

PIX/ASA as a Remote VPN Server with Extended Authentication using CLI and ASDM Configuration Example

Document ID: 68795

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Background Information

Configurations

- Configure the ASA/PIX as a Remote VPN Server using ASDM
- Configure the ASA/PIX as a Remote VPN Server using CLI
- Cisco VPN Client Password Storage Configuration
- Disable the Extended Authentication

Verify

Troubleshoot

- Incorrect Crypto ACL

Related Information

Introduction

This document describes how to configure the Cisco 5500 Series Adaptive Security Appliance (ASA) to act as a remote VPN server using the Adaptive Security Device Manager (ASDM) or CLI. 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.

Refer to PIX/ASA 7.x and Cisco VPN Client 4.x with Windows 2003 IAS RADIUS (Against Active Directory) Authentication Configuration Example in order to set up the remote access VPN connection between a Cisco VPN Client (4.x for Windows) and the PIX 500 Series Security Appliance 7.x. The remote VPN Client user authenticates against the Active Directory using a Microsoft Windows 2003 Internet Authentication Service (IAS) RADIUS server.

Refer to PIX/ASA 7.x and Cisco VPN Client 4.x for Cisco Secure ACS Authentication Configuration Example in order to set up a remote access VPN connection between a Cisco VPN Client (4.x for Windows) and the PIX 500 Series Security Appliance 7.x using a Cisco Secure Access Control Server (ACS version 3.2) for extended authentication (Xauth).

Prerequisites

Requirements

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

Note: Refer to Allowing HTTPS Access for ASDM or PIX/ASA 7.x: SSH on the Inside and Outside Interface Configuration Example to allow the device to be remotely configured by the ASDM or Secure Shell (SSH).

Components Used

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

- Cisco Adaptive Security Appliance Software Version 7.x and later
- Adaptive Security Device Manager Version 5.x and later
- Cisco VPN Client Version 4.x and later

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 and later.

Conventions

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

Background Information

Remote access configurations provide secure remote access for Cisco VPN clients, such as mobile users. A remote access VPN lets remote users securely access centralized network resources. The Cisco VPN Client complies with the IPSec protocol and is specifically designed to work with the security appliance. However, the security appliance can establish IPSec connections with many protocol-compliant clients. Refer to the ASA Configuration Guides for more information on IPSec.

Groups and users are core concepts in the management of the security of VPNs and in the configuration of the security appliance. They specify attributes that determine users access to and use of the VPN. A group is a collection of users treated as a single entity. Users get their attributes from group policies. Tunnel groups identify the group policy for a specific connections. If you do not assign a particular group policy to a users, the default group policy for the connection applies.

A tunnel group consists of a set of records that determines tunnel connection policies. These records identify the servers to which the tunnel users are authenticated, as well as the accounting servers, if any, to which connections information is sent. They also identify a default group policy for the connections, and they contain protocol-specific connection parameters. Tunnel groups include a small number of attributes that pertains to the creation of the tunnel itself. Tunnel groups include a pointer to a group policy that defines user-oriented attributes.

Note: In the sample configuration in this document, local user accounts are used for authentication. If you would like to use another service, such as LDAP and RADIUS, refer to Configuring an External RADIUS Server for Authorization and Authentication.

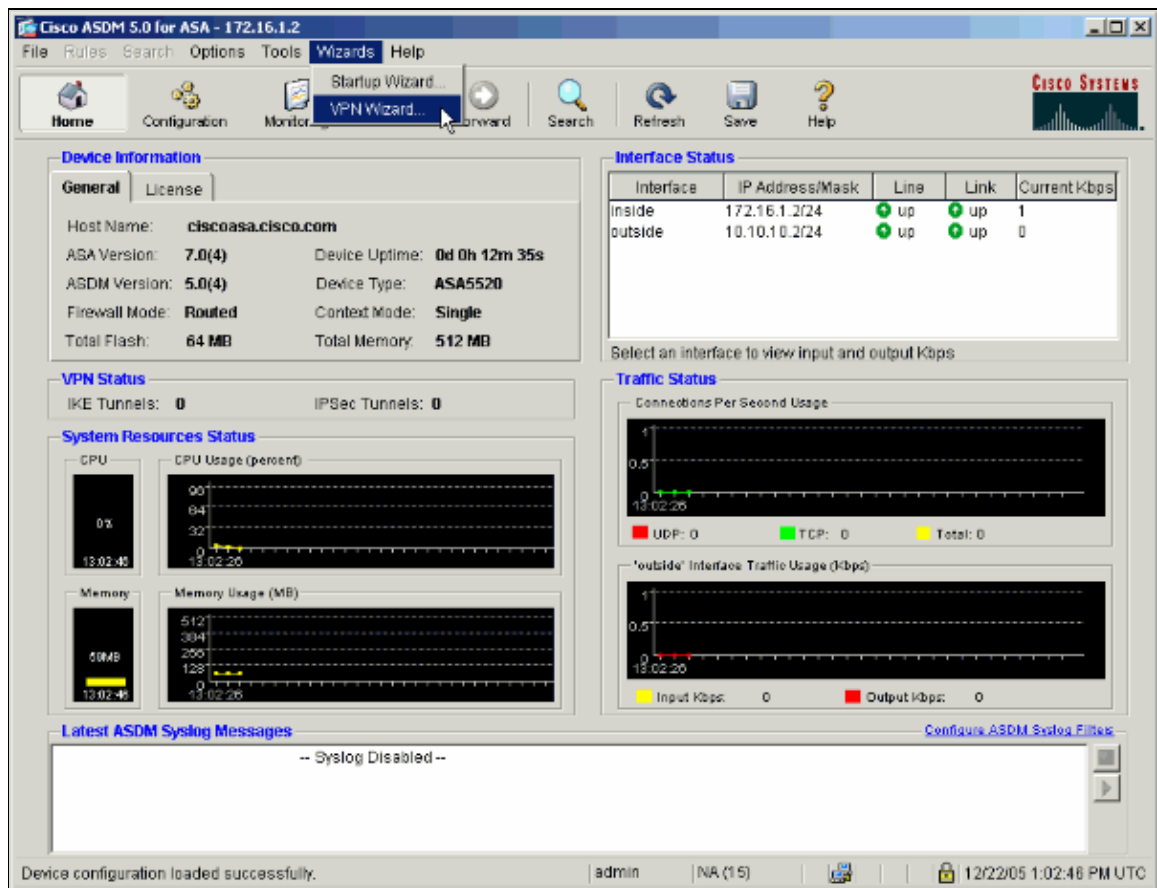
The Internet Security Association and Key Management Protocol (ISAKMP), also called IKE, is the negotiation protocol that hosts agree on how to build an IPSec Security Association. Each ISAKMP negotiation is divided into two sections, Phase1 and Phase2. Phase1 creates the first tunnel to protect later ISAKMP negotiation messages. Phase2 creates the tunnel that protects data that travels across the secure connection. Refer to ISAKMP Policy Keywords for CLI Commands for more information on ISAKMP.

