**✅ Firewall Configuration Mini Project Solution**

**🎯 Objective**

To gain hands-on experience with **firewall rules**, understand how traffic is filtered, and learn to allow/deny traffic based on ports and services.

**🛠️ Step-by-Step Guide (Linux – UFW)**

(Also includes Windows version after this)

**✅ LINUX (UFW)**

**1. Open UFW (Uncomplicated Firewall)**

Check if it's installed:

bash

CopyEdit

sudo ufw status

If not:

bash

CopyEdit

sudo apt install ufw

sudo ufw enable

🖼️ Screenshot Tip: Show ufw status output.

**2. List Current Rules**

bash

CopyEdit

sudo ufw status numbered

📌 Example:

vbnet

CopyEdit

Status: active

To Action From

-- ------ ----

22/tcp ALLOW Anywhere

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

bash

CopyEdit

sudo ufw deny 23

🖼️ Screenshot Tip: Show the updated rule with ufw status.

**4. Test Port Block**

Try to connect:

bash

CopyEdit

telnet localhost 23

Expected output:

vbnet

CopyEdit

Trying 127.0.0.1...

telnet: Unable to connect to remote host: Connection refused

**5. Allow SSH (Port 22)**

bash

CopyEdit

sudo ufw allow 22

🖼️ Screenshot Tip: Show rules list with both 22 ALLOW and 23 DENY.

**6. Remove Telnet Block Rule (Restore State)**

bash

CopyEdit

sudo ufw delete deny 23

**7. Document Commands Used**

| **Action** | **Command** |
| --- | --- |
| Enable firewall | sudo ufw enable |
| Deny port 23 | sudo ufw deny 23 |
| Allow SSH (port 22) | sudo ufw allow 22 |
| Delete port 23 rule | sudo ufw delete deny 23 |
| List rules | sudo ufw status numbered |

**8. Summary: How Firewalls Filter Traffic**

Firewalls work by applying **rules** that determine whether to **allow** or **block** network traffic based on **ports**, **protocols**, **IP addresses**, or **applications**. They act as the first layer of defense to control both **inbound** and **outbound** traffic.