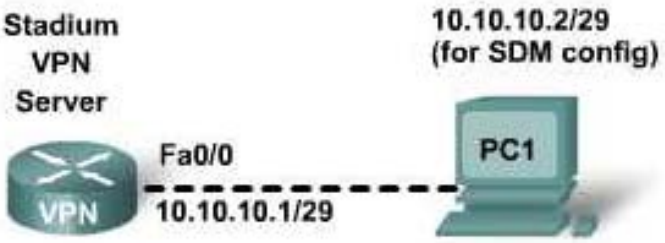
# Lab 8.3.4.3 Creating a Cisco EasyVPN Server (Optional Lab)





## Objectives

- Configure basic router global settings using IOS for SDM access.
- Configure EasyVPN Server using SDM on a Cisco router.

## 640-802 CCNA Exam Objective

This lab contains skills that relate to the following CCNA exam objective:

- Describe VPN technology (including: importance, benefits, role, impact, components).

## Expected Results and Success Criteria

Before starting this lab, read through the tasks that you are expected to perform. What do you expect the result of performing these tasks will be?

_____

_____

_____

How is the ability to create a VPN server important in network design and prototyping?

_____

_____

## Background / Preparation

In this lab you will configure a Cisco 1841 router as a VPN server using the SDM graphical user interface and the EasyVPN Server Wizard. This router will simulate the VPN server in the Stadium network prototype for remote worker access. The router will provide the endpoint for an IPSec VPN tunnel for VPN clients. You will test the VPN configuration using the built-in test options according to the test plan outlined previously in Lab 8.3.2.

**NOTE:** Even if the equipment is not available to actually perform this lab, you should read through it to get a better understanding of how VPNs function.

The following resources are required:

- Cisco 1841 router with IOS 12.4 Advanced IP Services IOS image, a Virtual Private Network (VPN) Module, and SDM version 2.4 installed
- Windows XP computer with Internet Explorer 5.5 or higher and SUN Java Runtime Environment (JRE) version 1.4.2_05 or later (or Java Virtual Machine (JVM) 5.0.0.3810).
- Access to PC network TCP/IP configuration and command prompt
- Console cable with DB-9 to RJ-45 adapter
- Cabling as shown in the topology and described in test plan Lab 8.3.2

## Task 1: Build the Network and Configure the Devices for SDM Access

### Step 1: Configure basic router settings for SDM access

**NOTE:** If the PC used in this lab is also connected to your Academy LAN or to the Internet, ensure that you record the cable connections and TCP/IP settings so that these can be restored at the conclusion of the lab.

a. Connect to the PC to the router console port using a serial cable with a DB-9/RJ-45 adapter. Use the **erase startup-config** and the **reload** commands from the privileged EXEC prompt, to ensure that you are starting with a clean configuration.

b. Configure basic routers settings to prepare the router for access using SDM.

```
Router(config)#hostname VPN
VPN(config)#line console 0
VPN(config-line)#password cisco
VPN(config-line)#login
VPN(config-line)#line vty 0 4
VPN(config-line)#password cisco
VPN(config-line)#login
VPN(config-line)#enable password cisco
VPN(config)#enable secret class
VPN(config)#no ip domain-lookup
VPN(config)#
VPN(config)#interface Fa0/0
VPN(config-if)#ip address 10.10.10.1 255.255.255.248
VPN(config-if)#no shutdown
VPN(config-if)#
VPN(config-if)#ip http server
VPN(config)#ip http authentication local
VPN(config)#username admin privilege 15 password 0 cisco123
VPN(config)#end
```

c. Copy the **running-config** to the **startup-config**.

### Step 2: Configure the PC to connect to the router and launch Cisco SDM

a. Disable any popup blocker programs. Popup blockers prevent SDM windows from displaying.

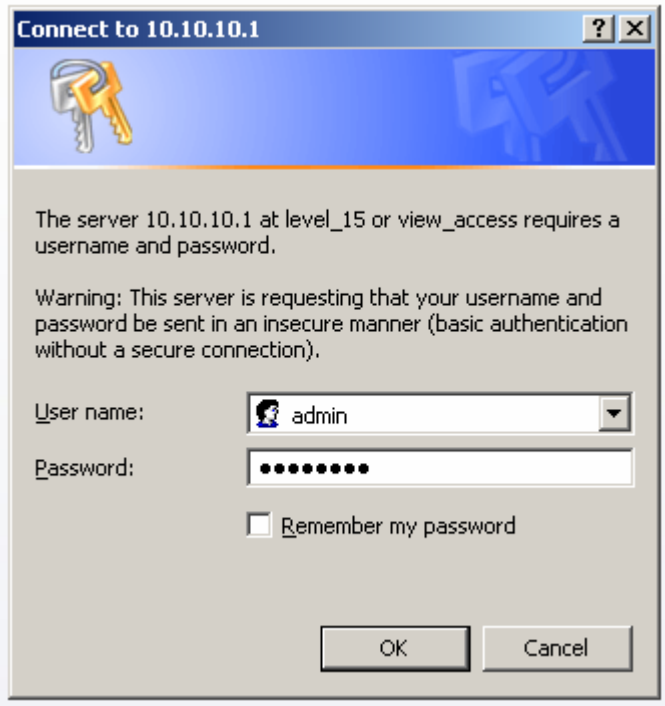
b. Connect the PC NIC to the FastEthernet 0/0 port on the Cisco 1841 ISR router with an Ethernet crossover cable. This in-band connection will be used to configure VPN using the PCs browser and the SDM graphical user interface.

**NOTE:** An SDM router other than the 1841 may require connection to different port in order to access SDM.

c. Configure the IP address of the PC as 10.10.10.2 with a subnet mask of 255.255.255.248.

d. SDM does not load automatically on the router. You must open the web browser to reach the SDM. Open the web browser on the PC and connect to the following URL: http://10.10.10.1

