



# APPENDIX H

## Remote Access VPN User Interface Reference

---

The pages that you access by selecting the **Remote Access VPN** folder from the **Policy** selector in **Device View** enable you to configure remote access VPNs. The following topics describe the pages that help you configure remote access VPNs for Cisco IOS security routers, PIX Firewalls, Catalyst 6500/7600 devices, and Adaptive Security Appliance (ASA) devices and the policies that will be assigned to them.



### Note

- You must have read-write permissions to modify a remote access VPN policy. For more information, see [Modify Policies Permissions, page 2-14](#).
- You can also discover policies on devices in remote access VPNs that are already deployed in your network, so that Security Manager can manage them. For more information, see [Discovering Remote Access VPN Policies, page 10-2](#).

These topics describe the main pages available from the Remote Access VPN folder:

- [Remote Access Configuration Wizard, page H-2](#)
- [User Group Policy Page, page H-3](#)
- [Tunnel Group Policy Page, page H-4](#)
- [Remote Access VPN Defaults Page, page H-15](#)
- [IPsec Proposal Page, page H-16](#)

- [IKE Proposal Page, page H-36](#)
- [High Availability Page, page H-37](#)
- [Public Key Infrastructure Page, page H-39](#)
- [VPN Global Settings Page, page H-42](#)
- [ASA Cluster Load Balance Page, page H-50](#)
- [DN Matching Policy Page, page H-52](#)
- [DN Matching Rules Page, page H-54](#)

## Remote Access Configuration Wizard

Use the Remote Access Configuration wizard to configure your device with the policies that enable it to act as a remote access VPN server.

Depending on the device type, you must configure a user group or tunnel group policy first. A user group policy is configured on an IOS security router, PIX Firewall, or Catalyst 6500/7600 device. Tunnel group policies are configured on ASA devices or PIX Firewalls version 7.0. Other policies are then assigned to the device. These can be factory default policies provided by Security Manager or shared policies that were created in Security Manager. See [Assigning the Default Remote Access VPN Policies, page 10-11](#).



### Note

---

You cannot use the wizard to edit a remote access VPN. Each time you launch the wizard, any previous user group (or tunnel group) policy assignment is removed from the device, and you must create it again.

---

The following topics describe the steps in the Remote Access Configuration wizard:

- [User Group Policy Page, page H-3](#)
- [Tunnel Group Policy Page, page H-4](#)
- [Remote Access VPN Defaults Page, page H-15](#)



### Tip

---

You can also configure a user group or tunnel group policy on your device from the Remote Access VPN Policies folder.

---

### Navigation Path

1. Click the **Device View** button on the toolbar.
2. From the Device selector, select the device to configure as your remote access server.
3. Select **Remote Access VPN > Configuration Wizard** from the Policy selector.

### Related Topics

- [Using the Remote Access Configuration Wizard, page 10-4](#)

## User Group Policy Page

Use the User Group Policy page to specify the user groups you want to use for your remote access VPN server.



#### Note

---

The User Group Policy page is available if the selected device is a Cisco IOS router, PIX 6.3 Firewall, or Catalyst 6500/7600 device.

---

### Navigation Path

Do one of the following in Device view:

- Open the [Remote Access Configuration Wizard, page H-2](#), then click **Remote Access Configuration Wizard**.
- Select **Remote Access VPN > User Group Policy** from the Policy selector.



#### Note

---

You can also open the User Group Policy page from Policy view. For more information, see [Managing Shared Remote Access VPN Policies in Policy View, page 10-35](#).

---

### Related Topics

- [Remote Access Configuration Wizard, page H-2](#)
- [User Group Policies in Remote Access VPNs, page 10-6](#)
- [Configuring User Group Policies, page 10-7](#)

- [Understanding User Group Objects, page 8-180](#)
- [Creating User Group Objects, page 8-181](#)

### Field Reference

**Table H-1**      *User Group Policy Page*

Element	Description
Available User Groups	<p>Lists the predefined user groups available for selection.</p> <p>Select the required user groups and click &gt;&gt;.</p> <p>In Security Manager, user groups are objects. If the required user group is not in the list, click <b>Create</b> to open the User Groups Editor dialog box, which enables you to create or edit a user group object.</p>
Selected User Groups	<p>Displays the selected user groups.</p> <p>To remove a user group from this list, select it and click &lt;&lt;.</p> <p>To modify the properties of a user group, select it and click <b>Edit</b>.</p>
>> button	Click to move a selected user group from the Available User Groups list to the Selected User Groups list.
<< button	Click to remove a selected user group from the Selected User Groups list to the Available User Groups list.
Save button	<p>Available only if you opened this page from the Remote Access VPN Policies folder, and if you are authorized to modify this policy.</p> <p>Saves your changes to the server but keeps them private.</p> <p><b>Note</b> To publish your changes, click the <b>Submit</b> button on the toolbar.</p>

## Tunnel Group Policy Page

Use the Tunnel Group Policy page to view the tunnel group policies defined on your remote access VPN server. From this page, you can create tunnel group policies or edit existing policies.



**Note** The Tunnel Group Policy page is available only for PIX Firewalls version 7.0, or ASA devices.

### Navigation Path

Do one of the following in Device view:

- Open the [Remote Access Configuration Wizard, page H-2](#), then click **Remote Access Configuration Wizard**.
- Select **Remote Access VPN > Tunnel Group Policy (PIX 7.0/ASA)** from the Policy selector.



**Note** You can also open the Tunnel Group Policy page from Policy view. For more information, see [Managing Shared Remote Access VPN Policies in Policy View, page 10-35](#).

### Related Topics

- [Tunnel Group Policies in Remote Access VPNs, page 10-8](#)
- [Configuring Tunnel Group Policies, page 10-9](#)
- [Remote Access Configuration Wizard, page H-2](#)
- [Tunnel Group Editor Dialog Box, page H-6](#)

### Field Reference

**Table H-2** *Tunnel Group Policy (PIX 7.0/ASA) Page*

Element	Description
Tunnel Group Name	The name of the tunnel group that contains the policies for the tunnel connection.
Group Policy Name	The name of the group policy to be applied to the tunnel group. A group policy is a collection of user-oriented attribute/value pairs stored either internally on the device or externally on a RADIUS server.

**Table H-2** Tunnel Group Policy (PIX 7.0/ASA) Page (continued)

Element	Description
Create button	Click to create a tunnel group policy. The Tunnel Group Policy Editor dialog box opens. See <a href="#">Tunnel Group Editor Dialog Box, page H-6</a> .
Edit button	Select the row of a tunnel group in the table, then click to open the Tunnel Group Policy Editor dialog box for editing the selected tunnel group. See <a href="#">Tunnel Group Editor Dialog Box, page H-6</a> .
Delete button	Select the rows of one or more tunnel groups, then click to delete.
Save button	Available if you opened this page from the Remote Access VPN Policies folder, and if you are authorized to modify this policy.  Saves your changes to the server but keeps them private.  <b>Note</b> To publish your changes, click the <b>Submit</b> button on the toolbar.

## Tunnel Group Editor Dialog Box

Use the Tunnel Group Editor dialog box to create or edit tunnel group policies on your remote access VPN server.



### Note

This dialog box is available only when the selected device is a PIX Firewall version 7.0, or an ASA device.

The following tabs are available on the Tunnel Group Policy Editor dialog box:

- [Tunnel Group Editor > General Tab, page H-7](#)
- [Tunnel Group Editor > IPsec Tab, page H-10](#)
- [Tunnel Group Editor > Advanced Tab, page H-12](#)
- [Tunnel Group Editor > Client VPN Software Update Tab, page H-14](#)

### Navigation Path

Open the [Tunnel Group Policy Page, page H-4](#), then click **Create**, or select a device in the table and click **Edit**. For more information, see [Table H-2 on page H-5](#).

**Related Topics**

- [Tunnel Group Policies in Remote Access VPNs, page 10-8](#)
- [Configuring Tunnel Group Policies, page 10-9](#)
- [Tunnel Group Editor Dialog Box, page H-6](#)

**Tunnel Group Editor > General Tab**

Use the General tab of the Tunnel Group Policy Editor to specify the global AAA settings for your tunnel group. On this tab you can also select the method (or methods) of address assignment to use.

**Navigation Path**

Open the [Tunnel Group Editor Dialog Box, page H-6](#), or click the **General** tab from any other tab on the Tunnel Group Policy Editor.

**Related Topics**

- [Tunnel Group Policies in Remote Access VPNs, page 10-8](#)
- [Configuring Tunnel Group Policies, page 10-9](#)
- [Tunnel Group Editor Dialog Box, page H-6](#)
- [Creating ASA User Group Objects, page 8-45](#)
- [Creating AAA Server Group Objects, page 8-19](#)
- [Creating Network/Host Objects, page 8-130](#)

**Field Reference**

**Table H-3** *Tunnel Group Editor Dialog Box > General Tab*

Element	Description
Tunnel Group Name	The name of the tunnel group that contains the policies for this IPsec connection.

