🛡️ Configuración de WireGuard VPN

🔍 Ver estado del servicio

wg show

▶️ Iniciar y activar el servicio

systemctl start wireguard.service

systemctl enable wireguard.service

systemctl restart wireguard.service

📁 Ubicación de archivos de configuración y claves

/etc/wireguard

🛠️ Creación del VPN

1. 🔄 Actualizar el sistema e instalar WireGuard

sudo apt update && sudo apt install wireguard

2. 🔑 Generar claves

wg genkey | tee servidorpriv.key | wg pubkey | tee servidor_public.key

---

⚙️ Configuración del archivo wg0.conf

🖊️ Crear el archivo

sudo nano wg0.conf

🧩 Parámetros del servidor

- **Address**: red virtual que se va a crear (ej. 10.10.0.1/24)
- **ListenPort**: puerto de escucha (ej. 51820)
- **PrivateKey**: clave privada del servidor
- **PostUp / PostDown**: comandos para enrutar el tráfico a través de la interfaz de red (ej. enp6s0)

```
[Interface]
Address = 10.10.10.1/24
ListenPort = 51820
PrivateKey = cDIRvBqinJb+44EL0e45YHe38XIuXEwsON7vttKlI18=
PostUp = ufw route allow in on wg0 out on enp6s0
PostDown = ufw route delete allow in on wg0 out on enp6s0
```

👥 Parámetros de los clientes (peers)

Por cada cliente se debe añadir un bloque [Peer] con:

- **PublicKey**: clave pública del cliente
- **AllowedIPs**: IP asignada al cliente (ej. 10.10.0.2/32)

```
[Peer]

#Cliente1
PublicKey = bMu3k/ISBKQ4RNF8/3Tg9DdlBt0xd0+NTzGVDN0Z2zw=
AllowedIPs = 10.10.10.2/32
```

🔥 Configuración del firewall

1. Permitir tráfico UDP en el puerto de WireGuard

ufw allow 51820/udp

2. Activar el reenvío de paquetes

sysctl -w net.ipv4.ip_forward=1

sudo sysctl -p

cat /proc/sys/net/ipv4/ip_forward

3. Añadir reglas NAT en UFW

Editar el archivo:

sudo nano /etc/ufw/before.rules

Agregar:

START WireGuard Rules

*nat

:POSTROUTING ACCEPT [0:0]

-A POSTROUTING -s 10.10.0.0/24 -o enp6s0 -j MASQUERADE

COMMIT

END WireGuard Rules

```
# Don't delete these required lines, otherwise there will be errors
#Wireguard
*nat
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -s 10.10.10.0/24 -o enp6s0 -j MASQUERADE
COMMIT
#End Wireguard
```

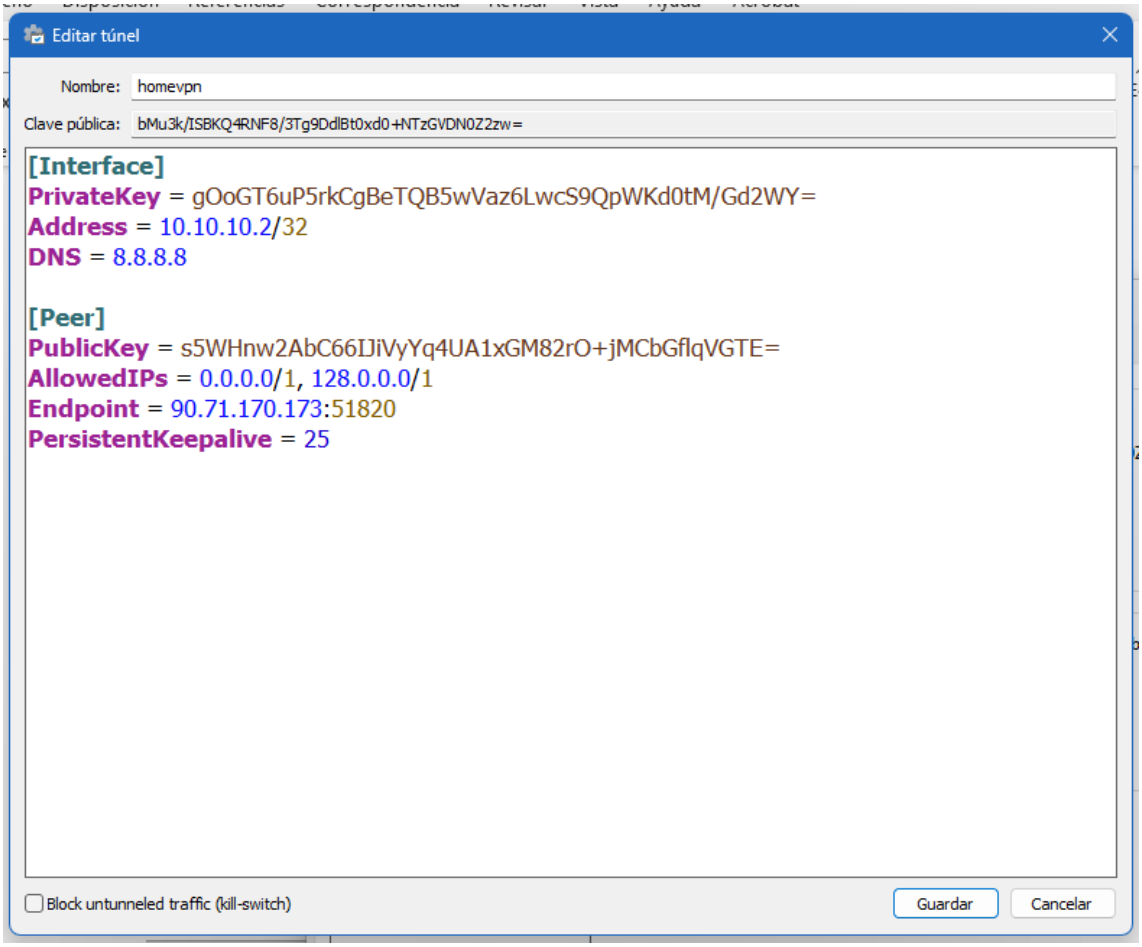
4. Reiniciar servicios

systemctl restart wireguard.service

ufw reload

💻 **Configuración del cliente**

- **Nombre**: identificador del cliente
- **PrivateKey**: clave privada del cliente
- **Address**: IP asignada (ej. 10.10.0.2/32)
- **DNS**: servidor DNS (ej. 8.8.8.8)
- **Peer (servidor)**:
    - **PublicKey**: clave pública del servidor
    - **AllowedIPs**: 0.0.0.0/0 para enrutar todo el tráfico
    - **Endpoint**: IP pública del router + puerto del servidor (ej. mi.router.com:51820)



Configuración del router

Asegúrate de abrir el puerto UDP 51820 en el router para permitir la conexión externa al servidor WireGuard.