

# **Firewalld (Linux) - Firewall Implementation and Security Testing**

## **Project Report**

## **Table of Contents**

1. Introduction
2. Objectives of the Project
3. Overview of Firewall
4. Installation and Setup
5. Firewall Configuration and Management
6. Security Features of Firewall
7. Firewall Testing and Security Validation
8. Troubleshooting and FAQs
9. Future Enhancements
10. Conclusion

---

## 1. Introduction

In today's digital world, security is a top priority for both individual users and enterprises. Cyber threats such as unauthorized access, data breaches, and malicious attacks pose serious risks to any system connected to the internet. To mitigate these risks, firewalls play a critical role in managing network traffic and preventing unauthorized access.

**Firewalld** is a modern firewall management tool for Linux systems that provides a **dynamic and customizable firewall** solution. It acts as an interface for **iptables**, offering an easy-to-use command-line utility and support for **zones, services, and rules** to regulate incoming and outgoing traffic.

This report focuses on **Firewalld implementation, configuration, security testing, and troubleshooting techniques** to help users secure their Linux environments effectively.

---

## 2. Objectives of the Project

The primary objectives of this project are:

- ✓ **Understanding Firewalld** – Learn about Firewalld as a Linux firewall tool and how it works.
  - ✓ **Implementation** – Install and configure Firewalld on a Linux system.
  - ✓ **Security Testing** – Evaluate Firewalld's effectiveness in blocking unauthorized access and malicious activities.
  - ✓ **Troubleshooting** – Identify and resolve common issues related to Firewalld.
  - ✓ **Enhancement & Future Scope** – Explore possible improvements and additional security measures.
- 

## 3. Overview of Firewalld

### What is Firewalld?

Firewalld is a **dynamic firewall management tool** used in Linux operating systems, replacing older firewall tools like iptables. It provides:

- **Support for firewall zones** to define different levels of security.
- **Easy rule management** for services and ports.
- **Runtime and permanent configurations**, allowing instant updates without restarting the firewall.
- **IPv4 and IPv6 support** for modern networking environments.
- **Integration with security tools** like SELinux and Fail2Ban for enhanced protection.

### How Firewalld Works

Firewalld manages firewall rules using **zones**, which define different levels of trust for networks. Each network interface is assigned a zone, which then controls the traffic flow.

Example zones include:

- **Public:** For untrusted networks with strict rules.
  - **Home/Work:** For trusted internal networks with relaxed rules.
  - **DMZ (Demilitarized Zone):** For public-facing services like web and mail servers.
  - **Trusted:** Allows all incoming and outgoing connections.
- 

## 4. Installation and Setup

### Step 1: Install Firewalld

For **RHEL, CentOS, Fedora**:

```
sudo yum install firewalld -y
```

For **Ubuntu, Debian**:

```
sudo apt install firewalld -y
```

### Step 2: Start and Enable Firewalld

```
sudo systemctl start firewalld
```

```
sudo systemctl enable firewalld
```

### Step 3: Check Firewalld Status

```
sudo firewall-cmd --state
```

If Firewalld is running, it should return:

Running

---

## 5. Firewall Configuration and Management

### Adding Firewall Rules

To allow **SSH (port 22)** permanently:

```
sudo firewall-cmd --permanent --add-service=ssh
```

```
sudo firewall-cmd --reload
```

To allow **HTTP (port 80)** and **HTTPS (port 443)**:

```
sudo firewall-cmd --permanent --add-service=http
```

```
sudo firewall-cmd --permanent --add-service=https
```

```
sudo firewall-cmd --reload
```

### Blocking a Specific IP Address

To block traffic from an IP address (e.g., 192.168.1.100):

```
sudo firewall-cmd --permanent --add-rich-rule='rule family="ipv4" source address="192.168.1.100" drop'
```

```
sudo firewall-cmd --reload
```

### Port Forwarding (NAT Configuration)

To forward **external port 8080 to internal port 80**:

```
sudo firewall-cmd --permanent --add-forward-port=port=8080:proto=tcp:toport=80
```

```
sudo firewall-cmd --reload
```

---

## 6. Security Features of Firewall

Firewalld enhances security through the following features:

- **Zone-Based Security:** Segregates traffic based on trust levels.
- **Service Management:** Allows/block services dynamically.
- **Rich Rules:** Enables fine-grained traffic filtering.
- **Logging & Monitoring:** Tracks network activities for security audits.
- **Integration with SELinux:** Enhances access control.

---

## 7. Firewall Testing and Security Validation

## 1. Checking Open Ports

To verify active firewall rules and open ports:

```
sudo firewall-cmd --list-all
```

## 2. Testing Blocked IPs

If an IP (e.g., 192.168.1.100) is blocked, it should not be able to connect. To test:

```
ping 192.168.1.100
```

Expected Output:

Request timed out.

## 3. Port Scanning with Nmap

Run an **Nmap scan** to check which ports are open:

```
nmap -p 1-65535 localhost
```

---

## 8. Troubleshooting and FAQs

### Common Issues & Solutions



Issue	Possible Cause	Solution
firewalld: command not found	Firewalld not installed	Install using yum or apt
Firewall rules not working	Misconfigured settings	Restart firewall: <code>firewall-cmd --reload</code>
Can't access SSH	Port 22 blocked	Allow SSH: <code>firewall-cmd --add-service=ssh</code>

For more solutions, check **TROUBLESHOOTING.md** in the repository.

---

## 9. Future Enhancements

- 🚀 **Automated Firewall Rule Management** – Develop scripts for auto-configuration.
- 🚀 **Integration with Security Tools** – Link Firewalld with IDS/IPS for real-time monitoring.

-  **Cloud Firewall Support** – Expand Firewallld rules to secure cloud deployments.
  -  **Web-Based GUI** – Implement a graphical interface for easier management.
- 

## 10. Conclusion

Firewalld is a **powerful, flexible, and easy-to-use** firewall management tool for Linux. It simplifies the process of securing a network by offering **zone-based configurations, service management, and rich rules**.

By implementing Firewalld, administrators can **effectively control incoming and outgoing traffic, block unauthorized access, and monitor security threats**. Through **proper configuration, testing, and troubleshooting**, Firewalld ensures robust network protection against cyber threats.

This project provides a **detailed step-by-step guide** to setting up Firewalld, configuring security rules, and testing its effectiveness. As cybersecurity threats continue to evolve, **enhancing firewall capabilities with additional security layers** will be essential for maintaining a secure network environment.

---

## References

1. **Official Firewalld Documentation:** <https://firewalld.org/documentation/>
2. **Linux Firewall Guide:** <https://linuxhandbook.com/firewalld/>
3. **RedHat Firewalld Security Guide:** [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/)

 For any questions or contributions, visit our GitHub repository!