Guía de Configuración OpenVPN Cliente con mGuard

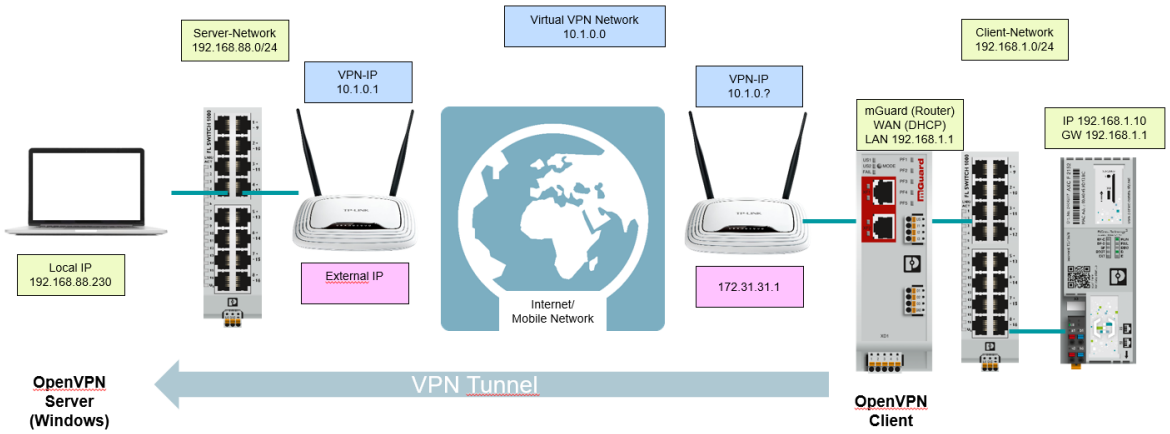


Tabla de contenido

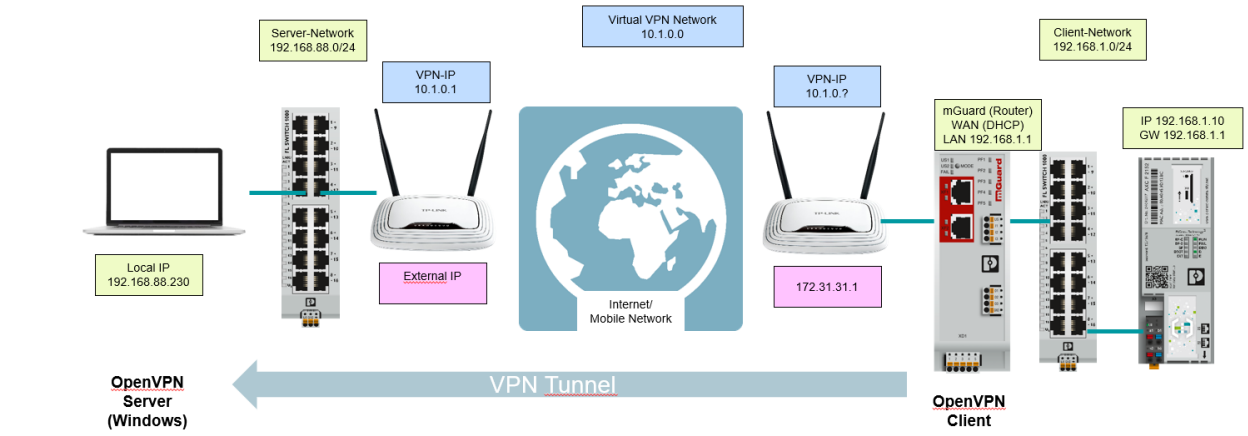
1 Introducción

Esta guía muestra como configurar una conexión OpenVPN entre:

OpenVPN Server (Windows)

OpenVPN Client (mGuard en modo Router)

El ejemplo desarrollado es el siguiente.



2 Instalación de OpenVPN en Windows

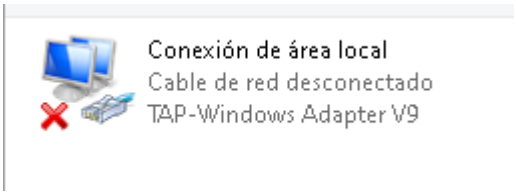
Descarga la versión actual desde este link:

Community Downloads | OpenVPN

https://openvpn.net/community-downloads/

Confirma todas las opciones por defecto de la instalación.

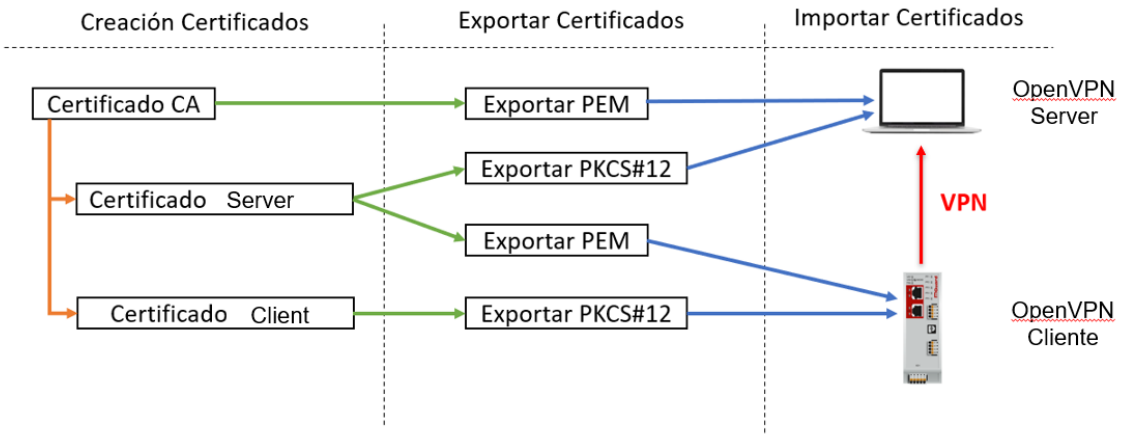
Comprueba que se ha instalado un nuevo adaptador TAP en la configuración de red e internet de Windows



3 Certificados X.509

Para crear los certificados se puede utilizar el programa freeware **XCA**.

La distribución de certificados que se seguirán es el indicado en la figura.



3.1 Creación de una base de datos XCA

Abra el programa **XCA**.

1. Seleccione el menú **File > New Database**
2. Especifique un nombre y una localización de la base de datos.
3. Pulse **Save**.
4. Escriba una contraseña para proteger el uso de la base de datos de certificados.

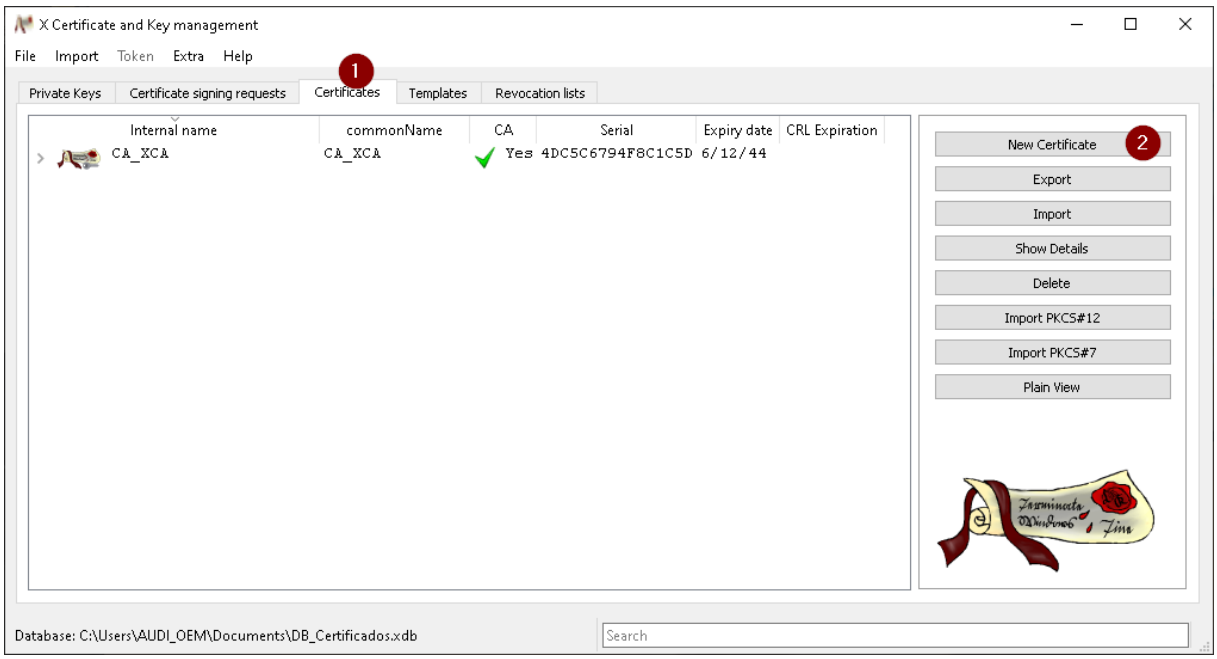
3.2 Creación de un certificado CA

Para poder crear y utilizar certificados que no sean autofirmados, sino creados por una autoridad certificadora (CA) se puede crear un certificado CA.