Table H-3 Tunnel Group Editor Dialog Box &gt; General Tab (continued)

Element	Description
Group Policy	<p>The group policy to be applied to the tunnel group. A group policy is a collection of user-oriented attribute/value pairs stored either internally on the device or externally on a RADIUS server.</p> <p>Click <b>Select</b> to open a dialog box that lists all available ASA user groups and enables you to create an ASA group policy object.</p>
<b>AAA</b>	
Authentication Server Group	<p>The name of the authentication server group (LOCAL if the users are defined on the local device).</p> <p><b>Note</b> The default is LOCAL.</p> <p>Click <b>Select</b> to open a dialog box that lists all available AAA server groups and enables you to create AAA server group objects.</p> <p><b>Note</b> If you want to set the authentication server group per interface, click the <b>Advanced</b> tab.</p>
User LOCAL if Server Group fails	<p>When selected, enables fallback to the local database for authentication, if the selected authentication server group fails.</p>
Authorization Server Group	<p>The name of the authorization server group (LOCAL, external server, or none).</p> <p>Click <b>Select</b> to open a dialog box that lists all available AAA server groups and enables you to create AAA server group objects.</p>
User must exist in the authorization database to connect	<p>When selected, specifies that the username of the remote client must exist in the database so that a successful connection can be established. If the username does not exist in the authorization database, then the connection is denied.</p>

Table H-3 Tunnel Group Editor Dialog Box &gt; General Tab (continued)

Element	Description
Accounting Server Group	<p>The name of the accounting server group (LOCAL, external server, or none).</p> <p>Click <b>Select</b> to open a dialog box that lists all available AAA server groups and enables you to create AAA server group objects.</p>
Strip Realm from Username	<p>When selected, removes the realm from the username before passing the username to the AAA server. A realm is an administrative domain. Enabling this option allows the authentication to be based on the username alone.</p> <p>You must select this check box if your AAA server cannot parse delimiters.</p>
Strip Group from Username	<p>When selected, removes the group name from the username before passing the username to the AAA server. Enabling this option allows the authentication to be based on the username alone.</p> <p>You must select this check box if your server cannot parse delimiters.</p>
<b>Client Address Assignment</b>	
DHCP Server	<p>The servers to use for client address assignments. The server uses the DHCP servers in the order listed. You can add up to 10 servers.</p> <p>The DHCP Server field displays a default DHCP server. DHCP servers are network objects. If you want to use a different DHCP server, or select additional DHCP servers, click <b>Select</b> to open the Network/Hosts selector that lists all available network hosts and enables you to create network host objects.</p>

**Table H-3** Tunnel Group Editor Dialog Box > General Tab (continued)

Element	Description
Address Pools	<p>The local address pools from which IP addresses will be assigned. The server uses these pools in the order listed. If all addresses in the first pool have been assigned, it uses the next pool, and so on. You can specify up to 6 pools.</p> <p>Address pools are predefined network objects. If you want to use a different address pool, or select additional address pools, click <b>Select</b> to open the Network/Hosts selector that lists all available network hosts and enables you to create network host objects.</p>
OK button	Saves your changes locally on the client and closes the dialog box.

## Tunnel Group Editor > IPsec Tab

Use the IPsec tab of the Tunnel Group Policy Editor to specify IPsec and IKE parameters for the tunnel group policy.

### Navigation Path

Open the [Tunnel Group Editor Dialog Box, page H-6](#), then click the **IPsec** tab.

### Related Topics

- [Tunnel Group Policies in Remote Access VPNs, page 10-8](#)
- [Configuring Tunnel Group Policies, page 10-9](#)
- [Tunnel Group Editor Dialog Box, page H-6](#)

### Field Reference

**Table H-4** Tunnel Group Editor Dialog Box > IPsec Tab

Element	Description
Preshared Key	The value of the preshared key for the tunnel group. The maximum length of a preshared key is 128 characters.

Table H-4 Tunnel Group Editor Dialog Box &gt; IPsec Tab (continued)

Element	Description
Trustpoint Name	Select the trustpoint name if any trustpoints are configured, and if certificates are to be used for authentication. A trustpoint represents a CA/identity pair and contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate.
IKE Peer ID Validation	Select whether IKE peer ID validation is ignored, required, or checked only if supported by a certificate. During IKE negotiations, peers must identify themselves to one another. <b>Note</b> The default option is Required.
Enable sending certificate chain	When selected, enables the sending of the certificate chain for authorization. A certificate chain includes the root CA certificate, identity certificate, and key pair.
Enable password update with RADIUS authentication	When selected, enables passwords to be updated with the RADIUS authentication protocol.  For more information, see <a href="#">Supported AAA Server Types, page 8-25</a> .
<b>ISAKMP Keep Alive</b>	
Monitor Keep Alive	When selected (the default), enables you to configure IKE keepalive as the default failover and routing mechanism. For more information, see <a href="#">About IKE Keepalive, page 9-79</a> .  <b>Note</b> The IKE keepalive settings you define here apply only to ASA devices and PIX Firewalls version 7.0. For Cisco IOS routers, Catalyst 6500/7600 devices, and PIX Firewalls version 6.3, you define these settings when configuring the VPN global settings. See <a href="#">ISAKMP/IPsec Settings Tab, page H-43</a> .
Confidence Interval	The number of seconds that a device waits between sending IKE keepalive packets. The default is 300 seconds.
Retry Interval	The number of seconds a device waits between attempts to establish an IKE connection with the remote peer. The default is 2 seconds.

Table H-4 Tunnel Group Editor Dialog Box &gt; IPsec Tab (continued)

Element	Description
<b>Authorization Settings</b>	
User Entire DN as the Username	<p>Select to use the entire distinguished name (DN) as the identifier for the username.</p> <p>A distinguished name (DN) is a unique identification, made up of individual fields, that can be used as the identifier when matching users to a tunnel group. Distinguished name (DN) rules are used for enhanced certificate authentication on PIX Firewalls and ASA devices.</p> <p>For more information, see <a href="#">DN Matching Policies, page 10-30</a>.</p>
Specify individual DN fields as the username	<p>When selected (the default), enables you to use individual DN fields as the username when matching users to the tunnel group.</p> <p>A DN certificate is made up of different field identifiers that can be used to match users to tunnel groups.</p>
Primary DN Field	<p>Available if you selected the option to use individual DN fields as the username.</p> <p>Select the primary DN field identifier to be used for identification from the list. The default is <b>UID (User ID)</b>.</p>
Secondary DN Field	<p>Available if you selected the option to use individual DN fields as the username.</p> <p>Select the secondary DN field identifier to be used for identification, from the list. Select <b>None</b> if no secondary field identifier is required.</p>
OK button	Saves your changes locally on the client and closes the dialog box.

## Tunnel Group Editor > Advanced Tab

Use the Advanced tab of the Tunnel Group Policy Editor to specify interface-specific information for your tunnel group.

### Navigation Path

Open the [Tunnel Group Editor Dialog Box, page H-6](#), then click the **Advanced** tab.

**Related Topics**

- [Tunnel Group Policies in Remote Access VPNs, page 10-8](#)
- [Configuring Tunnel Group Policies, page 10-9](#)
- [Tunnel Group Editor Dialog Box, page H-6](#)
- [Creating Interface Role Objects, page 8-115](#)
- [Creating AAA Server Group Objects, page 8-19](#)
- [Creating Network/Host Objects, page 8-130](#)

**Field Reference****Table H-5 Tunnel Group Editor Dialog Box > Advanced Tab**

Element	Description
<b>Interface-Specific Authentication Server Groups</b>	
Interface Role	The interface role to be associated with the authentication server group.  Click <b>Select</b> to open a dialog box that lists all available interfaces and sets of interfaces defined by interface roles, and enables you to create interface role objects.
Server Group	The server group to be associated with the selected interface role.  Click <b>Select</b> to open a dialog box that lists all available AAA server groups and enables you to create AAA server group objects.
Use LOCAL if server group fails.	When selected, enables fallback to the LOCAL database if the selected server group fails.
Add button (>>)	Click to add the specified interface role and server group to the list.
Remove button (<<)	Click to remove an associated interface role and server group from the list.
<b>Interface-Specific Client Address Pools</b>	
Interface Role	The interface on which to assign addresses to the client.  Click <b>Select</b> to open a dialog box that lists all available interfaces and sets of interfaces defined by interface roles, and enables you to create interface role objects.

**Table H-5** Tunnel Group Editor Dialog Box > Advanced Tab (continued)

Element	Description
Address Pool	The address pool to use to assign to a client address the selected interface.  Address pools are predefined network objects. Network objects can contain one or more network or host IP addresses, interfaces, or other network objects. Click <b>Select</b> to open a dialog box that lists all available network hosts and enables you to create network host objects.
Add >> button	Click to add the specified interface role and address pool to the list.
Remove button	Click to remove an associated interface role and address pool from the list.
OK button	Saves your changes locally on the client and closes the dialog box.

## Tunnel Group Editor > Client VPN Software Update Tab

Use the Client VPN Software Update tab of the Tunnel Group Policy Editor to view and edit the client type, VPN client revisions, and image URL for each client VPN software package installed.

### Navigation Path

Open the [Tunnel Group Editor Dialog Box, page H-6](#), then click the **Client VPN Software Update** tab.

### Related Topics

- [Tunnel Group Policies in Remote Access VPNs, page 10-8](#)
- [Configuring Tunnel Group Policies, page 10-9](#)
- [Tunnel Group Editor Dialog Box, page H-6](#)

## Field Reference

Table H-6 Tunnel Group Editor Dialog Box &gt; Client VPN Software Update Tab

Element	Description
<b>Windows Configuration</b>	
All Windows Platforms	When selected (the default), enables you to configure the specific revision level and URL of the VPN client on all Windows platforms. After you select this option, enter the appropriate information in the fields provided.
Various Windows Platforms	When selected, enables you to configure the specific revision level and URL of the VPN client on Windows 95/98/ME or NT4.1/2000/XP platforms. After you select this option, enter the appropriate information in the fields provided.
<b>VPN3002 Hardware Client</b>	
VPN Client Revisions	The specific revision level of the VPN3002 client.
Image URL	The specific URL of the VPN3002 client software image.
OK button	Saves your changes locally on the client and closes the dialog box.

## Remote Access VPN Defaults Page

Use the VPN Defaults page of the Remote Access Configuration wizard to view and select the default policies that will be assigned to the device you are configuring as a remote access VPN server.

The page displays all the available policy types that can be assigned to your device. Each policy type has a list from which you can select to assign either the factory default or a shared policy that was created (and submitted or approved, depending on the workflow mode) using Security Manager.

### Navigation Path

- Open the [Remote Access Configuration Wizard, page H-2](#), click **Remote Access Configuration Wizard**, and then click **Next** on the User Group Policy or Tunnel Group Policy page.

