IT Essentials 5.0

10.3.1.8 Lab - Configure a Windows 7 Firewall

Print and complete this lab.

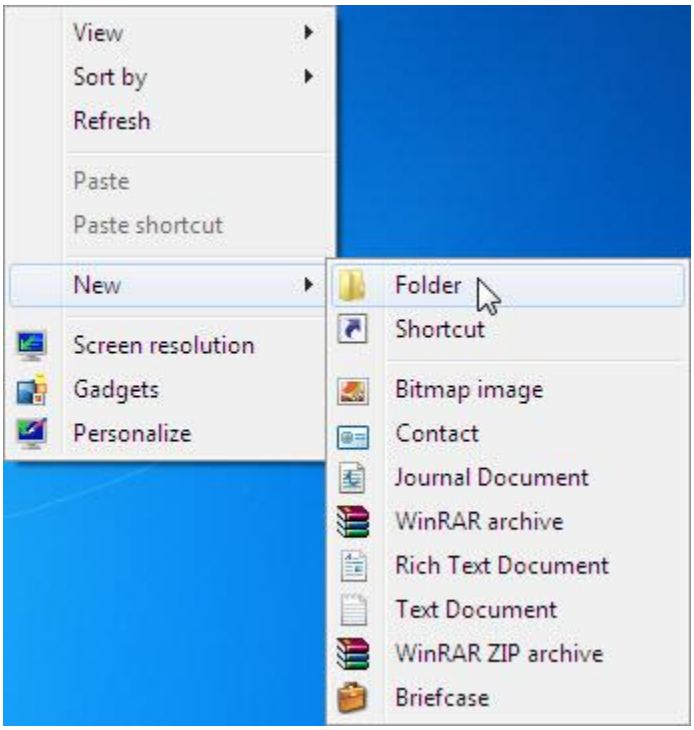
In this lab, you will explore the Windows 7 Firewall and configure some advanced settings.

Recommended Equipment

- Two computers directly connected or connected through a hub or switch
- Windows 7 installed on both computers
- Computers are in the same workgroup and share the same subnet mask

Step 1

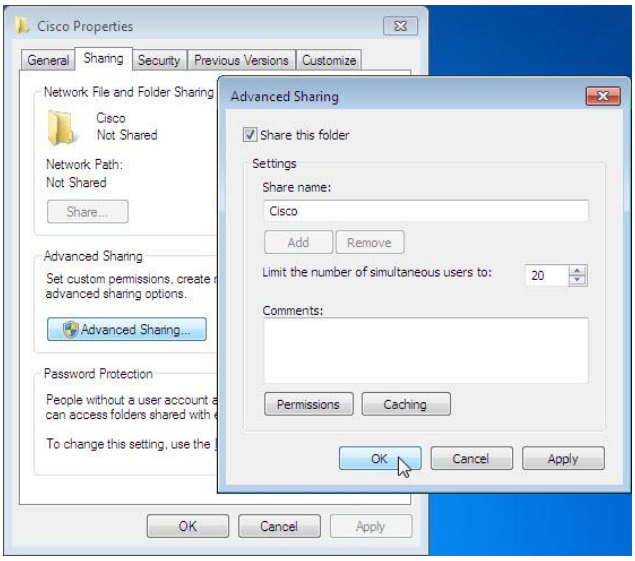
For computer 1, right-click on the desktop, select **New > Folder**.



Name the folder Cisco.

Right-click on the **Cisco** folder then select **Share with > Advanced sharing > Advanced Sharing**.

