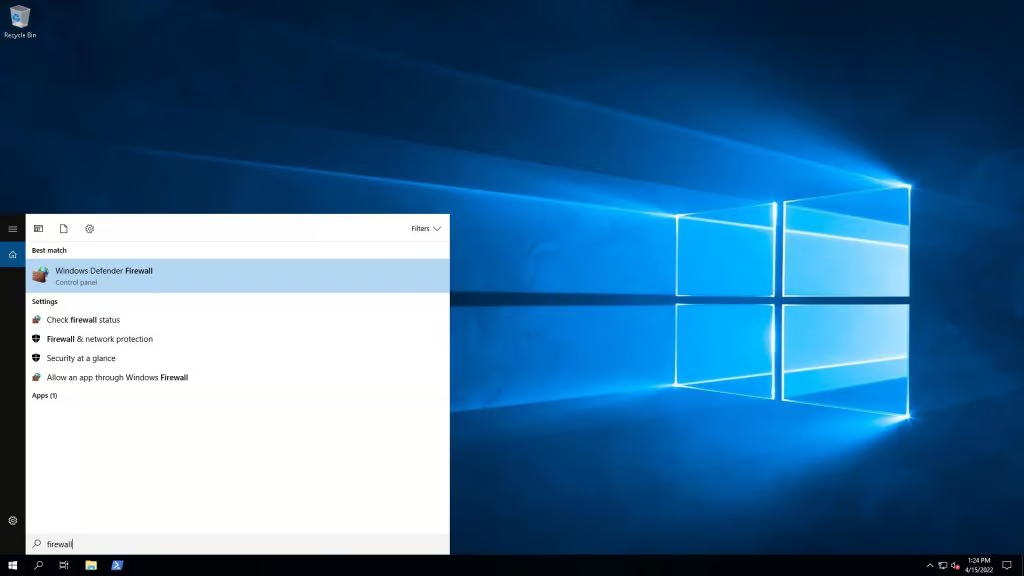
**TASK 4**

**Step 1: Access the Windows firewall management console**

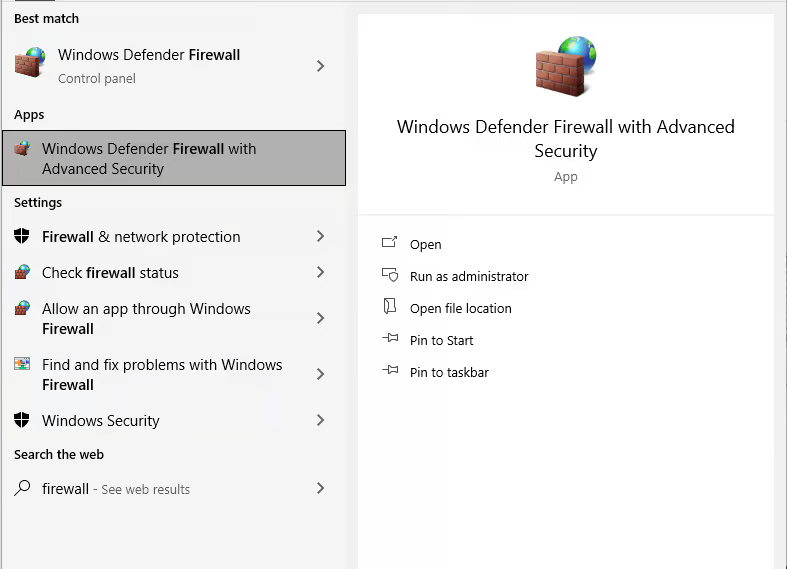
You can view various settings from the management console, such as the Overview of the Domain Profile and multiple wizards to execute tasks within the Windows Firewall.

1. Log into your server via [Remote Desktop](https://www.liquidweb.com/blog/accessing-your-windows-server-with-remote-desktop/).

