Table of Contents

ASA as a Remote VPN Server using ASDM Configuration Example

Document ID: 68795

Introduction

This document describes how to use the Cisco Adaptive Security Device Manager (ASDM) to configure the Cisco 5500 Series Adaptive Security Appliance (ASA) to act as a remote VPN server. The ASDM delivers world−class security management and monitoring through an intuitive, easy−to−use Web−based management interface. Once the Cisco ASA configuration is complete, it can be verified using the Cisco VPN Client.

Prerequisites

Requirements

This document assumes that the ASA is fully operational and configured to allow the Cisco ASDM to make configuration changes.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Adaptive Security Appliance Software Version 7.0(4)
- Device Manager Version 5.0(4)
- Cisco VPN Client Version 4.0.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This configuration can also be used with Cisco PIX Security Appliance Version 7.x.

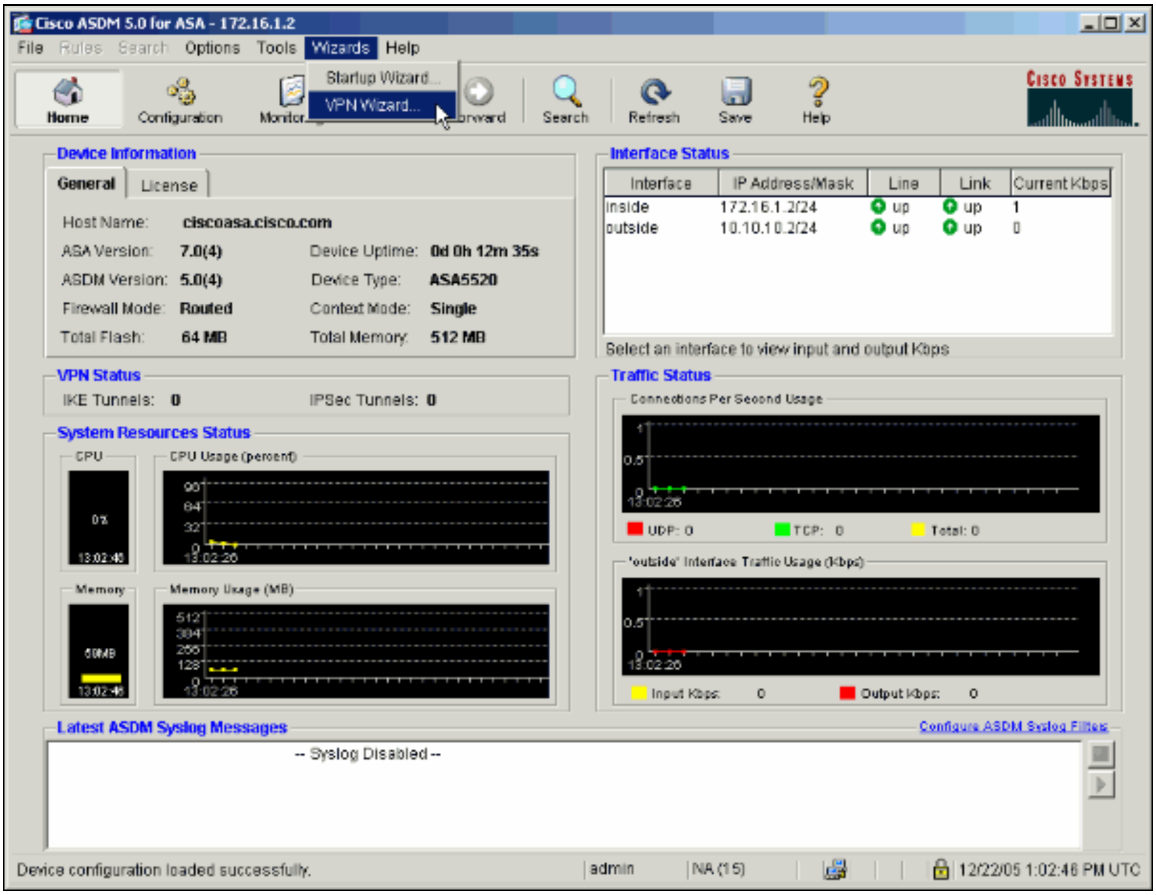
Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure the Cisco ASA as a Remote VPN Server

Complete these steps to configure the Cisco ASA as a remote VPN server using ASDM.

1. Select **Wizards > VPN Wizard** from the Home window.



Host Name: ciscoasa.cisco.com
ASA Version: 7.0(4) Device Uptime: 0d 0h 12m 35s
ASDM Version: 5.0(4) Device Type: ASA5520
Firewall Mode: Routed Context Mode: Single
Total Flash: 64 MB Total Memory: 512 MB

Interface	IP Address/Mask	Line	Link	Current Kbps
inside	172.16.1.2/24	up	up	1
outside	10.10.10.2/24	up	up	0

Select an interface to view input and output Kbps

IKE Tunnels: 0 IPSec Tunnels: 0

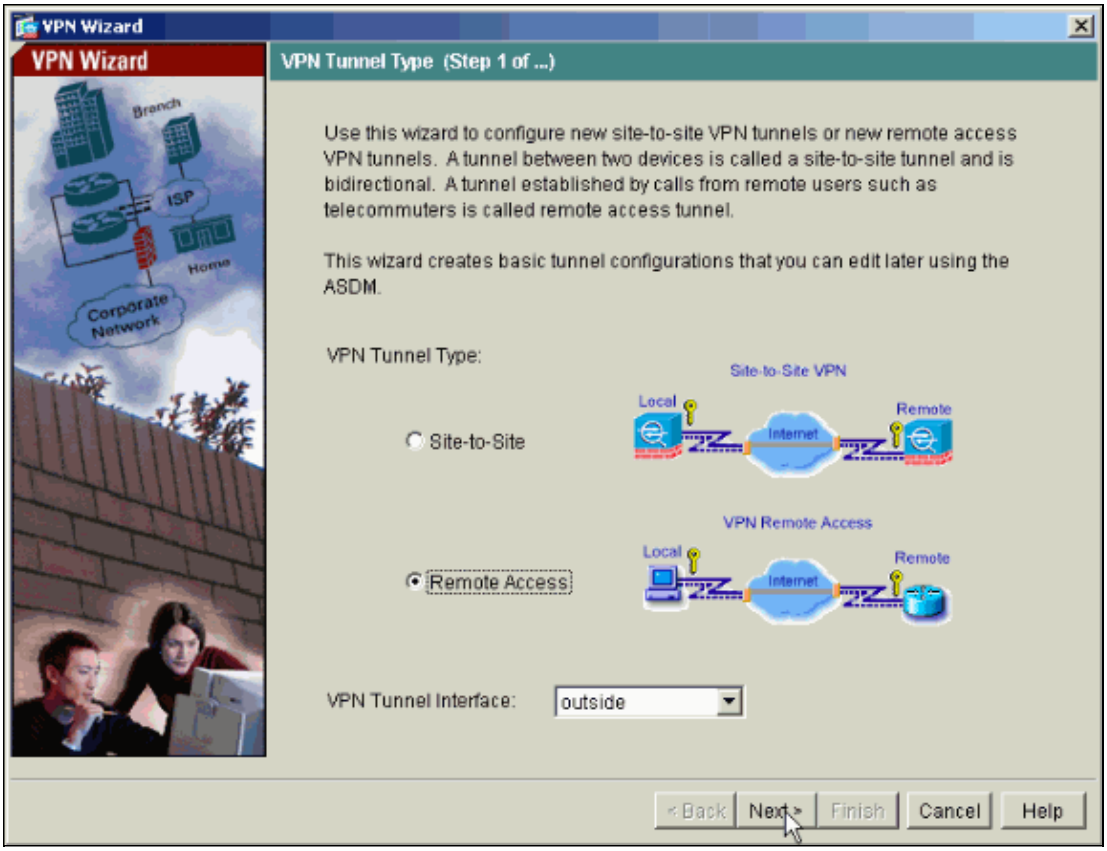
UDP: 0 TCP: 0 Total: 0

Input Kbps: 0 Output Kbps: 0

-- Syslog Disabled --

Device configuration loaded successfully. | admin | NA (15) | 12/22/05 1:02:46 PM UTC

2. Select the **Remote Access** VPN tunnel type and ensure that the VPN Tunnel Interface is set as desired.



VPN Wizard

VPN Tunnel Type (Step 1 of ...)

Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel.

This wizard creates basic tunnel configurations that you can edit later using the ASDM.

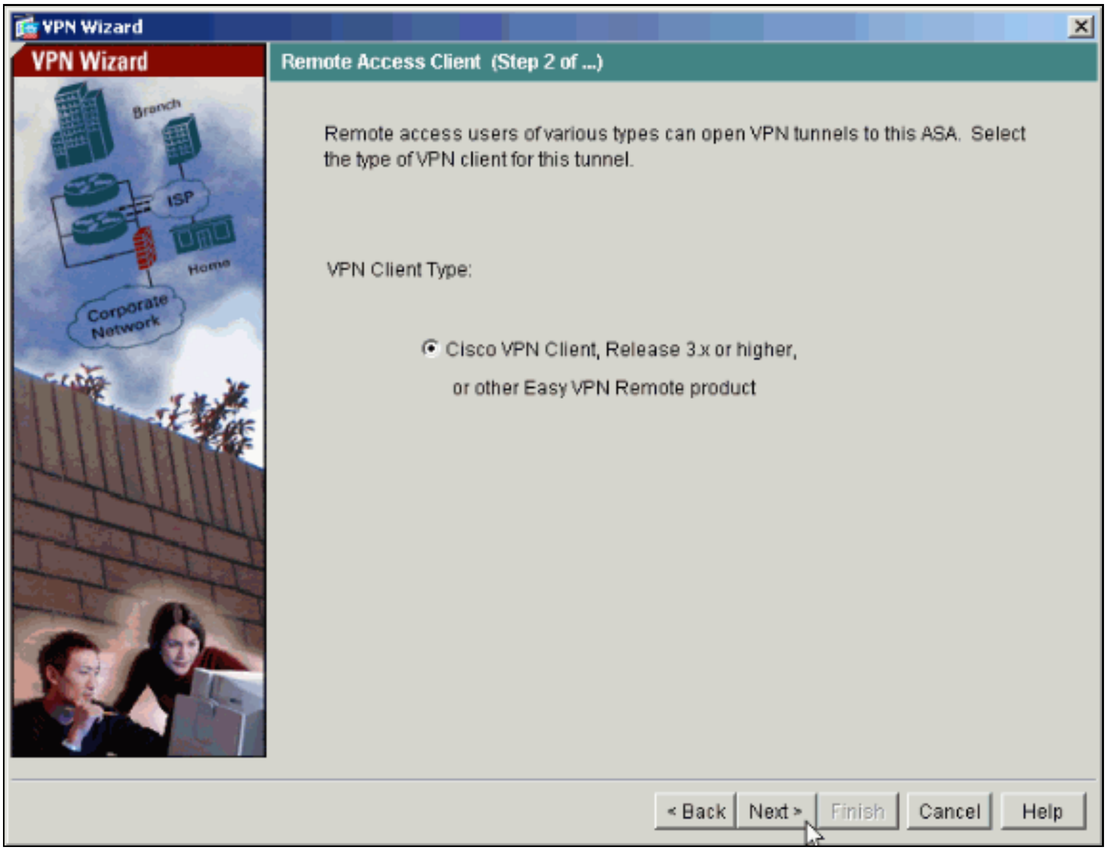
VPN Tunnel Type:

○ Site-to-Site

● Remote Access

VPN Tunnel Interface: outside

3. The only VPN Client Type available is already selected. Click **Next**.



VPN Wizard

Remote Access Client (Step 2 of ...)

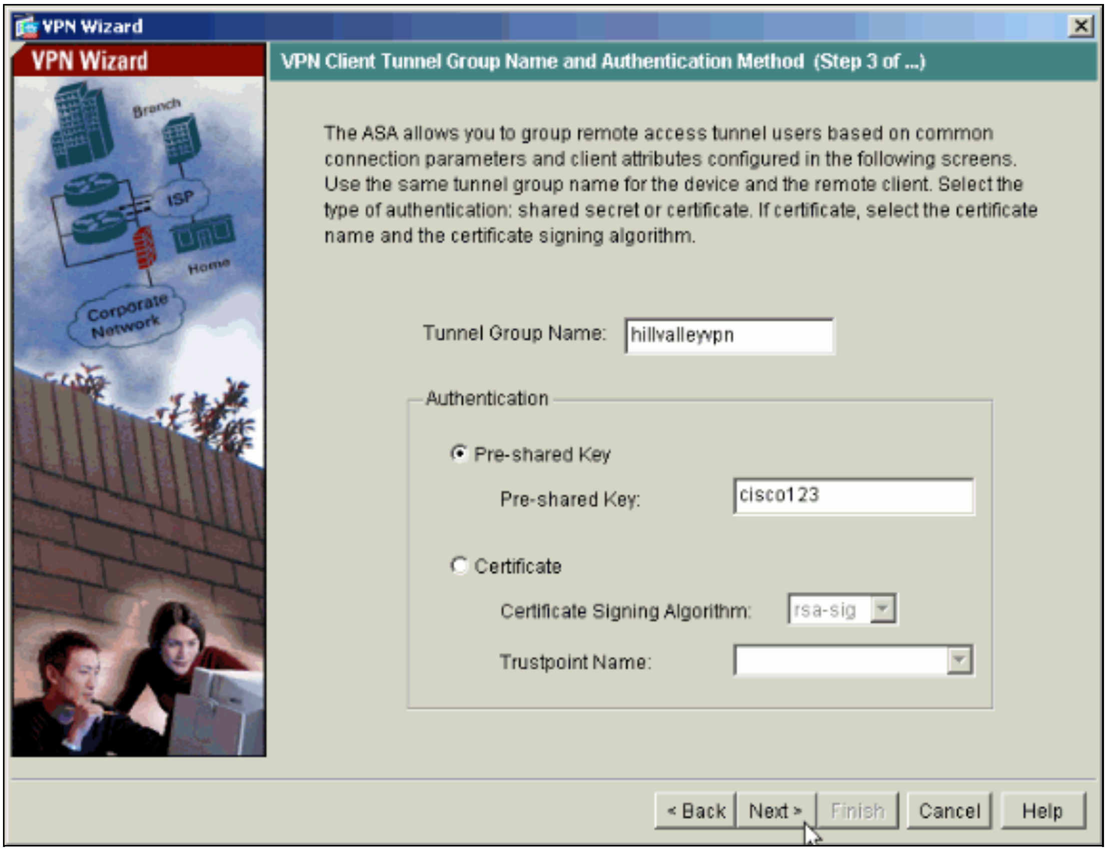
Remote access users of various types can open VPN tunnels to this ASA. Select the type of VPN client for this tunnel.

VPN Client Type:

● Cisco VPN Client, Release 3.x or higher, or other Easy VPN Remote product

4. Enter a name for the Tunnel Group Name. Supply the authentication information to use.

Pre−shared Key is selected in this example.



VPN Wizard

VPN Client Tunnel Group Name and Authentication Method (Step 3 of ...)

The ASA allows you to group remote access tunnel users based on common connection parameters and client attributes configured in the following screens. Use the same tunnel group name for the device and the remote client. Select the type of authentication: shared secret or certificate. If certificate, select the certificate name and the certificate signing algorithm.

