Acceso,Autenticación y Configuración de un Servidor VPN

UO282978

Contenido

Introducción

Este trabajo trata sobre la instalación, configuración y acceso a un servidor VPN. Para este trabajo he decidido usar OpenVPN y Ubuntu Server por diversos motivos que explicare más adelante. Mostrare los usos de un servidor VPN que no mucha gente conoce (no solo sirve para cambiar la dirección IP…), pero antes de meternos a instalar o configurar nada explicare un poco la materia que trataremos.

VPN

¿Qué es una VPN?

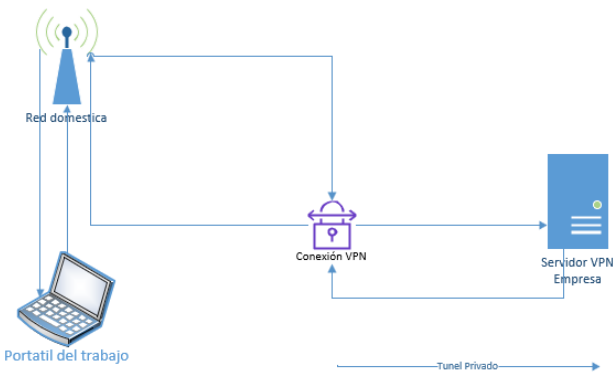
Una VPN (Virtual Private Network, en español Red Privada Virtual) es una herramienta de tecnología de la información que permite a los usuarios conectarse a Internet de manera segura y privada a través de un túnel cifrado. Esto significa que cuando utiliza una VPN, el tráfico de Internet del usuario pasa a través de un servidor remoto en lugar de pasar directamente a través de su conexión a Internet normal.

¿Para qué sirve una VPN?

Una VPN proporciona varias ventajas, como la protección de la privacidad y la seguridad de la conexión a Internet del usuario, así como la posibilidad de acceder a contenido que podría estar bloqueado en su ubicación geográfica.

Pero quitando los usos más conocidos de las VPN, también debemos conocer otras utilidades como sería lo útiles que son para las empresas, ya que permiten a los trabajadores acceder de forma segura a la red de la empresa desde cualquier lugar y en cualquier momento, lo que facilita la colaboración y la productividad. Su uso ha aumentado desde la llegada de la pandemia y el trabajo remoto, yo mismo he trabajado con una red VPN desde el portátil del trabajo para acceder a contenido que se nos tenía asignado o para poder subir cosas al servidor.

Hay muchas diferentes opciones de servicios VPN disponibles en el mercado, y pueden ser utilizados en dispositivos como ordenadores, teléfonos móviles y tablets. Es importante tener en cuenta que, aunque las VPN ofrecen una gran cantidad de beneficios, no son infalibles y no deben ser consideradas como la única medida de seguridad en línea. Es importante tomar otras precauciones de seguridad, como utilizar contraseñas seguras y mantener actualizado el software de seguridad en todos sus dispositivos. Pero en este trabajo vamos a centrarnos en como montar nuestro propio servidor VPN, administrarlo y simular como cliente el conectarnos y hacer uso de este.



¿Porque usar una VPN?

Hay varias razones por las que algunas personas y empresas pueden utilizar una VPN:

1. Acceso remoto seguro: Una VPN puede proporcionar acceso remoto seguro a los recursos de una empresa, como servidores y bases de datos, lo que permite a los empleados trabajar de forma remota de manera segura.
2. Protección de la privacidad: Una VPN cifra el tráfico de red y evita que los datos sean interceptados por terceros, lo que puede proteger la privacidad de los usuarios al navegar por Internet.
3. Acceso a contenido restringido: Una VPN puede permitir a los usuarios acceder a contenido restringido o bloqueado en su ubicación actual, como sitios web o servicios en línea.
4. Protección contra ataques de redes Wifi públicas: Una VPN puede proteger a los usuarios contra ataques y vigilancia cuando se conectan a redes Wifi públicas.

Respecto a las empresas, no existe una ley específica en España que obligue a las empresas a utilizar una VPN (Red Privada Virtual). Sin embargo, existen varias leyes y regulaciones que pueden requerir que las empresas protejan la privacidad y la seguridad de la información de sus empleados y clientes, lo que puede requerir la implementación de medidas de seguridad como una VPN. Algunas de estas leyes y regulaciones incluyen:

1. Ley Orgánica de Protección de Datos (LOPD): Esta ley establece los derechos y obligaciones de las empresas en cuanto a la protección de datos personales y la privacidad de los empleados y clientes.
2. Reglamento General de Protección de Datos (RGPD): Este reglamento establece las normas que deben seguirse para la protección de datos personales en la Unión Europea y se aplica a todas las empresas que operan en la UE.
3. Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI): Esta ley establece las normas que deben seguirse en materia de comercio electrónico y protección de datos en Internet.

¿Las VPN me hacen completamente anónimo en internet?