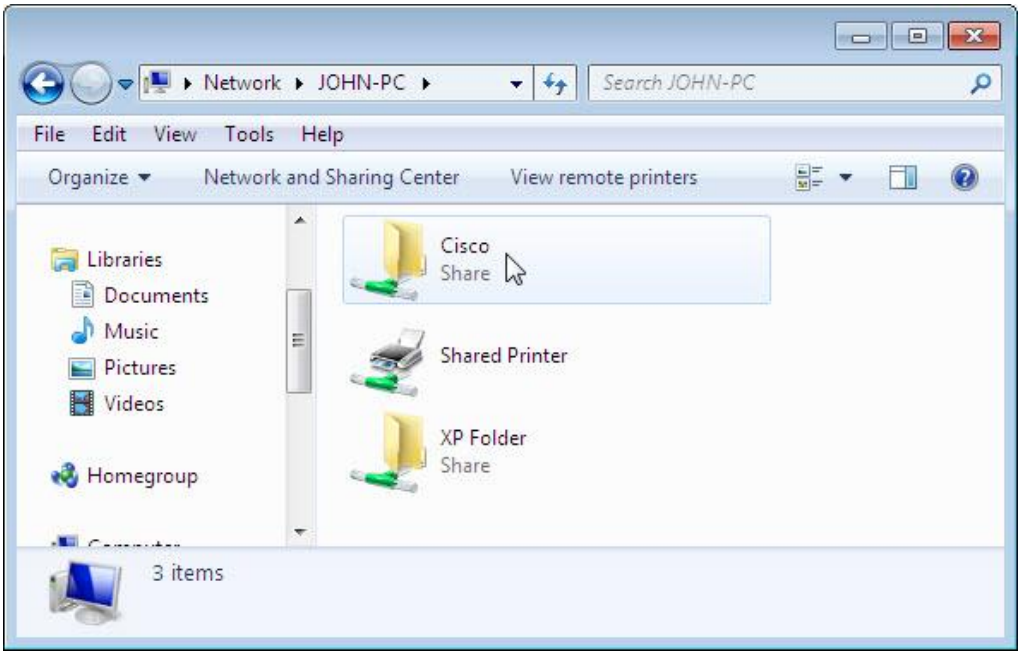
The “Advanced Sharing” window opens.



Share the folder, use the default name **Cisco**.

From computer 2 click **Start > Control Panel > Network and Sharing Center > Network** icon.

Double-click **computer 1**.



Can you see the shared folder Cisco?

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

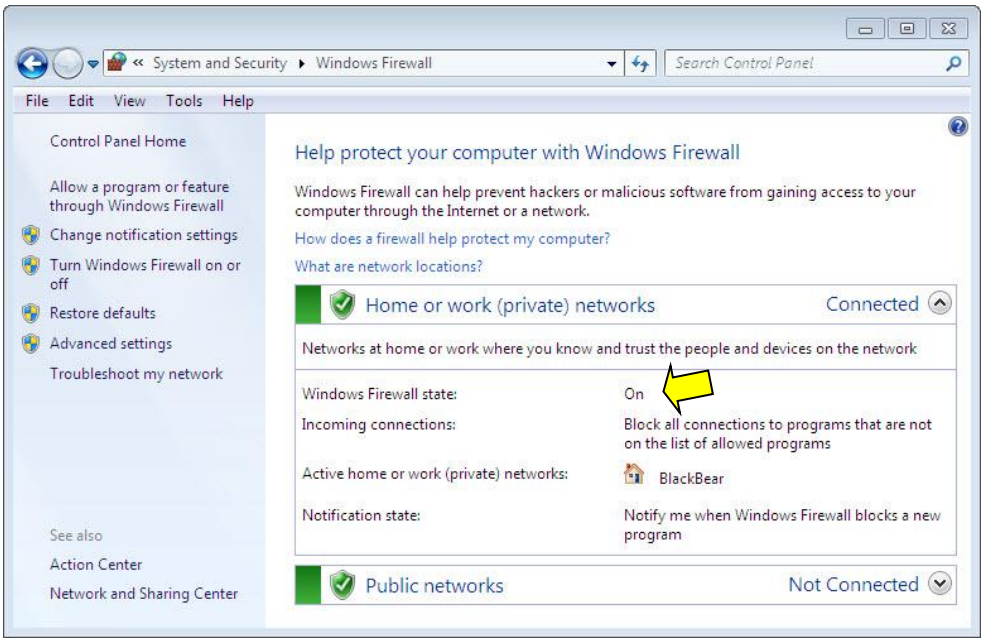
Close **Network**.

Note: Use computer 1 for the rest of the lab unless otherwise stated.

Step 2

Navigate to the Windows 7 Firewall:

Click **Start > Control Panel > System and Security > Windows Firewall**.

