EJERCICIO: Crear una VPN sencilla con WireGuard

🎯 Objetivo

Aprender a crear una **VPN punto a punto** con **WireGuard**, usando pares de claves públicas y privadas para autenticación.

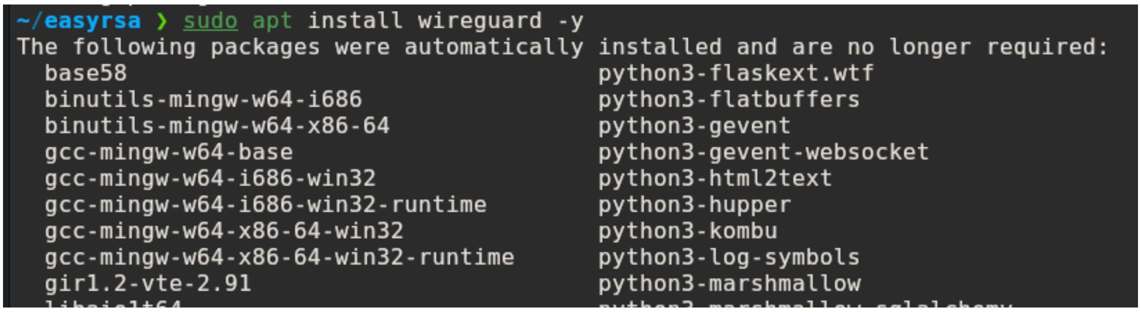
🧰 Requisitos

Dos máquinas virtuales Linux (por ejemplo, Kali o Ubuntu):

- una será el **servidor**
- otra el **cliente**

Instala WireGuard en ambas:

```
sudo apt update

sudo apt install wireguard -y
```



```
~/easyrsa ❯ sudo apt install wireguard -y
The following packages were automatically installed and are no longer required:
  base58                                  python3-flaskext.wtf
  binutils-mingw-w64-i686                 python3-flatbuffers
  binutils-mingw-w64-x86-64               python3-gevent
  gcc-mingw-w64-base                      python3-gevent-websocket
  gcc-mingw-w64-i686-win32                python3-html2text
  gcc-mingw-w64-i686-win32-runtime        python3-hupper
  gcc-mingw-w64-x86-64-win32              python3-kombu
  gcc-mingw-w64-x86-64-win32-runtime      python3-log-symbols
  gir1.2-vte-2.91                         python3-marshmallow
```

🔹 1. Crear las claves

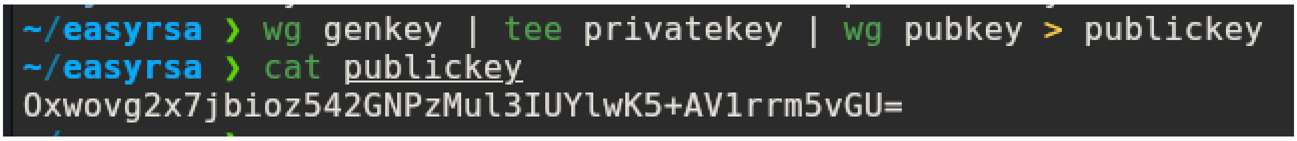
En cada máquina (servidor y cliente):

wg genkey | tee privatekey | wg pubkey > publickey

Esto genera:

- privatekey → clave privada
- publickey → clave pública

📍 Guarda esas claves, las necesitarás para configurar los peers.



```
~/easyrsa ❯ wg genkey | tee privatekey | wg pubkey > publickey
~/easyrsa ❯ cat publickey
0xwovg2x7jbioz542GNPzMul3IUYlwK5+AV1rrm5vGU=
```

