Chapter 8 Lab B: Configuring a Remote Access VPN Server and Client

Topology

Note: ISR G2 devices have Gigabit Ethernet interfaces instead of FastEthernet Interfaces.
IP Addressing Table

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Default Gateway</th>
<th>Switch Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Fa0/1</td>
<td>192.168.1.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
<td>S1 Fa0/5</td>
</tr>
<tr>
<td></td>
<td>S0/0/0 (DCE)</td>
<td>10.1.1.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>R2</td>
<td>S0/0/0</td>
<td>10.1.1.2</td>
<td>255.255.255.252</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>S0/0/1 (DCE)</td>
<td>10.2.2.2</td>
<td>255.255.255.252</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>R3</td>
<td>Fa0/1</td>
<td>192.168.3.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
<td>S3 Fa0/5</td>
</tr>
<tr>
<td></td>
<td>S0/0/1</td>
<td>10.2.2.1</td>
<td>255.255.255.252</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>PC-A</td>
<td>NIC</td>
<td>192.168.1.3</td>
<td>255.255.255.0</td>
<td>192.168.1.1</td>
<td>S1 Fa0/6</td>
</tr>
<tr>
<td>PC-C</td>
<td>NIC</td>
<td>192.168.3.3</td>
<td>255.255.255.0</td>
<td>192.168.3.1</td>
<td>S3 Fa0/18</td>
</tr>
</tbody>
</table>

Objectives

**Part 1: Basic Router Configuration**
- Configure host names, interface IP addresses, and access passwords.
- Configure static routing.

**Part 2: Configuring a Remote Access VPN**
- Configure a zone-based firewall (ZBF) on R3 using CCP.
- Configure Router R3 to support Cisco Easy VPN Server using CCP.
- Configure the Cisco VPN Client on PC-A and connect to R3.
- Verify the configuration.
- Test VPN functionality.

Background

VPNs can provide a secure method of transmitting data over a public network, such as the Internet. A common VPN implementation is used for remote access to a corporate office from a telecommuter location such as a small office or home office (SOHO).

In this lab, you build a multi-router network and configure the routers and hosts. You configure a remote access IPsec VPN between a client computer and a simulated corporate network. You start by using CCP to configure a zoned-based firewall (ZBF) to prevent connections from outside the corporate network. You next use CCP to configure Cisco Easy VPN Server on the corporate gateway router. Finally, you configure the Cisco VPN Client on a host and connect to the corporate network through a simulated ISP router.

The Cisco VPN Client allows organizations to establish end-to-end, encrypted (IPsec) VPN tunnels for secure connectivity for mobile employees or teleworkers. It supports Cisco Easy VPN, which allows the client to receive security policies upon a VPN tunnel connection from the central site VPN device (Cisco Easy VPN Server), minimizing configuration requirements at the remote location. Easy VPN is a scalable solution for remote access deployments for which it is impractical to individually configure policies for multiple remote PCs.

Router R1 represents a remote site, and R3 represents the corporate headquarters. Host PC-A simulates an employee connecting from home or a small office over the Internet. Router R2 simulates an Internet ISP router and acts as a passthrough with no knowledge of the VPN connection running through it.

**Note:** The router commands and output in this lab are from a Cisco 1841 with Cisco IOS Release 12.4(20)T (Advanced IP image). Other routers and Cisco IOS versions can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab.
Depending on the router model and Cisco IOS version, the commands available and the output produced might vary from what is shown in this lab.

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

### Required Resources

- 3 routers with Cisco 1841 with Cisco IOS Release 12.4(20)T1 or comparable
- 2 switches (Cisco 2960 or comparable)
- PC-A: Windows XP, Vista, or Windows 7 with Cisco VPN Client
- PC-C: Windows XP, Vista, or Windows 7 with CCP 2.5 installed
- Serial and Ethernet cables as shown in the topology
- Rollover cables to configure the routers via the console

**CCP Notes:**

- Refer to Chp 00 Lab A for instructions on how to install 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 Configuration

In Part 1, you set up the network topology and configure basic settings, such as the interface IP addresses and static routing. Perform the steps on the routers as indicated.

Step 1: Cable the network as shown in the topology.
Attach the devices shown in the topology diagram, and cable as necessary.

