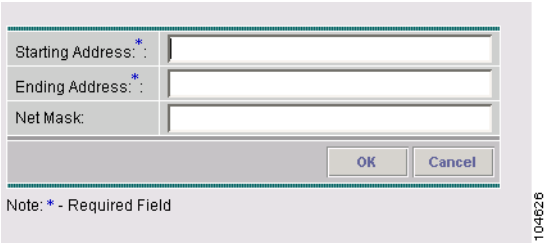
Note From the ISC home page, you can navigate to this page by clicking **Service Design** > **Policies** > **Create** > **IPsec Policy** > **Remote Access VPN Policy**, entering values in the Remote Access VPN Policy – General Editor, and then clicking **Next**.

Figure 4-8 The Remote Access VPN Policy – Address Pools Page



Step 2 Click **Create** to add the remote access IP address pool. The Address Pools dialog box appears as shown in Figure 4-9.

Figure 4-9 Address Pools Dialog Box



Step 3 Follow the instructions in Table 4-3 to enter values in the address pool fields.

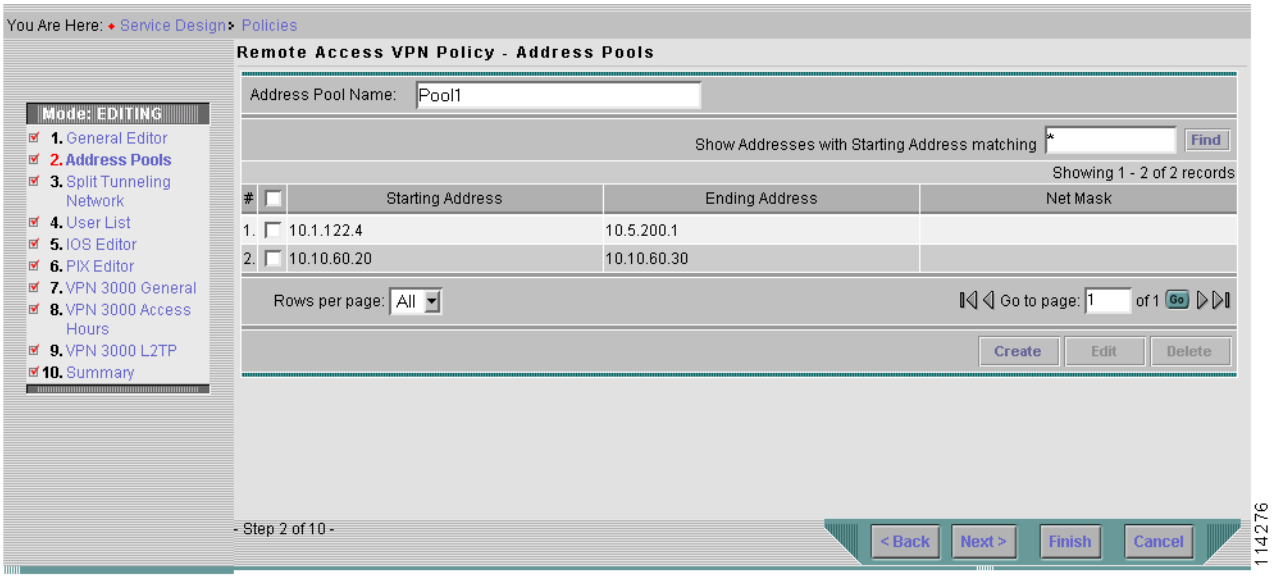
Table 4-3 Address Pools Fields

Field Name	Type	Instructions
Starting Address	text box	Enter the starting address of the IP address pool.
Ending Address	text box	Enter the ending address of the IP address pool. The address pool range must be within a single subnet.
Net Mask	text box	Enter the netmask to enable autodetection of the remote access address pool during creation of the service on the CPE devices, so that the remote access address pool can be detected by peer devices. We recommend that you enter the netmask here in the remote access policy, instead later of in the service request.

Step 4 Click **OK** when done to return to the Remote Access VPN Policy – Address Pools page.

Step 5 The **Address Pool Name** field is enabled once an Address Pool is defined, as shown in Figure 4-10. If you want to use with something other than the Cisco IOS or PIX Firewall autogenerated name for this address pool, enter a name here for the address pools defined on this page.

Figure 4-10 The Remote Access VPN Policy – Address Pools Page



Step 6 Click **Next** to continue to the Split Tunneling Network page as shown in Figure 4-11 in the "Defining Split Tunneling Networks (Optional)" section on page 4-12.

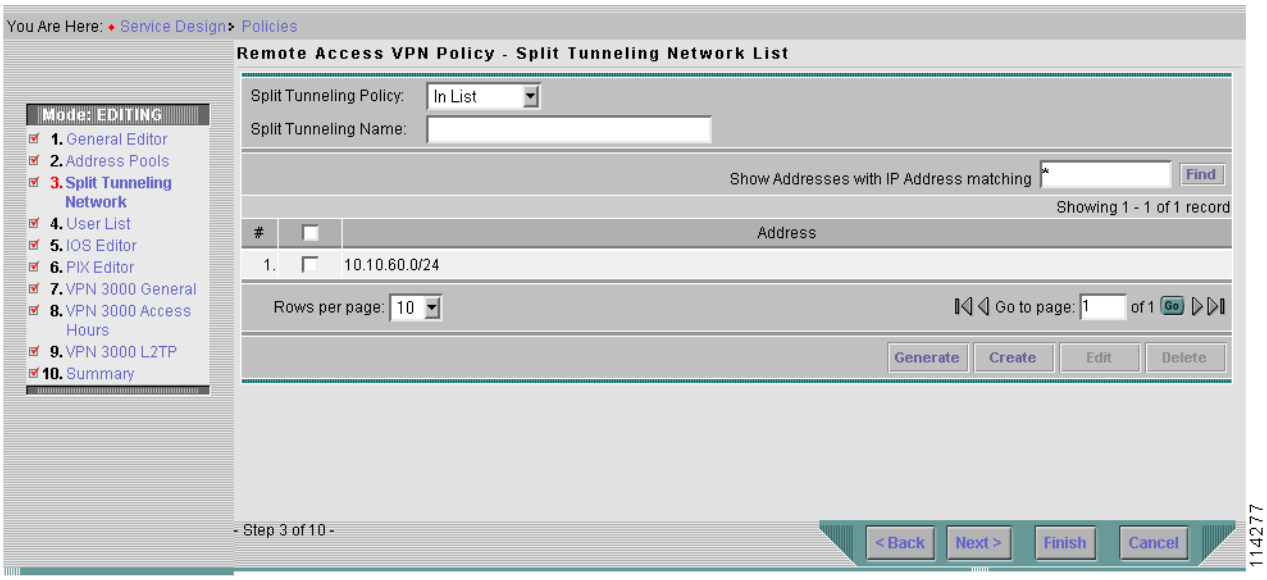
Defining Split Tunneling Networks (Optional)

You can enable or disable split tunneling for remote users. To set the split tunneling parameters, perform the following steps:

Step 1 The Remote Access VPN Policy – Split Tunneling Network List page appears as shown in Figure 4-11.

Note From the ISC home page, you can navigate to the Split Tunneling Network page by clicking **Service Design > Policies > Create > IPsec Policy > Remote Access VPN Policy**, entering values for the General Editor and Address Pools pages, and then clicking **Split Tunneling**.

Figure 4-11 Remote Access VPN Policy – Split Tunneling Network List Page



Step 2 Follow the instructions in Table 4-4 to choose your split tunneling options. For example, click **Create** to add IP addresses to the split tunneling network list.

Note Once the list is populated using **Create**, **Generate**, or both options, you can edit the list until it contains the desired networks from which traffic must travel through the IPsec tunnel.

