

Práctica de Aula 3.4 – OpenVPN



Introducción

Para realizar la actividad vamos a necesitar 2 maquinas windows 10 (Un servidor y un cliente) donde instalaremos un servidor VPN.

Estas maquinas deberán estar configuradas en 2 redes completamente diferentes para que la IP que pase el VPN sea diferente a la del cliente.

Ademas de conectar el servidor como adaptador puente y el cliente como NAT, para que la NAT genere una red virtual distinta a la del servidor y permita la conexión y el servidor estará como un host mas de nuestra red original.

-Cliente:

```
VPN_cliente [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.3448]
(c) Microsoft Corporation. All rights reserved.

C:\Users\alumno>ipconfig

Windows IP Configuration

Unknown adapter OpenVPN Wintun:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::a1ad:901a:eb2d:3872%15
IPv4 Address. . . . . : 192.168.1.4
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

-Servidor:

```
VPN_servidor [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

C:\Windows\system32\cmd.exe
Windows IP Configuration

Unknown adapter OpenVPN Wintun:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

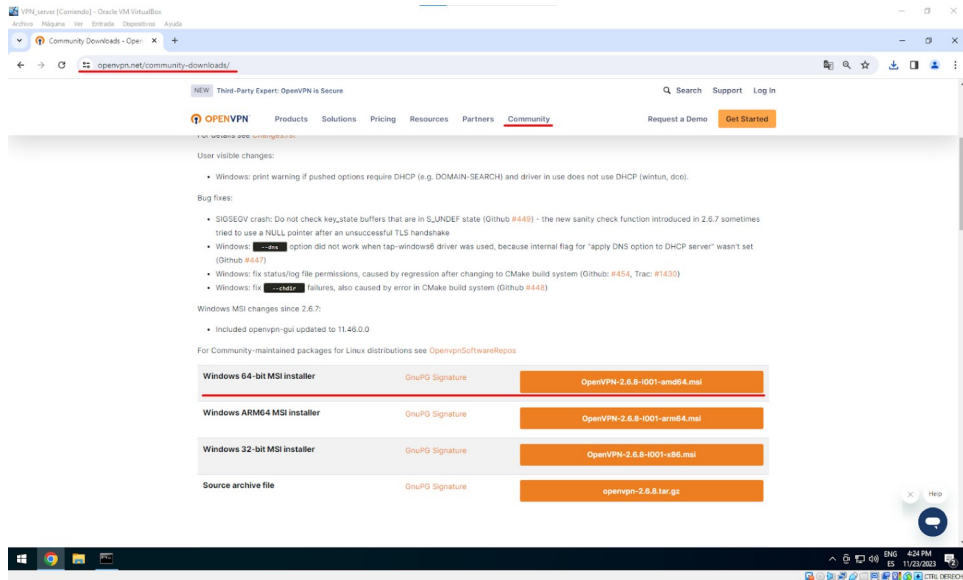
Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : DOMDPTOINF3MPP.INF
Link-local IPv6 Address . . . . . : fe80::a1ad:901a:eb2d:3872%14
IPv4 Address. . . . . : 192.168.52.168
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.52.1
```

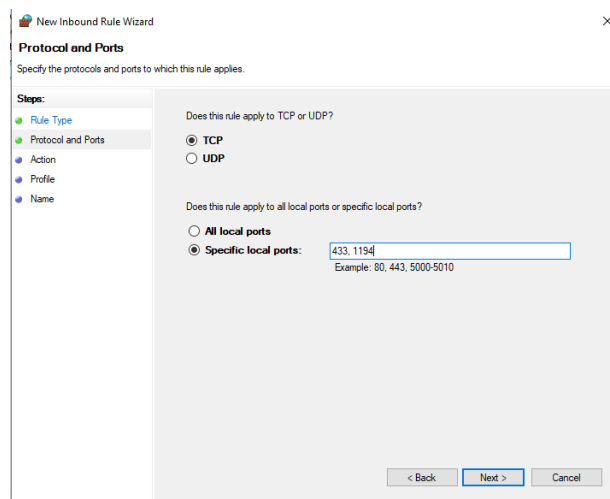
1. Descarga e instalación

Empezamos con la instalación de OpenVPN que es un software libre que no ayudara a crear una VPN a la que podremos acceder de forma remota desde nuestro cliente usando los certificados que nos proporciona.

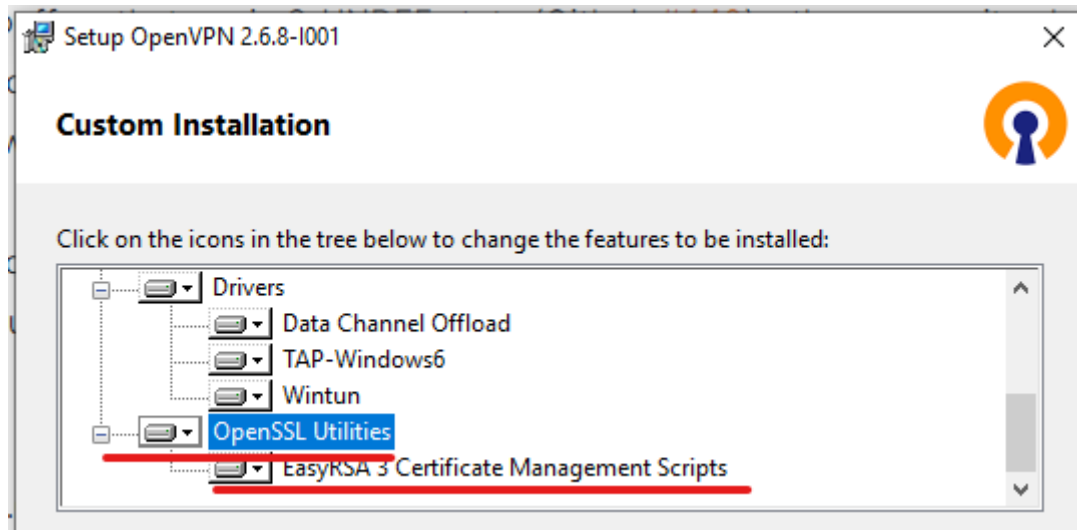
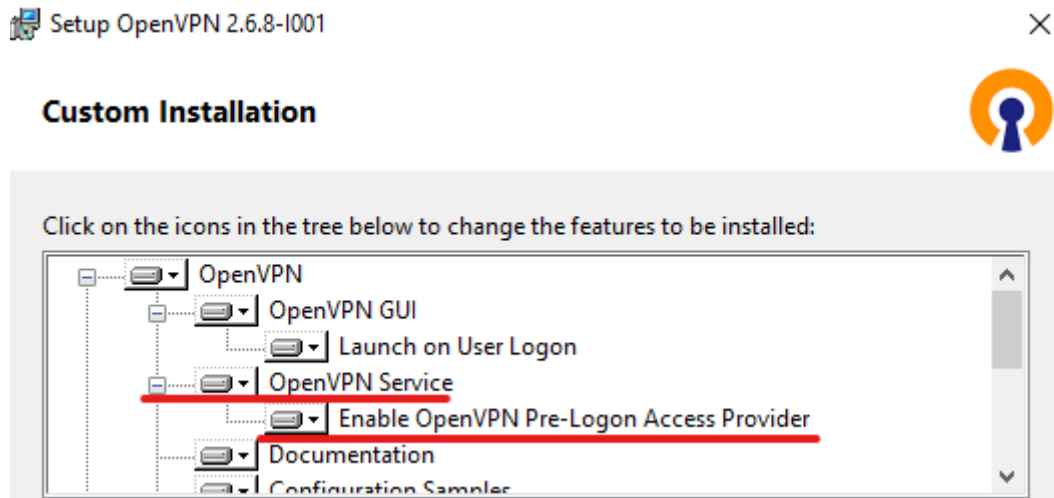
Entramos a la pagina oficial de OpenVPN y descargamos el archivo de instalación.



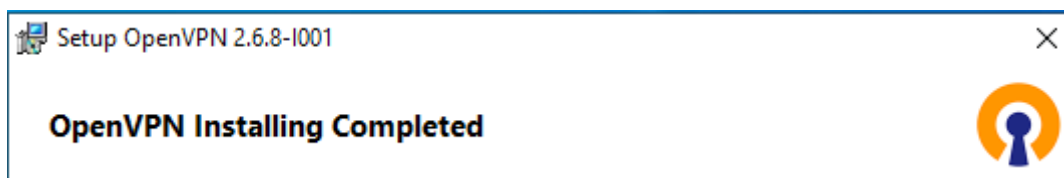
Para que OpenVPN pueda dar servicios TCP y UDP deberemos abrir los puertos 443 y 1194 desde la configuración del firewall de nuestro equipo nuestro equipo servidor.



Activamos las opciones remarcadas en las imagenes para que el encriptado funcione correctamente



Ahora ejecutaremos la instalación del OpenVPN hasta que nos salga esta pantalla.



2. Creación de los certificados

ENCRIPTADO:

Ejecutamos el comando “easysrsa init-pki” para que nos genere la carpeta pki

