



**INSTITUTO POLITECNICO  
NACIONAL**



**ESCUELA SUPERIOR DE INGENIERIA  
MECANICA Y ELECTRICA**

**INGENIERIA EN COMUNICACIONES Y  
ELECTRONICA**

**ALUMNA:**

HERNANDEZ LABASTIDA DAYSI

**GRUPO:**

5CM7

**MATERIA:**

MICROPROCESADORES

**PROYECTO: CREACIÓN DE UN SERVIDOR VPN**

**TITULAR DE LA ASIGNATURA:**

GALICIA GALICIA ROBERTO

**OBJETIVO:** Ofrecer una conexión remota y segura por WEB desde cualquier proveedor de Internet, con el fin de poder hacer uso de los recursos internos del servicio.

## **MARCO TEORICO**

**VPN:** es una red privada virtual que permite una inclusión segura de la red de área local (LAN) sobre una red pública o no controlada como es Internet. Es un sistema muy eficaz para proteger la comunicación entre dos servidores y evitar que se puedan entrometer en la transferencia de datos entre ambos.

### **Protocolos VPN**

Los protocolos VPN son los **métodos** mediante los cuales se conecta su dispositivo al servidor VPN. Algunos protocolos favorecen la **velocidad**, otros favorecen la **seguridad** y algunos simplemente funcionan mejor en determinadas condiciones de red.

### **Ventajas de una conexión VPN**

¿Cuáles son las principales ventajas de una conexión VPN? Además de que nos permite disfrutar de una conexión a red con todas las características de la red privada a la que queremos acceder podemos destacar:

1. Confidencialidad de los datos: la información únicamente podrá ser decodificada por los miembros de esta conexión VPN.
2. Integridad de los datos: el contenido está encriptado y además de no ser interpretados, no podrán ser alterados ni modificados durante la transmisión.
3. Autenticación y autorización: imposibilita que acceda un equipo externo a los miembros autorizados.
4. Velocidad y coste: La conexión VPN funciona más veloz en la transferencia de información y ahorra dinero en los equipos y servicios que se estén ofreciendo dentro de la red local.

**DDNS:** Es un complemento del sistema DNS. Se crea un nombre de Dominio, el cual pasa a representar la dirección IP del usuario, incluso si la dirección IP cambia el DDNS seguirá siendo el mismo.

Esto se debe a que siempre que se modifique la dirección IP del router, este comunica la dirección IP actual al servicio DDNS, que actualiza la petición en el mismo dominio y responde a la dirección IP

**DIRECCIÓN IP:** (IP es un acrónimo para Internet Protocol) son un número único e irrepetible con el cual se identifica una computadora conectada a una red que corre el protocolo IP.

## **INTRODUCCIÓN**

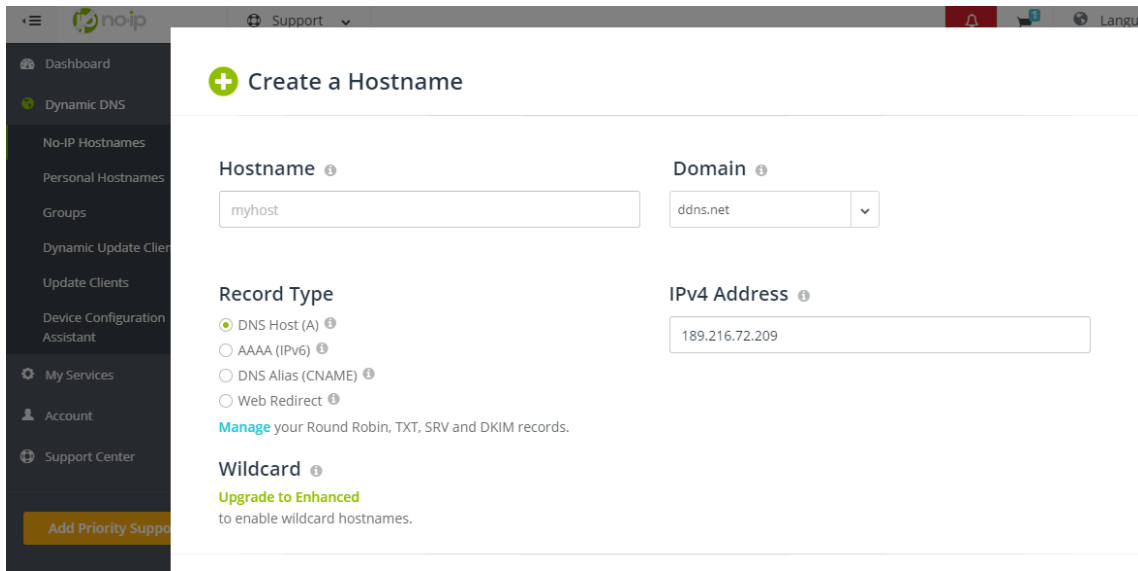
La presente información se dedica a analizar de forma general a las VPN, sus características y funcionamiento, así como las tecnologías que utiliza para enviar los datos de forma segura a través de una red pública. Las VPN están cobrando cada vez mayor popularidad debido a las grandes ventajas que ofrece.

Debido a que no existe un estándar en la industria de las telecomunicaciones respecto a las VPN, el término se ha prestado ha diferentes interpretaciones, y en ocasiones genera confusión, puesto que cada fabricante de dispositivos VPN o cada proveedor de servicios VPN ofrece soluciones que muchas veces difieren de sus competidores y en ocasiones hasta resultan contradictorias.

La seguridad es el aspecto más importante en una VPN. Debido a que se trata de información privada de las corporaciones circulando a través de una red pública, es necesario el uso de fuertes métodos de encriptación y autenticación de los datos con el fin de lograr el envío seguro de la información.

## DESARROLLO

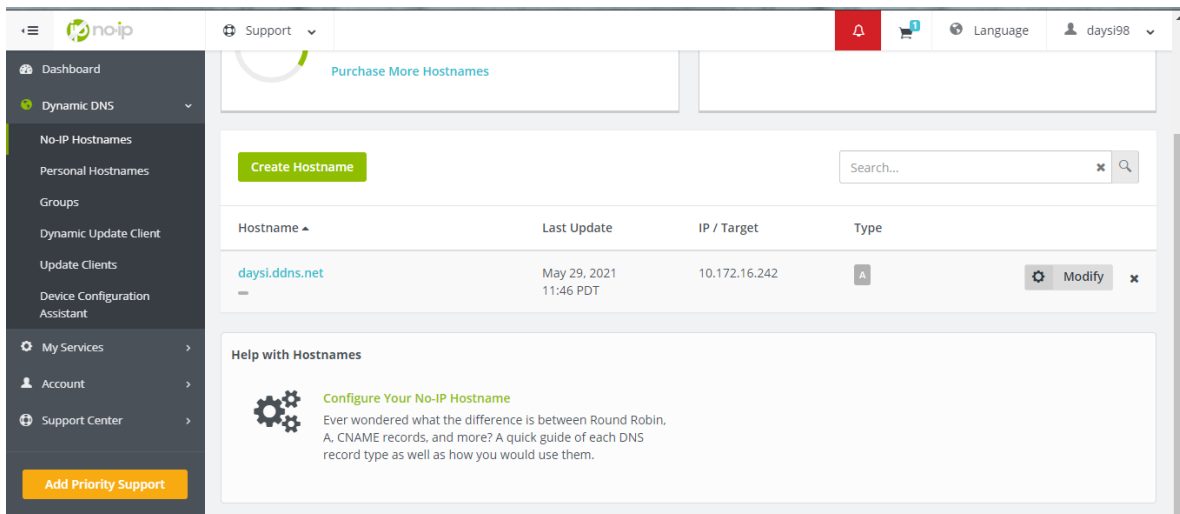
Primero creamos nuestro hostname, ingresamos a la pagina:  
<https://www.noip.com/>



The screenshot shows the 'Create a Hostname' page on the No-IP website. The left sidebar contains navigation links: Dashboard, Dynamic DNS, No-IP Hostnames, Personal Hostnames, Groups, Dynamic Update Client, Update Clients, Device Configuration Assistant, My Services, Account, and Support Center. The main content area has the following fields:

- Hostname:** A text input field containing 'myhost'.
- Domain:** A dropdown menu showing 'ddns.net'.
- Record Type:** Radio buttons for 'DNS Host (A)' (selected), 'AAAA (IPv6)', 'DNS Alias (CNAME)', and 'Web Redirect'. Below these is a link: 'Manage your Round Robin, TXT, SRV and DKIM records.'
- IPv4 Address:** A text input field containing '189.216.72.209'.
- Wildcard:** A section with the text 'Upgrade to Enhanced to enable wildcard hostnames.'

Creamos nuestra cuenta y procedemos a agregar nuestro nombre de dominio



The screenshot shows the No-IP dashboard after account creation. The top navigation bar includes 'Support', a bell icon, a shopping cart icon, 'Language', and a user profile 'daysi98'. The left sidebar is the same as in the previous screenshot. The main content area features a 'Purchase More Hostnames' button and a 'Create Hostname' button. Below these is a table with the following data:

Hostname	Last Update	IP / Target	Type
daysi.ddns.net	May 29, 2021 11:46 PDT	10.172.16.242	A

Below the table is a 'Help with Hostnames' section with a gear icon and the text: 'Configure Your No-IP Hostname. Ever wondered what the difference is between Round Robin, A, CNAME records, and more? A quick guide of each DNS record type as well as how you would use them.'

Procedemos a buscar nuestra dirección ip.