Table 4-4 Split Tunneling Fields

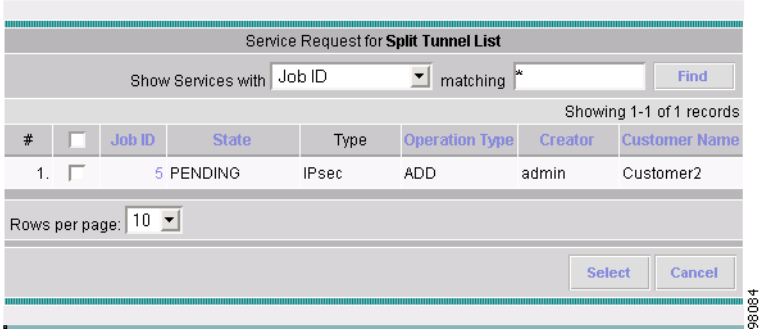
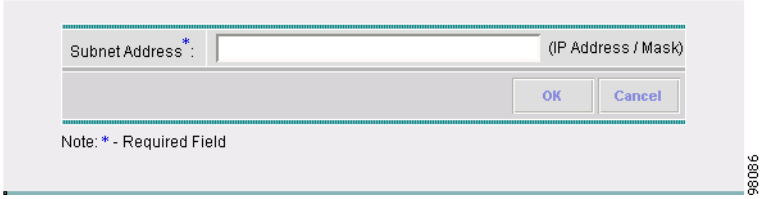
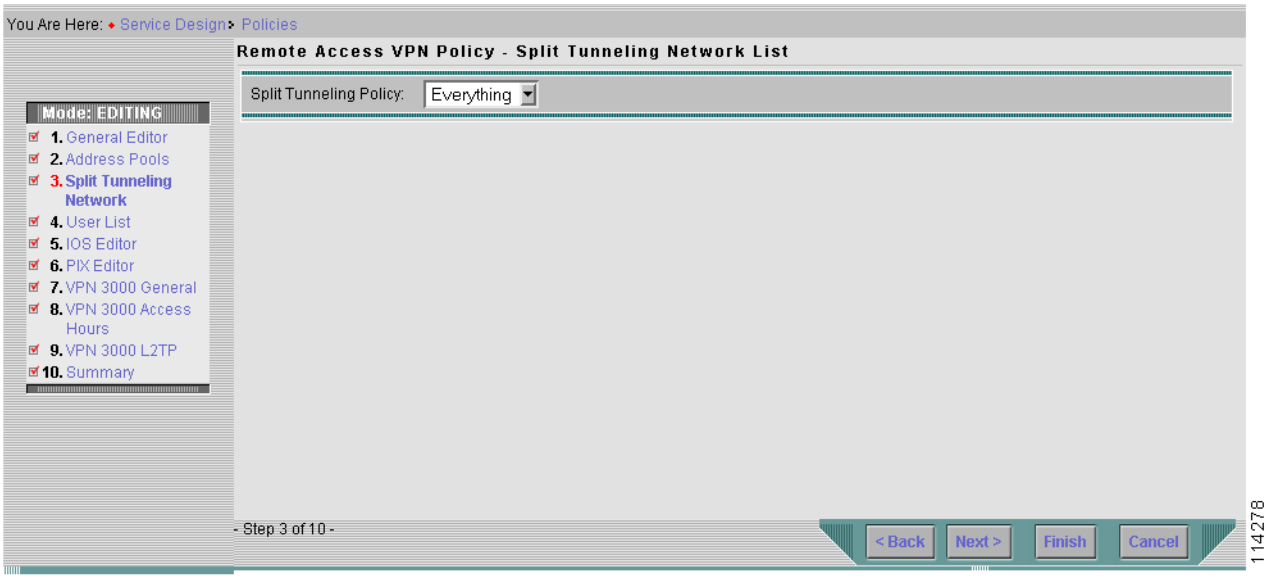
Field Name	Type	Instructions
Split Tunneling Policy	drop-down list	Select one of the following methods for split tunneling: • **Everything** – This option sends all traffic, both VPN-bound traffic and Internet-bound traffic, through the VPN tunnel to the CPE device. If you select **Everything** there are no further values enter, as shown in Figure 4-14. • **In List** – This option sends only traffic matching the listed networks through the VPN tunnel to the CPE device. The non-matching traffic is sent to the CPE device unencrypted. If you select this option, you must click **Create** or **Generate** and create the list of network addresses from which traffic travels through the IPsec tunnel. All other traffic is sent to the client LAN. • **Not In List** – Supported for the VPN 3000 only. This option sends all traffic to addresses in the selected list to the client LAN and sends all other traffic through the VPN tunnel. If you select this option, you must click **Create** or **Generate** and create the list of network addresses.
Split Tunneling Name	text box	(Optional) If you want to use a name other than the Cisco IOS or PIX Firewall autogenerated name for the list of network addresses for which split tunneling is enabled, enter the name here.
Generate	**Generate** button	Click **Generate** if you want to automatically create the list of private subnets from an existing site-to-site IPsec VPN. Since a VPN may be represented by one or more service requests, after clicking **Generate** select all the service requests from which the list of private subnets is to be extracted. When you click **Generate**, the Service Request for Split Tunnel List dialog box appears as shown in Figure 4-12. *Figure 4-12 The Service Request for Split Tunnel List Page* 
Create	**Create** button	Click **Create** and the Subnet Address for Split Tunneling dialog box appears as shown in Figure 4-13. Enter a subnet address for Split Tunneling and click **OK**. *Figure 4-13 Subnet For Split Tunneling Dialog Box* 

Figure 4-14 The Everything Option for Split Tunneling



Step 3 Click **Next** to continue to the User List page as described in the "Defining the Remote Access User List (Optional)" section on page 4-14.

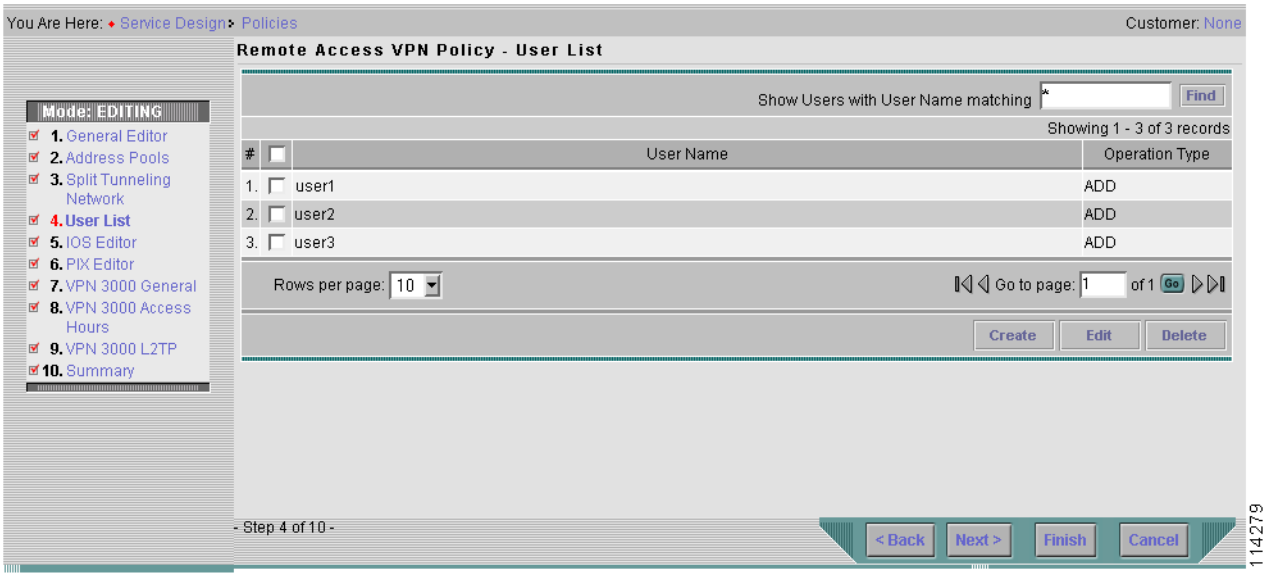
Defining the Remote Access User List (Optional)

In this section, you can enter one or more user profiles to store locally on the CPE device (as opposed to storing the user profiles on a AAA Server).

Note Use this feature only if you chose **Internal** as the user authentication method for the VPN group in the remote access policy. (This is specified in the **Authentication Server** field on the Remote Access VPN Policy – General Editor page.)