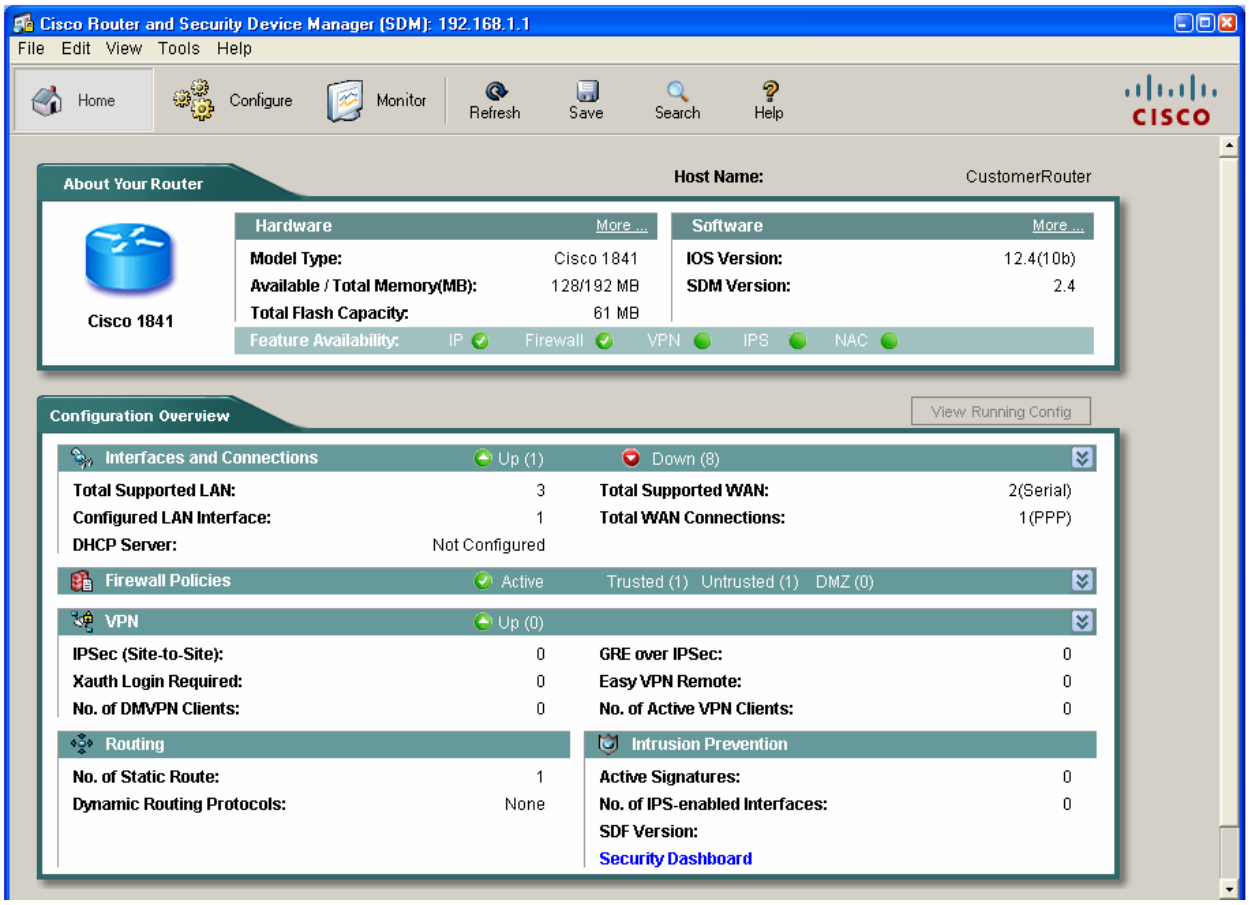
e. In the **Connect to** dialog box, enter **admin** for the username and **cisco123** for the password. Click **OK**. The main SDM web application will start and you will be prompted to use HTTPS. Click **Cancel**. In the Security Warning window, click **Yes** to trust the Cisco application.



f. Verify that you are using the latest version of SDM. The initial SDM screen that displays immediately after the login shows the current version number. It is also displayed on the main SDM screen shown below, along with IOS version.

**NOTE:** If the current version is not 2.4 or higher, notify your instructor before continuing with this lab. You will need to download the latest zip file from http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm and save it to the PC being used to access the router SDM. From the **Tools** menu of the SDM GUI, use the **Update SDM** option to specify the location of the zip file and start the update.

Also note that the Windows XP computer you are using must have Internet Explorer 5.5 or higher and SUN Java Runtime Environment (JRE) version 1.4.2_05 or later (or Java Virtual Machine (JVM) 5.0.0.3810). If it does not, SDM will not start. You will need to download and install JRE on the PC before continuing with the lab.




## Step 3: Configure SDM to show Cisco IOS CLI commands

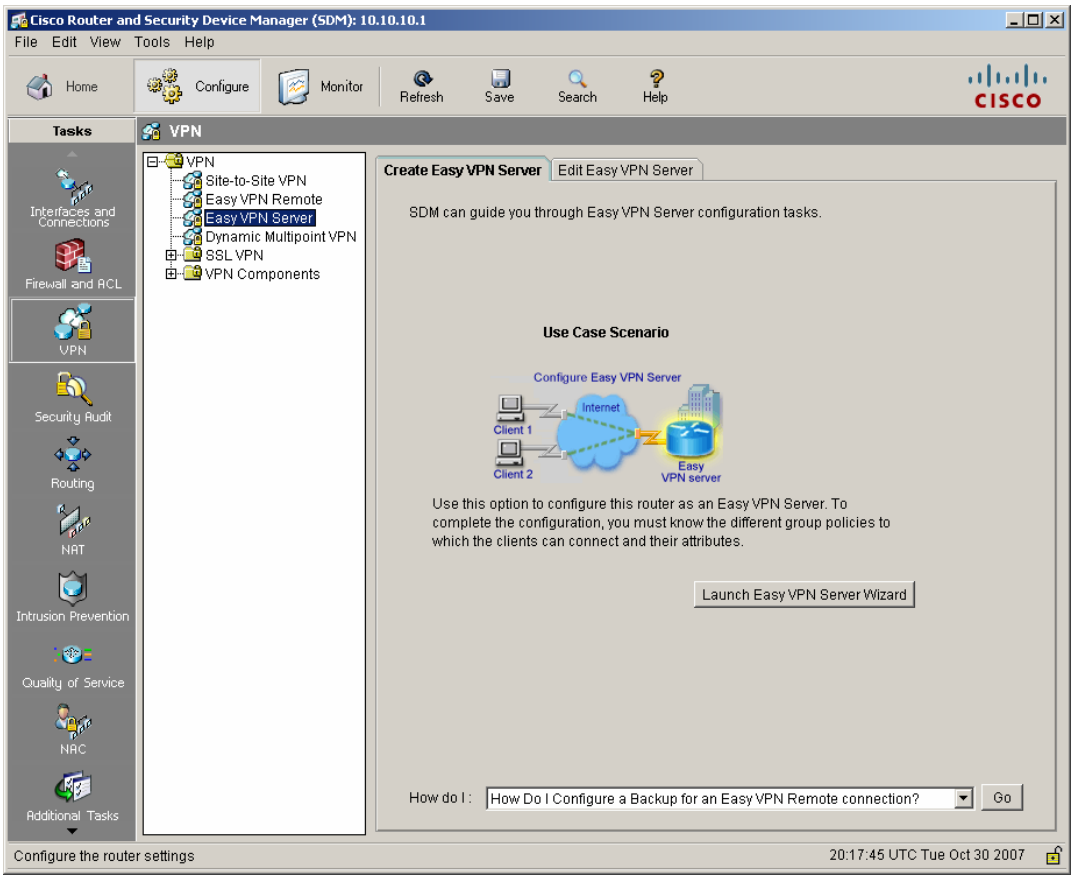
a. From the **Edit** menu in the main SDM window, select **Preferences**.

