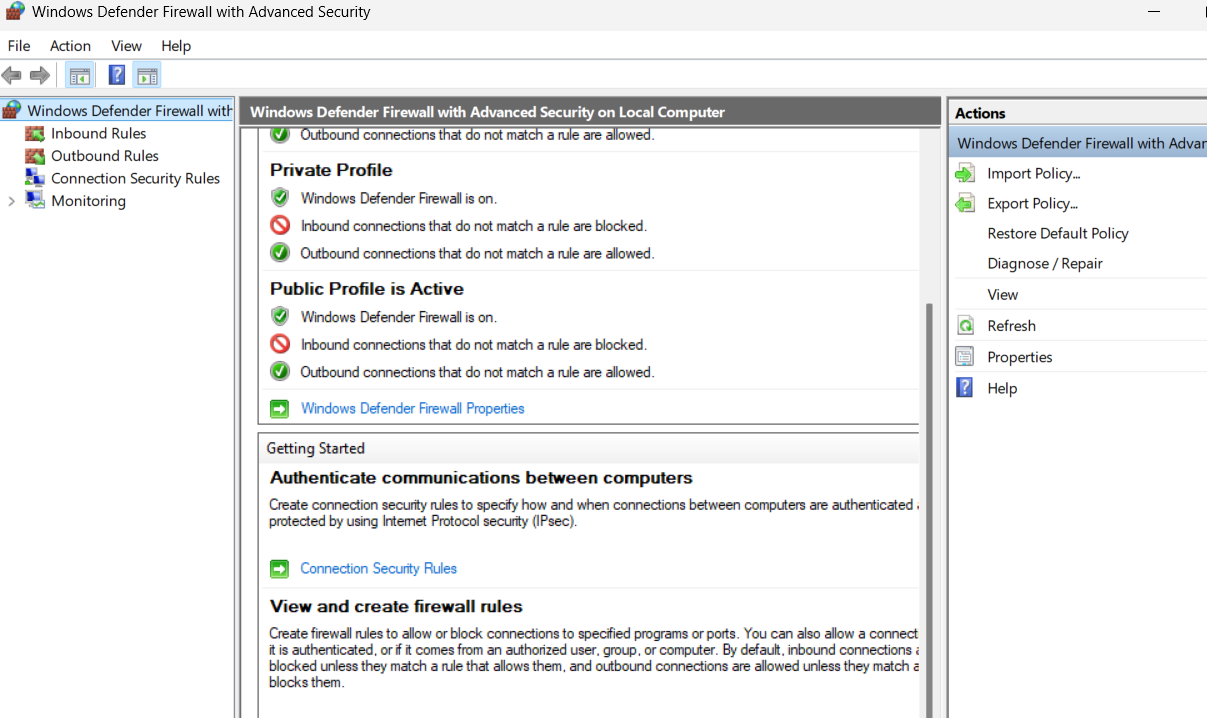
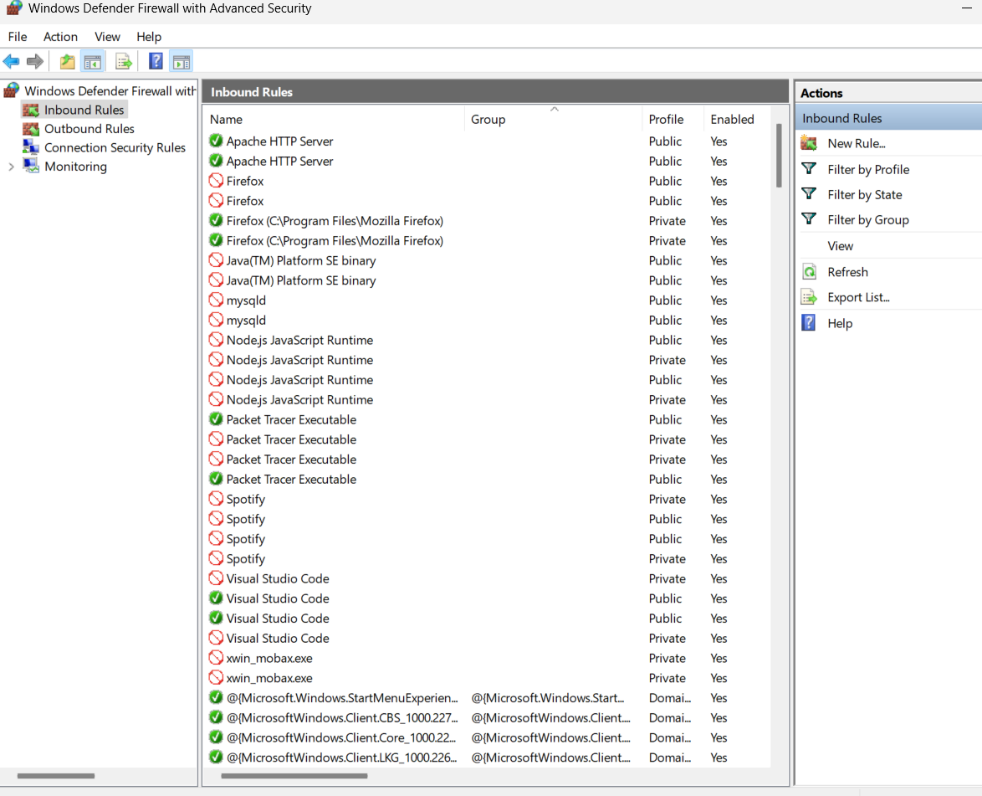
**🔹 Windows Firewall (GUI)**

### **1. Open Firewall Configuration Tool**

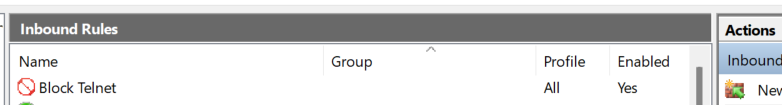
* Press Win + R, type wf.msc, press Enter.
* This opens **Windows Defender Firewall with Advanced Security**.

### **2. List Current Firewall Rules**

* Click **Inbound Rules** on the left panel to view current rules.

### **🡺Add a Rule to Block Inbound Traffic on Port 23 (Telnet)**

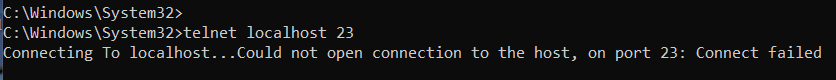
* In right pane, click **New Rule...**
* Select **Port** → Click **Next**.
* Choose **TCP** and enter **23** in Specific local ports → Next.
* Select **Block the connection** → Next.
* Keep all profiles checked (Domain, Private, Public) → Next.
* Name the rule (e.g., Block Telnet) → Finish.



### **4. Test the Rule**

* Open Command Prompt.
* Enable Telnet client if needed (Control Panel → Programs → Turn Windows features on or off → Telnet Client).
* Run:

telnet localhost 23



### **6. Remove the Test Block Rule**

* In **Inbound Rules**, find your Block Telnet rule.
* Right-click → **Delete**.

### **7. Documentation of Windows GUI Steps**

* Open wf.msc
* View Inbound Rules
* Create new port block rule (TCP 23)
* Test connection with Telnet
* Delete the rule after testing

**8. Summary: How Firewalls Filter Traffic**

* Firewalls check incoming and outgoing traffic using rules.
* They inspect each packet based on IP, port, and protocol.
* If a packet matches a block rule, it gets dropped or rejected.
* If it matches an allow rule, it goes through to the application.
* Firewalls work at different levels like network, transport, and application.
* This helps protect systems from attacks, malware, and unauthorized access by only allowing safe connections.