Answers: 6.1.4.8 Lab – Configure Firewall Settings

Objectives

In this lab, you will configure firewall settings to use MAC address filtering, a DMZ, and single port forwarding on a wireless router to manage the connections and traffic through the wireless router.

Background / Scenario

You recently purchased a wireless router for your home and want to configure MAC filtering to limit the number of devices connecting to the network wireless. Furthermore, you would like to allow your game console to be connected from the Internet by enabling DMZ. As an alternative to enabling DMZ, you will manually forward the specific ports for the desired games.

Required Resources

- A Windows computer with wired and wireless network cards installed
- Wireless router
- Ethernet patch cable

Instructions

Part 1: Log into the Wireless Router

Step 1: Connect the computer to the router.

a. Ask the instructor for the following information that is used during the lab and record the information below.

Questions:

Router Address Information:

IP address:

Type your answers here.

Subnet mask:

Type your answers here.

Router name:

Type your answers here.

DHCP Server Setting Information:

Start IP address:

Type your answers here.

Maximum number of users:

Type your answers here.

Default Router Access:

Router Username / Password:

Type your answers here.

Assigned SSID:

Your Assigned SSID:

Type your answers here.

Note: Only use configurations assigned by the instructor.

b. Plug in the power for the wireless router. Boot the computer and log in as an administrator.

c. Connect the computer to one of the **Ethernet** ports on the wireless router with an Ethernet patch cable.

Note: If this is the first time connecting to the lab router, follow these instructions to set a network location. This will be explained later in the course.

d. If prompted by the **Set Network Location** window, select **Public network**. Click **Close** to accept the network location Public.

e. Open a command prompt and type **ipconfig** to determine the IP address of the default gateway, which should be the IP address of your wireless router. If it is necessary to renew the IP address, enter **ipconfig /renew** at the prompt.

What is the default gateway for the computer?

Type your answers here.

Step 2: Log in to the router.

a. Open **Microsoft Edge** or other web browsers. Enter the IP address of your default gateway in the **Address** field, and then press **Enter**.

b. In the **Windows Security** window, enter administrative user credentials provided by your instructor.

Part 2: Configure Firewall Settings

In this part, you will configure the firewall settings on the router. You will configure MAC filtering to control the devices that could connect to the local network wirelessly. You will also configure the DMZ and single port forwarding to allow forwarding of external traffic to a device in the local private network.

Note: The steps outlined in this part may not be the same for your router. Please refer to the manufacturer's instruction manual for your specific router.

Step 1: Configure MAC filtering

MAC filtering requires the router to check if the devices are allowed to connect the network. This could prevent malicious network activities from unauthorized devices. Although it is difficult to spoof the MAC address because it is hardware-encoded, determined hackers can still circumvent this security feature.

a. The MAC filtering setting, if available, is generally associated with the advanced, wireless, security or firewall settings.

b. Enable MAC filtering.

c. Deny or allow access for the listed MAC addresses.

d. Add the MAC addresses to the MAC filter list.

e. Save the settings.

Step 2: Configure DMZ

A wireless router can block attempts by devices from an external network, such as the internet, to connect to the devices on a private local network. If there is a need for a device to connect to devices on the local network, the DMZ can be enabled on the router. When the DMZ is enabled, all traffic originating from an external source is forwarded to a single device on the local network.

Note: When a DMZ is used to forward all the inbound traffic to a device on the local network, the local device is no longer protected by the router's firewall.

a. The DMZ setting, if available, is generally associated with the advanced, security, or firewall settings.

b. Enable DMZ.

c. Specify a range of IP address or any source IP address.

d. Provide the IP address or MAC address of the host in the DMZ.

e. Save the settings.

Step 3: Single Port Forwarding

Port forwarding allows remote computers to connect to specific services on a specific device within a private local network based on the source IP address, destination TCP port number, and other characteristics of the traffic.

Depending on the router model, more than one port forwarding rule could be configured. With more than one rule configured, the order of the rule on the screen determines the order in which the packets are checked against the rules.

a. The single port forwarding setting, if available, is generally associated with the application/game or firewall settings.

b. Enable single port forwarding and input the desired applications, internal and external ports, protocol and IP address.

c. Save the settings.

Reflection Question

For your router model, what are other available firewall configurations? List them and describe their functions below.

Type your answers here.