# Firewall Configuration and Testing

## Introduction

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predefined security rules. It acts as a protective barrier between trusted internal networks and untrusted external networks such as the internet. Firewalls help prevent unauthorized access, cyber attacks, and data breaches.

## Tools Used

- UFW (Uncomplicated Firewall) – Linux (Ubuntu / Kali)

## Firewall Concepts

- **Inbound Traffic**: Data entering the system
- **Outbound Traffic**: Data leaving the system
- **Allow Rule**: Permits specific network traffic
- **Deny Rule**: Blocks unauthorized traffic
- **Port**: Communication endpoint (e.g., 22 for SSH, 80 for HTTP)
- **IP Address**: Unique identifier of a device on a network

## Firewall Configuration Steps

### Enable Firewall (UFW)

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

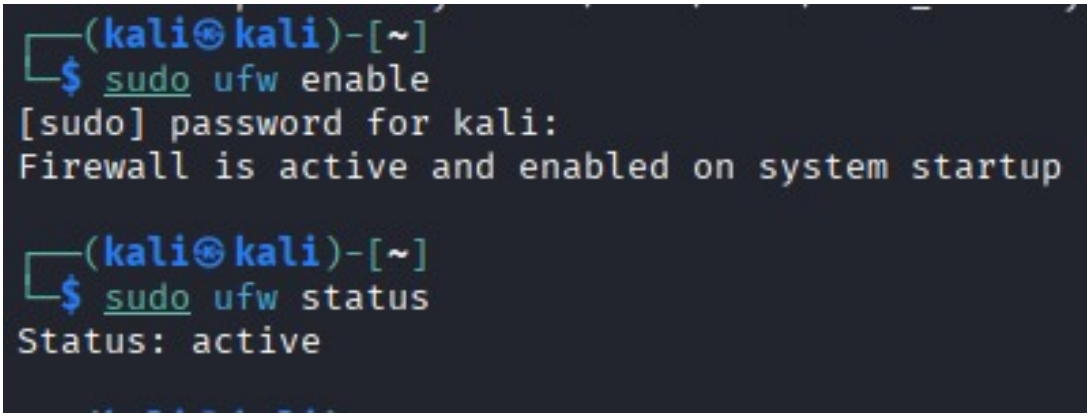


Figure 1: Enabling UFW and Checking Firewall Status

## Configure Firewall Rules

Allow SSH (Port 22):

```
sudo ufw allow 22
```

Allow HTTP (Port 80):

```
sudo ufw allow 80
```

Deny FTP (Port 21):

```
sudo ufw deny 21
```

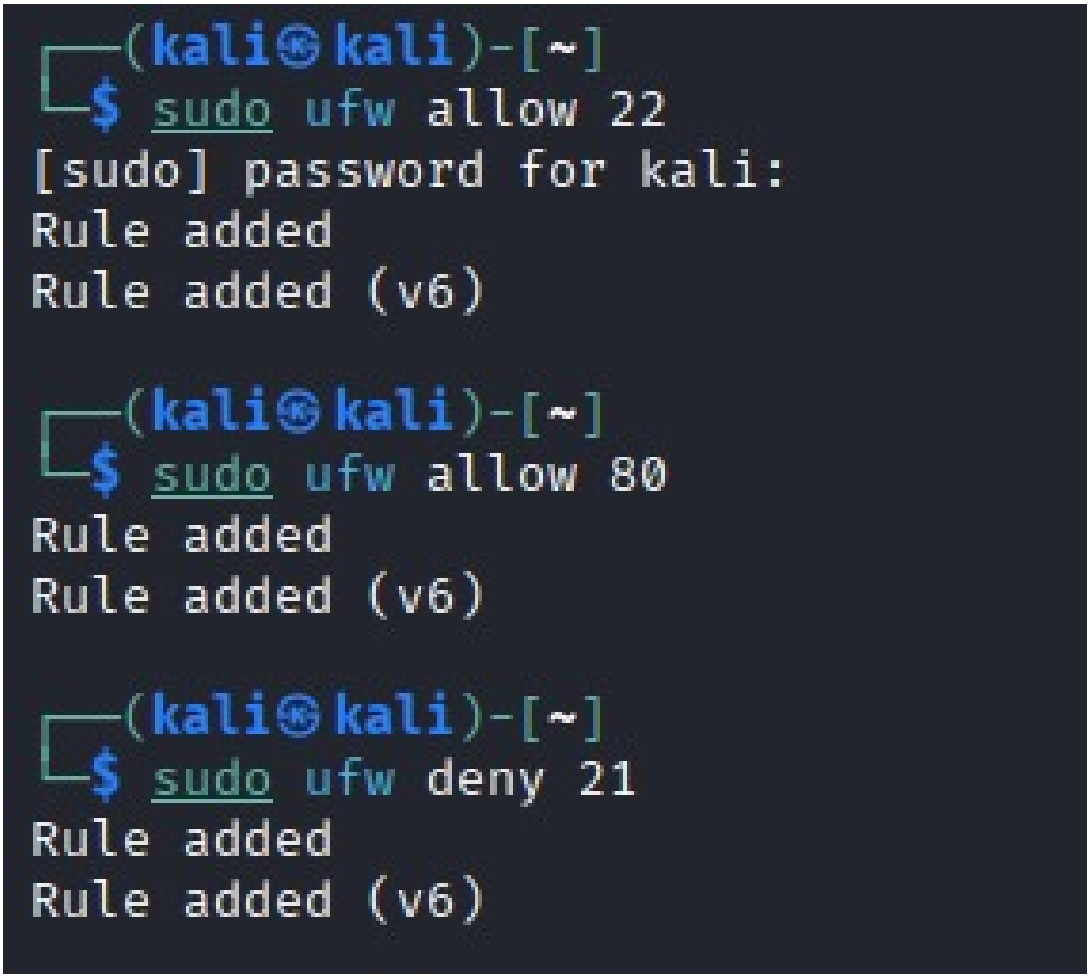


Figure 2: Configuring Allow and Deny Firewall Rules

### Allow or Deny Specific Ports

Allow a range of ports:

```
sudo ufw allow 1000:2000/tcp
```

Block Telnet (Port 23):

```
sudo ufw deny 23
```

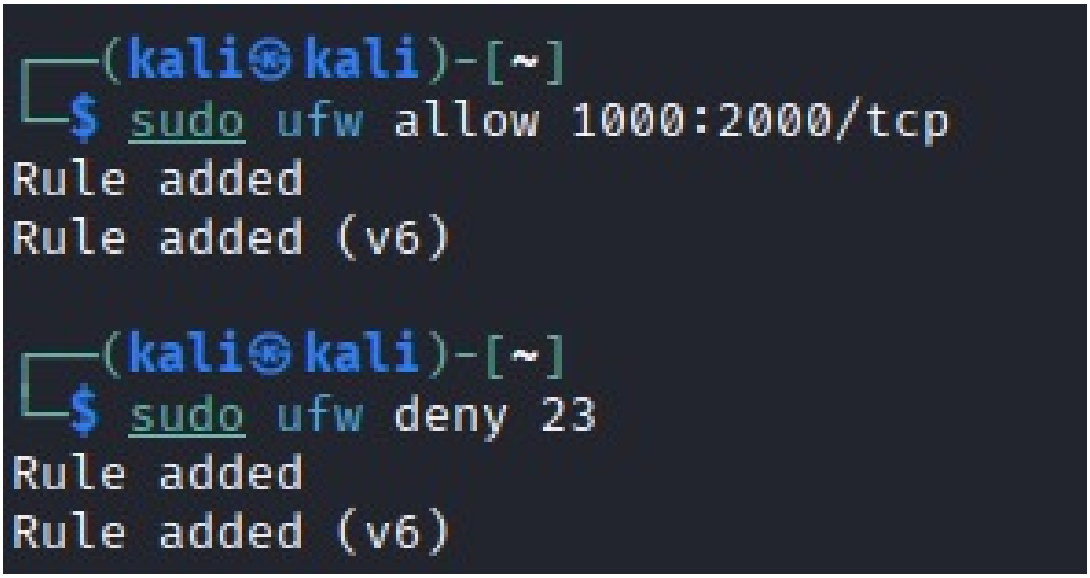


Figure 3: Allowing Port Range and Blocking Telnet Port

## Testing Connectivity

Test network connectivity using ping:

```
ping google.com
```

Scan open ports using Nmap:

```
nmap localhost
```

Allowed ports appear as *open* and blocked ports appear as *filtered or closed*.

