Configuración de una VPN con Open VPN

Se entiende que ya está instalado OpenVpn Server

Paso de configuración inicial:

Debemos iniciar una ventana de DOS desde la opción ejecutar escribiendo CMD, luego debemos llegar hasta el directorio easy-rsa

C:\program files\OpenVpn\easy-rsa

Una vez ahí, ejecutaremos el siguiente comando

Init-config

Debido a que algunos datos se nos solicitaran varias veces cada vez que creemos un certificado podemos utilizar este paso (opcional) para setear esos valores con el fin de no escribirlos cada vez que creemos un certificado, Deberás ejecutar el siguiente comando (no se salga de la ventana donde se encuentra, desde ahí, ejecútelo)

notepad vars.bat

Asignaremos los siguientes campos en verde con sus propios datos, según los necesite su organización

set KEY_COUNTRY=**CL** (Este es el código de país)

set KEY_PROVINCE=**MT** (Su provincia o region)

set KEY_CITY=Santiago (Su Comuna)

set KEY_ORG=**BDT** (el nombre de su organizacion, use algo corto y fácil)

set KEY_EMAIL=**usuario@dominio.com** (su dirección de correo)

Una vez realizados los pasos anteriores solo debemos guardar y cerrar notepad y continuar con nuestra ventana de DOS, ahora debemos ejecutar 3 comandos uno seguido del otro respetando la forma de escritura indicada.

Este comando **build-ca** te solicitara los datos que ya hemos seteado anteriormente País, Estado, Ciudad, Organización, Departamento, Nombre del Servidor y Correo electrónico, estos valores los debes repetir durante todo el proceso cada vez que te los pida, debes tener extrema precaución con el **nombre host(hostname)** que cambiará en la parte de configuración de las llaves(certificados) del cliente y debe ser diferente para cada certificado, el paso opcional evita tener que escribir la mayoría de estos campos, solo deberás presionar ENTER cada que te los pida.

Debes estar atento ya que no todos los datos que te solicitara la creación del certificado los pudimos setear, por eso debes fijarte bien. El campo **organization unit name** deberá ser igual siempre para todos los certificados que crees.

Los comandos y el orden son los siguientes

---

vars
clean-all
build-ca

Con estos comandos lo que hemos hecho es crear un certificado de autoridad y se ha guardado en el directorio

C:\program files\open vpn\easy-rsa\keys

Ahora debemos crear la llave privada y el certificado de nuestro servidor, esto lo realizaremos ejecutando 2 comandos uno seguido del otro respetando la forma de escritura, siempre desde nuestra ventana de DOS.

---

vars
build-key-server (aquí el nombre del servidor)

En donde dice aquí el nombre del servidor, debes dar un nombre a tu servidor por ejemplo **servidor-vpn** debes omitir los paréntesis, ósea quedaría de la siguiente manera.

build-key-server servidor-vpn

y presionas ENTER, recuerda que en cada línea que terminas de escribir debes presionar ENTER

Una vez presiones ENTER este comando te pedirá completar los campos ya nombrados te pedirá asignar una clave (**muy importante que no debes perder**) y hará dos preguntas a las que debes contestar que si presionando la letra **Y** (yes)

Ya terminado ese proceso debe aparecer un mensaje como este

Write out database with 1 new entries
Data Base Updated
unable to write 'random state'

Y ahora siempre desde nuestra ventana de DOS ejecutaremos el siguiente comando

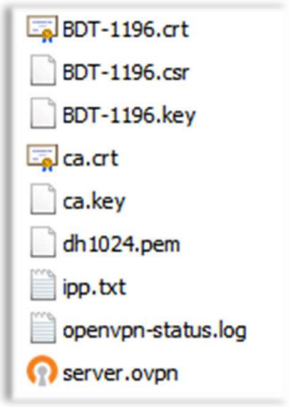
---

build-dh

Aquí debes esperar que termine de crear puntos y que te muestre el cursos parpadeando nuevamente en. (puede demorar)

C:\program files\openvpn\easy-rsa

Básicamente hasta aquí el servidor ya está instalado, los archivos que se deben copiar a la carpeta **CONFIG** son los 6 primeros:



Los nombres claramente cambiaran según ustedes hallan elegido los propios, no deben ser igual a los que se muestran en la imagen a excepción de 3.

