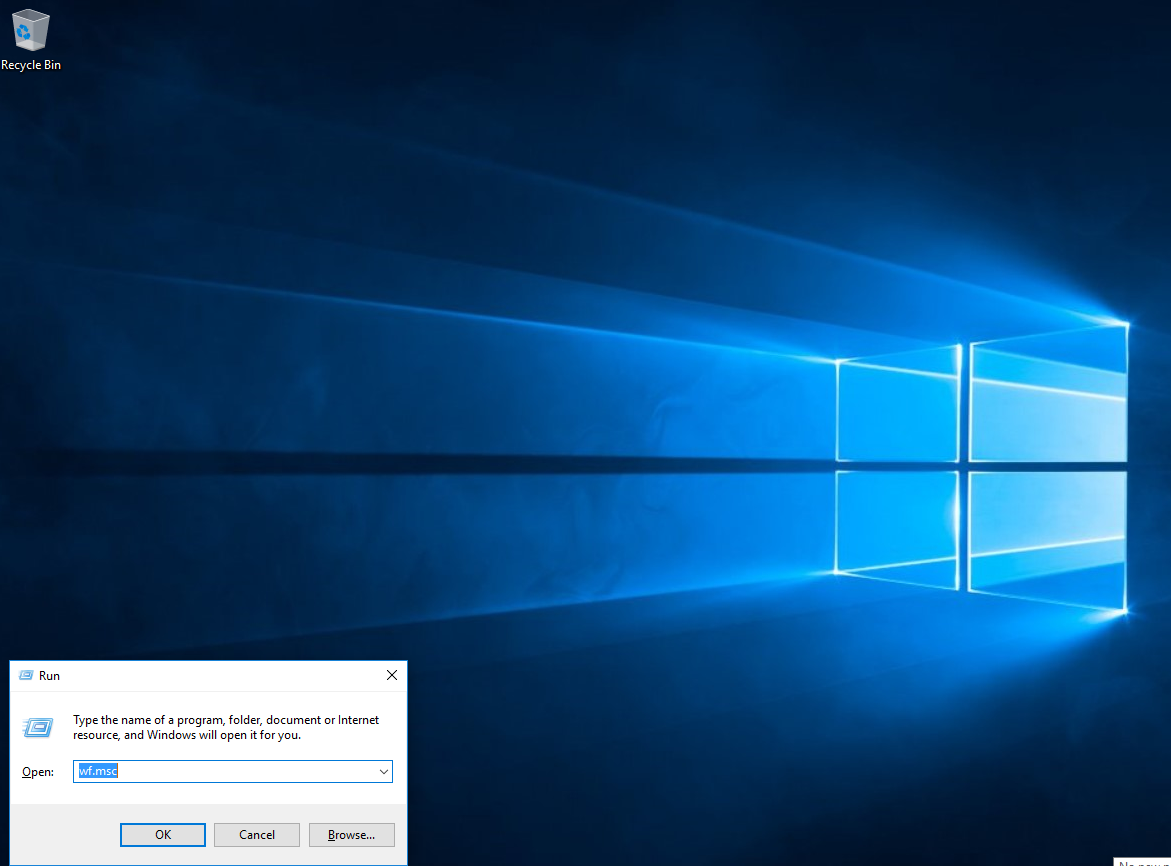
**🔒 Task 4: Configure and Use Windows Firewall to Filter Traffic**

**🎯 Objective:**

To understand and demonstrate the configuration of inbound firewall rules in Windows, specifically to **block Telnet (port 23)** and **allow SSH (port 22)** traffic using Windows Defender Firewall with Advanced Security.