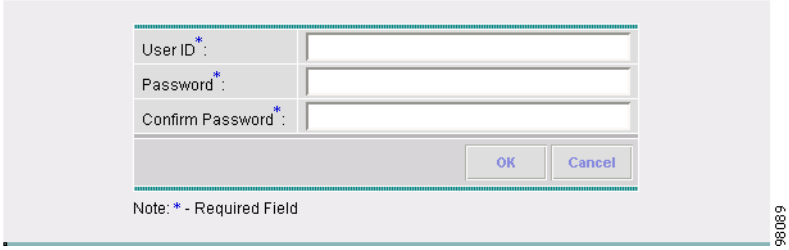
Step 1 The Remote Access VPN Policy – User List page appears as shown in Figure 4-15.

Figure 4-15 The Remote Access VPN Policy – User List Page



Step 2 Click **Create**. The User Creation dialog box appears as shown in Figure 4-16.

Figure 4-16 User List Dialog Box



Step 3 Follow the instructions in Table 4-5 to enter values in the User List dialog box fields.

Table 4-5 User List Dialog Box Fields

Field Name	Type	Instructions
User ID	text box	Enter the user name to add to the user list.
Password	text box	Enter the password for this user.
Confirm Password	text box	Retype the user password. This must match exactly what you typed in the **Password** field.

Step 4 Click **Create** again if you would like to add another user. You can enter multiple users.

Step 5 Click **OK** when done.

Step 6 Click **Next** to continue to the Cisco IOS Editor page as described in the "Defining Cisco IOS Software-Specific Parameters" section on page 4-16.

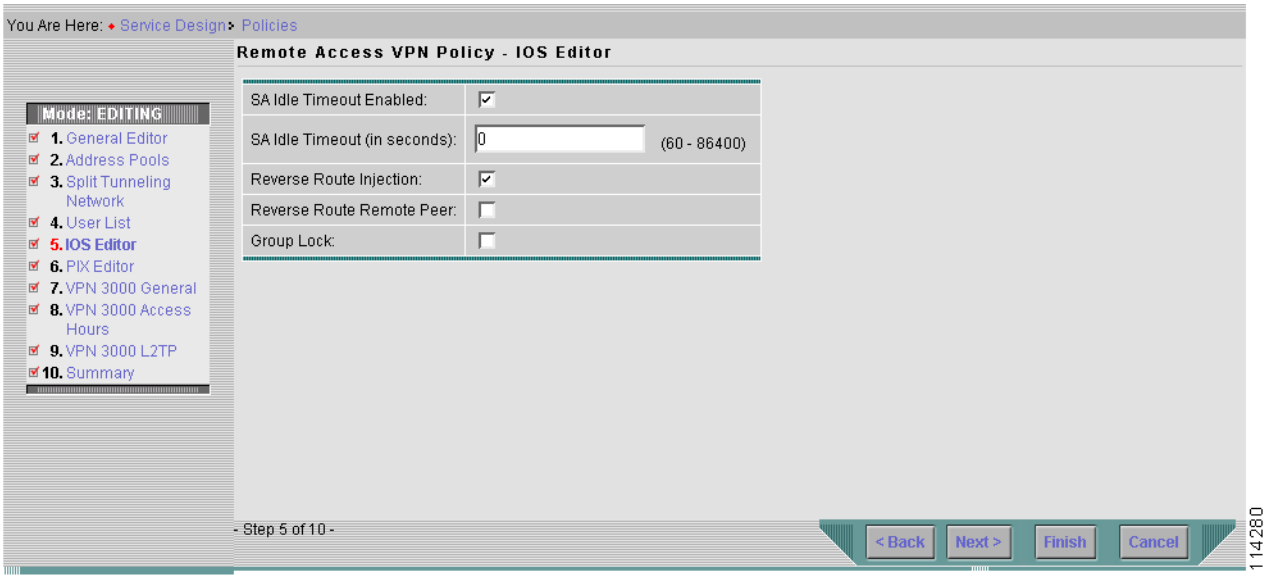
Defining Cisco IOS Software-Specific Parameters

In the Remote Access VPN Policy – Cisco IOS Editor page, you can select the values for the SA idle timeout as well as enable Reverse Route Injection (RRI). It is recommended that you select both the RRI and RRI peer options. In remote access, RRI is used to inject the host route into the routing table for the IP address that was allocated out of the remote access address pool. (RRI uses the host address as the route destination in the route entry of the routing table.) This allows the creation of a static route for a remote, protected network.

Perform the following steps if you are provisioning remote access on Cisco IOS devices in your network:

Step 1 The Remote Access VPN Policy – Cisco IOS Editor page appears as shown in Figure 4-17.

Figure 4-17 The Remote Access VPN Policy – Cisco IOS Editor Page



Step 2 Follow the instructions in Table 4-6 to set the Cisco IOS-specific parameters.

Table 4-6 Cisco IOS Editor Fields

Field Name	Type	Instructions
SA Idle Timeout Enabled	checkbox	Check to enable a security association (SA) idle timeout.
SA Idle Timeout	text box	To enable this option, you must first check **SA Idle Timeout Enabled**, and then you can enter a timeout value, from 60 to 86,4000 seconds, after which to automatically delete the IPsec security associations.

Table 4-6 Cisco IOS Editor Fields

Field Name	Type	Instructions
Reverse Route Injection	checkbox	Check to enable reverse route injection (RRI). RRI injects the host route into the routing table for the IP address that was allocated out of the remote access address pool. (RRI uses the host address as the route destination in the route entry of the routing table.) This allows the creation of a static route for a remote, protected network. This feature is also used for Network-Based Remote Access. For more information on Network-Based Remote Access, refer to the *Cisco IP Solution Center Integrated VPN Management Suite Network-Based IPsec VPN User Guide, 3.2*.
Reverse Route Remote Peer	checkbox	To enable this option, you must first check **Reverse Route Injection** and then you can check **Reverse Route Remote Peer**, as shown in Figure 4-17. The **Reverse Route Remote Peer** option creates a route in the routing table for the remote tunnel endpoint.
Group Lock	checkbox	The **Group Lock** option ties user group membership to IKE negotiation user authentication during XAuth. Check the box to enable. Uncheck the box to disable this option.

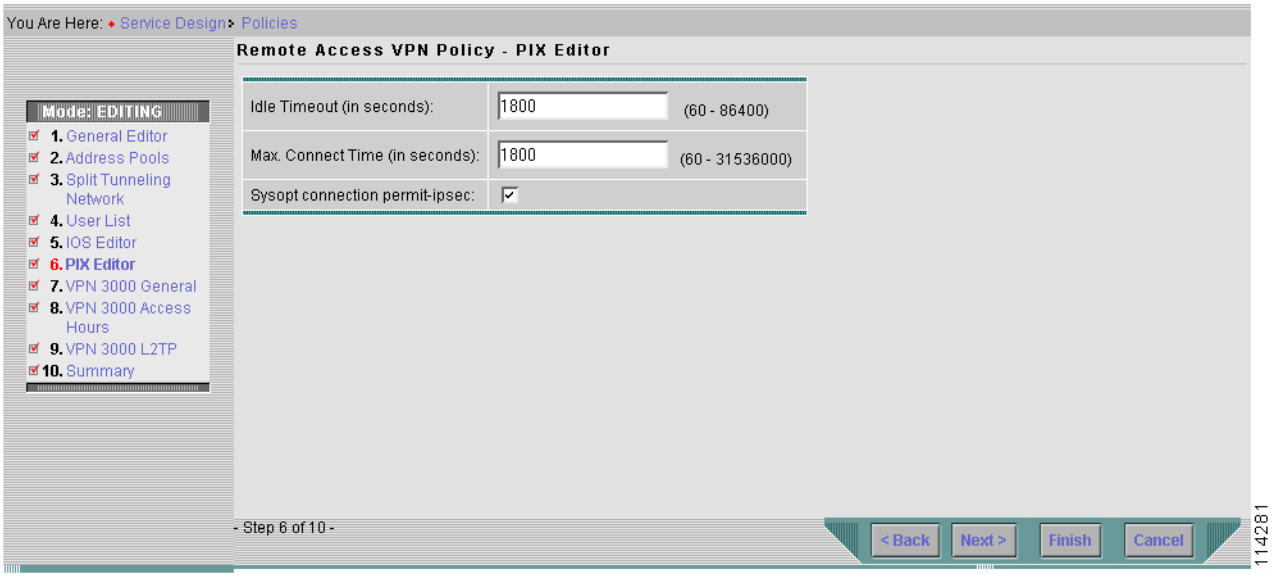
Step 3 Click **Next** to continue to the Remote Access VPN Policy – PIX Firewall Editor page as described in the "Defining PIX Firewall-Specific Parameters" section on page 4-17.

