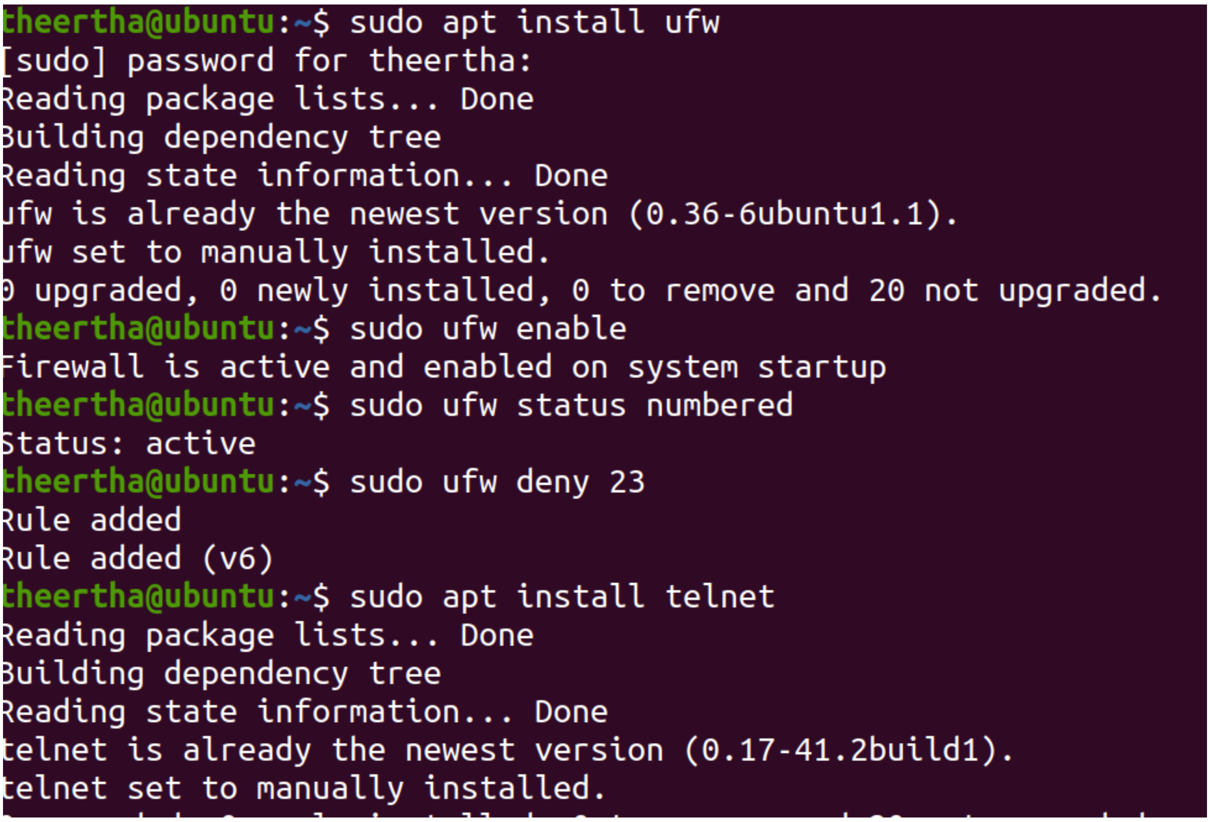
Task 4 : Setup and Use a Firewall on Windows/Linux

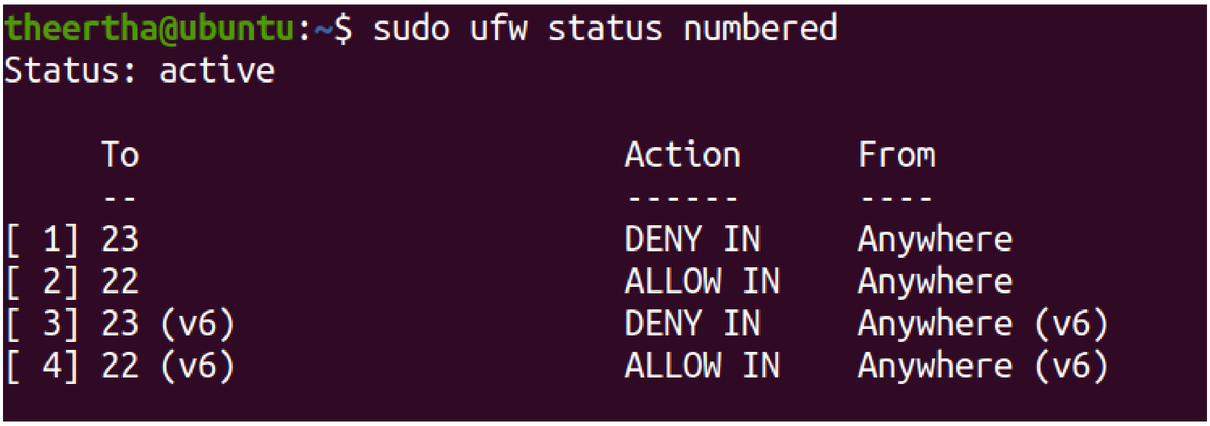
Objective: To understand and demonstrate basic firewall management using either Windows Firewall or UFW (Uncomplicated Firewall) on Linux. The task involves configuring rules to block and allow network traffic and documenting the process.

