

MANUAL DE INSTALACIÓN Y CONFIGURACIÓN DE UNA VPN EXTERNA



En este manual se enseñará a instalar y configurar su propia VPN externa desde cero.

C.F.G.S: Administración de sistemas informáticos en red.
Autores: Daniel Polo Gómez y Álvaro Vizuite Martín.
Tutor: Ramón González.
IES La Arboleda.



Esta obra está bajo una [Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional](https://creativecommons.org/licenses/by-nc-sa/4.0/).

Índice

1. Introducción	2
1.1 ¿Qué es una VPN?	2
1.2 Para qué sirven las conexiones VPN	3
1.3 Ventajas de VPN.....	4
1.4 Inconvenientes de VPN.....	4
2. Creación de la VPN	5
2.1 Instalación.....	5
2.2 Configuración.....	6
3. Configuración del servidor	9
4. Prueba de funcionamiento en Windows.....	17
5. Bibliografía.....	21

1. Introducción

1.1 ¿Qué es una VPN?

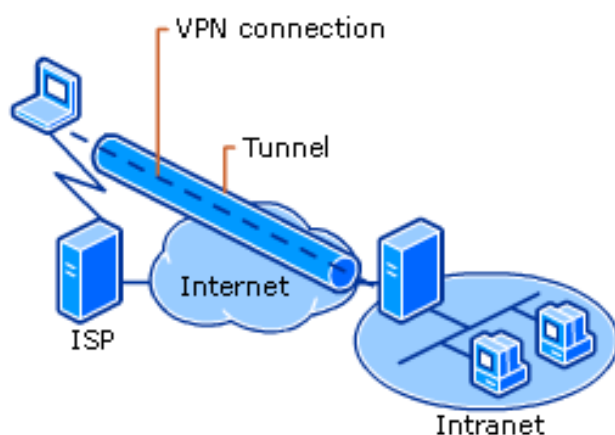
Las conexiones VPN se están empezando a tener más en cuenta. Inicialmente tenían un uso común en las empresas y organizaciones, la gran versatilidad de este tipo de conexiones y sus múltiples usos las hacen cada vez más populares.

VPN son las siglas de Virtual Private Network, o red privada virtual. La palabra clave aquí es virtual, es esta propiedad la que genera la necesidad de la VPN en sí, así como la que permite a las conexiones VPN ofrecerte los múltiples usos que veremos más adelante.

Una conexión VPN lo que te permite es crear una red local sin necesidad que los usuarios estén físicamente conectados entre sí, sino a través de Internet. Obtienen las ventajas de la red local, con una mayor flexibilidad, pues la conexión es a través de Internet y puede por ejemplo ser de una punta del mundo a la otra.

Normalmente, mientras usas Internet tu dispositivo se pone en contacto con tu proveedor de Internet, que es el que conecta con los distintos servicios web para ofrecerte, por ejemplo, los vídeos de YouTube.

Cuando te conectas a una conexión VPN, esto cambia. Todo tu tráfico de red sigue yendo desde tu dispositivo a tu proveedor de Internet, pero de ahí se dirige directo al servidor VPN, desde donde partirá al destino. Idealmente la conexión está cifrada, de modo que tu proveedor de Internet realmente no sabe a qué estás accediendo. A efectos prácticos, tu dirección IP es la del servidor VPN, en muchos aspectos es como si estuvieras físicamente ahí, conectándome a Internet.



1.2 Para qué sirven las conexiones VPN

Actualmente uno de los usos más importantes de las VPN es el teletrabajo, permite la interconectividad en redes que no están físicamente conectadas, como es el caso de trabajadores que trabajan fuera de la oficina o empresas con sucursales en varias ciudades que necesitan acceder a una única red privada. Además, el acceso está protegido, la conexión está previsiblemente cifrada y el trabajador tiene el mismo acceso que si estuviera presencialmente ahí.

Otra función de las VPN es la de evitar censura y bloqueos geográficos de contenido, al conectarte con VPN, tu dispositivo se comunica con el servidor VPN, y es éste el que habla a Internet. Si estás en China y el servidor VPN está en Estados Unidos, generalmente los servidores web creerán que estás navegando desde este país, dejándote acceder a los contenidos disponibles únicos de allí.

Además de todos los usos mencionados anteriormente también da una capa extra de seguridad, es común que las conexiones VPN vengan acompañadas de un cifrado de los paquetes que se transmiten con ellas, por lo que es normal oír la recomendación de que, si necesitas conectarte a un punto de acceso Wi-Fi público, al menos uses te conectes con una VPN.

Otro uso común de las conexiones VPN se encuentra en las descargas P2P. Las conexiones VPN también tienen usos en la descarga P2P aunque bajes torrents completamente legales.

Desgraciadamente cada vez es más común que los proveedores de Internet decidan inmiscuirse en lo que enviamos y recibimos en la Red.

Algunos proveedores bloquean por completo las descargas P2P, mientras que otros simplemente la boicotean para que funcione mal seas tú mismo el que lo deje. Igual que puedes usar una conexión VPN para evitar la censura de tu país, también puedes en ocasiones evitar que tu proveedor de Internet boicotee tus descargas P2P.

1.3 Ventajas de VPN

- Funciona en todas las aplicaciones, ya que enruta todo el tráfico de Internet, a diferencia de los servidores proxy, que sólo puedes usar en el navegador web y un par de aplicaciones más que dejan configurar las opciones de conexión avanzadas.
- Se conecta y desconecta fácilmente, además, una vez configurado, puedes activar y desactivar la conexión cuando quieras.
- Seguridad adicional en puntos de acceso Wifi, siempre y cuando la conexión este cifrada.
- Falseo de tu ubicación, como ya hemos visto en el apartado anterior, una conexión VPN es un modo eficaz de evitar la censura o acceder a contenido limitado a cierta región.
- Tu proveedor de Internet no puede saber a qué te dedicas en Internet. Con una VPN no sabrán a qué te dedicas, pero sí lo sabrá la compañía que gestiona el VPN.

1.4 Inconvenientes de VPN

Usar conexiones VPN parece estar lleno de ventajas: más seguridad, privacidad mejorada, salto de los bloqueos geográficos... Antes de usar un servicio de VPN, hay algunos apartados que debes tener en cuenta:

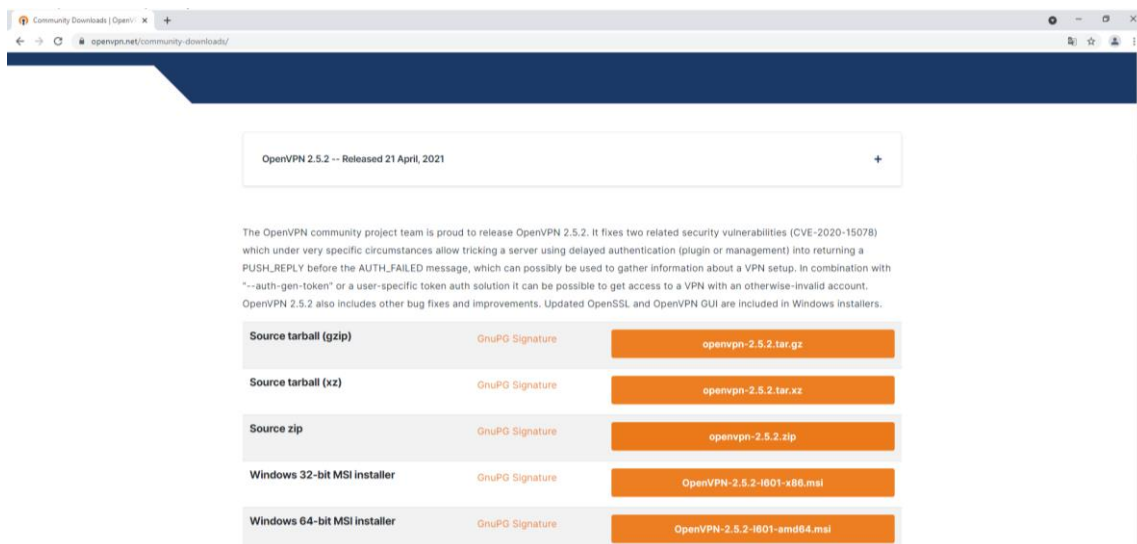
- El precio. Aunque hay servicios VPN gratuitos, obviamente no puedes esperar mucho de ellos, pues con frecuencia estarán muy limitados, serán muy lentos o no serán muy fiables.
- La velocidad. La diferencia entre conectarte a Internet directamente o que tus datos tracen una ruta que atraviesa medio mundo puede ser abrumadora. Si tu servidor VPN está muy lejos, experimentarás mucha latencia a la hora de navegar por la red. Además de latencia, es normal que la velocidad de descarga y subida máxima estén limitadas.
- Su seguridad no es infalible. Solo porque el icono de la conexión tenga un candado no quiere decir que la conexión sea segura, especialmente si estamos hablando de conexiones VPN basadas en el protocolo PPTP.
- No siempre pueden falsear tu ubicación. Especialmente en el móvil, cada vez hay más tecnologías por las cuales se puede triangular y aproximar tu ubicación más allá de tu dirección IP.
- No te proporcionan anonimato. Usar una VPN no supone que la navegación sea anónima.