2. Click the **Search**icon on the bottom-left of the taskbar and type **firewall**.



3. Click on **Windows Defender Firewall with Advanced Security**. This action opens the Windows Firewall Management Console.



**Step 2: View and configure inbound rules in the console**

1. From the left-hand navigation, click **Inbound Rules** to expose the Inbound Rules pane on the right.

Click the **Enabled**column at the top to sort your rules by status until the value of Yes is at the top. Make a note of the preconfigured rules.

**Open a Port in Windows Server Firewall**

1. Open the firewall manager again.

2. Click **Inbound Rules** from the left pane to reveal the Inbound Rules pane on the right.

3. Click **New Rule** in the right-hand pane to open the New Inbound Rule Wizard.

4. In the New Inbound Rule Wizard, under the Rule Type section, select the Port radio button and click **Next**.

5. In the Protocol and Ports section, select TCP or UDP. Next, select the radio button for All local ports or Specific local ports. For this tutorial, choose Specific local ports and enter the corresponding port number. If listing multiple ports, split them with a comma. Once completed, click **Next**.

6. In the Action section, select **Allow the connection** (or choose the setting for your requirements) and click **Next**.

7. In the Profile section, select all appropriate profiles for when this rule applies and click **Next**.

8. Finally, give your new rule a descriptive name so that it is easy to find later, and click **Finish**.

**Close a port in Windows Server firewall**

If you need to close a previously opened port, find and disable the rule that opens the port using these steps.

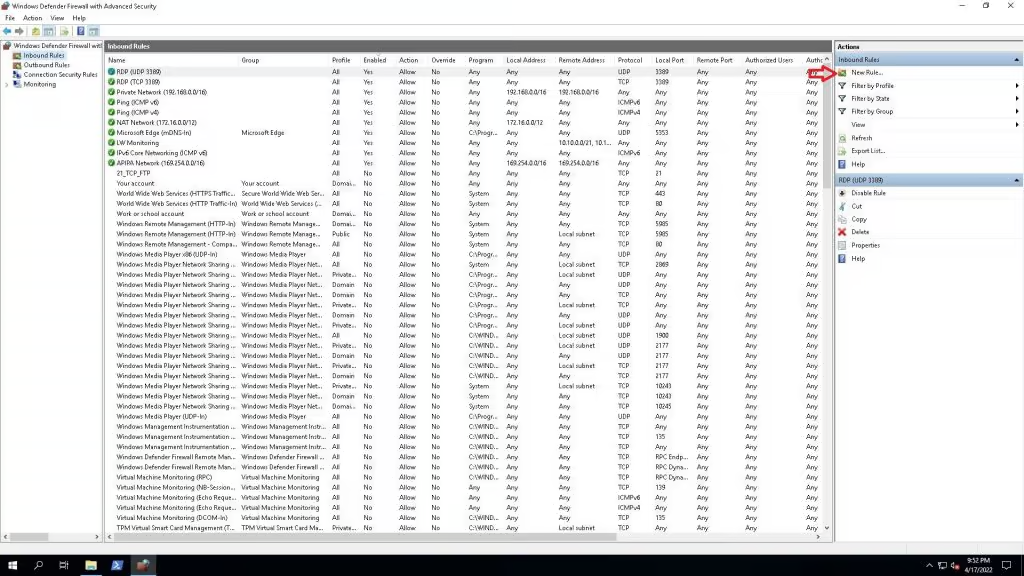
1. Open the firewall manager.