En nuestro cmd colocamos los comandos de ipconfig

```
C:\ Símbolo del sistema
Microsoft Windows [Versión 10.0.19042.928]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\drago>ipconfig

Configuración IP de Windows

Adaptador desconocido Conexión de área local:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet Ethernet:

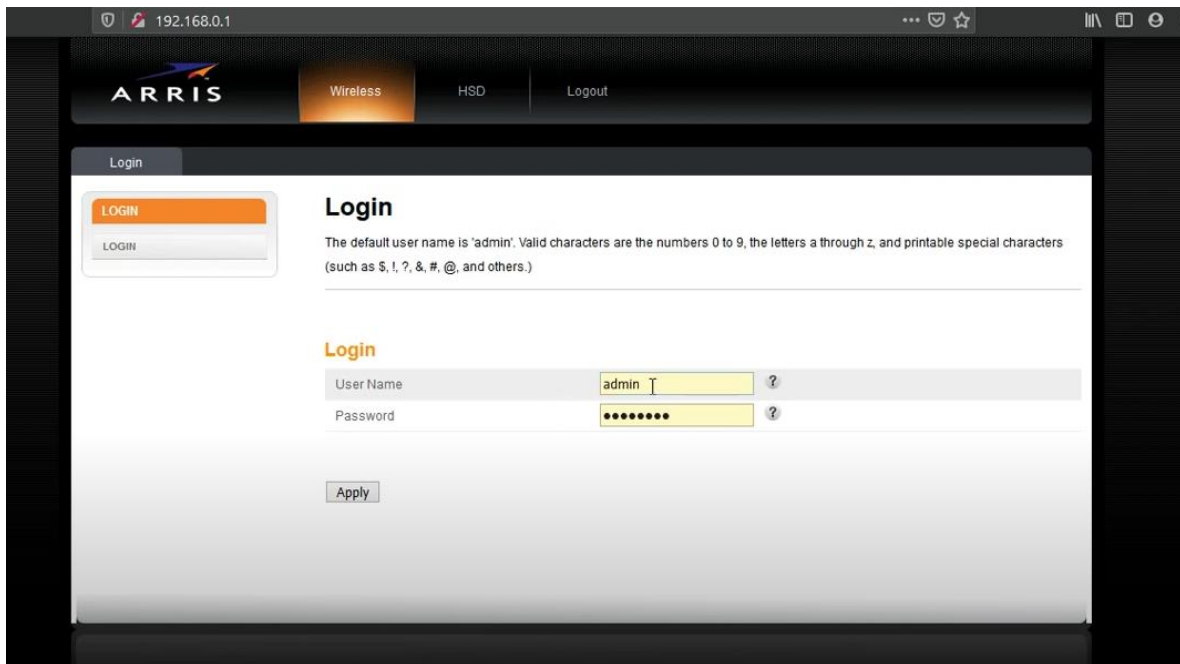
    Sufijo DNS específico para la conexión. . :
    Vínculo: dirección IPv6 local. . . : fe80::f40d:902a:3aa8:dde1%10
    Dirección IPv4. . . . . : 192.168.0.10
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.0.1

C:\Users\drago>
```

Ahora vamos a configurar nuestro router, copiamos nuestra dirección ip y la colocamos en el buscador de nuestro navegador

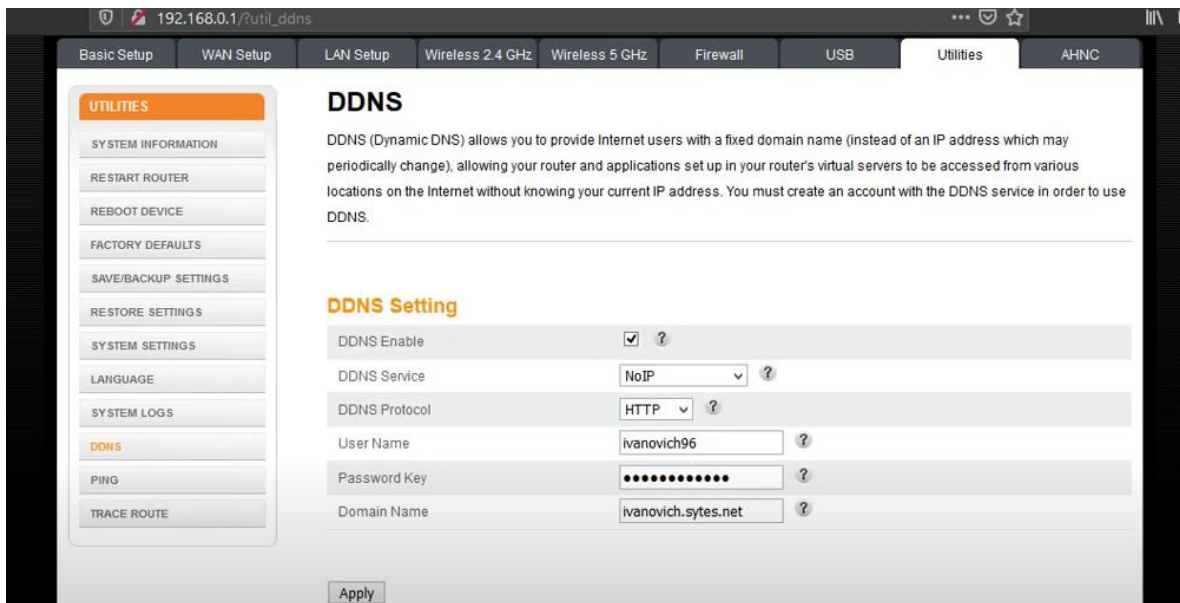


Al dar enter después de haber copiado nuestra dirección ip , nos aparecerá la ventana siguiente , donde nos pide el usuario y contraseña éste viene en el router.

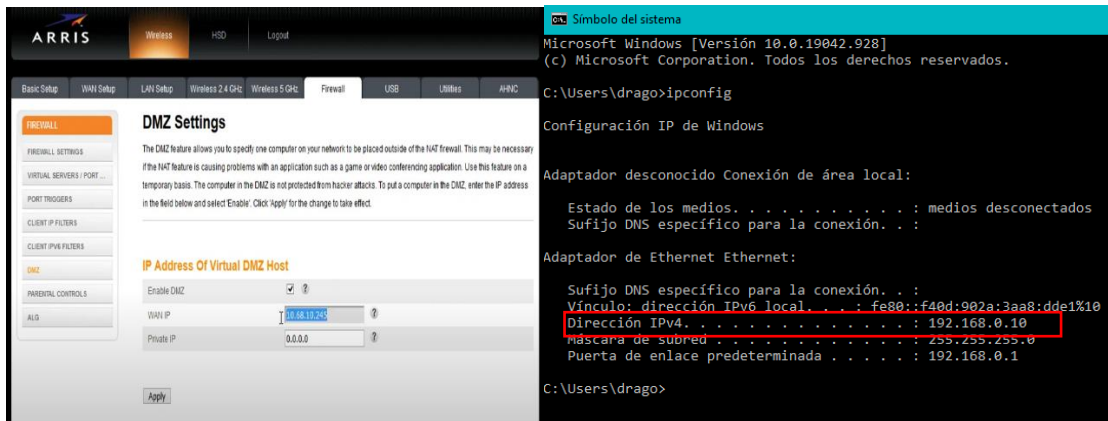


Una vez que se pudo iniciar sesión nos vamos a la sección de DDNS

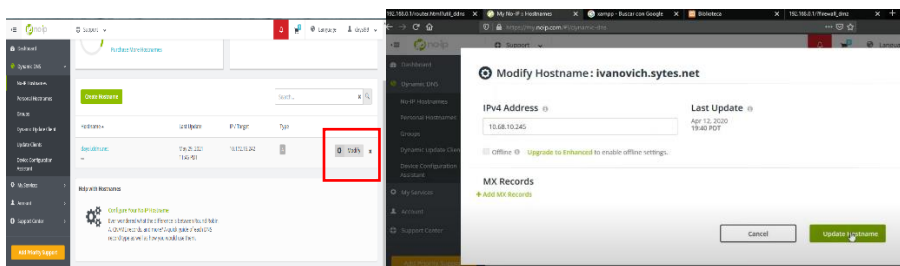
Rellenamos cada uno de los campos , en el usuario y contraseña ponemos el mismo que utilizamos al darnos de alta en No-IP y de igual forma ponemos el nombre de dominio que creamos



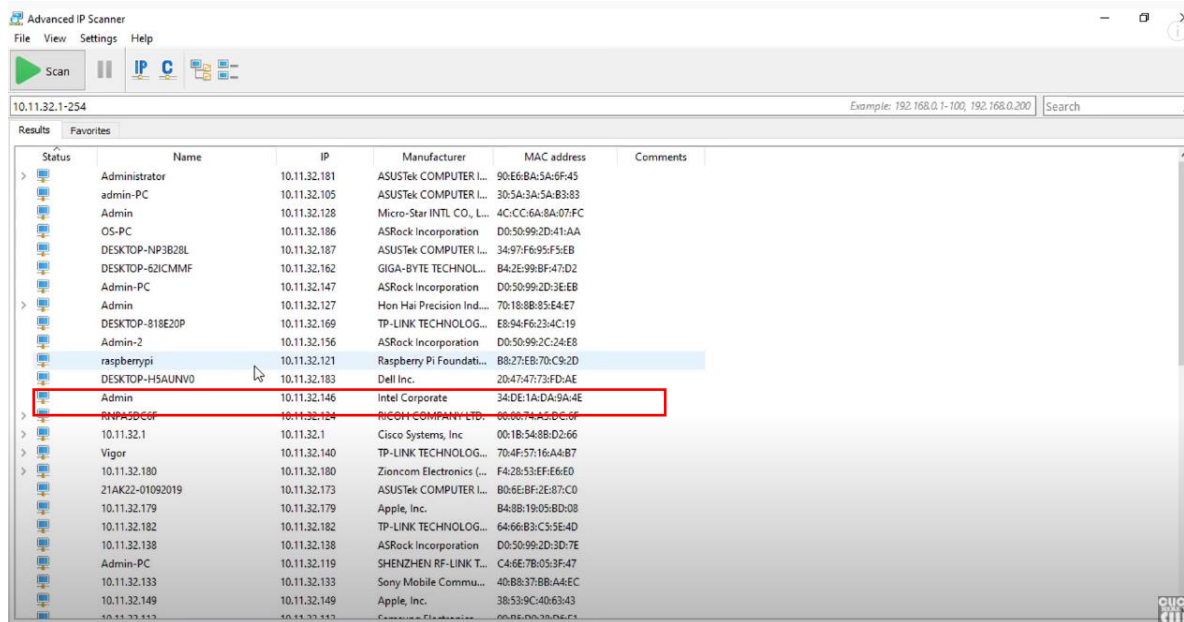
Nos vamos a la sección DMZ y agregamos la dirección ip