Step 2: Configure basic settings for all routers.

a. Configure host names as shown in the topology.
b. Configure the physical interface IP addresses as shown in the IP addressing table.
c. Configure a clock rate for the routers with a DCE serial cable attached to their serial interface.
   ```
   R1(config)# interface S0/0/0
   R1(config-if)# clock rate 64000
   ```
d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
   ```
   R1(config)# no ip domain-lookup
   ```

Step 3: Configure static default routes on R1 and R3.

Configure a static default route from R1 to R2 and from R3 to R2.
   ```
   R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2
   R3(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2
   ```

Step 4: Configure static routes on R2.

a. Configure a static route from R2 to the R1 LAN.
   ```
   R2(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.1
   ```
b. Configure a static route from R2 to the R3 LAN.
   ```
   R2(config)# ip route 192.168.3.0 255.255.255.0 10.2.2.1
   ```

Step 5: Configure PC host IP settings.

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

Step 6: Verify connectivity between PC-A and R3.

From PC-A, ping the R3 S0/0/1 interface at IP address 10.2.2.1.
   ```
   PC-A:~> ping 10.2.2.1
   ```
Are the results successful? _____
If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 7: Configure a minimum password length.

Note: Passwords in this lab are set to a minimum of 10 characters, but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

Use the `security passwords` command to set a minimum password length of 10 characters.
   ```
   R1(config)# security passwords min-length 10
   ```
Step 8: Configure the enable secret password and console and vty lines.

a. Configure the enable secret password cisco12345 on R1.
   
   ```
   R1(config)# enable secret cisco12345
   ```

b. Configure a console password and enable login for router R1. For additional security, the exec-timeout command causes the line to log out after 5 minutes of inactivity. The logging synchronous command prevents console messages from interrupting command entry.

   Note: To avoid repetitive logins during this lab, the exec-timeout can be set to 0 0, which prevents it from expiring. However, this is not considered a good security practice.

   ```
   R1(config)# line console 0
   R1(config-line)# password ciscoconpass
   R1(config-line)# exec-timeout 5 0
   R1(config-line)# login
   R1(config-line)# logging synchronous
   ```

c. Configure the password on the vty lines for router R1.

   ```
   R1(config)# line vty 0 4
   R1(config-line)# password ciscovtypass
   R1(config-line)# exec-timeout 5 0
   R1(config-line)# login
   ```

d. Repeat these configurations on R2 and R3.

Step 9: Encrypt clear text passwords.

a. Use the service password-encryption command to encrypt the console, aux, and vty passwords.

   ```
   R1(config)# service password-encryption
   ```

b. Issue the show run command. Can you read the console, aux, and vty passwords? Why or why not?

   ____________________________________________________________

   c. Repeat this configuration on R2 and R3.

Step 10: Configure a login warning banner on routers R1 and R3.

Configure a message-of-the-day (MOTD) warning banner to unauthorized users.

   ```
   R1(config)# banner motd $Unauthorized access strictly prohibited and prosecuted to the full extent of the law$
   ```

Step 11: Save the basic running configuration for all three routers.

   Save the running configuration to the startup configuration from the privileged EXEC prompt.

   ```
   R1# copy running-config startup-config
   ```

Part 2: Configuring a Remote Access VPN

In Part 2 of this lab, configure a firewall and a remote access IPsec VPN. You will use CCP to configure R3 as a VPN server. On PC-C you will enable and configure the Cisco VPN client.

Task 1: Prepare R3 for CCP Access

Step 1: Configure HTTP router access and a AAA user.

a. Enable the HTTP server on R3.
R3(config)# ip http server

Note: For added security, you can enable the HTTP secure server on R3 using the ip http server command. The HTTP server and the HTTP secure server are disabled by default.

b. Create an admin01 account on R3 with privilege level 15 and a password of admin01pass for use with AAA.

   R3(config)# username admin01 privilege 15 password 0 admin01pass

c. Configure R3 so that CCP use the local database to authenticate web sessions.