Defining PIX Firewall-Specific Parameters

Perform the following steps if you are provisioning remote access on Cisco PIX security appliances in your network:

Step 1 The Remote Access VPN Policy – PIX Firewall Editor page appears as shown in Figure 4-18.

Figure 4-18 The Remote Access VPN Policy – PIX Firewall Editor Page



Step 2 Use the instructions in Table 4-7 to enter values for the PIX Firewall-specific parameters.

Table 4-7 PIX Firewall Editor Fields

Field Name	Type	Instructions
Idle Timeout	text box	Enter the inactivity timeout for the VPN client. The default is 1800 seconds.
Max Connect Time (in seconds)	text box	Enter maximum connection time between the VPN client and server. The default is 1800 seconds.
Sysopt Connection Permit IPsec	checkbox	Check to implicitly permit IPsec traffic. The default setting is checked. This option issues a PIX Firewall **sysopt permit-ipsec-connection** command to permit IPsec traffic to pass through PIX Firewalls without checking the traffic against conduit or access-list command statements in the firewall configuration.

Step 3 Click **Next** to continue to the Remote Access VPN Policy – VPN 3000 Editor page as described in the "Defining VPN 3000-Specific Parameters" section on page 4-18.

Defining VPN 3000-Specific Parameters

Perform the following steps if you are provisioning remote access on VPN 3000 devices in your network:

Step 1 The Remote Access VPN Policy – VPN 3000 Editor page appears as shown in Figure 4-19.

Figure 4-19 The Remote Access VPN Policy – VPN 3000 Editor Page

Step 2 Follow the instructions in Table 4-8 to enter VPN 3000-specific parameters.

Table 4-8 VPN 300 Editor Fields

Field Name	Type	Instructions
Simultaneous Logins	text box	Enter the number of simultaneous logins for this group.
Min Password Length	text box	Enter the minimum password length for users in this group.
Allow Alphabetic Only Passwords	checkbox	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Strip Realm	checkbox	Check the **Strip Realm** checkbox to remove the realm qualifier of the user name during authentication. When enabled, authentication is based on the username alone. Otherwise, authentication is based on the full *username@realm* string. You must enable this option if your server is unable to parse delimiters.
Idle Timeout	text box	Enter the idle timeout in minutes for this group.
Max Connect Time	text box	Enter the maximum connection time in minutes for this group.
IKE Peer Identity	drop-down list	Select whether or not to validate the identity of the peer using the peer device certificate.
IKE Keepalives	checkbox	Check to enable the use of IKE keepalives for members of this group.
Authentication on Rekey	checkbox	Check to re-authenticate the user on an IKE (Phase-1) rekey.

Table 4-8 VPN 300 Editor Fields (continued)

Field Name	Type	Instructions
Allow IPsec Through NAT	checkbox	The **Allow IPsec through NAT** option lets you use the Cisco VPN Client to connect to the VPN Concentrator via UDP through a firewall or router that is running NAT. Enabling this feature creates runtime filter rules that forward UDP traffic for the configured port even if other filter rules on the interface drop UDP traffic. These runtime rules exist only while there is an active IPsec through NAT session. The system passes inbound traffic to IPsec for decryption and unencapsulation, and then passes it on to the destination. The system passes outbound traffic to IPsec for encryption and encapsulation, applies a UDP header, and forwards it. Check to enable the IPsec client to operate through a firewall using NAT via UDP. Uncheck (disable) this option to prevent to IPsec clients from operating through a firewall that is using NAT.
IPsec Through NAT Port	text box	If you selected **Allow IPsec Through NAT**, enter the UDP port to be used for IPsec traffic, using any port from 4001 to 49151. The default is 10000.
Allow Password Storage on Client	checkbox	Check to allow the IPsec client to store its password locally.
Banner	text box	Enter the banner text to display for this group. The banner cannot exceed 512 characters.

Step 3 Click **Next** to continue to the VPN 3000 Access Hours page as shown Figure 4-20 in the "Defining the VPN 3000 Access Hours" section on page 4-20.

Defining the VPN 3000 Access Hours

For connections made through VPN 3000 devices in your network, you can control when a user has access to your private network through the remote access VPN.

Perform the following steps to restrict user access to specific hours during the day or night:

Step 1 The Remote Access VPN Policy – Access Hours page appears as shown in Figure 4-20.

Figure 4-20 The Remote Access VPN Policy – Access Hours Page

Step 2 Follow the instructions in Table 4-9 to enter values for each day of the week.

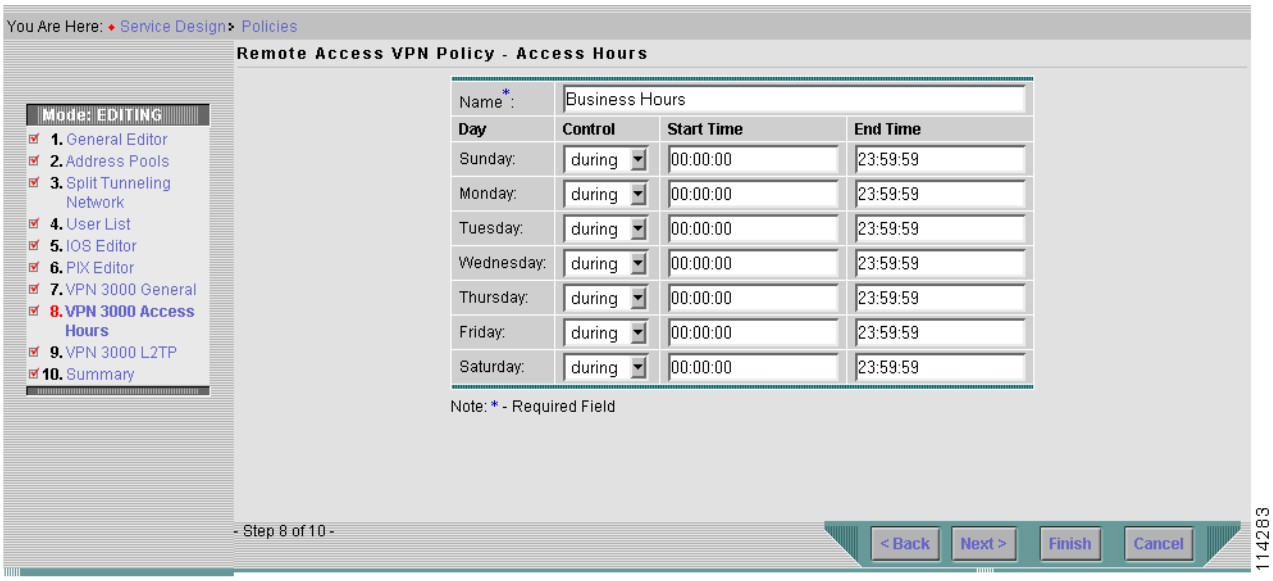


Table 4-9 Remote Access VPN Policy – Access Hours Fields

Field Name	Type	Instructions
Name	text box	Enter a name to identify the access hours assigned to this group.
Control	drop-down list	There are two control options: • **during** – Allow access during the hours in the specified range (default). • **except** – Allow access except during the hours in the specified range.
Start Time	text box in time format	Enter starting time of the access time range.
End Time	text box in time format	Enter ending time of the access time range.

Step 3 Click **Next** to continue to the VPN 3000 L2TP page as described in the "Defining the VPN 3000 L2TP Parameters" section on page 4-21.

