



## CHAPTER 11

# Managing Remote Access VPNs

---

A virtual private network (VPN) consists of multiple remote peers securely transmitting private data to one another over an unsecured network, such as the Internet. Remote access VPNs use tunnels to encapsulate data packets within normal IP packets for forwarding over IP-based networks, using encryption to ensure privacy and authentication to ensure integrity of data.

Remote access VPNs permit secure, encrypted connections between a company's private network and remote users, by establishing an encrypted IPsec tunnel across the Internet using broadband cable, DSL, or Internet service provider (ISP) dial connection.

A remote access VPN comprises a VPN client and a VPN headend device, or VPN gateway. The VPN client software resides on a user's workstation and initiates the VPN tunnel access to the corporate network. At the other end of the VPN tunnel is the VPN gateway at the edge of the corporate site.

When a VPN client initiates a connection to the VPN gateway device, negotiation consists of authenticating the device through Internet Key Exchange (IKE), followed by user authentication using IKE Extended Authentication (Xauth). Next the group profile is pushed to the VPN client using mode configuration, and an IPsec security association (SA) is created to complete the VPN connection.

For remote access VPNs, AAA (authentication, authorization, and accounting) is used for secure access. With user authentication, a valid username and password must be entered before the connection is completed. Usernames and passwords can be stored on the VPN device itself or on an external AAA server, that can provide authentication to numerous other databases. For more information on using AAA servers, see [Understanding AAA Server Objects, page 9-22](#).

**Note**

You can also use the Easy VPN technology to configure remote access VPN policies in site-to-site VPN topologies. Security policies are configured on hardware clients, such as routers, whereas in remote access VPNs, policies are configured on PCs running Cisco VPN client software. For more information, see [Understanding Easy VPN, page 10-109](#).

**Related Topics**

- [Working with Policies in Remote Access VPNs, page 11-3](#)
- [Discovering Remote Access VPN Policies, page 11-2](#)

## Discovering Remote Access VPN Policies

Security Manager allows you to import the configurations of remote access VPN policies during policy discovery. You can discover configurations on devices that are already deployed in your remote access VPN network, so that Security Manager can manage them. These configurations are imported into Security Manager as remote access VPN policies. Remote access VPN policy discovery can be performed by importing the configuration of a live device or by importing a configuration file.

When you initiate policy discovery on a device in a remote access VPN, the system analyzes the configuration on the device and then translates this configuration into Security Manager policies so that the device can be managed. Warnings are displayed if the imported configuration completes only a partial policy definition. If additional settings are required, you must go to the relevant page in the Security Manager interface to complete the policy definition. You can also rediscover the configurations of devices that are already managed with Security Manager.

**Note**

You should perform deployment immediately after you discover the policies on a device before you make any changes to policies or unassign policies from the device; otherwise, the changes that you configure in Security Manager might not be deployed to the device.

Be aware that after rediscovery on a device any shared policies that were configured on the device are replaced by the local policies that are discovered.

---

To perform discovery of all remote access VPN policies that are configured on a selected device in a remote access VPN, select the **RA VPN Policies** check box in the Create Discovery Task dialog box. For more information, see [Discover Policies On Device Dialog Box, page D-17](#).

#### Related Topics

- [Discovering Policies, page 7-7](#)
- [Discovering Policies on Devices Already in Security Manager, page 7-10](#)
- [Understanding Policies, page 7-1](#)
- [Working with Policies in Remote Access VPNs, page 11-3](#)

## Working with Policies in Remote Access VPNs

A remote access VPN policy defines the IPsec parameters that the VPN client and VPN gateway use to create the VPN tunnel. In some cases, several types of policies might be required to define a full configuration image that can be assigned to devices. Other remote access VPN policies can be assigned individually to devices.

You can set up and configure a remote access VPN on Cisco IOS routers, PIX Firewalls, Catalyst 6500 /7600 devices, and Adaptive Security Appliance (ASA) devices.

In Device view, you can view and configure remote access VPN policies for devices. To access Device view, select **View > Device View** or click the **Device View** button on the toolbar. You can right-click a policy in the Policy selector to display menu options that enable you to share the policy and assign the shared policy to or unassign it from the selected device. For more information, see [Performing Basic Policy Management, page 7-18](#).

In Policy View, you can also view all shared policies for each policy type in a remote access VPN, edit policies, and modify their assignments to devices. See [Managing Shared Remote Access VPN Policies in Policy View, page 11-35](#).

**Note**

You must have read-write permissions to modify a remote access VPN policy. For more information, see [Modify Policies Permissions, page 2-13](#).

The following topics provide information about the policies you can configure on a remote access VPN from the Device view:

- [User Group Policies in Remote Access VPNs, page 11-6](#)
- [Tunnel Group Policies in Remote Access VPNs, page 11-8](#)
- [IPsec Proposals in Remote Access VPNs, page 11-12](#)
- [IKE Proposals in Remote Access VPNs, page 11-18](#)
- [Cluster Load Balancing, page 11-21](#)
- [Public Key Infrastructure Policies in Remote Access VPNs, page 11-25](#)
- [VPN Global Settings in Remote Access VPNs, page 11-27](#)
- [DN Matching Policies, page 11-31](#)
- [DN Matching Rules, page 11-33](#)

**Related Topics**

- [Chapter H, “Remote Access VPN User Interface Reference”](#)
- [Using the Remote Access Configuration Wizard, page 11-4](#)
- [Discovering Remote Access VPN Policies, page 11-2](#)

## Using the Remote Access Configuration Wizard

The Remote Access Configuration wizard enables you to configure your device as a remote access VPN server, quickly and easily. After the policies are configured, specific security parameters defined in these policies are pushed to the client by the server, minimizing configuration on the client.

Depending on the device type, the first step of the wizard requires you to configure a user group or tunnel group policy. A user group policy must be configured on an IOS security router, PIX Firewall, or Catalyst 6500/7600 device. Tunnel group policies must be configured on ASA devices or PIX Firewalls version 7.0.

The wizard then assigns other policies that are required to complete the configuration to the device. These policies can be the default policies predefined by Security Manager, or shared policies that you created using Security Manager. For more information, see [Assigning the Default Remote Access VPN Policies](#), page 11-11.

**Note**

---

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

---

The following policies can assigned to a device to configure it as a remote access VPN server:

- User Group ( IOS router, PIX Firewall, or Catalyst 6500/7600 device only)
- Tunnel Group (ASA device or PIX Firewall version 7.0 only)
- IPsec Proposal
- High Availability
- IKE Proposals
- Public Key Infrastructure (PKI)
- VPN Global Settings
- Cluster Load Balance (ASA device or PIX Firewall version 7.0 only)
- DN Matching (ASA device or PIX Firewall version 7.0 only)
- DN Matching Rules (ASA device or PIX Firewall version 7.0 only)

**Note**

---

You can also configure these policies on your device individually from the Remote Access VPN Policies folder.

