Packet Tracer - Skills Integration Challenge

Objectives

Part 1: Set Up a Home Wireless Network

Part 2: Configure and Use a Remote-Access VPN

Part 3: Configure and Use a Site-to-Site VPN

Background/Scenario

In this Packet Tracer Skills Integration Challenge activity, you will play the role of four different network users in Greenville. Acting as these users, you will demonstrate many of the cybersecurity skills you learned during this course. You will configure a wireless network within the home site, establish a remote-access VPN connection between the Cafe and Data Center sites, and restore a site-to-site VPN connection between the HQ and Branch Office sites. In addition, you will perform a variety of additional tasks including registering devices with an IoT server, remotely verifying IoT devices are sending data, configure email settings, validate file integrity, configure user wireless access in HQ, add an FTP account, decrypt user credentials, restore a router configuration and back up a router configuration.

Note: This activity starts in **Greenville**. You have access to all of the locations. Some device names have changed to match the scenario. Some features on some devices may be locked. Switching to **Logical** mode is disabled.

Note: You may find it help to **Fast Forward Time** (Alt+D) to speed up convergence in Packet Tracer.

Required Resources

The **CSE-LABVM** installed in VirtualBox

Instructions

Part 1: Set Up a Home Wireless Network

Jose just bought a new wireless router for his home and needs to configure it to support wireless, including wireless connections for IoT devices. He plans to check the status of his IoT devices while he is away from home. Therefore, we will create a new user account and register his devices with the **IoT Registration Server**.

Step 1: Configure the Home wireless network.

a. The **Home Wireless Router** is currently set to the default factory settings. Jose first determines its IP address, and then from **Home Office PC**, uses **admin** as the username and password to log into the **Home Wireless Router**.

b. Jose then configures the **Home Wireless Router** with the following settings:

Router IP address:

- IP address: **172.16.10.1**
- Subnet mask: **255.255.255.0**

DHCP

- Starting IP address: **225**
- Maximum number of Users: **25**

- DNS Server: **10.2.0.125**

Wireless Networks

- **HomeGW** network on **2.4 GHz** and **5 GHz - 2** radios
  - Network mode is **Auto**
  - SSID: **HomeGW**
  - WPA2 Personal password: **cisco12345!**
  - Enable SSID broadcast
- Enable the **Guest** network on **5 GHz - 1** radio
  - SSID: **Guest**
  - WPA2 Personal password: **homeguestpass**
  - Prevent guests to see each other and access the local network

Administrative Tasks

- Set the router password to **cisconetacadrocks**
- Disable **Remote Management**

Step 2: Configure laptops to access the wireless networks.

a. **Jose Laptop** needs access to the **HomeGW** network.

b. **Guest Laptop** needs access to the **Guest** network.

Step 3: Verify all wired and wireless devices have IP addressing.

If necessary, use **ipconfig** command options to force DHCP requests. On IoT devices, you may need to toggle **DHCP** and **Static**.

Step 4: Register the Home IoT devices to the IoT Registration server.

a. Jose signs up for a new user on the **IoT Registration Server** (10.3.0.125) with a username and password of his choice.

b. Jose then verifies that the IoT devices, **Home Doors**, **Home_Siren**, and **Home_Webcam**, are connected to the **HomeGW** network and registers each with the **IoT Registration Server**.

Step 5: Verify remote access to the Home IoT devices.

From the **Cafe**, Jose uses the **Jose VPN Laptop** to access the **IoT Registration Server** and verifies that the IoT devices are sending data.

Part 2: Configure and Use a Remote-Access VPN

One of Jose's responsibilities for work is to monitor the status of the IoT devices at the **Data Center**. He just bought a new laptop and goes to the **Cafe** to set it up. The laptop needs email configured and VPN access to the **Data Center** so he can send emails and upload files securely while he is away from the Data Center. Mariel, at the **Data Center**, will verify the integrity of Jose's file upload.

Step 1: Use the following settings to configure an email account on Jose VPN Laptop.

- Name: **Jose**
- Email address: **jose@mail.cybercloud.com**
- Incoming / Outgoing mail server: **172.19.0.4**

- User Name: **jose**
- Password: **josepass**

Step 2: Configure a remote-access VPN.

Jose configures the remote-access VPN on **Jose VPN Laptop** so he can access the **DC IoT Server**.

- GroupName: **REMOTE**
- Group Key: **CISCO**
- Host IP (Server IP): **10.0.0.2**
- Username: **VPN**
- Password: **ciscorocks**

Step 3: Verify VPN access.

Jose then verifies the status of the **Data Center** IoT devices by logging in at **172.31.0.2** with username **admin** and password **ciscorocks**.

Step 4: Upload a file to the DC FTP site.

a. While connected over VPN, Jose connects to the FTP server at **172.19.0.3** with username **jose** and password **josepass**.

b. He then uploads the **Instructions.txt** file.

Step 5: Send an email to Mariel about the file upload.

a. Jose opens **draft_email.txt** file in the **Text Editor** and then copies all of the content.

b. He then pastes the contents into a new email to **mariel@mail.cybercloud.com** and sends it.

