elurk informática

SOBERANÍA DIGITAL · GUÍA PASO A PASO

Monta tu propia VPN. WireGuard sobre pfSense.

Acceso remoto cifrado a tu red de siempre, desde el portátil o el móvil. Sin pagar una suscripción a una VPN comercial y sin entregarle tu tráfico a un tercero.

pfSense CE 2.7 o superior

Configuración de acceso remoto (road warrior)

Edición 2026

Antes de empezar

Una VPN comercial te cifra el tráfico, sí. Pero ese tráfico pasa por servidores que no son tuyos, de una empresa que decide qué registra y qué no. Cambias el ojo de tu operador por el ojo de otro.

Con WireGuard sobre tu pfSense el planteamiento es distinto: el túnel termina en **tu propio router**. Te conectas a tu red de casa o de la oficina como si estuvieras dentro, llegas a tus equipos y a tus servicios, y si quieres, sacas también tu navegación por tu propia línea. Tu disco. Tu control.

WireGuard es además rápido y minúsculo: unas pocas miles de líneas de código frente a las cientos de miles de IPsec u OpenVPN. Menos código es menos superficie donde algo puede fallar.

> **QUÉ VAS A CONSEGUIR**
>
> Un túnel cifrado permanente entre tus dispositivos y tu red. Cada equipo se conecta con su propia clave, lo das de alta o de baja en segundos, y eliges si solo accede a tu red local o si enruta también todo Internet por tu línea.

Lo que necesitas a mano

- [ ] Un firewall con **pfSense CE 2.7** o superior, ya funcionando, con acceso de administrador.
- [ ] Una **IP pública** en la WAN. Si es dinámica, configura antes un dominio dinámico (Dynamic DNS) en **Services ▸ Dynamic DNS** y usa ese nombre en lugar de la IP.
- [ ] Poder **abrir un puerto UDP** hacia el firewall. Si tu router del operador está delante en modo router, redirige ahí ese puerto; lo ideal es tener el pfSense con IP pública directa.
- [ ] La **app WireGuard** en cada dispositivo cliente: escritorio (Windows, macOS, Linux) o móvil (Android, iOS), descargada desde `wireguard.com/install` o la tienda oficial.

> **OJO**
>
> A lo largo de la guía usamos la red de túnel `10.6.6.0/24` y el puerto `51820` como ejemplo, y suponemos que tu red local es `192.168.1.0/24`. Cambia estos valores por los tuyos. La red del túnel debe ser **distinta** de tu red local y de cualquier red desde la que te conectes (por ejemplo, el wifi de un hotel).

1. Instala el paquete WireGuard

pfSense no trae WireGuard de fábrica, pero lo instala en un clic desde su gestor de paquetes.

Ruta

`System ▸ Package Manager ▸ Available Packages`

Busca `WireGuard`, pulsa **Install** y confirma. Al terminar tendrás un menú nuevo en `VPN ▸ WireGuard`.

NOTA

Mantén el paquete y el propio pfSense actualizados. Las correcciones de seguridad de un componente expuesto a Internet no son opcionales.

2. Crea el túnel (el lado servidor)

El túnel es el extremo que vive en tu pfSense y al que se conectarán todos tus dispositivos.

`VPN ▸ WireGuard ▸ Tunnels ▸ Add Tunnel`

CAMPO	VALOR
Enable Tunnel	Marcado
Description	`WG-AccesoRemoto`
Listen Port	`51820`
Interface Keys	Pulsa **Generate** para crear el par de claves del servidor
Interface Addresses	`10.6.6.1/24`

Guarda con **Save Tunnel** y luego **Apply Changes**.

OJO · ANÓTALO

Copia la **clave pública** del túnel (Public Key). La necesitarás en cada dispositivo cliente. La **clave privada** del servidor nunca sale del pfSense: ni la copies, ni la compartas.

3. Asigna y habilita la interfaz

Asignar el túnel como interfaz propia te da control fino del firewall y del enrutado. Es el camino limpio.

1. Ve a **Interfaces ▸ Assignments**. En *Available network ports* elige el túnel (`tun_wg0`) y pulsa **Add**.
2. Entra en la interfaz nueva (aparecerá como `OPT1` o similar). Marca **Enable**, ponle un nombre como `WIREGUARD` y deja *IPv4 Configuration Type* en **None** (la dirección ya la pusiste en el túnel).
3. Guarda y aplica.

> **POR QUÉ**
>
> Sin asignar la interfaz, las reglas viven en una pestaña genérica "WireGuard". Asignándola, tienes una pestaña propia con reglas, NAT y gateway tratados como cualquier otra interfaz. Más orden, menos sorpresas.

