Linux Firewall Configuration Task Documentation (UFW)

Objective

To configure and test UFW (Uncomplicated Firewall) on a Linux system by blocking a specific port (Telnet – 23), allowing SSH (port 22), and restoring the original state.

System Information

- **Operating System:** Ubuntu/Debian-based Linux
- **Firewall Tool:** UFW (Uncomplicated Firewall)
- **User:** Kali
- **Date:** 30/05/2025

Step-by-Step Procedure

1. Install UFW (if not installed)

sudo apt update

sudo apt install ufw

2. Enable UFW

Important: Allow SSH before enabling if connected remotely

sudo ufw allow 22/tcp

sudo ufw enable

3. List Current Firewall Rules

sudo ufw status verbose

4. Block Inbound Traffic on Port 23 (Telnet)

sudo ufw deny 23/tcp

5. Test the Block Rule

Attempt to connect to port 23 locally:

***Using telnet**

telnet localhost 23

Expected Output: Connection refused or timeout (i.e., the port is blocked).

6. Allow SSH (Port 22)

sudo ufw allow 22/tcp

7. Remove the Block Rule (Restore Original State)

sudo ufw delete deny 23/tcp

Summary

- **UFW** was installed and enabled.
- **Port 23 (Telnet)** was blocked using a firewall rule.
- Connectivity to port 23 was tested and confirmed to be blocked.
- **Port 22 (SSH)** was allowed to ensure remote access.
- The Telnet block rule was removed, restoring the system's original firewall state.

Conclusion:
Firewalls like UFW control traffic by allowing or denying connections based on port, protocol, and IP. This helps secure the system against unauthorized access and unwanted network activity.

Summary: How Firewalls Filter Traffic

A **firewall** is a security system that controls incoming and outgoing network traffic based on predetermined rules. It acts as a barrier between a trusted internal network and untrusted external networks (like the internet).

How Firewalls Filter Traffic:

1. **Rule-Based Filtering:**
    - Firewalls use **rules** to decide whether to **allow** or **block** traffic.

- Rules are based on:
    - **Port numbers** (e.g., block port 23 for Telnet)
    - **IP addresses** (e.g., allow only specific IPs)
    - **Protocols** (e.g., TCP, UDP, ICMP)

2. **Inbound vs. Outbound Filtering:**
    - **Inbound traffic**: Coming into your system from outside (e.g., remote login attempts).
    - **Outbound traffic**: Leaving your system to external services (e.g., browsing a website).
    - Firewalls can control both.
3. **Stateful Inspection:**
    - Most modern firewalls are **stateful**, meaning they keep track of active connections and allow return traffic automatically (e.g., if you request a webpage, the response is allowed).
4. **Default Policies:**
    - Firewalls usually have a **default policy**:
        - Deny all and only allow specific traffic (more secure).
        - Allow all and only block specific traffic (less secure).

Purpose:

- Prevent **unauthorized access**
- Block **malware or exploits**
- Allow **trusted communication**
- Enforce **network policies**

Screenshots:

```
┌──(kali㉿vbox)-[~]
└─$ sudo apt install ufw

The following packages were automatically installed and are no longer required:
  apg                          libpoppler145
  fonts-inter-variable         libpython3.12-minimal
  gnome-accessibility-themes   libpython3.12-stdlib
  gnome-themes-extra           libpython3.12t64
  icu-devtools                 libutempter0
  libflac12t64                 python3-aioconsole
  libfuse3-3                   python3-dunamai
  libgail-common               python3-nfsclient
  libgail18t64                 python3-poetry-dynamic-versioning
  libgeos3.13.0                python3-pywerview
  libglapi-mesa                python3-requests-ntlm
  libgtk2.0-0t64               python3-setproctitle
  libgtk2.0-bin                python3-tomlkit
  libgtk2.0-common             python3.12-tk
  libicu-dev                   ruby-zeitwerk
  liblbfgsb0                   sphinx-rtd-theme-common
Use 'sudo apt autoremove' to remove them.

Installing:
  ufw

Suggested packages:
  rsyslog

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 16
  Download size: 169 kB
  Space needed: 880 kB / 11.8 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 1s (217 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 423047 files and directories currently installed.)
Preparing to unpack .../archives/ufw_0.36.2-9_all.deb ...
Unpacking ufw (0.36.2-9) ...
Setting up ufw (0.36.2-9) ...
Creating config file /etc/ufw/before.rules with new version
Creating config file /etc/ufw/before6.rules with new version
Creating config file /etc/ufw/after.rules with new version
Creating config file /etc/ufw/after6.rules with new version
update-rc.d: We have no instructions for the ufw init script.
update-rc.d: It looks like a non-network service, we enable it.
```

```
┌──(kali㉿vbox)-[~]
└─$ sudo ufw enable

Firewall is active and enabled on system startup

┌──(kali㉿vbox)-[~]
└─$ sudo ufw allow 22/tcp
sudo ufw enable

Rule added
Rule added (v6)
Firewall is active and enabled on system startup

┌──(kali㉿vbox)-[~]
└─$ 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)


┌──(kali㉿vbox)-[~]
└─$ sudo ufw deny 23/tcp

Rule added
Rule added (v6)

┌──(kali㉿vbox)-[~]
└─$ sudo ufw allow 22/tcp

Skipping adding existing rule
Skipping adding existing rule (v6)

┌──(kali㉿vbox)-[~]
└─$ sudo ufw delete deny 23/tcp

Rule deleted
Rule deleted (v6)

┌──(kali㉿vbox)-[~]
└─$ sudo ufw deny 23/tcp

Rule added
```

```
┌──(kali㉿vbox)-[~]
└─$ sudo ufw delete deny 23/tcp

Rule deleted
Rule deleted (v6)

┌──(kali㉿vbox)-[~]
└─$ sudo ufw deny 23/tcp

Rule added
Rule added (v6)

┌──(kali㉿vbox)-[~]
└─$ telnet localhost 23

Trying ::1...
Connection failed: Connection refused
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused

┌──(kali㉿vbox)-[~]
└─$ sudo ufw allow 22/tcp

Skipping adding existing rule
Skipping adding existing rule (v6)

┌──(kali㉿vbox)-[~]
└─$ sudo ufw delete deny 23/tcp

Rule deleted
Rule deleted (v6)
```