

Cisco Router as a Remote VPN Server using SDM Configuration Example

Document ID: 70374

Introduction

Prerequisites

Requirements

Components Used

Conventions

Configure

Network Diagram

Configuration Procedure

Verify

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document describes how to use the Cisco Security Device Manager (SDM) to configure the Cisco router to act as an Easy VPN Server. Cisco SDM allows you to configure your router as a VPN server for the Cisco VPN Client using an easy-to-use Web-based management interface. Once the Cisco router configuration is complete, it can be verified using the Cisco VPN Client.

Prerequisites

Requirements

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

Note: Refer to Allowing HTTPS Access for SDM in order to allow the router to be configured by the SDM.

Components Used

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

- Cisco 3640 Router with Cisco IOS® Software Release 12.3(14T)
- Security Device Manager Version 2.31
- Cisco VPN Client Version 4.8

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.

Conventions

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

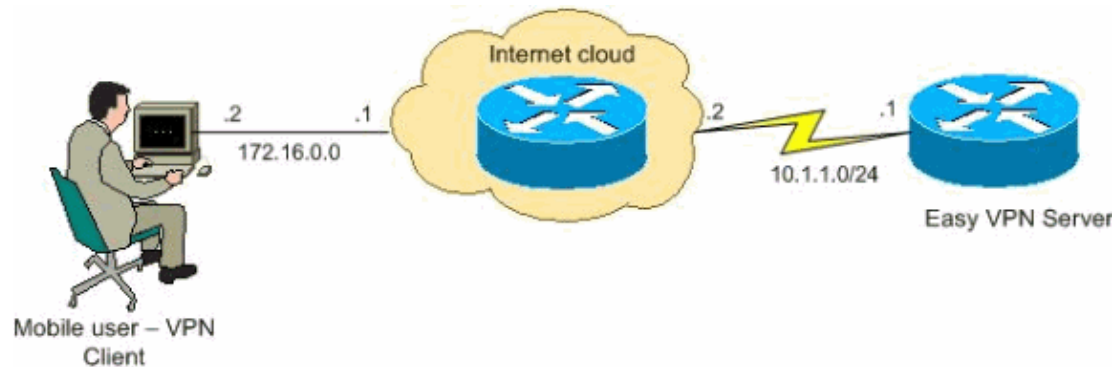
Configure

In this section, you are presented with the information to configure the Easy VPN Server feature which allows a remote end user to communicate using IPsec with any Cisco IOS® VPN gateway.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

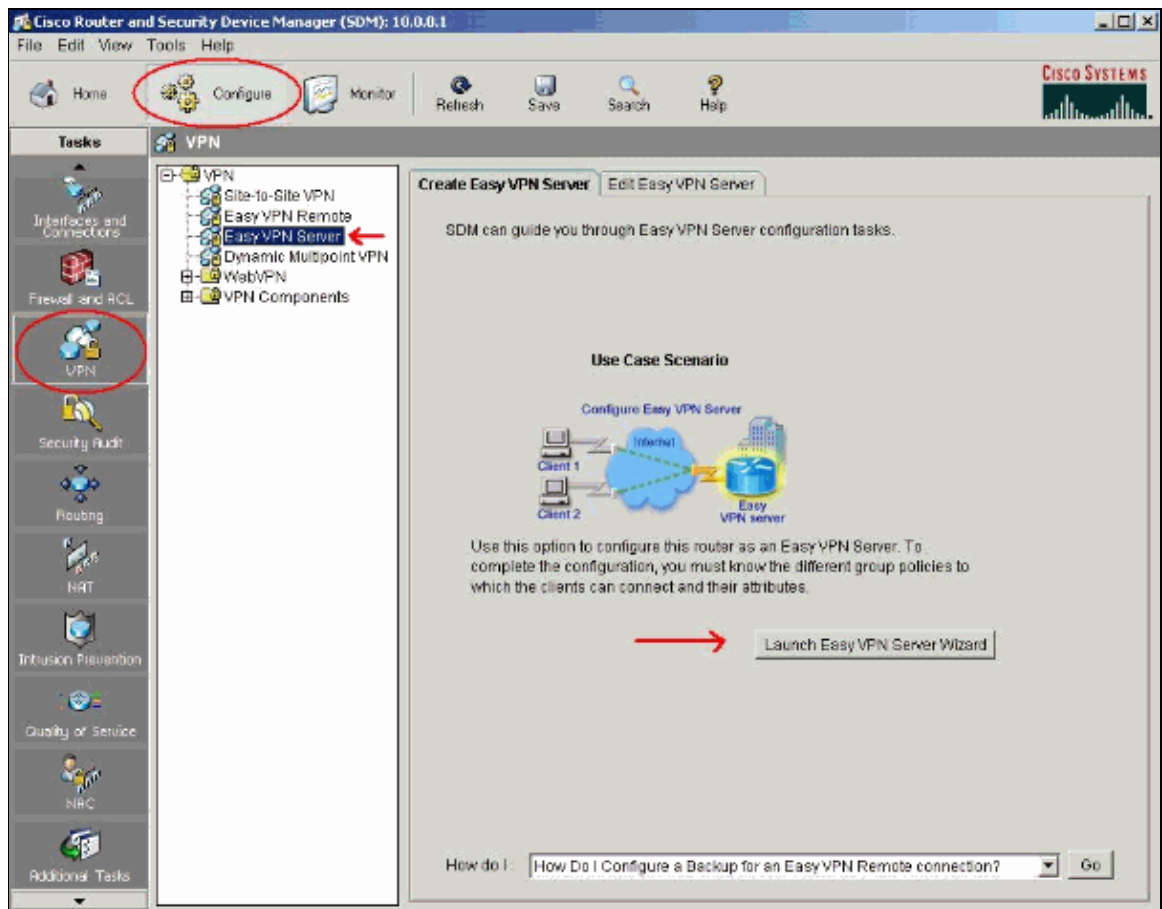
This document uses this network setup:



Configuration Procedure

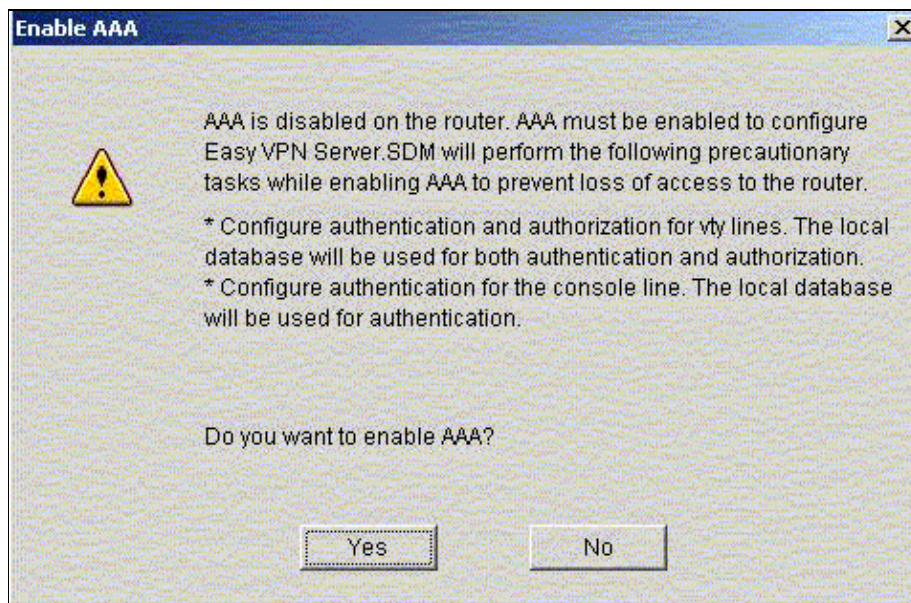
Complete these steps to configure the Cisco router as a remote VPN server using SDM.

