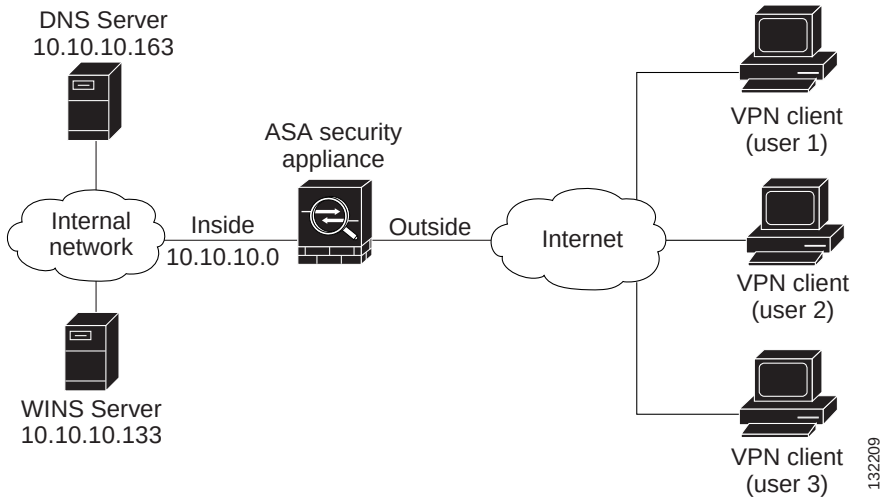
Scenario: Remote-Access VPN Configuration

A remote-access Virtual Private Network (VPN) enables you to provide secure access to off-site users. ASDM enables you to configure the adaptive security appliance to create secure connections, or tunnels, across the Internet.

Figure 7-1 shows an adaptive security appliance configured to accept requests from and establish secure connections with VPN clients over the Internet.

Figure 7-1 Network Layout for Remote Access VPN Scenario



Implementing the Remote-Access Scenario

The following sections provide instructions for configuring the adaptive security appliance in a remote-access deployment, using example parameters from the remote-access scenario illustrated in Figure 7-1.

Information to Have Available

- Range of IP addresses to be used for an IP pool
- List of users to be used in creating a local authentication database, unless you will be using a AAA server for authentication
- Networking information to be used by remote clients, 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

Configuring the Remote-Access VPN

The ASDM VPN Wizard enables you to configure the adaptive security appliance as a remote-access VPN headend device in a series of simple steps:

1. Configure the Adaptive Security Appliance for Remote-Access VPN.
2. Select VPN Clients.
3. Specify the VPN Tunnel Group Name and Authentication Method.
4. Specify a User Authentication Method.
5. Configure User Accounts (optional).
6. Configure Address Pools.
7. Configure Client Attributes.
8. Configure the IKE Policy.
9. Configure IPSec Encryption and Authentication parameters.

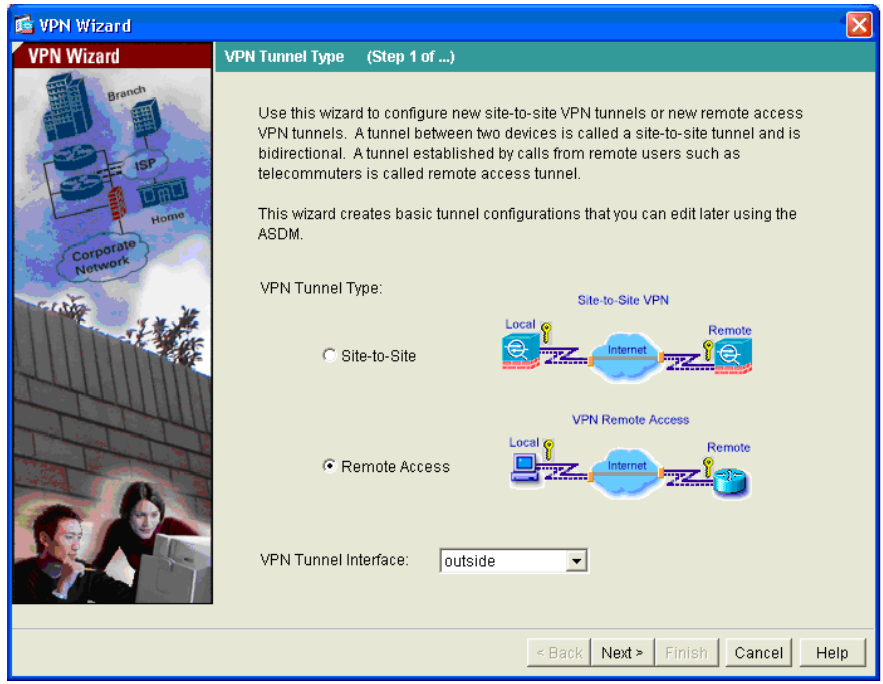
10. Specify Address Translation Exception and Split Tunneling.
11. Verify the Remote-Access VPN Configuration.