Tunnel Group Name: hillvalleyvpn

Authentication

● Pre-shared Key

Pre-shared Key: cisco123

○ Certificate

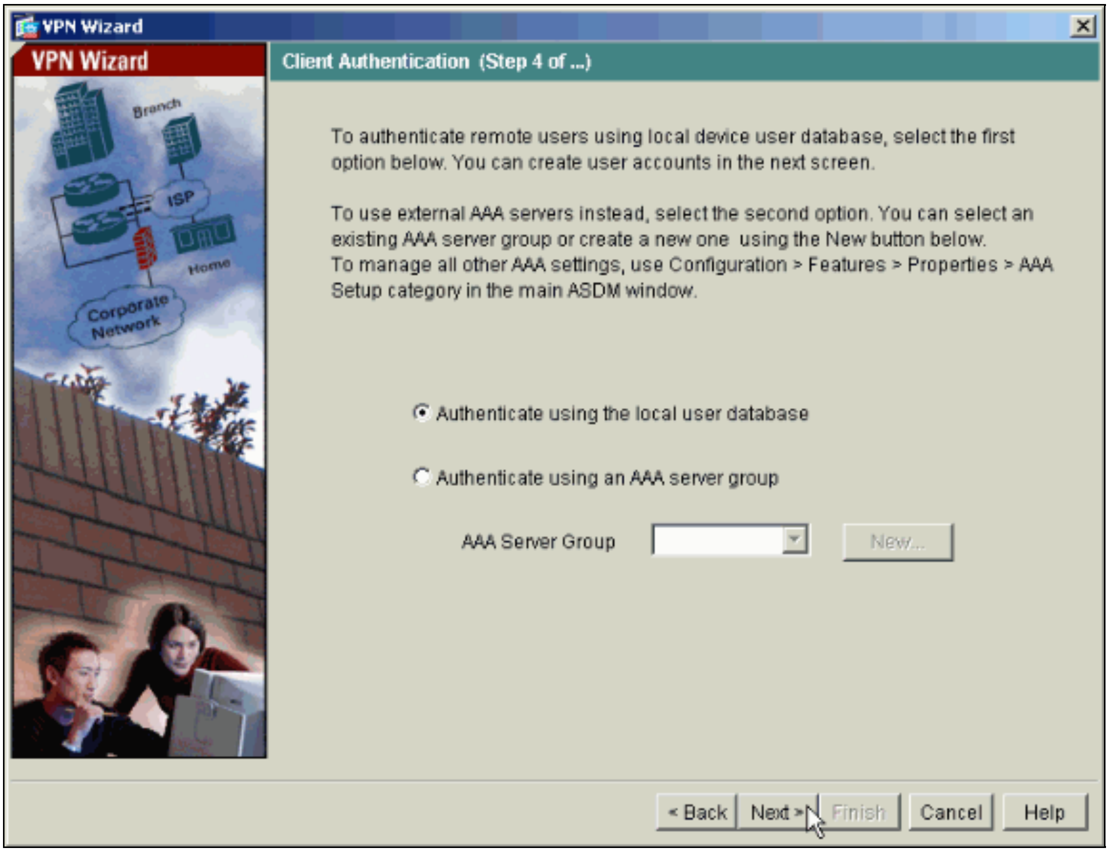
Certificate Signing Algorithm: rsa-sig

Trustpoint Name:

5. Choose whether you want remote users to be authenticated to the local user database or to an external AAA server group.

   Note: You add users to the local user database in step 6.

   Note: Refer to Authentication and Authorization Server Groups for VPN Users via ASDM Configuration Example for how to configure an external AAA server group via ASDM.



Client Authentication (Step 4 of ...)

To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next screen.

To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below.
To manage all other AAA settings, use Configuration > Features > Properties > AAA Setup category in the main ASDM window.

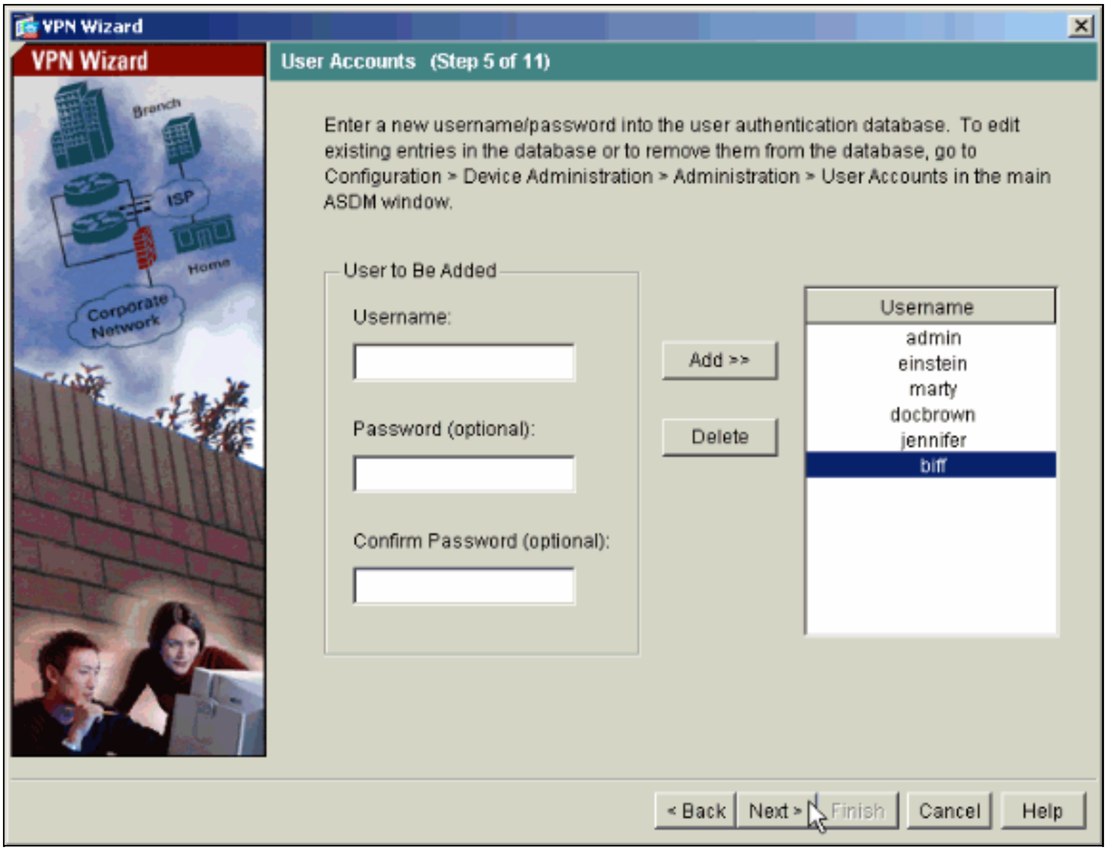
● Authenticate using the local user database

○ Authenticate using an AAA server group

AAA Server Group

6. Add users to the local database if necessary.

   Note: Do not remove existing users from this window. Select **Configuration** > **Device Administration** > **Administration** > **User Accounts in the main ASDM window** to edit existing entries in the database or to remove them from the database.


VPN Wizard

User Accounts (Step 5 of 11)

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 > Device Administration > Administration > User Accounts in the main ASDM window.

