Table of Contents

Cybersecurity Practical Lab

Kali Linux Firewall Hardening Using GUFW (Graphical User Interface)

written by Haya Alibrahim

Introduction

This project demonstrates practical firewall hardening on a Kali Linux virtual machine using the GUFW graphical user interface. The main objective is to strengthen system security by managing firewall rules, reducing unnecessary network exposure, enabling logging, and validating security behavior through real-time monitoring.

Instead of relying only on command-line tools, this project focuses on user-friendly firewall management using a graphical interface. This approach reflects real-world environments where system administrators and security analysts often use visual tools for configuration, monitoring, and troubleshooting.

The project simulates an insecure configuration by opening multiple ports and allowing unrestricted access. These insecure settings are then mitigated by applying strict firewall rules such as restricting SSH access to the internal network, blocking insecure legacy services, enabling logging, and organizing firewall rule priorities. Each step is documented using screenshots and verification checks.

In addition, troubleshooting scenarios such as package dependency conflicts and system service restarts were handled and documented to demonstrate real-world problem-solving skills. The final result is a hardened firewall configuration with clear documentation that can be reused as a learning reference or operational guide.

Environment Setup

This project was implemented on a Kali Linux virtual machine running on a desktop environment. The system was configured with internet access and administrative privileges to allow firewall configuration.

The GUFW application was installed and used as the primary graphical firewall management tool. All configurations were performed through the graphical interface to simulate real-world administrative workflows.

Tool Overview (GUFW)

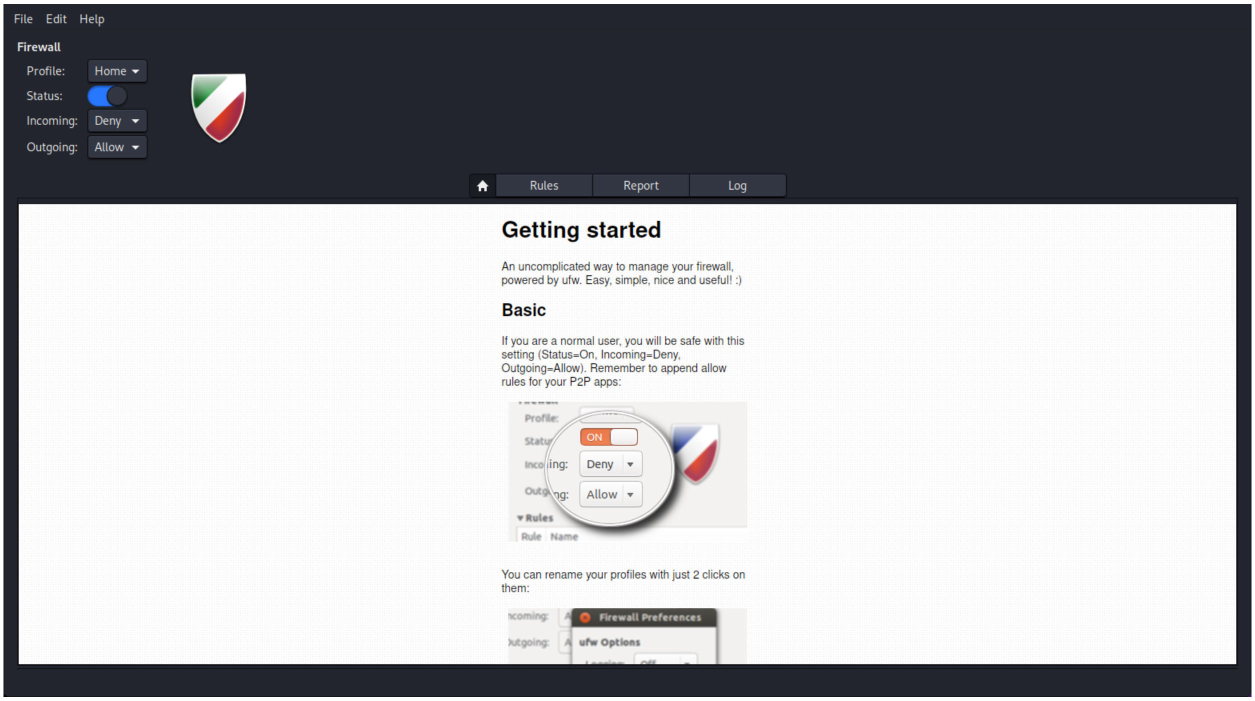
GUFW is a graphical front-end for the Uncomplicated Firewall (UFW). It provides an easy-to-use interface for managing firewall rules, enabling and disabling the firewall, monitoring logs, and managing security profiles without relying heavily on command-line operations.

GUFW allows administrators to:

- Create and manage firewall rules.
- Enable logging and traffic monitoring.
- Configure default security policies.
- Apply profiles for different environments.