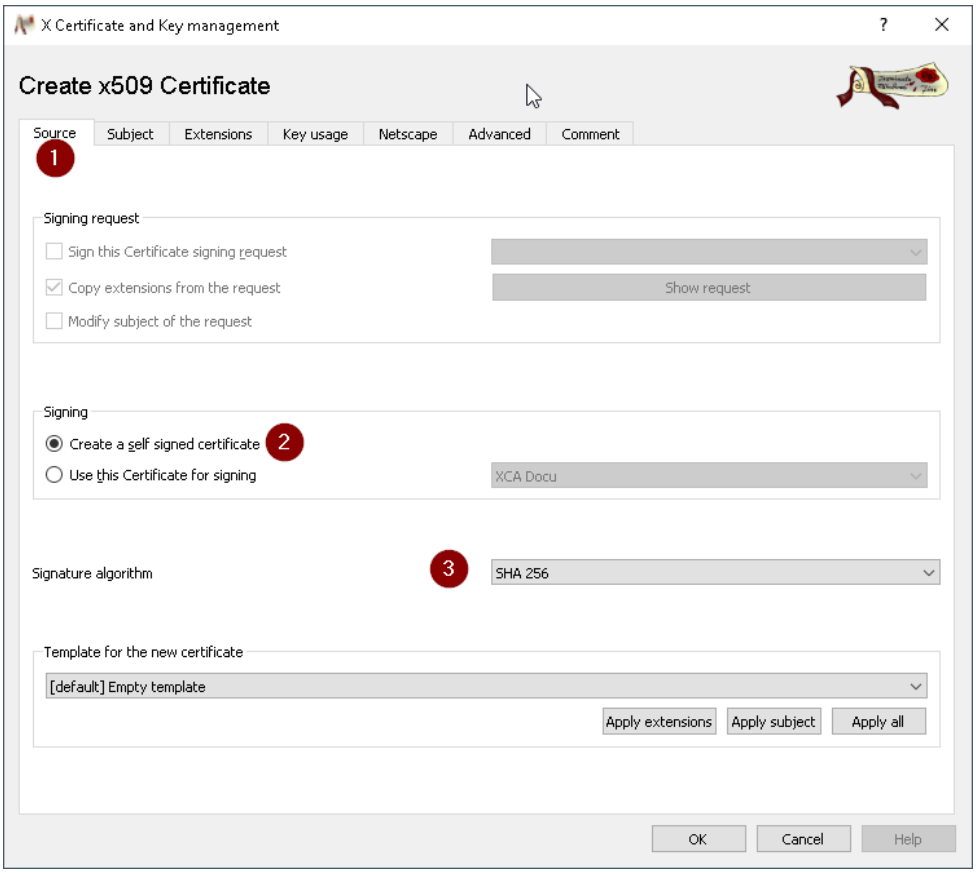
El certificado CA será un certificado autofirmado.

Este certificado CA será el que utilicemos para firmar todo el resto de certificados.

1. Desde la pestaña **Certificates** (1)
2. **New Certificate** (2)

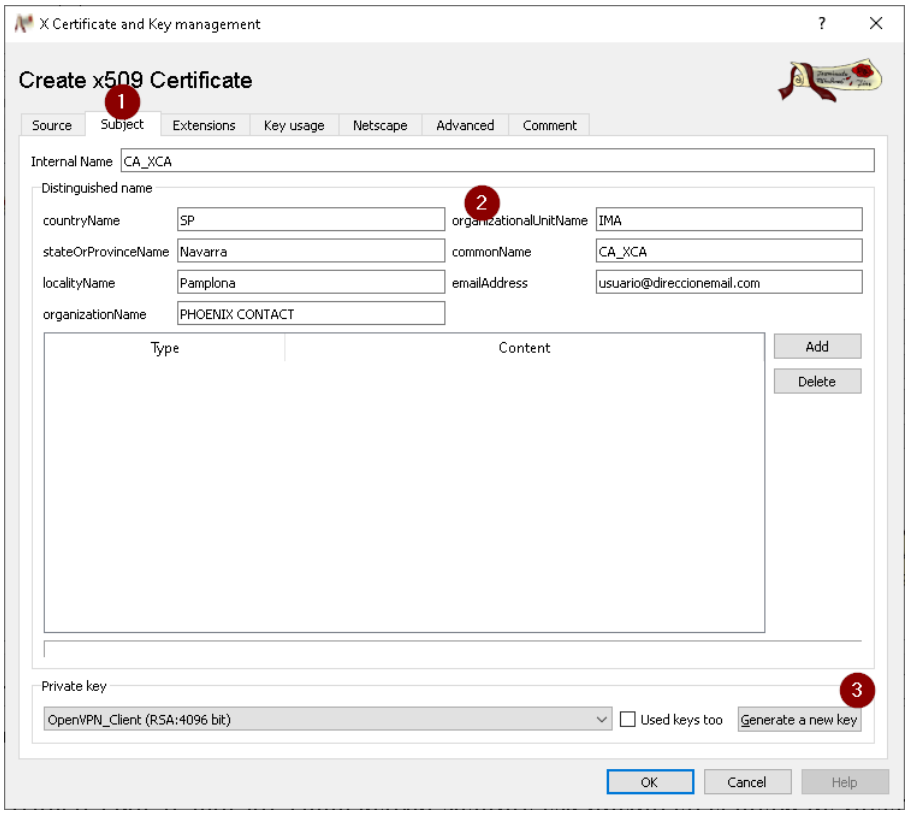


1. Seleccione la pestaña **Source** (1)
2. Seleccione que el certificado **CA** sea autofirmado (2)
3. Seleccione el algoritmo de firma **SHA 256** (3)

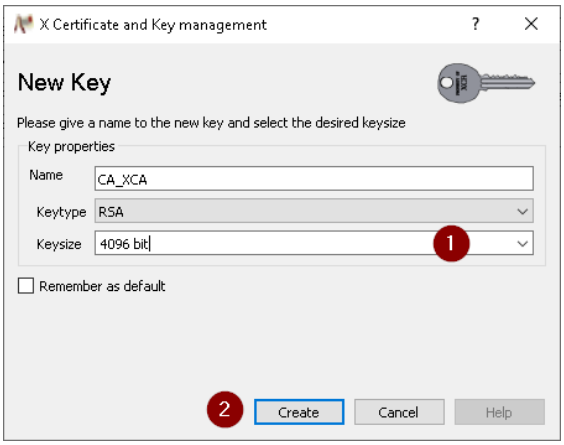


Seleccione la pestaña **Subject** (1)

1. Rellene los campos de **Distinguished Name** e **Internal Name** (2). Es importante que los campos **Internal Name** y **Common Name** tengan el mismo nombre.



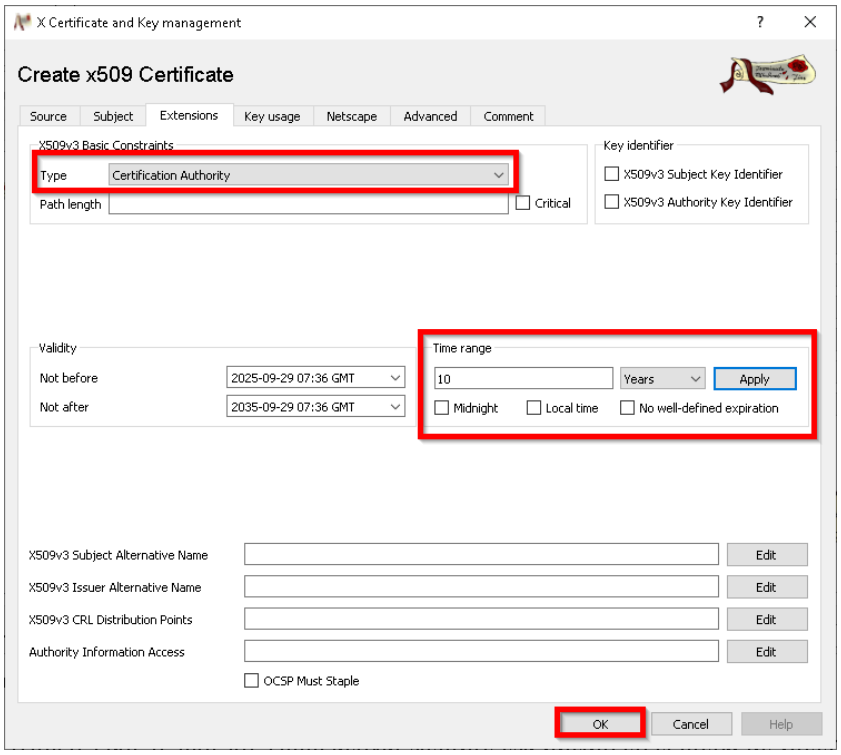
2. Pulse **Generate a new key** (3). En el siguiente diálogo seleccione la **Keysize** (2) y pulse **Create** (3)



Seleccione la pestaña **Extensions**.

3. Seleccione el tipo **Certification Authority**
4. Seleccione el rango de validez del certificado que les interese. Tenga en cuenta que el resto de certificados que dependan de éste podrán tener como máximo ese rango de validez.

