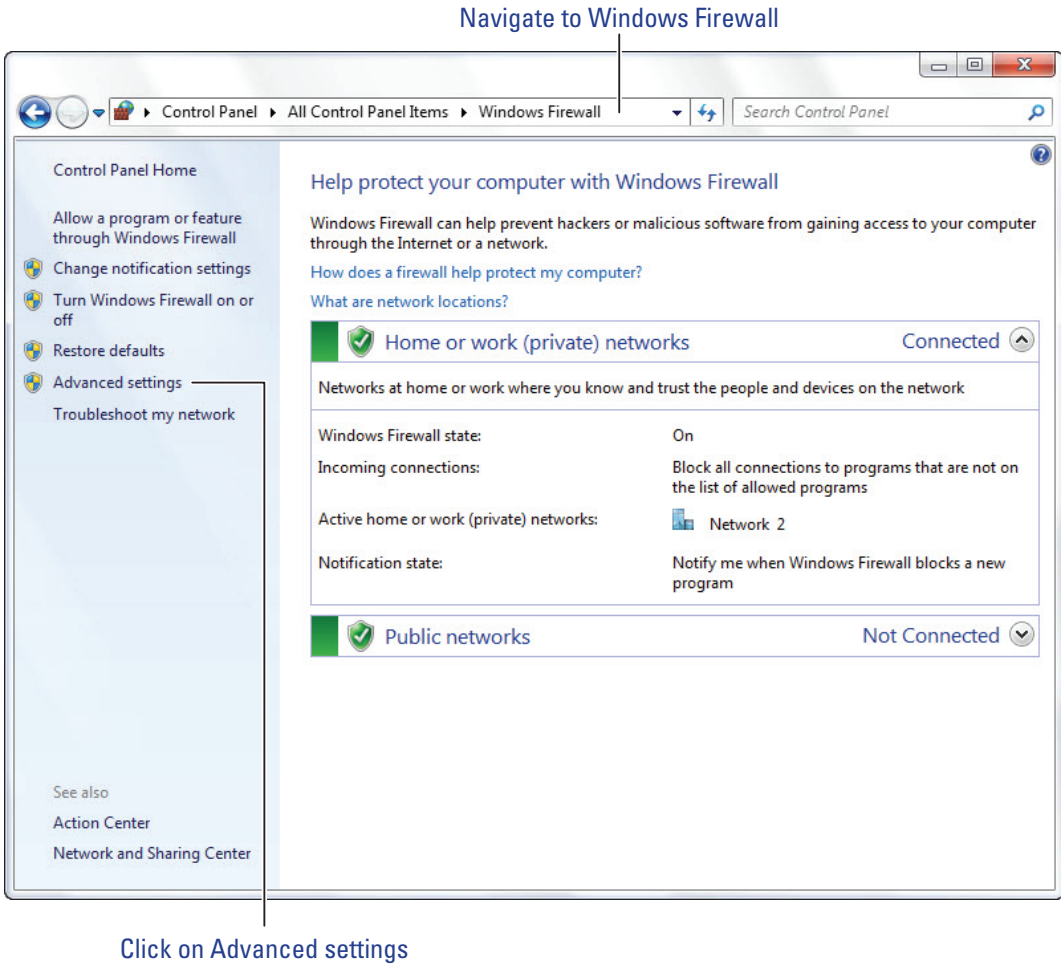
Note The screenshots below reflect a Windows 2007 operating system. Navigating through the firewall settings in other editions of Windows will be slightly different.

