Packet Tracer – Configuring VPN Tunnel Mode

Addressing Table

Device	Private IP Address	Subnet Mask	Site
File Backup Server	10.44.2.254	255.255.255.0	Gotham Healthcare Branch

Objectives

Part 1: Sending Unencrypted FTP Traffic

Part 2: Configuring the VPN Tunnel between Metropolis and Gotham

Part 3: Sending Encrypted FTP Traffic

Background

In this activity, you will observe the transfer of unencrypted FTP traffic between two geographic sites. You will then configure a VPN tunnel between two geographic sites and send encrypted FTP traffic. The IP addressing, network configuration, and service configurations are already complete. You will use the client devices in the differing geographic regions to transfer FTP data securely and insecurely.

Part 1: Sending Unencrypted FTP Traffic

Step 1: Access the Cyber Criminals Sniffer.

a. Click the **Cyber Criminals Sniffer** and click the **GUI** tab.

b. Click the **Clear** button to remove any possible traffic entries viewed by the sniffer.

c. Minimize the **Cyber Criminals Sniffer**.

Step 2: Connect to the FTP Backup server using an insecure FTP connection.

a. Click the **Metropolis Bank HQ** site and click **Phil's** laptop.

b. Click the **Desktop** tab and click on **Command Prompt**.

c. Use the **ipconfig** command to view the current IP address of **Phil's** PC.

d. Connect to the **File Backup** server at **Gotham Healthcare Branch** by entering **ftp 10.44.2.254** in the command prompt.

a. Enter the username of **cisco** and password of **cisco** to login to the **File Backup** server.

Step 3: View the traffic on the Cyber Criminals Sniffer.

a. Maximize the **Cyber Criminals Sniffer** that was previously minimized.

b. Click the **FTP** messages displayed on the sniffer and scroll to the bottom of each one.

What information is displayed in clear text?

Part 2: Configuring the VPN Tunnel between Metropolis and Gotham

a. Within the **Metropolis Bank HQ** site, click the **HQ_Router**.

b. Copy the IPSec VPN site-to site configuration below and paste it into **HQ_Router**.

```
enable
configure terminal
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp key vpnpass address 209.165.201.19
!
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
 description VPN connection to Branch_Router
 set peer 209.165.201.19
 set transform-set VPN-SET
 match address 110
!
interface GigabitEthernet0/1
crypto map VPN-MAP
!
access-list 110 permit ip 10.44.1.0 0.0.0.255 10.44.2.0 0.0.0.255
!
end
copy run start
```

c. The required mirror configuration of the IPSec VPN has already been implemented on the **Branch_Router** of the **Gotham Healthcare Branch** site.

Part 3: Sending Encrypted FTP Traffic

Step 1: Send FTP traffic from Sally’s PC to the File Backup server.

a. Within the **Metropolis Bank HQ** site, click **Sally’s** computer.

b. Click the **Desktop** tab and then click **Command Prompt**.

c. Use the **ipconfig** command to view the current IP address of **Sally’s** PC.

d. Connect to the **File Backup** server at **Gotham Healthcare Branch** by entering **ftp 10.44.2.254** in the command prompt. (It may take 2-5 attempts)

e. Enter the username of **cisco** and password of **cisco** to login to the **File Backup** server

f. Use the **put** command to upload the file **FTPupload.txt** to the **File Backup** server.

Step 2: View the traffic on the Cyber Criminals Sniffer

a. Maximize the **Cyber Criminals Sniffer** that was previously minimized.

b. Click the **FTP** messages displayed on the sniffer.

Are there any FTP messages sourced from the IP of **Sally’s** computer? Explain.

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Send unencrypted FTP traffic	Step 3	20	
Part 3: Send encrypted FTP traffic	Step 2	30	
	Questions	**50**	
	Packet Tracer Score	**50**	
	Total Score	**100**	