Firewall Setup and Testing on Windows/Linux

This document provides a detailed guide to configuring and testing firewall rules on both Linux (using UFW – Uncomplicated Firewall) and Windows (using Windows Defender Firewall). The purpose of the firewall is to control incoming and outgoing network traffic based on defined security rules. By completing these steps, we demonstrate how to block or allow traffic on specific ports, test connectivity, and restore the original configuration after testing.

Linux (UFW) Detailed Steps:

1. Open the terminal and check if UFW (Uncomplicated Firewall) is active using:
sudo ufw status
This shows whether the firewall is active and lists existing rules. 2. To view current firewall rules with numbers (for easier deletion later), use:
sudo ufw status numbered 3. Add a rule to block inbound traffic on port 23 (commonly used for Telnet):
sudo ufw deny 23/tcp
This prevents any TCP connection attempts on port 23. 4. Test the rule by attempting to connect locally:
telnet localhost 23
The connection should fail if the rule is working correctly. 5. Add a rule to allow SSH connections on port 22 (important for remote management):
sudo ufw allow 22/tcp 6. Remove the test block rule to restore the system to its original state:
sudo ufw delete deny 23/tcp 7. Take a screenshot of the sudo ufw status output showing applied rules. 8. Document the exact commands used and explain how they affect network traffic.

Windows Firewall Detailed Steps:

1. Open the Windows Firewall configuration tool: - Press **Win + R**, type wf.msc, and press Enter. - This opens Windows Defender Firewall with Advanced Security. 2. In the left pane, select **Inbound Rules** to view existing rules. 3. Create a new rule to block Telnet traffic on port 23: - Click **New Rule** → select **Port** → choose **TCP**. - Enter **23** as the specific local port. - Select **Block the connection** and apply it to all profiles (Domain, Private, Public). - Give the rule a name (e.g., “Block Telnet”) and finish. 4. Test the rule by opening Command Prompt and typing:
telnet localhost 23
The connection should fail, confirming the rule works. 5. Add a rule to allow SSH traffic (port 22): - Repeat the same process, but this time select **Allow the connection**. - Name the rule (e.g., “Allow SSH”). 6. To restore the firewall to its original state, delete the Telnet blocking rule: - In **Inbound Rules**, right-click the “Block Telnet” rule and select **Delete**. 7. Capture a screenshot of the Inbound Rules window showing the applied rules. 8. Document each GUI step followed for clarity.

Summary:

A firewall acts as a filter between a trusted internal network and untrusted external networks, such as the Internet. It enforces rules that determine which packets are allowed or denied based on criteria like port numbers, protocols, or IP addresses. In this task, rules were applied to block Telnet (port 23) and allow SSH (port 22). Testing confirmed the functionality, and rules were later removed to restore the firewall to its original state. Screenshots of the firewall status and rule configurations serve as evidence of successful implementation.