---

2. Configurar el servidor

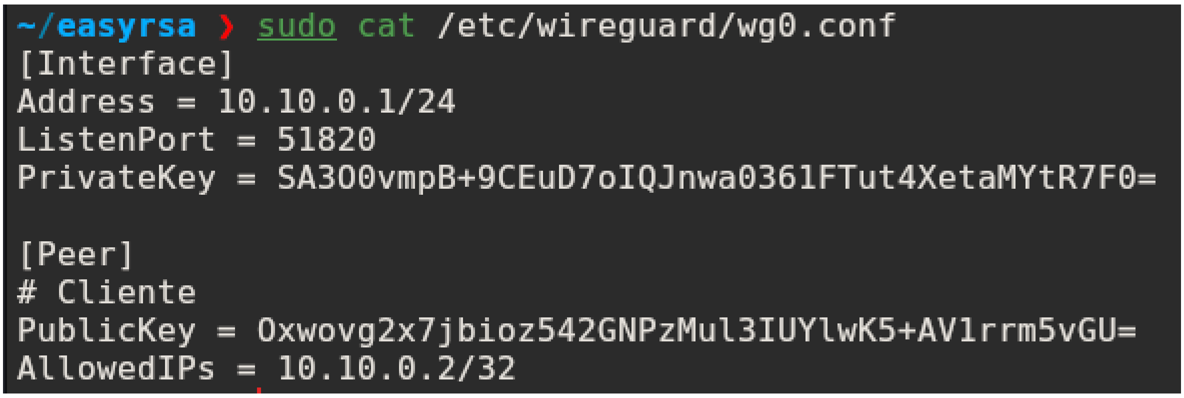
Edita el archivo /etc/wireguard/wg0.conf:

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

Pega esto (ajusta la IP de red y el puerto):

```
[Interface]
Address = 10.10.0.1/24
ListenPort = 51820
PrivateKey = (aquí la clave privada del servidor)

[Peer]
# Cliente
PublicKey = (clave pública del cliente)
AllowedIPs = 10.10.0.2/32
```

Guarda y cierra (**Ctrl + O**, Enter, **Ctrl + X**).



```
~/easyrsa ❯ sudo cat /etc/wireguard/wg0.conf
[Interface]
Address = 10.10.0.1/24
ListenPort = 51820
PrivateKey = SA3O0vmpB+9CEuD7oIQJnwa0361FTut4XetaMYtR7F0=

[Peer]
# Cliente
PublicKey = Oxwovg2x7jbioz542GNPzMul3IUYlwK5+AV1rrm5vGU=
AllowedIPs = 10.10.0.2/32
```

3. Configurar el cliente

En el cliente, edita:

sudo nano /etc/wireguard/wg0.conf

Pega esto:

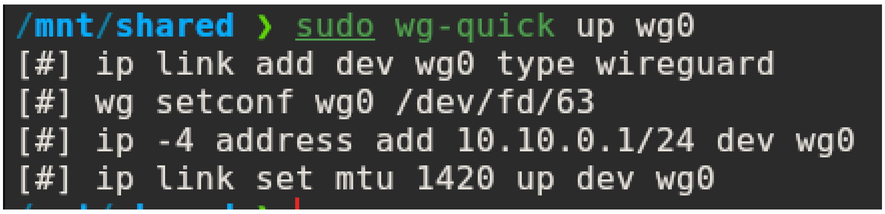
```
[Interface]
Address = 10.10.0.2/24
PrivateKey = (clave privada del cliente)
```

```
[Peer]

# Servidor

PublicKey = (clave pública del servidor)

Endpoint = <IP_del_servidor>:51820

AllowedIPs = 10.10.0.0/24

PersistentKeepalive = 20
```

🔹 4. Activar la VPN

En ambas máquinas:

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

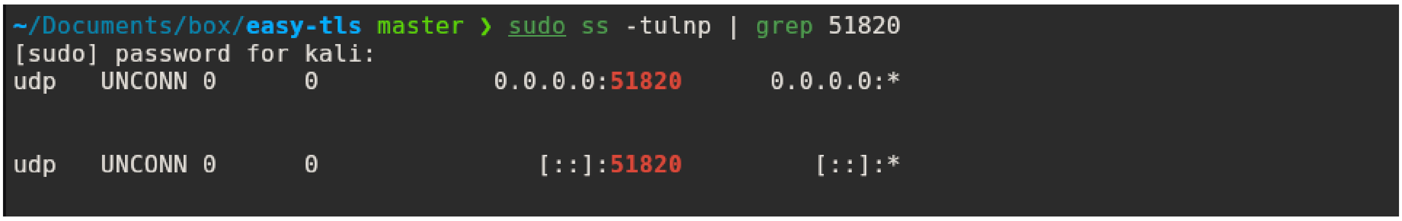


```
/mnt/shared ❯ sudo wg-quick up wg0
[#] ip link add dev wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 10.10.0.1/24 dev wg0
[#] ip link set mtu 1420 up dev wg0
```

