



Scenario: IPsec Remote-Access VPN Configuration

This chapter describes how to use the security appliance to accept remote-access IPsec VPN connections. A remote-access VPN enables you to create secure connections, or tunnels, across the Internet, thus providing secure access to off-site users.

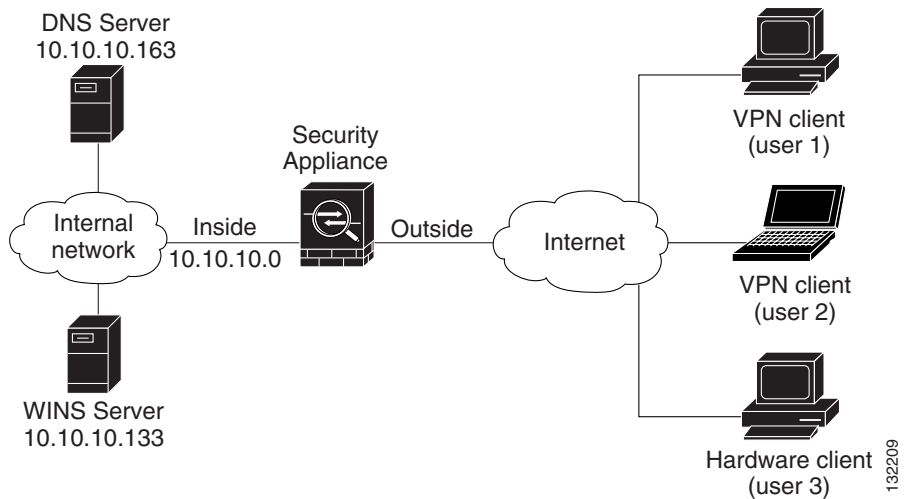
If you are implementing an Easy VPN solution, this chapter describes how to configure the Easy VPN server (sometimes called a headend device).

This chapter includes the following sections:

- [Example IPsec Remote-Access VPN Network Topology, page 3-1](#)
- [Implementing the IPsec Remote-Access VPN Scenario, page 3-2](#)
- [What to Do Next, page 3-18](#)

Example IPsec Remote-Access VPN Network Topology

[Figure 3-1](#) shows an security appliance configured to accept requests from and establish IPsec connections with VPN clients, such as a Cisco Easy VPN hardware client, over the Internet.

Figure 3-1 Network Layout for Remote Access VPN Scenario

Implementing the IPsec Remote-Access VPN Scenario

This section describes how to configure the security appliance to accept IPsec VPN connections from remote clients and devices. If you are implementing an Easy VPN solution, this section describes how to configure an Easy VPN server (also known as a headend device).

Values for example configuration settings are taken from the remote-access scenario illustrated in [Figure 3-1](#).

This section includes the following topics:

- [Information to Have Available, page 3-3](#)
- [Starting ASDM, page 3-3](#)
- [Configuring the PIX 515E for an IPsec Remote-Access VPN, page 3-5](#)
- [Selecting VPN Client Types, page 3-6](#)

- [Specifying the VPN Tunnel Group Name and Authentication Method, page 3-7](#)
- [Specifying a User Authentication Method, page 3-8](#)
- [\(Optional\) Configuring User Accounts, page 3-10](#)
- [Configuring Address Pools, page 3-11](#)
- [Configuring Client Attributes, page 3-12](#)
- [Configuring the IKE Policy, page 3-13](#)
- [Configuring IPsec Encryption and Authentication Parameters, page 3-15](#)
- [Specifying Address Translation Exception and Split Tunneling, page 3-16](#)
- [Verifying the Remote-Access VPN Configuration, page 3-17](#)

Information to Have Available

Before you begin configuring the security appliance to accept remote access IPsec VPN connections, make sure that you have the following information available:

- Range of IP addresses to be used in an IP pool. These addresses are assigned to remote VPN clients as they are successfully connected.
- List of users to be used in creating a local authentication database, unless you are using a AAA server for authentication.
- Networking information to be used by remote clients when connecting to the VPN, including:
 - IP addresses for the primary and secondary DNS servers
 - IP addresses for the primary and secondary WINS servers
 - Default domain name
 - List of IP addresses for local hosts, groups, and networks that should be made accessible to authenticated remote clients

Starting ASDM

To run ASDM in a web browser, enter the factory default IP address in the address field: **<https://192.168.1.1/admin/>**.

Implementing the IPsec Remote-Access VPN Scenario



Note

Remember to add the “s” in “**https**” or the connection fails. HTTPS (HTTP over SSL) provides a secure connection between your browser and the security appliance.

The Main ASDM window appears.

