

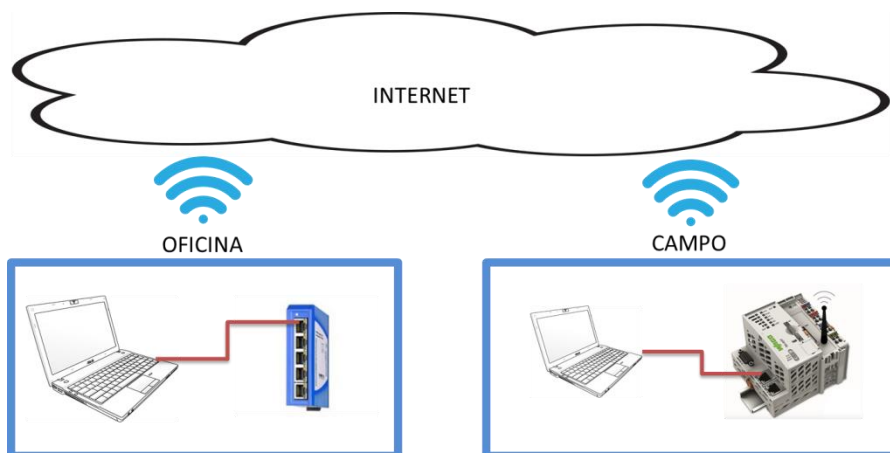
Crear y montar una red VPN para comunicación remota

ÍNDICE

Introducción	3
Crear los archivos de la VPN en Windows.....	5
Instalación de OpenVPN.....	5
Creación de los certificados necesarios para la VPN.....	6
Modificación archivos vars.bat	8
Creación de la clave Diffie-Hellman	9
Creación de la autoridad de certificación	10
Creación de los archivos para clientes y servidor	11
Configurar OpenVPN para usar los certificados.....	14
Firewall de Windows	17
Convertir los certificados creados en Windows para su uso en Linux	21
Instalación de certificados en PFC200.....	21
Apéndices	24
Crear Servidor DNS.....	24

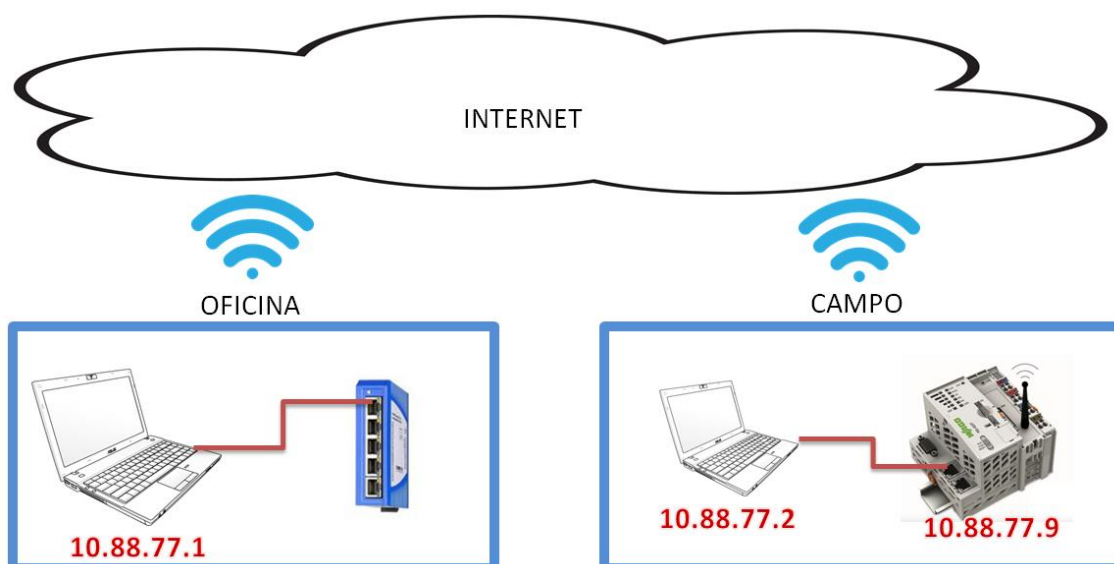
Introducción

En muchas ocasiones necesitamos acceder de manera remota a un equipo, o conectarnos a nuestro servidor desde fuera de nuestra oficina. Para realizar esto, tenemos varias opciones, pero la más eficiente y económica es crear una red VPN (Virtual Private Network).



Utilizando como guía el esquema anterior, nuestra idea sería comunicar con el PLC o el equipo instalado en campo, para poder realizar programaciones o guardar datos de manera remota. En este caso, nuestro proveedor de internet, debería suministrarnos una tarjeta SIM con IP fija, para poder conectarnos a ella y así acceder a nuestros equipos de campo.

En nuestra instalación demo, vamos a optar por crear una red para mantenerlos conectados, pero que a la vez sea segura.



Para la demo, nosotros vamos a utilizar una red cableada, por lo que evitaremos el uso de una tarjeta SIM con IP fija, aunque sí tenemos que referenciar nuestra red a un punto fijo, en el que instalaremos nuestro servidor VPN.

Esto se puede conseguir mediante una DNS fija (*El sistema de nombres de dominio (DNS, por sus siglas en inglés, Domain Name System) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada*), o una dirección IP fija. Al final de este documento, agregaremos un apéndice, para la creación de una DNS de manera gratuita.

Para crear una red VPN, necesitamos disponer de un servidor, que instalaremos en nuestra IP fija, o al que redireccionaremos nuestra DNS, y el número de clientes deseado.

En el servidor gestionaremos los derechos de la red, y es el que tendrá que estar encendido siempre, para que todos los clientes se conecten a él.

Cada cliente dispondrá de su propia dirección IP, permitiéndole comunicarse con el servidor, y con cada uno de los clientes conectados a la red.

En función del equipo conectado, si está basado en Windows o en Linux, los certificados varían, debido a su distribución. Por este motivo, para certificados creados en Windows/Linux, si se quieren utilizar en un equipo con el otro sistema operativo, es necesario realizar una modificación.

A continuación, vamos a explicar cómo crear y modificar todos los archivos que vamos a necesitar para nuestra VPN.

Crear los archivos de la VPN en Windows

Para crear una VPN existen varios software en el mercado que podemos utilizar. Nosotros utilizaremos el software OpenVPN, gratuito y ampliamente extendido.

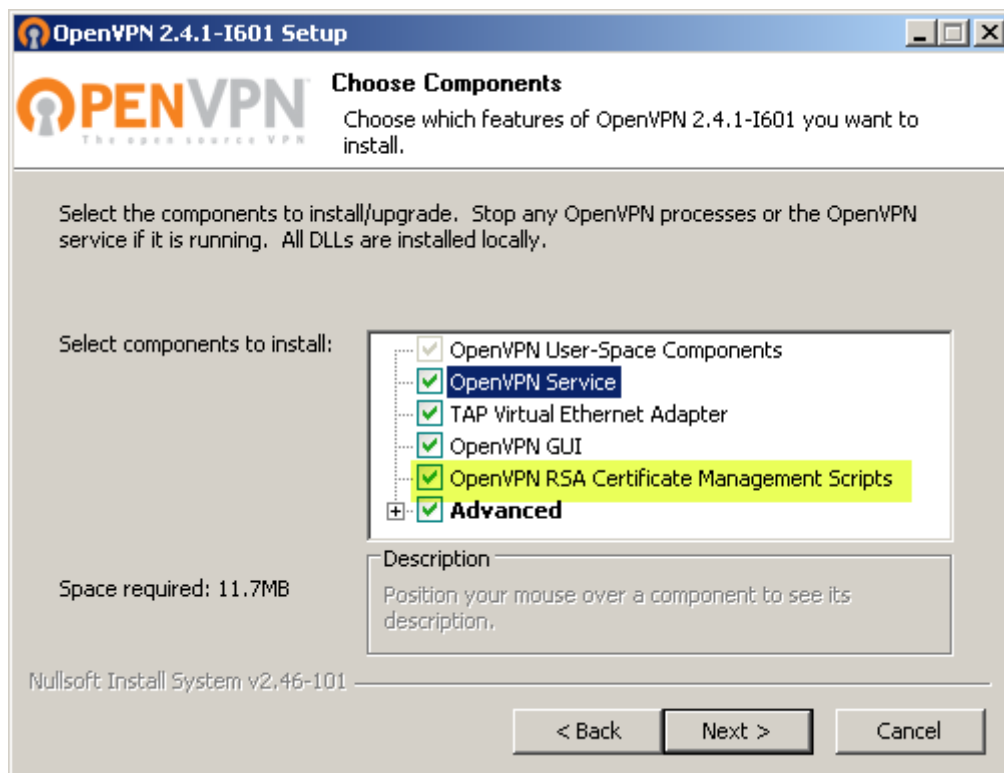
Los pasos a seguir para la instalación y generación de certificados son sencillos. En función del sistema operativo con el que vamos a trabajar, el proceso puede variar. Nosotros vamos a trabajar con Windows, y vamos a realizar un cambio para comunicar con Linux. Nuestras cabeceras trabajan sobre Linux, por lo que es necesario crear/modificar los archivos de configuración en Linux.