Step 6: Verify the integrity of the file uploaded to the FTP server.

a. In the **Data Center**, Mariel accesses her laptop and opens the email from Jose.

b. She then uses her credentials (**mariel** / **marielpass)** to download **Instructions.txt** from the FTP server at **172.19.0.3**.

c. To verify the integrity of the file, Mariel copies its content, opens the **CSE-LABVM**, pastes the content into the **echo -n** 'file-contents' **| md5sum** command, and compares the hash sent in Jose's email.

Part 3: Configure and Use a Site-to-Site VPN

Divya in **HQ** needs to configure her laptop for wireless access. She then needs to add an FTP account to the FTP server. Meanwhile, Rick in the **Branch Office** is responsible for restoring site-to-site VPN access between **Branch Office** and **HQ**. To do so, he will download the backup router configuration stored locally. He will then back up the configuration offsite at **HQ**, but must first get FTP credentials from Divya.

Step 1: Configure wireless access for laptop at HQ.

Divya in **HQ** configures her laptop to connect to the wireless network.

- SSID: **HQ-INT**
- WPA2 User ID: **divya**
- WPA2 Password: **DivyaPass!**

Step 2: Configure new credentials on the FTP server.

Divya adds a new user to the **FTP** server in the **Wiring Closet**.

- Username: **mary**
- Password: **cisco321**
- Permission: **RWDNL**

Step 3: Restore and verify site-to-site VPN.

a. In the **Branch Office**, Rick logs into the console on **BRouter1** with password **BRsecurity** and then enters **BRc1sc0@!** as the enable password.

b. From the **Branch#** prompt, he copies the **Branch-config** file from the **BR Server** at **10.0.3.30** and applies it to the configuration in RAM.

Record the command:

c. Rick needs to modify the ACL. He removes ACL 102, and then adds the following ACL.

```
config t
no access-list 102
access-list 102 permit ip 10.0.3.0 0.0.0.255 10.1.0.0 0.0.255.255
access-list 102 permit ip 10.0.3.0 0.0.0.255 10.2.0.0 0.0.255.255
access-list 102 permit ip 10.0.3.0 0.0.0.255 10.3.0.0 0.0.255.255
```

d. Finally, Rick tests the VPN connection by pinging the **HQ Mail** server at **192.168.75.3**.

Step 4: Back up the BRouter1 configuration offsite.

a. Rick sends an email **divya@mail.cyberhq.com** informing her that the VPN connection has been re-established and that he would like to back up the VPN configuration offsite.

b. At **HQ**, Divya opens the email from Rick. She then opens the **draft-email.txt** in her **Text Editor**, copies the content, paste it into a reply to Rick, and sends it.

c. Rick reads the email from Divya and then uses the **CSE-LABVM** to decrypt his FTP credentials. His decryption password is **rick**.

d. Rick then configures **BRouter1** with the FTP username and password so that he can establish an FTP session directly from the router.

```
Branch# config t
Branch(config)# ip ftp username username
Branch(config)# ip ftp password password
Branch(config)# end
```

e. Rick verifies connectivity to the **FTP** server by pinging it at **192.168.75.2**.

f. Rick uses the **copy running-config ftp** command to upload the **BRrouter1** running-config file to the HQ **FTP** server. He uses **Branch-config-VPN** and the destination file name.

Record the command:

Answer Key

Part 1: Set Up a Home Wireless Network

Step 1: Configure the Home wireless network.

Step 2: Configure laptops to access the wireless networks.

Step 3: Verify all wired and wireless devices have IP addressing.

Step 4: Register the Home IoT devices to the IoT Registration server.

Step 5: Verify remote access to the Home IoT devices.

Part 2: Configure and Use a Remote-Access VPN

Step 1: Use the following settings to configure an email account on Jose VPN Laptop.

Step 2: Configure a remote-access VPN.

Step 3: Verify VPN access.

Step 4: Upload a file to the DC FTP site.

Step 5: Send an email to Mariel about the file upload.

Step 6: Verify the integrity of the file uploaded to the FTP server.

Part 3: Configure and Use a Site-to-Site VPN

Step 1: Configure wireless access for laptop at HQ.

Step 2: Configure new credentials on the FTP server.

Step 3: Restore and verify site-to-site VPN.

From the **Branch#** prompt, he copies the **Branch-config** file from the **BR Server** at **10.0.3.30** and applies it to the configuration in RAM.

Record the command below:

```
Branch# copy tftp running-config
Address or name of remote host []? 10.0.3.30
Source filename []? Branch-config
Destination filename [running-config]?

Accessing tftp://10.0.3.30/Branch-config...
Loading Branch-config from 10.0.3.30: !
[OK - 2546 bytes]

2546 bytes copied in 0 secs
Branch#
```

Step 4: Back up the BRouter1 configuration offsite.

Rick uses the **copy running-config ftp** command to upload the **BRrouter1** running-config file to the HQ **FTP** server. He uses **Branch-config-VPN** and the destination file name.

Record the command below:

```
Branch# copy running-config ftp
Address or name of remote host []? 192.168.75.2
Destination filename []? Branch-config-VPN

Writing running-config...
[OK - 2524 bytes]

2524 bytes copied in 0.042 secs (60000 bytes/sec)
Branch#
```