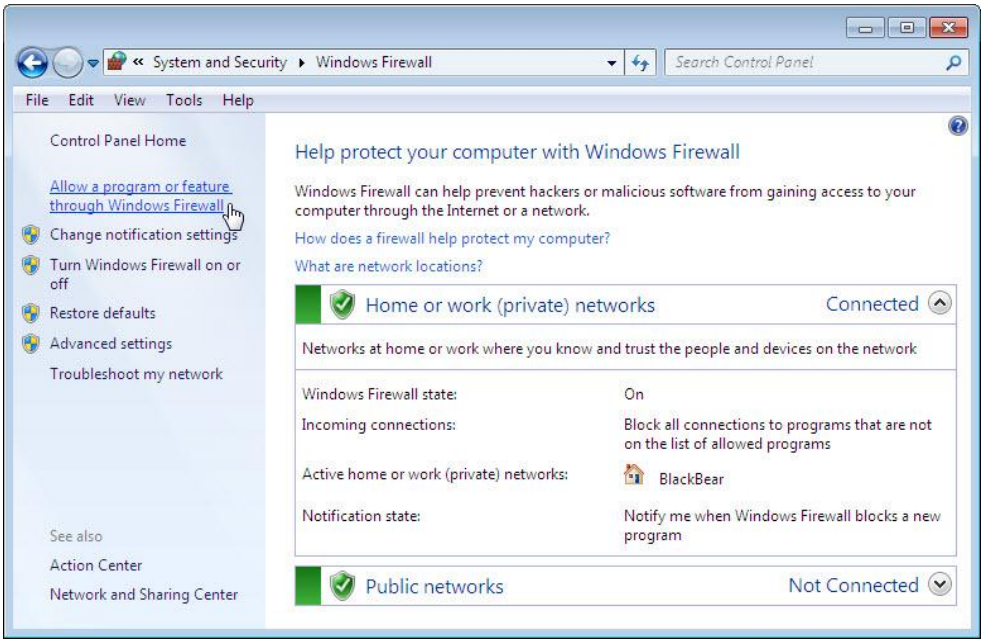


The Firewall indicator shows the status of the firewall. The normal setting is "**On**".

In the space below, state the benefits of Windows Firewall.

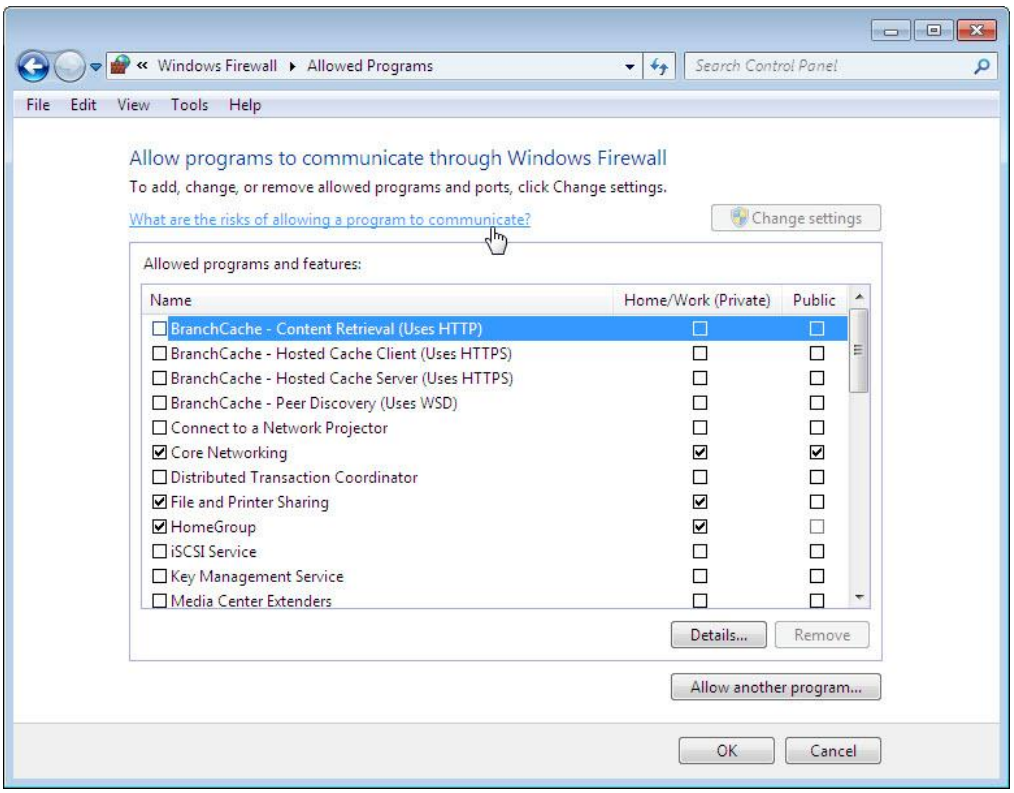
Step 3

Click **Allow a program or feature through Windows Firewall**.



Step 4

The “Allowed Programs” window opens.