- ✓ ca.crt
- ✓ ca.key
- ✓ dh1024.pem

Los archivos ipp.txt y openvpn-status.log no se crean en este proceso que hemos revisado arriba, aparecerán automáticamente cuando arranca el servicio de OpenVpn.

El archivo **server.ovpn** es el que veremos ahora, en verde estará la opción que deben activar, lo demás debe quedar tal cual aparece en el archivo, si usted desea realizar otro tipo de configuración o experimentar con OpenVpn, podrá hacer usos de ellas. He dejado el encabezado o primera línea de algunas opciones para no hacer tan extenso el archivo, debes ubicarlas en tu configuración.

Archivo de configuración servidor OpenVpn

Which TCP/UDP port should OpenVPN listen on?
port 1194

TCP or UDP server?
proto tcp
;proto udp

the firewall for the TUN/TAP interface.
;dev tap
dev tun

Windows needs the TAP-Win32 adapter name
#Vease procesos de creacion de TAP
dev-node **TAP-1** (**usted coloca el nombre que necesite aquí**)

SSL/TLS root certificate (ca), certificate
ca **ca.crt**
cert **BDT-1196.crt**
key **BDT-1196.key** # This file should be kept secret

Diffie hellman parameters
dh **dh1024.pem**

Configure server mode and supply a VPN subnet
server **10.10.7.0 255.255.255.0** (**usted coloca la red que necesite aquí**)

Maintain a record of client <-> virtual IP address
ifconfig-pool-persist ipp.txt

Push routes to the client to allow it
push "route 192.168.0.104 255.255.255.255" (esto es opcional y segun la red que usted necesite)

Uncomment this directive to allow different
clients to be able to "see" each other.
client-to-client

Select a cryptographic cipher.
cipher BF-CBC # Blowfish (default)

Una vez haya terminado de configurar su archive, debe guardarlo en la carpeta, con la extensión ovpn **no txt**

C:\program files\openvpn\config

Como se muestra en la imagen anterior.

Revocar un certificado

```
# ESTA LINEA PERMITE VALIDAR LOS CERTIFICADOS CADUCADOS O DADOS DE BAJA
crl-verify crl.pem
```

Debe estar des-comentada **sin** el símbolo # delante, si el símbolo está presente aunque se haya revocado satisfactoriamente un certificado, la revocación no tendrá efecto.

Para revocar un certificado debemos ir desde nuestra ventana de DOS a:

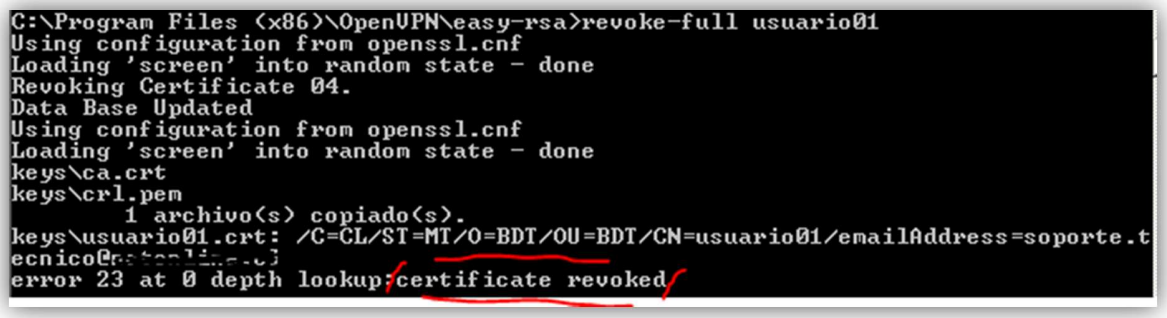
C:\program files\openvpn\easy-rsa

Una vez estemos ahí debemos ejecutar los siguientes comandos

---

vars
revoke-full (nombre del certificado cliente)

