Basic Firewall Setup Project

# Abstract

The firewall setup project aims to create a basic and functional firewall that helps protect a network from unauthorized access while allowing legitimate traffic to pass through. This project focuses on configuring basic firewall rules using command-line tools like iptables (Linux) or firewalld, ensuring that both incoming and outgoing traffic is filtered according to the defined security policies. The setup enhances security by defining rules that control the flow of data between internal networks and external networks, providing protection against a range of potential attacks.

# Description

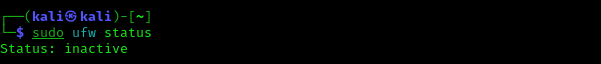
This project is designed to configure a basic firewall setup, which is essential in securing any network by controlling traffic flow based on predefined security rules. The project focuses on using Linux-based firewall configuration tools like iptables or firewalld to create specific firewall rules that manage traffic to and from the network.

Features:  
- Basic firewall rules to control incoming and outgoing traffic.  
- Allow/block traffic based on protocols, ports, and IP addresses.  
- Protect against unauthorized access.  
- Easily configurable via command-line interface (CLI).

# Step-by-Step Commands with Descriptions

## Check the Current Status of the Firewall

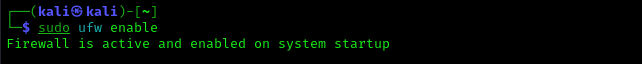
sudo ufw status



This command checks the current status of the firewall on a system using `ufw`. It shows whether the firewall is active and which rules are currently applied.

## Enable the Firewall

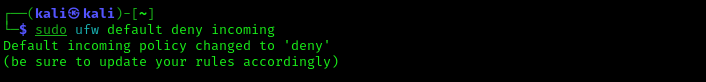
sudo ufw enable



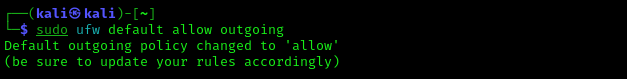
This command enables the firewall, which will start filtering traffic according to the default and custom rules that are configured.

## Set Default Rules for Incoming and Outgoing Traffic

sudo ufw default deny incoming



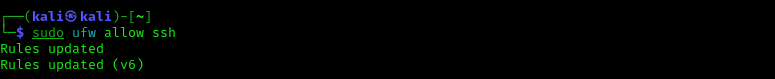
sudo ufw default allow outgoing ( Add youre own trusted ip )

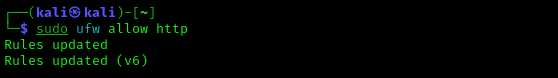


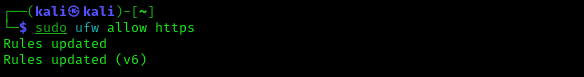
These commands define the default behavior for incoming and outgoing traffic. Deny all incoming traffic by default while allowing outgoing traffic.

## Allow Specific Ports (e.g., SSH, HTTP, HTTPS)

sudo ufw allow ssh

  
sudo ufw allow http

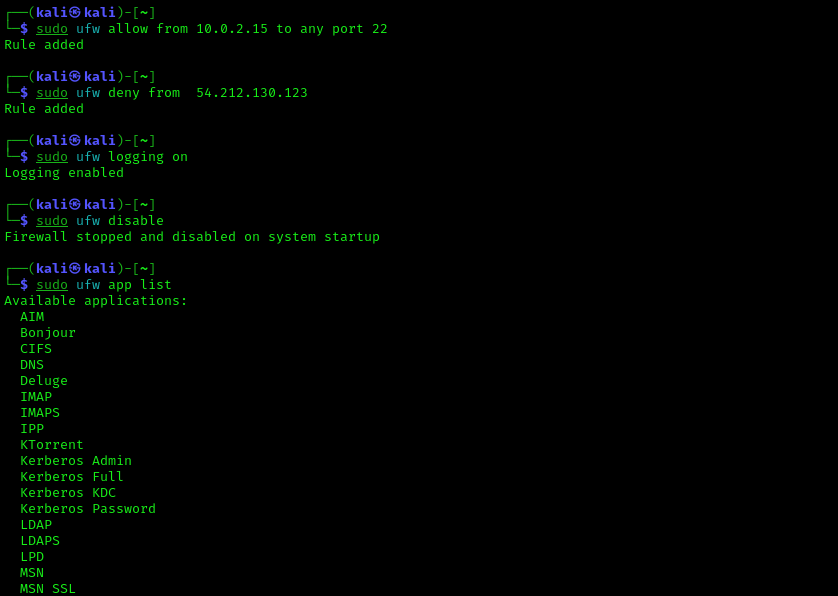
  
sudo ufw allow https



These commands allow traffic on SSH (port 22), HTTP (port 80), and HTTPS (port 443).

