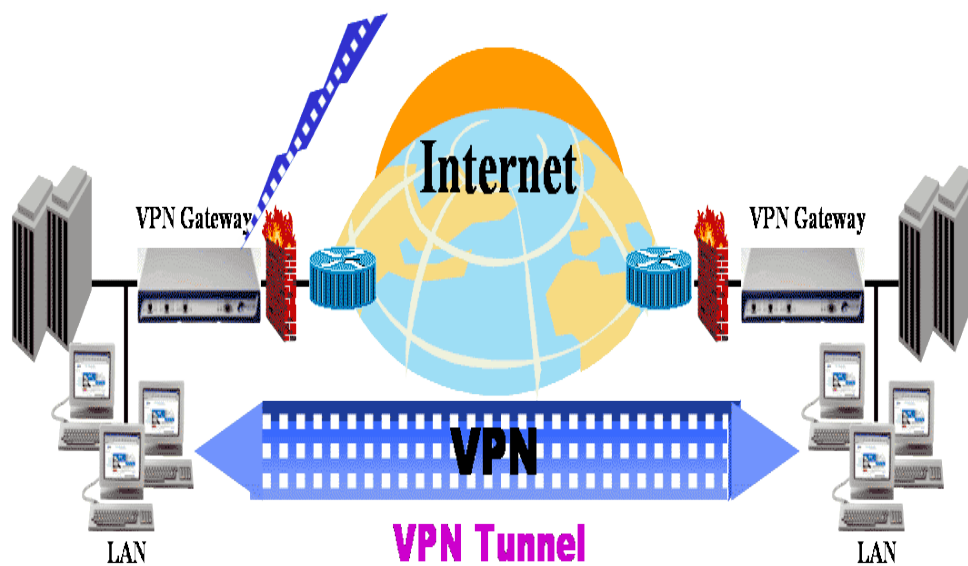




Configuración de openVPN



OpenVPN es una completa herramienta de código abierto solución SSL VPN que reúne una amplia gama de configuraciones, incluyendo acceso remoto, VPNs site-to-site, la seguridad Wi-Fi, y escala empresarial soluciones de acceso remoto con equilibrio de carga, conmutación por error y multa de grano de acceso de control proporcional. OpenVPN ofrece una rentable alternativa ligera a otras tecnologías de VPN disponibles en el mercado.

Cobertizos ligeros OpenVPN de diseño de muchas de las complejidades y el modelo de seguridad se basa en SSL, el estándar de la industria para comunicaciones seguras a través de Internet. OpenVPN implementa OSI extensión de la capa 2 o 3 red segura mediante el protocolo SSL / TLS, soporta flexibles métodos de autenticación de cliente basada en certificados, tarjetas inteligentes, y / o autenticación de 2 factores, y permite que el usuario o grupo específicos, las políticas de control de acceso usando las reglas de firewall aplicada a la interfaz de VPN virtual. OpenVPN no es un proxy de aplicación web y no opera a través de un navegador web.

Vamos a ver cómo instalar y configurar OpenVPN en SUSE Linux y openSUSE

Instalar OpenVPN

Antes de comenzar la instalación, planifique la configuración de VPN en consecuencia. Esto incluye la elección encamina [recomendado] o modo puente (modo enrutado separa las subredes y, por consiguiente difusión no atraviesan mientras que las gotas de puente en la misma subred LAN y por lo tanto las emisiones se permite a través de VPN), Rango IP para el sector privado vpn etc

yast2-install openvpn

Esto instala el software OpenVPN en /usr/share/openvpn

Copiar en /etc/

Copie el directorio /usr/share/openvpn al directorio /etc/ para evitar una actualización overriding las configuraciones. Además, la instalación por defecto carga un script de inicio /etc/init.d/openvpn que busca configuraciones en el directorio /etc/openvpn y por lo tanto tiene más sentido.

cp -r /usr/share/openvpn/etc/

```
linux-5g3q:~ # cp -r /usr/share/openvpn/etc/  
linux-5g3q:~ #
```

Generar Maestro Autoridad de Certificación (CA) certificado y la clave

Cambiar el directorio a /etc/openvpn/easy-rsa/2.0/ y ejecute los siguientes comandos para inicializar la limpieza, la limpieza todas las claves existentes y construir la CA.

cd /etc/openvpn/easy-rsa/2.0/

```
opensuse :/etc/openvpn/easy-rsa/2.0/ # ../vars
```

```
opensuse /etc/openvpn/easy-rsa/2.0 :// # ./clean-all
```

```
opensuse :/etc/openvpn/easy-rsa/2.0/ # ./build ca
```

```
linux-5g3q:~ # cd /etc/openvpn/easy-rsa/2.0/  
linux-5g3q:/etc/openvpn/easy-rsa/2.0 #
```

```
linux-5g3q:/etc/openvpn/easy-rsa/2.0 # . ./vars  
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/  
2.0/keys  
linux-5g3q:/etc/openvpn/easy-rsa/2.0 #
```

```
linux-5g3q:/etc/openvpn/easy-rsa/2.0 # ./clean-all  
linux-5g3q:/etc/openvpn/easy-rsa/2.0 #
```

```

linux-5g3q:/etc/openvpn/easy-rsa/2.0 # ./build-ca
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to '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) [US]:US
State or Province Name (full name) [CA]:CA
Locality Name (eg, city) [SanFrancisco]:Sanfrancisco
Organization Name (eg, company) [Fort-Funston]:Fort-Funston
Organizational Unit Name (eg, section) [changeme]:server
Common Name (eg, your name or your server's hostname) [changeme]:server
Name [changeme]:rawel
Email Address [mail@host.domain]:mail@host.domain
linux-5g3q:/etc/openvpn/easy-rsa/2.0 # █

