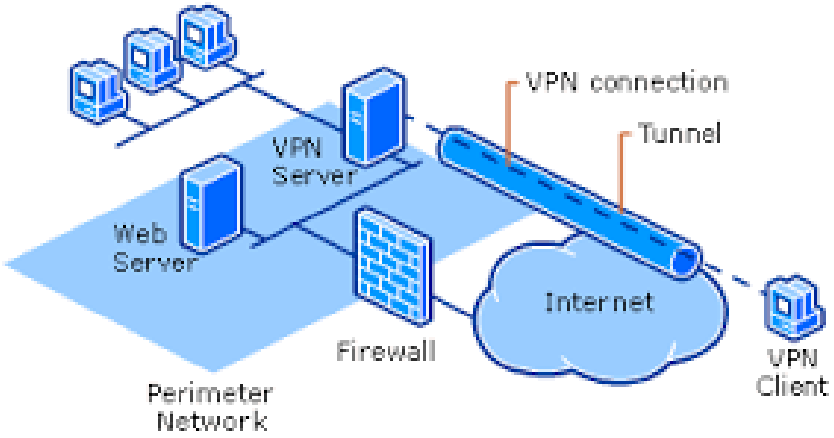
Conexiones VPN con OpenVPN

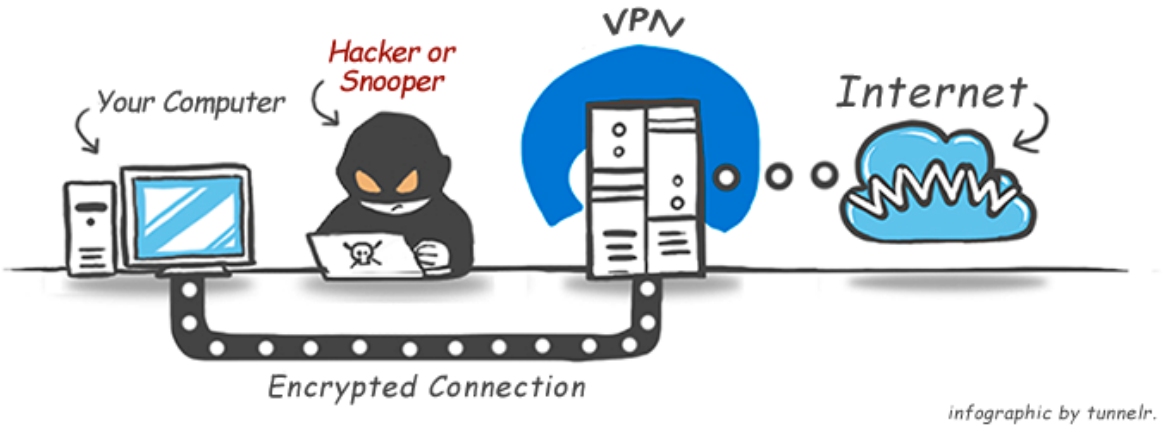
Introducción

Una red privada virtual (RPV), en inglés: Virtual Private Network (VPN), es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.1 Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.



Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

La conexión VPN a través de Internet es técnicamente una unión wide area network (WAN) entre los sitios pero al usuario le parece como si fuera un enlace privado— de allí la designación "virtual private network".



OpenVPN

Introducción

OpenVPN es una solución de conectividad basada en software libre: SSL (Secure Sockets Layer) VPN Virtual Private Network (red virtual privada), OpenVPN ofrece conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente, resulta una muy buena opción en tecnologías Wi-Fi (redes inalámbricas IEEE 802.11) y soporta una amplia configuración, entre ellas balanceo de cargas. Está publicado bajo la licencia GPL, de software libre.