**Related Topics**

- [Assigning the Default Remote Access VPN Policies, page 10-11](#)
- [Managing Shared Remote Access VPN Policies in Policy View, page 10-35](#)

**Field Reference****Table H-7 Remote Access Configuration Wizard > VPN Defaults Page**

Element	Description
Policy type	<p>For each policy type, select the default remote access VPN policy to assign to your device.</p> <p>You can accept the Factory Default policy or select a shared VPN policy that appears in the list.</p> <p><b>Note</b> If you want to assign a default policy that is not in the list, you can change the policy defaults selection in the Administration tool's VPN Policy Defaults page. For more information, see <a href="#">Configuring VPN Policy Defaults, page 2-98</a>.</p>
View Content button	<p>Opens a page that displays the contents of the selected remote access VPN policy.</p> <p><b>Note</b> If you make any changes on this page, you cannot save them.</p>

## IPsec Proposal Page

An IPsec proposal defines the external interface through which remote access clients connect to the server, and the encryption and authentication algorithms used to protect the data in the VPN tunnel.

Use the IPsec Proposal page to create or edit IPsec policy definitions for your remote access VPN. For more information on IPsec proposals, see [Understanding IPsec Tunnel Policies, page 9-72](#) and [About Crypto Maps, page 9-73](#).

**Navigation Path**

1. Click the **Device View** button on the toolbar.
2. From the Device Selector, select the device on which to configure the IPsec Proposal.
3. Select **Remote Access VPN > IPsec Proposal** from the Policy selector.

**Note**

You can also open the IPsec Proposal page from Policy view. For more information, see [Managing Shared Remote Access VPN Policies in Policy View, page 10-35](#).

**Related Topics**

- [IPsec Proposals in Remote Access VPNs, page 10-12](#)
- [Configuring an IPsec Proposal on a Remote Access VPN Server, page 10-14](#)
- [Defining Accounts and Credential Policies, page 14-75](#)
- [Remote Access Configuration Wizard, page H-2](#)
- [IPsec Proposal Editor Dialog Box \(for PIX and ASA Devices\), page H-19](#)
- [IPsec Proposal Editor Dialog Box \(for IOS Routers and Catalyst 6500/7600 Devices\), page H-22](#)

**Field Reference****Table H-8** *IPsec Proposal Page*

Element	Description
Endpoint	The external interface (or inside VLAN for a Catalyst 6500/7600 device) through which remote access clients will connect to the server.
Transform Sets	The transform set(s) selected for the policy (the default is <b>tunnel_3des_sha</b> ).  Transform sets specify which authentication and encryption algorithms will be used to secure the traffic in the tunnel.

Table H-8 IPsec Proposal Page (continued)

Element	Description
RRI	<p>Shows whether Reverse Route Injection (RRI) is enabled or disabled on the crypto map for the support of VPN clients.</p> <p>For more information, see <a href="#">About Reverse Route Injection, page 9-76</a>.</p>
AAA Authorization	<p>Supported on Cisco IOS routers and Catalyst 6500/7600 devices only.</p> <p>Displays the selected AAA server groups for authorization.</p> <p>AAA Authorization defines the order in which group policies are searched and whether they are configured on the local server or on an external AAA server.</p>
AAA Authentication	<p>Supported on Cisco IOS routers and Catalyst 6500/7600 devices only.</p> <p>Displays selected AAA server groups for authentication.</p> <p>AAA authentication is required to enable IKE Extended Authentication (Xauth) as the user authentication method. It determines the username and password storage location. Usernames and passwords can be stored on the device (local) or on an external AAA server, which can provide authentication to numerous other databases.</p>
VRF	<p>Supported on Cisco IOS routers and Catalyst 6500/7600 devices only.</p> <p>Shows whether VRF settings for the proposal are enabled or disabled. For more information, see <a href="#">Understanding VRF-Aware IPsec, page 9-51</a>.</p>
DVTI	<p>Supported on Cisco IOS routers only.</p> <p>Shows whether a dynamic virtual template interface is configured on the device. For more information, see <a href="#">Using Dynamic Virtual Template Interfaces in Remote Access VPNs, page 10-13</a>.</p>

**Table H-8** IPsec Proposal Page (continued)

Element	Description
Create button	<p>Click to open the IPsec Proposal Editor dialog box to create an IPsec proposal.</p> <p>If the device is a PIX Firewall or ASA device, see <a href="#">IPsec Proposal Editor Dialog Box (for PIX and ASA Devices)</a>, page H-19.</p> <p>If the device is a Cisco IOS router or Catalyst 6500/7600, see <a href="#">IPsec Proposal Editor Dialog Box (for IOS Routers and Catalyst 6500/7600 Devices)</a>, page H-22.</p>
Edit button	<p>Select the row of a proposal from the table, then click to open the IPsec Proposal Editor dialog box to edit the selected proposal.</p> <p>If the device is a PIX Firewall or ASA device, see <a href="#">IPsec Proposal Editor Dialog Box (for PIX and ASA Devices)</a>, page H-19.</p> <p>If the device is a Cisco IOS router or Catalyst 6500/7600, see <a href="#">IPsec Proposal Editor Dialog Box (for IOS Routers and Catalyst 6500/7600 Devices)</a>, page H-22.</p>
Delete button	Select the rows of one or more proposals, then click to delete.
Save button	<p>Available only if you are authorized to modify this policy.</p> <p>Saves your changes to the server but keeps them private.</p> <p><b>Note</b> To publish your changes, click the <b>Submit</b> button on the toolbar.</p>

## IPsec Proposal Editor Dialog Box (for PIX and ASA Devices)

Use the IPsec Proposal Editor to create or edit an IPsec proposal for a device in your remote access VPN.

The elements in this dialog box differ according to the selected device. [Table H-9](#) describes the elements in the IPsec Proposal Editor dialog box when a PIX 7.0 or ASA device is selected.



### Note

For a description of the elements in the dialog box when a Cisco IOS router or Catalyst 6500/7600 is selected, see [Table H-10 on page H-23](#).

**Navigation Path**

Open the [IPsec Proposal Page, page H-16](#), then click **Create**, or select a proposal from the list and click **Edit**.

**Related Topics**

- [IPsec Proposal Page, page H-16](#)
- [Configuring an IPsec Proposal on a Remote Access VPN Server, page 10-14](#)
- [Understanding IPsec Tunnel Policies, page 9-72](#)
- [Creating Interface Role Objects, page 8-115](#)
- [Creating AAA Server Group Objects, page 8-19](#)

**Field Reference**

**Table H-9** *IPsec Proposal Editor (for PIX and ASA Devices)*

Element	Description
External Interface	<p>The external interface (endpoint) through which remote access clients connect to the server.</p> <p>An endpoint can be an interface or a set of interfaces that are defined by a particular interface role. Click <b>Select</b> to open a dialog box that lists all available interfaces and sets of interfaces defined by interface roles, and enables you to create interface role objects.</p>

**Table H-9** IPsec Proposal Editor (for PIX and ASA Devices)

Element	Description
Transform Sets	<p>The transform set or sets to use for your tunnel policy (the default is <b>tunnel_3des_sha</b>).</p> <p>Transform sets specify which authentication and encryption algorithms will be used to secure the traffic in the tunnel.</p> <p>A default transform set is displayed. If you want to use a different transform set or select additional transform sets, click <b>Select</b> to open a dialog box that lists all available transform sets and enables you to create transform set objects. For more information, see <a href="#">IPsec Transform Sets Page, page F-423</a>.</p> <p>If more than one of your selected transform sets is supported by both peers, the transform set that provides the highest security will be used.</p> <p><b>Note</b> You can select up to six transform sets.</p> <p>For more information, see <a href="#">About Transform Sets, page 9-74</a>.</p>
Reverse Route Injection	<p><b>Note</b> Available only for ASA devices.</p> <p>Select the required option to configure Reverse route Injection (RRI) on the crypto map in your tunnel policy:</p> <ul style="list-style-type: none"> <li>• <b>None</b>—To disable the RRI configuration on the crypto map.</li> <li>• <b>Standard</b>—This is the default. It creates routes based on the destination information defined in the crypto map access control list (ACL).</li> </ul> <p>For more information, see <a href="#">About Reverse Route Injection, page 9-76</a>.</p>
Enable Network Address Translation Traversal	<p><b>Note</b> Available only for ASA devices.</p> <p>When selected (the default), enables you to configure NAT traversal on the device.</p> <p>You use NAT traversal when a device (referred to as the middle device) is located between a VPN-connected hub and spoke, that performs NAT on the IPsec flow.</p> <p>For more information, see <a href="#">About NAT Traversal, page 9-81</a>.</p>

**Table H-9** IPsec Proposal Editor (for PIX and ASA Devices)

Element	Description
User Authentication (Xauth)/AAA Authentication Method	<p><b>Note</b> Available only for PIX devices.</p> <p>The AAA or Xauth user authentication method that defines the order in which user accounts are searched.</p> <p>Xauth allows all Cisco IOS software AAA authentication methods to perform user authentication in a separate phase after the IKE authentication phase 1 exchange.</p> <p>Click <b>Select</b> to open a dialog box that lists all available AAA server groups and enables you to create AAA server group objects.</p>
OK button	<p>Saves your changes locally on the client and closes the dialog box.</p> <p>The changes appear in the table of the IPsec Proposal page.</p>

## IPsec Proposal Editor Dialog Box (for IOS Routers and Catalyst 6500/7600 Devices)

Use the IPsec Proposal Editor to create or edit an IPsec proposal for a device in your remote access VPN.

If you select an IOS router, the IPsec Proposal Editor dialog box displays two tabs—**General** and **Dynamic VTI/VRF Aware IPsec**. If you select a Catalyst 6500/7600, the **FWSM Settings** tab is also displayed.

Click the appropriate tab to specify general IPsec settings, configure Dynamic VTI or VRF Aware IPsec, or both, on the selected device, or configure FWSM on a Catalyst 6500/7600 device.

### Navigation Path

Open the [IPsec Proposal Page](#), page H-16, then click **Create**, or select a proposal from the list and click **Edit**. The IPsec Proposal Editor dialog box opens, displaying the **General** tab.

### Related Topics

- [IPsec Proposal Page](#), page H-16
- [VPNSM/VPN SPA Settings Dialog Box](#), page H-26

- [FWSM Settings Tab \(IPsec Proposal Editor\)](#), page H-29
- [Dynamic VTI/VRF Aware IPsec Tab \(IPsec Proposal Editor\)](#), page H-31
- [Configuring an IPsec Proposal on a Remote Access VPN Server](#), page 10-14
- [Creating Interface Role Objects](#), page 8-115
- [Creating AAA Server Group Objects](#), page 8-19

### Field Reference

[Table H-10](#) describes the elements in the General tab of the IPsec Proposal Editor dialog box, if you selected an IOS router or Catalyst 6500/7600.