✅ Si todo está bien, verás algo como:

```
[#] ip link add wg0 type wireguard

[#] wg setconf wg0 /dev/fd/63

[#] ip -4 address add 10.10.0.1/24 dev wg0

[#] ip link set mtu 1420 up dev wg0

[#] ip -4 route add 10.10.0.2/32 dev wg0
```

🔹 5. Comprobar la conexión

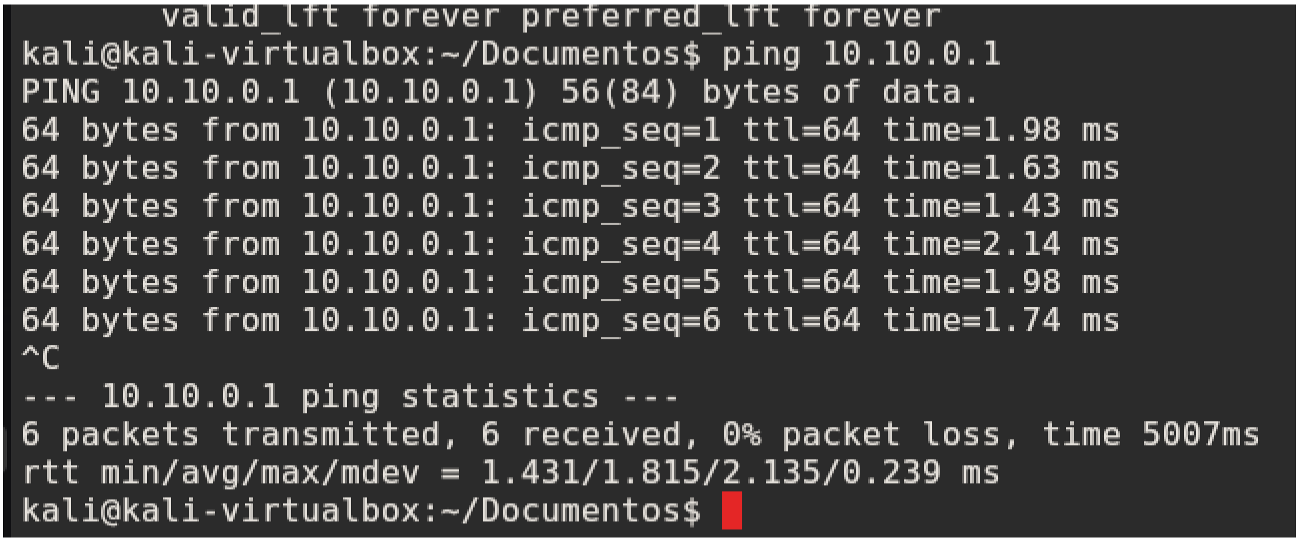


```
~/Documents/box/easy-tls master ❯ sudo ss -tulnp | grep 51820
[sudo] password for kali:
udp   UNCONN 0      0            0.0.0.0:51820      0.0.0.0:*


udp   UNCONN 0      0               [::]:51820         [::]:*
```