```

Responda a las preguntas le pedirá que cree el amo CA certificado y la clave

Generar certificado y llave para el servidor

opensuse: /etc/openvpn/easy-rsa/2.0/ # ./build-key-server

```

linux-5g3q:/etc/openvpn/easy-rsa/2.0 # ./build-key-server server
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'server.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) [US]:US
State or Province Name (full name) [CA]:CA
Locality Name (eg, city) [SanFrancisco]:Sanfrancisco
Organization Name (eg, company) [Fort-Funston]:Fort-Funston
Organizational Unit Name (eg, section) [changeme]:server
Common Name (eg, your name or your server's hostname) [server]:server
Name [changeme]:rawel
Email Address [mail@host.domain]:mail@host.domain

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:12345
An optional company name []:so3

```

```
Using configuration from /etc/openvpn/easy-rsa/2.0/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'US'
stateOrProvinceName    :PRINTABLE:'CA'
localityName            :PRINTABLE:'Sanfrancisco'
organizationName        :PRINTABLE:'Fort-Funston'
organizationalUnitName :PRINTABLE:'server'
commonName              :PRINTABLE:'server'
name                   :PRINTABLE:'rawel'
emailAddress            :IA5STRING:'mail@host.domain'
Certificate is to be certified until Apr  6 02:24:45 2023 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
linux-5g3q:/etc/openvpn/easy-rsa/2.0 # █
```

Responda a las preguntas le pedirá que cree el certificado del servidor y la clave.

Generar certificado y llave para el Cliente

He aquí que yo crearé una clave para un cliente llamado vpnhost1.

Opensuse: /etc/openvpn/easy-rsa/2.0/ # ./vpnhost1 build-key

Responda a las preguntas le pedirá que cree el certificado de cliente y clave. Repita el procedimiento como certificado de cliente muchas y clave según sea necesario.

```
Linux-5g3q:/etc/openvpn/easy-rsa/2.0 # ./build-key vpnhost1
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'vpnhost1.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) [US]:US
State or Province Name (full name) [CA]:CB
Locality Name (eg, city) [SanFrancisco]:Sanfrancisco
Organization Name (eg, company) [Fort-Funston]:Fort-Funston
Organizational Unit Name (eg, section) [changeme]:server
Common Name (eg, your name or your server's hostname) [vpnhost1]:vpnhost1
Name [changeme]:rawel
Email Address [mail@host.domain]:mail@host.domain

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:12345
An optional company name []:so3
```

```
Using configuration from /etc/openvpn/easy-rsa/2.0/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'US'
stateOrProvinceName :PRINTABLE:'CB'
localityName      :PRINTABLE:'Sanfrancisco'
organizationName  :PRINTABLE:'Fort-Funston'
organizationalUnitName:PRINTABLE:'server'
commonName        :PRINTABLE:'vpnhost1'
name              :PRINTABLE:'rawel'
emailAddress      :IASSTRING:'mail@host.domain'
Certificate is to be certified until Apr  6 02:35:14 2023 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]
Write out database with 1 new entries
Data Base Updated
linux-5g3q:/etc/openvpn/easy-rsa/2.0 # █
```

Si recibió el mensaje de error siguiente al final de la creación del certificado cliente:

**failed to update database
TXT_DB error number 2**

Esto es probablemente debido a que han generado su propio certificado de firma con el mismo nombre común (CN) información de que el certificado de la CA que ha generado antes. Simplemente introduzca un nombre común diferente cada vez que se pide debe hacer el truco.

Generar Diffie Hellman (DH) parámetros

Generar los parámetros Diffie Hellman para el servidor OpenVPN

opensuse: /etc/openvpn/easy-rsa/2.0/ # ./build dh

```
linux-5g3q:/etc/openvpn/easy-rsa/2.0 # ./build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
.....++*++*++*
linux-5g3q:/etc/openvpn/easy-rsa/2.0 # █
```

Ahora, usted puede ver todos los archivos clave creados en el directorio

Ls -l o dir /etc/openvpn/easy-rsa/2.0/keys/

Donde

ca.crt - certificado raíz para el servidor y todos los clientes

ca.key Root CA clave para la máquina de firmar una clave única

. dh <n> pem - DH parametros para el servidor (dh1024.pem aquí)

server.crt y server.key - Certificado de servidor y la clave (el nombre será el nombre común entró AAT el momento de la generación del certificado)

vpnhost1.crt y vpnhost1.key - certificado de cliente y la clave (el nombre será el nombre común entró AAT el momento de la generación del certificado)

Crear un archivo de configuración del servidor

Los ficheros de configuración de ejemplo se instalan en el directorio `/usr/share/doc/packages/openvpn/simple-config-files/`. Copie el archivo `server.conf` a `/etc/openvpn/`.

```
# cp /usr/share/doc/packages/openvpn/simple-config-files/server.conf /etc/openvpn/
```

```
linux-5g3q:/etc/openvpn/easy-rsa/2.0 # cp /usr/share/doc/packages/openvpn/sample-config-files/server.conf /etc/openvpn/
linux-5g3q:/etc/openvpn/easy-rsa/2.0 #
```

Edite el archivo y modificar los parámetros del **servidor**.

```
linux-5g3q:/etc/openvpn/easy-rsa/2.0 # vi /etc/openvpn/server.conf
```

Edite las líneas

ca ca.crt

cert server.crt

clave server.key

y cambiarlo según su configuración. De acuerdo con nuestra configuración, los archivos deben estar en `/etc/openvpn/easy-rsa/2.0/keys`. En mi servidor es como:

ca /etc/openvpn/easy-rsa/2.0/keys/ca.crt

cert /etc/openvpn/easy-rsa/2.0/keys/server.crt

key /etc/openvpn/easy-rsa/2.0/keys/server.key

dh /etc/openvpn/easy-rsa/2.0/keys/dh1024.pem

```
# 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 /etc/openvpn/easy-rsa/2.0/keys/ca.crt
cert /etc/openvpn/easy-rsa/2.0/keys/server.crt
key /etc/openvpn/easy-rsa/2.0/keys/server.key

# This file should be kept secret

# Diffie hellman parameters.
# Generate your own with:
# openssl dhparam -out dh1024.pem 1024
# Substitute 2048 for 1024 if you are using
# 2048 bit keys.

dh /etc/openvpn/easy-rsa/2.0/keys/dh1024.pem
```

Ahora, está todo listo para probar ejecutar el servidor.