Configure the Adaptive Security Appliance for Remote-Access VPN

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

Step 1 Launch ASDM by entering the factory default IP address in the address field of a web browser: **https://192.168.1.1/admin/**.

Step 2 In the main ASDM window, click **VPN Wizard** option from the Wizards drop-down list. The VPN Wizard Step 1 window appears.



Step 3 In Step 1 of the VPN Wizard, perform the following steps:

a. Click the **Remote Access VPN** option.

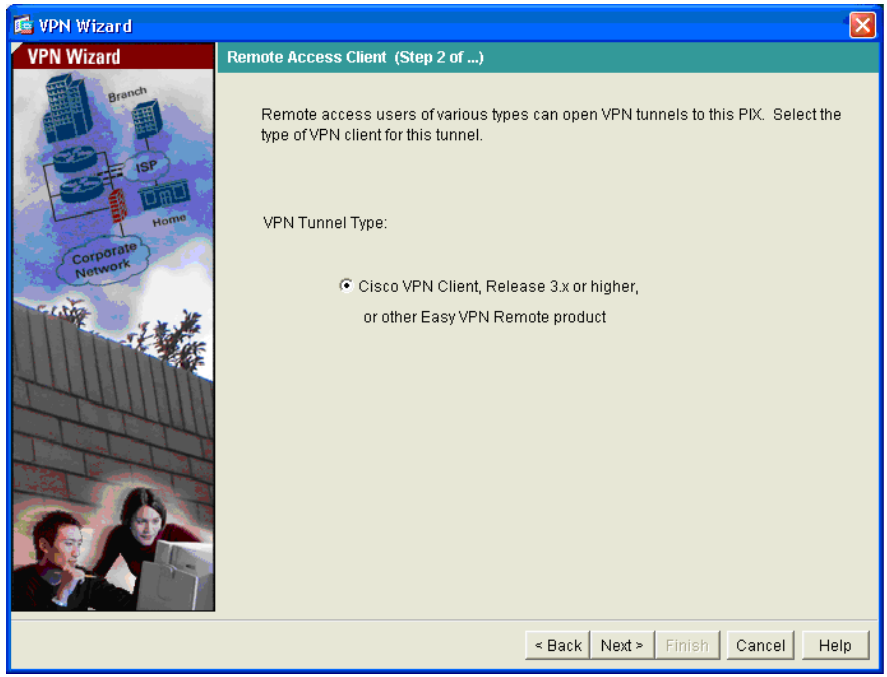
b. From the drop-down list, click **outside** as the enabled interface for the incoming VPN tunnels.

c. Click **Next** to continue.

Select VPN Clients

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

Step 1 Click the radio button to allow remote access users to connect to the adaptive security appliance using either a Cisco VPN client or any other Easy VPN remote products.



