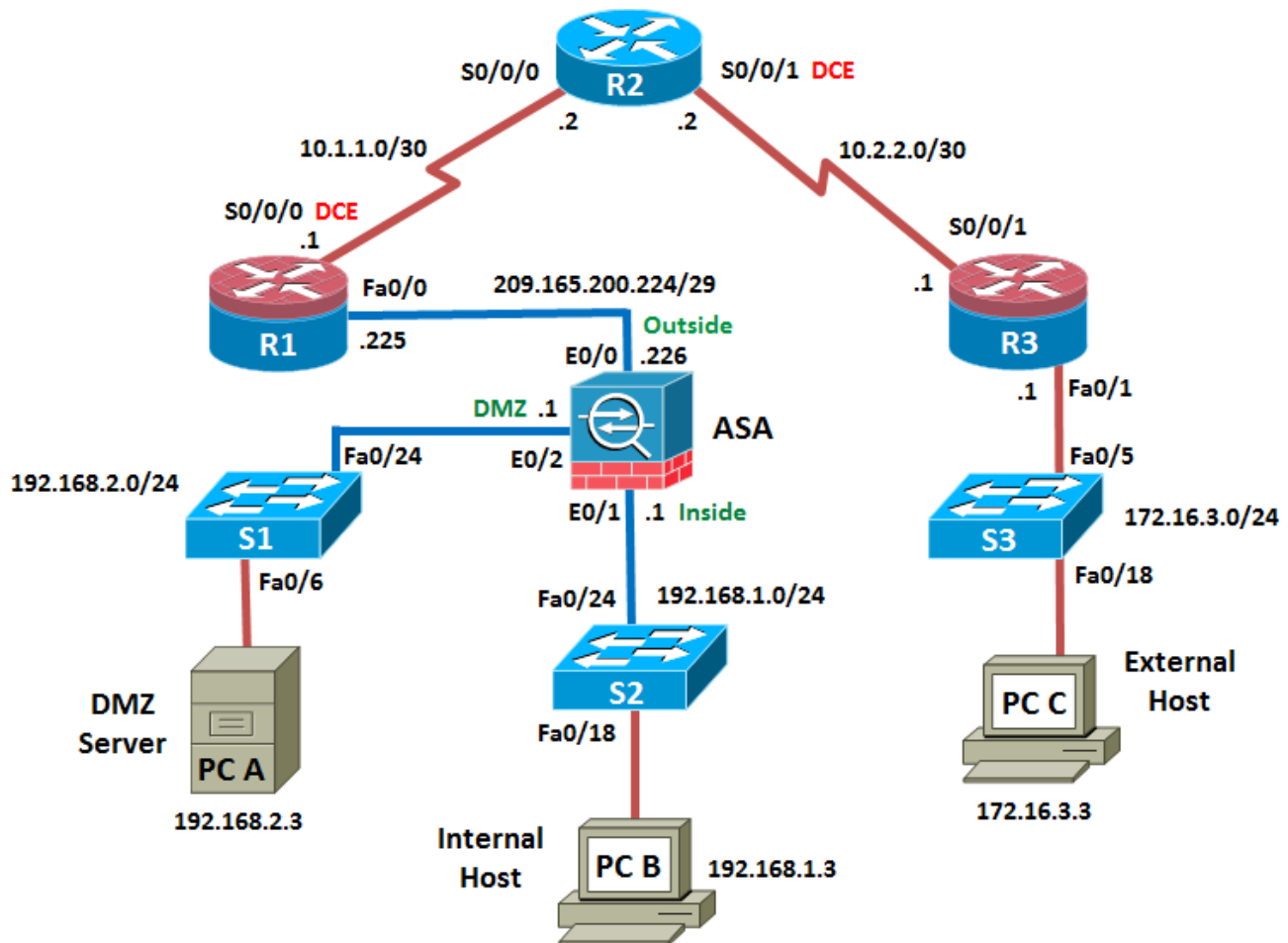


## Chapter 10 Lab H: Configuring a Site-to-Site IPsec VPN using CCP on an ISR and ASDM on an ASA 5510

### Topology



**Note:** ISR G2 devices have Gigabit Ethernet interfaces instead of Fast Ethernet Interfaces.

## IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	FA0/0	209.165.200.225	255.255.255.248	N/A	ASA E0/0
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	FA0/1	172.16.3.1	255.255.255.0	N/A	S3 FA0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
ASA	E0/0 (outside)	209.165.200.226	255.255.255.248	NA	R1 FA0/0
	E0/1 (inside)	192.168.1.1	255.255.255.0	NA	S2 FA0/24
	E0/2 (dmz)	192.168.2.1	255.255.255.0	NA	S1 FA0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 FA0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 FA0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 FA0/18

## Objectives

### Part 1: Basic Router/Switch/PC Configuration

- Cable the network as shown in the topology.
- Configure hostnames, interface IP addresses for routers, switches and PCs.
- Configure static routing, including default routes, between R1, R2 and R3.
- Configure R3 HTTP access to enable CCP management.
- Verify connectivity between hosts, switches and routers.

### Part 2: Basic ASA Configuration

- Access the ASA console.
- Clear previous configuration settings.
- Load the ASA CLI command script to configure basic settings.
- Verify access to ASA/ASDM.

### Part 3: Configuring the ISR as a Site-to-Site IPsec VPN Endpoint Using CCP

- Configure basic VPN connection information settings.
- Configure IKE policy parameters.
- Configure a transform set.
- Define traffic to protect.
- Verify the VPN configuration on R3.

### Part 4: Configuring the ASA as a Site-to-Site IPsec VPN Endpoint Using ASDM

- Identify peer device and access interface.
- Specify IKE version.
- Specify traffic to protect.
- Configure authentication methods.

- Specify encryption algorithm.
- Verify VPN functionality.
- Monitor the VPN connection and traffic.

### Background / Scenario

In addition to acting as a remote access VPN concentrator, the ASA can provide Site-to-Site IPsec VPN tunneling. The tunnel can be configured between two ASAs or between an ASA and another IPsec VPN-capable device such as an ISR, as is the case with this lab.

Your company has two locations connected to an ISP. Router R1 represents a CPE device managed by the ISP. Router R2 represents an intermediate Internet router. Router R3 connects users at the remote branch office to the ISP. The ASA is an edge CPE security device that connects the internal corporate network and DMZ to the ISP while providing NAT services to inside hosts.

Management has asked you to provide a dedicated Site-to-Site IPsec VPN tunnel between the ISR router at the remote branch office and the ASA device at the corporate site. This tunnel will protect traffic between the branch office LAN and the corporate LAN, as it passes through the Internet. The Site-to-Site VPN does not require a VPN client on the remote or corporate site host computers. Traffic from either LAN to other Internet destinations is routed by the ISP and is not protected by the VPN tunnel. The VPN tunnel will pass through R1 and R2, which are not aware of its existence.

In Part 1 of the lab you will configure the topology and non-ASA devices. In Part 2 you will prepare the ASA for ASDM access. In Part 3 you will use the CCP VPN Wizard to configure the R3 ISR as a Site-to-Site IPsec VPN endpoint. In Part 4 you will configure the ASA as a Site-to-Site IPsec VPN endpoint using the ASDM VPN Wizard.

**Note:** The routers used with this lab are Cisco 1841 with Cisco IOS Release 12.4(20)T (Advanced IP image). The switches are Cisco WS-C2960-24TT-L with Cisco IOS Release 12.2(46)SE (C2960-LANBASEK9-M image). Other routers, switches, and Cisco IOS versions can be used. However, results and output may vary.

The ASA that is used with this lab is a Cisco model 5510 with four FastEthernet routed interfaces, running OS version 8.4(2) and ASDM version 6.4(5) and comes with a Base license that allows a maximum of 50 VLANs.

**Note:** Make sure that the routers and switches have been erased and have no startup configurations.

### Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(20)T1 or comparable)
- 3 switches (Cisco 2960 or comparable)
- 1 ASA 5510 (OS version 8.4(2) and ASDM version 6.4(5) and Base license or comparable)
- PC-A: Windows XP, Vista, or Windows 7 with PuTTY SSH client (Web server optional)
- PC-B: Windows XP, Vista, or Windows 7 with PuTTY SSH client and Java 6 (ASDM loaded on the PC is optional)
- PC-C: Windows XP, Vista, or Windows 7 with PuTTY SSH client, Java 6 and CCP version 2.5.
- Serial and Ethernet cables as shown in the topology
- Rollover cables to configure the routers and ASA via the console

#### CCP Note s:

- Refer to Chp 00 Lab A for instructions on how to install and run CCP. Hardware/software recommendations for CCP include Windows XP, Vista, or Windows 7 with Java version 1.6.0\_11 up to 1.6.0\_21, Internet Explorer 6.0 or above and Flash Player Version 10.0.12.36 and later.
- If the PC on which CCP is installed is running Windows Vista or Windows 7, it may be necessary to right-click on the CCP icon or menu item, and choose **Run as administrator**.

- In order to run CCP, it may be necessary to temporarily disable antivirus programs and O/S firewalls. Make sure that all pop-up blockers are turned off in the browser.

## Part 1: Basic Router/Switch/PC Configuration

In Part 1 of this lab, you will set up the network topology and configure basic settings on the routers such as interface IP addresses and static routing.

**Note:** Do not configure any ASA settings at this time.

### Step 1: Cable the network and clear previous device settings.

Attach the devices shown in the topology diagram and cable as necessary. Make sure that the routers and switches have been erased and have no startup configurations.

### Step 2: Configure basic settings for routers and switches.

- Configure host names as shown in the topology for each router.
- Configure router interface IP addresses as shown in the IP Addressing Table.
- Configure a clock rate for routers with a DCE serial cable attached to their serial interface. Router R1 is shown here as an example.

```
R1(config)# interface S0/0/0
R1(config-if)# clock rate 64000
```

- Configure the host name for the switches. Other than host name, the switches can be left in their default configuration state. Configuring the VLAN management IP address for the switches is optional.

### Step 3: Configure static routing on the routers.

- Configure a static default route from R1 to R2 and from R3 to R2.
- Configure a static route from R2 to the R1 Fa0/0 subnet (connected to ASA interface E0/0) and a static route from R2 to the R3 LAN.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/0
R3(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/1

R2(config)# ip route 209.165.200.224 255.255.255.248 Serial0/0/0
R2(config)# ip route 172.16.3.0 255.255.255.0 Serial0/0/1
```

### Step 4: Configure the enable and VTY passwords on R3.

On R3, set the enable password to **class** and the console and VTY passwords to **cisco**. Configure these settings on R1 and R2. R3 is shown here as an example.

```
R3(config)# enable secret class

R3(config)# line vty 0 4
R3(config-line)# password cisco
R3(config-line)# login

R3(config)# line con 0
R3(config-line)# password cisco
R3(config-line)# login
```

**Step 5: Configure HTTP access, a username, and local authentication prior to starting CCP.**

- a. From the CLI, enable the HTTP server and configure a username of **admin** and password of **cisco123** for use with CCP on R3.

```
R3(config)# ip http server
R3(config)# username admin privilege 15 secret cisco123
```

- b. Use the local database to authenticate web sessions with CCP.

```
R3(config)# ip http authentication local
```

**Step 6: Configure PC host IP settings.**

Configure a static IP address, subnet mask, and default gateway for PC-A, PC-B, and PC-C as shown in the IP Addressing Table.

**Step 7: Verify connectivity.**

From PC-C, ping the R1 Fa0/0 IP address (209.165.200.225). If these pings are not successful, troubleshoot the basic device configurations before continuing.

**Note:** If you can ping from PC-C to R1 Fa0/0 you have demonstrated that static routing is configured and functioning correctly.

**Step 8: Save the basic running configuration for each router and switch.****Part 2: Basic ASA Configuration****Step 1: Access the ASA console.**

- a. Accessing the ASA via the console port is the same as with a Cisco router or switch. Connect to the ASA Console port with a rollover cable.
- b. Use a terminal emulation program such as TeraTerm or HyperTerminal to access the CLI, and use the serial port settings of 9600 baud, eight data bits, no parity, one stop bit, and no flow control.
- c. If prompted to enter Interactive Firewall configuration (Setup mode), answer **no**.
- d. Enter privileged mode with the **enable** command and password (if set). By default the password is blank so you can just press **Enter**. If the password has been changed to that specified in this lab, the password will be **class**. In addition, the hostname and prompt will be **CCNAS-ASA>**, as shown here. The default ASA hostname and prompt is **ciscoasa>**.

```
CCNAS-ASA> enable
Password: class (or press Enter if none set)
```

**Step 2: Clear the previous ASA configuration settings.**

- a. Use the **write erase** command to remove the **startup-config** file from flash memory.