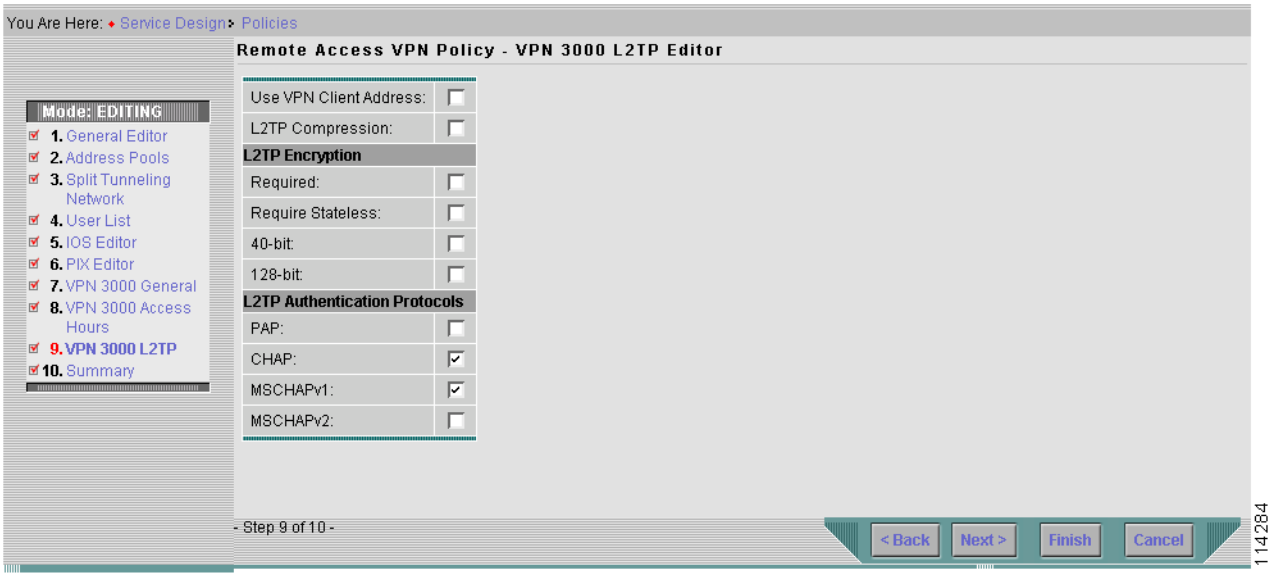
Defining the VPN 3000 L2TP Parameters

L2TP provides tunneling of PPP. An L2TP session defines the communications transactions between the LAC and the LNS that support tunneling of a single PPP connection. For further information on VPN 3000 L2TP parameters, refer to the VPN 3000 online help.

If you selected the **L2TP over IPsec** option in the Tunneling Protocols field, you must set values for the parameters in this section.

Step 1 The Remote Access VPN Policy – VPN 3000 L2TP Editor page appears as shown in Figure 4-21.

Figure 4-21 The Remote Access VPN Policy – VPN 3000 L2TP Page



Step 2 Follow the instructions in Table 4-10 to select options for VPN 3000 L2TP tunneling.

Table 4-10 Remote Access VPN Policy – VPN 3000 L2TP Editor Fields

Field Name	Type	Instructions
Use Client Address	checkbox	Check the box if you want to accept and use an IP address received from the client.
L2TP Compression	checkbox	Check the box if you want to enable compression for L2TP connections for this group.
Required	checkbox	Check the box if you want to require encryption.
Require Stateless	checkbox	When enabled, during connection setup the L2TP clients must agree to use stateless encryption to encrypt data or they will not be connected. With stateless encryption, the encryption keys are changed on every packet. Otherwise, the keys are changed after some number of packets or whenever a packet is lost. Stateless encryption is more secure, but it requires more processing. However, its performance can improve in a lossy environment (where packets are lost), such as the Internet. This option is unchecked (disabled) by default. Do not check this option if you use the **NT Domain** option for user authentication. The NT Domain authentication cannot negotiate encryption. Check the box if you want to enable stateless encryption.
40-Bit	checkbox	Check the box if you want to use 40-bit encryption.
128-Bit	checkbox	Check the box if you want to use 128-bit encryption.
PAP	checkbox	Check the box to use Password Authentication Protocol (PAP), or uncheck the box to disable use of this protocol.
CHAP	checkbox	Check the box to use Challenge-Handshake Authentication Protocol (CHAP), or uncheck the box to disable use of this protocol.

Table 4-10 Remote Access VPN Policy – VPN 3000 L2TP Editor Fields (continued)

Field Name	Type	Instructions
MSCHAPv1	checkbox	Check the box to use Microsoft Challenge-Handshake Authentication Protocol version 1 (MSCHAPv1), or uncheck the box to disable use of this protocol.
MSCHAPv2	checkbox	Check the box to use Microsoft Challenge-Handshake Authentication Protocol version 2 (MSCHAPv2), or uncheck the box to disable use of this protocol.

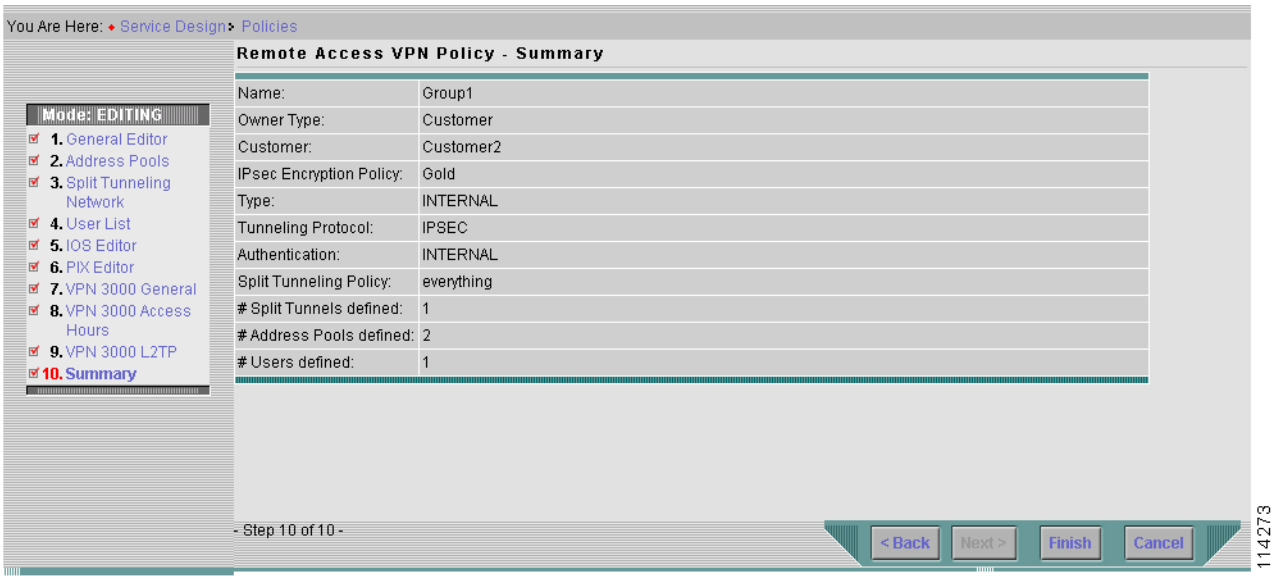
Step 3 Click **Next** to continue to the Remote Access VPN Policy Summary page as described in the "Summary Page" section on page 4-23.

Summary Page

When you have completed entering all the remote access parameters, the Remote Access VPN Policy – Summary page is displayed. Perform the following steps to save your remote access policy:

Step 1 The Remote Access VPN Policy – Summary page appears as shown in Figure 4-22.