## Allow Traffic from a Specific IP Address

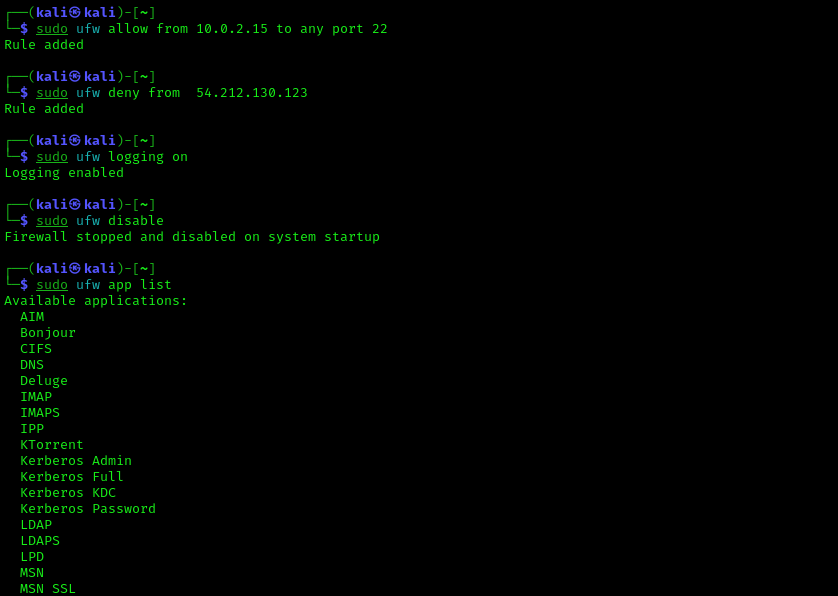
sudo ufw allow from [Add youre own trusted ip ]



This command allows all traffic from the specified IP address (192.168.1.100).

## Block Traffic to a Specific IP

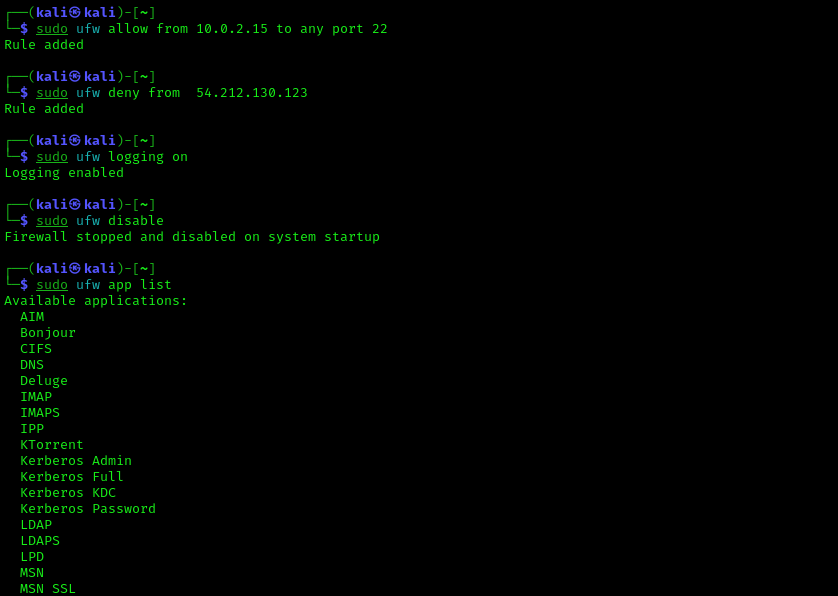
sudo ufw deny [Add youre own untrusted ip ]



This command blocks traffic to ip. It's useful to prevent unauthorized services.

## Enable Logging for the Firewall

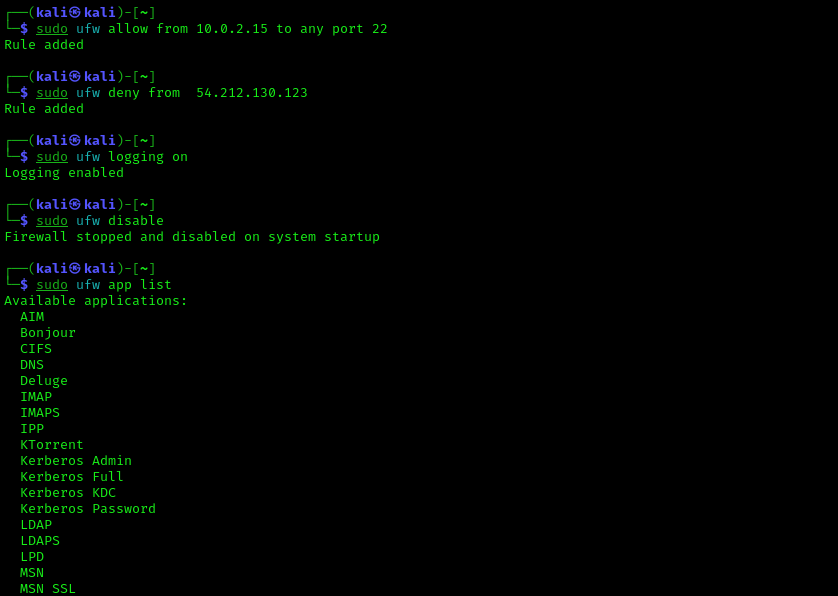
sudo ufw logging on



This command enables logging for the firewall, helping to monitor traffic actions.

## Disable Firewall (if needed)

sudo ufw disable



This command disables the firewall, leaving the system unprotected.

# Conclusion

Setting up a basic firewall ensures the security of a system or network by controlling which traffic is allowed in and out. Using these commands, you can create custom firewall rules that fit your network’s security requirements, blocking malicious traffic while allowing legitimate access.