Iniciar OpenVPN

opensuse: ~ # openvpn /etc/openvpn/server.conf

```
Linux-5g3q:/etc/openvpn/easy-rsa/2.0 # openvpn /etc/openvpn/server.conf
Sun Apr  7 23:51:47 2013 OpenVPN 2.2.2 i586-suse-linux-gnu [SSL] [LZ02] [
EPOLL] [PKCS11] [eurephia] built on Dec 14 2011
Sun Apr  7 23:51:47 2013 NOTE: OpenVPN 2.1 requires '--script-security 2'
or higher to call user-defined scripts or executables
Sun Apr  7 23:51:47 2013 Diffie-Hellman initialized with 1024 bit key
Sun Apr  7 23:51:47 2013 TLS-Auth MTU parms [ L:1542 D:138 EF:38 EB:0 ET:
0 EL:0 ]
Sun Apr  7 23:51:47 2013 Socket Buffers: R=[163840->131072] S=[163840->13
1072]
Sun Apr  7 23:51:47 2013 ROUTE default_gateway=192.168.230.2
Sun Apr  7 23:51:48 2013 TUN/TAP device tun0 opened
Sun Apr  7 23:51:48 2013 TUN/TAP TX queue length set to 100
Sun Apr  7 23:51:48 2013 /bin/ip link set dev tun0 up mtu 1500
Sun Apr  7 23:51:48 2013 /bin/ip addr add dev tun0 local 10.8.0.1 peer 10
.8.0.2
Sun Apr  7 23:51:48 2013 /bin/ip route add 10.8.0.0/24 via 10.8.0.2
Sun Apr  7 23:51:48 2013 Data Channel MTU parms [ L:1542 D:1450 EF:42 EB:
135 ET:0 EL:0 AF:3/1 ]
Sun Apr  7 23:51:48 2013 UDPv4 link local (bound): [undef]:1194
Sun Apr  7 23:51:48 2013 UDPv4 link remote: [undef]
Sun Apr  7 23:51:48 2013 MULTI: multi_init called, r=256 v=256
Sun Apr  7 23:51:48 2013 IFCONFIG POOL: base=10.8.0.4 size=62
Sun Apr  7 23:51:48 2013 IFCONFIG POOL LIST
Sun Apr  7 23:51:48 2013 Initialization Sequence Completed
```

Ahora para comprobar que nuestro servidor nos a habilitado la interfaz de acceso VPN (como usuario **root**) escribimos el comando:

#ifconfig

y veremos que se a agregado la interfaz **tun0**.

Si hacemos desde, el servidor, un ping al IP de esa interfaz del cliente veremos

que se realiza sin problemas ya que la VPN se ha establecido correctamente.
(Esta prueba será hara cuando se haya configurado el cliente bien al final)

```
linux-5g3q:/etc/openvpn/easy-rsa/2.0 # ifconfig
eth0    Link encap:Ethernet  HWaddr 00:0C:29:68:41:FB
        inet addr:192.168.230.138  Bcast:192.168.230.255  Mask:255.255.
255.0
        inet6 addr: fe80::20c:29ff:fe68:41fb/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:3951 errors:0 dropped:0 overruns:0 frame:0
        TX packets:2813 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:4905719 (4.6 Mb)  TX bytes:241289 (235.6 Kb)
        Interrupt:19 Base address:0x2000

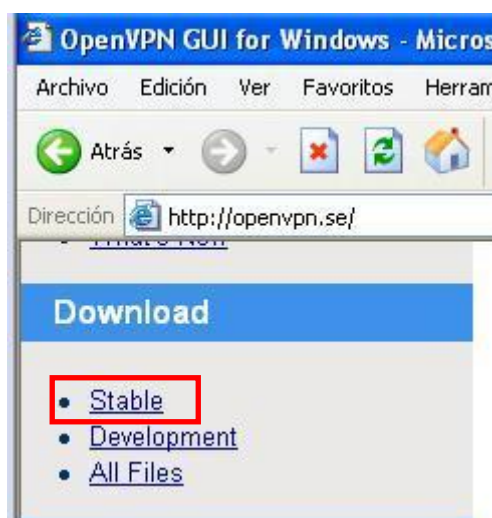
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:86 errors:0 dropped:0 overruns:0 frame:0
        TX packets:86 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:15284 (14.9 Kb)  TX bytes:15284 (14.9 Kb)

tun0    Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
0-00-00-00
        inet addr:10.8.0.1  P-t-P:10.8.0.2  Mask:255.255.255.255
        UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:100
        RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

linux-5g3q:/etc/openvpn/easy-rsa/2.0 # █
```

Cliente (Windows XP)

En el caso de Windows XP se debe instalar openVPN y openVPN-GUI (<http://openvpn.se>).