#### Note

For a description of the elements in the dialog box if you selected a PIX Firewall or ASA device, see [Table H-9 on page H-20](#).

**Table H-10**      *IPsec Proposal Editor > General Tab*

Element	Description
External Interface	<p>The external interface through which remote access clients will connect to the server.</p> <p>An external interface can be defined by a specific interface role. Interface roles are predefined objects. Click <b>Select</b> to open a dialog box that lists all available interfaces and sets of interfaces defined by interface roles, and enables you to create interface role objects.</p>

Table H-10 IPsec Proposal Editor &gt; General Tab (continued)

Element	Description
Inside VLAN	<p><b>Note</b> Available only if the selected device is a Catalyst 6500/7600.</p> <p>The inside VLAN that serves as the inside interface to the VPN Services Module (VPNSM) or VPN SPA.</p> <p>Click <b>Select</b> to open a dialog box in which you define the settings that enable you to configure a VPN Services Module (VPNSM) external interface or a VPN SPA blade on the Catalyst 6500/7600 device. See <a href="#">VPNSM/VPN SPA Settings Dialog Box, page H-26</a>.</p> <p>For information about configuring a VPNSM, see <a href="#">Configuring a Catalyst VPN Services Module (VPNSM) VPN Interface, page 9-41</a>.</p> <p>For information about configuring a VPN SPA, see <a href="#">Configuring a Catalyst VPN Shared Port Adapter (VPN SPA) Blade, page 9-43</a>.</p>
Transform Sets	<p>The transform set or sets to use for your tunnel policy. Transform sets specify which authentication and encryption algorithms are used to secure the traffic in the tunnel.</p> <p>A default transform set is displayed. If you want to use a different transform set or select additional transform sets, click <b>Select</b> to open a dialog box that lists all available transform sets and enables you to create transform set objects. For more information, see <a href="#">IPsec Transform Sets Page, page F-423</a>.</p> <p>If more than one of your selected transform sets is supported by both peers, the transform set that provides the highest security is used.</p> <p><b>Note</b> You can select up to six transform sets.</p> <p>For more information, see <a href="#">About Transform Sets, page 9-74</a>.</p>

Table H-10 IPsec Proposal Editor &gt; General Tab (continued)


Element	Description
Reverse Route Injection	<p>Select one of the following options to configure Reverse Route Injection (RRI) on the crypto map:</p> <ul style="list-style-type: none"> <li>• <b>None</b>—To disable the configuration of RRI on the crypto map.</li> <li>• <b>Standard</b>—The default. It creates routes according to the destination information defined in the crypto map access control list (ACL).</li> <li>• <b>Remote Peer</b>—To create two routes, one for the remote endpoint and one for route recursion to the remote endpoint through the interface to which the crypto map is applied.</li> <li>• <b>Remote Peer IP</b>—To specify an interface or address as the explicit next hop to the remote VPN device. Then click <b>Select</b> to open the Network/Hosts Selector, from which you can select the IP address of the remote peer to use as the next hop.</li> </ul> <p> <b>Note</b> You can select the <b>Allow Value Override per Device</b> check box to override the default route, if required.</p> <p>For more information, see <a href="#">About Reverse Route Injection, page 9-76</a>.</p>
Group Policy Lookup/AAA Authorization Method	<p>The AAA authorization method list that defines the order in which the group policies are searched. Group policies can be configured on the local server or on an external AAA server.</p> <p><b>Note</b> The default is LOCAL.</p> <p>Click <b>Select</b> to open a dialog box that lists all available AAA server groups and enables you to create AAA server group objects.</p>

Table H-10 IPsec Proposal Editor &gt; General Tab (continued)

Element	Description
User Authentication (Xauth)/AAA Authentication Method	<p>The AAA or Xauth user authentication method that defines the order in which user accounts are searched.</p> <p><b>Note</b> The default authentication method is LOCAL.</p> <p>Xauth allows all Cisco IOS software AAA authentication methods to perform user authentication in a separate phase after the IKE authentication phase 1 exchange.</p> <p>For more information about defining user accounts, see <a href="#">Defining Accounts and Credential Policies, page 14-75</a>.</p> <p>Click <b>Select</b> to open a dialog box that lists all available AAA server groups and enables you to create AAA server group objects.</p>
OK button	<p>Saves your changes locally on the client and closes the dialog box.</p> <p>The changes appear in the table of the IPsec Proposal page.</p>

## VPNSM/VPN SPA Settings Dialog Box



### Note

This dialog box is available only if the selected device is a Catalyst 6500/7600.

Use the VPNSM/VPN SPA Settings dialog box to specify the settings for configuring a VPN Services Module (VPNSM) or a VPN Shared Port Adapter (VPN SPA) on a Catalyst 6500/7600 device.



### Note

- Before you define the VPNSM or VPN SPA settings, you must import your Catalyst 6500/7600 device to the Security Manager inventory and discover its interfaces. For more information, see [Procedure for Configuring a VPNSM or VPN SPA Blade, page 9-45](#).
- Before you configure VPNSM or VPN SPA with VRF-Aware IPsec on a device, verify that an IPsec proposal with VRF-Aware IPsec *and* an IPsec proposal without VRF-Aware IPsec were not configured on the device.

For more information about VPNSM, see [Configuring a Catalyst VPN Services Module \(VPNSM\) VPN Interface](#), page 9-41.

For more information about VPN SPA, see [Configuring a Catalyst VPN Shared Port Adapter \(VPN SPA\) Blade](#), page 9-43.

### Navigation Path

1. Open the [IPsec Proposal Page](#), page H-16, then click **Create**, or select a proposal from the list and click **Edit**. The IPsec Proposal Editor dialog box opens.
2. In the General tab of the IPsec Proposal Editor dialog box, click **Select** next to the Inside VLAN field.

### Related Topics

- [IPsec Proposal Page](#), page H-16
- [IPsec Proposal Editor Dialog Box \(for IOS Routers and Catalyst 6500/7600 Devices\)](#), page H-22
- [FWSM Settings Tab \(IPsec Proposal Editor\)](#), page H-29
- [Creating Interface Role Objects](#), page 8-115

### Field Reference

**Table H-11** *VPNSM/VPN SPA Settings Dialog Box*

Element	Description
Inside VLAN	The inside VLAN that serves as the inside interface to the VPNSM or VPN SPA, and to which the required crypto maps will be applied.  If required, click <b>Select</b> to open a dialog box that lists all available interfaces and sets of interfaces defined by interface roles, from which you can make your selection, or create interface role objects.
Slot	From the list of available slots, select the VPNSM blade slot number to which the inside VLAN interface is connected or the number of the slot in which the VPN SPA blade is inserted.  For more information, see <a href="#">Adding VPN SPA Slot Locations</a> , page 5-35.

Table H-11 VPNSM/VPN SPA Settings Dialog Box (continued)

Element	Description
Subslot	<p>The number of the subslot (0 or 1) on which the VPN SPA blade is installed.</p> <p><b>Note</b> If you are configuring a VPNSM, select the blank option.</p>
External Port	<p>The external port or VLAN that connects to the inside VLAN.</p> <p><b>Note</b> If VRF-Aware IPsec is configured on the device, the external port or VLAN must have an IP address. If VRF-Aware IPsec is not configured, the external port or VLAN must <i>not</i> have an IP address.</p> <p>Click <b>Select</b> to open a dialog box that lists all available interfaces and sets of interfaces defined by interface roles, from which you can make your selection, or create interface role objects.</p> <p><b>Note</b> You must specify an interface or interface role that differs from the one specified for the inside VLAN.</p>
Enable Failover Blade	<p>When selected, enables you to configure a failover VPNSM or VPN SPA blade for intrachassis high availability.</p> <p><b>Note</b> A VPNSM blade and VPN SPA blade cannot be used on the same device as primary and failover blades.</p>
Failover Slot	<p>From the list of available slots, select the VPNSM blade slot number that serves as the failover blade, or the number of the slot in which the failover VPN SPA blade is inserted.</p>
Failover Subslot	<p>Select the number of the subslot (0 or 1) on which the failover VPN SPA blade is actually installed.</p> <p><b>Note</b> If you are configuring a VPNSM, select the blank option.</p>
OK button	<p>Saves your changes locally on the client and closes the dialog box.</p>

## FWSM Settings Tab (IPsec Proposal Editor)

**Note**

---

The FWSM Settings tab is available only if the selected device is a Catalyst 6500/7600.

---

Use the FWSM tab of the IPsec Proposal Editor dialog box to specify settings that enable you to connect between a Firewall Services Module (FWSM) and an IPsec VPN Services Module (VPNSM) or VPN SPA blade that is already configured on a Catalyst 6500/7600 device.

For more information, see [Configuring a Firewall Services Module \(FWSM\) Interface with VPNSM or VPN SPA, page 9-48](#).

**Note**

---

Before defining the FWSM settings, you must import your Catalyst 6500/7600 device to the Security Manager inventory and define (or discover) any required security contexts. Then open Cisco Catalyst Device Manager (Cisco CDM) and discover the FWSM configurations on the device, and then create a VLAN to serve as the inside interface to the FWSM.

For more information, see:

- [Configuring a Firewall Services Module \(FWSM\) Interface with VPNSM or VPN SPA, page 9-48](#)
  - [Discovering Policies, page 6-7](#)
  - [Creating or Editing VLANs, page 16-13](#)
- 

### Navigation Path

1. Open the [IPsec Proposal Page, page H-16](#), then click **Create**, or select a proposal from the list and click **Edit**.
2. In the IPsec Proposal Editor dialog box, click the **FWSM Settings** tab.