2. Creación de la VPN

2.1 Instalación

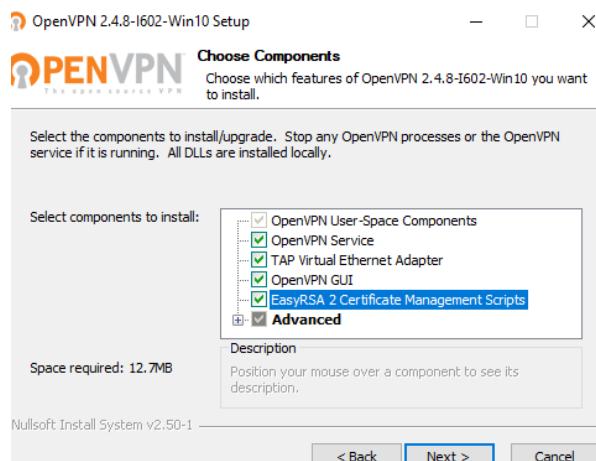
Lo primero será disponer de una máquina virtual o anfitrión con Windows 10. En nuestro caso estamos utilizando la versión de Windows 10 pro.

Una vez instalado Windows 10, procederemos a descargar el programa OpenVPN, el cual usaremos para crear nuestra VPN externa. Nosotros hemos elegido la versión para Windows de 64 bits, pero elegiremos la que mejor nos convenga para nuestro sistema operativo.



1. Descargando OpenVPN

Una vez descargada la versión que queremos vamos a instalar el programa. Dentro del instalador, seleccionamos los componentes llamados TAP y EasyRSA2, los cuales usaremos para nuestra VPN.

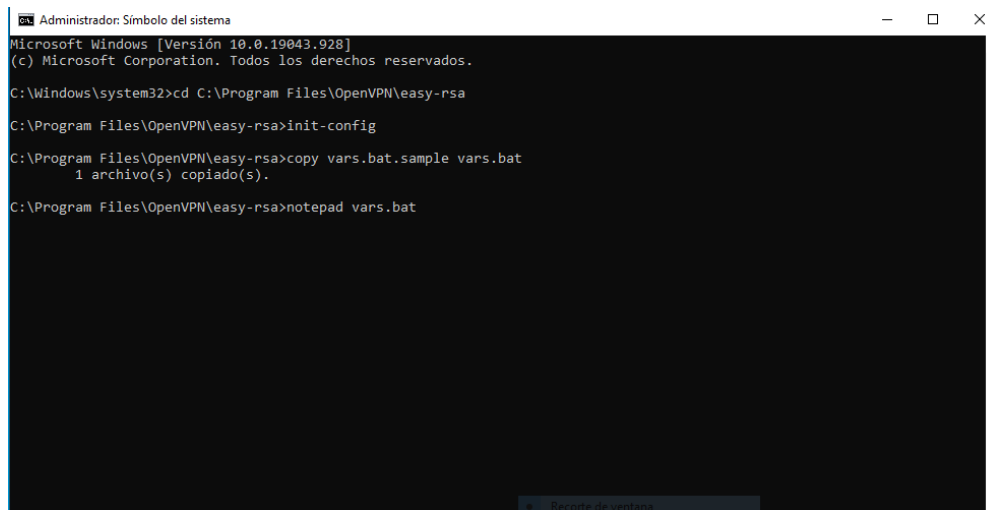


2. Instalación OpenVPN Componentes

2.2 Configuración

Instalado el programa, continuamos con la configuración del archivo vars.bat que será el encargado de suministrar la información para los certificados que vayamos a emitir. Este proceso lo haremos desde el intérprete de comandos, lo ejecutaremos como administrador para que no haya ningún problema a la hora de aplicar los comandos.

Nos situamos en la ruta easy-rsa dentro de la carpeta de instalación de OpenVPN, dentro usaremos el comando init-config para iniciar la configuración, después, copiaremos el fichero de ejemplo y le cambiaremos el nombre creando el archivo vars.bat



```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.19043.928]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>cd C:\Program Files\OpenVPN\easy-rsa
C:\Program Files\OpenVPN\easy-rsa>init-config
C:\Program Files\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
1 archivo(s) copiado(s).
C:\Program Files\OpenVPN\easy-rsa>notepad vars.bat
```

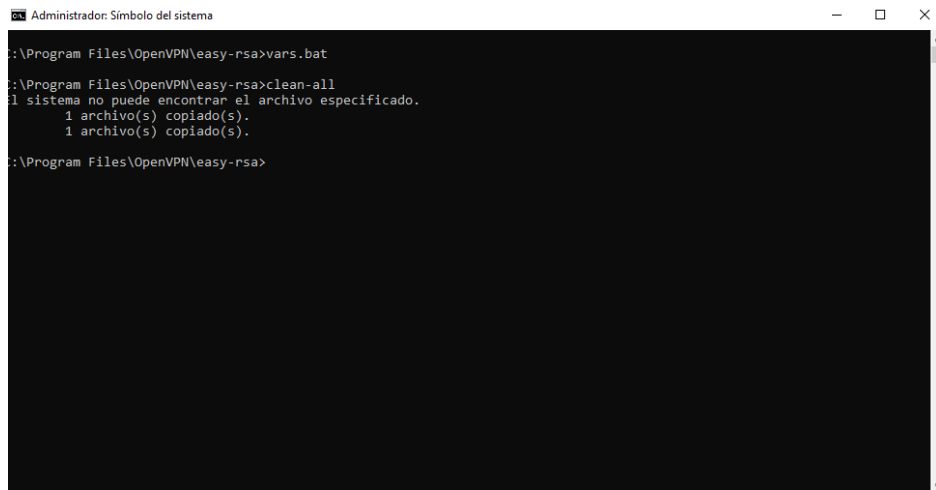
3. Cambiando directorio y creando archivo vars.bat

Dentro del archivo que previamente creamos, cambia las siguientes líneas por nuestros datos, estos serán los que se emitan junto a los certificados que después crearemos para acceder a la VPN. Hecho esto cierra y guarda el archivo.

```
set KEY_COUNTRY=ES
set KEY_PROVINCE=MA
set KEY_CITY=Alcorcon
set KEY_ORG=LockVPN
set KEY_EMAIL=mininombre@gmail.com
```

4. Cambiando datos archivo vars.

Una vez guardado el archivo, lo abrimos y ejecutamos un segundo archivo llamado clean-all

A screenshot of a Windows command prompt window titled "Administrador: Símbolo del sistema". The window has a black background with white text. The command prompt shows the following sequence of commands and output:

```
C:\Program Files\OpenVPN\easy-rsa>vars.bat
C:\Program Files\OpenVPN\easy-rsa>clean-all
1 sistema no puede encontrar el archivo especificado.
1 archivo(s) copiado(s).
1 archivo(s) copiado(s).
C:\Program Files\OpenVPN\easy-rsa>
```

5. Ejecutando archivo vars y clean-all.

2.2 Generando Certificados

Ahora se procede a crear los certificados del servidor que serán los que necesitaremos para poder conectarnos después a la VPN.