Una VPN puede proporcionar un nivel adicional de privacidad y seguridad al navegar por Internet, pero no garantiza el anonimato completo. Sobre todo, porque los proveedores de muchas VPN recopilan datos como la dirección IP de origen y el historial de navegación.

Ubuntu Server

¿Por qué Ubuntu Server?

Es una de las distribuciones más usadas tanto para servidores como para entornos de escritorio junto a Debian,CentOS,Fedora…

Pero los motivos por los que he decidido realizar el trabajo con Ubuntu Server son los siguientes:

1. Facilidad de uso: Ubuntu Server tiene una gran cantidad de herramientas y utilidades que facilitan la administración del servidor.
2. Actualizaciones regulares y soporte a largo plazo: Recibe actualizaciones regulares y tiene un ciclo de vida de soporte a largo plazo, lo que significa que los usuarios se espera recibir soporte y actualizaciones durante un período prolongado de tiempo.
3. Amplia compatibilidad con hardware: Es compatible con una amplia variedad de hardware, lo que significa que es posible utilizarlo en una gran cantidad de configuraciones de servidor diferentes.
4. Amplia comunidad y soporte: Tiene una amplia comunidad de usuarios y un equipo de soporte dedicado que pueden proporcionar ayuda y soporte técnico a los usuarios. Al igual que escogí OpenVPN, Ubuntu es una distribución con amplio material en internet, lo cual nos servirá en caso de tener alguna duda o problema contar con amplios resultados de posibles soluciones.

Instalación

En este caso ya cuento con una maquina virtualizada con ProxMox de Ubuntu Server del anterior trabajo, pero en caso de necesitar ayuda con la misma podríamos seguir el propio tutorial que nos pone Ubuntu en su página web: Instalación de Ubuntu Server

OpenVPN

¿Por qué OpenVPN?

OpenVPN es una buena alternativa a otros softwares de VPN porque es una solución de código abierto y de alta calidad que ofrece una gran cantidad de características y opciones de configuración avanzadas. Algunas de las ventajas de OpenVPN incluyen:

1. Seguridad: Utiliza cifrado de alta calidad para proteger su conexión a Internet y garantizar que el tráfico del usuario en la red sea privado.
2. Flexibilidad: Es compatible con una amplia variedad de plataformas y sistemas operativos, lo que significa que puede utilizarse en una gran cantidad de dispositivos.
3. Personalización: Permite configurar y personalizar su conexión VPN de muchas maneras diferentes, lo que le da un gran control sobre cómo se utiliza la VPN.
4. Escalabilidad: Es una solución escalable que se puede utilizar tanto para conexiones individuales como para redes empresariales.

Al ser OpenVPN una solución de código abierto, significa que está disponible para cualquiera que desee utilizarlo y contribuir al desarrollo. Esto ha llevado a una amplia comunidad de

desarrolladores y usuarios que han contribuido a mejorarlo y perfeccionarlo a lo largo del tiempo. En resumen, OpenVPN es una buena opción para aquellos que buscan una solución de VPN de alta calidad y altamente personalizable.

Alternativas a OpenVPN (Protocolos)

OpenVPN utiliza un protocolo de red privada virtual propietario llamado OpenVPN Protocol. Este protocolo utiliza cifrado de alta calidad y es compatible con una amplia variedad de plataformas y sistemas operativos.

OpenVPN Protocol utiliza un esquema de cifrado basado en TLS (Transport Layer Security) y OpenSSL, lo que le permite ofrecer una gran cantidad de opciones de cifrado y autenticación. Además, OpenVPN Protocol utiliza una técnica llamada "enmascaramiento de clave", lo que significa que el cifrado se hace a través de una clave aleatoria que cambia constantemente durante la sesión de conexión. Esto hace que sea muy difícil para los atacantes descifrar la conexión y protege la privacidad y seguridad del usuario.

Hay muchas alternativas al protocolo de OpenVPN en el mercado, algunas de las cuales serían:

1. PPTP (Point-to-Point Tunneling Protocol): Es un protocolo de VPN de uso general que se ha utilizado durante mucho tiempo y que es relativamente fácil de configurar y utilizar. Sin embargo, PPTP tiene algunas vulnerabilidades de seguridad conocidas y puede no ser la opción más segura disponible.
2. L2TP/IPSec (Layer 2 Tunneling Protocol/Internet Protocol Security): Es una opción de VPN más segura que PPTP que utiliza cifrado de alta calidad. Sin embargo, puede ser un poco más complicado de configurar y utilizar que algunas otras opciones.
3. IKEv2 (Internet Key Exchange version 2): Es un protocolo de VPN relativamente nuevo que ofrece un rendimiento excelente y una conexión estable. También es relativamente fácil de configurar y utilizar.
4. WireGuard: Es un protocolo de VPN relativamente nuevo que se ha destacado por su rendimiento excepcional y su diseño simple y eficiente. Es relativamente fácil de configurar y utilizar, y ha ganado una gran cantidad de popularidad en los últimos años.

En resumen, hay muchas opciones de VPN disponibles en el mercado, cada una con sus propias ventajas y desventajas. Es importante investigar y comparar diferentes opciones para encontrar la que mejor se adapte a nuestras necesidades.