### Related Topics

- [IPsec Proposal Page, page H-16](#)
- [IPsec Proposal Editor Dialog Box \(for IOS Routers and Catalyst 6500/7600 Devices\), page H-22](#)

- [Configuring a Firewall Services Module \(FWSM\) Interface with VPNSM or VPN SPA, page 9-48](#)
- [Creating Interface Role Objects, page 8-115](#)

### Field Reference

**Table H-12** *IPsec Proposal Editor > FWSM Tab*

Element	Description
Enable FWSM Settings	When selected, enables you to configure the connection between the FWSM and the VPNSM or VPN SPA on the selected Catalyst 6500/7600 device.
FWSM Inside VLAN	The VLAN that serves as the inside interface to the Firewall Services Module (FWSM).  If required, click <b>Select</b> to open a dialog box that lists all available interfaces and sets of interfaces defined by interface roles, and in which you can make your selection, or create interface role objects.
FWSM Blade	From the list of available blades, select the blade number to which the selected FWSM inside VLAN interface is connected.
Security Context	You can partition an FWSM into multiple virtual firewalls, known as security contexts. Each security context has its own security policy, interfaces, and administrators. You can define security contexts when you import a Catalyst 6500/7600 device into the Security Manager inventory.  If the selected FWSM inside VLAN is part of a security context, enter its name in this field. The name is case-sensitive.  For more information, see <a href="#">Security Contexts Page, page L-265</a> .
OK button	Saves your changes locally on the client and closes the dialog box.

## Dynamic VTI/VRF Aware IPsec Tab (IPsec Proposal Editor)

**Note**

---

The Dynamic VTI/VRF Aware IPsec tab is available only when the selected device is a Cisco IOS router or Catalyst 6500/7600.

---

Use the Dynamic VTI/VRF Aware IPsec tab of the IPsec Proposal Editor to configure VRF Aware IPsec settings (on a Cisco IOS router or Catalyst 6500/7600 device), configure a dynamic virtual interface on a Cisco IOS router, or do both, in your remote access VPN.

For more information, see:

- [Understanding VRF-Aware IPsec, page 9-51](#)
- [IPsec Proposals in Remote Access VPNs, page 10-12](#)

**Navigation Path**

1. Open the [IPsec Proposal Page, page H-16](#), then click **Create**, or select a proposal from the list and click **Edit**.
2. In the IPsec Proposal Editor dialog box, click the **Dynamic VTI/VRF Aware IPsec** tab.

**Related Topics**

- [IPsec Proposal Page, page H-16](#)
- [Configuring an IPsec Proposal on a Remote Access VPN Server, page 10-14](#)
- [Understanding IPsec Tunnel Policies, page 9-72](#)
- [Creating User Group Objects, page 8-181](#)
- [Creating Interface Role Objects, page 8-115](#)

## Field Reference

Table H-13 IPsec Proposal Editor &gt; Dynamic VTI/VRF Aware IPsec Tab

Element	Description
Enable Dynamic VTI	<p>When selected, enables Security Manager to implicitly create a dynamic virtual template interface on an IOS router.</p> <p><b>Note</b> Dynamic VTI can be configured only on IOS routers running Cisco IOS Release 12.4(2)T and later, except 7600 devices. If the device does not support Dynamic VTI, an error message is displayed.</p> <p>For more information, see <a href="#">Using Dynamic Virtual Template Interfaces in Remote Access VPNs, page 10-13</a>.</p>
Enable VRF Settings	<p>When selected, enables you to configure VRF settings on the device for the selected hub-and-spoke topology.</p> <p><b>Note</b> To remove VRF settings that were defined for the VPN topology, deselect this check box.</p>
User Group	<p>When you configure a remote access VPN server, remote clients must have the same group name as the user group object configured on the VPN server so that they can connect to the device.</p> <p>Select the name of the user group associated with the device.</p> <p>If the user group is not included in the list, click <b>Select</b> to open a dialog box that lists all available user groups and enables you to create a user group object.</p>
CA Server	<p>Select the Certification Authority (CA) server to use for managing certificate requests for the device.</p> <p>If the required CA server is not included in the list, click <b>Select</b> to open a dialog box that lists all available CA servers and enables you to create a PKI enrollment object. For more information, see <a href="#">PKI Enrollment Dialog Box, page F-438</a>.</p> <p>For more information about IPsec configuration with CA servers, see <a href="#">Public Key Infrastructure Policies in Remote Access VPNs, page 10-24</a>.</p>

Table H-13 IPsec Proposal Editor &gt; Dynamic VTI/VRF Aware IPsec Tab (continued)

Element	Description
Specify Virtual Template IP	<p>Available if you selected the <b>Enable Dynamic VTI</b> check box.</p> <p>Specify the virtual template interface to use by clicking one of the following radio buttons:</p> <ul style="list-style-type: none"> <li>• <b>Use IP</b>—To use an IP address as the virtual template interface. Then specify the private IP address in the <b>IP</b> field.</li> </ul> <p>If required, click <b>Select</b> to open the Network/Hosts selector in which you can select a host to be used as the IP address.</p> <ul style="list-style-type: none"> <li>• <b>Use Loopback Interface</b>—To use the IP address taken from an existing loopback interface as the virtual template interface. Then, in the <b>Role</b> field, enter the interface or click <b>Select</b> to select it from the list of interface roles.</li> </ul> <p><b>Note</b> A virtual template IP address is configured only on a server in a remote access VPN.</p>
VRF Solution	<p>Available if you selected the <b>Enable VRF Settings</b> check box.</p> <p>Click one of the following radio buttons to configure the required VRF solution:</p> <ul style="list-style-type: none"> <li>• <b>1-Box (IPsec Aggregator + MPLS PE)</b>—One device serves as the Provider Edge (PE) router that does the MPLS tagging of the packets in addition to IPsec encryption and decryption from the Customer Edge (CE) devices. For more information, see <a href="#">VRF-Aware IPsec One-Box Solution, page 9-52</a>.</li> <li>• <b>2-Box (IPsec Aggregator Only)</b>—The PE device does only the MPLS tagging, while the IPsec Aggregator device does the IPsec encryption and decryption from the CEs. For more information, see <a href="#">VRF-Aware IPsec Two-Box Solution, page 9-54</a>.</li> </ul>
VRF Name	<p>The name of the VRF routing table on the IPsec Aggregator. The VRF name is case-sensitive.</p>

Table H-13 IPsec Proposal Editor &gt; Dynamic VTI/VRF Aware IPsec Tab (continued)

Element	Description
Route Distinguisher	<p>The unique identifier of the VRF routing table on the IPsec Aggregator.</p> <p>This unique route distinguisher maintains routing separation for each VPN across the MPLS core to the other PE routers.</p> <p>The identifier can be in either of the following formats:</p> <ul style="list-style-type: none"> <li>• <i>IP address:X</i> (where <i>X</i> is in the range of 0-999999999).</li> <li>• <i>N:X</i> (where <i>N</i> is in the range of 0-65535, and <i>X</i> is in the range of 0-999999999).</li> </ul> <p><b>Note</b> You cannot override the RD identifier after deploying the VRF configuration to your device. To modify the RD identifier after deployment, you must manually remove it through the device CLI and then deploy again.</p>
Interface Towards Provider Edge	<p>Available only if the 2-Box radio button is selected.</p> <p>The VRF forwarding interface on the IPsec Aggregator towards the PE device.</p> <p><b>Note</b> If the IPsec Aggregator (hub) is a Catalyst VPN service module, you must specify a VLAN.</p> <p>Interfaces and VLANs are predefined interface role objects. If required, click <b>Select</b> to open a dialog box that lists all available interfaces and sets of interfaces defined by interface roles, in which you can make your selection or create interface role objects.</p>
Routing Protocol	<p>Available only if the 2-Box radio button is selected.</p> <p>Select the routing protocol to use between the IPsec Aggregator and the PE.</p> <p>If the routing protocol for the secured IGP differs from the routing protocol between the IPsec Aggregator and the PE, select the routing protocol for redistributing the routing to the secured IGP.</p> <p>The options are BGP, EIGRP, OSPF, RIPv2, or Static route.</p> <p>For information about these protocols, see <a href="#">Chapter 14, “Managing Routers”</a>.</p>

Table H-13 IPsec Proposal Editor &gt; Dynamic VTI/VRF Aware IPsec Tab (continued)

Element	Description
AS Number	<p>Available only if the 2-Box radio button is selected.</p> <p>The number to use to identify the autonomous system (AS) area between the IPsec Aggregator and the PE.</p> <p>If the routing protocol for the secured IGP differs from the routing protocol between the IPsec Aggregator and the PE, enter an AS number that identifies the secured IGP into which the routing will be redistributed from the IPsec Aggregator and the PE. This is relevant only if GRE or DMVPN are applied.</p> <p>The AS number must be between 1 and 65535.</p>
Process Number	<p>Available only if the 2-Box radio button is selected, and if the selected routing protocol is OSPF.</p> <p>The routing process ID number to use to configure the routing between the IPsec Aggregator and the PE.</p> <p>The process number must be between 1 and 65535.</p>
OSPF Area ID	<p>Available only if the 2-Box radio button is selected, and if the selected routing protocol is OSPF.</p> <p>The ID number of the area in which the packet belongs. You can enter any number from 0 to 4294967295.</p> <p><b>Note</b> All OSPF packets are associated with a single area, so all devices must have the same area ID number.</p>
Redistribute Static Route	<p>Available only if the 2-Box radio button is selected, and for any selected routing protocol other than Static route.</p> <p>When selected, enables static routes to be advertised in the routing protocol configured on the IPsec Aggregator towards the PE device.</p> <p><b>Note</b> If this check box is deselected and Enable Reverse Route Injection is enabled (default) for the IPsec proposal, static routes are still advertised in the routing protocol on the IPsec Aggregator.</p>
OK button	<p>Saves your changes locally on the client and closes the dialog box.</p> <p>The changes appear in the table of the IPsec Proposal page.</p>

# IKE Proposal Page

Use the IKE Proposal page to select the IKE proposals to use for your remote access VPN server.

## Navigation Path

1. Click the **Device View** button on the toolbar.
2. From the Device Selector, select the device on which you want to configure the IKE Proposal.
3. Select **Remote Access VPN > IKE Proposal** from the Policy selector.



### Note

You can also open the IKE Proposal page from Policy view. For more information, see [Managing Shared Remote Access VPN Policies in Policy View, page 10-35](#).