Volvemos al terminal y escribimos el comando `build-ca` con el que generaremos la autoridad certificadora con la que podremos emitir nuestros certificados. Nos aparecerán rellenados algunos campos con los datos que previamente agregamos, le damos a enter y nos fijaremos especialmente en el campo llamado Common name, aquí debemos poner el nombre de nuestro servidor VPN, es importante recordarlo para después.

Una vez hecho el certificado podemos crear las claves del servidor.

```
Administrador: Símbolo del sistema
C:\Program Files\OpenVPN\easy-rsa>build-ca
generating a RSA private key
.....++++
.....++++
writing new private key to 'keys/ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [ES]:
State or Province Name (full name) [MA]:
Locality Name (eg, city) [Alcorcon]:
Organization Name (eg, company) [LockVPN]:
Organizational Unit Name (eg, section) [changeme]:LockVPN-Trabajo
Common Name (eg, your name or your server's hostname) [changeme]:LockVPN-Server
Name [changeme]:Alvaro_Daniel
Email Address [mininombe@gmail.com]:

C:\Program Files\OpenVPN\easy-rsa>
```

6. Creando certificado CA.

Ahora escribimos el comando `build-key-server server` para crear las claves del servidor, el procedimiento es muy parecido al anterior, enter hasta que lleguemos al common name y escribiremos el nombre que pusimos antes para nuestro servidor. Al final nos saldrán dos preguntas para firmar y terminar la creación de las claves.

```
Administrador: Símbolo del sistema

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:LockVPN
Using configuration from openssl-1.0.0.cnf
Can't open keys/index.txt.attr for reading, No such file or directory
5168:error:02001002:system library:fopen:No such file or directory:crypto/bio/bss_file.c:74:fopen('keys/index.txt.attr',
'r')
5168:error:2006D080:BIO routines:BIO_new_file:no such file:crypto/bio/bss_file.c:81:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'ES'
stateOrProvinceName  :PRINTABLE:'MA'
localityName         :PRINTABLE:'Alcorcon'
organizationName     :PRINTABLE:'LockVPN'
organizationalUnitName:PRINTABLE:'LockVPN-Trabajo'
commonName           :PRINTABLE:'LockVPN-Server'
name                 :T61STRING:'Alvaro_Daniel'
emailAddress         :IASSTRING:'mininombe@gmail.com'
Certificate is to be certified until Jun  1 17:24:15 2031 GMT (3650 days)
Sign the certificate? [y/n]:y

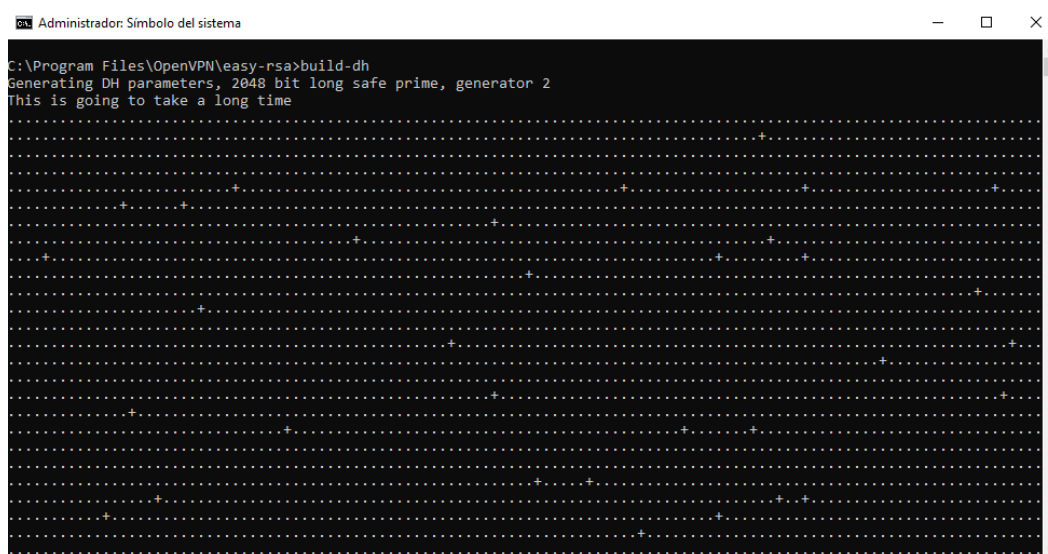
1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenVPN\easy-rsa>
```

7. Creación claves del servidor.

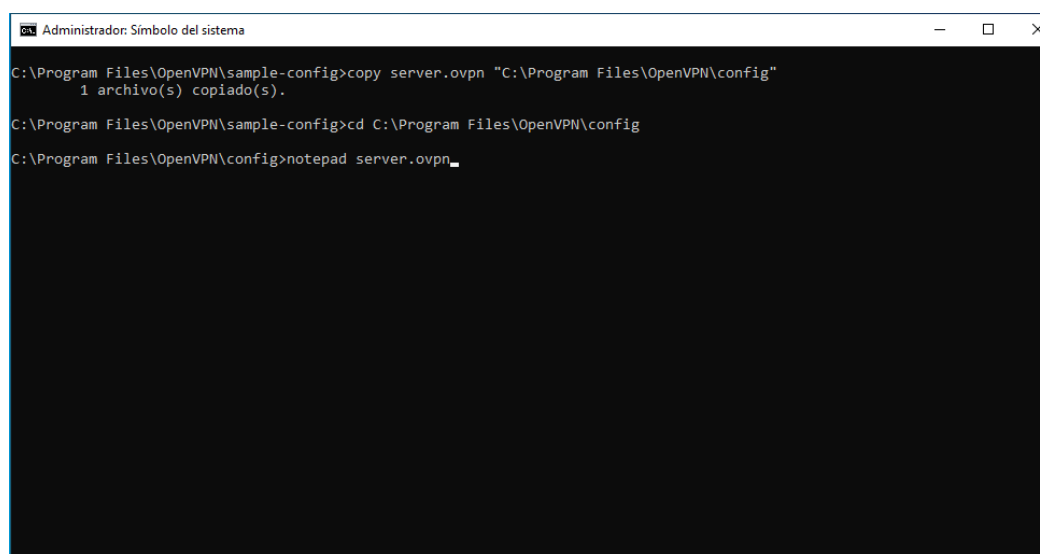
3. Configuración del servidor

Ahora encriptaremos los ficheros con el comando build-dh, tardará un tiempo dependiendo de nuestro ordenador.



8. Encriptación ficheros

Una vez encriptados los ficheros, copiaremos desde la carpeta sample-config que está ubicada en la carpeta de instalación de OpenVPN, el archivo server.ovpn a la carpeta config. Después de copiar el fichero, vamos a abrirlo con cualquier editor de texto. Lo que se pretende hacer es configurar nuestro servidor VPN implementando los parámetros correctos para que se pueda crear el servidor y conectar los clientes.



9. Copiando archivo server.ovpn

Dentro del archivo iremos al apartado donde podremos escoger el protocolo que vayamos a usar, para evitar problemas con el servidor nosotros usaremos el protocolo IPv4, el archivo debería quedar como la siguiente captura.

```
*server: Bloc de notas
Archivo Edición Formato Ver Ayuda
;local a.b.c.d

# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one. You will need to
# open up this port on your firewall.
port 1194

# TCP or UDP server?
;proto ucp
proto udp4
```

10. Eliendo protocolo.

Más abajo del archivo, podremos elegir el método de tunelización entre tap y tun, nosotros priorizaremos el método tap ya que admite mayor cantidad de protocolos.

```
38 # "dev tun" will create a routed IP tunnel,
39 # "dev tap" will create an ethernet tunnel.
40 # Use "dev tap0" if you are ethernet bridging
41 # and have precreated a tap0 virtual interface
42 # and bridged it with your ethernet interface.
43 # If you want to control access policies
44 # over the VPN, you must create firewall
45 # rules for the TUN/TAP interface.
46 # On non-Windows systems, you can give
47 # an explicit unit number, such as tun0.
48 # On Windows, use "dev-node" for this.
49 # On most systems, the VPN will not function
50 # unless you partially or fully disable
51 # the firewall for the TUN/TAP interface.
52 dev tap
53 #dev tun
54
55 # Windows needs the TAP-Win32 adapter name
56 # from the Network Connections panel if you
57 # have more than one. On XP SP2 or higher,
58 # you may need to selectively disable the
59 # Windows firewall for the TAP adapter.
60 # Non-Windows systems usually don't need this.
61 ;dev-node NtTap
62
63 # SSL/TLS root certificate (ca), certificate
```