En la imagen anterior copiamos WAN IP y lo colocamos en IPv4 adress



Instalaremos el programa de advanced IP scanner y buscamos la dirección IP de nuestra Raspberry



Nos dirigimos a nuestra Raspberry , abrimos la terminal y colocamos el comando de **ssh pi@(dirección IP de raspberry)**, en la contraseña ponemos raspberry

```
C:\Users\NETVN>ssh pi@10.11.32.121
The authenticity of host '10.11.32.121 (10.11.32.121)' can't be established.
ECDSA key fingerprint is SHA256:cSgjk75dClyB/wh2Iay4rky2MEvkD75LbFAH06JSIhk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.11.32.121' (ECDSA) to the list of known hosts.
pi@10.11.32.121's password: raspberry
```

Escribimos el comando **sudo passwd** y agregamos la contraseña que nosotros querramos , esto es para crear super usuarios

```
pi@raspberrypi:~ $ sudo passwd
sudo: passwd: command not found
pi@raspberrypi:~ $ sudo passwd
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
```

Una vez echo el paso anterior escribimos **su** y colocamos la contraseña que habíamos dado anteriormente

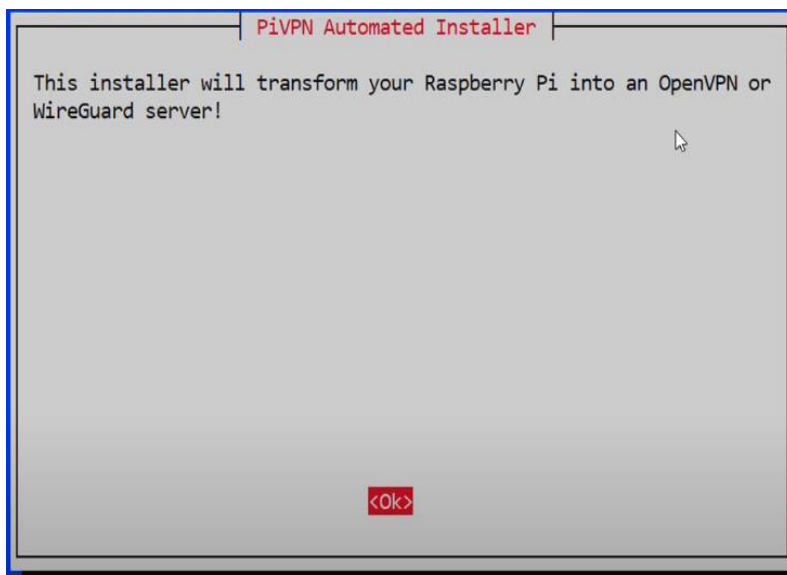
```
pi@raspberrypi:~ $ su
Password:
```

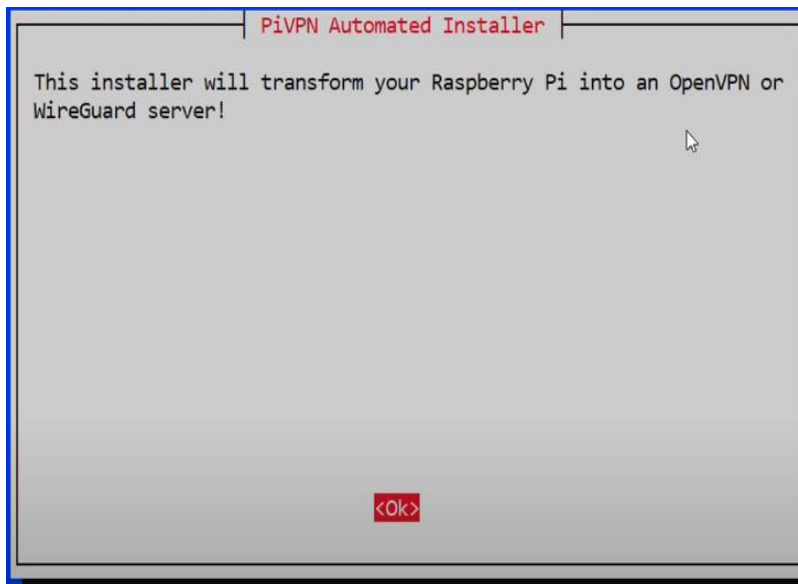


Ahora procedemos a instalar el pivpn con el comando: **curl -L https://install.pivpn.io | bash**

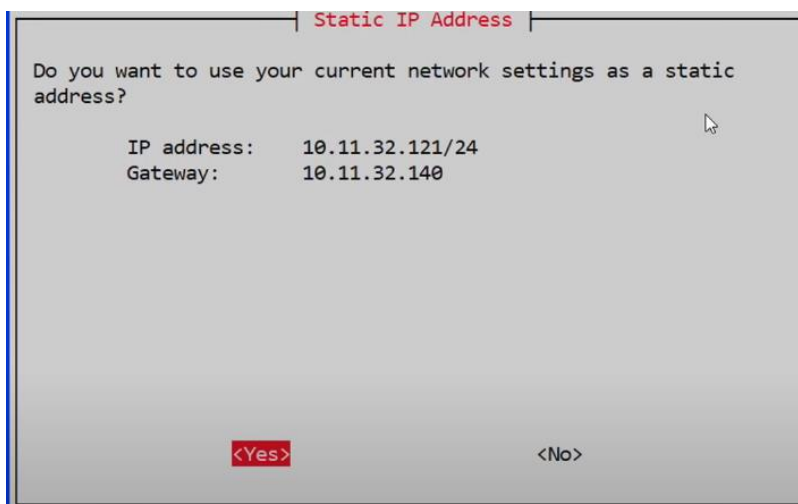
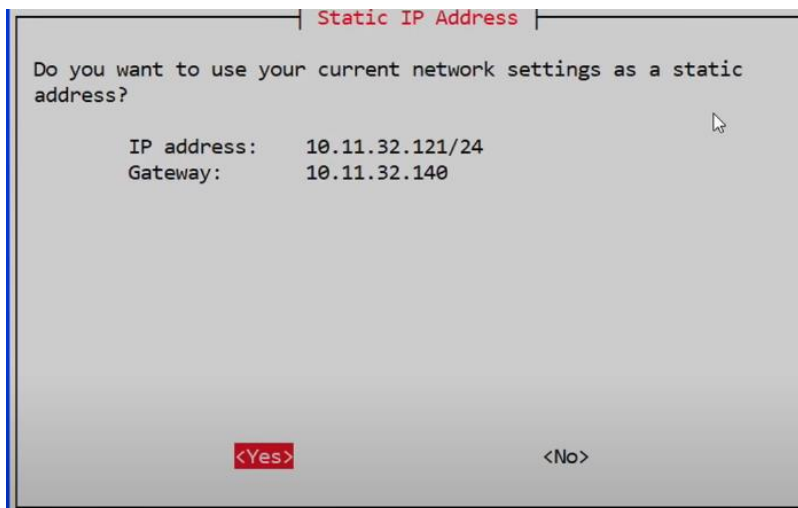
```
pi@raspberrypi: ~  
pi@raspberrypi:~$ su  
Password:  
root@raspberrypi:/home/pi# curl -L https://install.pivpn.io | bash  
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current  
                                 Dload  Upload  Total   Spent    Left   Speed  
100  162  100  162    0     0   109      0  0:00:01  0:00:01 --:--:--  109
```