---

To access the Remote Access Configuration wizard:

1. Select **View > Device View** or 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.

#### 4. Click **Remote Access Configuration Wizard**.

#### Related Topics

- [Working with Policies in Remote Access VPNs, page 11-3](#)
- [Configuring User Group Policies, page 11-7](#)
- [Configuring Tunnel Group Policies, page 11-9](#)
- [Assigning the Default Remote Access VPN Policies, page 11-11](#)

## User Group Policies in Remote Access VPNs

When you configure a remote access VPN server, you must create user groups to which remote clients will belong. A user group policy specifies the attributes that determine user access to and use of the VPN. User groups simplify system management, enabling you to quickly configure VPN access for large numbers of users.

For example, in a typical remote access VPN, you might allow a finance group to access one part of a private network, a customer support group to access another part, and an MIS group to access other parts. In addition, you might allow specific users within MIS to access systems that other MIS users cannot access. User group policies provide the flexibility to do so securely.

Remote clients must have the same group name as the user group configured on the VPN server so that they can connect to the device; otherwise, a connection cannot be established. When a remote client establishes a connection to the VPN server, the group policies for that user group are pushed to all clients belonging to the same user group. You can configure user groups on the local remote access VPN server and external AAA servers.



#### Note

---

The remote access VPN server on which you define a user group policy can be a Cisco IOS router, PIX 6.3 Firewall, or 6500 /7600 device.

---

On the User Group Policy page, you can specify the user groups you want to assign to your remote access VPN server. You can create and edit user group policies. You can open the User Group Policy page from the Remote Access Configuration wizard or from the Remote Access VPN Policies folder.

**Related Topics**

- [Configuring User Group Policies, page 11-7](#)
- [User Groups Objects Page, page F-547](#)

## Configuring User Group Policies

This procedure describes how to specify the user groups to assign to your remote access VPN server.

**Before You Begin**

In Device view (**View > Device View**), select the required device (Cisco IOS router, PIX Firewall, or Catalyst 6500 /7600 ).

**Related Topics**

- [User Group Policy Page, page H-3](#)
- [Using the Remote Access Configuration Wizard, page 11-4](#)
- [User Group Policies in Remote Access VPNs, page 11-6](#)
- [Managing Shared Remote Access VPN Policies in Policy View, page 11-35](#)
- [Understanding User Group Objects, page 9-199](#)

- 
- Step 1** Open the User Group Policy page.
- a. From the wizard:
    - Select **View > Device View > Remote Access VPN > Configuration Wizard**.
    - Click **Remote Access Configuration Wizard**.
  - b. From the Remote Access VPN Policies folder:
    - Select **View > Device View > Remote Access VPN > RA VPN Policies > User Group Policy**, from the Policy selector.
- Step 2** From the User Group Policy page, select the required user groups from the **Available User Groups list**, and click >>. For a description of the elements on this page, see [Table H-1 on page H-4](#).

User groups are objects. If the required user group is not in the list, click **Create** to open the User Groups Editor dialog box that enables you to create or edit a user group object.

- Step 3** If you opened the User Group Policy page from the wizard, click **Next** to advance to the next step of the wizard. See [Assigning the Default Remote Access VPN Policies, page 11-11](#).

If you opened the User Group Policy page from the Remote Access VPN Policies folder, click **Save** to save your changes to the server.



---

**Note** To publish your changes, click the **Submit** button on the toolbar.

---

## Tunnel Group Policies in Remote Access VPNs

A tunnel group is a set of records which contain VPN tunnel connection policies, including the attributes that pertain to creating the tunnel itself.

Tunnel groups identify the group policy for a specific connection, which includes user-oriented attributes. If you do not assign a tunnel group policy to a user, the default group policy for the connection applies.

You can create one or more tunnel groups specific to your environment. Tunnel groups can be configured on the local remote access VPN server or on external AAA servers.

On the Tunnel Group Policy page, you can view the tunnel group policies defined on your remote access VPN server. You can create and edit tunnel group policies. You can open the Tunnel Group Policy page from the Remote Access Configuration wizard or from the Remote Access VPN Policies folder.

### **RADIUS SDI Authentication**

When you configure a tunnel group policy, if the authentication server group that you select uses SDI as the protocol, Radius SDI authentication is enabled. RADIUS SDI refers to the process of the secure gateway performing SDI authentication using a RADIUS SDI proxy, which communicates with the SDI server.

When this feature is enabled, you are prompted for the username and password from the RADIUS server for the Easy VPN and remote access VPN clients in response to an IKE Xauth challenge from the RADIUS authentication server or headend. Xauth lets you deploy IPsec on VPNs using RADIUS as your user authentication method within the IKE protocol.

A VPN client handles Radius SDI authentication the same as native SDI authentication, which makes authentication easier for VPN Client users to authenticate using SDI. This feature provides authentication to a user, who has the VPN client installed on their system, by prompting for a username and a password, and then verifies them with the information stored in the RADIUS database.

**Note**

---

You can configure tunnel group policies only on PIX Firewalls version 7.0, or ASA devices.

---

**Related Topics**

- [Configuring Tunnel Group Policies, page 11-9](#)
- [Tunnel Group Policy Page, page H-4](#)

## Configuring Tunnel Group Policies

This procedure describes how to create or edit tunnel group policies on your remote access VPN server.

**Before You Begin**

In Device view (**View > Device View**), select the required device (PIX 7.0 or ASA device).

**Related Topics**

- [Tunnel Group Policy Page, page H-4](#)
- [Tunnel Group Policies in Remote Access VPNs, page 11-8](#)
- [Managing Shared Remote Access VPN Policies in Policy View, page 11-35](#)

---

**Step 1** Open the Tunnel Group Policy page.

- a. From the wizard:

- Select **View > Device View > Remote Access VPN > Configuration Wizard**.
  - Click **Remote Access Configuration Wizard**.
- b. From the Remote Access VPN Policies folder:
- Select **View > Device View > Remote Access VPN > RA VPN Policies > Tunnel Group Policy (PIX 7.0/ASA)**, from the Policy selector.
- Step 2** Click **Create** in the Tunnel Group Policy page, or select a device from the table on the Tunnel Group Policy page and click **Edit**. The Tunnel Group Editor dialog box opens, displaying the General tab. For a description of the elements on the Tunnel Group Policy page, see [Table H-2 on page H-5](#).
- Step 3** On the General tab, specify the global AAA settings for your tunnel group and select which method (or methods) of address assignment to use. For a description of the elements on the General tab, see [Table H-3 on page H-7](#).
- Step 4** Click the **IPsec** tab to specify IPsec and IKE parameters for the tunnel group policy. For a description of the elements on the IPsec tab, see [Table H-4 on page H-10](#).
- Step 5** Click the **Advanced** tab to specify interface-specific information for your tunnel group policy. For a description of the elements on the Advanced tab, see [Table H-5 on page H-12](#).
- Step 6** Click the **Client VPN Software Update** tab to view and edit the client type, VPN Client revisions, and image URL for each client VPN software package installed. For a description of the elements on the Client VPN Software Update tab, see [Table H-6 on page H-13](#).
- Step 7** After you finish creating or editing your tunnel group policy, click **OK** to save your changes locally on the client and close the Tunnel Group Policy Editor dialog box.
- Step 8** If you opened the Tunnel Group Policy page from the wizard, click **Next** to advance to the next step of the wizard. See [Assigning the Default Remote Access VPN Policies, page 11-11](#).
- If you opened the Tunnel Group Policy page from the Remote Access VPN Policies folder, click **Save** to save your changes to the server.



