Firewall Configuration Documentation

Last Updated: 27/06/2025

1. Introduction

This document provides a comprehensive guide to configuring and managing firewall rules using both command-line (CLI) and graphical (GUI) methods on Linux systems.

Supported Tools:

- UFW (Uncomplicated Firewall) - Default on Ubuntu/Debian
- GUFW - GUI for UFW
- iptables - Traditional Linux firewall
- firewalld - Used in RHEL/CentOS/Fedora

2. Command-Line (CLI) Configuration

2.1 Basic UFW Commands

Command	Description
sudo ufw enable	Enable the firewall
sudo ufw disable	Disable the firewall
sudo ufw reset	Reset all rules to default
sudo ufw status	Show current rules
sudo ufw status verbose	Detailed rule listing
sudo ufw status numbered	Rules with numbers (for deletion)

2.2 Rule Management

| Command | Description |

sudo ufw allow 22/tcp	Allow SSH (Port 22)
sudo ufw deny 23/tcp	Block Telnet (Port 23)
sudo ufw allow from 192.168.1.10	Allow traffic from a specific IP
sudo ufw delete deny 23/tcp	Remove a rule

2.3 Logging & Troubleshooting

Command	Description
sudo ufw logging on	Enable firewall logging
sudo ufw logging medium	Set logging level (low, medium, high, full)
sudo tail -f /var/log/ufw.log	View live firewall logs
sudo grep -i ufw /var/log/syslog	Check system logs for UFW activity

3. Graphical (GUI) Configuration

3.1 GUFW (UFW GUI) Setup

Installation:

```
sudo apt install gufw  # Debian/Ubuntu/Kali
```

Basic Usage:

1. Open GUFW:

- GUI: Search "Firewall" in applications

- Terminal: sudo gufw

2. Toggle firewall: On/Off

3. Default policies:

- Incoming: Deny (recommended)

- Outgoing: Allow

4. Add rules:

- Click "+" -> Choose Predefined/Simple/Advanced

- Example:

- Action: Allow

- Port: 80 (HTTP)

- Protocol: TCP

- Direction: In

Logging in GUFW:

- Go to "Reports" tab

- Filter logs by date, severity, or rule

4. Example Configuration Workflow

Scenario:

- Allow SSH (22), HTTP (80), HTTPS (443)

- Block Telnet (23)

CLI Method:

```
sudo ufw enable

sudo ufw allow 22/tcp

sudo ufw allow 80/tcp

sudo ufw allow 443/tcp

sudo ufw deny 23/tcp

sudo ufw status numbered
```

GUI Method (GUFW):

1. Open GUFW -> Turn On

2. Click "+" -> Simple

- Action: Allow | Port: 22 | Protocol: TCP | Direction: In

3. Repeat for 80 (HTTP) and 443 (HTTPS)

4. Add Deny rule for 23 (Telnet)

5. Verify in the rules list

5. Logging & Troubleshooting

5.1 Checking Firewall Logs

```
sudo tail -f /var/log/ufw.log

sudo grep -i ufw /var/log/syslog

sudo dmesg | grep -i firewall
```

5.2 Common Issues & Fixes

Issue	Solution
ufw.log missing?	Run sudo ufw logging on
Locked out after enabling UFW?	Use physical console or reboot into recovery mode
Rules not applying?	Restart UFW: sudo ufw disable && sudo ufw enable

6. Conclusion

This document covers CLI (UFW/iptables) and GUI (GUFW) methods for firewall management.