## Related Topics

- [Remote Access Configuration Wizard, page H-2](#)
- [Understanding IKE, page 9-67](#)
- [IKE Proposals in Remote Access VPNs, page 10-18](#)
- [Configuring IKE Proposals on a Remote Access VPN Server, page 10-18](#)
- [Creating IKE Proposal Objects, page 8-54](#)

## Field Reference

**Table H-14**     *IKE Proposal Page*

Element	Description
Available IKE Proposals	<p>Lists the predefined IKE proposals available for selection.</p> <p>Select the required IKE proposals and click &gt;&gt;.</p> <p>IKE proposals are predefined objects. If the required IKE proposal is not included in the list, click <b>Create</b> to open the IKE Editor dialog box that enables you to create or edit an IKE proposal object.</p>

Table H-14 IKE Proposal Page (continued)

Element	Description
Selected IKE Proposals	Lists the selected IKE proposals. To remove an IKE proposal from this list, select it and click <<. To modify the properties of an IKE proposal, select it and click <b>Edit</b> .
>> button	Click to move a selected IKE proposal from the Available IKE Proposals list to the Selected IKE Proposals list.
<< button	Click to remove a selected IKE proposal from the Selected IKE Proposals list to the Available IKE Proposals list.
Save button	Available only if you are authorized to modify this policy. Saves your changes to the server but keeps them private. <b>Note</b> To publish your changes, click the <b>Submit</b> button on the toolbar.

## High Availability Page

Use the High Availability page to configure a High Availability (HA) policy on a Cisco IOS router in a remote access VPN.

### Navigation Path

1. Click the **Device View** button on the toolbar.
2. From the Device Selector, select the device on which to configure a High Availability policy.
3. Select **Remote Access VPN > High Availability** from the Policy selector.



### Note

You can also open the High Availability page from Policy view. For more information, see [Managing Shared Remote Access VPN Policies in Policy View, page 10-35](#).

**Related Topics**

- [High Availability in Remote Access VPNs, page 10-19](#)
- [Configuring a High Availability Policy, page 10-20](#)

**Field Reference****Table H-15 High Availability Page**

Element	Description
Inside Virtual IP	<p>The IP address that will be shared by the hubs in the HA group and will represent the inside interface of the HA group. The virtual IP address must be on the same subnet as the inside interfaces of the hubs in the HA group.</p> <p><b>Note</b> You must provide an inside virtual IP that matches the subnet of one of the interfaces on the device, in addition to a VPN virtual IP that matches the subnet of one of the device's interfaces and is configured with an IPsec proposal; otherwise an error is displayed.</p> <p><b>Note</b> If there is an existing standby group on the device, make sure that the IP address you provide is different from the virtual IP address already configured on the device.</p> <p>You can choose the required IP address by clicking <b>Select</b>. The Network/Hosts selector opens, in which you can select a network from which the IP address will be allocated.</p>
Inside Mask	The subnet mask for the inside virtual IP address.
VPN Virtual IP	<p>The IP address that will be shared by the hubs in the HA group and will represent the VPN interface of the HA group. This IP address will serve as the hub endpoint of the VPN tunnel.</p> <p>You can choose the required IP address by clicking <b>Select</b>. The Network/Hosts selector opens, in which you can select a network from which the IP address will be allocated.</p> <p><b>Note</b> If there is an existing standby group on the device, make sure that the IP address you provide is different from the virtual IP address already configured on the device.</p>
VPN Mask	The subnet mask for the VPN virtual IP address.

**Table H-15 High Availability Page (continued)**

Element	Description
Hello Interval	The duration in seconds (within the range of 1-254) between each hello message sent by a hub to the other hubs in the group to indicate status and priority. The default is 5 seconds.
Hold Time	The duration in seconds (within the range of 2-255) that a standby hub will wait to receive a hello message from the active hub before concluding that the hub is down. The default is 15 seconds.
Standby Group Number (Inside)	The standby number of the inside hub interface that matches the internal virtual IP subnet for the hubs in the HA group. The number must be within the range of 0-255. The default is 1.
Standby Group Number (Outside)	The standby number of the outside hub interface that matches the external virtual IP subnet for the hubs in the HA group. The number must be within the range of 0-255. The default is 2.  <b>Note</b> The outside standby group number must be different to the inside standby group number.
Failover Server	The IP address of the inside interface of the remote peer device.  You can click <b>Select</b> to open the Network/Hosts Selector, from which you can select a host from which the IP address of the remote peer will be allocated.
Save button	Available only if you are authorized to modify this policy.  Saves your changes to the server but keeps them private.  <b>Note</b> To publish your changes, click the <b>Submit</b> button on the toolbar.

## Public Key Infrastructure Page

Use the Public Key Infrastructure page to select the CA servers to use for creating a Public Key Infrastructure (PKI) policy for generating enrollment requests for CA certificates.

### Navigation Path

1. Click the **Device View** button on the toolbar.
2. From the Device Selector, select the device on which you want to configure a PKI policy.
3. Select **Remote Access VPN > Public Key Infrastructure** from the Policy selector.



#### Note

---

You can also open the Public Key Infrastructure page from Policy view. For more information, see [Managing Shared Remote Access VPN Policies in Policy View, page 10-35](#).

---

### Related Topics

- [Public Key Infrastructure Policies in Remote Access VPNs, page 10-24](#)
- [Configuring a PKI Policy in a Remote Access VPN, page 10-25](#)
- [Configuring Public Key Infrastructure Policies, page 9-92](#)
- [PKI Enrollments Page, page F-436](#)
- [Creating PKI Enrollment Objects, page 8-137](#)

## Field Reference

Table H-16 Public Key Infrastructure Page

Element	Description
Available CA Servers	<p>Lists the CA servers available for selection.</p> <p>Select the required CA server(s) and click &gt;&gt;.</p> <p>CA servers are defined as PKI enrollments objects that contain server information and enrollment parameters required for creating enrollment requests for CA certificates.</p> <p>If the required CA server is not included in the list, click <b>Create</b> to open a dialog box that enables you to create a PKI enrollment object. You can also edit the properties of a CA server by selecting it and clicking <b>Edit</b>.</p> <p><b>Note</b> When creating or editing a PKI enrollment object, you must configure each remote component (spoke) with the name of the user group to which it connects. You specify this information in the Organization Unit (OU) field in the Certificate Subject Name tab of the PKI Enrollment Editor dialog box. In addition, the certificate issued to the client should have OU as the name of the user group. For more information, see <a href="#">Defining Additional PKI Attributes</a>, page 8-144.</p>
Selected CA Servers	<p>The selected CA servers.</p> <p>To remove a CA server from this list, select it and click &lt;&lt;.</p> <p><b>Note</b> You can select more than one CA server at a time.</p>
>> button	Click to move one or more selected CA servers from the Available CA Servers list to the Selected CA Servers list.
<< button	Click to move one or more selected CA server from the Selected CA Servers list to the Available CA Servers list.

Table H-16 Public Key Infrastructure Page (continued)

Element	Description
Save button	<p>Available only if you are authorized to modify this policy.</p> <p>Saves your changes to the server but keeps them private. To publish your changes, click the <b>Submit</b> button on the toolbar.</p> <p><b>Note</b> To save the RSA key pairs and the CA certificates permanently to flash memory on a PIX Firewall version 6.3 between reloads, you must configure the "ca save all" command. You can do this manually on the device or using a FlexConfig (see <a href="#">Chapter 19, "Managing FlexConfigs"</a>).</p>

## VPN Global Settings Page

Use the VPN Global Settings page to define global settings for IKE, IPsec, NAT, and fragmentation that apply to devices in your remote access VPN.

The following tabs are available on the VPN Global Settings page:

- [ISAKMP/IPsec Settings Tab, page H-43](#)
- [NAT Settings Tab, page H-46](#)
- [General Settings Tab, page H-47](#)

### Navigation Path

1. Click the **Device View** button on the toolbar.
2. From the Device Selector, select the device on which you want to configure the global VPN settings.
3. Select **Remote Access VPN > VPN Global Settings** from the Policy selector.



### Note

You can also open the VPN Global Settings page from Policy view. For more information, see [Managing Shared Remote Access VPN Policies in Policy View, page 10-35](#).

## ISAKMP/IPsec Settings Tab

Use the ISAKMP/IPsec Settings tab of the VPN Global Settings page to specify global settings for IKE and IPsec.

### Navigation Path

Open the [VPN Global Settings Page](#), page H-42, or click the **ISAKMP/IPsec Settings** tab from any other tab in the VPN Global Settings page.

### Related Topics

- [VPN Global Settings Page](#), page H-42
- [VPN Global Settings in Remote Access VPNs](#), page 10-27
- [Configuring Global Settings in a Remote Access VPN](#), page 10-27
- [Understanding IKE](#), page 9-67
- [Understanding IPsec Tunnel Policies](#), page 9-72
- [Understanding ISAKMP/IPsec Settings](#), page 9-79

### Field Reference

**Table H-17**      *VPN Global Settings > ISAKMP/IPsec Settings Tab*

Element	Description
<b>ISAKMP Settings</b>	
Enable Keepalive	When selected, enables you to configure IKE keepalive as the default failover and routing mechanism for your devices.  <b>Note</b> The IKE keepalive settings you configure here apply only to Cisco IOS routers, Catalyst 6500/7600 devices, and PIX Firewalls version 6.3. For ASA devices and PIX Firewalls version 7.0, you configure these settings when creating a tunnel group. See <a href="#">Tunnel Group Editor &gt; IPsec Tab</a> , page H-10.
Interval (seconds)	The number of seconds that a device waits between sending IKE keepalive packets. The default is 10 seconds.
Retry (seconds)	The number of seconds a device waits between attempts to establish an IKE connection with the remote peer. The default is 2 seconds.