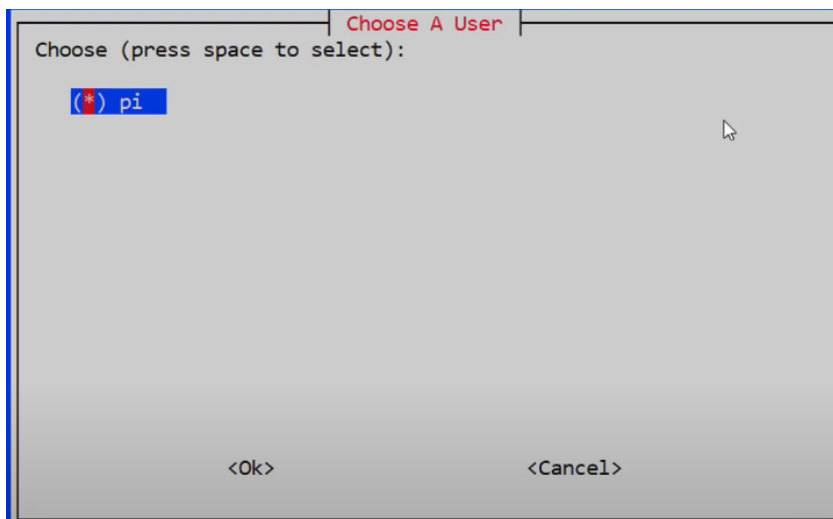
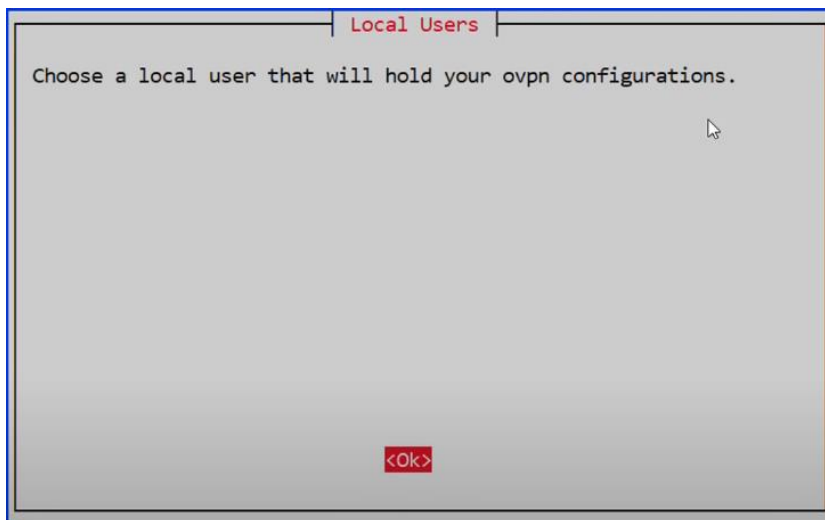
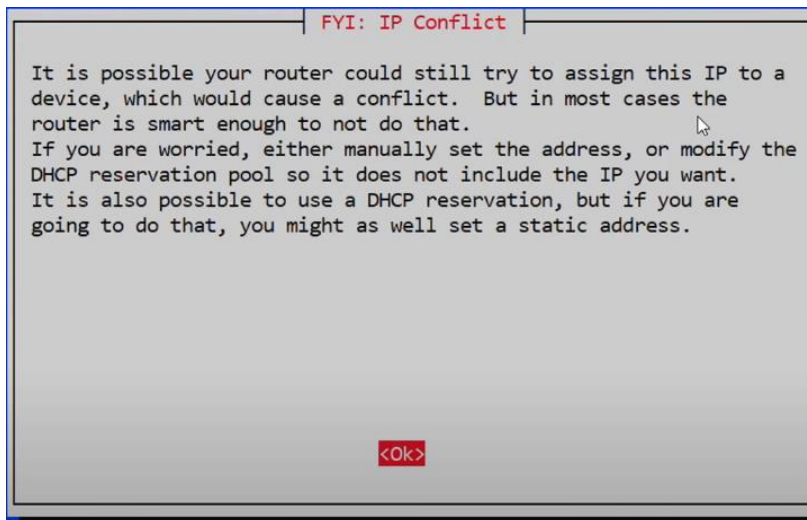
Nos aparecerán las siguientes ventanas y seguiremos los pasos como se muestran



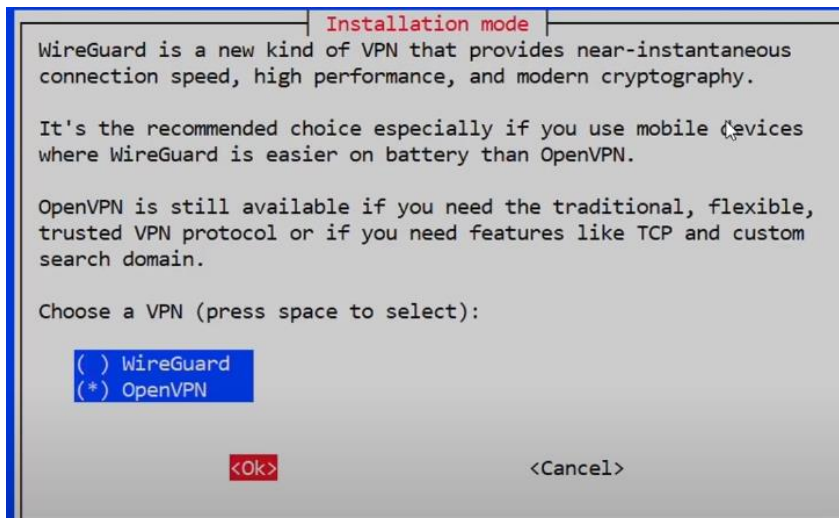


Confirmamos que la dirección ip es correcta

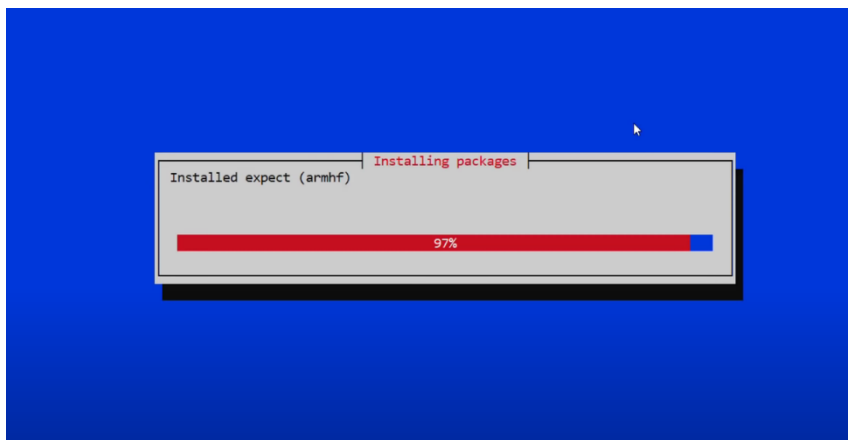
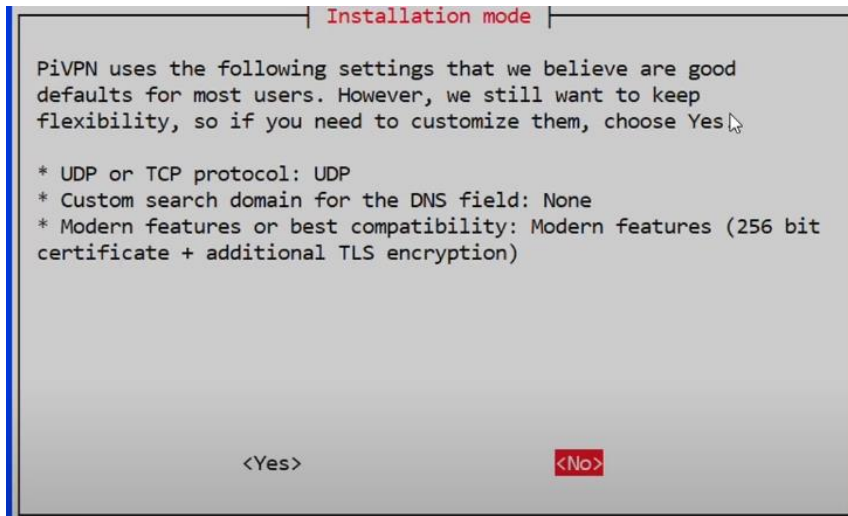