```
CCNAS-ASA# write erase
Erase configuration in flash memory? [confirm]
[OK]
CCNAS-ASA#
```

**Note:** The IOS command **erase startup-config** is not supported on the ASA.

- b. Use the **reload** command to restart the ASA. This will cause the ASA to come up in CLI Setup mode. If you see the message System config has been modified. Save? [Y]es/[N]o:, respond with "N".

```
CCNAS-ASA# reload
Proceed with reload? [confirm] <enter>
```

```
CCNAS-ASA#
***
*** --- START GRACEFUL SHUTDOWN ---
Shutting down isakmp
Shutting down File system
***
*** --- SHUTDOWN NOW ---
Process shutdown finished
Rebooting.....
CISCO SYSTEMS
Embedded BIOS Version 1.0(12)13 08/28/08 15:50:37.45
```

<output omitted>

### Step 3: Bypass Setup Mode.

When the ASA completes the reload process, it should detect that the **startup-config** file is missing and go into Setup mode. If it does not come up in this mode, repeat Step 2.

- a. When prompted to pre-configure the firewall through interactive prompts (Setup mode), respond with **"no"**.

```
Pre-configure Firewall now through interactive prompts [yes]? no
```

- b. Enter privileged EXEC mode with the **enable** command. The password should be blank (no password) at this point.

### Step 4: Use the CLI script to configure the ASA.

In this step you will use the modified running-config from Lab 10E to preconfigure basic settings, the firewall and DMZ.

- a. Ensure that there is no previous configuration in the ASA, other than the defaults that the ASA automatically inserts, using the **show run** command.
- b. Enter CLI global configuration mode. When prompted to enable anonymous call-home reporting, respond **"no"**.

```
ciscoasa> enable
Password: <enter>
```

```
ciscoasa# conf t
ciscoasa(config)#
```

- c. Copy and paste the **Pre-VPN Configuration Script** commands listed below at the ASA global config mode prompt to bring it to the point where you can start configuring the SSL VPNs.
- d. Observe the messages as the commands are applied to ensure that there are no warnings or errors. If prompted to replace the RSA keypair, respond **"yes"**.
- e. After script commands have been applied, issue the **write mem** (or **copy run start**) command to save the running configuration to the startup configuration and the RSA keys to non-volatile memory.

**Lab 10H Pre-VPN ASA Configuration Script:**

```
hostname CCNAS-ASA
!
domain-name ccnasecurity.com
!
enable password class
passwd cisco
!
interface Ethernet0/0
  nameif outside
  security-level 0
  ip address 209.165.200.226 255.255.255.248
  no shut
!
interface Ethernet0/1
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shut
!
interface Ethernet0/2
  nameif dmz
  security-level 70
  ip address 192.168.2.1 255.255.255.0
  no shut
!
object network inside-net
  subnet 192.168.1.0 255.255.255.0
!
object network dmz-server
  host 192.168.2.3
!
access-list OUTSIDE-DMZ extended permit ip any host 192.168.2.3
!
object network inside-net
  nat (inside,outside) dynamic interface
!
object network dmz-server
  nat (dmz,outside) static 209.165.200.227
!
access-group OUTSIDE-DMZ in interface outside
!
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
!
username admin password cisco123
!
aaa authentication telnet console LOCAL
aaa authentication ssh console LOCAL
aaa authentication http console LOCAL
!
http server enable
http 192.168.1.0 255.255.255.0 inside
ssh 192.168.1.0 255.255.255.0 inside
telnet 192.168.1.0 255.255.255.0 inside
telnet timeout 10
ssh timeout 10
!
class-map inspection_default
  match default-inspection-traffic
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
```