Table H-17 VPN Global Settings &gt; ISAKMP/IPsec Settings Tab

Element	Description
Periodic	<p>Available only if Enable Keepalive is selected and supported on routers running IOS version 12.3(7)T and later, except 7600 devices.</p> <p>When selected, enables you to send dead-peer detection (DPD) keepalive messages even if there is no outbound traffic to be sent. Usually, DPD keepalive messages are sent between peer devices only when no incoming traffic is received but outbound traffic needs to be sent.</p> <p>For more information, see <a href="#">About IKE Keepalive, page 9-79</a>.</p>
Identity	<p>During Phase I IKE negotiations, peers must identify themselves to each other.</p> <p>Select to use the IP address or the host name that the device will use to identify itself in IKE negotiations. You can also select a distinguished name (DN) to identify a user group name.</p>
SA Requests System Limit	<p>Supported on routers running Cisco IOS Release 12.3(8)T and later, except 7600 routers.</p> <p>The maximum number of SA requests allowed before IKE starts rejecting them.</p> <p>You can enter a value in the range of 0-99999.</p> <p><b>Note</b> Make sure the value you enter equals or exceeds the number of peers connected to the device.</p>
SA Requests System Threshold	<p>Supported on Cisco IOS routers and Catalyst 6500/7600 devices.</p> <p>The percentage of system resources that can be used before IKE starts rejecting new SA requests.</p>
<b>IPsec Settings</b>	
Enable Lifetime	Select to enable you to configure the global lifetime settings for the crypto IPsec SAs on the devices in your remote access VPN.
Lifetime (secs)	The number of seconds a security association will exist before expiring. The default is 3,600 seconds (1 hour).

Table H-17 VPN Global Settings &gt; ISAKMP/IPsec Settings Tab

Element	Description
Lifetime (kbytes)	The volume of traffic (in kilobytes) that can pass between IPsec peers using a given security association before it expires. The default is 4,608,000 kilobytes.
Xauth Timeout (seconds)	Supported on Cisco IOS routers and Catalyst 6500/7600 devices. The number of seconds the device will wait for a system response to the Xauth challenge.  When negotiating tunnel parameters for establishing IPsec tunnels in a remote access configuration, Xauth adds another level of authentication that identifies the user who requests the IPsec connection. Using the Xauth feature, the client waits for a "username/password" challenge after the IKE SA was established. When the end user responds to the challenge, the response is forwarded to the IPsec peers for an additional level of authentication.
Max Sessions	Supported on PIX 7.0 and ASA devices.  The maximum number of SAs that can be enabled simultaneously on the device.
Enable IPsec via Sysopt (PIX and ASA only)	Supported on ASA devices, and PIX Firewalls versions 6.3 or 7.0. When selected (the default), specifies that any packet that comes from an IPsec tunnel is implicitly trusted (permitted).
Save button	Available only if you are authorized to modify this policy. Saves your changes to the server but keeps them private.  <b>Note</b> To publish your changes, click the <b>Submit</b> button on the toolbar.

## NAT Settings Tab

Use the NAT Settings tab of the VPN Global Settings page to define global Network Address Translation (NAT) settings that enable devices that use internal IP addresses to send and receive data through the Internet.

### Navigation Path

Open the [VPN Global Settings Page](#), page H-42, then click the **NAT Settings** tab.

### Related Topics

- [Understanding NAT](#), page 9-80
- [VPN Global Settings Page](#), page H-42
- [VPN Global Settings in Remote Access VPNs](#), page 10-27
- [Configuring Global Settings in a Remote Access VPN](#), page 10-27

### Field Reference

**Table H-18**      *VPN Global Settings > NAT Settings Tab*

Element	Description
Enable Traversal Keepalive	<p>When selected, enables you to configure NAT traversal keepalive on a device.</p> <p>NAT traversal keepalive is used for the transmission of keepalive messages when there is a device (middle device) located between a VPN-connected hub and spoke, and that device performs NAT on the IPsec flow.</p> <p><b>Note</b> On Cisco IOS routers, NAT traversal is enabled by default. If you want to disable the NAT traversal feature, you must do this manually on the device or using a FlexConfig (see <a href="#">Chapter 19, “Managing FlexConfigs”</a>).</p> <p>For more information, see <a href="#">About NAT Traversal</a>, page 9-81.</p>

**Table H-18**      **VPN Global Settings > NAT Settings Tab**

Element	Description
Interval	Available when NAT Traversal Keepalive is enabled.  The interval, in seconds, between the keepalive signals sent between the spoke and the middle device to indicate that the session is active. The NAT keepalive value can be from 5 to 3600 seconds. The default is 10 seconds.
Enable Traversal over TCP	Supported on PIX 7.0 and ASA devices.  When selected, encapsulates both the IKE and IPsec protocols within a TCP packet and enables secure tunneling through both NAT and PAT devices and firewalls.
TCP Ports	Available only when Enable Traversal over TCP is selected.  The TCP ports for which you want to enable NAT traversal. You must configure TCP ports on the remote clients and on the VPN device. The client configuration must include at least one of the ports you set for the security appliance. You can enter up to 10 ports.
Save button	Available only if you are authorized to modify this policy.  Saves your changes to the server but keeps them private.  <b>Note</b> To publish your changes, click the <b>Submit</b> button on the toolbar.

## General Settings Tab

Use the General Settings tab of the VPN Global Settings page to define fragmentation settings and other global settings on devices in your remote access VPN.

### Navigation Path

Open the [VPN Global Settings Page, page H-42](#), then click the **General Settings** tab.

### Related Topics

- [Understanding Fragmentation, page 9-82](#)

- [VPN Global Settings in Remote Access VPNs](#), page 10-27
- [Configuring Global Settings in a Remote Access VPN](#), page 10-27
- [VPN Global Settings Page](#), page H-42

### Field Reference

**Table H-19**      **VPN Global Settings > General Settings Tab**

Element	Description
<b>Fragmentation Settings</b>	
Fragmentation mode	<p>Supported on Cisco IOS routers and Catalyst 6500/7600 devices. Fragmentation minimizes packet loss in a VPN tunnel when packets are transmitted over a physical interface that cannot support the original size of the packet.</p> <p>Select the required fragmentation mode option from the list:</p> <ul style="list-style-type: none"> <li>• <b>No Fragmentation</b> — Select if you do not want to fragment prior to IPsec encapsulation.</li> <li>• <b>End to End MTU Discovery</b> — Select to use ICMP messages for the discovery of MTU.</li> </ul> <p>End-to-end MTU discovery uses Internet Control Message Protocol (ICMP) messages to determine the maximum MTU that a host can use to send a packet through the VPN tunnel without causing fragmentation.</p> <ul style="list-style-type: none"> <li>• <b>Local MTU Handling</b> — Select to set the MTU locally on the devices. This option is typically used when ICMP is blocked.</li> </ul>
Local MTU Size	<p>Supported on Cisco IOS routers and Catalyst 6500/7600 devices, when Local MTU Handling is the selected fragmentation mode option.</p> <p><b>Note</b> The permitted MTU size is between 68 and 65535 bytes depending on the VPN interface.</p>

Table H-19 VPN Global Settings &gt; General Settings Tab (continued)

Element	Description
DF Bit	<p>Supported on Cisco IOS routers, Catalyst 6500/7600 devices, PIX 7.0 and ASA devices.</p> <p>A Don't Fragment (DF) bit is a bit in an IP header that determines whether a device is allowed to fragment a packet.</p> <p>Select the required setting for the DF bit:</p> <ul style="list-style-type: none"> <li>• <b>Copy</b>—To copy the DF bit from the encapsulated header in the current packet to all the device's packets. If the packet's DF bit is set to fragment, all packets will be fragmented.</li> <li>• <b>Set</b>—To set the DF bit in the packet you are sending. A packet that exceeds the MTU will be dropped and an ICMP message sent to the packet's initiator.</li> <li>• <b>Clear</b>—To cause the device to fragment packets regardless of the original DF bit setting. If ICMP is blocked, MTU discovery fails and packets are fragmented only after encryption.</li> </ul>
Enable Fragmentation Before Encryption	<p>Supported on Cisco IOS routers, Catalyst 6500/7600 devices, PIX 7.0 and ASA devices.</p> <p>When selected, enables fragmentation before encryption, if the expected packet size exceeds the MTU.</p> <p>Lookahead Fragmentation (LAF) is used before encryption takes place to calculate the packet size that would result after encryption, depending on the transform sets configured on the IPsec SA. If the packet size exceeds the specified MTU, the packet will be fragmented before encryption.</p>
Enable Notification on Disconnection	<p>Supported on PIX 7.0 and ASA devices.</p> <p>When selected, enables the device to notify qualified peers of sessions that are about to be disconnected. The peer receiving the alert decodes the reason and displays it in the event log or in a pop-up window. This feature is disabled by default.</p> <p>IPsec sessions may be dropped for several reasons, such as, a security appliance shutdown or reboot, session idle timeout, maximum connection time exceeded, or administrator cut-off.</p>

Table H-19 VPN Global Settings &gt; General Settings Tab (continued)

Element	Description
Enable Spoke-to-Spoke Connectivity through the Hub	Supported on PIX 7.0 and ASA devices. When selected, enables direct communication between spokes in a hub-and-spoke VPN topology, in which the hub is an ASA or PIX 7.0 device.
Enable Default Route	Supported on Cisco IOS routers and Catalyst 6500/7600 devices. When selected, the device uses the configured external interface as the default outbound route for all incoming traffic.
Save button	Available only if you are authorized to modify this policy. Saves your changes to the server but keeps them private. <b>Note</b> To publish your changes, click the <b>Submit</b> button on the toolbar.

## ASA Cluster Load Balance Page

Use the Cluster Load Balance page to enable load balancing for an ASA device in your remote access VPN.



### Note

Load balancing requires an active 3DES/AES license. The ASA device checks for the existence of this crypto license before enabling load balancing. If it does not detect an active 3DES or AES license, the device prevents load balancing, and also prevents internal configuration of 3DES by the load balancing system.

### Navigation Path

1. Click the **Device View** button on the toolbar.
2. From the Device selector, select the device on which you want to configure load balancing.



### Note

You can configure load balancing only on an ASA device.

3. Select **Remote Access VPN > ASA Cluster Load Balance** from the Policy selector.

**Note**

You can also open the Cluster Load Balance page from Policy view. For more information, see [Managing Shared Remote Access VPN Policies in Policy View, page 10-35](#).

