# Firewall Configuration and Testing Report

Date: 2025-10-26 18:38:19

## Objective

To configure and test firewall rules for blocking and allowing specific network ports using both GUI and command-line tools.

## System Used

• Windows 10 / Kali Linux (as applicable)

## Procedure

1. Opened the firewall tool (Windows Defender Firewall or UFW).  
2. Listed all existing firewall rules.  
3. Added a rule to block inbound traffic on port 23 (Telnet).  
4. Tested by attempting Telnet connection; it was blocked successfully.  
5. Added a rule to allow SSH (port 22) to ensure remote access.  
6. Removed the test rule to restore the firewall to its original configuration.

## Commands Used

Windows:  
• netsh advfirewall firewall show rule name=all  
• netsh advfirewall firewall add rule name="Block Telnet" dir=in action=block protocol=TCP localport=23  
• netsh advfirewall firewall delete rule name="Block Telnet"  
  
Linux (UFW):  
• sudo ufw status verbose  
• sudo ufw deny 23/tcp  
• sudo ufw allow 22/tcp  
• sudo ufw delete deny 23/tcp

## Observation

When port 23 was blocked, any attempt to connect to Telnet service failed, confirming that the firewall successfully filtered incoming traffic on that port.

## Conclusion

Firewalls play a crucial role in network security by filtering traffic based on defined rules. They can block or allow connections depending on source, destination, port, and protocol, thereby protecting the system from unauthorized access.