Objective: Configure and test basic firewall rules to allow or block traffic.

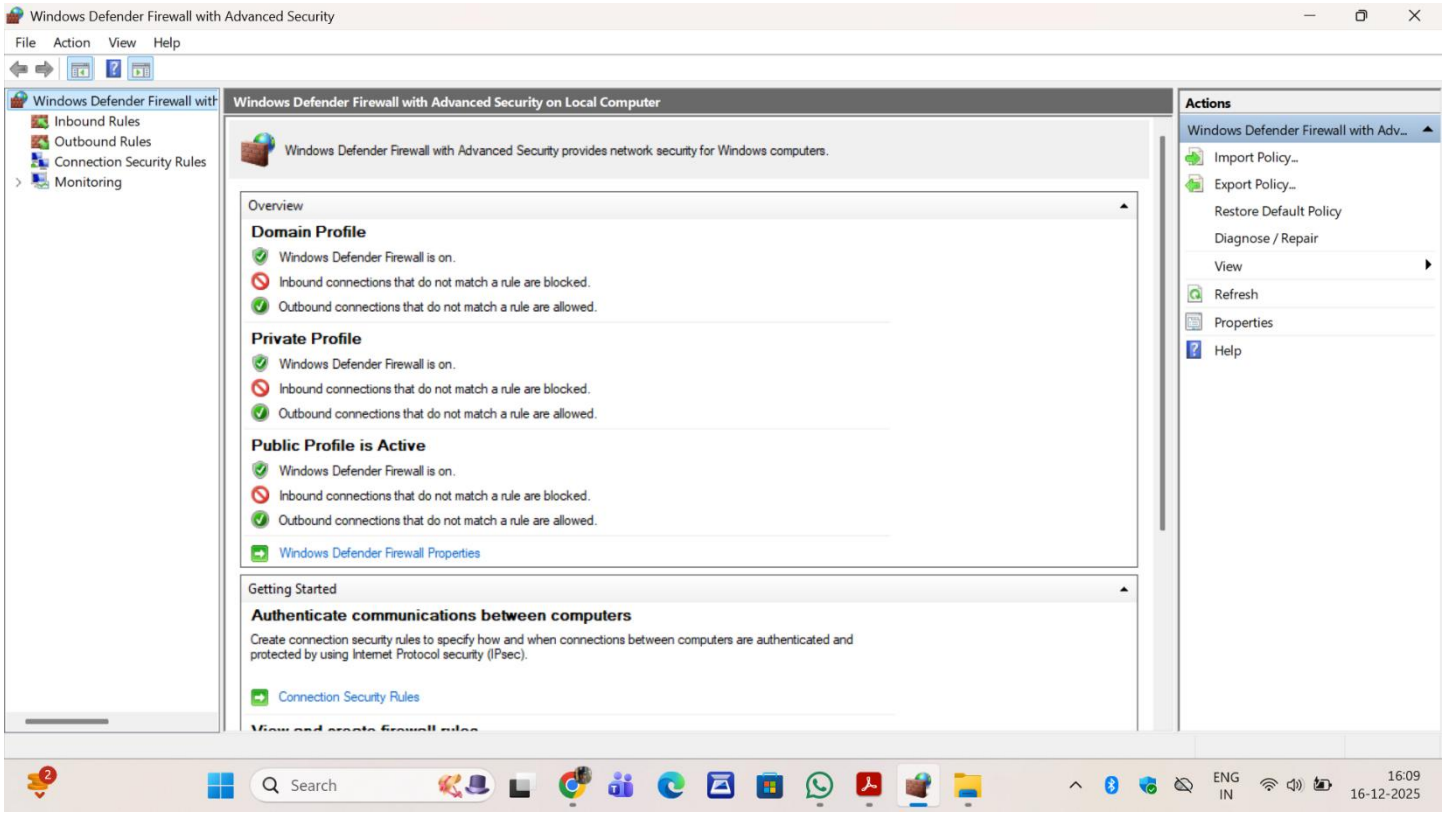
Tools: Windows Firewall

Deliverables: Screenshot/configuration file showing firewall rules applied.

a. Open firewall configuration tool (Windows Firewall or terminal for UFW).