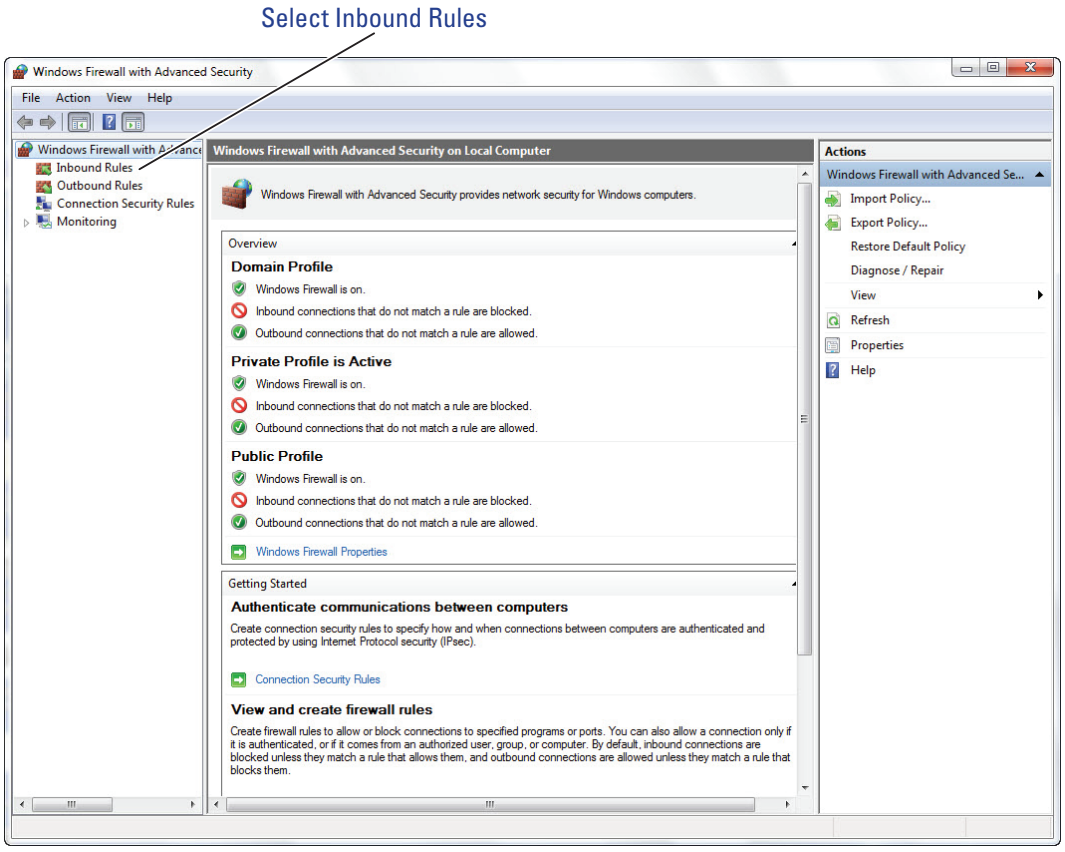
1 Navigate to your Windows Firewall settings from your PC's control panel. See Figure 10. Then, click on Advanced settings.

Figure 10 Windows Firewall



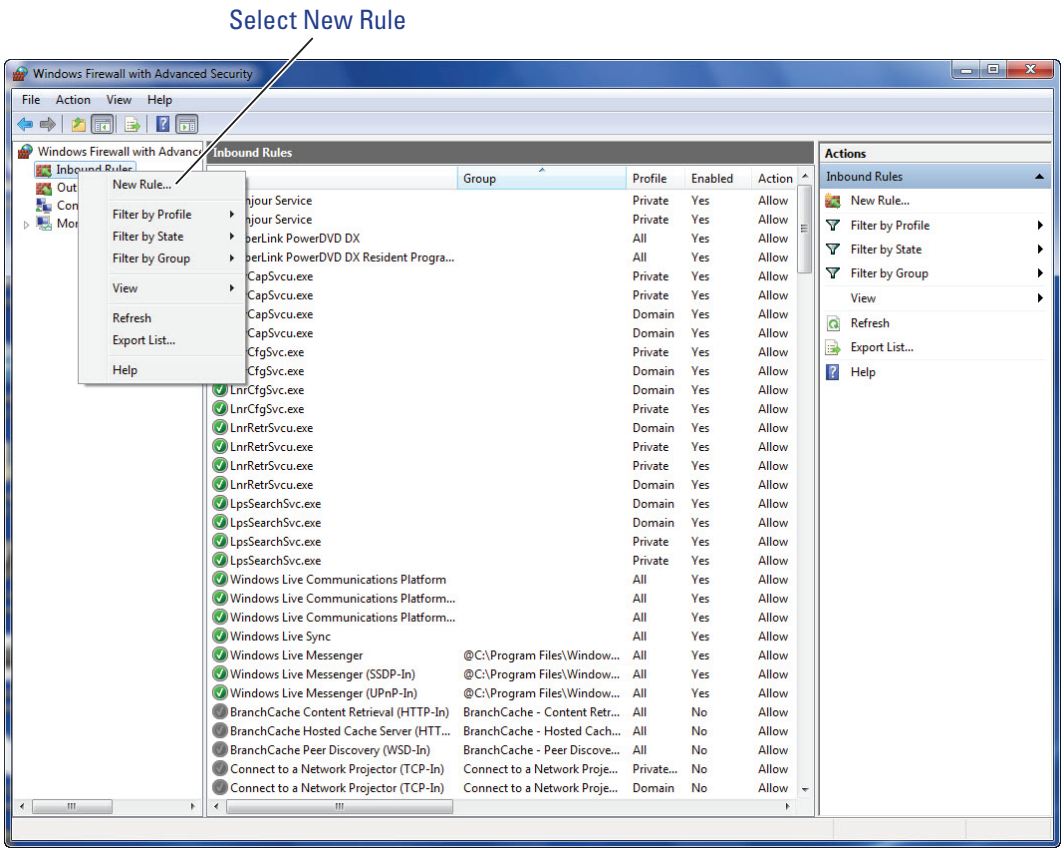
2 Select Inbound Rules.

