# Firewall Configuration and Testing (Kali Linux)

Example System:

- OS: Kali Linux 2025  
- Firewall Tool: UFW (Uncomplicated Firewall)  
- Objective: Demonstrate firewall rule management — add, test, and remove rules safely

## 1. Open Firewall Configuration Tool

Kali Linux includes UFW but it’s disabled by default. Enable it first:

* sudo ufw enable

If it’s not installed:

* sudo apt install ufw -y

## 2. List Current Firewall Rules

To view the current status and active rules:

* sudo ufw status numbered  
    
  Status: active

## 3. Add Rule to Block Inbound Traffic on Port 23 (Telnet)

Telnet runs on port 23, which is considered insecure. Block it using:

* sudo ufw deny 23/tcp

Rule added  
Rule added (v6)

You can confirm it was added:

* sudo ufw status  
    
  Status: active

To Action From

-- ------ ----

23/tcp DENY Anywhere

23/tcp (v6) DENY Anywhere (v6)

## 4. Test the Rule

Now test whether port 23 is blocked.

Option 1: Using Telnet

* telnet 127.0.0.1 23

Trying 127.0.0.1...

telnet: Unable to connect to remote host: Connection refused

Option 2: Using Nmap

* sudo nmap -p 23 localhost  
    
  Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-26 18:25 IST

Nmap scan report for localhost (127.0.0.1)

Host is up (0.00016s latency).

Other addresses for localhost (not scanned): ::1

PORT STATE SERVICE

23/tcp closed telnet

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

## 5. Add Rule to Allow SSH (Port 22)

SSH is commonly used for remote administration and should be allowed:

* sudo ufw allow 22/tcp  
    
  Rule added

Rule added (v6)

Verify with:

* sudo ufw status  
    
  Status: active

To Action From

-- ------ ----

23/tcp DENY Anywhere

22/tcp ALLOW Anywhere

23/tcp (v6) DENY Anywhere (v6)

22/tcp (v6) ALLOW Anywhere (v6)

## 6. Remove the Test Block Rule

After verifying your test, remove the Telnet block rule:

* sudo ufw delete deny 23/tcp  
    
  Rule deleted

Rule deleted (v6)

Then check again:

* sudo ufw status  
    
  Status: active

To Action From

-- ------ ----

22/tcp ALLOW Anywhere

22/tcp (v6) ALLOW Anywhere (v6)

## 7. Documentation of Commands Used

|  |  |
| --- | --- |
| **Action** | **Command** |
| Enable Firewall | sudo ufw enable |
| List Rules | sudo ufw status numbered |
| Block Telnet Port 23 | sudo ufw deny 23/tcp |
| Allow SSH Port 22 | sudo ufw allow 22/tcp |
| Test Port | telnet 127.0.0.1 23 or sudo nmap -p 23 localhost |
| Delete Rule | sudo ufw delete deny 23/tcp |

## 8. Summary — How Firewall Filters Traffic

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on pre-set rules.  
- Inbound filtering: Controls data packets coming into your system.  
- Outbound filtering: Controls packets going out of your system.  
- Allow rules: Permit safe connections (e.g., SSH on port 22).  
- Deny rules: Block insecure or unused services (e.g., Telnet on port 23).  
- Default policy: Can be set to allow or deny traffic if no specific rule matches.  
  
In short, firewalls act like security guards, filtering traffic to protect your system from unauthorized access.