Packet Tracer - Configure Firewall Settings

Objectives

- Configure MAC Filtering on a wireless router.
- Configure DMZ on a wireless router.
- Configure Single Port Forwarding on a wireless router.

Introduction

In this activity, you will configure a wireless router to:

- Rely on MAC filtering to increase security
- Allow access to a server in the DMZ
- Disable the DMZ and configure support for Single Port Forwarding

Instructions

Step 1: Connect to the wireless router.

a. Connect to the wireless router configuration web page at **192.168.0.1** from **PC0**.

b. Use **admin** for both the user name and password.

c. Navigate to wireless settings to determine the SSID and passphrase for connection to WRS1. Record the SSID and passphrase below.

Questions:

SSID:

Type your answers here.

Passphrase:

Type your answers here.

Step 2: Configure laptop as wireless client.

a. Connect **Laptop0** to the **WRS1** wireless network using the security settings configured on the wireless router. Click **Desktop** > **PC Wireless**. Select **Connect** tab. Press **Refresh**. Select the desired SSID and click **Connect**. Provide the passphrase and select **Connect**.

b. Close the **PC Wireless** window and click **Command Prompt**.

c. At the prompt, enter **ipconfig /all** and record the IP and MAC addresses of **Laptop0** below.

Questions:

Laptop0 IP Address:

Type your answers here.

MAC address:

Type your answers here.

d. Repeat the above steps to connect **Laptop1** to **WRS1**.

Step 3: Configure WRS1 to support MAC filtering.

a. On **PC0**, go to the wireless router's configuration page at 192.168.0.1.

b. Navigate to **Wireless > Wireless MAC Filter**.

c. Select **Enabled** and **Permit PCs listed below to access wireless network**.

d. Type in the MAC address **for Laptop0** in the **MAC 01:** field. Notice the MAC address must be in the **XX:XX:XX:XX:XX:XX** format. Click **Save Settings**.

e. To verify connectivity, open a command prompt. Issue the ping command to the default gateway to 192.168.0.1 from **Laptop0** and **Laptop1**.

```
C:\> ping 192.168.0.1
```

Question:

Were both laptop able to connect to the WRS1 network? Why are you unable to associate with the access point?

Type your answers here.

Step 4: Test connectivity through the Telco Cloud.

a. Open a **Command Prompt** on **Laptop0**.

b. In **Laptop0**, test connectivity to **Remote PC** by issuing the **ping 209.165.201.29** command. The first few pings may fail while the network converges. Issue the command again if you did not get successful replies.

c. Open **Remote PC** and then browse to the address of the internal web page hosted at **Server0**, which is **www.acompany.com**. A **Request Timeout** message should display. A webpage requests from **Remote PC** to **Server0** is not successful because **WRS1** does not know which internal device should receive it. Port forwarding must be configured on **WRS1**.

Step 5: Configure DMZ.

A demilitarized zone (DMZ) is where a portion of the company network is exposed to an untrusted external network, such as the internet.

a. On **PC0**, reconnect to the wireless router's configuration page.

b. Navigate to **Application & Gaming** > **DMZ**.

c. Click **Enabled**.

d. In the Destination: field, enter **20** for the IP address **192.168.0.20**.

e. Scroll to the bottom and save the settings.

f. Browse to **www.acompany.com** from **Remote PC**. You should now see the web page hosted by **Server0**.

g. After you have verified that you were able to reach the webpage, disable **DMZ** and save the settings.

Step 6: Configure WRS1 to forward a single port to Server0.

Depending on the router model, the open ports of a server in the DMZ can be exposed to an untrusted external network. To limit the number of exposed ports, single port forwarding can be configured on the router.

a. On **PC0**, reconnect to the wireless router's configuration page. Navigate to **Application & Gaming** > **Single Port Forwarding**.

b. On the left-hand menu, choose **HTTP** from the first drop-down box. Change the **To IP Address** to match **Server0**’s IP address, **192.168.0.20**. Also, check the **Enabled** checkbox at the end of the row.

c. Scroll to the bottom of the window and click **Save Settings**.

d. You should now be able to reach the webpage hosted on **Server0**. Browse to **www.acompany.com** on **Remote PC**. You should now see the web page hosted by **Server0**.