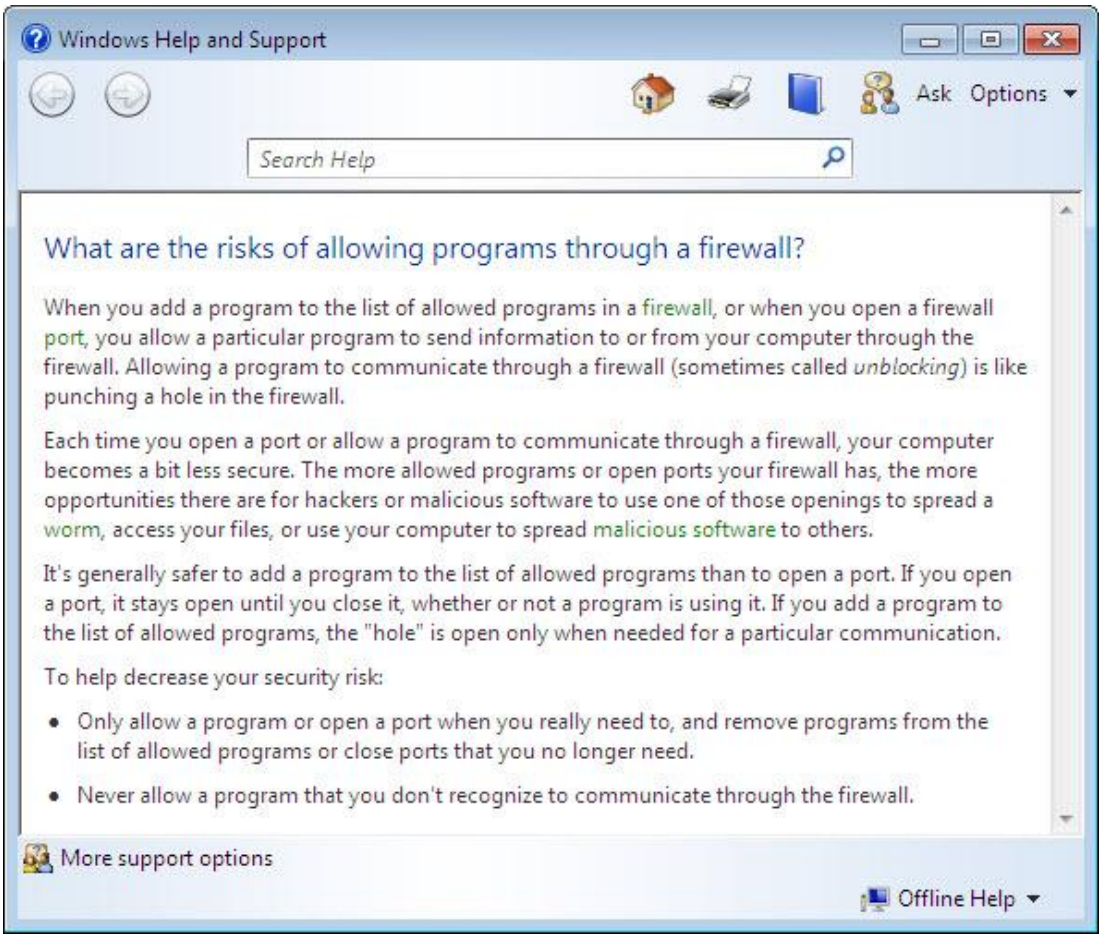


Programs and services that Windows Firewall is not blocking will be listed with a check mark.

You can add applications to this list. This may be necessary if your customer has an application that requires outside communications but for some reason the Windows Firewall cannot perform the configuration automatically. You must be logged on to this computer as an administrator to complete this procedure.

Click **What are the risks of allowing a program to communicate?**.

The “Windows Help and Support” window opens.



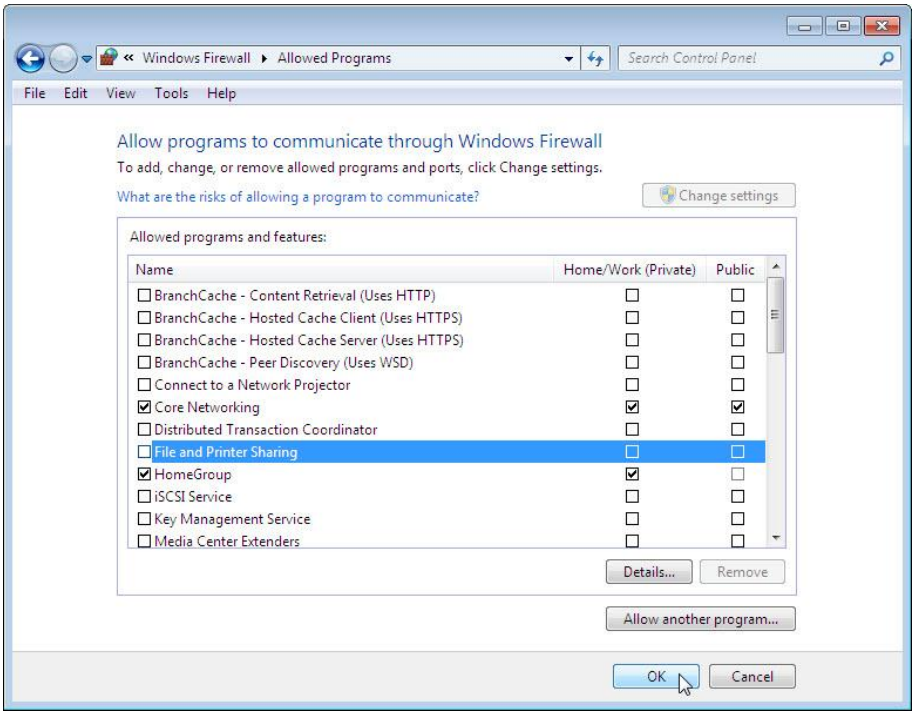
Creating too many exceptions in your Programs and Services file can have negative consequences. Describe a negative consequence of having too many exceptions.