Instalación de OpenVPN

El primer paso, es descargar el software de su página web:

<https://openvpn.net/index.php/open-source/downloads.html>

Durante la instalación, nos dará la opción de elegir que componentes instalar. Es importante marcar las opciones resaltadas en amarillo, para poder crear certificados. Posteriormente nos aparecerá una ventana emergente, que nos indicará si permitimos la instalación del TAP-Adapter. Debemos aceptar, pues es el adaptador de red a través del que nos conectaremos a la red VPN.

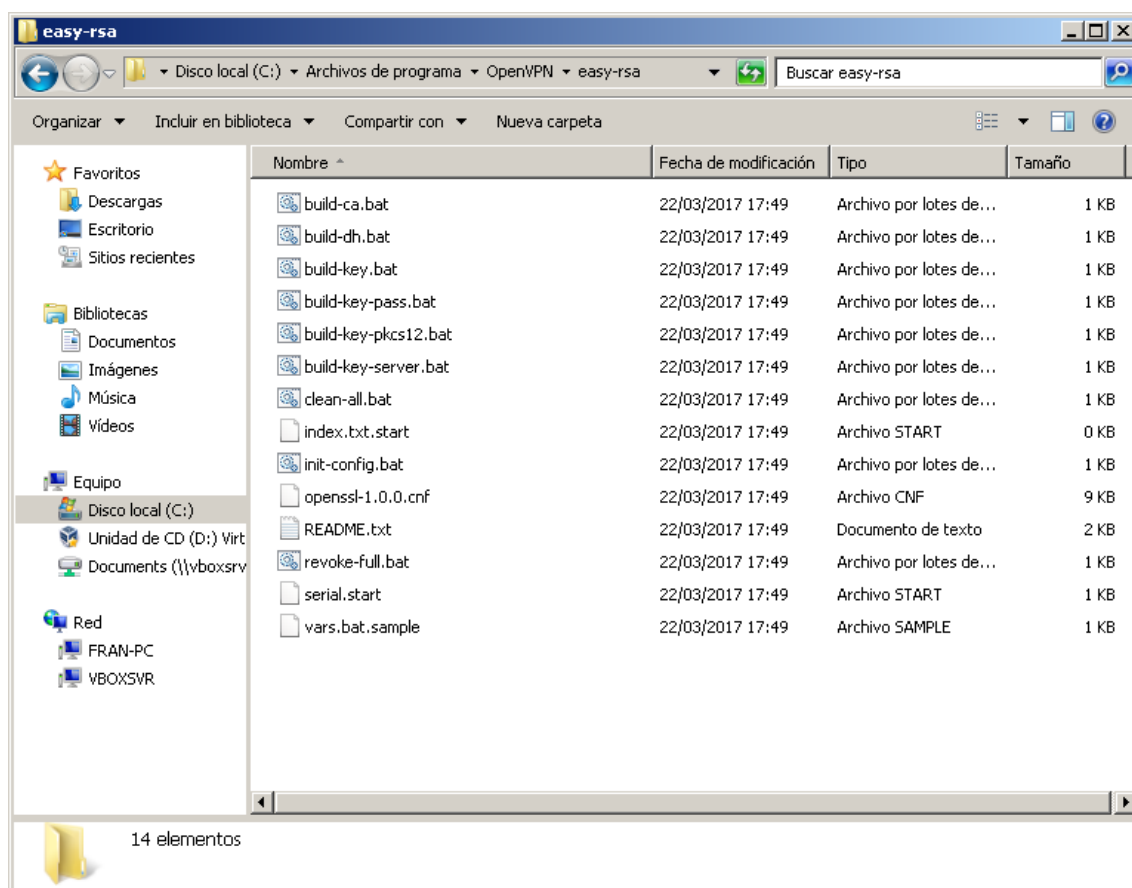


Creación de los certificados necesarios para la VPN

Para poder crear nuestros certificados tanto para el servidor como los clientes, necesitamos generar unas claves para que los elementos del túnel puedan acreditarse y así generar conexiones seguras. Los pasos que tenemos que seguir son:

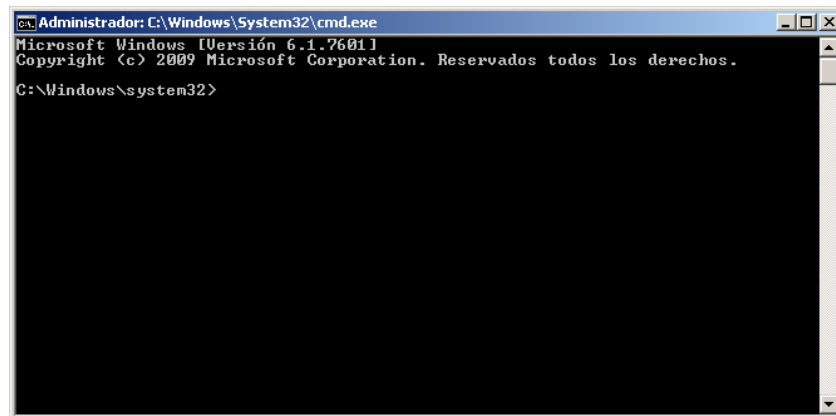
1. Crear el certificado CA para que la CA (Certification Authority) pueda firmar y revocar los certificados de los clientes.
2. Crear una clave y un certificado para los clientes.
3. Firmar la petición de los certificados usando el certificado CA, haciéndolas válidas.
4. Asignar las claves y los certificados a los diferentes equipos que van a estar en la VPN.
5. Modificar la configuración de OpenVPN para que use los certificados y las claves creadas.

Para la creación de estos documentos, vamos a utilizar las herramientas que nos aporta OpenVPN, easy-rsa. Si abrimos la dirección de instalación de OpenVPN, tenemos una carpeta con todas las herramientas necesarias.

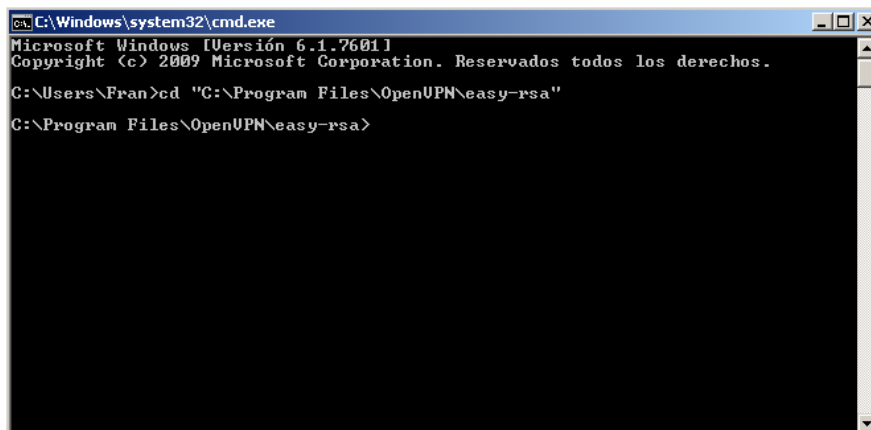


Primer paso para la creación de los certificados es crear una nueva carpeta en esta dirección y nombrarla como “keys”, y copiar los archivos “serial.start” e “index.txt.start”, renombrándolos, quitando la terminación .start.

La manera más sencilla para el arranque de estos programas, es abrir una ventana de símbolo del sistema. Para ello, vamos a inicio, y en el buscador que nos ofrece, buscamos “cmd”. Hacemos click derecho, e iniciamos como administradores.