Descargar OpenVPN

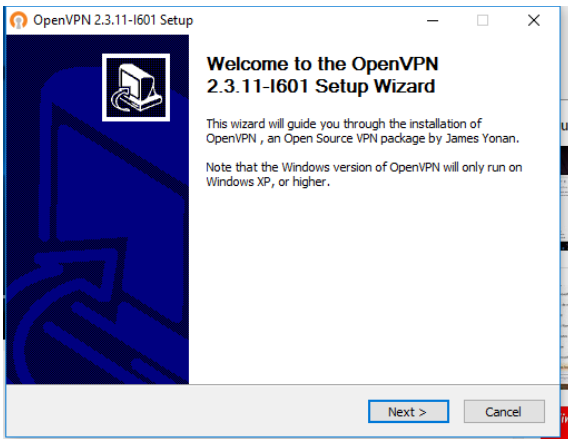
Entramos en la página web de OpenVPN https://openvpn.net/ y pulsamos en el link **comunity**.

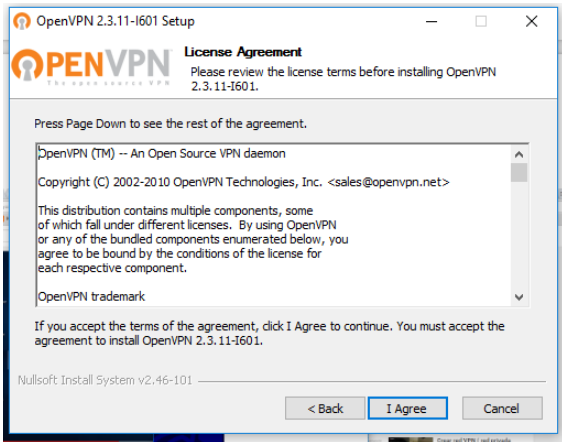
Pulsamos en **Downloads**

Y luego sobre la versión para windows de 64bits, nos descargamos un fichero llamado

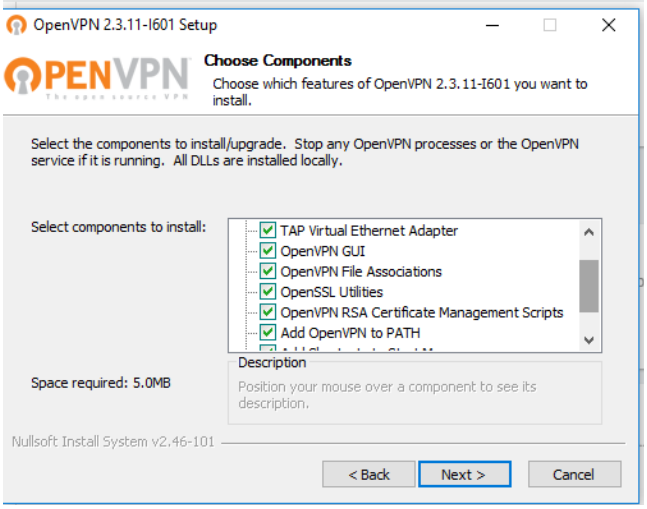
openvpn-install-2.3.11-I601-x86_64.exe

Instalamos OpenVPN

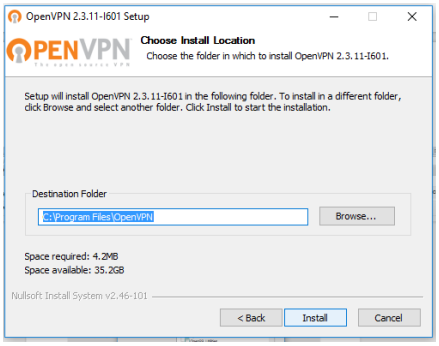


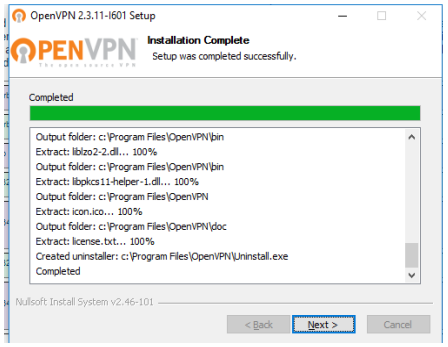


Importante en esta pantalla, marcar todas las opciones...

