



VPN

Wireguard

Instalación y configuración





VPN Wireguard

Configuración VPN con Wireguard

© Tecnocrática 2023

Indice

Indice.....	2
Características de la VPN Wireguard.....	3
Creación de un cliente Wireguard en el Panel	4
Instalación del cliente VPN Wireguard	6
Descarga	6
Configuración del cliente VPN Wireguard.....	9
Activación del túnel VPN.....	13
Observaciones finales.....	14

Características de la VPN Wireguard

El cliente VPN Wireguard, permite la conexión segura de los ordenadores de su organización a sus servidores alojados en los servicios CLOUD de Tecnocrática

WireGuard tiene como objetivo proporcionar una VPN que sea simple y altamente efectiva. En cuanto a la seguridad WireGuard utiliza Curve25519 para el intercambio de claves, ChaCha20 para la encriptación, Poly1305 para la autenticación de datos, SipHash para claves de hashtables y BLAKE2s para el hashing.

Protocolos todos altamente seguros, Curve25519 es una curva elíptica (ECC) que ofrece 256 bits de seguridad y está diseñada para su uso con el esquema de intercambio de clave Diffie-Hellman (ECDH) de curva elíptica. Es una de las curvas ECC más rápidas, con un alto nivel de seguridad

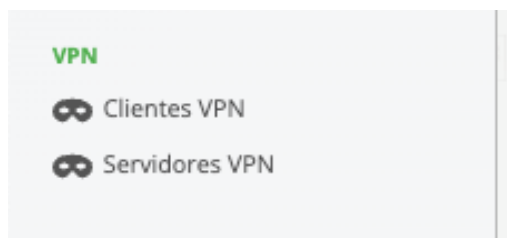
Creación de un cliente Wireguard en el Panel

El cliente VPN Wireguard se crea desde el panel de Tecnocrática en el área de Neodigit para ello nos dirigiremos al panel (<https://panel.neodigit.net>)

Introduciremos nuestro correo electrónico y nuestra contraseña del panel.

En la parte izquierda del panel tenemos una serie de opciones, abajo nos encontramos con dos opciones en VPN (como vemos en la imagen)

- Clientes VPN
- Servidor VPN



La opción de clientes VPN es un sistema de VPN que permite la navegación de forma segura.

La opción de servidor VPN, nos permite definir un servidor VPN al que vamos a asociar una serie de clientes que al usar la VPN podrán acceder a los recursos de la empresa, como por ejemplo los servidores de tu empresa alojados en la nube de Tecnocrática en nuestros centros de proceso de datos (CPD) , así como los recursos de las diferentes oficinas o delegaciones de la empresa a los que queramos que accedan los usuarios, si previamente se ha configurado o bien un equipo con conexión VPN al CPD o bien con el servicio DirectConnect de Tecnocrática.

Pulsando en Servidores VPN tendremos la lista de servidores VPN contratados, y pulsando en cualquiera de ellos (normalmente suele ser uno), nos aparecerá la lista de usuarios a los que queremos proporcionar el acceso VPN, pulsando en cualquiera de ellos, nos aparecerán las opciones de configuración:

Crear

Servidores VPN

Nombre

Crea cliente VPN

Transferencia

Solicitar baja

Servidor VPN vpn

NOMBRE

vpn

HOSTNAME

vpn

IPADDRESS (ADMIN)

REMOTEID (ADMIN)

ESTADO

Activo

DIRECCIÓN IPv4

DIRECCIÓN IPv6

EXPIRACIÓN

07/04/2023

CONTRASEÑA (ADMIN)

CLIENTES VPN (3/200)

Nombre

TestVPN1

TestVPN2

TestVPN3

Como vemos en esta pantalla tenemos lo siguiente:

En la parte superior izquierda, tenemos un botón que nos permite descargar el fichero que necesitaremos más adelante para configurar el túnel VPN en nuestro ordenador o dispositivo.

Las opciones de PUBKEY y PSK, son sólo para configuraciones avanzadas.

En la opción resaltada en azul claro, tenemos un enlace para descargar el programa de conexión VPN (Wireguard)

Por último, el código QR sirve para poder configurarlo en dispositivos móviles o tablets.

En esta caso, el código QR se ha tachado por privacidad, como el resto de los datos.

Descargar perfil

Transferencia

Eliminar

Cliente VPN test

NOMBRE

testpedro

DIRECCIÓN IPv4 (ADMIN)

10.