Figure 11 Inbound Rules



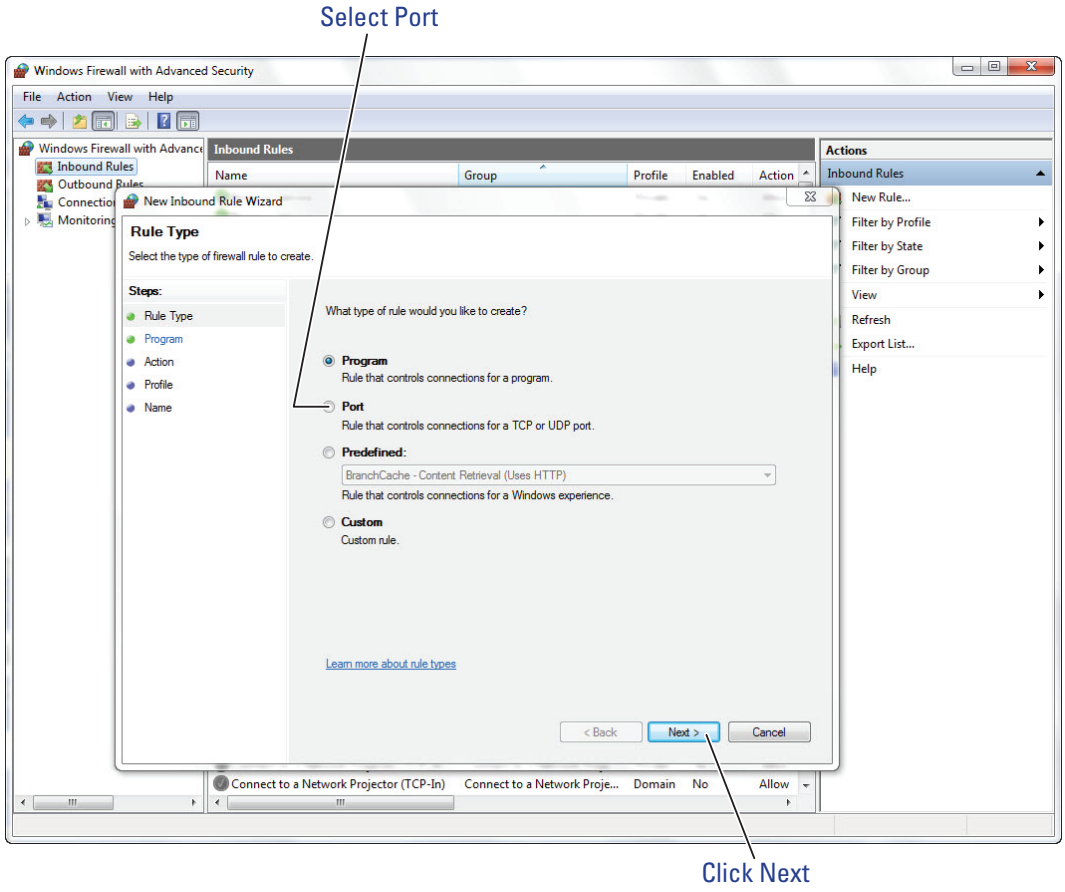
3 Right click on Inbound Rules to open an option menu. Select New Rule from the menu.