b. Select the **Preview commands before delivering to router** check box. With this check box checked, you can see the Cisco IOS CLI commands that you will use to perform a configuration function on the router before these commands are sent to the router. You can learn about Cisco IOS CLI commands this way.

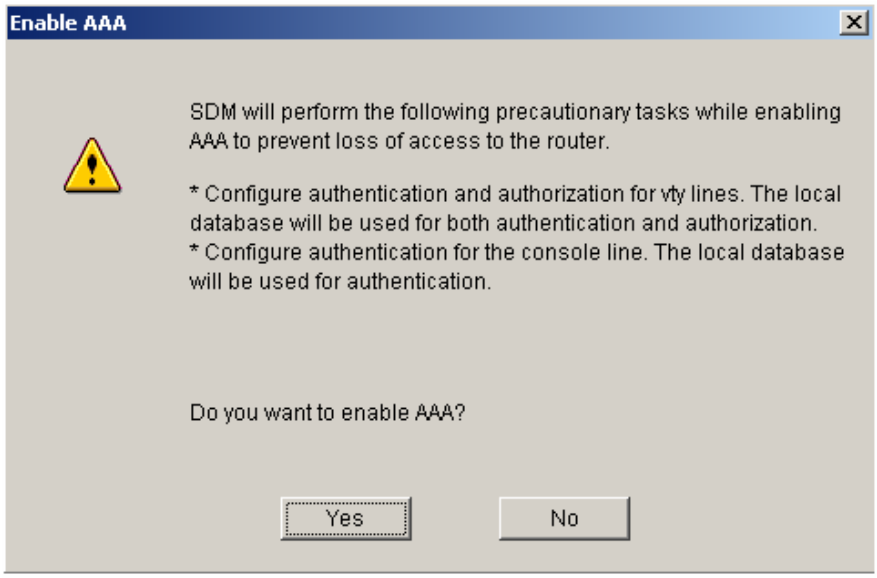
## Task 2: Use EasyVPN to configure the router as a VPN server

### Step 1: Launch the EasyVPN Server Wizard

a. From the **Configure** menu, click the **VPN** button to view the VPN configuration page. Select **Easy VPN Server** from the main VPN window, and then click **Launch Easy VPN Server Wizard**.



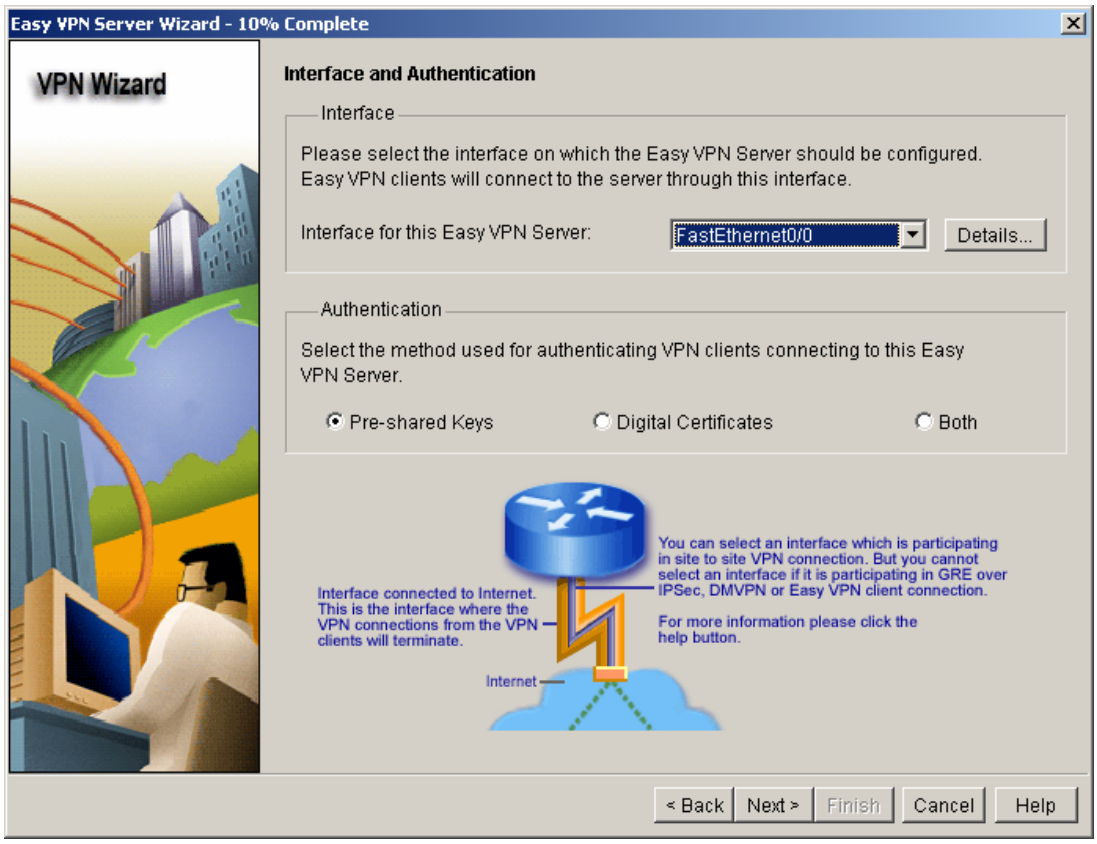
b. The Enable AAA window will display. AAA must be enabled on the router before the Easy VPN Server configuration starts. Click **Yes** to continue with the configuration. Click the **Deliver** button to deliver the AAA configuration to the router. The AAA has been successfully enabled on the router's message displays on the window.