DIRECCIÓN IPv6 (ADMIN)

fd98: /128

PSK (ADMIN)

darmB14Uak


PUBKEY (ADMIN)

BAIQjdH1

SOFTWARE

Pincha aquí para descargar el cliente Wireguard

QR



PERFIL PERSONAL

Conexión de 10 Mbps simétricos

Instalación del cliente VPN Wireguard

Descarga

URL para las descargas

<https://www.wireguard.com/install/>

Aquí vemos varias opciones

The screenshot shows the WireGuard website's 'Installation' page. The header includes the WireGuard logo and navigation links: 'Installation', 'Quick Start', and 'Interworkings'. On the right side of the header are links for 'Whitepaper', 'Donate', and 'git'. A left sidebar lists various operating systems and their corresponding installation methods. The main content area, titled 'Installation', provides detailed instructions for each OS, including version compatibility and terminal commands for installation.

Installation

Windows [7, 8, 8.1, 10, 2012, 2016, 2019] - v0.3.3
Download Windows Installer
Browse MSIs

macOS [app store] - v0.0.20200127-17
Download from App Store

Ubuntu [module - v1.0.20201112 & tools - v1.0.20200827]
\$ sudo apt install wireguard

Android [play store - v1.0.20200927 & f-droid - v1.0.20200927]
Download from Play Store
Download from F-Droid

iOS [app store - v0.0.20200127-17]
Download from App Store

Debian [module - v1.0.20201112 & tools - v1.0.20200827]
apt install wireguard
Users with Debian releases older than Bullseye should enable backports.

Fedora [tools - v1.0.20200827]
\$ sudo dnf install wireguard-tools

Mageia [tools - v1.0.20200827]
\$ sudo urpmi wireguard-tools

Arch [module - v1.0.20201112 & tools - v1.0.20200827]
\$ sudo pacman -S wireguard-tools
Users of kernels < 5.6 may also choose wireguard-lts or wireguard-dkms + linux-headers, depending on which kernel is used.

OpenSUSE/SLE [tools - v1.0.20200827]
\$ sudo zypper install wireguard-tools

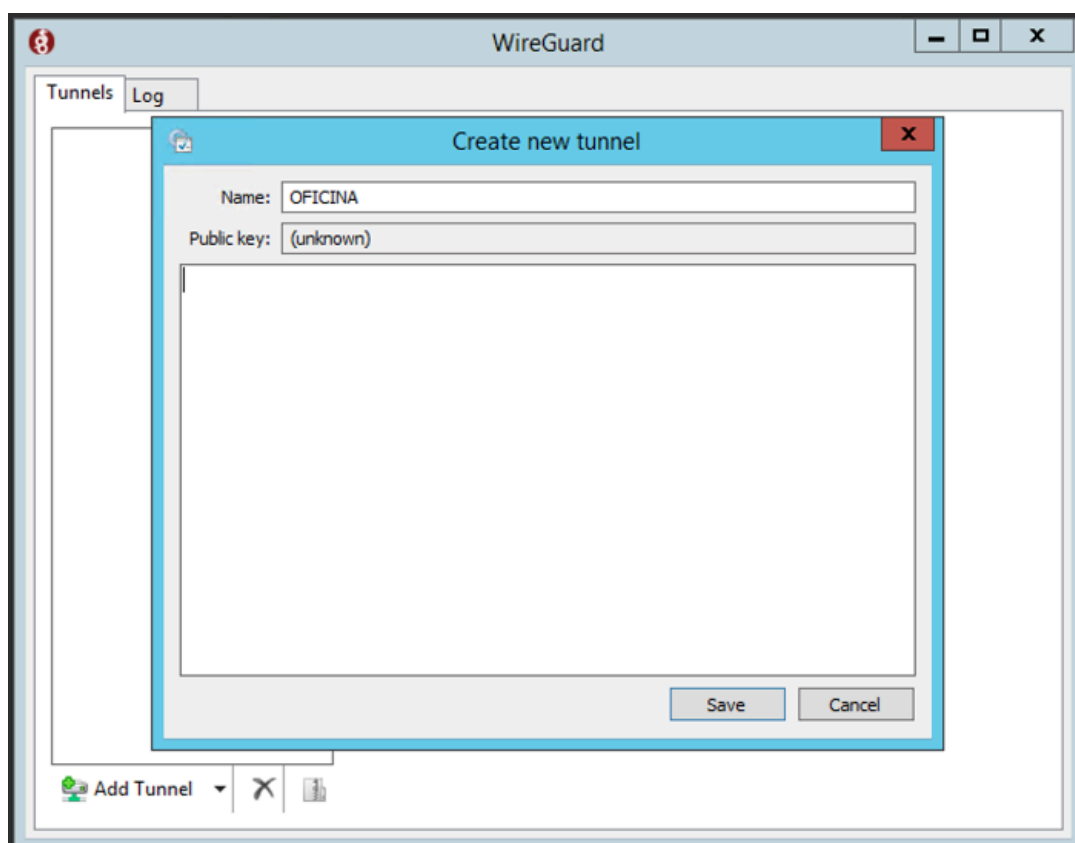
Slackware [module - v1.0.20201112 & tools - v1.0.20200827]
\$ for i in wireguard-linux-compat wireguard-tools; do wget https://slackbuilds.org/slackbuilds/14.2/network/\$i.tar.gz && tar -xzf \$i.tar.gz && cd \$i && OUTPUT=\$(pwd) ./\$i.SlackBuild && sudo upgradepkg --install-new ./\$i*.tgz && cd .; done

