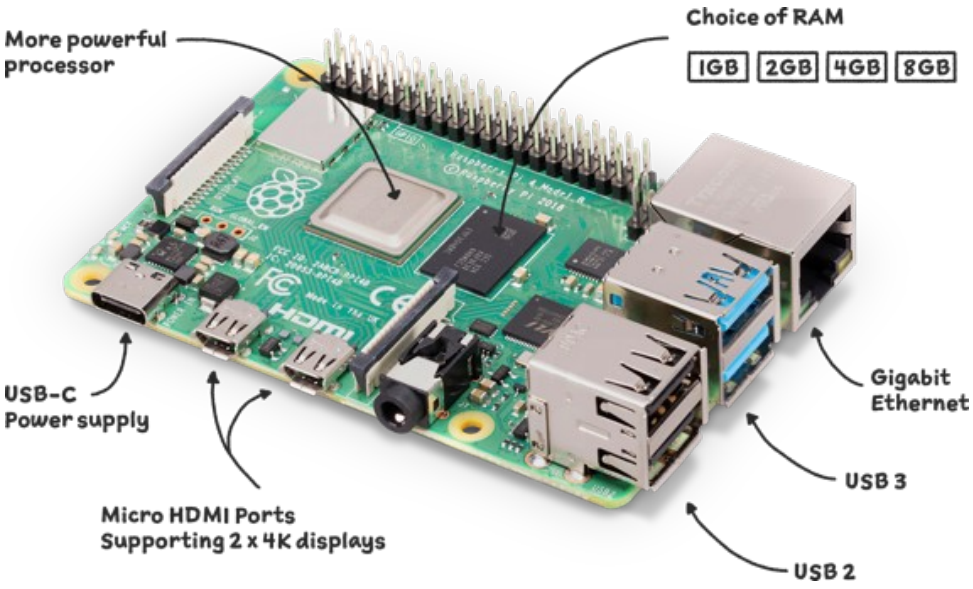
Como instalar una VPN WireGuard en casa

Instalación de una VPN (WireGuard) en tu hogar con una Raspberry Pi 4

Vamos a instalar un servidor de red privada virtual en tu hogar que te permitirá acceder a tu red local desde cualquier sitio como si estuvieras en casa y en un modo seguro. Las ventajas de una vpn son claras: independientemente de a que red estés conectado en cada momento, la red wifi de un hotel, la de un café … todas las comunicaciones van a ir encriptadas y con quien te comuniques le va a parecer que estás conectado desde tu casa. Por ejemplo, si estás en un hotel en Méjico y te conectas a Netflix, te servirá contenidos como si estuvieras en casa. Si te conectas a un banco estarás asegurando la conexión porque toda la comunicación va encriptada hasta tu casa y de ahí le llegará al banco a través se supone de tu router doméstico. Todo son ventajas.

Para poder hacer la instalación de un servidor de VPN en tu casa vas a necesitar, por supuesto, un ordenador en el que instalar el servidor VPN, que en este caso es **WireGuard**, que es un servidor fiable, con las últimas técnicas de encriptación, ligero (no necesita de grandes rescursos) y de muy sencilla administración y de software libre.

Para este tutorial se ha elegido como máquina servidora una Raspberry Pi 4 que es un ordenador basado en procesadores ARM de bajo coste que podemos utilizar para tener servidores en casa, además de VPN, podríamos instalar un servidor web y prescindir de empresas de hosting de páginas, un servidor NAS para tener almacenadas nuestras películas y fotografías, etc. Estamos hablando de un ordenador completo del tamaño de un paquete de cigarrillos con conexiones de red, wifi, usb, hdmi, bluetooh, con hasta 8 Gb de ram por un precio de menos de 100€. Puedes comprarlo en https://www.raspberrypi.com/products/raspberry-pi-4-model-b/.



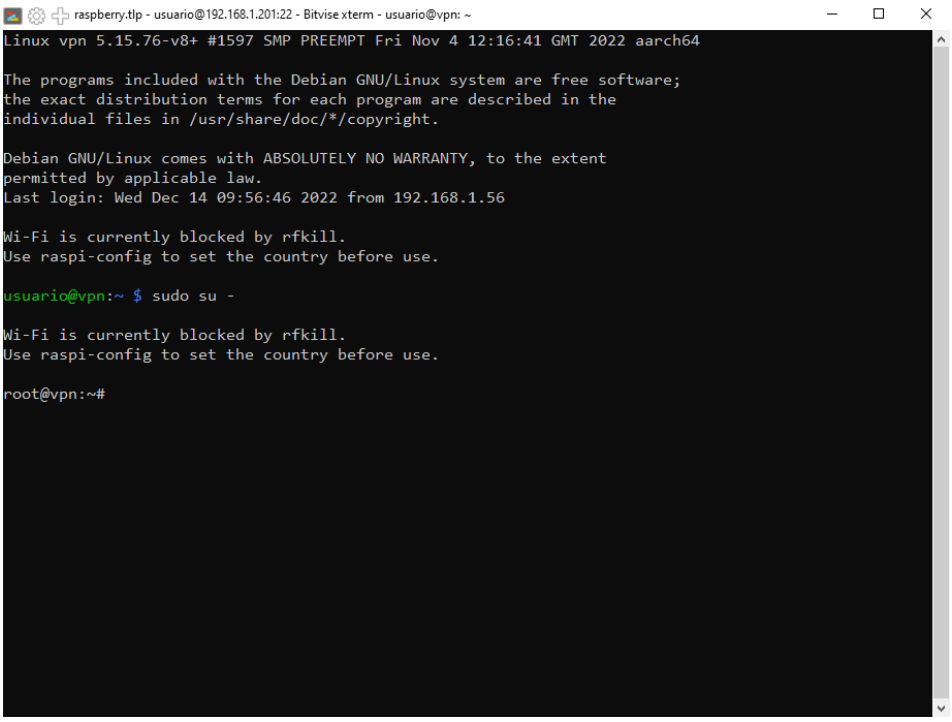
La alimentación se hace a través de un puerto USB-C como se ve en la imagen, es por lo tanto de muy bajo consumo.

No tiene disco duro interno, pero si una ranura que admite tarjetas microSD en la se realizará la instalación del sistema operativo. El almacenamiento externo se realizará a través de los puertos USB o a través de sistemas de archivos distribuidos haciendo uso de su conexión Ethernet o Wifi. Necesitaremos por tanto una tarjeta microSD, que para este uso particular nos vale con 32Gb de tamaño. En ella vamos a instalar el sistema operativo. ¿Que sistema opeartivo? Podemos en principio instalar cualquier sistema operativo que funcione en arquitecturas ARM, la mayoría basados en Linux. Las distribuciones importantes tienen versiones para este tipo de arquitectura. La propia casa Raspberry dispone de una distribución basada en Debian que es la que vamos a utilizar. Le llama Raspberry Pi OS y podemos encontrarlo en https://www.raspberrypi.com/software/operating-systems/. En Raspberry han pensado en facilitar la grabación del sistema operativo en la tarjeta SD poniendo a nuestra disposición un herramienta llamada Raspberry Pi Imager que se encargará de ello. Podemos encontrarla en https://www.raspberrypi.com/software/. Hay versiones para Linux, Windows y MacOS.

En otro artículo de esta web, **Instalación de Raspberry PI OS en Raspebrry PI 4,** se trata la instalación del sistema operativo, el cambio de dirección IP para hacerla fija y la instalación del servidor de SSH que nos permitirá el acceso remoto a la Raspberry PI 4 de forma segura. Se recomienda al lector la lectura previa de dicho artículo.

Instalación del servidor WireGuard

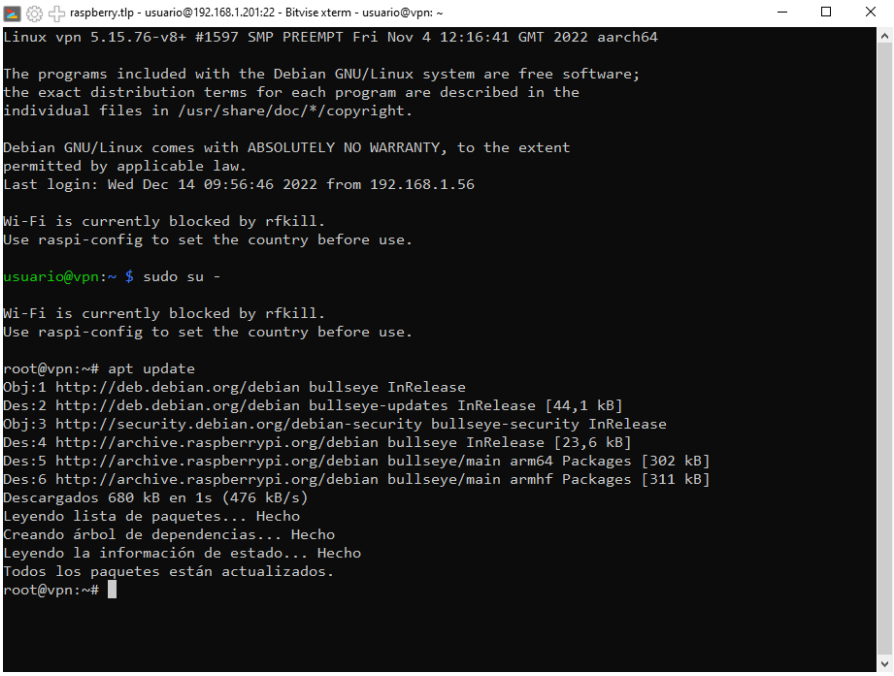
Vamos a instalar el servidor de VPN Wire Guard. Para ello necesitamos ejecutar comandos que precisan que se haga en modo administrador para ello deberemos preceder cada comando del comando **sudo**. Para no tener que escribir cada vez **sudo** lo que vamos a hacer es iniciar una sesión en modo administrador **root** de forma que todos los comandos se ejecutarán en modo administrador, para ello ejecutamos **sudo su -**



Vemos que en el prompt ya aparece **root** como usuario.