**Related Topics**

- [Cluster Load Balancing, page 10-22](#)
- [Configuring a Cluster Load Balance Policy, page 10-23](#)
- [Creating Interface Role Objects, page 8-115](#)

**Field Reference**

**Table H-20**      *ASA Cluster Load Balance Page*

Element	Description
<b>VPN Load Balancing</b>	
Participate in Load Balancing Cluster	Select to specify that the device belongs to the load-balancing cluster.
<b>VPN Cluster Configuration</b>	
Cluster IP Address	The single IP address that represents the entire virtual cluster. The IP address should be in the same subnet as the external interface.
UDP Port	The UDP port for the virtual cluster in which the device is participating. If another application is using this port, enter the UDP destination port number that you want to use for load balancing.  The default is 9023.
Enable IPsec Encryption	Select this check box to ensure that all load-balancing information communicated between the devices is encrypted.  When the check box is selected, you must also specify and verify a shared secret. The security appliances in the virtual cluster communicate via LAN-to-LAN tunnels using IPsec.
IPsec Shared Secret	The shared secret to be communicated between IPsec peers if you enabled IPsec encryption. This can be a case-sensitive value between 4 and 16 characters, without spaces.

Table H-20 ASA Cluster Load Balance Page (continued)

Element	Description
<b>Priority</b>	
Accept default device value	When selected (the default), accepts the default priority value assigned to the device.
Configure same priority on all devices in the cluster	When selected, enables you to configure the same priority value to all the devices in the cluster. The priority indicates the likelihood of this device becoming the virtual cluster master, either at startup or when the existing master fails.  Enter a value between 1 and 10.
<b>VPN Server Configuration</b>	
Public interfaces	The public interfaces to be used on the server.  Interfaces are predefined objects. You can click <b>Select</b> to open a dialog box that lists all available interfaces, and sets of interfaces defined by interface roles, in which you can make your selection, or create interface role objects.
Private Interfaces	The private interfaces to be used on the server.  Interfaces are predefined objects. You can click <b>Select</b> to open a dialog box that lists all available interfaces, and sets of interfaces defined by interface roles, in which you can make your selection, or create interface role objects.
Save button	Available only if you are authorized to modify this policy.  Saves your changes to the server but keeps them private.  <b>Note</b> To publish your changes, click the <b>Submit</b> button on the toolbar.

## DN Matching Policy Page

Use the DN Matching Policy page to configure the DN rule matching policies for any remote client connecting to the device.

Distinguished Name (DN) rules are used for enhanced certificate authentication on PIX Firewalls version 7.0 and ASA devices.

**Navigation Path**

1. Click the **Device View** button on the toolbar.
2. From the Device Selector, select the device on which you want to configure the DN Matching policy.
3. Select **Remote Access VPN > DN Matching Policy** from the Policy selector.

**Note**

You can also open the DN Matching Policy page from Policy view. For more information, see [Managing Shared Remote Access VPN Policies in Policy View, page 10-35](#).

**Related Topics**

- [DN Matching Policies, page 10-30](#)
- [Configuring a DN Matching Policy, page 10-31](#)
- [DN Matching Rules Page, page H-54](#)

**Field Reference**

**Table H-21**      **DN Matching Policy Page**

<b>Element</b>	<b>Description</b>
Use Configured Rules to Match a Certificate to a Group	When selected, the server uses the configured DN rules to establish authentication and determine which tunnel group to map the client to.
Use Certificate Organization Unit field to Determine the Group	When selected (default), the server uses the organizational unit (OU) field of the DN to establish authentication and determine which tunnel group to map the client to.
Use IKE Identity to Determine the Group	When selected (default), the server uses the IKE identity of the DN to establish authentication and determine which tunnel group to map the client to.
User Peer IP Address to Determine the Group	When selected (the default), the server uses the peer IP address of the DN to establish authentication and determine which tunnel group to map the client to.

Table H-21 DN Matching Policy Page (continued)

Element	Description
Save button	<p>Available only if you are authorized to modify this policy.</p> <p>Saves your changes to the server but keeps them private.</p> <p><b>Note</b> To publish your changes, click the <b>Submit</b> button on the toolbar.</p>

## DN Matching Rules Page

Use the DN Matching Rules page to configure the DN rule matching rules and parameters for any remote client connecting to the device.

Distinguished Name (DN) rules are used for enhanced certificate authentication on PIX Firewalls version 7.0 and ASA devices.



### Note

A tunnel group must exist in the configuration before you can create and map a DN Matching rule to it. If you unassign a tunnel group after creating a DN Matching rule, the DN rules that are mapped to the tunnel group are unassigned. See [Configuring Tunnel Group Policies, page 10-9](#).

### Navigation Path

1. Click the **Device View** button on the toolbar.
2. From the Device Selector, select the device on which you want to configure the DN Matching Rules policy.
3. Select **Remote Access VPN > DN Matching Rules** from the Policy selector.



### Note

You can also open the DN Matching Rules page from Policy view. For more information, see [Managing Shared Remote Access VPN Policies in Policy View, page 10-35](#).

### Related Topics

- [DN Matching Rules, page 10-32](#)
- [Configuring a DN Matching Rules Policy, page 10-33](#)

- [DN Matching Policy Page](#), page H-52
- [DN Rule Dialog Box \(Upper Pane\)](#), page H-56
- [DN Rule Dialog Box \(Lower Pane\)](#), page H-57

### Field Reference

**Table H-22**      **DN Matching Rules Page**

Element	Description
<b>Upper Pane</b>	
Mapped to Tunnel Group	The tunnel group to which the DN matching rule is mapped.
Priority	The priority number of the DN matching rule. A lower number has higher priority.
Create button	Click to open the dialog box for creating a DN matching rule. The DN Rule dialog box appears. See <a href="#">DN Rule Dialog Box (Upper Pane)</a> , page H-56.
Edit button	Select the row of a DN matching rule from the upper pane, then click to open the dialog box for editing the selected DN matching rule. See <a href="#">DN Rule Dialog Box (Upper Pane)</a> , page H-56.
Delete button	Select the rows of one or more rules, then click to delete.
<b>Lower Pane</b>	
Field	The specified field of the DN matching rule. The certificate field can be either Subject or Issuer.
Component	The matching component of the certificate for the DN matching rule.
Operator	The operator of the matching rule.
Value	The value of the matching rule. The displayed value must match the value in the client certificate.
Create button	Click to open the DN Rule dialog box for creating a new DN matching rule. See <a href="#">DN Rule Dialog Box (Lower Pane)</a> , page H-57.
Edit button	Select the row of a DN matching rule from the lower pane, then click to open the dialog box for editing the selected DN matching rule. See <a href="#">DN Rule Dialog Box (Lower Pane)</a> , page H-57.
Delete button	Select the rows or one or more rules, then click to delete.

**Table H-22**      **DN Matching Rules Page (continued)**

Element	Description
Default Tunnel Group	Select the default tunnel group to be used if no matching rules are found.
Save button	Available only if you are authorized to modify this policy. Saves your changes to the server but keeps them private. <b>Note</b> To publish your changes, click the <b>Submit</b> button on the toolbar.

## DN Rule Dialog Box (Upper Pane)

Use the upper pane of the DN Matching Rules page to specify the priority and tunnel groups to which the rules will be mapped. You can create a new DN matching rule or edit an existing one in the DN Rule dialog box.

### Navigation Path

On the [DN Matching Rules Page, page H-54](#), click **Create** in the upper pane or select a row in the upper table and click **Edit**.

### Related Topics

- [DN Matching Rules Page, page H-54](#)
- [DN Rule Dialog Box \(Lower Pane\), page H-57](#)

### Field Reference

**Table H-23**      **DN Rule Dialog Box (Upper Pane)**

Element	Description
Tunnel Group	Select the tunnel group to which the DN matching rule will apply. Clients attempting to connect to this tunnel group must satisfy DN matching rule conditions to connect to the device.

**Table H-23**      **DN Rule Dialog Box (Upper Pane) (continued)**

Element	Description
Priority	<p>The priority number of the matching rule. A lower number has a higher priority. For example, a matching rule with a priority number of 2, has a higher priority than a matching rule with a priority number of 5.</p> <p>If multiple rules are established for the same tunnel group, the device will go through the rules in numerical order. All matching rules must be satisfied for a remote client to connect to the device.</p>
OK button	Saves your changes locally on the client and closes the dialog box.

## DN Rule Dialog Box (Lower Pane)

The lower pane of the DN Matching rules page displays the details of the tunnel group mapping selected in the upper pane. In this pane, you create the DN matching rules that must be satisfied for a remote client to connect to the device. You can create a DN matching rule or edit an existing one in the DN Rule dialog box.

### Navigation Path

On the [DN Matching Rules Page, page H-54](#), click **Create** in the lower pane or select a row in the lower table and click **Edit**.

### Related Topics

- [DN Matching Rules Page, page H-54](#)
- [DN Rule Dialog Box \(Upper Pane\), page H-56](#)

### Field Reference

**Table H-24**      **DN Rule Page (Lower Pane)**

Element	Description
Field	Select the field for the matching rule according to the <b>Subject</b> or the <b>Issuer</b> of the client certificate.

Table H-24 DN Rule Page (Lower Pane) (continued)

Element	Description
Component	Select the component of the client certificate to use for the matching rule.
Operator	<p>Select the operator for the matching rule as follows:</p> <ul style="list-style-type: none"> <li>• Equals—The certificate component must match the entered value. If they do not match exactly, the connection is denied.</li> <li>• Contains—The certificate component must contain the entered value. If the component does not contain the value, the connection is denied.</li> <li>• Does Not Equal—The certificate component <i>cannot</i> equal the entered value. For example, for a selected certificate component of Country, and an entered value of USA, if the client county value equals USA, then the connection is denied.</li> <li>• Does Not Contain—The certificate component <i>cannot</i> contain the entered value. For example, for a selected certificate component of Country, and an entered value of USA, if the client county value contains USA, the connection is denied.</li> </ul>
Value	The value of the matching rule. The value entered is associated with the selected component and operator.
OK button	Saves your changes locally on the client and closes the dialog box.