Wireguard:

```
sudo apt install wireguard
```

```
sudo mkdir -p /etc/wireguard/keys; wg genkey | sudo tee /etc/wireguard/keys/server.key | wg pubkey | sudo tee /etc/wireguard/keys/server.key.pub
```

(crea llave publica y privada)

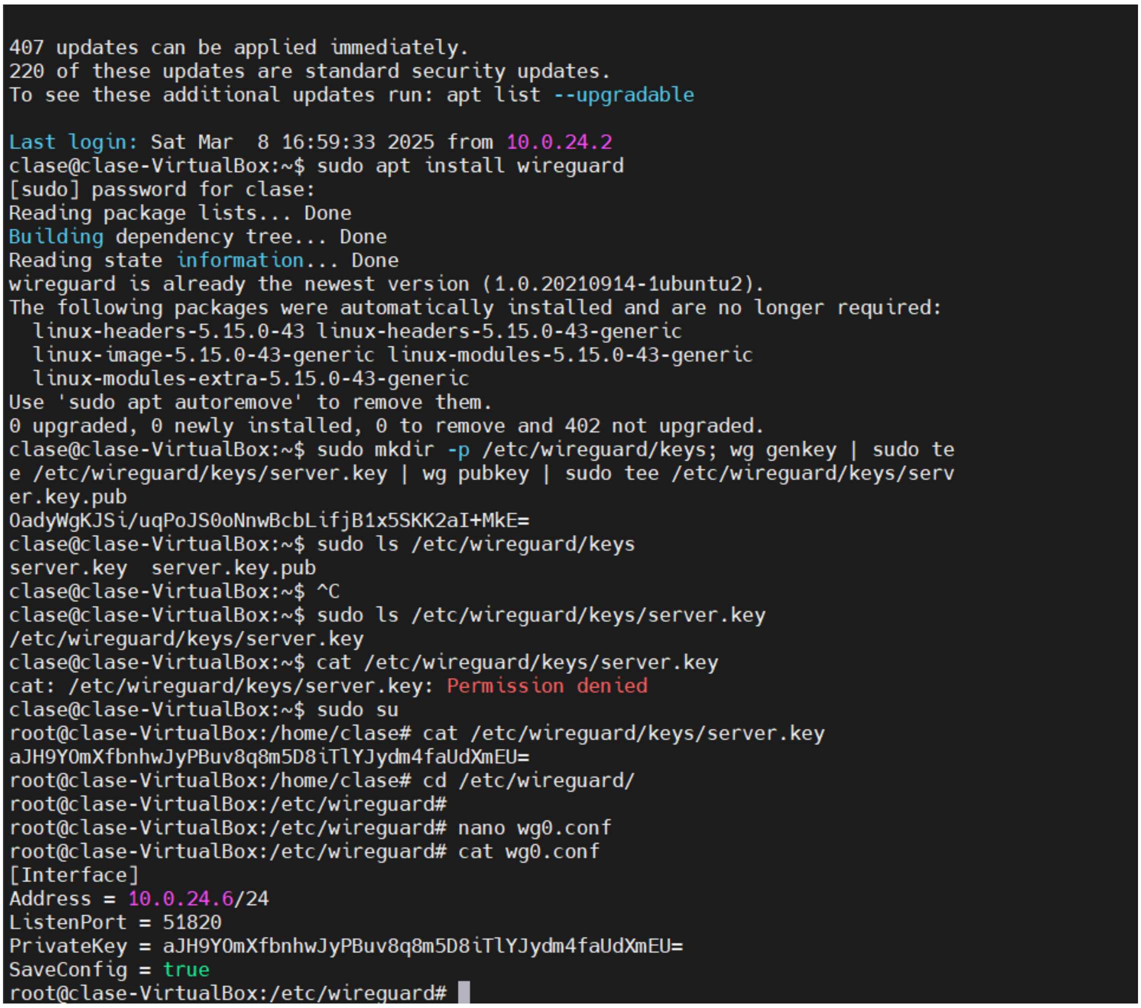
```
sudo ls /etc/wireguard/keys
```

(esto mira la carpeta de las llaves)

Nano wg0.conf:

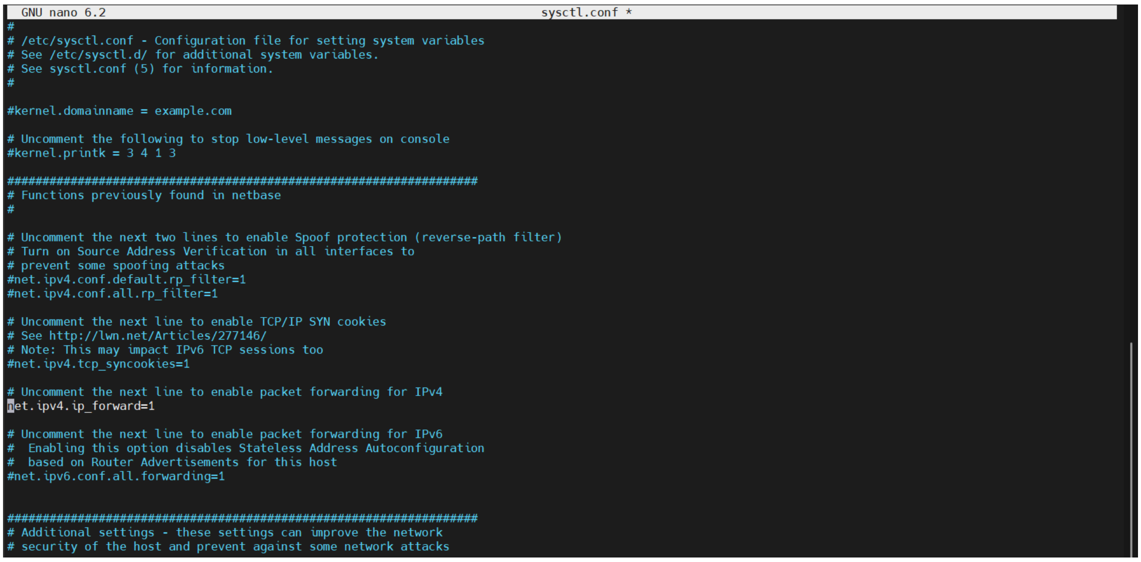
```
[Interface]

Address = 10.0.24.6/24

ListenPort = 51820

PrivateKey = aJH9YOmXfbnhwJyPBuv8q8m5D8iTlYJydm4faUdXmEU=

SaveConfig = true
```

Y hacemos un cat



```
407 updates can be applied immediately.
220 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Last login: Sat Mar  8 16:59:33 2025 from 10.0.24.2
clase@clase-VirtualBox:~$ sudo apt install wireguard
[sudo] password for clase:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wireguard is already the newest version (1.0.20210914-1ubuntu2).
The following packages were automatically installed and are no longer required:
  linux-headers-5.15.0-43 linux-headers-5.15.0-43-generic
  linux-image-5.15.0-43-generic linux-modules-5.15.0-43-generic
  linux-modules-extra-5.15.0-43-generic
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 402 not upgraded.
clase@clase-VirtualBox:~$ sudo mkdir -p /etc/wireguard/keys; wg genkey | sudo te
e /etc/wireguard/keys/server.key | wg pubkey | sudo tee /etc/wireguard/keys/serv
er.key.pub
OadyWgKJSi/uqPoJS0oNnwBcbLifjB1x5SKK2aI+MkE=
clase@clase-VirtualBox:~$ sudo ls /etc/wireguard/keys
server.key  server.key.pub
clase@clase-VirtualBox:~$ ^C
clase@clase-VirtualBox:~$ sudo ls /etc/wireguard/keys/server.key
/etc/wireguard/keys/server.key
clase@clase-VirtualBox:~$ cat /etc/wireguard/keys/server.key
cat: /etc/wireguard/keys/server.key: Permission denied
clase@clase-VirtualBox:~$ sudo su
root@clase-VirtualBox:/home/clase# cat /etc/wireguard/keys/server.key
aJH9YOmXfbnhwJyPBuv8q8m5D8iTlYJydm4faUdXmEU=
root@clase-VirtualBox:/home/clase# cd /etc/wireguard/
root@clase-VirtualBox:/etc/wireguard#
root@clase-VirtualBox:/etc/wireguard# nano wg0.conf
root@clase-VirtualBox:/etc/wireguard# cat wg0.conf
[Interface]
Address = 10.0.24.6/24
ListenPort = 51820
PrivateKey = aJH9YOmXfbnhwJyPBuv8q8m5D8iTlYJydm4faUdXmEU=
SaveConfig = true
root@clase-VirtualBox:/etc/wireguard# 
```