```
policy-map global_policy
  class inspection_default
    inspect icmp
  !
prompt hostname context
no call-home reporting anonymous
!
crypto key generate rsa modulus 1024
```

### Step 5: Verify HTTPS ASDM access.

This step is intended to verify HTTPS connectivity from PC-B to the ASA. ASDM settings will be configured in Part 4 of the lab.

- Open a browser on PC-B and test the HTTPS access to the ASA by entering `https://192.168.1.1`.  
**Note:** Be sure to specify the HTTPS protocol in the URL.
- After entering the URL above, you should see a security warning about the website's security certificate. Click **Continue to this website**. The ASDM welcome page will display. From this screen, you can install ASDM on the PC, Run ASDM as browser-based Java applet directly from the ASA or Run the Startup wizard. Click the **Run ASDM** button.
- The ASDM-IDM Launcher will display. Login as user **admin** with password **cisco123**. ASDM will load the current configuration into the GUI.

**Note:** The process may vary depending on the browser used. This example is for Internet Explorer.

## Part 3: Configuring the ISR as a Site-to-Site IPsec VPN Endpoint Using CCP

In Part 3 of this lab, you will configure R3 as an IPsec VPN endpoint for the tunnel between R3 and the ASA. Routers R1 and R2 are unaware of the tunnel.

**Note:** If the PC on which CCP is installed is running Windows 7, it may be necessary to right-click on the CCP icon or menu item, and choose **Run as administrator**.

It may be necessary to temporarily disable antivirus programs and O/S firewalls in order to run CCP. The minimum recommended Windows PC requirements to run CCP are:

- Internet Explorer with Java 6 plug-in version 1.6.0-11
- Adobe Flash Player version 10
- 1 GB RAM
- Screen resolution of 1024 x 768

**Note:** If you receive the following Java-related error message from CCP during the VPN configuration process, perform the steps indicated in the message:

Security component has failed. In order to work on Router or Security features, do the following. Go to **Java Control panel > Advanced tab > Java Plug-in** tree Entry. Uncheck the check box for **Enable next-generation Java Plug-in**. Re-launch CCP after this.

### Step 1: Run the CCP application on PC-C and discover R3.

- Run the CCP application on PC-C. In the **Select/Manage Community** window, enter the R3 Fa0/0 IP address **172.16.3.1**, username **admin**, and **cisco123** as the password. Click the **OK** button.



Select / Manage Community

New Community

Enter information for up to 10 devices for the selected community

	IP Address/Hostname	Username	Password	Connect Securely
1.	172.16.3.1	admin	*****	<input type="checkbox"/>
2.				<input type="checkbox"/>
3.				<input type="checkbox"/>
4.				<input type="checkbox"/>
5.				<input type="checkbox"/>
6.				<input type="checkbox"/>
7.				<input type="checkbox"/>
8.				<input type="checkbox"/>
9.				<input type="checkbox"/>
10.				<input type="checkbox"/>

☐ Discover all devices

OK Cancel

- b. In the **Community Information** panel, click on the **Discover** button to discover and connect to R3. If the PC-C CCP application can make an HTTP connection to R3, the **Discovery Status** will change to **"Discovered"**. If the discovery process fails, use the **Discover Details** button to determine the problem so that you can resolve the issue.



## Step 2: Start the CCP VPN wizard to configure R3.

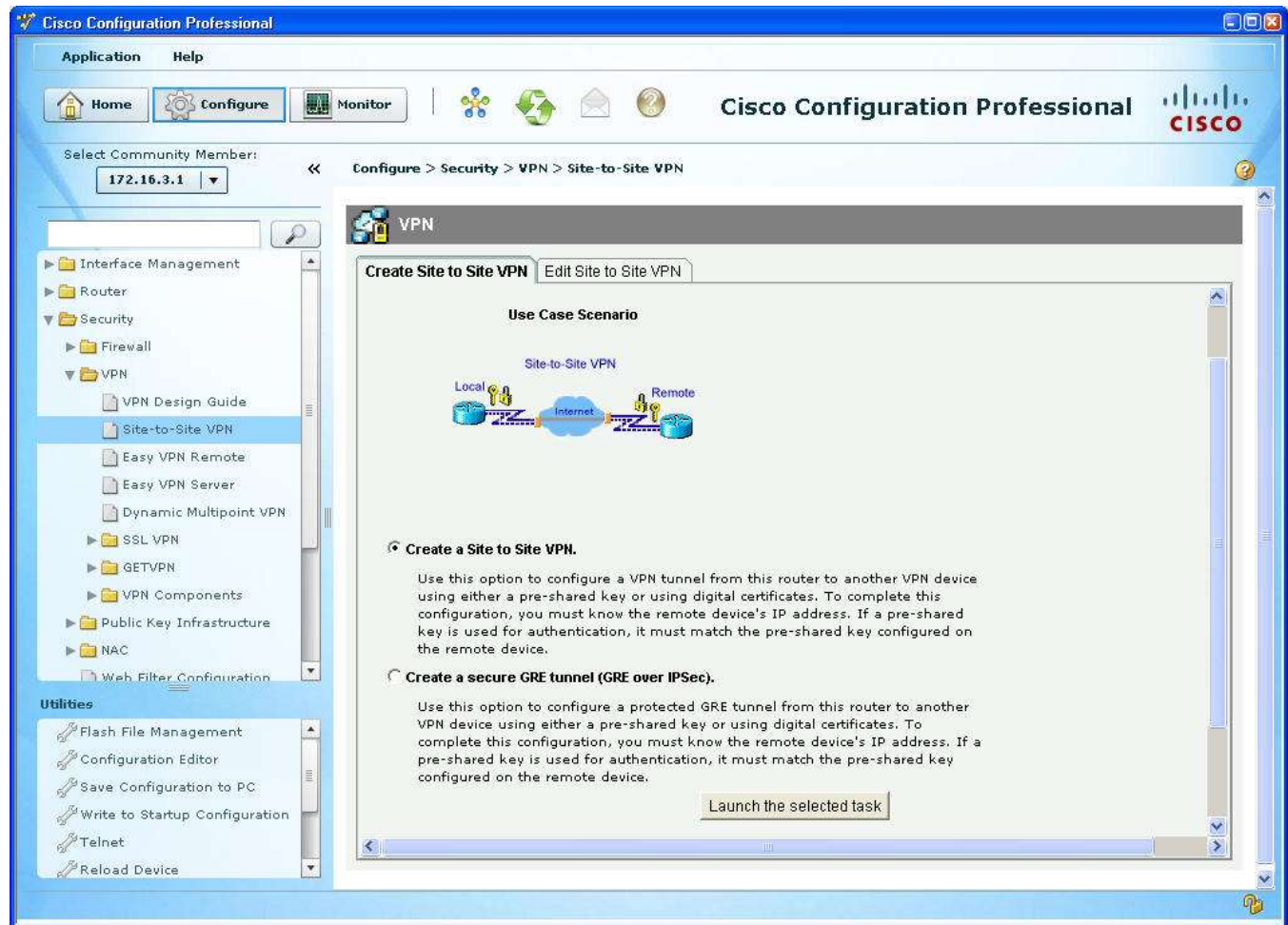
- Click the **Configure** button at the top of the CCP screen, and choose **Security > VPN > Site-to-Site VPN**. Read the on-screen text describing the Site-to-Site VPN.

What must you know to complete the configuration?

---



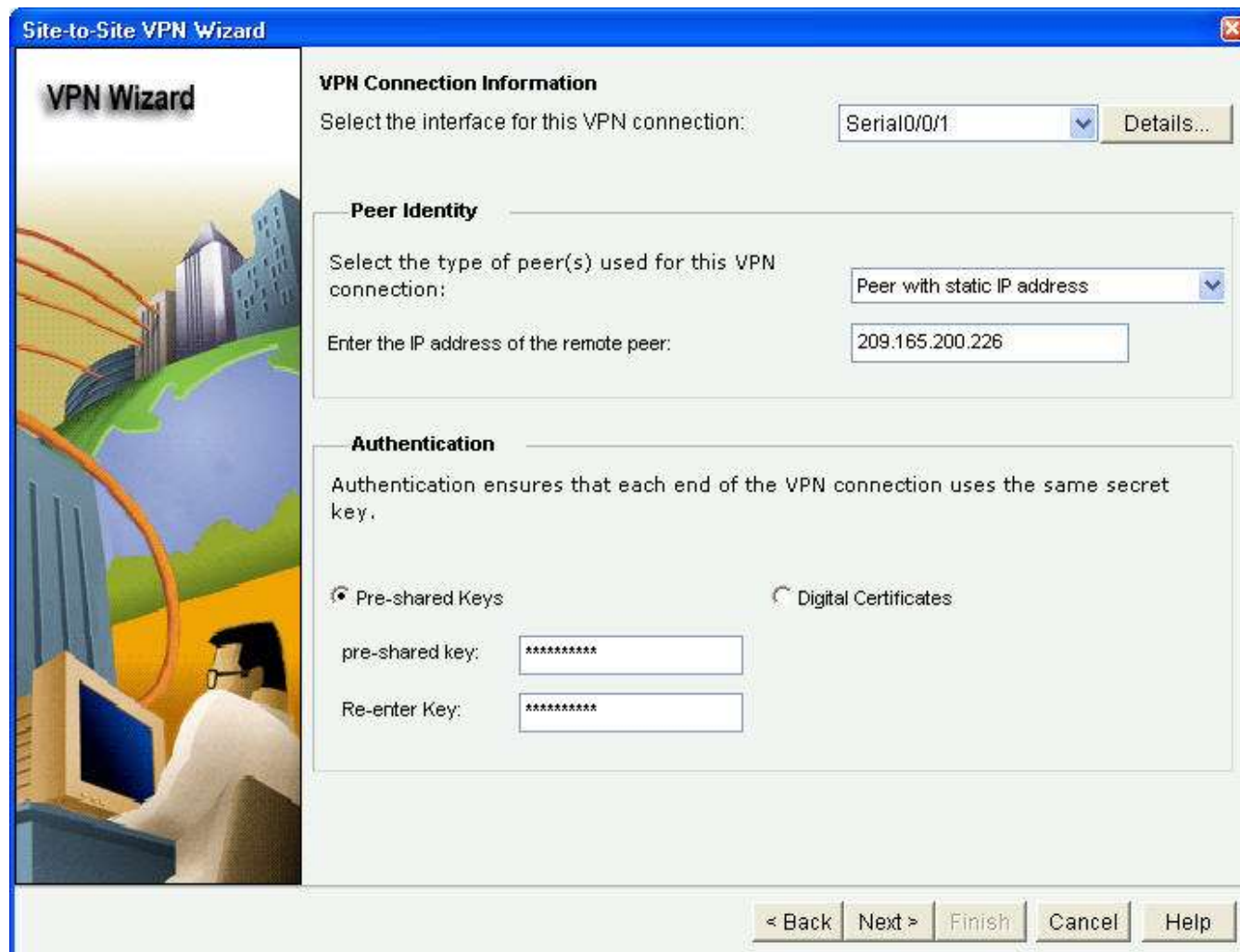
---



- b. Click the **Launch the selected task** button to begin the CCP Site-to-Site VPN wizard.
- c. From the initial Site-to-Site VPN wizard screen, choose the **Step by step wizard**, and then click **Next**.

### Step 3: Configure basic VPN connection information settings.

- a. On the VPN Connection Information screen, select the interface for the connection, which should be R3 Serial0/0/1.