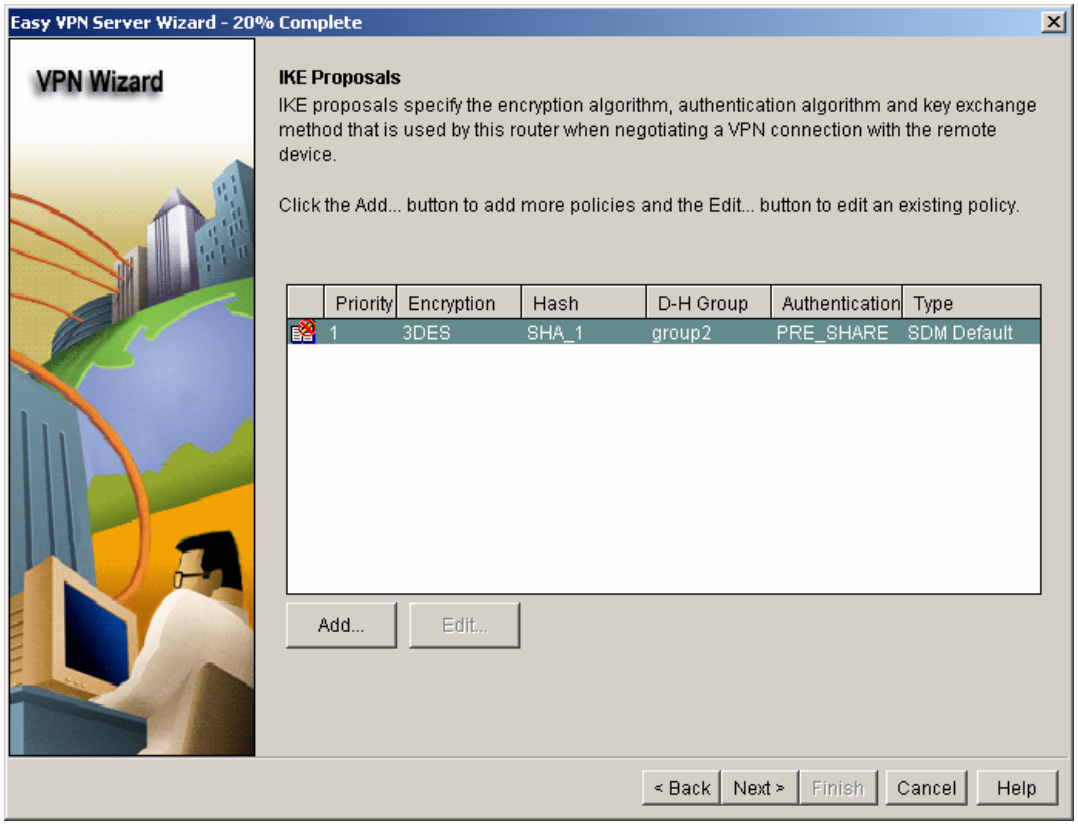

c. Click **OK** to continue to the VPN Wizard Welcome screen. Click **Next** to start the **Easy VPN Server Wizard**.

### Step 2: Select the Interface and Authentication method

a. Select the interface on which the client connections terminate and the authentication type. This connection terminates on Fa0/0 and pre-shared keys will be used.

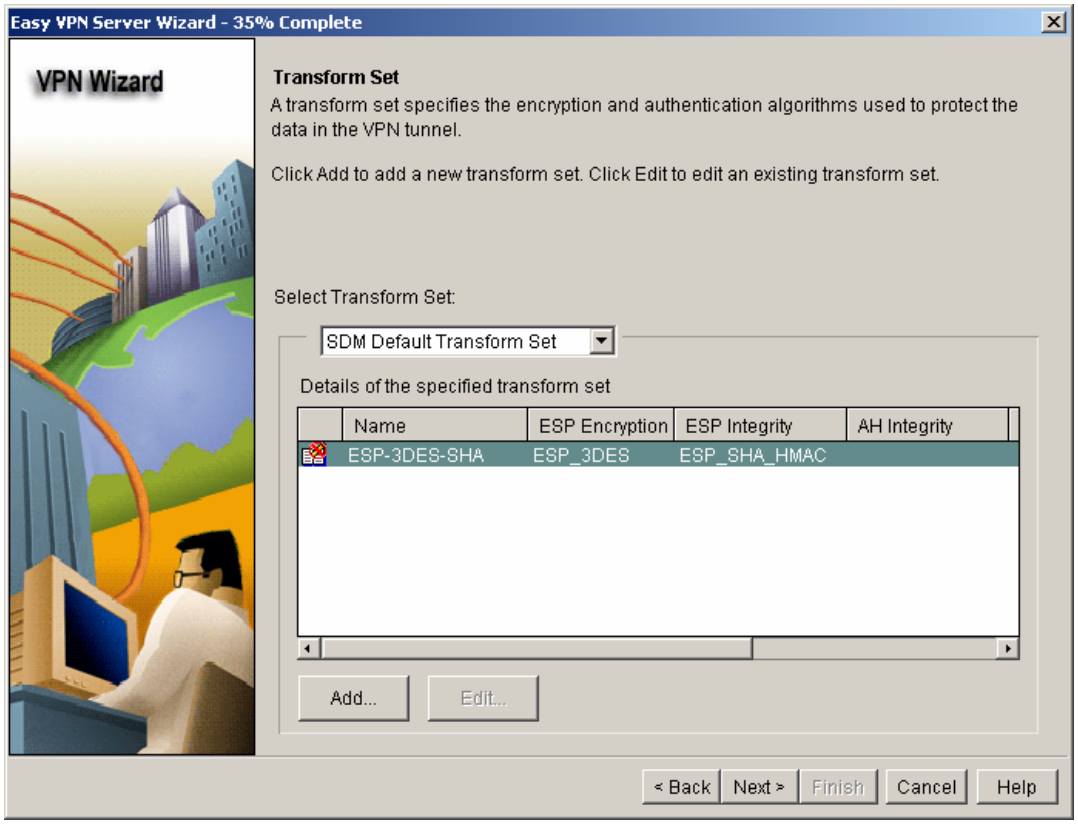


b. Click **Next** to configure the Internet Key Exchange (IKE) policies. Use the **Add** button to create the new policy. Configurations on both sides of the tunnel must match exactly. However, the Cisco VPN Client automatically selects the proper configuration for itself. Therefore, no IKE configuration is necessary on the client PC.