User to Be Added

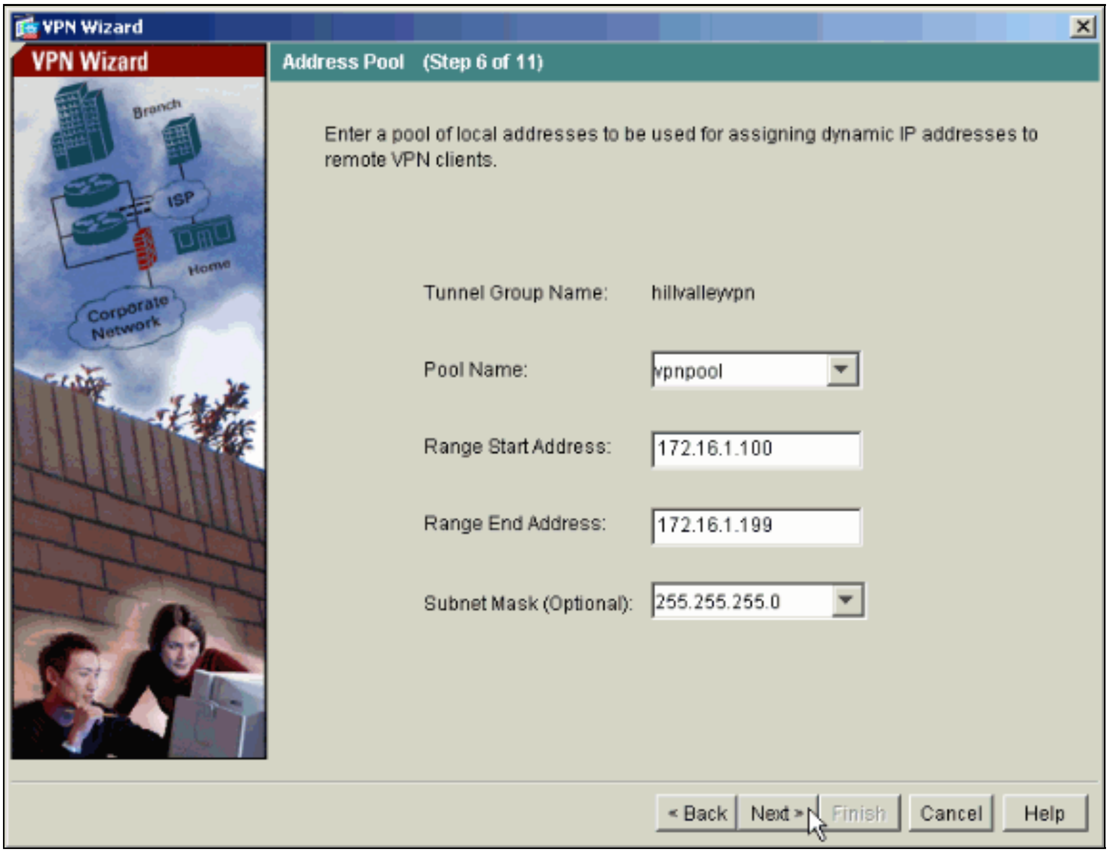
Username:

Password (optional):

Confirm Password (optional):

Username
admin
einstein
marty
docbrown
jennifer
biff

7. Define a pool of local addresses to be dynamically assigned to remote VPN Clients when they connect.


VPN Wizard

Address Pool (Step 6 of 11)

Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.

Tunnel Group Name: hillvalleyvpn

Pool Name: vpnpool

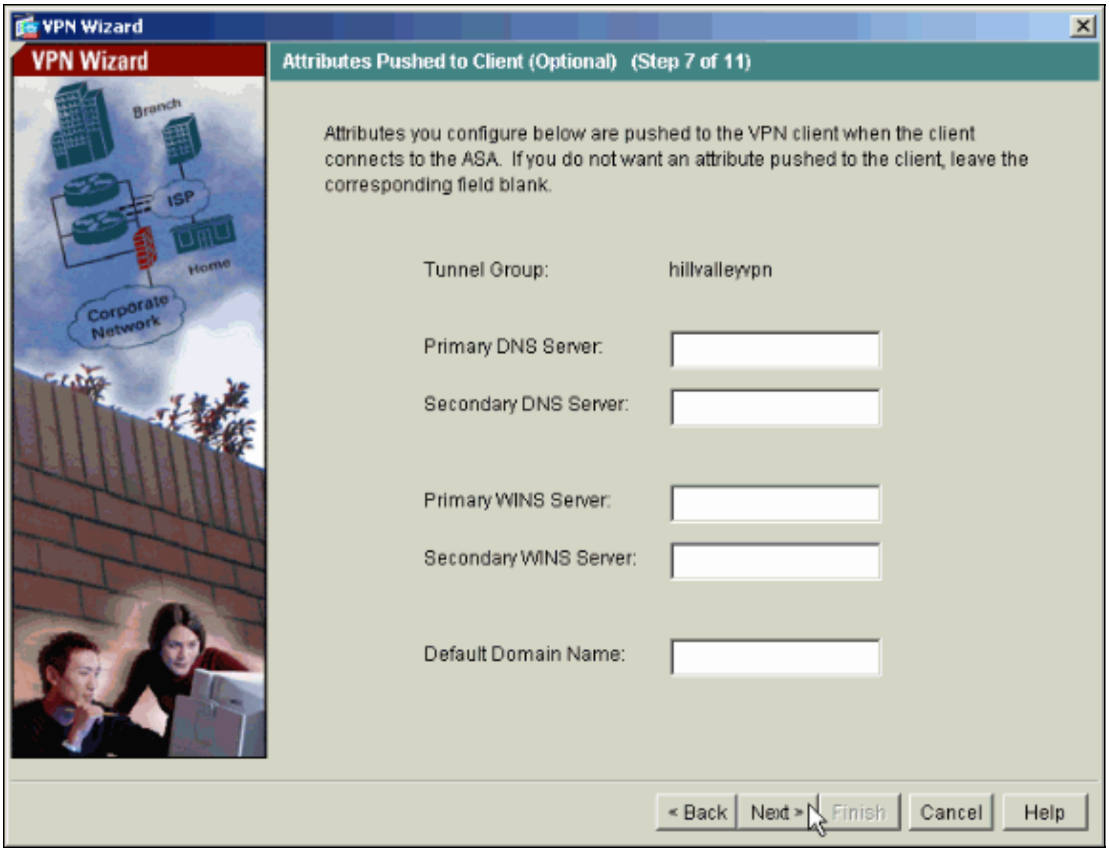
Range Start Address: 172.16.1.100

Range End Address: 172.16.1.199

Subnet Mask (Optional): 255.255.255.0

8. *Optional:* Specify the DNS and WINS server information and a Default Domain Name to be pushed

to remote VPN Clients.



Attributes Pushed to Client (Optional) (Step 7 of 11)

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.

Tunnel Group: hillvalleyvpn

Primary DNS Server:

Secondary DNS Server:

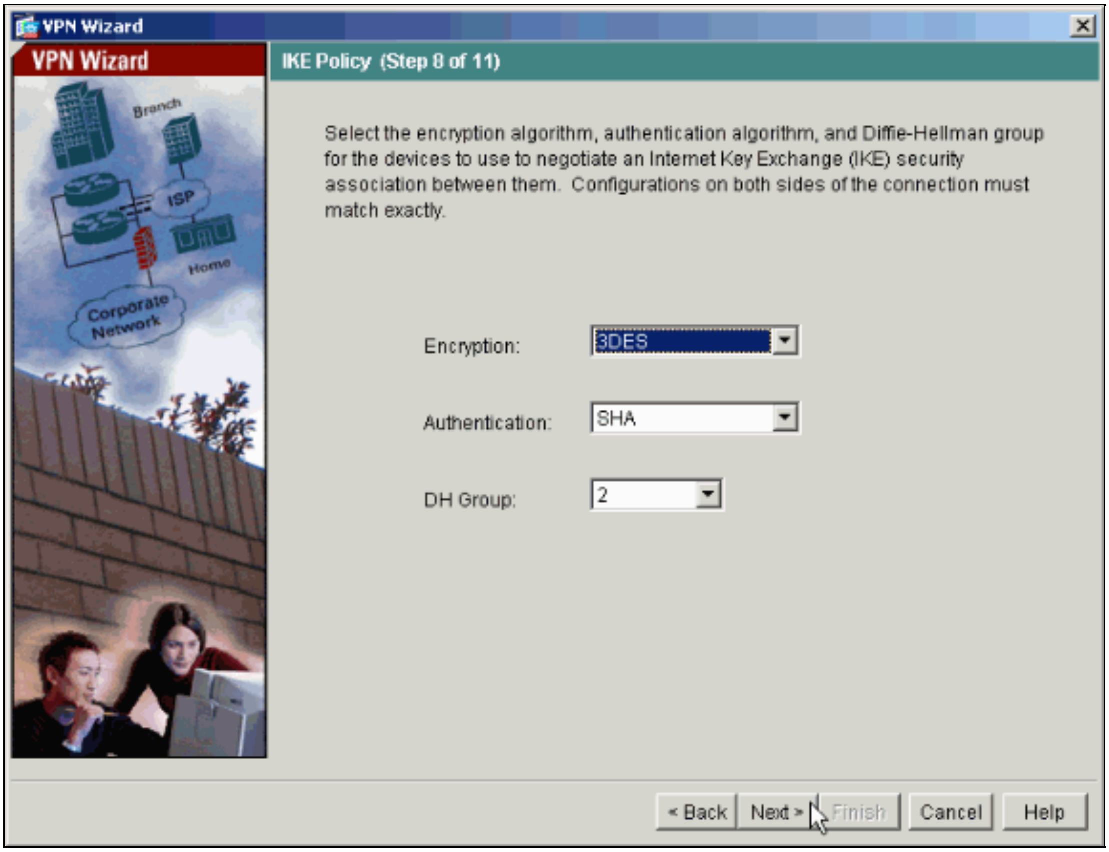
Primary WINS Server:

Secondary WINS Server:

Default Domain Name:

9. Specify the parameters for IKE, also known as IKE Phase 1.

   Configurations on both sides of the tunnel must match exactly. However, the Cisco VPN Client automatically selects the proper configuration for itself. Therefore, no IKE configuration is necessary on the client PC.



IKE Policy (Step 8 of 11)

Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.

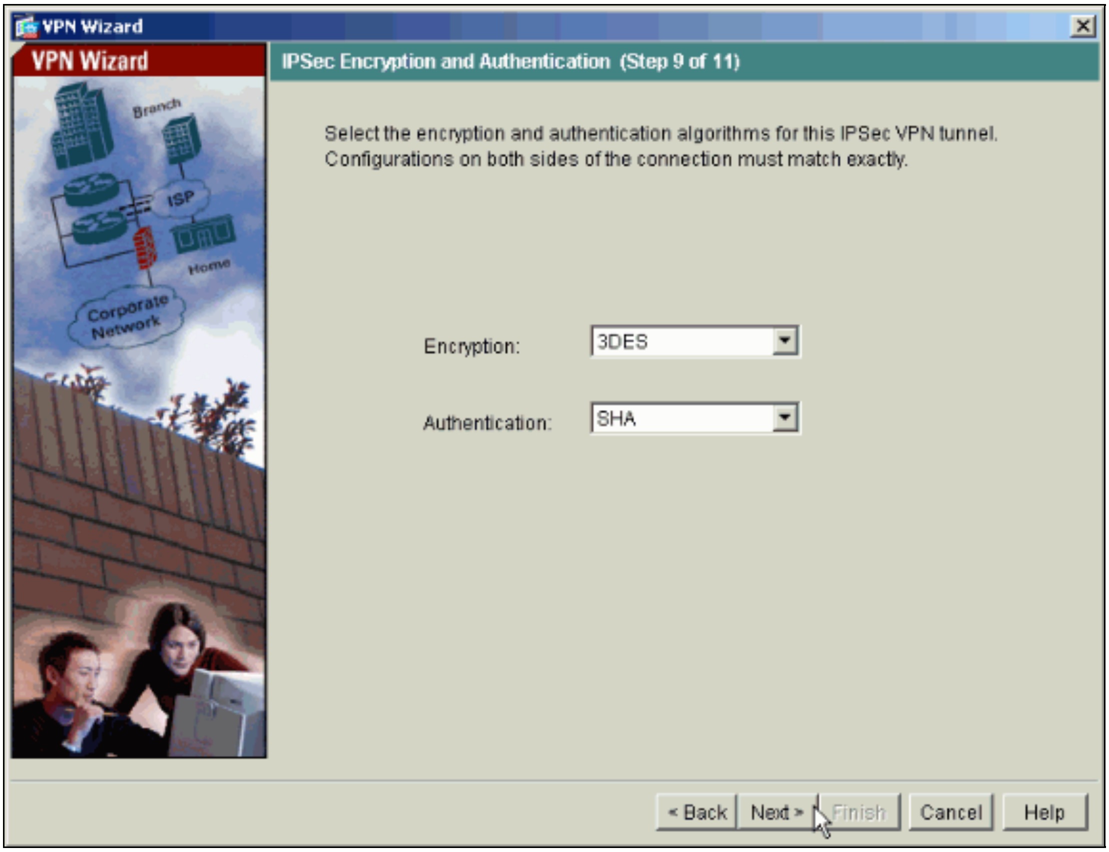
Encryption: 3DES

Authentication: SHA

DH Group: 2

10. Specify the parameters for IPsec, also known as IKE Phase 2.

    Configurations on both sides of the tunnel must match exactly. However, the Cisco VPN Client automatically selects the proper configuration for itself. Therefore, no IKE configuration is necessary on the client PC.



IPSec Encryption and Authentication (Step 9 of 11)

Select the encryption and authentication algorithms for this IPSec VPN tunnel. Configurations on both sides of the connection must match exactly.

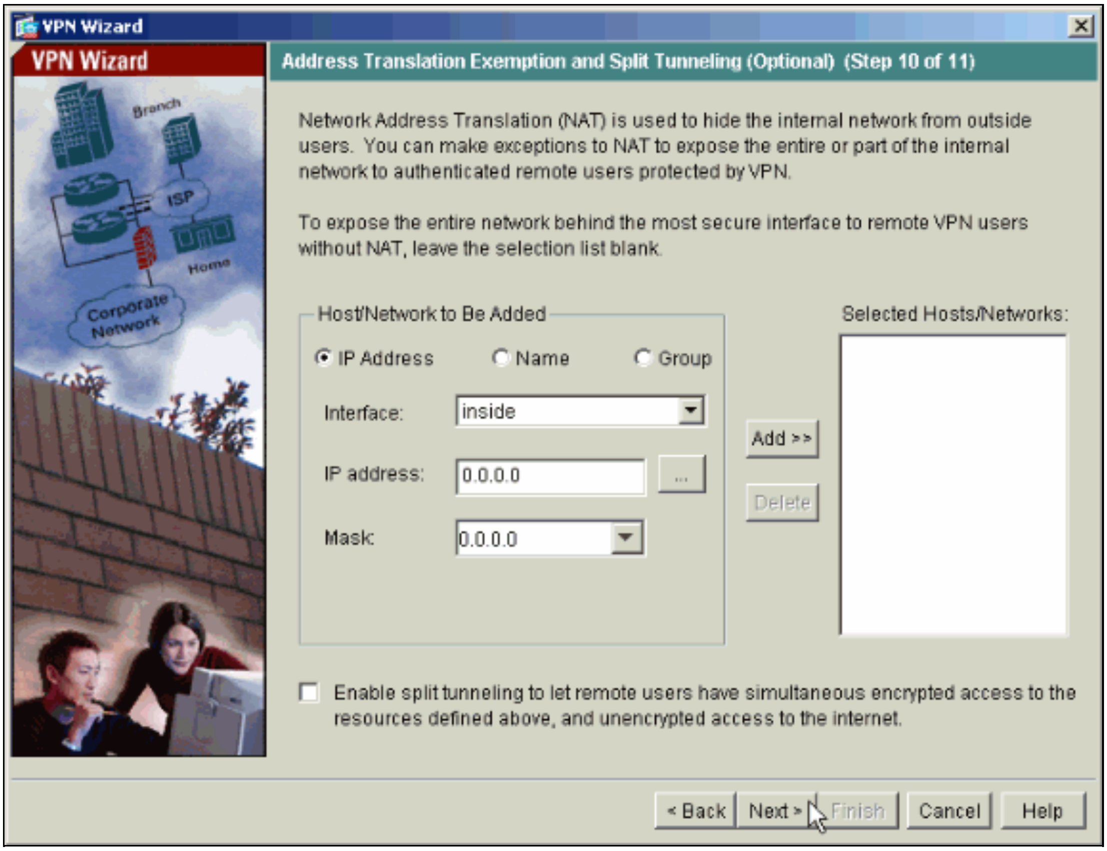
Encryption: 3DES

Authentication: SHA

11. Specify which, if any, internal hosts or networks should be exposed to remote VPN users.

    If you leave this list empty, it allows remote VPN users to access the entire inside network of the ASA.