Firewall Hardening Steps

4.1 Launching the GUFW Firewall Interface



Firewall

Profile: Home

Status:

Incoming: Deny

Outgoing: Allow

Getting started

An uncomplicated way to manage your firewall, powered by ufw. Easy, simple, nice and useful! :)

Basic

If you are a normal user, you will be safe with this setting (Status=On, Incoming=Deny, Outgoing=Allow). Remember to append allow rules for your P2P apps:

Profile:

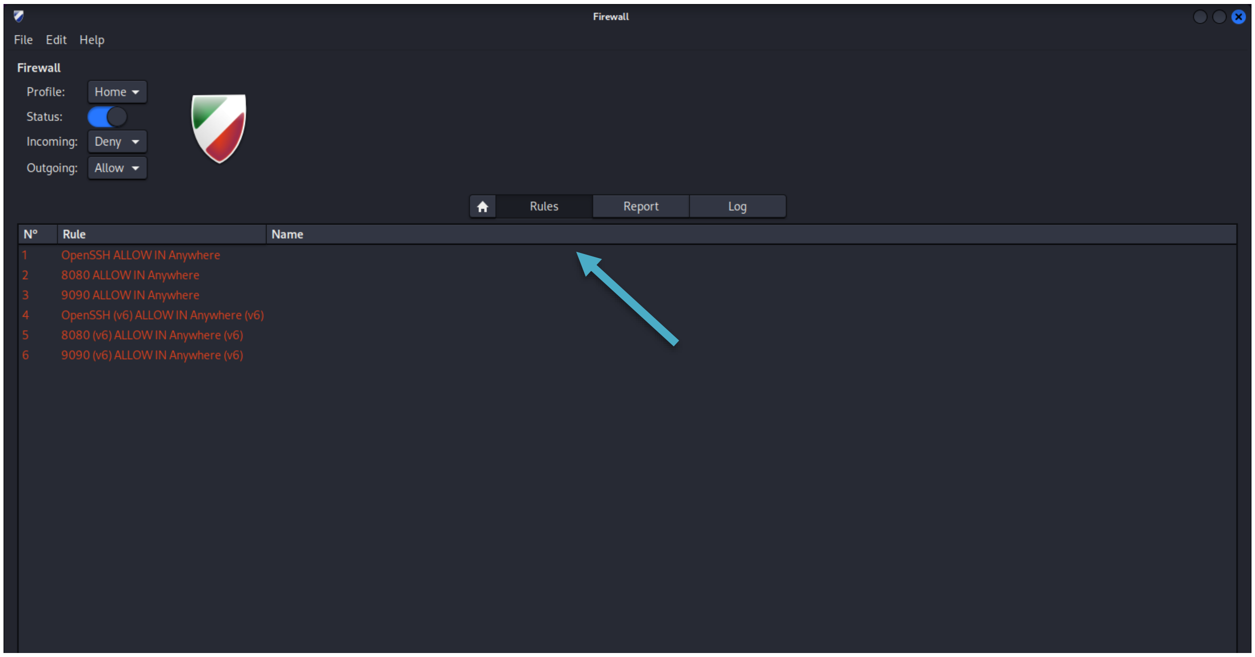
Status: ON

Incoming: Deny

Outgoing: Allow

You can rename your profiles with just 2 clicks on them:

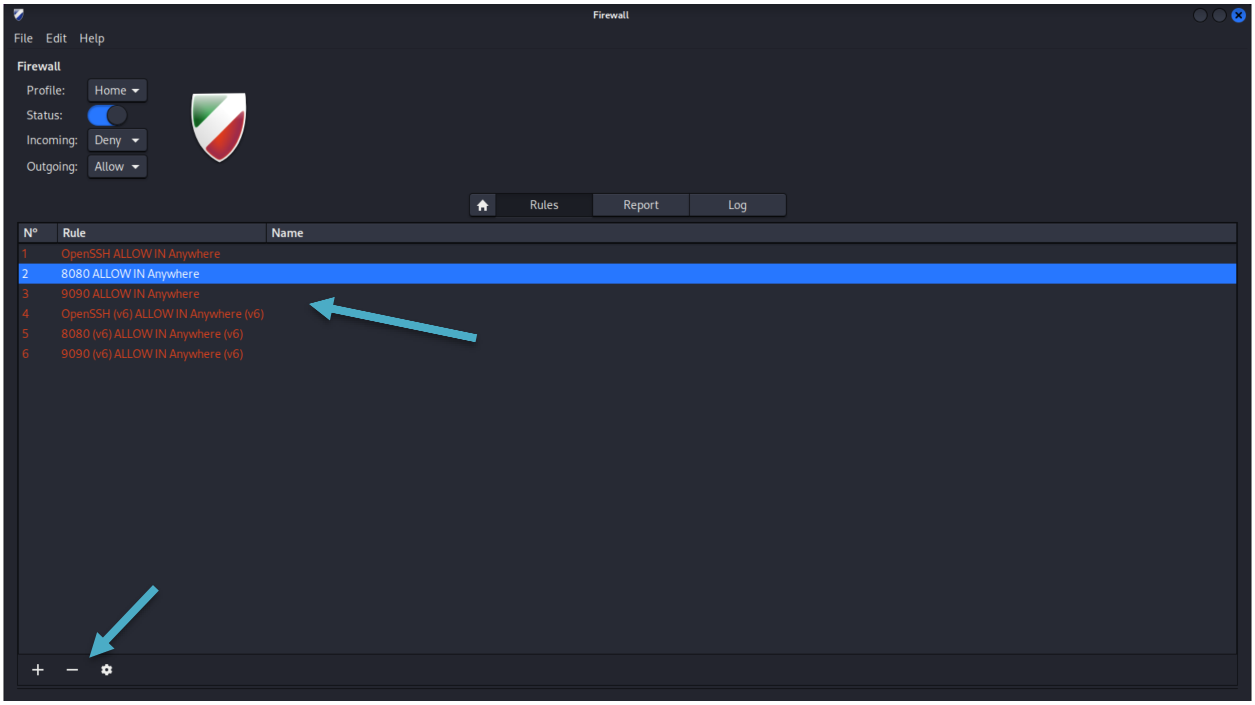
4.2 Viewing Current Firewall Rules



Profile: Home
Status: on
Incoming: Deny
Outgoing: Allow

Nº	Rule	Name
1	OpenSSH ALLOW IN Anywhere	
2	8080 ALLOW IN Anywhere	
3	9090 ALLOW IN Anywhere	
4	OpenSSH (v6) ALLOW IN Anywhere (v6)	
5	8080 (v6) ALLOW IN Anywhere (v6)	
6	9090 (v6) ALLOW IN Anywhere (v6)	