The screenshot displays the Cisco ASDM 5.2 Main window. The top menu bar includes File, Options, Tools, Wizards, and Help. Below the menu is a toolbar with icons for Home, Configuration, Monitoring, Back, Forward, Packet Tracer, Refresh, Save, and Help. The main content area is divided into several sections:

- Device Information:**
 - General tab selected.
 - Host Name: SecurityAppliance1
 - ASA Version: 7.2(0)72
 - ASDM Version: 5.2(0)30
 - Firewall Mode: Routed
 - Total Flash: 64 MB
 - Device Uptime: 1d 1h 48m 24s
 - Device Type: ASA/PIX
 - Context Mode: Single
 - Total Memory: 512 MB
- VPN Status:**
 - IKE Tunnels: 0
 - WebVPN Tunnels: 0
 - SVC Tunnels: 0
- System Resources Status:**
 - CPU:** CPU Usage (percent) graph showing 0% usage.
 - Memory:** Memory Usage (MB) graph showing 68MB usage.
- Interface Status:**

Interface	IP Address/Mask	Line	Link	Kbps
dmz	10.30.30.1/24	down	down	0
inside	10.10.10.1/24	down	down	0
management	172.23.62.22/24	up	up	5
outside	209.165.200.225/24	down	down	0
- Traffic Status:**
 - Connections Per Second Usage graph.
 - UDP: 0, TCP: 0, Total: 0.
 - Outside Interface Traffic Usage (Kbps) graph.
 - Input Kbps: 0, Output Kbps: 0.

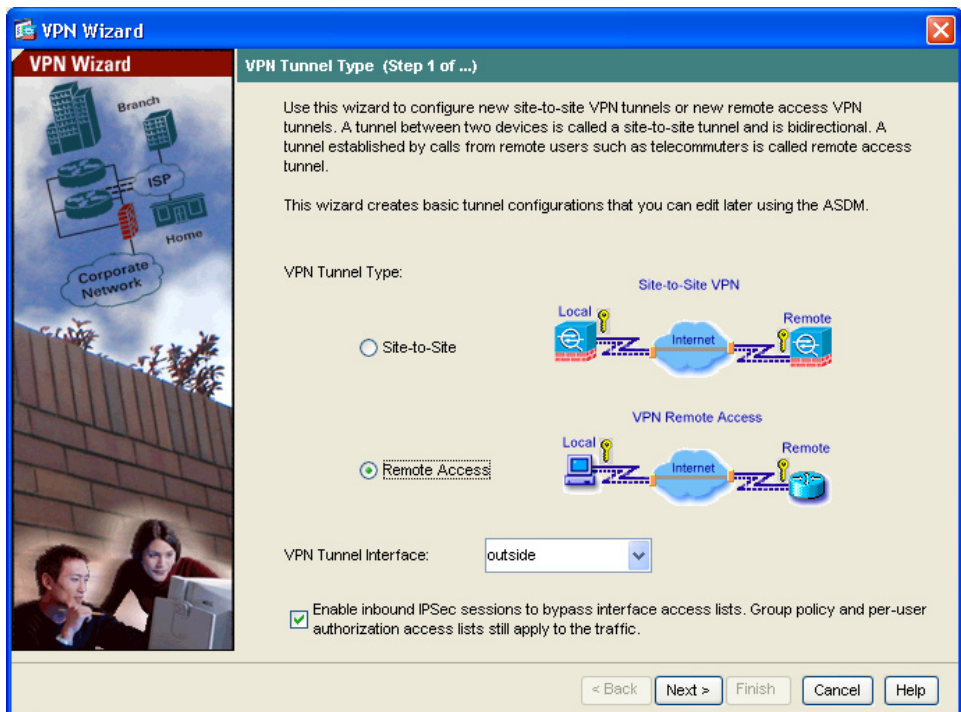
The status bar at the bottom shows: Device configuration loaded successfully. | <admin> | 15 | 5/10/06 1:08:18 AM PDT.

153891

Configuring the PIX 515E for an IPsec Remote-Access VPN

To begin the process for configuring a remote-access VPN, perform the following steps:

- Step 1** In the main ASDM window, choose **VPN Wizard** from the Wizards drop-down menu. The VPN Wizard Step 1 screen appears.

