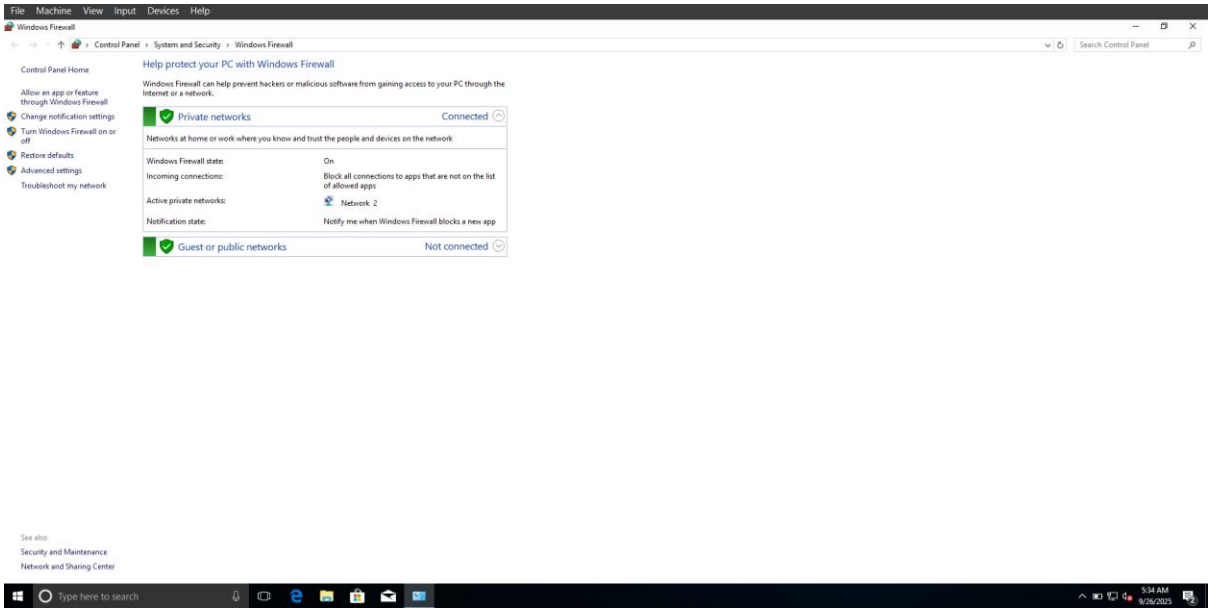
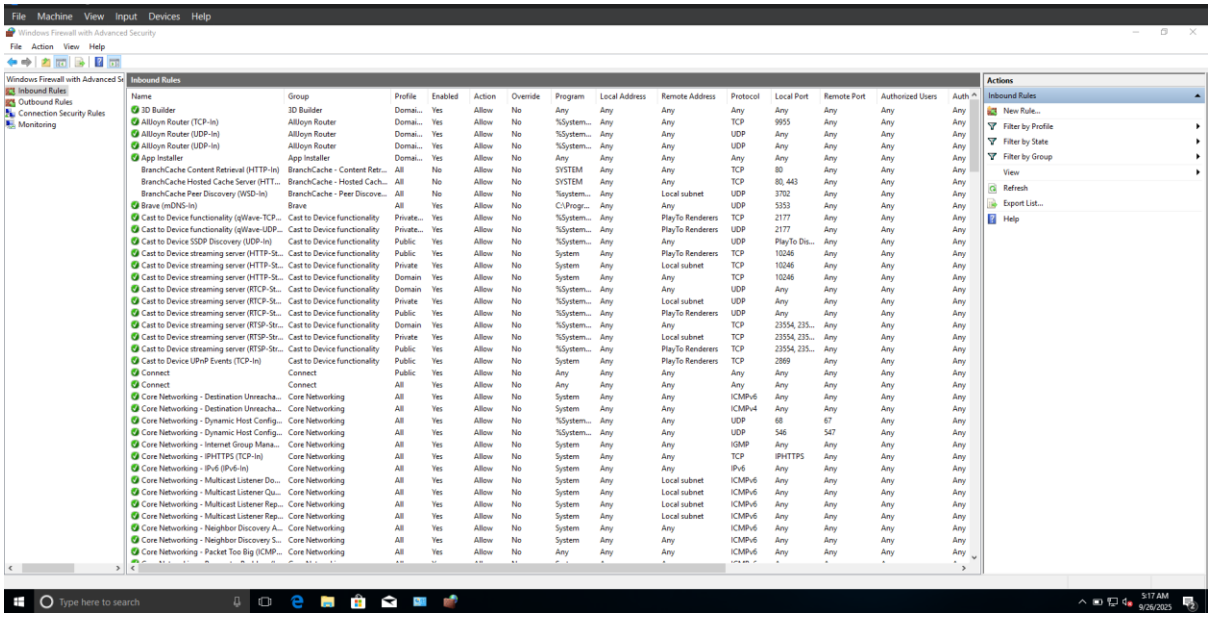
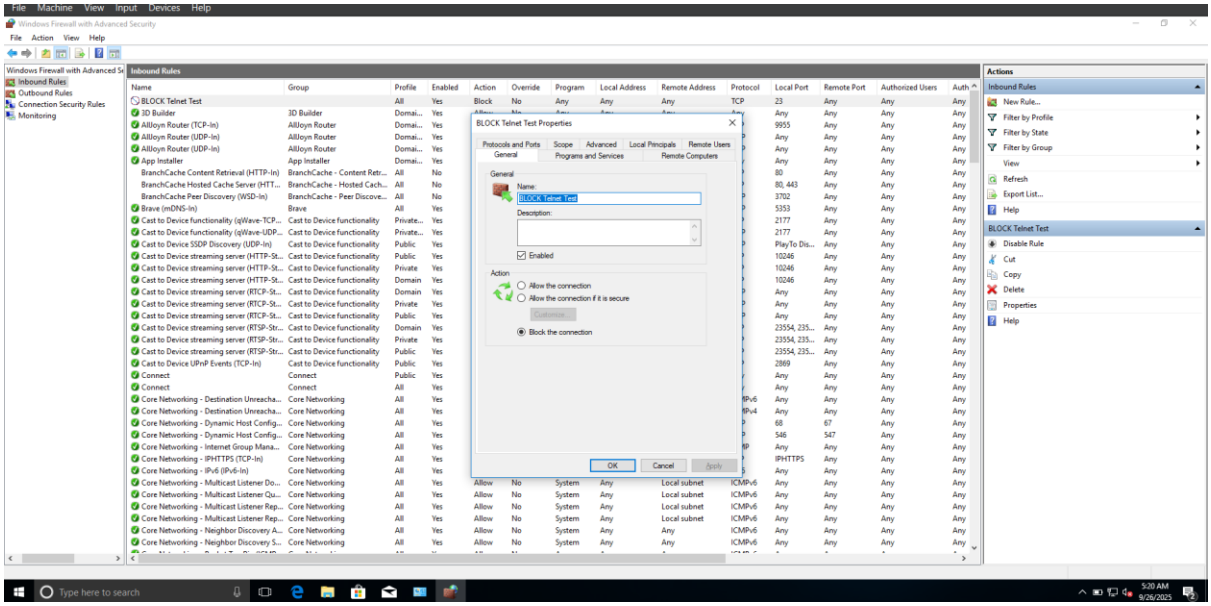
1.Open firewall configuration tool (Windows Firewall or terminal for UFW).