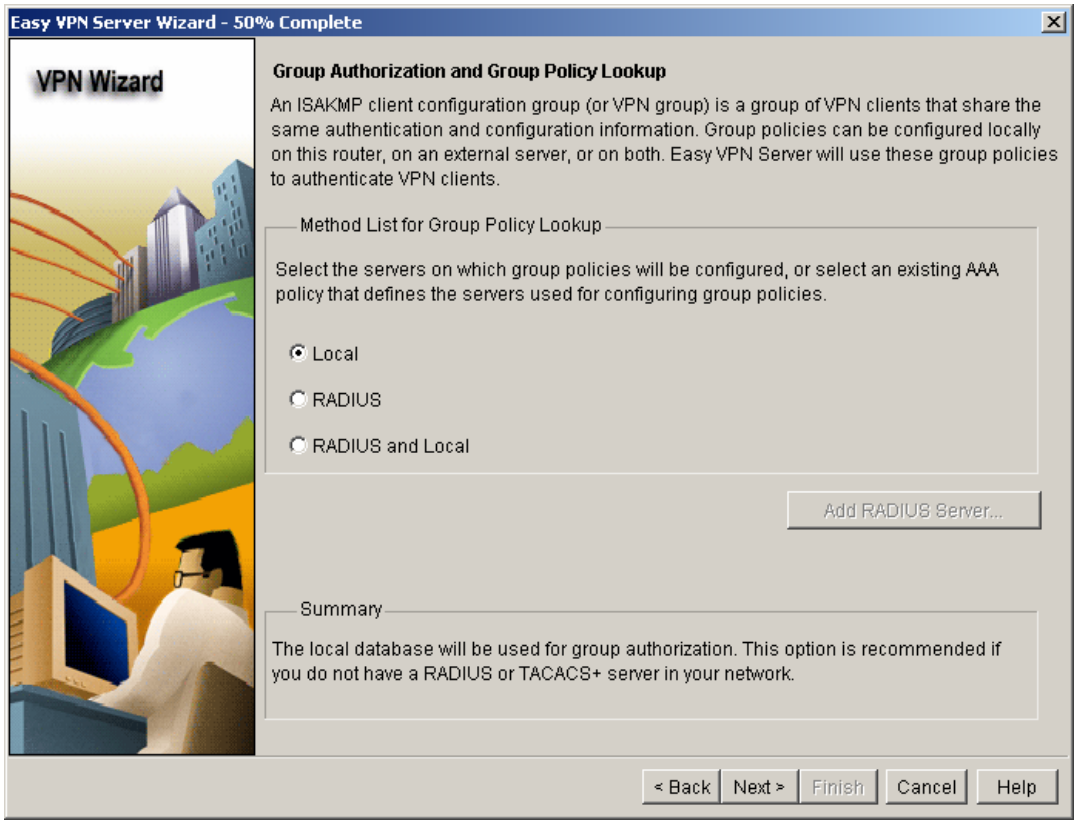
### Step 3: Specify the Transform Set

Click **Next** to accept the default transform set for data encryption and authentication algorithms.



### Step 4: Specify Group Authorization and Group Policy Lookup

Click **Next** to create a new Authentication, Authorization, and Accounting (AAA) authorization network method list for group policy lookup. Accept the default of **Local** for policy lookup.



### Step 5: Configure User Authentication (XAuth)

a. You can store user authentication details on an external server, such as a RADIUS server or a local database or on both. Select the **Enable User Authentication** checkbox and accept the default of **Local Only**.

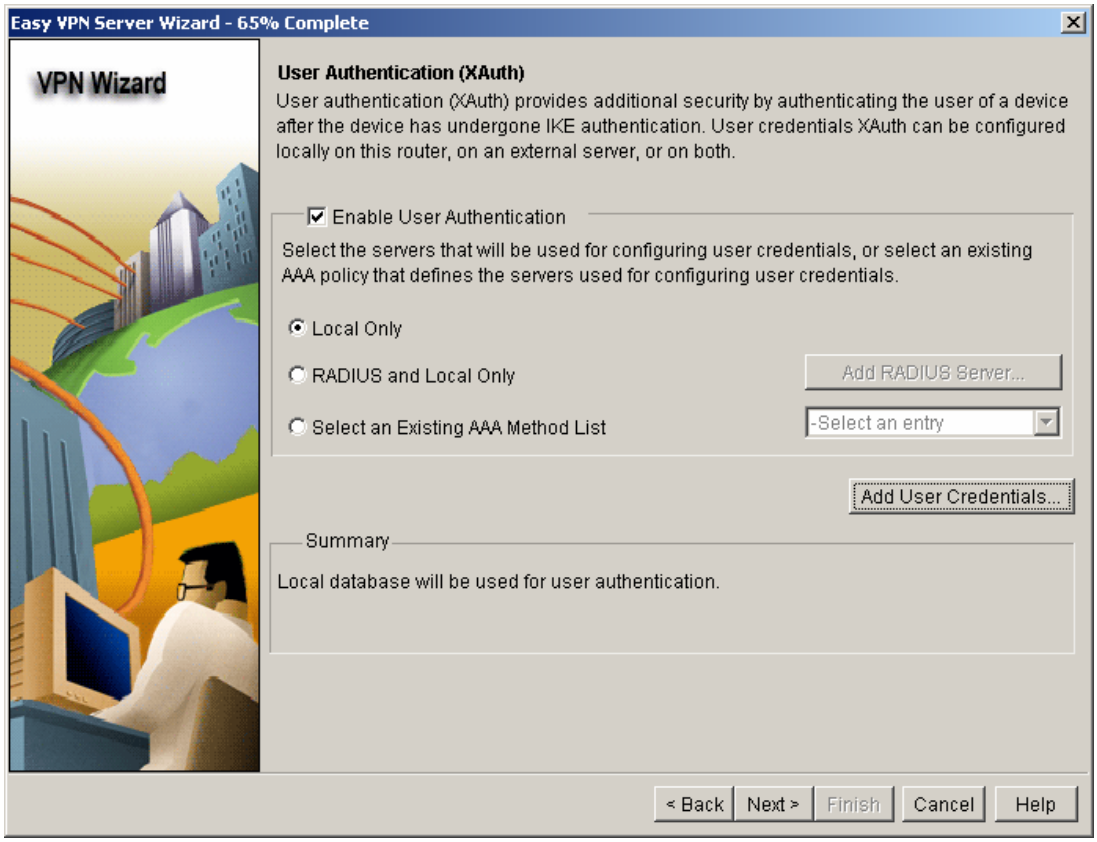
b. Click the **Add User Credentials** button to see users currently defined or to add users.