1. Select **Configure > VPN > Easy VPN Server** from the Home window and click **Launch Easy VPN Server Wizard**.

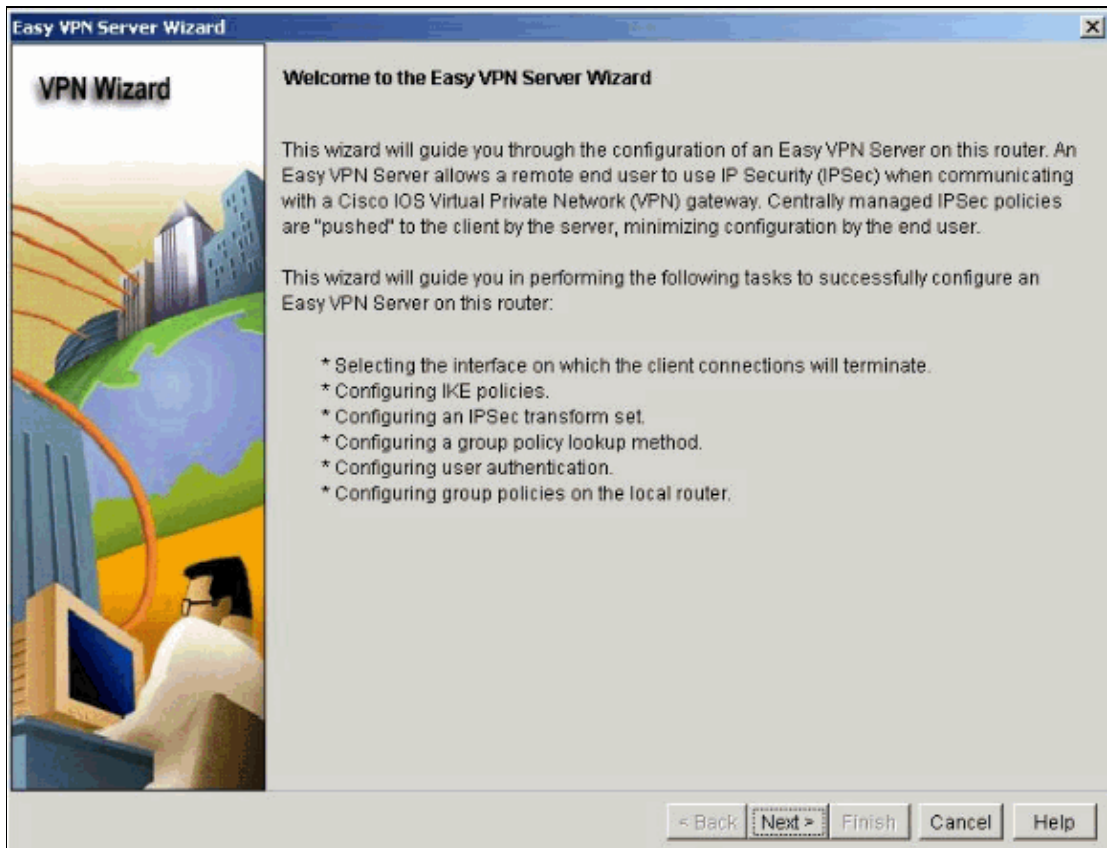


2. AAA must be enabled on the router before the Easy VPN Server configuration starts. Click **Yes** to continue with the configuration.

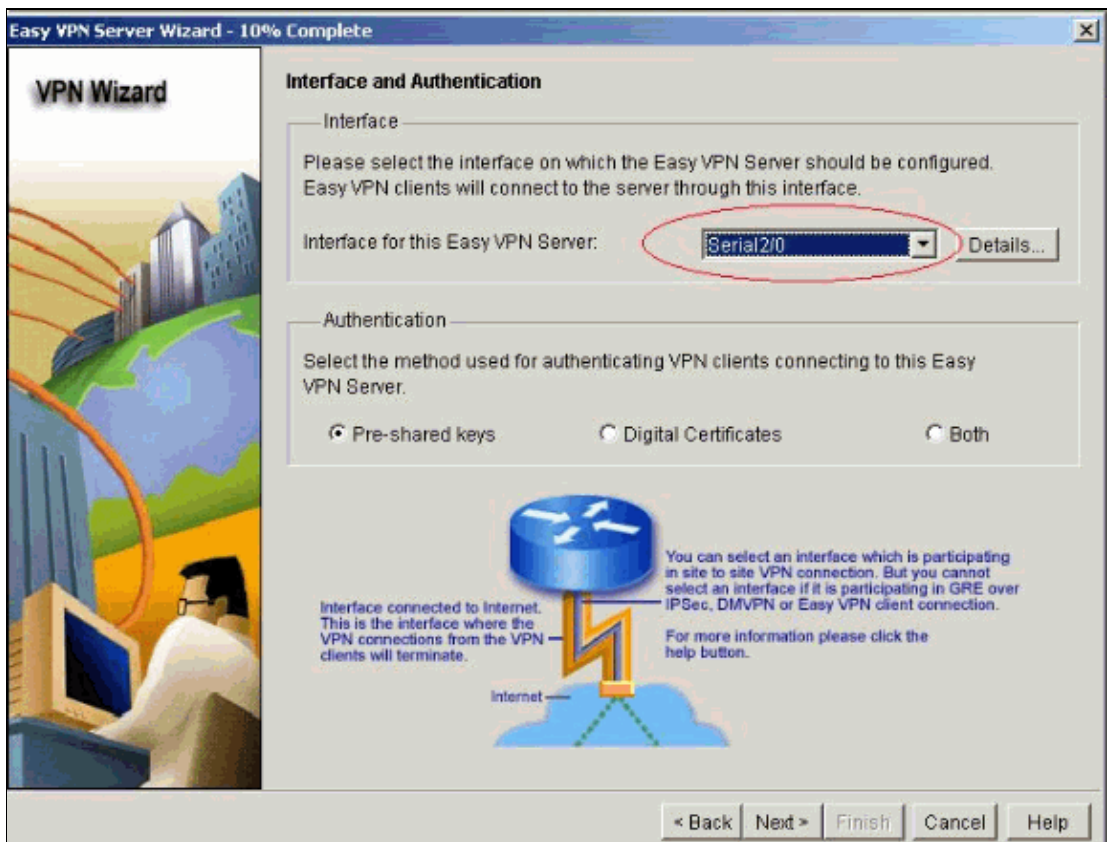
The 'AAA has been successfully enabled on the router' message displays on the window. Click **OK** to start the Easy VPN Server configuration.