---

**Note** To publish your changes, click the **Submit** button on the toolbar.

---

## Assigning the Default Remote Access VPN Policies

The VPN Defaults page of the Remote Access Configuration Wizard displays all the available policy types that can be assigned to your device. For each policy type, you can assign either the factory default policy (a private policy), or a shared policy that you created using Security Manager. When you click **Finish**, the selected policies are assigned to your device.

To assign a policy that is not listed, you can change the policy defaults selection in the VPN Policy Defaults page (**Tools > Security Manager Administration > VPN Policy Defaults**). On this page, you can view the default policies available for assignment to remote access VPN devices. These include the factory defaults, in addition to any shared VPN policies that you created and submitted or approved (depending on the workflow mode), with Security Manager.



---

**Note** In Policy view, you can view all shared policies that were defined for each policy type in a remote access VPN, edit individual policies, and modify their device assignments. For more information, see [Managing Shared Policies in Policy View, page 7-39](#).

---



---

**Note** Default policies are not available for User Group and Tunnel Group policies. You must define a user group policy (or tunnel group policy for ASA devices and PIX Firewalls version 7.0) each time you configure your remote access VPN server.

If you try to select a default policy that is locked by another user, a warning is displayed. You can change the default in the VPN Defaults page of the wizard in order to bypass the lock, or you can just cancel the configuration of your device until the lock is approved. For more information, see [Understanding Locking, page 7-53](#).

---

**Before You Begin**

- In Device view (**View > Device View**), select the required device.
- Make sure that the default policies you want to assign to this device are selected on the VPN Policy Defaults page (**Tools > Security Manager Administration > VPN Policy Defaults**).

**Related Topics**

- [Remote Access VPN Defaults Page, page H-14](#)
- [VPN Policy Defaults Page, page A-52](#)
- [Using the Remote Access Configuration Wizard, page 11-4](#)

- 
- Step 1** Open the VPN Defaults page by clicking **Next** on the User Group Policy page of the Remote Access Configuration wizard. If the device is an ASA or PIX Firewall version 7.0, click **Next** on the Tunnel Group Policy page. For a description of the elements on the VPN Defaults page, see [Table H-7 on page H-15](#).
- Step 2** For each policy type, select the policy to assign to your device.
- You can select the Factory Default policy or select a shared VPN policy that appears in the list. If a shared policy was not already selected in the Administration tool's VPN Policy Defaults page, none will be assigned.
- Step 3** To view the contents of a selected VPN policy, click the **View Content** button.
- Step 4** Click **Finish** to save your wizard definitions and assign the remote access VPN policies to your device. The wizard closes.
- 

## IPsec Proposals in Remote Access VPNs

An IPsec proposal is a collection of one or more crypto maps. A crypto map combines all the components required to set up IPsec security associations (SAs), including IPsec rules, transform sets, remote peer(s), and other parameters that might be necessary to define an IPsec SA.

When configuring an IPsec proposal, you must define the external interface through which the remote access clients connect to the server, and the encryption and authentication algorithms that protect the data in the VPN tunnel. You can also select a group authorization (Group Policy Lookup) method that defines the

order in which group policies are searched (on the local server or on external AAA servers) and a user authentication (Xauth) method that defines the order in which user accounts are searched.

For more information on IPsec tunnel concepts, see [Understanding IPsec Tunnel Policies, page 10-72](#). For information about user accounts, see [Defining Accounts and Credential Policies, page 15-73](#).

On the IPsec Proposal page, you can view the default IPsec proposal that is available for assignment to your remote access VPN. From this page, you can create a new IPsec proposal or edit the default

When you create or edit an IPsec proposal, you may also configure:

- A VPN Services Module (VPNSM) interface or VPN SPA on a Catalyst 6500/7600 device (see [Configuring a Catalyst VPN Services Module \(VPNSM\) VPN Interface, page 10-39](#)).
- A Cisco IPsec VPN Shared Port Adapter (VPN SPA) blade on a Catalyst 6500/7600 device (see [Configuring a Catalyst VPN Shared Port Adapter \(VPN SPA\) Blade, page 10-41](#)).
- A Firewall Services Module and a VPN Services Module on a Catalyst 6500/7600 device (see [Configuring a Firewall Services Module \(FWSM\) Interface with VPNSM or VPN SPA, page 10-48](#)).
- VRF-Aware IPsec on a Catalyst 6500/7600 device (see [Configuring VRF-Aware IPsec Settings, page 10-56](#)).
- A dynamic virtual interface on an IOS router (see [PVC Dialog Box—QoS Tab, page K-63](#)).

### Using Dynamic Virtual Template Interfaces in Remote Access VPNs

Dynamic virtual template interfaces (VTIs) provide highly secure and scalable connectivity for remote-access VPNs, replacing dynamic crypto maps and the dynamic hub-and-spoke method for establishing tunnels. you can use dynamic VTIs for both the server and remote configuration. The tunnels provide an on-demand separate virtual access interface for each VPN session. The configuration of the virtual access interfaces is duplicated from a virtual template configuration, which includes the IPsec configuration and any features configured on the virtual template interface. Dynamic VTIs provide efficiency in the use of IP addresses and provide secure connectivity. They enable dynamically downloadable per-group and per-user policies to be configured on a RADIUS server. Dynamic VTI simplifies VRF-Aware IPsec deployment, as the VRF is configured on the interface.

When this feature is enabled, Security Manager implicitly creates the virtual template interface for the selected device in a remote access VPN. All you must do is provide the IP address on the server that will be used as the virtual template interface, or use an existing loopback interface. The virtual template interface is created on the remote client without an IP address.

You can configure dynamic VTI when configuring an IPsec proposal on your remote access VPN server.

**Note**

---

You can configure dynamic VTI only on routers running Cisco IOS Release 12.4(2)T and later, except 7600 devices.

You can configure dynamic VTI with or without VRF-Aware IPsec.