El primer paso, será dirigirnos a nuestra carpeta “easy-rsa” dentro de la ventana de símbolo del sistema, con el comando cd. Para ello, escribimos la dirección de la carpeta: cd “C:\Program Files\OpenVPN\easy-rsa”. (Nota: la ruta puede variar en función de la carpeta donde se haya instalado OpenVPN)



Una vez localizados en la carpeta, iniciamos el archivo “init-config.bat”:

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

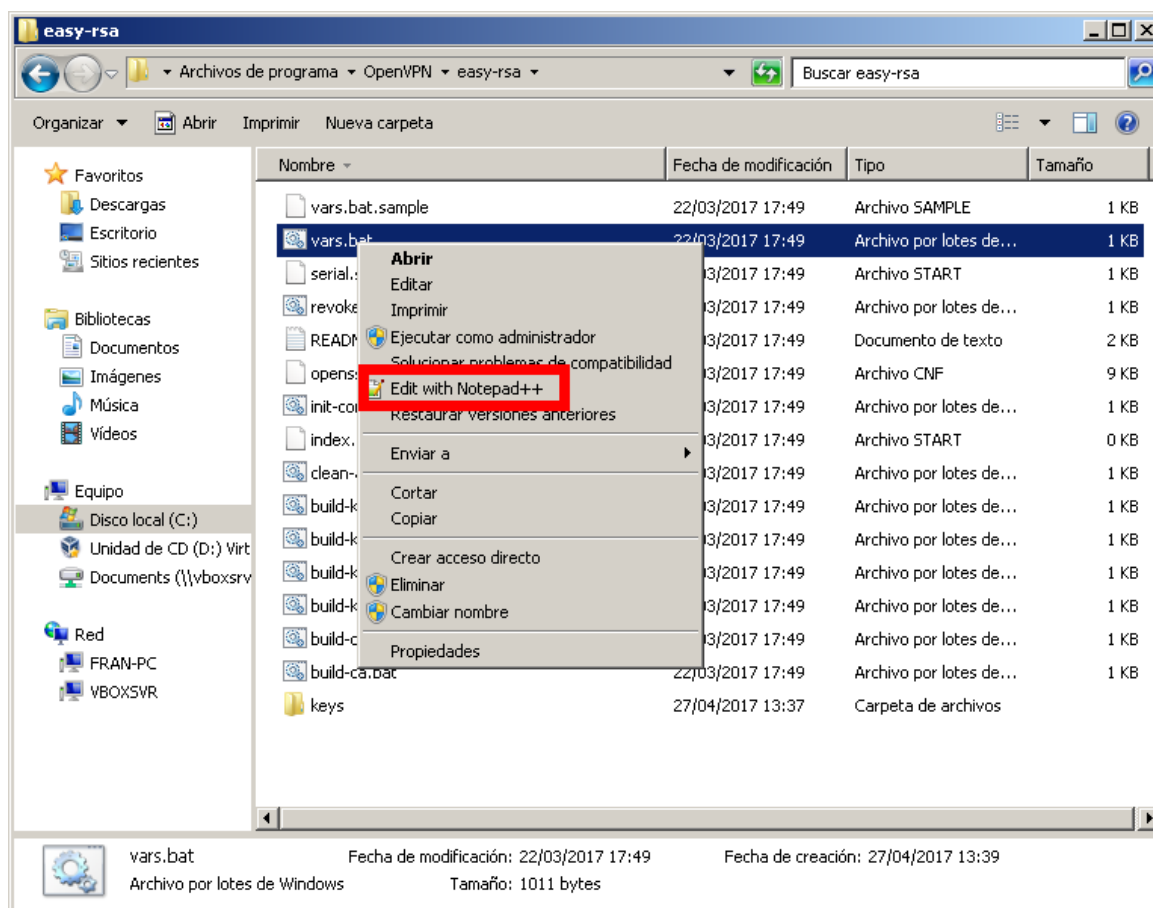
Este comando nos copia la plantilla del archivo “vars.bat.sample” al archivo “vars.bat”.

Modificación archivos vars.bat

En este archivo “vars.bat”, tenemos que realizar una serie de modificaciones, unos necesarios para crear nuestros certificados, y otros que nos ahorrarán trabajo a la hora de crearlos. Para modificarlo, pulsamos con el botón derecho, y abrimos con nuestro editor de texto (en mi caso lo editaré con el software *Notepad++*, pero puede utilizarse cualquier editor, incluido *Bloc de Notas*).

En este archivo, debemos modificar los siguientes valores, para asegurar que nuestro sistema está bien direccionado:

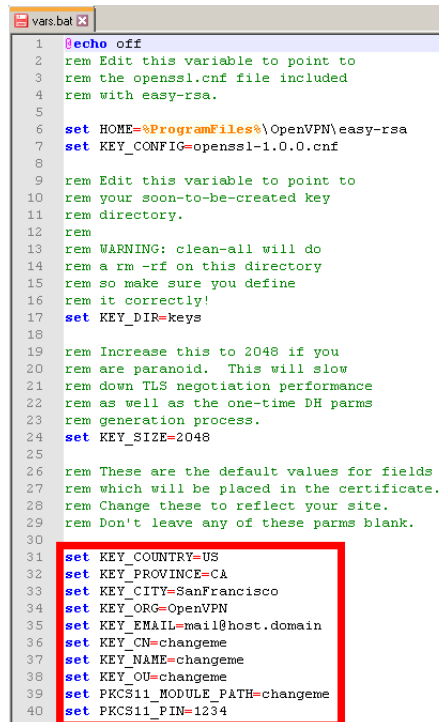
```
set HOME=%ProgramFiles%\OpenVPN\easy-rsa
set KEY_CONFIG=openssl-1.0.0.cnf
set KEY_DIR=keys
set KEY_SIZE=2048
```



La línea “set KEY_SIZE=2048”, por defecto está seleccionado 1024, y es aconsejable seleccionar 2048, para aumentar nuestro nivel de seguridad.

Las variables marcadas no afectan a la funcionalidad, pero si las modificamos, a la hora de crear nuestros archivos, nos ahorrará trabajo. En nuestro caso:

set KEY_COUNTRY=ES	(País)
set KEY_PROVINCE=MA	(Provincia)
set KEY_CITY=Alcobendas	(Ciudad)
set KEY_ORG=Dicomat	(Organización)
set KEY_EMAIL=ingenieria@dicomat-asetyc.com	(Correo email)



```

1  @echo off
2  rem Edit this variable to point to
3  rem the openssl.cnf file included
4  rem with easy-rsa.
5
6  set HOME=%ProgramFiles%\OpenVPN\easy-rsa
7  set KEY_CONFIG=openssl-1.0.0.cnf
8
9  rem Edit this variable to point to
10 rem your soon-to-be-created key
11 rem directory.
12 rem
13 rem WARNING: clean-all will do
14 rem a rm -rf on this directory
15 rem so make sure you define
16 rem it correctly!
17 set KEY_DIR=keys
18
19 rem Increase this to 2048 if you
20 rem are paranoid. This will slow
21 rem down TLS negotiation performance
22 rem as well as the one-time DH parms
23 rem generation process.
24 set KEY_SIZE=2048
25
26 rem These are the default values for fields
27 rem which will be placed in the certificate.
28 rem Change these to reflect your site.
29 rem Don't leave any of these parms blank.
30
31 set KEY_COUNTRY=US
32 set KEY_PROVINCE=CA
33 set KEY_CITY=SanFrancisco
34 set KEY_ORG=OpenVPN
35 set KEY_EMAIL=mail@host.domain
36 set KEY_CN=changeme
37 set KEY_NAME=changeme
38 set KEY_OU=changeme
39 set PKCS11_MODULE_PATH=changeme
40 set PKCS11_PIN=1234
  
```

Una vez modificado el archivo, guardamos y ejecutamos “vars.bat” del mismo modo que hicimos con “init-config.bat”.

```
C:\Program Files\OpenVPN\easy-rsa>vars.bat
```

Creación de la clave Diffie-Hellman

Para permitir la comunicación segura y secreta, OpenVPN utiliza un algoritmo matemático para generar una clave que asegurará que sólo hablen entre ellos aquellos equipos que conozcan la clave precompartida.

OpenVPN pone a nuestra disposición el comando para crear este archivo, “build-dh.bat”. Esta creación puede tomar un poco de tiempo.

Aunque nos salga el siguiente mensaje: “WARNING: can’t open config file: /etc/ssl/openssl.cnf”, la creación funciona sin problemas.

Avd. de la Industria, 36

28108 Alcobendas (Madrid)

www.dicomat-asetyc.com

Teléfono: 902 99 2015

ingenieria@dicomat-asetyc.com

Francisco Moreno

Mayo 2017

[illegible]

Creación de la autoridad de certificación

Para generarla, llamamos a la función “build-ca.bat”. Este certificado lo utilizaremos para firmar todos los certificados de los clientes y así autenticar las máquinas. Dependiendo de lo que hayamos cambiado en “vars.bat”, nos sugerirán unos parámetros u otros.

```
C:\Program Files\OpenUPN\easy-rsa>build-ca.bat
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating a 2048 bit 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) [Alcobendas]:
Organization Name (eg, company) [Dicomat]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]:SERVER-DICOMAT
Name [changeme]:
Email Address [ingenieria@dicomat-asetyc.com]:
```

Como se puede apreciar, las variables que predefiní en el archivo “vars.bat”, aparecen como la opción por defecto. Sólo habría que pulsar *Enter* para pasar a la siguiente. Si se quiere modificar, escribiríamos el nombre que quisiéramos.

Este comando nos crea los archivos “ca.crt” y “ca.key”. El comando “build-dh.bat” creó el archivo “dh2048.pem” (si no hemos modificado este valor, por defecto obtendremos “dh1024.pem”).

Creación de los archivos para clientes y servidor

El primer paso será crear los archivos para nuestro servidor. Para ello, utilizaremos el comando “build-key-server.bat VPN-Server”, siendo *VPN-Server* el nombre de nuestro servidor elegido.

De nuevo, si hemos modificado el archivo “vars.bat”, nos ahorraremos tiempo a la hora de rellenar los campos. El campo importante, es **Common Name**. En este campo debemos ser muy específicos, y agregar un nombre característico a nuestro servidor, en nuestro caso *VPN-Server*.