Hacemos sudo nano /etc/sysctl.conf

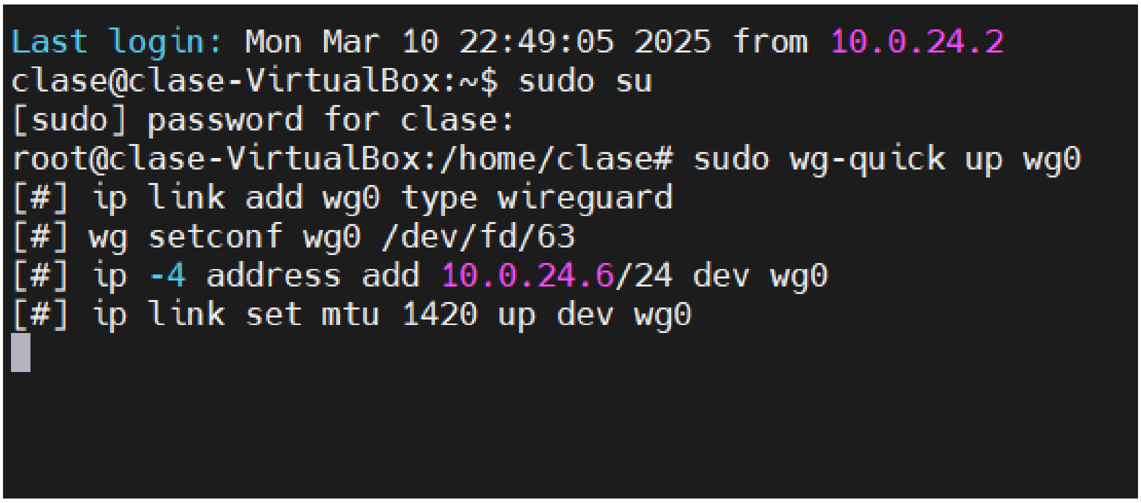


```
  GNU nano 6.2                                          sysctl.conf *
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#

#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

###################################################################
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1


###################################################################
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
```

root@clase-VirtualBox:/etc# sudo nano sysctl.conf

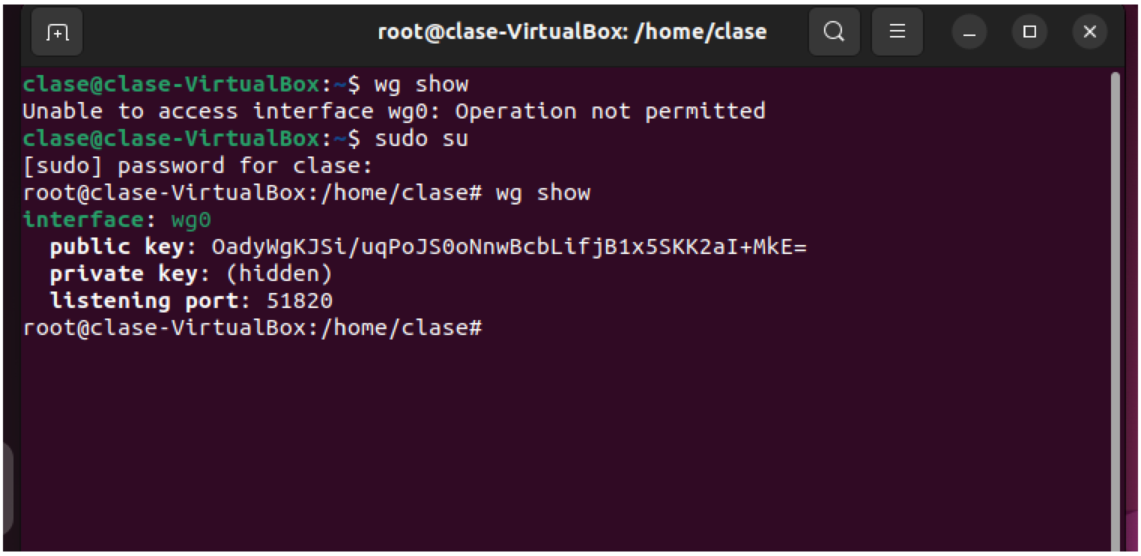
cd wireguard/

sudo wg-quick up wg0



```
Last login: Mon Mar 10 22:49:05 2025 from 10.0.24.2
clase@clase-VirtualBox:~$ sudo su
[sudo] password for clase:
root@clase-VirtualBox:/home/clase# sudo wg-quick up wg0
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 10.0.24.6/24 dev wg0
[#] ip link set mtu 1420 up dev wg0
```

cuando lo levantamos , se cae ssh , por lo tanto moba



```
clase@clase-VirtualBox:~$ wg show
Unable to access interface wg0: Operation not permitted
clase@clase-VirtualBox:~$ sudo su
[sudo] password for clase:
root@clase-VirtualBox:/home/clase# wg show
interface: wg0
  public key: OadyWgKJSi/uqPoJS0oNnwBcbLifjB1x5SKK2aI+MkE=
  private key: (hidden)
  listening port: 51820
root@clase-VirtualBox:/home/clase#
```

Prepare your server

sudo apt update && sudo apt upgrade

Check to see if your server needs a reboot:

```
cat /var/run/reboot-required
```

```
sudo reboot
```

