Technical Report: Firewall Setup and Testing on Kali Linux

(Navneet Bijalwan)

---

1. Introduction

1.1 Objective

The purpose of this report is to document the process of configuring and testing **firewall rules** on **Kali Linux** using **UFW (Uncomplicated Firewall)**. Firewalls are a crucial component in cybersecurity, acting as barriers to unauthorized access while permitting legitimate connections. This guide aims to:

- Implement firewall rules to enhance system security.
- Block unwanted inbound traffic.
- Allow essential services such as **SSH (Secure Shell)** for secure remote management.
- Test and validate firewall settings.

1.2 Importance of Firewalls in Cybersecurity

In today's digital age, **network security** is more critical than ever. **Firewalls** serve as the first line of defense against malicious activities such as:

- **Port scanning attacks:** Hackers use automated tools to scan open ports and exploit vulnerabilities.
- **Unauthorized access:** Without proper firewall rules, intruders can gain control over sensitive systems.
- **Denial of Service (DoS) attacks:** Attackers flood the system with requests, causing service disruptions.

Setting up a robust firewall helps in **securing sensitive data**, preventing unauthorized connections, and **monitoring network traffic** efficiently.

---

2. Tools and Technologies Used

2.1 Operating System

- **Kali Linux**: A specialized Linux distribution widely used for penetration testing and cybersecurity research.

2.2 Firewall Management Tool

- **UFW (Uncomplicated Firewall)**: A simplified firewall management tool built on top of **iptables**, providing an easier way to configure firewall rules.

2.3 Additional Testing Utilities

- **Telnet**: Used to test blocked ports.
- **SSH**: Ensures secure remote access while filtering unauthorized traffic.
- **Firewalk**: A tool for testing firewall rule behavior.
- **ftester**: Simulates packet traffic to verify firewall settings.

---

3. Firewall Configuration and Rule Implementation

3.1 Installing and Enabling UFW

Before configuring firewall rules, install and activate **UFW**:

```
sudo apt update && sudo apt install ufw -y
```

```
sudo ufw enable
```

After enabling **UFW**, it automatically begins blocking all **incoming** connections while permitting outgoing traffic.

3.2 Listing Existing Firewall Rules

Before applying new rules, check the existing configurations:

```
sudo ufw status verbose
```

This command displays currently allowed and denied traffic, helping users modify rules accordingly.

3.3 Blocking Inbound Traffic on Port 23 (Telnet)

Telnet is an **insecure** protocol that transmits data without encryption. To **block Telnet traffic**, configure UFW with:

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

This ensures no unauthorized Telnet connections can be made.

3.4 Allowing SSH Access on Port 22

Since SSH provides secure remote login capabilities, allow its traffic:

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

Without this rule, SSH connections would be rejected, preventing remote administration.

3.5 Removing Temporary Block Rule

After testing firewall behavior, remove the Telnet restriction:

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

This restores the system to its previous state.

---

4. Firewall Testing Methods

4.1 Manual Testing Using Telnet and SSH

Telnet Test (Expected to Fail)

To verify that **port 23** is blocked:

```
telnet localhost 23
```

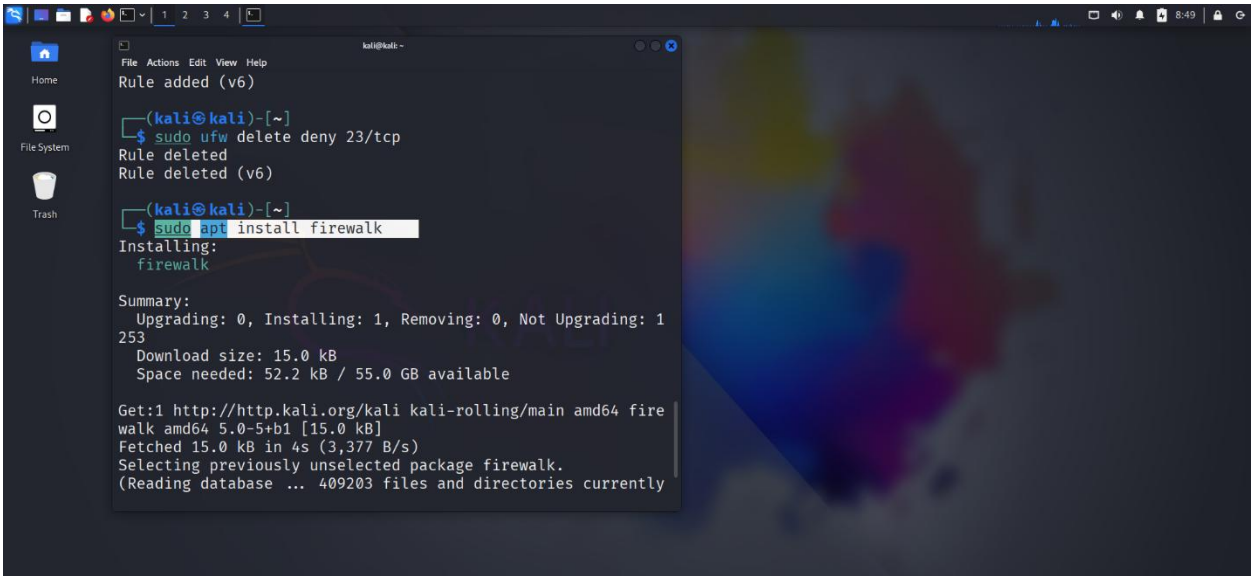
If properly configured, the connection attempt should result in an error.