    You can also enable split tunneling on this window. Split tunneling encrypts traffic to the resources defined earlier in this procedure and provides unencrypted access to the Internet at large by not tunneling that traffic. If split tunneling is *not* enabled, all traffic from remote VPN users is tunneled to the ASA. This can become very bandwidth and processor intensive, based on your configuration.



Address Translation Exemption and Split Tunneling (Optional) (Step 10 of 11)

Network Address Translation (NAT) is used to hide the internal network from outside users. You can make exceptions to NAT to expose the entire or part of the internal network to authenticated remote users protected by VPN.

To expose the entire network behind the most secure interface to remote VPN users without NAT, leave the selection list blank.

Host/Network to Be Added

● IP Address ○ Name ○ Group

Interface: inside

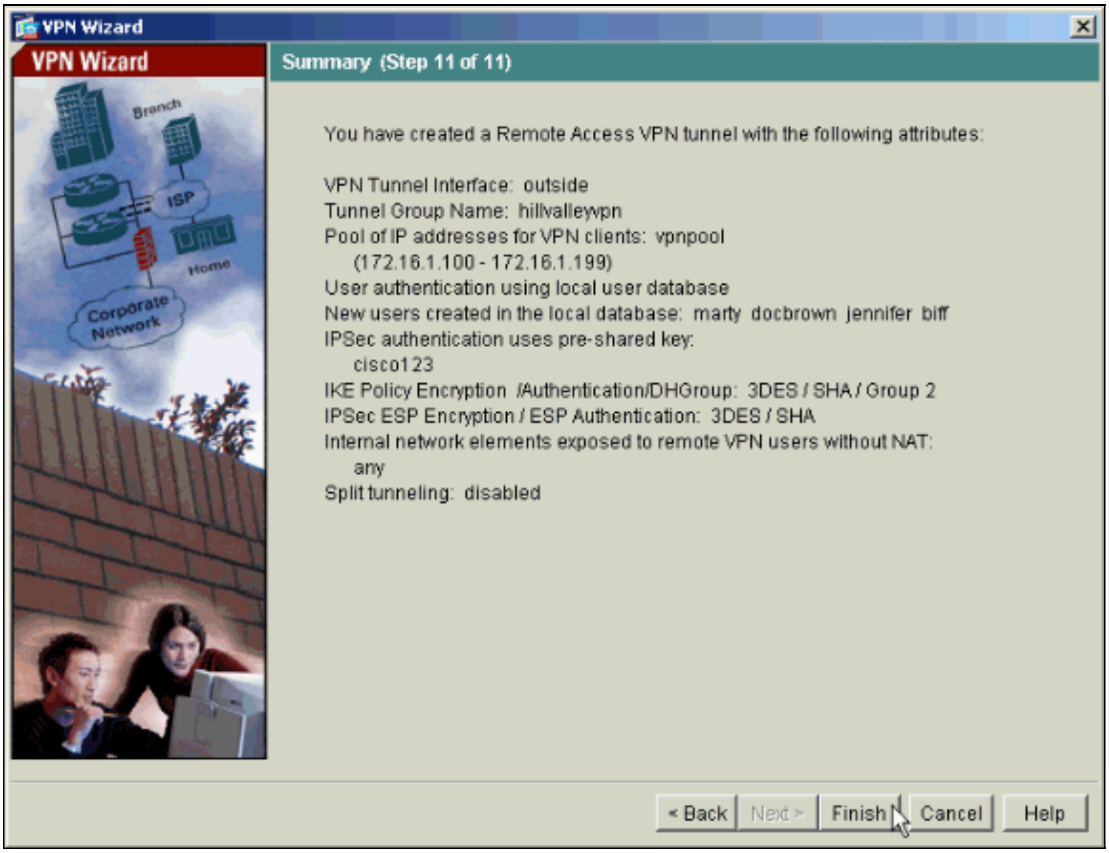
IP address: 0.0.0.0

Mask: 0.0.0.0

Selected Hosts/Networks:

□ Enable split tunneling to let remote users have simultaneous encrypted access to the resources defined above, and unencrypted access to the internet.

12. This window shows a summary of the actions that you have taken. Click **Finish** if you are satisfied with your configuration.



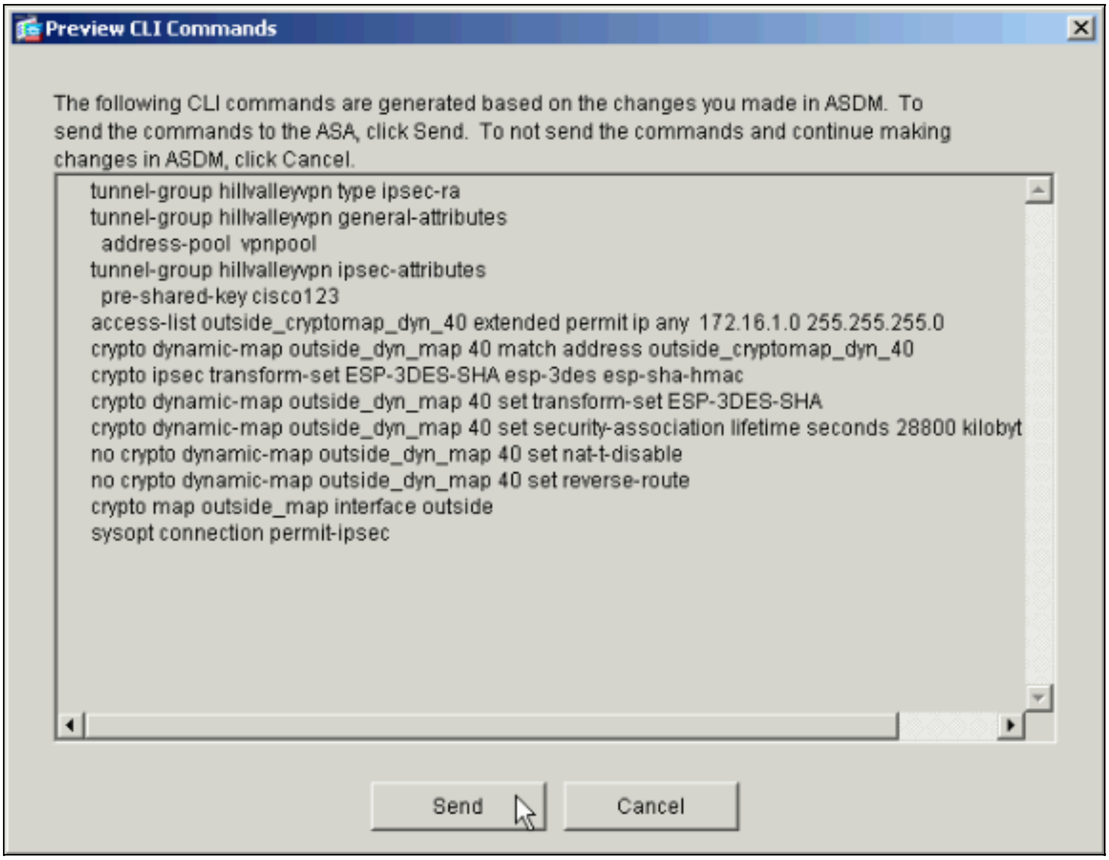
Summary (Step 11 of 11)

You have created a Remote Access VPN tunnel with the following attributes:

VPN Tunnel Interface: outside
Tunnel Group Name: hillvalleyvpn
Pool of IP addresses for VPN clients: vpnpool
    (172.16.1.100 - 172.16.1.199)
User authentication using local user database
New users created in the local database: marty docbrown jennifer biff
IPSec authentication uses pre-shared key:
    cisco123
IKE Policy Encryption /Authentication/DHGroup: 3DES / SHA / Group 2
IPSec ESP Encryption / ESP Authentication: 3DES / SHA
Internal network elements exposed to remote VPN users without NAT:
    any
Split tunneling: disabled

13. If you have it configured to do so, the ASA displays a preview of the commands that will be added to

the running configuration. Click **Send** to send the commands to the ASA.