   R3(config)# ip http authentication local

Step 2: Access CCP and discover R3.

a. Run the CCP application on PC-C. In the Select/Manage Community window, input the R1 IP address 192.168.3.1 in the Hostname/Address field, admin01 in the Username field and admin01pass in the Password field. Click on the OK button.

b. At the CCP Dashboard, click the Discovery button to discover and connect to R3. If the discovery process fails, click the Discover Details button to determine the problem in order to resolve the issue.
Task 2: Configure a ZBF Firewall on R3

Step 1: Use the CCP firewall wizard to configure a zone-based firewall (ZBF) on R3.

a. Click the **Configure** button at the top of the CCP screen, and choose Security > Firewall > Firewall.

b. Choose **Basic Firewall** and click the **Launch the selected task** button. On the Basic Firewall Configuration wizard screen, click Next.

c. Check the **Inside (Trusted)** check box for FastEthernet0/1 and the **Outside (Untrusted)** check box for Serial0/0/1. Click Next. Click OK when the CCP launch warning for Serial0/0/1 is displayed.
d. In the next window, select **Low Security** for the security level and click **Next**.

e. In the Summary window, click **Finish**.

f. Click **Deliver** to send the commands to the router. Click **OK** in the Commands Delivery Status window. Click **OK** on the Information window. You are returned to the Edit Firewall Policy tab as shown below.

---

**Step 2: Verify firewall functionality.**

a. From PC-C, ping the R2 interface S0/0/1 at IP address 10.2.2.2.
Are the pings successful? Why or why not?

b. From external router R2, ping PC-C at IP address 192.168.3.3

Are the pings successful? Why or why not?

Task 3: Use the CCP VPN Wizard to Configure the Easy VPN Server

Step 1: Launch the Easy VPN Server wizard and configure AAA services.

a. Click the **Configure** button at the top of the CCP home screen. Choose **Security > VPN > Easy VPN Server**.

b. Click on the **Launch Easy VPN Server Wizard** button.

c. The Easy VPN Server wizard checks the router configuration to see if AAA is enabled. If AAA is not enabled, the Enable AAA window displays. AAA must be enabled on the router before the Easy VPN Server configuration starts. Click **Yes** to continue with the configuration.

d. When prompted to deliver the configuration to the router, click **Deliver**.

e. In the Command Delivery Status window, click **OK**. When the message “AAA has been successfully enabled on the router” displays, click **OK**.

f. When returned to the Easy VPN Server wizard window, click **Next**.

g. Now that AAA is enabled, you can start the Easy VPN Server wizard by clicking the **Launch Easy VPN Server Wizard** button. Read through the descriptions of the tasks that the wizard guides you through.
How does the client receive the IPsec policies?

____________________________________________________________________________________

How does the Easy VPN remote server configuration differ from the site-to-site?

____________________________________________________________________________________

h. Click Next when you are finished answering the above questions.

Step 2: Configure the virtual tunnel interface and authentication.

a. Select the interface on which the client connections terminate. Click the Unnumbered to radio button and select the Serial0/0/1 interface from the pull-down menu.

b. Choose Pre-shared Keys for the authentication type and click Next to continue.
Step 3: Select an IKE proposal.

a. In the IKE Proposals window, the default IKE proposal is used for R3.

![IKE Proposals](image)

What is the encryption method used with the default IKE policy? 

What is the hash algorithm used to ensure that the keys have not been tampered with?

b. Click Next to accept the default IKE policy.

**Note:** Configurations on both sides of the tunnel must match exactly. The Cisco VPN client automatically selects the proper configuration for itself. Therefore, an IKE configuration is not necessary on the client PC.

Step 4: Select the transform set.

a. In the Transform Set window, the default CCP transform set is used. What ESP encryption method is used with the default transform set?
b. Click **Next** to accept the default transform set.

**Step 5: Specify group authorization and group policy lookup.**

a. In the Group Authorization and Group Policy Lookup window, choose the **Local** option.

b. Click **Next** to create a new AAA method list for group policy lookup that uses the local router database.
Step 6: Configure user authentication (XAuth).

a. In the User Authentication (XAuth) window, you can select where user credentials will be configured. You can select an external server, such as a RADIUS server, a local database, or both. Check the Enable User Authentication check box and accept the default of Local Only.

b. Click the Add User Credentials button. In the User Accounts window, you can view currently defined users or add new users.

Where does the router look for valid user accounts and passwords to authenticate remote VPN users when they attempt to log in? ____________________________________________________________

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

How was this user defined? ______________________________________________________________________________________

c. In the User Accounts window, click the Add button to add another user. Enter the username VPNuser1 with a password of VPNuser1pass. Select the check box for encrypting the password using the MD5 hash algorithm. Leave the privilege level at 1.