Configurations

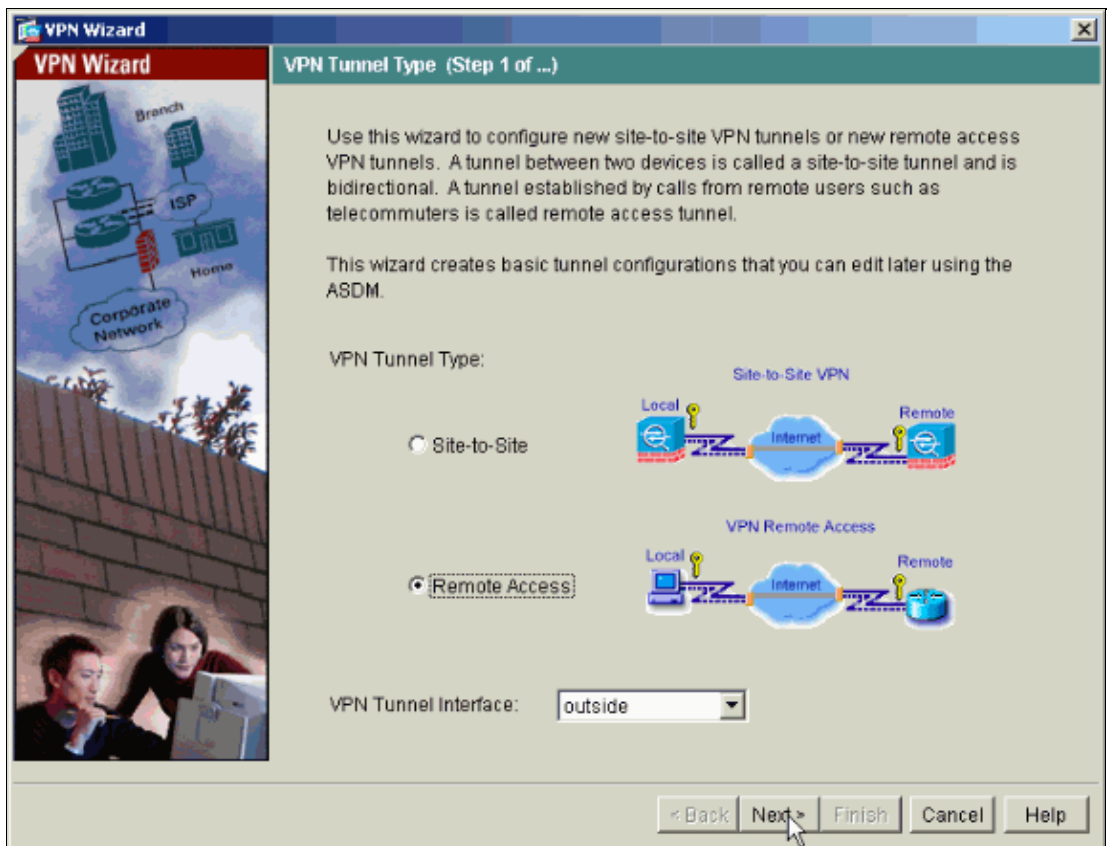
Configure the ASA/PIX as a Remote VPN Server using ASDM

Complete these steps in order to configure the Cisco ASA as a remote VPN server using ASDM:

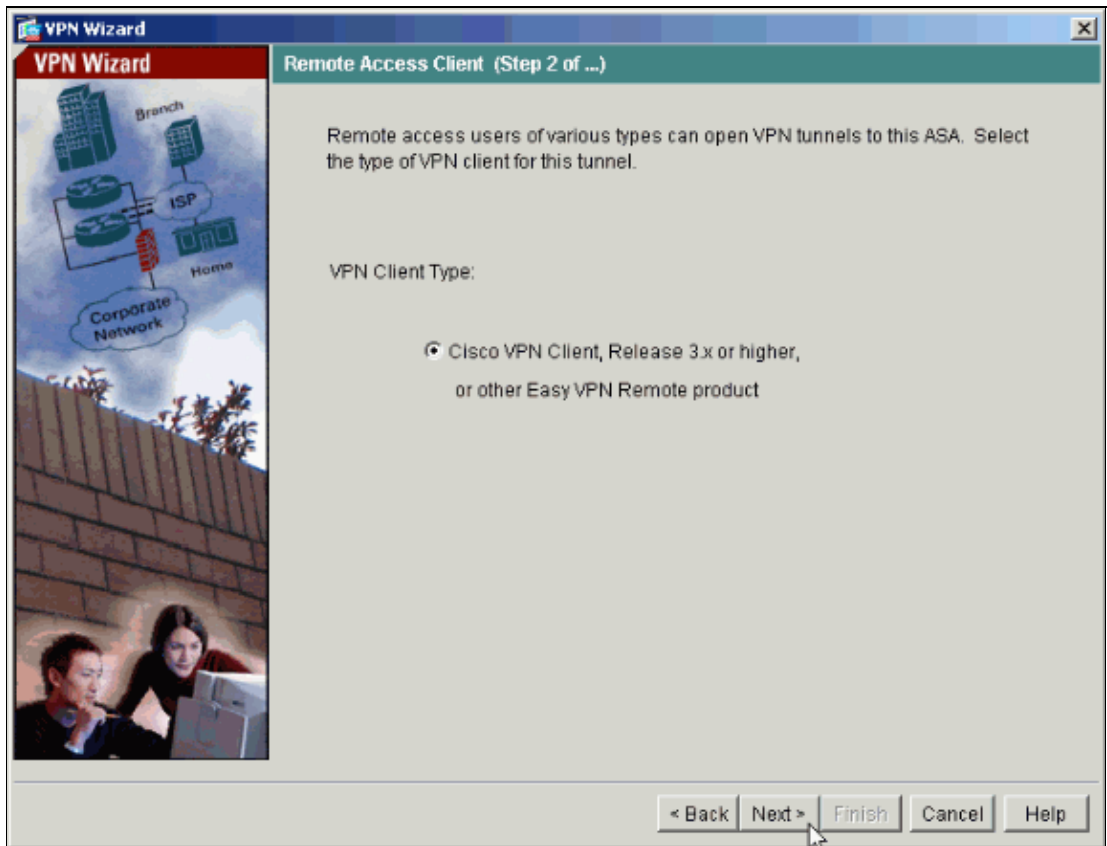
1. Select **Wizards > VPN Wizard** from the Home window.