What is the name of the user currently defined and what is the user privilege level?

_____

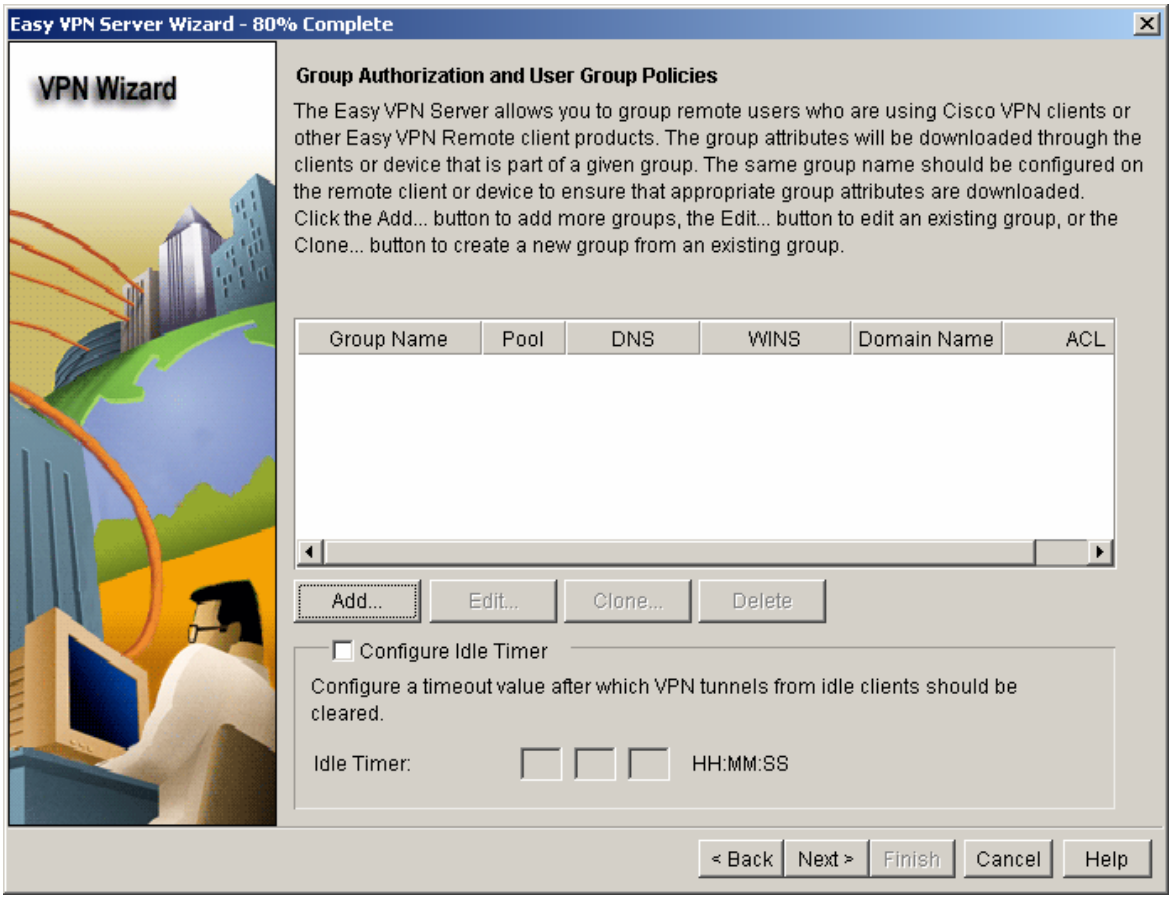
How was this user defined?

