# 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

## Steps and Configuration

1. Open the firewall configuration tool:

- On Windows: Open Control Panel → System and Security → Windows Defender Firewall.

- On Linux: Use the terminal with UFW commands.

2. List current firewall rules:

- Windows: View inbound/outbound rules in the firewall GUI.

- Linux: Run `sudo ufw status verbose`.

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

- Windows: Add a new inbound rule in Windows Firewall GUI.

- Linux: `sudo ufw deny 23`

4. Test the rule by attempting to connect on port 23 locally or remotely.

5. Add a rule to allow SSH (port 22) if on Linux:

- `sudo ufw allow 22`

6. Remove the test block rule to restore original state:

- `sudo ufw delete deny 23`

7. Document commands or GUI steps used with screenshots.

## Summary

The firewall acts as a security filter that monitors and controls incoming and outgoing network traffic based on predetermined security rules. By applying basic firewall rules, we can block unwanted access (e.g., Telnet on port 23) while allowing secure connections (e.g., SSH on port 22). This exercise demonstrates how firewall rules help protect a system from unauthorized access.