3. Click **Next** to start the Easy VPN Server Wizard.

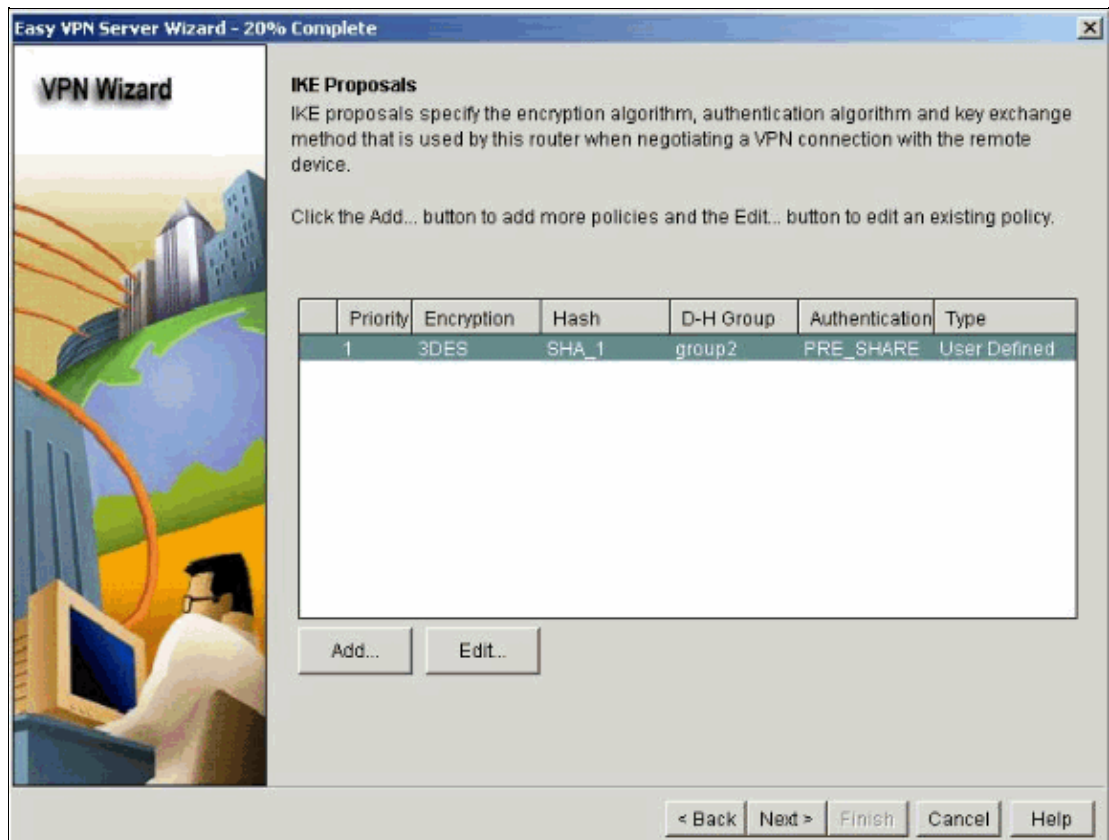


4. Select the interface on which the client connections terminate and the authentication type.

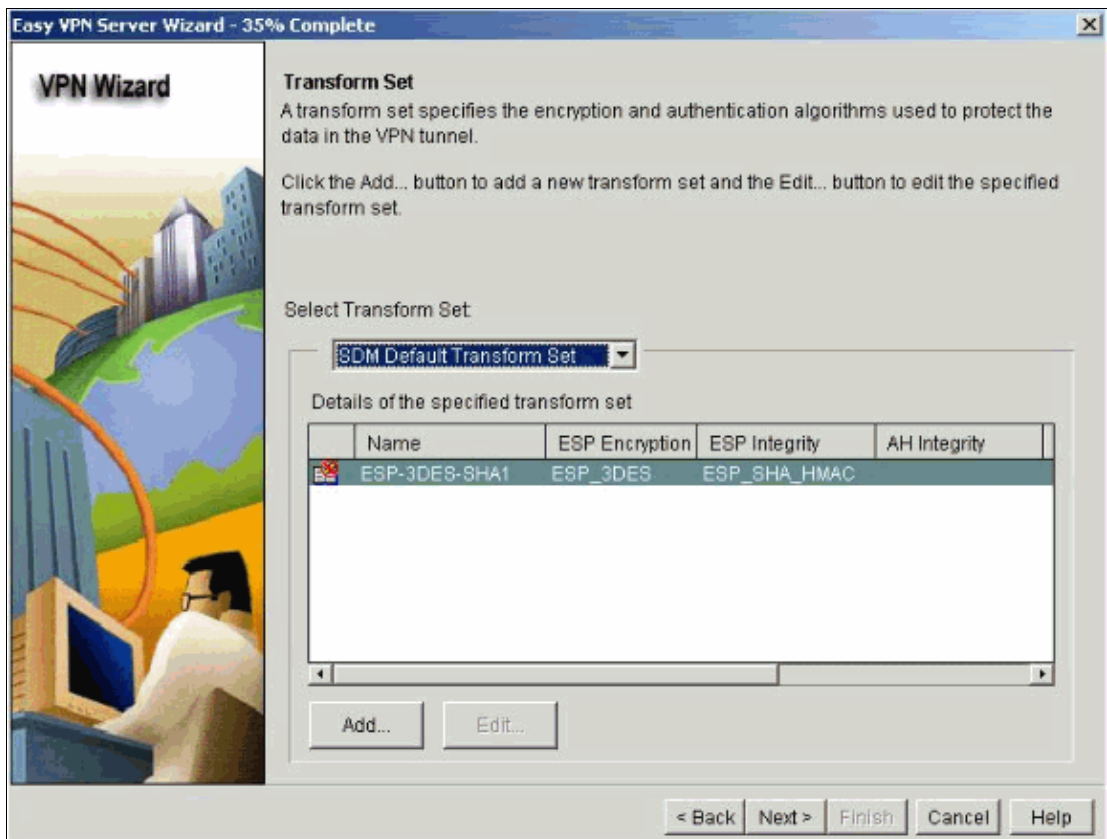


5. Click **Next** to configure the Internet Key Exchange (IKE) policies and use the **Add** button to create the new policy.