```
Welcome to the EasyRSA 3 Shell for Windows.
Easy-RSA 3 is available under a GNU GPLv2 license.

Invoke './easysrsa' to call the program. Without commands, help is displayed.

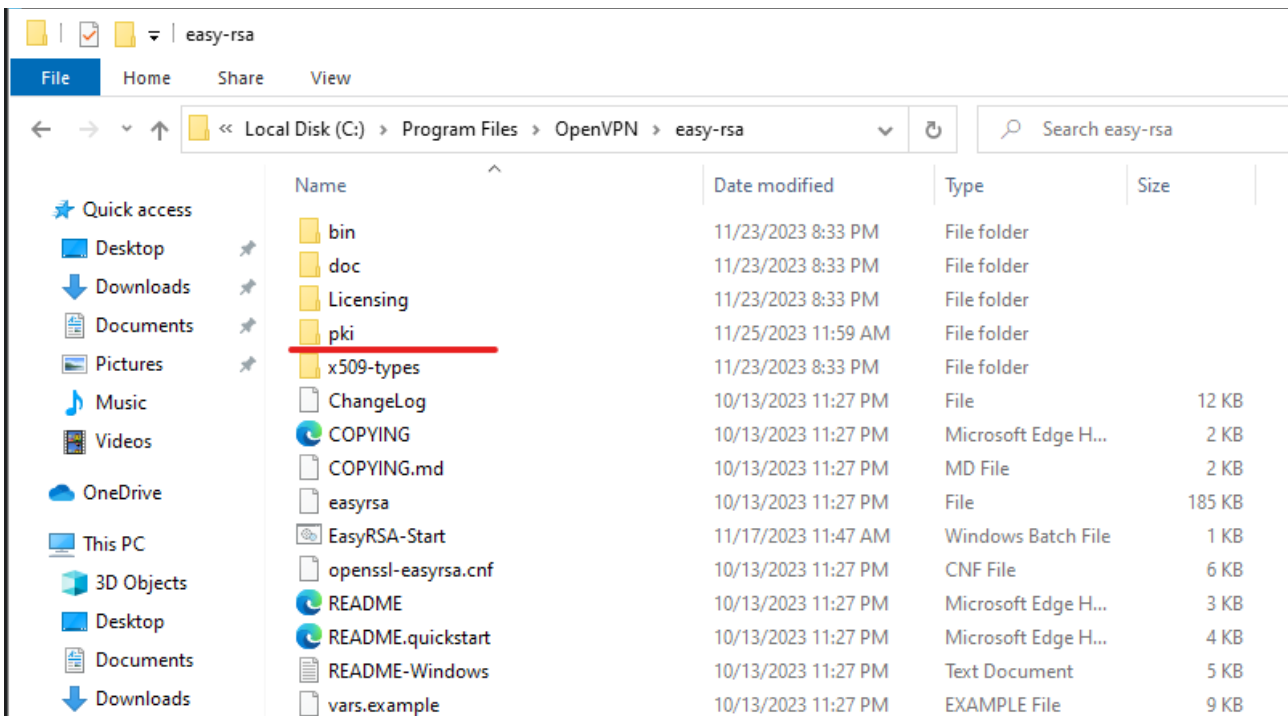
EasyRSA Shell
# easysrsa init-pki

Notice
-----
'init-pki' complete; you may now create a CA or requests.

Your newly created PKI dir is:
* C:/Program Files/OpenVPN/easy-rsa/pki

Using Easy-RSA configuration:
* undefined

EasyRSA Shell
#
```



Introducido el comando al final de este indicamos el nombre del servidor el cual es VPN_server, a continuación nos pedira introducir una contraseña que sera la que nos pedira openvpn al querer usar estos certificados.

```
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
Notice
-----
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: C:/Program Files/OpenVPN/easy-rsa/pki/reqs/VPN_server.req
* key: C:/Program Files/OpenVPN/easy-rsa/pki/private/VPN_server.key

You are about to sign the following certificate:
Request subject, to be signed as a server certificate
for '825' days:

subject=
  commonName                = VPN_server

Type the word 'yes' to continue, or any other input to abort.
Confirm request details:
```

Ahora nos pedira si queremos continuar introduciendo la palabra yes, y este nos pedira la clave certificadora que creamos al principio junto a las carpetas, una vez introducida nos dira que se han generado dos certificados y que estos tiene un tiempo de expiracion que en nuestro caso es el 27 de febrero.