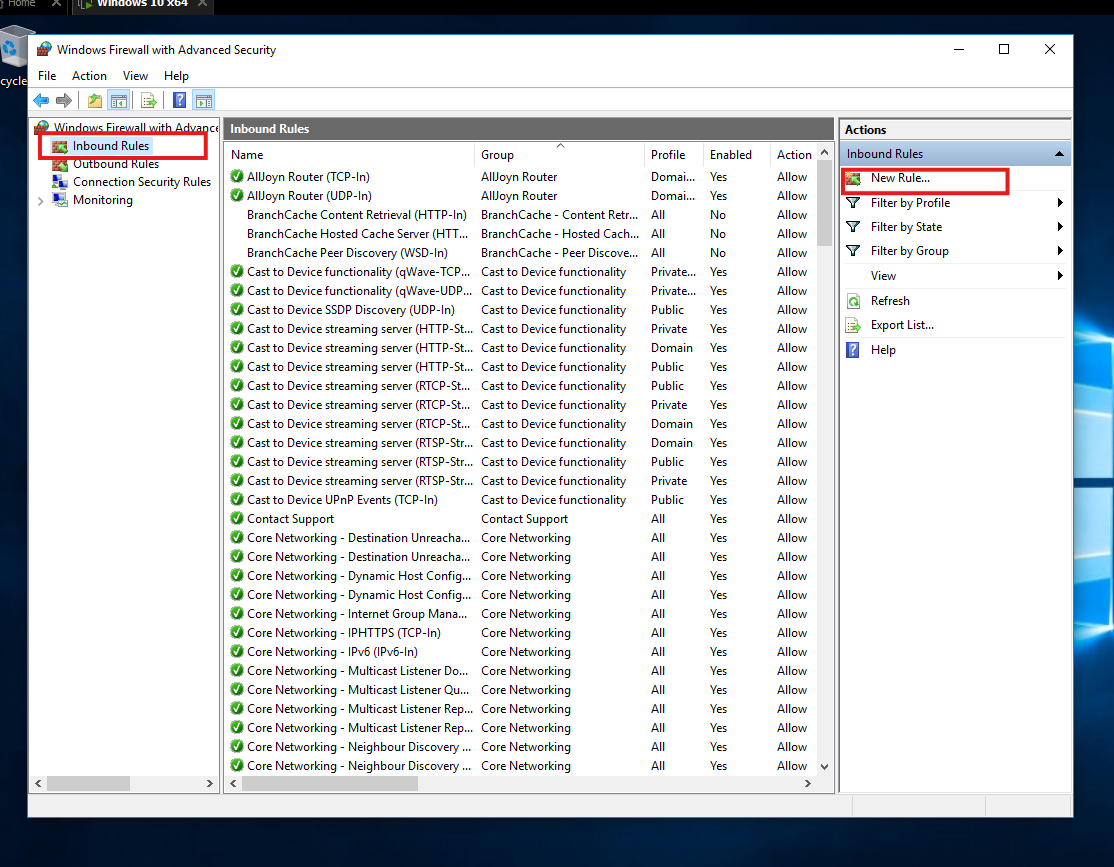
**📷 Step-by-Step Process with Screenshots & Descriptions**