Después de estos datos, nos da la opción de agregar una contraseña, que sería requerida cada vez que se solicitase el uso de los certificados. De todos modos, si se agrega una contraseña aquí, nadie podrá conectarse con el servidor sin esta contraseña.

```
C:\Program Files\OpenVPN\easy-rsa>build-key-server.bat VPN-Server
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating a 2048 bit RSA private key
.....+++
writing new private key to 'keys\VPN-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) [ES]:
State or Province Name (full name) [MA]:
Locality Name (eg, city) [Alcobendas]:
Organization Name (eg, company) [Dicomat]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme:VPN-Server
Name [changeme]:
Email Address [ingenieria@dicomat-asetyc.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
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:'Alcobendas'
organizationName        :PRINTABLE:'Dicomat'
organizationalUnitName  :PRINTABLE:'changeme'
commonName              :PRINTABLE:'VPN-Server'
name                   :PRINTABLE:'changeme'
emailAddress            :IA5STRING:'ingenieria@dicomat-asetyc.com'
Certificate is to be certified until Apr 25 14:37:36 2027 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
```

A la pregunta de si queremos que se firmen los certificados, debemos responder “Sí” (marcaremos “y” en ambas ocasiones).

Para crear el cliente, realizaremos el mismo procedimiento, llamando a la función “build-key.bat VPN-Client”. En este caso, crearemos el cliente *VPN-Client*. Es importante darle el nombre en la casilla “**commonName**”.

```
C:\Archivos de programa\OpenVPN\easy-rsa>vars.bat

C:\Archivos de programa\OpenVPN\easy-rsa>build-key.bat VPN-Client
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'keys\VPN-Client.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) [Alcobendas]:
Organization Name (eg, company) [Dicomat]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]:VPN-Client
Name [changeme]:
Email Address [ingenieria@dicomat-asetyc.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
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:'Alcobendas'
organizationName        :PRINTABLE:'Dicomat'
organizationalUnitName  :PRINTABLE:'changeme'
commonName              :PRINTABLE:'VPN-Client'
name                   :PRINTABLE:'changeme'
emailAddress            :IA5STRING:'ingenieria@dicomat-asetyc.com'
Certificate is to be certified until Apr 26 06:16:37 2027 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

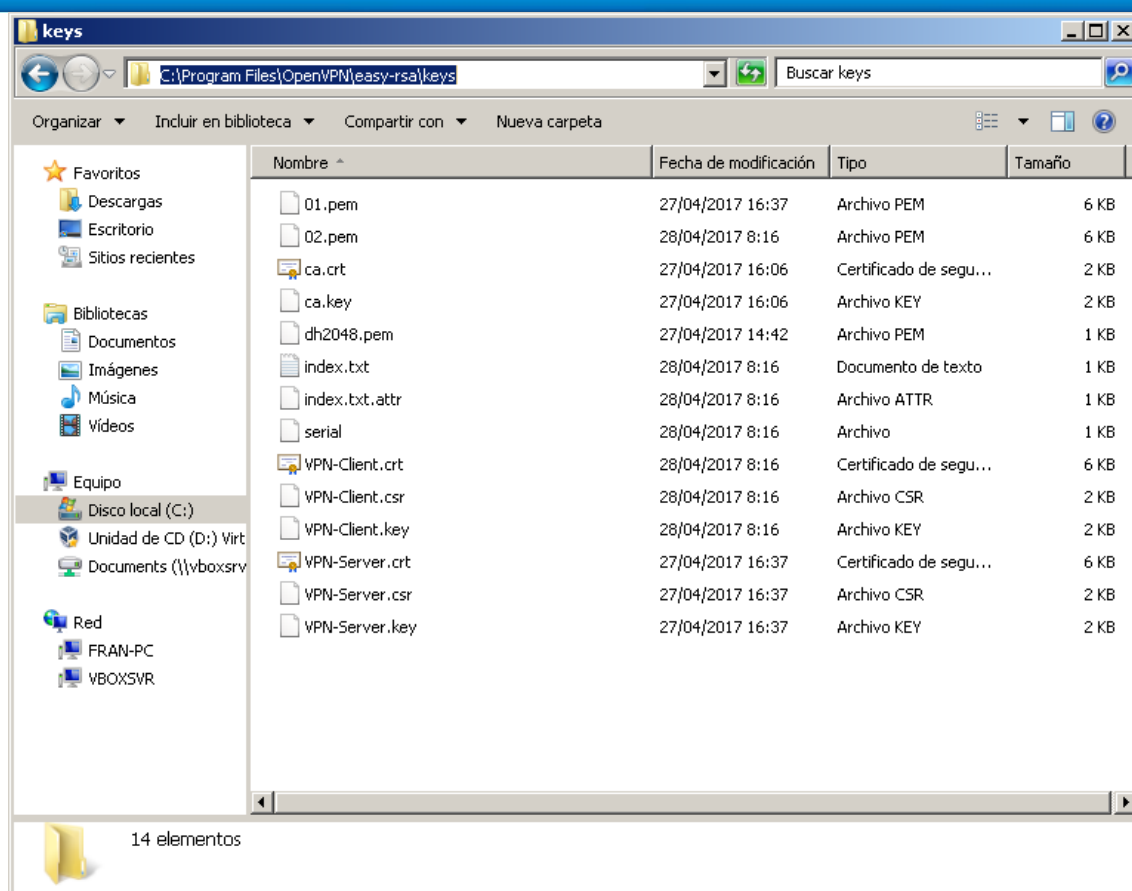
C:\Program Files\OpenVPN\easy-rsa>
```

Repitiendo este proceso, y variando el nombre de los clientes, podemos crear todos los certificados que queramos.

NOTA:

Si una vez terminado el proceso, y pasado el tiempo, necesitamos crear nuevos certificados, deberemos utilizar este mismo proceso, pero agregando primero la línea “vars.bat”, y posteriormente “build-key.bat VPN-Client”. Es importante que las claves se encuentren alojadas en la carpeta que creamos (en nuestro ejemplo, C:\Archivos de programa\OpenVPN\easy-rsa\keys, para que el software las pueda localizar).

Si vamos a nuestra carpeta donde tenemos las claves creadas (C:\Archivos de programa\OpenVPN\easy-rsa en nuestro caso), podremos ver todos los certificados creados, tanto los de servidor como los de clientes:



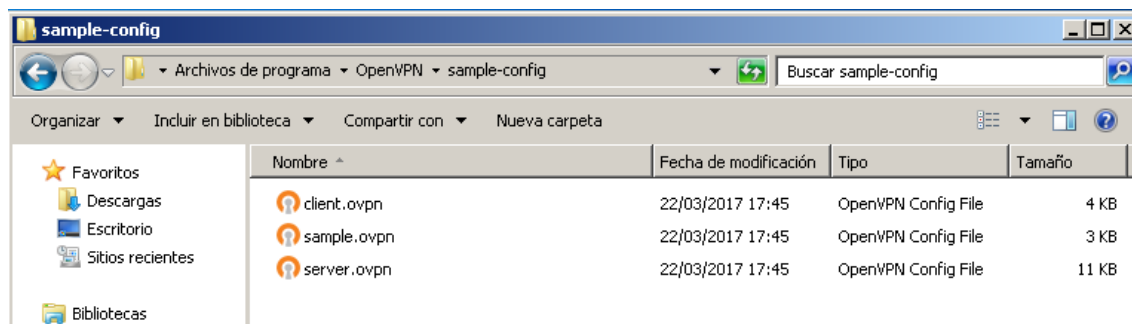
Ahora debemos transferir estos certificados a nuestro cliente y nuestro servidor. Los certificados deben transferirse de manera segura, evitando el envío directo por correo, que pueda modificar nuestras claves. Estos certificados deben de distribuirse de la siguiente forma:

Archivo	Localización
VPN-Server.crt	En el VPN-Server
VPN-Server.key	En el VPN-Server
VPN-Server.csr	Se puede eliminar
VPN-Client.crt	En el VPN-Client
VPN-Client-key	En el VPN-Client
VPN-Client.csr	Se puede eliminar
ca.crt	Debe estar disponible en ambos equipos
ca.key	Debe mantenerse secreto, sólo en la CA, ya que permite la creación de certificados firmados para entrar a nuestra red.
dm2048.pem	Debe estar disponible en ambos equipos

Estos archivos deben copiarse en la dirección C:\Archivos de programa\OpenVPN\config\keys

Configurar OpenVPN para usar los certificados

OpenVPN nos ofrece también los archivos de configuración por defecto, para realizar una comunicación rápida. Podemos encontrarlos en la dirección C:\Archivos de programa\OpenVPN\sample-config.



NOTA:

En nuestro caso, suministramos un archivo de configuración, con las características principales, que puede modificarse para ser tanto maestro como esclavo, y que dispone de varias opciones adicionales, comentadas para que puedan activarse si se quiere.