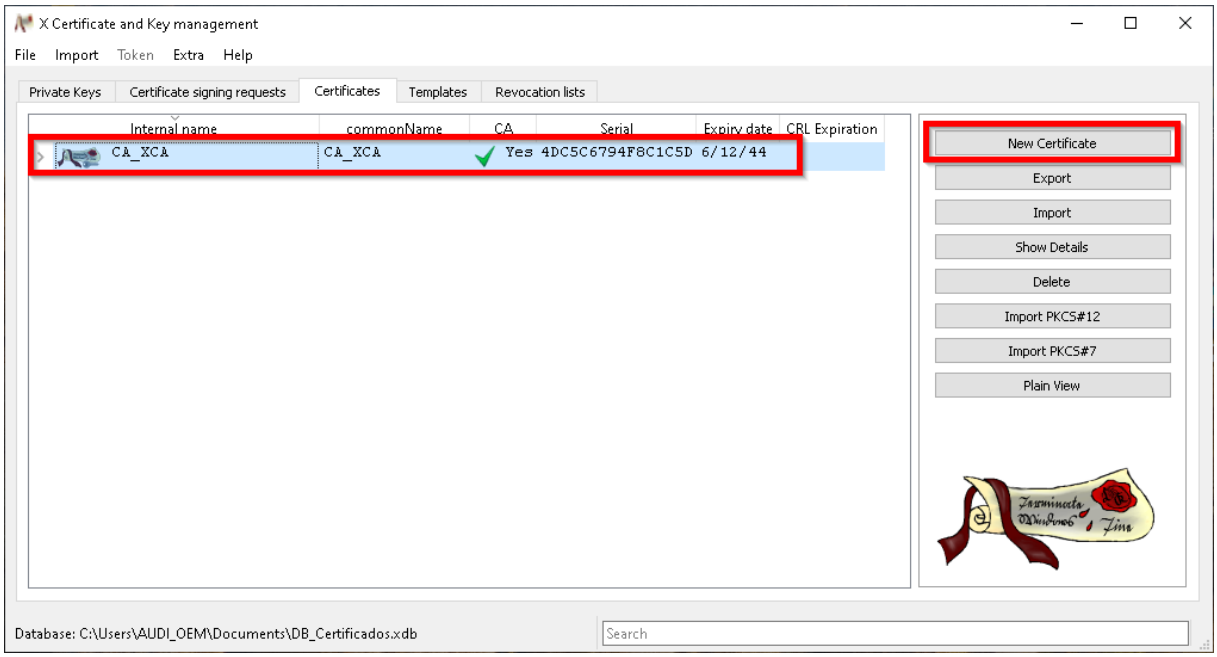
5. Pulse **Apply** y **OK** para terminar



3.3 Creación de un certificado

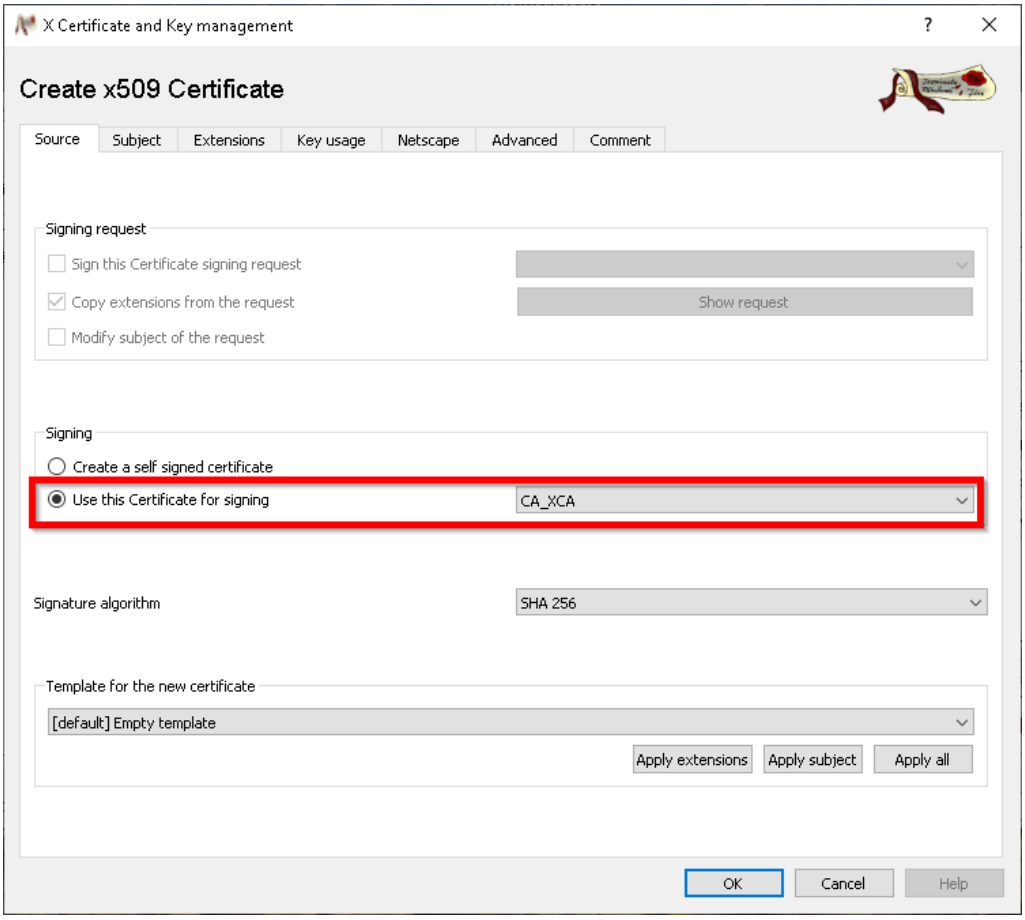
Una vez creado un certificado CA ya se pueden generar certificados firmados por esa CA. Estos certificados pueden ser, por ejemplo, el certificado a utilizar en el servidor (Windows) o el Cliente VPN (mGuard).

1. Seleccione la pestaña **Certificates**
2. Seleccione el certificado CA anteriormente creado
3. Pulse **New Certificate**