_____

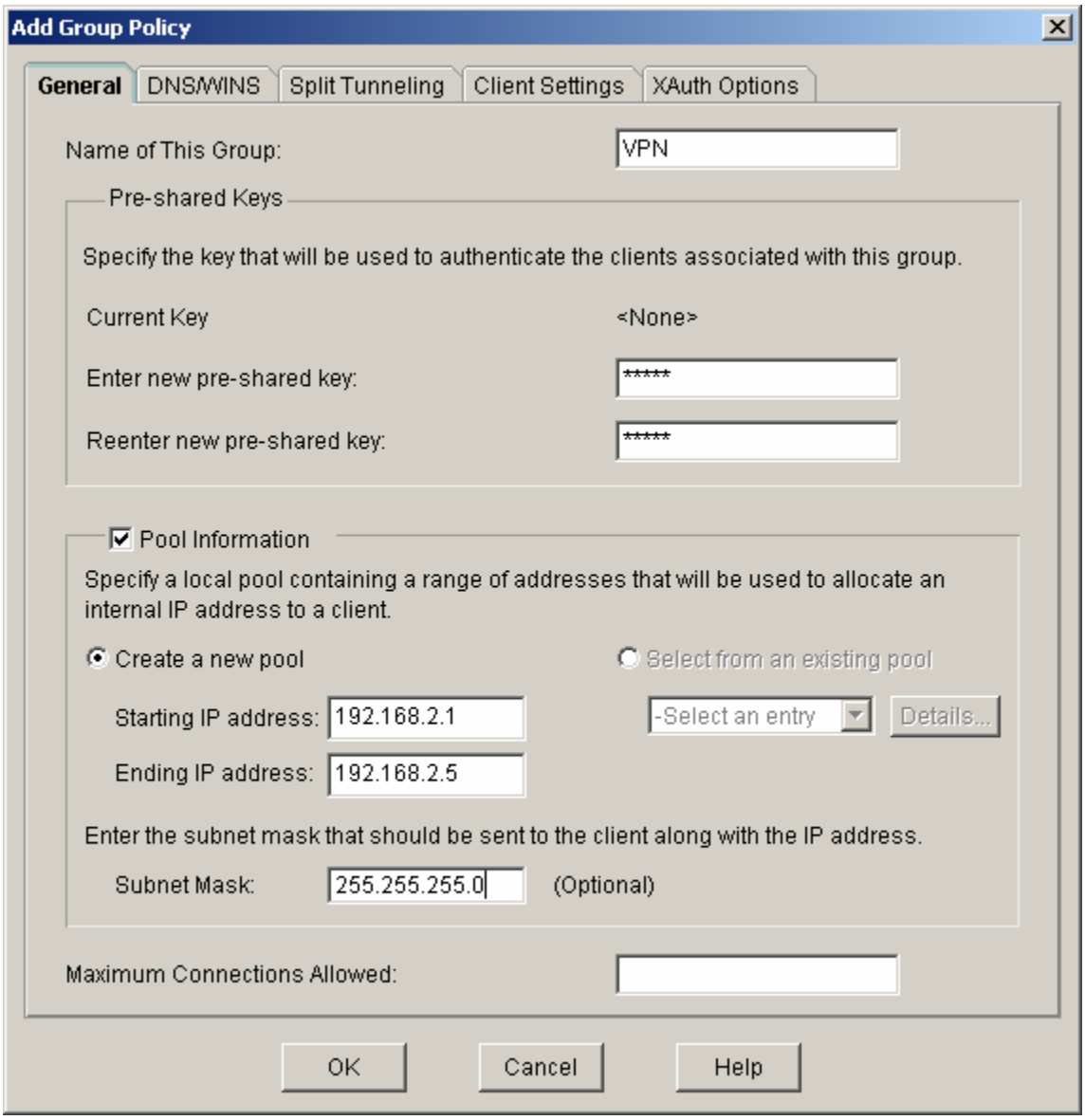


### Step 6: Configure the Group Policy

a. Click **Next** to go to the Group Authorization and User Group Policies screen. You must create at least one group policy for the VPN server.



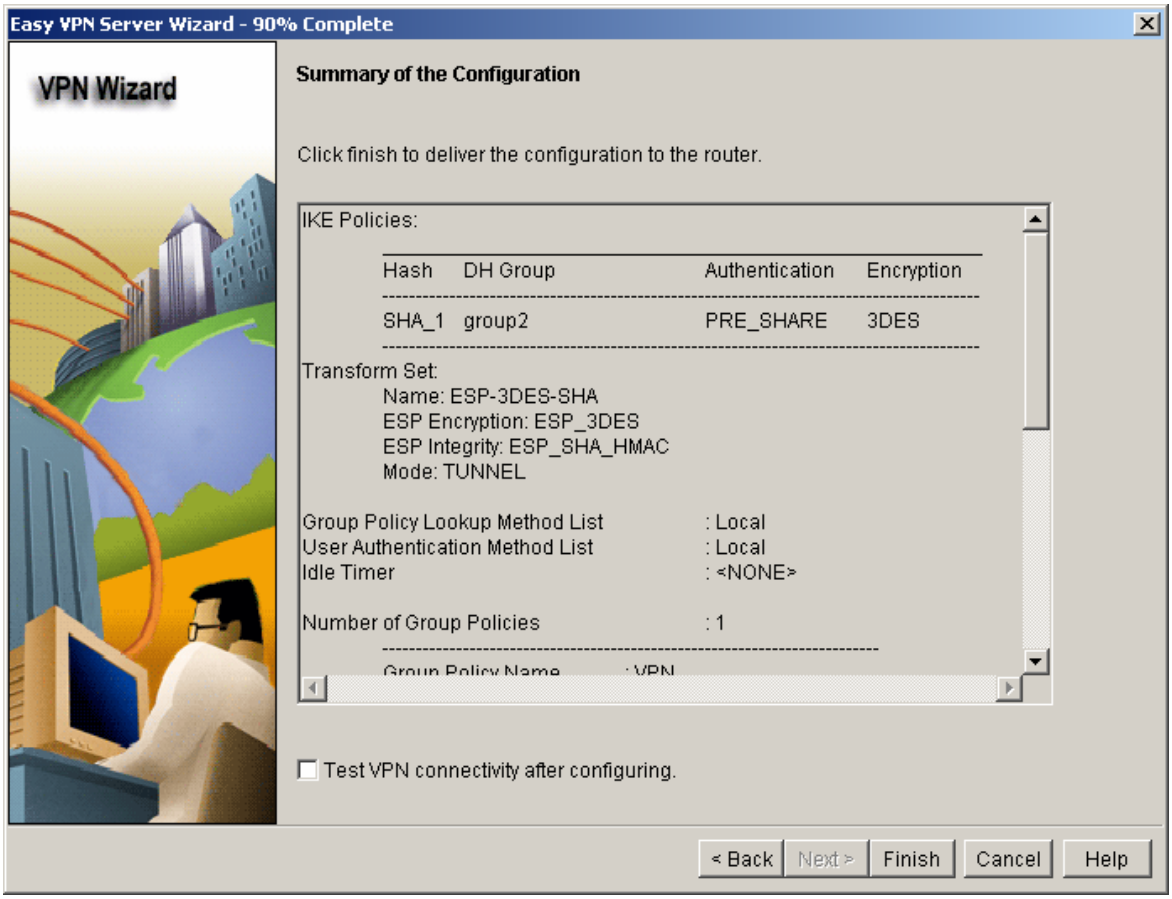
b. Click **Add** to create a policy. Enter **VPN** as the Tunnel Group Name. Enter a new pre-shared key of **cisco** and then re-enter it. Leave the Pool Information box checked and enter a starting address, an ending address, and a subnet mask as shown. Click **OK** to accept the entries. When you return to the Group Authorization screen, click **Next**.