Figure 12 New Rule



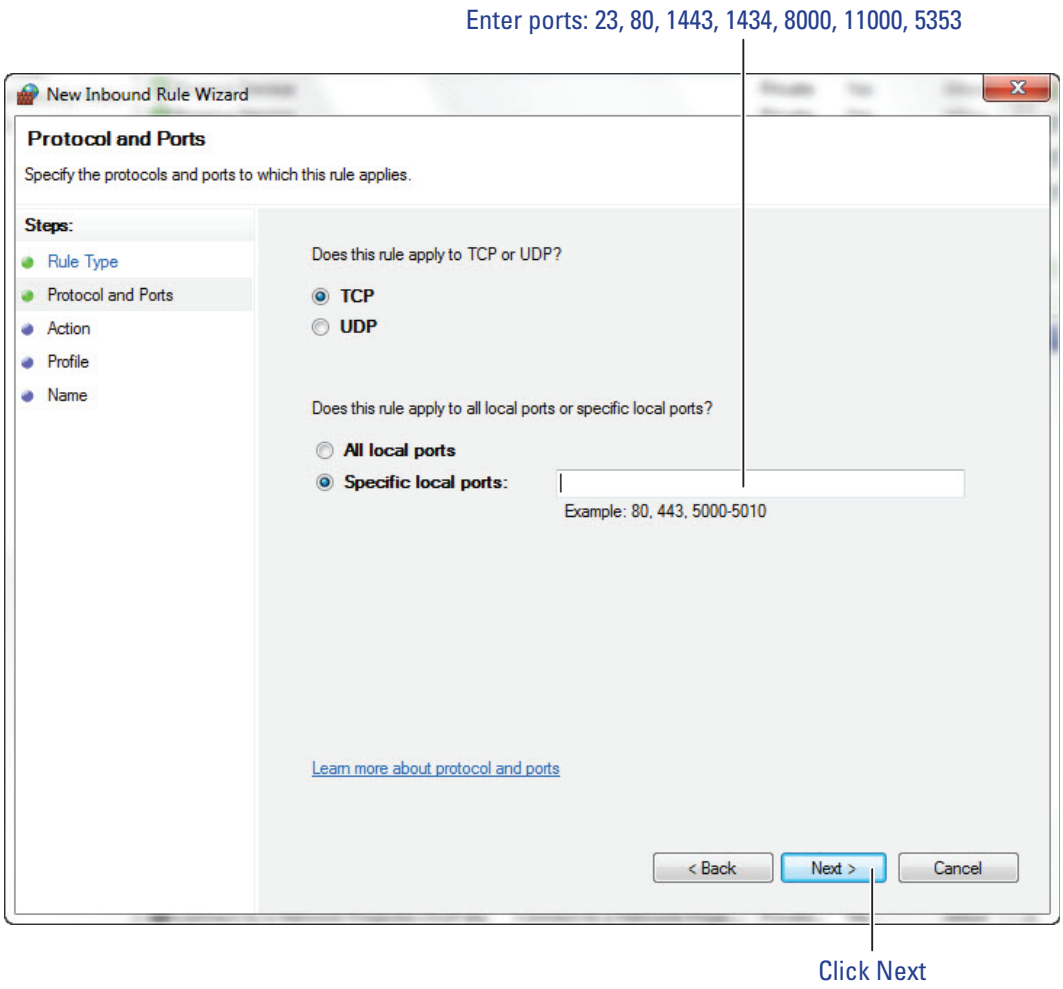
4 In the New Inbound Rule Wizard window, select Port. Click Next to continue.