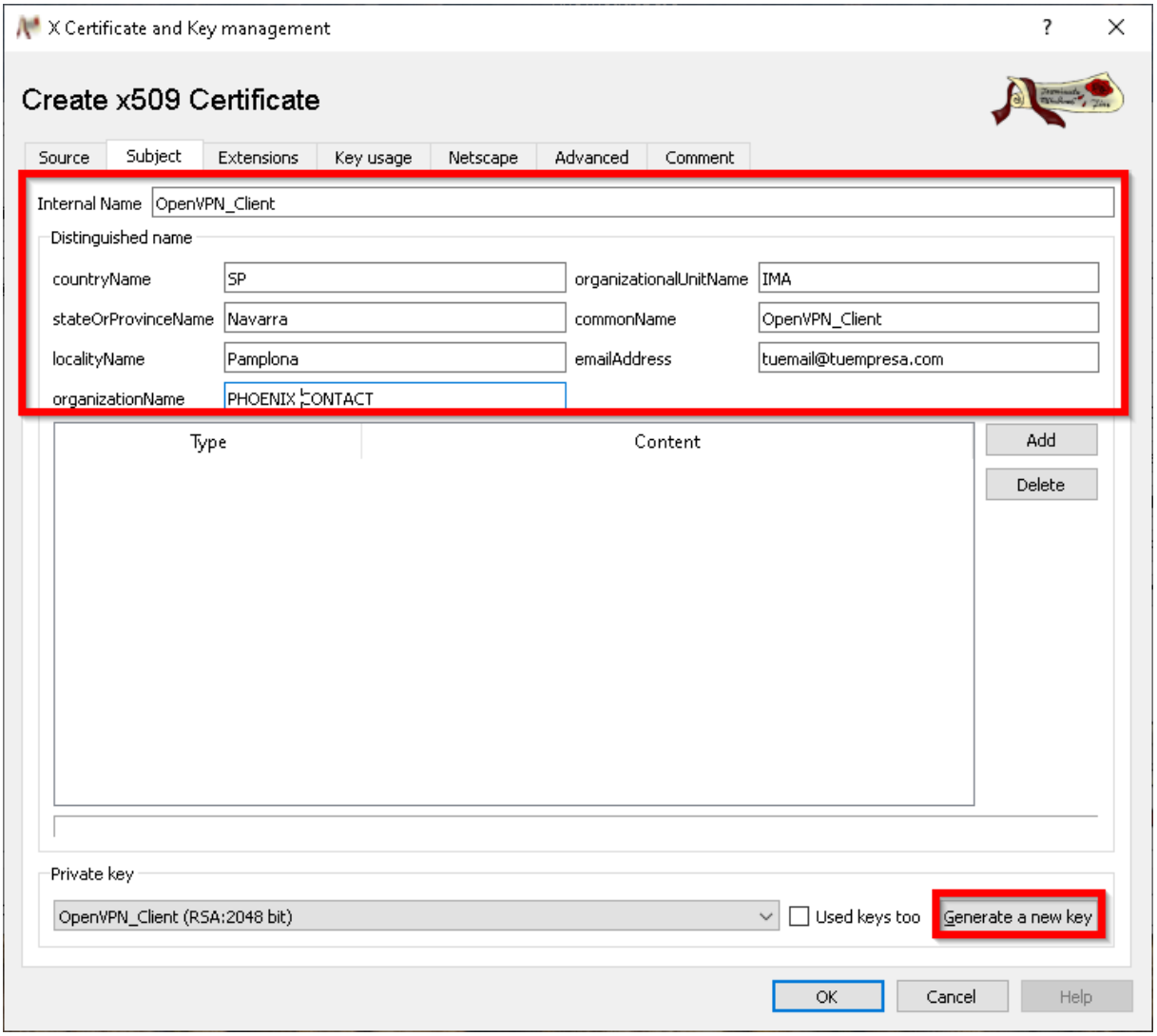
Seleccione la pestaña **Source**

1. En la sección **Signing** seleccione el certificado CA con el que se firmará el certificado a crear.



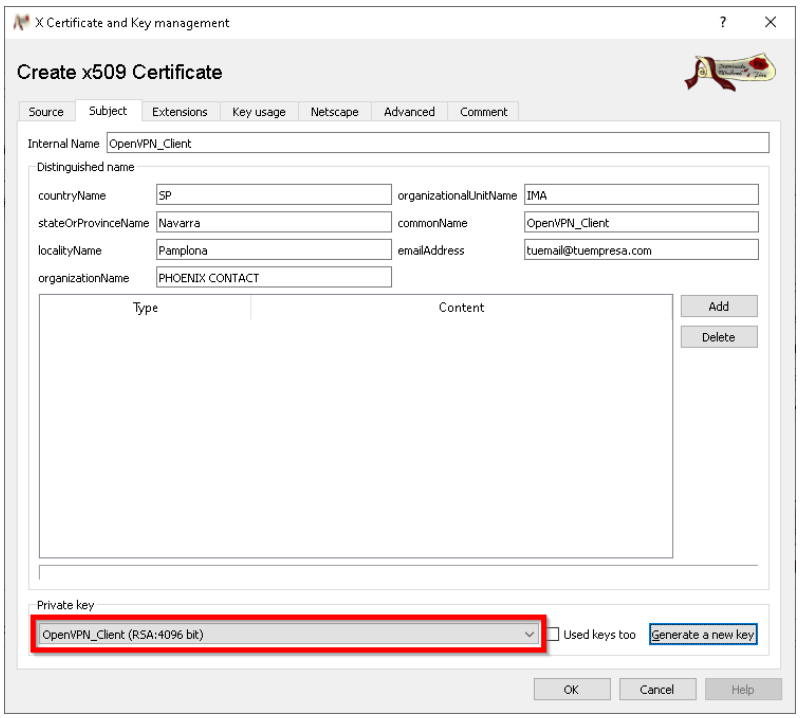
Seleccione la pestaña **Subject**.

1. Rellene los campos **Internal Name** y **Distinguished Name**
   Recuerde utilizar el mismo nombre en **Internal Name** que en **Common Name**



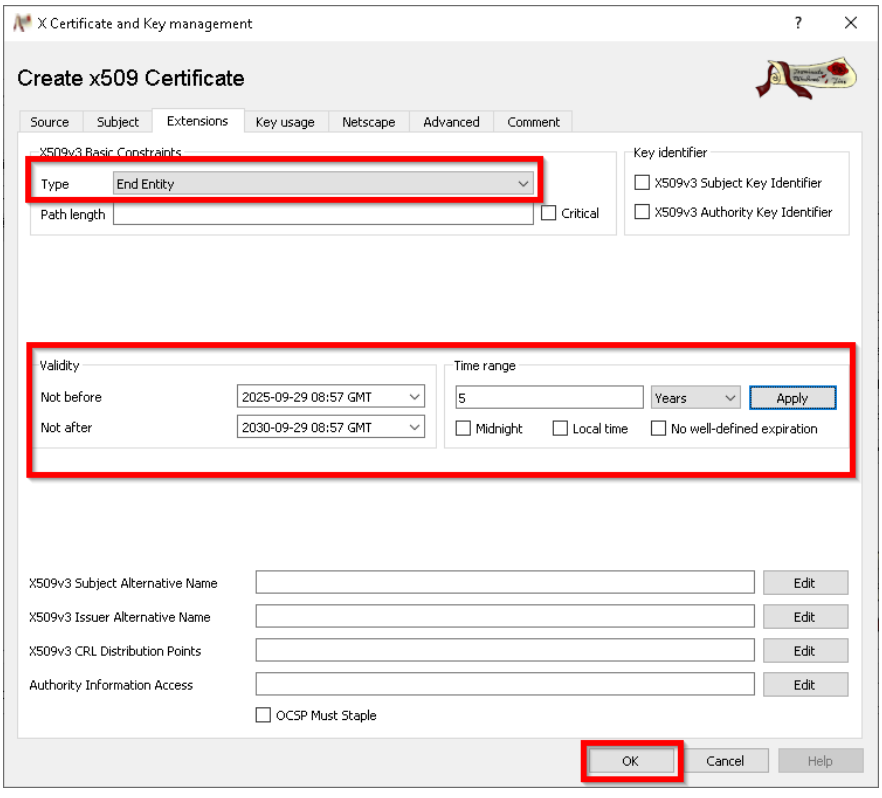
2. Pulse el botón **Generate a new key**
3. En el siguiente dialogo seleccione el tamaño de la llave privada del certificado en **Keysize** y pulse **Create.** Se recomienda un tamaño de 4096 bits.

Una vez creada aparece bajo **Private Key**

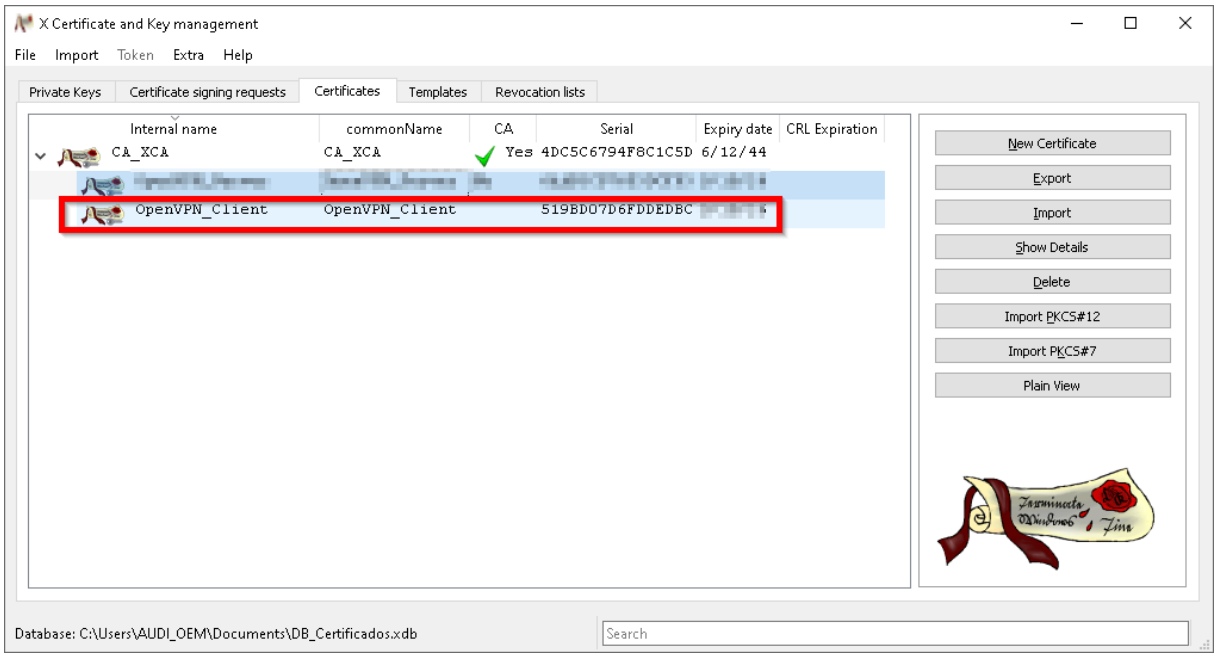


Seleccione la pestaña **Extensions**

1. Seleccione en **Type: End Entity**
2. Seleccione el rango de duración del certificado a partir de las fechas de validez.



El certificado cliente se ha creado y aparece debajo de su certificado CA.

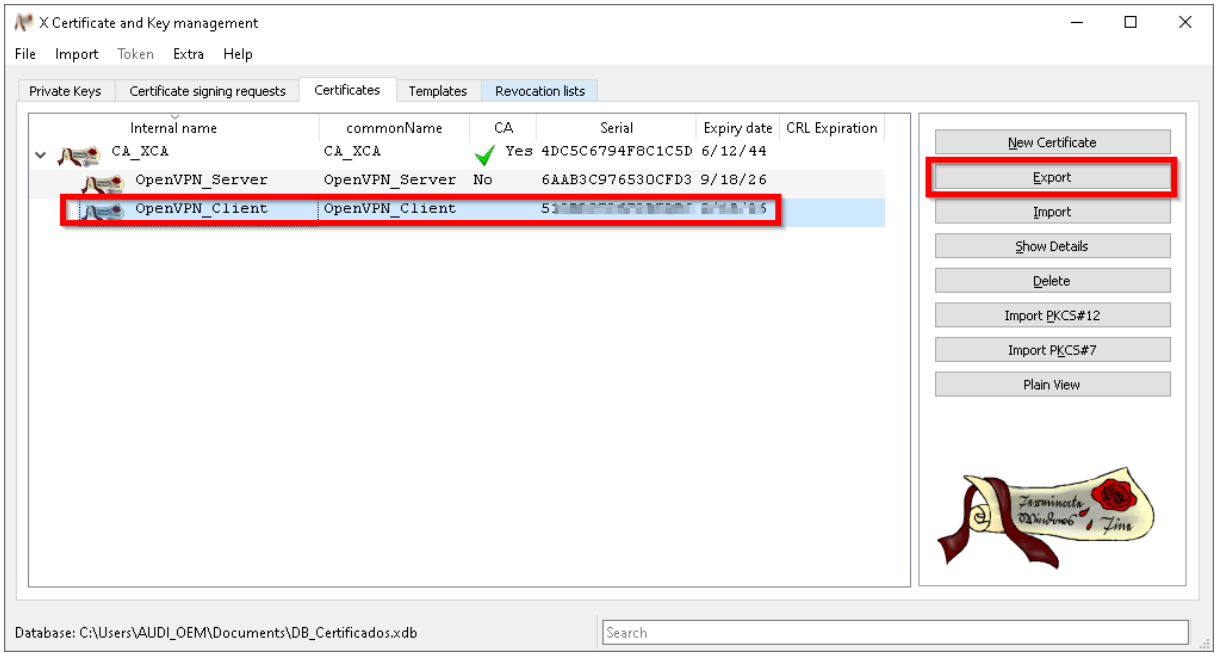


Repita el proceso para crear el certificado para el Server.