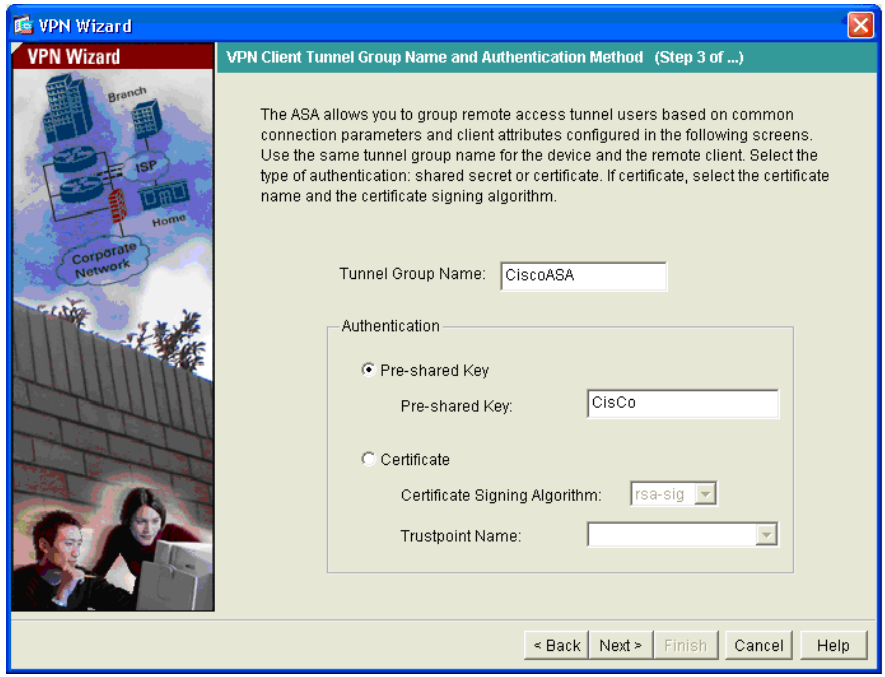
Note Although there is currently only one selection on this screen, it is set up so that other tunnel types can be enabled easily as they become available.

Step 2 Click **Next** to continue.

Specify the VPN Tunnel Group Name and Authentication Method

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

Step 1 Enter a Tunnel Group Name (such as "CiscoASA") for the set of users that use common connection parameters and client attributes.



Step 2 Specify the type of authentication that you want to use by performing one of the following steps:

- To use static preshared keys for authentication, click **Pre-Shared Key**, and enter a key (such as "CisCo").
- To use digital certificates for authentication, click **Certificate**, click the Certificate Signing Algorithm (rsa-sig/dsa-sig) from the drop-down list, and then click a pre-configured trustpoint name from the drop-down list.

Step 3 Click **Next** to continue.

Specify a User Authentication Method

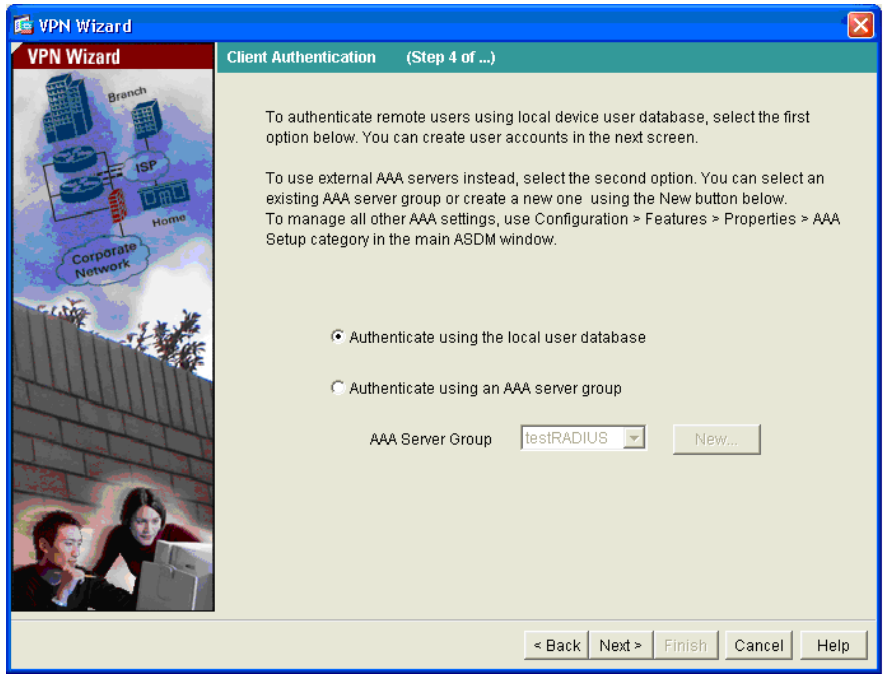
Users can be authenticated either by a local authentication database or by using external authentication, authorization, and accounting (AAA) servers (RADIUS, TACACS+, SDI, NT, and Crabbers).