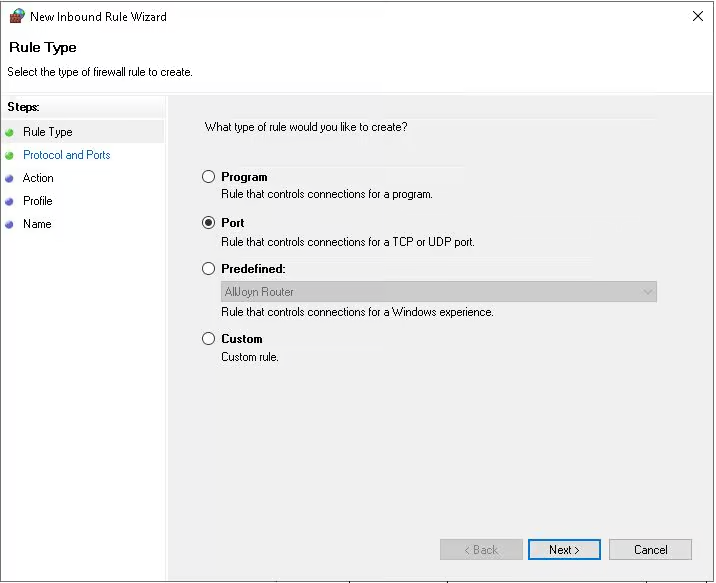
2. Click **Inbound Rules** from the left pane to reveal the Inbound Rules pane on the right.

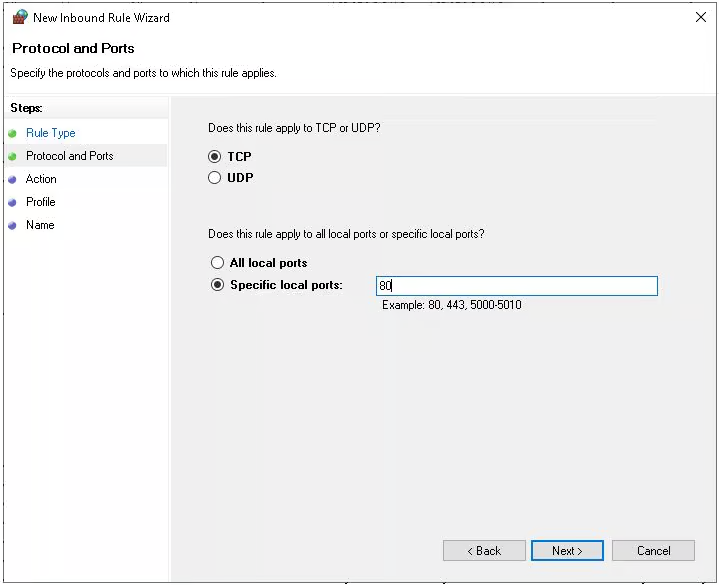
3. Click the **Enabled**column at the top to sort your rules by status until the value of Yes is at the top.

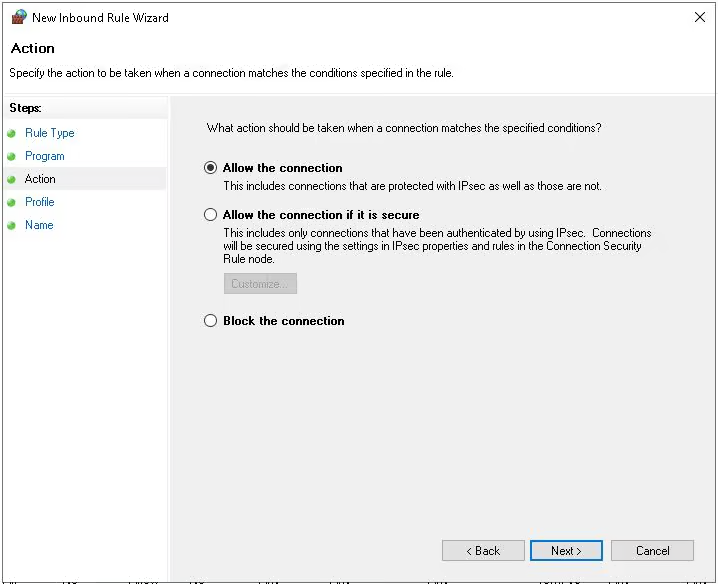
4. Locate the rule for the local port you would like to close.