Here I use Ubuntu 22.04 (Linux), UFW as Firewall Tool.



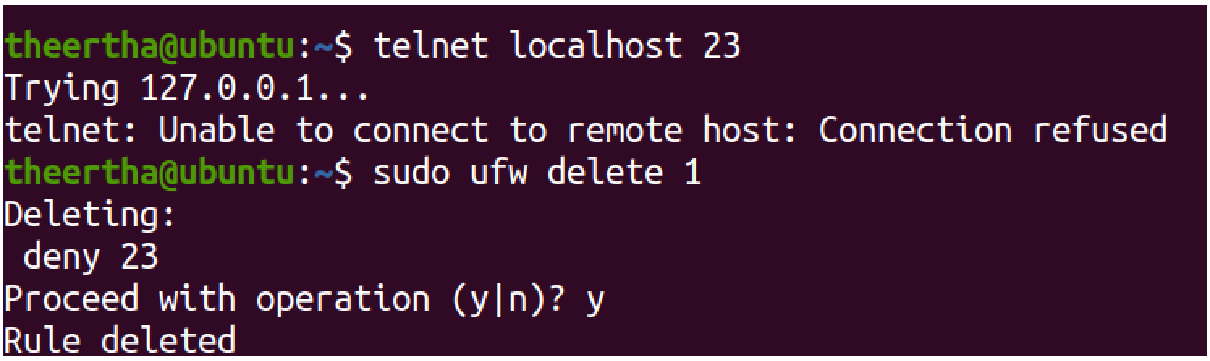
```
theertha@ubuntu:~$ sudo apt install ufw
[sudo] password for theertha:
Reading package lists... Done
Building dependency tree
Reading state information... Done
ufw is already the newest version (0.36-6ubuntu1.1).
ufw set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 20 not upgraded.
theertha@ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
theertha@ubuntu:~$ sudo ufw status numbered
Status: active
theertha@ubuntu:~$ sudo ufw deny 23
Rule added
Rule added (v6)
theertha@ubuntu:~$ sudo apt install telnet
Reading package lists... Done
Building dependency tree
Reading state information... Done
telnet is already the newest version (0.17-41.2build1).
telnet set to manually installed.
```

Enabled UFW and Blocked Telnet.