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

Step 1 Click the appropriate radio button to specify the type of user authentication that you want to use:

- A local authentication database
- An external AAA server group

Step 2 Click a preconfigured server group from the drop-down list, or click **New** to add a new server group.

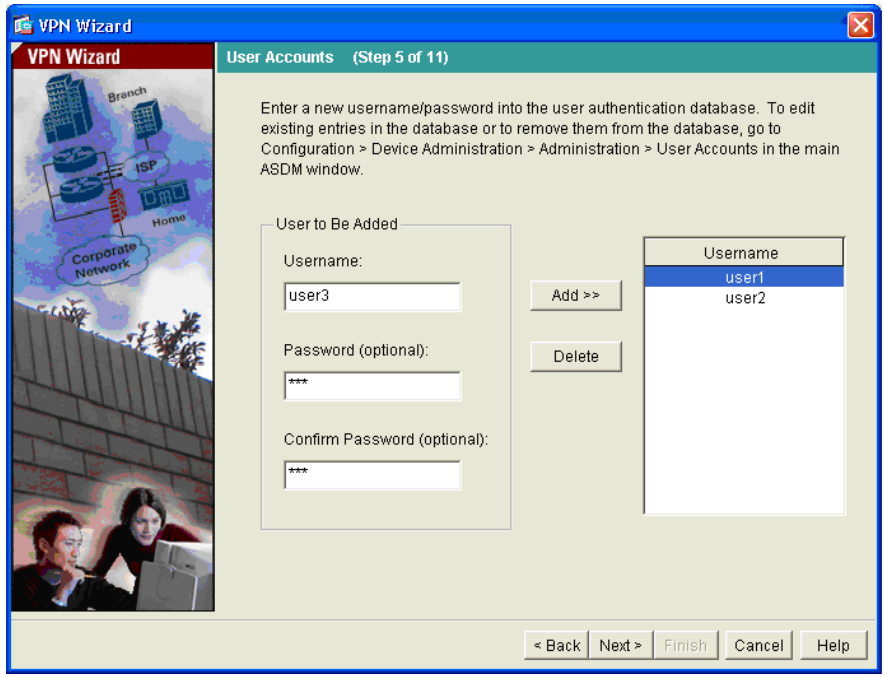


Step 3 Click **Next** to continue.

Configure User Accounts (optional)

If you have chosen to authenticate users with the local user database, create new user accounts. In Step 5 of the VPN Wizard, perform the following steps:

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



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

Configure 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 to 209.166.201.20.

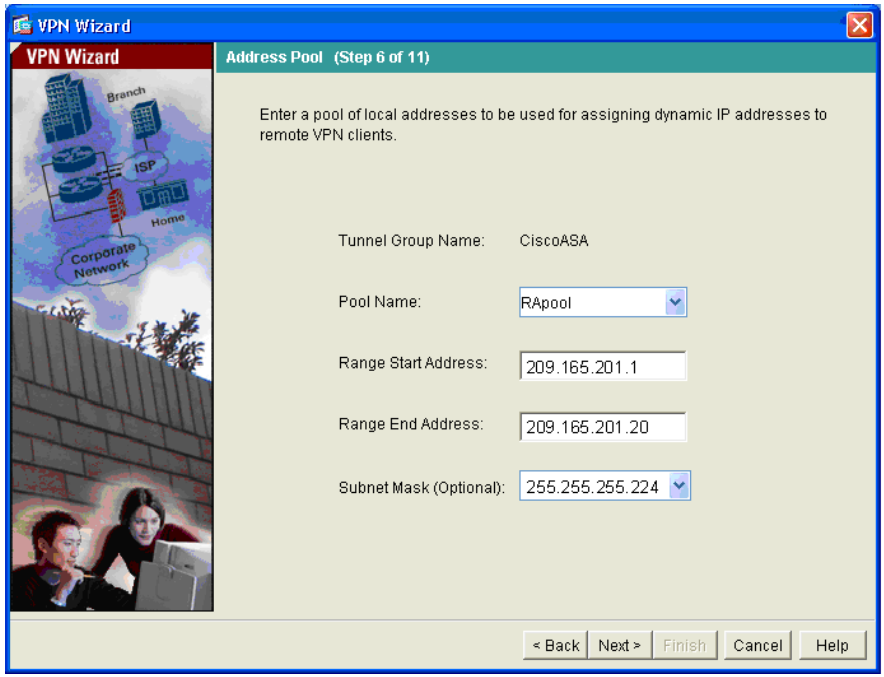
In Step 6 of the VPN Wizard, perform the following steps:

Step 1 From the drop-down list, enter a pool name or click a preconfigured pool.