Close Windows Help and Support window.

Step 5

From computer 1:

Click on “Allowed Programs” window so it is active.

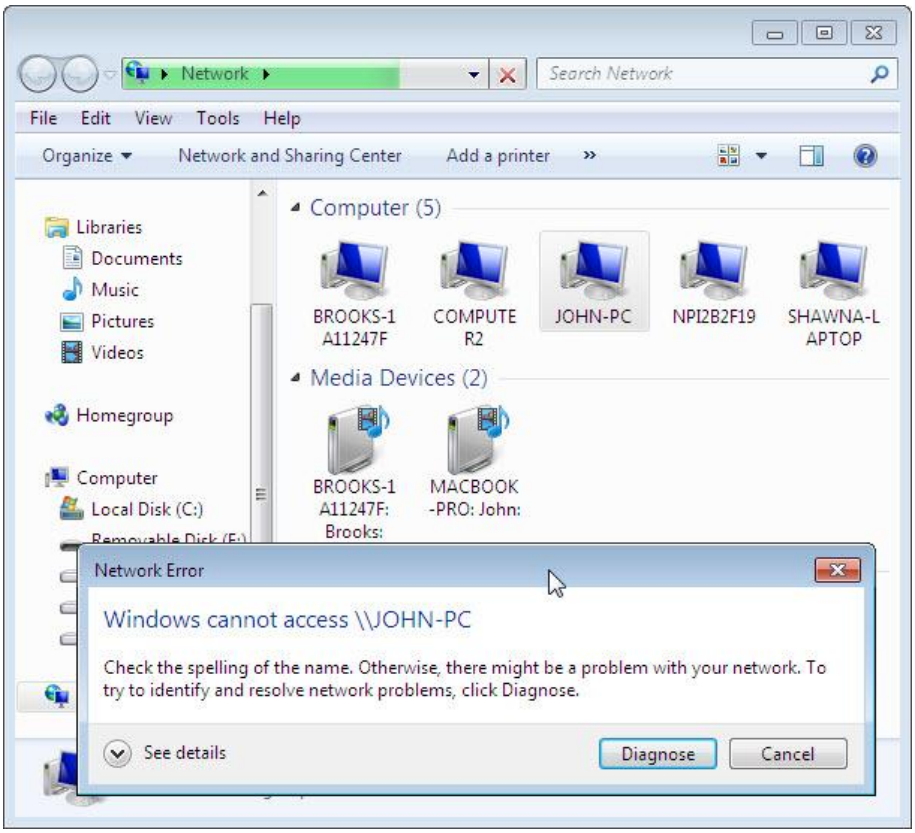


To turn off an exception, remove the check mark from **File and Printer Sharing > OK**.

From computer 2:

Open the network connect to computer 1.

