Packet Tracer – Configuring VPN Transport Mode (Instructor Version)

**Instructor Note**: Red font color or gray highlights indicate text that appears in the instructor copy only.

1. Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Private IP Address | Public IP Address | Subnet Mask | Site |
| **Private\_FTP server** | 10.44.2.254 | N/A | 255.255.255.0 | Gotham Healthcare Branch |
| **Public\_FTP server** | 10.44.2.253 | 209.165.201.20 | 255.255.255.0 | Gotham Healthcare Branch |
| **Branch\_Router** | N/A | 209.165.201.19 | 255.255.255.248 | Gotham Healthcare Branch |
| **Phil’s computer** | 10.44.0.2 | N/A | 255.255.255.0 | Metropolis Bank HQ |

1. Objectives

**Part 1: Sending Unencrypted FTP Traffic**

**Part 2: Configuring the VPN Client within Metropolis**

**Part 3: Sending Encrypted FTP Traffic**

1. Background

In this activity, you will observe the transfer of unencrypted FTP traffic between a client and a remote site. You will then configure a VPN client to connect to the Gotham Healthcare Branch site and send encrypted FTP traffic. The IP addressing, network configuration, and service configurations are already complete. You will use a client device within Metropolis Bank HQ to transfer unencrypted and encrypted FTP data.

1. Sending Unencrypted FTP Traffic
   * 1. Access the Cyber Criminals Sniffer.
        1. Click the **Cyber Criminals Sniffer** and click the **GUI** tab.
        2. Click the **Clear** button to remove any possible traffic entries viewed by the sniffer.
        3. Minimize the **Cyber Criminals Sniffer**.
     2. Connect to the Public\_FTP server using an insecure FTP connection.
        1. Click the **Metropolis Bank HQ** site and click **Phil’s** laptop.
        2. Click the **Desktop** tab and click on **Command Prompt**.
        3. Use the **ipconfig** command to view the current IP address of **Phil’s** computer.
        4. Connect to the **Public\_FTP** server at **Gotham Healthcare Branch** by entering **ftp 209.165.201.20** in the command prompt.
        5. Enter the username of **cisco** and password of **publickey** to login to the **Public\_FTP** server.
        6. Use the **put** command to upload the file **PublicInfo.txt** file to the **Public\_FTP** server.
     3. View the traffic on the Cyber Criminals Sniffer.
        1. Maximize the **Cyber Criminals Sniffer** that was previously minimized.
        2. Click the **FTP** messages displayed on the sniffer and scroll to the bottom of each one.

What information is displayed in clear text?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

USER **cisco** PASS **publickey** and the filename of **PublicInfo.txt**

* + - 1. Type **quit** to exit **Public\_FTP** server.

1. Configuring the VPN Client on Phil’s Computer
   * + 1. From **Phil’s** computer, use the **ping** command and target the IP address of the **Branch\_Router**. The first few pings may timeout. Enter the **ping** to get four successful pings.
       2. On the **Desktop** tab, click on **VPN**
       3. Within the **VPN Configuration** window, enter the following settings:

GroupName: **VPNGROUP**

Group Key: **123**

Host IP (Server IP): **209.165.201.19**

Username: **phil**

Password: **cisco123**

* + - 1. Click **Connect** and Click **OK** on the next window.

What is the Client IP for the client-to-site VPN connection?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

10.44.2.200 (this may vary between 10.44.2.200 to 10.44.2.230)

1. Sending Encrypted FTP Traffic
   * 1. View the current IP addressing on Phil’s computer.
        1. Within the **Metropolis Bank HQ** site, click **Phil’s** computer.
        2. Click the **Desktop** tab and click on **Command Prompt**.
        3. Use the **ipconfig** command to view the current IP address of **Phil’s** PC.

What extra IP address is now shown that was not shown before in Part 1 Step 2c?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tunnel Interface IP Address: 10.44.2.200 (this may vary between 10.44.2.200 to 10.44.2.230)

* + 1. Send encrypted FTP traffic from Phil’s computer to the Private\_FTP server.
       1. Connect to the **Private\_FTP** server at **Gotham Healthcare Branch** by entering **ftp 10.44.2.254** in the command prompt.
       2. Enter the username of **cisco** and password of **secretkey** to login to the **Private\_FTP** server.
       3. Upload the file **PrivateInfo.txt** file to the **Private\_FTP** server.
    2. View the traffic on the Cyber Criminals Sniffer
       1. Maximize the **Cyber Criminals Sniffer** that was previously minimized.
       2. Click the **FTP** messages displayed on the sniffer.

Are there any FTP messages displaying the password of internal or the file upload of PrivateInfo.txt? Explain.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

No, the client-to-site VPN is using encryption and the Cyber Criminals Sniffer cannot decrypt the traffic to view it.

1. Suggested Scoring Rubric

|  |  |  |  |
| --- | --- | --- | --- |
| Activity Section | Question Location | Possible Points | Earned Points |
| Part 1: Sending Unencrypted FTP Traffic | Step 3 | 20 |  |
| Part 2: Configure the VPN Client on Phil’s Computer | Step 1 | 10 |  |
| Part 3: Send Encrypted FTP Traffic | Step 1 | 10 |  |
| Step 3 | 20 |  |
| **Questions** | | **60** |  |
| **Packet Tracer Score** | | **40** |  |
| **Total Score** | | **100** |  |