How to set up a firewall in Linux

You should set up a firewall to prevent others from accessing your computer and protecting you from network attacks. In today's article, you will learn how to set up firewalls in Linux and add rules to allow access to other devices on a local network or specific ports.

To keep your computer safe, you should set up a firewall to prevent others from accessing your computer and protecting you from network attacks. However, if you are a new Linux user, you may not know how to configure a firewall in your system.

In today's article, you will learn how to set up firewalls in Linux and add rules to allow access to other devices on the local network or specific ports.

UFW = Uncomplicated Firewall

You will use UFW to manage the Linux firewall, because it is easy to use and is installed by default in many distributions.

In Ubuntu, ufw is disabled by default. You can check its status with the command:

```
sudo ufw status
```

If it doesn't work and you want to check if turning on ufw makes a difference, use the command:

```
sudo ufw enable
```

To turn off the firewall, use the command:

```
sudo ufw disable
```

Check out the existing application rules

To view the list of applications for which the firewall has set rules, use the command:

```
sudo ufw app list
```

You can check which ports are open for those rules by:

```
sudo ufw app info APP_NAME
```

You can check which ports are open for rules
Note : You should enter **APP_NAME** exactlyas it appears in the results of the previous command.

Create new rule

If you want to enable a firewall but only allow access to the PC from other devices on the local network, enter:

```
sudo ufw allow from 192.168.178.0/24
```

Remember to change **192.168.178.0/24** in the example as your local network's IP range.

To grant access only to a specific port, such as port 80, if you are running a local Web server, use:

```
sudo ufw allow from 192.168.178.0/24 to any port 80
```

Of course, you can change port 80 to any other port you want.

To open a series of ports on your computer with a single command, you can enter:

```
sudo ufw allow STARTING_PORT:ENDING_PORT/PROTOCOL
```

For example, to open all ports from **50,000** to **52,000** for both TCP and UDP to use with the torrent client, use:

```
sudo ufw allow 50000:52000/tcp sudo ufw allow 50000:52000/udp
```

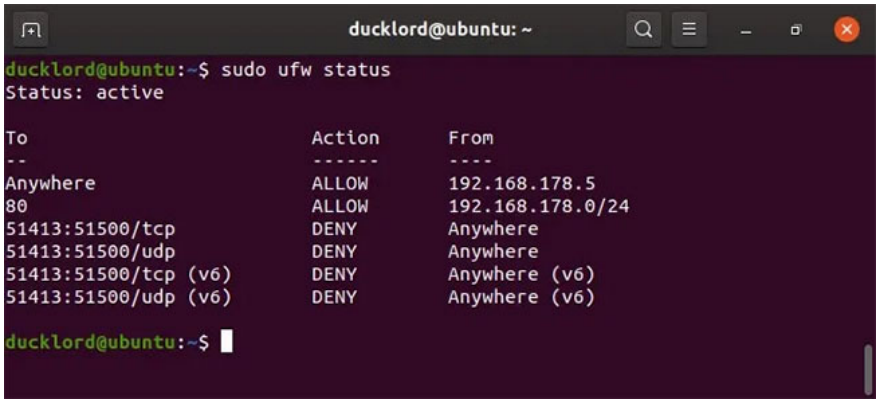
Similarly, if you have opened a series of ports, as done here for use with the popular Transmission torrent client and want to close them, change the **allow** to **deny** in the above command, as follows:

```
sudo ufw deny 51413:51500/udp sudo ufw deny 51413:51500/tcp
```