```
Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes

Using configuration from C:/Program Files/OpenVPN/easy-rsa/pki/openssl-easyrsa.cnf
Enter pass phrase for C:/Program Files/OpenVPN/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName          :ASN.1 12:'VPN_server'
Certificate is to be certified until Feb 27 11:29:40 2026 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
-----
Certificate created at:
* C:/Program Files/OpenVPN/easy-rsa/pki/issued/VPN_server.crt

Notice
-----
Inline file created:
* C:/Program Files/OpenVPN/easy-rsa/pki/inline/VPN_server.inline

EasyRSA Shell
#
```


Y al igual que en la configuración del server se generaran los archivos de los certificados para el cliente y un tiempo de expiración

```
Enter pass phrase for C:/Program Files/OpenVPN/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName      :ASN.1 12:'VPN_client'
Certificate is to be certified until Feb 27 11:55:34 2026 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
-----
Certificate created at:
* C:/Program Files/OpenVPN/easy-rsa/pki/issued/VPN_client.crt

Notice
-----
Inline file created:
* C:/Program Files/OpenVPN/easy-rsa/pki/inline/VPN_client.inline

EasyRSA Shell
```

Ahora generaremos el archivo **Diffie-Hellman** el cual se encarga de cifrar la clave secreta por internet de forma segura basándose en las propiedades de la exponenciación modular, la cual transforma la contraseña en una formula matemática donde cada parte (cliente y servidor tiene un numero para resolver la formula).

```
EasyRSA Shell
# easyrsa gen-dh
No Easy-RSA 'vars' configuration file exists!

Using SSL:
* openssl OpenSSL 3.1.4 24 Oct 2023 (Library: OpenSSL 3.1.4 24 Oct 2023)
Generating DH parameters, 2048 bit long safe prime
```

Aqui se demuestra que se creo el archivo correctamente

```
DH parameters appear to be ok.

Notice
-----

DH parameters of size 2048 created at:
* C:/Program Files/OpenVPN/easy-rsa/pki/dh.pem

EasyRSA Shell
```

Ahora salimos del .bat y nos dirigimos a la carpeta bin que se encuentra en openvpn, para generar en ella la clave secreta que permitirá conectar el cliente al server con el certificado

```
EasyRSA Shell
# exit

C:\Program Files\OpenVPN\easy-rsa>cd ..