Figure 13 Create Port Rule



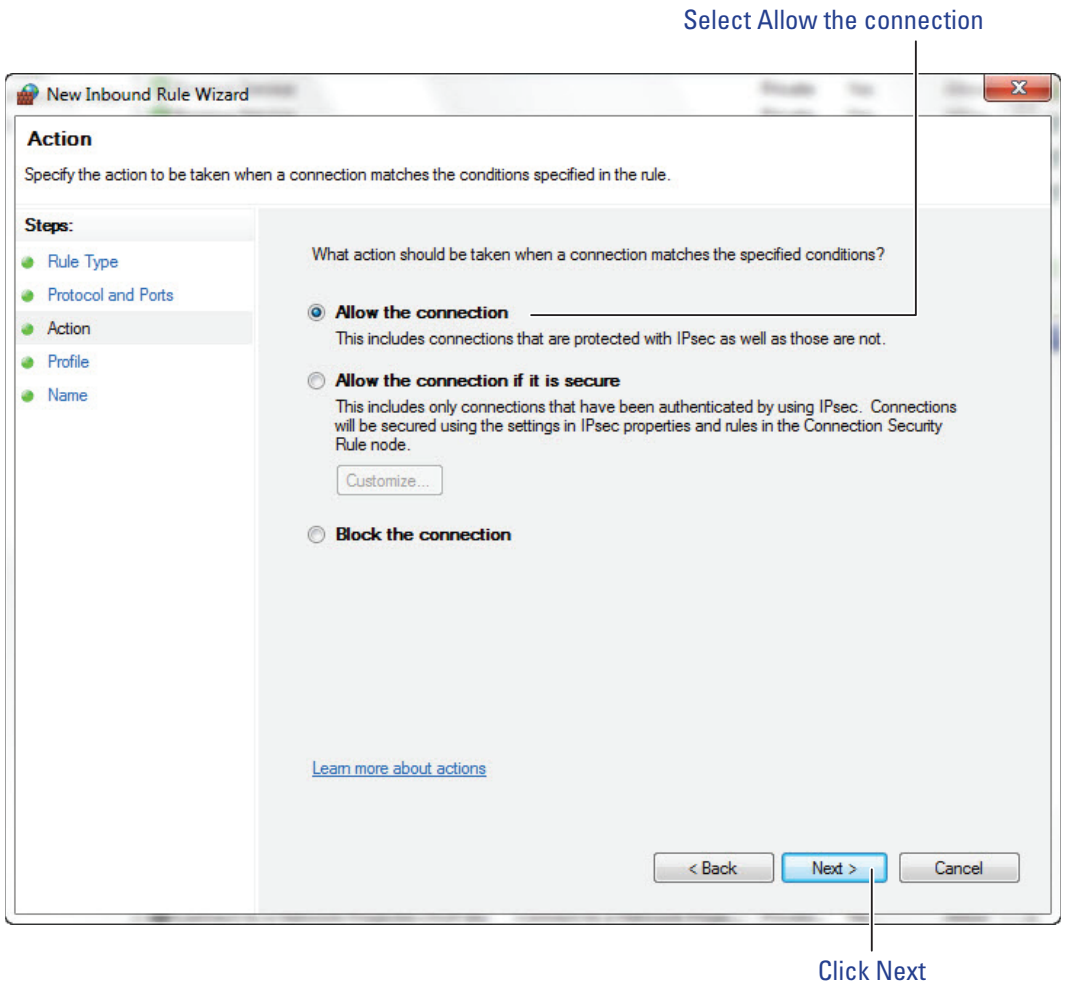
5 Enter the following ports into the “Specific local posts” field: 23, 80, 1443, 1434, 8000, 11000, 5353. Then, click Next to continue.

Figure 14 Enter Ports



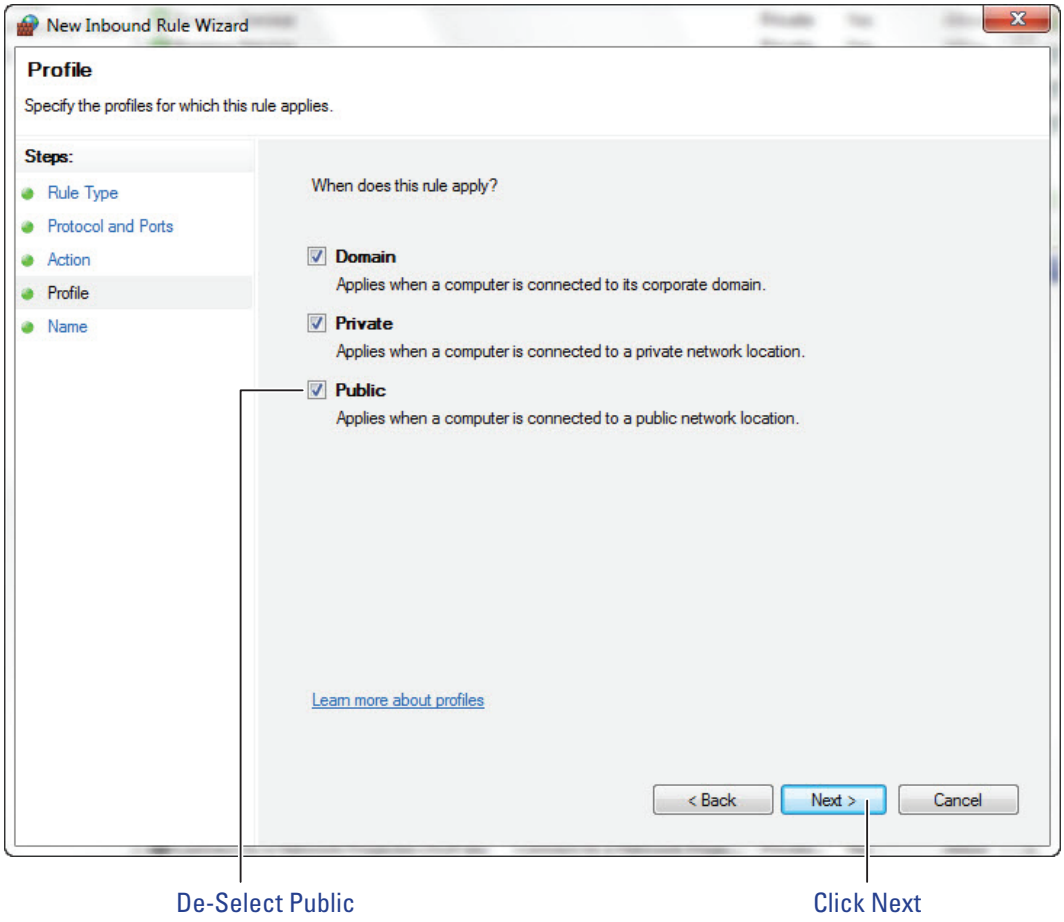
6 Select Allow the connection. Click Next to continue. See Figure 15.