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

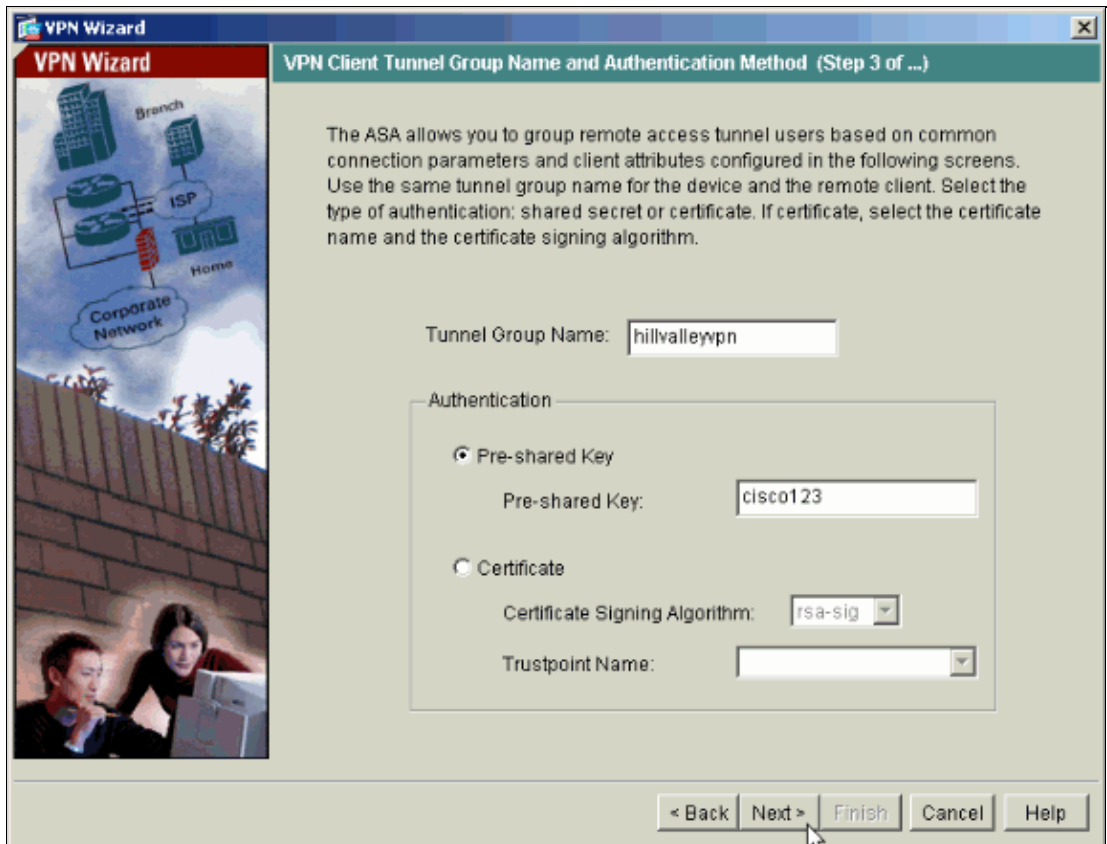


3. The only VPN Client Type available is already selected. Click **Next**.



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

Pre-shared Key is selected in this example.

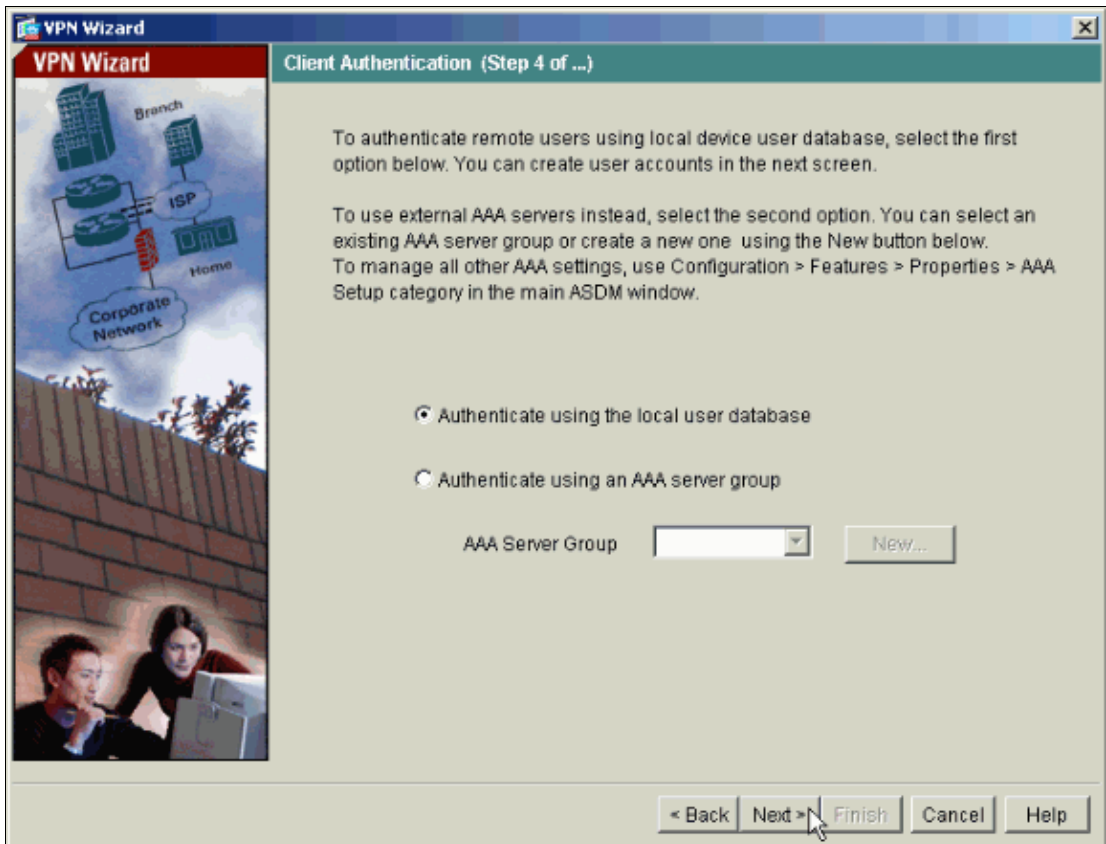


Note: There is not a way to hide/encrypt the pre-shared key on the ASDM. The reason is that the ASDM should only be used by people who configure the ASA or by people who are assisting the customer with this configuration.