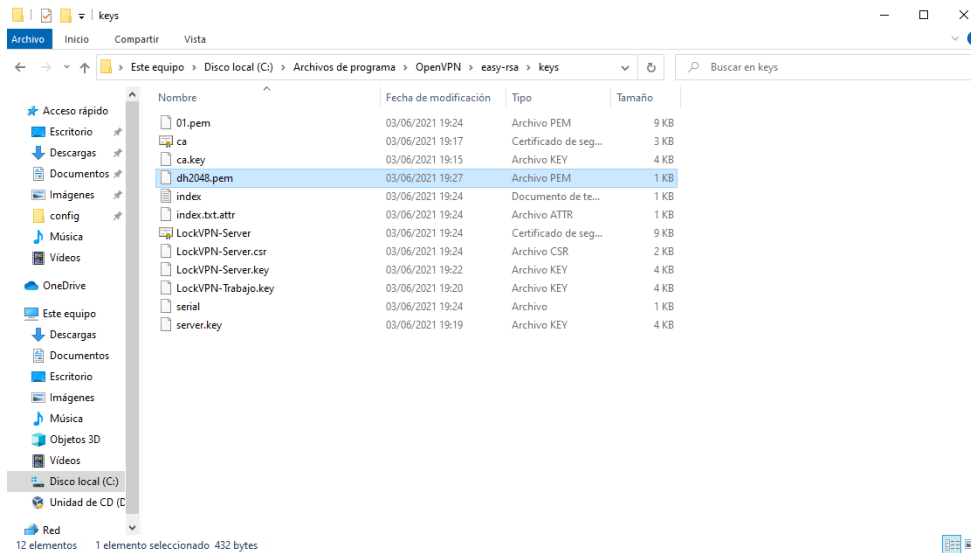
11. Eliendo método de tunelización.

Ahora debemos indicarle al servidor el directorio donde coger los certificados y las claves para conectar con el servidor en las siguientes líneas.

```
74 #
75 # Any X509 key management system can be used.
76 # OpenVPN can also use a PKCS #12 formatted key file
77 # (see "pkcs12" directive in man page).
78 ca "C:\Program Files\OpenVPN\config\ca.crt"
79 cert "C:\Program Files\OpenVPN\config\LockVPN-Server.crt"
80 key "C:\Program Files\OpenVPN\config\LockVPN-Server.key" # This file should be kept secret
81
82 # Diffie hellman parameters.
83 # Generate your own with:
84 # openssl dhparam -out dh2048.pem 2048
85 dh "C:\Program Files\OpenVPN\config\dh2048.pem"
86
87 # Network topology
88 # Should be subnet (addressing via IP)
89 # unless Windows clients v2.0.9 and lower have to
90 # be supported (then net30, i.e. a /30 per client)
91 # Defaults to net30 (not recommended)
92 ;topology subnet
93
```

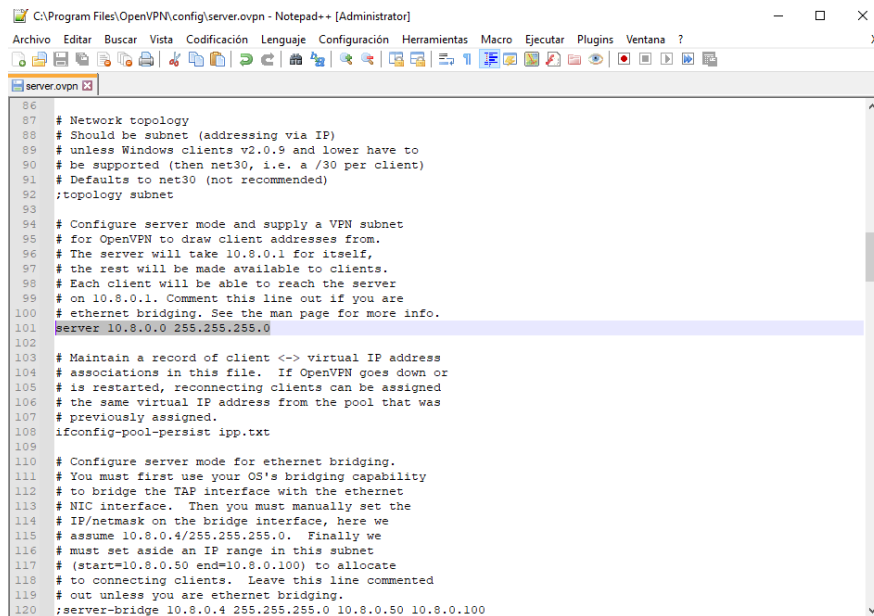
12. Indicando donde encontrar los certificados.

Antes de guardar, revisaremos si existe un fichero llamado dh2048pem o si se llama dh4096pem, en cuyo caso cambiaremos.



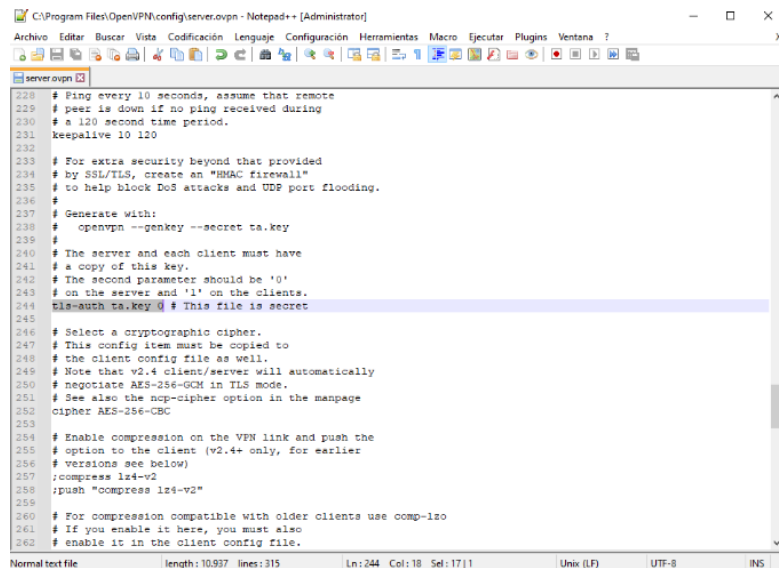
13. Revisando fichero dh2048.

Ahora modificaremos el campo de asignación de la dirección IP del servidor, podemos dejarla como estaba, pero también se puede cambiar si queremos asignar el servidor a otra IP.



14. Rango IP del servidor.

Por último, debemos tener el valor 0 y no el 1. Ya que el valor 0 se deja para el servidor y el 1 se deja para el fichero de configuración del cliente. Guardamos y cerramos el fichero. Si no nos deja lo guardaremos primero en otro lado y luego lo sustituiremos por el antiguo.

