

Firewall Configuration & Testing Report (UFW – Linux)

1. Introduction

This report explains the process of configuring, applying, and testing firewall rules in a Linux environment using UFW (Uncomplicated Firewall). The objective was to understand how firewall rules filter network traffic and to perform operations such as listing rules, blocking ports, allowing ports, and verifying rule behavior.

2. System Used

- Operating System: Linux (Ubuntu/Debian-based)
- Firewall Tool: UFW (Uncomplicated Firewall)
- Objective: Basic firewall rule creation, testing inbound/outbound behavior

3. Step-by-Step Procedure

Below are the steps performed to configure and test firewall rules using UFW. Screenshots can be inserted after each step.

Step 1: Check Firewall Status

Commands:

```
sudo ufw status  
sudo ufw enable
```

Step 2: List Existing Firewall Rules

Command:

```
sudo ufw status numbered
```

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

Command:

```
sudo ufw deny 23
```

Step 4: Test the Block Rule

Command:

```
telnet 127.0.0.1 23
```

Step 5: Allow SSH (Port 22)

Command:

```
sudo ufw allow 22
```

Step 6: Remove the Test Block Rule

Command:

```
sudo ufw delete deny 23
```

Screenshots:

The screenshot shows a terminal window with the following session history:

```
(mayur㉿kali)-[~]
$ sudo apt update
$ sudo apt install ufw
Get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.9 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.6 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [114 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [259 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [187 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [894 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [11.3 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [28.4 kB]
Fetched 75.0 MB in 40s (1,885 kB/s)
765 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer required:
  kde-style-oxygen-qt6 libgdata22 liboxygentstyle6-6 libsigsegv2 libtheoradec1 python3-packaging-whl
  libbluray2 libgeos3.13.1 liboxygentstyleconfig6-6 libsoup-2.4-1 libtheoraenc1 python3-wheel-whl
  libgdal36 libhdf4-0-alt libqt5ct-common1.8 libsoup2.4-common libudfread0
  libgdata-common libogdi4.1 libsframe1 libtheora0 libvpx9
Use 'sudo apt autoremove' to remove them.

Installing:
  ufw

Suggested packages:
  rsyslog
```

```
mayur@kali:~$ sudo ufw status
Status: inactive

mayur@kali:~$ sudo ufw enable
Firewall is active and enabled on system startup

mayur@kali:~$ sudo ufw status numbered
Status: active

mayur@kali:~$ sudo ufw deny 23
Rule added
Rule added (v6)

mayur@kali:~$ telnet 127.0.0.1 23
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
```

```
mayur@kali:~$ telnet 127.0.0.1 23
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused

mayur@kali:~$ sudo ufw allow 22
Rule added
Rule added (v6)

mayur@kali:~$ sudo ufw delete deny 23
Rule deleted
Rule deleted (v6)
```

4. Summary

A firewall filters traffic by inspecting incoming and outgoing packets and making decisions based on defined rules. UFW simplifies firewall rule creation, allowing administrators to permit or deny specific ports and services easily. This enhances system security by reducing the attack surface and controlling communication channels.

5. Conclusion

Through this task, practical experience was gained in managing UFW firewall rules. This strengthened understanding of traffic filtering, port management, and overall system security through firewall configuration.