Lo primero es actualizar la lista de paquetes de la distribución:

```
apt update
```



En nuestro caso aparecerá que está ya actualizada porque hemos hecho una instalación tomando la imagen del sistema directamente de la web de raspberry y haciendo la instalación acto seguido, pero pudiera ser que no fuera así. Si hubiera algún paquete a actualizar ejecutaríamos:

```
apt dist-upgrade
```

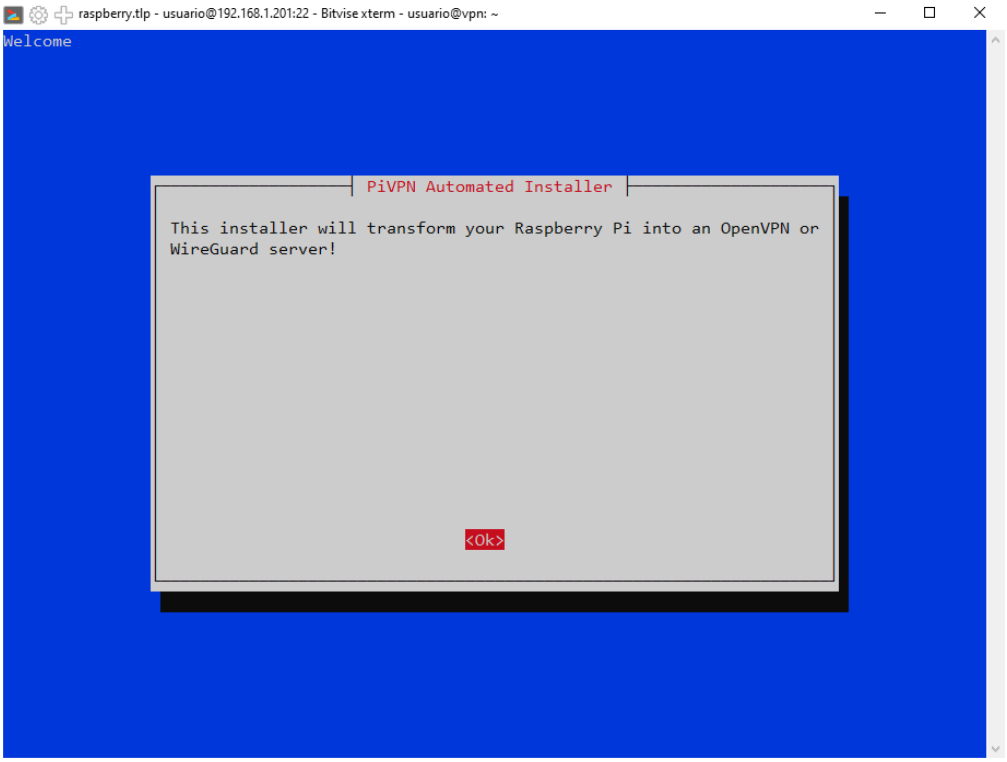
para actualizar el sistema a las últimas versiones.

Para hacer la instalación muy sencilla vamos a descargar un script que realiza la instalación casi de forma automática. Lo podemos encontrar en
https://raw.githubusercontent.com/pivpn/pivpn/master/auto_install/install.sh

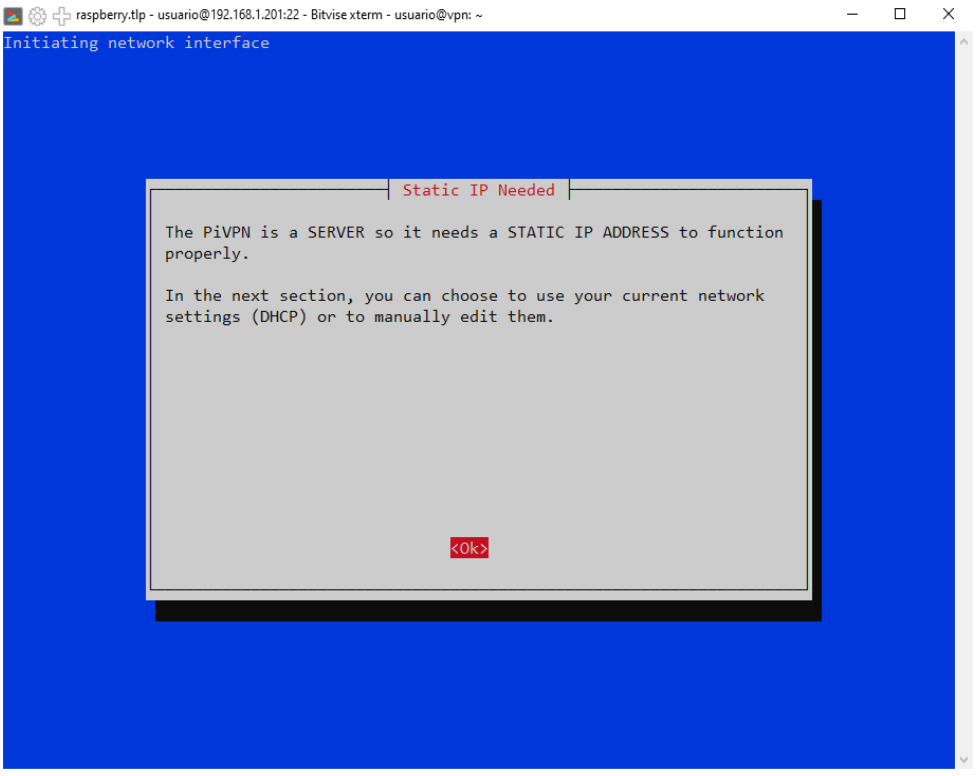
y lo descargaremos y ejecutaremos con el comando:

```
curl -L https://raw.githubusercontent.com/pivpn/pivpn/master/auto_install/install.sh | bash
```

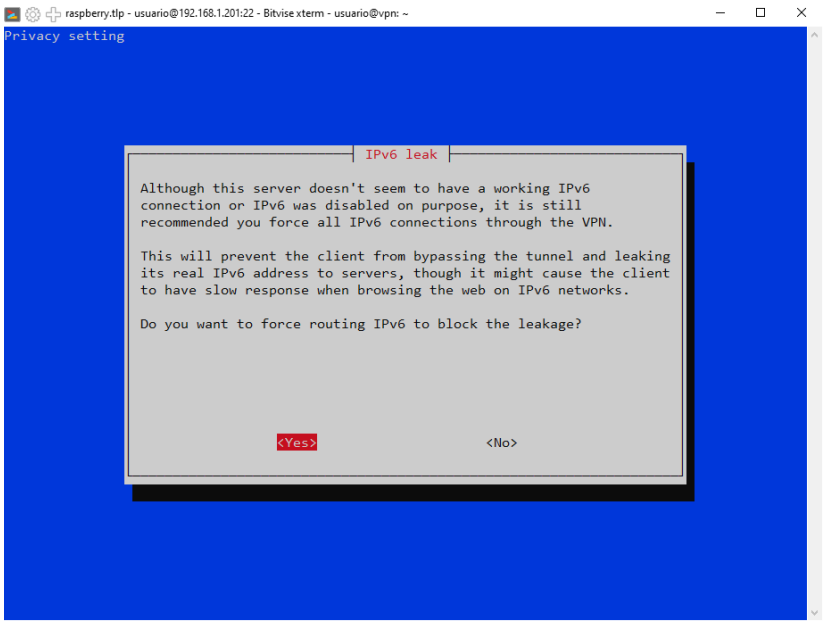
Nos aparecerá:



Tras pulsar <**Ok>**:

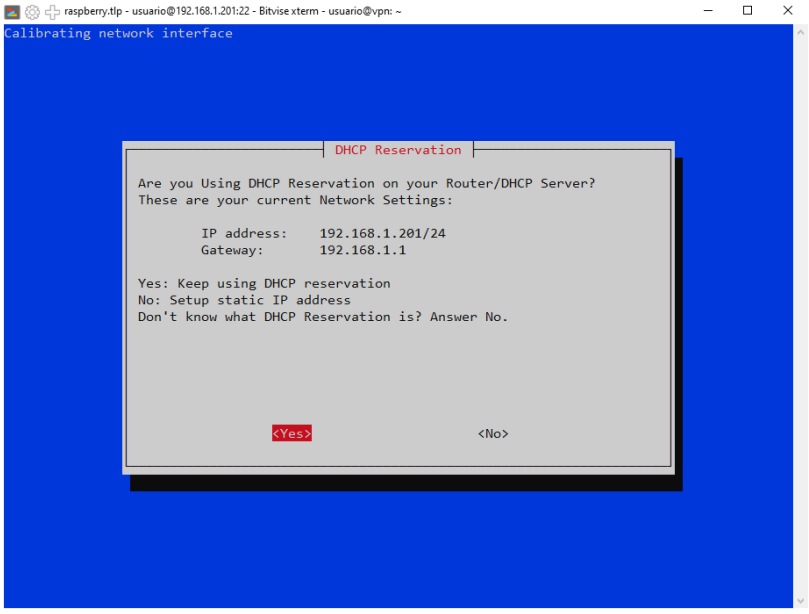


Nos avisa de que necesitamos que nuestro equipo tenga una dirección ip estática fija lo que ya hicimos. Pulsamos **<Ok>**.

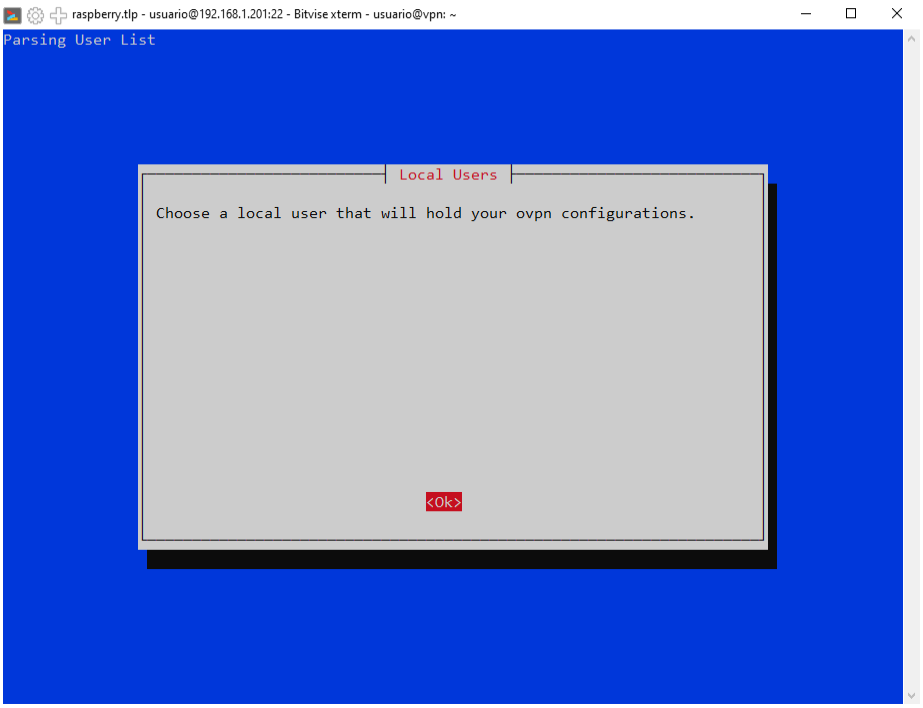


En esta nos habla de IP v6 que no hemos configurado así que dejamos la opción por defecto, pulsamos **<Yes>**