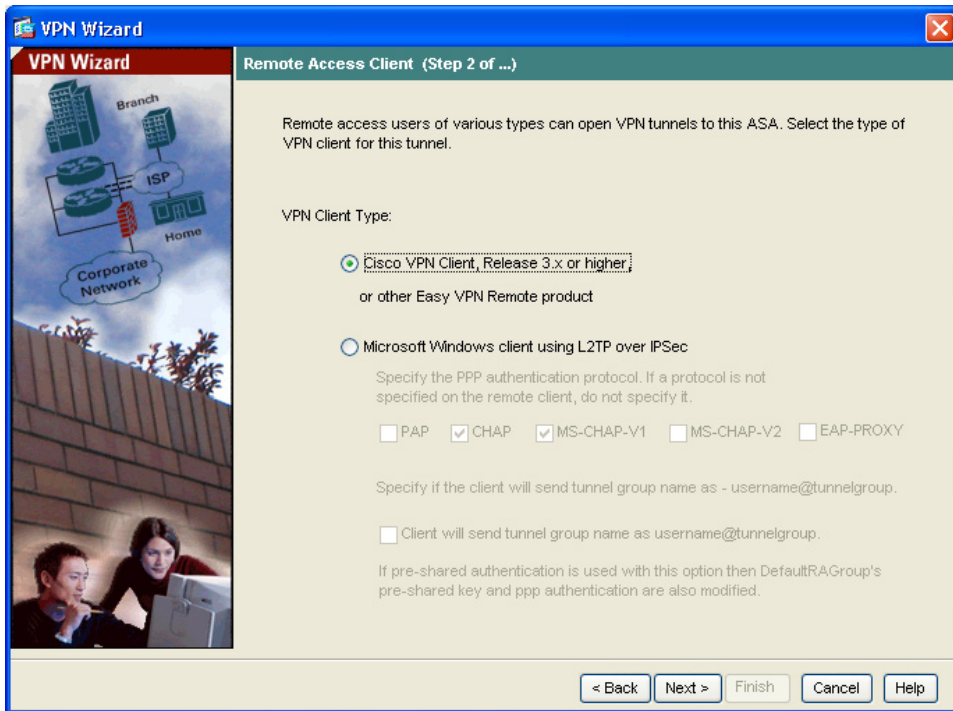


- Step 2** In Step 1 of the VPN Wizard, perform the following steps:
- Click the **Remote Access VPN** radio button.
 - From the drop-down list, choose **Outside** as the enabled interface for the incoming VPN tunnels.
 - Click **Next** to continue.

Selecting VPN Client Types

In Step 2 of the VPN Wizard, perform the following steps:

- Step 1** Specify the type of VPN client that will enable remote users to connect to this security appliance. For this scenario, click the **Cisco VPN Client** radio button. You can also use any other Cisco Easy VPN remote product.



- Step 2** Click **Next** to continue.

Specifying the VPN Tunnel Group Name and Authentication Method

In Step 3 of the VPN Wizard, perform the following steps:

Step 1 Specify the type of authentication that you want to use by performing one of the following steps:

- To use a static preshared key for authentication, click the **Pre-Shared Key** radio button and enter a preshared key (for example, “Cisco”). This key is used for IPsec negotiations between the security appliances.
- To use digital certificates for authentication, click the **Certificate** radio button, choose the Certificate Signing Algorithm from the drop-down list, and then choose a preconfigured trustpoint name from the drop-down list.

If you want to use digital certificates for authentication but have not yet configured a trustpoint name, you can continue with the Wizard by using one of the other two options. You can revise the authentication configuration later using the standard ASDM screens.

- Click the **Challenge/Response Authentication (CRACK)** radio button to use that method of authentication.

Implementing the IPsec Remote-Access VPN Scenario

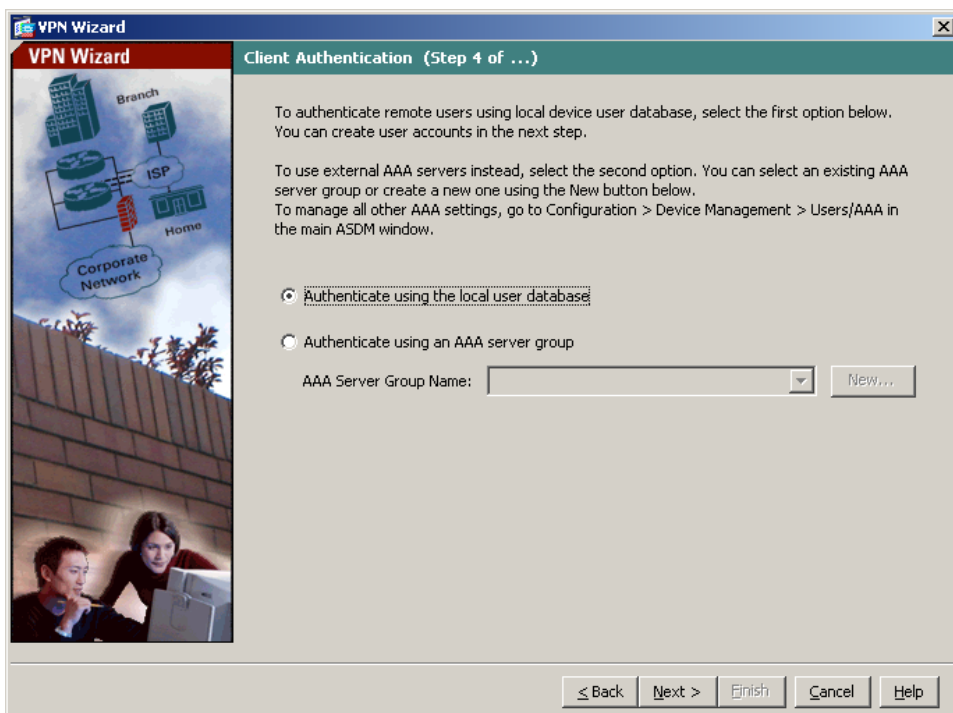
- Step 2** Enter a Tunnel Group Name (such as “Cisco”) for the set of users that use common connection parameters and client attributes to connect to this security appliance.
- Step 3** Click **Next** to continue.