Disable the rule and reset the firewall

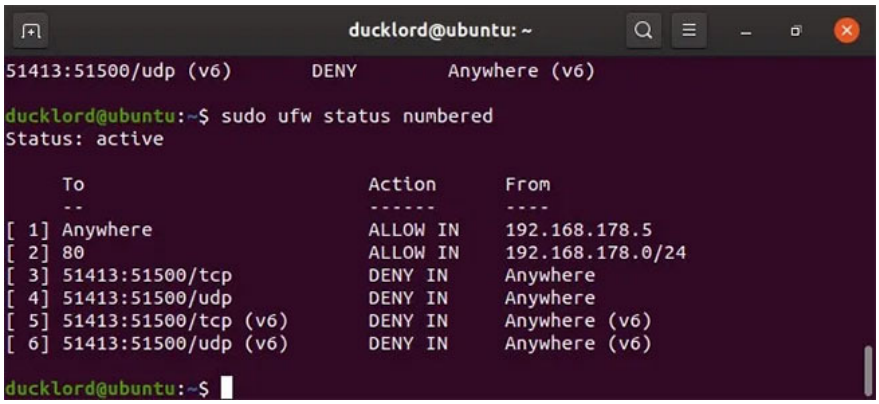
After setting up a new rule, you can reuse the **status** command to see all the rules.

```
sudo ufw status
```



Use the status command to see all the rules
To be able to delete rules, you must first use this command:

```
sudo ufw status numbered
```



The list will now have a number next to each item
The list will now have a number next to each item. To delete a rule, use:

```
sudo UFW delete RULE_NUMBER
```

For example:

```
sudo ufw delete 3
```

If you want to delete all your custom rules and revert the firewall to the original configuration, start by disabling it with the command:

```
sudo ufw disable
```

Then, reset the firewall configuration using:

```
sudo ufw reset
```

GUFW = Graphic interface for UFW

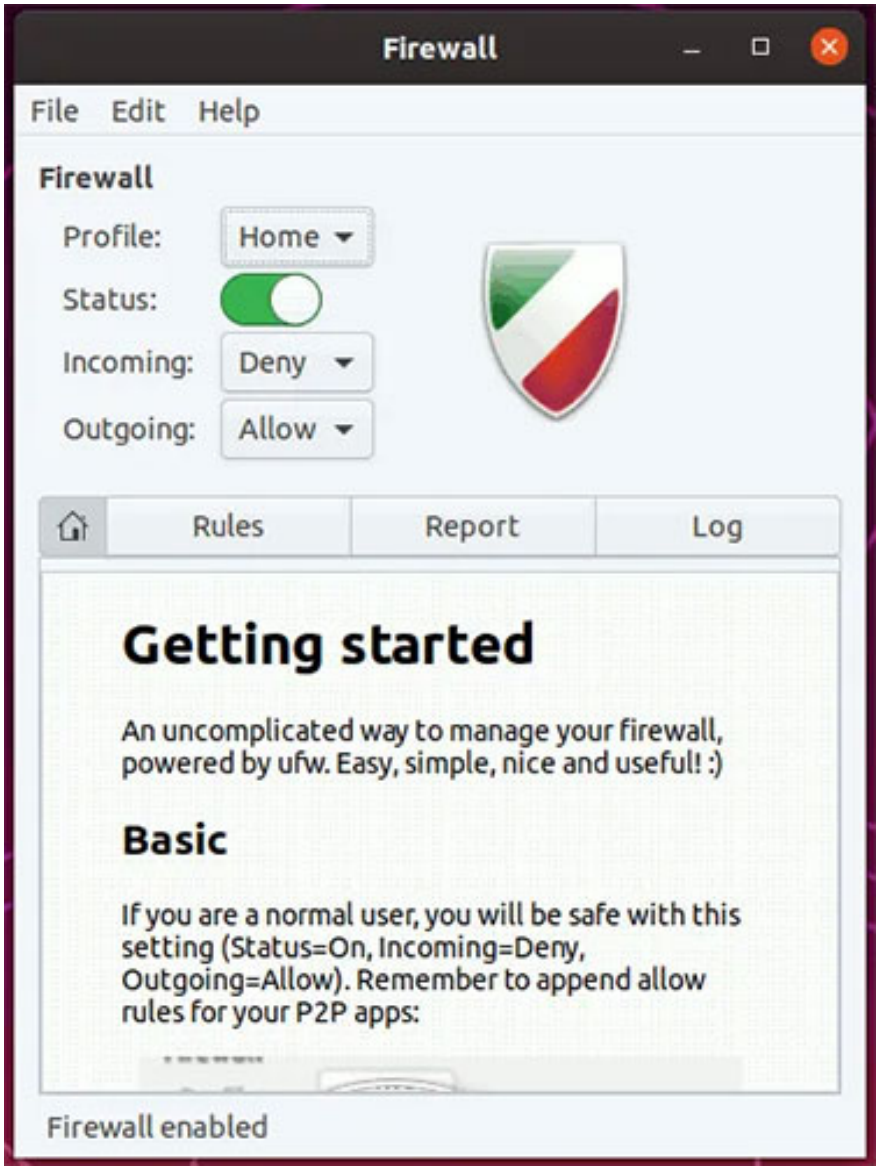
If you find the above part a bit complicated, you can use GUFW to manage your firewall graphically.