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

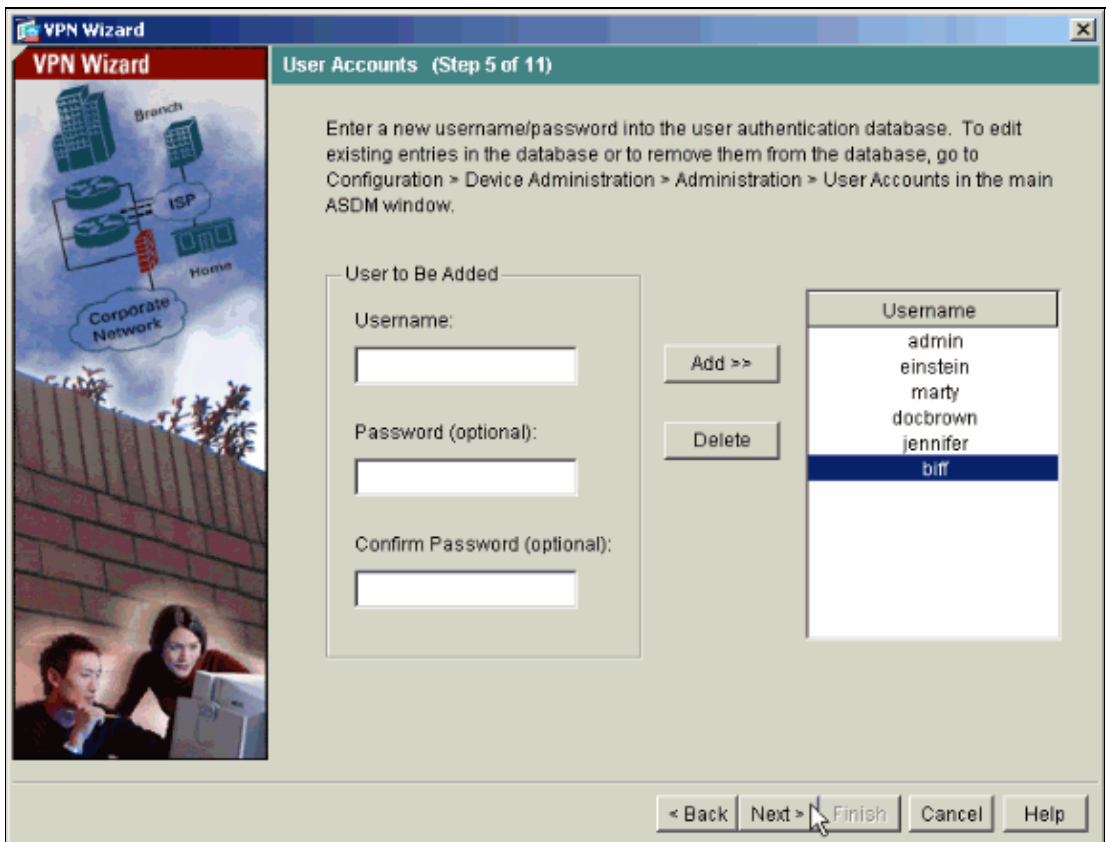
Note: You add users to the local user database in step 6.

Note: Refer to PIX/ASA 7.x Authentication and Authorization Server Groups for VPN Users via ASDM Configuration Example for information on how to configure an external AAA server group via ASDM.



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.



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

The screenshot shows the 'VPN Wizard' window at 'Step 6 of 11', titled 'Address Pool'. The left sidebar contains a network diagram with 'Branch', 'ISP', 'Home', and 'Corporate Network' components, and an image of two people at a computer. The main area contains the following configuration fields:

- Tunnel Group Name: hillvalleyvpn
- Pool Name: vpnpool (dropdown menu)
- Range Start Address: 172.16.1.100
- Range End Address: 172.16.1.199
- Subnet Mask (Optional): 255.255.255.0 (dropdown menu)

At the bottom, there are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. A mouse cursor is pointing at the 'Next >' button.

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

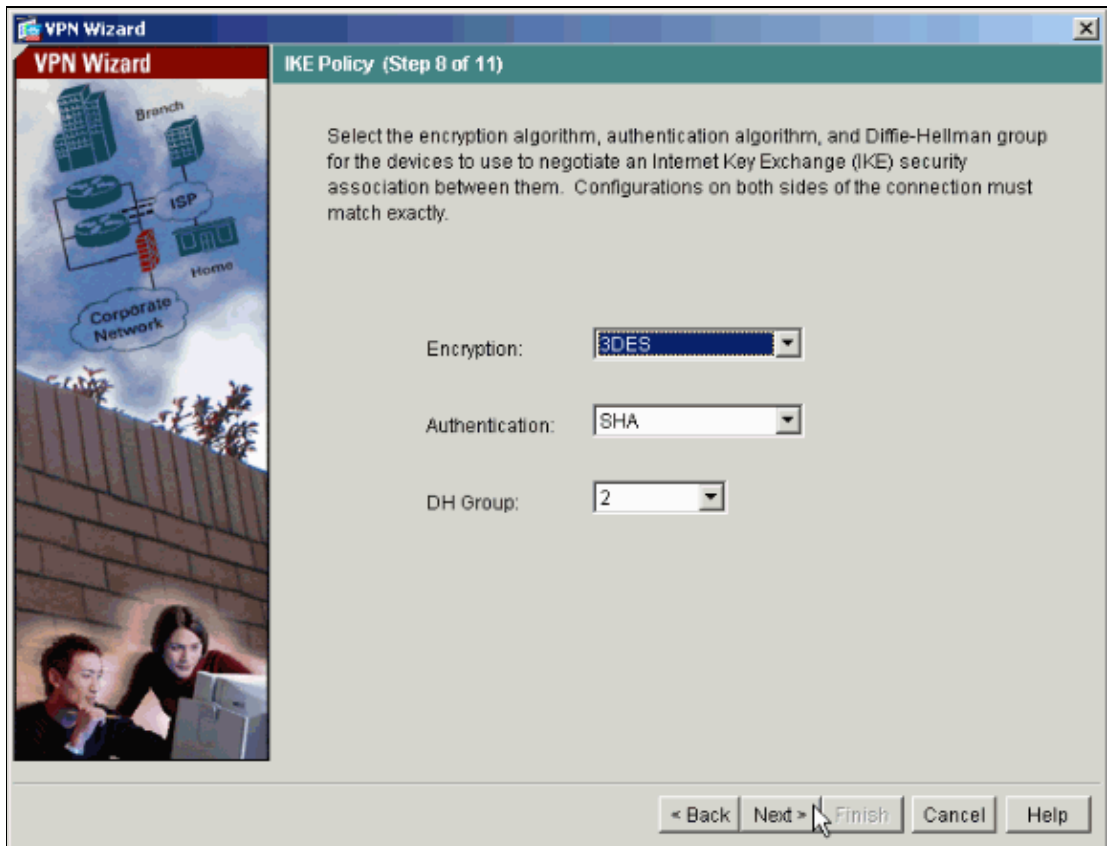
The screenshot shows the 'VPN Wizard' window at 'Step 7 of 11', titled 'Attributes Pushed to Client (Optional)'. The left sidebar is identical to the previous screen. The main area contains the following configuration fields:

- Tunnel Group: hillvalleyvpn
- Primary DNS Server: [Empty text box]
- Secondary DNS Server: [Empty text box]
- Primary WINS Server: [Empty text box]
- Secondary WINS Server: [Empty text box]
- Default Domain Name: [Empty text box]

At the bottom, there are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'. A mouse cursor is pointing at the 'Next >' button.