Specifying a User Authentication Method

Users can be authenticated either by a local authentication database or by using external authentication, authorization, and accounting (AAA) servers (RADIUS, TACACS+, SDI, NT, Kerberos, and LDAP).

In Step 4 of the VPN Wizard, perform the following steps:

- Step 1** If you want to authenticate users by creating a user database on the security appliance, click the **Authenticate Using the Local User Database** radio button.
- Step 2** If you want to authenticate users with an external AAA server group:
- Click the **Authenticate Using an AAA Server Group** radio button.
 - Choose a preconfigured server group from the drop-down list, or click **New** to add a new server group.



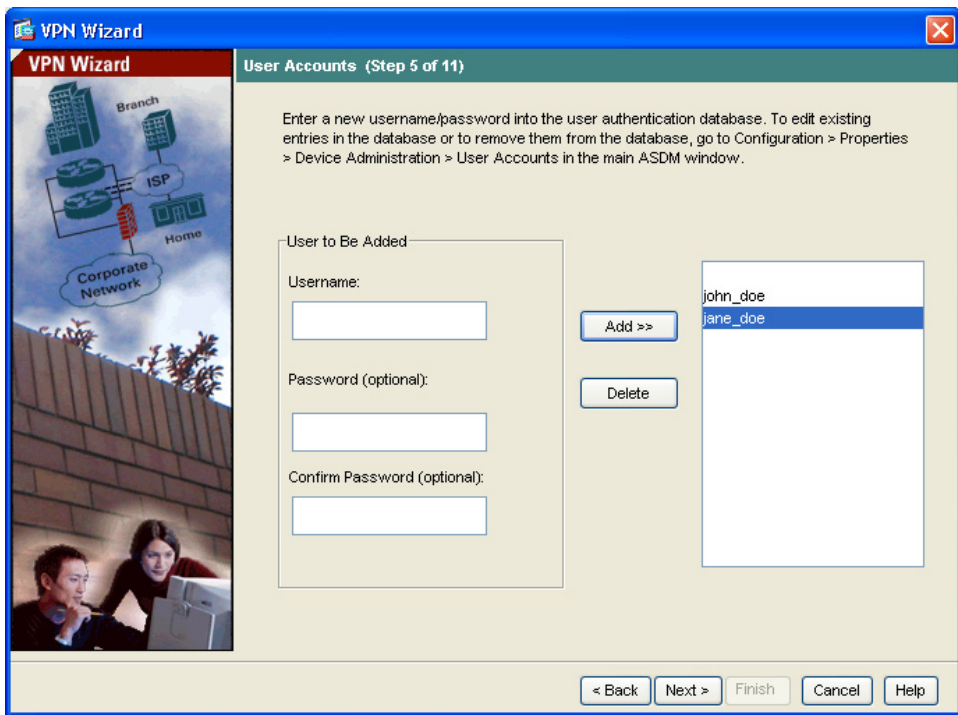
- Step 3** Click **Next** to continue.

(Optional) Configuring User Accounts

If you have chosen to authenticate users with the local user database, you can create new user accounts here. You can also add users later using the ASDM configuration interface.

In Step 5 of the VPN Wizard, perform the following steps:

- Step 1** To add a new user, enter a username and password, and then click **Add**.



The screenshot shows the 'VPN Wizard' window, specifically the 'User Accounts (Step 5 of 11)' tab. The window has a blue title bar and a red close button. On the left, there is a 'VPN Wizard' sidebar with a diagram showing a 'Corporate Network' connected to an 'ISP' and a 'Home' network. The main area is titled 'User Accounts (Step 5 of 11)' and contains the following text: 'Enter a new username/password into the user authentication database. To edit existing entries in the database or to remove them from the database, go to Configuration > Properties > Device Administration > User Accounts in the main ASDM window.'

Below the text, there is a section titled 'User to Be Added' with three input fields: 'Username:', 'Password (optional):', and 'Confirm Password (optional):'. To the right of these fields are two buttons: 'Add >>' and 'Delete'. Further right is a list box containing two entries: 'john_doe' and 'jane_doe', with 'jane_doe' selected. At the bottom of the window are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. A vertical text '153914' is visible on the right side of the window.

- Step 2** When you have finished adding new users, click **Next** to continue.