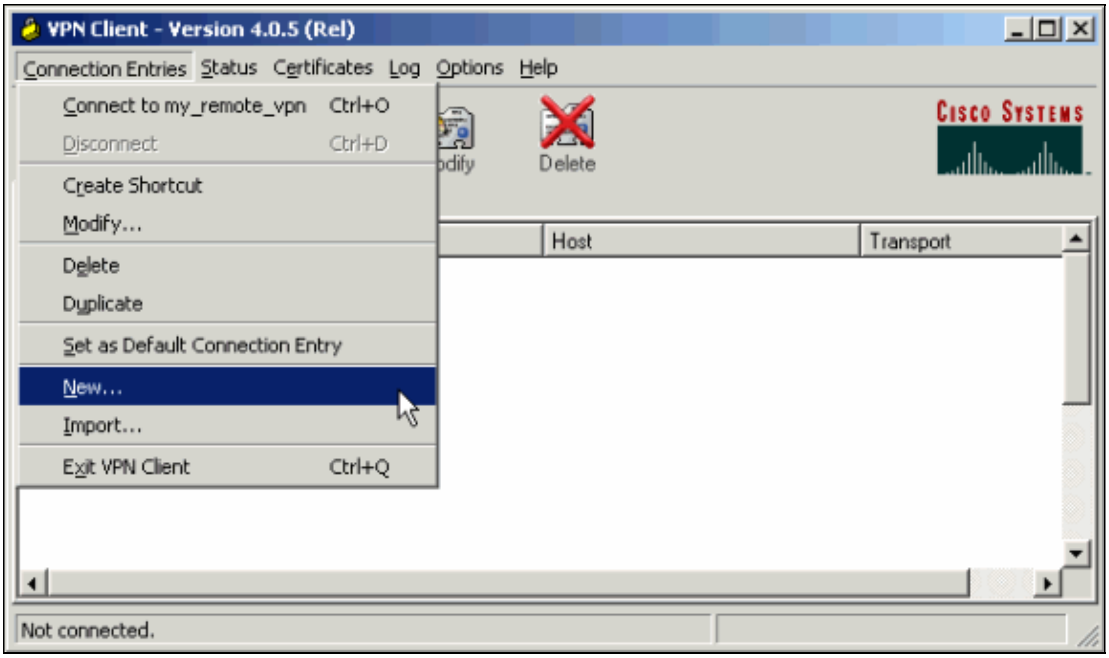
The following CLI commands are generated based on the changes you made in ASDM. To send the commands to the ASA, click Send. To not send the commands and continue making changes in ASDM, click Cancel.

```
tunnel-group hillvalleyvpn type ipsec-ra
tunnel-group hillvalleyvpn general-attributes
 address-pool vpnpool
tunnel-group hillvalleyvpn ipsec-attributes
 pre-shared-key cisco123
access-list outside_cryptomap_dyn_40 extended permit ip any 172.16.1.0 255.255.255.0
crypto dynamic-map outside_dyn_map 40 match address outside_cryptomap_dyn_40
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto dynamic-map outside_dyn_map 40 set transform-set ESP-3DES-SHA
crypto dynamic-map outside_dyn_map 40 set security-association lifetime seconds 28800 kilobyt
no crypto dynamic-map outside_dyn_map 40 set nat-t-disable
no crypto dynamic-map outside_dyn_map 40 set reverse-route
crypto map outside_map interface outside
sysopt connection permit-ipsec
```

Verify

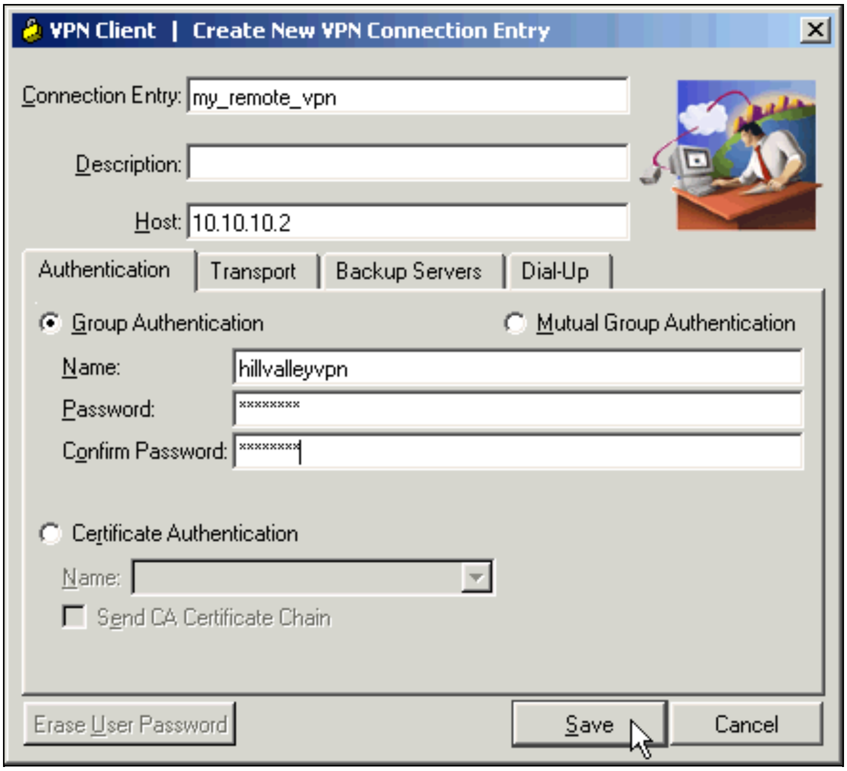
Attempt to connect to the Cisco ASA using the Cisco VPN Client in order to verify that the ASA is successfully configured.

1. Select **Connection Entries** > **New**.



2. Fill in the details of your new connection.

   The Host field should contain the IP address or hostname of the previously configured Cisco ASA. The Group Authentication information should correspond to that used in step 4. Click **Save** when you are finished.