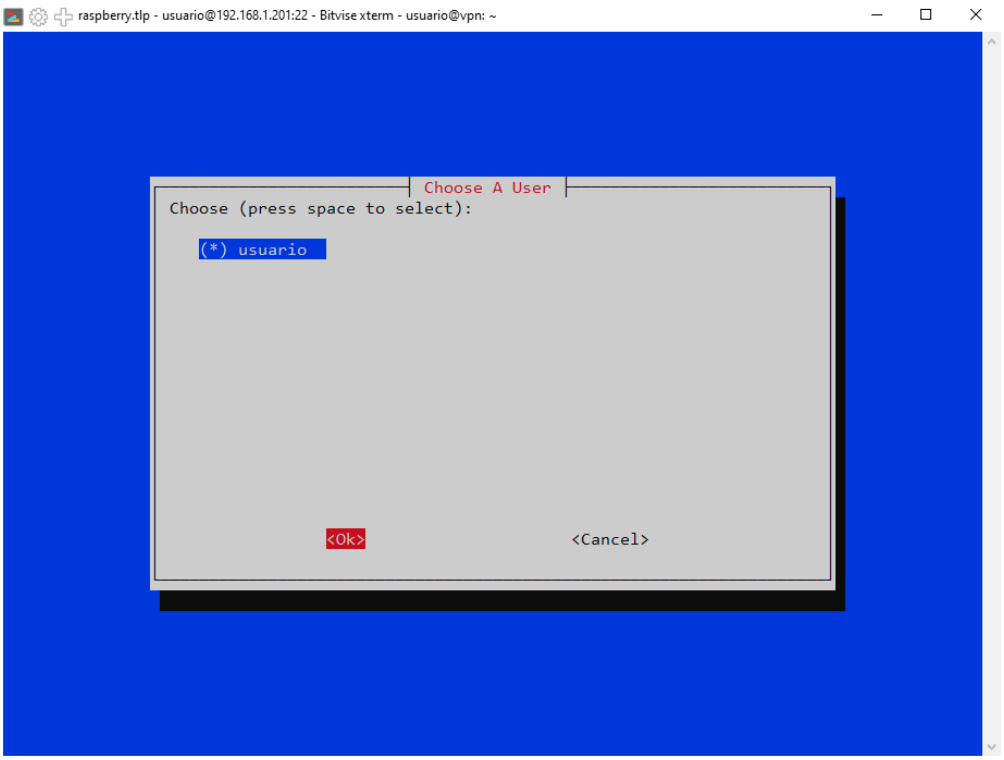
NOTA: Para movernos por las diferentes opciones y ya que no se dispone de ratón, pulsamos tabulador que es la tecla con dos flechas que aparece sobre Bloq Mayús en la parte izquierda del teclado. En las pantallas en las que aparezcan opciones en forma parecida a option button o opciones de radio nos moveremos entre ellas con el tabulador y para seleccionar o deseleccionar pulsaremos el espaciador



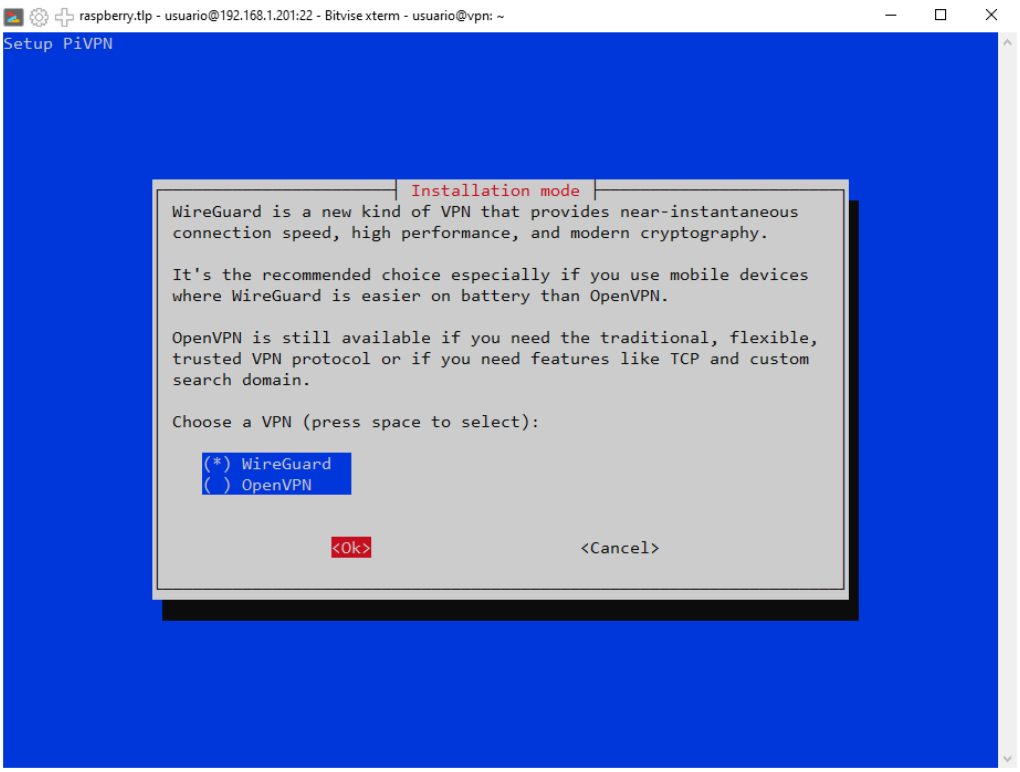
En esta nos da nuestra dirección actual y nos consulta sobre si ya hemos hecho reserva en el servidor DHCP de esta dirección para que no entre en conflicto con otra y que si es fija. En nuestro caso le decimos **<Yes>**. Si no hubiéramos puesto la dirección estática al comienzo aquí tendríamos la oportunidad de configurar a mano el archivo de configuración de red para poner la dirección estática. Tras pulsar **<Yes>**



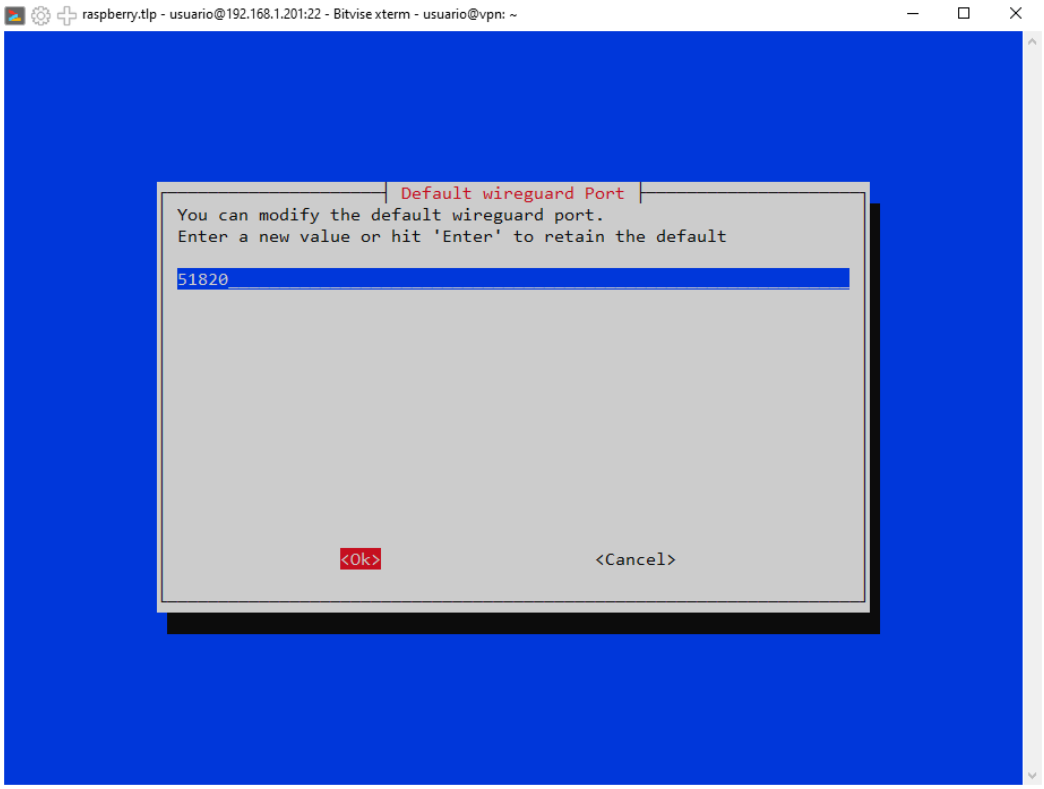
Nos va a solicitar el nombre de un usuario local que va a poder manipular los archivos de configuración de la VPN. En nuestro caso no hay opciones puesto que solo hay un usuario en el sistema, aparte del superusuario **root**. Pulsamos **<Ok>**