**✅ Step 1: Open Windows Firewall Configuration Tool**



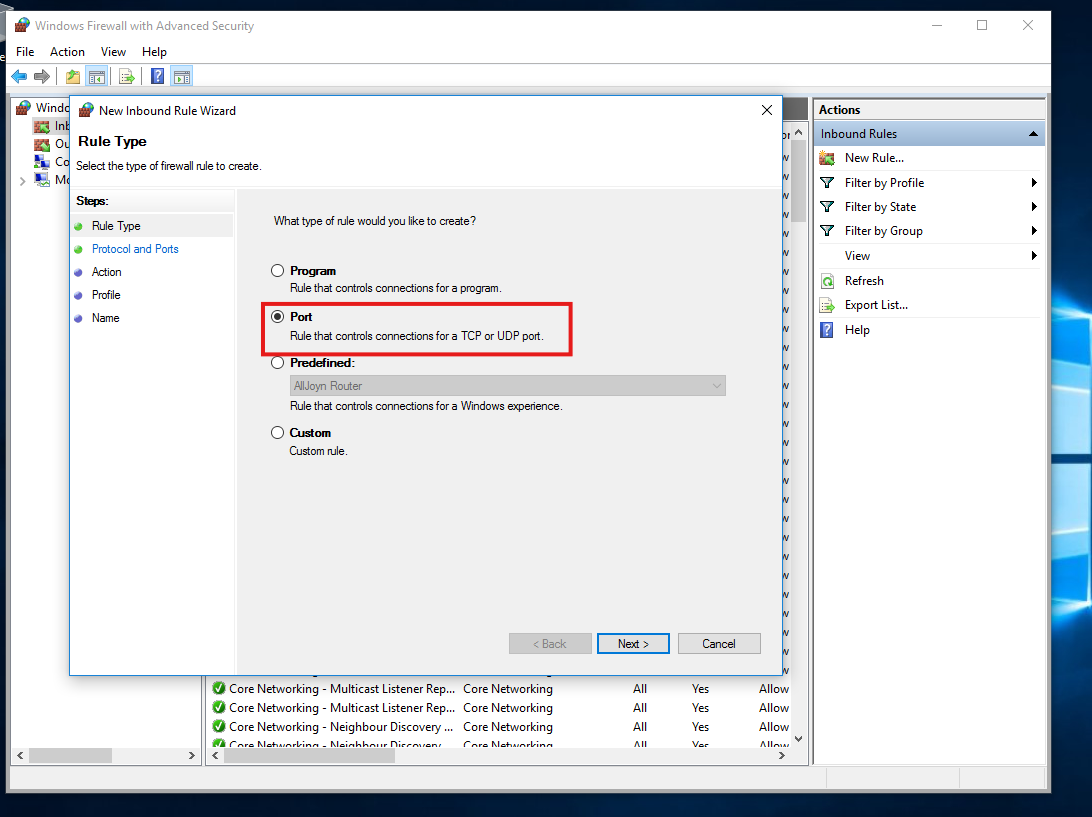
* Press Win + R, then type wf.msc in the **Run** dialog box to launch **Windows Defender Firewall with Advanced Security**.
* This is the management console used for advanced firewall configuration.

**✅ Step 2: Navigate to Inbound Rules and Create a New Rule**



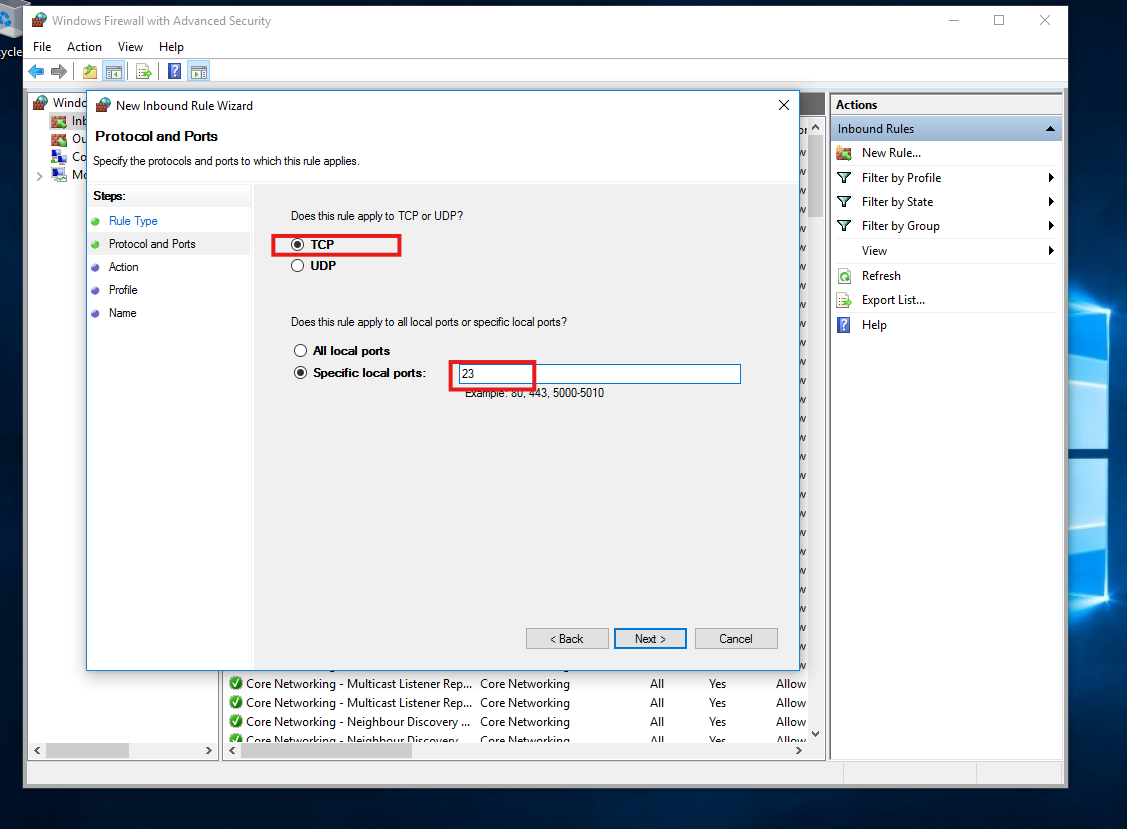
* On the left sidebar, select **Inbound Rules** to manage traffic coming into your system.
* Click **New Rule** on the right-hand side to begin creating a custom firewall rule.