Open Firewall Tool

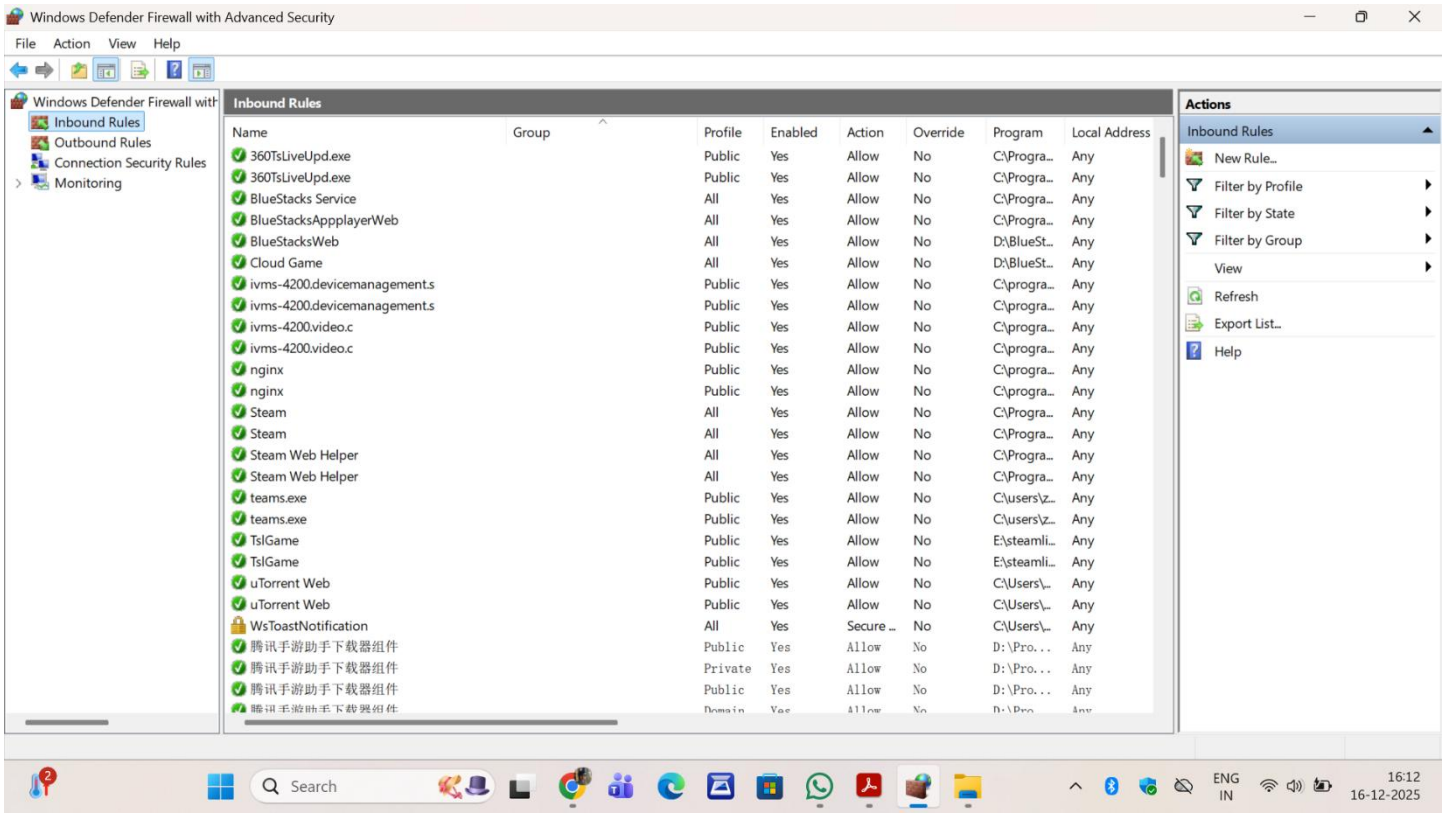
- Press **Win + R**
- Type wf.msc → **Enter**



b. List current firewall rules.

