# Firewall Configuration Report (Windows Firewall)

Date: June 27, 2025

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

## 1. Steps Performed

1. Opened Control Panel > Windows Defender Firewall > Advanced settings.  
2. Navigated to Inbound Rules.  
3. Clicked 'New Rule'.  
4. Selected 'Port', chose TCP, and entered port 23 to block Telnet.  
5. Chose 'Block the connection' and applied to all profiles.  
6. Named the rule 'Block Telnet'.  
7. Tested the rule using Telnet or Nmap — port 23 should be unreachable.  
8. Created a new rule to allow port 22 (SSH), similar steps but chose 'Allow the connection'.  
9. Deleted the Telnet block rule to restore original settings.

## 2. Summary

Windows Firewall allows users to control incoming and outgoing traffic by creating rules. In this task, a rule was created to block TCP traffic on port 23 (Telnet), effectively preventing remote Telnet access. Another rule was created to allow SSH (port 22) traffic. These rules help control access and secure the system by only permitting necessary connections.

## 3. Deliverables

• Screenshot of 'Inbound Rules' showing the 'Block Telnet' rule.  
• Screenshot of Telnet or Nmap test showing port 23 blocked.  
• Screenshot of 'Allow SSH' rule (port 22).  
• Screenshot after deleting or disabling the Telnet block rule.