Configuring Address Pools

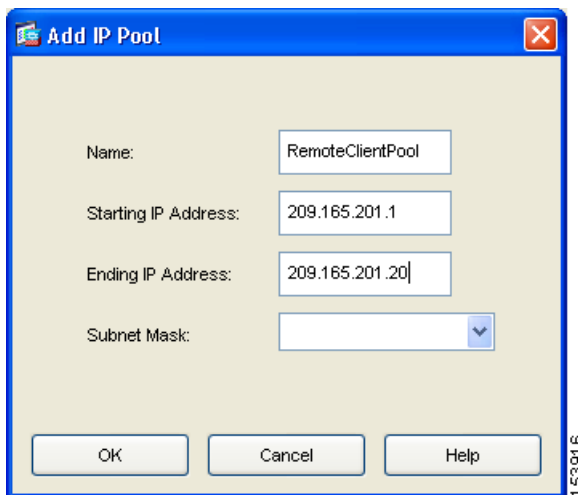
For remote clients to gain access to your network, you must configure a pool of IP addresses that can be assigned to remote VPN clients as they are successfully connected. In this scenario, the pool is configured to use the range of IP addresses 209.165.201.1–209.166.201.20.

In Step 6 of the VPN Wizard, perform the following steps:

Step 1 Enter a pool name or choose a preconfigured pool from the drop-down list.

Alternatively, click **New** to create a new address pool.

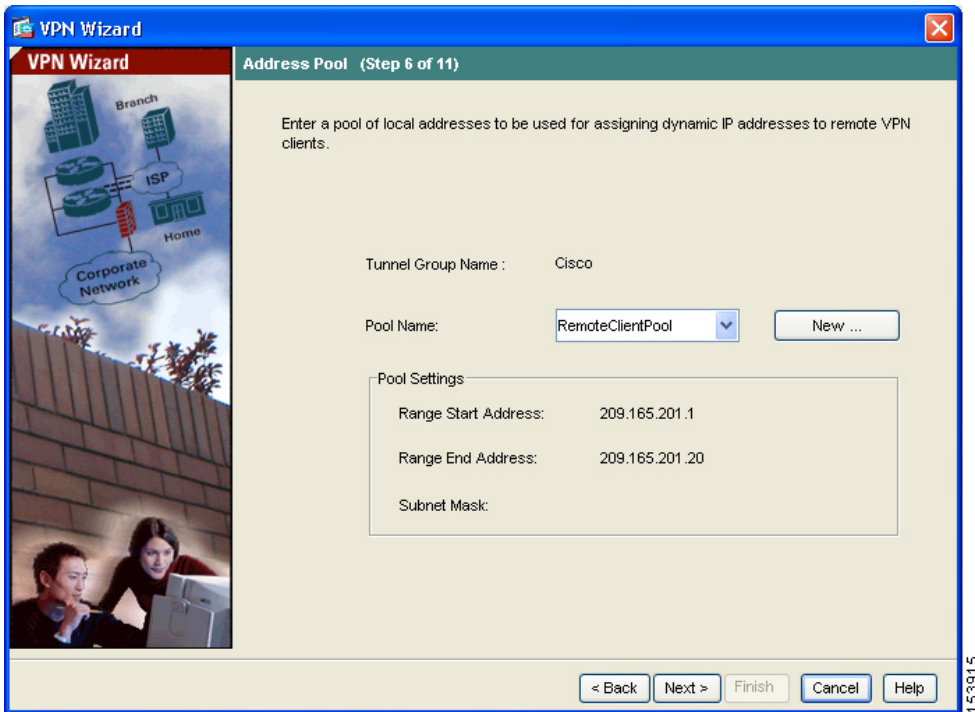
The Add IP Pool dialog box appears.



Step 2 In the Add IP Pool dialog box:

- a. Enter the Starting IP address and Ending IP address of the range.
- b. (Optional) Enter the Netmask for the range of IP addresses.
- c. Click **OK** to return to Step 6 of the VPN Wizard.

Implementing the IPsec Remote-Access VPN Scenario



Step 3 Click **Next** to continue.

