



Creating a Secure Cloud Server with UpCloud



Installing and securing cloud server using wireguard

The steps to this are the following

-Deploy- Using upcloud we are going to deploy the server

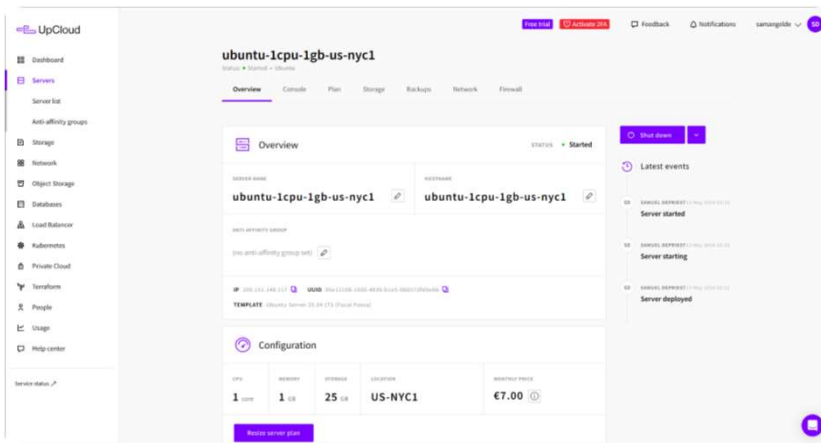
SSH- We are going to use SSH with PuttY to access the server with a OTP

Wireguard- We are going to install wireguard into the server which is a Ubuntu based Linux distro

Firewall- We are going to setup the ufw and allow wireguard to access through it using port 51820/udp



Deploying the server



- I was able to use upcloud.com for a cloud service provider to manage and deploy my server. I went with a Ubuntu linux distro for this project. This was simple as choosing the plan, designating the password for SSH, then using putty to access it.

Installing Wireguard

```
root@ubuntu-1cpu-1gb-us-nyc1: ~  
1 start/stop).  
See system logs and 'systemctl status snapd.mounts-pre.target' for details.  
Processing triggers for mime-support (3.64ubuntu1) ...  
Processing triggers for libc-bin (2.31-0ubuntu9.15) ...  
Processing triggers for man-db (2.9.1-1) ...  
Processing triggers for plymouth-theme-ubuntu-text (0.9.4git20200323-0ubuntu6.2)  
...  
update-initramfs: deferring update (trigger activated)  
Processing triggers for install-info (6.7.0.dfsg.2-5) ...  
Processing triggers for ca-certificates (20230311ubuntu0.20.04.1) ...  
Updating certificates in /etc/ssl/certs...  
0 added, 0 removed; done.  
Running hooks in /etc/ca-certificates/update.d...  
done.  
Processing triggers for initramfs-tools (0.136ubuntu6.7) ...  
update-initramfs: Generating /boot/initrd.img-5.11.0-38-generic  
root@ubuntu-1cpu-1gb-us-nyc1:~# sudo apt-get wireguard  
E: Invalid operation wireguard  
root@ubuntu-1cpu-1gb-us-nyc1:~# sudo apt-get install wireguard  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following additional packages will be installed:  
wireguard-tools
```

- After gaining SSH I then ran `sudo apt update` and after that `sudo apt-get update && sudo apt-get upgrade -y`. This provided all the tools needed plus updating ones already available. After doing this, I ran `sudo apt-get install wireguard` so we could encrypt the traffic on the server. This was a easy and smooth installation.

```

root@ubuntu-lcpu-lgb-us-nycl:~#
wireguard-tools
Suggested packages:
  openresolv | resolvconf
The following NEW packages will be installed:
  wireguard wireguard-tools
0 upgraded, 2 newly installed, 0 to remove and 8 not upgraded.
Need to get 86.6 kB of archives.
After this operation, 344 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu focal-updates/universe amd64 wireguard-to
ols amd64 1.0.20200513-1-20.04.2 [83.3 kB]
Get:2 http://archive.ubuntu.com/ubuntu focal-updates/universe amd64 wireguard al
1 1.0.20200513-1-20.04.2 [3,264 B]
Fetched 86.6 kB in 0s (1,421 kB/s)
Selecting previously unselected package wireguard-tools.
(Reading database ... 67057 files and directories currently installed.)
Preparing to unpack .../wireguard-tools_1.0.20200513-1-20.04.2_amd64.deb ...
Unpacking wireguard-tools (1.0.20200513-1-20.04.2) ...
Selecting previously unselected package wireguard.
Preparing to unpack .../wireguard_1.0.20200513-1-20.04.2_all.deb ...
Unpacking wireguard (1.0.20200513-1-20.04.2) ...
Setting up wireguard-tools (1.0.20200513-1-20.04.2) ...
wg-quick.target is a disabled or a static unit, not starting it.
Setting up wireguard (1.0.20200513-1-20.04.2) ...
Processing triggers for man-db (2.9.1-1) ...
root@ubuntu-lcpu-lgb-us-nycl:~# sudo modprobe wireguard
root@ubuntu-lcpu-lgb-us-nycl:~# sudo apt install ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
ufw is already the newest version (0.36-6ubuntu1.1).
0 upgraded, 0 newly installed, 0 to remove and 8 not upgraded.
root@ubuntu-lcpu-lgb-us-nycl:~# sudo ufw allow ssh sudo ufw allow 51820/udp
ERROR: Wrong number of arguments
root@ubuntu-lcpu-lgb-us-nycl:~# sudo ufw allow ssh
Rules updated
Rules updated (v6)
root@ubuntu-lcpu-lgb-us-nycl:~# sudo ufw allow 51820/udp
Command 'suda' not found, did you mean:
  command 'sudo' from deb sudo (1.8.31-1ubuntu1.5)
  command 'sudo' from deb sudo-ldap (1.8.31-1ubuntu1.5)
Try: apt install <deb name>
root@ubuntu-lcpu-lgb-us-nycl:~# sudo ufw allow 51820/udp
Rules updated
Rules updated (v6)
root@ubuntu-lcpu-lgb-us-nycl:~# sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y/n)? y
Firewall is active and enabled on system startup
root@ubuntu-lcpu-lgb-us-nycl:~# sudo ufw status
Status: active

To               Action      From
--
22/tcp           ALLOW      Anywhere
51820/udp        ALLOW      Anywhere
22/tcp (v6)     ALLOW      Anywhere (v6)
51820/udp (v6)  ALLOW      Anywhere (v6)

```

Installing and setting up ufw

- After installing wireguard we then installed and implemented rules with ufw. Ufw is a unproblematic firewall that is easy to use. We installed it with `sudo apt-get install ufw`. Once this finished we then setup the allow connection at port 51820/udp which is where wireguard operates through with `sudo ufw allow 51820/udp`. We then enabled the rule for ssh connection with `sudo ufw allow ssh`. We then enabled the fire wall with `sudo ufw enable`, and verified it was running and up with `sudo ufw status`.