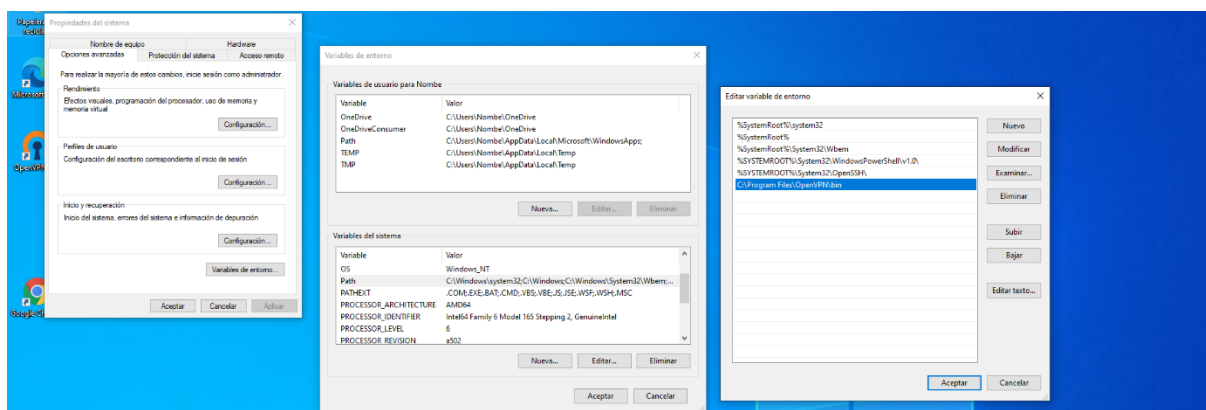


```

server.ovpn
228 # Ping every 10 seconds, assume that remote
229 # peer is down if no ping received during
230 # a 120 second time period.
231 keepalive 10 120
232
233 # For extra security beyond that provided
234 # by SSL/TLS, create an "HMAC firewall"
235 # to help block DoS attacks and UDP port flooding.
236 #
237 # Generate with:
238 #   openvpn --genkey --secret ta.key
239 #
240 # The server and each client must have
241 # a copy of this key.
242 # The second parameter should be '0'
243 # on the server and '1' on the clients.
244 tls-auth ta.key 0 # This file is secret
245
246 # Select a cryptographic cipher.
247 # This config item must be copied to
248 # the client's config file as well.
249 # Note that v2.4 client/server will automatically
250 # negotiate AES-256-GCM in TLS mode.
251 # See also the ncp-cipher option in the manpage
252 cipher AES-256-CBC
253
254 # Enable compression on the VPN link and push the
255 # option to the client (v2.4+ only, for earlier
256 # versions see below)
257 ;compress lz4-v2
258 ;push "compress lz4-v2"
259
260 # For compression compatible with older clients use comp-lzo
261 # If you enable it here, you must also
262 # enable it in the client config file.
  
```

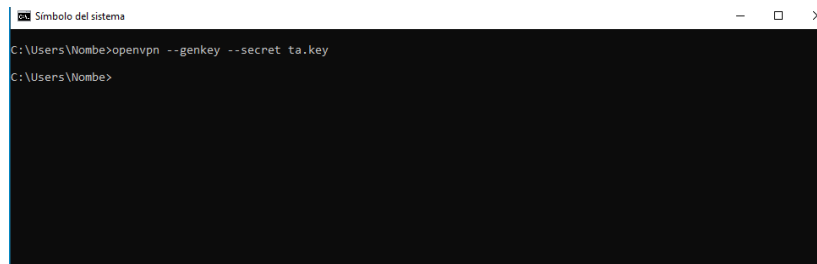
15. Comprobando campo `tls-auth ta.key`

Una vez guardado el anterior fichero, entraremos en las variables de entorno del sistema y modificaremos el path de Windows donde se añadirá la carpeta bin.



16. Editando Path de Windows.

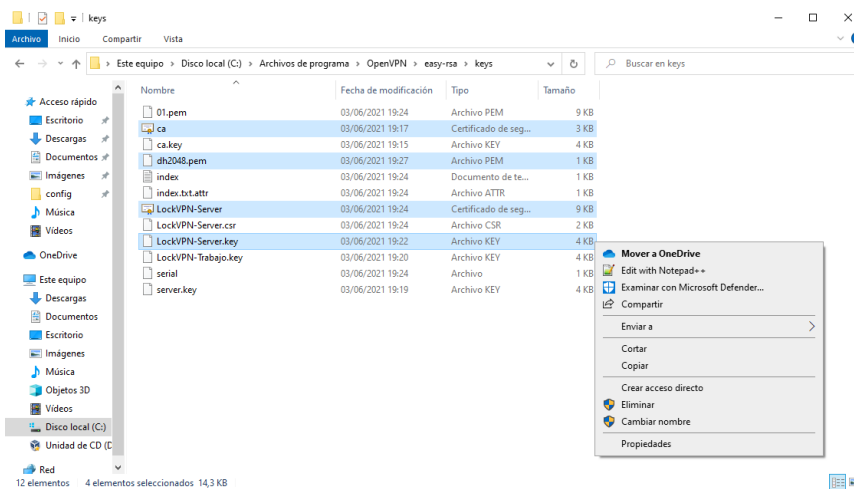
Una vez editado y guardado el path, nos iremos al cmd y ejecutaremos el siguiente comando con el cual vamos a generar la última clave necesaria para el servidor.



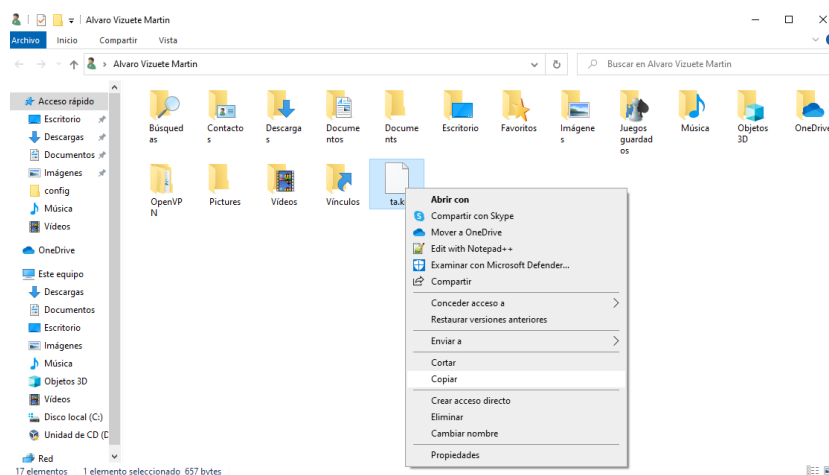
17. Generando última clave servidor.

Ahora buscaremos las diferentes claves generadas para el servidor, normalmente se encuentran en los directorios OpenVPN\easy-rsa\keys o directamente en easy-rsa\.

El archivo ta.key lo encontraremos desde el buscador de Windows para ubicarlo más fácilmente. Copiamos todos estos archivos a la carpeta config.



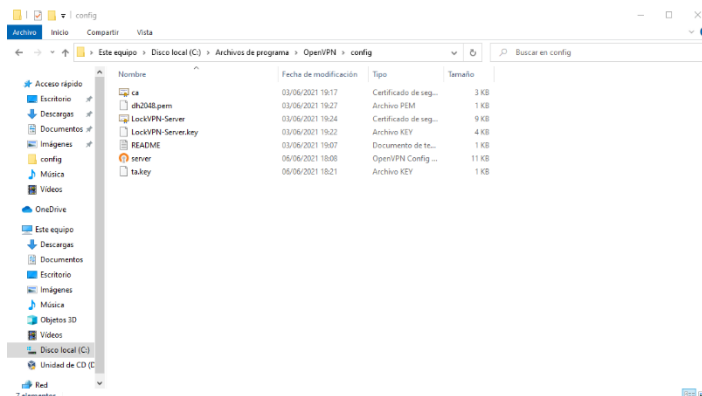
18. Copiando claves servidor.



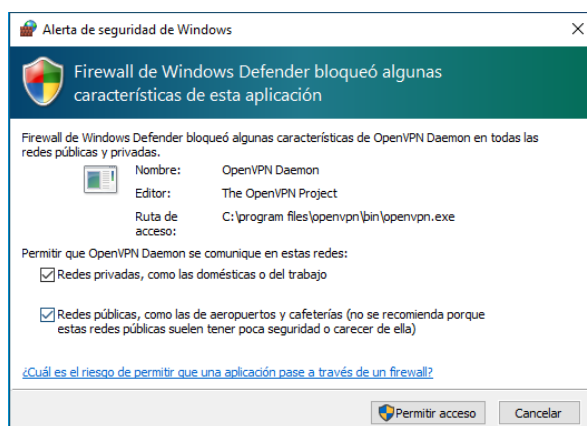
19. Copiando archivo ta.key.

Cuando hayamos terminado de copiar todas las claves a la carpeta config ejecutaremos el programa, ya sea desde su acceso directo en el escritorio o si no desde el buscador de Windows.