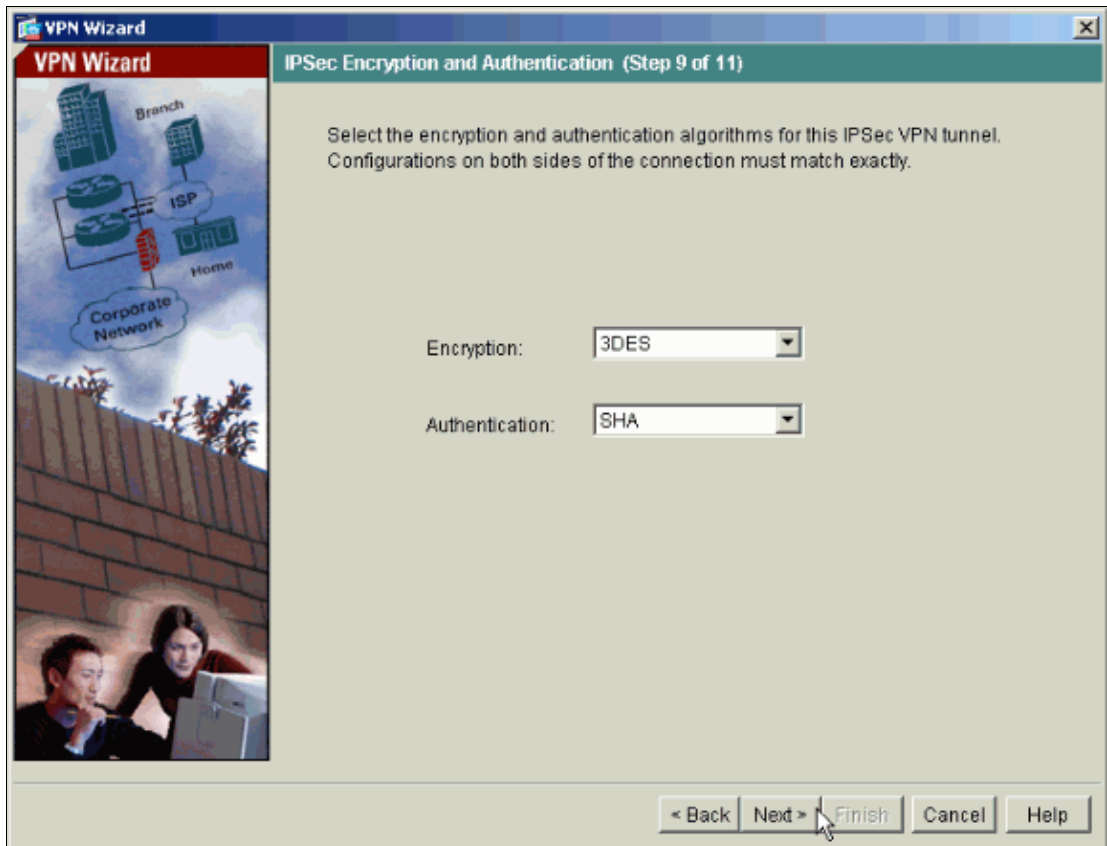
9. Specify the parameters for IKE, also known as IKE Phase 1.

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.



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

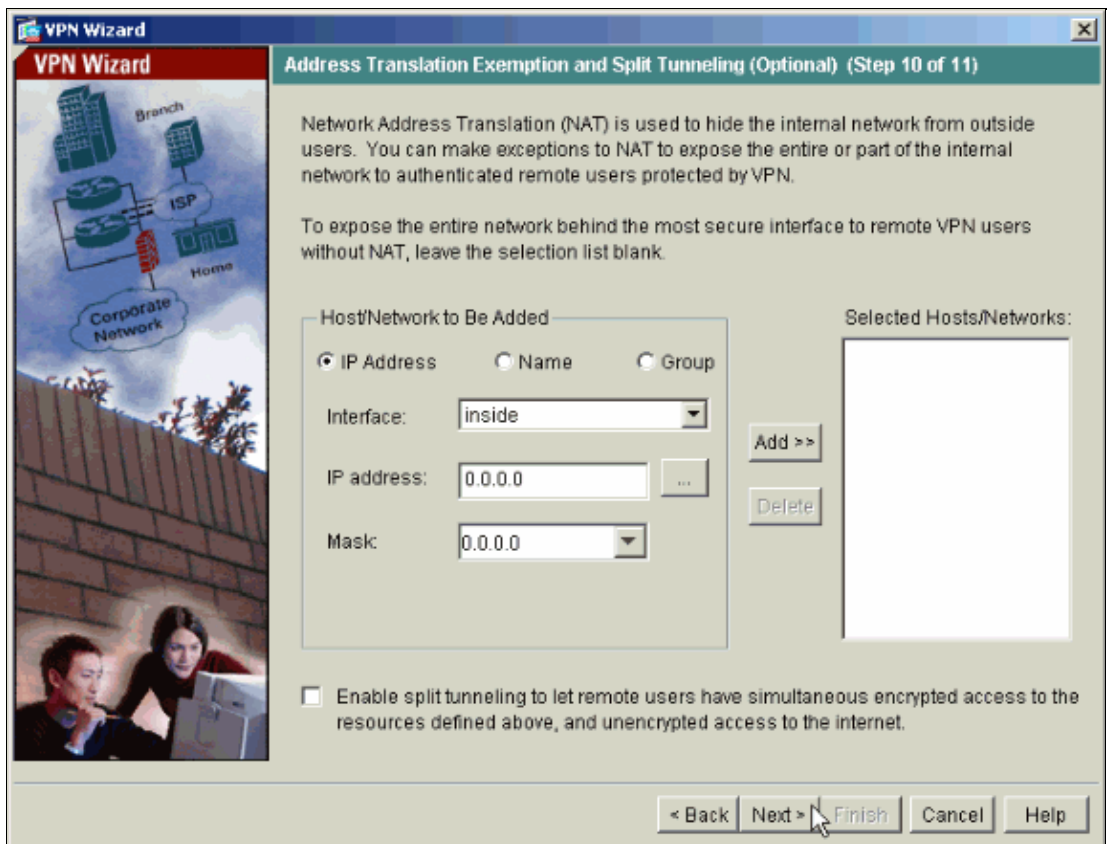
Configurations on both sides of the tunnel must match exactly. However, the Cisco VPN Client automatically selects the proper configuration for itself. Therefore, no IKE configuration is necessary on the client PC.



