How to Setup a Firewall (Ubuntu)

This post is a part of a series of short, practical guides for beginners to Linux operating systems, especially Ubuntu. In this post, we will discuss the benefits of a firewall and subsequently, the setup guide.

Why Set Up a Firewall?

Setting of a firewall for Ubuntu lies in three primary reasons:

1. **Security:** A firewall safeguards your device controlling incoming and outgoing network traffic based on predetermined security rules.

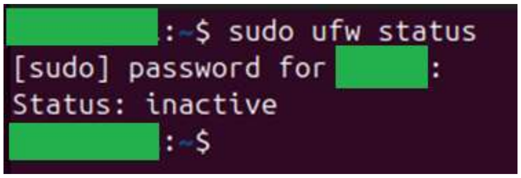
2. **Access Control:** It allows you to specify which services or applications can be access from outside your network. This process will reduce the risk of unauthorized access.

3. **Network Segmentation:** Firewalls can help segment your network and limit the potential threat of malware or attackers within your network.

Steps to Set Up UFW in Ubuntu

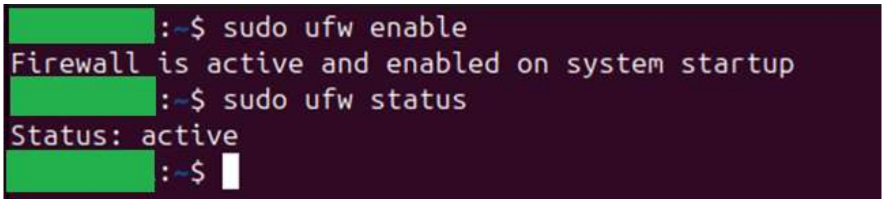
The **Uncomplicated Firewall (UFW)** is a simple firewall application that is included with Ubuntu and can be installed on other distributions of Linux. By default, UFW is disabled.

In order to see the status of UFW, open Terminal and type in the following command line: **sudo ufw status**



```
[redacted]:~$ sudo ufw status
[sudo] password for [redacted]:
Status: inactive
[redacted]:~$
```

To enable UFW, enter the following command: **sudo ufw enable**



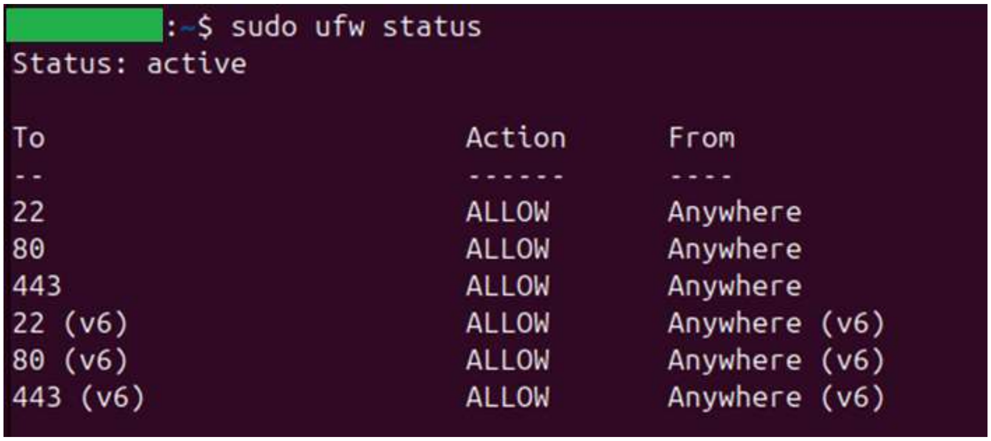
```
[redacted]:~$ sudo ufw enable
Firewall is active and enabled on system startup
[redacted]:~$ sudo ufw status
Status: active
[redacted]:~$ 
```

By default, ALL incoming traffic is blocked. Here are a few command lines to allow UFW. Proceed to allow for SSH, HTTP and HTTPS.