Left Sidebar:

- Installation
- Windows [7, 8, 8.1, 10, 2012, 2016, 2019]
- macOS [app store]
- Ubuntu [module & tools]
- Android [play store & f-droid]
- iOS [app store]
- Debian [module & tools]
- Fedora [tools]
- Mageia [tools]
- Arch [module & tools]
- OpenSUSE/SLE [tools]
- Slackware [module & tools]
- Alpine [module & tools]
- Gentoo [module & tools]
- Exherbo [module & tools]
- NixOS [module & tools]
- Nix on Darwin [userspace go & tools]
- OpenWRT [module & tools]
- Oracle Linux 8 [UEK6 & tools]
- Red Hat Enterprise Linux 8 [module-kmod, module-dkms, & tools]
- CentOS 8 [module-plus, module-kmod, module-dkms, & tools]
- Oracle Linux 7 [UEK6 & tools]
- Red Hat Enterprise Linux 7 [module-kmod, module-dkms, & tools]
- CentOS 7 [module-plus, module-kmod, module-dkms, & tools]
- FreeBSD [userspace go & tools]
- OpenBSD [tools]
- Termux [tools]

Elegiremos la versión acorde con nuestro sistema operativo.

La descargamos y procedemos a la instalación. El sistema nos preguntará en el caso de tener habilitado el control de cuentas de usuario, si deseamos instalarlo

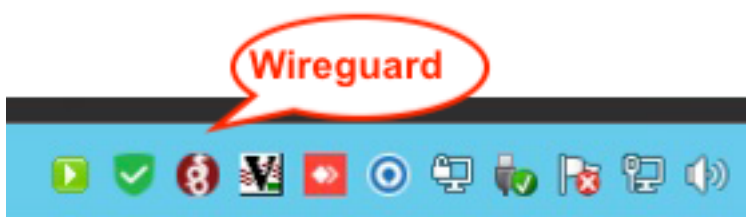


Confirmamos pulsando si, que deseamos instalarlo.

Una vez instalado, nos aparecerá una nueva aplicación en el menú de aplicaciones. Pulsando Inicio, nos aparecerá la aplicación Wireguard

