UFW Installation and Configuration Report

Executive Summary

This report documents a UFW (Uncomplicated Firewall) installation and configuration session performed on a Kali Linux system. The session demonstrates successful firewall installation, rule configuration, testing, and rule management operations.

System Information

- **Operating System**: Kali Linux (kali-rolling distribution)
- **UFW Version**: 0.36.2-9
- **Architecture**: amd64
- **Database Status**: 547,721 files and directories currently installed

Installation Process

Package Installation

The UFW installation was initiated and completed successfully with the following characteristics:

- **Download Size**: 169 kB
- **Installation Space**: 880 kB (out of 37.1 GB available)
- **Download Speed**: 230 kB/s
- **Source Repository**: http://kali.download/kali kali-rolling/main

Configuration Files Created

During installation, UFW automatically created several configuration files:

- /etc/ufw/before.rules - IPv4 rules applied before user rules
- /etc/ufw/before6.rules - IPv6 rules applied before user rules
- /etc/ufw/after.rules - IPv4 rules applied after user rules
- /etc/ufw/after6.rules - IPv6 rules applied after user rules

System Integration

- **Service Integration**: Successfully created systemd service symlink
- **Auto-start**: Enabled UFW service for system startup
- **Menu Integration**: Updated Kali menu system
- **Documentation**: Updated man page database

Firewall Configuration

Default Policy Settings

UFW was configured with the following default policies:

- **Incoming Traffic**: DENY (blocked by default)
- **Outgoing Traffic**: ALLOW (permitted by default)
- **Routed Traffic**: DENY (forwarding blocked)
- **Logging**: Enabled (low level)
- **New Profiles**: Skip

Rule Configuration Testing

Rule Addition

A specific deny rule was added for Telnet service:

sudo ufw deny 23/tcp

This command resulted in:

- IPv4 rule creation (Rule #1)
- IPv6 rule creation (Rule #2)
- Both rules configured to deny incoming TCP traffic on port 23

Connectivity Testing

Network connectivity tests were performed using netcat (nc):

1. **Localhost Test**: nc -v 127.0.0.1 23
    - Result: Connection refused
    - Expected behavior for blocked service
2. **Remote Host Test**: nc -v 192.168.1.5 23
    - Result: Connection refused with inverse DNS lookup failure
    - Confirms rule effectiveness across network interfaces

Rule Management Operations

Rule Verification

Multiple status checks were performed using:

sudo ufw status numbered

This provided numbered rule listings for easy management and verification.

Rule Deletion

Demonstrated selective rule removal:

- Deleted IPv6 rule (Rule #2) using: sudo ufw delete 2
- Confirmed deletion with user prompt
- Maintained IPv4 rule (Rule #1) intact

Security Analysis

Positive Security Aspects

1. **Default Deny Policy**: Implements security best practice of denying incoming connections by default
2. **Dual-Stack Protection**: Automatically configured both IPv4 and IPv6 rules
3. **Service Integration**: Properly integrated with systemd for automatic startup
4. **Logging Enabled**: Provides audit trail for security events
5. **Rule Granularity**: Supports specific port and protocol targeting

Configuration Recommendations

1. **Logging Level**: Consider increasing from "low" to "medium" for better visibility
2. **Rule Documentation**: Implement comments for complex rules to aid future management
3. **Regular Auditing**: Establish periodic review schedule for firewall rules
4. **Backup Strategy**: Consider backing up UFW configuration before major changes

Technical Observations

Installation Efficiency

- Clean installation with no dependency conflicts
- Minimal disk space impact (880 kB)
- Fast download and installation process
- No system restart required

Rule Behavior

- Rules apply immediately upon creation
- IPv6 support is automatically included
- Numbered rule system facilitates easy management
- Deletion operations require confirmation for safety

Conclusion

The UFW installation and configuration session completed successfully, demonstrating:

- Proper package installation and system integration
- Effective rule creation and testing methodology
- Successful rule management and deletion procedures
- Confirmation of firewall effectiveness through connectivity testing

The firewall is now active and properly configured with appropriate default policies and demonstrates the administrator's competency in basic firewall management operations.

Recommendations for Next Steps

1. Configure additional service-specific rules as needed
2. Implement application-specific profiles
3. Set up log monitoring and analysis
4. Document firewall policy and procedures
5. Consider integration with intrusion detection systems


sudo ufw status numbered
Status: active
(jeryston㉿kali)-[~]
$ sudo ufw status numbered
Status: active
(jeryston㉿kali)-[~]
$ sudo ufw deny 23/tcp
Rule added
Rule added (v6)
(jeryston㉿kali)-[~]
$ sudo ufw status numbered
Status: active
To Action From
-- ------ ----
[1] 23/tcp DENY IN Anywhere
[2] 23/tcp (v6) DENY IN Anywhere (v6)
(jeryston㉿kali)-[~]
$ nc -v 127.0.0.1 23
localhost [127.0.0.1] 23 (telnet) : Connection refused
(jeryston㉿kali)-[~]
$ nc -v 192.168.1.5 23
192.168.1.5: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.1.5] 23 (telnet) : Connection refused
(jeryston㉿kali)-[~]
$ sudo ufw status numbered
Status: active
To Action From
-- ------ ----
[1] 23/tcp DENY IN Anywhere
[2] 23/tcp (v6) DENY IN Anywhere (v6)
(jeryston㉿kali)-[~]
$ sudo ufw delete 2
Deleting:
deny 23/tcp
Proceed with operation (y|n)? y
Rule deleted (v6)
(jeryston㉿kali)-[~]
$