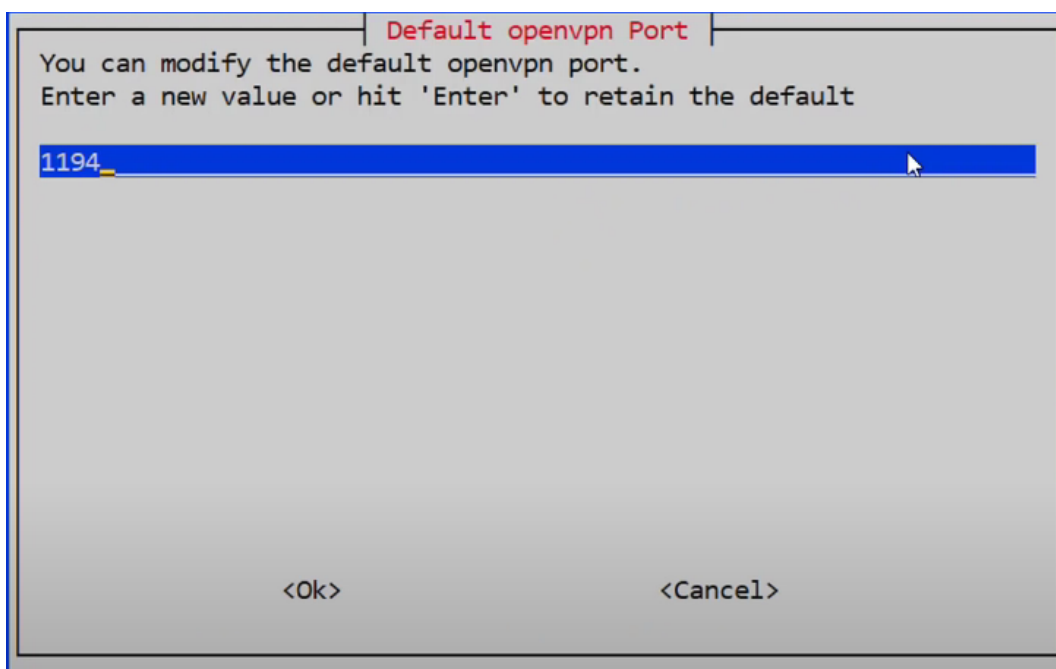


Elegimos la opción openVPN



Damos no





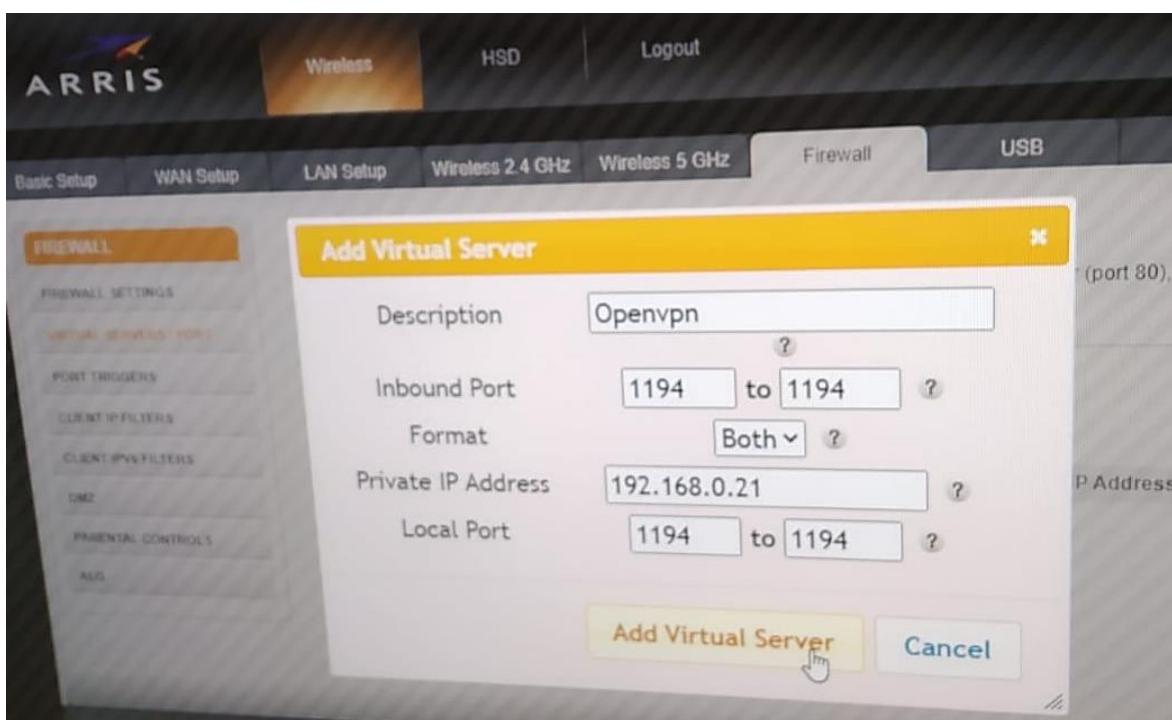
Default openvpn Port

You can modify the default openvpn port.  
Enter a new value or hit 'Enter' to retain the default

1194

<Ok> <Cancel>

Nos vamos a la pagina donde configuramos el router donde vamos a configurar el puerto a trabajar y guardamos los cambios



ARRIS

Wireless HSD Logout

Basic Setup WAN Setup LAN Setup Wireless 2.4 GHz Wireless 5 GHz Firewall USB

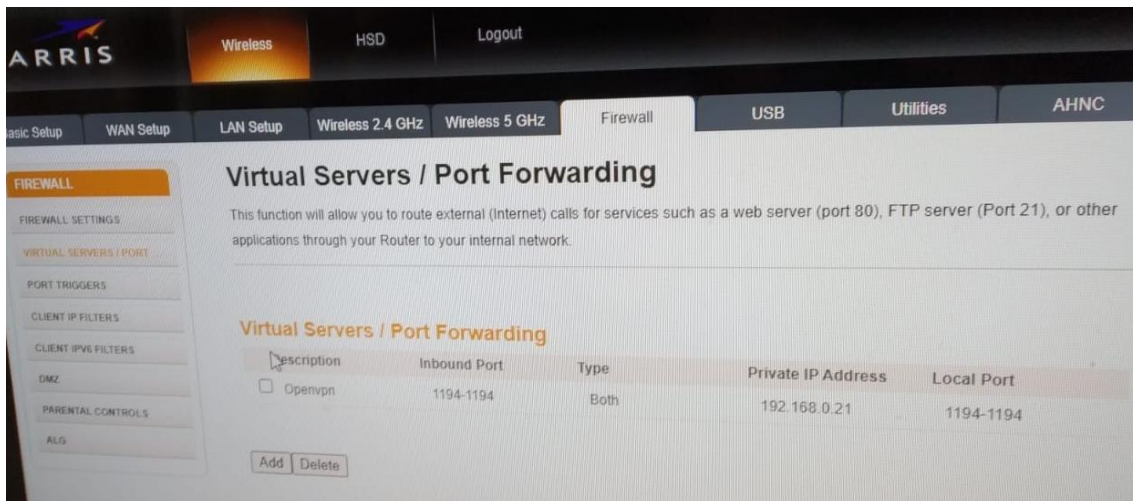
**ADD VIRTUAL SERVER**

DESCRIPTION Inbound Port Format Private IP Address Local Port

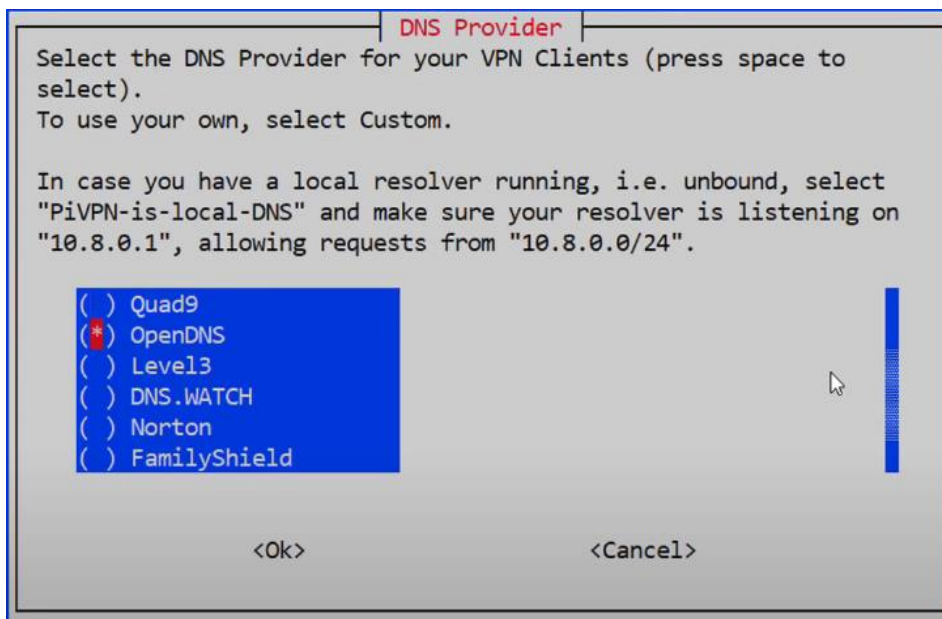
Openvpn 1194 to 1194 Both 192.168.0.21 1194 to 1194

Add Virtual Server Cancel

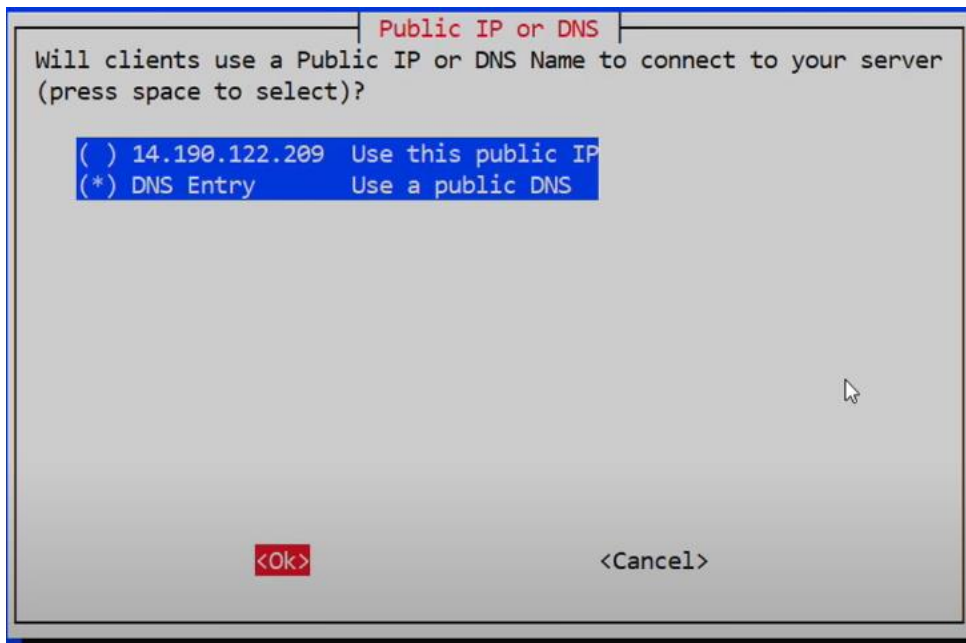
Ahora nos movemos a virtual servers/port , vemos el Puerto donde trabajaremos confirmamos y agregamos



