Step 1: Firewall Concepts

A firewall acts as a gatekeeper between your computer and the network. It uses a **Rule-Based System** to inspect incoming and outgoing packets.

- **Implicit Deny:** The best practice of blocking all traffic by default and only opening specific "holes" (ports) for services you trust.
- **Ports:** Think of these as "doors." For example, Web traffic uses port 80/443, while SSH uses port 22.

Step 2 & 3: Configure Rules (Allow/Deny)

Open your terminal and follow these commands to set up a secure baseline.

1. **Check Status:**

sudo ufw status

2. **Set Defaults (The "Deny All" Strategy):**

sudo ufw default deny incoming

sudo ufw default allow outgoing

3. **Allow Essential Services:**
    - **SSH (so you don't lock yourself out):** sudo ufw allow 22/tcp
    - **HTTP/HTTPS:** sudo ufw allow 80/tcp and sudo ufw allow 443/tcp
4. **Enable the Firewall:**

sudo ufw enable

Step 4 & 5: Test Connectivity & Observe Logs

Once enabled, you need to verify that your rules actually work.

- **Connectivity Test:** From another machine (or using an online port scanner), try to connect to your IP.
    - telnet [Your-IP] 80 (Should connect)
    - telnet [Your-IP] 23 (Should timeout/fail because port 23 is blocked)
- **Logging:** View the "gatekeeper's" notes to see blocked attempts:

sudo tail -f /var/log/ufw.log

Step 6: Block a Malicious IP

If you notice an IP address repeatedly trying to connect to a restricted port in your logs, you can "blacklist" it specifically.

- **Command:** sudo ufw deny from 192.168.1.50
- This rule takes precedence and ensures that specific source can't touch any part of your system.

Step 7 & 8: Documentation & Impact

To complete your **Deliverable**, you should create a simple table like the one below:

Firewall Rules Documentation

Rule Number	Action	Protocol	Port	Source	Purpose
1	ALLOW	TCP	22	Any	Remote Administration (SSH)
2	ALLOW	TCP	80, 443	Any	Web Server Access
3	DENY	ALL	ALL	192.168.1.50	Blocked malicious actor
4	DENY	ALL	ALL	Any	Default Deny (Security Baseline)