Si todo ha salido bien, debe mostrar un mensaje como este



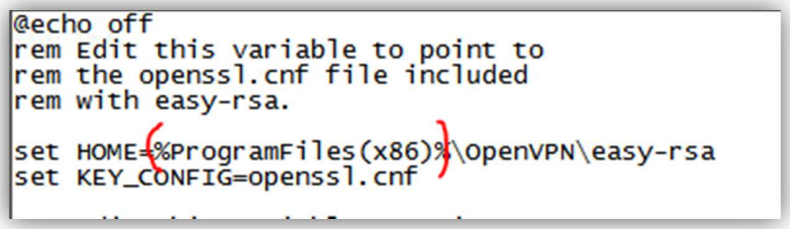
El error 23 nos indica que el certificado no se pudo validar, por lo que la revocación fue exitosa.

Nota:

Aquí puede suceder que debido al nombre de la carpeta que se usó para la instalación de OpenVpn en c:\ necesites hacer un cambio, si te aparece instalado dentro de Program Files (x86) ó Archivos de programa (x86) deberás hacer un cambio en el archivo vars.bat.

Para hacer este cambio, busca el archivo dentro de la carpeta easy-rsa de tu instalación de OpenVpn y haz clic con el botón derecho sobre él y selecciona EDITAR

Se abrirá un bloc de notas con los comandos del archivo vars.bat, debes realizar la modificación según se muestra en la imagen.



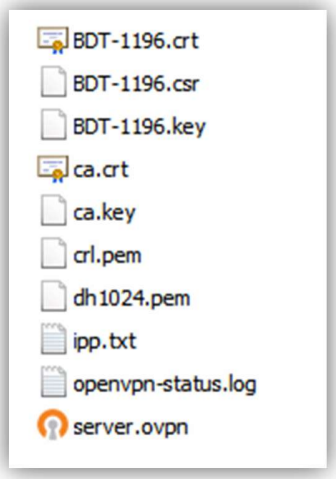
Si tu instalación de OpenVpn se efectuó en Program Files (x86) ó Archivos de programa (x86) debes dejarlo así, la instalación por defecto usa %ProgramFiles%

Y presionas, Archivo/Guardar, esto solucionara el error que aparece cuando el comando revoke-full no encuentra la ruta correcta.

La revocación genera un archivo llamado **crl.pem** este archivo es creado en el directorio C:\program files (x86)\openvpn\easy-rsa\keys y debe ser copiado a la carpeta de configuración del servidor OpenVpn, en este caso

C:\program files (x86)\openvpn\config

Y deberá ser vuelto a copiar cada vez que revoques un certificado.
Según pruebas realizadas el archivo **crl.pem** también puede quedar en el directorio **keys** lo que permitiría no tener que hacer la copia del archivo a la carpeta configuración cada vez que se revoque un archivo, idealmente realicen sus propias pruebas de funcionamiento de esta función ya que no todas las instalaciones son iguales.



En teoría los archivos que deberían quedar en nuestra carpeta CONFIG deberían ser los que ven en la imagen de la izquierda, lógicamente, los nombres cambiaran.

Otro problema común que se presenta en Windows es al momento de realizar el push route a direcciones IP de equipos específicos dentro de la red, la solución existe pero es algo laboriosa, se debe comenzar activado el reenvío de TCP/IP y esto lo haremos desde regedit.

Primero iremos a **incio/ejecutar** y escribiremos **regedit** y buscaremos esta línea

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Y deberemos modificar el siguiente valor

Nombre de valor: IPEnableRouter
Tipo de valor: REG_DWORD
Información del valor: 1 (este debería aparecer en 0 se debe cambiar a 1)

El valor 1 habilita el reenvío de TCP/IP para todas las conexiones de red instaladas y utilizadas por este equipo.

Una vez hecho el cambio, cierre el Editor de registro, cierre todo lo que tenga abierto y reinicie el equipo.

Hasta aquí la configuración del servidor estaría completa, como comente anteriormente puedes probar tus propias configuraciones pero si has seguido los pasos como se indican arriba deberías tener tu servidor funcionando correctamente.

Ahora veremos, **Equipos clientes y servidores en la red.**