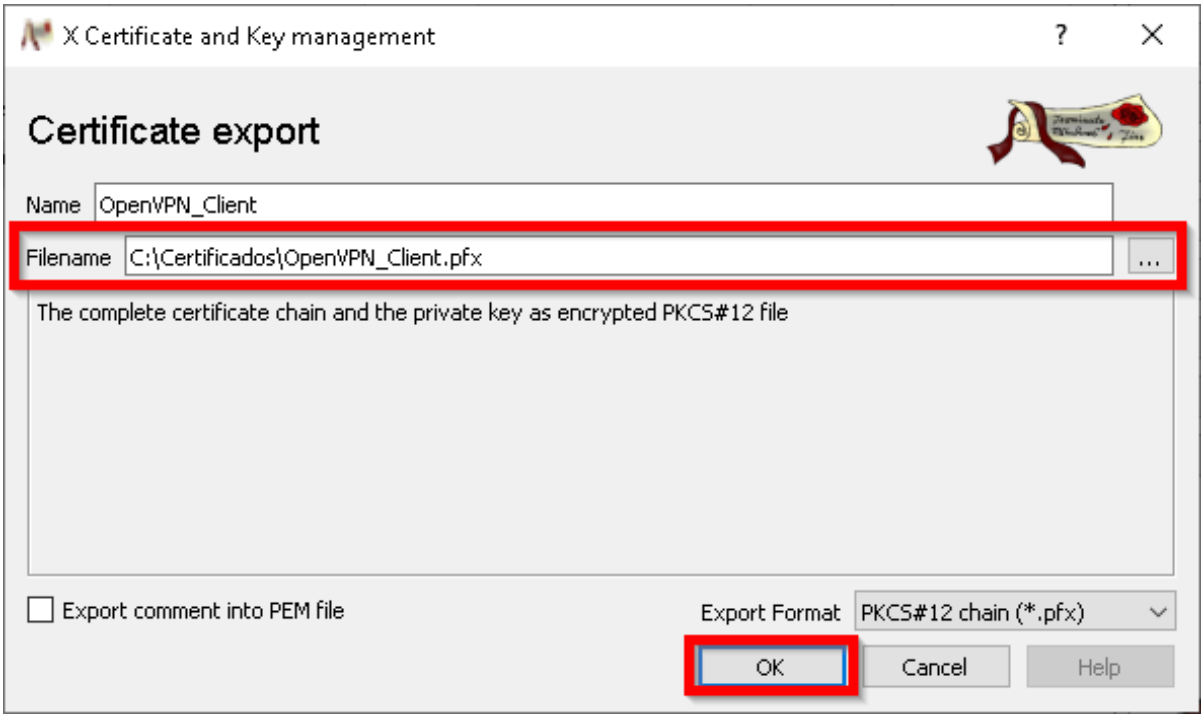
3.4 Exportar los certificados

Una vez creados los certificados, éstos se deben exportar para poderlos utilizar tanto en el Cliente (mGuard) como en el Servidor (Windows) de modo que ambos se puedan autenticar entre si.

1. Seleccione el certificado a exportar y pulse **Export**



2. Seleccione la ruta y el nombre del certificado a exportar.
3. Elija el formato del certificado. Exportar tanto en formato **pfx** como **crt**

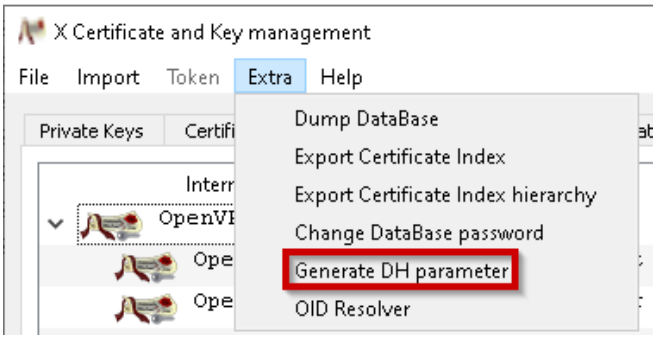


4. Pulse Ok

5. Repita el proceso para exportar el certificado CA (solo con formato **crt**). Al final debe tener estos cinco ficheros exportados.

3.5 Creación de fichero de parámetros Diffie Hellmann

Desde la misma herramienta XCA creamos el fichero de parámetros de Diffie Hellman, en este ejemplo de 2048 bits.



Guarda con el nombre **dh2048.pem** en el directorio **C:\Program Files\OpenVPN\config.**

Para mayor comodidad se pueden también copiar los cinco certificados recién exportados en el mismo directorio **config.**

4 Configuración del OpenVPN Server

Utiliza un editor de texto para crear un fichero de configuración con el nombre “OPENVPN_Tunnel.opvn”. Asegúrese que no se añada una extensión “.txt” adicional en el nombre del fichero.

Guarda este fichero en el directorio **C:\Program Files\OpenVPN\config**

En el siguiente texto se incluye el contenido del fichero **OPENVPN_Tunnel.opvn**

Utiliza estos valores como valores por defecto para tu configuración cambiando las rutas según tu red como se explica en el siguiente punto.

```
# Configuracion para un OpenVPN Server

port 1194                       # Puerto escucha servidor OpenVPN
proto udp4                      # Protocolo de transporte udp sobre IPv4
dev tun                         # Adaptador red TUN OpenVPN

server 10.1.0.0 255.255.255.0   # Red interna OpenVPN
pkcs12 OpenVPN_Server.pfx       # Certificado privado OpenVPN Server
dh dh2048.pem                   # Parametros Diffie-Hellman intercambio seguro claves

keepalive 10 60                 # ping de vida cada 10 sg y desconecta a los 60 sino hay respuesta
persist-key                     # Mantiene la clave en memoria al reiniciar/releer configuración
persist-tun                     # Mantiene la interfaz TUN activa al reiniciar/releer configuración
verb 3

compress migrate                # Compatibilidad con clientes antiguos
data-ciphers AES-256-GCM:AES-128-GCM        # Cifrados datos permitidos (prioridad AES-256-GCM)
ncp-ciphers AES-256-GCM:AES-128-GCM         # Cifrados negociación parametros de cifrado (NCP)

push "route 192.168.88.0 255.255.255.0" # Ruta Servidor a los clientes

client-config-dir ccd       # Carpeta con configuraciones específicas por cliente (basado en el CN del cert)
route 192.168.1.0 255.255.255.0 # Ruta cliente
```

4.1 Enrutamiento

El programa **OpenVPN** instalado en Windows es el que corre el servidor de OpenVPN.

El fichero de configuración está creado y guardado en el directorio **config**

Para el enrutamiento en la subred del servidor por parte del cliente se debe incluir una línea con el comando **push** en el fichero de configuración.

En este ejemplo el servidor se conecta desde la subred **192.168.88.0/24**.

```
push "route 192.168.88.0 255.255.255.0" # Ruta Servidor para los clientes
```

Crea una carpeta con el nombre **ccd** en **c:\Program Files\OpenVPN\config**.

Especifica el nombre de la carpeta en el fichero de configuración.

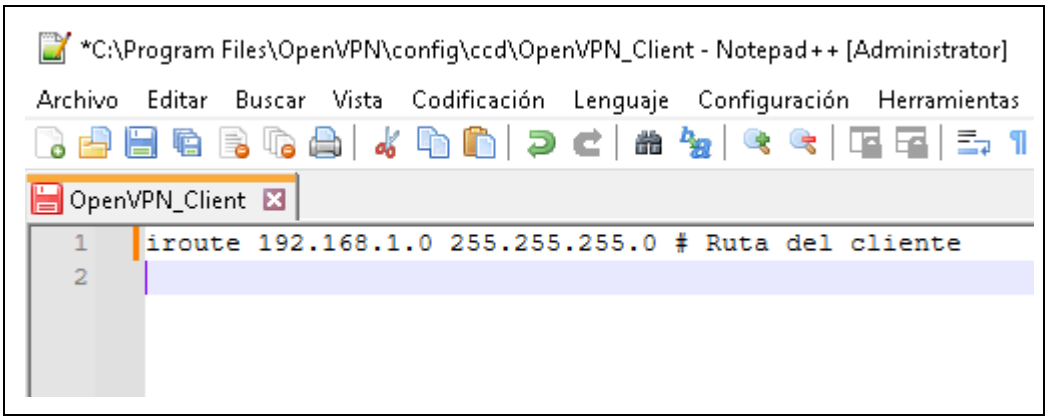
```
client-config-dir ccd          # Carpeta con configuraciones específicas por cliente (basado en el CN del cert)
```

Crea dentro de la carpeta **ccd** un fichero de texto con el nombre del certificado de cliente.

Tenga en cuenta que el nombre es sensible a las mayúsculas y minúsculas.