Cuando lo iniciemos por primera vez le otorgaremos permisos de redes privadas en el firewall y si pensamos usarlo de forma remota como en nuestro caso también le permitiremos las redes públicas.

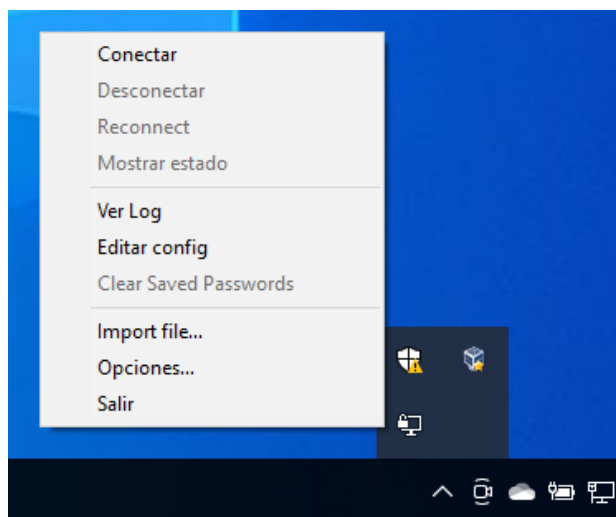


20. Copiadas las claves en la carpeta config.



21. Permitiendo conexiones Firewall.

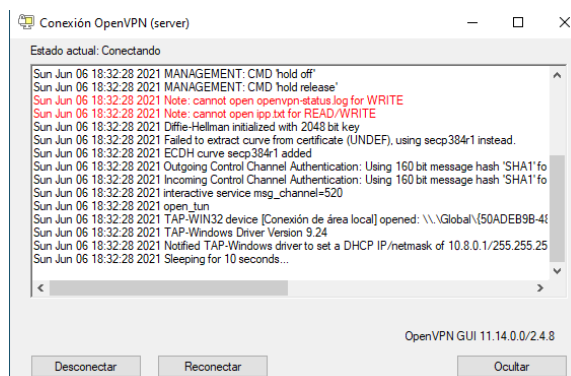
Una vez hayamos aceptado los permisos del Firewall nos debe aparecer en la barra de tareas el siguiente icono. Con el clic derecho nos dejara la opción de conectarnos, lo probamos para ver si funciona, aunque sea en local.



22. Conectándose desde la barra de tareas.

Cuando hagamos clic en conectar nos aparecerá esta pantalla con la que nos demuestra que se está conectando con el servidor y asignando la nueva IP.

Terminado el proceso la ventana se cerrará y nos saldrá una notificación con nuestra nueva IP.

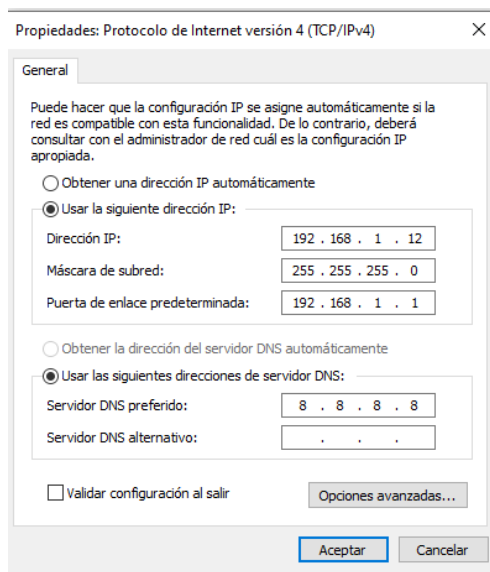


23. Interfaz conectando al servidor.



24. Conexión lograda nueva IP.

Ahora configuraremos el servidor para que nos deje acceder desde cualquier ordenador siempre y cuando tenga certificados válidos para el servidor. Para empezar y facilitar las cosas estableceremos en una IP fija dentro de la red.



25. Estableciendo IP fija.

Establecida la IP fija, para podernos conectar a nuestro servidor VPN desde cualquier sitio, debemos entrar en la configuración router y abrir el puerto que usa OpenVPN, concretamente el puerto 1194 UDP, además hay activar el reenvío de puertos si nuestro ordenador no lo tiene activado.

Con esto ya podremos conectarnos desde el exterior a nuestra VPN.

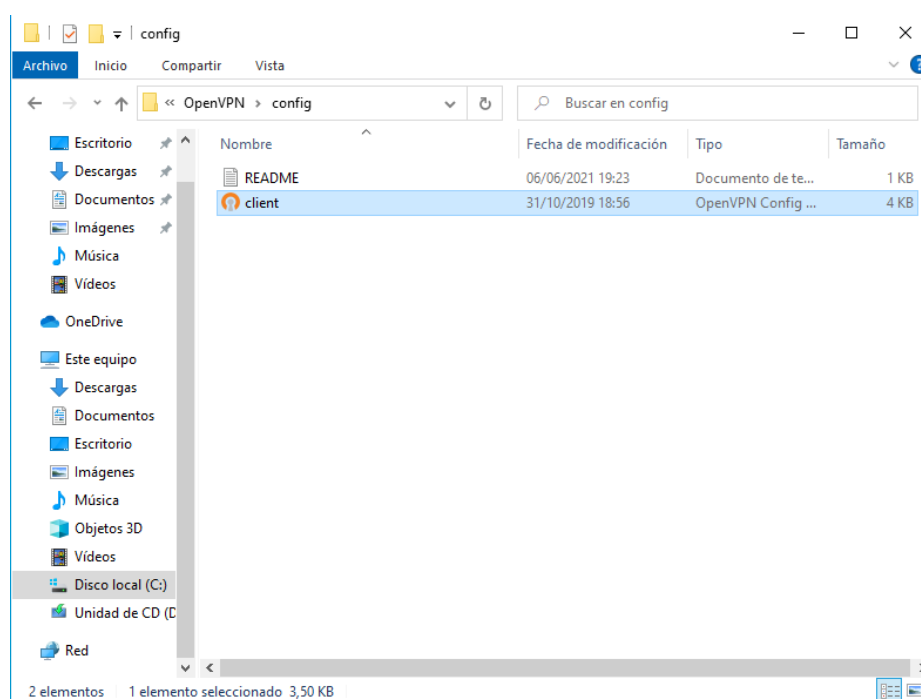
Personalizar reglas						
estado	aplicación / servicio	puerto interno	puerto externo	protocolo	IPv4 del dispositivo	
	FTP Server ▼	21	21	TCP ▼		<button>añadir</button>
✓	SSL	1194	1194	UDP	192.168.1.12	<button>delete</button>

26. Activando Reenvío de puertos y creando regla.

4. Prueba de funcionamiento en Windows

Cuando hayamos terminado de hacer todos los pasos anteriores, para probar la conexión del cliente podemos pedirle a alguien que nos ayude o podemos hacerlo en otra máquina.

Lo ideal sería que alguien de la red externa nos ayudara para ver su eficacia al 100%. Ahora bien, para el cliente, instalaremos los mismos componentes que instalamos en el servidor y copiaremos el archivo cliente de la carpeta sample-config, como hicimos antes con el servidor en la carpeta config.