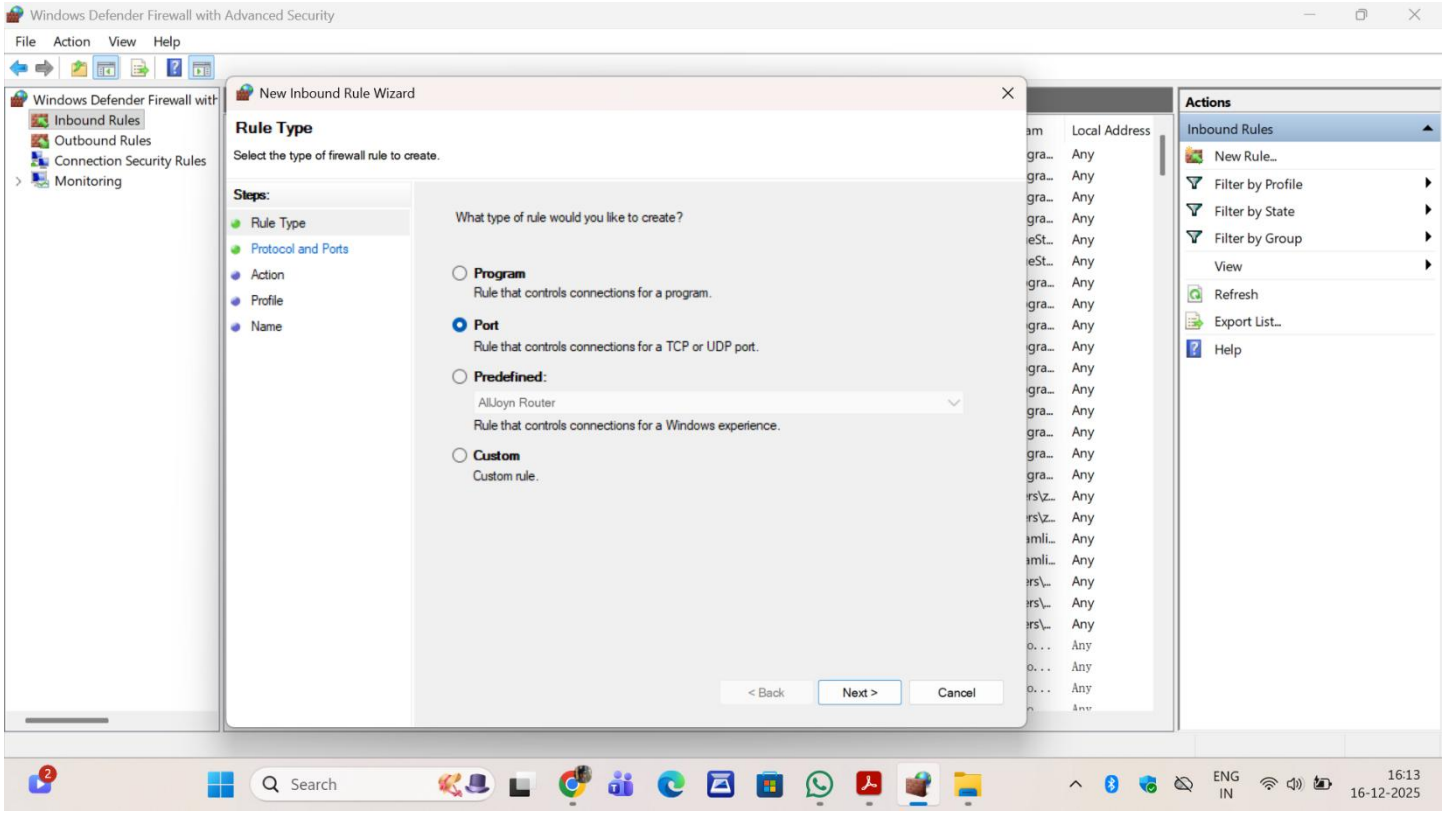
List Current Rules

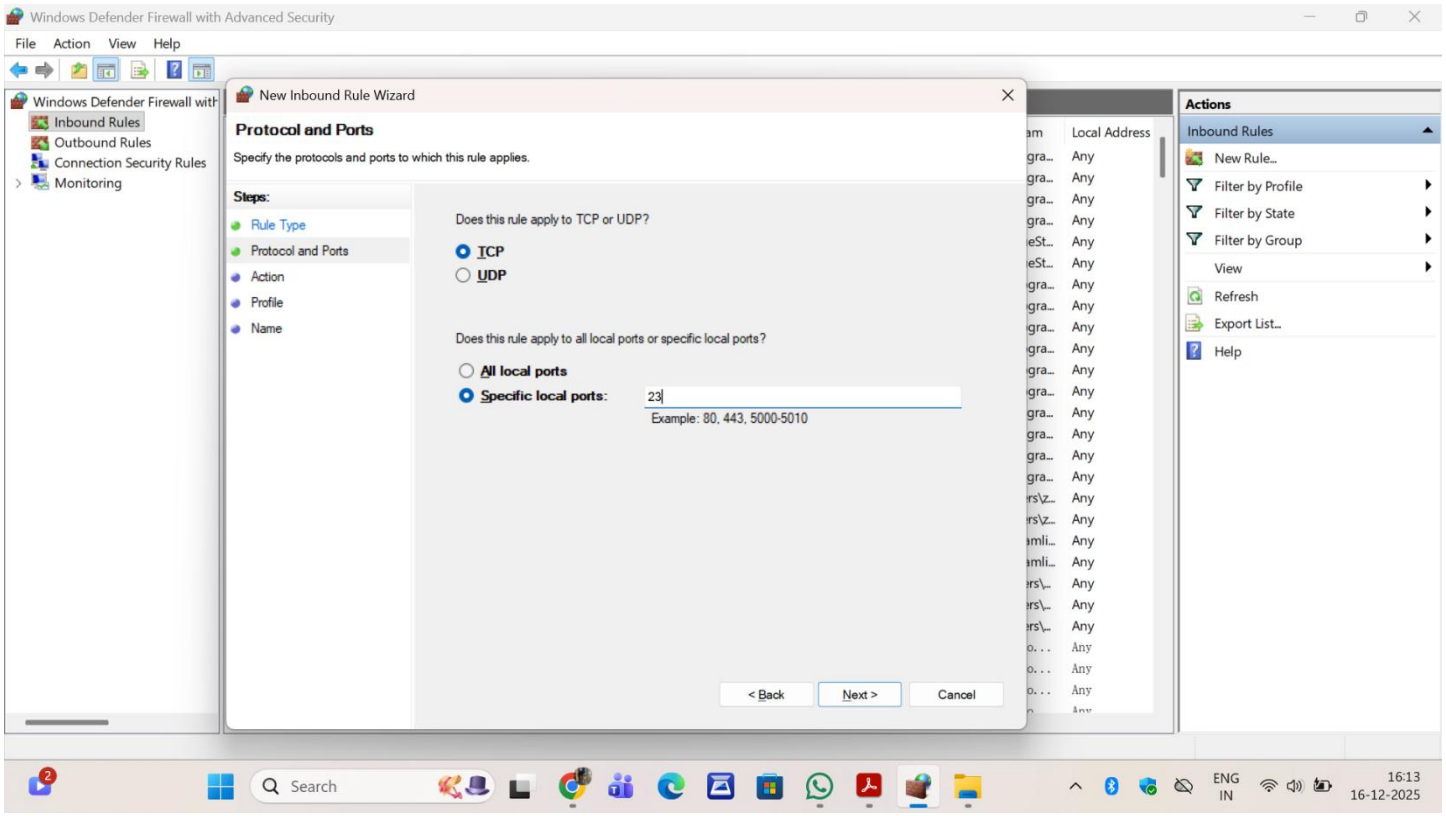
- **Click Inbound Rules**
- **Existing rules are displayed**