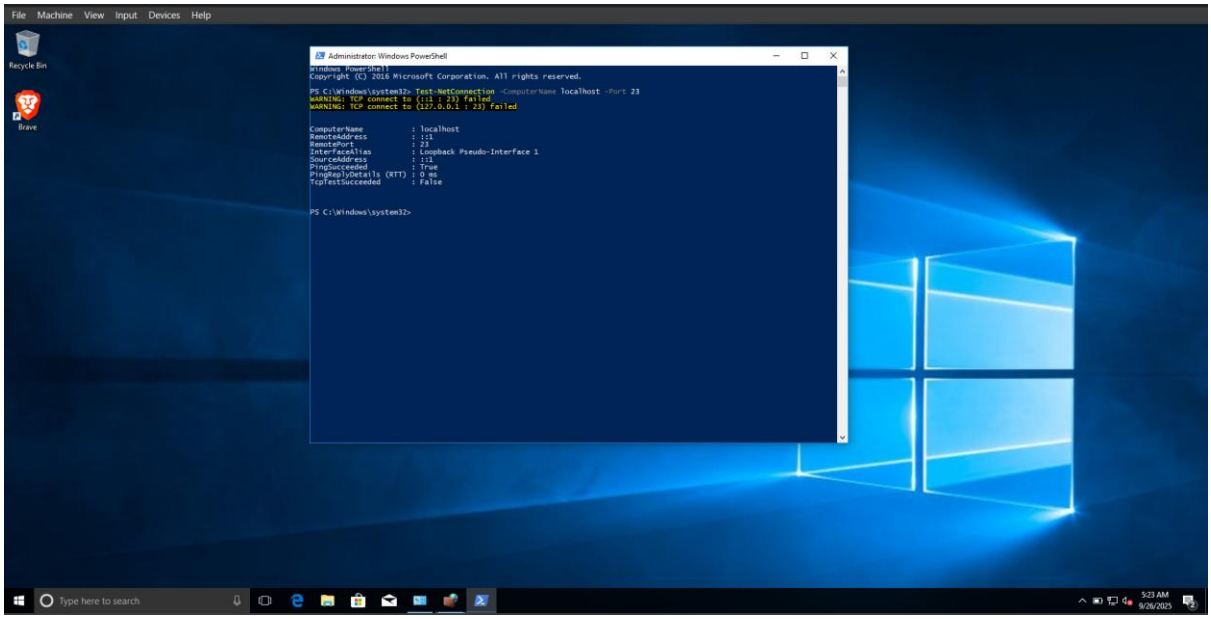
2.List current firewall rules.