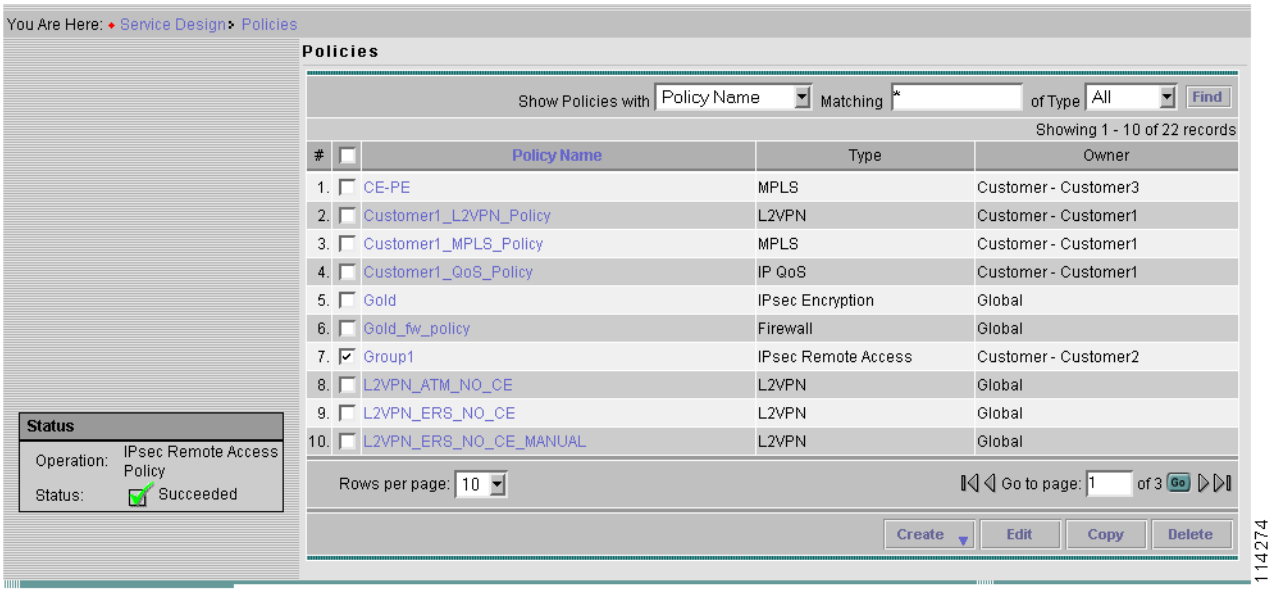
Figure 4-22 The Remote Access VPN Policy – Summary Page



Step 2 Click **Finish** when you are done reviewing the VPN policy summary, or click **Back** to return to a previous page within the Remote Access VPN Policy pages to update a parameter.

Step 3 After you click **Finish**, the Polices page appears with the status of the policy displayed in the lower left corner of the page, under **Status**, as shown in Figure 4-23.

Figure 4-23 The Policies Page with Policy Status Displayed



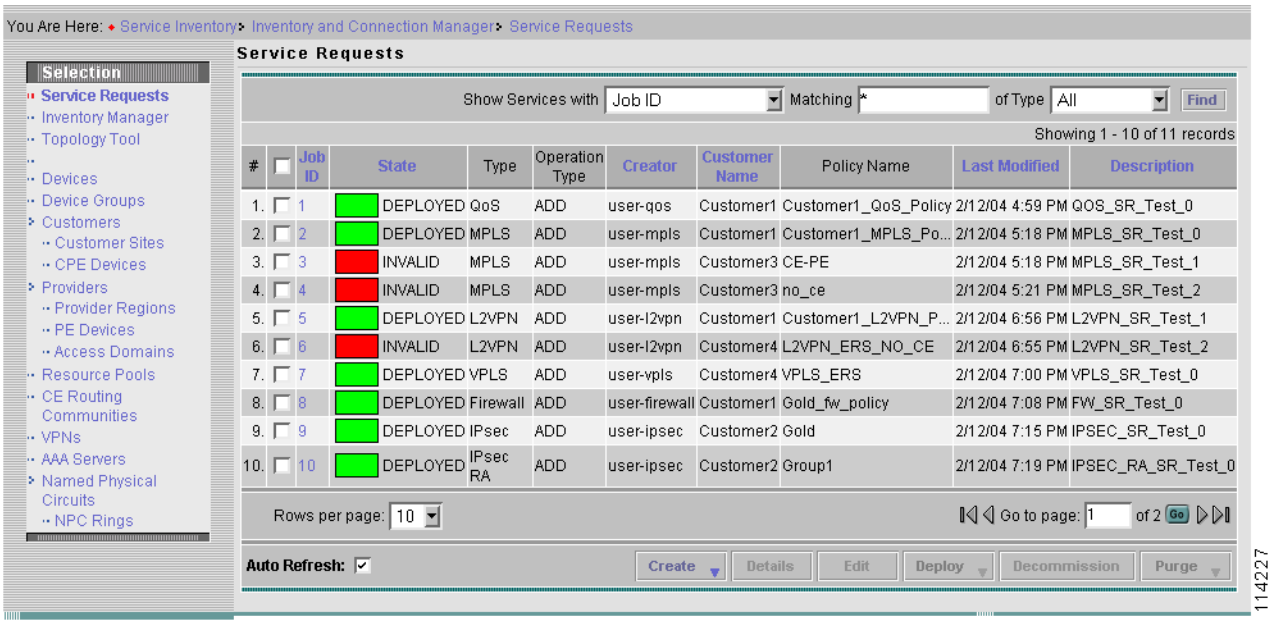
Step 4 Continue on to the "Creating Remote Access VPN Service Requests" section on page 4-25.

Creating Remote Access VPN Service Requests

Once the remote access policy is created, perform the following steps to create a remote access service request:

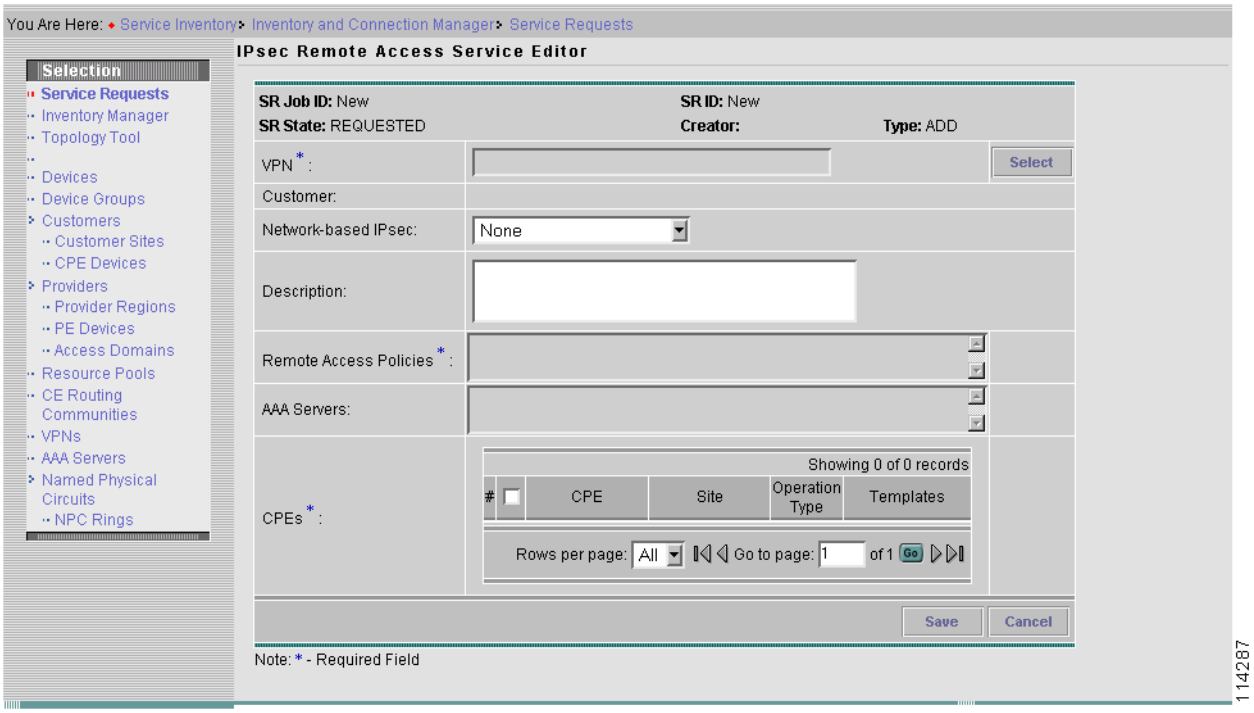
Step 1 Click **Home > Service Inventory > Inventory and Connection Manager > Service Requests**. The Service Requests page appears as shown in Figure 4-24.