sudo ufw allow 22	Allow 22 for SSH
sudo ufw allow 80	Allow 80 for HTTP
sudo ufw allow 443	Allow 443 for HTTPS
ufw default allow	Allow all connections by default
ufw default deny	Drop all connections by default
ufw allow port	Allow traffic on port
ufw deny port	Block port
ufw deny from ip	Block ip address
sudo ufw allow <app_name>	To allow application profiles
sudo ufw allow samba	Allows samba

How to Setup a Firewall (Ubuntu)

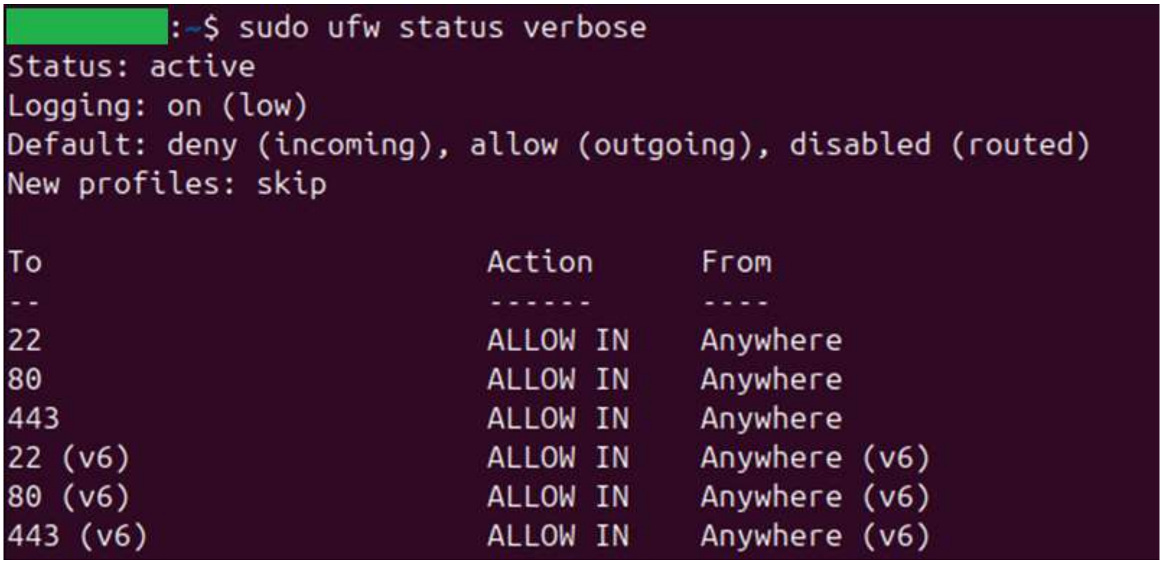
To find out the status of the UFW, type in the following command line: **sudo ufw status**



```
[redacted]:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
80                         ALLOW       Anywhere
443                        ALLOW       Anywhere
22 (v6)                    ALLOW       Anywhere (v6)
80 (v6)                    ALLOW       Anywhere (v6)
443 (v6)                   ALLOW       Anywhere (v6)
```

sudo ufw status verbose – Shows all Rules currently configured for ufw



```
[redacted]:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22                         ALLOW IN    Anywhere
80                         ALLOW IN    Anywhere
443                        ALLOW IN    Anywhere
22 (v6)                    ALLOW IN    Anywhere (v6)
80 (v6)                    ALLOW IN    Anywhere (v6)
443 (v6)                   ALLOW IN    Anywhere (v6)
```

<u>Additional useful UFW commands</u>

sudo ufw status numbered – Shows rules in numbered order so that you can delete specific rules.
sudo ufw delete 1 – Deletes rule based on number.

sudo ufw disable – Disables ufw
sudo ufw reset – Deletes all rules and disables ufw

The default firewall configuration tool for Ubuntu is ufw. Developed to ease iptables firewall configuration, ufw provides a user-friendly way to create an IPv4 or IPv6 host-based firewall. By default, UFW is disabled. **Gufw** is a GUI that is available as a frontend.