Figure 15 Allow the Connection



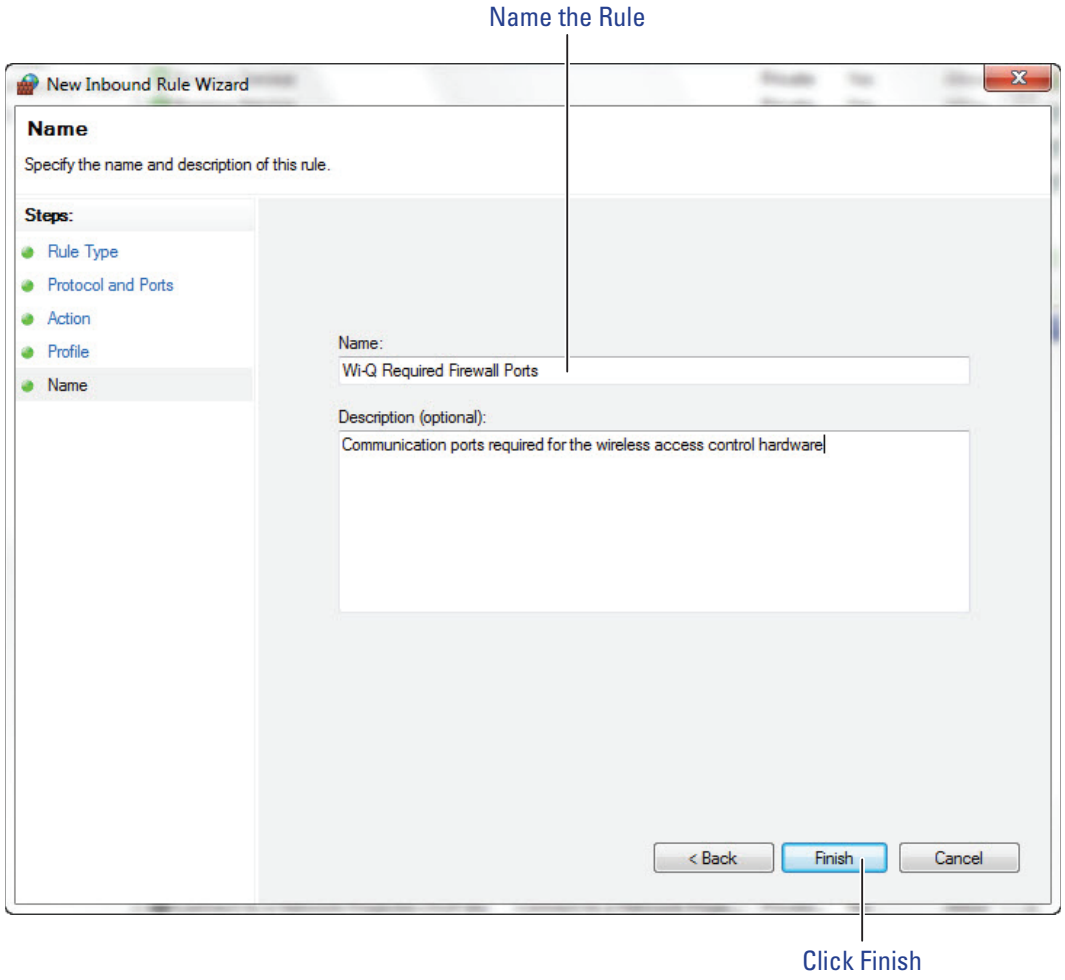
7 De-select the Public option. Click Next.