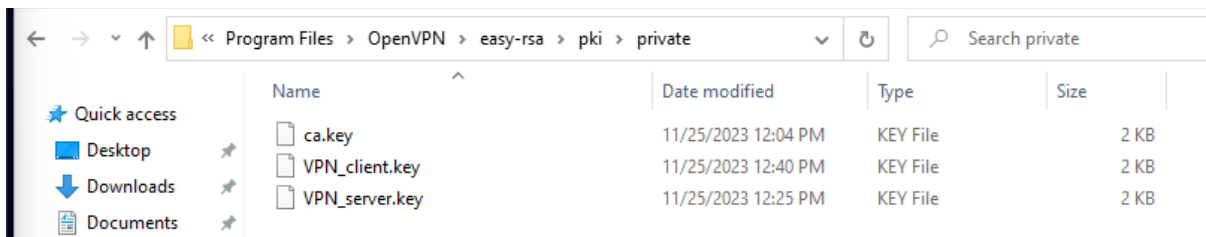
C:\Program Files\OpenVPN>cd bin

C:\Program Files\OpenVPN\bin>openvpn --genkey secret ta.key

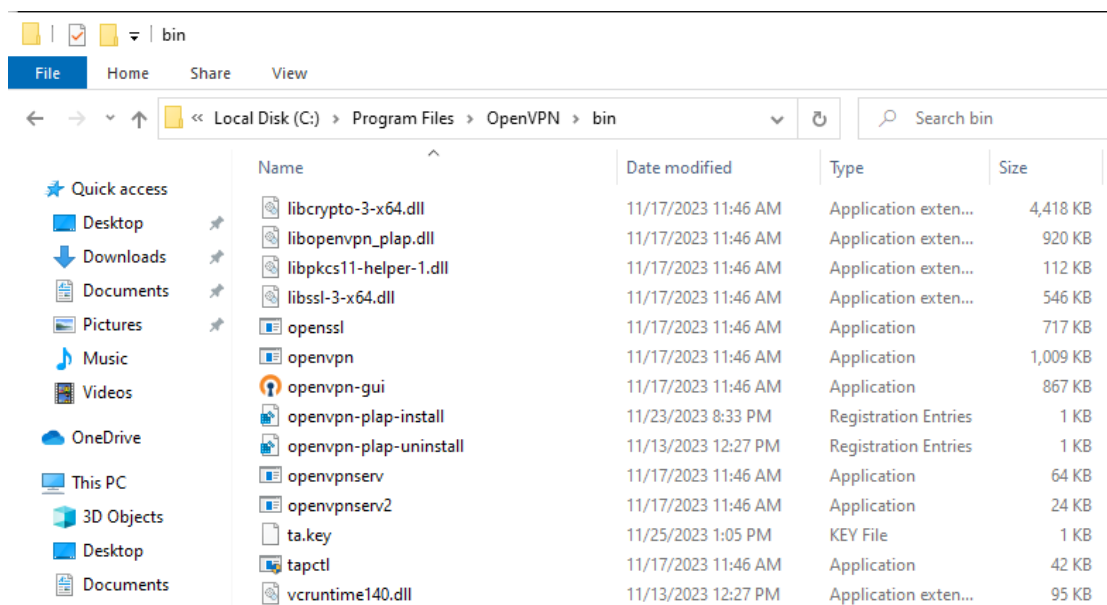
C:\Program Files\OpenVPN\bin>
```

Prueba de correcto funcionamiento mostrando los archivos creados:

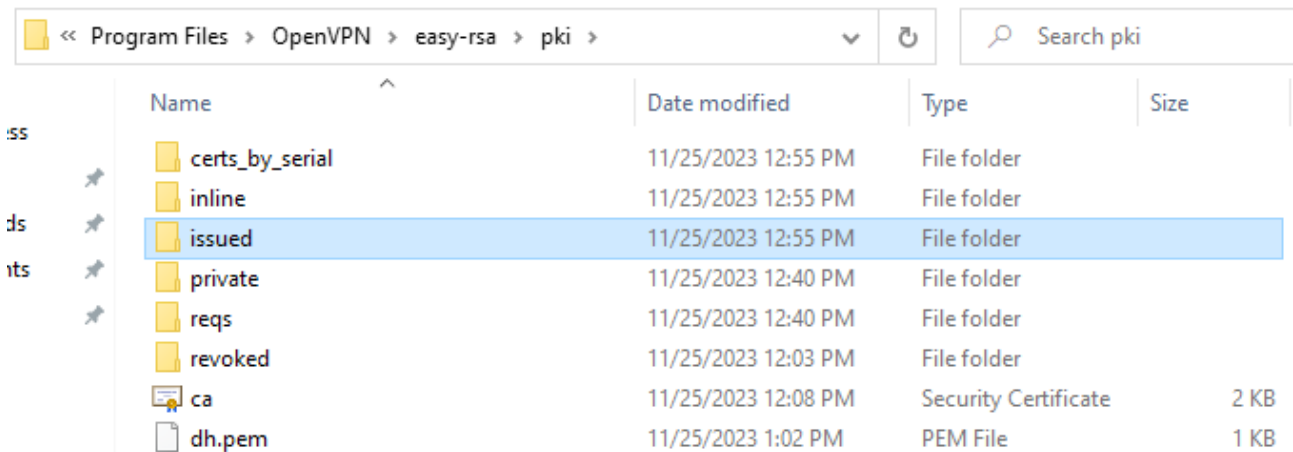
1°



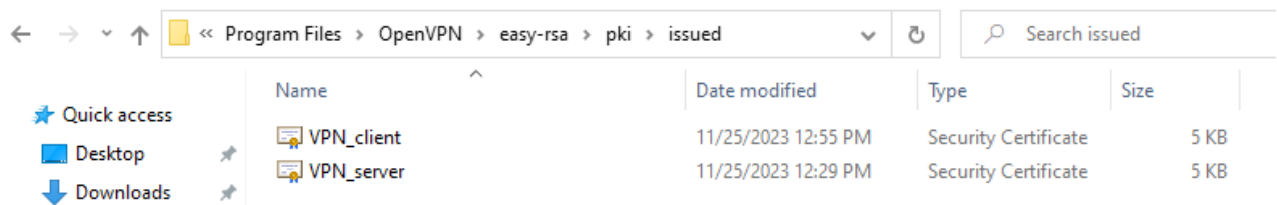
2°



3°

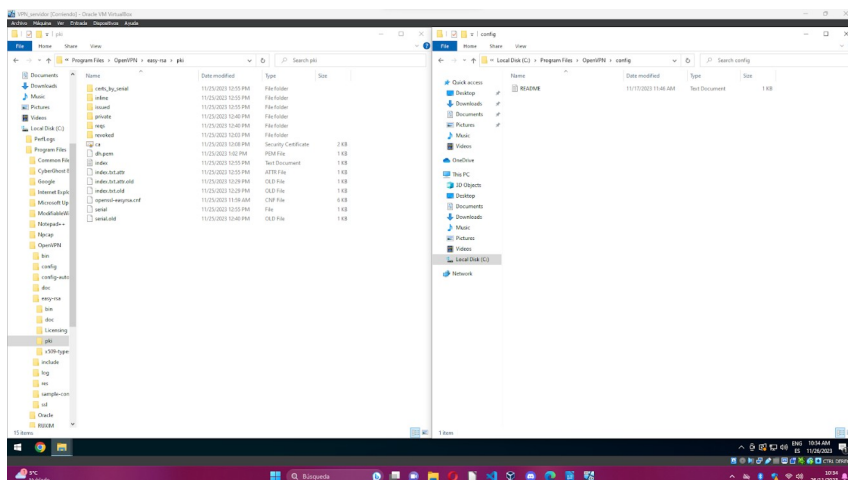


4°

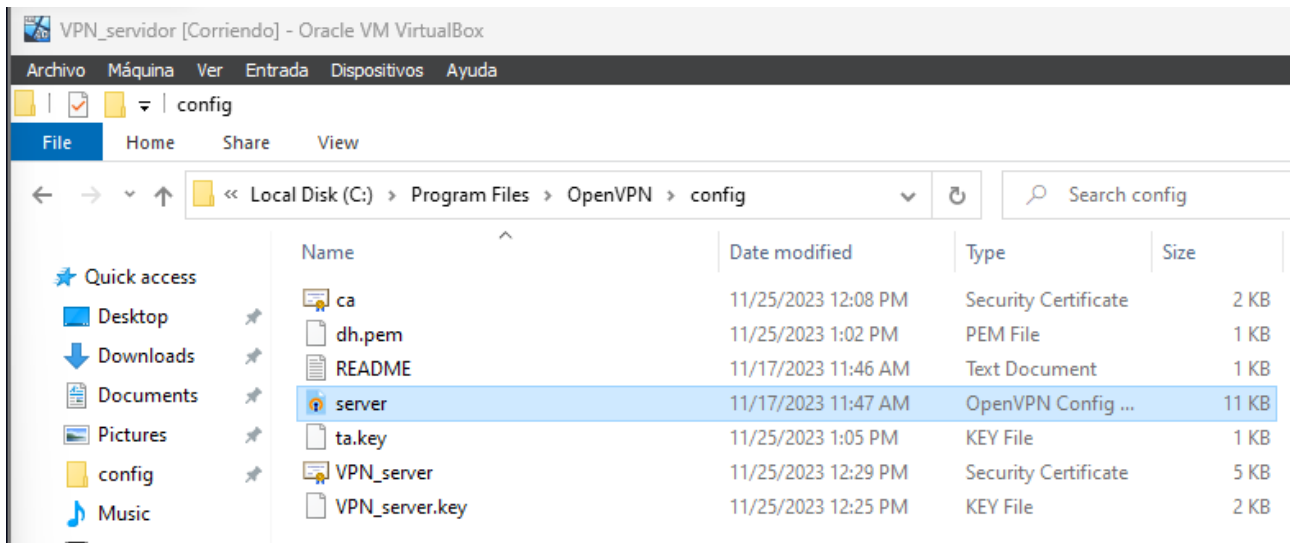


3. Configuración del servidor

Para poder configurar OpenVPN tendremos que pasar varios de los archivos creados anteriormente a la carpeta de configuración de openvpn



Después de pasar todos los archivos necesarios la configuración debe quedarte de la siguiente manera. Recordando que es copiar no mover los archivos.



Ahora modificaremos el contenido del archivo servers el cual solo quitaremos el “;” al dev tap, dándole la prioridad para que así genere una red virtual por ethernet tunelada. Y colocaremos al dev tun el “;” para dejarlo en segundo plano.