You can also configure dynamic VTI in a site-to-site Easy VPN topology. For more information, see [Understanding Easy VPN, page 10-109](#).

---

**Related Topics**

- [Configuring an IPsec Proposal on a Remote Access VPN Server, page 11-14](#)
- [IPsec Proposal Page, page H-15](#)

## Configuring an IPsec Proposal on a Remote Access VPN Server

This procedure describes how to create or edit an IPsec proposal for your remote access VPN server.

**Note**

---

On a Catalyst 6500/7600, you can also configure a VPN Services Module (VPNSM) interface or VPN SPA, a Firewall Services Module with a VPN Services Module, and/or VRF-Aware IPsec.

If the device is a router IOS version 12.4(2)T or later, except 7600 device, you can configure a dynamic virtual interface on it.

If the device is a PIX 7.0, ASA, or IOS router except 7600, you can also configure reverse route injection on the crypto map.

---

### Before You Begin

- In Device view (**View > Device View**), select the device on which you want to configure the IPsec proposal.

### Related Topics

- [PVC Dialog Box—QoS Tab, page K-63](#)
- [Understanding VRF-Aware IPsec, page 10-51](#)
- [Managing Shared Remote Access VPN Policies in Policy View, page 11-35](#)
- [IPsec Proposals in Remote Access VPNs, page 11-12](#)
- [IPsec Proposal Page, page H-15](#)
- [IPsec Proposal Editor Dialog Box \(for PIX and ASA Devices\), page H-18](#)
- [IPsec Proposal Editor Dialog Box \(for IOS Routers and Catalyst 6500/7600 Devices\), page H-20](#)
- [VPN/VPN SPA Settings Dialog Box, page H-23](#)
- [FWSM Settings Tab \(IPsec Proposal Editor\), page H-25](#)
- [Understanding IPsec Tunnel Policies, page 10-72](#)

---

**Step 1** In Device view, select **Remote Access VPN > RA VPN Policies > IPsec Proposal** from the Policy selector. The IPsec Proposal page opens.

For a description of the elements on the IPsec Proposal page, see [Table H-8 on page H-16](#).

**Step 2** Click **Create** on the IPsec Proposal page, or select a row in the table on the IPsec Proposal page, and click **Edit**. The IPsec Proposal Editor dialog box opens.



---

**Note** The elements in IPsec Proposal Editor dialog box differ depending on the selected device.

---

**Step 3** If the selected device is a PIX 7.0 or an ASA device:

- a. Select the external interface through which remote access clients will connect to the server.
- b. Select the transform set or sets to be used for your tunnel policy.

- c. If you do not want to configure Reverse Route Injection (RRI) on the device's crypto map, select the None option from the list.

The default option, Standard, creates routes based on the destination information defined in the crypto map access control list (ACL). For more information, see [About Reverse Route Injection, page 10-75](#).

- d. If required, enable the configuration of Network Address Translation Traversal (NAT-T) on an ASA device. See [Understanding NAT, page 10-79](#).
- e. For a PIX device, specify the AAA or Xauth user authentication method to define the order in which user accounts are searched.
- f. Click **OK** to save your changes locally on the client and close the dialog box. The changes appear in the table of the IPsec Proposal page.

For a description of the elements on the IPsec Proposal Editor dialog box, see [Table H-9 on page H-18](#).

- Step 4** If the selected device is a Cisco IOS router or Catalyst 6500/7600, the IPsec Proposal Editor dialog box opens displaying the General tab.




---

**Note** The IPsec Proposal Editor dialog box displays two tabs—General and Dynamic VTI/VRF Aware IPsec. If the selected device is a Catalyst 6500/7600, the FWSM Settings tab is also displayed.

---

- a. In the General tab (for a description of the elements in the General tab, see [Table H-10 on page H-21](#)):
  - Specify the external interface through which remote access clients will connect to the server.




---

**Note** **Important:** If the selected device is a Catalyst 6500/7600, specify the inside VLAN that serves as the inside interface to the VPN Services Module (VPNSM) or VPN SPA. Click Select to open a dialog box in which you define the settings that enable you to configure a VPNSM or VPN SPA. For a description of the elements in the VPNSM/VPN SPA Settings dialog box, see [Table H-11 on page H-24](#)

---

For information about configuring a VPNSM, see [Configuring a Catalyst VPN Services Module \(VPNSM\) VPN Interface, page 10-39](#).

For information about configuring a VPN SPA, see [Configuring a Catalyst VPN Shared Port Adapter \(VPN SPA\) Blade](#), page 10-41.

- Select the transform set(s) to be used for your tunnel policy.
  - If required, enable reverse route injection (RRI) to ensure that a static route is created on the device for each assigned address to the client.
  - To configure reverse route injection (RRI) on the device's crypto map, select the required option from the Reverse Route Injection list. For more information, see [About Reverse Route Injection](#), page 10-75.
  - Select an AAA authorization method list to use for defining the order in which the group policies are searched. Group policies can be configured on the local server or on an external AAA server.
  - Select the AAA or Xauth user authentication method to use for defining the order in which user accounts are searched.
- b.** If the selected device is a Catalyst 6500/7600, click the **FWSM** tab and define the settings that enable you to connect between a Firewall Services Module (FWSM) and an IPsec VPNSM blade or VPN SPA blade that is already configured on a Catalyst 6500/7600 device. For a description of the elements in the FWSM Settings tab, see [Table H-12 on page H-27](#). For more information, see [Configuring a Firewall Services Module \(FWSM\) Interface with VPNSM or VPN SPA](#), page 10-48.
- c.** Click the **Dynamic VTI/VRF Aware IPsec** tab to configure a dynamic virtual interface, VRF-Aware IPsec settings, or both on the device. For a description of the elements on this tab, see [Table H-13 on page H-28](#).

**Step 5** After you finish creating or editing your IPsec proposal, click **OK** to save your changes locally on the client, and close the IPsec Proposal Editor dialog box.

The changes appear in the table of the IPsec Proposal page.

**Step 6** Click **Save** to save your changes to the server.



---

**Note** To publish your changes, click the **Submit** button on the toolbar.

---

## IKE Proposals in Remote Access VPNs

Internet Key Exchange (IKE), also called ISAKMP, is the negotiation protocol that enables two hosts to agree on how to build an IPsec security association. To configure your device for remote access VPNs, you must specify the encryption algorithm, authentication algorithm, and key exchange method that the device should use when negotiating a VPN connection with the remote clients.

An IKE proposal is a set of algorithms that two peers use to secure the IKE negotiation between them. IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations. You can create multiple, prioritized policies at each peer to ensure that at least one policy will match a remote peer's policy.

For more information on IKE concepts, see [Understanding IKE, page 10-67](#).