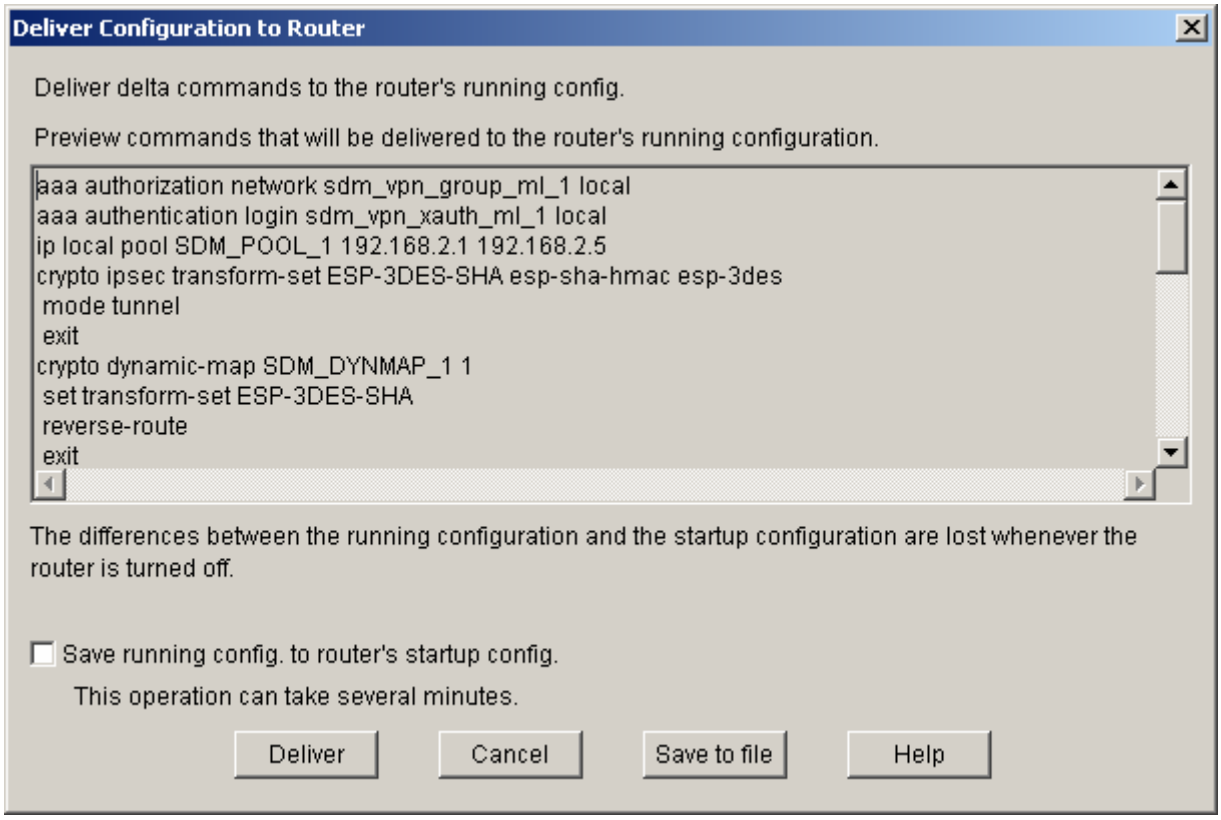
### Step 7: Review the Summary of the Configuration you created

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



### Step 8: Deliver the configuration to router

This window shows the IOS commands that will be delivered to the router as a result of selections and entries you have made. Select the checkbox **Save running-config to router's startup config**. Click **Deliver** to complete the transfer of commands to the router.

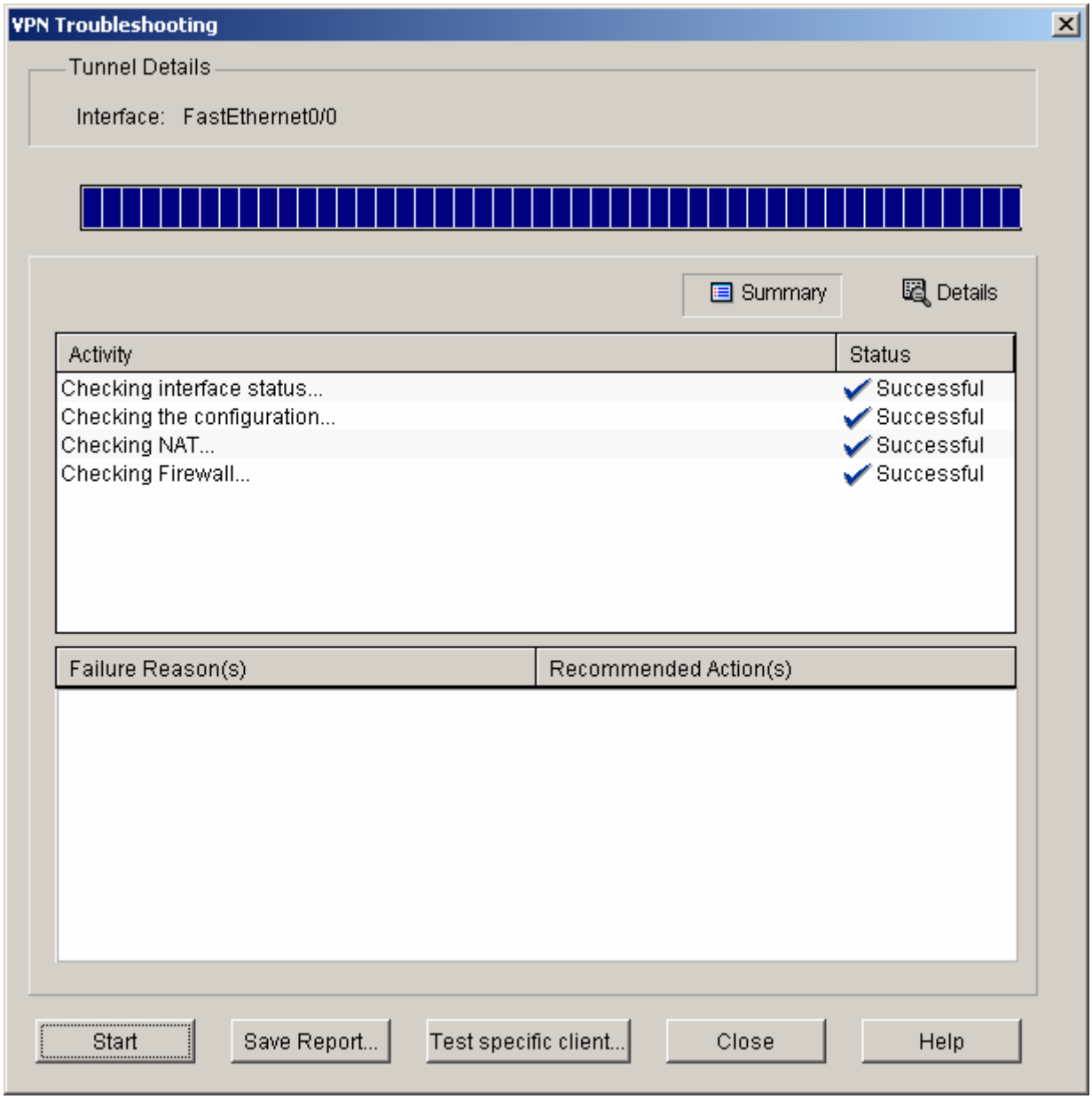


### Step 9: Test the basic VPN config on the router

a. Test the VPN configuration according to Test 1 in the Lab 8.3.2. “Creating a VPN Connectivity Test Plan.”

b. After the commands have been delivered, you will be returned to the main VPN configuration screen. Select the name of the VPN configuration you created and click **Test VPN Server** in the lower right corner of the screen. You should get a response similar to the following example:



### Task 3: Reflection

Why would you configure VPN using the SDM EasyVPN Server instead of using the command line?

_____

_____

_____

_____

Summarize the steps that are configured by the SDM EasyVPN server

_____

_____

_____

_____

_____

_____