**✅ Step 3: Choose Rule Type – Port**



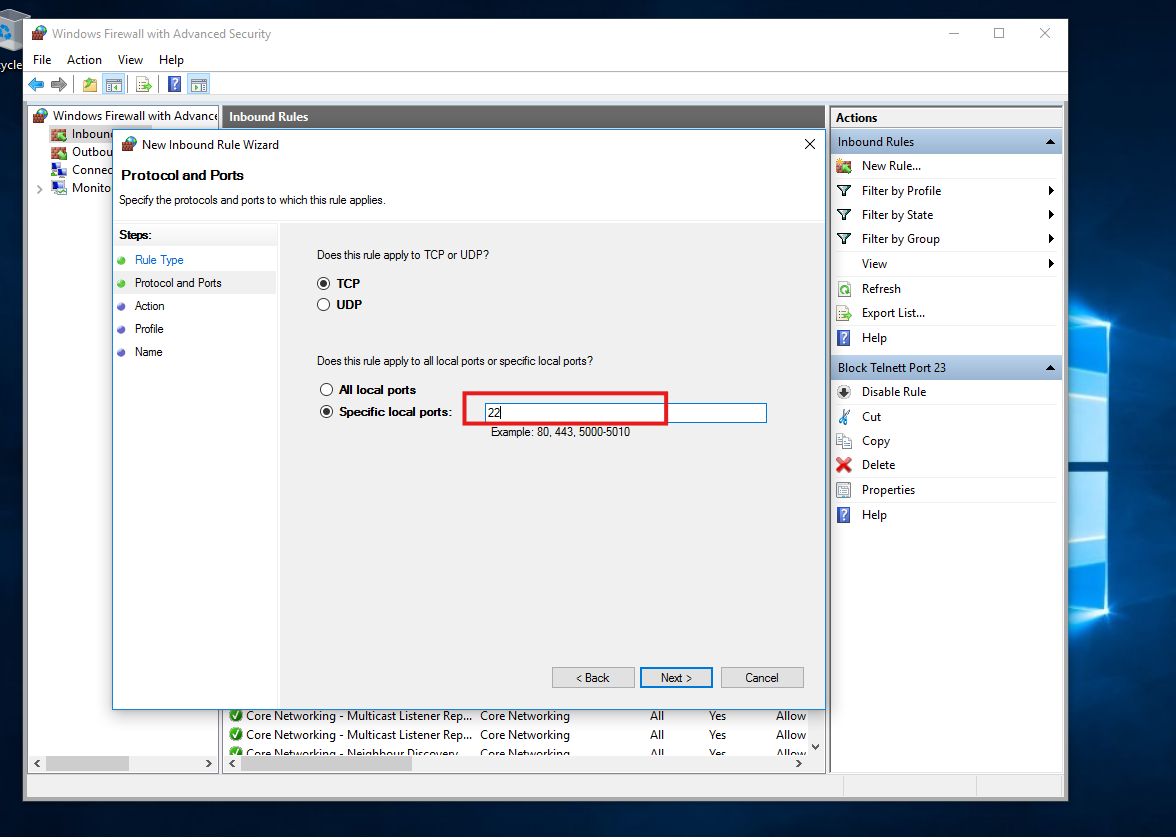
* In the **New Inbound Rule Wizard**, select **Port** (to control traffic based on TCP or UDP ports).
* This allows us to filter specific service ports like Telnet (23) or SSH (22).