On the IKE Proposal page, you can select the IKE proposals to assign to your remote access VPN server. You can create and edit IKE proposals.

### Related Topics

- [Configuring IKE Proposals on a Remote Access VPN Server, page 11-18](#)
- [IKE Proposal Page, page H-32](#)
- [Managing Shared Remote Access VPN Policies in Policy View, page 11-35](#)

## Configuring IKE Proposals on a Remote Access VPN Server

This procedure describes how to specify the IKE proposals you want to assign to your remote access VPN server.

### Before You Begin

In Device view (**View > Device View**), select the required device.

### Related Topics

- [IKE Proposal Page, page H-32](#)
- [IKE Proposals in Remote Access VPNs, page 11-18](#)
- [Managing Shared Remote Access VPN Policies in Policy View, page 11-35](#)

- 
- Step 1** In Device view, select **Remote Access VPN > RA VPN Policies > IKE Proposal** from the Policy selector. The IKE Proposal page opens.
- Step 2** On the IKE Proposal page, select the required IKE proposals from the Available IKE Proposals list, and click >>. For a description of the elements on this page, see [Table H-14 on page H-33](#).
- IKE proposals are objects. If the required IKE proposal is not included in the list, click Create to open the IKE Editor dialog box that enables you to create or edit an IKE proposal object. For more information, see [Table F-46 on page F-89](#).
- Step 3** Click **Save** to save your changes to the server.



---

**Note** To publish your changes, click the **Submit** button on the toolbar.

---

## High Availability in Remote Access VPNs

In Security Manager, High Availability (HA) is supported by the creation of an HA group made up of two or more hub devices that use Hot Standby Routing Protocol (HSRP) to provide transparent, automatic device failover. By sharing a virtual IP address, the hubs in the HA group present the appearance of a single virtual device or default gateway to the hosts on a LAN. One hub in the HA group is always active and assumes the virtual IP address, while the others are standby hubs. The hubs in the group watch for hello packets from active and standby devices. If the active device becomes unavailable for any reason, a standby hub takes ownership of the virtual IP address and takes over the hub functionality. This transfer is seamless and transparent to hosts on the LAN, and to the peering devices.

In remote access VPNs, High Availability (HA) is supported on Cisco IOS routers running IP over LANs.

Stateful SwitchOver (SSO) is used to ensure that state information is shared between the HSRP devices in the HA group. If a device fails, the shared state information enables the standby device to maintain IPsec sessions without having to re-establish the tunnel or renegotiate the security associations.

**Note**

When configuring an HA group, 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. See [Configuring an IPsec Proposal on a Remote Access VPN Server, page 11-14](#).

A remote access VPN server device on which HA is configured cannot be configured as a hub in a site-to-site VPN topology on which HA is configured, using the same outside interface that was used for the remote access VPN server.

For a description of the High Availability page, on which you can provide information for configuring an HA group, see [Table H-15 on page H-34](#).

**Related Topics**

- [Configuring a High Availability Policy, page 11-20](#)
- [High Availability Page, page H-33](#)
- [Configuring an IPsec Proposal on a Remote Access VPN Server, page 11-14](#)

## Configuring a High Availability Policy

This procedure describes the steps required to configure a high availability policy on an IOS router in your remote access VPN.

**Before You Begin:**

- In Device view (**View > Device View**), select the required IOS router.
- Make sure an IPsec proposal is configured on the device.

**Related Topics**

- [High Availability in Remote Access VPNs, page 11-19](#)
- [High Availability Page, page H-33](#)

- 
- Step 1** In Device view, select **Remote Access VPN > High Availability** from the Policy selector. The High Availability page opens. For a description of the elements on this page, see [Table H-15 on page H-34](#).

- Step 2** Specify the virtual IP addresses (and subnet masks) that represent the inside interface and the VPN interface of the HA group, in the relevant fields.



---

**Note** 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.

---

- Step 3** Specify the hello interval and hold time, in seconds.

- Step 4** Specify the standby number of the inside hub interface that matches the internal virtual IP subnet, and the outside hub interface that matches the external virtual IP subnet, for the hubs in the HA group. The numbers must be within the range of 0-255.



---

**Note** Inside and outside standby group numbers must be different.

---

- Step 5** Specify the IP address of the inside interface of the remote peer device which acts as the failover server.

- Step 6** Click **Save** to save your changes to the server.



---

**Note** To publish your changes, click the **Submit button** on the toolbar.

---

## Cluster Load Balancing

In a remote client configuration in which you are using two or more devices connected to the same network to handle remote sessions, you can configure these devices to share their session load. This feature is called load balancing. Load balancing directs session traffic to the least loaded device, thus distributing the load among all devices. Load balancing is effective only on remote sessions initiated with an ASA device.

To implement load balancing, you must group two or more devices on the same private LAN-to-LAN network into a virtual cluster. All devices in the virtual cluster carry session loads. One device in the virtual cluster, called the virtual cluster master, directs incoming calls to the other devices, called secondary devices. The virtual cluster master monitors all devices in the cluster, keeps track of how busy each is, and distributes the session load accordingly.

The virtual cluster appears to outside clients as a single virtual cluster IP address. This IP address is not tied to a specific physical device—it belongs to the current virtual cluster master. A VPN client trying to establish a connection connects first to this virtual cluster IP address. The virtual cluster master then sends back to the client the public IP address of the least-loaded available host in the cluster. In a second transaction (transparent to the user), the client connects directly to that host. In this way, the virtual cluster master directs traffic evenly and efficiently across resources.

The role of virtual cluster master is not tied to a physical device—it can shift among devices. If a machine in the cluster fails, the terminated sessions can immediately reconnect to the virtual cluster IP address. The virtual cluster master then directs these connections to another active device in the cluster. Should the virtual cluster master itself fail, a secondary device in the cluster immediately takes over as the new virtual session master. Even if several devices in the cluster fail, users can continue to connect to the cluster as long as any one device in the cluster is available.

The Cluster Load Balance page enables you to configure load balancing on your VPN device. You must explicitly enable load balancing, as it is disabled by default. All devices that participate in a cluster must share the same cluster-specific values: IP address, encryption settings, encryption key, and port.

#### Related Topics

- [Enabling Redirection Using an FQDN, page 11-22](#)
- [Configuring a Cluster Load Balance Policy, page 11-23](#)
- [ASA Cluster Load Balance Page, page H-45](#)

## Enabling Redirection Using an FQDN

By default, the ASA sends only IP addresses in load-balancing redirection to a client. If certificates are in use that are based on DNS names, the certificates will be invalid when redirected to a secondary device. As a VPN cluster master, this

security appliance can send a fully qualified domain name (FQDN) of a cluster device (another security appliance in the cluster) when redirecting VPN client connections to that cluster device. The security appliance uses reverse DNS lookup to resolve the FQDN of the device to its outside IP address to redirect connections and perform VPN load balancing. All outside and inside network interfaces on the load-balancing devices in a cluster must be on the same IP network.