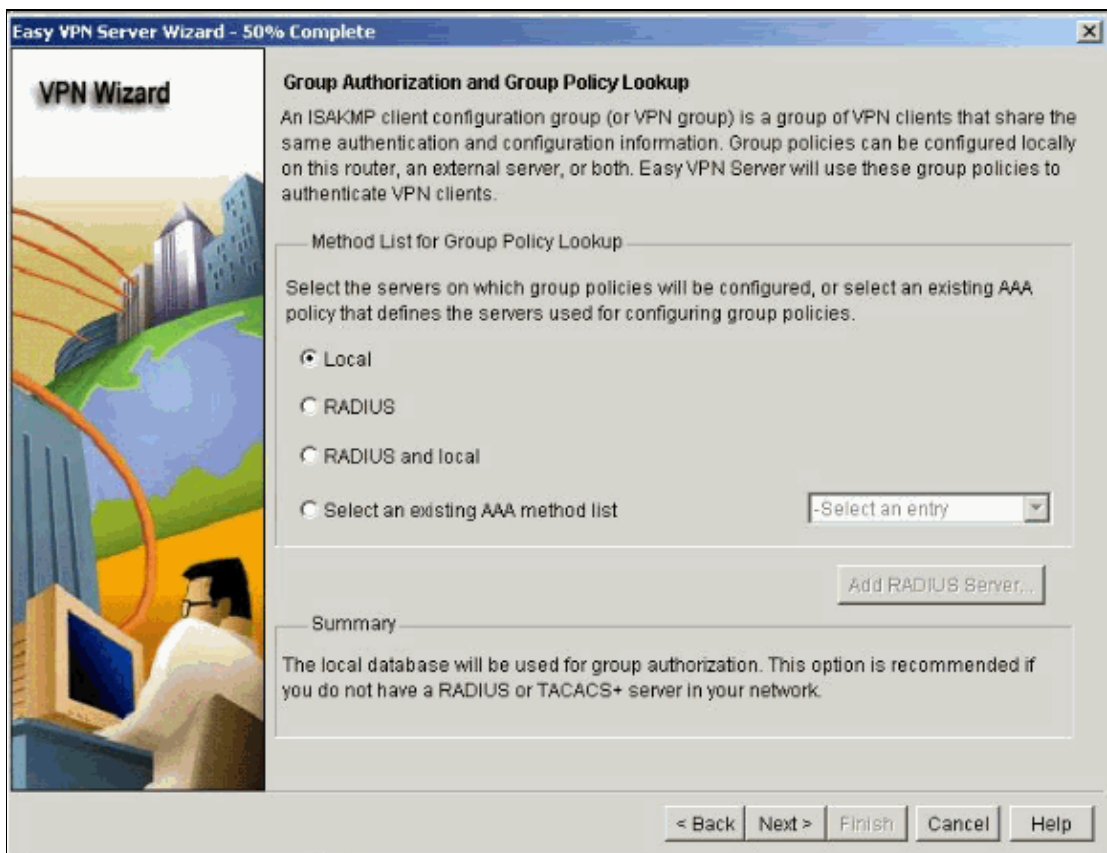
Configurations on both sides of the tunnel must match exactly. However, the Cisco VPN Client automatically selects the proper configuration for itself. Therefore, no IKE configuration is necessary on the client PC.



6. Click **Next** to choose the default transform set or add the new transform set to specify the encryption and authentication algorithm. In this case, the default transform set is used.

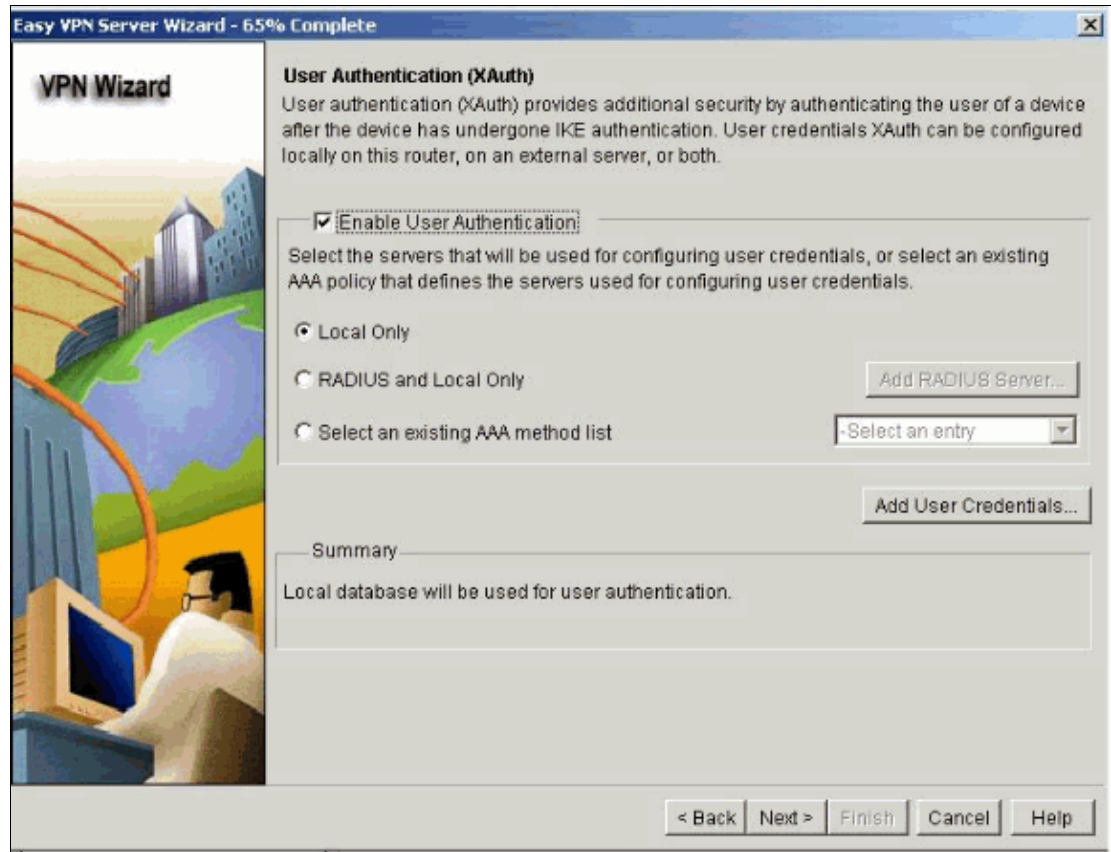


- Click **Next** to create a new Authentication, Authorization, and Accounting (AAA) authorization network method list for group policy lookup or to choose an existing network method list used for group authorization.



- Configure user authentication on the Easy VPN Server.

You can store user authentication details on an external server such as a RADIUS server or a local database or on both. An AAA login authentication method list is used to decide the order in which user authentication details should be searched.



Easy VPN Server Wizard - 65% Complete

VPN Wizard

User Authentication (XAuth)
User authentication (XAuth) provides additional security by authenticating the user of a device after the device has undergone IKE authentication. User credentials XAuth can be configured locally on this router, on an external server, or both.

☒ **Enable User Authentication:**

Select the servers that will be used for configuring user credentials, or select an existing AAA policy that defines the servers used for configuring user credentials.

☒ Local Only

☐ RADIUS and Local Only Add RADIUS Server...

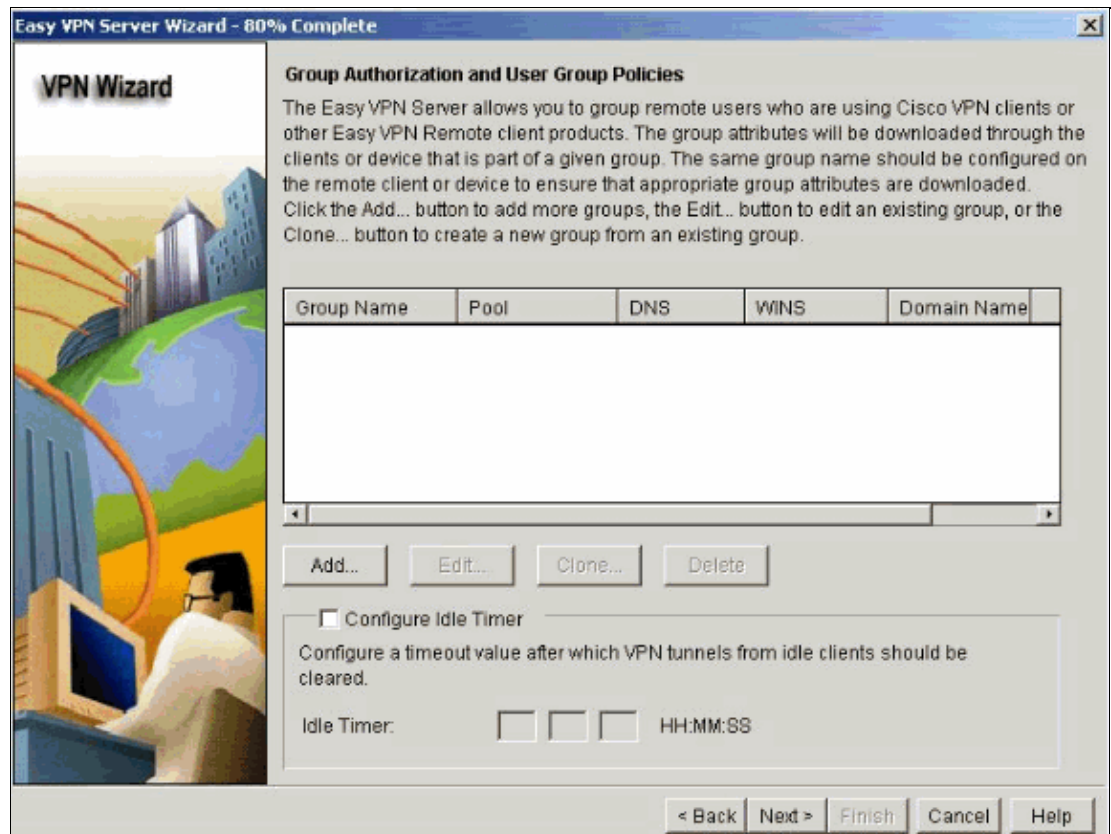
☐ Select an existing AAA method list -Select an entry