Para editar el archivo de configuración, necesitamos un editor de texto (en nuestro caso utilizaremos Notepad++) y modificar las variables que consideremos.

```

1 #####
2 #####
3 #####
4 ##### Archivo configuración #####
5 ##### VPN-DICOMAT #####
6 #####
7 #####
8 #####
9
10 ## Este archivo se puede modificar mediante editor
11 ## de texto, debe ser nombrado .ovpn para Windows,
12 ## y .conf para Linux. Con este archivo, OpenVPN
13 ## se activará de forma correcta.
14
15 ## Se dejan las líneas principales descomentadas.
16 ## Comentar o descomentar en función de las caracte-
17 ## rísticas a seleccionar.
18
19
20 # remote.- apunta hacia el otro extremo de nuestro
21 # tunel VPN. Si el certificado vamos a usarlo para
22 # el servidor, se puede dejar la línea comentada,
23 # y estaría configurado en modo servidor, sólo
24 # escuchando.
25
26 # Para el cliente, habría que cambiar 'myremote'
27 # por nuestro host remoto. Puede ser una IP fija o
28 # un servidor DNS.
29 remote myremote
30
31
32 # port.- Para utilizar un puerto en concreto, descomentar
33 # la línea. El puerto por defecto para UDP es 1194.
34 # El puerto seleccionado, debe ser redireccionado en
35 # el router a la dirección del servidor.
36 ; port 1194
37
38
39 # proto.- Elegir uno de los 3 protocolos soportados por
40 # OpenVPN. Si se deja comentado, por defecto será udp

```

Salvo las líneas básicas de configuración, el resto de líneas se encuentran comentadas, para que el usuario se encargue de elegir las que considere oportunas.

La configuración básica a utilizar para el servidor sería la compuesta por las siguientes opciones:

```
dev tap
ifconfig 10.3.0.1 255.255.255.0
tls-server
dh keys/dh2048.pem
ca keys/ca.crt
cert keys/VPN-Server.crt
key keys/VPN-Server.key
```

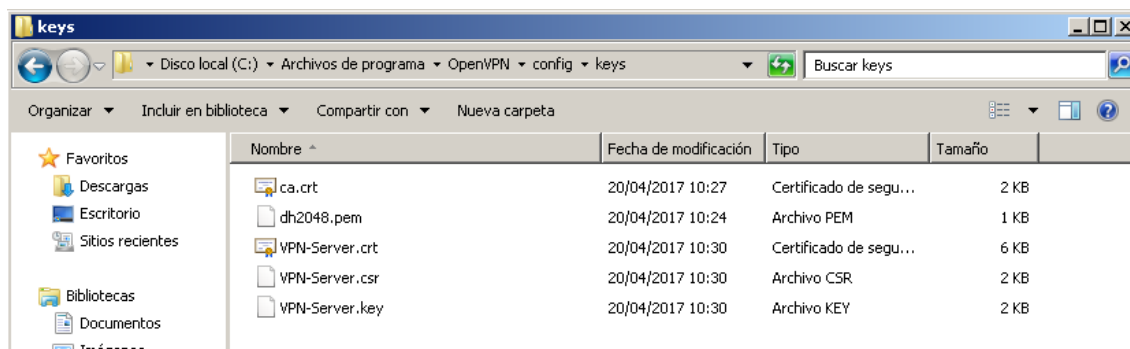
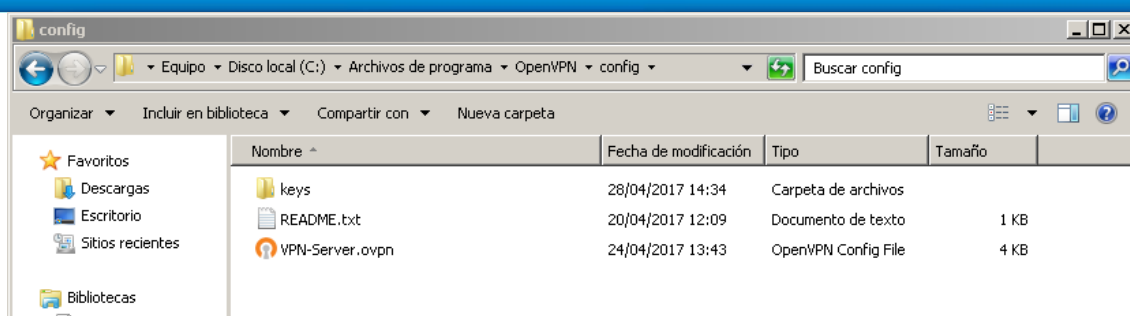
Y para el cliente:

```
remote 10.10.10.103
dev tap
tls-client
ifconfig 10.3.0.2 255.255.255.0
dh keys/dh2048.pem
ca keys/ca.crt
cert keys/VPN-Client.crt
key keys/VPN-Client.key
```

Al igual que hicimos con las claves, debemos copiar este archivo a la carpeta C:\Archivos de programa\OpenVPN\config. Dependiendo de la configuración elegida para crear este archivo, la disposición de las claves puede variar. En nuestro caso, utilizaremos nuestra plantilla:

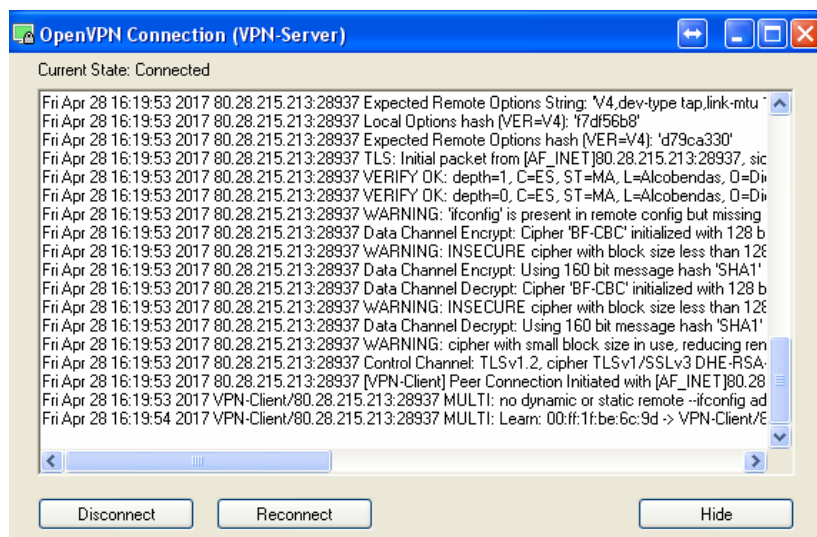
```
143 # dh.- Define la clave Deffie-Hellmann a usar
144 dh keys/dh2048.pem
145
146
147 # ca.- Define el certificado CA a usar
148 ca keys/ca.crt
149
150
151 # cert.- Define el certificado de la máquina
152 # local
153 cert keys/VPN-Client.crt
154
155
156 # key.- Define la clave de la máquina local
157 key keys/VPN-Client.key
```

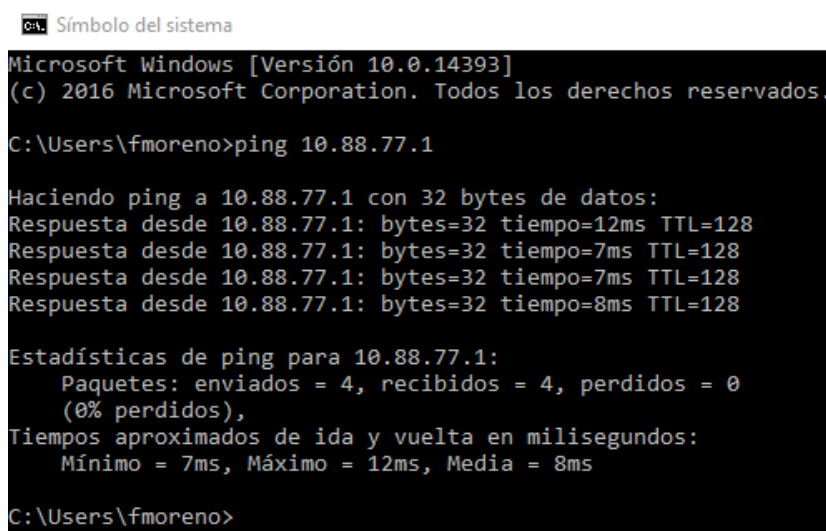
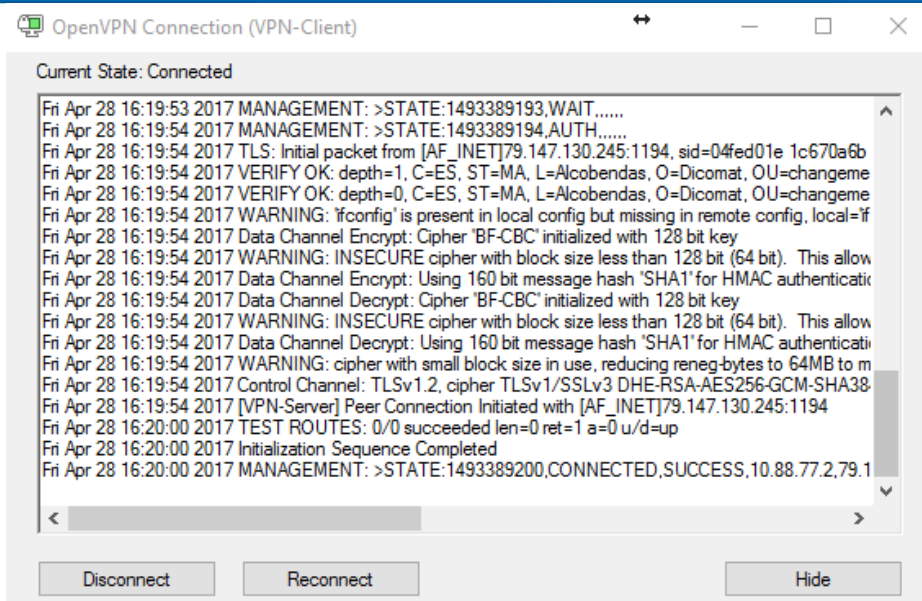
De este modo, indicamos que nuestras claves se encuentran en la carpeta keys, en la misma dirección que nuestro archivo de configuración:



Una vez que tenemos nuestros archivos en la posición correcta, sólo nos falta iniciar el servidor y el cliente. Es importante iniciar OpenVPN con derechos de administrador, para que pueda iniciarse correctamente. Tanto en el servidor como en el cliente.

Para comprobar la conexión, es tan sencillo como realizar un ping, tal y como vemos a continuación. En nuestra red de prueba, hemos seleccionado las IP 10.88.77.XX.



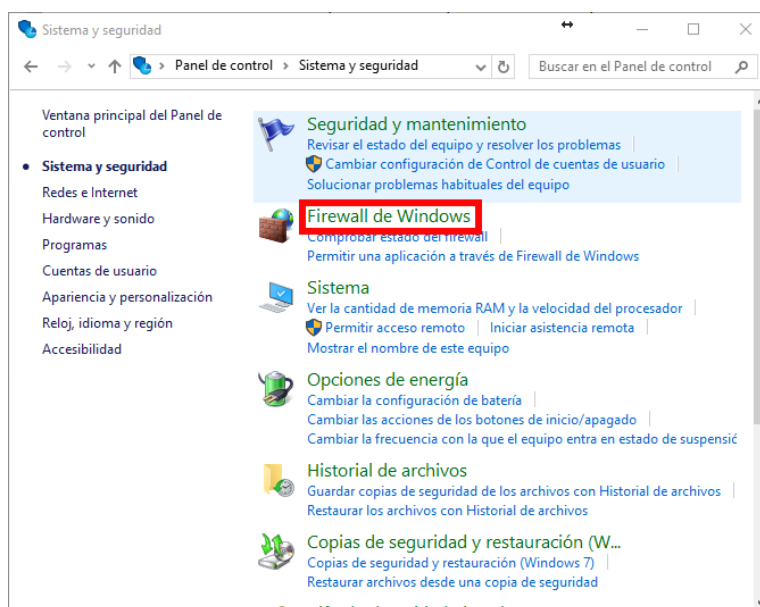
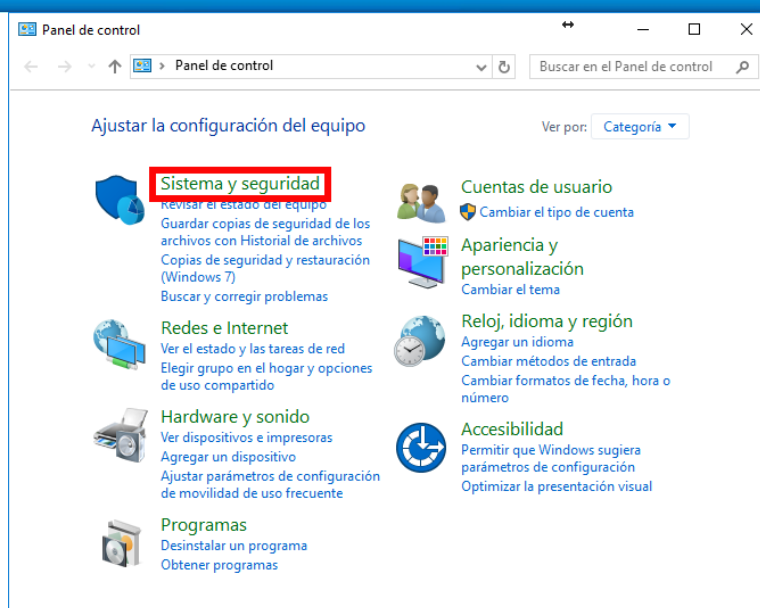


Firewall de Windows

En Windows, si tenemos habilitado el Firewall, este nos impedirá realizar la conexión, ya que limita las conexiones entrantes.

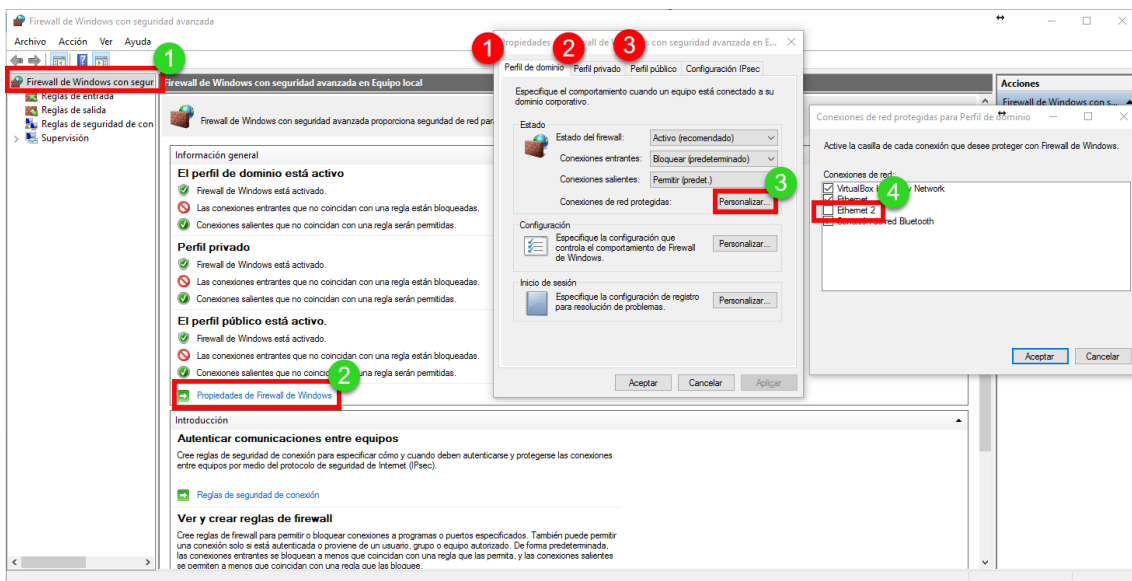
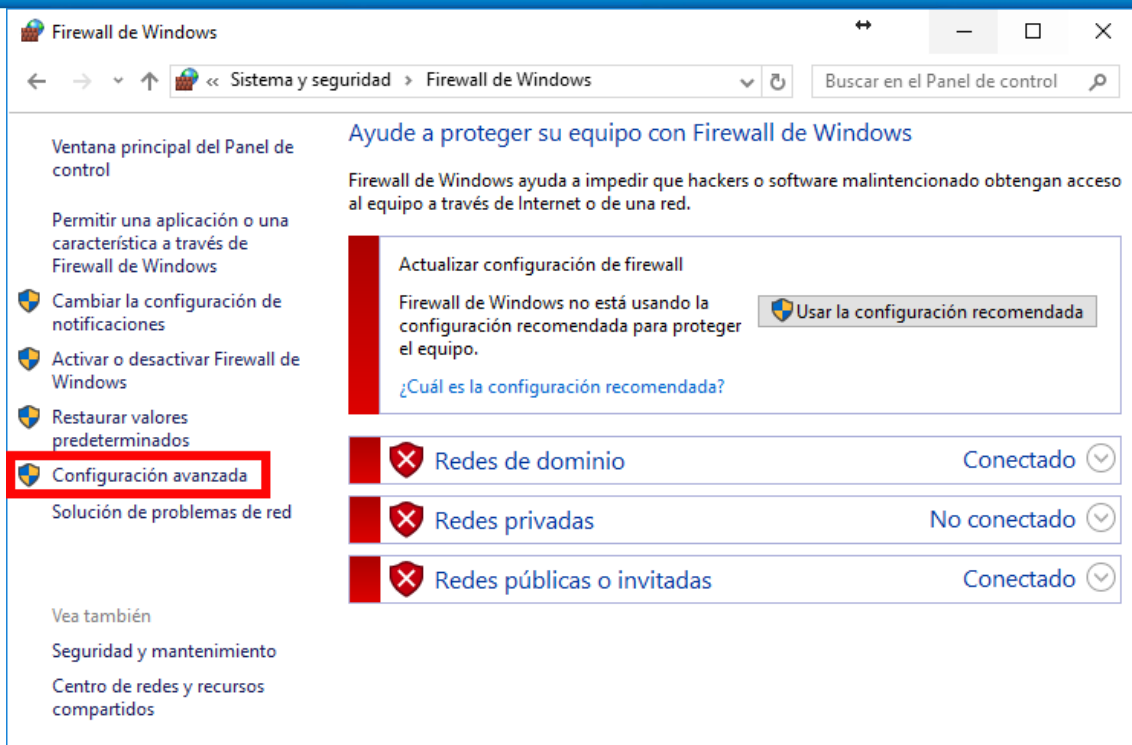
Para poder comunicar sin interferencias del Firewall, debemos desactivarlo. Podemos desactivarlo completamente, o desactivarlo sólo para el adaptador de nuestra VPN. En nuestro caso, vamos a explicar la solución de desactivarlo para nuestro adaptador de red.