Alternativas a OpenVPN (Software)

Una de las alternativas que podemos encontrar es SoftEther VPN, este es muy similar a OpenVPN aun así por diversos motivos (como que OpenVPN es posiblemente el más grande o que existe muchísimo contenido y tutoriales acerca de OpenVPN en internet) me he decantado por OpenVPN. Aun así, es difícil decir si cual es "mejor", ya que ambas son herramientas de VPN de alta calidad con diferentes ventajas y desventajas.

Instalación (Ubuntu Server)

Antes de instalar nada lo primero y más recomendable es una vez conectados al servidor actualizar el mismo, para ello introduciremos los siguientes comandos:

```
sudo apt update
sudo apt upgrade
```

Debemos saber la IP pública de nuestro servidor. Se supone que esta misma ya la sabríamos en caso de que este servidor fuera proporcionado por un hosting pues necesitamos dicha IP para conectarnos vía FTP o SSH. En caso de tratarse de un servidor ya sea domestico o empresarial pero que no contemos con la IP pública podríamos verificarla mediante otro dispositivo conectado a la red en la página: myip.com .

En cualquier caso, podemos comprobarlo desde el mismo servidor mediante el siguiente comando (existen otros comandos posibles, pero este es un ejemplo):

```
host myip.opendns.com resolver1.opendns.com
```

Por motivos evidentes he censurado mi dirección IP pública, pero sería el resultado arrojado en terminal marcado con una línea roja.

Una vez realizados estos pasos podemos proceder a la instalación de OpenVPN.

Para instalar OpenVPN como servidor existen varias opciones, en este caso voy a utilizar un script que nos permite instalarlo y facilitar el trabajo de configuración.

```
wget https://git.io/vpn -O openvpn-install.sh
```

Hay que tener cuidado cuando se descarga un script de internet, sobre todo cuando requiere usar root para instalarse. En caso de tener los conocimientos necesarios podríamos comprobar el código del script con la orden “less”.

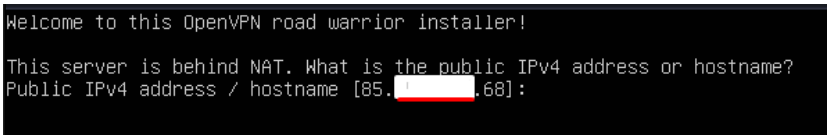
Ahora debemos dar permisos al script con:

```
chmod +x openvpn-install.sh
```

Para ejecutar el script deberíamos introducir en la terminal lo siguiente:

```
sudo bash openvpn-install.sh
```

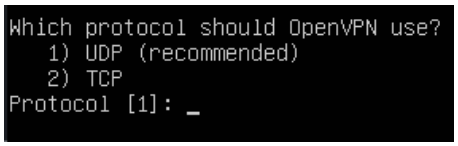
Al ejecutar el script nos saldría lo siguiente:



En rojo otra vez vendría indicada nuestra IP pública (en este caso al usar este script no sería necesario consultarla previamente, pero si no tuviéramos este script si sería necesario).

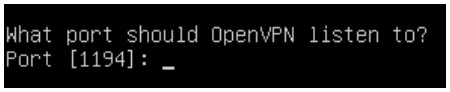
Si nuestra IP pública es correcta presionaríamos *Enter* para proseguir con la instalación.

A continuación, nos preguntaría lo siguiente:

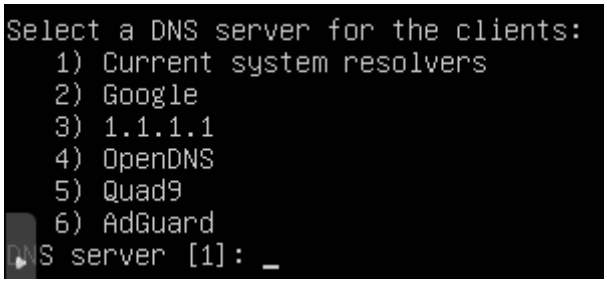


Que protocolo deseamos usar, en este caso usaremos UPD (el recomendado) aunque en caso de ser necesario usar TCP seleccionaríamos la opción 2. Para ello tecleamos el número de la opción a escoger y presionaríamos *Enter*.

A continuación, nos preguntaría porque puerto desearíamos conectarnos mediante OpenVPN.



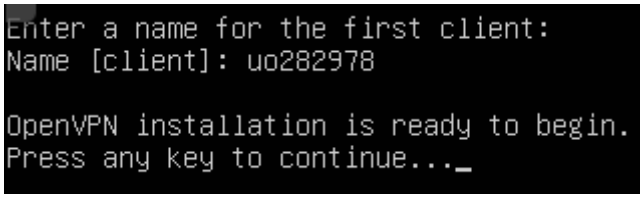
Podríamos introducir otro puerto, pero en este caso voy a dejar la opción por defecto (pulsaríamos *Enter* para continuar con la instalación).