Add User Credentials...

Summary
Local database will be used for user authentication.

< Back Next > Finish Cancel Help

9. This window allows you to add, edit, clone, or delete user group policies on the local database.



Easy VPN Server Wizard - 80% Complete

VPN Wizard

Group Authorization and User Group Policies
The Easy VPN Server allows you to group remote users who are using Cisco VPN clients or other Easy VPN Remote client products. The group attributes will be downloaded through the clients or device that is part of a given group. The same group name should be configured on the remote client or device to ensure that appropriate group attributes are downloaded. Click the Add... button to add more groups, the Edit... button to edit an existing group, or the Clone... button to create a new group from an existing group.

Group Name	Pool	DNS	WINS	Domain Name

Add... Edit... Clone... Delete

☐ **Configure Idle Timer**
Configure a timeout value after which VPN tunnels from idle clients should be cleared.

Idle Timer: HH:MM:SS

< Back Next > Finish Cancel Help

10. Enter a name for the Tunnel Group Name. Supply the pre-shared key used for authentication information.

Create a new pool or select an existing pool used to allocate the IP addresses to the VPN Clients.

The screenshot shows the 'Add Group Policy' dialog box with the 'General' tab selected. The 'Name of This Group' field contains 'vpn'. The 'Pre-shared keys' section has a 'Current Key' of '<None>' and two masked input fields for 'Enter new pre-shared key' and 'Reenter new pre-shared key'. The 'Pool Information' section is checked, and the 'Create a new pool' radio button is selected. The 'Starting IP address' is '192.168.2.1' and the 'Ending IP address' is '192.168.2.5'. The 'Subnet Mask' is '255.255.255.0' (Optional). The 'Maximum Connections Allowed' field is empty. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Add Group Policy

General | DNS/WWW | Split Tunneling | Client Settings | XAuth Options

Name of This Group:

Pre-shared keys

Specify the key that will be used to authenticate the clients associated with this group.

Current Key:

Enter new pre-shared key:

Reenter new pre-shared key:

☒ **Pool Information**

Specify a local pool containing a range of addresses that will be used to allocate an internal IP address to a client.

☒ Create a new pool ☐ Select from an existing pool

Starting IP address:

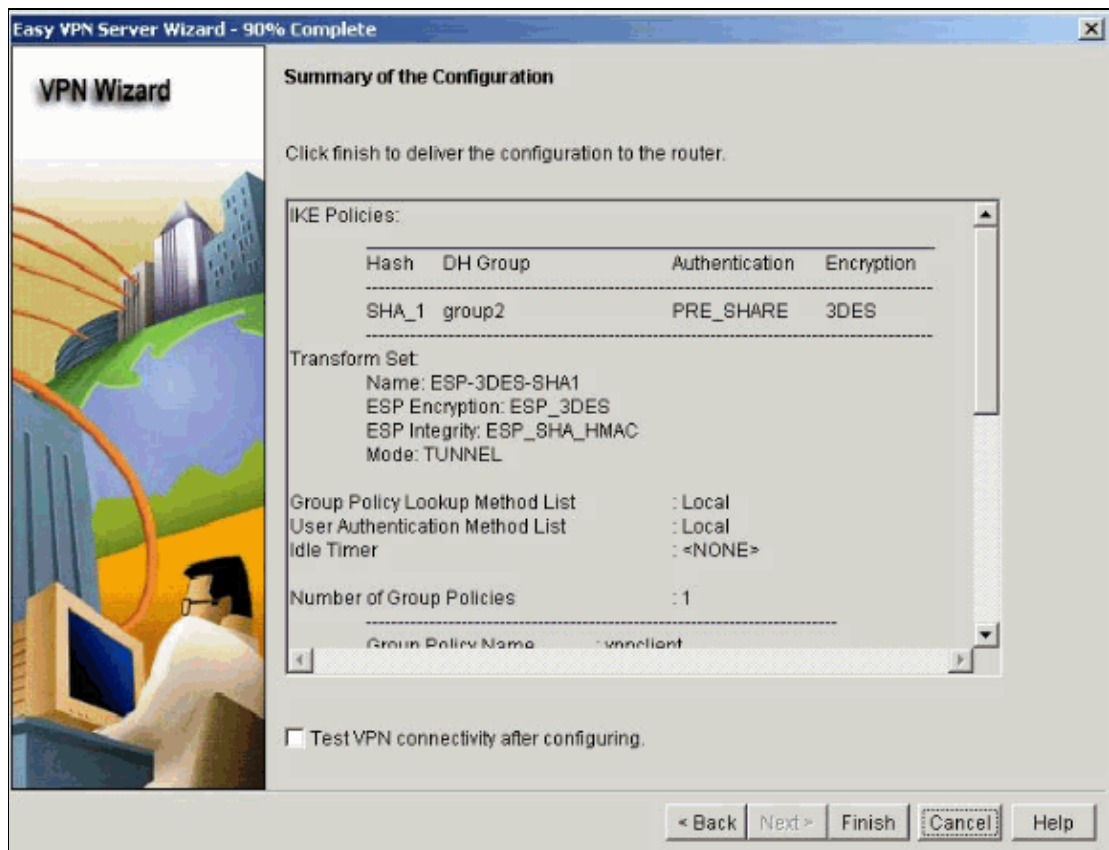
Ending IP address:

Enter the subnet mask that should be sent to the client along with the IP address.