Hacer click en el link de descarga del archivo:

Download Stable Release

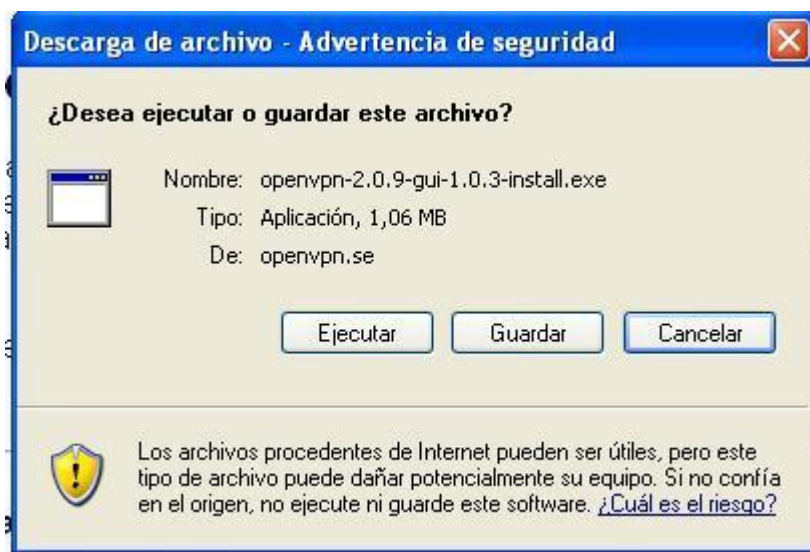
If you already have a working installation of OpenVPN, you can use the "A" to download the OpenVPN GUI executable alone. Make sure you save it i openvpn.exe, as OpenVPN GUI is dependent on the OpenSSL DLLs that this folder.

If you don't have OpenVPN installed, use the installation package below, \ OpenVPN and OpenVPN GUI for you.

Installation Package (Both 32-bit and 64-bit TAP driver included):

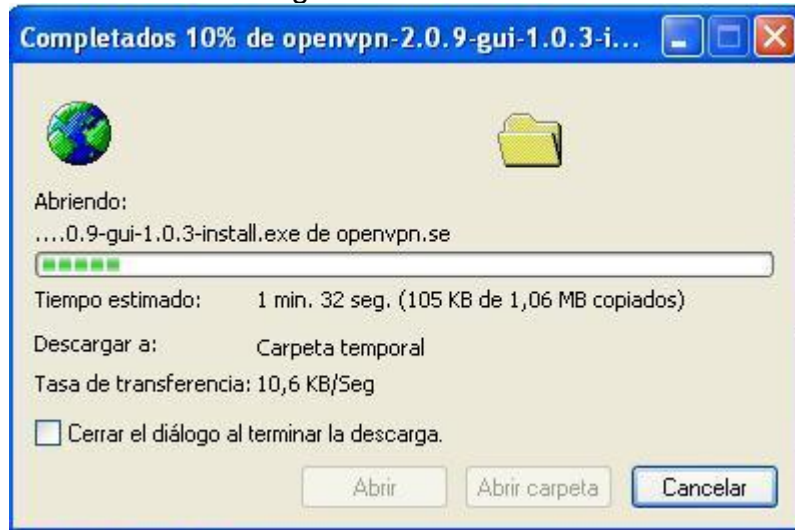
[openvpn-2.0.9-gui-1.0.3-install.exe](#)

Luego en el asistente de descarga hacemos click en ejecutar.

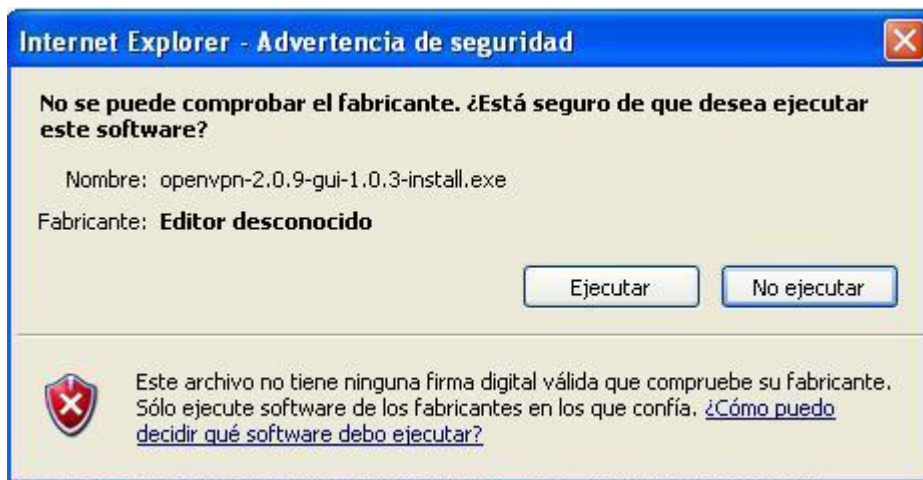


Esperamos a que se complete la descarga.

Hacer click en el link de descarga del archivo:



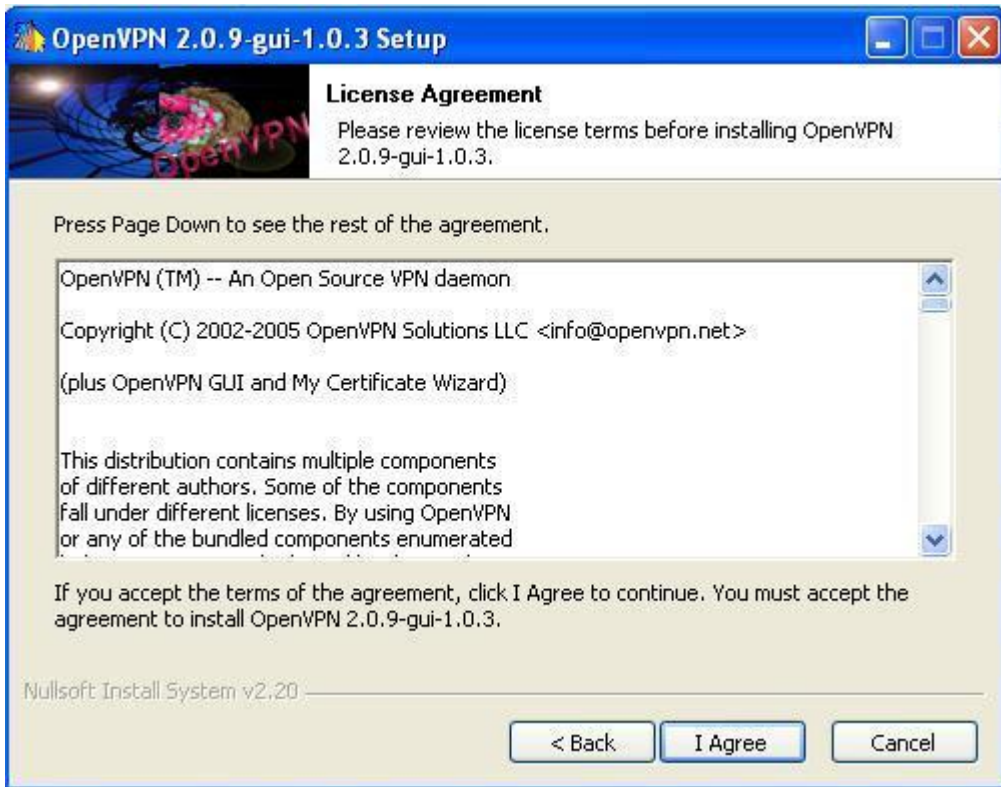
Hacemos click en ejecutar para comenzar a instalar.



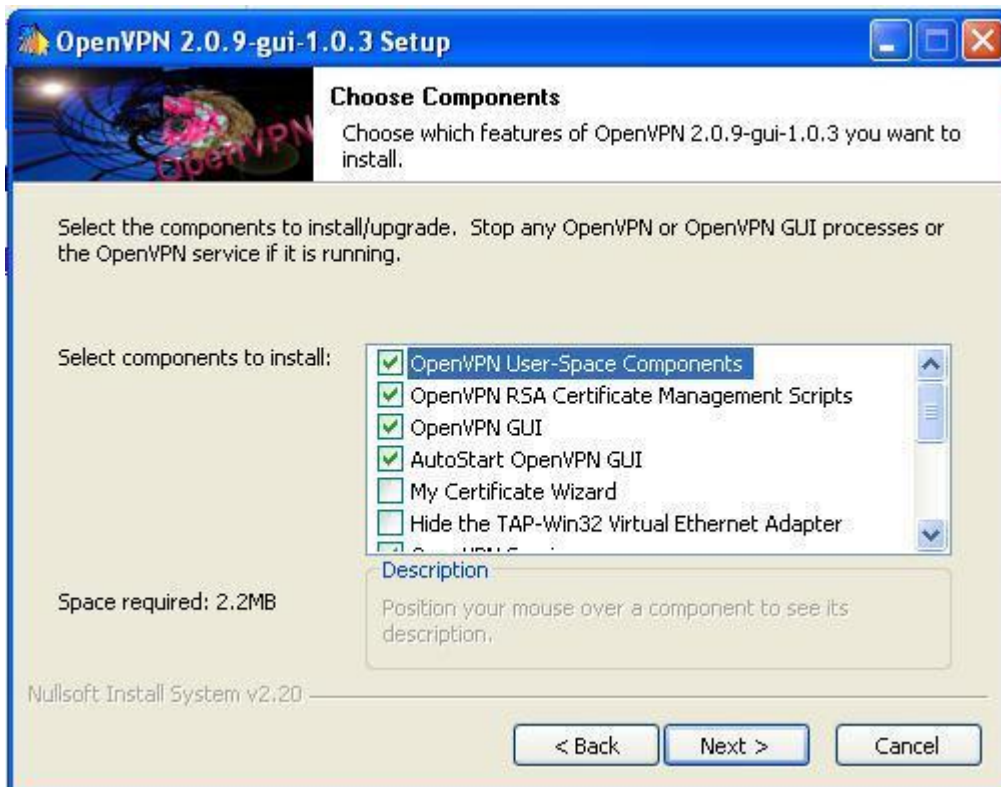
Click en **Next**.



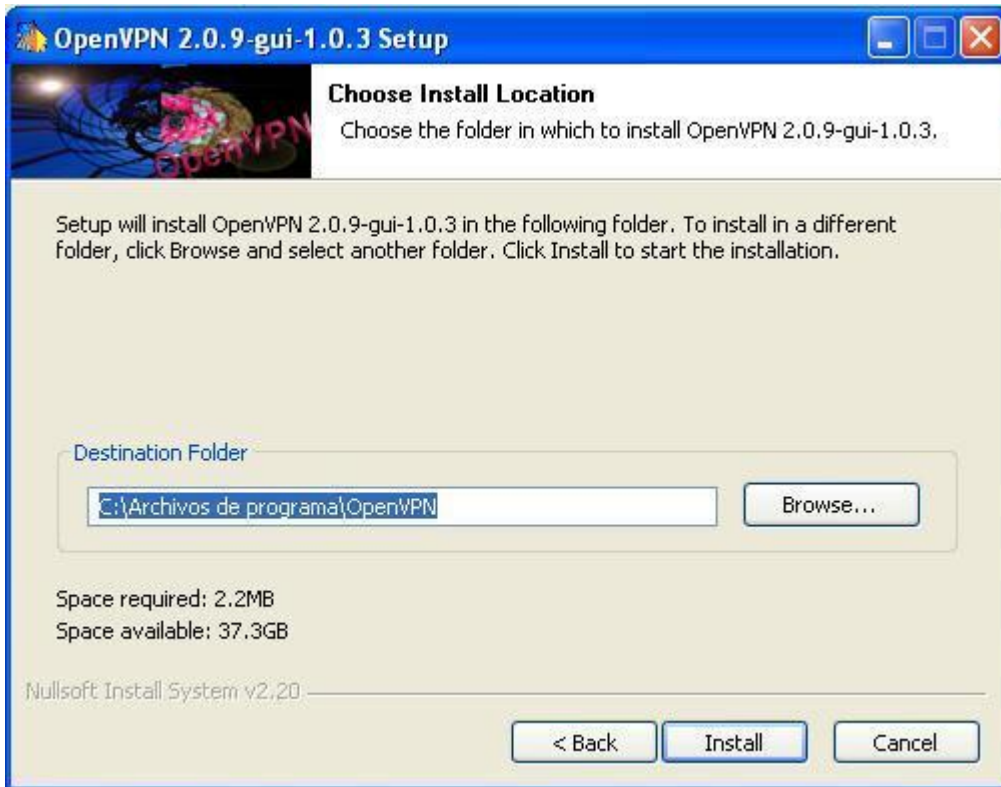
Click en **I Agree**.