After you enable load balancing using FQDNs, add an entry for each of your ASA outside interfaces into your DNS server, if such entries are not already present. Each ASA outside IP address should have a DNS entry associated with it for lookups. These DNS entries must also be enabled for Reverse Lookup. Enable DNS lookups on your ASA and define your DNS server IP address on the ASA.

#### Related Topics

- [Cluster Load Balancing, page 11-21](#)
- [Configuring a Cluster Load Balance Policy, page 11-23](#)

## Configuring a Cluster Load Balance Policy


#### Before You Begin

In Device view (**View > Device View**), select the required ASA device.

#### Related Topics

- [Managing Shared Remote Access VPN Policies in Policy View, page 11-35](#)
- [Cluster Load Balancing, page 11-21](#)
- [Enabling Redirection Using an FQDN, page 11-22](#)
- [ASA Cluster Load Balance Page, page H-45](#)

- 
- Step 1** In Device view, select **Remote Access VPN > RA VPN Policies > ASA Cluster Load Balance** from the Policy selector. The ASA Cluster Load Balance page opens. For a description of the elements on this page, see [Table H-20 on page H-46](#).
- Step 2** Select the **Participating in Load Balancing Cluster** check box to specify the device belongs to the load-balancing cluster.

- Step 3** Specify the single IP address that represents the entire virtual cluster. Choose an IP address that is in the same subnet as the external interface.
- Step 4** Specify the UDP port for the virtual cluster to which the device belongs. If another application is using this port, enter the UDP destination port number to use for load balancing. The default is 9023.
- Step 5** If required, select **Enable IPsec Encryption** to ensure that all load-balancing information communicated between the devices is encrypted.
- Step 6** If you selected the **Enable IPsec Encryption** check box, you must specify an **IPsec Shared Secret** password. The security appliances in the virtual cluster communicate via LAN-to-LAN tunnels using IPsec. This password must match the passwords passed on by the client.
- Step 7** In the **Priority** area, select one of the following options:
- **Accept default device value**—To accept the default priority value assigned to the device.
  - **Configure same priority on all devices in the cluster**—To configure the same priority value to all the devices in the cluster. Then enter the priority number (between 1-10) to indicate the likelihood of the device becoming the virtual cluster master, either at startup or when the existing master fails.
- Step 8** Specify the public and private interfaces to be used on the server.
-  **Note** Interfaces are objects. You can click **Select** to open a dialog box that lists all available interface roles and interfaces and in which you can create interface role objects. For more information, see [Understanding Interface Role Objects, page 9-132](#).
- Step 9** If required, select the **Send FQDN to client instead of an IP address when redirecting** check box to enable redirection using FQDNs. This check box is available only for ASA devices running 8.0.2 or later. For more information, see [Enabling Redirection Using an FQDN, page 11-22](#).

**Note**

To use VPN load balancing, you must have an ASA Model 5510 with a Plus license or an ASA Model 5520 or higher. VPN load balancing also requires an active 3DES/AES license. The security appliance checks for the existence of this crypto license before enabling load balancing. If it does not detect an active 3DES or AES license, the security appliance prevents the enabling of load balancing and also prevents internal configuration of 3DES by the load balancing system unless the license permits this usage.

**Step 10** Click **Save** to save your changes to the server.

**Note**

To publish your changes, click the **Submit** button on the toolbar.

## Public Key Infrastructure Policies in Remote Access VPNs

Security Manager supports IPsec configuration with Certification Authority (CA) servers, also known as trustpoints, that manage Public Key Infrastructure (PKI) certificate requests and issue certificates to the devices in a remote access VPN. You can create a Public Key Infrastructure (PKI) policy to generate PKI enrollment requests for PKI certificates and RSA keys, and manage keys and certificates. These services provide centralized key management for the participating devices.

For more information, see [Understanding Public Key Infrastructure Policies](#), page 10-86.

In Security Manager, CA servers are defined as PKI enrollment objects that you can use in your PKI policies. A PKI enrollment object contains the server information and enrollment parameters that are required for creating enrollment requests for CA certificates. For more information, see [Understanding PKI Enrollment Objects](#), page 9-154.

**Note**

In remote access VPNs, digital certificates are used for user authentication. 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. Remote clients should also be configured to use digital certificates for user authentication during IKE negotiations, by specifying the user group name when configuring ISAKMP settings (see [Configuring Global Settings in a Remote Access VPN, page 11-28](#)).

**Related Topics**

- [Configuring a PKI Policy in a Remote Access VPN, page 11-26](#)
- [Public Key Infrastructure Page, page H-36](#)

## Configuring a PKI Policy in a Remote Access VPN

This procedure describes how to specify the CA server(s) that will be used to create a Public Key Infrastructure (PKI) policy in your remote access VPN.

**Before You Begin**

- In Device view (**View > Device View**), select the device on which you are configuring PKI.
- Make sure the selected device has Cisco IOS Release 12.3(7)T or later.
- Please read [Prerequisites for Successful PKI Enrollment, page 10-88](#).

**Related Topics**

- [Managing Shared Remote Access VPN Policies in Policy View, page 11-35](#)
- [Public Key Infrastructure Policies in Remote Access VPNs, page 11-25](#)
- [Understanding Public Key Infrastructure Policies, page 10-86](#)
- [Prerequisites for Successful PKI Enrollment, page 10-88](#)
- [Public Key Infrastructure Page, page H-36](#)
- [Understanding PKI Enrollment Objects, page 9-154](#)

- Step 1** In Device view, select **Remote Access VPN > RA VPN Policies > Public Key Infrastructure** from the Policy selector. The Public Key Infrastructure page opens. For a description of the elements on this page, see [Table H-16 on page H-37](#)
- Step 2** Select the required CA server(s) from the Available CA Servers list and click >>. If the required CA server is not included in the list, click **Create** to open the PKI Enrollment dialog box which enables you to create or edit a PKI enrollment object. For more information, see [PKI Enrollment Dialog Box, page F-481](#).



---

**Note** When creating or editing a PKI enrollment object, make sure you 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 [Defining Additional PKI Attributes, page 9-163](#).

---

- Step 3** Click **Save** to save your changes to the server.



---

**Note** To publish your changes, click the **Submit** button on the toolbar.

---



---

**Note** To save the RSA key pairs and the CA certificates permanently between reloads to flash memory on a PIX firewall version 6.3, you must configure the "ca save all" command. You can do this manually on the device or by using a FlexConfig (see [Chapter 20, "Managing FlexConfigs"](#)).

---

## VPN Global Settings in Remote Access VPNs

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

A full description of VPN global settings is provided in [Understanding VPN Global Settings, page 10-78](#).