Step 2 Enter the start of the range of IP addresses to be used in the pool.

Step 3 Enter the end of the range of IP addresses to be used in the pool.

Step 4 From the drop-down list, enter the subnet mask or click a preconfigured value.



Step 5 Click **Next** to continue.

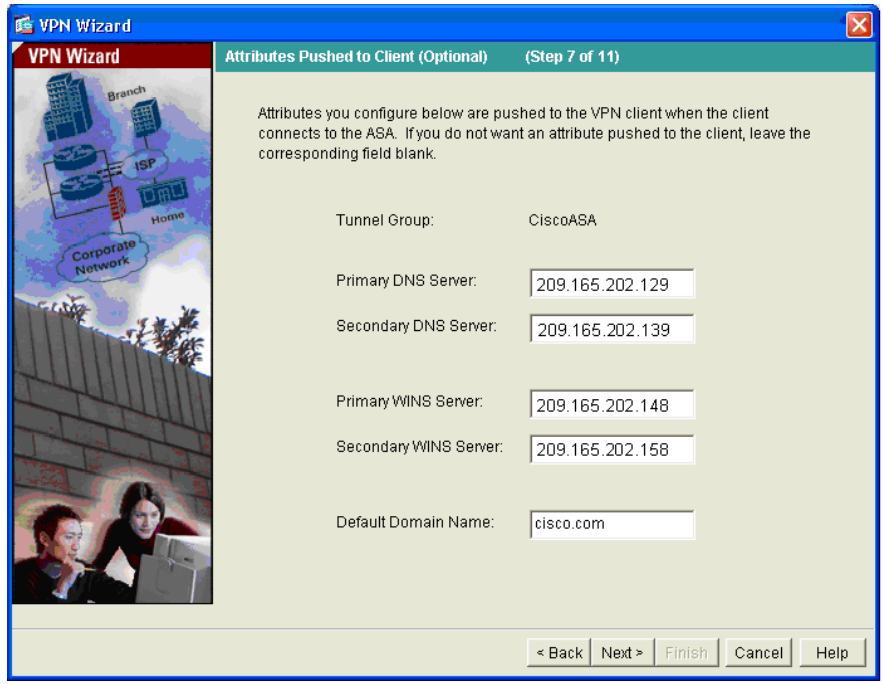
Configure Client Attributes

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 adaptive security appliance pushes this information to the remote 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 used by remote clients.



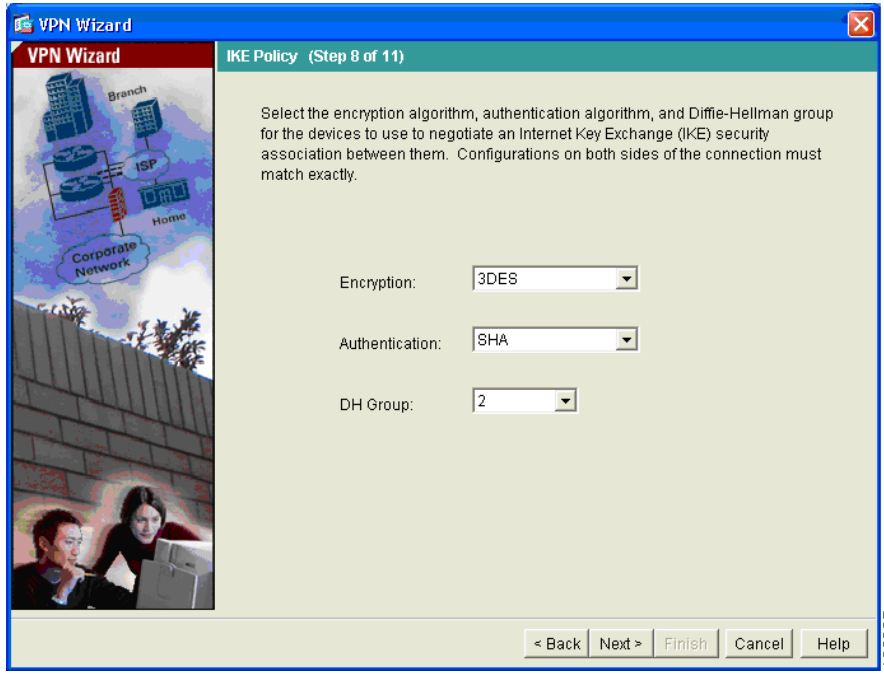
Step 2 Click **Next** to continue.