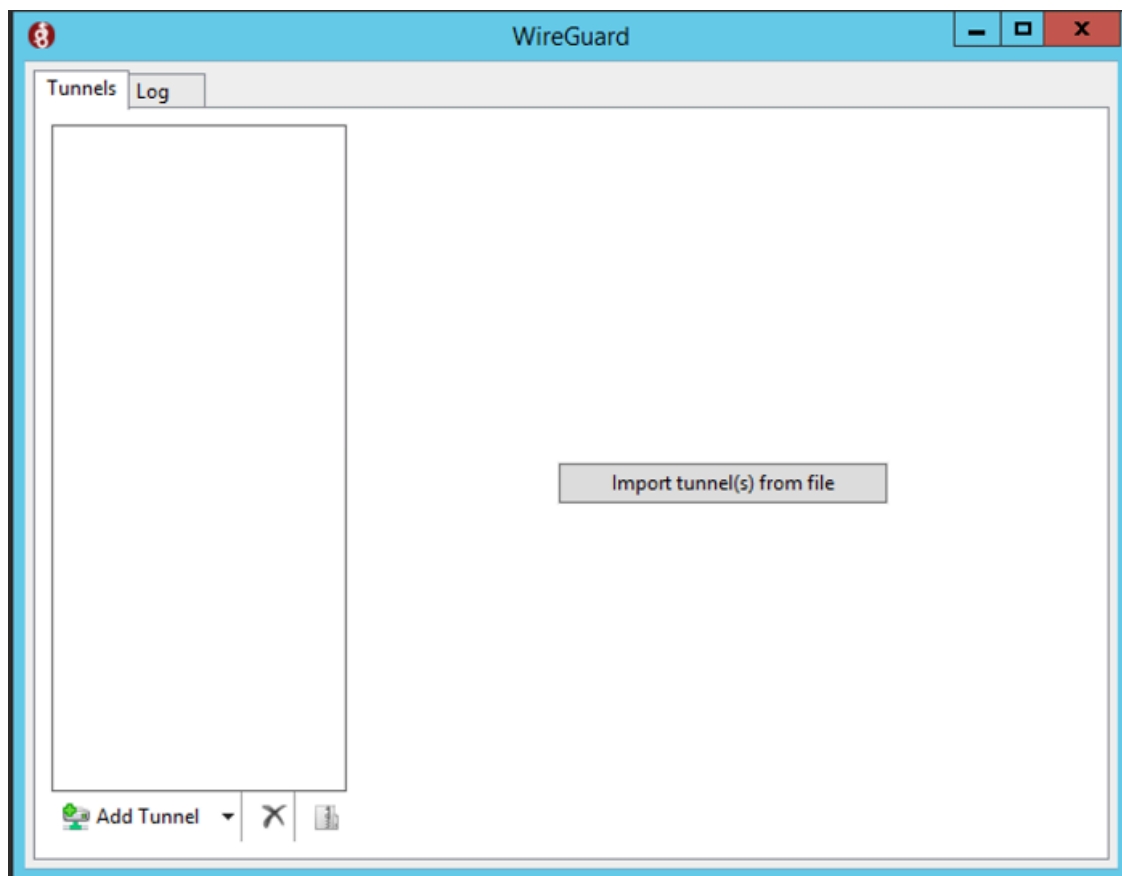


Cuando la iniciemos aparecerá un nuevo icono en el área de notificaciones del sistema (en la parte inferior derecha, donde está la hora). Pulsando en este icono, se lanzará la interfaz de configuración y administración

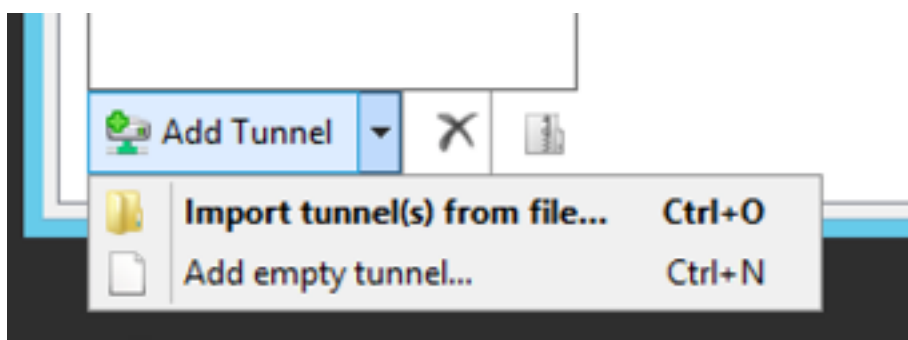


Configuración del cliente VPN Wireguard

En la ventana principal del cliente Wireguard, nos aparecerán las siguientes opciones:

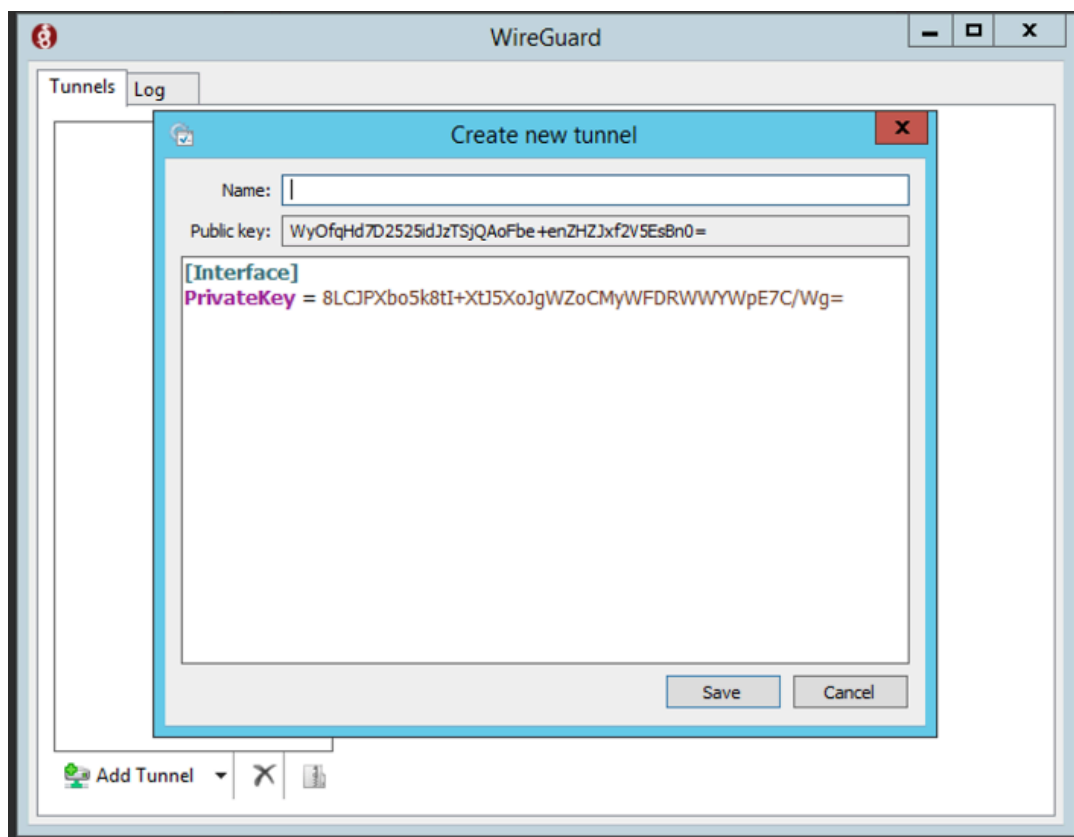


Para agregar nuestro túnel, seleccionaremos en la parte inferior (donde aparece Add Tunnel), y nos aparecerán dos opciones



Seleccionamos la opción de Add empty tunnel, y nos aparecerá una ventana como la que vemos en la siguiente imagen.

A partir de ahí vamos a proceder a configurar nuestro túnel.
En nombre pondremos el nombre que queramos (Oficina, Mi casa, etc)
A continuación borraremos todo lo que hay en la casilla inferior



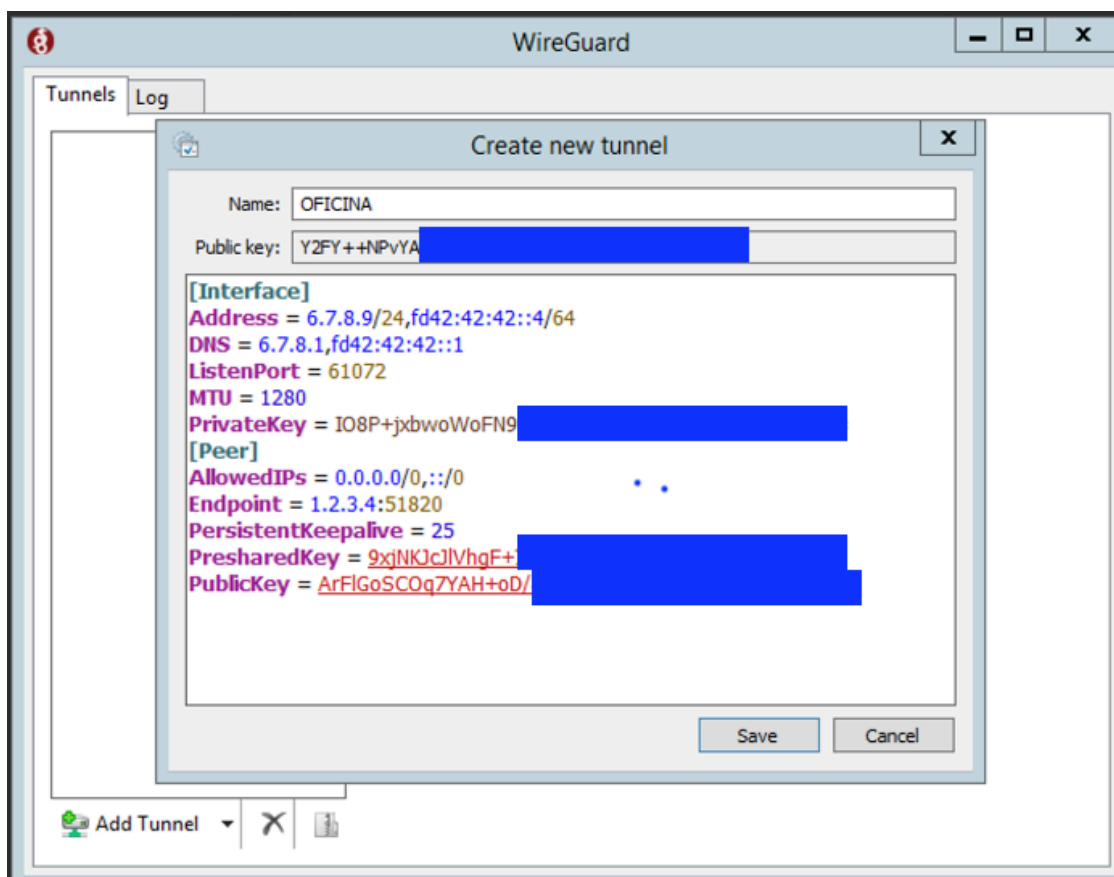
Deberá quedar como lo que aparece en la siguiente imagen