El primer paso será abrir las opciones avanzadas del firewall de Windows. Una vez hayamos entrado en él, a través del panel de control, se nos mostrará la siguiente ventana (W10):

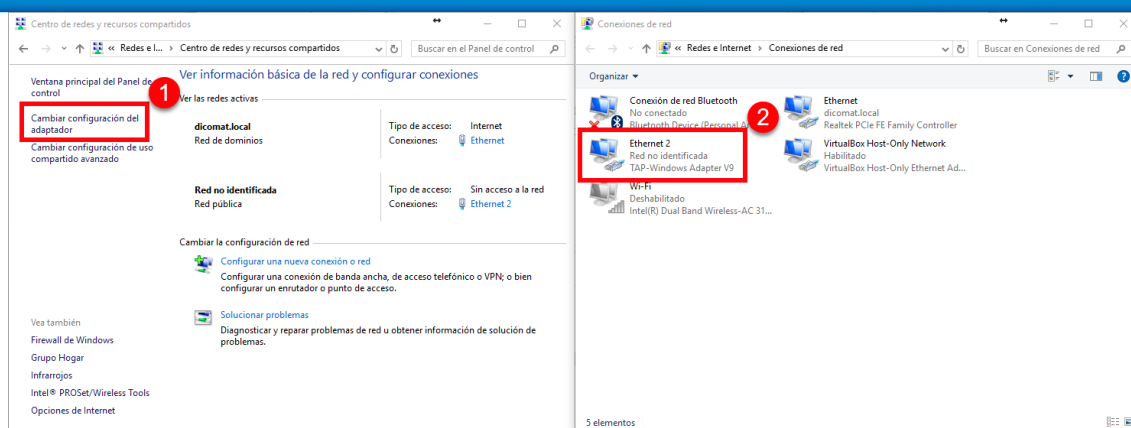


A continuación, vamos a configuración avanzada, para poder desactivar el Firewall en nuestro adaptador. Una vez que lo desactivemos, nos aparecerá en rojo, tal y como vemos en la imagen. No es importante, ya que sólo desactivaremos el Firewall para el adaptador de VPN, y a través de ella vamos a conectarnos a equipos seguros.

Primero, seguimos los pasos marcados en verde, para desactivar el adaptador de red que pertenece a la VPN (en la imagen siguiente se puede ver cómo identificarlo), y repetir el proceso para “Perfil privado” y “Perfil público”.



Si vamos al centro de redes y recursos compartidos (a través del panel de control), podemos ver nuestros adaptadores de red. Nos fijaremos en el que nos informe de que el adaptador es TAP-Windows Adapter, que es el adaptador instalado por OpenVPN.



Conexión del PFC100/200 a la red VPN

Convertir los certificados creados en Windows para su uso en Linux

Para poder instalar los certificados en la cabecera, necesitamos hacer una conversión de archivos. Esto se debe a que existen diferencias entre la codificación de los archivos de texto entre Windows y Linux, de ahí que debamos realizar una corrección en los archivos “.ovpn” y “.key”.

En Windows, nuestro fichero de configuración tiene la extensión “.ovpn”, mientras que en Linux es “.conf”. Esto se debe a que en Windows, en los ficheros de texto, las líneas terminan con CR LF, mientras que en Linux terminan sólo con LF.

Antes de realizar la conversión, debemos de tener en cuenta lo siguiente: Si convertimos nuestro fichero “.ovpn” a “.conf” directamente, nuestro equipo no se conectará. Si recordamos de la modificación del archivo “.ovpn” (sección “Configurar OpenVPN para usar los certificados”), en nuestro archivo modificábamos la dirección donde íbamos a colocar los ficheros. En nuestro PFC200, las direcciones son las siguientes:

/etc/openvpn/openvpn.conf

(nuestro archivo de configuración se renombra siempre que lo subamos al PFC)

/etc/certificates/

/etc/certificates/keys

Teniendo en cuenta estas direcciones, en nuestro archivo deberíamos de establecer lo siguiente:

dh /etc/certificates/keys/dh2048.pem

ca /etc/certificates/ca.crt

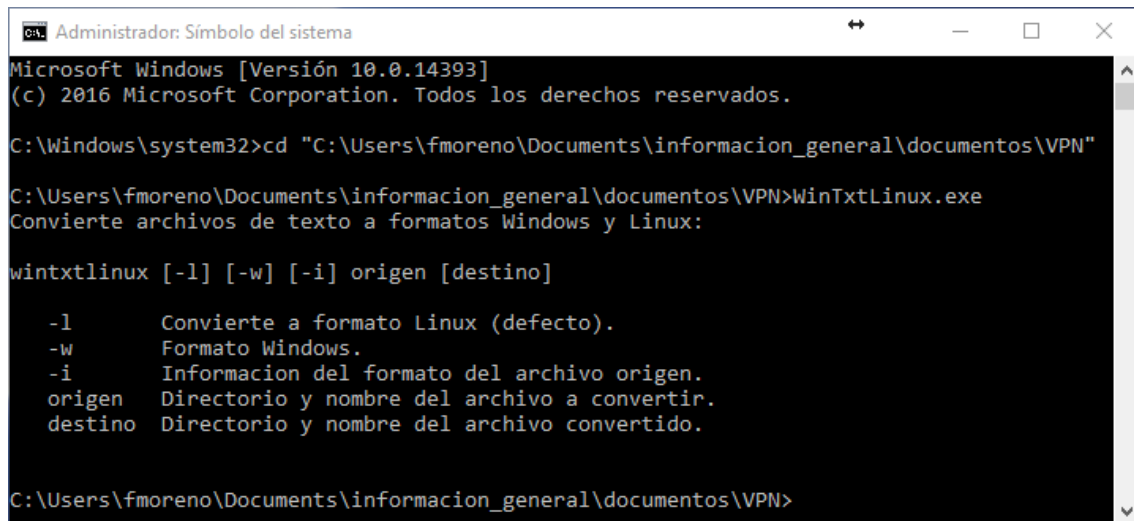
cert /etc/certificates/VPN-Client-Linux.crt

key /etc/certificates/keys/VPN-Client-Linux.key

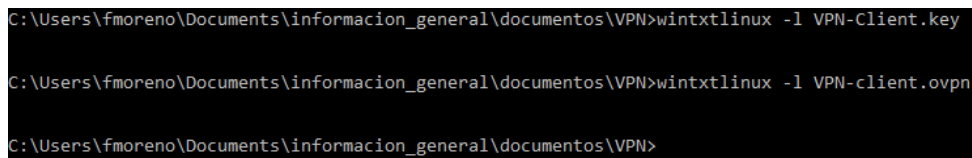
Una vez cambiando este direccionamiento en el archivo “.ovpn”, podemos proceder a convertir el archivo.

Hemos desarrollado una aplicación para este asunto, que modifica los archivos, de un formato a otro. La aplicación se llama “WinTxtLinux.exe”**, y debe abrirse en una ventana de Símbolo del sistema.

Llamamos a la aplicación, accediendo a su dirección mediante el comando `cd`, tal y como hemos realizado anteriormente, y nos mostrará las diferentes opciones disponibles:



Para cambiar nuestros archivos, debemos llamar al programa, agregar `-l`, para escribir en Linux, y agregar a la línea la dirección donde se encuentra el archivo que vamos a convertir, en el caso en el que tengamos los archivos separados.



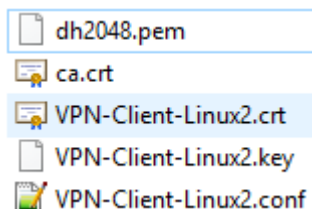
Una vez hecho el cambio, deberemos renombrar el archivo `“.ovpn”` a `“.conf”`, para completar la conversión.