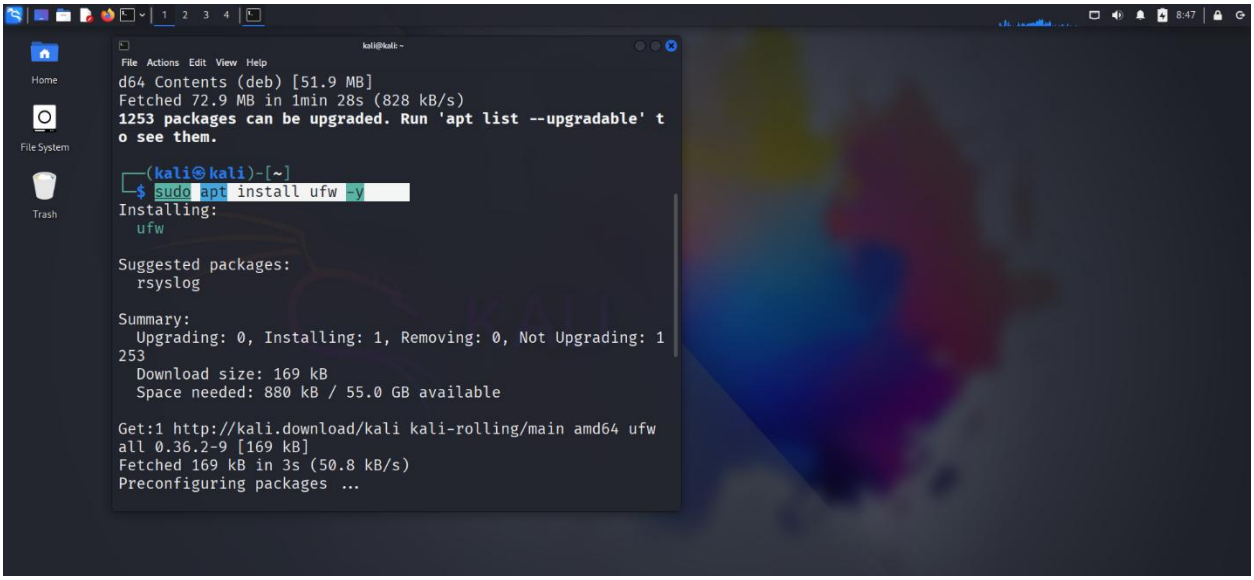
SSH Test (Expected to Succeed)

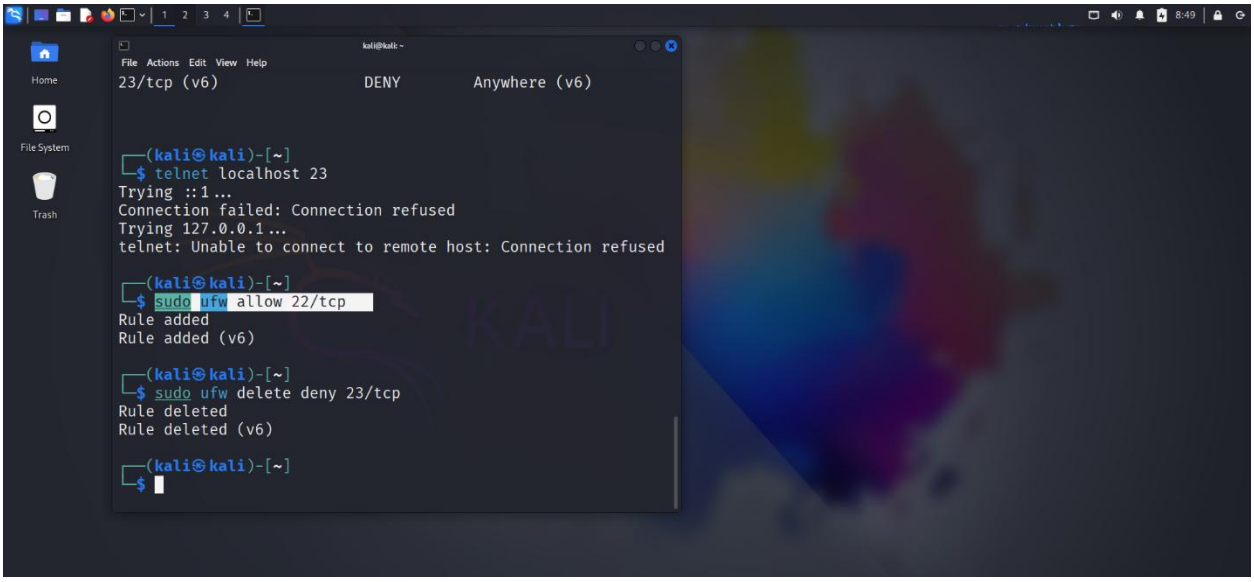
Verify **port 22** is accessible:

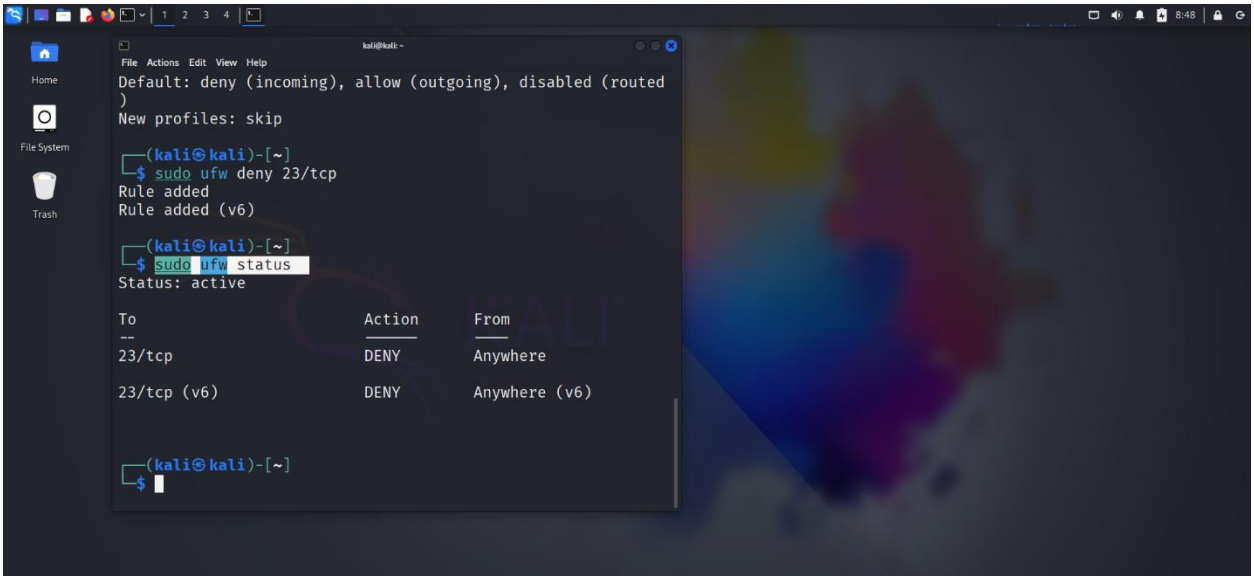
ssh user@localhost -p 22

Since SSH is **allowed**, the connection should be successful.









4.2 Using Firewalk for Firewall Analysis

Firewalk helps analyze how firewalls handle packets:

sudo apt-get install firewalk

firewalk -S 23 -D <target-IP>

This command checks whether packets sent to **port 23** are dropped, confirming firewall rules are applied correctly.

4.3 Using ftester for Firewall Simulation

Ftester helps simulate network packets:

```
sudo apt install ftester

ftest -c <source-IP>:23:<dest-IP>:23:S:TCP
```

This verifies **whether blocked ports are inaccessible** from external sources.

---

5. Firewall Functionality and Cybersecurity Insights

5.1 How Firewalls Operate

A **firewall** enforces security policies by filtering network packets. It can:

- **Block specific ports** to protect services from intrusion.
- **Allow essential traffic** for legitimate connections.
- **Inspect and filter packets** to enhance security.
- **Mitigate cyber threats** such as unauthorized access attempts.

5.2 Real-World Applications of Firewalls

Beyond personal computers, firewalls are widely used in:

1. **Corporate Networks:** Large enterprises use firewalls to secure internal communication.
2. **Cloud Security:** Cloud platforms like **AWS** and **Azure** utilize firewalls for traffic filtering.
3. **Penetration Testing:** Ethical hackers configure firewalls for **network security assessments**.

5.3 Observations from Firewall Testing

After implementing and testing firewall rules, several insights were gained:

- **Blocking Telnet successfully prevented insecure remote access.**
- **Allowing SSH enabled secure communication while restricting unnecessary access.**

- **Firewalk and ftester confirmed firewall efficiency by rejecting unauthorized packets.**

---

6. Conclusion

Firewalls are **essential** for securing systems from cyber threats. This report detailed the process of configuring, testing, and validating firewall rules using **UFW** on **Kali Linux**. The testing process confirmed the firewall's effectiveness in restricting unauthorized traffic while allowing essential services.

6.1 Final Recommendations

- Regularly review firewall rules to **adapt to evolving security threats**.
- Monitor logs (sudo ufw logging on) for suspicious activity.
- Implement additional security measures such as **intrusion detection systems (IDS)**.

Firewall protection should never be considered optional—it is a necessity for cybersecurity in today's interconnected world.
