Firewall Configuration and Traffic Filtering Report

# 1. Objective

To demonstrate fundamental firewall management skills, including listing, modifying, testing, and removing firewall rules on both Windows and Linux systems. This task provides insight into how firewalls filter network traffic based on configured rules.

# 2. Opening the Firewall Configuration Tool

## Windows:

- Open Control Panel → System and Security → Windows Defender Firewall.  
- Alternatively, search for “Windows Defender Firewall” in the Start menu.

## Linux (UFW):

- Open Terminal.  
- Use `sudo ufw` commands to manage firewall settings.

# 3. Listing Current Firewall Rules

## Windows:

netsh advfirewall firewall show rule name=all

## Linux (UFW):

sudo ufw status numbered

# 4. Adding a Rule to Block Inbound Traffic on Port 23 (Telnet)

## Windows:

netsh advfirewall firewall add rule name="Block Telnet" dir=in action=block protocol=TCP localport=23

## Linux (UFW):

sudo ufw deny 23/tcp

# 5. Testing the Firewall Rule

Method:  
- Attempt to Telnet into the system using:  
 telnet <IP\_Address> 23  
- Expected Result: Connection refused or timeout due to blocked port.

# 6. Adding a Rule to Allow SSH (Port 22 – Only for Linux)

sudo ufw allow 22/tcp  
  
Note: This is critical to avoid locking yourself out of remote access.

# 7. Removing the Test Block Rule (Restoring Original State)

## Windows:

netsh advfirewall firewall delete rule name="Block Telnet"

## Linux (UFW):

sudo ufw delete deny 23/tcp

# 8. Summary of Commands / GUI Steps Used

|  |  |  |
| --- | --- | --- |
| Action | Windows Command | Linux (UFW) Command |
| View rules | netsh advfirewall firewall show rule name=all | sudo ufw status numbered |
| Block Port 23 (Telnet) | netsh advfirewall firewall add rule name="Block Telnet" ... | sudo ufw deny 23/tcp |
| Allow SSH (Port 22) | Not required by default | sudo ufw allow 22/tcp |
| Remove Port 23 block rule | netsh advfirewall firewall delete rule name="Block Telnet" | sudo ufw delete deny 23/tcp |

# 9. How Firewalls Filter Traffic

Firewalls operate based on configured rules to allow or deny network packets entering or exiting a system. Each rule consists of:  
- Direction (Inbound/Outbound)  
- Protocol (TCP/UDP)  
- Port number  
- Action (Allow/Deny)  
  
These rules act like gatekeepers, enforcing network security policies and reducing the system’s attack surface.

# 10. Outcome

- Learned to list, create, and remove firewall rules using GUI and CLI.  
- Understood how port filtering enhances system security.  
- Gained hands-on skills to manage basic network traffic on both Windows and Linux systems.

Prepared by:  
Keerthivasan E  
Intern at Elevate Labs