Configure 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.

To specify the IKE policy, 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 adaptive security appliance during an IKE security association.

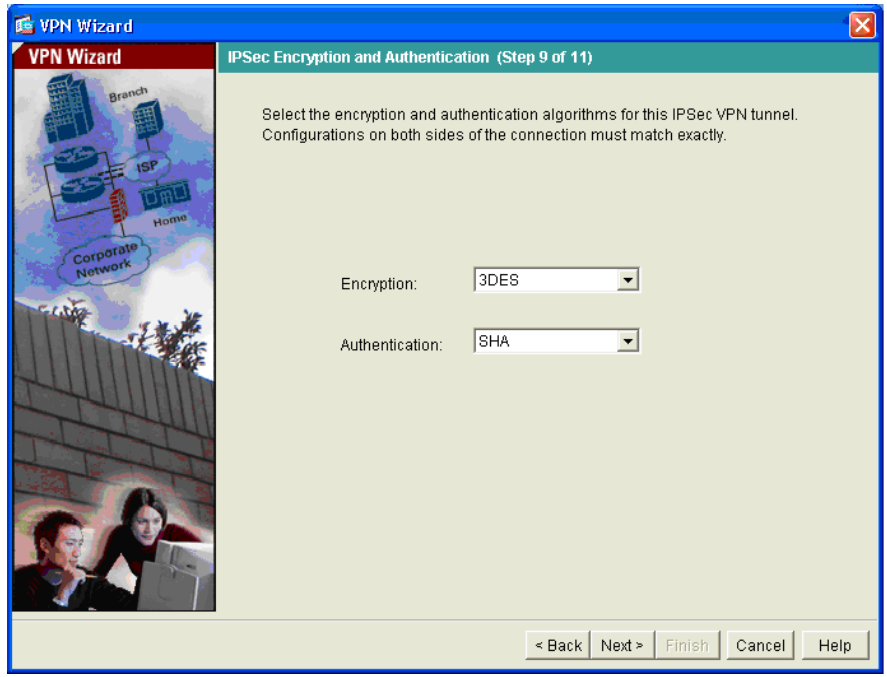


Step 2 Click **Next** to continue.

Configure 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).



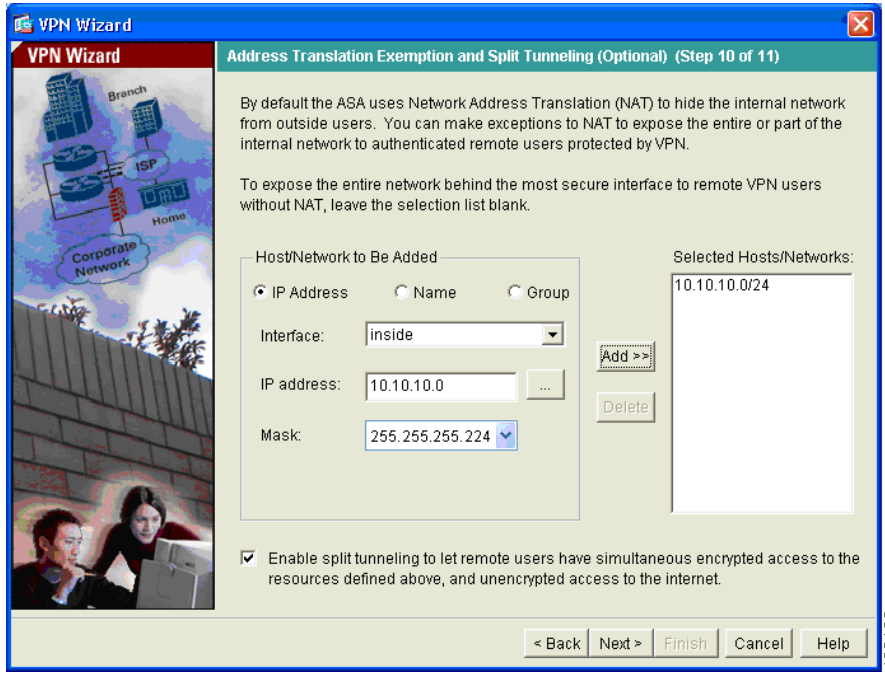
Step 2 Click **Next** to continue.