Global VPN settings comprise:

- ISAKMP/IPsec settings that enable you to configure ISAKMP (IKE) and IPsec parameters that allow peers to negotiate in establishing a VPN tunnel in a remote access VPN. For more information, see [Understanding ISAKMP/IPsec Settings, page 10-78](#).
- Network Address Translation (NAT) settings to enable devices that use internal IP addresses to send and receive data through the Internet. For more information, see [Understanding NAT, page 10-79](#).
- General Settings, including fragmentation settings and the maximum transmission unit (MTU) handling parameters that you can configure on the devices in your remote access VPN. For more information, see [Understanding Fragmentation, page 10-81](#).

#### Related Topics

- [Configuring Global Settings in a Remote Access VPN, page 11-28](#)
- [VPN Global Settings Page, page H-38](#)

## Configuring Global Settings in a Remote Access VPN

Follow the procedure below to define global settings in your remote access VPN.

#### Before You Begin

In Device view (**View > Device View**), select the required device.

#### Related Topics

- [Managing Shared Remote Access VPN Policies in Policy View, page 11-35](#)
- [VPN Global Settings in Remote Access VPNs, page 11-27](#)
- [VPN Global Settings Page, page H-38](#)
- [ISAKMP/IPsec Settings Tab, page H-39](#)
- [NAT Settings Tab, page H-41](#)
- [General Settings Tab, page H-43](#)

**Step 1** In Device view, select **Remote Access VPN > RA VPN Policies > VPN Global Settings** from the Policy selector.

The VPN Global Settings page opens, displaying the ISAKMP/IPsec Settings tab. For a description of the elements on the ISAKMP/IPsec Settings tab, see [Table H-17 on page H-39](#).

**Step 2** In the **ISAKMP/IPsec Settings** tab, specify global settings for IKE and IPsec, as follows:

- a. Select **Enable Keepalive** to configure IKE keepalive as the default failover and routing mechanism for your devices. (Applies to Cisco IOS routers, Catalyst 6500 /7600 devices, and PIX Firewalls version 6.3.)
- b. Enter the number of seconds a device must wait between sending IKE keepalive packets.
- c. Enter the number of seconds a device must wait between attempts to establish an IKE connection with the remote peer.
- d. Select **Periodic** if you want to send dead-peer detection (DPD) keepalive messages, even if there is no outbound traffic to be sent (for routers except 7600).
- e. Specify whether the device uses an IP address or hostname to identify itself in IKE negotiations. You can also specify to use a distinguished name (DN) to identify a user group name.
- f. Specify the maximum number of SA requests allowed before IKE starts rejecting them (for routers except 7600).
- g. Specify the percentage of system resources that can be used before IKE starts rejecting new SA requests (for Cisco IOS routers and Catalyst 6500 /7600 devices).
- h. Select **Enable Lifetime** to configure the global lifetime settings for the crypto IPsec SAs on the devices in your remote access VPN.
- i. Specify the number of seconds an SA will exist before expiring.
- j. Specify the volume of traffic (in kilobytes) that can pass between IPsec peers using a given SA before it expires.
- k. Specify the Xauth timeout, that is, the number of seconds the device will wait for a system response to the Xauth challenge (Cisco IOS routers and Catalyst 6500 /7600 devices).

- l. Specify the maximum number of SAs that can be enabled simultaneously on the device (ASA or PIX 7.0 devices only).
- m. Select **Enable IPsec via Sysopt** to specify that any packet that comes from an IPsec tunnel be implicitly trusted (PIX 6.3, PIX 7.0, and ASA devices only).

**Step 3** Click the **NAT Settings** tab to define global NAT settings that apply to devices that use internal IP addresses to send and receive data through the public Internet. For a description of the elements on the **NAT Settings** tab, see [Table H-18 on page H-42](#).

- a. Select **Enable Traversal Keepalive** for the transmission of keepalive messages when a device (referred to as the middle device) located between a VPN-connected hub and spoke performs NAT on the IPsec flow.
- b. Specify the interval (between 5 and 3600 seconds) between the keepalive signals sent between the spoke and the middle device to indicate that the session is active.
- c. Select **Enable Traversal over TCP** (for ASA or PIX 7.0 devices only) to encapsulate both the IKE and IPsec protocols within a TCP packet, and enable secure tunneling through both NAT and PAT devices and firewalls.
- d. Enter the TCP ports for which you want to enable NAT traversal (ASA or PIX 7.0 devices only).

**Step 4** Click the **General Settings** tab to define fragmentation and other global settings on the devices in your remote access VPN. For a description of the elements on the **General Settings** tab, see [Table H-19 on page H-43](#).

- a. Select the fragmentation mode from the following options:
  - **No Fragmentation**—Select if you do not want to fragment before IPsec encapsulation.
  - **End to End MTU Discovery**—Select to use ICMP messages for the discovery of MTU.
  - **Local MTU Handling**—Select to set the MTU locally on the devices. This option is typically used when ICMP is blocked.

See [Understanding Fragmentation, page 10-81](#).

- b. Specify the MTU size (between 68 and 65535 bytes depending on the VPN interface).

- c. Select the required setting for the DF bit (for Cisco IOS routers, ASA, or PIX 7.0 devices)—**Copy, Set, or Clear**.
- d. Select **Enable Fragmentation Before Encryption** (for Cisco IOS routers, ASA, or PIX 7.0 devices) to fragment before encryption, if the expected packet size exceeds the MTU (Cisco IOS routers only).
- e. Select **Enable Notification on Disconnection** (for ASA or PIX 7.0 devices only) to notify qualified peers of sessions that are about to be disconnected.
- f. Select **Enable Spoke-to-Spoke Connectivity** through the Hub (for ASA, or PIX 7.0 devices only) to enable direct communication between spokes in a hub-and-spoke VPN topology, in which the hub is an ASA device or a PIX Firewall version 7.0.
- g. Select **Enable Default Route** (for Cisco IOS routers only) to use the device's configured external interface as the default outbound route for all incoming traffic.

**Step 5** Click **Save** to save your changes to the server.

To publish your changes, click the **Submit** button on the toolbar.

---

## DN Matching Policies

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

A DN is a unique identification, made up of individual fields, that can be used as the identifier when matching users to a tunnel group.

Certificate group matching lets you define rules to match a user's certificate to a permission group based on fields in the DN. To establish authentication, you can use any field of the certificate, or you can have all certificate users share a permission group.

To match user permission groups based on fields of the certificate, you define rules that specify the fields to match for a group and then enable each rule for that selected group. A tunnel group must already exist in the configuration before you can create a rule for it.

After you define rules, you must configure a certificate group matching policy to define the method for identifying the permission groups of certificate users. You can match the group from the DN rules, the Organization Unit (OU) field, the IKE identify, or the peer IP address. You can use any or all of these methods.