A continuación, nos pide escoger el servidor DNS para los clientes.

En este caso para este trabajo escogeré la opción 2, la opción de Google en cualquier caso cualquier opción es válida.

Ahora el programa nos pedirá crear la cuenta de nuestro primer cliente o usuario de nuestra VPN, creare una cuenta de ejemplo como primer usuario.



Además, nos indicaría el script que ya esta preparada la instalación y que presionemos una tecla para continuar. Presionaríamos el *Enter* y la instalación procedería a instalarse OpenVPN.

Como ultima salida del script tenemos que nos ha generado un archivo de configuración del cliente que hemos creado y que para crear un nuevo cliente podemos ejecutar de nuevo el script.

Verificar Servicio OpenVPN y Configuración

Verificar Servicio Firewall

Verificar que la salida de este comando:

```
sudo systemctl cat openvpn-iptables.service
```

Es igual o similar a la siguiente:

```
root@ubuntuuo:/home/uo282978# systemctl cat openvpn-iptables.service
# /etc/systemd/system/openvpn-iptables.service
[Unit]
Before=network.target
[Service]
Type=oneshot
ExecStart=/usr/sbin/iptables -t nat -A POSTROUTING -s 10.8.0.0/24 ! -d 10.8.0.0/24 -j SNAT --to 192.168.0.17
ExecStart=/usr/sbin/iptables -I INPUT -p udp --dport 1194 -j ACCEPT
ExecStart=/usr/sbin/iptables -I FORWARD -s 10.8.0.0/24 -j ACCEPT
ExecStart=/usr/sbin/iptables -I FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
ExecStop=/usr/sbin/iptables -t nat -D POSTROUTING -s 10.8.0.0/24 ! -d 10.8.0.0/24 -j SNAT --to 192.168.0.17
ExecStop=/usr/sbin/iptables -D INPUT -p udp --dport 1194 -j ACCEPT
ExecStop=/usr/sbin/iptables -D FORWARD -s 10.8.0.0/24 -j ACCEPT
ExecStop=/usr/sbin/iptables -D FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
RemainAfterExit=yes
[Install]
WantedBy=multi-user.target
```

Este comando nos muestra el servicio que creara las reglas en el firewall de la parte de conexiones.

También debemos asegurarnos de que nuestro firewall (UFW) no bloquee el puerto de acceso de OpenVPN.

```
root@ubuntuuo:/home/uo282978# ufw allow 1194
Rule added
Rule added (v6)
```

Verificar Configuración OpenVPN

Esto podremos hacerlo ejecutando el siguiente comando:

```
sudo less /etc/openvpn/server/server.conf
```

Deberíamos observar una salida parecida a lo siguiente, donde podemos observar el puerto que estamos utilizando, protocolo y confirmar que todo este correcto.

```
local 192.168.0.17
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh.pem
auth SHA512
tls-crypt tc.key
topology subnet
server 10.8.0.0 255.255.255.0
push "redirect-gateway def1 bypass-dhcp"
ifconfig-pool-persist ipp.txt
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
push "block-outside-dns"
keepalive 10 120
cipher AES-256-CBC
user nobody
group nogroup
persist-key
persist-tun
verb 3
crl-verify crl.pem
explicit-exit-notify
```

Verificar que se esté ejecutando OpenVPN

Podemos comprobarlo con el siguiente comando:

```
sudo systemctl status openvpn-server@server.service
```

```
root@ubuntuuo:/home/uo282978# systemctl status openvpn-server@server.service
● openvpn-server@server.service - OpenVPN service for server
     Loaded: loaded (/lib/systemd/system/openvpn-server@.service; enabled; preset: enabled)
     Active: active (running) since Sat 2022-12-31 02:41:56 UTC; 16min ago
       Docs: man:openvpn(8)
             https://community.openvpn.net/openvpn/wiki/Openvpn24ManPage
             https://community.openvpn.net/openvpn/wiki/HOWTO
   Main PID: 7699 (openvpn)
     Status: "Initialization Sequence Completed"
      Tasks: 1 (limit: 9396)
     Memory: 1.4M
        CPU: 384ms
     CGroup: /system.slice/system-openvpn\x2dserver.slice/openvpn-server@server.service
             └─7699 /usr/sbin/openvpn --status /run/openvpn-server/status-server.log --status-version 2 --suppress-timestamps --

dic 31 02:41:56 ubuntuuo openvpn[7699]: Socket Buffers: R=[212992->212992] S=[212992->212992]
dic 31 02:41:56 ubuntuuo openvpn[7699]: UDPv4 link local (bound): [AF_INET]192.168.0.17:1194
dic 31 02:41:56 ubuntuuo openvpn[7699]: UDPv4 link remote: [AF_UNSPEC]
dic 31 02:41:56 ubuntuuo openvpn[7699]: UID set to nobody
dic 31 02:41:56 ubuntuuo openvpn[7699]: GID set to nogroup
dic 31 02:41:56 ubuntuuo openvpn[7699]: Capabilities retained: CAP_NET_ADMIN
dic 31 02:41:56 ubuntuuo openvpn[7699]: MULTI: multi_init called, r=256 v=256
dic 31 02:41:56 ubuntuuo openvpn[7699]: IFCONFIG POOL IPv4: base=10.8.0.2 size=253
dic 31 02:41:56 ubuntuuo openvpn[7699]: IFCONFIG POOL LIST
dic 31 02:41:56 ubuntuuo openvpn[7699]: Initialization Sequence Completed
```

Podemos comprobar en verde como el servicio está activo y ejecutándose.

