Lab – Configure Windows Firewall

Introduction

In this lab, you will explore the Windows Firewall and configure some advanced settings.

Recommended Equipment

- Two Windows PCs directly connected or connected over the network
- Computers must be in the same workgroup and network

Instructions

Step 1: Create and share a folder on PC-1.

a. Log on to **PC-1** as a member of the administrator group. Ask your instructor for the user name and password.

b. Verify that you can ping **PC-2**.

c. On **PC-1**, right-click the desktop, select **New > Folder**. Name the folder **Cisco**.

d. Right-click the Cisco folder, and then select **Properties** > **Sharing** > **Advanced Sharing**. The **Advanced Sharing** window opens. Click **Share this folder** and use the default name **Cisco**. Click **OK**. Close the **Cisco Properties** window.

Step 2: Use File Explorer or Windows Explorer to view PC-1's shared folder.

a. Log on to **PC-2** as a member of the administrator group. Ask your instructor for the user name and password.

b. Open **File Explorer** or **Windows Explorer**. In the left pane, under **Network**, expand **PC-1**.

Question:

Under PC-1, are you able to see the shared folder **Cisco**?

Type your answers here.

Note: If you answered no, ask the instructor for help.

c. Close File Explorer or Windows Explorer.

Step 3: Open Windows Firewall on PC-1.

Note: Use **PC-1** for the rest of the lab unless otherwise stated.

a. To open the Windows Firewall window, click Control Panel > System and Security > Windows Defender Firewall or Windows Firewall.

b. The normal state for the Windows Firewall is **On**.

Question:

What are the benefits of Windows Firewall?

Type your answers here.

Step 4: Investigate the Windows Firewall Allowed Programs feature.

a. Click Allow an app or feature through Windows Defender Firewall. or Allow apps to communicate through Windows Firewall.

b. The **Allowed apps** window opens. Programs and services that Windows Firewall is not blocking will be listed with a check mark. Click **What are the risks of allowing an app to communicate?** or **What are the risks of allowing a program to communicate?**

Note: You can add applications to this list. This may be necessary if you have an application that requires outside communications but for some reason the Windows Firewall cannot perform the configuration automatically.

Creating too many exceptions in your Programs and Services file can have negative consequences.

Describe a negative consequence of having too many exceptions.

Type your answers here.

c. Close Windows Help and Support window.

Step 5: Configure the Windows Firewall Allowed apps feature.

a. In the **Allowed apps** window, click **Change settings**. Remove the check mark from **File and Printer Sharing**. Click **OK**.

b. On **PC-2**, using **File Explorer** or **Windows Explorer**, attempt to open the network connect to **PC-1**.

Question:

Can you connect to PC-1 and view the Cisco shared folder?

Type your answers here.

Did you receive an error message on PC-2? If so, what was the Error message?

Type your answers here.

c. Close all open windows on **PC-2**.

d. On **PC-1**, add a check mark to **File and Printer Sharing**. Click **OK**.

Note: You should be able to add the check mark without needing to click **Change settings**.

e. On **PC-2**, re-open File Explorer or Windows Explorer and attempt to connect to **PC-1**.

Question:

Can you connect to computer 1? Explain.

Type your answers here.

f. Close all open windows on **PC-2** and Log off .

g. Close all windows on **PC-1**.

Step 6: Explore Advanced Security features in Windows Firewall.

Note: Use **PC-1** for the rest of this lab.

a. Click **Control Panel** > in Small icons view, **Administrative Tools** > **Windows Defender Firewall with Advanced Security** or **Windows Firewall with Advanced Security**.

b. In the left panel of the **Windows Defender Firewall with Advanced Security** or **Windows Firwall with Advanced Security** window, you can select items to configure **Inbound Rules**, **Outbound Rules**, or **Connection Security Rules**. You can also click **Monitoring** to view the status of configured rules. Click **Inbound Rules**.

c. In the middle panel, scroll down until you find the inbound rule named **Files and Printer Sharing (Echo Request – ICMPv4-In)**. Right-click the rule and select **Properties**, then select the **Advanced** tab.

d. The **Advanced** tab displays the profile(s) used by the computer. Click **Customize** in the **Interface Types** area of the window.

e. The **Customize Interface Types** window displays the different connections configured for your computer. Leave **All interface types** selected, then click **OK**.

f. Click the **Programs and Services** tab. In the **Services** section, click **Settings...**.

List the short name of four services that are available in the **Customize Service Settnigs** window.

Type your answers here.

g. Click **Cancel** to close the **Customize Service Settings window**.

h. Click the **Protocols and Ports** tab.

Note: There are many applications that users do not normally see that also need to get through the Windows Firewall to access your computer. These are the network level programs that direct traffic on the network and the internet.

i. For the ICMP settings, click **Customize**.

j. The **Customize ICMP Settings** window opens. Allowing incoming echo requests is what allows network users to ping your computer to determine if it is present on the network.

List four of the Specific ICMP types.

Type your answers here.

k. Close all open windows on **PC-1**.

l. Right-click the **Cisco** folder on the Desktop, then select **Delete**.

Reflection Question

What are some possible reasons you may need to make firewall changes?

Type your answers here.