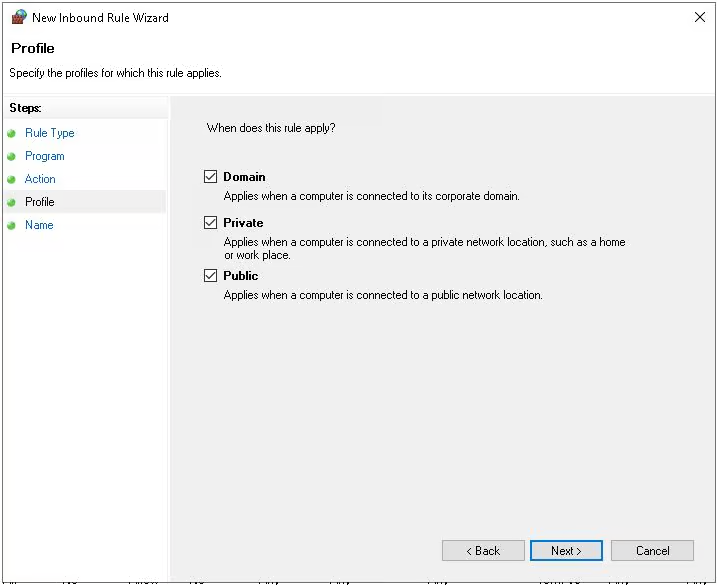
5. Right-click on the rule and select **Disable**.

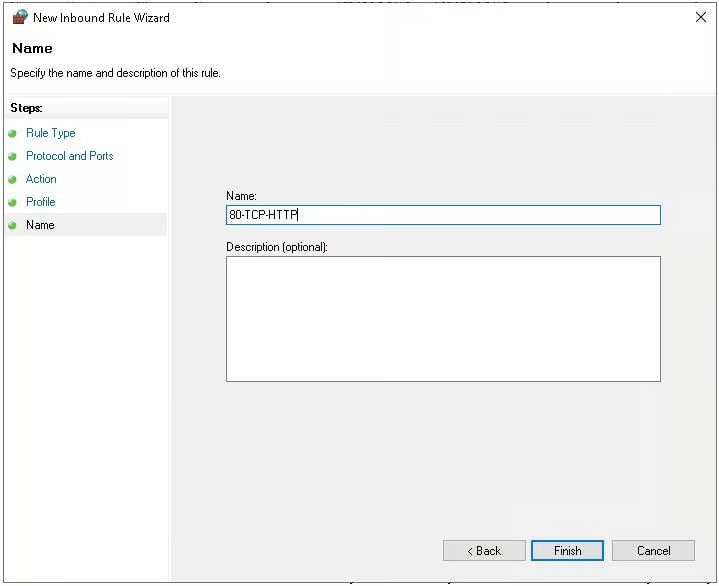












**Close a port in Windows Server firewall**

If you need to close a previously opened port, find and disable the rule that opens the port using these steps.

1. Open the firewall manager.

2. Click **Inbound Rules** from the left pane to reveal the Inbound Rules pane on the right.

3. Click the **Enabled**column at the top to sort your rules by status until the value of Yes is at the top.

4. Locate the rule for the local port you would like to close.

5. Right-click on the rule and select **Disable**.

**Open a port for a specific program in Windows Server firewall**

Some applications use more than one port or more than one protocol when communicating over the Internet. You can create a Program Rule Type in Windows Defender Firewall to simplify allowing traffic for these programs. These rules also add additional security, as the ports a program typically listens on are not open unless the defined program is running.

Here are the steps to open a port for a specific program.

1. Open the firewall manager.

2. Click **Inbound Rules** from the left pane to reveal the Inbound Rules pane on the right.

3. On the Inbound Rules pane, click **New Rule** to open the New Inbound Rule Wizard.

4. In the New Inbound Rule Wizard under Rule Type, select **Program**and click **Next**.

