Configuring and Testing Firewall Rules on Linux Using UFW

Configuring and Testing Firewall Rules on Linux Using UFW

Introduction

This report provides a clear step-by-step guide on how to configure and test firewall rules on a Linux system using UFW (Uncomplicated Firewall). UFW is a user-friendly front-end for managing iptables firewall rules, simplifying the process of securing network traffic.

Step-by-Step Guide

1. Open Firewall Configuration Tool

Open the terminal to interact with the firewall configuration.

Ctrl + Alt + T

2. List Current Firewall Rules

Check the currently active firewall rules with numbered identifiers.

sudo ufw status numbered

3. Add a Rule to Block Inbound Traffic on Port 23 (Telnet)

Block incoming connections on port 23 to prevent Telnet access.

sudo ufw deny 23

Verify the rule was added:

```
sudo ufw status numbered
```

4. Test the Rule

Test if port 23 is blocked by trying to connect locally using netcat.

```
nc -vz localhost 23
```

Expected result:

Connection refused or timed out - indicating the port is blocked.

If nc is not installed, install it with:

```
sudo apt install netcat -y
```

5. Add Rule to Allow SSH (Port 22)

Ensure SSH traffic is allowed for remote management.

```
sudo ufw allow 22/tcp
```

6. Remove the Test Block Rule to Restore Original State

1. List rules to find the rule number blocking port 23:

```
sudo ufw status numbered
```

2. Delete the blocking rule (replace X with the rule number):

```
sudo ufw delete X
```

3. Confirm the rule was removed:

```
sudo ufw status
```

Summary - How UFW Filters Traffic

- UFW simplifies management of iptables firewall rules.
- It filters network traffic based on ports, protocols (TCP/UDP), directions (inbound/outbound), and IP addresses.
- Rules are either allow or deny to control access, improving system security by blocking unwanted traffic.

If needed, I can also provide you a ready-to-run script automating these commands.