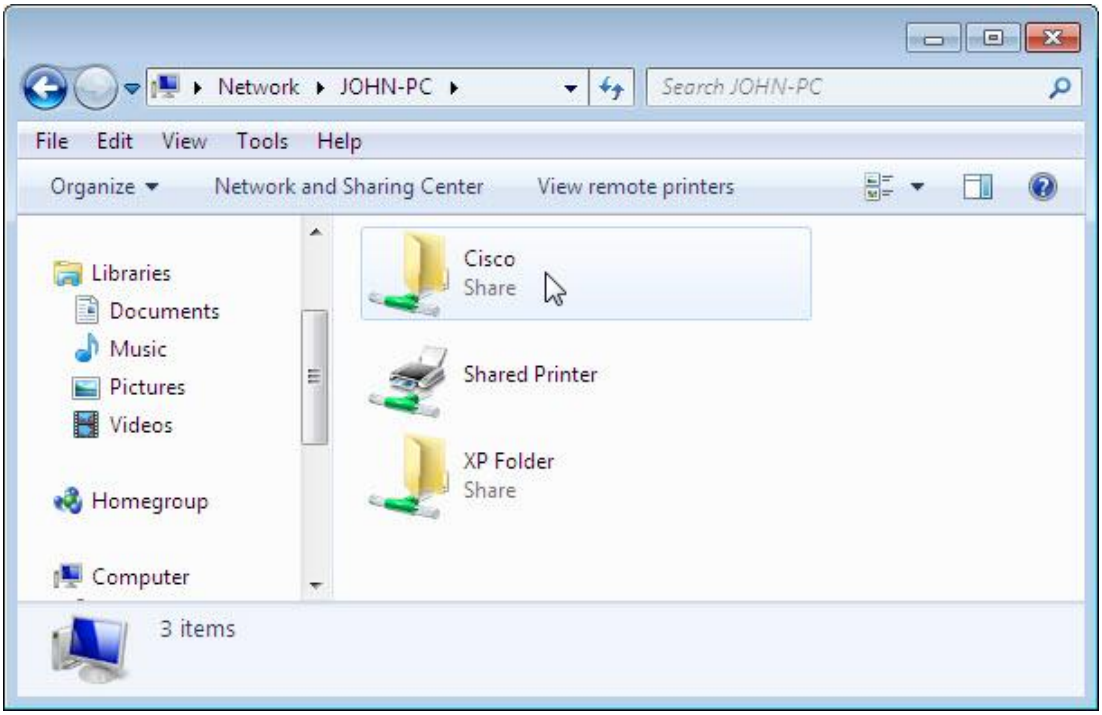
Click **Start > Control Panel > Network and Sharing Center > Network** icon.



Can you connect to computer 1?

From computer 1:
To turn on an exception add a check mark to **File and Printer Sharing > OK**.

From computer 2:
Refresh **Network** screen and connect to computer 1.

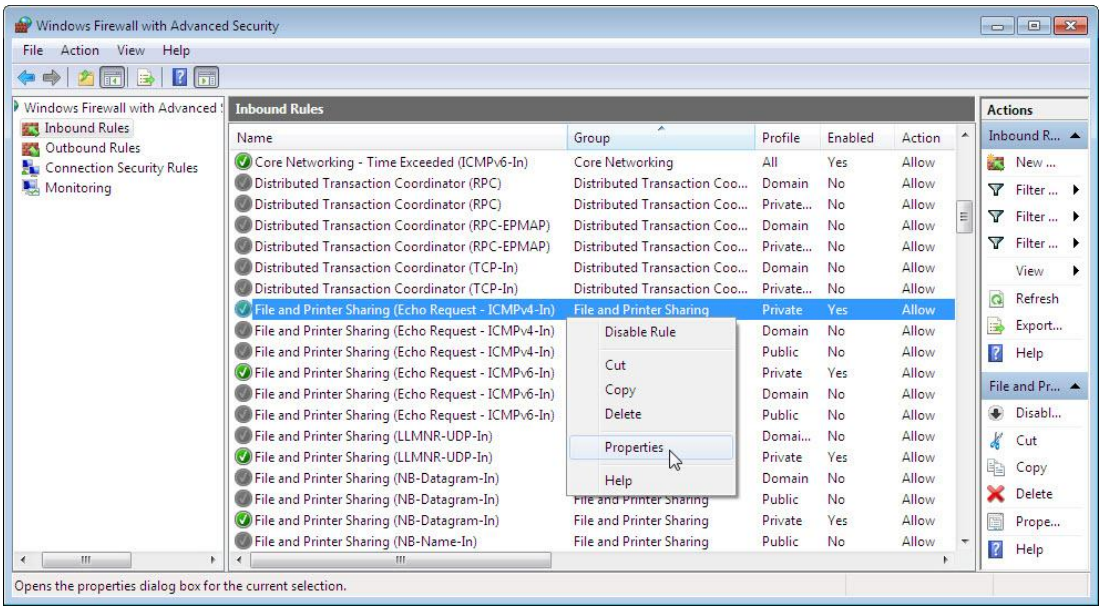


Can you connect to computer 1?

Log off computer 2. Use computer 1 for the rest of the lab.