Install WireGuard VPN Server

```
sudo apt install wireguard
```

Generate server keys

```
sudo mkdir -p /etc/wireguard/keys; wg genkey | sudo tee /etc/wireguard/keys/server.key | wg pubkey | sudo tee /etc/wireguard/keys/server.key.pub
```

```
cat /etc/wireguard/keys/server.key
```

Determine your “default” interface

Configure the “wireguard interface”

```
sudo nano /etc/wireguard/wg0.conf
```

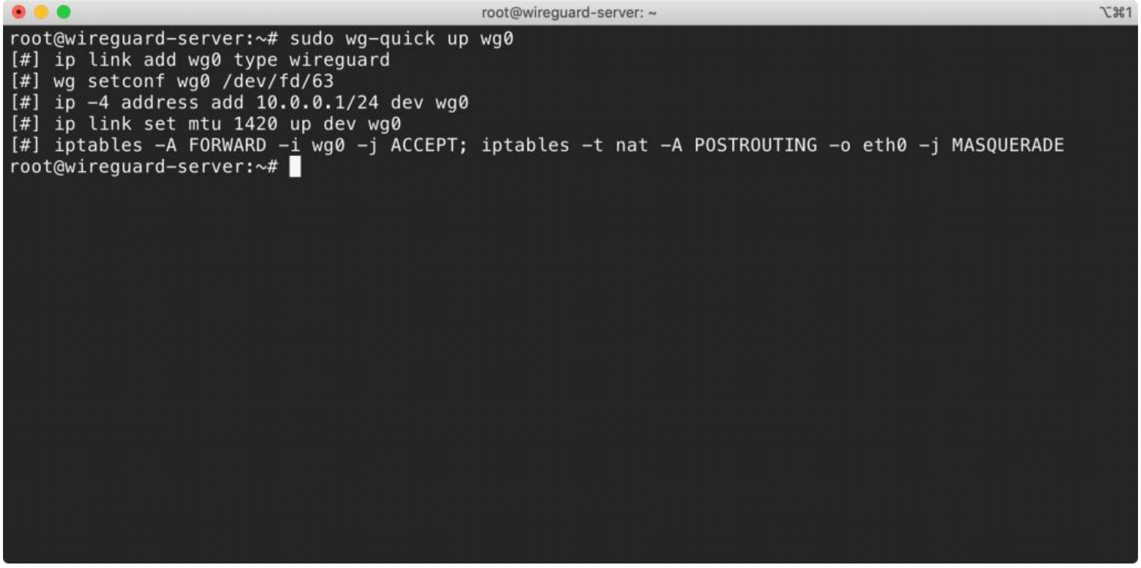
Contents of /etc/wireguard/wg0.conf:

```
[Interface]

Address = 10.0.0.1/24

ListenPort = 51820

PrivateKey = YOUR_SERVER_PRIVATE_KEY

PostUp = iptables -A FORWARD -i %i -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

PostDown = iptables -D FORWARD -i %i -j ACCEPT; iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE

SaveConfig = true
```

Bring up the “wireguard interface”

```
sudo wg-quick up wg0
```

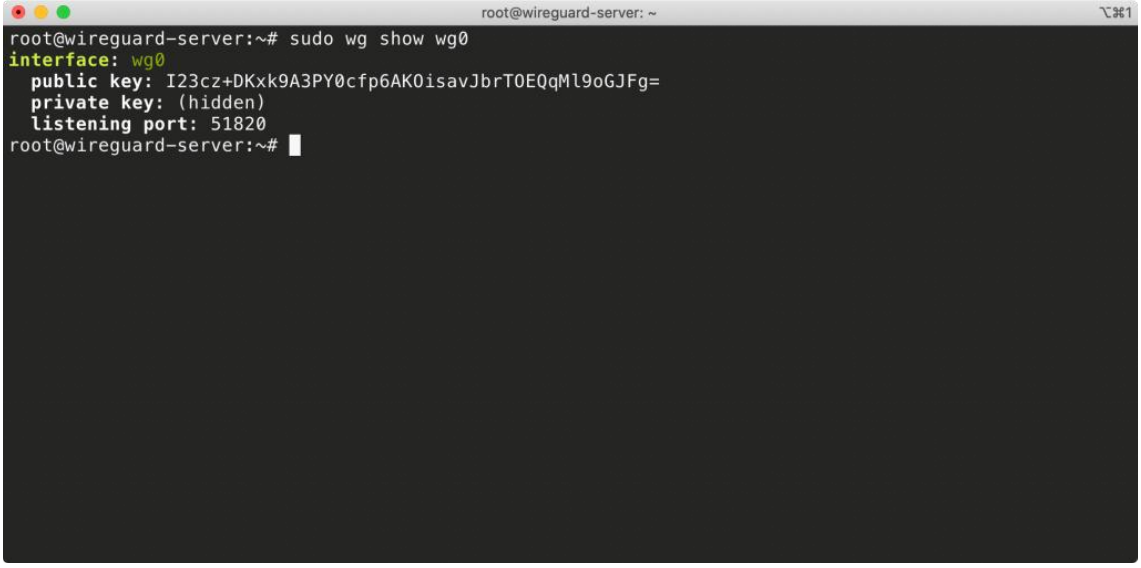
You should get output similar to the screenshot below



```
root@wireguard-server:~# sudo wg-quick up wg0
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 10.0.0.1/24 dev wg0
[#] ip link set mtu 1420 up dev wg0
[#] iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
root@wireguard-server:~# 
```