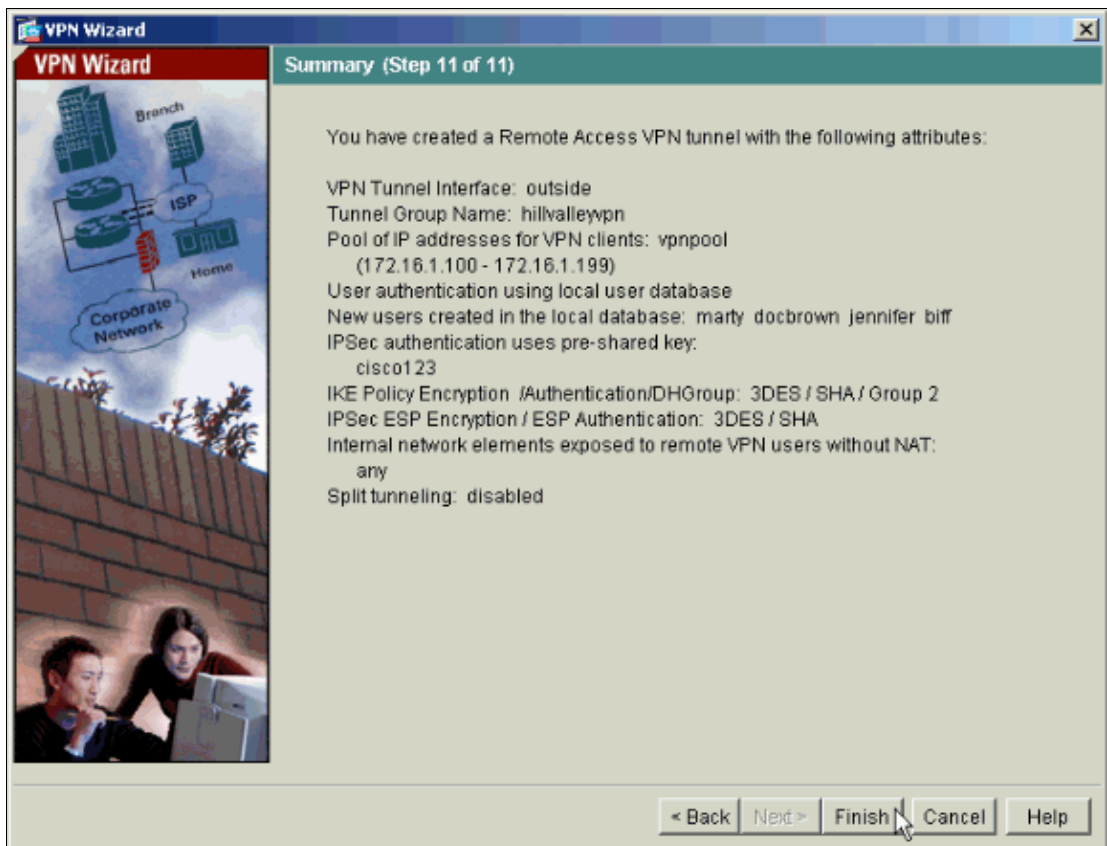
11. Specify which, if any, internal hosts or networks should be exposed to remote VPN users.

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.



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



Configure the ASA/PIX as a Remote VPN Server using CLI

Complete these steps in order to configure a remote VPN Access Server from the command line. Refer to Configuring Remote Access VPNs or Cisco ASA 5500 Series Adaptive Security Appliances–Command References for more information on each command that is used.

1. Enter the **ip local pool** command in global config mode in order to configure IP address pools to use for VPN remote access tunnels. In order to delete address pools, enter the no form of this command.

The security appliance uses address pools based on the tunnel group for the connection. If you configure more than one address pool for a tunnel group, the security appliance uses them in the order in which they are configured. Issue this command in order to create a pool of local addresses that can be used to assign dynamic addresses to remote-access VPN Clients:

```
ASA-AIP-CLI(config)#ip local pool vpnpool 172.16.1.100-172.16.1.199 mask
255.255.255.0
```

2. Issue this command:

```
ASA-AIP-CLI(config)#username marty password 12345678
```

3. Issue this set of commands in order to configure the specific tunnel:

- ◆ ASA-AIP-CLI(config)#**isakmp policy 1 authentication pre-share**
- ◆ ASA-AIP-CLI(config)#**isakmp policy 1 encryption 3des**
- ◆ ASA-AIP-CLI(config)#**isakmp policy 1 hash sha**
- ◆ ASA-AIP-CLI(config)#**isakmp policy 1 group 2**
- ◆ ASA-AIP-CLI(config)#**isakmp policy 1 lifetime 43200**
- ◆ ASA-AIP-CLI(config)#**isakmp enable outside**
- ◆ ASA-AIP-CLI(config)#**crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac**
- ◆ ASA-AIP-CLI(config)#**crypto dynamic-map outside_dyn_map 10 set transform-set ESP-3DES-SHA**
- ◆ ASA-AIP-CLI(config)#**crypto dynamic-map Outside_dyn_map 10 set reverse-route**
- ◆ ASA-AIP-CLI(config)#**crypto dynamic-map outside_dyn_map 10 set security-association lifetime seconds 288000**
- ◆ ASA-AIP-CLI(config)#**crypto map Outside_map 10 ipsec-isakmp dynamic Outside_dyn_map**
- ◆ ASA-AIP-CLI(config)#**crypto map outside_map interface outside**
- ◆ ASA-AIP-CLI(config)#**crypto isakmp nat-traversal**

4. *Optional:* If you would like the connection to bypass the access-list that is applied to the interface, issue this command:

```
ASA-AIP-CLI(config)#sysopt connection permit-ipsec
```

Note: This command works on 7.x images before 7.2(2). If you use image 7.2(2), issue the ASA-AIP-CLI(config)#**sysopt connection permit-vpn** command.

5. Issue this command:

```
ASA-AIP-CLI(config)#group-policy hillvalleyvpn internal
```

6. Issue these commands in order to configure client connection settings:

- ◆ ASA-AIP-CLI(config)#**group-policy hillvalleyvpn attributes**
- ◆ ASA-AIP-CLI(config)#(config-group-policy)#**dns-server value 172.16.1.11**
- ◆ ASA-AIP-CLI(config)#(config-group-policy)#**vpn-tunnel-protocol IPSec**
- ◆ ASA-AIP-CLI(config)#(config-group-policy)#**default-domain value test.com**

7. Issue this command:

```
ASA-AIP-CLI(config)#tunnel-group hillvalleyvpn ipsec-ra
```

8. Issue this command:

```
ASA-AIP-CLI(config)#tunnel-group hillvalleyvpn ipsec-attributes
```

9. Issue this command:

```
ASA-AIP-CLI(config-tunnel-ipsec)#pre-shared-key cisco123
```

10. Issue this command:

```
ASA-AIP-CLI(config)#tunnel-group hillvalleyvpn general-attributes
```

11. Issue this command in order to refer the local user database for authentication.

```
ASA-AIP-CLI(config-tunnel-general)#authentication-server-group LOCAL
```

12. Associate the group policy with the tunnel group

```
ASA-AIP-CLI(config-tunnel-ipsec)# default-group-policy hillvalleyvpn
```

13. Issue this command while in the general-attributes mode of the hillvalleyvpn tunnel-group in order to assign the vpnpool created in step 1 to the hillvalleyvpn group.

```
ASA-AIP-CLI(config-tunnel-general)#address-pool vpnpool
```