- b. In the Peer Identity section, select **Peer with static IP address** and enter the IP address of the remote peer, ASA interface E0/0 (209.165.200.226).
- c. In the Authentication section, click **Pre-shared Keys**, and enter the pre-shared VPN key **cisco12345**. Re-enter the key for confirmation. This key authenticates the initial exchange to establish the Security Association (SA) between devices. When finished, your screen should look similar to the following. Once you have entered these settings correctly, click **Next**.

The screenshot shows the 'Site-to-Site VPN Wizard' window. On the left is a vertical sidebar with the title 'VPN Wizard' and an illustration of a person at a computer with a cityscape in the background. The main area is titled 'VPN Connection Information' and contains three sections: 'VPN Connection Information' with a dropdown menu set to 'Serial0/0/1' and a 'Details...' button; 'Peer Identity' with a dropdown set to 'Peer with static IP address' and a text field for the IP address '209.165.200.226'; and 'Authentication' with a description, radio buttons for 'Pre-shared Keys' (selected) and 'Digital Certificates', and two text fields for a pre-shared key, both containing eight asterisks. At the bottom are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

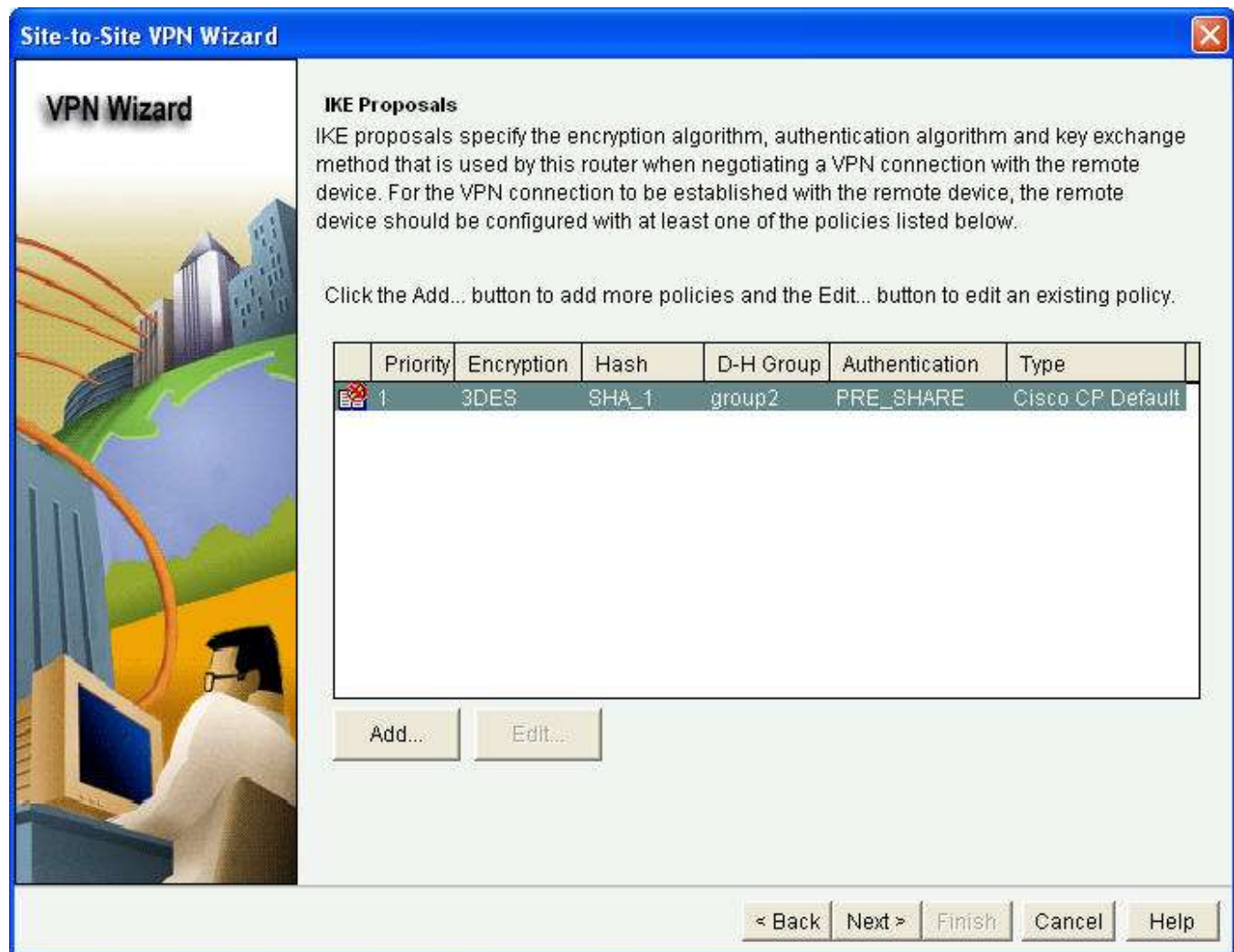
#### Step 4: Specify IKE Policy.

IKE Phase 1 policies are used while setting up the control channel between the two VPN endpoints for key exchange. This is also referred to as the IKE secure association (SA). In contrast, the IPsec policy is used during IKE Phase 2 to negotiate an IPsec security association to pass target data traffic.

On the IKE Proposals screen, a default policy proposal is displayed with a priority of 1. You can use this one or create a new one, if necessary. In this lab you will configure the R3 end of the VPN tunnel using the default IKE proposal. Click **Next** to continue.

Settings for the CCP default IKE Phase 1 policy for this ISR are:

- **Priority** = 1
- **Encryption** = 3DES
- **Hash** = SHA\_1
- **D-H Group** = group2
- **Authentication** = PRE\_SHARE



### Step 5: Configure a transform set.

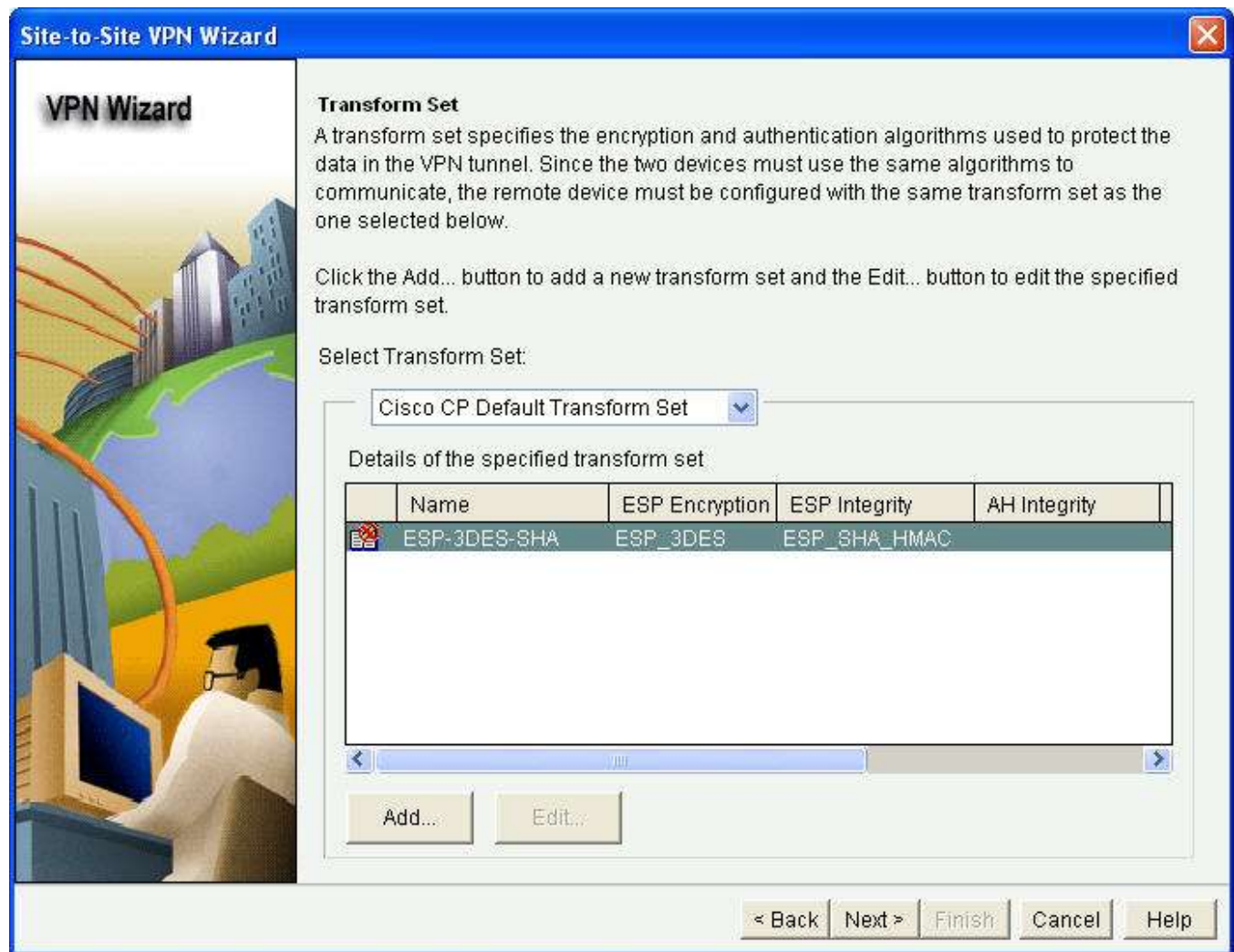
The transform set is the IPsec policy used to encrypt, hash, and authenticate packets that pass through the tunnel. The transform set is the IKE Phase 2 policy.

On the Transform Set screen, a default transform set is displayed. You can use this one or create a new one, if necessary. In this lab you will configure the R3 end of the VPN tunnel using the default transform set. Click **Next** to continue.

Settings for the CCP default IKE Phase 2 policy transform set for this ISR are:

- **Name** = ESP-3DES-SHA
- **ESP Encryption** = ESP\_3DES
- **ESP Integrity** = ESP\_SHA\_HMAC
- **Mode** = Tunnel

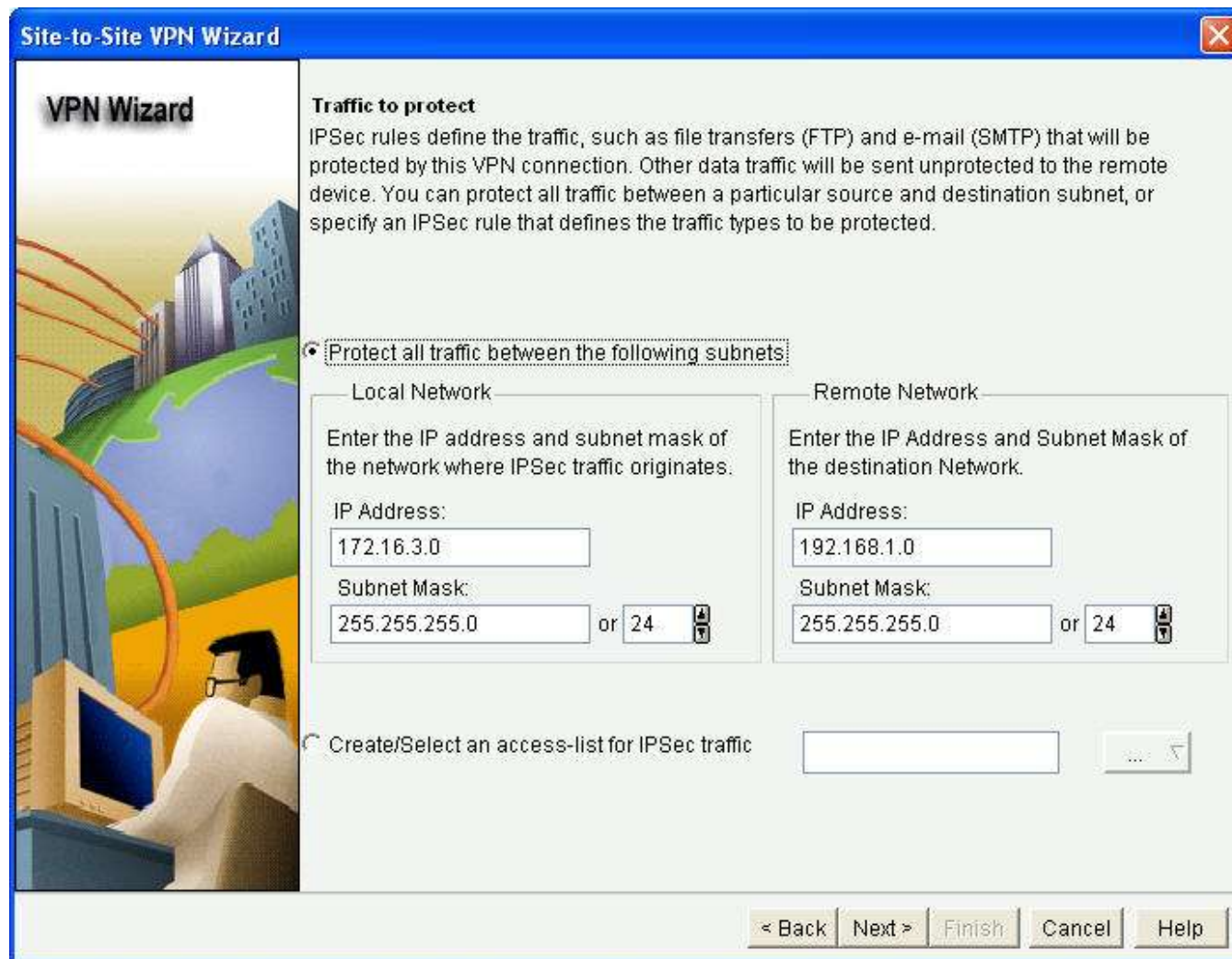




### Step 6: Specify traffic to protect.

You must define “interesting” traffic to be protected through the VPN tunnel. Interesting traffic is defined through an access list that is applied to the router. By entering the source and destination subnets that you would like to protect through the VPN tunnel, CCP generates the appropriate simple access list for you.

On the Traffic to protect screen, enter the information shown below. These are the opposite of the settings to be configured on the ASA later in the lab. When finished, click **Next**.



**Site-to-Site VPN Wizard**

**VPN Wizard**

**Traffic to protect**  
IPSec rules define the traffic, such as file transfers (FTP) and e-mail (SMTP) that will be protected by this VPN connection. Other data traffic will be sent unprotected to the remote device. You can protect all traffic between a particular source and destination subnet, or specify an IPSec rule that defines the traffic types to be protected.

☒ **Protect all traffic between the following subnets:**

Local Network	Remote Network
Enter the IP address and subnet mask of the network where IPSec traffic originates.	Enter the IP Address and Subnet Mask of the destination Network.
IP Address: 172.16.3.0	IP Address: 192.168.1.0