Habremos recibido un fichero de configuración, o un conjunto de instrucciones con la siguiente forma

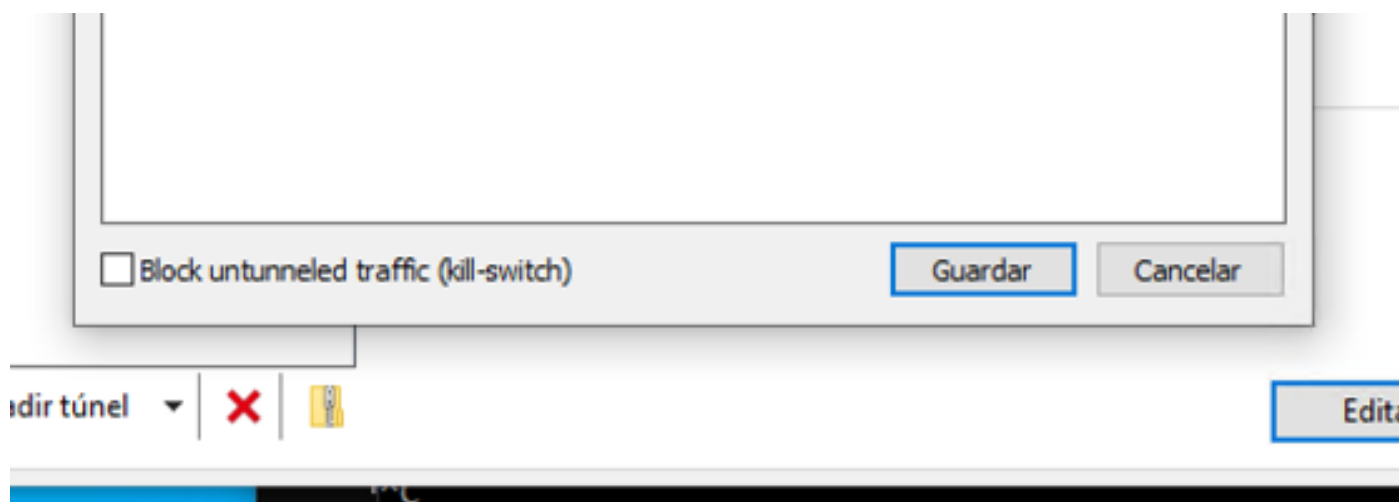
NOTA: Se han sustituido algunos caracteres por XXX por privacidad. Al igual que las direcciones IP

```
#Tecnocrática
[Interface]
Address = 6.7.8.9/24,fd42:42:42::4/64
DNS = 6.7.8.1,fd42:42:42::1
ListenPort = 61072
MTU = 1280
PrivateKey = IO8P+jxbwoWoFN93R9I9p+XXXXXXXXXXXXXXXXXXXX
[Peer]
AllowedIPs = 0.0.0.0/0,:::/0
Endpoint = 1.2.3.4:51820
PersistentKeepalive = 25
PresharedKey = 9xjNKJcJlVhgF+78JzSKXXXXXXXXXXXXXXXXXXXX
PublicKey = ArFlGoSCOq7YAH+oD/8GXXXXXXXXXXXXXXXXXXXX
```

Copiamos desde [Interface] hasta el final, y lo pegamos en nuestra configuración, quedando como se ve en la siguiente imagen