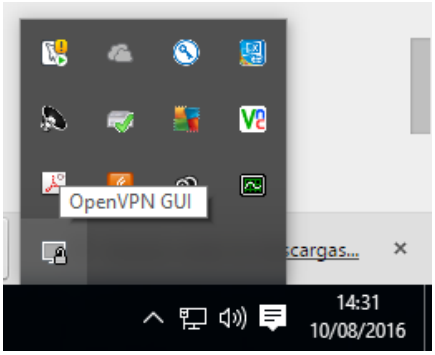


Proseguimos la instalación pulsando siguiente, siguientes, ...





Al finalizar tendremos en la barra de tareas un icono con openVpn



Configurando OpenVPN, generando certificados digitales y claves privadas

Pasos iniciales

1- Abrimos la consola de windows en **modo administrador**.

2- Nos situamos en la carpeta "C:\Program Files\OpenVPN\easy-rsa"

cd c:\Program Files\OpenVPN\easy-rsa

3- Iniciamos la configuración de OpenVPN:

init-config

Ejecuta el comando (esto es opcional)

vars

Ejecutamos el comando para limpiar la posibles restos de instalaciones anteriores, y así comenzar de nuevo

clean-all

Creación de certificados y claves de la autoridad de certificación CA y del servidor

Creamos el certificado y clave privada de la autoridad de certificación (CA) (no será una real ya que esto cuesta dinero, pero nos vale perfectamente si nos creamos una inventada):

build-ca

- Nos pedirá que rellenemos los datos típicos de pais, localidad, nombre, etc… Como Common Name le vamos a poner por ejemplo "OpenVPN-CA":
  - Country Name (2 letter code) [US]: ES
    State or Province Name (full name) [CA]: CORU
    Locality Name (eg, city) [SanFrancisco]: CORU
    Organization Name (eg, company) [OpenVPN]: CIP
    Organizational Unit Name (eg, section) []: Informatica
    Common Name (eg, your name or your server's hostname) []:OpenVPN-CA
    Email Address [mail@host.domain]: pepe@cip.es

Ahora creamos el certificado digital y la clave privada del servidor VPN (se usará la CA que acabamos de crear para firmar los certificados:

build-key-server server

- Como siempre rellenamos los datos. Recomiendo que en **Common Name** le pongamos **server** y cuando te pida **sign the certificate** pulsamos en 'y' y cuando pida **commit** pulsemos también en 'y'

Creación de los certificados y claves de los clientes:

Para cada cliente tenemos que crear certificados y claves por ejemplo vamos a crear uno para un usuario llamado rosa.

build-key rosa-pc

- Cuando te lo pida en "Common Name" pondremos por ejemplo rosa-pc

Repetiremos este paso para tantos clientes se conecten a nuestro servidor VPN

Generamos los parámetros Diffie Hellman, esto es necesario para configurar correctamente la encriptación

build-dh

Configurando ficheros del cliente o servidor VPN

Navega hasta la carpeta C:\Program Files\OpenVPN\easy-rsa\keys

Veremos los siguientes ficheros:

- ca.crt = certificado de la autoridad de certificación CA
- ca.key = clave privada de la autoridad de certificación CA
- server.crt = certificado del servidor
- server.csr = petición de firma de certificado del servidor
- server.key = clave privada del servidor
- rosa.crt = certificado del cliente rosa
- rosa.csr = petición de firma de certificado del cliente rosa
- rosa.key = clave privada de rosa
- dn1024.pem = parámetros Diffie Hellman para la encriptación

En el servidor tendríamos que copiar en la carpeta C:\Program Files\OpenVPN\config