En caso contrario debemos arrancarlo mediante la misma orden cambiando “status” por “start”.

Prueba de conexión Usuario-Servidor

Extraemos del servidor el archivo .ovpn del usuario creado anteriormente. Debemos tener mucho cuidado, ya que cualquier persona con el archivo podría conectarse a nuestro servidor VPN.

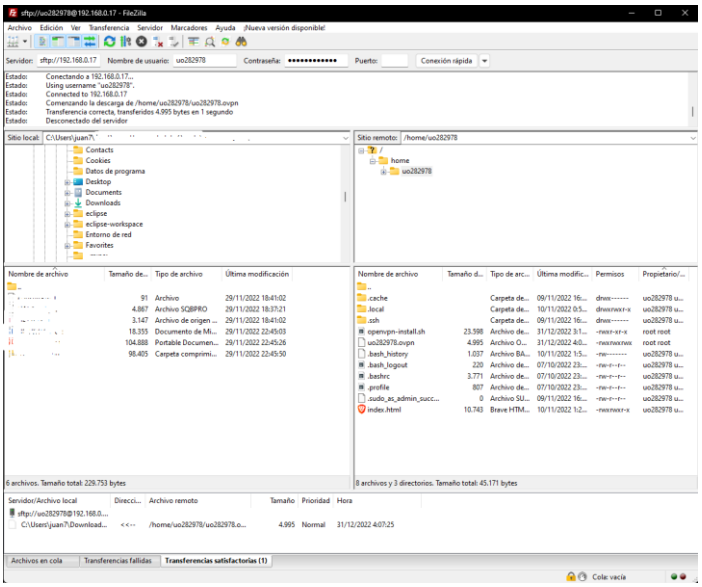
Para ello el método que he utilizado sería el siguiente:

```
root@ubuntuuo:/home/uo282978# cp /root/uo282978.ovpn /home/uo282978/
root@ubuntuuo:/home/uo282978# chmod 777 /home/uo282978/uo282978.ovpn
```

He copiado el archivo a un usuario con mi uo que tengo en el servidor y le he concedido permisos al archivo.

Luego he procedido a conectarme por FTP al servidor (ya que estoy virtualizando el servidor en VirtualBox y ProxMox) y ahora voy a pasarlo a mi portátil en el que estaré conectado a una red

distinta (la red de datos del móvil) para comprobar el funcionamiento de OpenVPN simulando ser un Cliente/Usuario que hace uso de la VPN.

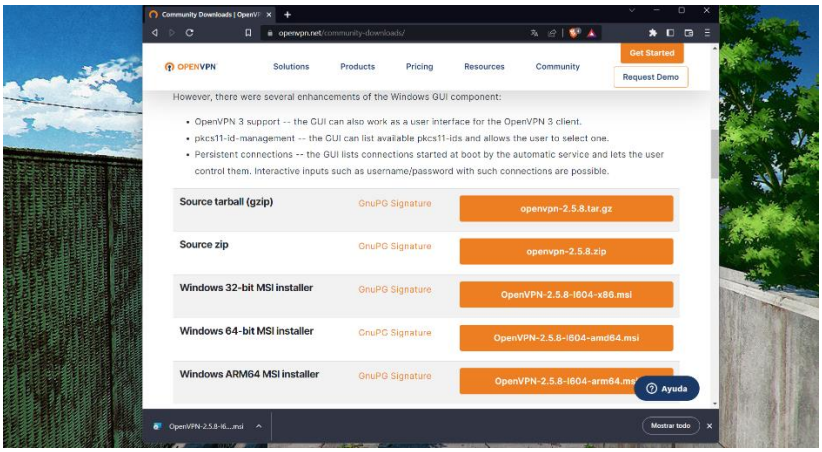


Para poder conectarnos a la VPN fuera de nuestra red es necesario abrir el puerto 1134 (el que configuremos para que use OpenVPN) por protocolo UDP. Para ello accederemos en el navegador a la IP local 192.168.0.1 y nos saldrá un panel de login donde meteremos usuario: admin,contraseña: admin . Y buscaremos donde poder abrir los puertos de nuestro router.

