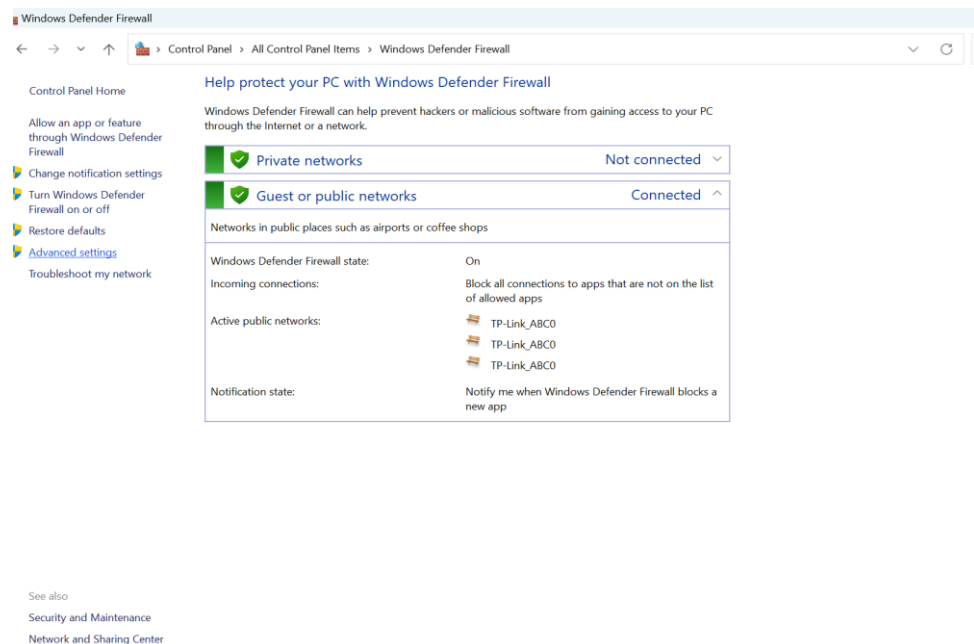**TASK-4**

Aim: Setup and Use a Firewall on Windows/Linux

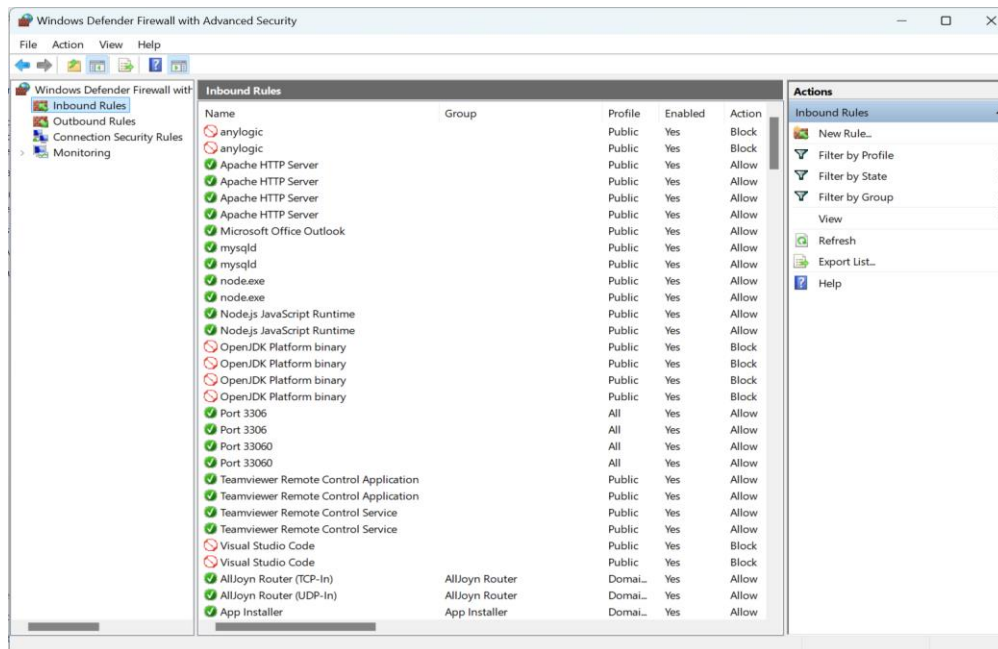**Step 1: Open Windows Firewall**

1. Press Win + R, type control, press Enter.

2. Click **"System and Security"** > **"Windows Defender Firewall"**.


Step 2: View Current Rules

1. Click **"Advanced settings"** on the left panel.

2. In the new window (**Windows Defender Firewall with Advanced Security**), you'll see:

   o **Inbound Rules**

   o **Outbound Rules**

Step 3: Block Inbound Traffic on Port 23 (Telnet)