27. Copiando cliente a carpeta config

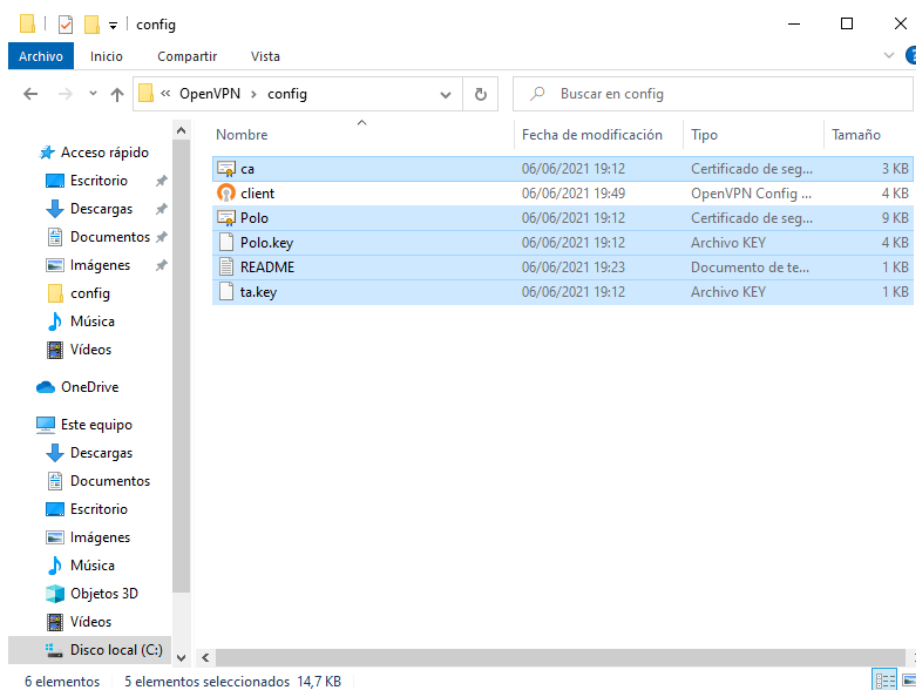
Volvemos al servidor y de nuevo abrimos el cmd como administrador. Una vez dentro, nos situaremos en la carpeta easy-rsa y ejecutamos el comando vars y build-key más el nombre del cliente que queramos.

Rellenamos todos los datos hasta que lleguemos al campo de Common Name, donde podremos con el nombre de usuario al que creamos el certificado.

```
Administrador: Símbolo del sistema - build-key Polo
C:\Windows\system32>cd C:\Program Files\OpenVPN\easy-rsa
C:\Program Files\OpenVPN\easy-rsa>vars
C:\Program Files\OpenVPN\easy-rsa>build-key Polo
Generating a RSA private key
.....++++
writing new private key to 'keys\Polo.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [ES]:
```

28. Creando certificado para el cliente.

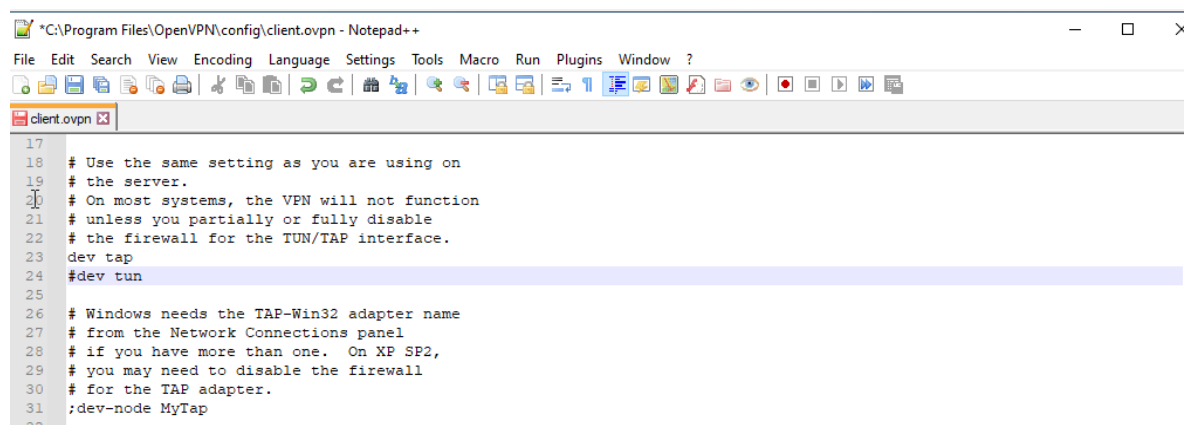
Hecho esto copiaremos estos certificados además de los correspondientes a la CA. Estos 4 archivos debemos colocarlos en la carpeta config como se hizo en pasos previos.



29. Certificados para el cliente.

Una vez hayamos copiado y colocado los certificados al equipo cliente en su sitio, empezaremos con su configuración.

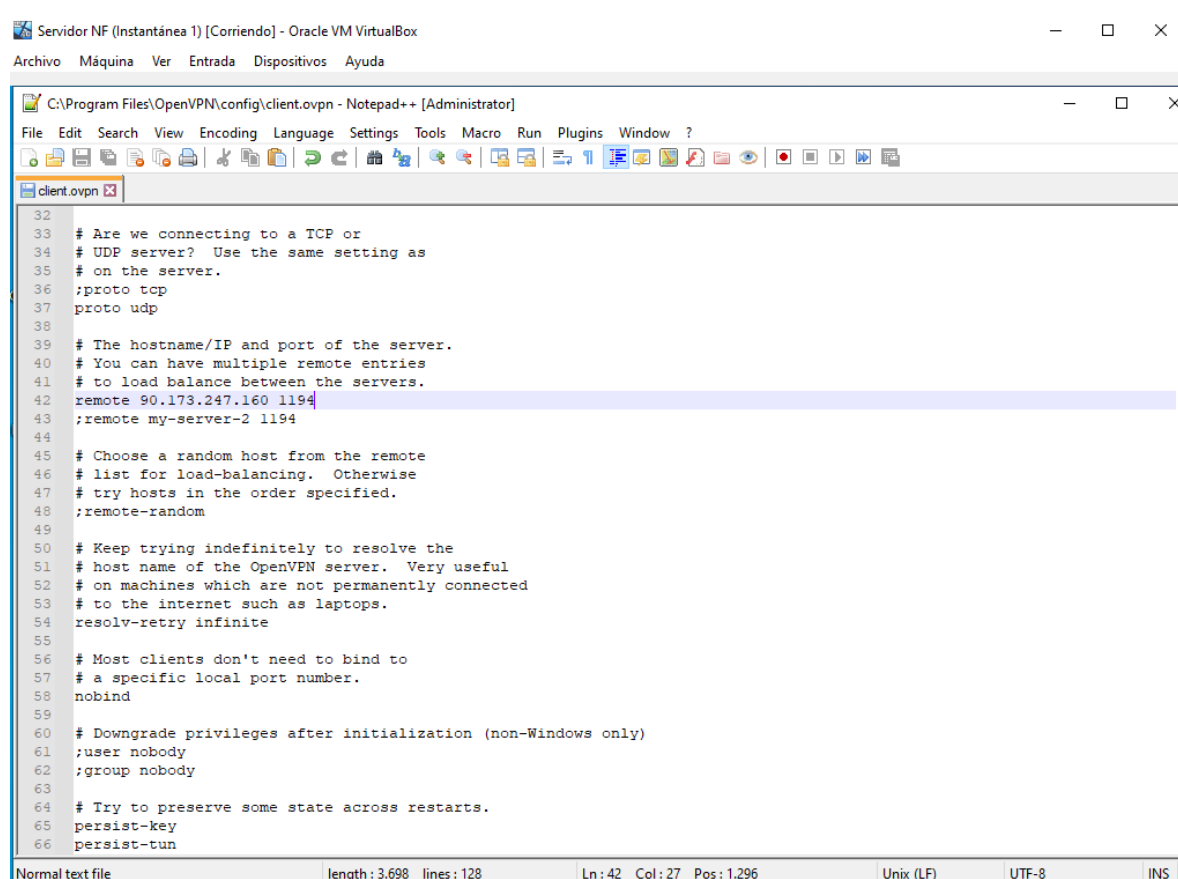
Entraremos al archivo cliente, en el cual tendremos que especificar que queremos usar el método tap como ya hicimos en el servidor.



```
17
18 # Use the same setting as you are using on
19 # the server.
20 # On most systems, the VPN will not function
21 # unless you partially or fully disable
22 # the firewall for the TUN/TAP interface.
23 dev tap
24 dev tap
25
26 # Windows needs the TAP-Win32 adapter name
27 # from the Network Connections panel
28 # if you have more than one. On XP SP2,
29 # you may need to disable the firewall
30 # for the TAP adapter.
31 ;dev-node MyTap
32
```