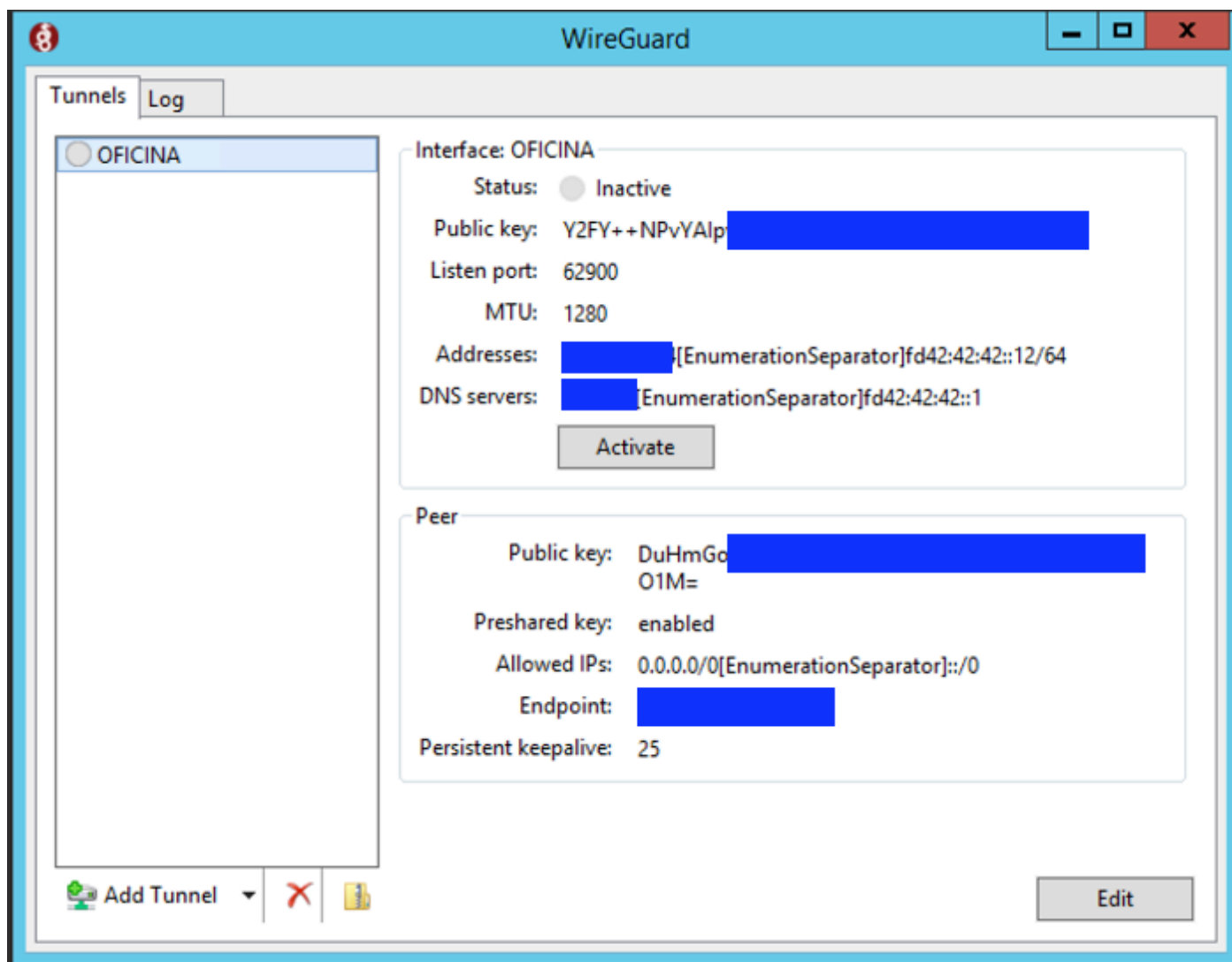


NOTA MUY IMPORTANTE: En la parte inferior hay una casilla de verificación en la que decidimos si todo el tráfico pasa por el túnel (kill-switch). SI la activamos podemos tener el problema de que dejemos de acceder a los equipos de nuestra red local (impresoras y demás) es conveniente no marcarla



Pulsamos en Save para guardar la configuración

La pantalla quedará con la configuración tal y como aparece en la siguiente imagen.