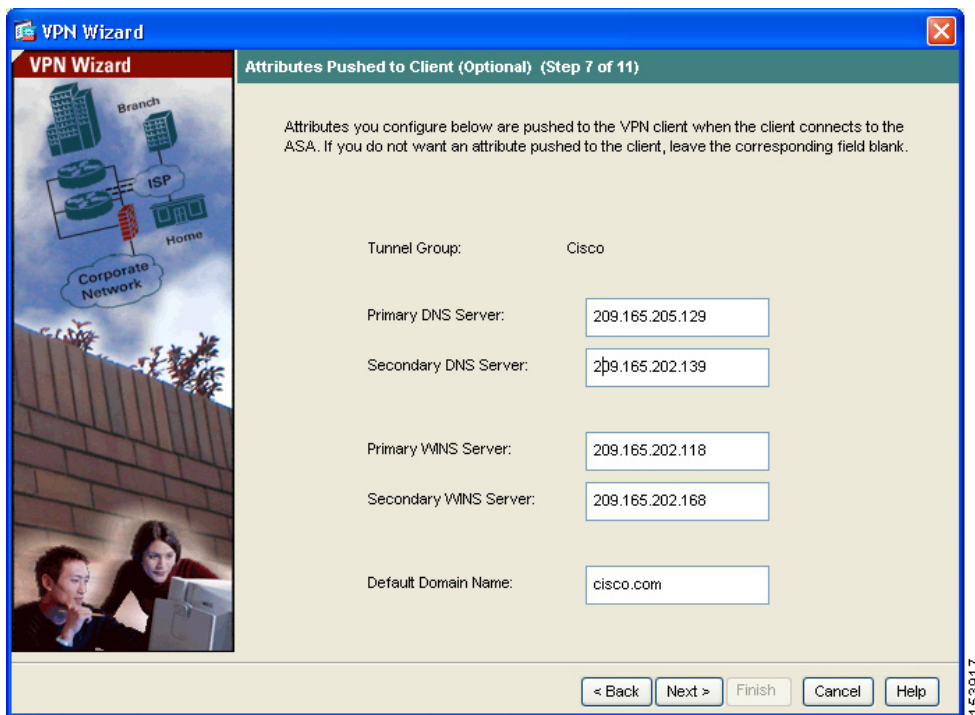
Configuring Client Attributes

To access your network, each remote access client needs basic network configuration information, such as which DNS and WINS servers to use and the default domain name. Rather than configuring each remote client individually, you can provide the client information to ASDM. The security appliance pushes this information to the remote client or Easy VPN hardware client when a connection is established.

Ensure that you specify the correct values, or remote clients will not be able to use DNS names for resolution or use Windows networking.

In Step 7 of the VPN Wizard, perform the following steps:

- Step 1** Enter the network configuration information to be pushed to remote clients.



The screenshot shows the 'VPN Wizard' window, specifically the 'Attributes Pushed to Client (Optional) (Step 7 of 11)' screen. The window has a blue title bar and a red close button. On the left, there is a diagram showing a 'Corporate Network' connected to an 'ISP' and then to a 'Branch' and 'Home' network. Below the diagram is a photo of two people working on a laptop. The main area is a light beige background with the text: 'Attributes you configure below are pushed to the VPN client when the client connects to the ASA. If you do not want an attribute pushed to the client, leave the corresponding field blank.' Below this text are several fields for configuration:

Attribute	Value
Tunnel Group:	Cisco
Primary DNS Server:	209.165.205.129
Secondary DNS Server:	209.165.202.139
Primary WINS Server:	209.165.202.118
Secondary WINS Server:	209.165.202.168
Default Domain Name:	cisco.com

At the bottom of the window are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. The 'Next >' button is highlighted. On the right side of the window, there is a vertical text label '153917'.

- Step 2** Click **Next** to continue.

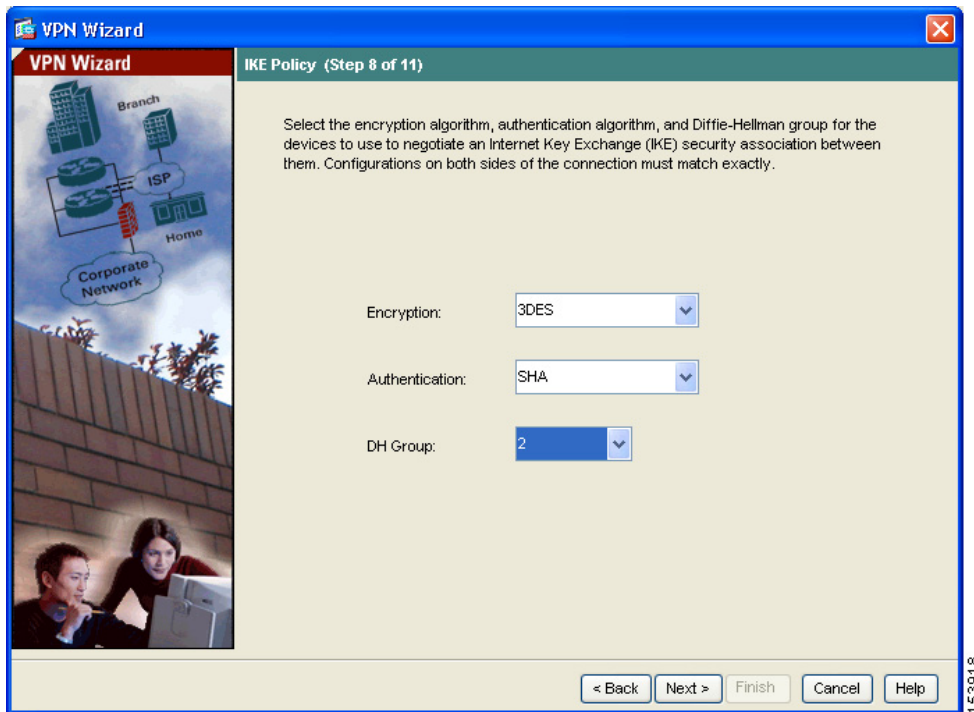
Configuring the IKE Policy

IKE is a negotiation protocol that includes an encryption method to protect data and ensure privacy; it is also an authentication method to ensure the identity of the peers. In most cases, the ASDM default values are sufficient to establish secure VPN tunnels.