Subnet Mask: (Optional)

Maximum Connections Allowed:

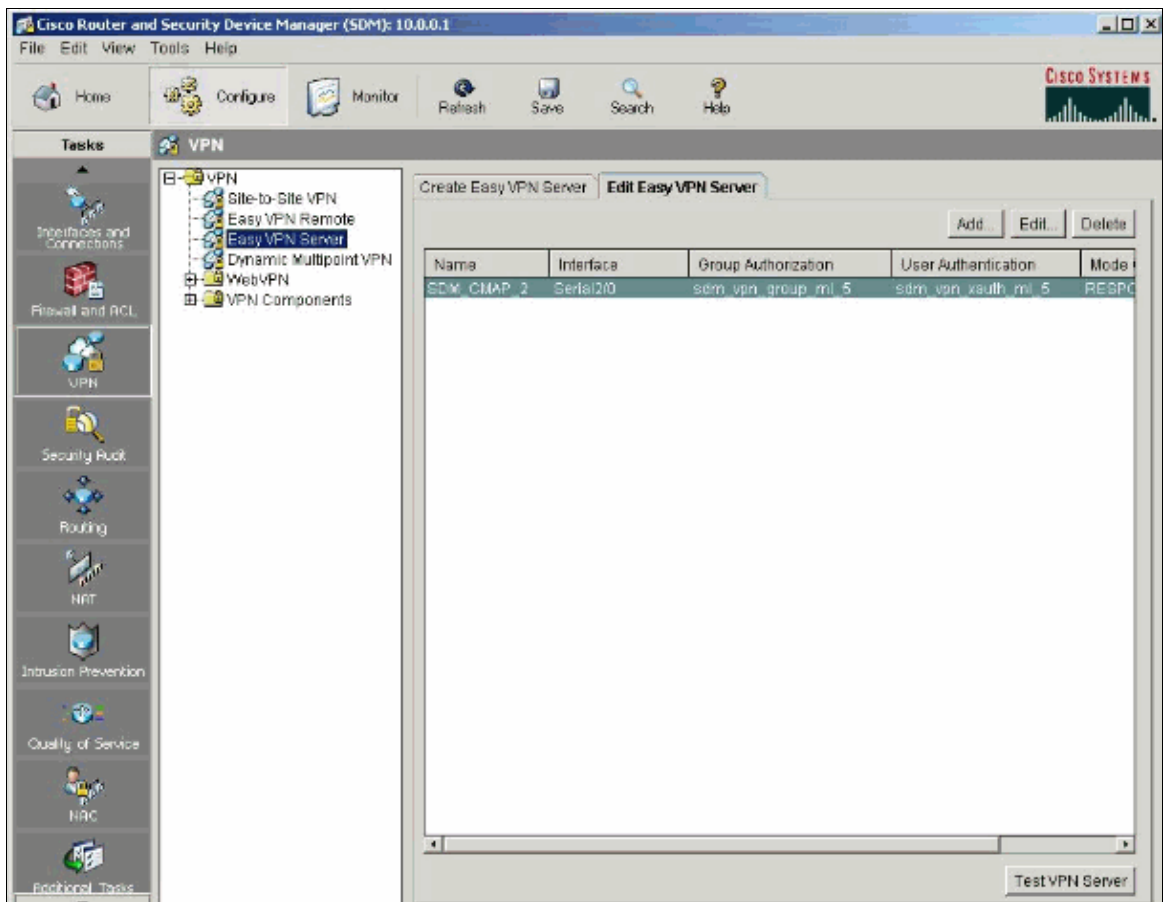
11. This window shows a summary of the actions that you have taken. Click **Finish** if you are satisfied with your configuration.



12. The SDM sends the configuration to the router to update the running configuration. Click **OK** to complete.



13. After completion, you can edit and modify the changes in the configuration, if needed.



Router Configuration (VPN Server)

Building configuration...

Current configuration : 3336 bytes

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
aaa new-model
!
!---- In order to set AAA authentication at login, use the aaa authentication login
!---- command in global configuration mode
.
aaa authentication login default local

!---- Here, list name "sdm_vpn_xauth_ml_1" is specified for
!---- the authentication of the clients.

aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authorization exec default local
aaa authorization network sdm_vpn_group_ml_1 local
!
aaa session-id common
```

```

!
resource policy
!
!
!
ip cef
!
!
!
!
!---- The RSA certificate generates after the
!---- ip http secure-server command is enabled.

crypto pki trustpoint TP-self-signed-392370502
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-392370502
  revocation-check none
  rsakeypair TP-self-signed-392370502
!
!
crypto pki certificate chain TP-self-signed-392370502
  certificate self-signed 01
    3082023C 308201A5 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
    30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
    69666963 6174652D 33393233 37303530 32301E17 0D303530 39323130 30323135
    375A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
    532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3339 32333730
    35303230 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
    ED61BD43 0AD90559 2C7D7DB1 BB3147AA 784F3B46 9E63E63C 5CD61976 6BC46596
    DB1AEB44 46644B18 8A890604 489B0447 B4B5C702 98272464 FFFD5511 A4BA79EC
    239BCEA2 823F94EE 438B2E0A 5D90E9ED 8158BC8D 04F67C21 AEE1DB6F 046A0EF3
    4C8798BE 0A171421 3FD5A690 7C735751 E7C58AA3 FB4CCE4F 5930212D 90EB4A33
    02030100 01A36630 64300F06 03551D13 0101FF04 05300301 01FF3011 0603551D
    11040A30 08820652 6F757465 72301F06 03551D23 04183016 8014B278 183F02DF
    5000A124 124FEF08 8B704656 15CD301D 0603551D 0E041604 14B27818 3F02DF50
    00A12412 4FEF088B 70465615 CD300D06 092A8648 86F70D01 01040500 03818100
    C12AB266 0E85DAF6 264AC86F 27761351 E31DF628 BE7792B2 991725ED AAB3BABE
    B1F1C6CA 7E5C0D19 B9793439 E5AEC78 C5ECBE56 871EB4D3 39B60AD1 AB0B97FE
    515B4CC6 81BEE802 DC02BD1B A0D10EE9 0FD79D72 B44C0143 6E39C06B D9178590
    57D02A8F 750DA100 ABEEB1F1 B02A8B1F B746942B 892D1514 B2CC9D58 A28F08E2
  quit
!
!
!
!
!
!
!
!
!
!
!---- Creates a user account with all privileges.

username sdmsdm privilege 15 password 0 sdmsdm
!
!

!---- Creates an isakmp policy 1 with parameters like
!---- 3des encryption, pre-share key authentication, and DH group 2.

crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2

```

```

crypto isakmp client configuration group vpn

!--- Defines the pre-shared key as sdmsdm.

key sdmsdm
 pool SDM_POOL_1
 netmask 255.255.255.0
!

!--- Defines transform set parameters.

crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
!
crypto dynamic-map SDM_DYNMAP_1 1
 set transform-set ESP-3DES-SHA
 reverse-route
!