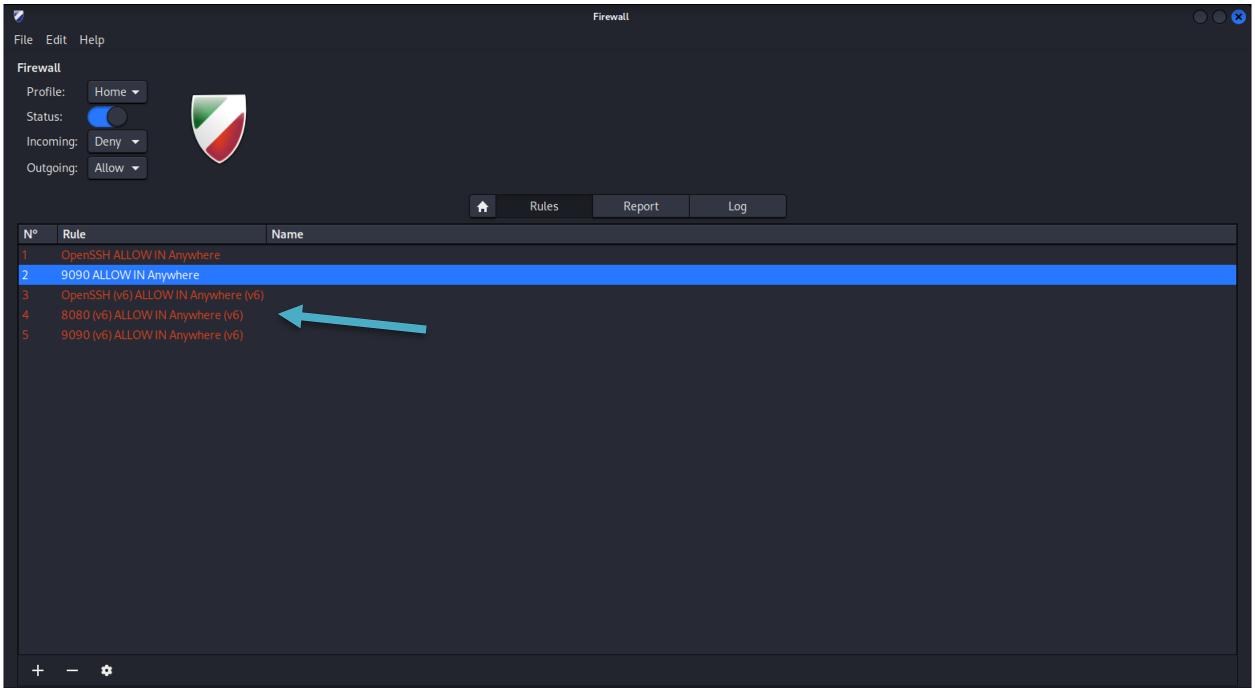
4.3 Identifying Unnecessary Open Ports and Selecting Port 8080 Rule for Removal



Profile: Home
Status: on
Incoming: Deny
Outgoing: Allow

Nº	Rule	Name
1	OpenSSH ALLOW IN Anywhere	
2	8080 ALLOW IN Anywhere	
3	9090 ALLOW IN Anywhere	
4	OpenSSH (v6) ALLOW IN Anywhere (v6)	
5	8080 (v6) ALLOW IN Anywhere (v6)	
6	9090 (v6) ALLOW IN Anywhere (v6)	

4.4 Selecting Port 9090 Rule for Removal



Firewall

Profile: Home

Status:

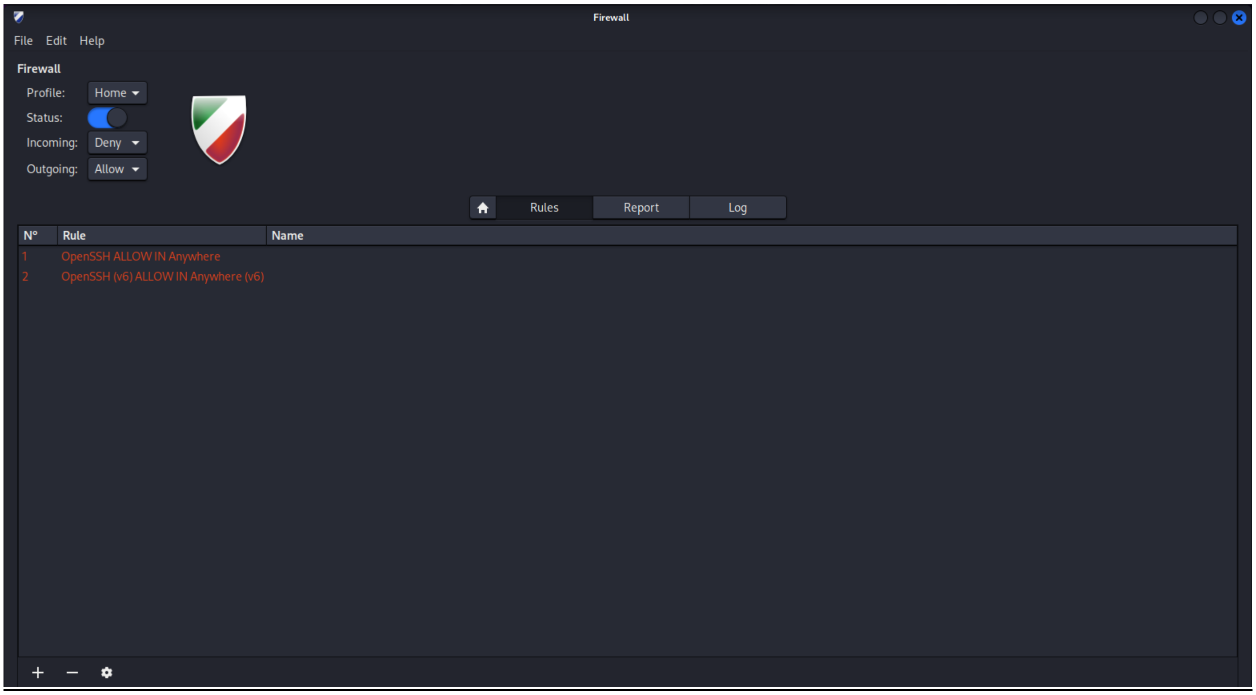
Incoming: Deny

Outgoing: Allow

Nº	Rule	Name
1	OpenSSH ALLOW IN Anywhere	
2	9090 ALLOW IN Anywhere	
3	OpenSSH (v6) ALLOW IN Anywhere (v6)	
4	8080 (v6) ALLOW IN Anywhere (v6)	
5	9090 (v6) ALLOW IN Anywhere (v6)	

4.5 Verify that ports 8080 and 9090 no longer appear in the firewall rules list

Only essential services should remain allowed.



Firewall

Profile: Home

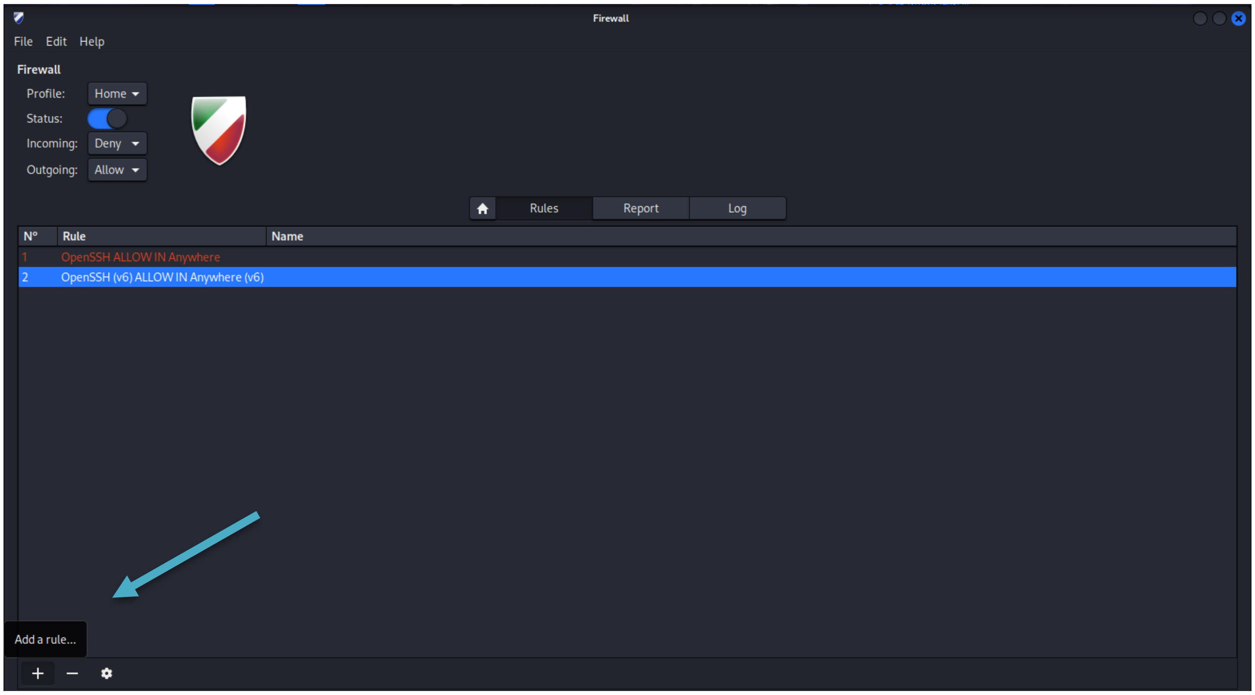
Status:

Incoming: Deny

Outgoing: Allow

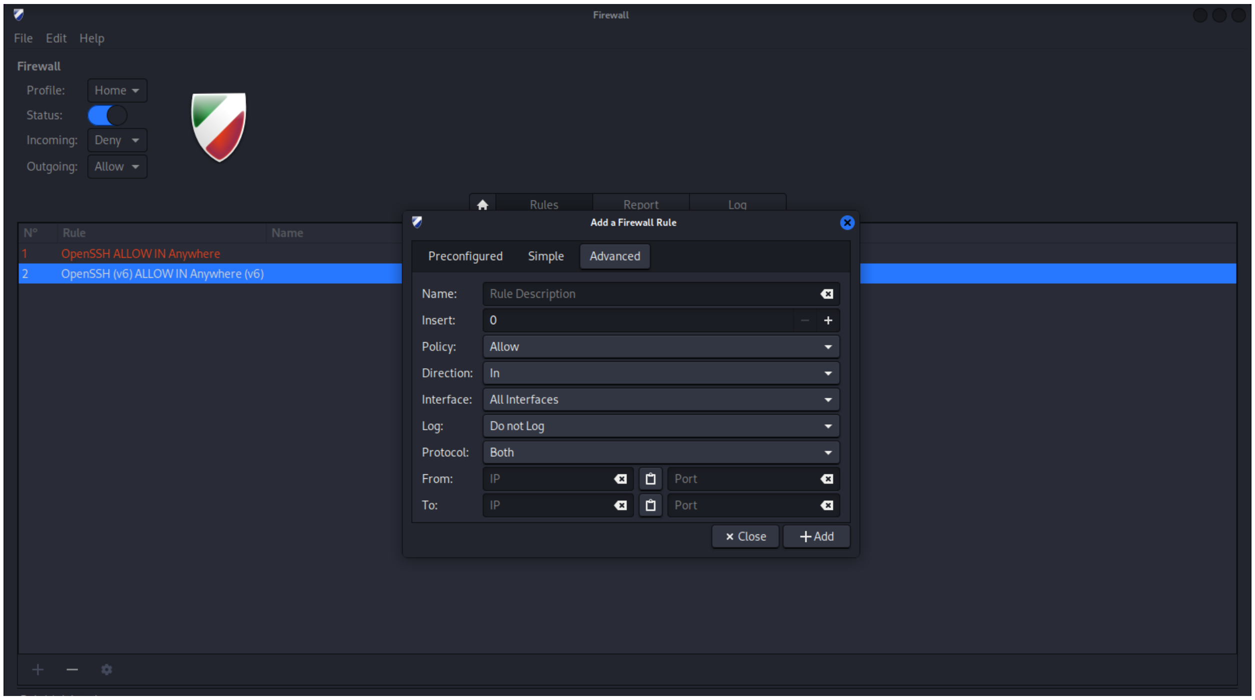
Nº	Rule	Name
1	OpenSSH ALLOW IN Anywhere	
2	OpenSSH (v6) ALLOW IN Anywhere (v6)	

4.6 Click on Add a Rule



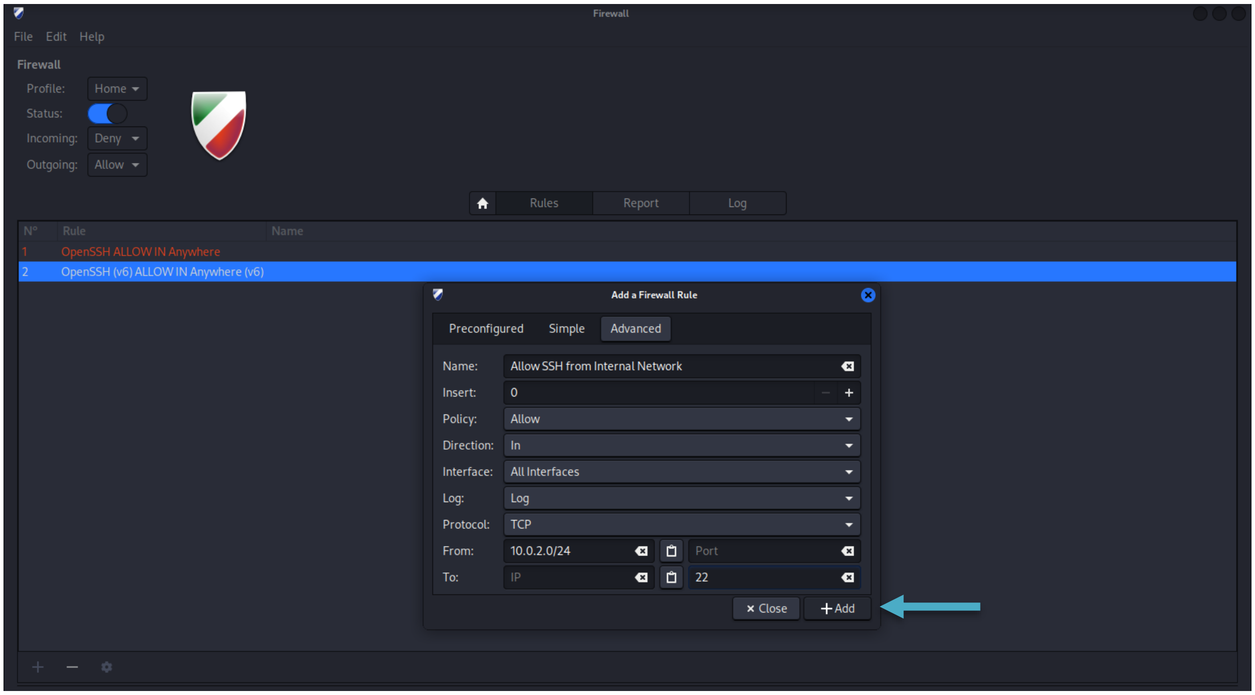
Nº	Rule	Name
1	OpenSSH ALLOW IN Anywhere	
2	OpenSSH (v6) ALLOW IN Anywhere (v6)	