What is the range of privilege level that can be set for a user? _________________________________________________
c. Click **OK** to accept the VPNuser1 entries, and then click **OK** to close the User Accounts window.

d. In the User Authentication (XAuth) window, click **Next** to continue.
Step 7: Specify group authorization and user group policies.

a. In the Group Authorization and User Group Policies window, you must create at least one group policy for the VPN server.

b. Click Add to create a group policy.

c. In the Add Group Policy window, enter **VPN-Access** as the name of this group. Enter a new pre-shared key of **cisco12345** and then re-enter it.

d. Leave the Pool Information box checked and enter a starting address of 192.168.3.100, an ending address of 192.168.3.150, and a subnet mask of 255.255.255.0.

e. Enter 50 for the Maximum Connections Allowed.

f. Click OK to accept the entries.
g. A CCP warning message displays indicating that the IP addresses in the pool and the IP address of the Fast Ethernet0/1 interface are in the same subnet. Click Yes to continue.

h. When you return to the Group Authorization window, check the **Configure Idle Timer** check box and enter one hour (1). This disconnects idle users if there is no activity for one hour and allows others to connect. Click Next to continue.

i. When the Cisco Tunneling Control Protocol (cTCP) window displays, do not enable cTCP. Click Next to continue.
j. When the Easy VPN Server Passthrough Configuration window displays, make sure that the **Action Modify** check box is checked. This option allows CCP to modify the firewall on S0/0/1 to allow IPsec VPN traffic to reach the internal LAN. Click **OK** to continue.
Step 8: Review the configuration summary and deliver the commands.

a. Scroll through the commands that CCP will send to the router. Do not check the check box to test the VPN. Click Finish.

b. When prompted to deliver the configuration to the router, click Deliver.

c. In the Command Delivery Status window, click OK. How many commands are delivered? ________

Step 9: Test the VPN Server.

a. You are returned to the main VPN window with the Edit Easy VPN Server tab selected. Click the Test VPN Server button in the lower right corner of the screen.

b. In the VPN Troubleshooting window, click the Start button.

Your screen should look similar to the one below. Click OK to close the information window. Click Close to exit the VPN Troubleshooting window.
Note: If you receive a failure after testing the VPN server, close the VPN Troubleshooting window.  
1. Click the Edit button on top right of Edit Easy VPN Server Tab.
2. Click OK in the Edit Easy VPN Server Connection window.
3. Click OK in the Easy VPN Server Passthrough Configuration window.
4. Check the box to the right of the FastEthernet0/1 interface indicating that it is inside (Trusted).
5. Rerun Test VPN Server by clicking on that button on bottom right of Edit Easy VPN Server Tab.
6. Click Start button and test should pass this time.

Task 4: Use the Cisco VPN Client to Test the Remote Access VPN

Step 1: (Optional) Install the Cisco VPN client.

If the Cisco VPN Client software on host PC-A is not installed, install it now. If you do not have the Cisco VPN Client software, contact your instructor.
Step 2: Configure PC-A as a VPN client to access the R1 VPN server.

a. Start the Cisco VPN Client and choose Connection Entries > New, or click the New icon with the red plus sign (+) on it.

b. Enter the following information to define the new connection entry. Click Save when you are finished.

Connection Entry: **VPN-R3**

Description: **Connection to R3 internal network**

Host: **10.2.2.1** (IP address of the R3 S0/0/1 interface)

Group Authentication Name: **VPN-Access** (defines the address pool configured in Task 2)

Password: **cisco12345** (pre-shared key configured in Task 2)

Confirm Password: **cisco12345**

**Note:** The group authentication name and password are case-sensitive and must match the ones created on the VPN Server.
Step 3: Test access from PC-A without a VPN connection.

In the previous step, you created a VPN connection entry on the VPN client computer PC-A but have not activated it, so the VPN tunnel is not yet up.

Open a command prompt on PC-A and ping the PC-C IP address at 192.168.3.3 on the R3 LAN. Are the pings successful? Why or why not?

