**Windows Firewall Configuration Report**

- DHARUNYA MAHALAKSHMI B

**Date:** Friday, September 26, 2025, 7 PM IST

**Executive Summary**

A firewall configuration and test were performed on my Windows computer using Windows Defender Firewall with Advanced Security. The objective was to demonstrate how to create, test, and remove a firewall rule to block inbound traffic on a specific port, and to document the process with evidence.

**Methodology**

* **Tool Used:** Windows Defender Firewall with Advanced Security
* **Scan Target:** Localhost (my computer)
* **Configuration Type:** Inbound rule for port blocking
* **Date:** September 26, 2025

**Steps Performed**

**1. Accessed Windows Defender Firewall with Advanced Security**

* Opened the firewall management console from the Start Menu.

**2. Reviewed Current Firewall Rules**

* Navigated to **Inbound Rules** to view existing rules and understand the current security posture.

**3. Created a Rule to Block Inbound Traffic on Port 23 (Telnet)**

* Initiated a new inbound rule for TCP port 23.
* Set the rule action to **Block the connection** for all profiles (Domain, Private, Public).
* Named the rule "Block Telnet" for clarity and future reference.

**4. Tested the Rule**

* Used Command Prompt to attempt a Telnet connection: telnet localhost 23.
* The connection was blocked, confirming the rule was effective.

**5. (Skipped) Allow SSH**

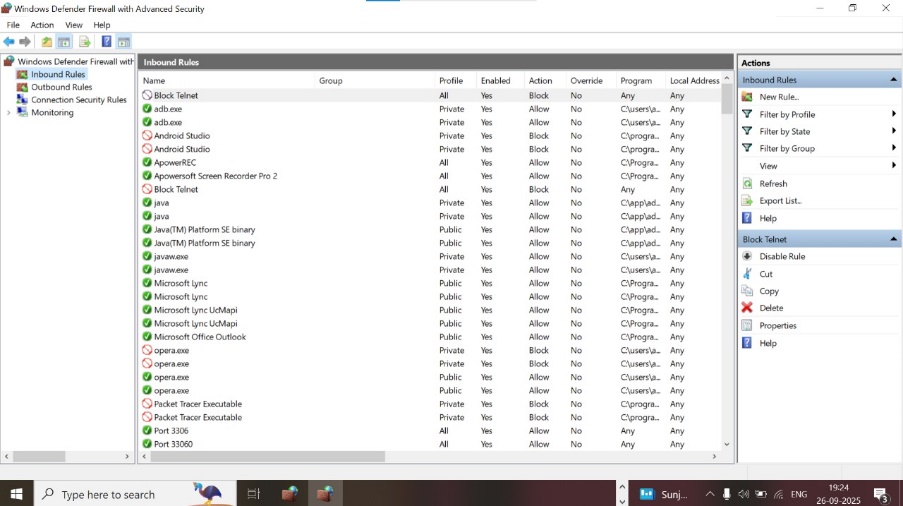
* SSH is not enabled by default on Windows, so this step was not required.

**6. Removed the Test Block Rule**

* Located and deleted the "Block Telnet" rule to restore the firewall to its original state.

**7. Documentation and Screenshots**

* Screenshots were taken of:
  + The Inbound Rules list showing the "Block Telnet" rule.



* + The Command Prompt with the failed Telnet connection message.



* These serve as evidence of the firewall rule in action and its removal.

**Summary: How the Firewall Filters Traffic**

Windows Defender Firewall filters network traffic by applying rules that allow or block connections based on criteria such as port, protocol, or application. By blocking port 23, the firewall prevented Telnet connections, demonstrating how rules can be used to control access and enhance system security. Removing the rule restored normal traffic flow.

**Conclusion**

Proper firewall configuration is essential for protecting systems from unauthorized access and network threats. This exercise demonstrated the process of creating, testing, and removing a firewall rule, highlighting the importance of regular review and documentation of firewall