Specify Address Translation Exception and Split Tunneling

The adaptive 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 exposed to authenticated remote users. Specify the resources to be exposed by host or network IP address, by name, or by group. (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 panel, click **Add** or **Delete**, as appropriate.

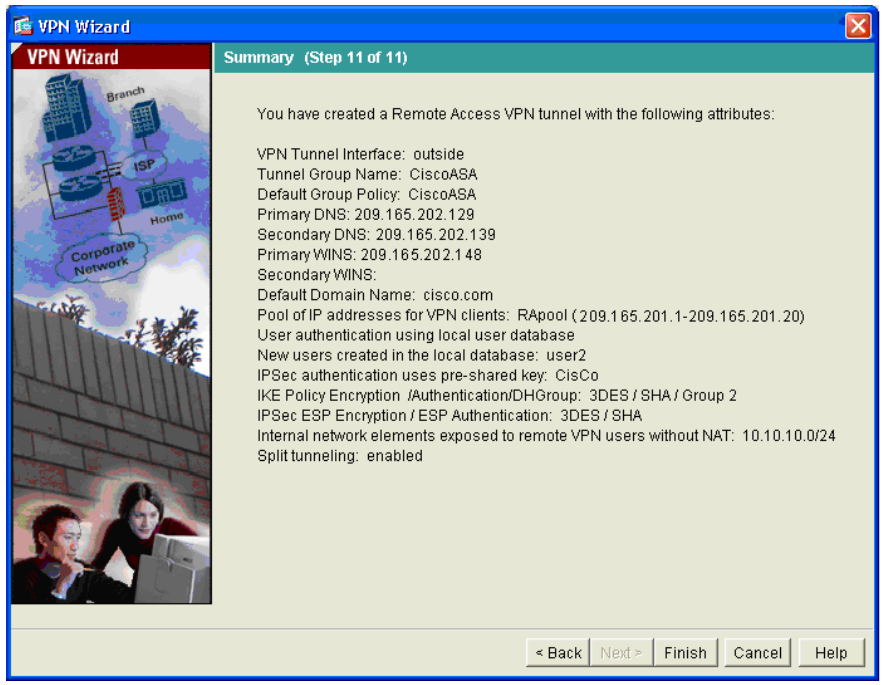


Note Enable split tunneling by clicking the radio button at the bottom of the screen. Split tunneling allows traffic outside the configured networks to be sent out directly to the Internet instead of over the encrypted VPN tunnel.

Step 2 When you have finished specifying resources to expose to remote clients, click **Next** to continue.

Verify the Remote-Access VPN Configuration

Review the configuration attributes for the VPN tunnel you just created. The displayed configuration should be similar to the following:



If you are satisfied with the configuration, click Finish to complete the Wizard and apply the configuration changes to the adaptive security appliance.

What to Do Next

If you are deploying the adaptive 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	*Cisco Security Appliance Command Line Configuration Guide*
Learn about daily operations	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*
Review hardware maintenance and troubleshooting information	*Cisco ASA 5500 Series Hardware Installation Guide*

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

To Do This ...	See ...
Configure the adaptive security appliance to protect a Web server in a DMZ	Chapter 6, “Scenario: DMZ Configuration”
Configure a site-to-site VPN	Chapter 8, “Scenario: Site-to-Site VPN Configuration”