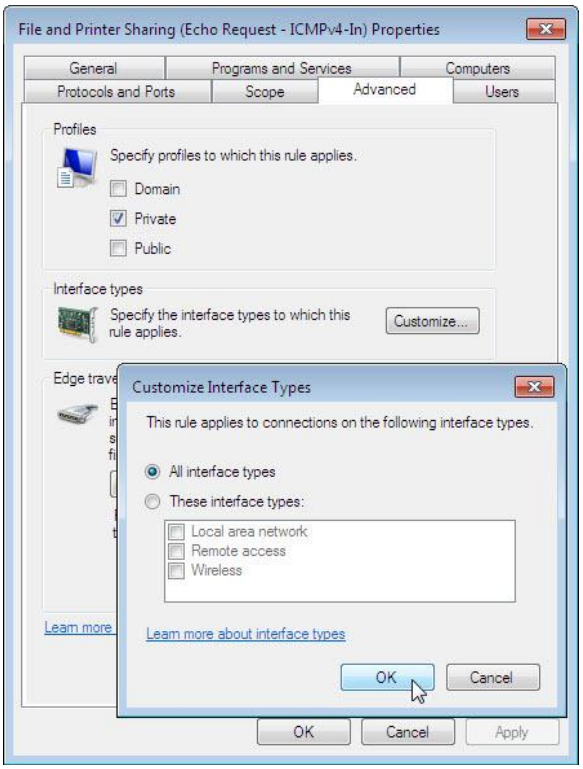
Step 6

Click **Start > Control Panel > System and Security > Administrative Tools > Windows Firewall with Advanced Security > Inbound Rules**.



Expand the window so you can see the full name of the Inbound rules. Locate Files and Printer Sharing (Echo Request – ICMPv4-In).

Right-click on the rule and select **Properties > Advanced** tab **> Customize**.