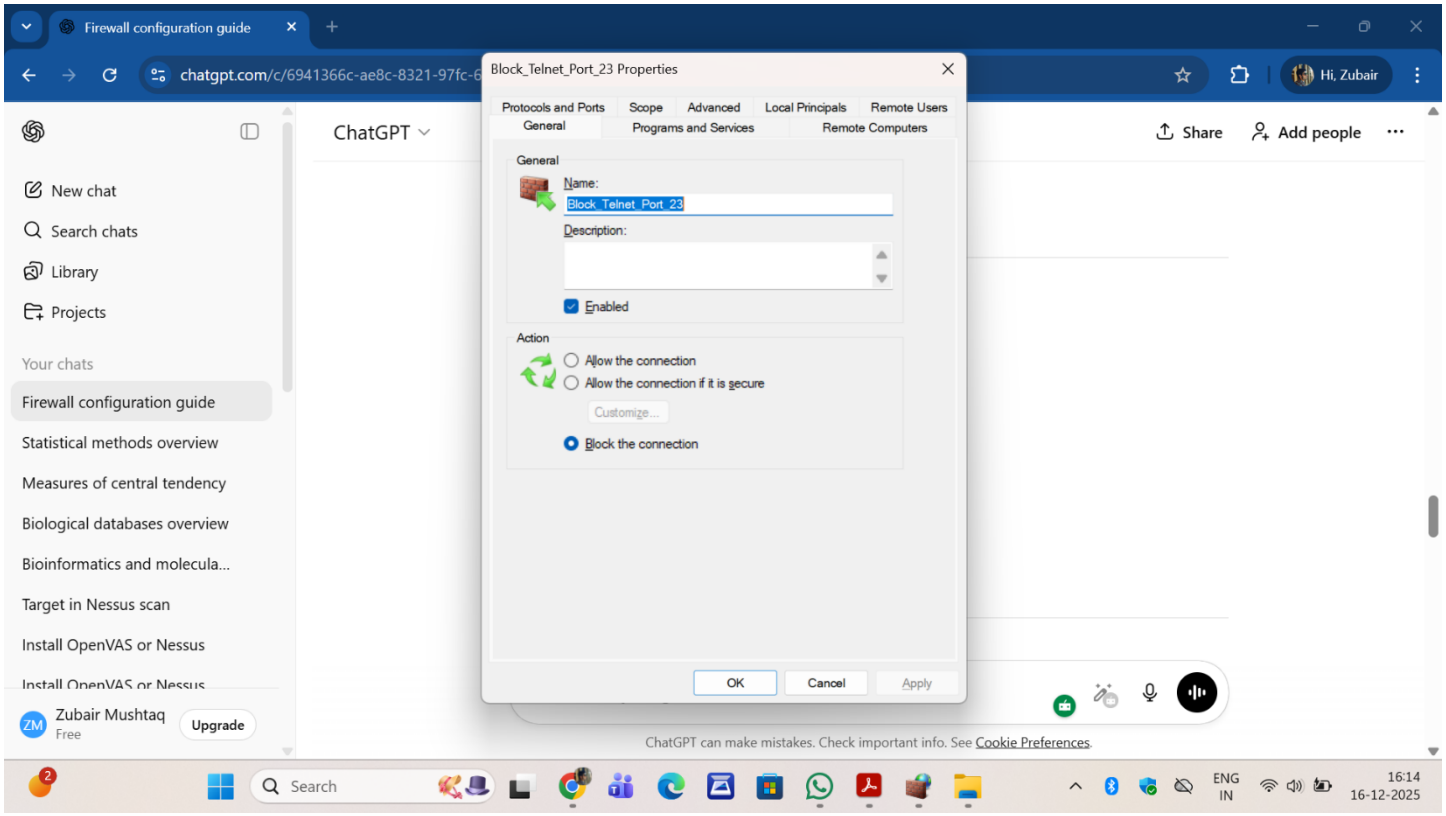


c. Add a rule to block inbound traffic on a specific port (e.g., 23 for Telnet).

