

# Linux Firewall Guide: UFW Installation & Configuration

## What is UFW?

UFW (Uncomplicated Firewall) is a user-friendly frontend for managing iptables firewall rules on Linux systems. It simplifies the process of setting up a host-based firewall to control incoming and outgoing network traffic based on security rules. UFW supports both IPv4 and IPv6 and is the default firewall configuration tool on Ubuntu

## Installation

### On Ubuntu/Debian-based Systems

UFW usually comes preinstalled. If it is not installed, you can install it using

```
Sudo apt update  
Sudo apt install ufw
```

Verify installation by checking the version:

```
Sudo ufw version
```

## Basic Configuration

### 1. Set Default Policies

Before enabling UFW, define the default behavior for incoming and outgoing traffic:

```
Sudo ufw default deny incoming  
Sudo ufw default allow outgoing
```

This configuration denies all incoming connections by default and allows all outgoing connections, which is a secure baseline

```
kali@kali: ~  
$ sudo ufw status  
Status: active  


| To            | Action | From          |
|---------------|--------|---------------|
| 9999/tcp      | DENY   | Anywhere      |
| 8888/tcp      | ALLOW  | Anywhere      |
| 9999/tcp (v6) | DENY   | Anywhere (v6) |
| 8888/tcp (v6) | ALLOW  | Anywhere (v6) |

  
$ sudo ufw enable  
Firewall is active and enabled on system startup  
  
$ sudo ufw allow 22/tcp  
Rule added  
Rule added (v6)  
  
$ sudo ufw deny 9999/tcp  
Skipping adding existing rule  
Skipping adding existing rule (v6)  
  
$ sudo ufw status numbered  
Status: active  


|       | To            | Action   | From          |
|-------|---------------|----------|---------------|
| [ 1 ] | 9999/tcp      | DENY IN  | Anywhere      |
| [ 2 ] | 8888/tcp      | ALLOW IN | Anywhere      |
| [ 3 ] | 22/tcp        | ALLOW IN | Anywhere      |
| [ 4 ] | 9999/tcp (v6) | DENY IN  | Anywhere (v6) |
| [ 5 ] | 8888/tcp (v6) | ALLOW IN | Anywhere (v6) |
| [ 6 ] | 22/tcp (v6)   | ALLOW IN | Anywhere (v6) |

  
$ sudo ufw allow from 192.168.1.100  
Rule added  
  
$ sudo ufw delete [rule-number]  
ERROR: Invalid syntax  
  
Usage: ufw COMMAND  
  
Commands:  
enable          enables the firewall  
disable         disables the firewall  
default ARG     set default policy  
logging LEVEL   set logging to LEVEL  
allow ARGS      add allow rule  
deny ARGS       add deny rule  
reject ARGS     add reject rule
```

## 2. Allow Essential Services

It is critical to allow SSH connections before enabling UFW to avoid locking yourself out:

Sudo ufw allow ssh

If SSH runs on a non-standard port, specify the port number:

Sudo ufw allow <port\_number>/tcp

You can allow or deny other services or ports similarly:

Sudo ufw allow 80/tcp

Sudo ufw deny 23/tcp

## Managing UFW

# Enable the Firewall

Sudo ufw enable

# Disable the Firewall

Sudo ufw disable

# Check Firewall Status and Rules

Sudo ufw status

```
(kali@kali)~$ sudo ufw status
status: active

To Action From
--
9999/tcp DENY Anywhere
8888/tcp ALLOW Anywhere
9999/tcp (v6) DENY Anywhere (v6)
8888/tcp (v6) ALLOW Anywhere (v6)

(kali@kali)~$ sudo ufw enable
Firewall is active and enabled on system startup

(kali@kali)~$ sudo ufw allow 22/tcp
Rule added
Rule added (v6)

(kali@kali)~$ sudo ufw deny 9999/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)

(kali@kali)~$ sudo ufw status numbered
Status: active

To Action From
--
[ 1] 9999/tcp DENY IN Anywhere
[ 2] 8888/tcp ALLOW IN Anywhere
[ 3] 22/tcp ALLOW IN Anywhere
[ 4] 9999/tcp (v6) DENY IN Anywhere (v6)
[ 5] 8888/tcp (v6) ALLOW IN Anywhere (v6)
[ 6] 22/tcp (v6) ALLOW IN Anywhere (v6)

(kali@kali)~$ sudo ufw allow from 192.168.1.100
Rule added

(kali@kali)~$ sudo ufw delete [rule-number]
ERROR: Invalid syntax

Usage: ufw COMMAND

Commands:
enable enables the firewall
disable disables the firewall
default ARG set default policy
logging LEVEL set logging to LEVEL
allow ARGS add allow rule
deny ARGS add deny rule
reject ARGS add reject rule
```

Command	Description
<code>sudo ufw enable</code>	Enable UFW firewall

<code>sudo ufw disable</code>	Disable UFW firewall
<code>sudo ufw status verbose</code>	Show detailed firewall status
<code>sudo ufw default deny incoming</code>	Set default incoming policy to deny
<code>sudo ufw default allow outgoing</code>	Set default outgoing policy to allow
<code>sudo ufw allow ssh</code>	Allow SSH connections
<code>sudo ufw allow &lt;port&gt;/tcp</code>	Allow TCP traffic on a port
<code>sudo ufw deny &lt;port&gt;/tcp</code>	Deny TCP traffic on a port

## DELETING THE RULES IN FIREWALL

- IF WE WANT TO DELETE THE RULES IN FIREWALL WE CAN USE THE FOLLOWING COMMAND:
- `sudo ufw delete <rule-number>`

## RESETTING THE UFW

- WE CAN USE THE COMMAND TO RESET THE ALL UFW RULES
- `sudo ufw reset.`