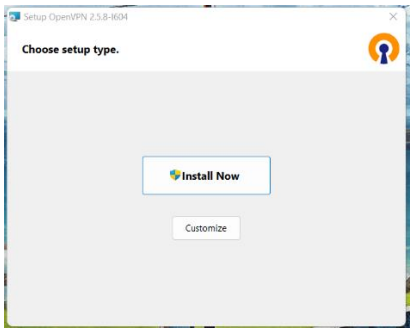
Una vez abiertos los puertos de nuestro router procedemos a descargar el cliente de OpenVPN

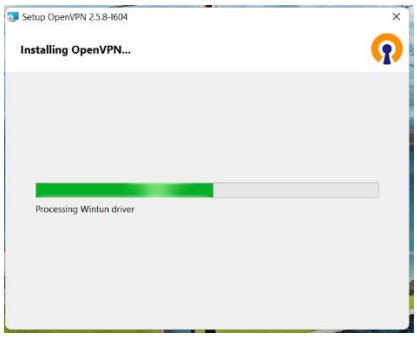
en el cliente (mi portátil) quien no esta conectado a la red en la que se ubica el servidor VPN (mi red móvil).

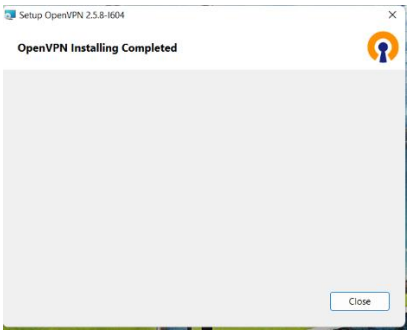
Descargaríamos la última versión para Windows en este caso (también se puede en MacOS y Linux).



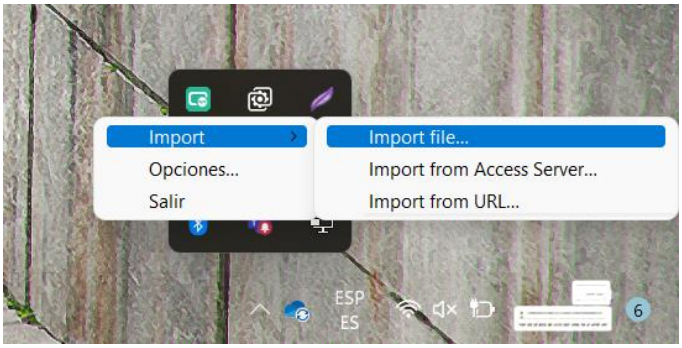
Ejecutamos el instalador y procedemos en la instalación

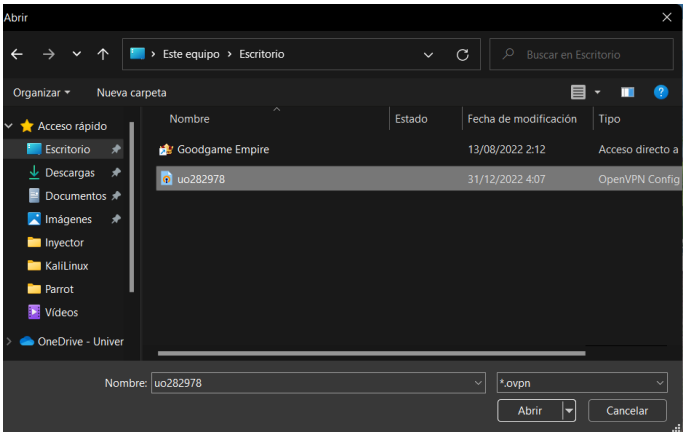






Una vez completada la instalación procederíamos a importar el archivo .ovpn que creamos para el usuario uo282978.

