**Fail2ban-:**

1. As usual Sudo apt update
2. Then Sudo apt upgrade
3. Sudo apt install fail2ban
4. Sudo enable fail2ban
5. Sudo disable fail2ban
6. Sudo status fail2ban

After that just rename the 2 files jail.confd and fail2banconfig.d

Using cmd

Cp jail.configd jail.local

Cp fail2ban.config fail2ban.local

Then just add the

Ban time – 10min

Ssh is enable

And response time - 10 min

Response time – 20 min

**Ufw (uncomplicated firewall) -:**

sudo ufw enable # Turn on firewall

sudo ufw disable # Turn off firewall

sudo ufw status # Show current status

sudo ufw status verbose

**Allow traffic - :**

sudo ufw allow 22 # Allow SSH (port 22)

sudo ufw allow 80 # Allow HTTP

sudo ufw allow 443 # Allow HTTPS

sudo ufw allow 8080 # Allow custom port

sudo ufw allow from 192.168.1.10 # Allow specific IP

sudo ufw allow from 192.168.1.0/24 # Allow whole subnet

**Deny / Reject Traffic - :**

sudo ufw deny 23 # Deny Telnet (example)

sudo ufw deny from 10.0.0.5 # Block specific IP

sudo ufw reject 25 # Reject SMTP (different from deny → sends reject response)