Running Config on the ASA Device

```
ASA-AIP-CLI(config)#show running-config  
ASA Version 7.2(2)  
!  
hostname ASAwAIP-CLI  
domain-name corp.com  
enable password WwXYvtKrnjXqGbul encrypted  
names  
!  
interface Ethernet0/0  
 nameif Outside  
 security-level 0  
 ip address 10.10.10.2 255.255.255.0  
!  
interface Ethernet0/1  
 nameif inside  
 security-level 100  
 ip address 172.16.1.2 255.255.255.0  
!  
interface Ethernet0/2  
 shutdown  
 no nameif  
 no security-level  
 no ip address  
!  
interface Ethernet0/3  
 shutdown  
 no nameif  
 no security-level  
 no ip address  
!  
interface Management0/0  
 shutdown  
 no nameif  
 no security-level  
 no ip address  
!  
passwd 2KFQnbNIdI.2KYOU encrypted
```

```
ftp mode passive
dns server-group DefaultDNS
  domain-name corp.com
pager lines 24
mtu Outside 1500
mtu inside 1500
ip local pool vpnpool 172.16.1.100-172.16.1.199 mask 255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
group-policy hillvalleyvpn1 internal
group-policy hillvalleyvpn1 attributes
  dns-server value 172.16.1.11
  vpn-tunnel-protocol IPSec
  default-domain value test.com
username marty password 6XmYwQ009tiYnUDN encrypted
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto dynamic-map Outside_dyn_map 10 set transform-set ESP-3DES-SHA
crypto dynamic-map outside_dyn_map 10 set security-association lifetime seconds 288000
crypto map Outside_map 10 ipsec-isakmp dynamic Outside_dyn_map
crypto map Outside_map interface Outside
crypto isakmp enable Outside
crypto isakmp policy 10
  authentication pre-share
  encryption 3des
  hash sha
  group 2
  lifetime 86400
crypto isakmp nat-traversal 20
tunnel-group hillvalleyvpn type ipsec-ra
tunnel-group hillvalleyvpn general-attributes
  address-pool vpnpool
  default-group-policy hillvalleyvpn
tunnel-group hillvalleyvpn ipsec-attributes
  pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
```

```
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:0f78ee7ef3c196a683ae7a4804ce1192
: end
ASA-AIP-CLI(config)#
```

Cisco VPN Client Password Storage Configuration

If you have numerous Cisco VPN Clients, it is very hard to remember all the VPN Client usernames and passwords. In order to store the passwords in the VPN Client machine, configure the ASA/PIX and the VPN Client as this section describes.

ASA/PIX

Use the **group-policy attributes** command in global configuration mode:

```
group-policy VPNusers attributes
password-storage enable
```

Cisco VPN Client

Edit the **.pcf file** and modify these parameters:

```
SaveUserPassword=1
UserPassword= <type your password>
```

Disable the Extended Authentication

In tunnel group mode, enter this command in order to disable the extended authentication, which is enabled by default, on the PIX/ASA 7.x:

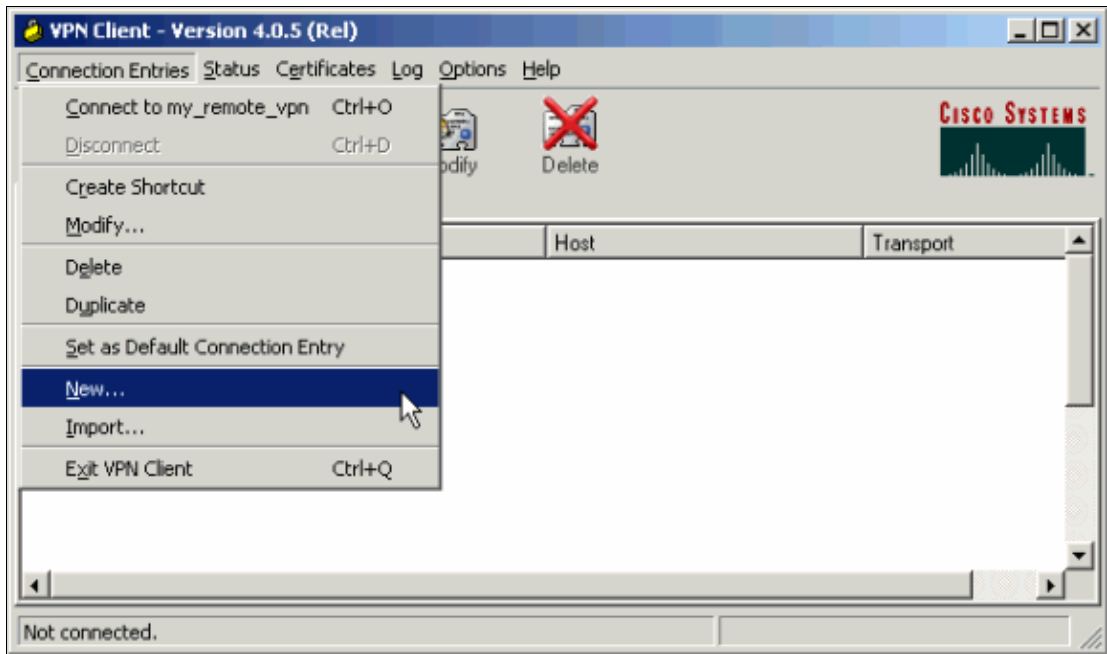
```
asa(config)#tunnel-group client ipsec-attributes
asa(config-tunnel-ipsec)#isakmp ikev1-user-authentication none
```

After you disable the extended authentication, the VPN Clients do not pop-up a username/password for an authentication (Xauth). Therefore, the ASA/PIX does not require the username and password configuration to authenticate the VPN Clients.

Verify

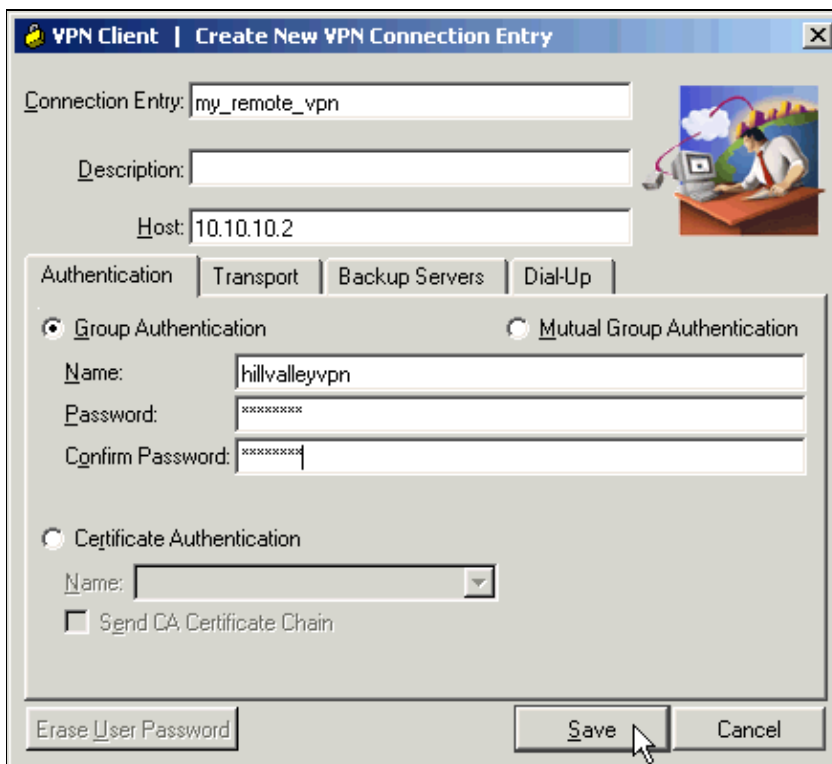
Attempt to connect to the Cisco ASA using the Cisco VPN Client in order to verify that the ASA is successfully configured.