Figure 4-24 The Service Requests Page



Step 2 Click **Create > IPsec RA**. The IPsec Remote Access Service Editor page appears as shown in Figure 4-25.

Figure 4-25 IPsec Remote Access Service Editor Page



Step 3 Follow the instructions in Table 4-11 to enter values for the IPsec Remote Access Service Editor fields.

Table 4-11 IPsec Remote Access Service Editor Fields

Field Name	Type	Instructions
VPN	**Select** button	Click **Select**. Choose the VPN you defined for your remote access policy. Click **OK**. The IPsec Remote Access Service Editor page appears as shown in Figure 4-28.
Network-based IPsec	drop-down list	Set to **None** unless you are using IPsec-to-MPLS mapping. For information on IPsec-to-MPLS mapping, refer to the *Cisco IP Solution Center Integrated VPN Management Suite Network-Based IPsec VPN User Guide, 3.2*.
Description	text box	(Optional) Enter a description to identify this particular service request.

Table 4-11 IPsec Remote Access Service Editor Fields (continued)

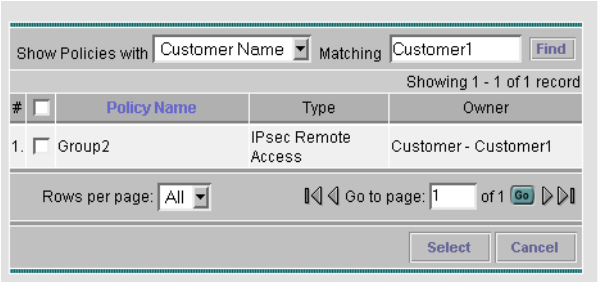
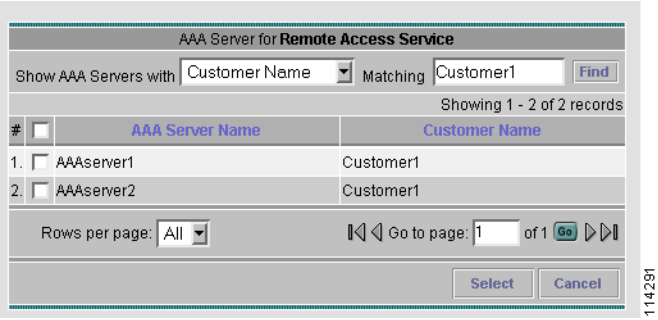
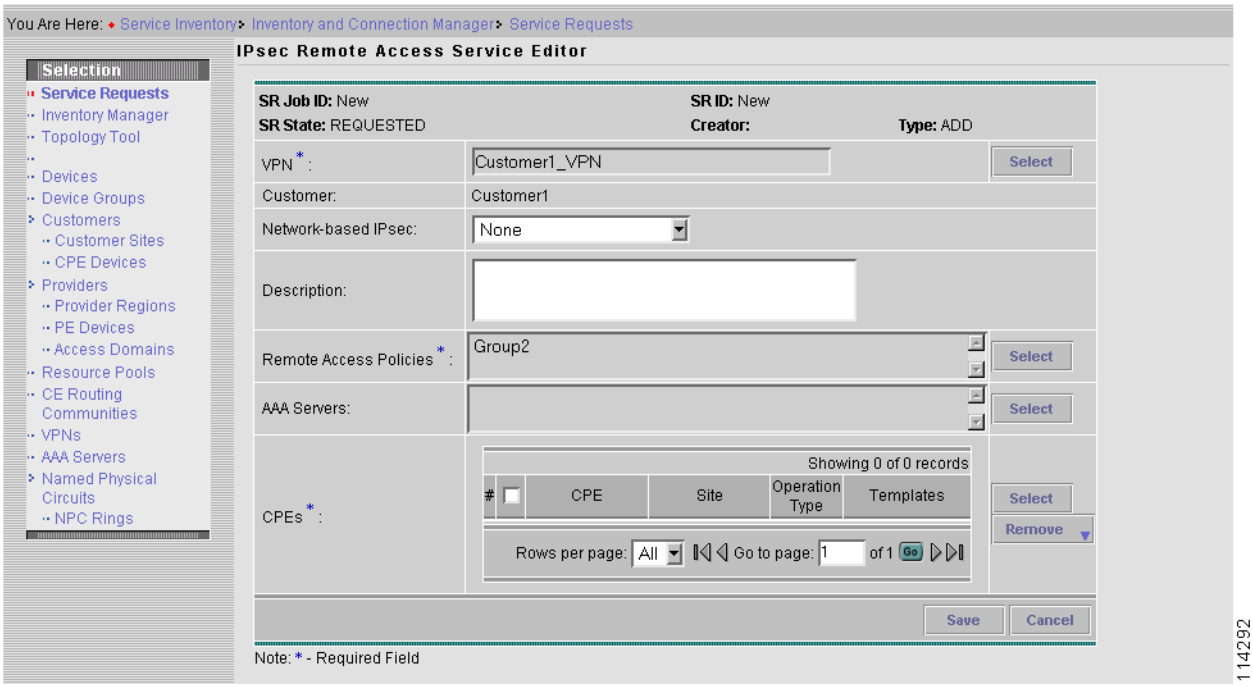
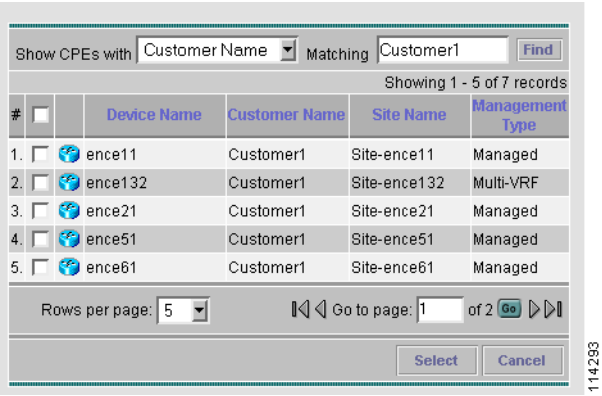
Field Name	Type	Instructions
Remote Access Policies	list	Specify the remote access policy to use in this service request by clicking **Select**. The Policy for Remote Access Service page appears as shown in Figure 4-26. Choose the policy and click **Select**. You can select multiple remote access policies. Each Remote Access Policy defines a user group, and using multiple remote access policies in the same service request enables you to configure multiple user groups on the same CPE device. ***Figure 4-26 The Policy for Remote Access Service Page*** 
AAA Servers	list	Specify the AAA server by clicking **Select**. The AAA Server for Remote Access Service page appears as shown in Figure 4-27. Choose the AAA server and click **Select**. You can select multiple AAA servers, for example, if you are using different servers for authentication and accounting or to configure backup AAA servers. (Optional) **AAA Server interface –** Specify an IP address of an interface to use for all outgoing RADIUS packets. Choose the AAA server Interface and click **Select**. ***Figure 4-27 The AAA Server for Remote Access Service Page*** 
CPEs	row	Continue to Step 4 for instructions on how to add CPE devices to your service request.