4. Da de alta cada dispositivo (peers)

Un *peer* es un dispositivo que se conecta: tu portátil, tu móvil, el portátil de un compañero. **Una clave por dispositivo.** No reutilices la misma configuración en dos sitios.

Primero, genera las claves en el propio dispositivo

Lo correcto es que la clave privada de cada cliente nazca y muera en ese cliente. En la app de escritorio o móvil, "Añadir túnel vacío" ya te genera el par. En Linux, por línea de comandos:

```
# Genera clave privada y su pública asociada
wg genkey | tee cliente.key | wg pubkey > cliente.pub
```

Te quedas con la **pública** del cliente para el siguiente paso. La privada se queda en el dispositivo.

Ahora, registra el peer en pfSense

VPN ▸ WireGuard ▸ Peers ▸ Add Peer

CAMPO	VALOR
Tunnel	El túnel `WG-AccesoRemoto` que creaste
Description	`Portatil-elurk` (un nombre por dispositivo)
Dynamic Endpoint	Marcado (el cliente se conecta desde IPs cambiantes)
Public Key	La **clave pública del cliente** generada arriba
Pre-shared Key	Pulsa **Generate**. Capa extra de cifrado simétrico, recomendable
Allowed IPs	`10.6.6.2/32` (la IP fija que asignas a ESTE dispositivo dentro del túnel)

Guarda y aplica. Para el segundo dispositivo, repite con `10.6.6.3/32`, el tercero `10.6.6.4/32`, y así sucesivamente.

> **OJO**
>
> En el lado servidor, **Allowed IPs** es un filtro: define qué IP de origen acepta de ese peer. Por eso aquí va un `/32` (una sola dirección). No confundir con el *Allowed IPs* del cliente, que significa otra cosa y lo verás en el paso 9.

5. Abre el puerto en el firewall (WAN)

Por defecto pfSense bloquea todo lo que entra por la WAN. Hay que dejar pasar el puerto de WireGuard.

Firewall ▸ Rules ▸ WAN ▸ Add

CAMPO	VALOR
Action	Pass
Interface	WAN
Protocol	UDP
Source	Any (o restringe a rangos de IP de confianza si los conoces)
Destination	WAN address
Destination Port Range	`51820` a `51820`
Description	`WireGuard entrante`

Guarda y aplica. Esta es la única puerta que abres a Internet, y solo deja pasar el protocolo cifrado.

6. Permite el tráfico dentro del túnel

Una cosa es aceptar la conexión (paso 5) y otra dejar que ese tráfico llegue a tu red. En la pestaña de la interfaz WireGuard se decide hasta dónde llega cada cliente.

Firewall ▸ Rules ▸ WIREGUARD ▸ Add

CAMPO	VALOR
Action	Pass
Interface	WIREGUARD
Protocol	Any
Source	`10.6.6.0/24` (la red del túnel)
Destination	Para empezar, *any*. Para afinar, solo tu red `192.168.1.0/24`

OJO · PRINCIPIO DE MÍNIMO PRIVILEGIO

Abrir *any* → *any* funciona, pero da a cada dispositivo acceso a todo. Si solo necesitas llegar a un servidor concreto (por ejemplo tu Nextcloud), crea la regla apuntando a esa IP y ese puerto. Menos puertas abiertas, menos que vigilar.

7. NAT de salida, solo si quieres túnel completo

¿Solo quieres llegar a tu red local? Sáltate este paso. **¿Quieres que todo tu Internet salga por tu línea** (útil en wifis públicos)? Entonces tu tráfico necesita enmascararse al salir por la WAN.

Firewall ▸ NAT ▸ Outbound

1. Cambia el modo a **Hybrid Outbound NAT** y guarda.
2. Añade una regla de mapeo:

CAMPO	VALOR
Interface	WAN
Source	`10.6.6.0/24`
Translation	Interface Address
Description	`NAT salida WireGuard`

Guarda y aplica. Con esto, cuando un cliente enrute todo su tráfico por el túnel, saldrá a Internet con la IP pública de tu pfSense.

8. DNS interno (para resolver nombres de tu red)

Si quieres que tus clientes resuelvan los nombres de tu red (y no filtren consultas DNS por fuera), apunta su DNS al pfSense y deja que el resolver acepte la red del túnel.

Services ▸ DNS Resolver (Unbound)

- En **Network Interfaces**, añade la interfaz `WIREGUARD` (además de LAN y Localhost) para que escuche también ahí.
- Si usas listas de acceso, asegúrate de que `10.6.6.0/24` está permitida.

En el cliente (paso 9) pondrás como DNS la IP del servidor en el túnel, `10.6.6.1`.