****Nota sobre la aplicación WinTxtLinux**

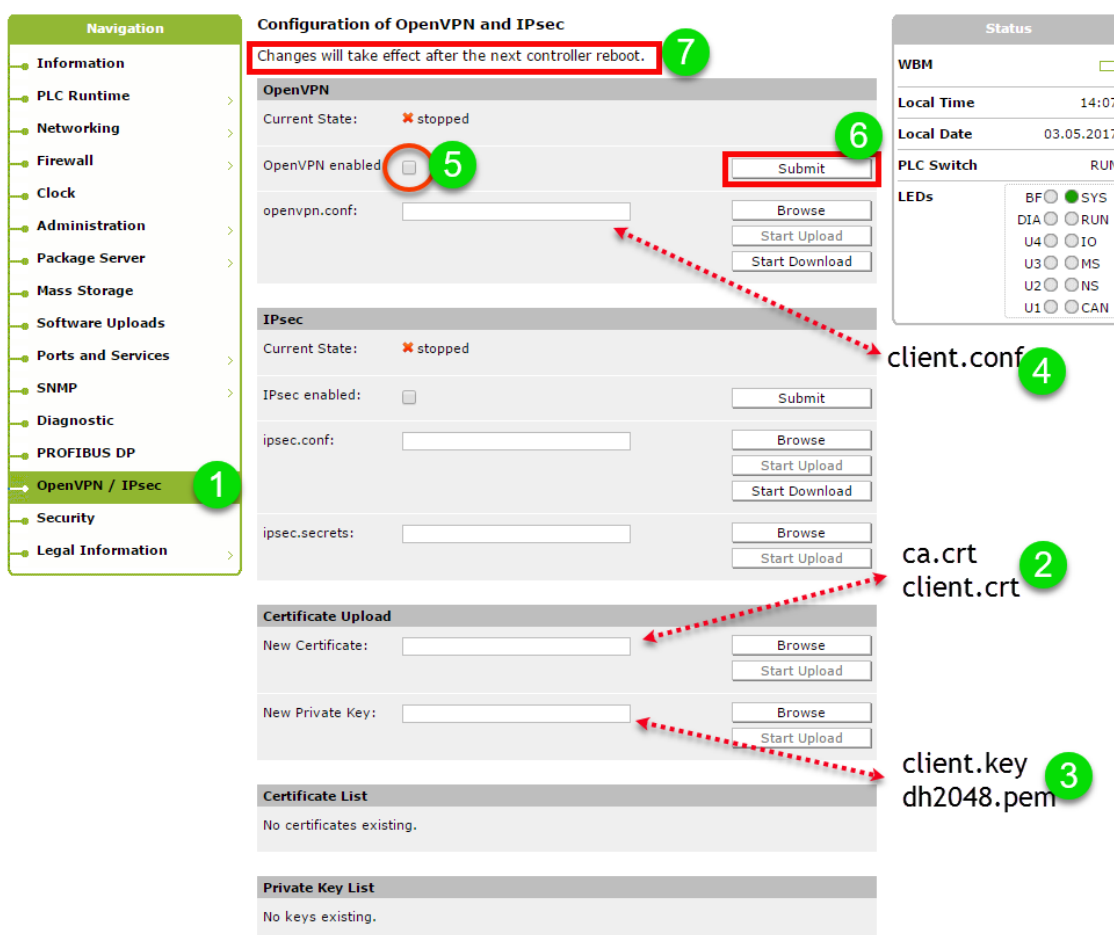
- El programa sobrescribe el archivo original, es importante realizar una copia, para guardar el archivo original.
- Es recomendable copiar el programa a la carpeta donde se tienen los archivos a modificar.
- Para seleccionar el archivo, se recomienda poner la inicial y pulsar tabulación, para que Windows encuentre el archivo que queremos. Esto se aconseja para evitar que símbolos en el nombre causen problemas en la conversión (de existir, Windows entrecomillaría el archivo).

Instalación de los archivos en el PFC100/200

Una vez realizado el paso anterior, estaremos en posesión de los archivos necesarios para unir nuestro PFC100/200 a la red. Los archivos necesarios para la conexión son los siguientes:



A través del webserver de nuestra cabecera, accedemos a la sección de OpenVPN/IPsec, y realizamos los pasos de la imagen:



The screenshot shows the 'Configuration of OpenVPN and IPsec' web interface. The left sidebar (Navigation) has 'OpenVPN / IPsec' highlighted with a green circle 1. The main content area has a red box around the warning 'Changes will take effect after the next controller reboot.' with a green circle 7. The 'OpenVPN' section shows 'Current State: stopped' and 'OpenVPN enabled' with a checkbox and a green circle 5. A 'Submit' button is highlighted with a green circle 6. The 'IPsec' section shows 'Current State: stopped' and 'IPsec enabled' with a checkbox. Red dotted arrows point from the 'client.conf' label (green circle 4) to the 'openvpn.conf' field, from the 'ca.crt' and 'client.crt' labels (green circle 2) to the 'Certificate Upload' section, and from the 'client.key' and 'dh2048.pem' labels (green circle 3) to the 'New Private Key' field. The 'Status' panel on the right shows system information like 'Local Time', 'Local Date', and 'PLC Switch'.

Una vez que reiniciemos nuestro equipo, puede tardar unos segundos en conectarse a la red, pero el estado cambiará a Enabled si hemos hecho la configuración correcta.

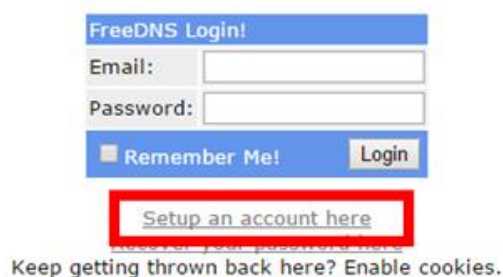
Apéndices

Crear Servidor DNS

Como siempre, tenemos varias opciones para realizar esto, algunas de pago y otras gratuitas, como por ejemplo: DynDNS, NoIP, FreeDNS...

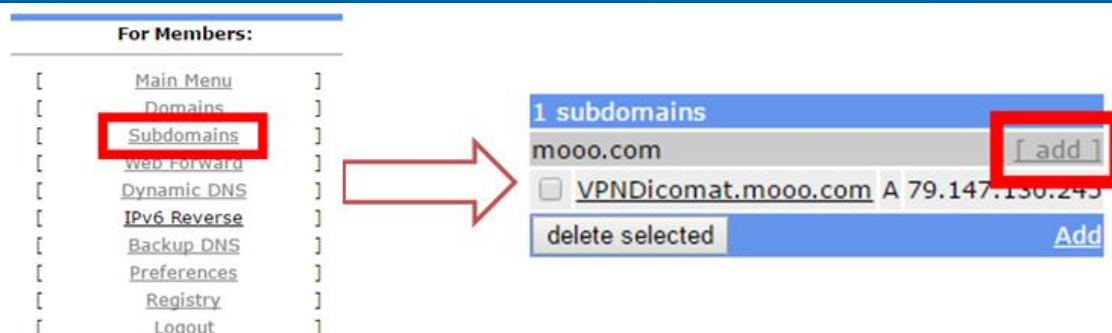
En nuestro caso, para este ejemplo, vamos a utilizar FreeDNS (<https://freedns.afraid.org/>). FreeDNS dispone de servidores gratuitos y de pago, en función de los requerimientos. Nosotros vamos a utilizar la opción gratuita.

Tenemos que crearnos una cuenta. Pinchando en cualquiera de los menús marcados “For Members”, nos abrirá el cuadro para iniciar sesión o registrarnos:



	Starter	\$60/yr	\$120/yr	\$300/yr	\$600/yr
Subdomain cap	5	50	100	250	500
Stealth Flags	None	3	6	15	30
Global Propagation times (TTLs, in seconds)	3600	60	60	60	60
Captchas Removed	No	Yes	Yes	Yes	Yes
Wildcard support	None	Unlimited	Unlimited	Unlimited	Unlimited
Professional Branding	None	None	None	Yes	Yes
Ad free	Yes	Yes	Yes	Yes	Yes
Status	Basic	Premium	Premium	Premium	Premium
*Make Your Plan Selection		➔ Select	➔ Select	➔ Select	➔ Select

Seleccionaremos la opción “Starter”, que es la opción básica, que nos limita a tener 5 subdominios en nuestra cuenta. El siguiente paso es agregar nuestros datos, y nos enviarán un correo para activar la cuenta.



Una vez que tengamos activa la cuenta, podremos ir al menú “Subdomains”, y agregar nuestro dominio.

Con esto, tendríamos nuestro servidor DNS activado y disponible para trabajar. Para que nuestro servidor redirija correctamente el tráfico a esta IP, necesitamos descargarnos un cliente DNS. Para ello iremos a la sección “Dynamic DNS”, y seleccionaremos “Dynamic DNS Clients”.

Esta selección nos abre un desplegable con diferentes opciones, según el sistema operativo donde vamos a instalar nuestro servidor. En nuestro caso, vamos a instalar el servidor en un ordenador con Windows, así que bajaremos a la sección “Windows client”, y seleccionaremos la primera opción, “FreeDNS Update”.

Una vez instalado, tendremos que iniciarlo y agregar nuestra cuenta, manteniéndolo siempre activado, mientras que queramos nuestro servidor operativo.