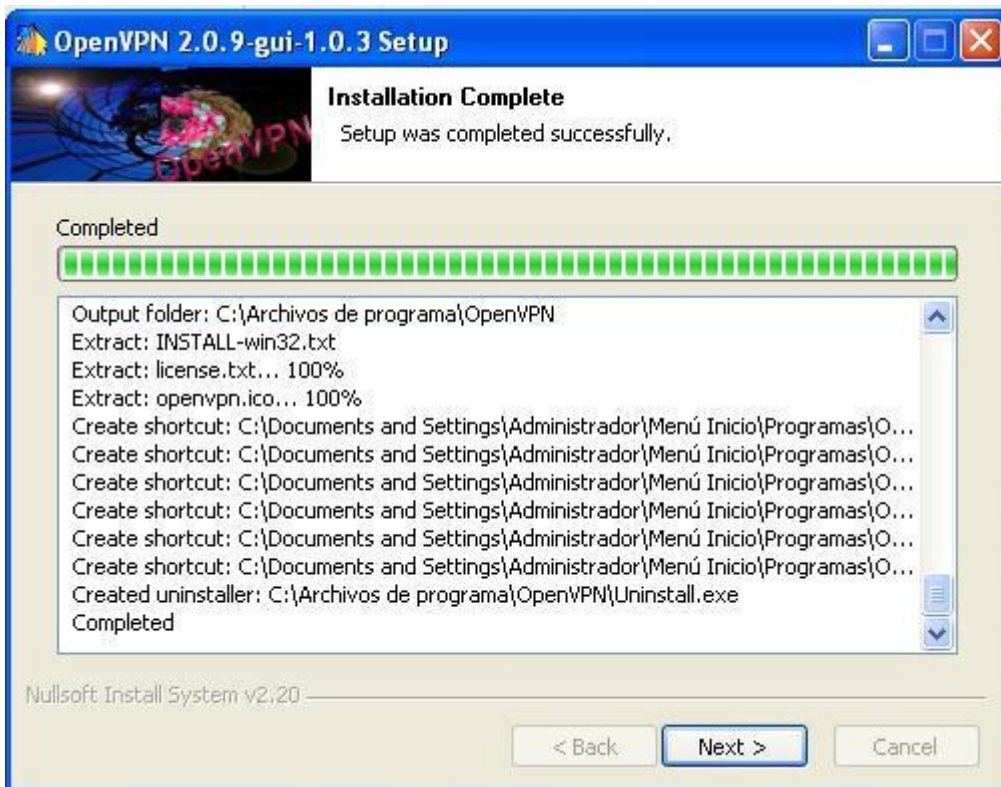
Click en **Next**.



Click en **Install**.



Click en **Next** (luego de haberse completado la instalación).

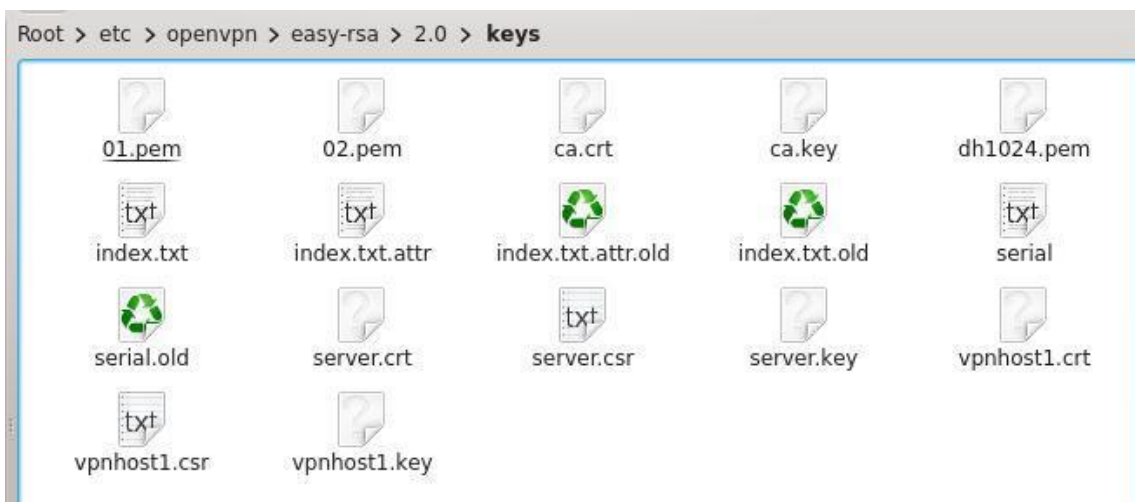


Y por último click en **Finish**.