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

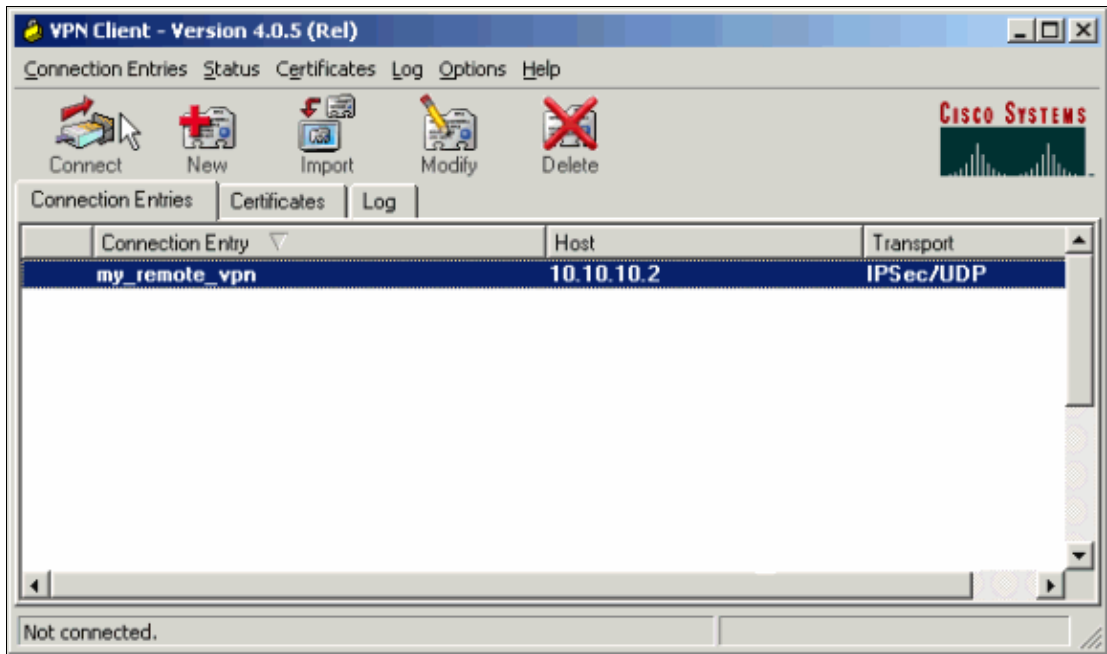


2. Fill in the details of your new connection.

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.



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

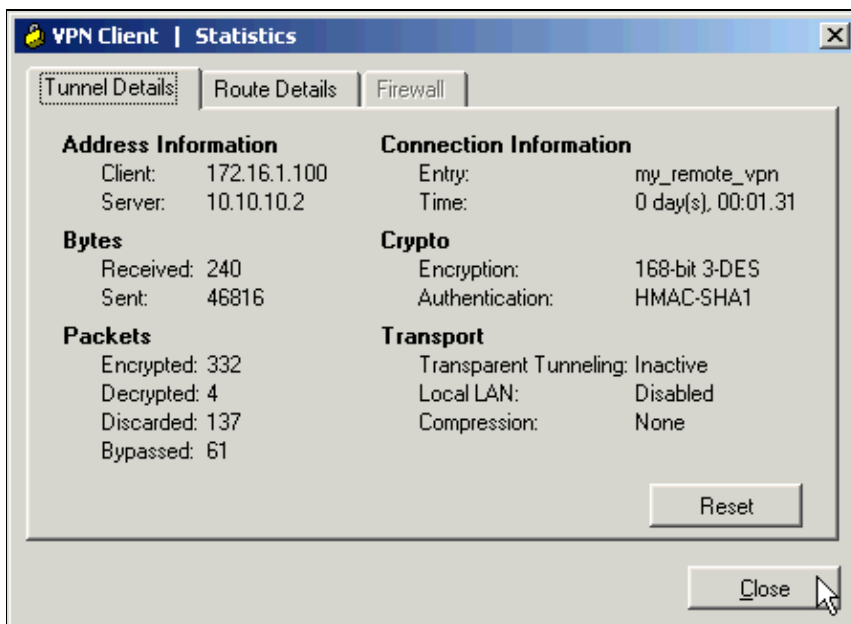


4. Enter a username and password for extended authentication. This information should match that specified in steps 5 and 6.

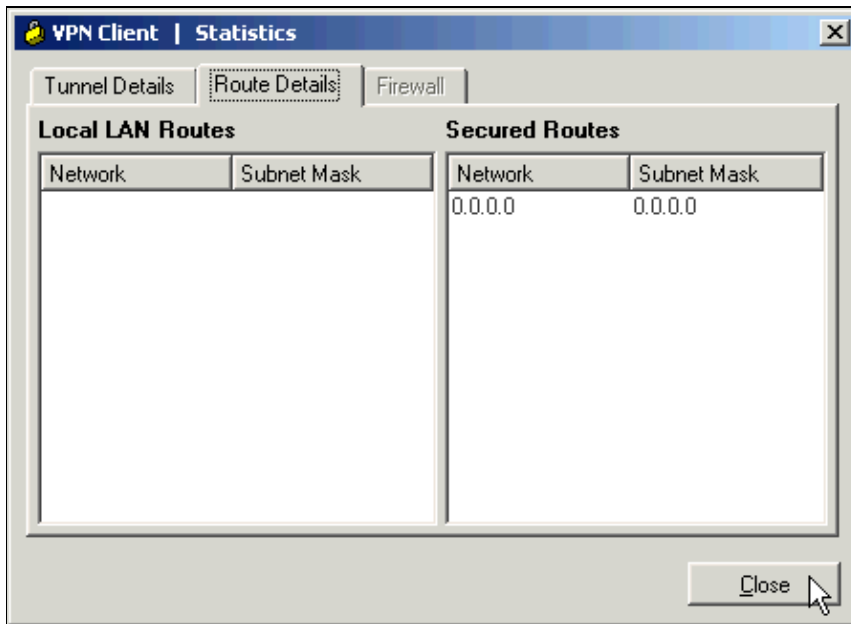


5. Once the connection is successfully established select **Statistics** from the Status menu to verify the details of the tunnel.

This window shows traffic and crypto information:



This window shows split tunneling information:



Troubleshoot

Use this section to troubleshoot your configuration.

Incorrect Crypto ACL

ASDM 5.0(2) is known to create and apply a crypto access control list (ACL) that can cause problems for VPN Clients that use split tunneling, as well as for hardware clients in network-extension mode. Use ASDM version 5.0(4.3) or later to avoid this problem. Refer to Cisco bug ID CSCsc10806 (registered customers only) for more details.

Related Information

- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Most Common L2L and Remote Access IPsec VPN Troubleshooting Solutions](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances Troubleshoot and Alerts](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Feb 25, 2008

Document ID: 68795