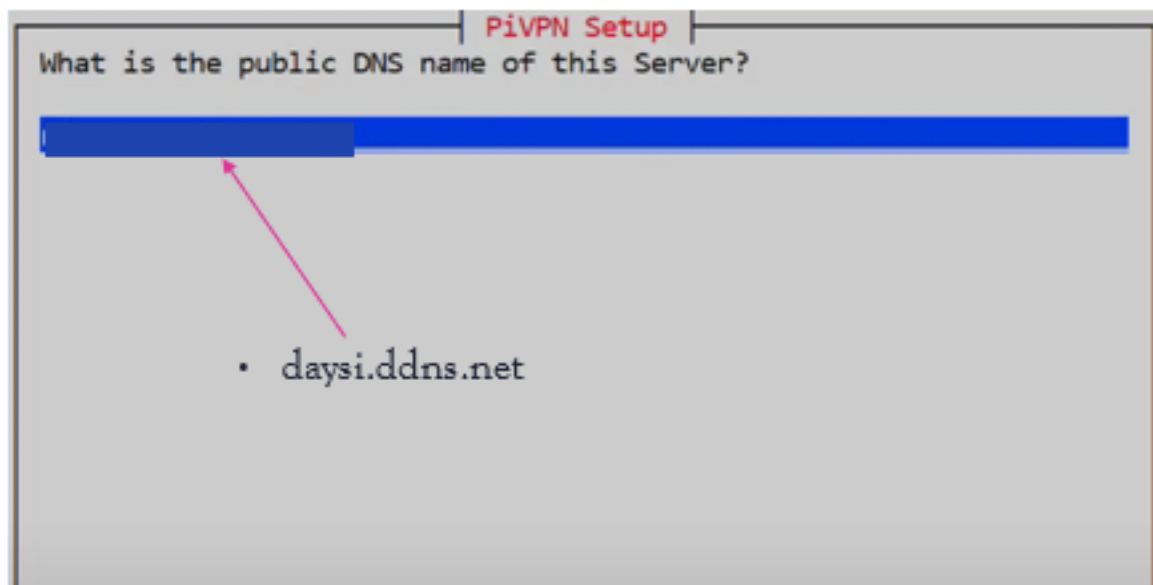
Elegimos la opción de openDNS

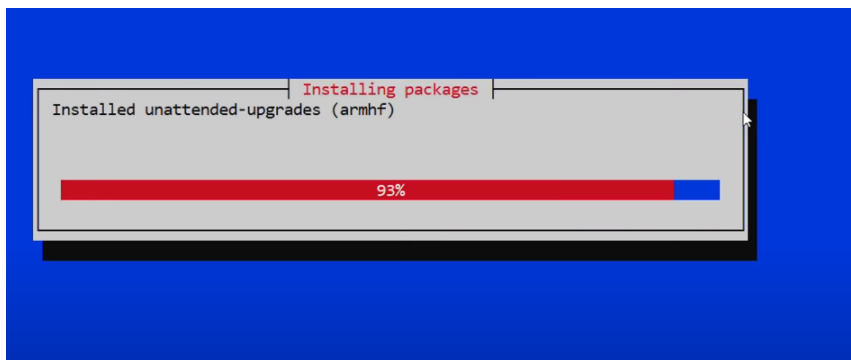
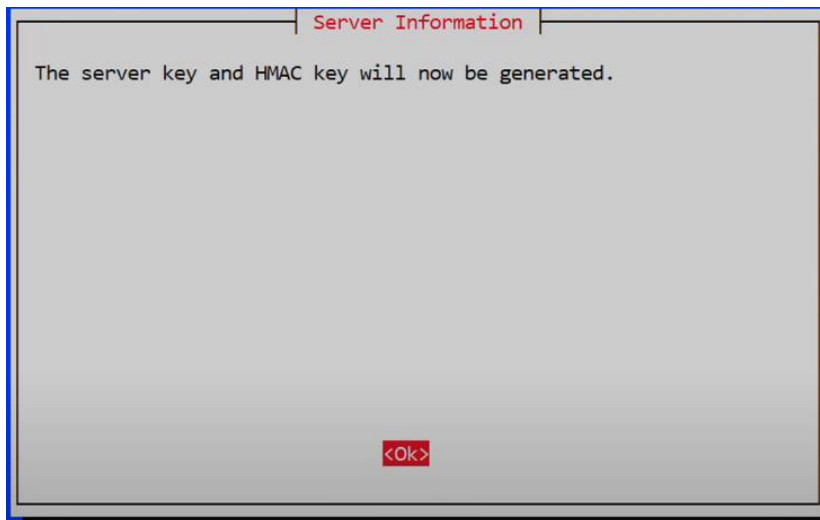


Elegimos DNS Entry

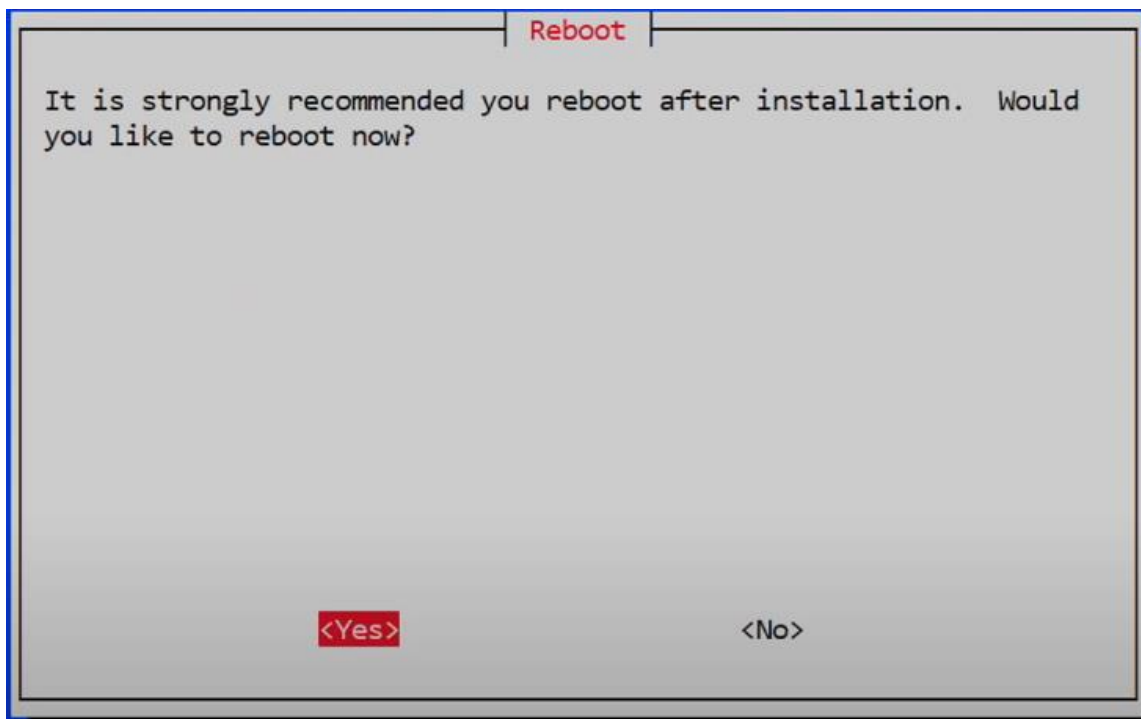


Coloco mi nombre de dominio

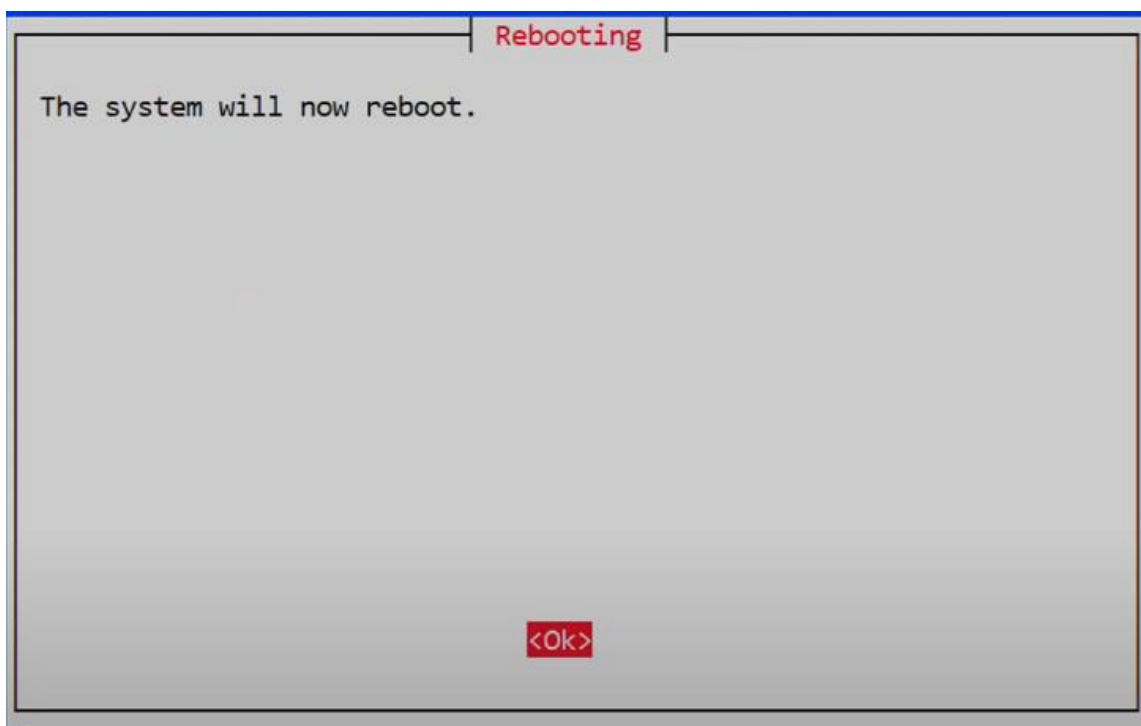
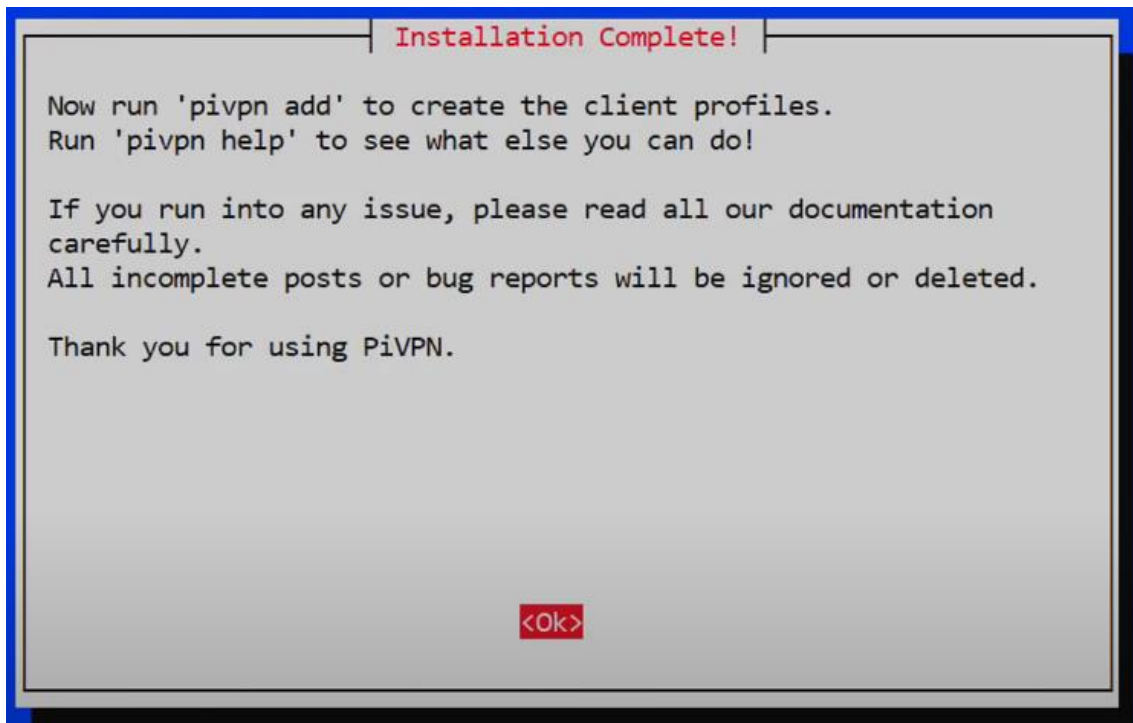