### Related Topics

- [Configuring a DN Matching Policy, page 11-32](#)
- [DN Matching Policy Page, page H-48](#)

## Configuring a DN Matching Policy

This procedure describes how to configure a DN Matching policy for a remote client trying to connect to a PIX 7.0, or an ASA server device.

### Before You Begin

- In Device view (**View > Device View**), select the required device (PIX 7.0 or ASA device).
- Make sure a tunnel group has been configured on the device. See [Configuring Tunnel Group Policies, page 11-9](#).

### Related Topics

- [Managing Shared Remote Access VPN Policies in Policy View, page 11-35](#)
- [DN Matching Policies, page 11-31](#)
- [Configuring a DN Matching Rules Policy, page 11-34](#)
- [DN Matching Policy Page, page H-48](#)

---

**Step 1** In Device view, select **Remote Access VPN > RA VPN Policies > DN Matching Policy** from the Policy selector. The DN Matching Policy page is displayed.

**Step 2** Select any, or all, of the following check boxes:

- a. Use **Configured Rules to Match a Certificate to a Group** to configure the server to use the configured DN rules to establish authentication.
- b. Use **Certificate Organization Unit (OU) Field to Determine the Group** to configure the server to use the OU field of the DN to establish authentication.
- c. Use **IKE Identify to Determine the Group** to configure the server to use the IKE identity of the DN to establish authentication.

- d. Use **Peer IP address to Determine the Group** to configure the server to use the peer IP address of the DN to establish authentication.
- e. For a description of the elements on the DN Matching Policy page, see [Table H-21 on page H-49](#).

**Step 3** Click **Save** to save your changes to the server.



---

**Note** To publish your changes, click the **Submit** button on the toolbar.

---

## DN Matching Rules



---

**Note**

DN Matching rules can be configured only on PIX Firewalls version 7.0, or ASA devices.

---

When configuring certificate group matching, you must define DN rules to match a remote client's certificate to a permission group, based on fields in the DN.

To match user permission groups based on fields of the certificate, you define rules that specify the fields to match for a group and then enable each rule for that selected group. A tunnel group must already exist in the configuration before you can create and map a rule to it.

After defining the DN rules, you must configure a certificate group matching policy to define the method for identifying the permission groups of certificate users. For more information, see [DN Matching Policies, page 11-31](#).



---

**Note**

A tunnel group must already 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 11-9](#).

---

**Related Topics**

- [Configuring Tunnel Group Policies, page 11-9](#)
- [Configuring a DN Matching Rules Policy, page 11-34](#)
- [DN Matching Rules Page, page H-49](#)

## Configuring a DN Matching Rules Policy

This procedure describes how to configure the DN Matching rules and parameters for any remote client trying to connect to a PIX Firewall version 7.0 or an ASA server device.

**Before You Begin**

- In Device view (**View > Device View**), select the required device (PIX 7.0 or ASA device).
- Make sure a tunnel group has been configured on the device. See [Configuring Tunnel Group Policies, page 11-9](#).

**Related Topics**

- [Managing Shared Remote Access VPN Policies in Policy View, page 11-35](#)
- [Tunnel Group Policies in Remote Access VPNs, page 11-8](#)
- [DN Matching Policies, page 11-31](#)
- [DN Matching Rules, page 11-33](#)
- [DN Matching Rules Page, page H-49](#)

- 
- Step 1** In Device view, select **Remote Access VPN > RA VPN Policies > DN Matching Rules** from the Policy selector. The DN Matching Rules page is displayed. For a description of the elements on this page, see [Table H-22 on page H-50](#).
- Step 2** Click **Create** in the upper pane to configure the priority and tunnel group mapping for your matching rules. The DN Rule page is displayed. For a description of the elements on this page, see [Table H-23 on page H-52](#).
- Step 3** Select a tunnel group from the list.
- Step 4** Enter the priority number for the matching rule. A lower number has higher priority.
- Step 5** Click **OK**. The DN Matching rule is displayed in the upper pane of the page.

- Step 6** Select the tunnel group mapping created in the upper pane to display the details in the lower pane.
- Step 7** Click **Create** in the lower pane to configure the DN Matching rule that must be satisfied in order for a remote client to connect to the device. The DN Rule page is displayed. For a description of the elements on this page, see [Table H-24 on page H-53](#).
- Step 8** Select the certificate field from the list.
- Step 9** Select the component of the rule you wish to configure.
- Step 10** Select the operator of the rule.
- Step 11** Enter the value for the matching rule.
- Step 12** Click **OK**. The DN Matching rule parameters are displayed in the lower pane of the page.
- Step 13** Click **Save** to save your changes to the server.



---

**Note** To publish your changes, click the **Submit** button on the toolbar.

---

## Managing Shared Remote Access VPN Policies in Policy View

In Policy view, you can view all shared policies for each policy type in a remote access VPN, modify individual policies, and apply the policies globally to multiple devices. You can also create shared policies that you can assign later to devices.

This procedure describes how to create or edit remote access VPN policies, and modify their assignments to devices, from Policy view.

### Related Topics

- [Working with Policies in Remote Access VPNs, page 11-3](#)
- [Managing Shared Policies in Policy View, page 7-39](#)

- 
- Step 1** Click the **Policy View** button on the toolbar.

- Step 2** Select the **Remote Access VPN** folder from the Policy selector. The folder opens, listing the types of IPsec policies that you can define for a remote access VPN. For more information, see [Policy View Selectors, page 7-41](#).
- Step 3** To view the shared policies defined for a policy type, select the policy type from the Policy Type selector. Any policies that are defined for the selected policy type are displayed in the Shared Policy selector in the lower pane.
- Step 4** To create a shared policy for a policy type:
- Right-click the policy type and select **New [policy type] Policy** from the shortcut menu. The Create a Policy dialog box opens.
  - Enter a name for the new policy and click **OK**. The new policy will appear in the Shared Policy selector for the selected policy type, displaying predefined definitions, which you can edit, if required.
- Step 5** To view or edit a policy's definitions, or do both:
- Select the policy in the Shared Policy selector. The **Details** tab in the work area of Policy view opens, displaying the definitions for the policy.
  - If required, modify the definitions for the policy. See [Working with Policies in Remote Access VPNs, page 11-3](#).
- Step 6** To view or edit a policy's assignments, or do both:
- Select the policy in the Shared Policy selector, and click the **Assignments** tab in the work area. For a description of the elements on this tab, see [Policy View—Assignments Tab, page D-29](#).
  - If required, modify the list of devices to which the policy is assigned. See [Modifying Policy Assignments in Policy View, page 7-44](#).
- Step 7** Click **Save** to save your changes to the server.



---

**Note** To publish your changes, click the **Submit** button on the toolbar.

---