Figure 4-28 The IPsec Remote Access Service Editor Page with VPN and Policy Selected



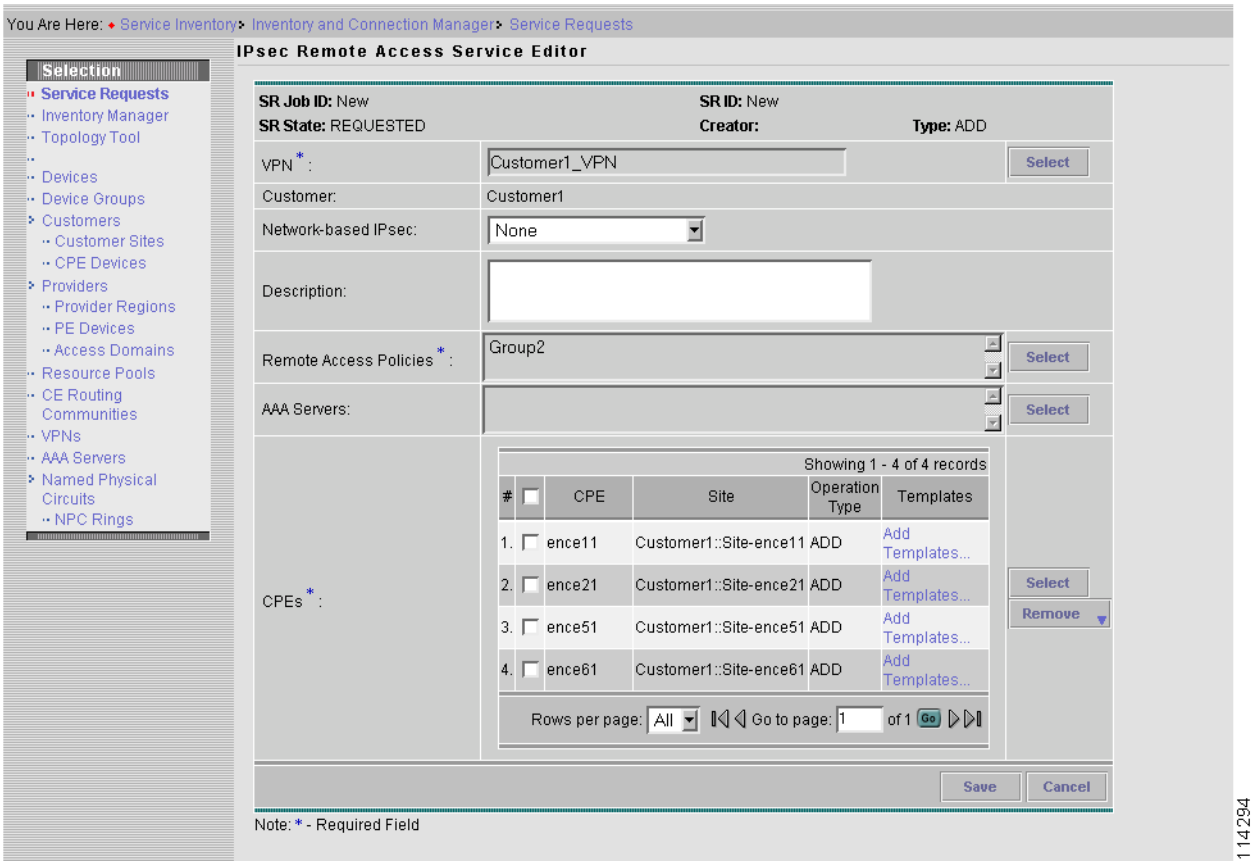
Step 4 On the main IPsec Remote Access Service Editor page, click the **Select** button in the **CPEs** row. The CPEs Associated with Remote Access Service dialog box appears as shown in Figure 4-29.

Figure 4-29 CPEs Associated with Remote Access Service Dialog Box



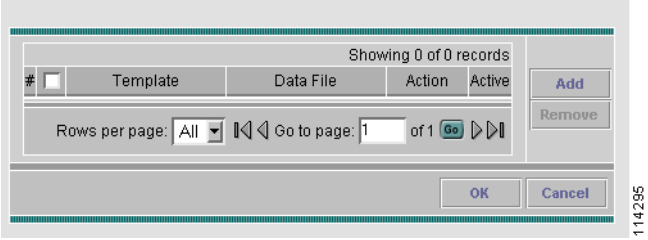
Step 5 Check the box next to the CPE devices you want in your remote access service request and click **Select**. The CPE devices you select will appear in the IPsec Remote Access Service Editor page, as shown in Figure 4-30.

Figure 4-30 The IPsec Remote Access Service Editor Page with CPEs Selected



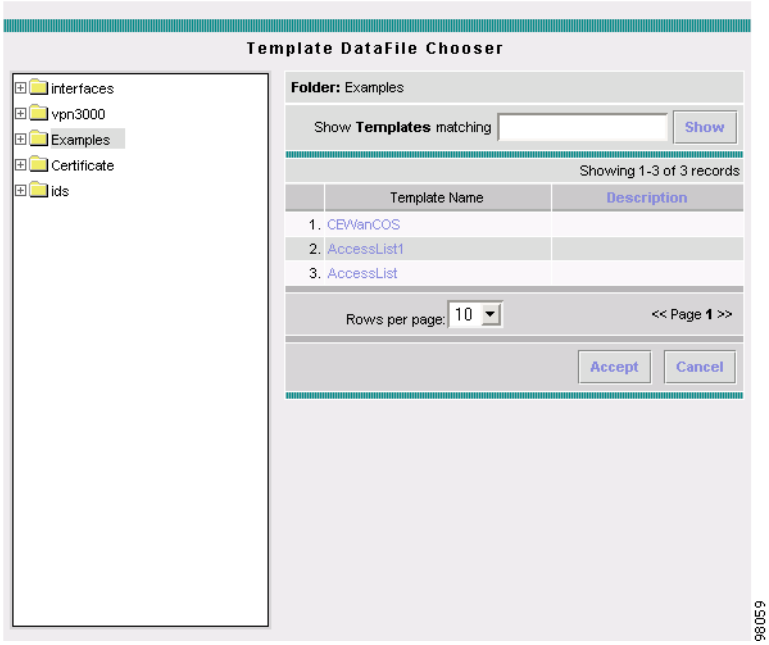
Step 6 (Optional) Click **Add Templates** to add a template to the service request. For features not supported by ISC, a template can be added to the service request and ISC will download the additional configuration information contained in the template to the CPE device. When you click on **Add Templates**, the Add/Remove Templates dialog box appears as shown in Figure 4-31.

Figure 4-31 Add/Remove Templates Dialog Box



Step 7 Click **Add**. The Template DataFile Chooser page appears as shown in Figure 4-32.

Figure 4-32 The Template DataFile Chooser Page



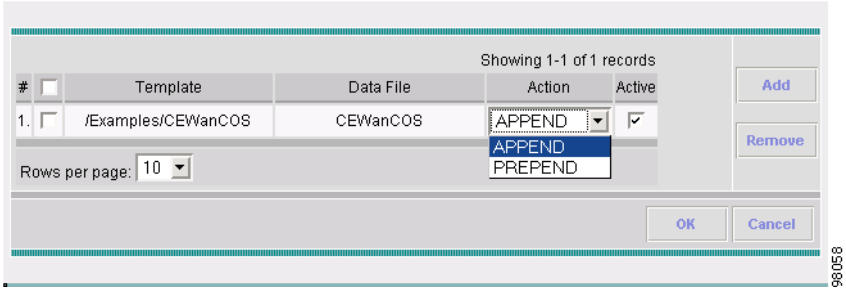
Step 8 The templates are in the left column and the associated data files are on the right. Choose a folder of templates or a single template by highlighting it. The page updates and displays the associated templates on the right side of the page.

Note If you are using a Sybase repository, sample templates are pre-populated in the embedded, empty repository that is shipped with your ISC software. These templates appear in the right side pane of the **Template Manager** window (which is directly accessible through **Service Design** > **Template Manager**). If you are using an Oracle repository, the new, empty repository for use with your ISC software is created during installation and, consequently, the sample templates are not pre-populated and will not appear in the Template Manager window. For information on adding templates to your repository, refer to the *Cisco IP Solution Center Infrastructure Reference, 3.2*.

Step 9 Check the box next to the templates you want to add to the CPE device configuration. To view the configlets for a template, check the box next to the template and click **View**.

Step 10 Click **Accept** to return to the Add/Remove Templates dialog box.

Figure 4-33 Add/Remove Templates Dialog Box with Template Added



Step 11 For each template, chose the appropriate fields as described in Table 4-12.

Table 4-12 Add/Remove Template Dialog Box Fields

Field Name	Type	Instructions
Action	drop-down list	Select one of the following options: • **APPEND** – Appends the template to the configlet generated by the service request (adds it after the other service request configlets). • **PREPEND** – Prepends the template to the configlet generated by the service request (adds it before the other service request configlets).
Active	checkbox	Check the **Active** box to enable deployment of the template. Unless you check **Active**, the template will not be instantiated. This allows you to temporarily disable a template on the devices in this service request, by unchecking the **Active** box and redeploying the service request.

Step 12 Click **OK** in the Add/Remove Templates dialog box.

Step 13 Click **Save** when done.

Step 14 Continue to the "Deploying Service Requests" section on page 7-1.