Packet Tracer - Configure a Remote Access VPN Client

Objectives

Part 1: Establish a Remote Access VPN

Part 2: Capture and Examine Network Traffic

Background / Scenario

Secure communications is often required between different offices in an organization or between remote workers and the main corporate network. A Virtual Private Network (VPN) can be used to create such a secure communication channel through a public network such as the internet. Site-to-site VPNs allow different corporate offices to securely communicate across a public WAN while remote-access VPNs allow mobile workers to securely communicate with a home corporate LAN.

All VPN traffic must be authenticated and then encrypted to provide private, secure communications. Internet Security Association and Key Management Protocol (ISAKMP) is part of the IPsec protocol suite and is used for negotiating, establishing, modifying, and deleting security associations (SA) and related parameters. It defines the procedures and packet formats used for peer authentication, the creation and management of SAs, and techniques for key generation. In ISAKMP, SA and key management are separate from any key exchange protocols. ISAKMP supports many actual key exchange protocols such as Internet Key Exchange (IKE).

In ISAKMP phase 1, peers authenticate, establish an ISAKMP SA, and agree on the mechanisms for further communication. In phase 2 this ISAKMP SA is used to negotiate further protocol SAs such as IPsec/ESP. After the initial establishment of an ISAKMP SA, multiple protocol SAs can be established.

For a secure tunnel to be created, VPN endpoints must be configured with the same security parameters. Remote-access VPNs require the installation of a VPN client on the remote worker's computer that is configured to match the security policies configured on corporate network's VPN gateway.

In this Packet Tracer (PT) activity, you will configure a remote-access VPN client to connect a laptop in the Cafe to a network in the Data Center. You will then use a “sniffer” to observe unencrypted and encrypted traffic.

Instructions

Part 1: Establish a Remote Access VPN

The **Cafe** is a popular place for remote workers. They come to have coffee, for conversation, and to work in a more relaxed environment. Free Wi-Fi offered in coffee shops and cafes are usually open, meaning that there is no privacy and traffic can be easily captured. To avoid that issue, remote access VPNs are commonly used.

In this Part, you will use a VPN client on a laptop in the **Cafe** to securely connect to an FTP server in the **Data Center**. The tunnel created by the VPN will encrypt any data transferred between the laptop and the server. The edge router in the **Data Center** is already configured for VPN traffic. Your task is to configure the VPN client to match this configuration.

Step 1: Create a VPN using Packet Tracer's VPN client.

a. Click the **Cafe** location, and then **VPN Laptop**.

b. Click **Desktop** > **Command Prompt**, and then enter the **ipconfig** command.

© 2021 - 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is the IP address assigned to this laptop?

c. Close the **Command Prompt**, and click **VPN**.

d. For **VPN Configuration**, enter the following:

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

e. Click **Connect** to continue.

Note: You may need to click **Connect** several times before you are connected as it may take some time for the protocols in Packet Tracer converge.

f. When connected, the client will receive an IP address from the VPN server in the Data Center. The IP address will be in the 172.18.1.150 - 200 range. Close the **VPN Configuration** window, and click **Command Prompt**. Enter the **ipconfig /all** command. The last line should show a **Tunnel Interface IP Address**.

Note: Although the **Tunnel Interface IP Address** is listed under the **Bluetooth Connection**, it not part of the Bluetooth configuration. The computer creates a new tunnel interface for the VPN connection.

What is the IP address?

Step 2: Verify the VPN connection on the VPN gateway in the Data Center.

a. Navigate to the **Data Center**.

b. Click **Data Center POP** > **DC_Edge-Rtr1**.

c. Click the **Config** tab, and then enter the **enable** command followed by the **show crypto isakmp sa** command. This command will display active IPsec security associations.

```
DC_Edge-Rtr1> enable
DC_Edge-Rtr1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id slot status
10.1.0.11 10.0.0.2 QM_IDLE 1070 0 ACTIVE


IPv6 Crypto ISAKMP SA
```

What status is listed in the output of the command?

What destination IP address is listed in the output and to what device is this address assigned?

© 2021 - 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 3: Test the VPN Connection.

To test the VPN, attempt to access the FTP server in the **Data Center** from the **VPN Laptop** and download a file.

a. Navigate back to the **VPN Laptop**. If necessary, click **Desktop** > **Command Prompt**.

b. Connect the FTP server at **172.19.0.3** and authenticate with username **remote** and password **ciscorocks**. If the connection fails, verify that the VPN is still connected and reconnect, if necessary.

   Record the command below:

c. Enter the **dir** command.

   What file is present in the directory?

d. Use the **get** command to download the file, and then **quit** the FTP session.

   Record the command below:

e. Close the **Command Prompt**, and the click **Text Editor**.

f. Click **File** > **Open** and open the downloaded file.

   What message is written in the txt file?

g. Close the **Text Editor**, and then click **Command Prompt**. Enter the command **ping 172.19.0.3**.

   Is it successful?

h. In the **Cafe**, click the **Cafe Customer** laptop > **Desktop** tab > **Command Prompt**, and then enter the command **ping 172.19.0.3**.

   Will it be successful? Explain.

Part 2: Capture and Examine Network Traffic

In the **Cafe**, there is a threat actor with a network sniffer connected to network. The threat actor plans to capture traffic, and then use it for malicious purposes. In this Part, you will play the role of the threat actor, sniffing unencrypted, and then encrypted traffic.

