

Step 1: Install UFW

A firewall essentially allows or denies incoming and/or outgoing connections to your machine.

We are going to use `ufw`, because it is very easy to use, hence the name: `Uncomplicated Firewall`.

To install it on Debian/Ubuntu, run: `sudo apt update && sudo apt install ufw`.

After that, we want to allow connection to the SSH port BEFORE enabling the firewall, or else you'll be locked out of the machine and will require to reinstall it.

To do that, run: `sudo ufw allow 22/tcp`.

This will allow incoming connection to port 22, which is the default port for SSH.

Now we want to enable the firewall, so run `sudo ufw enable`.

⚠ DO THIS AFTER ALLOWING INCOMING CONNECTIONS ON PORT 22 ⚠

We can make sure port 22 is open by running `sudo ufw status` and looking for a line that says `22/tcp ALLOW Anywhere`.

As you can probably guess, this line says port 22, using protocol `tcp`, is allowed, for anyone (`Anywhere`). You can also allow some IPs and IP ranges, etc. Look up the manual for more.

You will also have another line that says `22/tcp (v6) ALLOW Anywhere (v6)`. This is the same, except for IPv6.

Revision #6

Created 17 December 2025 18:18:54 by seres

Updated 19 December 2025 01:33:27 by seres