Subnet Mask: 255.255.255.0 or 24	Subnet Mask: 255.255.255.0 or 24

☐ Create/Select an access-list for IPSec traffic

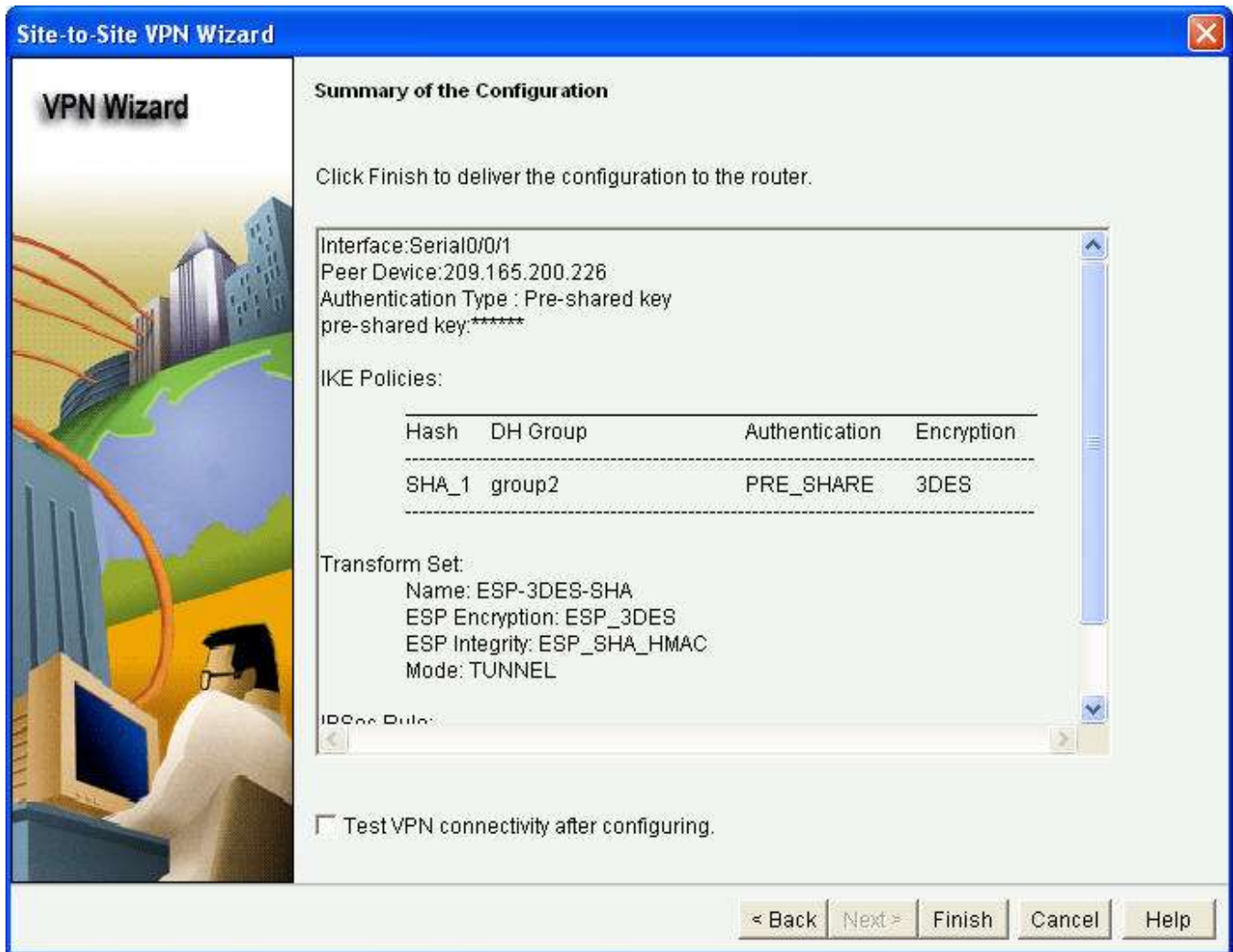
< Back   Next >   Finish   Cancel   Help

### Step 7: Review the summary of the configuration.

- Review the Summary of the Configuration screen. It should look similar to the one below. You can scroll down to see the IPsec rule (ACL) that CCP creates for R3, which permits all traffic from network 172.16.3.0/24 to network 192.168.1.0/24.
- Do NOT select the checkbox for **Test VPN connectivity after configuring**. This will be done after you configure the ASA side of the VPN tunnel.

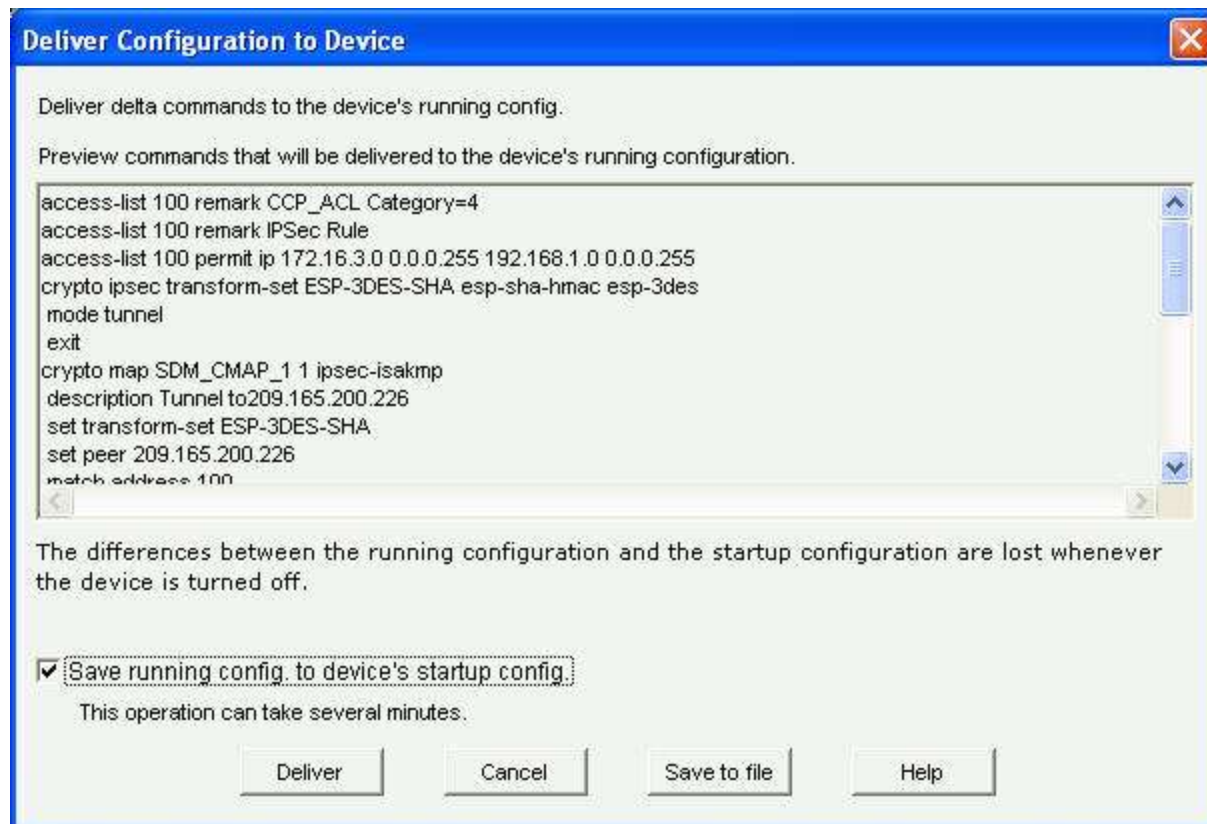
Click **Finish** to go to the Deliver Configuration to Device screen.

**Note:** Pay particular attention to the IKE Policies and Transform Set as you will configure the ASA to match these settings in the next part of the lab.



- c. On the Deliver Configuration to Device screen, select **Save running config. to device's startup config.** and click the **Deliver** button. After the commands have been delivered, click **OK**.
- d. You can also save these configuration commands for later editing or documentation purposes by clicking the **Save to file** button.

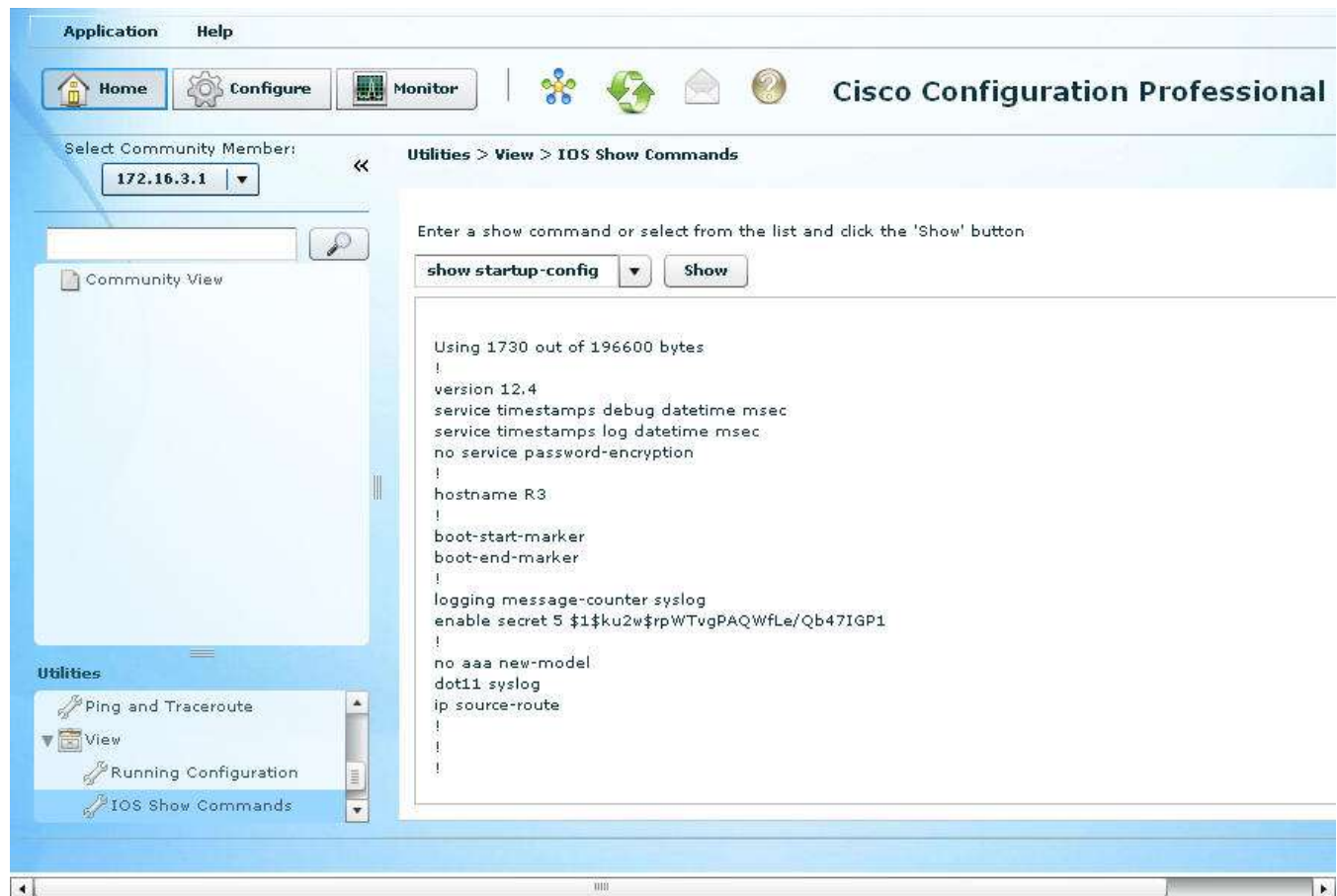




**Note:** If you receive an error message that CCP was unable to copy the running-config to the startup-config, you can verify that the commands were delivered by using the `show startup-config` CLI command on R3. If the startup-config has not been updated, use the `copy run start` command on R3.

- e. You can view the running config and startup config from within CCP. To view the running config, click the **Home** button, and under the Utilities section at the bottom left of the screen, click **View > Running Configuration**. The running config will display.
- f. To view the startup config, click the **Home > Utilities > View > IOS Show Commands**. Click the pull-down menu next to the command window, select the `show startup-config` command and then click the **Show** button. The startup configuration will display.

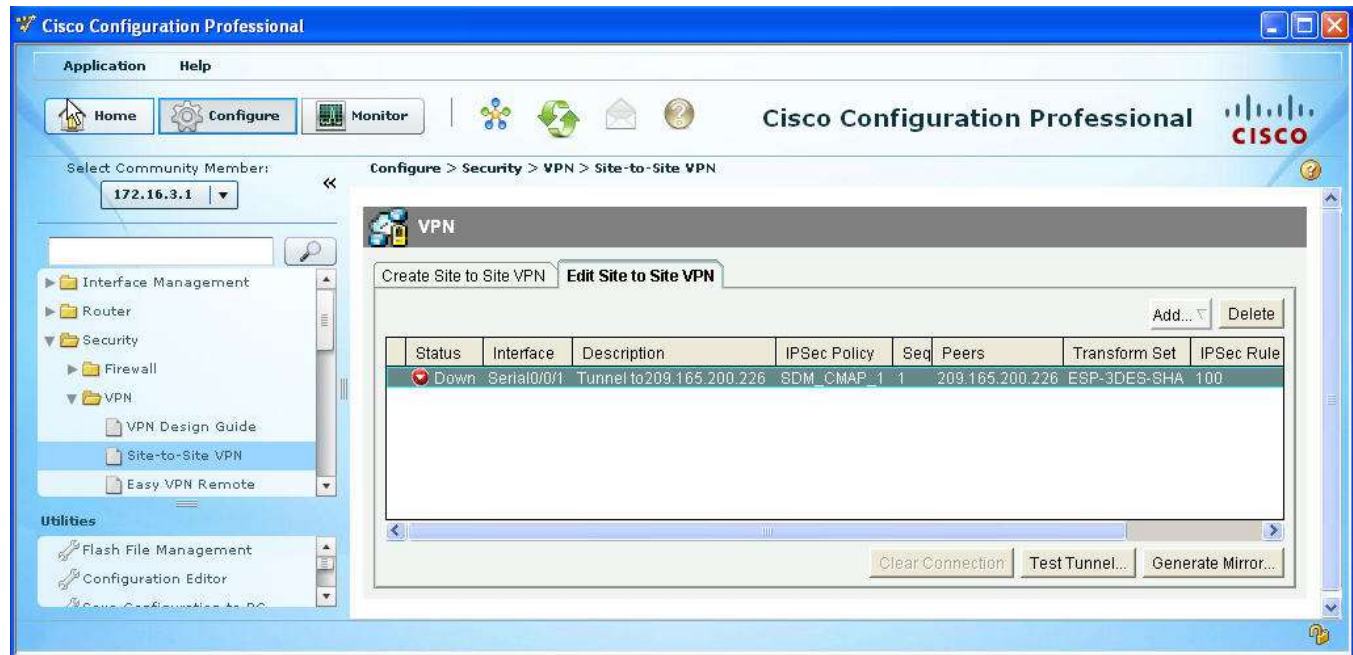
**Note:** There are several pre-defined `show` commands listed in the pull-down menu but you can also enter any valid IOS command, such as `show ip interface brief`, and then click the **Show** button.



### Step 8: Review the Site to Site VPN tunnel configuration.

- a. The Edit Site-to-Site VPN screen is displayed after the commands are delivered. To return to this screen, choose **Configure > Security > VPN > Site-to-Site VPN** and click the **Edit Site to Site VPN** tab. Use the scroll buttons to examine the configuration. The tunnel status is down at this point because the ASA end of the tunnel is not yet configured.

**Note:** Leave CCP running and connected to R3 on PC-C. You will use the **Test Tunnel** button on this screen to verify VPN functionality after configuring the ASA end of the tunnel.



## Part 4: Configuring the ASA as a Site-to-Site IPsec VPN Endpoint Using ASDM


In Part 4 of this lab, you will configure the ASA as an IPsec VPN tunnel endpoint. The tunnel between the ASA and R3 passes through R1 and R2.

### Step 1: Access ASDM.


- Open a browser on PC-B and test the HTTPS access to the ASA by entering **https://192.168.1.1**.

**Note:** Be sure to specify the HTTPS protocol in the URL.

- After entering the URL above, you should see a security warning about the website security certificate. Click **Continue to this website**. Click **Yes** for any other security warnings. At the ASDM welcome page, click the **Run ASDM** button. The ASDM-IDM Launcher will display. Login as user **admin** with password **cisco123**. ASDM will load the current configuration into the GUI.



# Cisco ASDM 6.4(5)



Cisco ASDM 6.4(5) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco security appliances.

Cisco ASDM can run as a local application or as a Java Web Start application.

### Run Cisco ASDM as a local application

When you run Cisco ASDM as a local application, it connects to your security appliance from your desktop using SSL. Running Cisco ASDM as an application has these advantages:

- You can invoke ASDM from a desktop shortcut. No browser is required.
- One desktop shortcut allows you to connect to *multiple* security appliances.

[Install ASDM Launcher and Run ASDM](#)

### Run Cisco ASDM as a Java Web Start application

You can run Cisco ASDM as a Java Web Start application that is dynamically downloaded from the security appliance.

- Click **Run ASDM** to run Cisco ASDM.
- Click **Run Startup Wizard** to run the Startup Wizard. The Startup Wizard walks you through, step by step, the initial configuration of your security appliance.

[Run ASDM](#) [Run Startup Wizard](#)

Copyright © 2006-2011 Cisco Systems, Inc. All rights reserved.



## Cisco ASDM-IDM Launcher



Enter username and password for 192.168.1.1

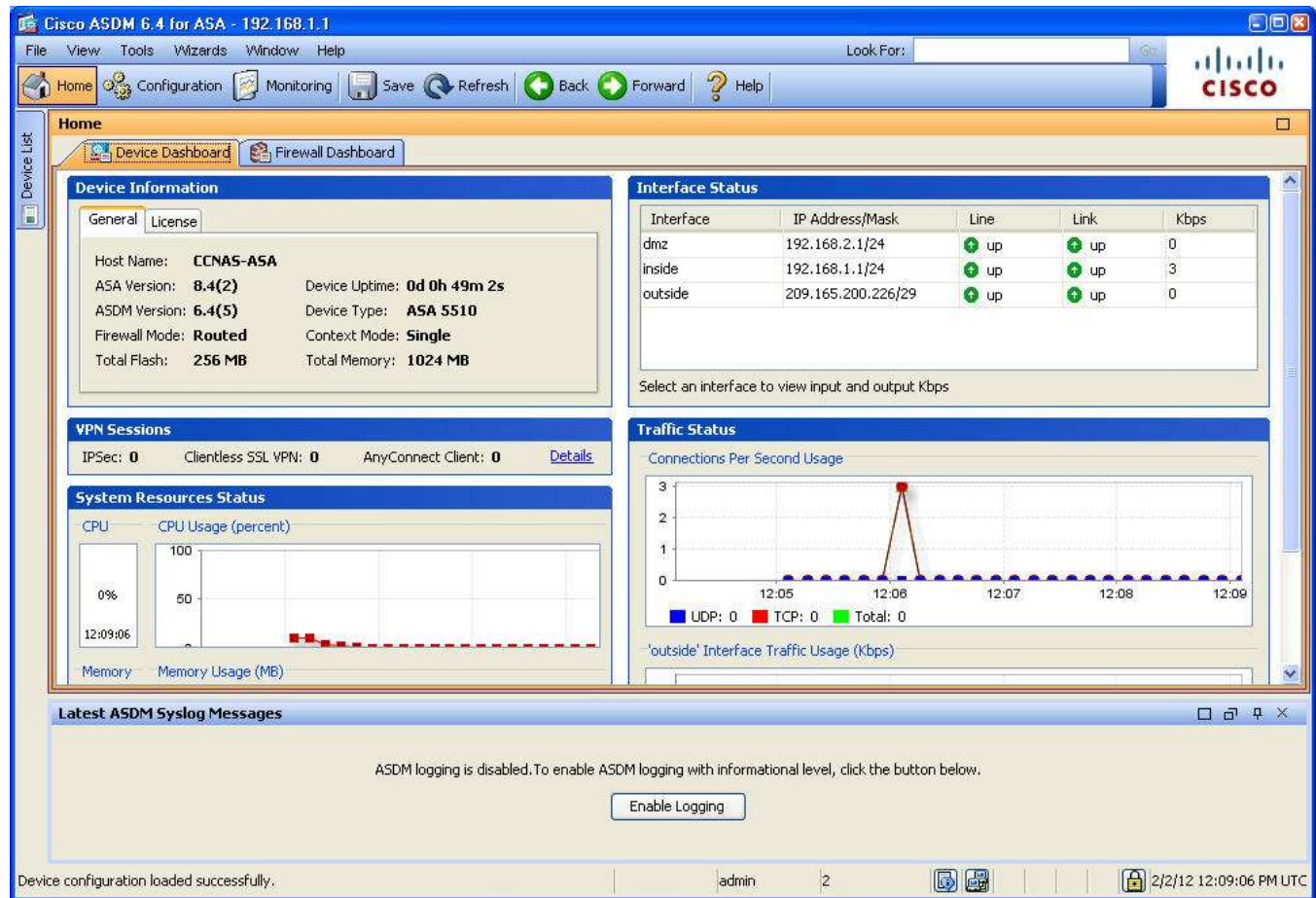
Username:

Password:



## Step 2: Review the ASDM Home screen.

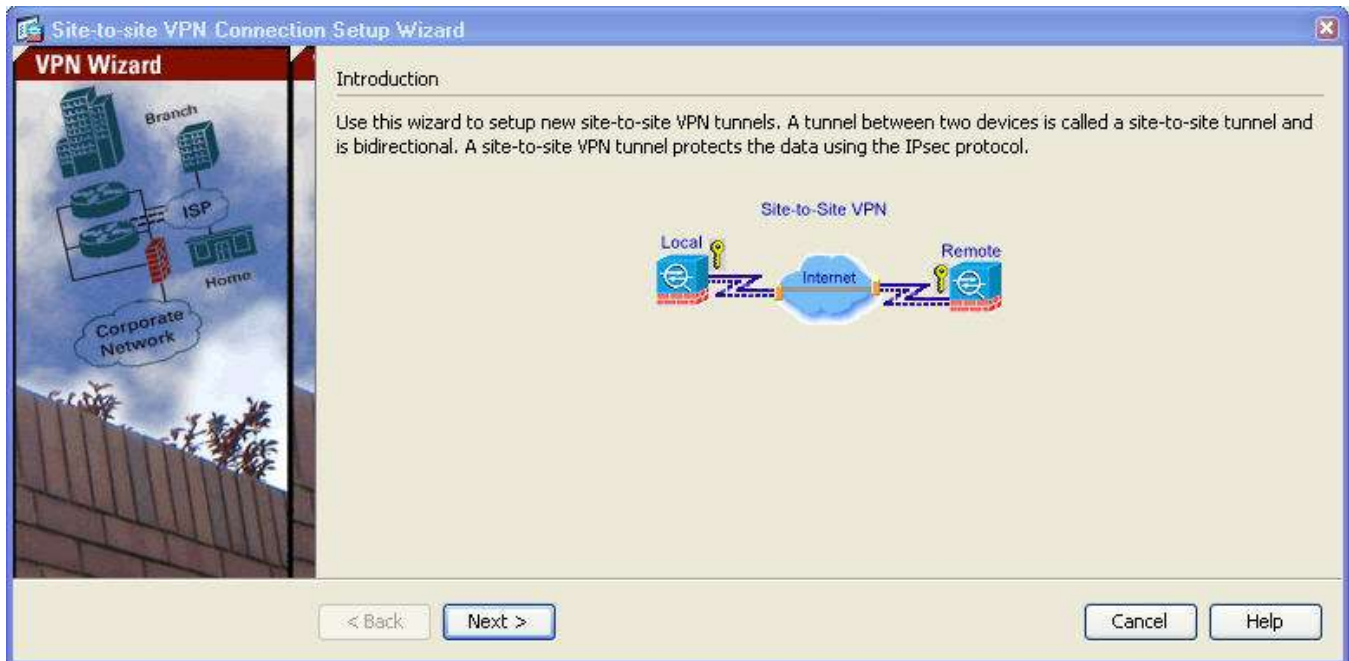
The Home screen displays showing the current ASA device configuration and some traffic flow statistics. Note the inside, outside and dmz interfaces which were configured in Part 2.



## Step 3: Start the VPN wizard.

- From the ASDM main menu, select the **Wizards > VPN Wizards > Site-to-Site VPN Wizard**. The Site-to-Site VPN Connection Setup Wizard Introduction screen is displayed.
- Review the on-screen text and topology diagram, and then click **Next** to continue.





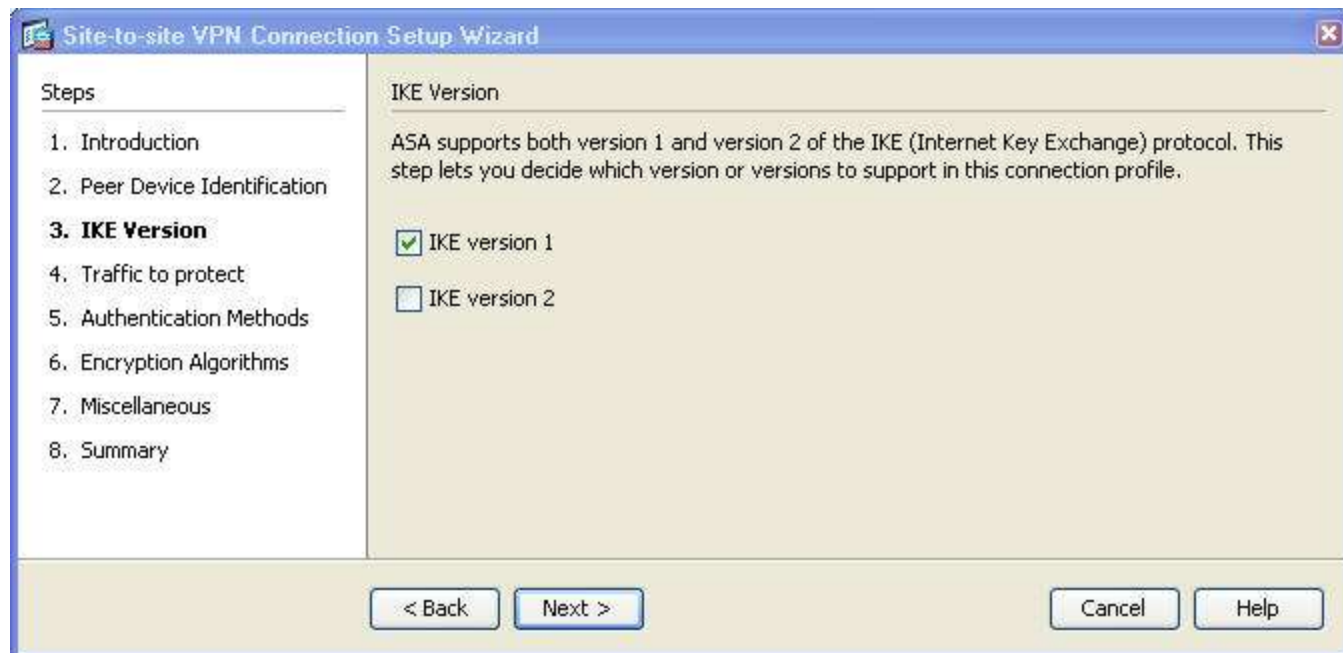
#### Step 4: Configure peer device identification.

On the Peer Device Identification screen, enter the IP address of the R3 Serial0/0/1 interface (**10.2.2.1**) as the Peer IP Address. Leave the default VPN Access Interface set to **outside**. The VPN tunnel will be between R3 S0/0/1 and ASA outside interface E0/0. Click **Next** to continue.



#### Step 5: Specify the IKE version.

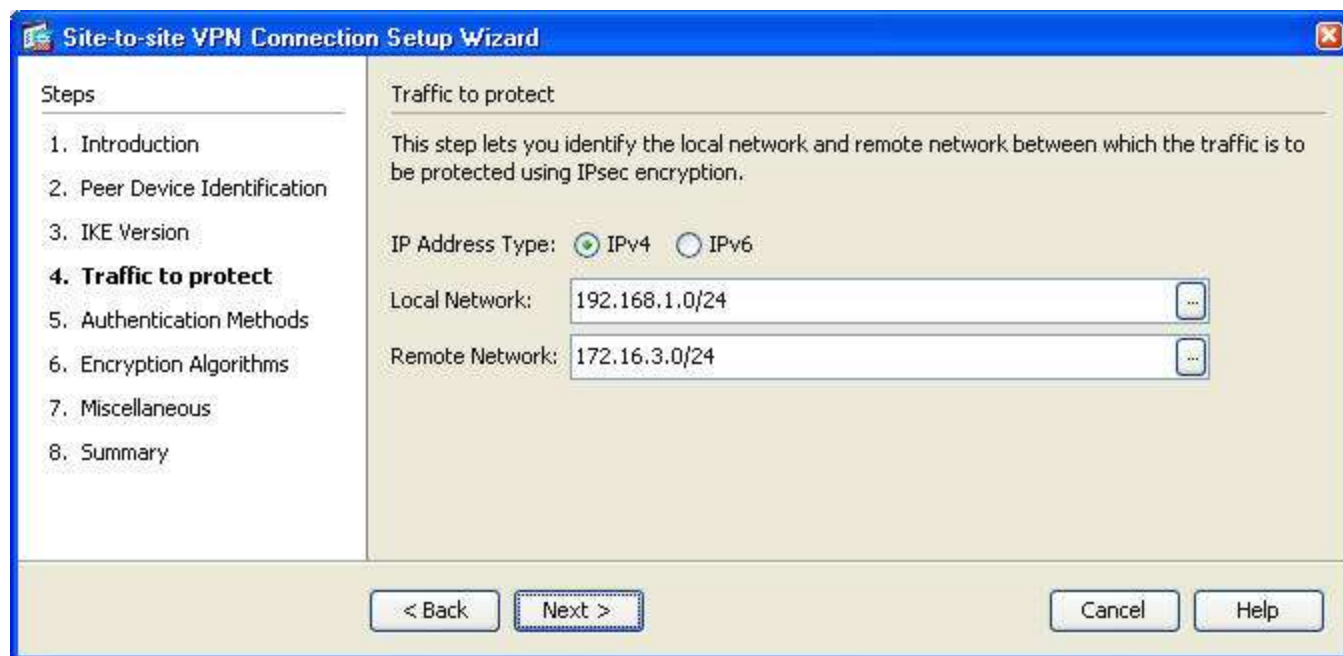
IKE version 1 simple pre-shared keys will be used. On the IKE Version screen, uncheck the **IKE version 2** checkbox and leave **IKE version 1** checked. Click **Next** to continue.



### Step 6: Specify the traffic to protect.

On the Traffic to protect screen, click **IPv4** and enter the inside network **192.168.1.0/24** as the Local Network and the R3 LAN **172.16.3.0/24** as the Remote Network. Click **Next** to continue. A message will display that the certificate information is being retrieved.

**Note:** If the ASA does not respond, you may need to close the window and continue to the next step. If prompted to authenticate, login again as **admin** with the password **cisco123**.



### Step 7: Configure authentication.

On the Authentication Methods screen, enter a Pre-shared Key of **cisco12345**. You will not be using a device certificate so leave it set to **None**. Click **Next** to continue.



### Step 8: Configure Encryption Algorithms (IKE policy and IPsec transform sets).

- a. On the Encryption Algorithms screen, click on the **Manage** button next to **IKE Policy**. Click **OK** to the message that IKE policy is global. On the Configure IKEv1 Policies screen, you will see many policies listed. Only IKE policy 120 is needed to establish the tunnel with R3 so you can delete all policies except 120. If you leave the others they will become part of the ASA configuration and are unnecessary. Select and click **Delete** for all policies except 120.

**Note:** The entire list of policies will be re-populated in the wizard if it is run again, in the event that it is necessary to change the IKE policy.

- b. Click **OK** to accept policy **120** and return to the Encryption Algorithms screen.
  - **Name** = pre-share-3des-sha
  - **Encryption** = 3DES
  - **Hash** = sha
  - **D-H Group** = 2
  - **Authentication** = pre-share
  - **Lifetime** = 86400
- c. On the Encryption Algorithms screen, click on the **Select** button next to IPsec Proposal. On the Select IPsec Proposals (Transform Sets) screen, remove all IPsec proposal entries from the Assigned entry field, except for ESP-3DES-SHA as this is the one R3 is using. All of the transform sets listed will still be inserted into the final ASA configuration but the crypto map only draws on the specific transform-set identified.
