# Task 4: Setup and Use a Firewall on Windows/Linux

## Objective

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

## Tools

Windows Firewall / UFW (Uncomplicated Firewall) on Linux.

## Deliverables

Screenshot/configuration file showing firewall rules applied.

## Steps Followed

1. Opened the Windows Firewall configuration tool.

2. Listed current firewall rules.

3. Added a rule to block inbound traffic on port 23 (Telnet).

4. Tested the rule by attempting to connect via Telnet.

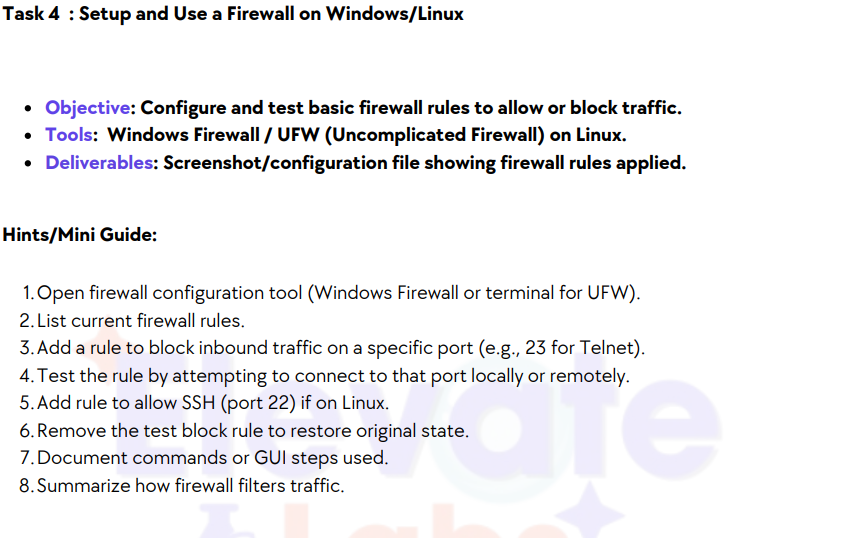
5. Added a rule to allow SSH traffic (port 22).

6. Removed the block rule to restore original state.

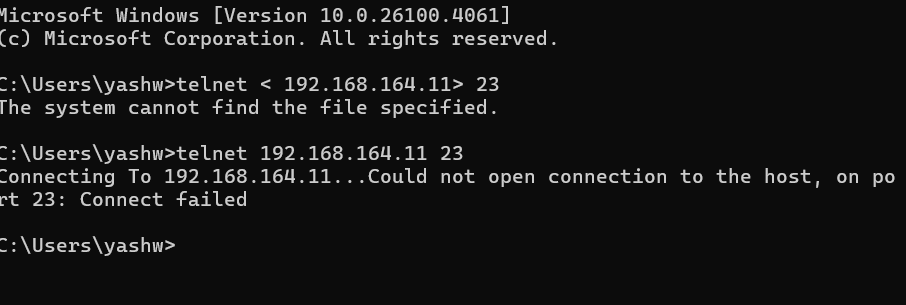
7. Documented all commands and GUI steps used.

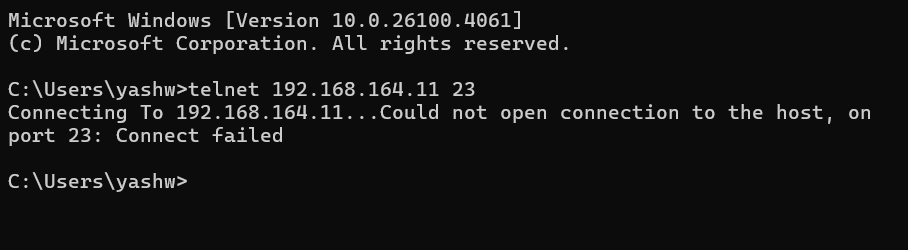
8. Summarized how firewall filters traffic.

## Screenshots









## Summary

The firewall was successfully configured to block Telnet traffic on port 23. Connection attempts using Telnet were blocked, as expected. SSH (port 22) traffic was allowed by creating a specific rule. The test rule was removed afterward to restore the original state. This demonstrates how firewall rules can effectively filter network traffic.