

Task 4: Setup and Use UFW Firewall on Linux

System: Ubuntu/Linux with UFW

Step 1: Install and Enable UFW

```
sudo apt update
sudo apt install ufw -y
sudo ufw enable
sudo ufw status verbose
```

Step 2: List Current Firewall Rules

```
sudo ufw status numbered
```

(Take a screenshot here for deliverable)

Step 3: Block Inbound Traffic on Port 23 (Telnet)

```
sudo ufw deny 23/tcp
```

Step 4: Test the Rule

```
telnet localhost 23
```

Or from remote: telnet <your-ip> 23

Step 5: Allow SSH on Port 22

```
sudo ufw allow 22/tcp
```

Step 6: Remove the Telnet Rule

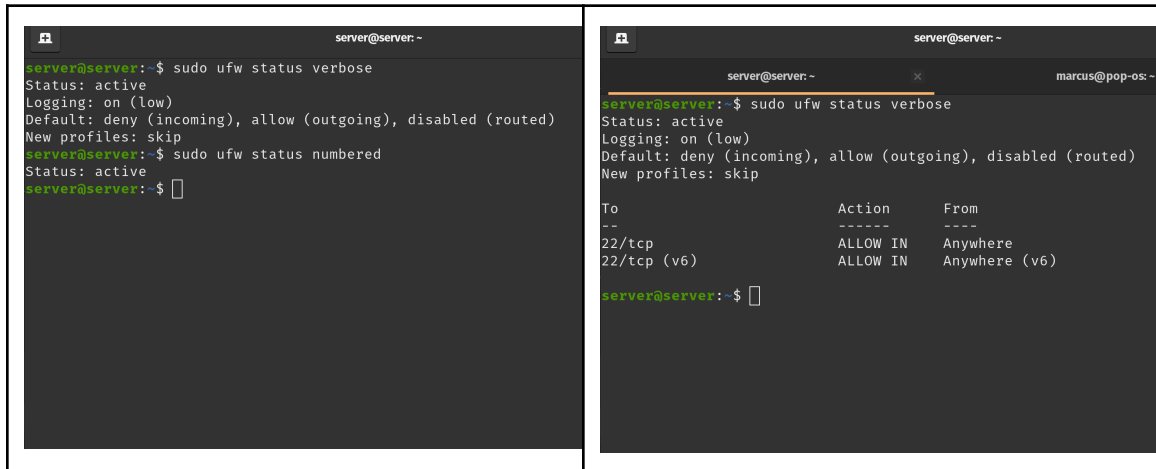
```
sudo ufw delete deny 23/tcp
```

Step 7: Documented Commands Used

```
sudo apt update
sudo apt install ufw -y
sudo ufw enable
sudo ufw status numbered
sudo ufw deny 23/tcp
```

```
telnet localhost 23
sudo ufw allow 22/tcp
sudo ufw delete deny 23/tcp
```

Step 8: Output difference



```
server@server: ~  
server@server:~$ sudo ufw status verbose  
Status: active  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip  
server@server:~$ sudo ufw status numbered  
Status: active  
server@server:~$
```

```
server@server: ~  
server@server:~$ sudo ufw status verbose  
Status: active  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip  


| To          | Action   | From          |
|-------------|----------|---------------|
| --          | -----    | ----          |
| 22/tcp      | ALLOW IN | Anywhere      |
| 22/tcp (v6) | ALLOW IN | Anywhere (v6) |

  
server@server:~$
```

Step 9: Summary – How UFW Filters Traffic

UFW (Uncomplicated Firewall) is a user-friendly interface for iptables. It allows administrators to easily allow or block traffic by port, IP, or protocol. Blocking Telnet (port 23) and allowing SSH (port 22) demonstrates secure access control. Firewall rules protect systems by reducing exposed attack surfaces.