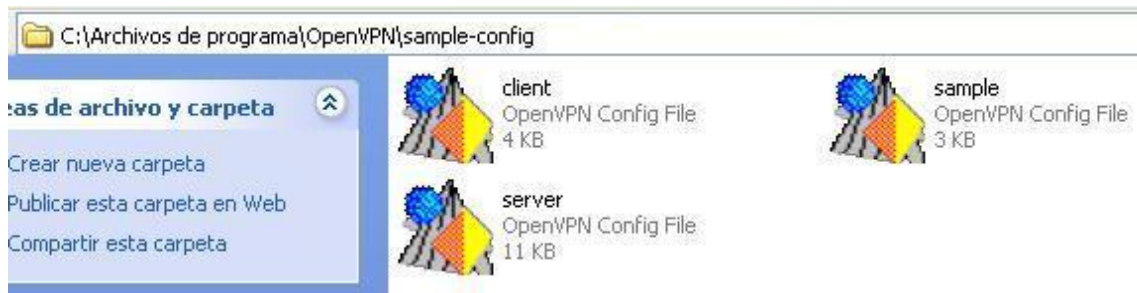


Una vez instalados copiamos los archivos entregados por el servidor (ca.crt, vpngost1.crt, vpngost1.key y todos los demás archivos) a un directorio en windows en específico, por ejemplo:

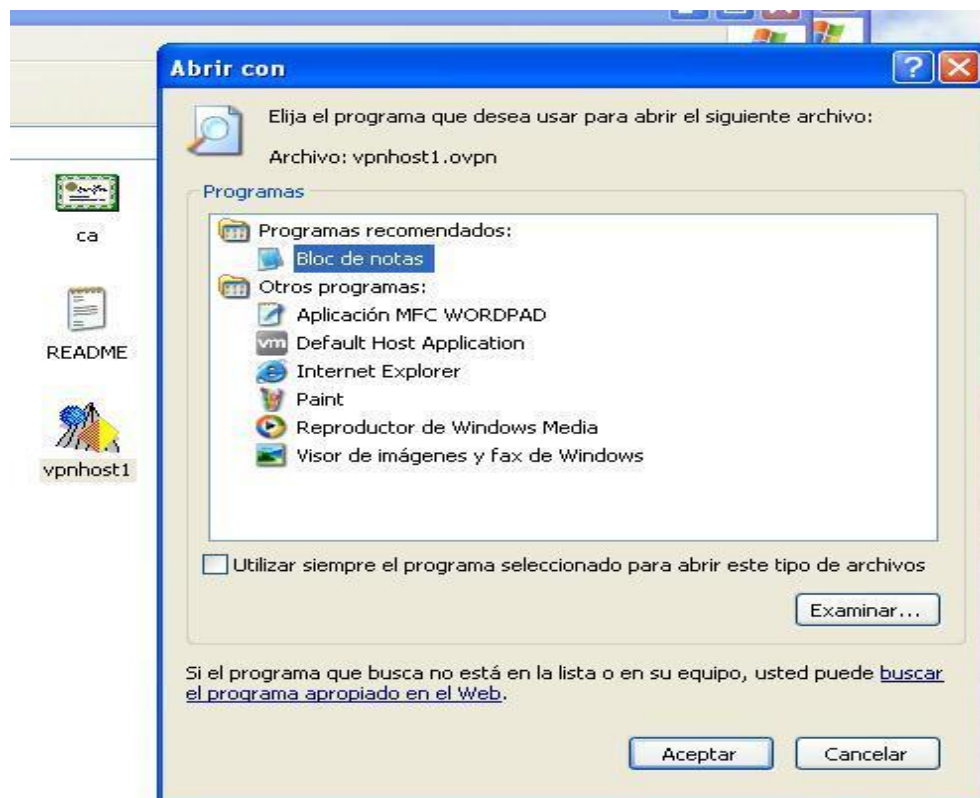
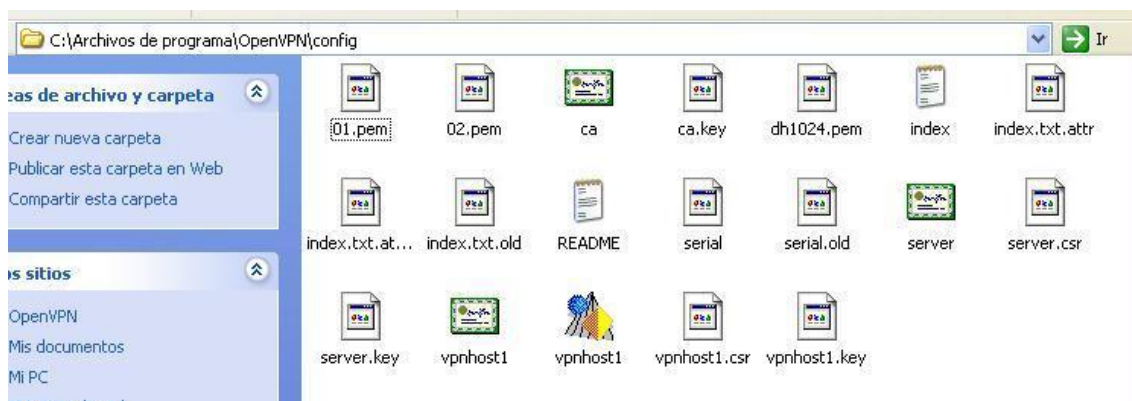
C:\Archivos de programa\OpenVPN\config



Una vez en el directorio `C:\Archivos de programa\OpenVPN\sample-config` y copiamos el archivo `client` a `C:\Archivos de programa\OpenVPN\config`.