**✅ Step 4: Define the Port to Block (Telnet – Port 23)**



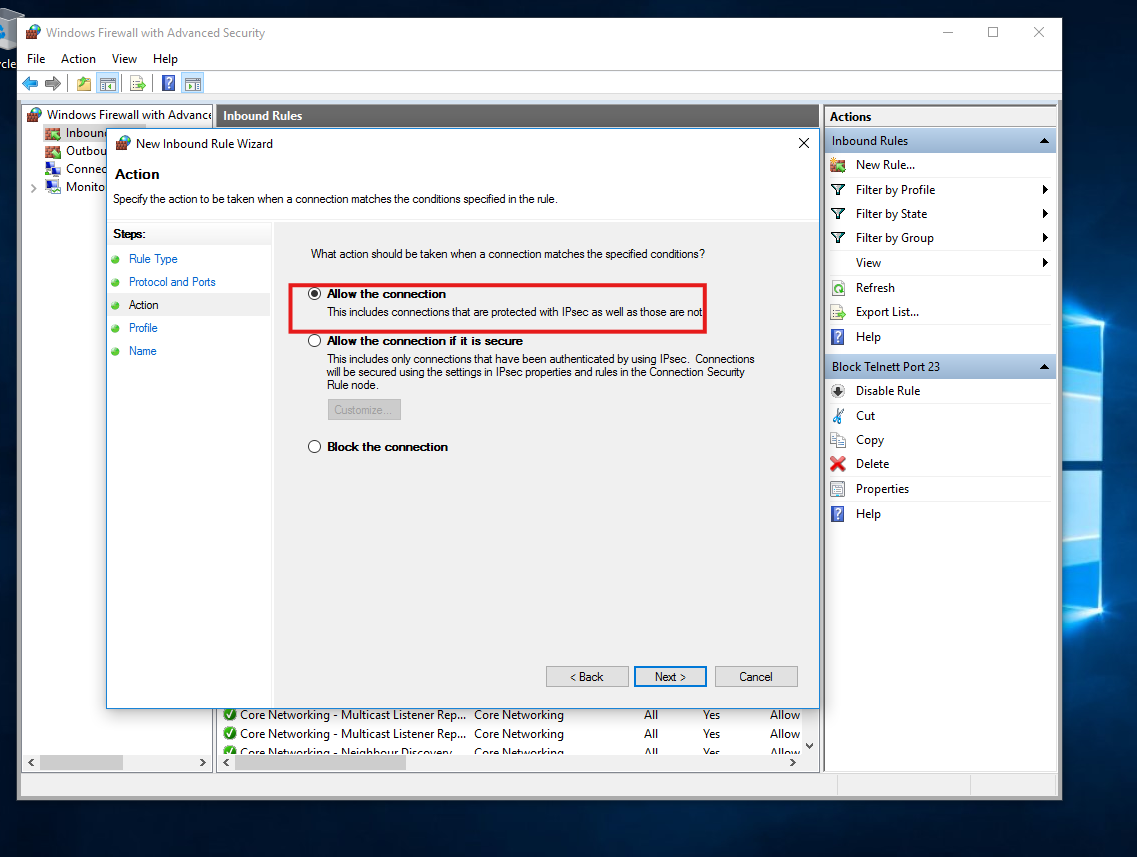
* Choose **TCP**, then enter port number **23** under **Specific local ports**.
* Telnet is an old protocol often disabled for security reasons, making it a good candidate for testing firewall rules.