```
*server - Notepad
File Edit Format View Help
# TCP or UDP server?
;proto tcp
proto udp

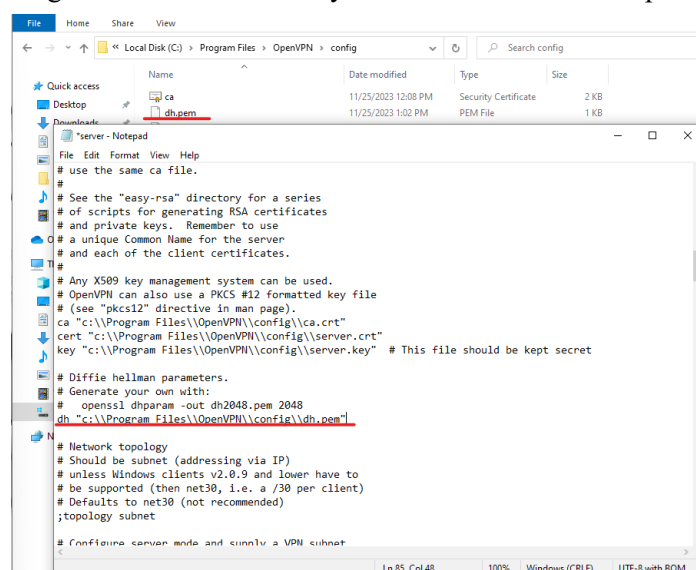
# "dev tun" will create a routed IP tunnel,
# "dev tap" will create an ethernet tunnel.
# Use "dev tap0" if you are ethernet bridging
# and have precreated a tap0 virtual interface
# and bridged it with your ethernet interface.
# If you want to control access policies
# over the VPN, you must create firewall
# rules for the the TUN/TAP interface.
# On non-Windows systems, you can give
# an explicit unit number, such as tun0.
# On Windows, use "dev-node" for this.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
dev tap
;dev tun
```

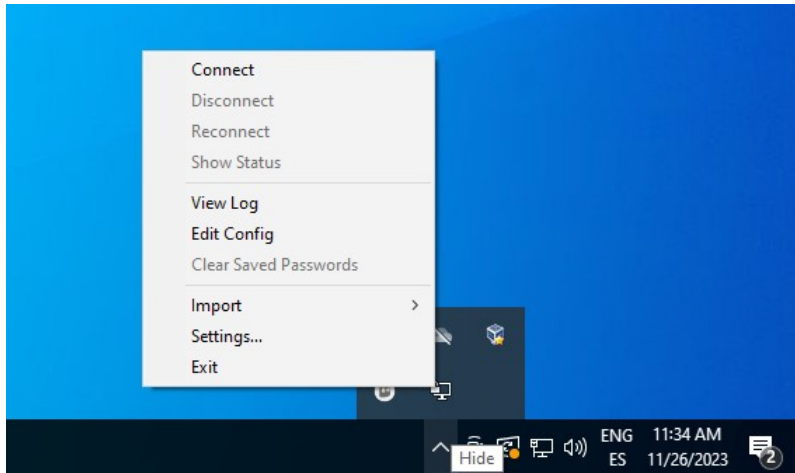
Ahora en el mismo archivo configuraremos las rutas de donde se encuentran el certificador, el certificado y la clave privada como nos indica el documento que debemos hacerlo.(doble barra para indicar la ruta y todo entrecomillado)

```
*server - Notepad
File Edit Format View Help
# you may need to selectively disable the
# Windows firewall for the TAP adapter.
# Non-Windows systems usually don't need this.
;dev-node MyTap