We can check the status of the **wg0** interface by running this command:

sudo wg show wg0



```
root@wireguard-server:~# sudo wg show wg0
interface: wg0
  public key: I23cz+DKxk9A3PY0cfp6AKOisavJbrTOEQqMl9oGJFg=
  private key: (hidden)
  listening port: 51820
root@wireguard-server:~# 
```

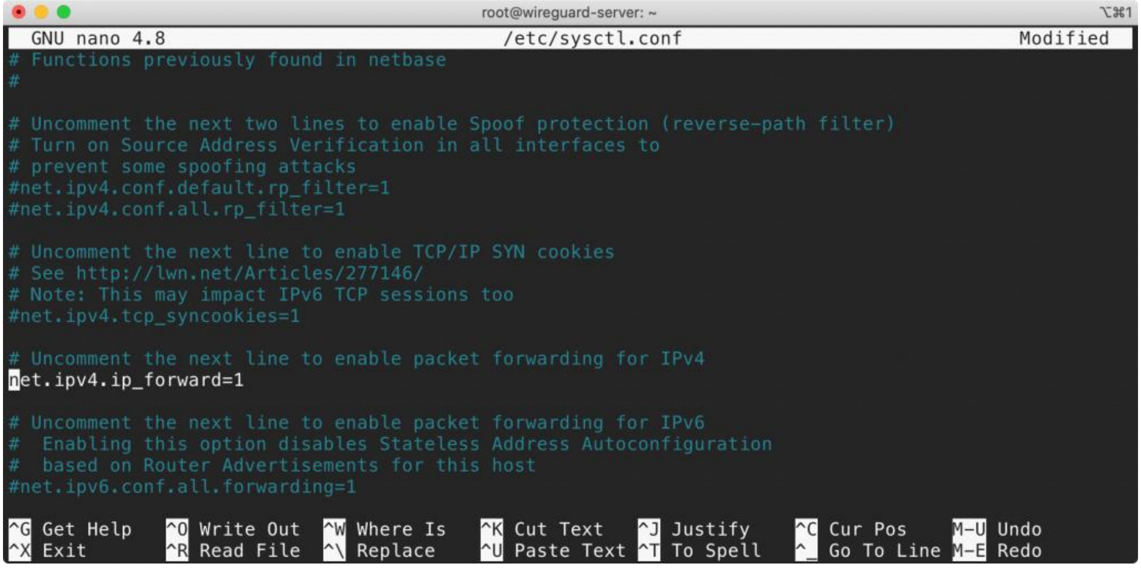
Start the “wireguard interface” automatically at boot

sudo systemctl enable wg-quick@wg0

Allow traffic forwarding

sudo nano /etc/sysctl.conf

You need to uncomment the line that says **net.ipv4.ip_forward=1**. It should look like this:



```
root@wireguard-server: ~                                                    ⌥⌘1
  GNU nano 4.8                      /etc/sysctl.conf                      Modified
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line  M-E Redo
```

TO SAVE: While in **nano**, press **CTRL + O** to save and **CTRL + X** to quit.

Apply our changes after saving:

sudo sysctl -p

---

sudo apt install wireguard

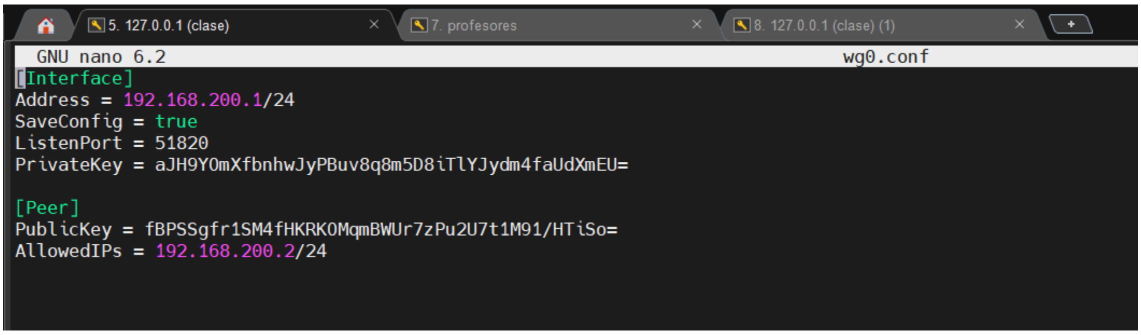
sudo mkdir -p /etc/wireguard/keys; wg genkey | sudo tee /etc/wireguard/keys/server.key | wg pubkey | sudo tee /etc/wireguard/keys/server.key.pub

(crea llave publica y privada)

sudo ls /etc/wireguard/keys

(esto mira la carpeta de las llaves)

Nano wg0.conf: tiene que estar creado al lado de carpeta keys.



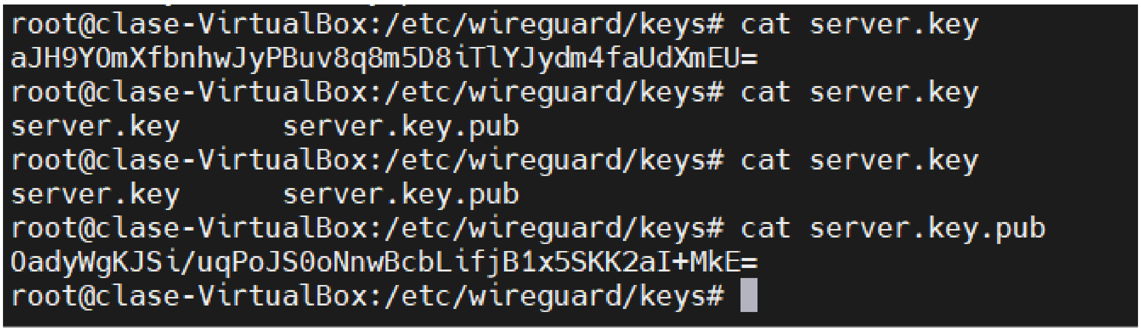
```
  GNU nano 6.2                                                   wg0.conf
[Interface]
Address = 192.168.200.1/24
SaveConfig = true
ListenPort = 51820
PrivateKey = aJH9YOmXfbnhwJyPBuv8q8m5D8iTlYJydm4faUdXmEU=

[Peer]
PublicKey = fBPSSgfr1SM4fHKRKOMqmBWUr7zPu2U7t1M91/HTiSo=
AllowedIPs = 192.168.200.2/24
```

Para hacer cualquier tipo de modicicacion, primero tener el wg-quick down wg0

Luego modificar, y despues hacer el wg-quick up wg0

Creamos la red esta imaginaria, la 200.1 y la 200.2

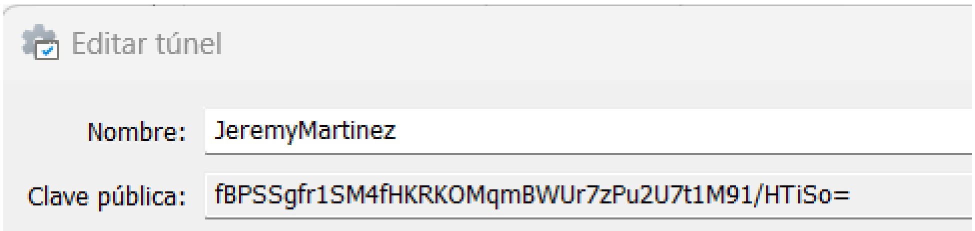
El peer que tenemos en el ubuntu, es la interface de la de wireguard



```
root@clase-VirtualBox:/etc/wireguard/keys# cat server.key
aJH9YOmXfbnhwJyPBuv8q8m5D8iTlYJydm4faUdXmEU=
root@clase-VirtualBox:/etc/wireguard/keys# cat server.key
server.key      server.key.pub
root@clase-VirtualBox:/etc/wireguard/keys# cat server.key
server.key      server.key.pub
root@clase-VirtualBox:/etc/wireguard/keys# cat server.key.pub
OadyWgKJSi/uqPoJS0oNnwBcbLifjB1x5SKK2aI+MkE=
root@clase-VirtualBox:/etc/wireguard/keys# 
```