Debe de haber un archivo por cada uno de los clientes con los que conecte el servidor. En el caso de esa guía sólo existe un cliente (mGuard).

Escribe dentro del fichero con el comando **iroute** la red del cliente a la que se conectará el servidor mediante el túnel. En este ejemplo es la **192.168.1.0/24**



5 Configuración del cliente OpenVPN en el mGuard

Antes de poder utilizar los certificados es necesario cargarlos en el mGuard.

Para ello **Menu Authentication → Certificates**.

5.1 Carga del certificado de máquina (mGuard)

Desde la pestaña **Machine Certificates** se crea una nueva fila con el icono (**+**).

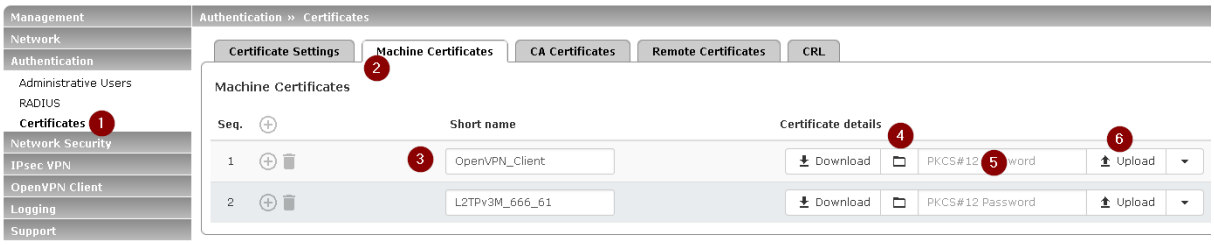
En **Short name** se escribe un nombre que identifique al certificado ej. **OpenVPN_Client** (3)

Buscamos con el icono de carpeta (4) el certificado **pfx** del cliente de OpenVPN anteriormente exportado.

Se escribe en el campo (5) la contraseña del certificado.

Se pulsa el botón Upload (6).

En la parte superior izquierda de la pantalla aparece en verde la confirmación de que el certificado se ha cargado con éxito.



5.2 Carga del certificado CA

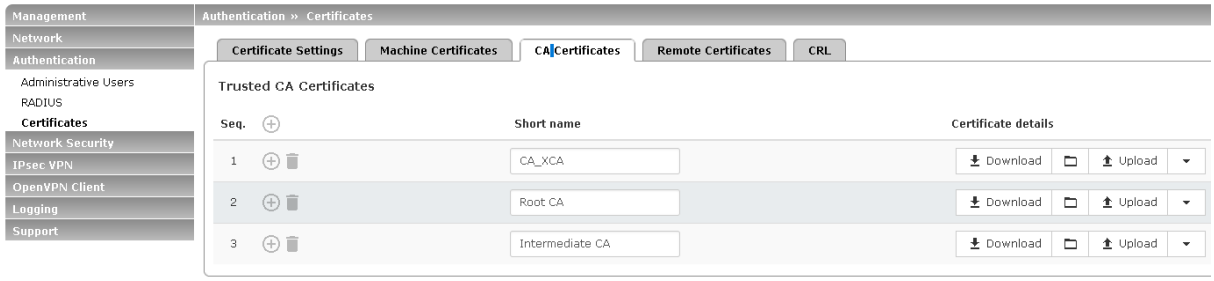
Desde la pestaña **CA Certificates** se crea una nueva fila con el icono (+).

En **Short name** se escribe un nombre que identifique al certificado ej. **CA_XCA.**

Buscamos con el icono de carpeta el certificado **crt** de la entidad certificadora anteriormente exportado ej. **CA_XCA.crt.**

Se pulsa el botón Upload.

En la parte superior izquierda de la pantalla aparece en verde la confirmación de que el certificado se ha cargado con éxito.



5.3 Carga del certificado remoto (server)

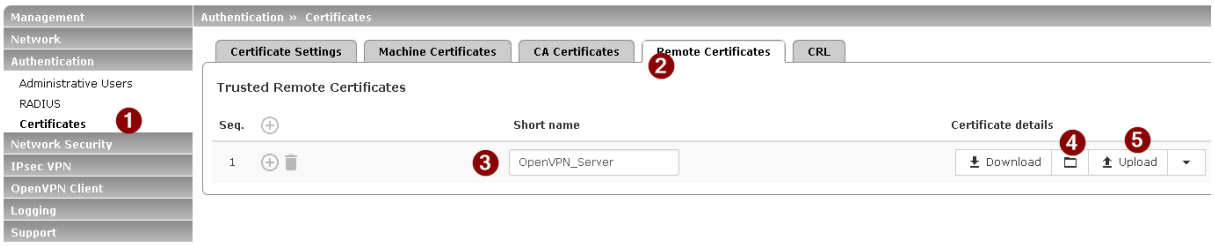
Desde la pestaña **Remote Certificates** se crea una nueva fila con el icono (**+**).

En **Short name** se escribe un nombre que identifique al certificado ej. **OpenVPN_Server.**

Buscamos con el icono de carpeta (4) el certificado **crt** del certificado del servidor anteriormente exportado ej. **OpenVPN_Server.crt.**

Se pulsa el botón Upload (5).

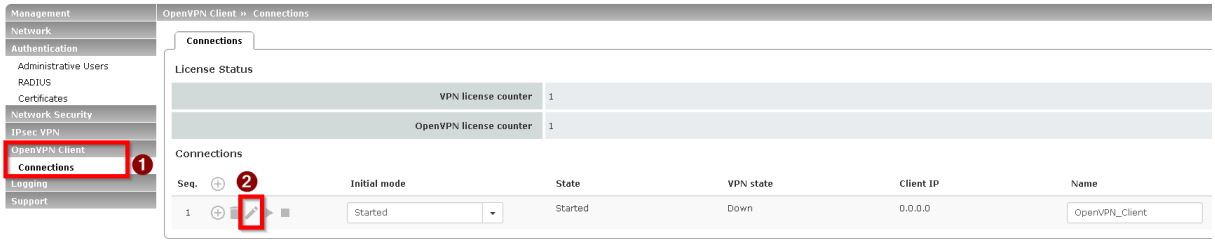
En la parte superior izquierda de la pantalla aparece en verde la confirmación de que el certificado se ha cargado con éxito.



5.4 Configuración del cliente OpenVPN

Desde el menú **OpenVPN Client → Connections**.

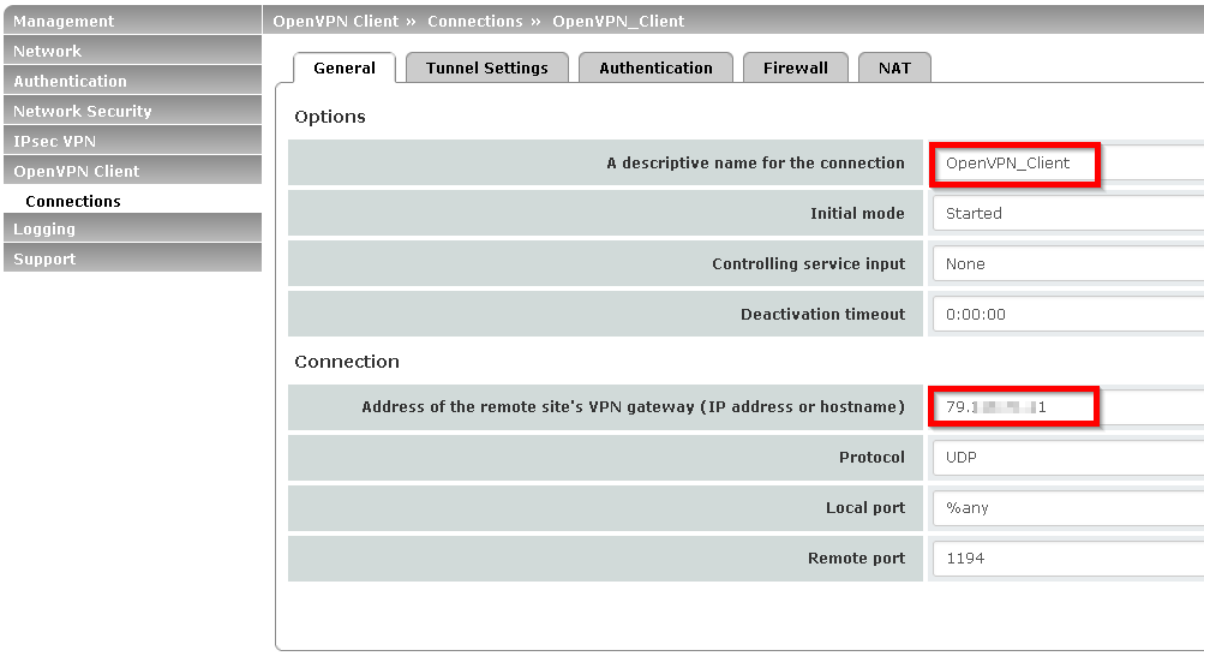
Se pulsa en el icono del lápiz (2).