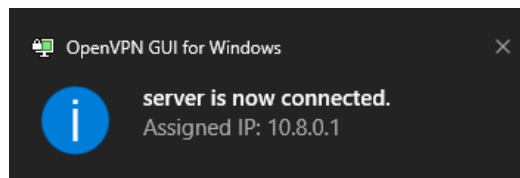
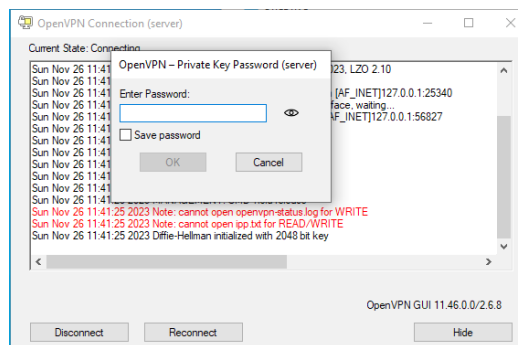
# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key). Each client
# and the server must have their own cert and
# key file. The server and all clients will
# use the same ca file.
#
# See the "easy-rsa" directory for a series
# of scripts for generating RSA certificates
# and private keys. Remember to use
# a unique Common Name for the server
# and each of the client certificates.
#
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca "c:\\Program Files\\OpenVPN\\config\\ca.crt"
cert "c:\\Program Files\\OpenVPN\\config\\server.crt"
key "c:\\Program Files\\OpenVPN\\config\\server.key" # This file should be kept secret
```

También debemos configurar la ruta de donde se encuentra el archivo de **diffie-hellman** el cual llamamos dh.pem, una vez hecho esto guardamos los cambios y tratamos de conectar la vpn



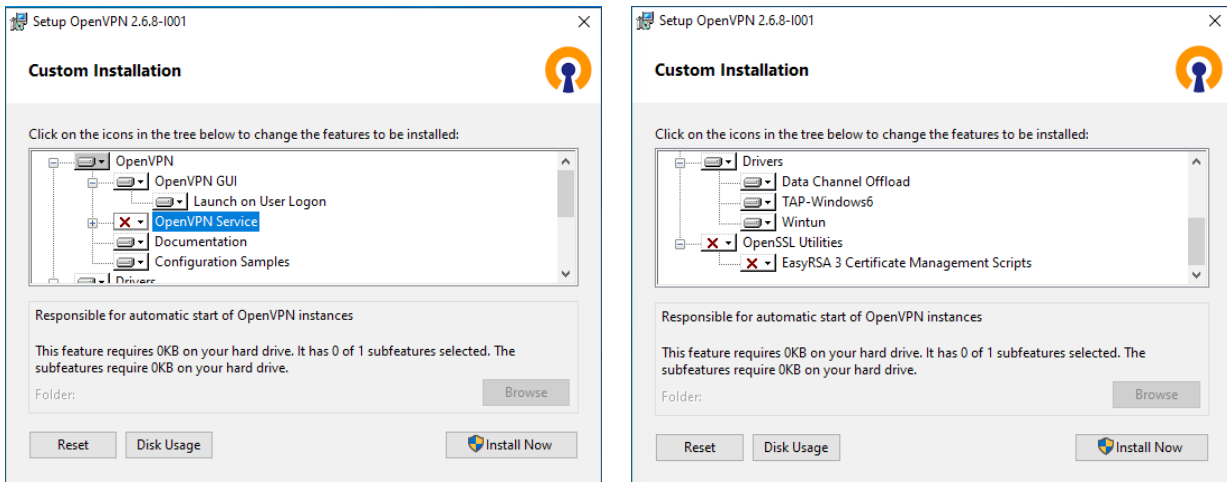


Si todo esta configurado correctamente debe salir esta pestaña pidiéndote la contraseña que pusimos anteriormente para el servidor. El cortafuegos saltara y solo tendremos que permitir el uso del server. Una vez hecho esto ya nos conectaríamos al servidor.



4. Instalación el Cliente

A diferencia de la instalación del servidor no utilizaremos OpenVPN Service ni OpenSSL Utilities ya que haremos uso del servidor que ya nos dará esas utilidades.

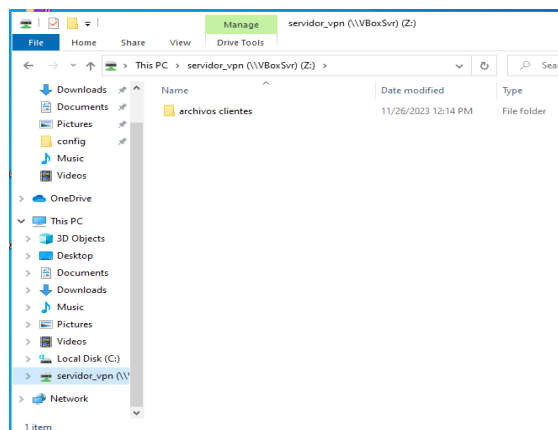


Ahora solo queda instalar.



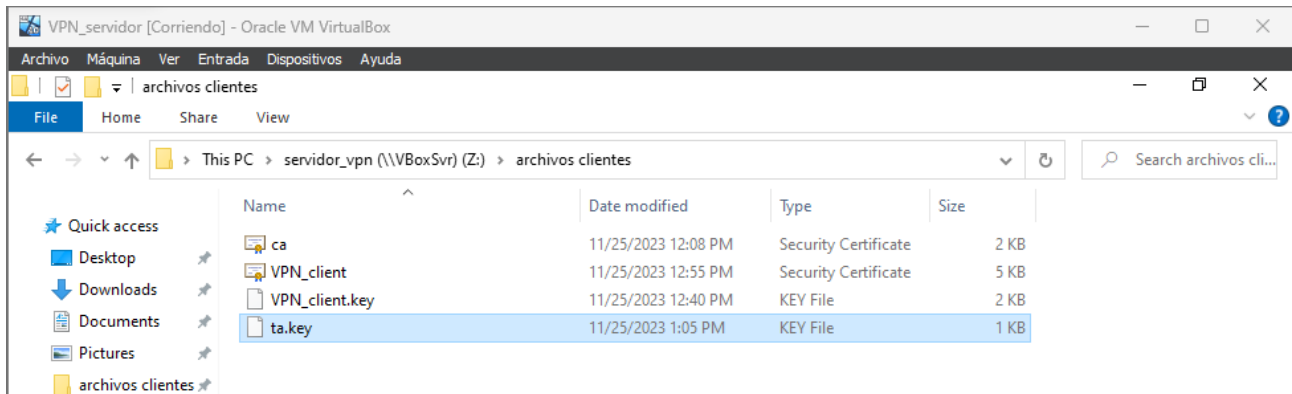
5. Copiar archivos de servidor al cliente

Para poder hacer esta parte necesitaremos de un recurso compartido que se le pueda dar al servidor como al cliente para pasarse “x” recursos de uno a otro, para ello hemos decidido hacer una carpeta compartida donde pasaremos todos los recursos.

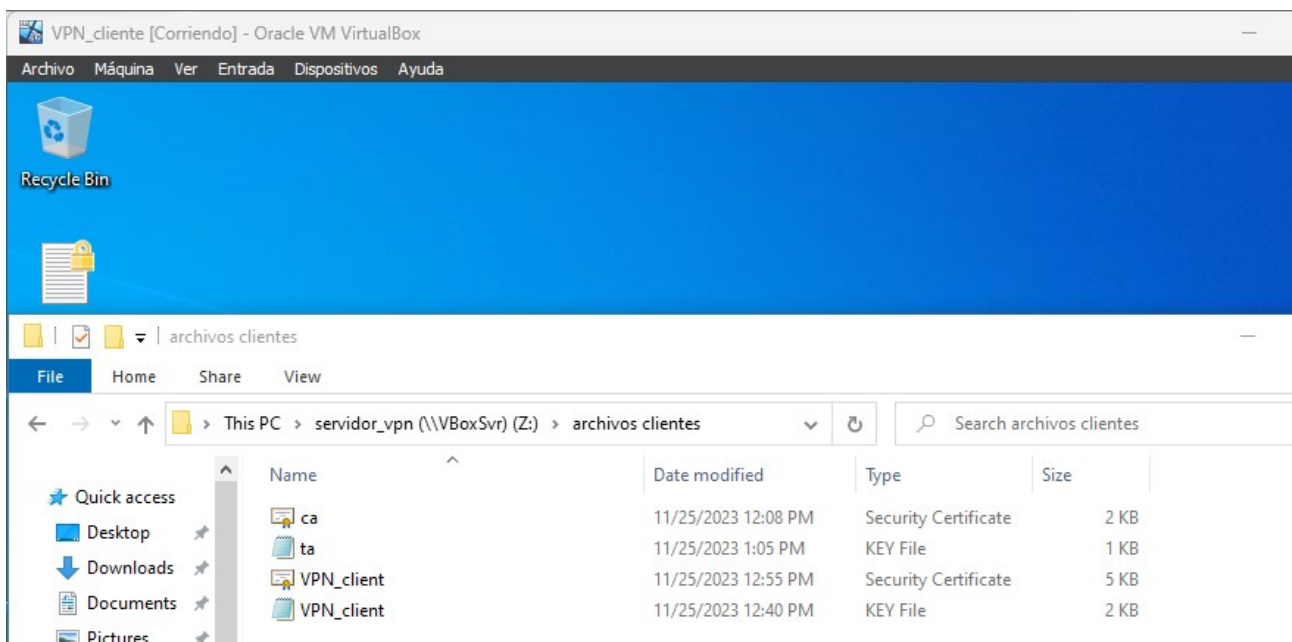


Los archivos que tendremos que pasar de una máquina a otra serán los siguientes:

SERVIDOR:

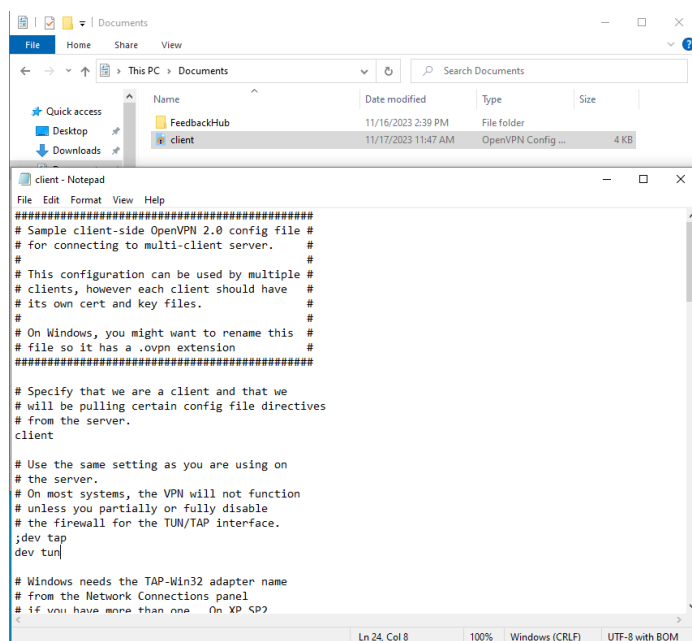


CLIENTE:



6. Configurar el cliente

Para empezar entraremos en el archivo de configuración del cliente.



