

VPN Propia: despliegue paso a paso

WireGuard ha cambiado las reglas de las VPN: configuración mínima, criptografía moderna e integrado en el kernel de Linux. En menos de media hora tienes tu propio túnel cifrado entre todos tus equipos.

PILA	TIEMPO	PASOS	PROBADO EN	SI PREFIERES QUE LO HAGA YO
WireGuard	~30 min	4	Ubuntu 24.04 LTS	70 €

Necesitas un VPS con un Ubuntu moderno (24.04 LTS) y el puerto UDP del túnel (51820 por defecto) abierto en UFW y en el firewall de tu proveedor.



Antes de copiar

En los comandos verás `tudominio.com`: sustitúyelo siempre por tu dominio real.

PASO 01 Instalar WireGuard

Está en los repositorios oficiales de Ubuntu. Activamos también el reenvío de paquetes para que el servidor pueda enrutar el tráfico de los clientes.

```
install.sh
```

```
sudo apt update && sudo apt install -y wireguard
echo "net.ipv4.ip_forward=1" | sudo tee /etc/sysctl.d/99-wireguard.conf
sudo sysctl --system
sudo ufw allow 51820/udp
```

PASO 02 Generar las claves del servidor

Cada extremo (el servidor y cada cliente) tiene su par de claves pública y privada. Genera primero las del servidor.

```
keys.sh
```

```
sudo -i
cd /etc/wireguard
umask 077
wg genkey | tee server.key | wg pubkey > server.pub
cat server.key    # anota la privada
cat server.pub    # anota la pública
```

PASO 03 Crear wg0.conf en el servidor

Pon en `PrivateKey` la clave privada anterior. Cada cliente nuevo se añade como un bloque `[Peer]`.

```
/etc/wireguard/wg0.conf
```

```
[Interface]
Address = 10.10.0.1/24
ListenPort = 51820
PrivateKey = <CLAVE_PRIVADA_SERVIDOR>
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

[Peer]
# Móvil
PublicKey = <CLAVE_PUBLICA_CLIENTE>
AllowedIPs = 10.10.0.2/32
```



Comprueba el nombre de tu interfaz

`eth0` es un ejemplo. En muchos VPS la interfaz se llama distinto (por ejemplo `ens6`). Míralo con `ip route | grep default` y cámbialo en las dos líneas.

PASO 04 Levantar el túnel y que arranque solo

Se activa como cualquier servicio de systemd, y con `enable` se levanta en cada reinicio.

```
enable.sh
```

```
sudo systemctl enable --now wg-quick@wg0  
sudo wg      # lista los clientes conectados
```



Cliente móvil

En la app oficial de WireGuard pulsa + , «Crear desde cero» y pega la configuración del cliente. Activa el túnel y verás un handshake en el servidor en pocos segundos.

¿Prefieres que lo haga por ti?

Lo implemento por ti por **70 €**, con la configuración de seguridad inicial y esta guía aplicada a tu servidor.