Firewall Configuration Report: UFW on Kali Linux

1. Introduction

This report documents UFW (Uncomplicated Firewall) configuration on Kali Linux VM. The objective was to learn basic firewall management, create rules to allow/block network traffic, test those rules, and understand traffic filtering mechanisms.

2. Environment Setup

- Operating System: Kali Linux 6.12.38+kali-arm64 (VM)
- Firewall Tool: UFW (Uncomplicated Firewall)
- User: jeff@kali
- Test Date: October 25, 2025

3. Initial Firewall Status

Command: sudo ufw status
Result: Firewall was inactive with no configured rules.

4. Configuration Steps

Step 1: Enable UFW
Command: sudo ufw enable
Result: "Firewall is active and enabled on system startup"

Step 2: Deny Telnet Traffic (Port 23)
Commands:

- sudo ufw deny 23
- sudo ufw deny 23/tcp (IPv6)

Result: Rule added for both IPv4 and IPv6
Purpose: Block insecure Telnet protocol to prevent unencrypted remote access

Step 3: Allow SSH Traffic (Port 22)
Commands:

- sudo ufw allow 22
- sudo ufw allow 22/tcp (IPv6)

Result: Rule added for both IPv4 and IPv6
Purpose: Allow secure SSH connections for remote administration

Step 4: View Active Rules
Command: sudo ufw status numbered

Result:

```
[1] 23        DENY IN    Anywhere
[2] 22        ALLOW IN   Anywhere
[3] 23 (v6)   DENY IN    Anywhere (v6)
[4] 22 (v6)   ALLOW IN   Anywhere (v6)
```

5. Testing Firewall Rules

Test 1: Telnet Connection (Port 23)
Command: telnet 127.0.0.1 23
Result: "Unable to connect to remote host: Connection refused"
Conclusion: Firewall successfully blocked Telnet on port 23 ✓

Test 2: SSH Connection (Port 22)
Command: ssh localhost
Result: Successfully connected and authenticated
Conclusion: Firewall allowed SSH on port 22 ✓

Test 3: Verify Firewall Status
Command: sudo ufw status verbose

Result:

```
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
```

6. How UFW Filters Traffic

Packet Filtering:

- Inspects incoming/outgoing network packets
- Checks packets against configured rules in order
- First matching rule determines allow/deny action

Default Policies:

- Incoming: DENY (blocks unsolicited connections)
- Outgoing: ALLOW (permits outbound connections)
- Routed: DISABLED (no packet forwarding)

Rule Processing:

- Rules processed in numerical order (1, 2, 3...)
- First match wins
- Port-specific rules for TCP/UDP protocols
- Separate handling for IPv4 and IPv6

7. Key Commands Reference

Firewall Control:

- sudo ufw enable - Activate firewall
- sudo ufw disable - Deactivate firewall
- sudo ufw status - Check status
- sudo ufw status numbered - List rules with numbers
- sudo ufw status verbose - Detailed information

Rule Management:

- sudo ufw allow [port] - Allow traffic on port
- sudo ufw deny [port] - Block traffic on port
- sudo ufw delete [number] - Remove rule by number

Testing:

- telnet [host] [port] - Test port connectivity
- ssh [host] - Test SSH connection

8. Screenshots

All configuration steps and test results captured in terminal screenshots:

- Initial firewall status
- UFW enable command
- Adding deny/allow rules
- Numbered rule listing
- Failed Telnet test
- Successful SSH test
- Verbose status output

[Screenshots uploaded to GitHub repository]

9. Conclusion

Key Learnings:

Firewall Management:
- Successfully configured UFW on Linux system
- Created ALLOW and DENY rules for specific ports
- Verified functionality through connection testing
- Learned status checking and rule viewing commands

Traffic Filtering:
- Understood packet inspection and rule application
- Learned default policies (deny incoming, allow outgoing)
- Recognized importance of allowing essential services (SSH) while blocking insecure ones (Telnet)

Port Knowledge:
- Port 22: SSH (secure remote access) - allowed
- Port 23: Telnet (insecure plaintext) - blocked
- Different ports serve different services with different security requirements

Security Practices:
- Default deny policy minimizes attack surface
- Only needed services should be explicitly allowed
- Regular firewall audits are important
- Logging helps track connection attempts

Practical Takeaway:
Firewalls are the first line of defense in network security. They prevent unauthorized access while allowing legitimate traffic. Understanding firewall configuration is essential for system administrators and security professionals.