Setup and Use a Firewall on Linux

By- Dhruv Bhatia

A firewall is a network security device either hardware or software-based which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects, or drops that specific traffic. It acts like a security guard that helps keep your digital world safe from unwanted visitors and potential threats.

- **Accept:** allow the traffic
- **Reject:** block the traffic but reply with an "unreachable error"
- **Drop:** block the traffic with no reply

Key Functions of a Firewall:

Function	Description
Packet Filtering	Examines headers of packets and blocks/allows based on IP, port, or protocol.
Stateful Inspection	Tracks active connections and only allows packets that are part of a known session.
Proxying	Acts as an intermediary between users and the internet to mask identity and filter content.
Rule-Based Access Control	Uses rules set by the administrator (e.g., block port 23, allow port 80).

UFW, or **Uncomplicated Firewall**, is a **user-friendly command-line interface** for managing **iptables**, the default firewall management tool in Linux.

Key Features:

- Simple syntax (e.g., ufw allow 22)
- Supports both IPv4 and IPv6
- Enables **default deny policies** for secure configurations
- Logs firewall activity
- Can manage rules per application or port

Step 1.Setting Up a Kali Linux Virtual Machine:

Step 2: Install ufw through the Linux Terminal

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

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 40
  Download size: 169 kB
  Space needed: 880 kB / 887 MB available

Get:1 http://kali.download/kali kali-rolling/main arm64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 1s (264 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 459082 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.
Created symlink '/etc/systemd/system/multi-user.target.wants/ufw.service' → '/usr/lib/systemd/system/ufw.service'.
Processing triggers for kali-menu (2025.3.0) ...
Processing triggers for rsyslog (8.2504.0-1) ...
Processing triggers for man-db (2.13.1-1) ...
```

Step 3 : Check the status of ufw

Command: sudo ufw status numbered

```
┌──(kali㉿vbox)-[~]
└─$ sudo ufw status numbered
Status: inactive
```

Step 4: Block inbound traffic on Telnet port (port 23)

Command: sudo ufw deny 23

```
┌──(kali㉿vbox)-[~]
└─$ sudo ufw deny 23
Rules updated
Rules updated (v6)
```

Step 5: Test the rule

```
┌──(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
```

Step 6: Allow SSH (port 22)

Command: sudo ufw allow 22

```
┌──(kali㉿vbox)-[~]
└─$ sudo ufw allow 22
Rules updated
Rules updated (v6)
```

Step 7: Try to establish a connection on port 22

We see that telnet is taking a lot of time because the connection establishment is in process, so there is a chance that connection will be completed.

```
┌──(kali㉿vbox)-[~]
└─$ telnet 192.168.101.189 22
Trying 192.168.101.189 ...
```

Step 8: View Final Rules

```
┌──(kali㉿vbox)-[~]
└─$ sudo ufw status verbose
[sudo] password for kali:
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
23                         DENY IN     Anywhere
22                         ALLOW IN    Anywhere
8080                       ALLOW IN    Anywhere
23 (v6)                    DENY IN     Anywhere (v6)
22 (v6)                    ALLOW IN    Anywhere (v6)
8080 (v6)                  ALLOW IN    Anywhere (v6)
```

UFW Commands Summary

Action	Command
Enable UFW	sudo ufw enable
View rules	sudo ufw status numbered
Deny port 23	sudo ufw deny 23
Allow SSH (port 22)	sudo ufw allow 22
Delete deny rule	sudo ufw delete deny 23
View final rules	sudo ufw status verbose

How Firewall Traffic Filtering Works ?

1. **Packet Arrives:**

   Every network request (e.g., loading a website, remote access) is broken into packets.

2. **Rule Check:**

   The firewall compares each packet's:

   - **Source IP address**
   - **Destination IP address**
   - **Port number** (e.g., 80 for HTTP, 22 for SSH)
   - **Protocol** (TCP, UDP, ICMP)

     Against its list of **rules**.

3. **Decision is Made:**
   - **Allow** – if the packet matches an "allow" rule.
   - **Deny/Block** – if it matches a "deny" rule.
   - **Drop Silently** – discard the packet without notifying the sender.
4. **State Tracking (if enabled):**

   In **stateful firewalls**, the firewall remembers active connections and only allows related traffic.