**Firewall Configuration: Step-by-Step Guide**

Below, you'll find the essential steps for firewall configuration and traffic filtering using both Windows Firewall (GUI) and UFW (Linux terminal), as well as a summary of how firewalls filter network traffic.

**1. Open Firewall Configuration Tool**

* **Windows Firewall (GUI):**
  + Press Win + R, type wf.msc, and hit Enter.
  + Alternatively, search “Windows Defender Firewall” in the Start menu.
* **UFW (Ubuntu/Linux terminal):**
  + Open Terminal (Ctrl+Alt+T).
  + Enter: sudo ufw status

**2. List Current Firewall Rules**

* **Windows Firewall:**
  + In the Firewall window, click on “Advanced Settings” → “Inbound Rules” to see existing rules.
* **UFW (Linux):**
  + Command: sudo ufw status numbered

**3. Add Rule to Block Inbound Traffic on Port 23 (Telnet)**

* **Windows Firewall:**
  + In “Inbound Rules”, click “New Rule…” (right-side pane).
  + Select “Port”, click Next.
  + Choose “TCP”, set “Specific local ports” to 23.
  + Select “Block the connection”, then proceed to finish the wizard.
* **UFW (Linux):**
  + Command: sudo ufw deny 23/tcp

**4. Test the Rule (Connect to Port 23 Locally/Remotely)**

* Try connecting using telnet:
  + Command: telnet localhost 23 (or from a remote machine: telnet [IP] 23)
  + Connection should fail, confirming the rule works.

**5. Add Rule to Allow SSH (Port 22, Linux Only)**

* **UFW (Linux):**
  + Command: sudo ufw allow 22/tcp
  + Check by: sudo ufw status

**6. Remove the Test Block Rule (Restore State)**

* **Windows Firewall:**
  + Find your created rule under “Inbound Rules”, right-click, “Delete”.
* **UFW (Linux):**
  + Command: sudo ufw delete deny 23/tcp
  + Or if numbered: sudo ufw delete [rule number] (check with sudo ufw status numbered)

**7. Documented Commands & GUI Steps**

**Windows Firewall (GUI)**

* Open firewall: wf.msc
* List rules: “Inbound Rules”
* Block port: New Rule → Port → TCP:23 → Block
* Remove rule: Delete created rule

**UFW (Linux terminal)**

bash

sudo ufw status

sudo ufw deny 23/tcp

telnet localhost 23 *# Test connection*

sudo ufw allow 22/tcp *# Allow SSH*

sudo ufw delete deny 23/tcp *# Remove block rule*

**8. How Firewalls Filter Traffic**

* **Firewalls filter traffic by enforcing rules about which connections (protocol, port, source, destination) are allowed or blocked.**
* They inspect network packets and permit or deny based on configured rules, for both inbound (from network to device) and outbound (from device to network) directions.
* This helps **protect devices from unauthorized access, malware, and exploits** by **restricting unwanted traffic while allowing legitimate communication**.