Implementing the IPsec Remote-Access VPN Scenario

To specify the IKE policy in Step 8 of the VPN Wizard, perform the following steps:

- Step 1** Click the Encryption (DES/3DES/AES), authentication algorithms (MD5/SHA), and the Diffie-Hellman group (1/2/5/7) used by the security appliance during an IKE security association.

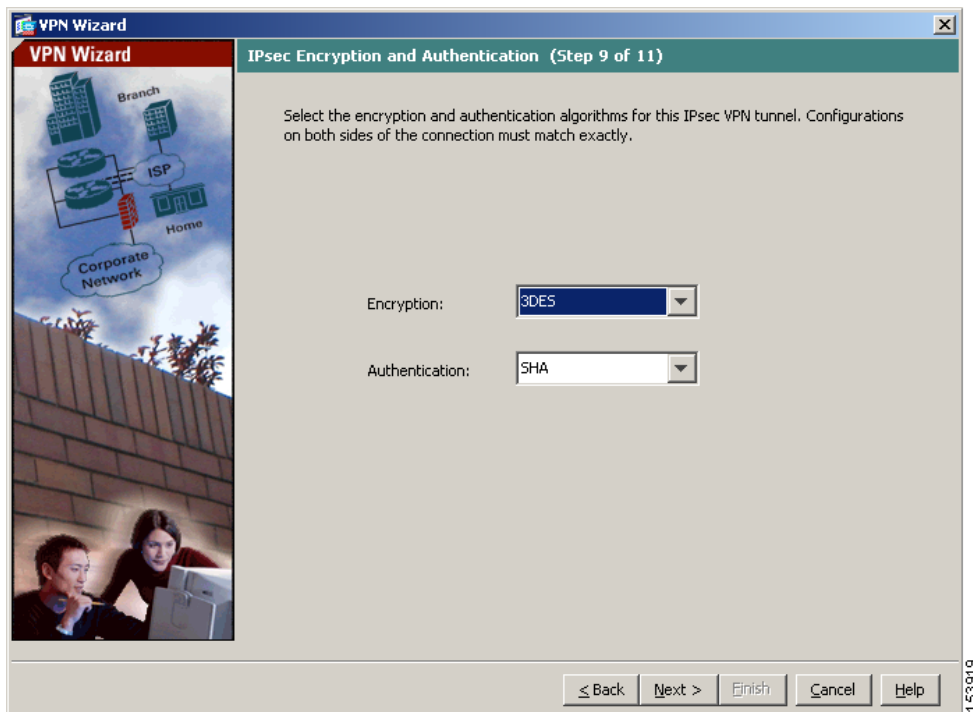


- Step 2** Click **Next** to continue.

Configuring IPsec Encryption and Authentication Parameters

In Step 9 of the VPN Wizard, perform the following steps:

- Step 1** Click the Encryption algorithm (DES/3DES/AES) and authentication algorithm (MD5/SHA).



- Step 2** Click **Next** to continue.

Specifying Address Translation Exception and Split Tunneling

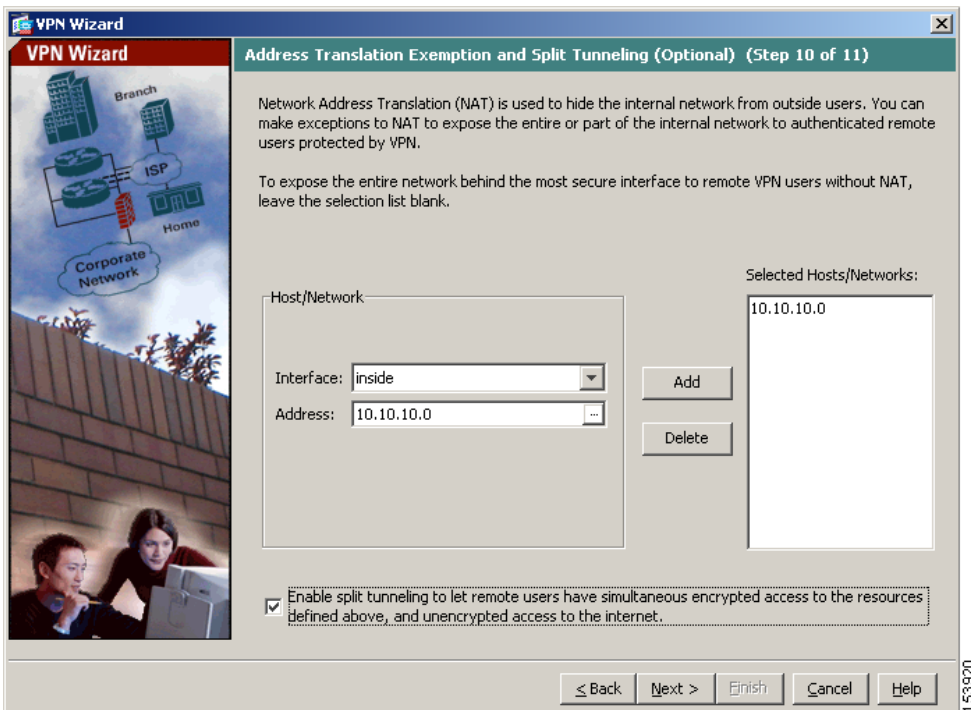
Split tunneling lets a remote-access IPsec client conditionally direct packets over an IPsec tunnel in encrypted form or to a network interface in clear text form.