1. **Inbound Rules → New Rule**
2. Select **Port**
3. Select **TCP** → Port **23**
4. Choose **Block the connection**
5. Apply to all profiles
6. Name rule: `Block_Telnet_Port_23`
7. Click **Finish**





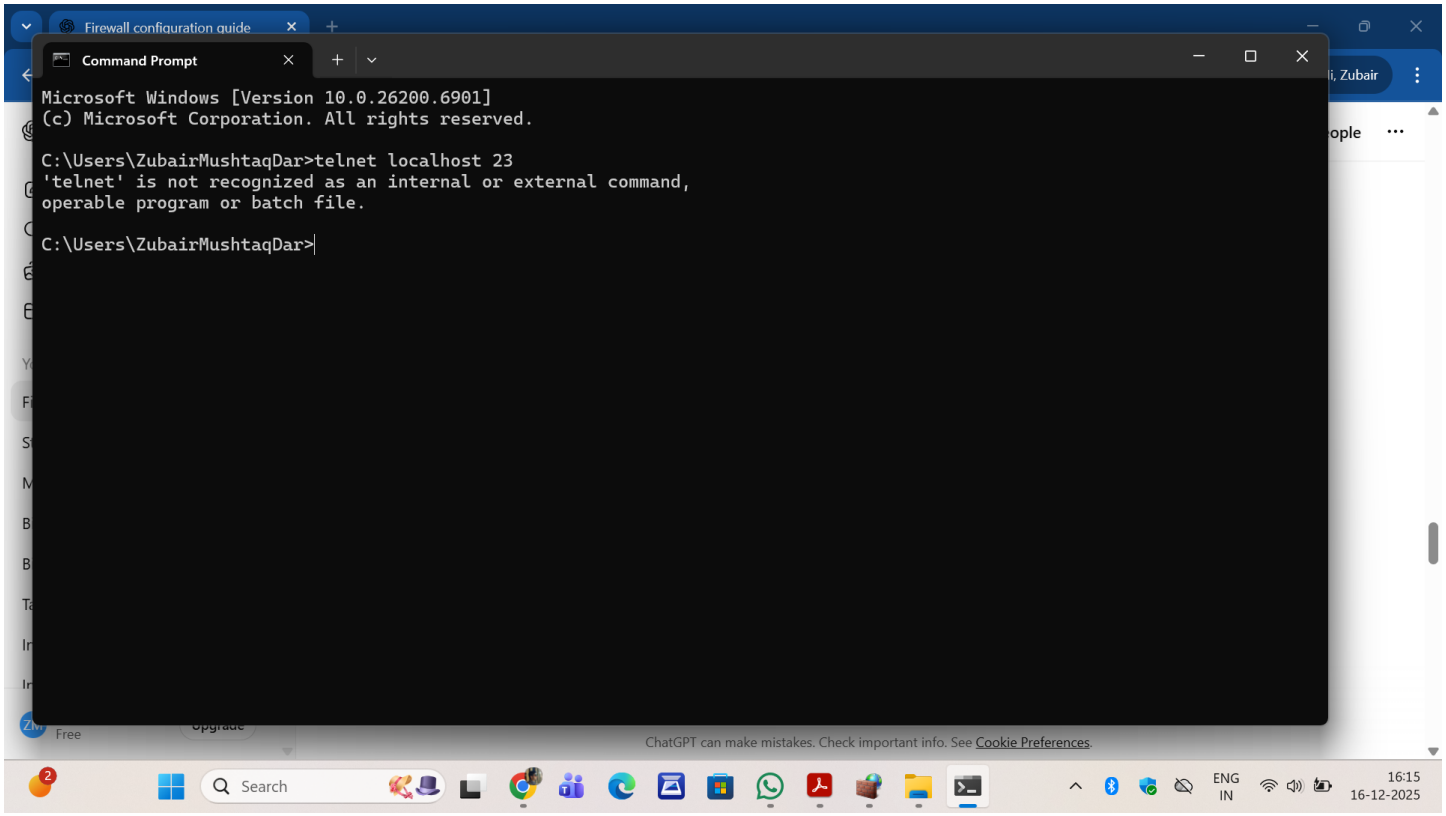


d. Test the rule by attempting to connect to that port locally or remotely.