9. Configura el cliente

Toda la configuración del dispositivo cabe en un archivo de texto. Este es el patrón:

```
[Interface]
PrivateKey = <clave privada del cliente>
Address    = 10.6.6.2/32
DNS        = 10.6.6.1

[Peer]
PublicKey    = <clave pública del túnel (paso 2)>
PresharedKey = <clave precompartida del peer (paso 4)>
Endpoint     = vpn.tudominio.es:51820
AllowedIPs   = 192.168.1.0/24, 10.6.6.0/24
PersistentKeepalive = 25
```

Túnel dividido o túnel completo

La línea **AllowedIPs** del cliente decide qué tráfico entra en el túnel:

QUIERES…	ALLOWEDIPS DEL CLIENTE
Solo acceder a tu red local (túnel dividido)	`192.168.1.0/24, 10.6.6.0/24`
Que TODO tu Internet pase por tu línea (túnel completo)	`0.0.0.0/0, ::/0`

`PersistentKeepalive = 25` mantiene viva la conexión cuando hay un NAT por medio. `Endpoint` es tu IP pública o tu dominio dinámico, con el puerto del paso 2.

En el móvil: el código QR

La app de WireGuard para Android e iOS importa la configuración escaneando un QR. Genera el QR a partir del archivo del cliente:

```
# En cualquier equipo Linux con qrencode instalado
qrencode -t ansiutf8 < cliente.conf
```

Abre la app, pulsa **+ ▸ Escanear desde código QR**, apunta a la pantalla, y listo.

> **OJO**
>
> Ese QR **es** la llave de tu red: contiene la clave privada. Trátalo como una contraseña. No lo mandes por WhatsApp ni lo dejes en una carpeta compartida. Genéralo, escanéalo, y borra el archivo.

10. Comprueba que funciona

- [ ] En pfSense, `VPN ▸ WireGuard ▸ Status`: el peer debe mostrar un **Latest Handshake** reciente (segundos). Si no hay handshake, el problema casi siempre está en el paso 5 (puerto) o en el `Endpoint` del cliente.
- [ ] Desde el cliente conectado, haz `ping 10.6.6.1`. Debe responder.
- [ ] Intenta llegar a un equipo de tu red, por ejemplo `ping 192.168.1.10` o abre tu Nextcloud por su IP local.
- [ ] Si montaste túnel completo, visita una web que muestre tu IP pública: debe ser la de tu pfSense, no la del wifi donde estás.

> **SI ALGO NO VA**
>
> Hay handshake pero no llegas a la red → revisa las reglas del paso 6. No hay handshake → puerto WAN (paso 5), o el router del operador no está reenviando el UDP 51820. Llegas a la red pero no navegas en túnel completo → falta el NAT del paso 7.

· Buenas prácticas que evitan disgustos

- **Una clave por dispositivo.** Si pierdes el móvil, borras solo ese peer en pfSense y el resto sigue intacto. Claves compartidas = revocar a ciegas.
- **La clave privada se queda en su dispositivo.** Genérala en el cliente, no en el servidor. Nadie más debería poder verla.
- **Usa clave precompartida (PSK).** Es una capa de cifrado simétrico extra, fácil de poner, gratis de tener.
- **Mínimo privilegio en el firewall.** Si un dispositivo solo necesita un servicio, no le abras toda la red.
- **Actualiza.** pfSense y el paquete WireGuard. Lo que mira a Internet se parchea.
- **Da de baja lo que ya no usas.** El portátil que se jubila, el peer que se borra. Una puerta que no usas no debería seguir abierta.

> **OJO · SIN MAGIA**
>
> Ninguna VPN, ni esta ni la más cara, te hace anónimo ni invulnerable. Lo que consigues aquí es concreto y honesto: tu tráfico cifrado de punta a punta y un acceso a tu red que controlas tú, no una empresa que vive de tus datos. La seguridad absoluta no existe; el control real, sí.

Ya tienes tu VPN. ¿Y ahora?

Has montado una pieza de soberanía digital de verdad: acceso remoto a tu red sin intermediarios. Es exactamente el tipo de cosa que hacemos en Elurk, montar infraestructura que controlas tú y enseñarte a usarla.

Si esto te ha resultado útil, en la **newsletter de Elurk** mandamos guías como esta y lo que vamos aprendiendo montando redes, servidores e IA local para empresas y particulares. Sin relleno y sin venderte humo.

Y si prefieres que lo montemos y lo mantengamos por ti, sobre tu pfSense o sobre uno nuevo, escríbenos a **info@elurk.com**. Te decimos con honestidad qué necesitas para tu caso real, ni más ni menos.

Elurk Informática · elurk.com · Tu informática, sin sorpresas.