____________________________________________________________________________________
____________________________________________________________________________________

Step 4: Establish a VPN connection and log in.

a. Select the newly created connection VPN-R3 and click the Connect icon. You can also double-click the connection entry.

b. Enter the previously created username VPNuser1 in the VPN Client User Authentication dialog box and enter the password VPNuser1pass. Click OK to continue. The VPN Client window minimizes to a lock icon in the tools tray of the taskbar. When the lock is closed, the VPN tunnel is up. When it is open, the VPN connection is down.
Task 5: Verify the VPN Tunnel between the Client, Server, and Internal Network

Step 1: Open the VPN Client icon.
   a. Double-click the VPN lock icon to expand the VPN Client window.
      What does it say about the connection status at the top of the window? ___________________________
   b. From the PC-A command line, issue the `ipconfig` command.
      What is the IP address of the first Local Area Connection? ___________________________
      What is the IP address of Local Area Connection 2? ___________________________

Step 2: Close the VPN connection and reopen it.
   a. Click the Disconnect icon in the VPN Client window to close the VPN-R3 connection.
   b. Click the Connect icon and log in again as VPNuser1.
      What is the IP address of Local Area Connection 2 now? ___________________________
      Note: Each time you disconnect and reconnect to the VPN server, you receive a new IP address until the limit is reached.

Step 3: Check the tunnel statistics.
   a. Choose Status > Statistics. Click the Tunnel Details tab.
b. What is the current address obtained from the R3 VPN server and what is the range of addresses that can be assigned?

What is the VPN server address? ____________________________
How many packets have been encrypted? ________________
What is the encryption method? ____________________________
What is the authentication method? ________________________

c. Leave the VPN Client Statistics window open.

Step 4: Test access from the client PC-A using the VPN connection.

a. With the VPN connection from computer PC-A to router R3 activated, open a command prompt on PC-A and ping the PC-C IP address at 192.168.3.3 on the R3 LAN. Are the pings successful?

________________________________________________________________________

b. How many packets have now been encrypted? _______________________________________

Step 5: Check the Cisco IOS message on R3 when the tunnel is created.

Open the console connection for R3 and locate the message displayed indicating that the virtual interface came up when the VPN Client connection was made.

What is the name of the interface on R3 that is activated for the VPN? ____________________________

Step 6: Verify the VPN connection information for PC-A.

a. From the PC-A command prompt, issue the ipconfig /all command to see the network connections.

b. What is the configuration for the first Local Area Connection?

IP Address: ____________________________________________________________
Subnet Mask: __________________________________________________________
Default Gateway: ________________________________________________________________
Description: ___________________________________________________________________

c. What is the configuration for Local Area Connection 2?
   IP Address: ________________________________________________________________
   Subnet Mask: _____________________________________________________________
   Default Gateway: __________________________________________________________
   Description: __________________________________________________________________

Step 7: Telnet from PC-A to R3.
   a. From the PC-A command prompt, telnet to R3 at the Fa0/1 IP address 192.168.3.1. Log in as
      admin01 with a password of admin01pass. What is the router command prompt and why is this?
      __________________________________________________________________________
   
   b. Issue the show run command to view the various commands generated by CCP to configure
      the VPN server.
   
   c. Issue the show users command to see connections to router R3. What connections are present?
      __________________________________________________________________________
   
   d. Close the Telnet connection using the quit or exit command.

Reflection
Why is VPN a good option for remote users?
______________________________________________________________________________
______________________________________________________________________________
______________________________________________________________________________

Router Interface Summary Table

<table>
<thead>
<tr>
<th>Router Model</th>
<th>Ethernet Interface #1</th>
<th>Ethernet Interface #2</th>
<th>Serial Interface #1</th>
<th>Serial Interface #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1800</td>
<td>Fast Ethernet 0/0 (Fa0/0)</td>
<td>Fast Ethernet 0/1 (Fa0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>1900</td>
<td>Gigabit Ethernet 0/0 (G0/0)</td>
<td>Gigabit Ethernet 0/1 (G0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>2800</td>
<td>Fast Ethernet 0/0 (Fa0/0)</td>
<td>Fast Ethernet 0/1 (Fa0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
<tr>
<td>2900</td>
<td>Gigabit Ethernet 0/0 (G0/0)</td>
<td>Gigabit Ethernet 0/1 (G0/1)</td>
<td>Serial 0/0/0 (S0/0/0)</td>
<td>Serial 0/0/1 (S0/0/1)</td>
</tr>
</tbody>
</table>

Note: 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.