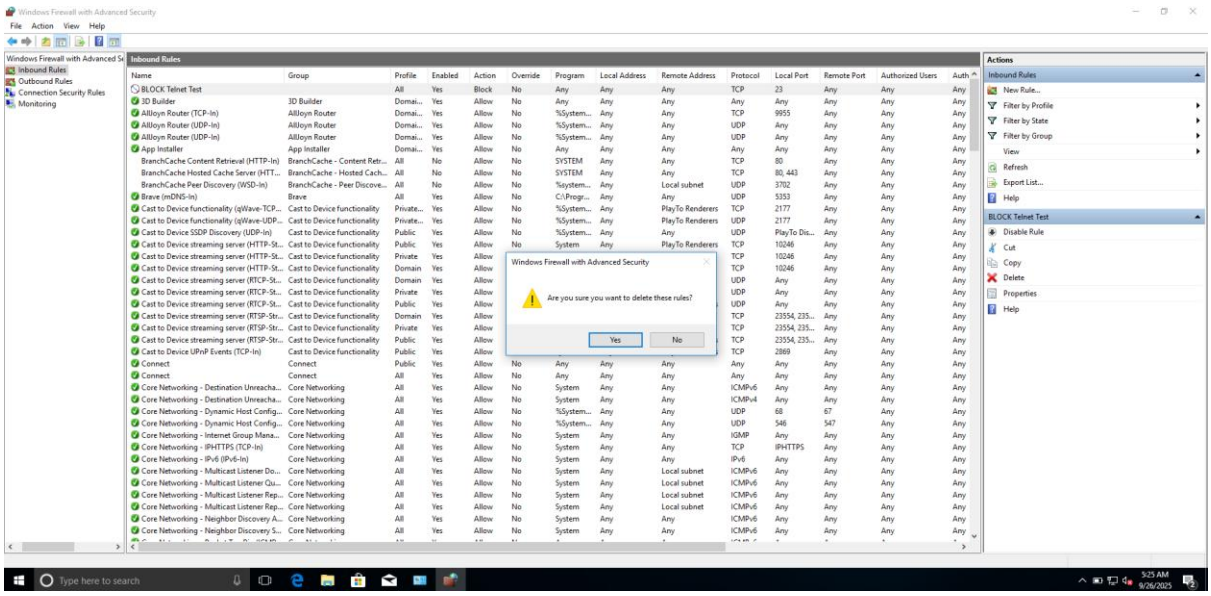
3.Add a rule to block inbound traffic on a specific port (e.g., 23 for Telnet).



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



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



7.Document commands or GUI steps used.

- **Process of creating a new firewall rule**
  1. In the right pane, click **"New Rule..."**2. Select **"Port"** and click **"Next"**.3. Select **"TCP"** and enter **"23"** for the specific local port. Click **"Next"**.4. Select **"Block the connection"**. Click **"Next"**.5. Ensure all profiles (Domain, Private, Public) are checked. Click **"Next"**.6. Give the rule a **Name** (e.g., "BLOCK Telnet Test") and click **"Finish"**.
- **Process of testing a new firewall rule**

Open another **PowerShell** window and run: `Test-NetConnection -ComputerName localhost -Port 23`

- **Deleting a new firewall rule**

1. In **"Inbound Rules"**, find the rule named **"BLOCK Telnet Test"**.2. Right-click the rule and select **"Delete"**.

8.Summarize how firewall filters traffic

- **Packet Arrival**: The firewall intercepts a data packet and extracts key information like its source/destination IP, protocol (e.g., TCP), and port numbers.
- **Stateful Inspection**: It first checks if the packet belongs to an **existing, approved connection**. If so, it allows the packet to pass immediately.
- **Rule-Based Evaluation**: If it's a new connection, the firewall compares the packet against its list of rules, starting from the top. It executes the **first rule that matches** the packet's criteria.
- **Action Taken**: The rule determines the action: **ALLOW** (the packet is forwarded), **DENY** (the packet is silently dropped), or **REJECT** (the packet is dropped, and an error is sent back).
- **Default Deny**: If the packet doesn't match any rule on the list, the firewall's **default policy** blocks the traffic. This "deny all" principle is a fundamental security measure.