1. In the left panel, click **Inbound Rules**.

2. In the right panel, click **New Rule…**

3. Select **Port** > Click **Next**.

4. Choose **TCP** > Select **Specific local ports** and enter: 23 > Click **Next**.

5. Select **Block the connection** > Click **Next**.

6. Check all three profiles (Domain, Private, Public) > Click **Next**.

7. Name it something like Block Telnet Port 23 > Click **Finish**.
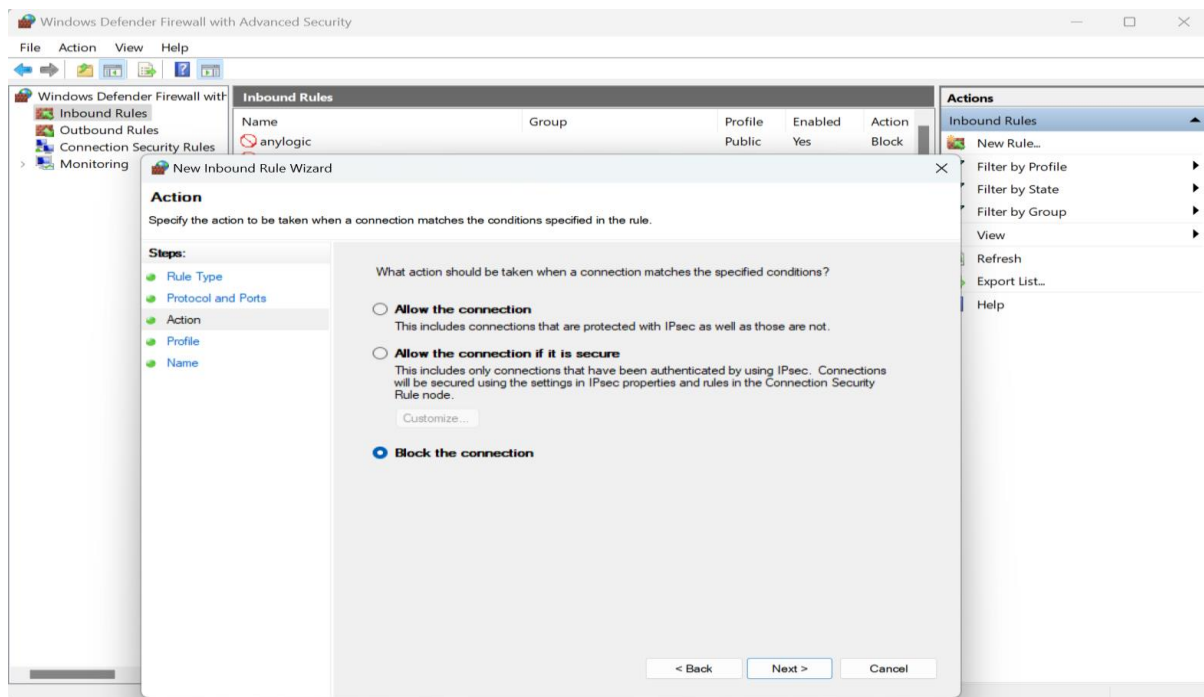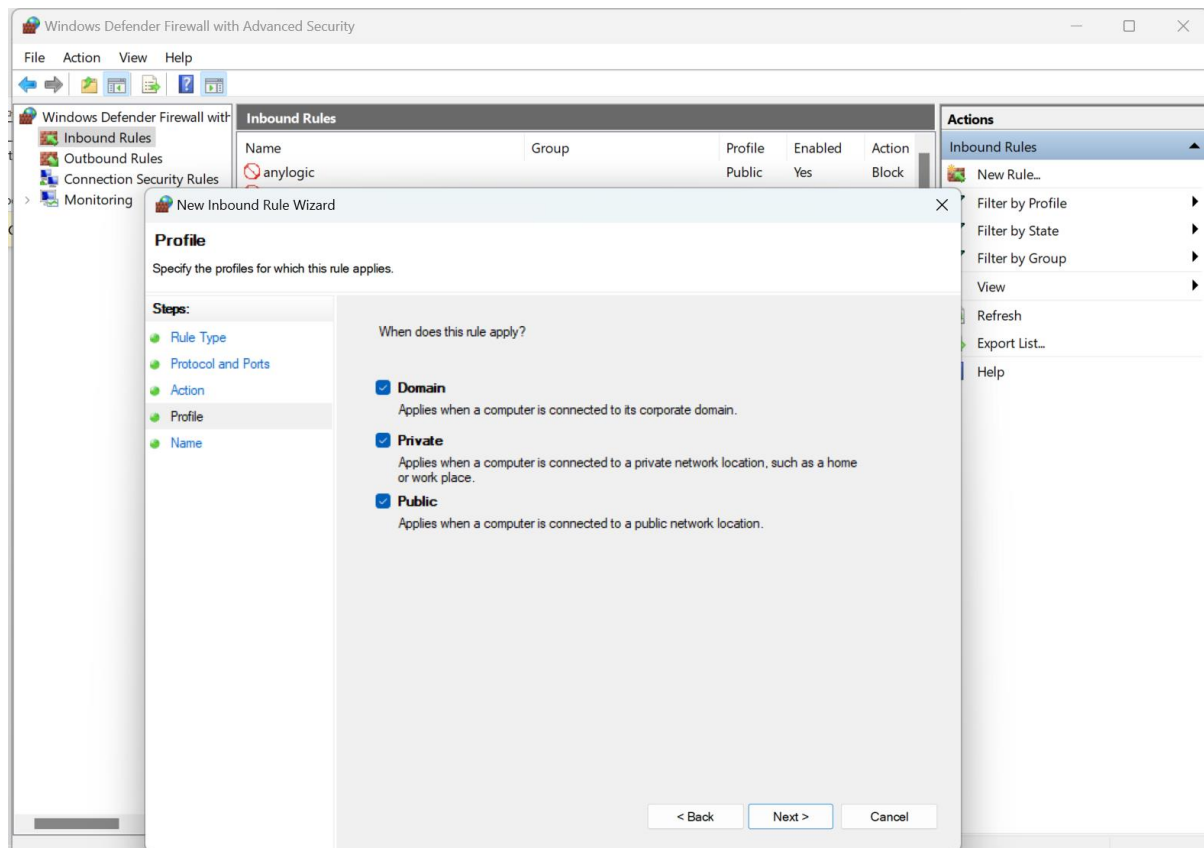
3. Select **Port** > Click **Next**.
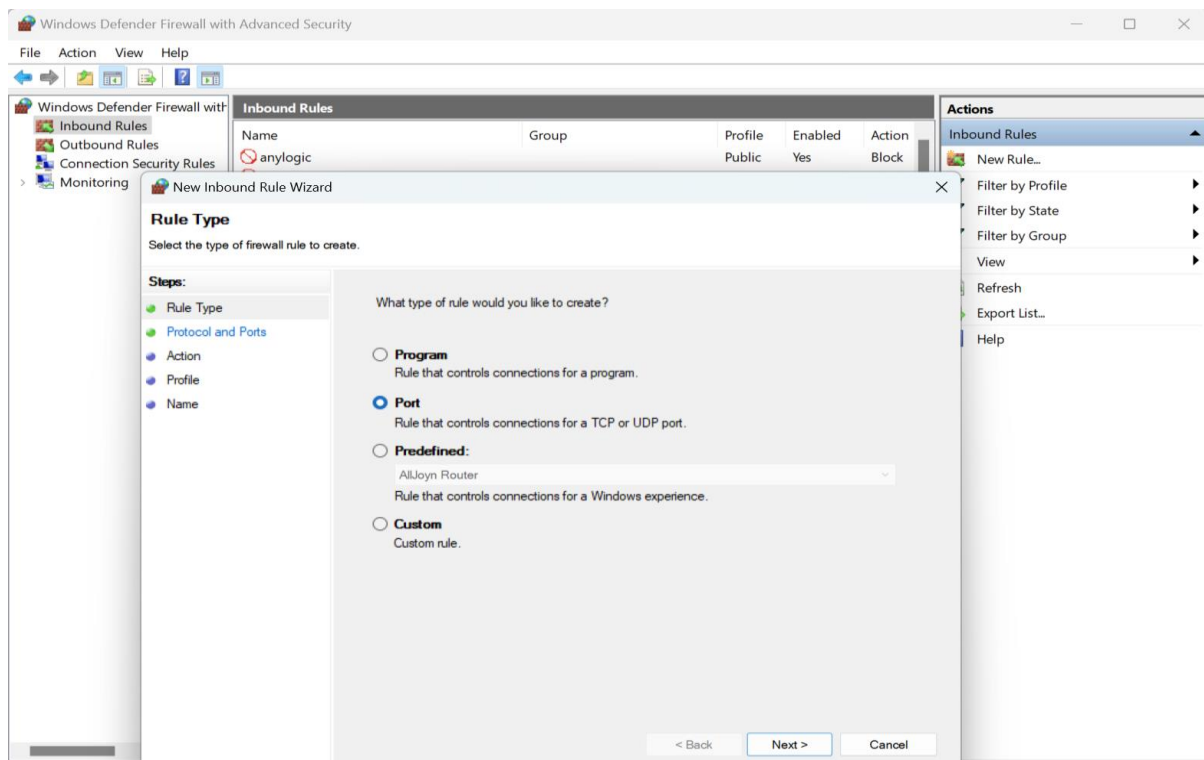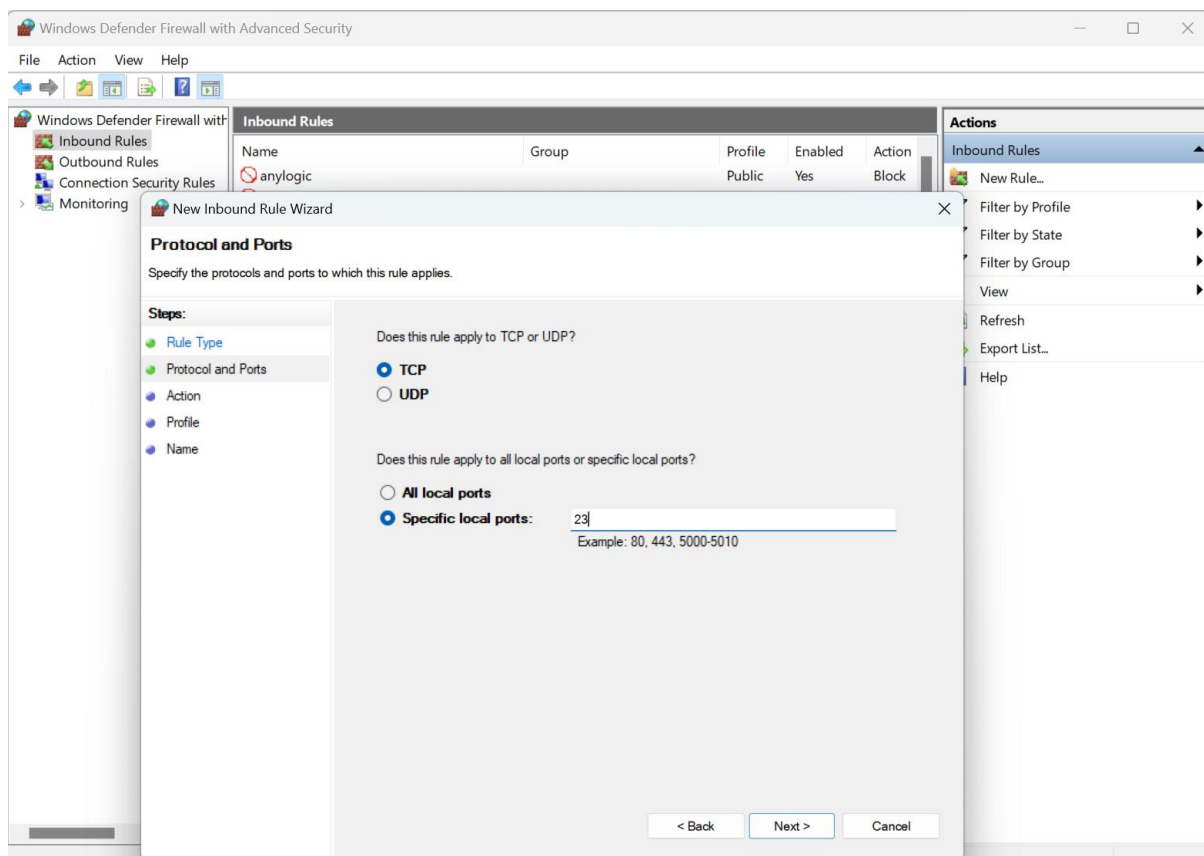
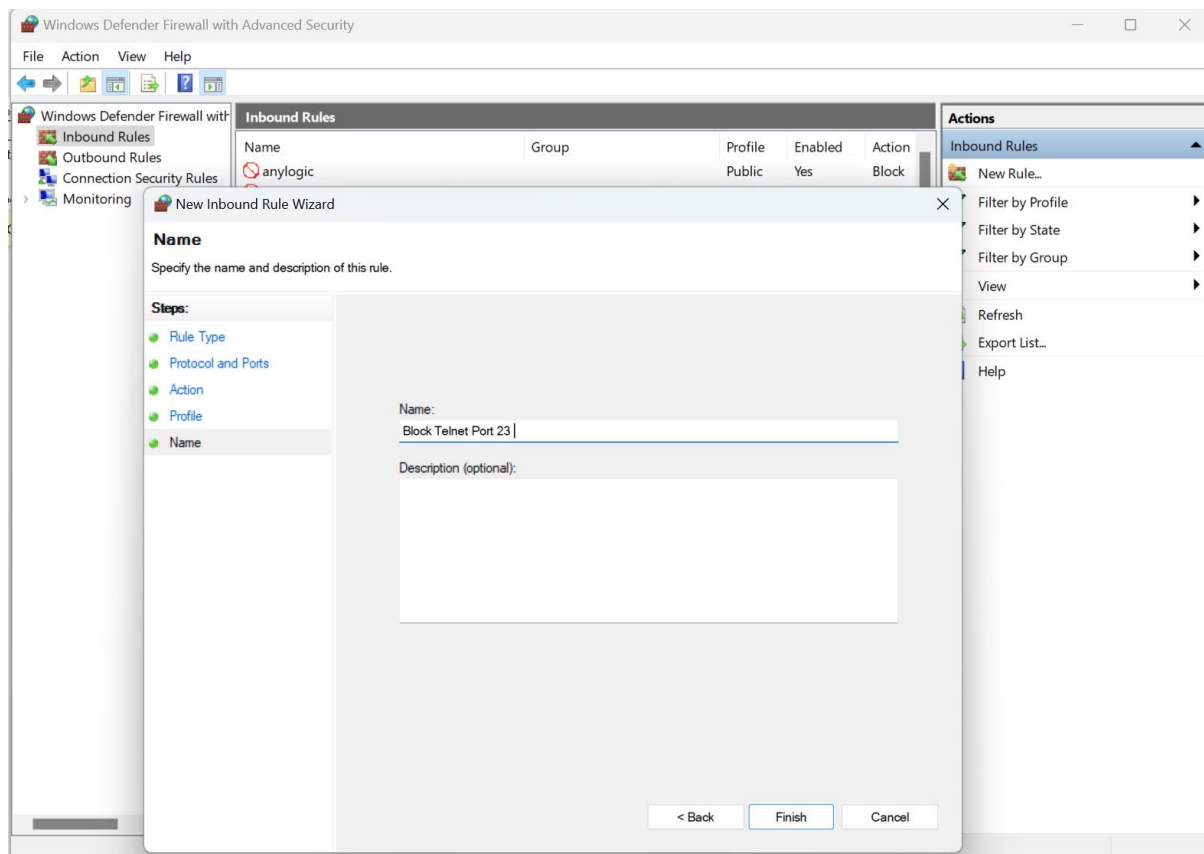4. Choose **TCP** > Select **Specific local ports** and enter: 23 > Click **Next**.

5.   Select **Block the connection** > Click **Next**.

6.   Check all three profiles (Domain, Private, Public) > Click **Next**.

7. Name it something like Block Telnet Port 23 > Click **Finish**.

Step 4: Test the Rule

- Use **Telnet** to test if the port is blocked (optional):

  1. Enable Telnet:

     - Open PowerShell or CMD as Admin.

     - Run: dism /online /Enable-Feature /FeatureName:TelnetClient

  2. Try: telnet localhost 23

  3. It should **fail to connect**.

     - Open PowerShell or CMD as Admin.

- Run: dism /online /Enable-Feature /FeatureName:TelnetClient

Step 6: Remove the Test Rule

1. Go back to **Inbound Rules**.

2. Find the rule named Block Telnet Port 23.

3. Right-click > **Delete** or **Disable**.