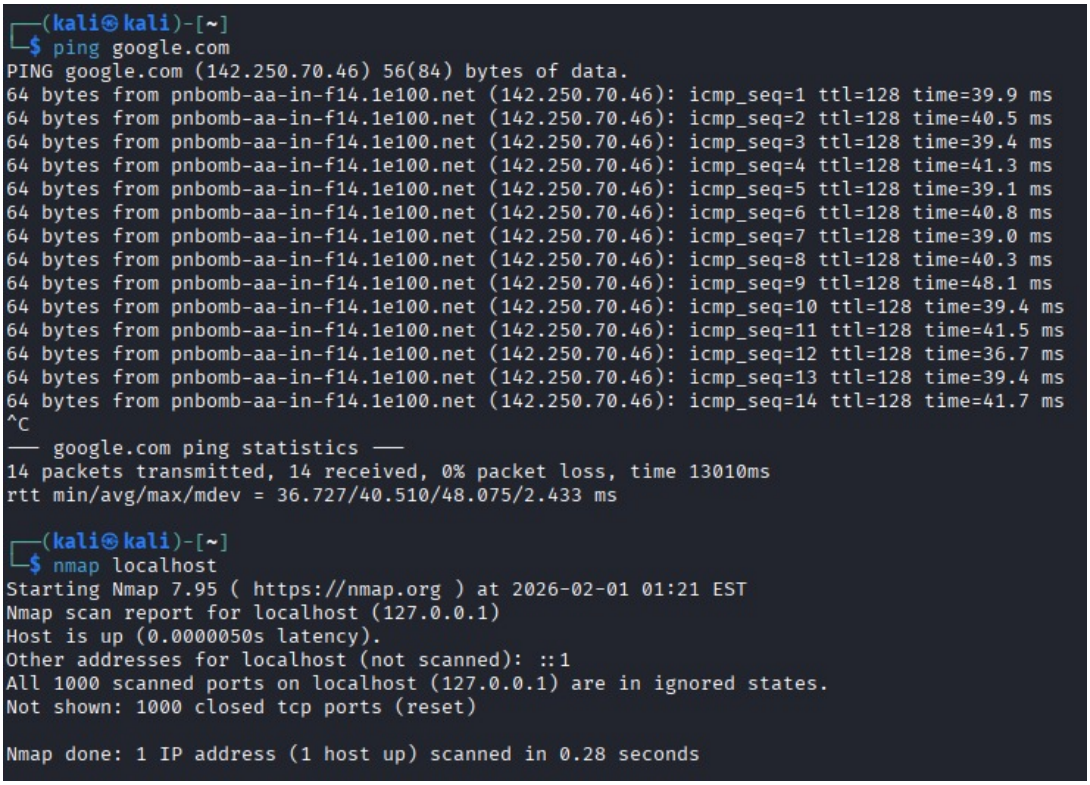


Figure 4: Testing Firewall Rules Using Ping and Nmap

## Firewall Logging

Enable logging:

```
sudo ufw logging on
```

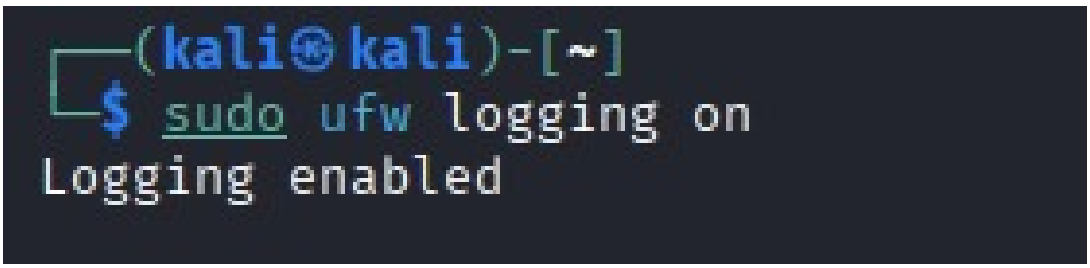


Figure 5: Firewall Log Monitoring

## Blocking Malicious IP Addresses

Block a specific IP address:

```
sudo ufw deny from 192.168.1.100
```

Block an entire subnet:

```
sudo ufw deny from 192.168.1.0/24
```

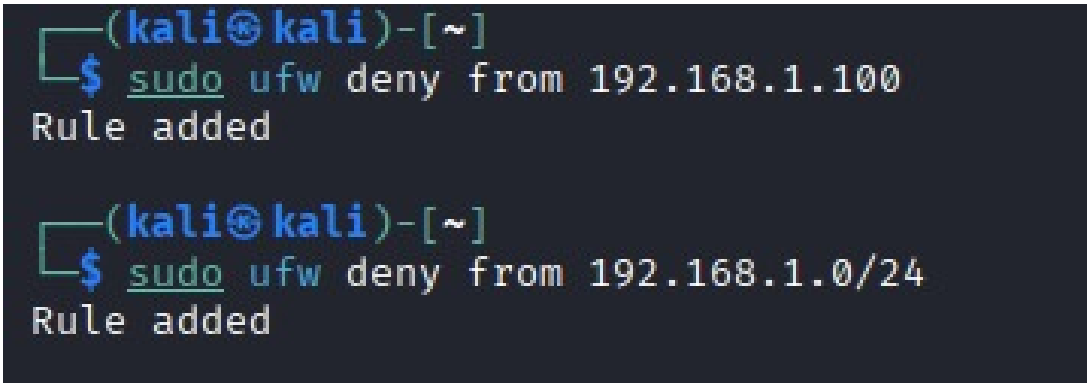


Figure 6: Blocking Malicious IP Address and Subnet

### Documenting Firewall Rules

List all firewall rules:

```
sudo ufw status numbered
```

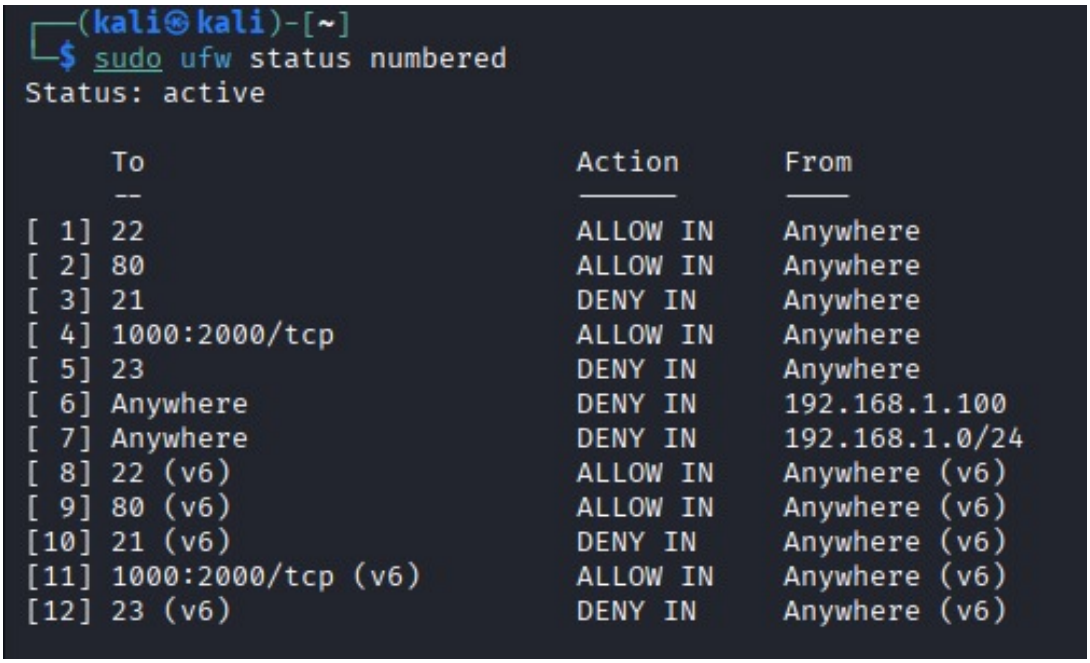


Figure 7: Documenting Firewall Rules

Firewall documentation should include allowed ports, blocked ports, blocked IP addresses, and the purpose of each rule.

## Impact of Firewall Rules

| Rule | Impact |
|---|---|
| Allow SSH (22) | Enables secure remote administration |
| Block FTP (21) | Prevents insecure file transfers |
| Block malicious IP | Protects against attacks and brute-force attempts |
| Enable logging | Helps monitor and analyze security events |

## Windows Firewall Testing (Brief)

Windows Defender Firewall allows users to configure inbound and outbound rules through the Advanced Security settings. Specific ports and applications can be allowed or blocked, and connectivity can be tested using Command Prompt or web browsers.

## Conclusion

Firewall configuration and testing are essential security practices for protecting systems and networks. Properly configured firewall rules, regular testing, log monitoring, and documentation significantly improve an organization's security posture.