- ca.crt
- server.crt
- server.key
- dn1024.pem

En el cliente tendríamos que copiar en la carpeta C:\Program Files\OpenVPN\config

- ca.crt
- rosa.crt
- rosa.key

Copiamos los ficheros de ejemplo situados en la carpeta **C:\Program Files\OpenVPN\sample-config** en la carpeta **C:\Program Files\OpenVPN\config**

Edición del fichero configuración del servidor

Edita el fichero server.ovpn

ca "ca.crt"
cert "server.crt"
key "server.key"

dh "dh1024.pem"

Edición del fichero de configuración del cliente

Edita el fichero client.ovpn

ca "ca.crt"
cert "rosa-pc.crt"
key "rosa-pc.key"

Edita la linea 42

remote mi-servidor 1194

(donde mi-servidor será la ip publica de tu servidor)

Configurando el firewall y el router

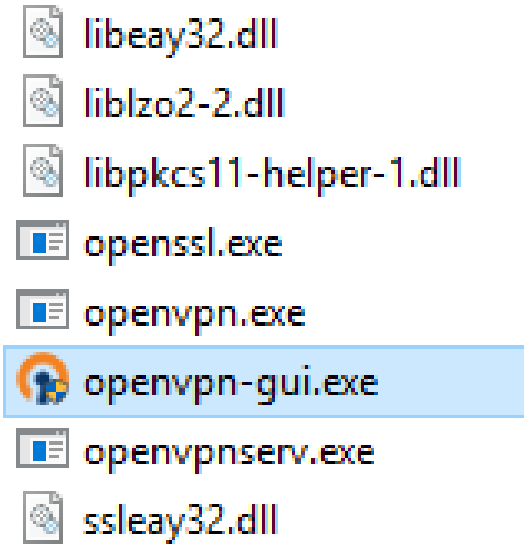
En nuestro servidor tendremos que abir el puerto UDP 1194 y en nuestro router redirigir las peticiones al puerto UDP 1194 a la ip donde tengamos montado el servidor VPN

Además será necesario que nuestra ip pública sea estática o usar en su defecto DDNS

También la ip privada del servidor VPN tendrá que ser estática

Arrancar GUI openVpn

Ejecutamos el openvpn-gui.exe



¿Cuáles son los usos de un VPN?

- **Acceso a una red de trabajo** mientras se está de viaje. Los VPNs se usan con frecuencia para aquellos profesionales que viajan y necesitan entrar en su red de trabajo mientras están lejos. Usar este método permite que los recursos se mantengan seguros porque en están en la nube.
- **Acceso a una red del hogar** mientras se está de viaje. También se puede usar para entrar al ordenador que hemos dejado en casa, como si estuviésemos usando una LAN (Local Network Area).
- **Esconde los datos de navegación**. Por ejemplo, si estás usando un Wi-Fi público, de esos que están disponibles sin contraseña en restaurantes y centros comerciales, todo lo que visites que no tenga conexión HTTPS estará visible para cualquiera que sepa dónde mirar. En cambio si tienes un VPN, lo único que podrán ver es la conexión al VPN; todo lo demás será anónimo.
- **Entrar en sitios con bloqueo geográfico**. Usualmente los problemas de bloqueo de región suelen pedir que estés en Estados Unidos. Esto sucede con Hulu, Pandora o el catálogo de Netflix que es más grande y completo en este país. A veces pasa también en ciertos vídeos de YouTube. Para evitar estas restricciones, sólo hay que usar un VPN que tenga localización de USA.
- **Evitar la censura en Internet**. Para aquellos gobiernos que deciden censurar ciertos sitios web, un VPN funciona muy bien para acceder a ellos sin problemas.

Otras opciones VPN

- TunnelBear
- Hola

Bibliografía

https://es.wikipedia.org/wiki/Red_privada_virtual
https://es.wikipedia.org/wiki/OpenVPN

Índice