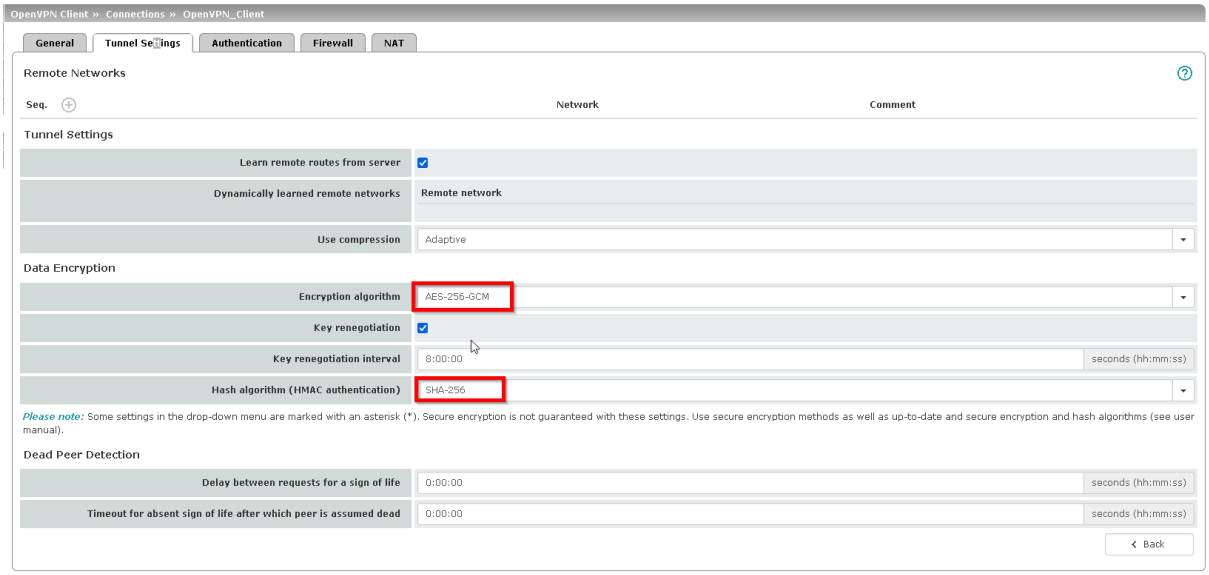
En la pestaña **General** en el campo **descriptive name** se le da un nombre identificativo a la conexión.

En el campo **Address of the remote site** se escribe la dirección IP pública detrás de la cual se encuentra el Servidor de OpenVPN. Si está dirección cambia se recomienda configurar un nombre DNS con algún tipo de proveedor DynDNS.

El resto de campos se dejan como en el siguiente screenshot.

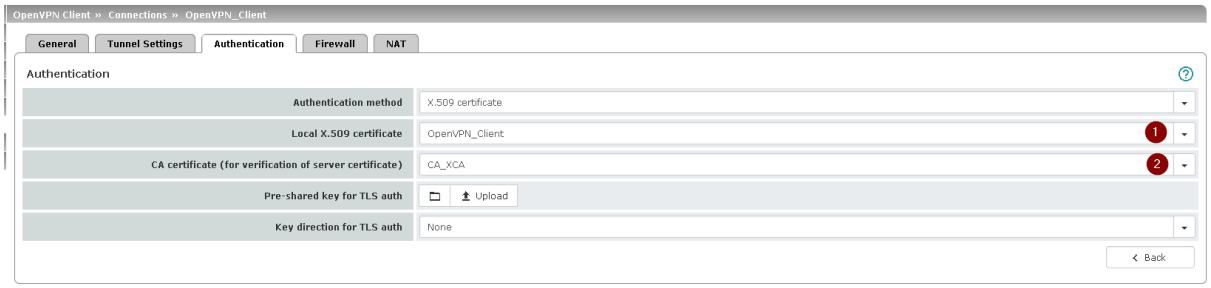


Desde la pestaña **Tunnel Settings → Data Encryption** se seleccionan los algoritmos de encriptación y autenticación. Estos deben coincidir con los algoritmos configurados en la parte del servidor OpenVPN.

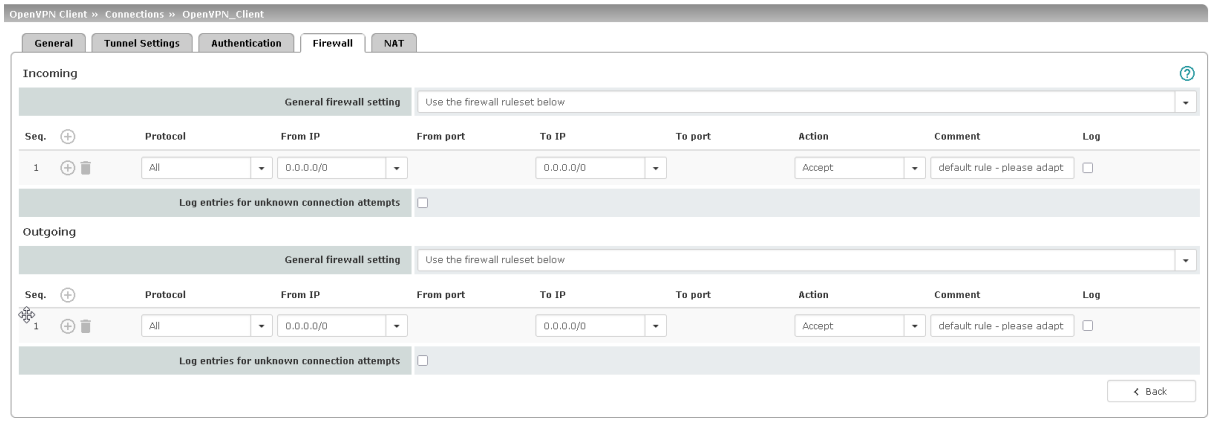


Desde la pestaña **Tunnel Settings → Authentication** se seleccionan el certificado del cliente (1) y entidad certificadora (2) a utilizar en el túnel OpenVPN.

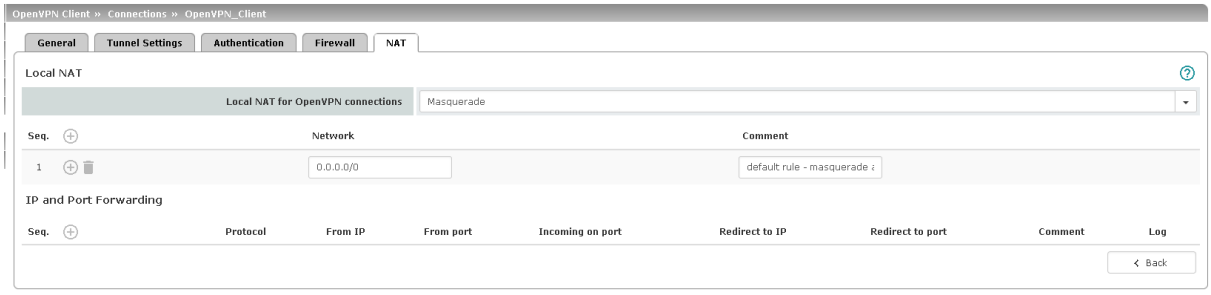
Estos certificados solo están disponibles si previamente han sido cargados en el mGuard.



Desde la pestaña **Tunnel Settings → Firewall** se configuran las reglas de firewall correspondientes al túnel OpenVPN. En este ejemplo se permite tráfico de entrada y salida sin restricción en la VPN.



Desde la pestaña **Tunnel Settings → NAT** se pueden configurar las reglas NAT correspondientes al túnel OpenVPN. En este ejemplo se enmascara todo el tráfico LAN.