Step 1: Configure a network sniffer to capture packets.

a. In **Cafe**, and click **Cafe Sniffer** > **GUI**.

b. Click **Show All/None** to clear all filters.

c. Click **Edit Filters**. Under **IPv4**, select **ICMP**. Under **Misc**, select **FTP**, **IPsec**, **ISAKMP**, **Telnet**, and **UDP**.

d. If the VPN is still established, disconnect it (**VPN Laptop** > **Desktop** > **VPN** > **Disconnect**).

e. Arrange your **VPN Laptop** and **Cafe Sniffer** windows side by side for the remaining tasks in this activity.

© 2021 - 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Step 2: Capture and examine unencrypted traffic.

a. On the **Cafe Sniffer**, click **Clear** to remove the previously captured packets from the buffer.

b. On the **VPN Laptop**, open the **Command Prompt** and telnet to the **DC_Edge_Rtr1** at **10.0.0.2**.

Record the command below:

Note: **DC_Edte_Rtr1** is not configured for Telnet access.

c. On the **Cafe Sniffer**, notice a Telnet packet was captured. Click it to examine its contents. Scroll to the bottom. Under the **TELNET** section, notice that the **TELNET DATA** is in clear text.

d. Click **Clear** to clear the filter screen.

e. On the **VPN Laptop,** attempt to connect to the FTP server at **172.19.0.3**.

What type(s) of traffic are captured?

Step 3: Capture and examine encrypted traffic.

a. Click **Clear**. On the **VPN Laptop**, re-establish the VPN session with the credentials you used in Part 1, Step 1.

On the **Cafe Sniffer**, what type of traffic is captured?

b. Click **Clear**. ISAKMP packets will continue to populate the buffer as the VPN connection sends keepalive messages.

c. On the **VPN Laptop**, ping the FTP server at **172.19.0.3**.

What type of traffic are captured?

d. Click **Clear**. On the **VPN Laptop**, re-establish an FTP session with the server at 172.19.0.3. The username is **remote** and the password is **ciscorocks**.

What type of traffic are captured?

e. Examine an ISAKMP packet.

In the UDP header, what port is being used by ISAKMP.

Reflection Question

Investigate available VPN applications.

On **physical** equipment, you would require a VPN service and their VPN client software loaded on the laptop.

Use the internet to research different VPN services/applications available for laptops, tablets and smartphones.

What are three examples of VPN services/applications that you could use on an open wireless network to protect your data?

© 2021 - 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

Answer Key

Part 1: Establish a Remote Access VPN

Step 1: Create a VPN using Packet Tracer's VPN client.

What is the IP address assigned to this laptop?

Answers may vary. The assigned IP address should be in the range of 192.168.0.11 to 192.168.0.254.

What is the IP address?

Answers may vary. It will be in the 172.18.1.150 - 200 range, but it will probably be 172.18.1.150.

Step 2: Verify the VPN connection on the VPN gateway in the Data Center.

What status is listed in the output of the command?

ACTIVE

What destination IP address is listed in the output and to what device is this address assigned?

10.1.0.11, which is the IP address of the Cafe router Internet facing interface G0/0.

Step 3: Test the VPN Connection.

Connect the FTP server at **172.19.0.3** and authenticate with username **remote** and password **ciscorocks**. If the connection fails, verify that the VPN is still connected and reconnect, if necessary.

Record the command below:

```
C:\> ftp 172.19.0.3
```

What file is present in the directory?

PTsecurity.txt

Use the **get** command to download the file, and then **quit** the FTP session

Record the command below:

```
ftp> get PTsecurity.txt
```

What message is written in the txt file?

Congratulations! You have successfully downloaded this file from the Data Center FTP server.

Is it successful?

Yes

Will it be successful? Explain.

The ping should not be successful because this laptop does not have VPN configured, and the edge router in the DC is configured with an ACL that denies pings.

Part 2: Capture and Examine Network Traffic

Step 1: Configure a network sniffer to capture packets.

Step 2: Capture and examine unencrypted traffic.

On the VPN Laptop, open the Command Prompt and telnet to the DC_Edge_Rtr1 at 10.0.0.2.

Record the command below:

```
C:\> telnet 10.0.0.2
```

© 2021 - 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

What type(s) of traffic are captured?

ICMP is generated because the FTP server cannot be reached. If you click one of the packets and view its details under the ICMP header, you will see that the ICMP type is 3 for Destination Unreachable and the Code is 1 for Host Unreachable.

Step 3: Capture and examine encrypted traffic.

On the **Cafe Sniffer**, what type of traffic is captured?

ISAKMP is used to establish the VPN tunnel.

What type of traffic are captured?

ISAKMP and IPsec. The ICMP traffic is hidden inside the secure IPsec tunnel.

What type of traffic are captured?

ISAKMP and IPsec. The FTP traffic is hidden inside the secure IPsec tunnel.

In the UDP header, what port is being used by ISAKMP.

ISAKMP uses UDP port 500.

Reflection Question

What are three examples of VPN services/applications that you could use on an open wireless network to protect your data?

Answers will vary. Examples of VPN applications are CyberGhost, IPVanish, and NordVPN.

© 2021 - 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public