**✅ Step 5: Create Another Rule to Allow Port 22 (SSH)**



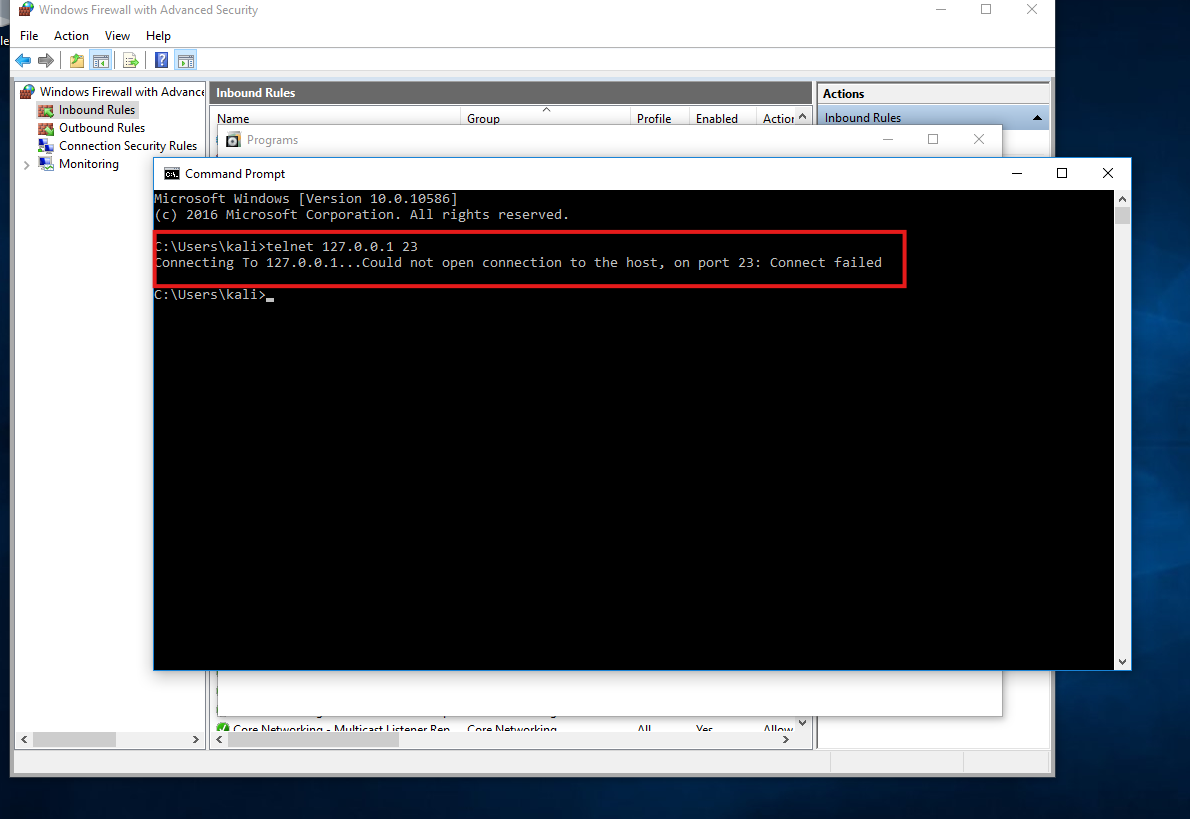
* You repeated the same process to allow **TCP traffic on port 22**, which is used for **SSH** access.
* This demonstrates fine-grained control over which services are allowed through the firewall.