  - **Name** = ESP-3DES-SHA
  - **Mode** = Tunnel
  - **ESP Encryption** = 3DES
  - **ESP Authentication** = SHA
- d. Click **OK** to assign the IPsec proposal and return to the Encryption Algorithms screen. When finished, the screen should look like the one below. Click **Next** to continue.





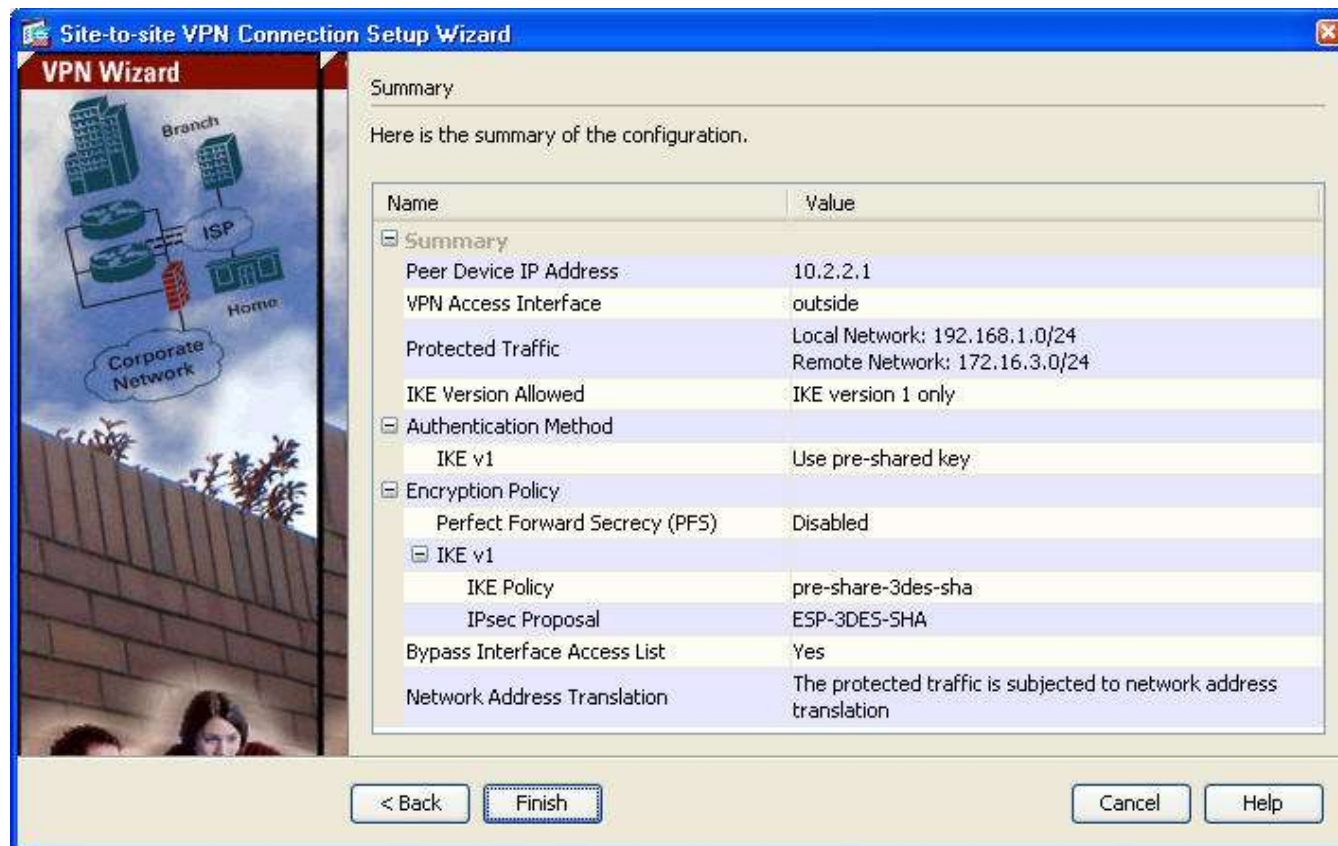
### Step 9: Configure Miscellaneous settings.

On the Miscellaneous screen, select the checkbox to **Enable inbound IPsec sessions to bypass interface access lists**. Select the checkbox to **Exempt ASA side host/network from address translation** for the **inside** interface. Click **Next** to continue.

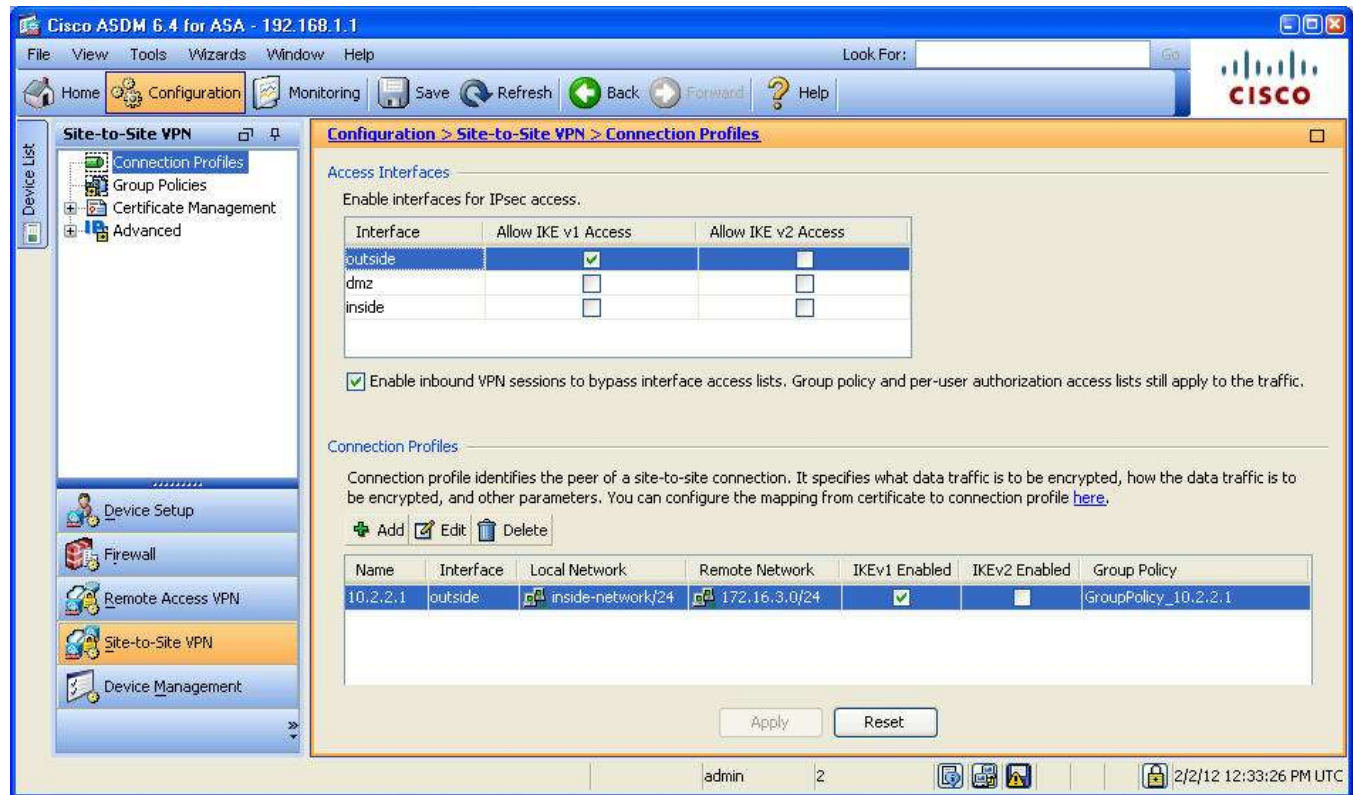


**Step 10: Review the configuration summary and deliver the commands to the ASA.**

- a. The Summary page is displayed next. Verify that the information configured in the Site-to-Site VPN wizard is correct. You can click the **Back** button to make changes or click **Cancel** and restart the VPN wizard (recommended).
- b. Click **Finish** to complete the process and deliver the commands to the ASA. If prompted to authenticate, login again as **admin** with a password of **cisco123**.

**Step 11: Verify the ASA VPN connection profile.**

The Configurations > Site-to-Site VPN > Connection Profiles screen will display showing the settings you just configured. From this window the VPN configuration can be verified and edited.

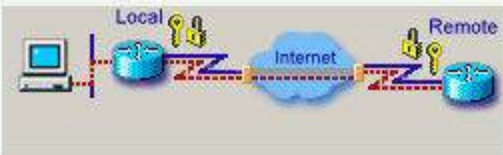


## Step 12: Test the VPN configuration from R3 using CCP.

- On PC-C, use CCP to test the IPsec VPN tunnel between the R3 ISR and the ASA. Choose **Configure > Security > VPN > Site-to-Site VPN** and click the **Edit Site to Site VPN** tab.
- From the Edit Site to Site VPN tab, click **Test Tunnel**.
- When the VPN Troubleshooting window displays, click the **Start** button to have CCP start troubleshooting the tunnel.
- When the CCP warning window displays indicating that CCP will enable router debugs and generate some tunnel traffic, click **Yes** to continue.
- On the next VPN Troubleshooting screen, the IP address of the host in the source network is displayed by default (R3 Fa0/1 = 172.16.3.1). Enter the IP address of host PC-B in the destination network field (192.168.1.3) and click **Continue** to begin the debugging process.

**VPN Troubleshooting**

Debugging the VPN session requires that VPN traffic be generated.



VPN traffic on this connection is defined as:

Action	Source	Destination	Service	Log
✓ Permit	172.16.3.0/0.0.0.255	192.168.1.0/0.0.0.255	ip	

☒ Have Cisco CP generate VPN traffic

Generate VPN Traffic by doing an extended ping to one of the hosts in destination network

Enter the IP address of a host in the source network :

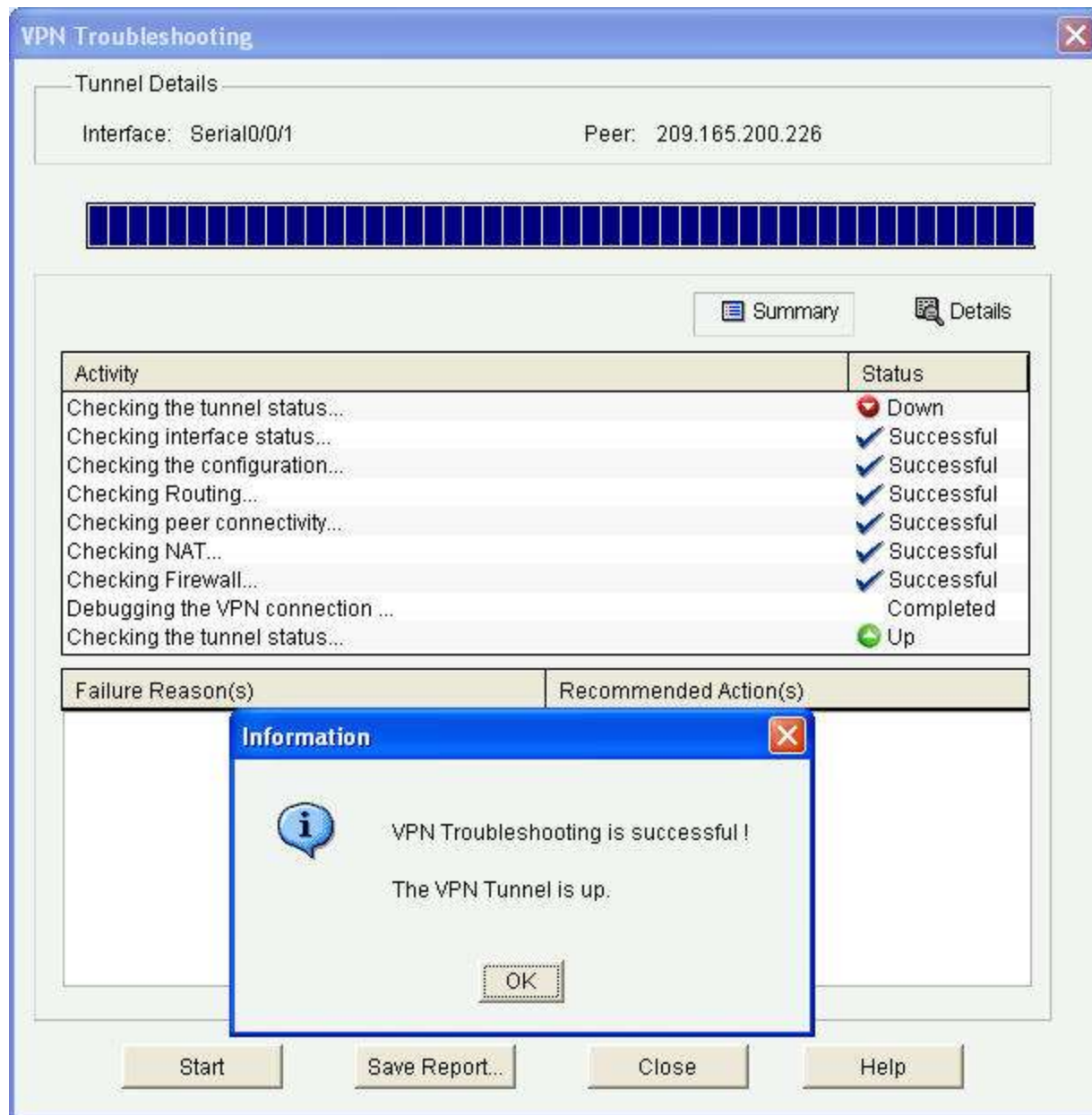
Enter the IP address of a host in the destination network:

☐ I will generate VPN traffic from the source network

VPN traffic can be generated by invoking an application that generates traffic on the VPN tunnel. This can be done from any host in the source network. Enter sufficient wait time.

Wait interval time (in minutes)

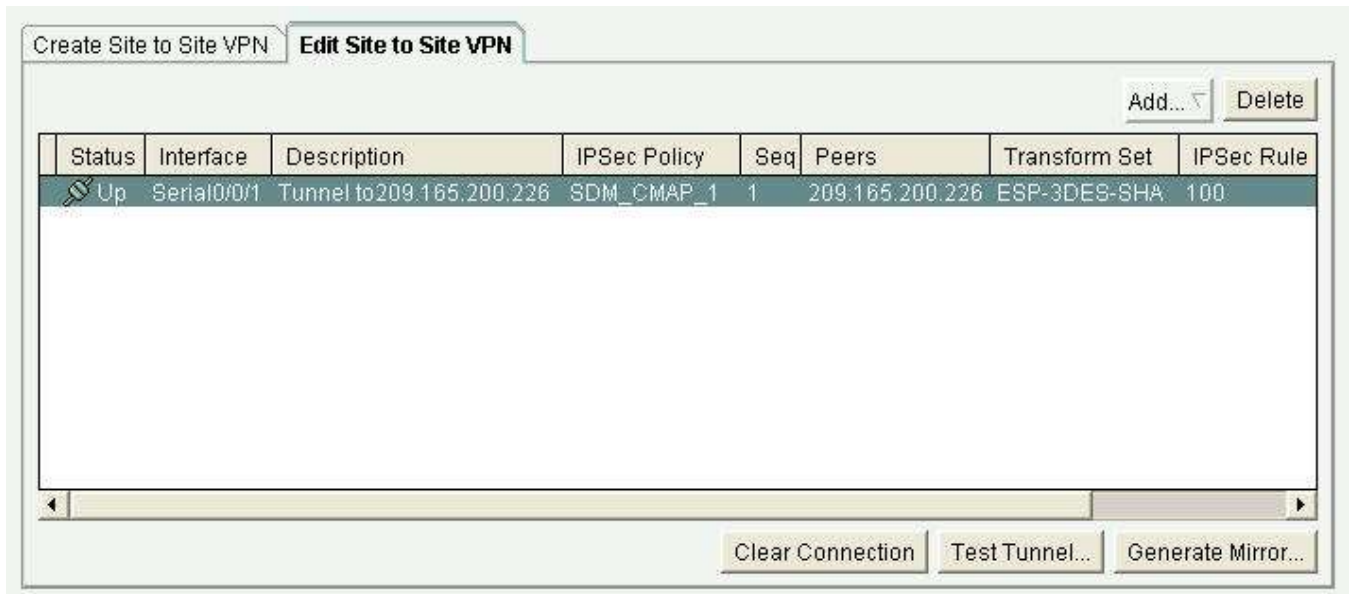
- f. If the debug is successful and the tunnel is up, you should see the screen below. If the testing fails, CCP displays failure reasons and recommended actions. Click **OK** to remove the window.



- g. You can save the report if desired; otherwise, click **OK** and then **Close**.
- h. On PC-C (CCP for R3), choose **Configure > Security > VPN > Site-to-Site VPN** and click the **Edit Site to Site VPN** tab. The tunnel Status should now be up.

**Note:** If you want to reset the tunnel and test again, you can click the **Clear Connection** button from the **Edit Site to Site VPN** window.





- i. You can further verify tunnel functionality by pinging from branch office PC-C to PC-B on the internal network. The pings should be successful.