The security appliance uses Network Address Translation (NAT) to prevent internal IP addresses from being exposed externally. You can make exceptions to this network protection by identifying local hosts and networks that should be made accessible to authenticated remote users. (In this scenario, the entire inside network 10.10.10.0 is exposed to all remote clients.)

In Step 10 of the VPN Wizard, perform the following steps:

Step 1 Specify hosts, groups, and networks that should be in the list of internal resources made accessible to authenticated remote users.

To add or remove hosts, groups, and networks dynamically from the Selected Hosts/Networks pane, click **Add** or **Delete**, respectively.



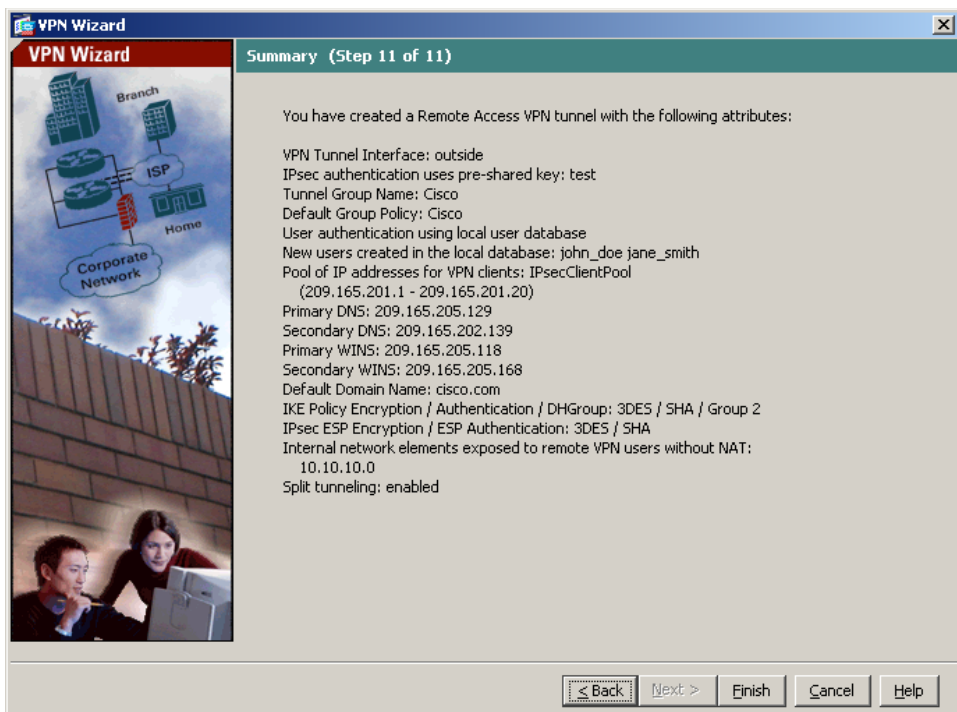
**Note**

Enable split tunneling by checking the **Enable Split Tunneling** check box at the bottom of the screen. Split tunneling allows traffic outside the configured networks to be sent out directly to the Internet instead of over the encrypted VPN tunnel.

Step 2 Click **Next** to continue.

Verifying the Remote-Access VPN Configuration

In Step 11 of the VPN Wizard, review the configuration attributes for the VPN tunnel you just created. The displayed configuration should be similar to the following:



153921

If you are satisfied with the configuration, click **Finish** to apply the changes to the security appliance.

If you want the configuration changes to be saved to the startup configuration so that they are applied the next time the device starts, from the File menu, click **Save**. Alternatively, ASDM prompts you to save the configuration changes permanently when you exit ASDM.

If you do not save the configuration changes, the old configuration takes effect the next time the device starts.

What to Do Next

If you are deploying the security appliance solely in a remote-access VPN environment, you have completed the initial configuration. In addition, you may want to consider performing some of the following steps:

To Do This ...	See ...
Refine configuration and configure optional and advanced features	<i>Cisco Security Appliance Command Line Configuration Guide</i>
Learn about daily operations	<i>Cisco Security Appliance Command Reference</i> <i>Cisco Security Appliance Logging Configuration and System Log Messages</i>

You can configure the security appliance for more than one application. The following sections provide configuration procedures for other common applications of the security appliance.

To Do This ...	See ...
Configure the security appliance to protect a Web server in a DMZ	Chapter 2, “Scenario: DMZ Configuration”
Configure a site-to-site VPN	Chapter 4, “Scenario: Site-to-Site VPN Configuration”