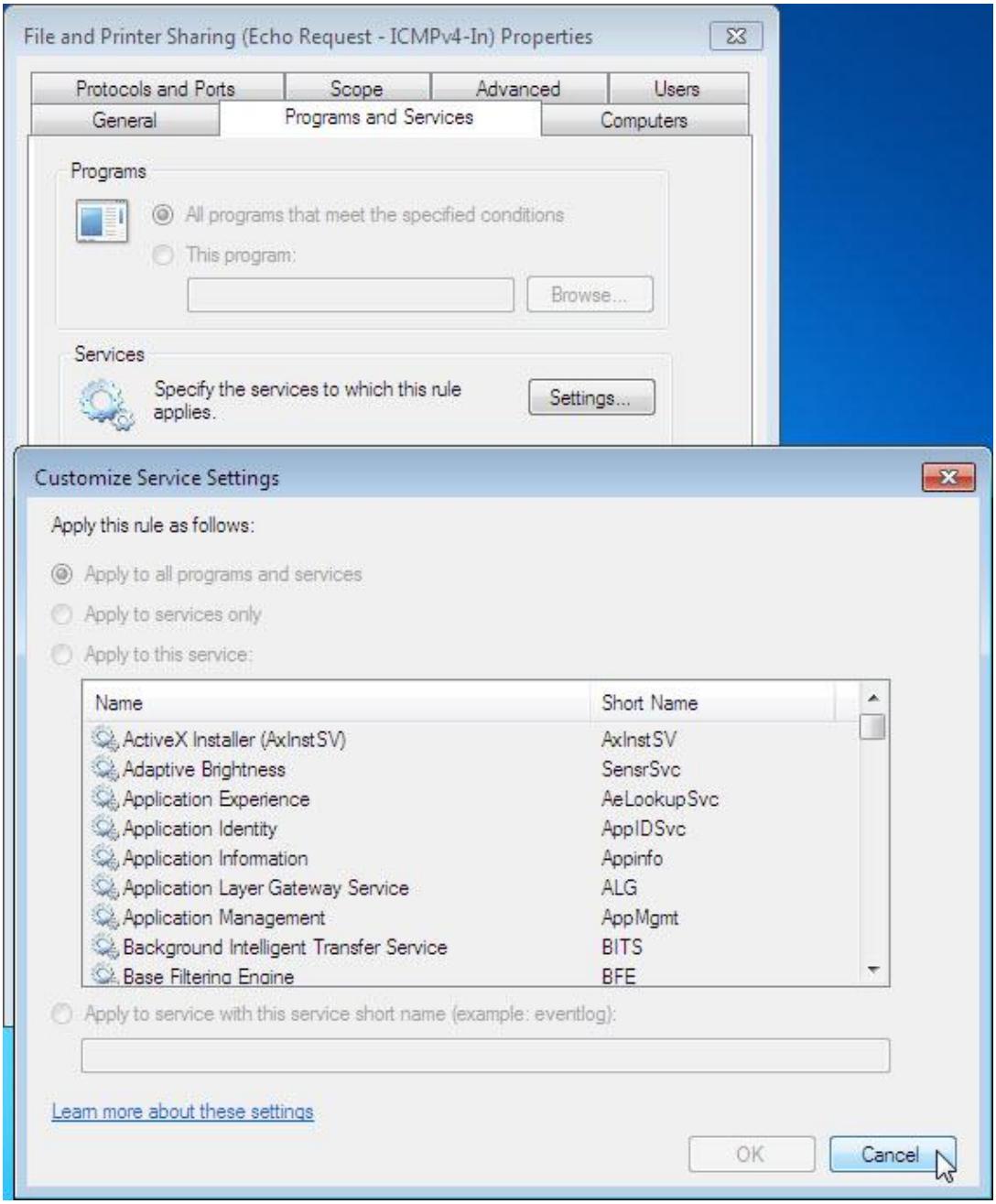


The Advance tab displays the profile(s) used by the computer and the “Customize Interface Types” window displays the different connections configured for your computer.

Click **OK**.

Click **Programs and Services** tab.

The “Customize Service Settings” window opens.



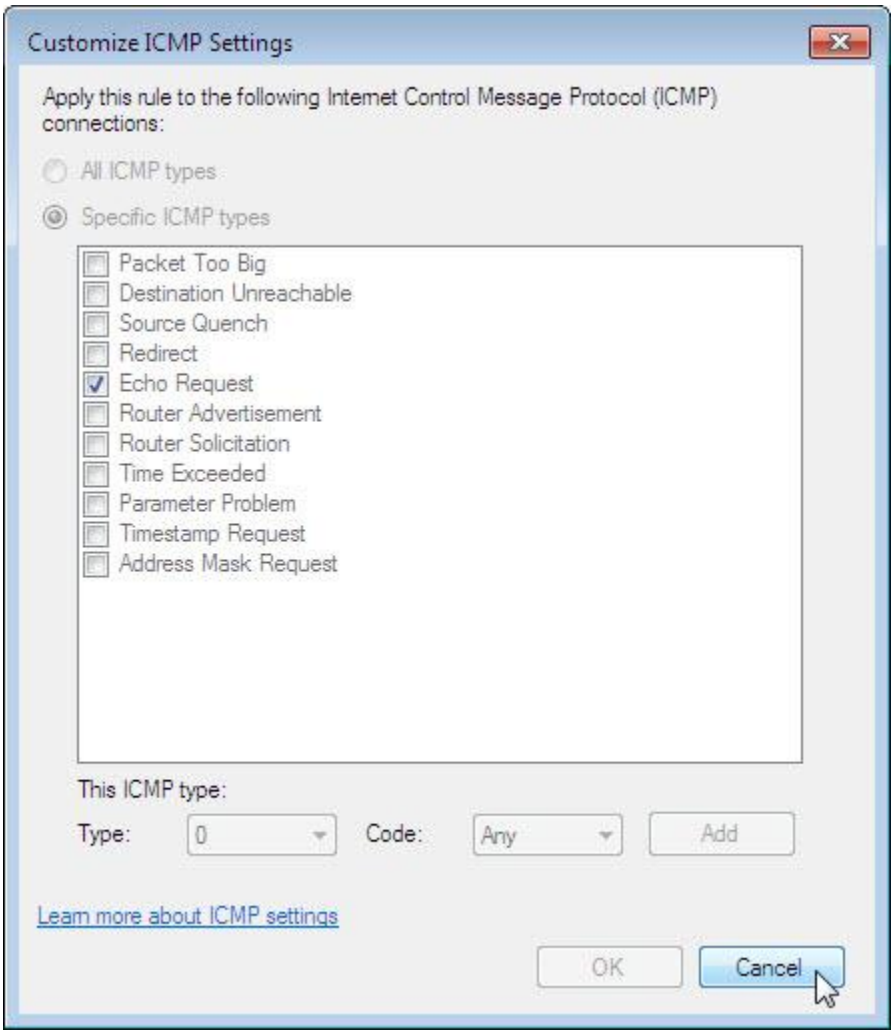
In the space below, list the short name of four services that are available.

Click **Cancel**.

Step 7

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 commands that direct traffic on the network and the Internet.

Click **Protocols and Ports** tab. For the ICMP settings, click the **Customize** button. You will see the menu where ICMP exceptions are configured.



In the example here, allowing incoming echo requests is what allows network users to ping your computer to determine if it is present on the network. It also allows you to see how fast information travels to and from your computer.

In the space below, list the Specific ICMP types.

Close all windows.