Una vez en `C:\Archivos de programa\OpenVPN\config` le cambiamos el nombre de `client` por `vpnhost1` lo abrimos con un editor de texto (notepad sirve) y apuntamos la configuración a la dirección en donde pusimos los certificados y la llave privada.



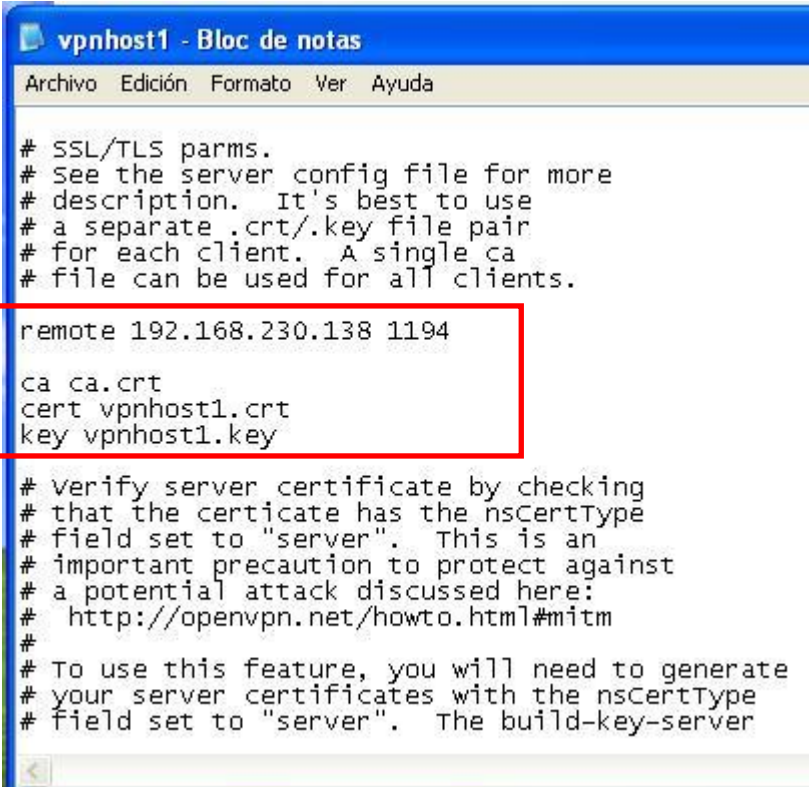
Ubicamos en el documento donde están estos archivos:

```
ca ca.crt
cert cliente1.crt
key cliente1.key
```

Luego modificamos estas líneas de manera que quede así:

```
remote 192.168.230.138 1194
```

```
ca ca.crt
cert vpnhost1.crt
key vpnhost1.key
```



```
vpnhost1 - Bloc de notas
Archivo Edición Formato Ver Ayuda

# 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.

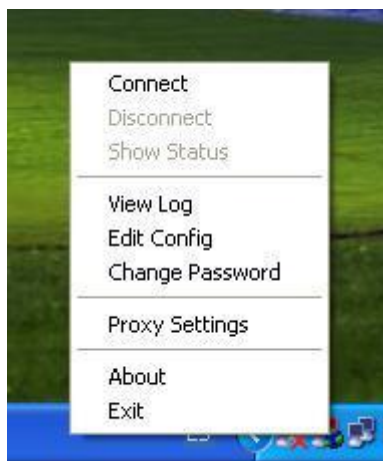
remote 192.168.230.138 1194
ca ca.crt
cert vpnhost1.crt
key vpnhost1.key

# Verify server certificate by checking
# that the certificate has the nsCertType
# field set to "server". This is an
# important precaution to protect against
# a potential attack discussed here:
# http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server". The build-key-server
```

Una vez listo guardamos el archivo y ejecutamos **openvpn-gui.exe** (se encuentra en la carpeta **bin** en el directorio de instalación de openVPN).



Al abrirlo veremos un icono de dos computadores rojos en la bandeja del sistema, si hacemos click derecho veremos un menú en donde la primera opción es **connect**:



Al pulsar conectar aparecerá una consola mostrando algunos datos y al finalizar aparecerá un mensaje avisando que la conexión se ha realizado:



Cliente (Linux)

En el cliente instalar `openvpn` como antes y tenemos que copiar el archivo **client.conf** de los archivos de configuración de ejemplo como con el servidor en el directorio `/etc/openvpn` y editar el archivo como muy parecida a la **server.conf** excepto.

Elegimos " **cliente** "para dejar claro que somos un cliente.

Introduzca la dirección IP remota del servidor OpenVPN. Carga de múltiples servidor de lista de equilibrado se puede agregar también.

Copie el certificado correspondiente y Archivos relevantes generados en el **servidor** en este **cliente**. Asegúrese de que este se lleva a cabo con seguridad. Modifique las entradas **ca.crt**, **vpngost1.crt**, **vpngost1.key** con caminos adecuados y nombres de archivo.

Para iniciar el cliente

openvpn /etc/openvpn/client.conf

Pruebe a conectar (puede ser un ping de una dirección IP) y comprobar si son capaces de conectarse a la red privada.

Link de referencia para configurar el cliente de Linux y más información sobre el tema:

<http://peloenpecho.blogcindario.com/2008/05/00003-armando-una-vpn-cliente-servidor-con-linux.html>

<http://www.susegeek.com/security/install-configure-openvpn-ssl-vpn-in-suse-opensuse-linux/>

<http://nicolasjolet.blogspot.com/2011/01/as-i-m-completely-unaware-of-openssl-use.html>

<http://metalklesk.blogspot.com/2008/07/vpn-segura-en-opensuse-110-y-windows-xp.html>

Y con esto hemos terminado con la práctica de **VPN!**