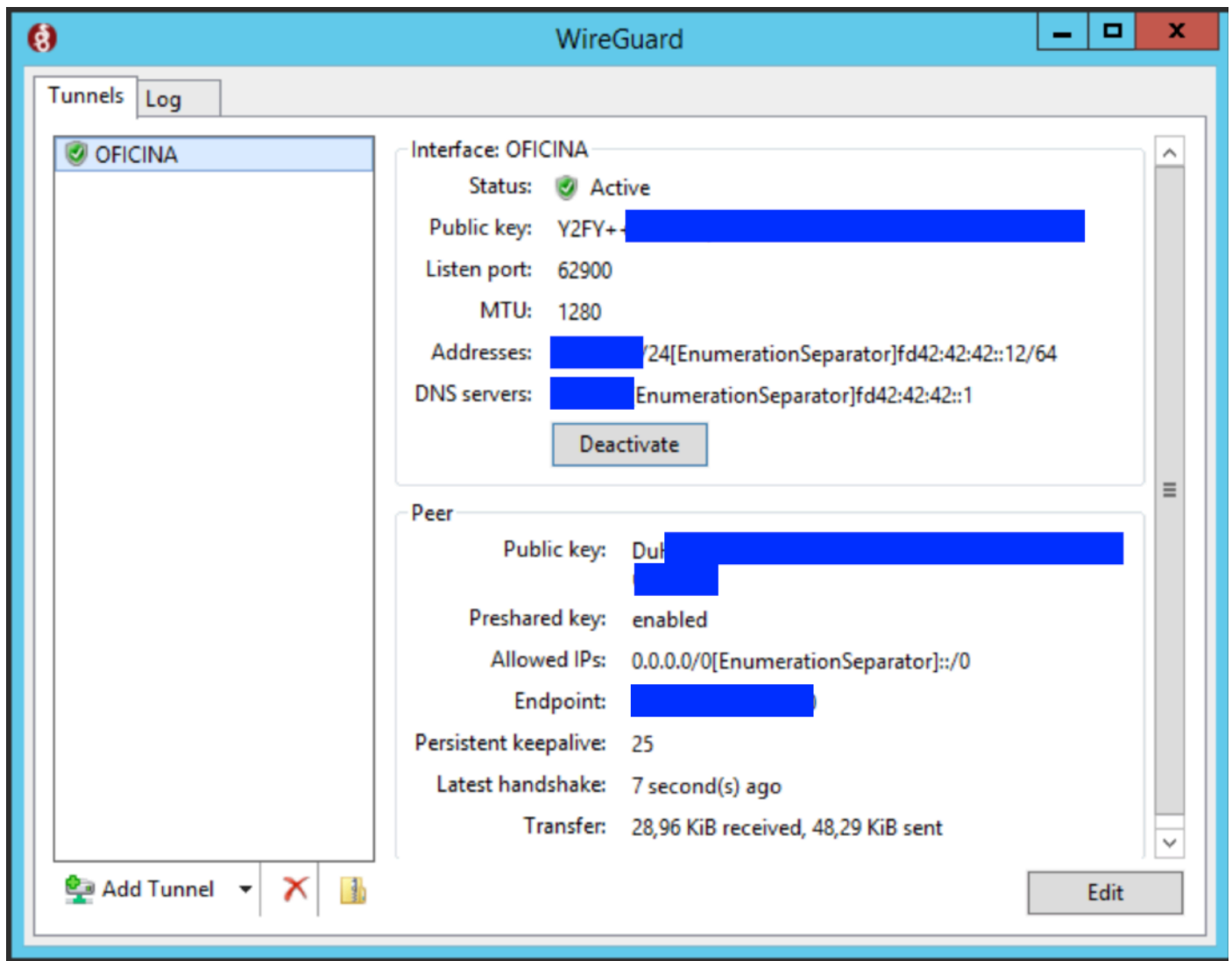


Nota: Si nos da un error al salvar, eso significa que alguno de los datos (Private Key, Preshared Key o Public Key) no está bien.

Activación del túnel VPN

A continuación procederemos a pulsar en Activate, para iniciar la conexión VPN

Aparecerá el status de activating, y una vez conectado aparecerá un escudo en verde como aparece en la imagen



A partir de este momento, nuestra conexión VPN está activa y funcionando.

Toda la información que usemos en nuestras conexiones Internet pasarán a través del túnel, y tendremos acceso a los equipos alojados en nuestra Nube Privada de Tecnocrática de forma segura y confidencial.

Observaciones finales

Como hemos comentado anteriormente, TODO el tráfico de internet que usemos mientras tenemos el túnel activo, pasará por la red de nuestra Nube Privada, con lo que además estará protegida por el firewall gestionado que Tecnocrática instala para proteger los equipos de su empresa.

Dicho firewall, tiene restringidos los accesos, permitiendo por defecto sólo la navegación Internet, el uso de FTP y el correo electrónico.

Además el tráfico se monitoriza, evitando en la medida de lo posible el acceso a webs potencialmente peligrosas

Si precisa por motivos relacionados con la actividad habitual de sue empresa, el acceso a puertos o protocolos no estándar desde la red de sus máquinas, se puede habilitar, pero recuerde:

LA SEGURIDAD ES LO PRIMERO, USE SOLO LA VPN PARA TEMAS LABORALES, PARA EL RESTO DE USO DE INTERNET DESCONECTE LA CONEXION VPN