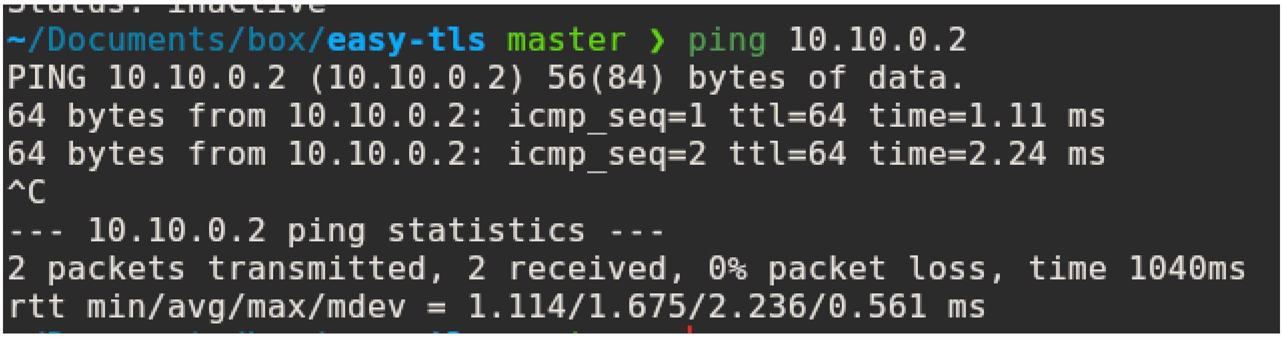
En el cliente:

```
ping 10.10.0.1
```

Si responde, la VPN está funcionando 🎉



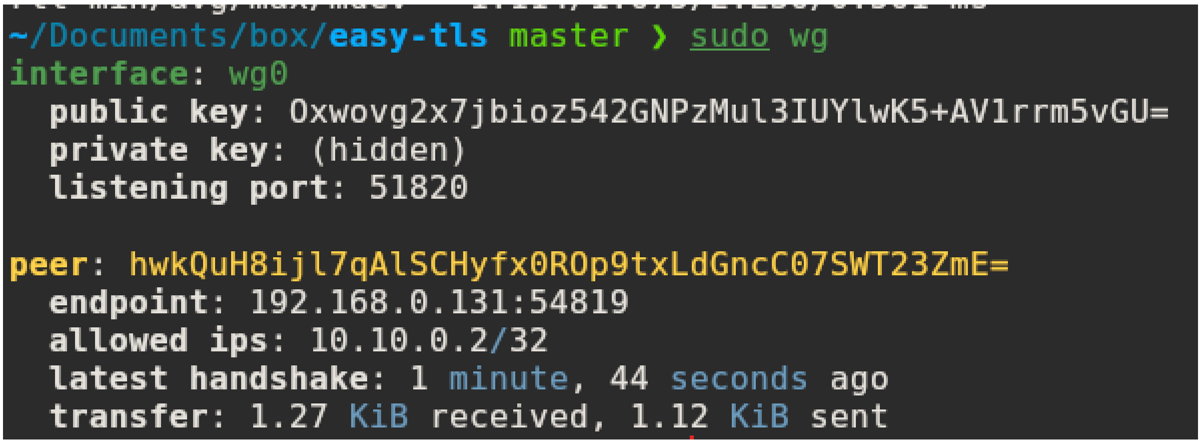
```
       valid_lft forever preferred_lft forever
kali@kali-virtualbox:~/Documentos$ ping 10.10.0.1
PING 10.10.0.1 (10.10.0.1) 56(84) bytes of data.
64 bytes from 10.10.0.1: icmp_seq=1 ttl=64 time=1.98 ms
64 bytes from 10.10.0.1: icmp_seq=2 ttl=64 time=1.63 ms
64 bytes from 10.10.0.1: icmp_seq=3 ttl=64 time=1.43 ms
64 bytes from 10.10.0.1: icmp_seq=4 ttl=64 time=2.14 ms
64 bytes from 10.10.0.1: icmp_seq=5 ttl=64 time=1.98 ms
64 bytes from 10.10.0.1: icmp_seq=6 ttl=64 time=1.74 ms
^C
--- 10.10.0.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 1.431/1.815/2.135/0.239 ms
kali@kali-virtualbox:~/Documentos$
```



```
~/Documents/box/easy-tls master ❯ ping 10.10.0.2
PING 10.10.0.2 (10.10.0.2) 56(84) bytes of data.
64 bytes from 10.10.0.2: icmp_seq=1 ttl=64 time=1.11 ms
64 bytes from 10.10.0.2: icmp_seq=2 ttl=64 time=2.24 ms
^C
--- 10.10.0.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1040ms
rtt min/avg/max/mdev = 1.114/1.675/2.236/0.561 ms
```

Puedes ver el estado:

```
sudo wg
```



```
~/Documents/box/easy-tls master ❯ sudo wg
interface: wg0
  public key: Oxwovg2x7jbioz542GNPzMul3IUYlwK5+AV1rrm5vGU=
  private key: (hidden)
  listening port: 51820

peer: hwkQuH8ijl7qAlSCHyfx0ROp9txLdGncC07SWT23ZmE=
  endpoint: 192.168.0.131:54819
  allowed ips: 10.10.0.2/32
  latest handshake: 1 minute, 44 seconds ago
  transfer: 1.27 KiB received, 1.12 KiB sent
```