1. Install GUW *(http://gufw.org/)* from Package Mananger or Software Center of distro.

2. Launch it.

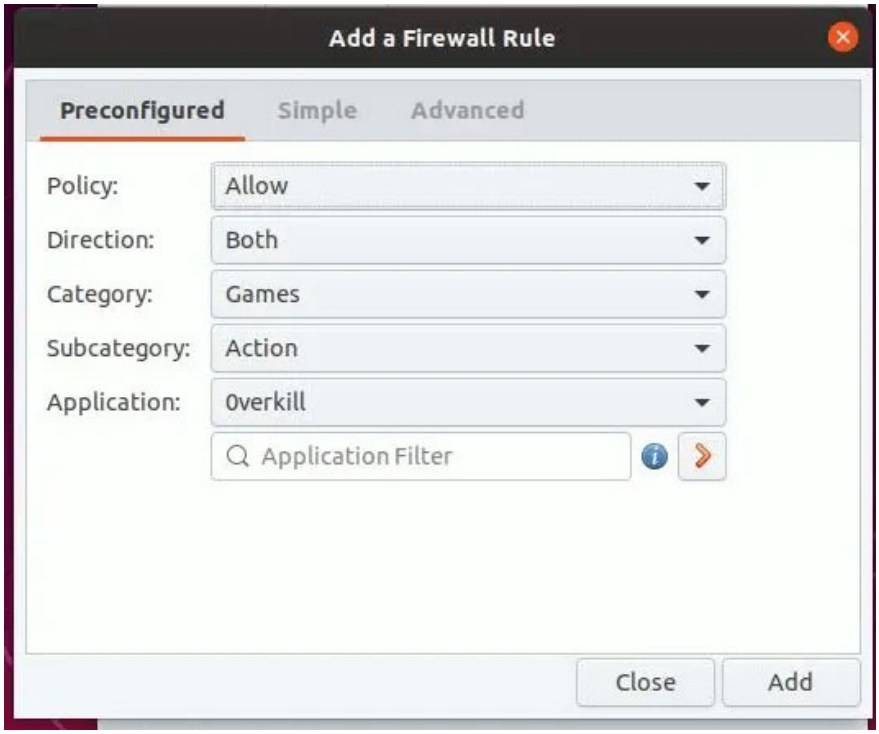
Launch GUW

3. To turn on the firewall, simply click the **Status** switch to activate. The default rule is to block all incoming connections and allow all outgoing connections.



Click the Status switch to activate

4. Click the **Rules** tab and press the + button at the bottom. Here, you can add rules to your firewall.



Click the Rules tab and press the + button to add rules

If you use a PC to access the Internet, you should turn on a firewall, create rules that allow you to use your computer safely, instead of disabling or removing it. If you're really worried, you can also install antivirus software for Linux, to make sure no malware can harm your computer and data.

You finished reading the article "**How to set up a firewall in Linux**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com