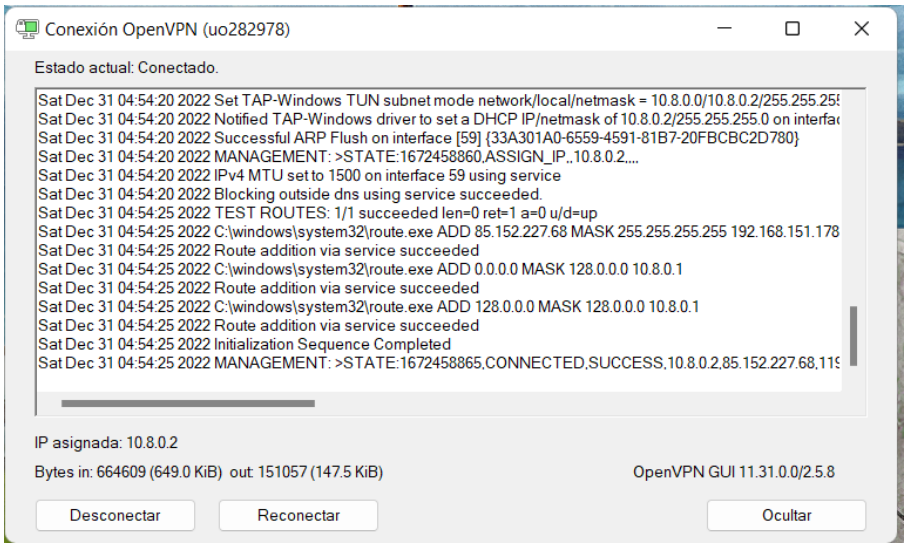




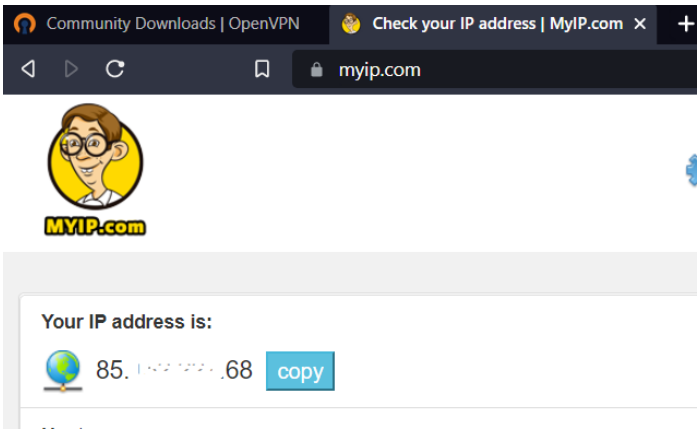
Una vez importado comprobaríamos nuestra IP pública fuera de la red del servidor VPN.

Como podemos ver la IP pública de la red móvil es 31.X.X.46 (muy distinta de la del servidor VPN 85.X.X.68

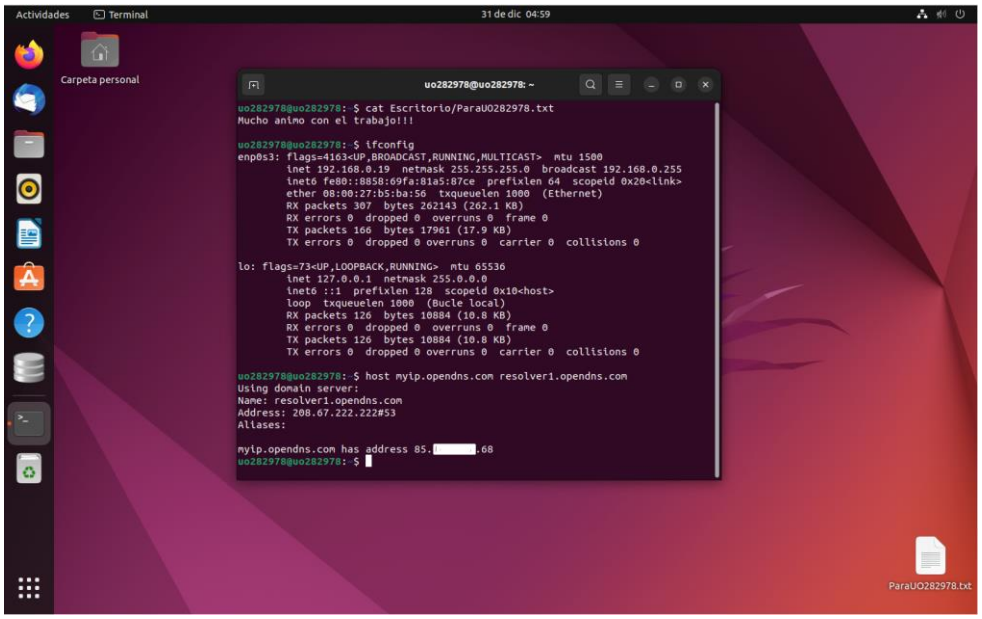
Nos conectaríamos mediante el perfil de uo282978 a nuestro servidor OpenVPN:



Y como podemos observar al ver nuestra IP pública ahora tenemos la del servidor VPN una vez conectados a él (es como si estuviéramos allí mismo conectados):



Para poder poner un ejemplo practico y sencillo de las posibilidades que esto tiene, he creado en una maquina virtual que esta en mi red de casa (como se puede observar en la salida de la IP pública) un archivo .txt llamado ParaUO282978 ¿Qué será lo que tendrá?



Como al conectarnos por VPN es como si estuviéramos físicamente en esa red, puedo conectarme por SSH mediante la IP local a la maquina Ubuntu en la red.

Y si miramos que dice el archivo podemos ver el mensaje de animo que nos ha dejado.

```
PS C:\Users\juan7> ssh uo282978@192.168.0.19
uo282978@192.168.0.19's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-53-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Se pueden aplicar 0 actualizaciones de forma inmediata.

Last login: Sat Dec 31 05:02:05 2022 from 192.168.0.17
uo282978@uo282978:~$ ls /home/uo282978/Escritorio/
ParaUO282978.txt
uo282978@uo282978:~$ cat /home/uo282978/Escritorio/ParaUO282978.txt
Mucho animo con el trabajo!!!

uo282978@uo282978:~$
```

Esto es un ejemplo sencillo que se me ha ocurrido para demostrar un uso de la VPN y cómo funciona, pero podemos poner una situación hipotética (pero bastante real hoy en día) donde un desarrollador por ejemplo desea teletrabajar desde casa y necesita acceder a su ordenador de la oficina porque necesita un archivo o realizar alguna acción en el y evidentemente no se encuentra con la posibilidad de hacerlo. Con una VPN es como si el propio desarrollador se encontrara sentado en su escritorio (al menos a nivel de red) y de forma segura la VPN crea un túnel que protege la información de analizadores de paquetes como WireShark que es utilizado de forma mal intencionada para rastrear el tráfico en redes Wifi públicas.