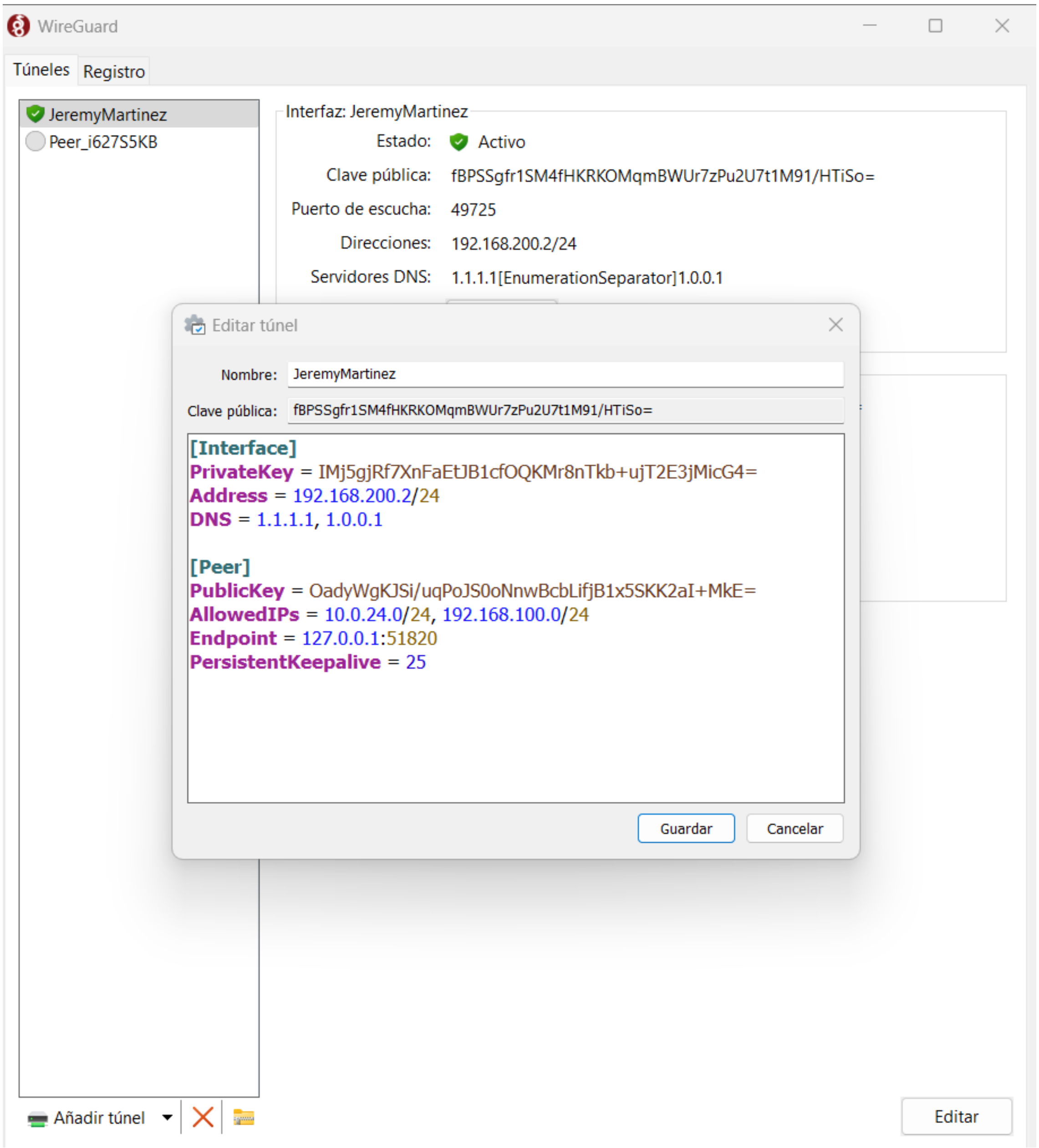
En el interface de ubuntu , foto de arriba, ponemos en private key.

La llave de el peer de la 200.2 de la foto de arriba, es la que nos genera al crear el tunel de wireguard