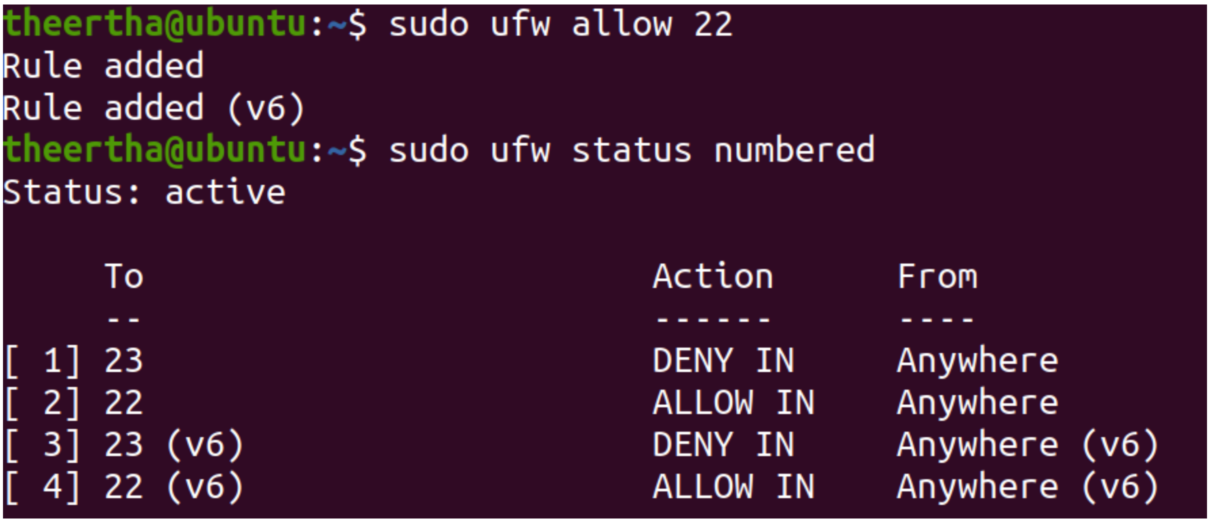
```
theertha@ubuntu:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 23                         DENY IN     Anywhere
[ 2] 22                         ALLOW IN    Anywhere
[ 3] 23 (v6)                    DENY IN     Anywhere (v6)
[ 4] 22 (v6)                    ALLOW IN    Anywhere (v6)
```

Tested using telnet localhost 23 to confirm the port was blocked.



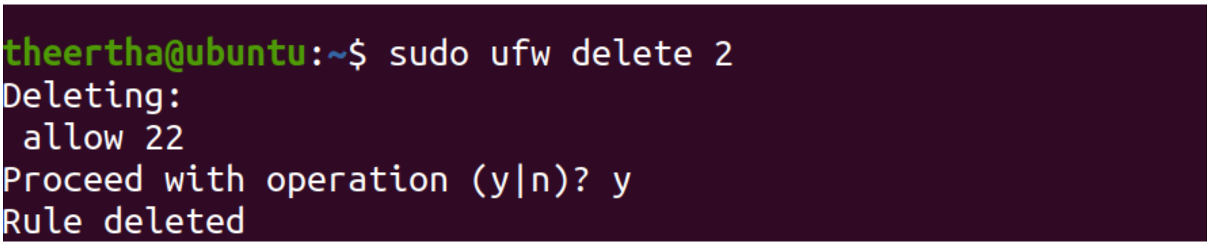
```
theertha@ubuntu:~$ telnet localhost 23
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
theertha@ubuntu:~$ sudo ufw delete 1
Deleting:
 deny 23
Proceed with operation (y|n)? y
Rule deleted
```

Allowed SSH.



```
theertha@ubuntu:~$ sudo ufw allow 22
Rule added
Rule added (v6)
theertha@ubuntu:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 23                         DENY IN     Anywhere
[ 2] 22                         ALLOW IN    Anywhere
[ 3] 23 (v6)                    DENY IN     Anywhere (v6)
[ 4] 22 (v6)                    ALLOW IN    Anywhere (v6)
```

Removed the Block Rule.



```
theertha@ubuntu:~$ sudo ufw delete 2
Deleting:
 allow 22
Proceed with operation (y|n)? y
Rule deleted
```

How Firewall Filters Traffic

A firewall is a security tool that monitors and controls network traffic based on a set of defined rules. It acts as a protective barrier between a trusted internal network and an untrusted external network, like the internet.

Firewalls filter traffic using the following mechanisms:

1. Rule-Based Filtering:
   Traffic is allowed or blocked based on rules that inspect:
   - Source and destination IP addresses
   - Port numbers (e.g., port 22 for SSH, port 23 for Telnet)
   - Protocol types (e.g., TCP, UDP)
   - Direction (inbound or outbound)
2. Inbound and Outbound Filtering:
   - Inbound rules block or allow traffic coming into your system.
   - Outbound rules manage traffic leaving your system.

3. Stateful vs. Stateless Inspection:
    - Stateless firewalls treat each packet in isolation.
    - Stateful firewalls track ongoing connections and allow related traffic automatically.
4. Default Deny Policy:
   Many firewalls block all traffic by default and allow only the traffic that matches specific “allow” rules, improving system security.
5. Logging and Monitoring:
   Firewalls often log all traffic activity, helping detect intrusions, audit actions, and troubleshoot network issues.

By applying these methods, a firewall ensures only legitimate and safe traffic reaches the system, effectively reducing the risk of unauthorized access and cyberattacks.