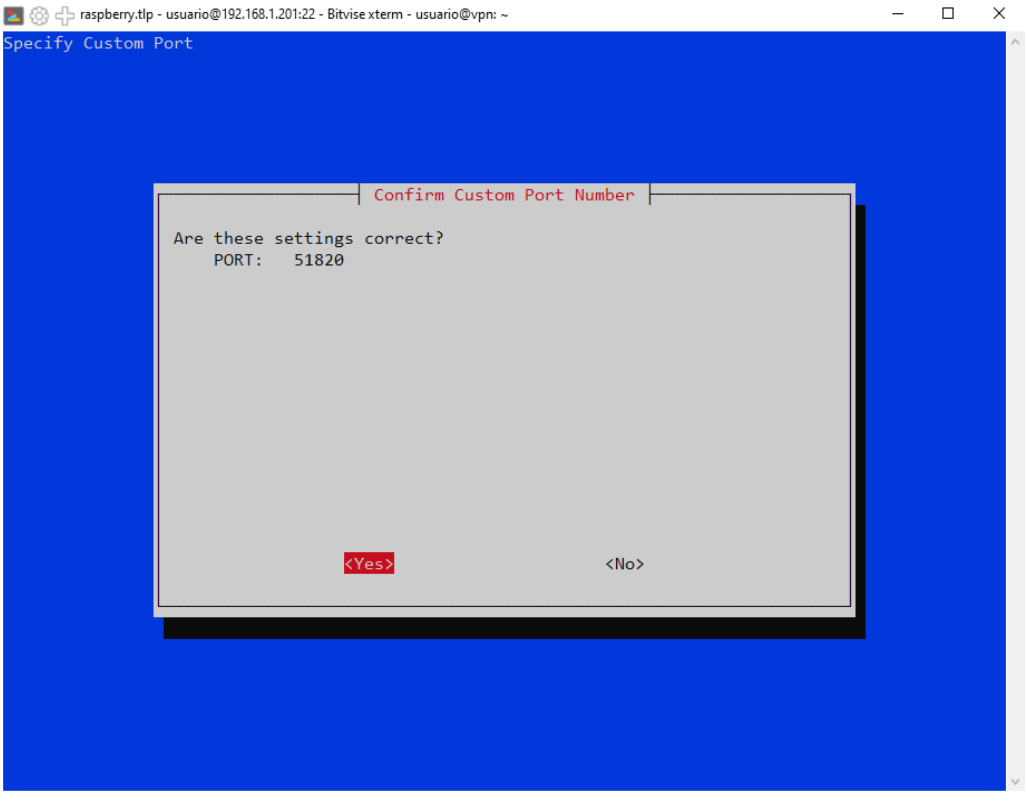
Pulsamos **<Ok>**



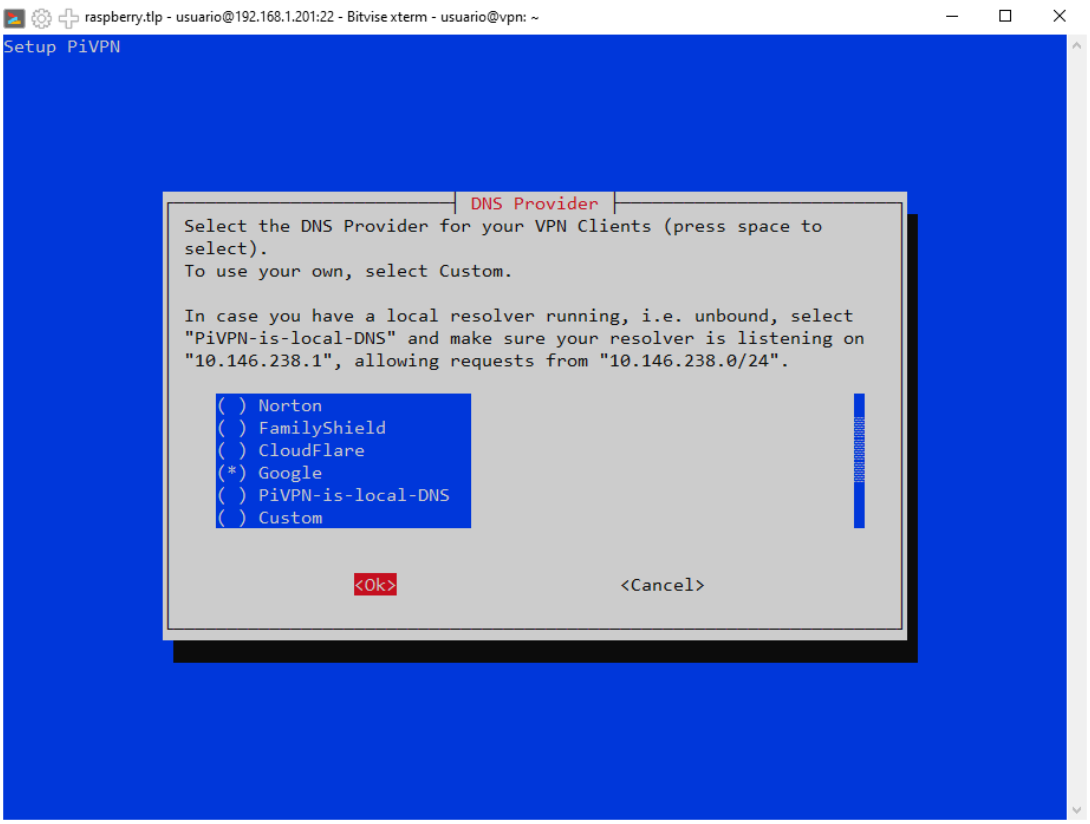
Nos pide elegir entre **WireGuard** y **OpenVPN**. Dejamos la opción por defecto y pulsamos en **<Ok>**



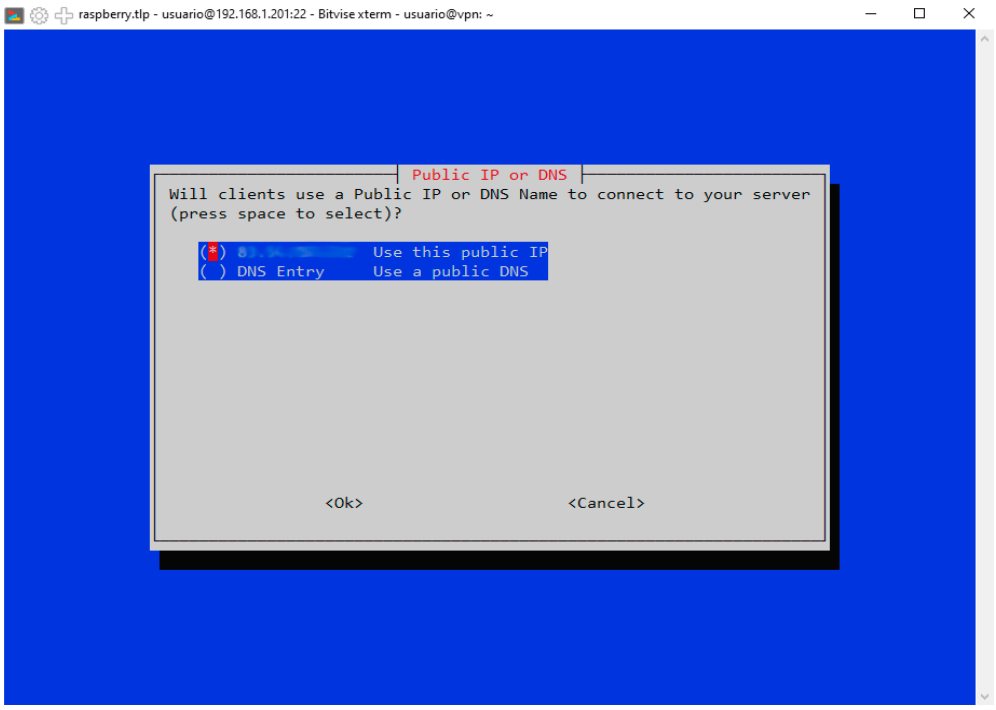
A continuación nos pide indicar cual es el número de puerto a través del cual se va a comunicar nuestro servidor VPN con el exterior. Este número es el número de puerto que luego habrá que abrir en el router para posibilitar la conexión desde el exterior. Es bueno cambiar el número ofrecido para complicar un poco los accesos malintencionados. Se debería elegir un número alto por encima de 1024 hasta 65000 y comprobar que ese puerto no está utilizado por otro servicio. Vamos a dejar el puerto por defecto **51820** y pulsamos **<Ok>**



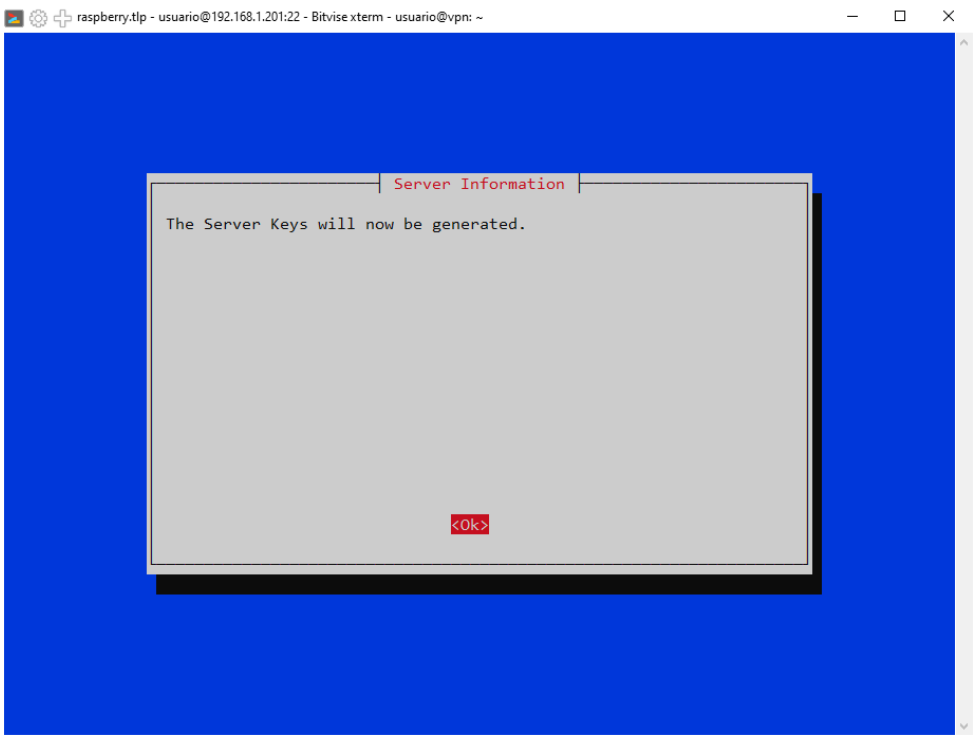
Nos pide confirmación. Pulsamos **<Ok>**.



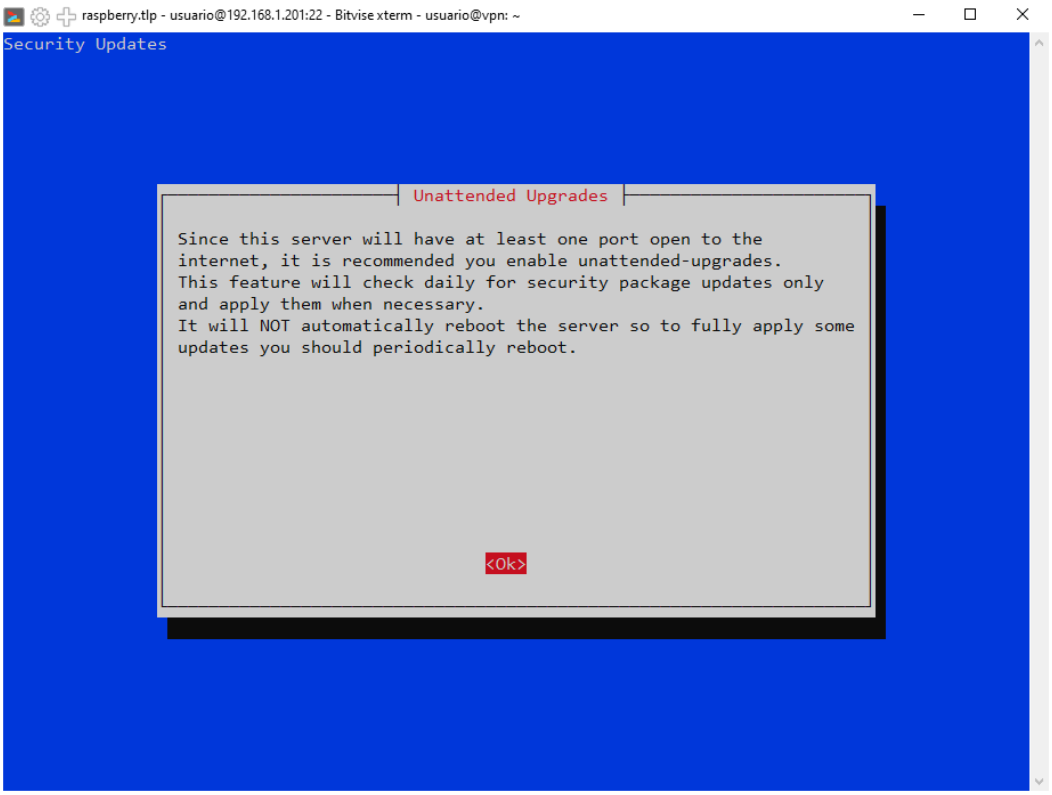
En esta se nos pide que elijamos que servidores DNS le vamos a ofrecer a los clientes que se conecten a la VPN. Podemos elegir cualquiera e incluso si disponemos de uno propio o que no esté en la lista seleccionando **Custom**. Para movernos entre las distintas opciones usaremos una vez que estemos en la lista con Tab, las teclas de flecha arriba y abajo, y para seleccionar pulsamos el espaciador. En ejemplo se ha seleccionado los servidores de Google. Una vez seleccionado pulsamos **<Ok>**.