Nombre: JeremyMartinez

Clave pública: fBPSSgfr1SM4fHKRKOMqmBWUr7zPu2U7t1M91/HTiSo=



JeremyMartinez

Peer_i627S5KB

Interfaz: JeremyMartinez

Estado: Activo

Clave pública: fBPSSgfr1SM4fHKRKOMqmBWUr7zPu2U7t1M91/HTiSo=

Puerto de escucha: 49725

Direcciones: 192.168.200.2/24

Servidores DNS: 1.1.1.1[EnumerationSeparator]1.0.0.1

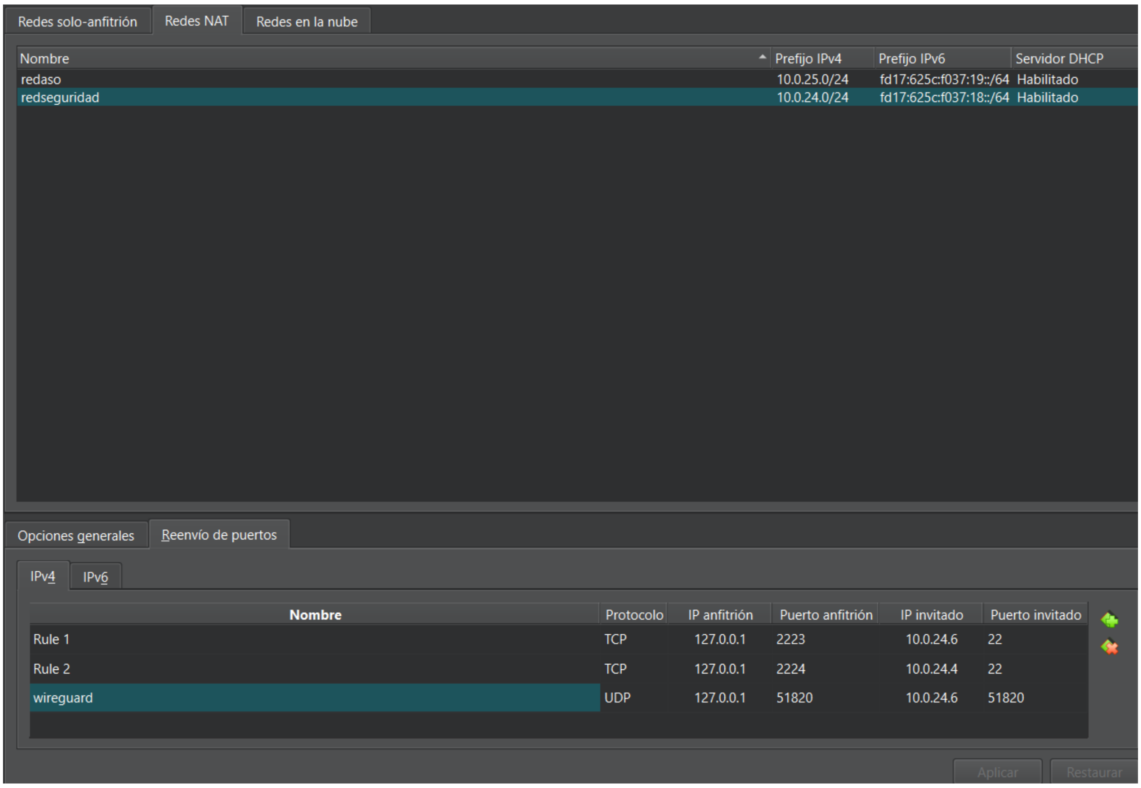
Nombre: JeremyMartinez

Clave pública: fBPSSgfr1SM4fHKRKOMqmBWUr7zPu2U7t1M91/HTiSo=

```
[Interface]
PrivateKey = IMj5gjRf7XnFaEtJB1cfOQKMr8nTkb+ujT2E3jMicG4=
Address = 192.168.200.2/24
DNS = 1.1.1.1, 1.0.0.1

[Peer]
PublicKey = OadyWgKJSi/uqPoJS0oNnwBcbLifjB1x5SKK2aI+MkE=
AllowedIPs = 10.0.24.0/24, 192.168.100.0/24
Endpoint = 127.0.0.1:51820
PersistentKeepalive = 25
```

```
[Interface]

PrivateKey = IMj5gjRf7XnFaEtJB1cfOQKMr8nTkb+ujT2E3jMicG4=

Address = 192.168.200.2/24

DNS = 1.1.1.1, 1.0.0.1


[Peer]

PublicKey = OadyWgKJSi/uqPoJS0oNnwBcbLifjB1x5SKK2aI+MkE=

AllowedIPs = 10.0.24.0/24, 192.168.100.0/24

Endpoint = 127.0.0.1:51820

PersistentKeepalive = 25
```

Para inspirarme, asi esta bien la estructura



Nombre	Prefijo IPv4	Prefijo IPv6	Servidor DHCP
redaso	10.0.25.0/24	fd17:625c:f037:19::/64	Habilitado
redseguridad	10.0.24.0/24	fd17:625c:f037:18::/64	Habilitado

Nombre	Protocolo	IP anfitrión	Puerto anfitrión	IP invitado	Puerto invitado
Rule 1	TCP	127.0.0.1	2223	10.0.24.6	22
Rule 2	TCP	127.0.0.1	2224	10.0.24.4	22
wireguard	UDP	127.0.0.1	51820	10.0.24.6	51820

root-truenas