Figure 16 De-select Public



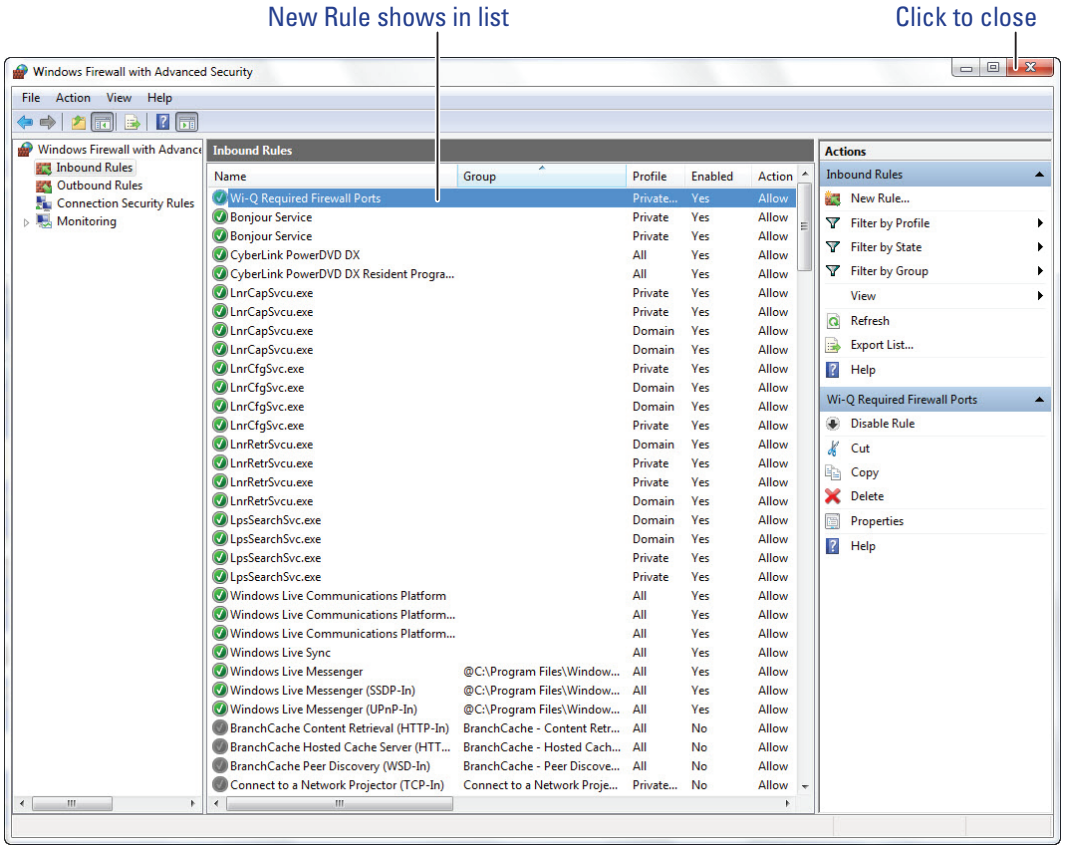
8 Give the new rule a name that can be easily identified by an administrator. Once finished, click Finish. See Figure 17.

Figure 17 Name the Rule



9 The new rule now appears in the list. The Firewall Settings module may now be closed. See Figure 18.

Figure 18 Inbound Rules List



Gather and Organize Segment Data (Task 4)

As the technical team works on planning and installing hardware using the Site Plan, a program administrator or other person responsible for the software side of program setup should be making plans to populate and configure Wi-Q AMS or Omnilock WAMS.

Device Information

You will need the MAC numbers, device names, capacities, and physical locations of all Portal Gateways so that you can easily identify them and assign them to the correct location within the AMS/WAMS Segment Tree. Ensure your site technical team will provide you this information as they work their way through the site.