Vamos a reiniciar nuestra raspberry







Una vez echo todo este proceso ya podemos agregar a nuestros usuarios con el comando **ipvpn add**

Colocamos el nombre de nuestro usuario y damos una contraseña

```

pi@raspberrypi:~
root@raspberrypi:/home/pi# pivpn add
::: Create a client ovpn profile, optional nopass
:::
::: Usage: pivpn <-a|add> [-n|--name <arg>] [-p|--password <arg>][nopass] [-d|--days <number>] [-b|--bitwarden] [-i|--iOS]
[-o|--ovpn] [-h|--help]
:::
::: Commands:
::: [none]           Interactive mode
::: nopass           Create a client without a password
::: -n,--name        Name for the Client (default: 'raspberrypi')
::: -p,--password    Password for the Client (no default)
::: -d,--days       Expire the certificate after specified number of days (default: 1080)
::: -b,--bitwarden   Create and save a client through Bitwarden
::: -i,--iOS         Generate a certificate that leverages iOS keychain
::: -o,--ovpn        Regenerate a .ovpn config file for an existing client
::: -h,--help       Show this help dialog

Enter a Name for the Client: net1
How many days should the certificate last? 1080
Enter the password for the client:
Enter the password again to verify:

```

Una vez agregado nuestro usuario se genera automaticamente una llave donde esta se encuentra en la carpeta de /home/pi/ovpns

```

writing new private key to '/etc/openvpn/easy-rsa/pki/easy-rsa-772.SxFZN8/tmp.8inLzg'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
Using configuration from /etc/openvpn/easy-rsa/pki/easy-rsa-772.SxFZN8/tmp.GAY4YR
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName      :ASN.1 12:'net1'
Certificate is to be certified until Aug  2 10:00:59 2023 GMT (1080 days)

Write out database with 1 new entries
Data Base Updated

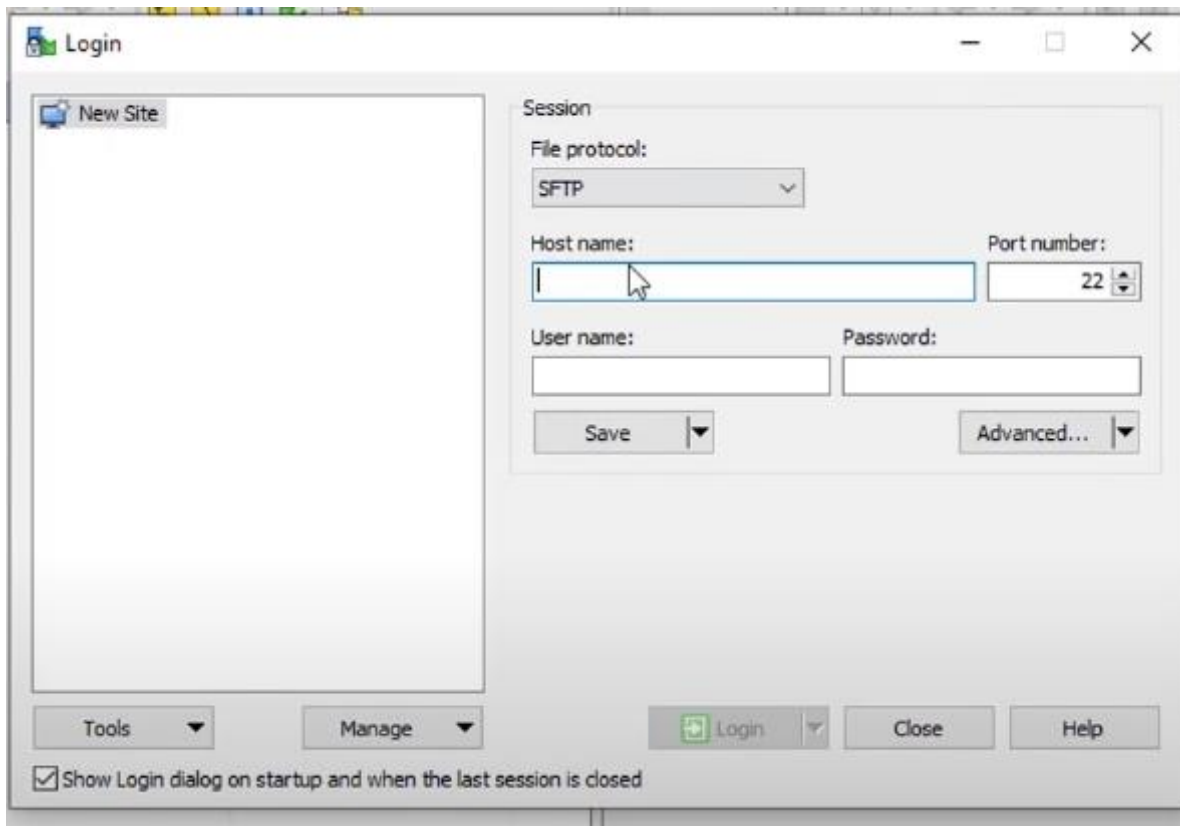
Client's cert found: net1.crt
Client's Private Key found: net1.key
CA public Key found: ca.crt
tls Private Key found: ta.key

=====
Done! net1.ovpn successfully created!
net1.ovpn was copied to:
/home/pi/ovpns
for easy transfer. Please use this profile only on one
device and create additional profiles for other devices.
=====

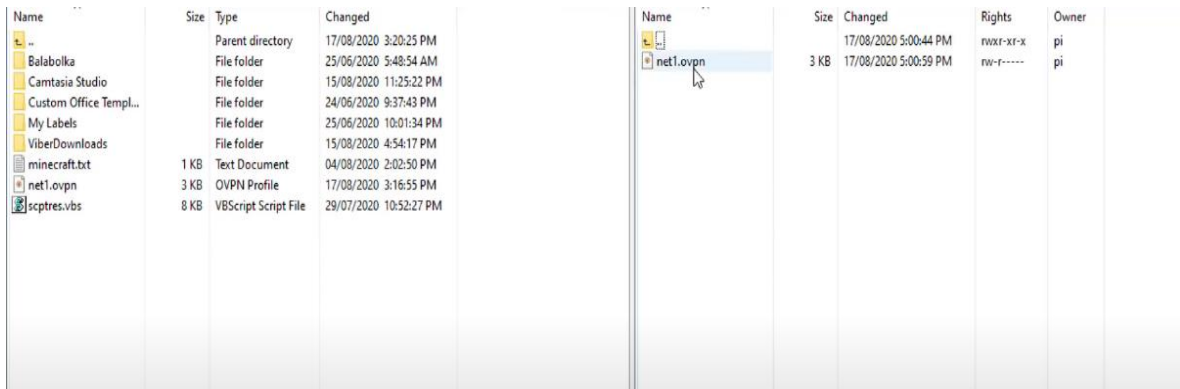
```

Instalamos DSCH para poder pasar las llaves de la raspberry a la computadora.