Connection Entry: my_remote_vpn

Description:

Host: 10.10.10.2

● Group Authentication ○ Mutual Group Authentication

Name: hillvalleyvpn

Password: ********

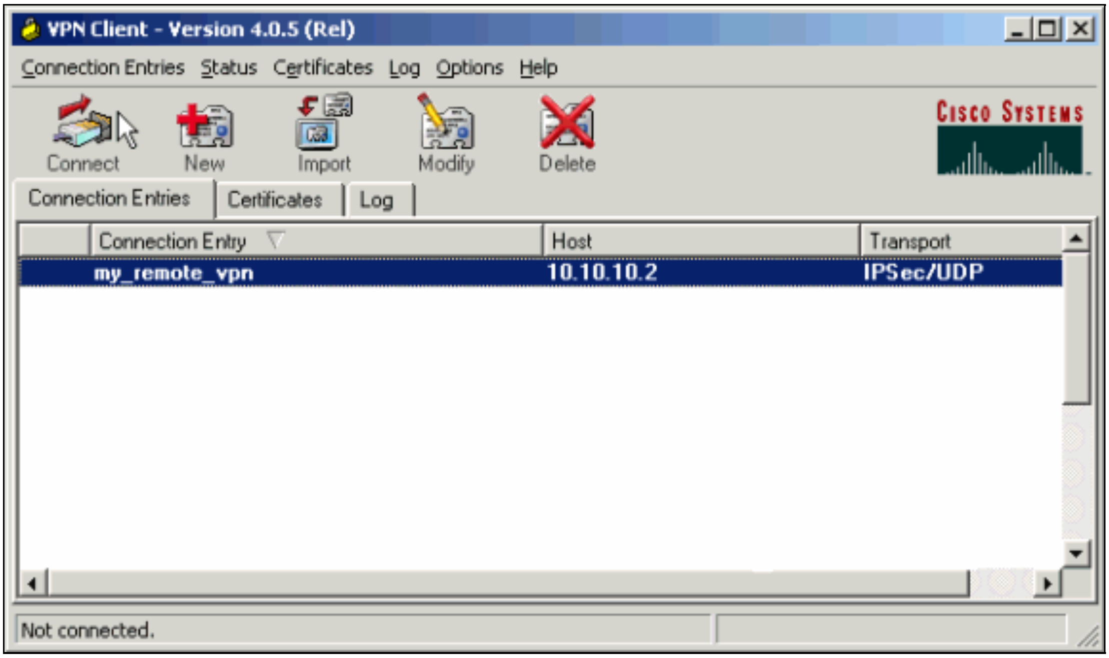
Confirm Password: ********

○ Certificate Authentication

Name:

□ Send CA Certificate Chain

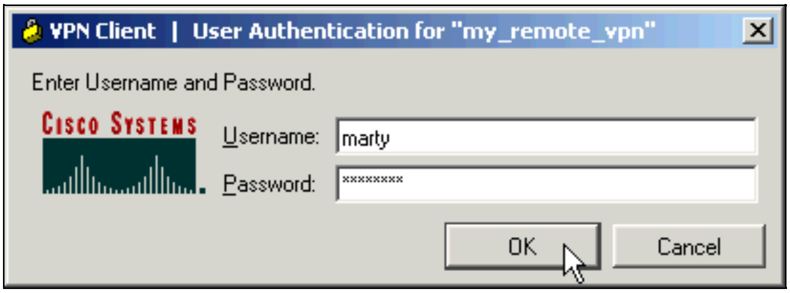
3. Select the newly created connection, and click **Connect**.


VPN Client - Version 4.0.5 (Rel)
Connection Entries Status Certificates Log Options Help
Connect
New
Import
Modify
Delete
Cisco Systems
Connection Entries
Certificates
Log

	Connection Entry	Host	Transport
	my_remote_vpn	10.10.10.2	IPSec/UDP

Not connected.

4. Enter a username and password for extended authentication. This information should match that specified in steps 5 and 6.



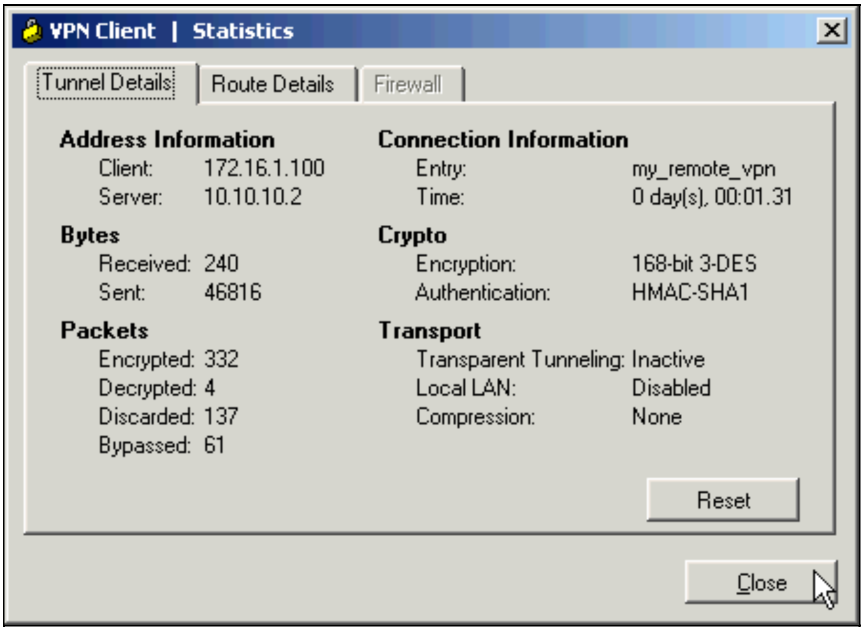
Enter Username and Password.

Username: marty

Password: ********

5. Once the connection is successfully established select **Statistics** from the Status menu to verify the details of the tunnel.

   This window shows traffic and crypto information:



Address Information
Client: 172.16.1.100
Server: 10.10.10.2

Bytes
Received: 240
Sent: 46816

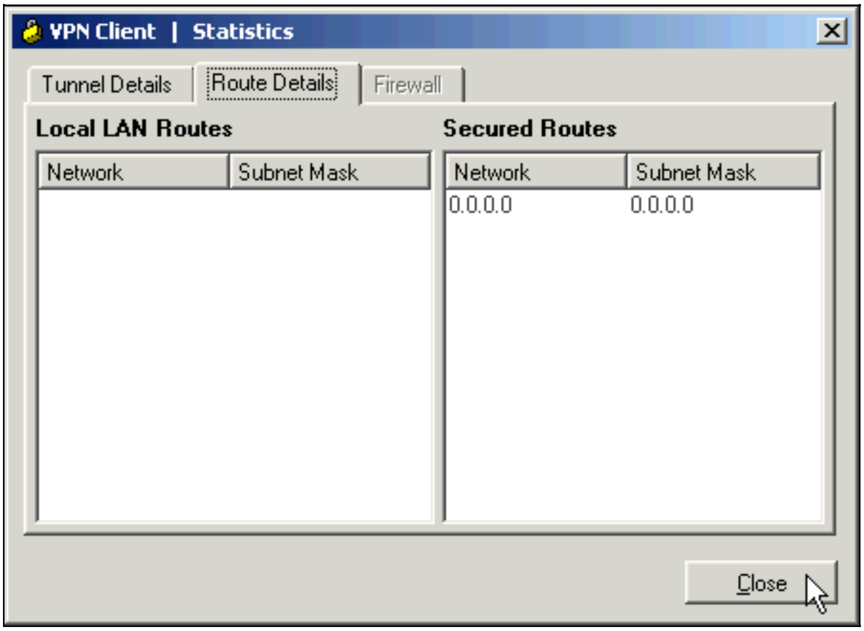
Packets
Encrypted: 332
Decrypted: 4
Discarded: 137
Bypassed: 61

Connection Information
Entry: my_remote_vpn
Time: 0 day(s), 00:01.31

Crypto
Encryption: 168-bit 3-DES
Authentication: HMAC-SHA1

Transport
Transparent Tunneling: Inactive
Local LAN: Disabled
Compression: None

This window shows split tunneling information:



Local LAN Routes

Network	Subnet Mask

Secured Routes

Network	Subnet Mask
0.0.0.0	0.0.0.0

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

NetPro Discussion Forums − Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums − Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- **Cisco ASA 5500 Series Adaptive Security Appliances**
- **Cisco ASA 5500 Series Adaptive Security Appliances Troubleshoot and Alerts**
- **Technical Support & Documentation − Cisco Systems**

Updated: Feb 22, 2006 Document ID: 68795