4.7 Creating an Advanced Firewall Rule in GUFW



Name: Rule Description
Insert: 0
Policy: Allow
Direction: In
Interface: All Interfaces
Log: Do not Log
Protocol: Both
From: IP Port
To: IP Port

4.8 Restricting SSH Access to Internal Network



Firewall

Profile: Home
Status:
Incoming: Deny
Outgoing: Allow

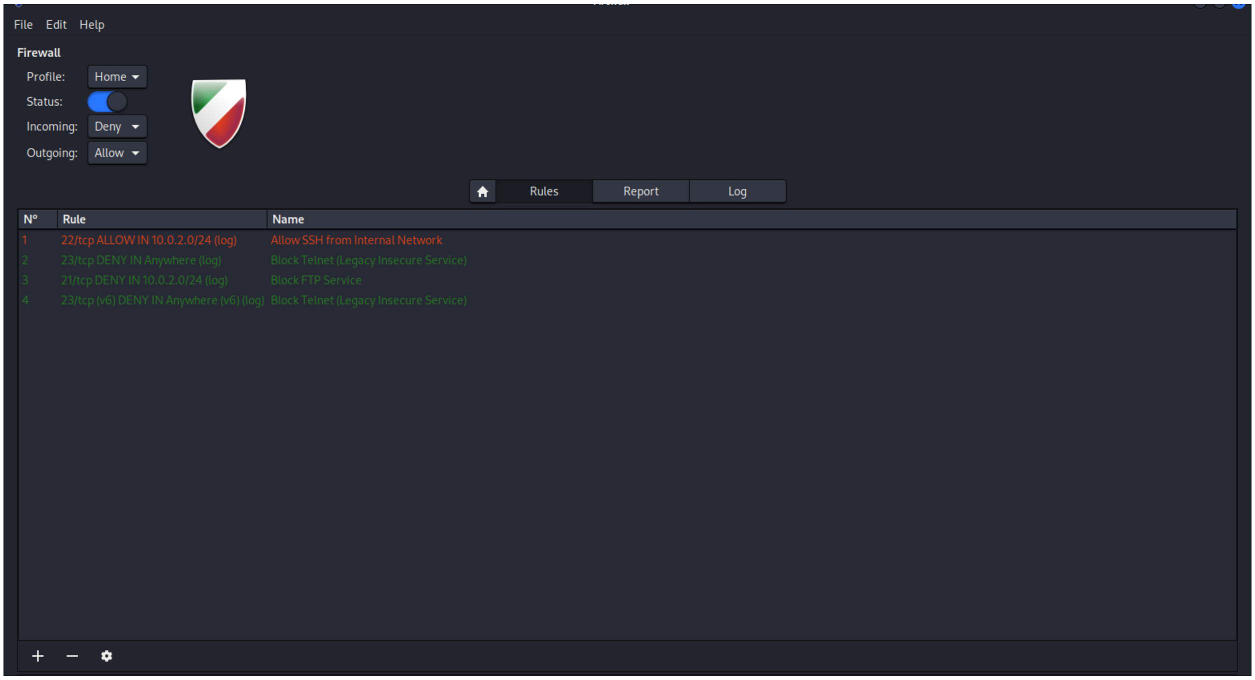
Nº	Rule	Name
1	OpenSSH ALLOW IN Anywhere	
2	OpenSSH (v6) ALLOW IN Anywhere (v6)	

Add a Firewall Rule

Name: Allow SSH from Internal Network
Insert: 0
Policy: Allow
Direction: In
Interface: All Interfaces
Log: Log
Protocol: TCP
From: 10.0.2.0/24 Port
To: IP 22

This figure shows a firewall rule allowing SSH connections only from the internal network range (10.0.2.0/24). Logging is enabled to monitor access attempts.

4.9 After Add new rule



Firewall

Profile: Home

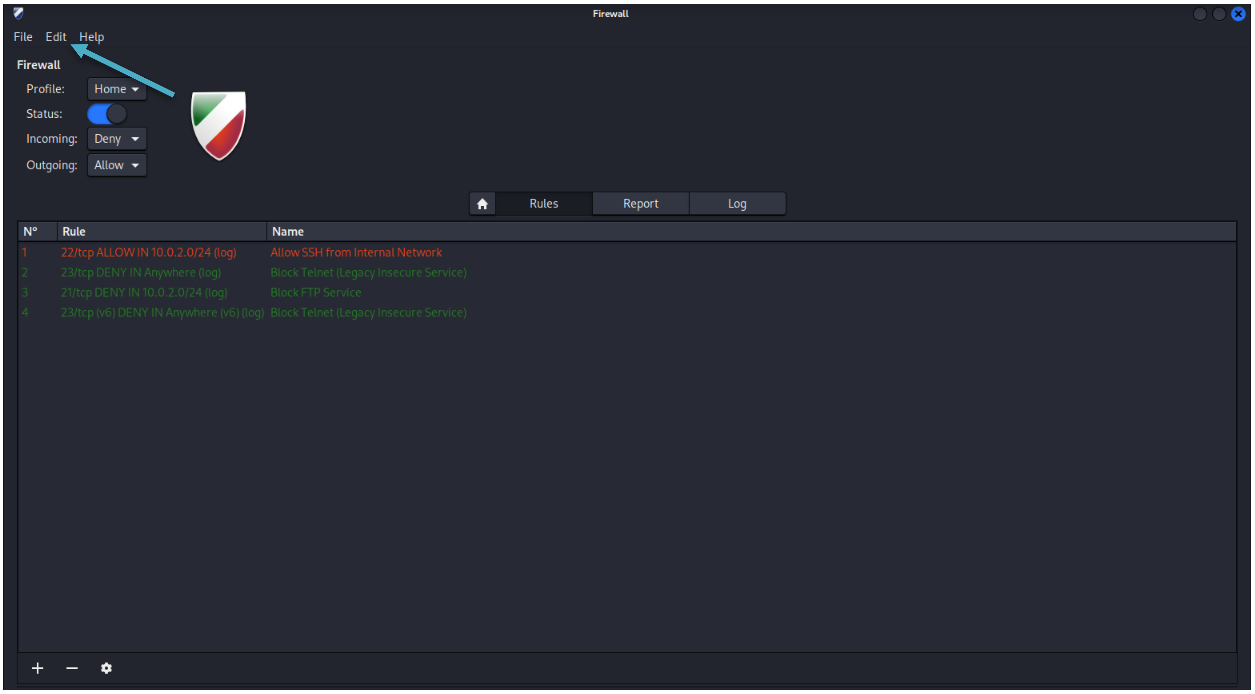
Status:

Incoming: Deny

Outgoing: Allow

Nº	Rule	Name
1	22/tcp ALLOW IN 10.0.2.0/24 (log)	Allow SSH from Internal Network
2	23/tcp DENY IN Anywhere (log)	Block Telnet (Legacy Insecure Service)
3	21/tcp DENY IN 10.0.2.0/24 (log)	Block FTP Service
4	23/tcp (v6) DENY IN Anywhere (v6) (log)	Block Telnet (Legacy Insecure Service)

4.10 Click on Edit



Firewall

Profile: Home

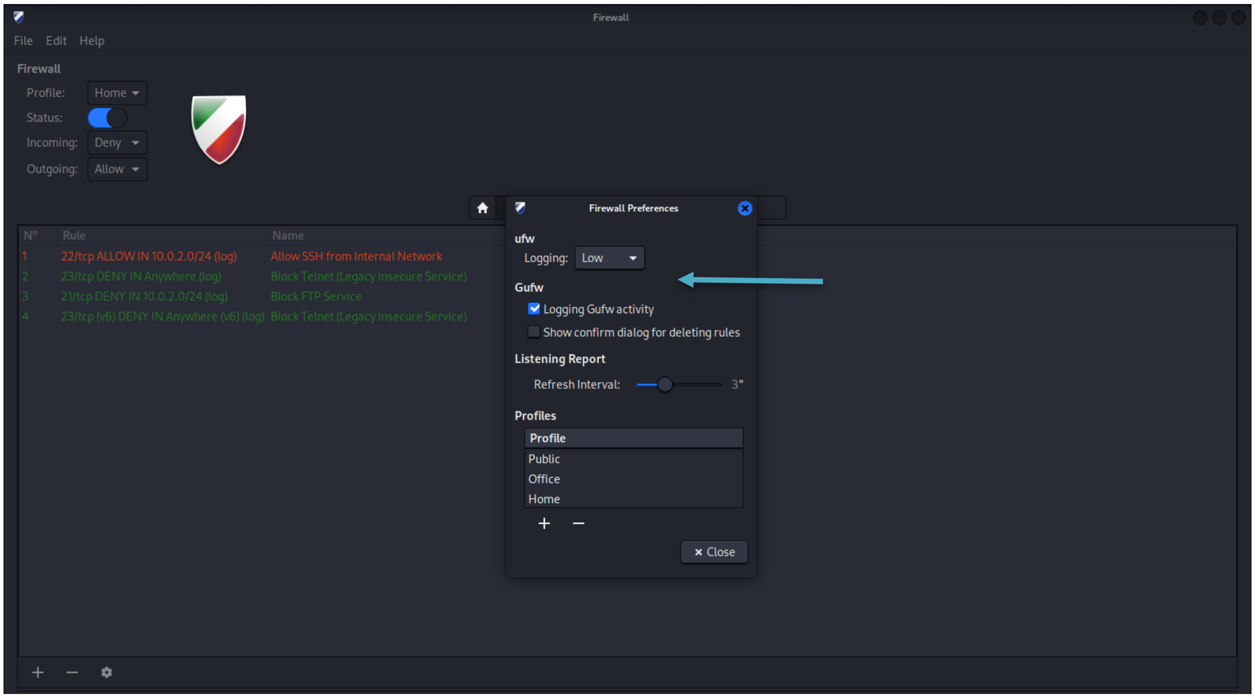
Status:

Incoming: Deny

Outgoing: Allow

Nº	Rule	Name
1	22/tcp ALLOW IN 10.0.2.0/24 (log)	Allow SSH from Internal Network
2	23/tcp DENY IN Anywhere (log)	Block Telnet (Legacy Insecure Service)
3	21/tcp DENY IN 10.0.2.0/24 (log)	Block FTP Service
4	23/tcp (v6) DENY IN Anywhere (v6) (log)	Block Telnet (Legacy Insecure Service)

4.11 From preferences change level



Firewall

Profile: Home

Status:

Incoming: Deny

Outgoing: Allow

Nº	Rule	Name
1	22/tcp ALLOW IN 10.0.2.0/24 (log)	Allow SSH from Internal Network
2	23/tcp DENY IN Anywhere (log)	Block Telnet (Legacy Insecure Service)
3	21/tcp DENY IN 10.0.2.0/24 (log)	Block FTP Service
4	23/tcp (v6) DENY IN Anywhere (v6) (log)	Block Telnet (Legacy Insecure Service)

ufw

Logging: Low

Gufw

☑ Logging Gufw activity

☐ Show confirm dialog for deleting rules

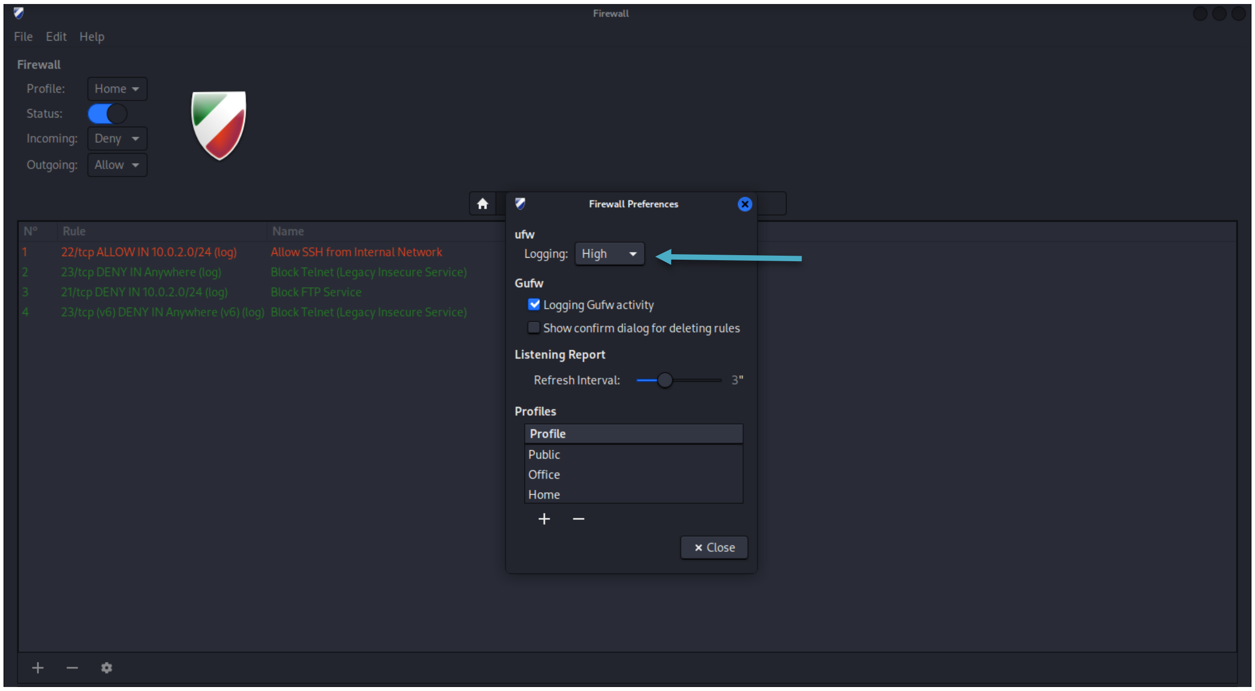
Listening Report

Refresh Interval: 3"

Profiles

Profile
Public
Office
Home

4.12 UFW logging has been changed to High to enable detailed traffic monitoring.



Firewall

Profile: Home

Status:

Incoming: Deny

Outgoing: Allow

Nº	Rule	Name
1	22/tcp ALLOW IN 10.0.2.0/24 (log)	Allow SSH from Internal Network
2	23/tcp DENY IN Anywhere (log)	Block Telnet (Legacy Insecure Service)
3	21/tcp DENY IN 10.0.2.0/24 (log)	Block FTP Service
4	23/tcp (v6) DENY IN Anywhere (v6) (log)	Block Telnet (Legacy Insecure Service)

ufw

Logging: High

Gufw

☑ Logging Gufw activity

☐ Show confirm dialog for deleting rules

Listening Report

Refresh Interval: 3"

Profiles

Profile
Public
Office
Home

Security Purpose and Benefits to the Organization and Employees

The firewall configuration steps performed in this guide are designed to protect both the organization's systems and its users from unauthorized network access and potential cyberattacks. By carefully controlling which ports and services are allowed, the organization reduces its overall attack surface and limits opportunities for attackers to exploit open services.

Allowing only required ports such as **SSH (22)**, **web service ports (8080)**, and **management service ports (9090)** ensures that employees can access necessary applications to perform their tasks while preventing exposure of unnecessary or risky services. At the same time, blocking unused or insecure services helps prevent malware infections, unauthorized access, and lateral movement inside the network.

Restricting access based on specific ports and, in some cases, internal network ranges also protects internal systems from external threats. This means that sensitive services such as remote administration can only be accessed by authorized staff from trusted networks, reducing the risk of credential theft and brute-force attacks from the internet.

Enabling firewall logging and monitoring allows the organization's IT and security teams to track suspicious activities, investigate incidents, and respond quickly to potential attacks. Logs provide valuable evidence during troubleshooting and security audits, helping improve compliance with organizational security policies and regulatory requirements.

From an employee perspective, these controls improve system reliability and data safety. Staff can work with reduced risk of service disruption, data leakage, or compromise of their accounts. Secure systems also protect personal information, work files, and internal communications from unauthorized access.

Overall, these firewall hardening steps support the organization's cybersecurity strategy by enforcing access control, improving visibility into network activity, and strengthening protection against both internal and external threats. This creates a safer digital environment where business operations can continue securely and efficiently.

The system is now securely configured with only authorized services accessible.