!--- Specifies the crypto map parameters.

crypto map SDM_CMAP_1 client authentication list sdm_vpn_xauth_ml_1
crypto map SDM_CMAP_1 isakmp authorization list sdm_vpn_group_ml_1
crypto map SDM_CMAP_1 client configuration address respond
crypto map SDM_CMAP_1 65535 ipsec-isakmp dynamic SDM_DYNMAP_1
!
!
!
!
interface Ethernet0/0
 no ip address
 shutdown
 half-duplex
!
interface FastEthernet1/0
 ip address 10.77.241.157 255.255.255.192
 duplex auto
 speed auto
!
interface Serial2/0
 ip address 10.1.1.1 255.255.255.0
 no fair-queue

!--- Applies the crypto map SDM_CMAP1 to the interface.

crypto map SDM_CMAP_1
!
interface Serial2/1
 no ip address
 shutdown
!
interface Serial2/2
 no ip address
 shutdown
!
interface Serial2/3
 no ip address
 shutdown

!--- Creates a local pool named SDM_POOL_1 for issuing IP
!--- addresses to clients.

ip local pool SDM_POOL_1 192.168.2.1 192.168.2.5

!--- Commands for enabling http and https required to launch SDM.

ip http server

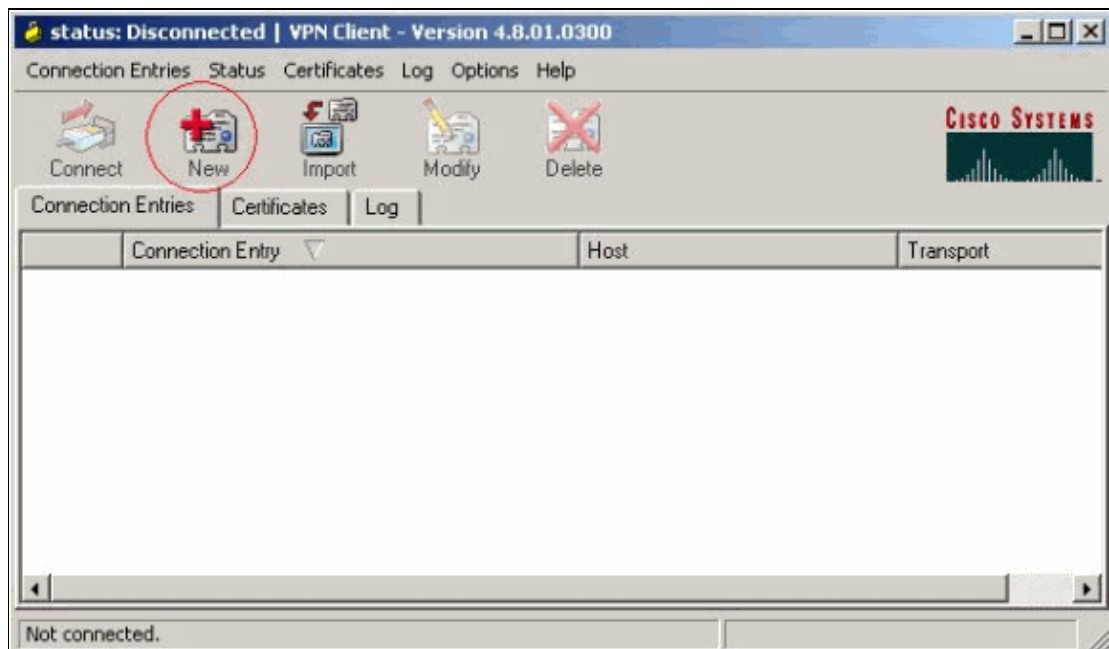
```

```
ip http secure-server
!  
!  
!  
!  
!  
control-plane  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
line con 0  
line aux 0  
line vty 0 4  
    password cisco  
!  
!  
end
```

Verify

Attempt to connect to the Cisco router using the Cisco VPN Client in order to verify that the Cisco router 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 tunnel end point of the Easy VPN Server (Cisco router). The Group Authentication information should correspond to that used in step 9. Click **Save** when you are finished.

VPN Client | Properties for "vpn"

Connection Entry:

Description:

Host:

Authentication | Transport | Backup Servers | Dial-Up

☒ Group Authentication ☐ Mutual Group Authentication

Name:

Password:

Confirm Password:

☐ Certificate Authentication

Name:

☐ Send CA Certificate Chain

Erase User Password Save Cancel

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

status: Disconnected | VPN Client - Version 4.8.01.0300

Connection Entries | Status | Certificates | Log | Options | Help

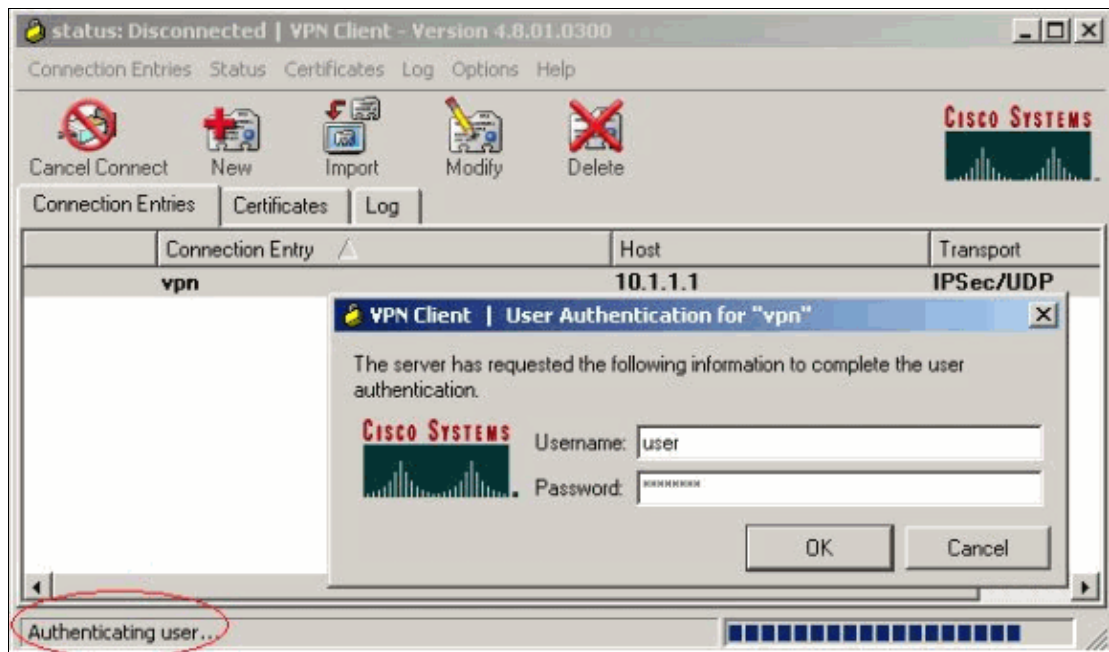
Connect New Import Modify Delete

Connection Entries | Certificates | Log

Connection Entry	Host	Transport
vpn	10.1.1.1	IPSec/UDP

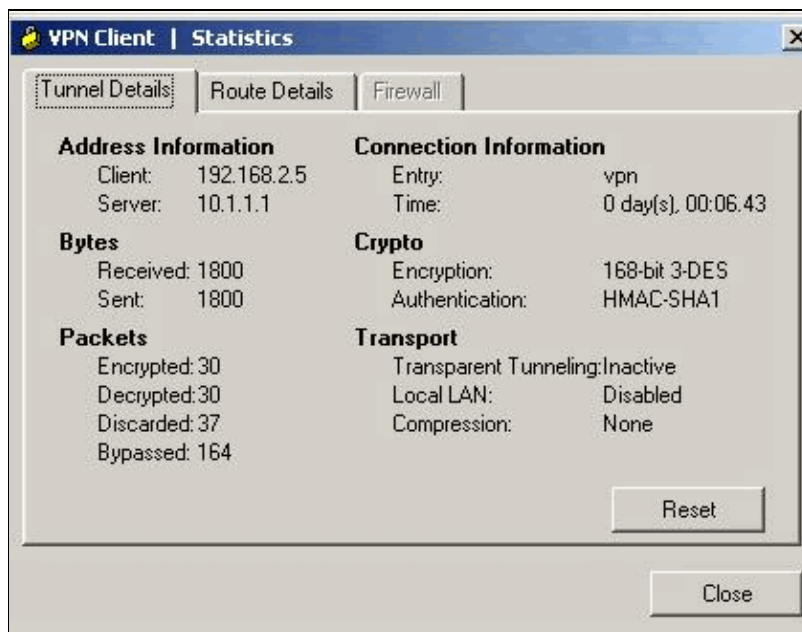
Not connected.

4. Enter a username and password for extended authentication (Xauth). This information is determined by the Xauth parameters in step 7.

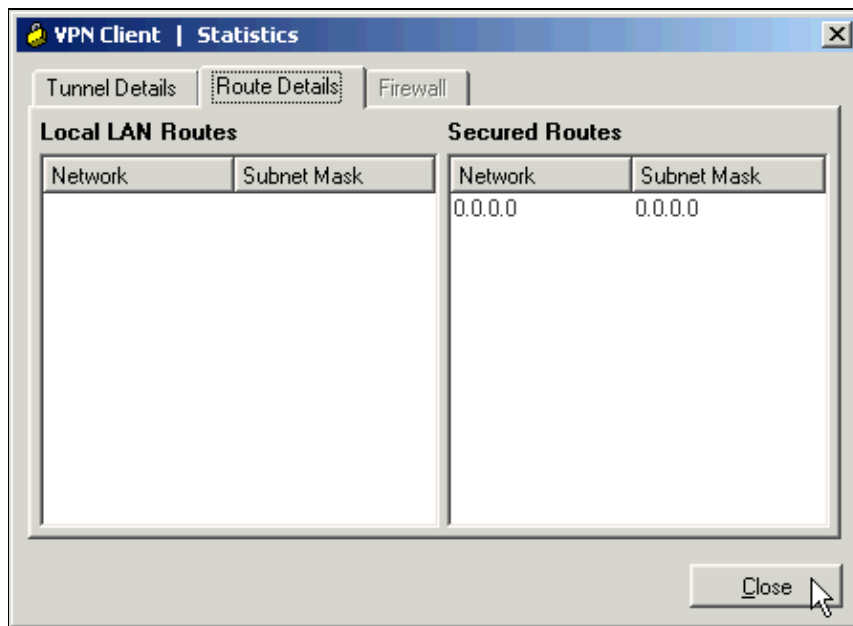


5. Once the connection is successfully established select **Statistics** from the Status menu to verify the details of the tunnel.

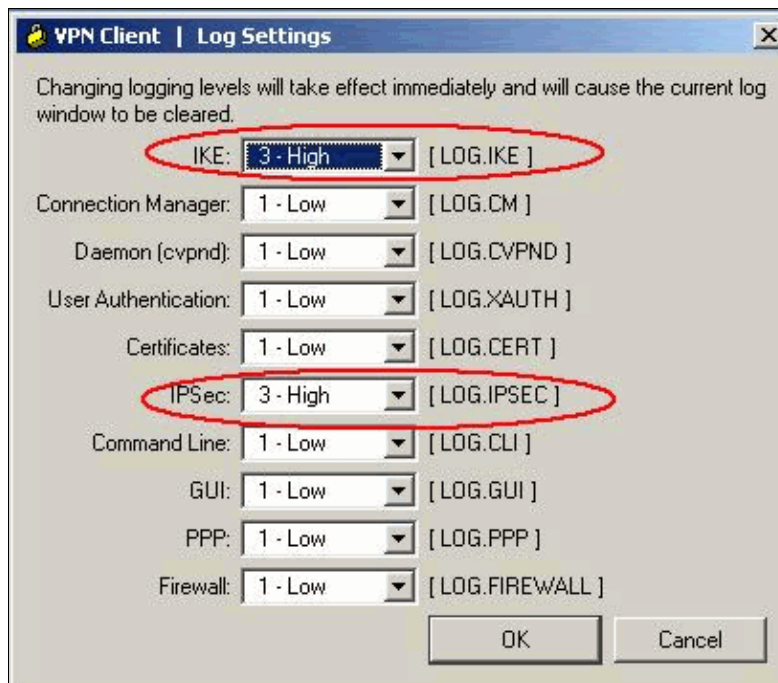
This window shows traffic and crypto information:



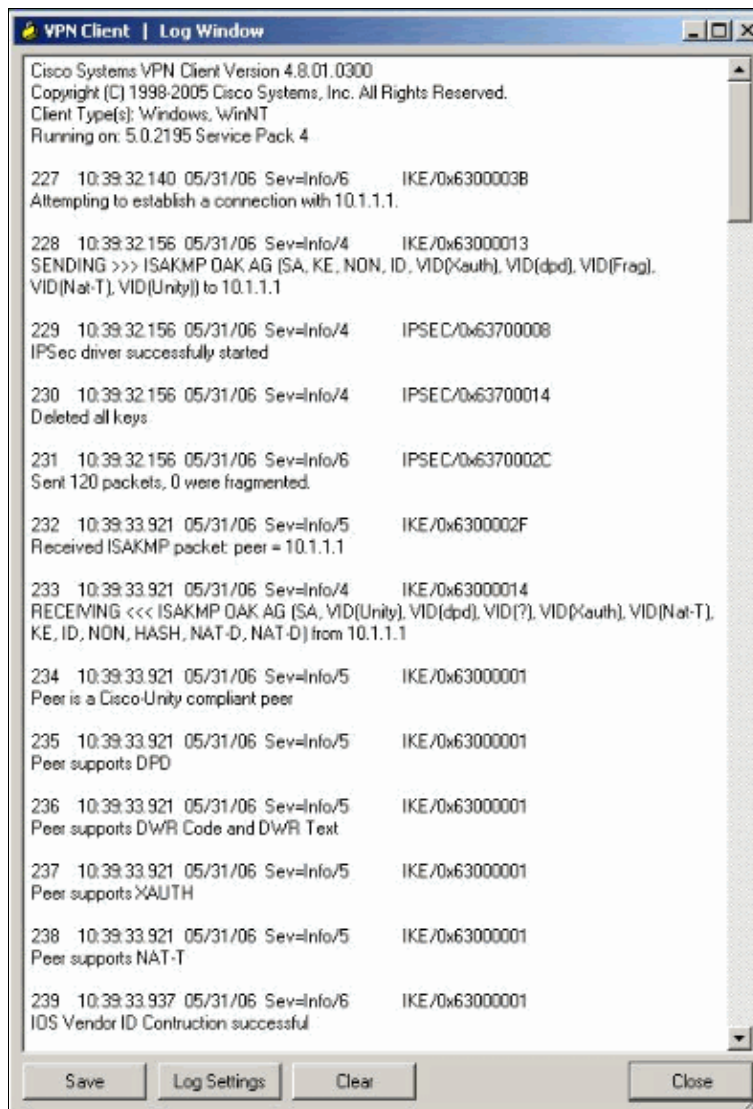
This window shows split tunneling information if configured:



6. Select **Log > Log Settings** to enable the log levels in the Cisco VPN Client.



7. Select **Log > Log Windows** to view the log entries in the Cisco VPN Client.



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

- [Downloading and Installing Cisco Router and Security Device Manager](#)
- [Cisco VPN Client Support Page](#)
- [IPsec Negotiation/IKE Protocols](#)
- [Technical Support & Documentation – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Sep 07, 2006

Document ID: 70374