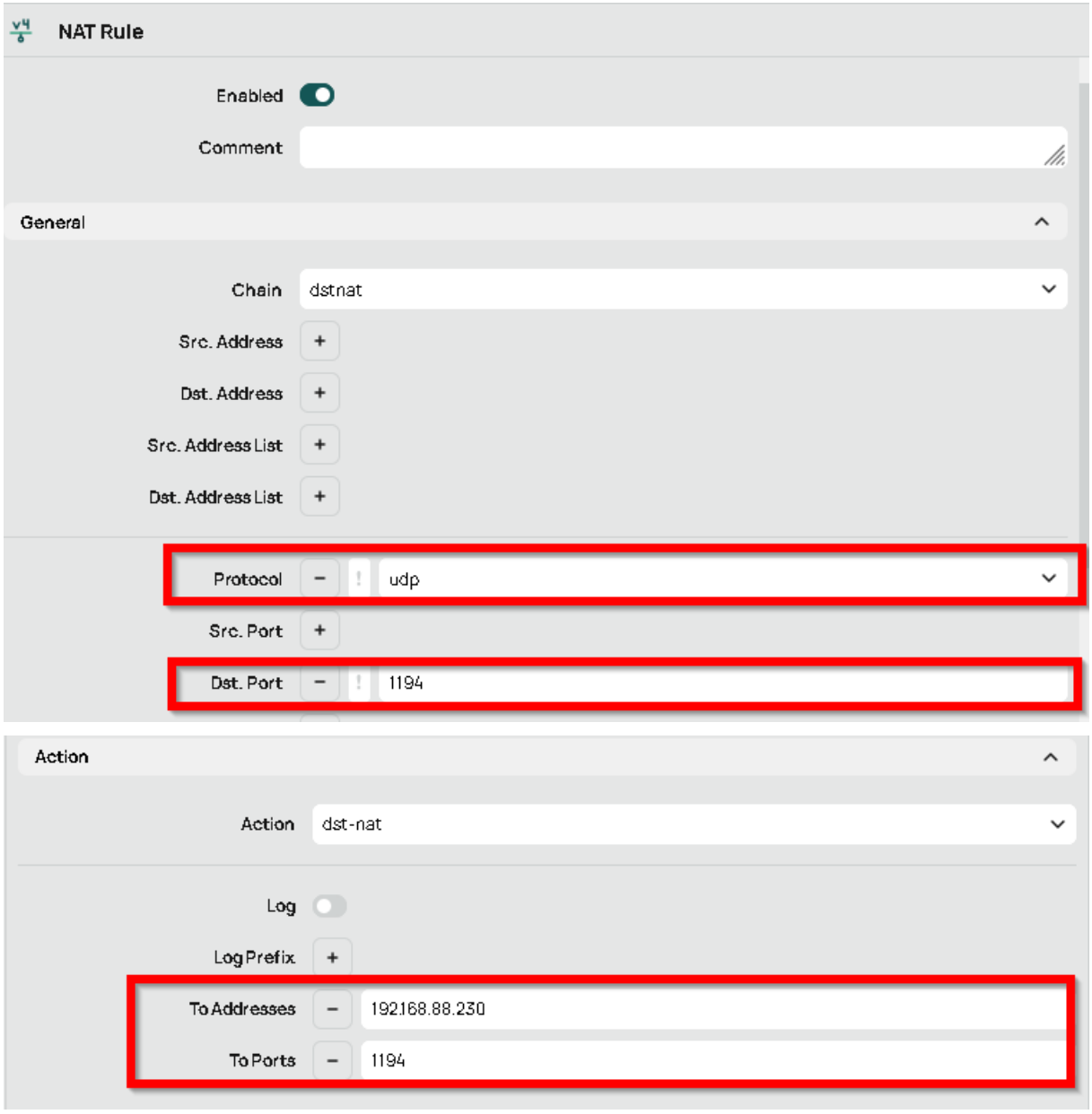


Todos los cambios hechos se muestran en verde y solo son guardados en el mGuard una vez se pulsa el icono del disco de la parte superior derecha.

6 Port Forwading puerto OpenVPN

En el Router de internet de la parte del servidor se debe configurar el port forwading para el puerto UDP 1194 (puerto OpenVPN) y la IP desde la que se ejecuta el servidor OpenVPN.

Es este ejemplo el servidor corre en la 192.168.88.230

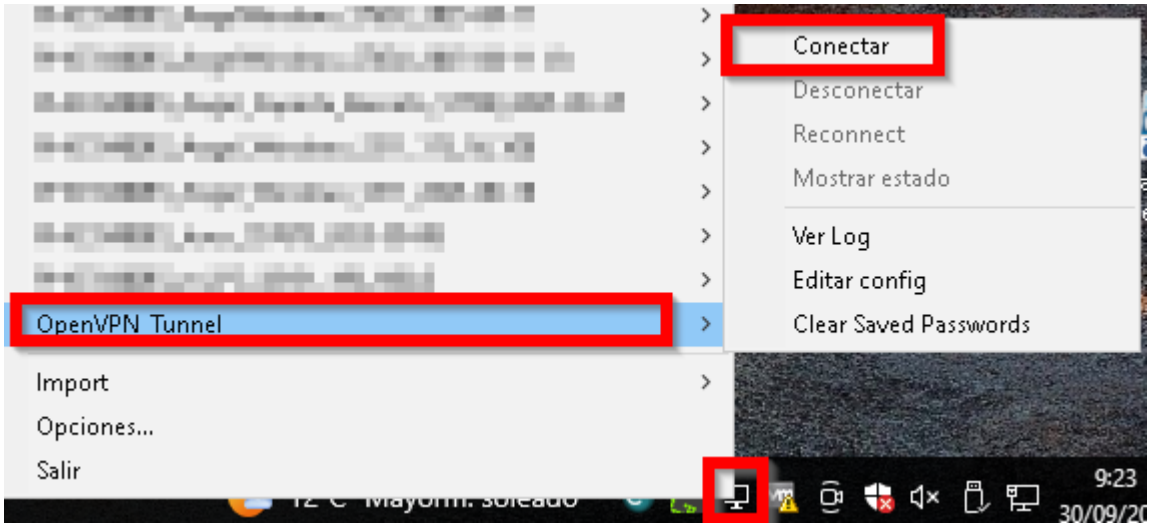


7 Conexión de la OpenVPN

Ejecutar la aplicación **OpenVPN GUI**.

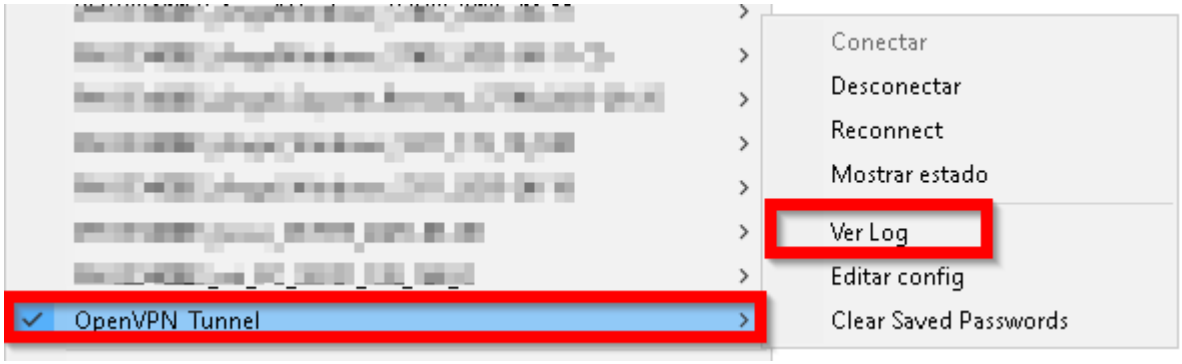
En la barra inferior de Windows aparece un icono de la aplicación.

Boton derecho -> (conexión OpenVPN Server) → Conectar



Una vez conectado la parte del servidor el icono de la aplicación aparece en verde.

8 Chequeo de la conexión



Se observa en el log del servidor la conexión con la parte del cliente mGuard..

OpenVPN_Tunnel.log: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
2025-09-30 15:32:06 88.10.110.177:53082 VERIFY OK: depth=1, O=PHOENIX CONTACT, OU=PxC, CN=CA_XCA
2025-09-30 15:32:06 88.10.110.177:53082 VERIFY OK: depth=0, C=SP, ST=Navarra, L=Pamplona, O=PxC,
2025-09-30 15:32:06 88.10.110.177:53082 peer info: IV_VER=2.6.8
2025-09-30 15:32:06 88.10.110.177:53082 peer info: IV_PLAT=linux
2025-09-30 15:32:06 88.10.110.177:53082 peer info: IV_TCPNL=1
2025-09-30 15:32:06 88.10.110.177:53082 peer info: IV_MTU=1600
2025-09-30 15:32:06 88.10.110.177:53082 peer info: IV_CIPHERS=AES-256-GCM
2025-09-30 15:32:06 88.10.110.177:53082 peer info: IV_PROTO=990
2025-09-30 15:32:06 88.10.110.177:53082 peer info: IV_LZO=1
2025-09-30 15:32:06 88.10.110.177:53082 peer info: IV_COMP_STUB=1
2025-09-30 15:32:06 88.10.110.177:53082 peer info: IV_COMP_STUBv2=1
2025-09-30 15:32:06 88.10.110.177:53082 Note: 'compress migrate' detected remote peer with compre
2025-09-30 15:32:06 88.10.110.177:53082 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_s
2025-09-30 15:32:06 88.10.110.177:53082 TLS: tls_multi_process: initial untrusted session promote
2025-09-30 15:32:06 88.10.110.177:53082 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_
2025-09-30 15:32:06 88.10.110.177:53082 [OpenVPN_Client] Peer Connection Initiated with [AF_INET]
2025-09-30 15:32:06 OpenVPN_Client/88.10.110.177:53082 MULTI_sva: pool returned IPv4=10.1.0.6, IF
2025-09-30 15:32:06 OpenVPN_Client/88.10.110.177:53082 OPTIONS IMPORT: reading client specific op
2025-09-30 15:32:06 OpenVPN_Client/88.10.110.177:53082 MULTI: Learn: 10.1.0.6 -> OpenVPN_Client/8
2025-09-30 15:32:06 OpenVPN_Client/88.10.110.177:53082 MULTI: primary virtual IP for OpenVPN_Clie
2025-09-30 15:32:06 OpenVPN_Client/88.10.110.177:53082 MULTI: internal route 192.168.1.0/24 -> Op
2025-09-30 15:32:06 OpenVPN_Client/88.10.110.177:53082 MULTI: Learn: 192.168.1.0/24 -> OpenVPN_Cl
2025-09-30 15:32:06 OpenVPN_Client/88.10.110.177:53082 SENT CONTROL [OpenVPN_Client]: 'PUSH_REPLY
2025-09-30 15:32:08 OpenVPN_Client/88.10.110.177:53082 Data Channel: cipher 'AES-256-GCM', peer-i
2025-09-30 15:32:08 OpenVPN_Client/88.10.110.177:53082 Timers: ping 10, ping-restart 120
2025-09-30 15:32:08 OpenVPN_Client/88.10.110.177:53082 Protocol options: protocol-flags cc-exit t
2025-09-30 15:33:17 MULTI: Learn: 192.168.1.1 -> OpenVPN_Client/88.10.110.177:53082
2025-09-30 15:33:25 MULTI: Learn: 192.168.1.10 -> OpenVPN_Client/88.10.110.177:53082
```

En el mGuard, desde el menú OpenVPN→ Connections se puede comprobar la VPN está establecida.