Packet Tracer – Configuring VPN Tunnel Mode

1. Addressing Table

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

1. Objectives

**Part 1: Sending Unencrypted FTP Traffic**

**Part 2: Configuring the VPN Tunnel between Metropolis and Gotham**

**Part 3: Sending Encrypted FTP Traffic**

1. 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.

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 FTP Backup 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** PC.
        4. A picture containing calendar

           Description automatically generated
        5. Connect to the **File Backup** 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 **cisco** to login to the **File Backup** server.
   * 1. 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?

Table

Description automatically generated

Table

Description automatically generated

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

1. Configuring the VPN Tunnel between Metropolis and Gotham
   * + 1. Within the **Metropolis Bank HQ** site, click the **HQ\_Router**.
       2. 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

* + - 1. The required mirror configuration of the IPSec VPN has already been implemented on the **Branch\_Router** of the **Gotham Healthcare Branch** site.

1. Sending Encrypted FTP Traffic
   * 1. Send FTP traffic from Sally’s PC to the File Backup server.
        1. Within the **Metropolis Bank HQ** site, click **Sally’s** computer.
        2. Click the **Desktop** tab and then click **Command Prompt**.
        3. Use the **ipconfig** command to view the current IP address of **Sally’s** PC.
        4. Calendar

           Description automatically generated with low confidence
        5. 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)
        6. Enter the username of **cisco** and password of **cisco** to login to the **File Backup** server
        7. Use the **put** command to upload the file **FTPupload.txt** to the **File Backup** 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 sourced from the IP of **Sally’s** computer? Explain.

\_\_\_\_\_No Because they were sent in a tunnel secretly. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. 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** |  |