30. Cambiando método tunelización cliente.

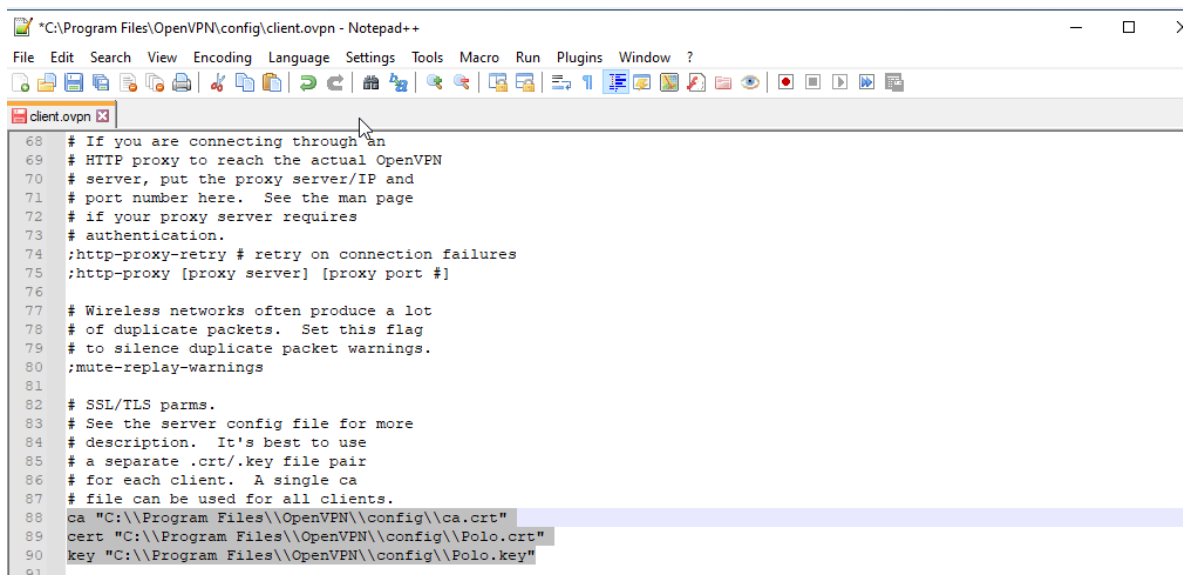
Más abajo del archivo deberemos especificar la IP donde está el servidor, poniendo la IP pública debería dejarnos conectar a nuestro servidor desde fuera, siempre y cuando hayamos hecho todo el proceso de reenvío de puertos.



```
32
33 # Are we connecting to a TCP or
34 # UDP server? Use the same setting as
35 # on the server.
36 ;proto tcp
37 proto udp
38
39 # The hostname/IP and port of the server.
40 # You can have multiple remote entries
41 # to load balance between the servers.
42 remote 90.173.247.160 1194
43 ;remote my-server-2 1194
44
45 # Choose a random host from the remote
46 # list for load-balancing. Otherwise
47 # try hosts in the order specified.
48 ;remote-random
49
50 # Keep trying indefinitely to resolve the
51 # host name of the OpenVPN server. Very useful
52 # on machines which are not permanently connected
53 # to the internet such as laptops.
54 resolv-retry infinite
55
56 # Most clients don't need to bind to
57 # a specific local port number.
58 nobind
59
60 # Downgrade privileges after initialization (non-Windows only)
61 ;user nobody
62 ;group nobody
63
64 # Try to preserve some state across restarts.
65 persist-key
66 persist-tun
```

31. Cambiando IP donde se encuentra el servidor.

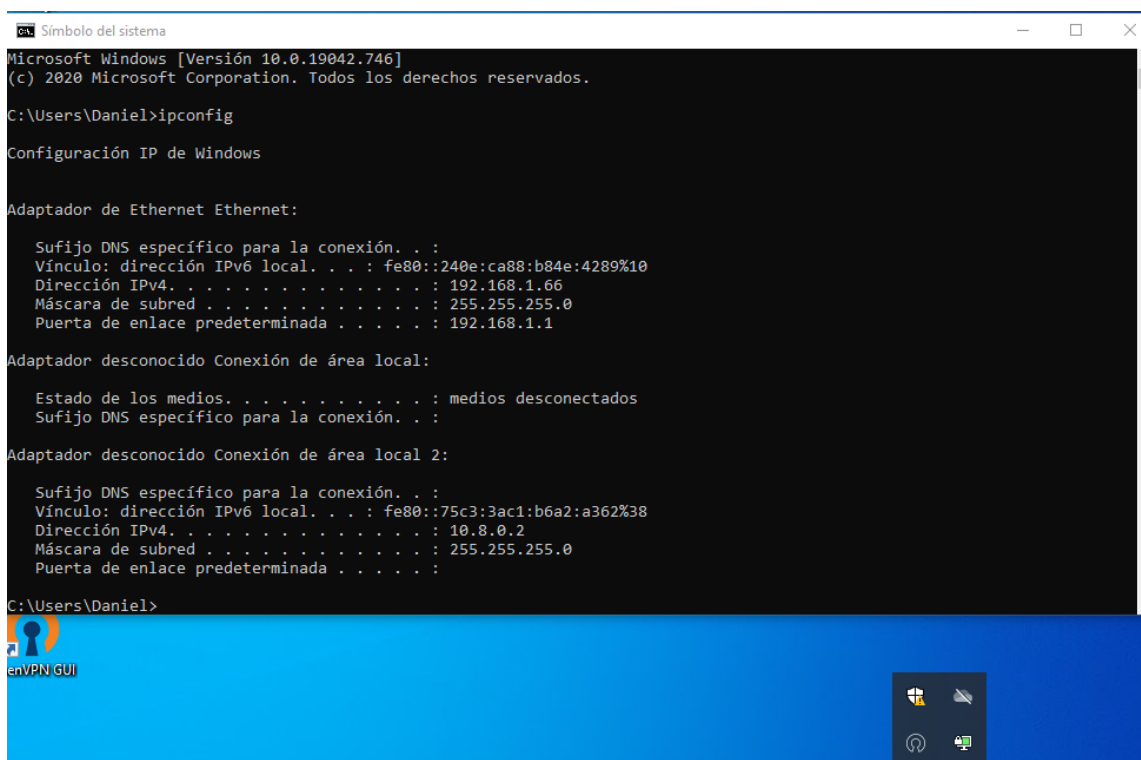
En el archivo, debemos especificar donde están localizados los certificados para que se puedan encontrar y verificar a la hora de acceder al servidor.



```
*C:\Program Files\OpenVPN\config\client.ovpn - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
client.ovpn
68 # If you are connecting through an
69 # HTTP proxy to reach the actual OpenVPN
70 # server, put the proxy server/IP and
71 # port number here. See the man page
72 # if your proxy server requires
73 # authentication.
74 ;http-proxy-retry # retry on connection failures
75 ;http-proxy [proxy server] [proxy port #]
76
77 # Wireless networks often produce a lot
78 # of duplicate packets. Set this flag
79 # to silence duplicate packet warnings.
80 ;mute-replay-warnings
81
82 # SSL/TLS parms.
83 # See the server config file for more
84 # description. It's best to use
85 # a separate .crt/.key file pair
86 # for each client. A single ca
87 # file can be used for all clients.
88 ca "C:\Program Files\OpenVPN\config\ca.crt"
89 cert "C:\Program Files\OpenVPN\config\Polo.crt"
90 key "C:\Program Files\OpenVPN\config\Polo.key"
91
```

32. Cambiando localización certificados cliente.

Guardado y cerrado el archivo ejecutaremos OpenSSL, y nos conectaremos como lo hicimos antes desde la barra de tareas. Cuando nos hayamos conectado nos asignará una IP del rango del servidor y ya estaríamos dentro de nuestra VPN.



```
Microsoft Windows [Versión 10.0.19042.746]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Daniel>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::240e:ca88:b84e:4289%10
    Dirección IPv4. . . . . : 192.168.1.66
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.1.1

Adaptador desconocido Conexión de área local:

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

Adaptador desconocido Conexión de área local 2:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::75c3:3ac1:b6a2:a362%38
    Dirección IPv4. . . . . : 10.8.0.2
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . :

C:\Users\Daniel>
```

33. Comprobación cambio de IP.

5. Bibliografía

<https://www.xataka.com/basics/que-es-una-conexion-vpn-para-que-sirve-y-que-ventajas-tiene>

<https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion>

<https://www.profesionalreview.com/2020/04/18/crear-vpn-openvpn-windows/>