En esta nos pedirá la forma en que los clientes, desde el exterior, podrán localizar nuestra VPN. Dos opciones la dirección pública de nuestro router que aparecerá de forma automática como primera opción, o una URL registrada que apunte a nuestro host. La primera es la más sencilla, pero tiene un problema que es que nuestro router tiene asignada una dirección pública que es dinámica, es decir, si reiniciamos nuestro router, cosa no digamos que muy habitual pero que si se da, nuestra ip pública cambiará y ya no llegaremos a nuestra VPN con esa dirección. La segunda, un poco más complicada, es tener un nombre de host en un dominio al que tengamos acceso y que siempre apunte a la dirección pública de nuestro router aunque cambie. Hay servicios en internet gratuitos para poder hacer esto, por ejemplo, https://www.duckdns.org/ En un artículo posterior explicaremos como se hace. Por ahora seleccionamos la primera opción y pulsamos **<Ok>**



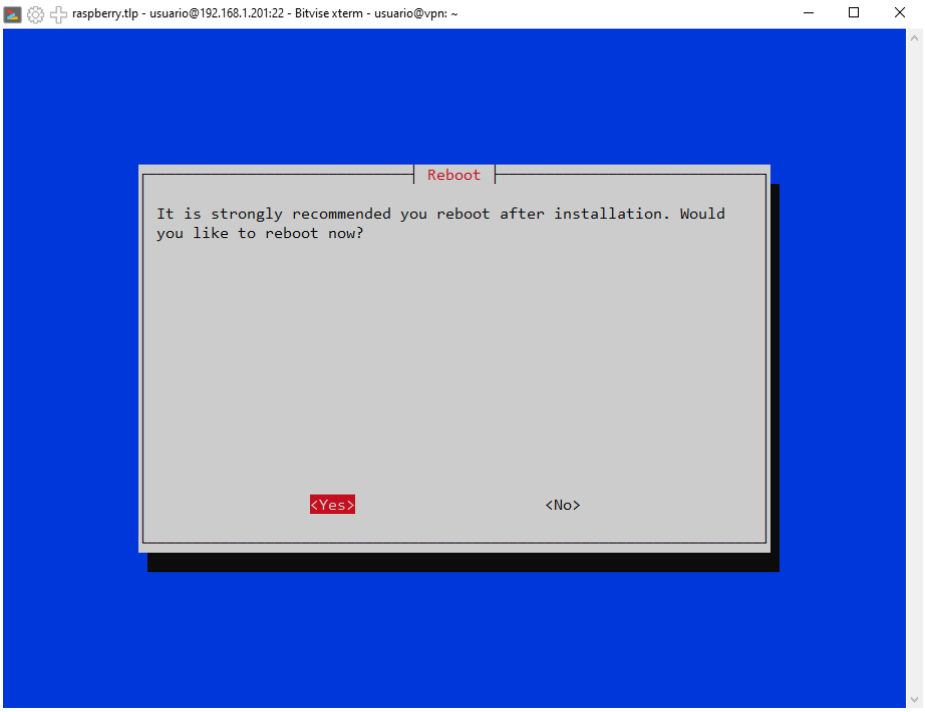
Es el momento de generar las claves de servidor. Pulsamos **<Ok>**.



Nos va a preguntar por si queremos que los paquetes del servidor se actualicen de forma desatendida. Pulsamos **<Ok>**

Es siempre recomendable. Pulsamos **<Yes>**

La instalación habrá terminado, nos recomienda utilizar el comando **pivpn** para hacer la gestión de los clientes y que reiniciemos el equipo:

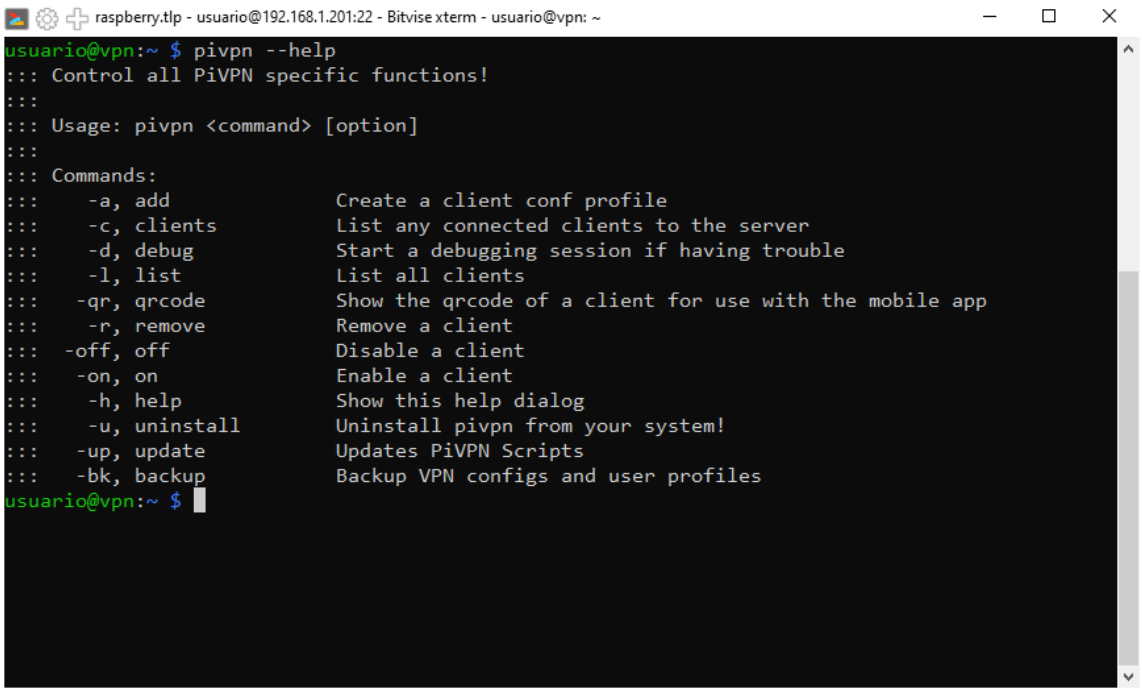


Pulsamos en **<Yes>,** y esperamos a que se reinicie. Volvemos a establecer la conexión y a abrir una nueva consola. Vamos a ver como utilizar el comando **pivpn**.

Si tecleamos:

```
pivpn --help
```

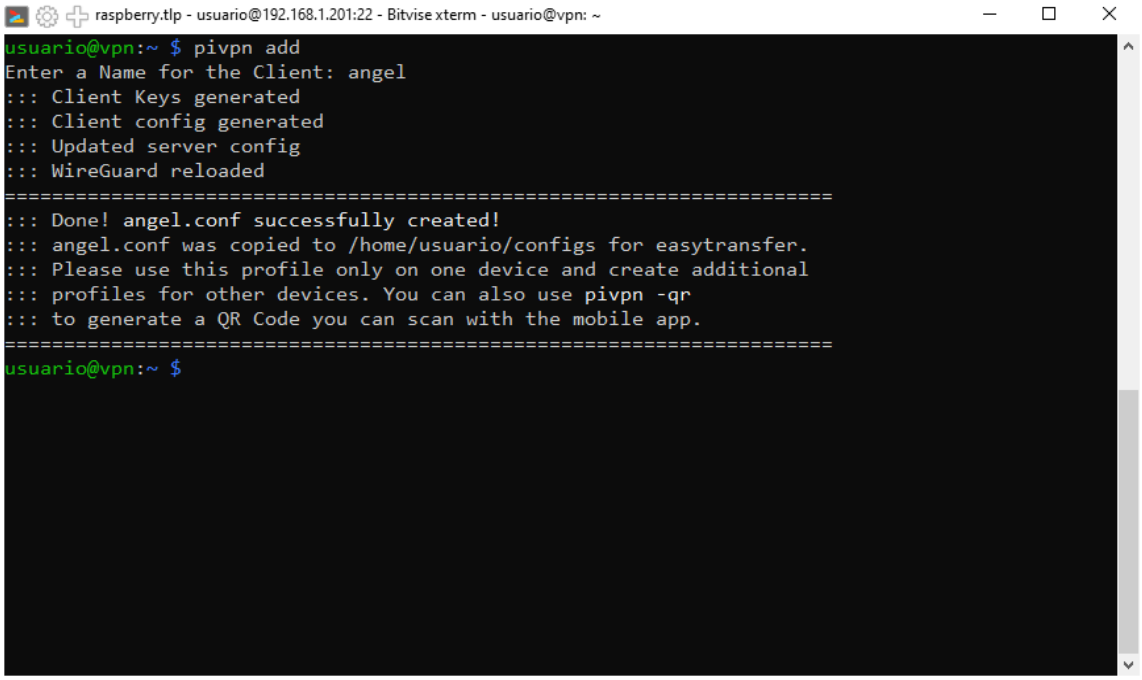
Veremos:



Vamos a crear la configuración para un nuevo cliente:

```
pivpn add
```

Nos preguntará por el nombre del nuevo cliente, en realidad por el nombre del archivo de configuración:



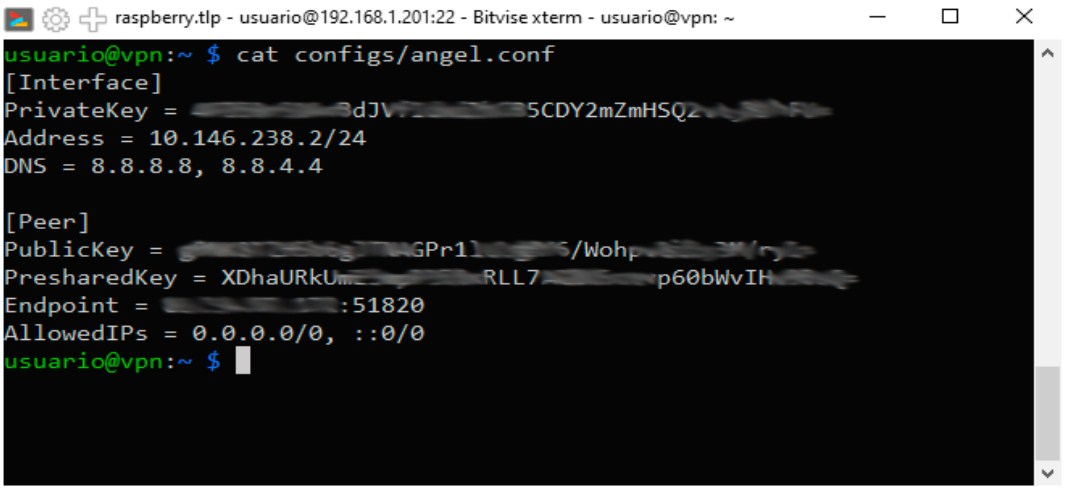
Nos dice que se han creado las key, el archivo de configuración del cliente y que se ha modificado el archivo de configuración del servidor y recargado el servidor para que actualice con los cambios.

También dice que el archivo de configuración del cliente lo podremos encontrar en la carpeta /**home/usuario/configs**.

Nótese que ya **no hemos tenido que cambiar a modo superusuario** con **sudo** puesto que ya habilitamos en la instalación a **usuario** para que pudiese gestionar el servidor de **VPN**.

Para que un cliente se pueda conectar tenemos que hacerle llegar este archivo de configuración creado, uno distinto por cada cliente que se vaya a conectar, o el código QR que generaremos utilizando el comando **pivpn -qr**, como se ve también en el mensaje anterior.

El contenido del archivo de configuración del cliente **angel** del ejemplo es:

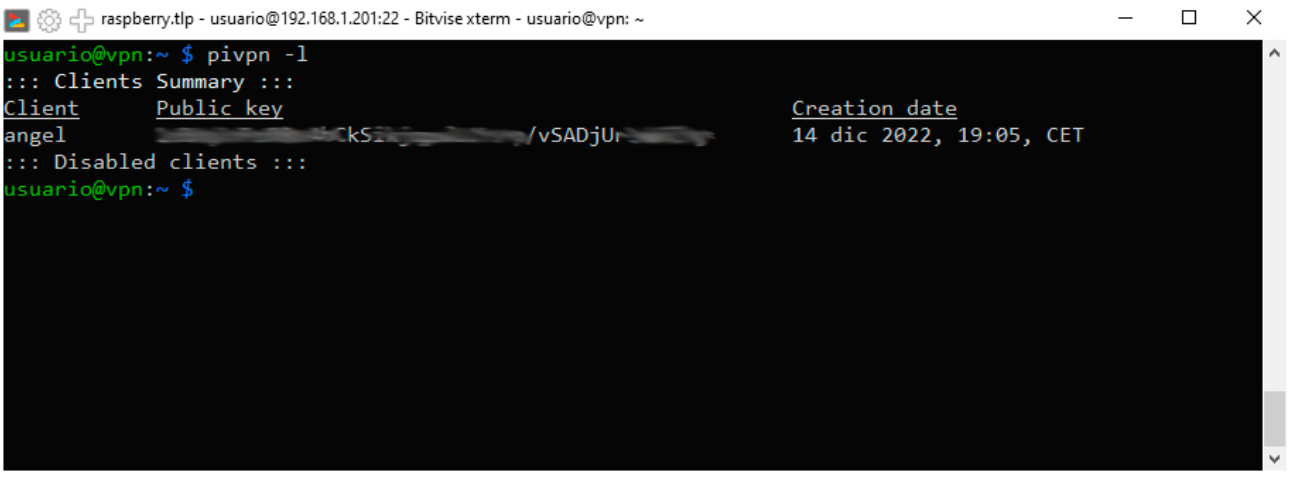


Vemos que aparece la dirección que se le va a asignar al cliente en la red local de la VPN cuando se conecte, por eso debe haber un archivo de configuración distinto por cada cliente que se conecte, así como su clave privada para la comunicación con el servidor. Se puede configurar el archivo de configuración del cliente para que en lugar de asignar un única dirección IP a este se le asigne dentro de un rango de direcciones, permitiendo así el uso de un mismo archivo para varios clientes.

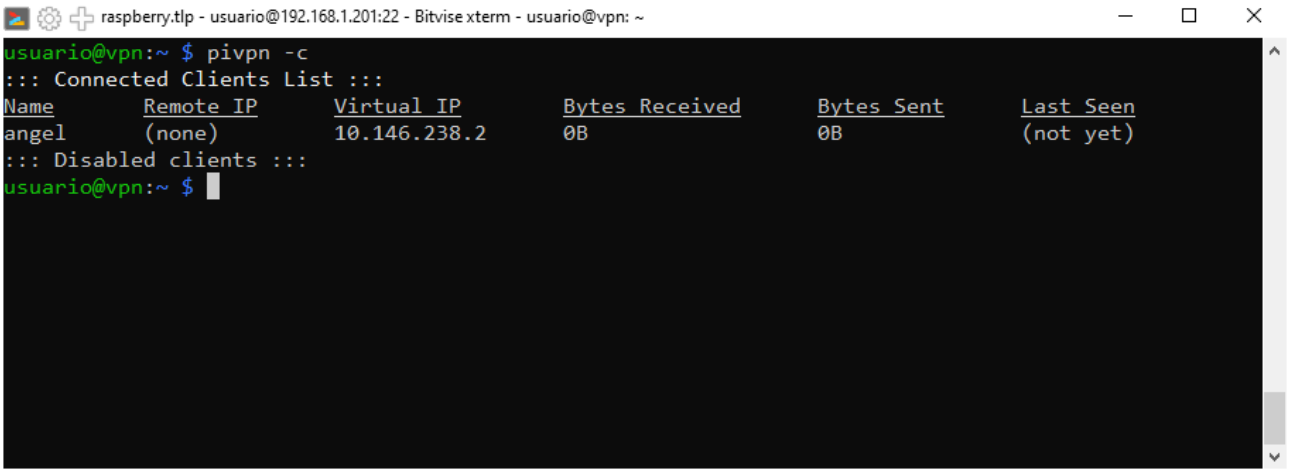
Por otro lado aparece en **EndPoint** la dirección pública del servidor de VPN y el puerto a través del cual se va conectar y la clave pública con la que el servidor encriptará la comunicación con el cliente.

Como gestores del servidor de VPN, con el contenido de estos archivos nunca vamos a hacer nada, simplemente hacérselos llegar a los clientes para que se puedan conectar.

Con **pivpn -l** veremos la lista de clientes que han sido creados y sus claves públicas:



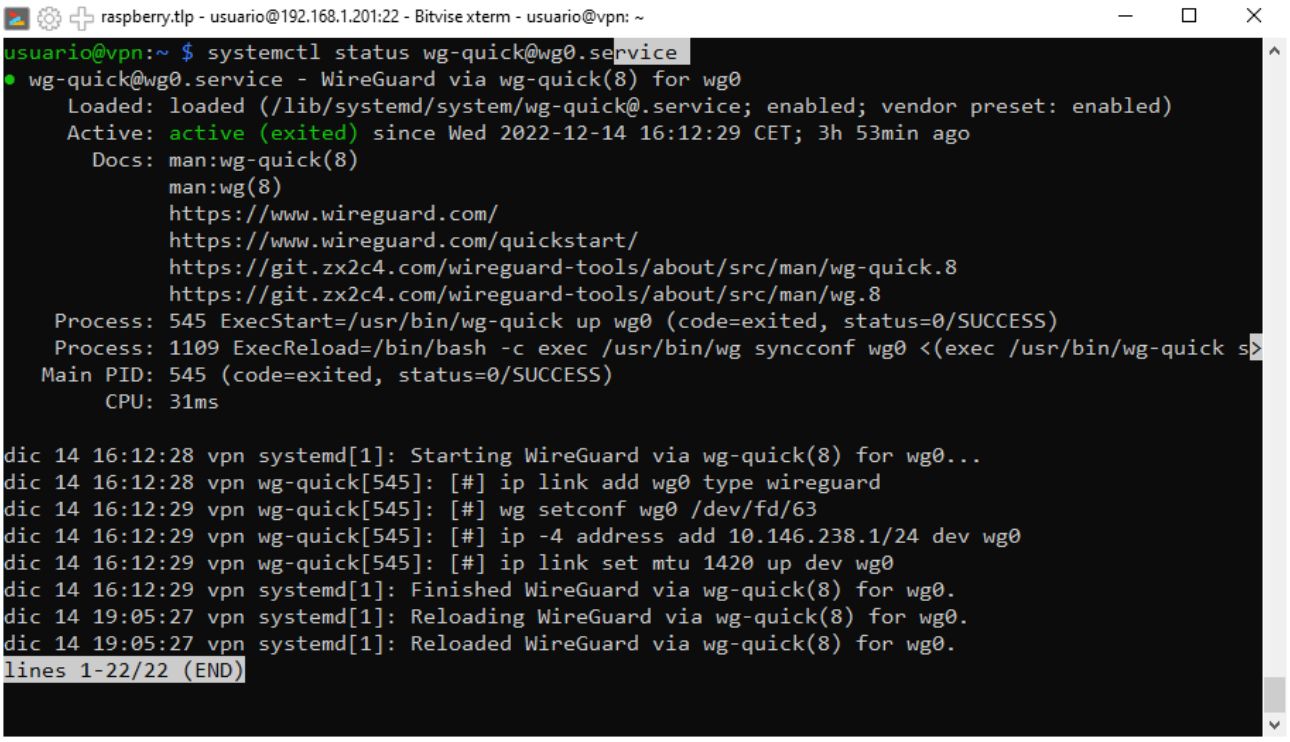
Con **pivpn -c** vemos los estados de conexión de los clientes y sus ip remotas si están conectados:



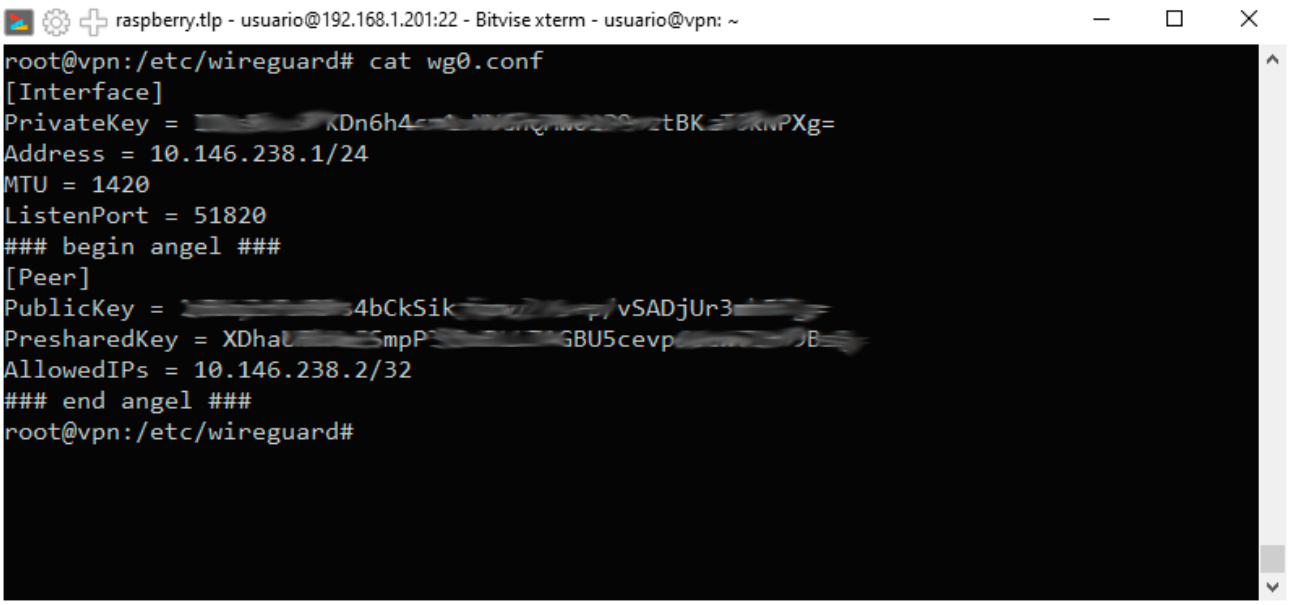
Con **pivpn -on** y con **pivpn -off** podemos habilitar o deshabilitar clientes sin llegar a eliminarlos. Y con **pivpn -r** podemos eliminar clientes.

Para ver el estado del servicio podemos ejecutar:

systemctl status wg-quick@wgo.service



En la carpeta **etc/wireguard** encontramos los archivos de configuración. Para acceder a esta carpeta lo hemos de hacer con privilegios de superadministrador. Encontraremos el archivo **wg0.conf**, con información del propio servidor y de los clientes dados de alta.



En la carpeta **configs** encontraremos copia de los archivos de configuración de los clientes y el archivo **clients.txt** con una lista de todos los clientes dados de alta.

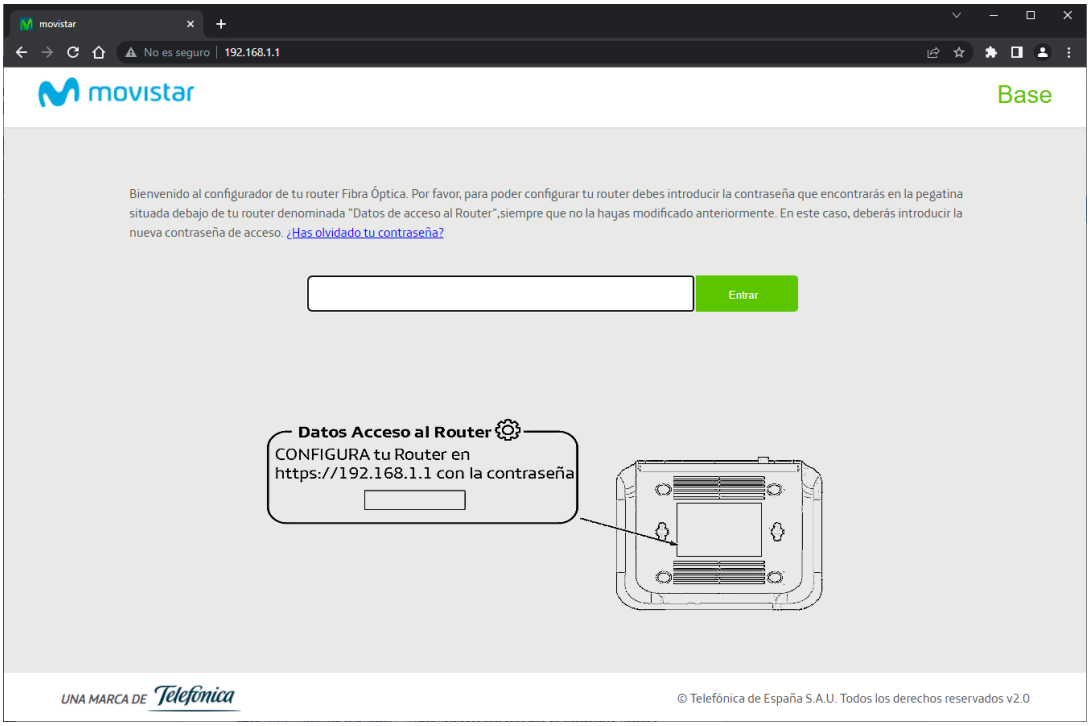
De todos estos archivos solo accederemos al archivo **wg0.conf** para cambiar, por ejemplo, el puerto para la conexión.

Hemos terminado la instalación y configuración del servidor **VPN**. Queda ver como un cliente se conecta y como abrir el puerto correspondiente en nuestro router.

Abrir puerto en router

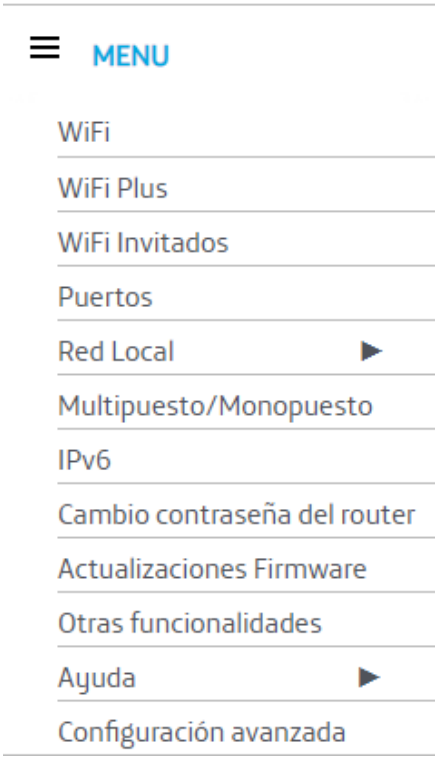
Para que desde el exterior de nuestra casa tengamos acceso al servidor VPN que está en nuestra red interna, debemos abrir el puerto que configuramos, el **51820** en el ejemplo, y redirigir todas las peticiones a través de este puerto a nuestro servidor VPN que teníamos en la dirección **192.168.1.201** en el ejemplo.

Nos conectamos a la administración web de nuestro router, para ello en un navegador accedemos a la dirección del mismo que será también la dirección de nuestra puerta de enlace. En el ejemplo **192.168.1.1 (**para ver la dirección de tu puerta de enlace puedes ejecutar **ipconfig** en una consola de comandos **Menu Inicio → Sistema Windows → Símbolo del Sistema)**

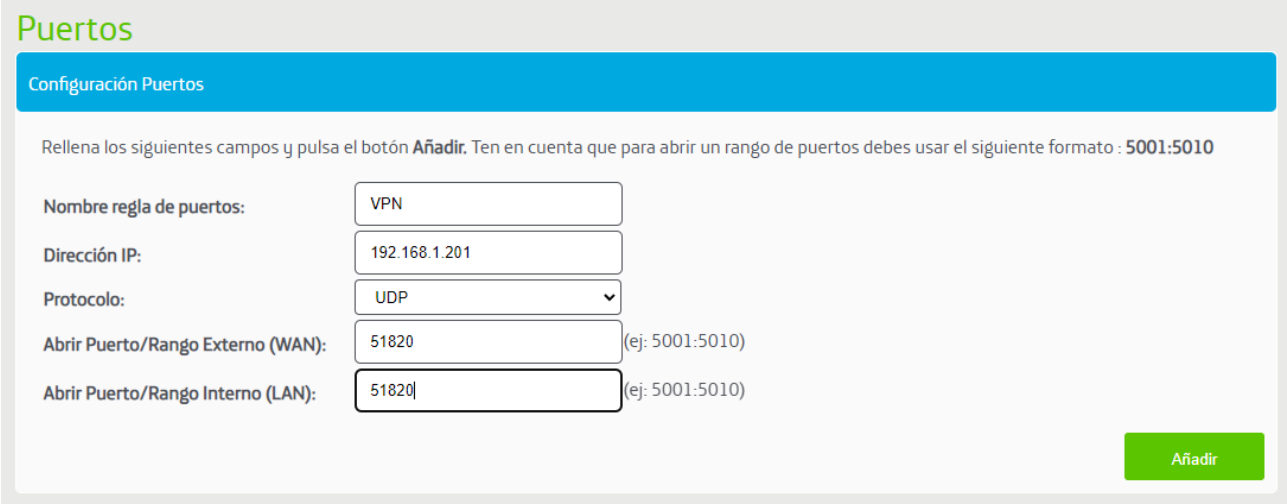


En este caso estamos accediendo a un router de la compañía Movistar. En la parte trasera del router estará la contraseña para acceso o de alguna otra manera debemos conocerla. Una vez introducida la contraseña:

En la opción **Menú → Puertos**



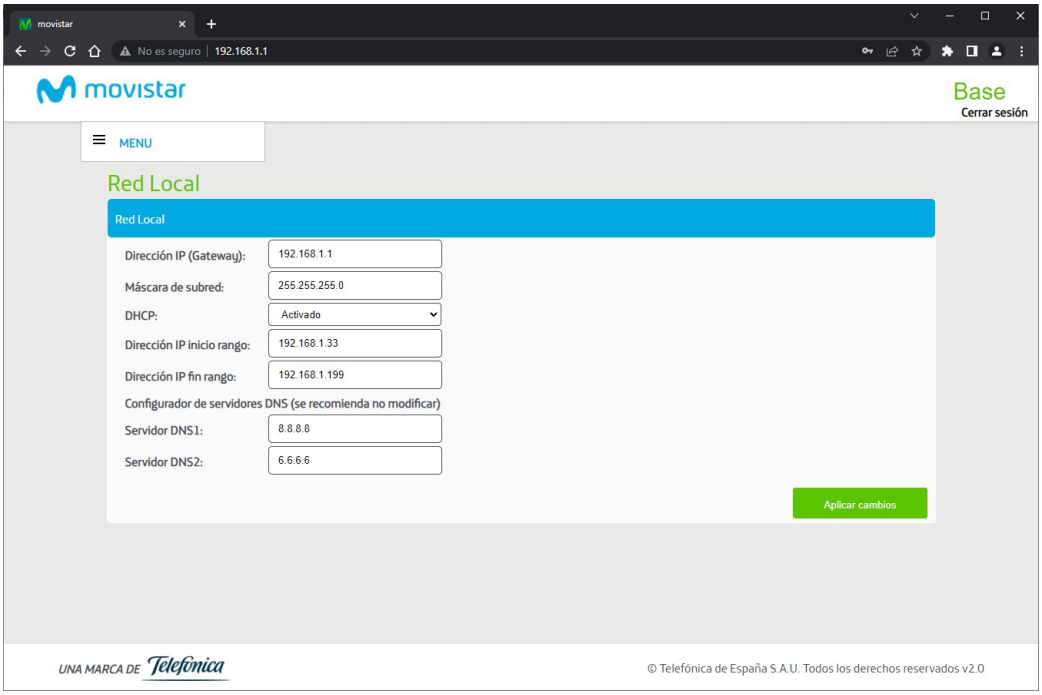
Introducimos los datos y pulsamos **Añadir**



Dirección IP es la dirección de nuestra Raspberry PI en nuestra red de área local, **Protocolo** ha de ser **UDP**, y en las cajas **Abrir Puerto** ponemos en ambas el mismo número que será el puerto en el que configuramos el servidor y los archivos de configuración de los clientes

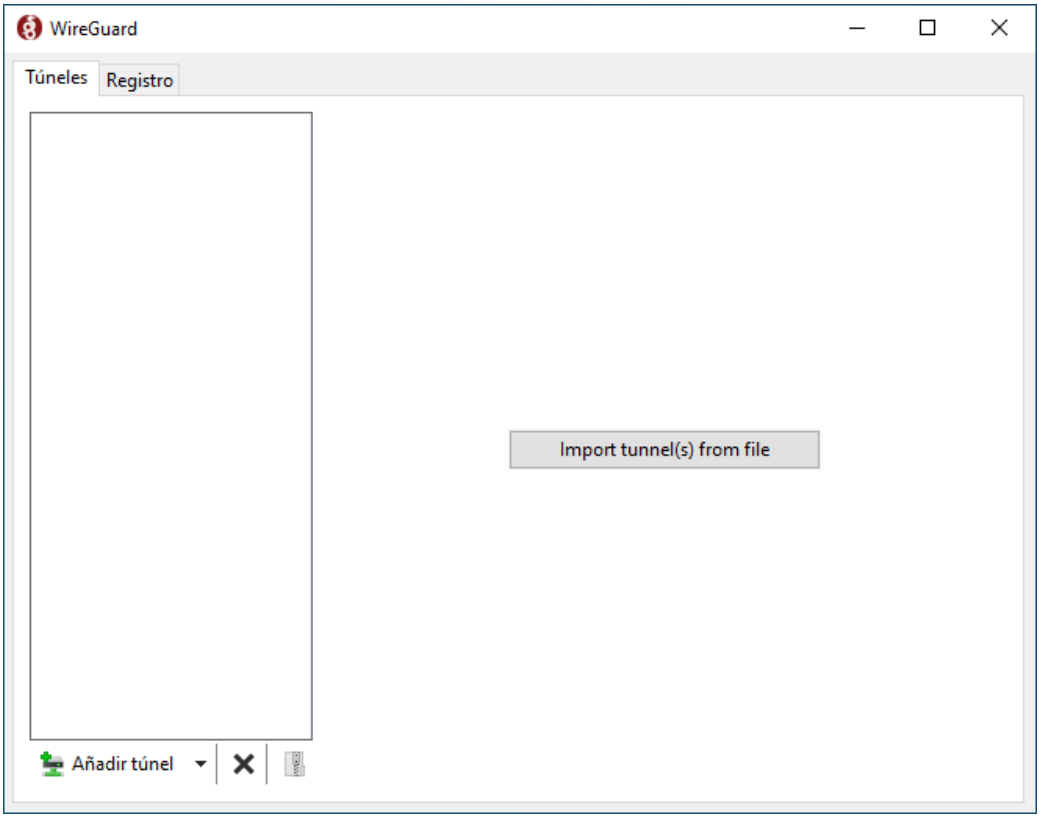
En otros modelos de router el procedimiento será similar o muy parecido.

Si deseamos ver cual es el rango de direcciones que asigna el servidor DHCP del router vamos a **Menú → Red Local → Configuración de red local**

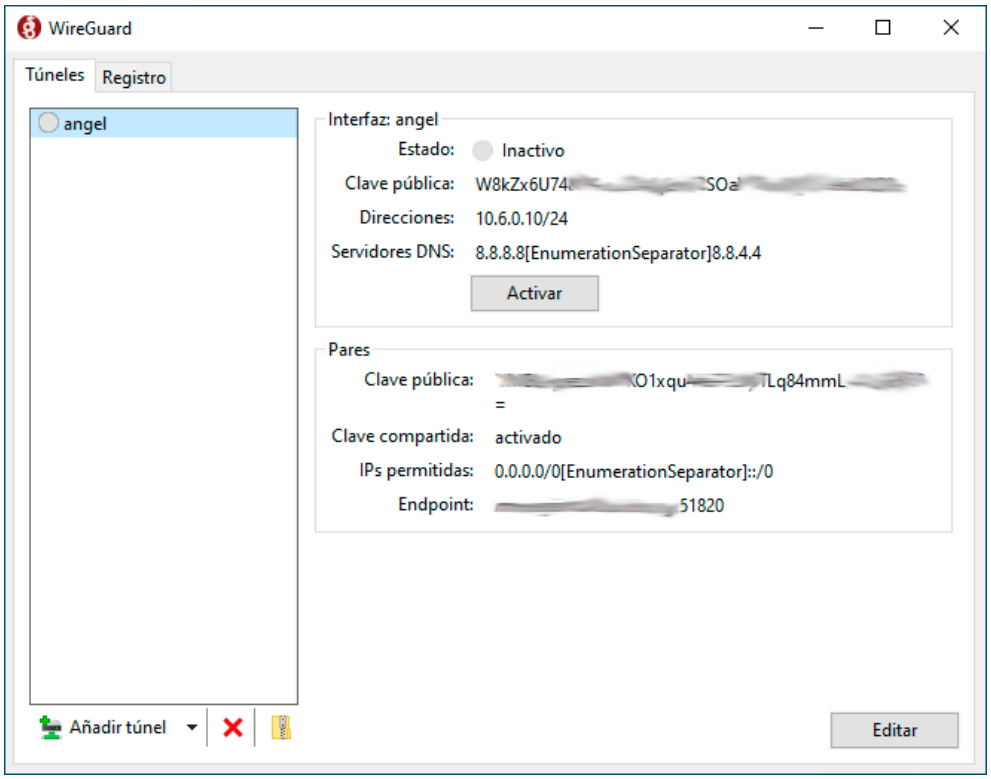


Conexión de un cliente a la VPN

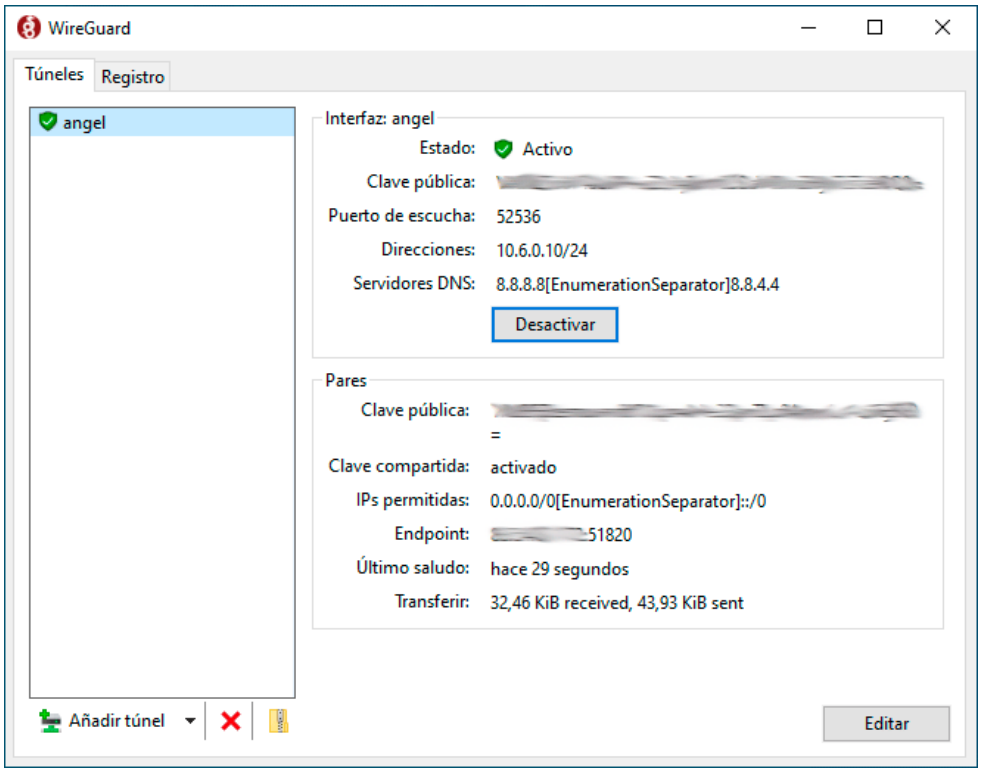
Para conectarnos a nuestra VPN necesitamos de un programa cliente para WireGuard y de un archivo de configuración que nos autentifique frente al servidor. El archivo ya lo hemos generado y hemos de hacerlo disponible para el cliente. El programa cliente lo debemos descargar de https://www.wireguard.com/install/ . Existen versiones para todo tipo de plataformas. Vamos a descargar e instalar el cliente para Windows. Tras lanzar el ejecutable vemos:



Pulsamos en **Import tunnel(s) from file** y cargamos el archivo de configuración de cliente que hemos hecho llegar desde el servidor:



Si pulsamos el botón **Activar** nos conectaremos al servidor VPN:



En el área de notificaciones veremos:

Para terminar la conexión pulsaremos en **Descactivar**.

NOTA: Ver el artículo "Como obtener una URL o dominio propio, gratis con dirección IP Dinámica" en esta misma web