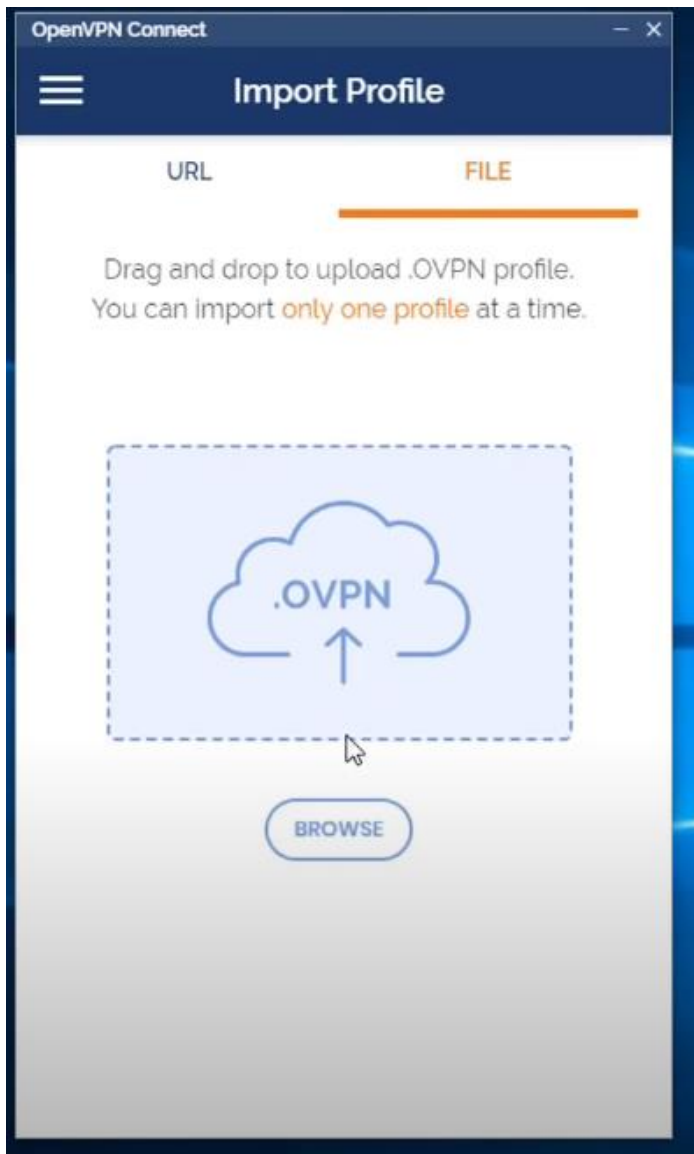
Colocamos la direccion IP de raspberry , en usuario colocamos pi y en la contraseña raspberry



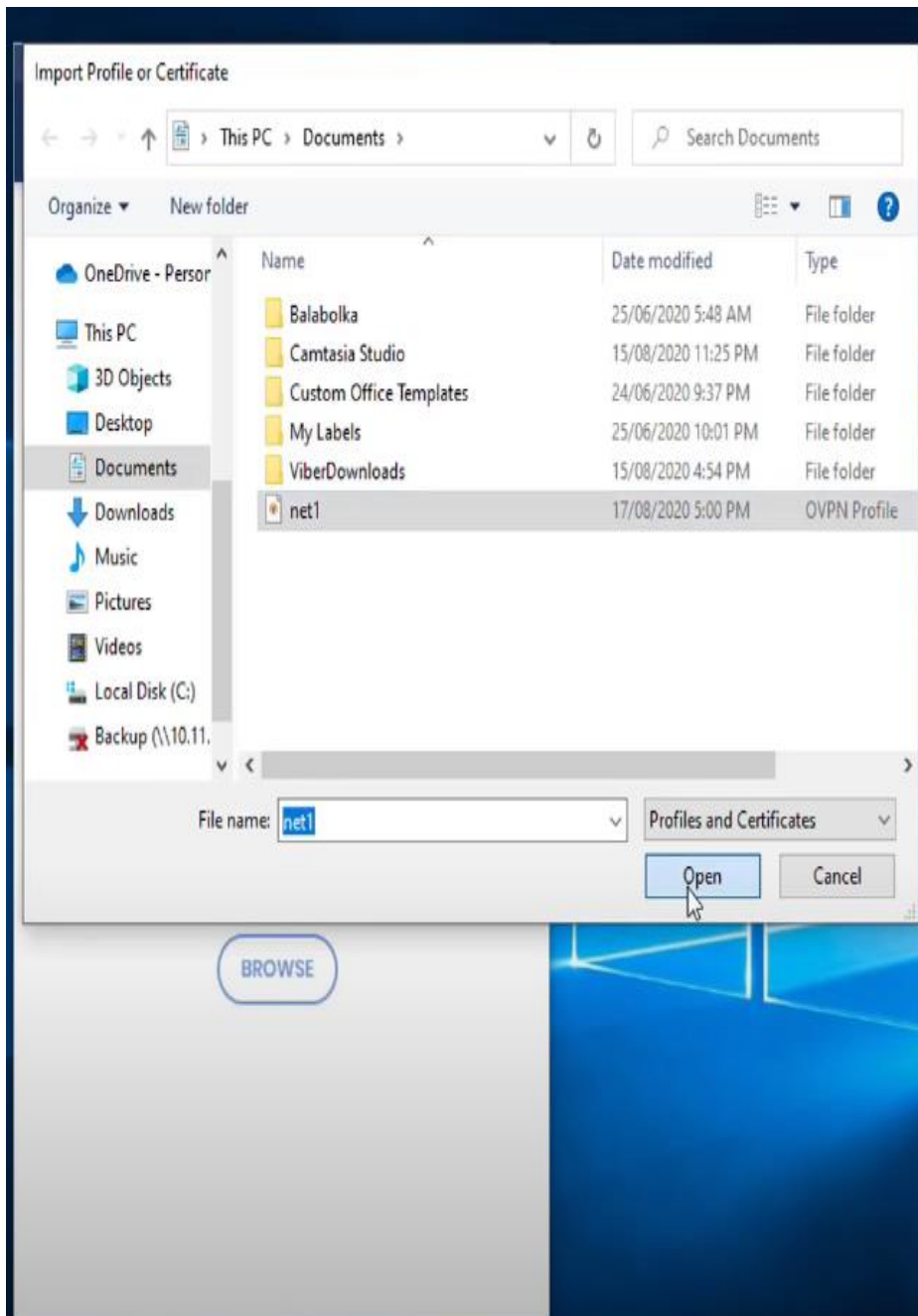
Ahora movemos la llave de raspberry a la computadora



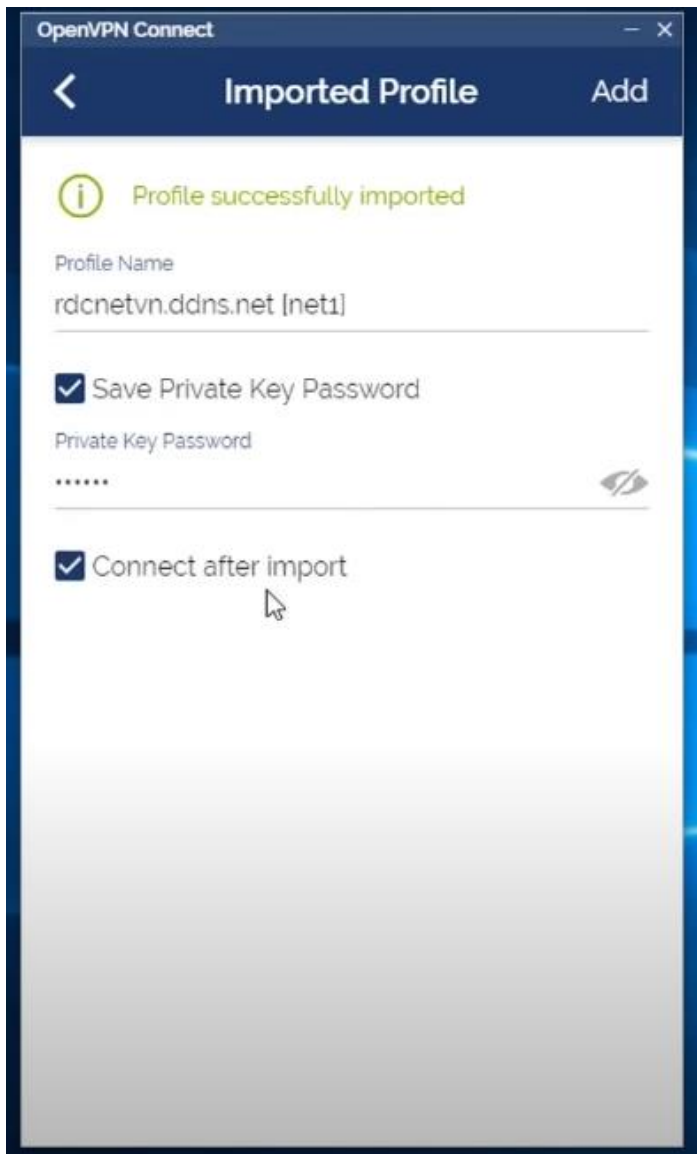
Instalamos el programa OPENVPN y procedemos a ejecutar



Ahora arrastramos la llave al programa



Le damos en save private key password, donde colocamos la contraseña que le dimos al usuario que creamos



Y listo ya tenemos nuestra conexión VPN

OpenVPN Connect



## Profiles



### CONNECTED



OpenVPN Profile  
rdcnnetvn.ddns.net [net1]

### CONNECTION STATS

2.7KB/s



0B/s

BYTES IN  
0 KB/S



BYTES OUT  
0 KB/S

DURATION  
00:00:04

PACKET RECEIVED  
2 sec ago

YOU



YOUR PRIVATE IP  
10.8.0.2