**✅ Step 6: Specify the Rule Action – Allow or Block**



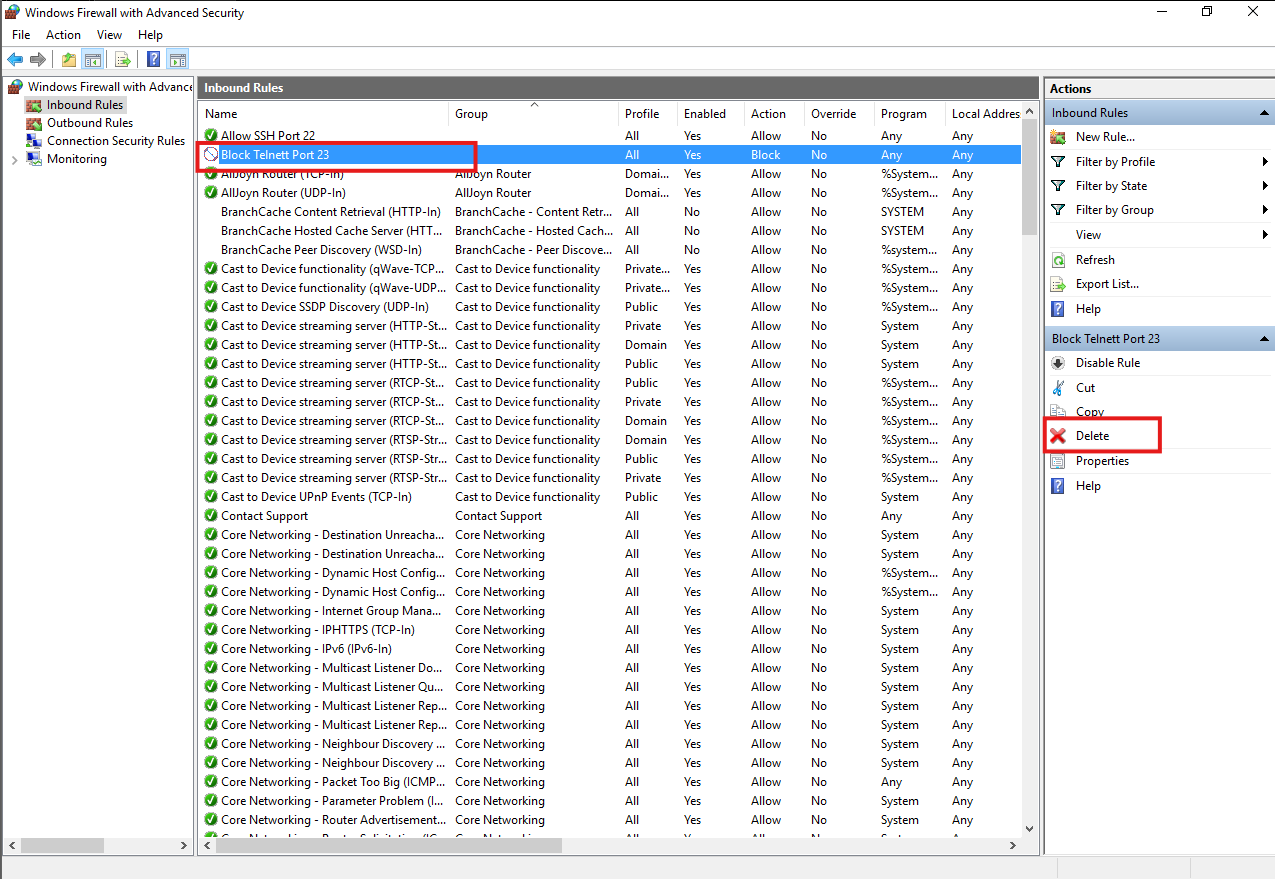
* For port **22**, you selected **“Allow the connection”** to ensure SSH traffic is permitted.
* For port **23**, you previously selected **“Block the connection”**, which prevents Telnet communication.

**✅ Step 7: Test the Rule – Blocked Telnet Connection**



* You used the **Telnet command** to test if port 23 is accessible.
* The error Could not open connection to the host, on port 23: Connect failed confirms that the firewall successfully blocked the traffic.

**✅ Step 8: Remove the Test Rule to Restore Defaults**



* Finally, you deleted the test rule for **port 23** by selecting the rule in Inbound Rules and clicking **Delete**.
* This ensures your system returns to its original network state.

**📘 Conclusion:**

This task provided hands-on experience in managing **Windows Firewall rules** to control network traffic:

* ✅ Created port-specific inbound rules
* ✅ Successfully blocked and tested a Telnet port
* ✅ Allowed secure SSH port access
* ✅ Understood the concept of protocol-based traffic filtering

**💡 Tools Used:**

* wf.msc (Windows Defender Firewall)
* Telnet Client (telnet 127.0.0.1 23)
* Command Prompt & GUI firewall interface