**Note:** Without the tunnel in place and bypassing NAT, it would be impossible for PC-C on the external network to ping PC-B on the private internal network.

### Step 13: Use ASDM Monitoring to verify the tunnel.

- a. From the ASDM menu bar, select Monitoring and click VPN from the panels at the lower left of the screen. Click **VPN Statistics > Sessions**. Click the **Filter By** drop down menu and select **IPsec Site-to-Site**. You should see the Site-to-Site IPsec VPN tunnel listed and active, as well as current VPN session information and statistics.

Cisco ASDM 6.4 for ASA - 192.168.1.1

File View Tools Wizards Window Help Look For:  Go

Home Configuration Monitoring Save Refresh Back Forward Help

Device List

- VPN
  - VPN Statistics
    - Sessions
    - Crypto Statistics
    - Compression Statistics
    - Encryption Statistics
    - Global IKE/IPsec Statistics
    - NAC Session Summary
    - Protocol Statistics
    - VLAN Mapping Sessions
  - Clientless SSL VPN
  - VPN Connection Graphs
  - WSA Sessions
- Interfaces
- VPN
- Routing
- Properties
- Logging

Monitoring > VPN > VPN Statistics > Sessions

Type	Active	Cumulative	Peak Concurrent	Inactive
Site-to-Site VPN	1	1		1
IKEv1 IPsec	1	1		1

Filter By: IPsec Site-to-Site -- All Sessions -- Filter

Connection Profile	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
10.2.2.1	10.2.2.1	IKEv1 IPsec	3DES	12:36:52 UTC Thu Feb 2 2012	0h:02m:03s	2900	2900

Details Logout Ping

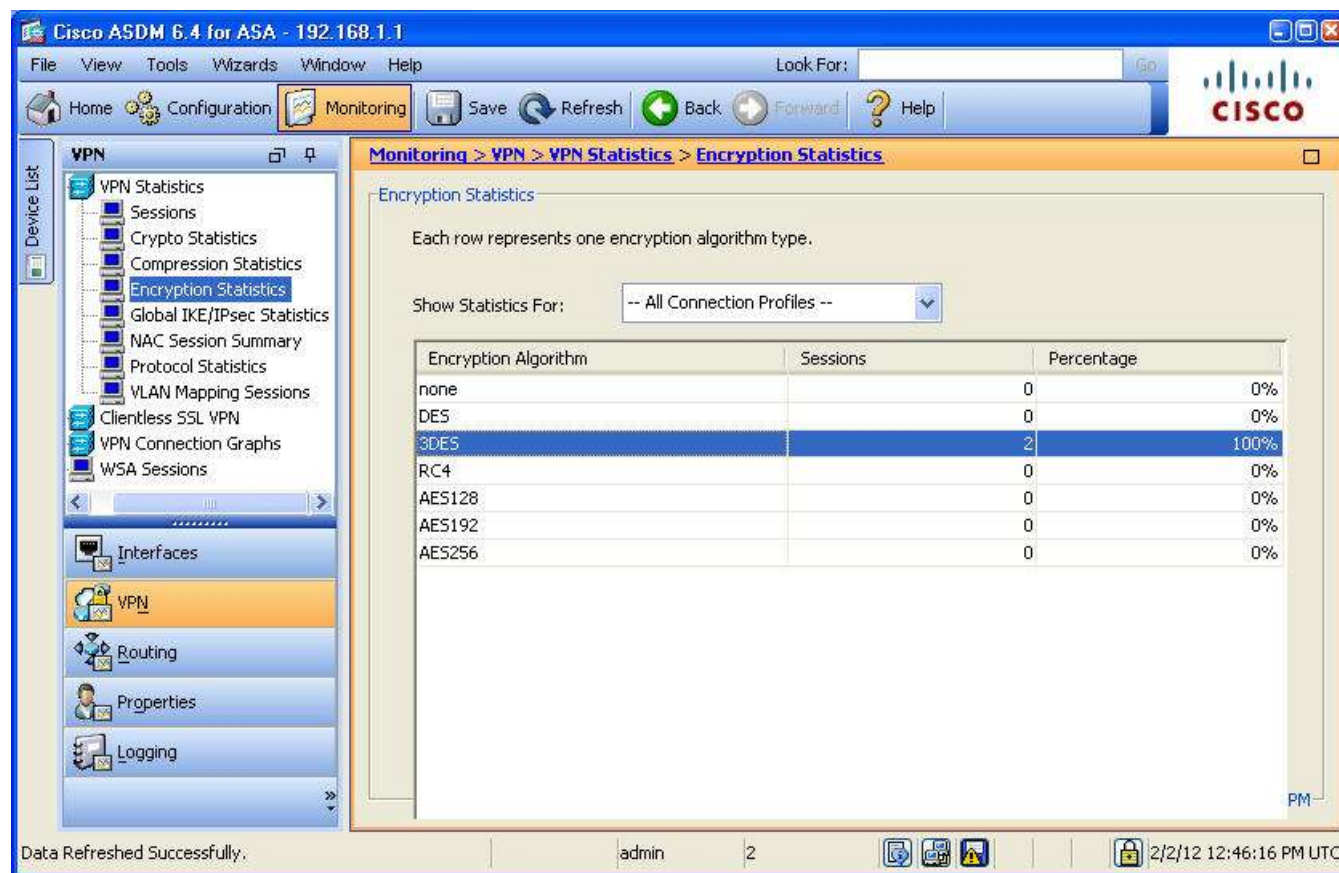
To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

Logout By: -- All Sessions -- Logout Sessions Refresh

Last Updated: 2/15/12 11:15:46 PM

Data Refreshed Successfully. admin 2 2/2/12 12:44:46 PM UTC

- b. Click **Encryption Statistics**. You should see one or more sessions using the 3DES encryption algorithm.



The screenshot shows the Cisco ASDM 6.4 for ASA - 192.168.1.1 interface. The left sidebar has the 'VPN' menu expanded, and 'Encryption Statistics' is selected. The main pane displays the 'Encryption Statistics' page, which includes a dropdown menu for 'Show Statistics For' set to '-- All Connection Profiles --'. Below this is a table showing encryption statistics.

Encryption Algorithm	Sessions	Percentage
none	0	0%
DES	0	0%
3DES	2	100%
RC4	0	0%
AES128	0	0%
AES192	0	0%
AES256	0	0%

Data Refreshed Successfully. admin 2 2/2/12 12:46:16 PM UTC

- c. Click **Crypto Statistics**. You should see values for the number of packets encrypted and decrypted as well as security association (SA) requests, etc.



Cisco ASDM 6.4 for ASA - 192.168.1.1

File View Tools Wizards Window Help Look For:  Go

Home Configuration Monitoring Save Refresh Back Forward Help

Device List

- VPN
  - VPN Statistics
    - Sessions
    - Crypto Statistics
    - Compression Statistics
    - Encryption Statistics
    - Global IKE/IPsec Statistics
    - NAC Session Summary
    - Protocol Statistics
    - VLAN Mapping Sessions
  - Clientless SSL VPN
  - VPN Connection Graphs
  - WSA Sessions
- Interfaces
- VPN
- Routing
- Properties
- Logging

Monitoring > VPN > VPN Statistics > Crypto Statistics

Crypto Statistics

Each row represents one crypto statistic.

Show Statistics For: All

Statistic	Value
Encrypt packet requests	81
Encapsulate packet requests	81
Decrypt packet requests	82
Decapsulate packet requests	82
HMAC calculation requests	98
SA creation requests	1
SA rekey requests	0
SA deletion requests	0
Next phase key allocation requests	2
Random number generation requests	0
Failed requests	0
Encrypt packet requests	0
Encapsulate packet requests	0
Decrypt packet requests	0
Decapsulate packet requests	0
HMAC calculation requests	0

Data Refreshed Successfully.

admin 2

2/2/12 12:50:26 PM UTC

**Reflection:**

1. What are some situations where a site-to-site IPsec VPN would be preferable as compared to a remote access SSL VPN?

---

---

---

---

2. What are some situations where a remote access VPN would be preferable as compared to site-to-site VPN?

---

---

---

---

**Router Interface Summary Table**

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (Fa0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2800	Fast Ethernet 0/0 (Fa0/0)	Fast Ethernet 0/1 (Fa0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
<b>Note:</b> To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				