Añadir/Eliminar Usuario

Para crear o eliminar un Usuario de nuestro servidor VPN lo primero que debemos hacer es ejecutar el script de instalación de OpenVPN que habíamos descargado anteriormente:

```
uo282978@ubuntuuo:~$ ls
index.html  openvpn-install.sh  uo282978.ovpn
uo282978@ubuntuuo:~$ sudo bash openvpn-install.sh
```

```
OpenVPN is already installed.

Select an option:
   1) Add a new client
   2) Revoke an existing client
   3) Remove OpenVPN
   4) Exit
Option: _
```

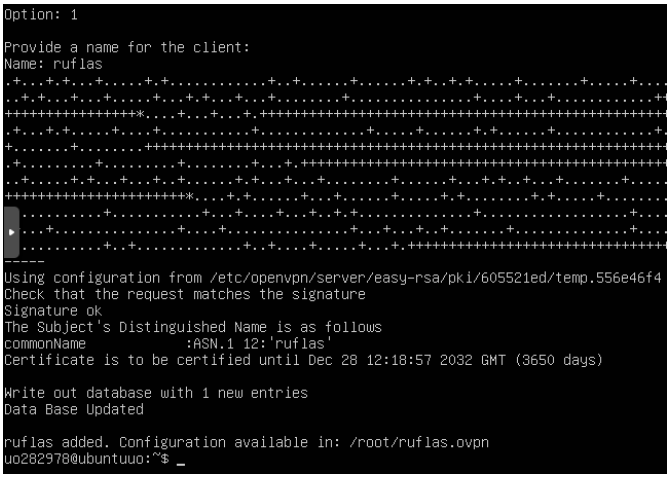
Una vez lo hayamos hecho, nos saldrán varias opciones al detectar el script que OpenVPN ya está instalado:

1. Crear un nuevo usuario
2. Eliminar un usuario existente
3. Eliminar OpenVPN del servidor
4. Salir del script

En este caso queremos añadir un nuevo usuario, el cual lo llamaremos “ruflas” quien podría ser perfectamente un trabajador que requiera acceso de forma segura a la red de la empresa,

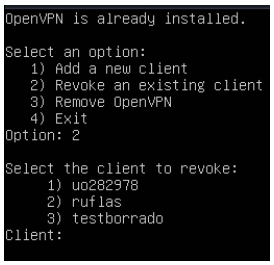
o ser mismamente yo, quien quiere trabajar de forma segura con algún dispositivo de mi red estando fuera de ella.

Teclearíamos la opción 1 (Añadir nuevo usuario) y presionaríamos *Enter*.

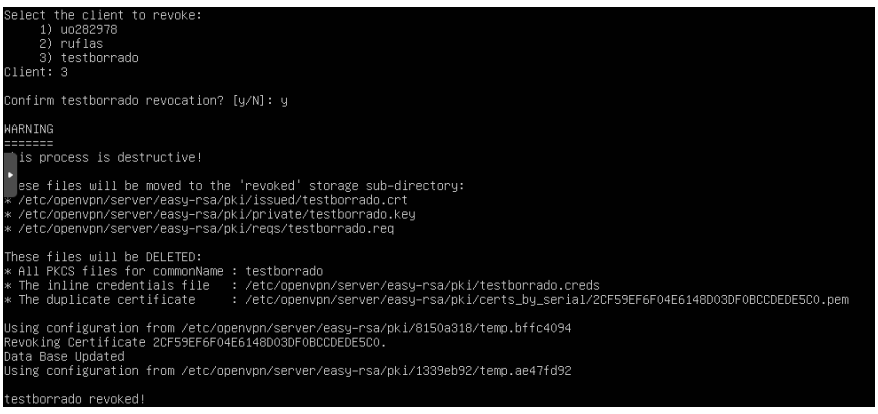


Nos indica que ya ha sido creado el usuario ruflas y que su archivo .ovpn para poder conectarse está en "/root/ruflas.ovpn". Ahora le daríamos al usuario su archivo .ovpn para poder acceder a la red (yo como ya he comentado antes lo sacare por FTP , pero hay muchas más formas).

Para poder eliminar un usuario haríamos lo mismo, pero en vez de teclear la opción 1, tendríamos que teclear la opción 2:



Nos saldría la lista de usuarios que tenemos en la VPN y seria teclear el numero del que deseamos borrar. En este caso eliminare al usuario "testborrado", nos preguntara si estamos seguros de eliminarlo y teclearemos "y":



Ya habríamos eliminado al usuario "testborrado" de nuestro servidor VPN.

Bibliografía

INCIBE (Instituto Nacional de Ciberseguridad)

Web de OpenVPN

Script de Instalación OpenVPN