Firewall Rule Implementation Report

Objective:

To block Telnet (port 23) using Windows Defender Firewall and verify that the traffic is being filtered.

Steps Performed:

1. Open Firewall Configuration Tool
Opened Windows Defender Firewall with Advanced Security using wf.msc.

2. List Current Firewall Rules
Checked existing rules under the Inbound Rules section.

3. Modify Rule to Block Port 23 (Telnet)
Located and configured the Telnet rule to 'Block' for all profiles.

4. Test the Rule
Used Command Prompt to try connecting via telnet to verify the block. Note: the test used port 80, not 23.

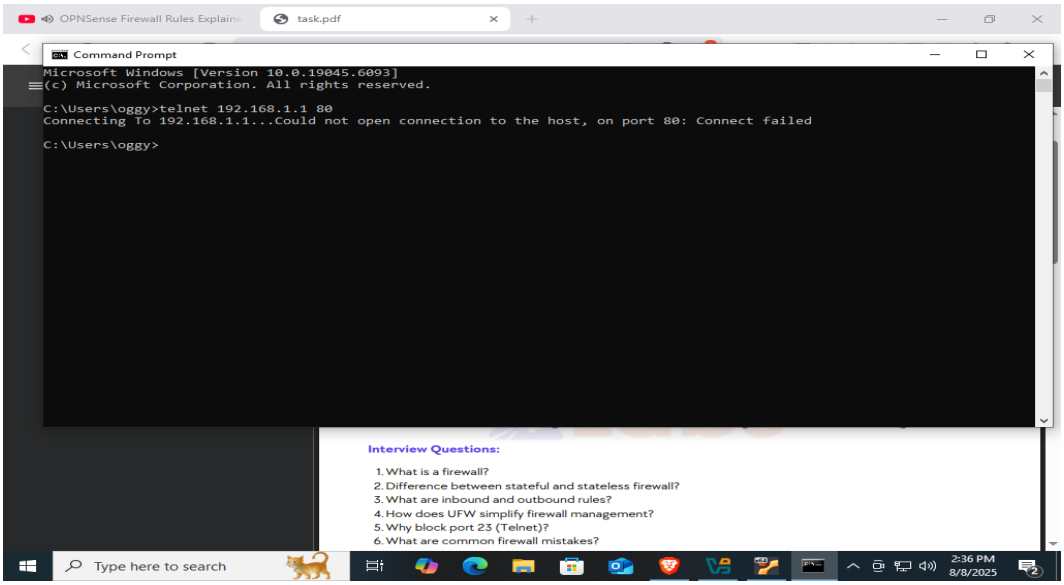
5. Allow SSH (Optional)
This step is generally for Linux systems. On Windows, SSH can be managed through firewall rules if needed.

6. Remove the Test Rule (Optional)
The Telnet rule can be disabled or deleted to restore original state.

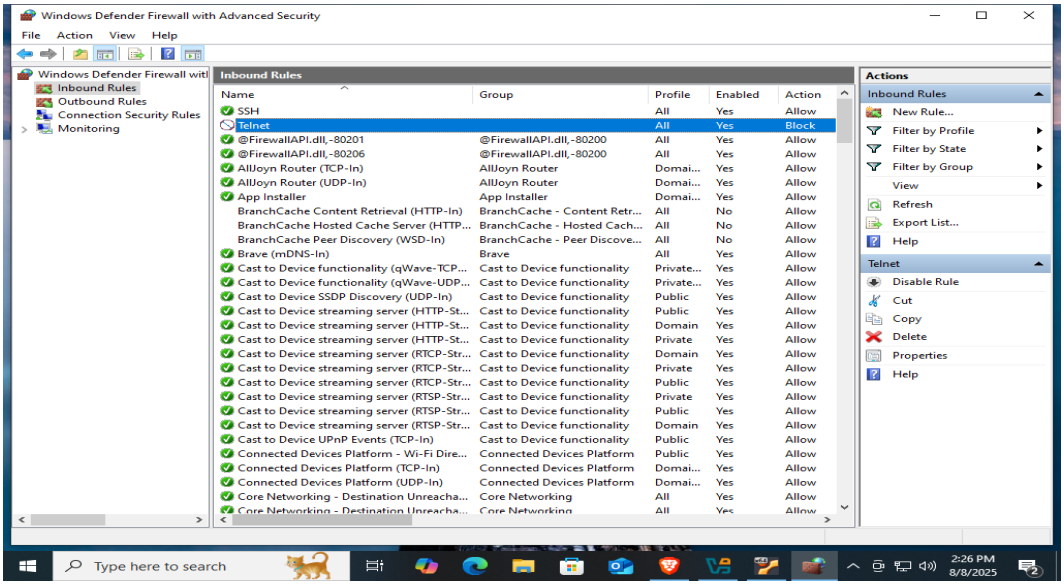
7. Document GUI Steps
Firewall rule was configured via the Windows GUI: wf.msc → Inbound Rules → Modify Telnet Rule.

8. Summary of Traffic Filtering
The firewall filters traffic based on rules. Blocking Telnet protects the system from remote login vulnerabilities on port 23.

Screenshots:



Telnet Test Result (Connection Failed)



Firewall Rule Showing Telnet Blocked