```
File Edit Format View Help
#####
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server. #
#
# This configuration can be used by multiple #
# clients, however each client should have #
# its own cert and key files. #
#
# On Windows, you might want to rename this #
# file so it has a .ovpn extension #
#####

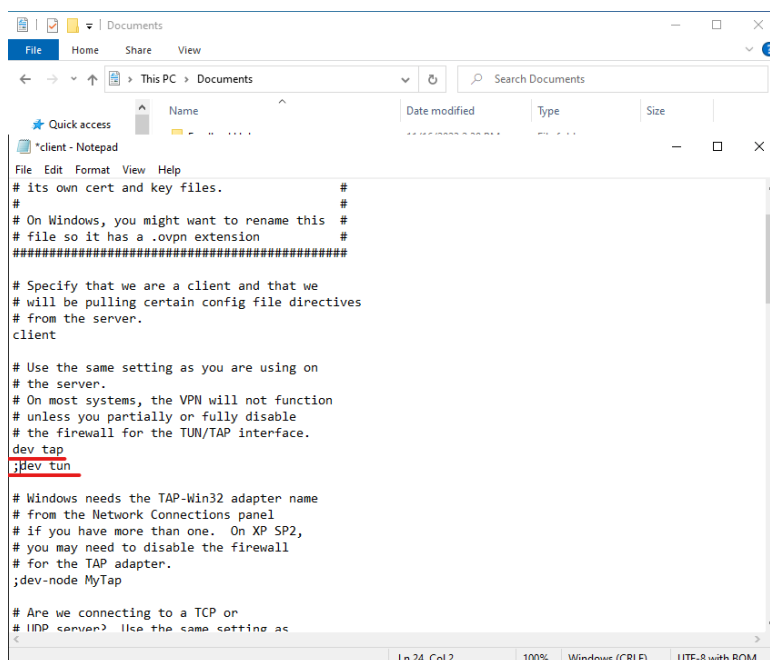
# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one. On XP SP2

```

A continuación cambiaremos el punto y coma de lugar como hicimos en el apartado del servidor para que el cliente pueda realizar una red virtual tunelada por ethernet.



```
File Edit Format View Help
# its own cert and key files. #
#
# On Windows, you might want to rename this #
# file so it has a .ovpn extension #
#####

# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client

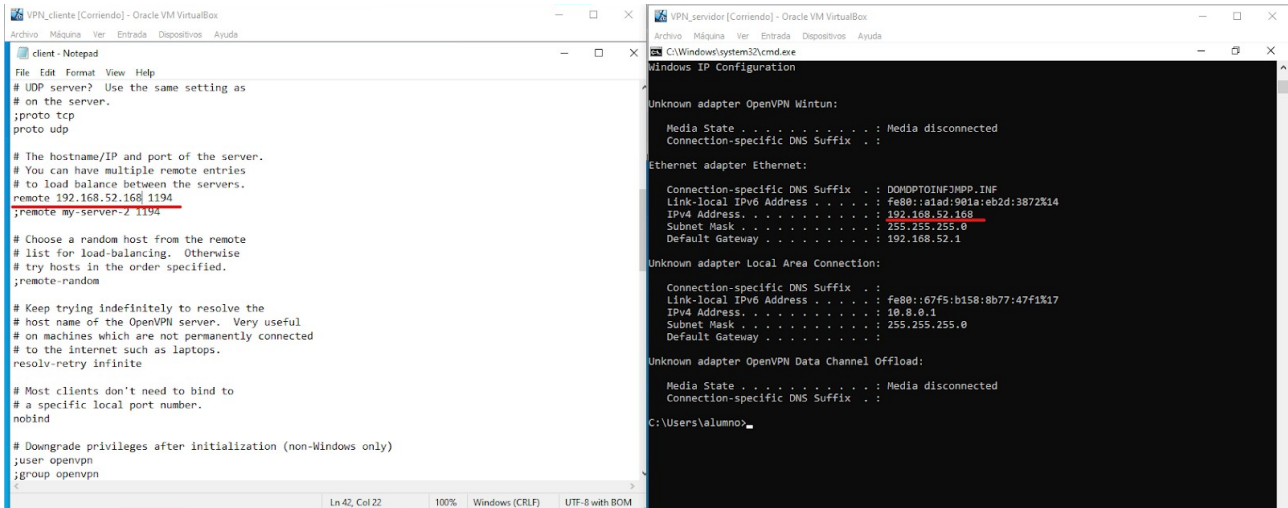
# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
;dev tun

# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one. On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap

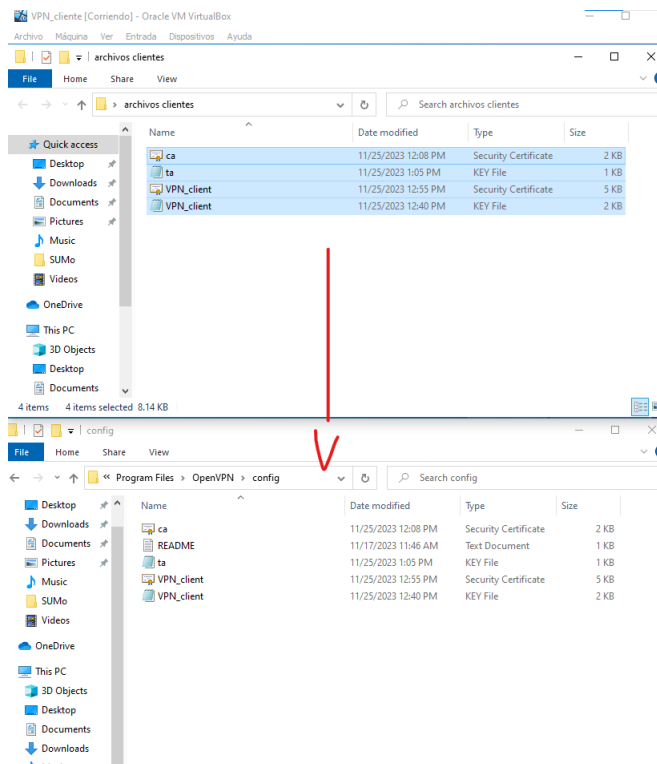
# Are we connecting to a TCP or
# UDP server? Use the same setting as

```

Ahora asignamos el hostname y el puerto de conexión con el servidor para poder conectarnos con el server.



Pasamos los archivos que configuramos anteriormente desde nuestra carpeta compartida a la carpeta de configuración para que el cliente tenga los certificados.



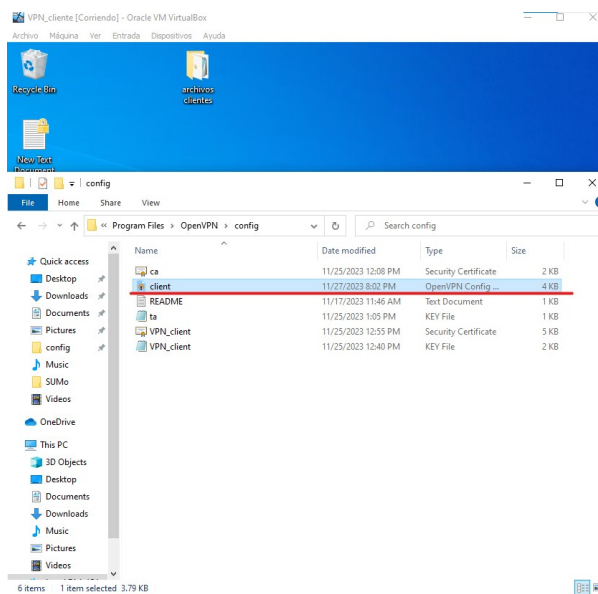
De nuevo en el archivo de configuración del cliente ponemos las rutas de los archivos que acabamos de pasar a la carpeta donde se encuentran los certificados y la clave del cliente

```
# SSL/TLS parms.  
# See the server config file for more  
# description. It's best to use  
# a separate .crt/.key file pair  
# for each client. A single ca  
# file can be used for all clients.  
ca "c:\\Program Files\\OpenVPN\\config\\ca.crt"  
cert "c:\\Program Files\\OpenVPN\\config\\VPN_client.crt"  
key "c:\\Program Files\\OpenVPN\\config\\VPN_client.key"
```

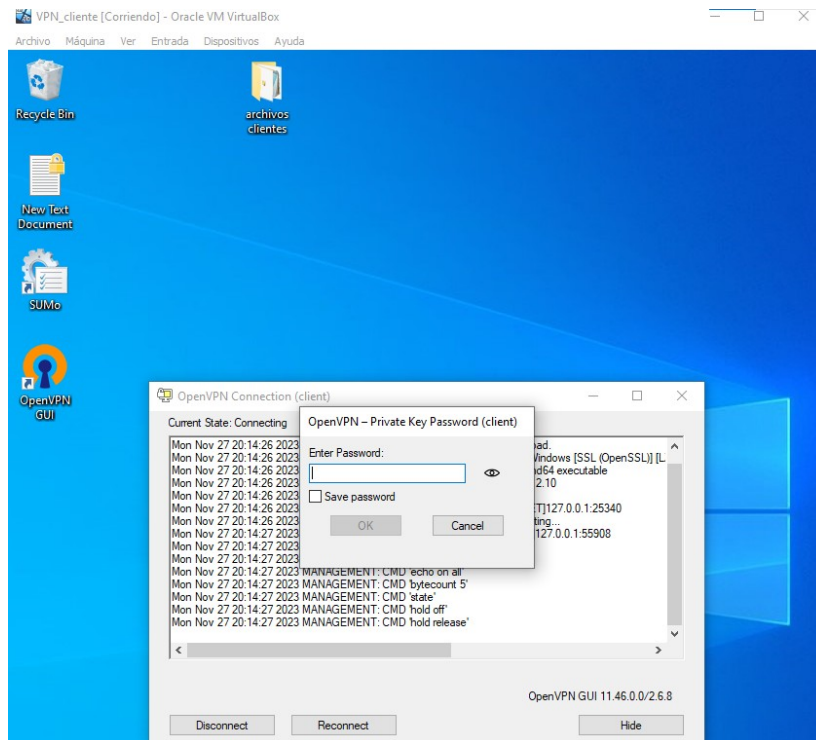
También le especificamos la ruta de la clave segura

```
# If a tls-auth key is used on the server  
# then every client must also have the key.  
tls-auth "c:\\Program Files\\OpenVPN\\config\\ta.key" 1
```

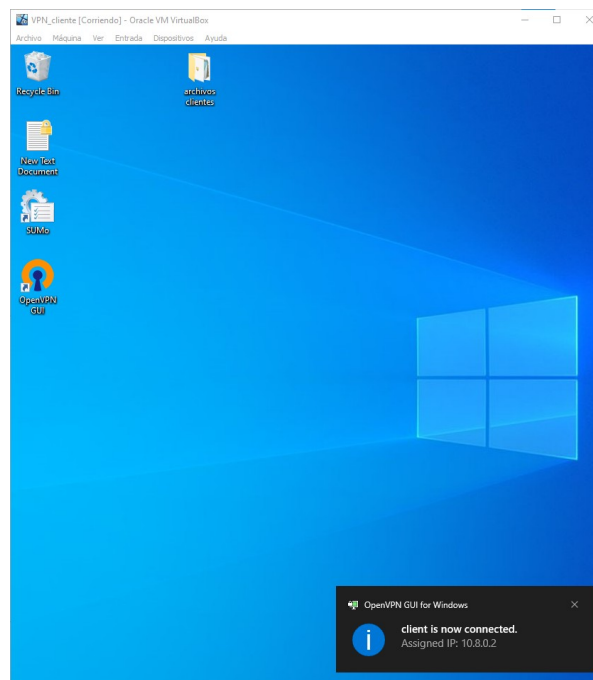
Y ahora copiamos el archivo de configuración de la carpeta



Y tratamos de conectarnos utilizando la contraseña.



Y ya tendremos el cliente conectado a nuestro servidor.



Aquí vemos como el servicio de VPN nos da la IP que ponía en la captura anterior

```
VPN_cliente [Corriendo] - Oracle VM VirtualBox
C:\Windows\system32\cmd.exe

C:\Users\alumno>ipconfig

Windows IP Configuration

Unknown adapter OpenVPN Wintun:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::a1ad:901a:eb2d:3072%15
    IPv4 Address. . . . . : 192.168.1.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Unknown adapter OpenVPN TAP-Windows6:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::6afa:8cfe:2cef:a3ba%8
    IPv4 Address. . . . . : 10.8.0.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Unknown adapter OpenVPN Data Channel Offload:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\alumno>
```