Open Command Prompt:

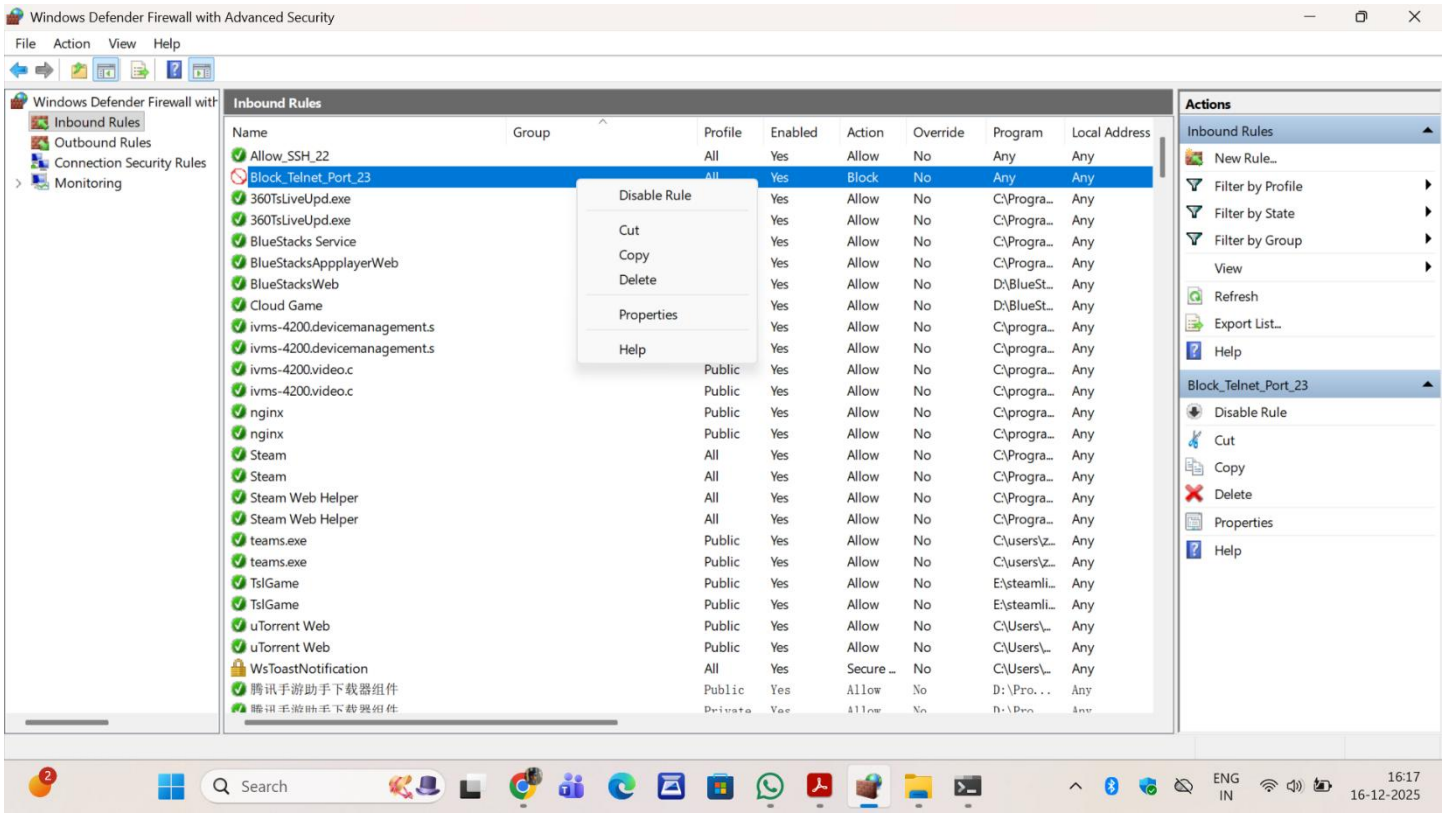
telnet localhost 23

Connection should **fail**



e. Remove the test block rule to restore original state.

1. Open **Run → wf.msc**
2. Click **Inbound Rules**
3. Locate the rule **Block_Telnet_Port_23**
4. Right-click the rule → **Delete**
5. Confirm deletion



f. Summarize how firewall filters traffic.

A firewall filters network traffic by applying predefined rules that allow or block data packets based on port numbers, protocols, IP addresses, and direction of traffic. This helps prevent unauthorized access while permitting legitimate communication.