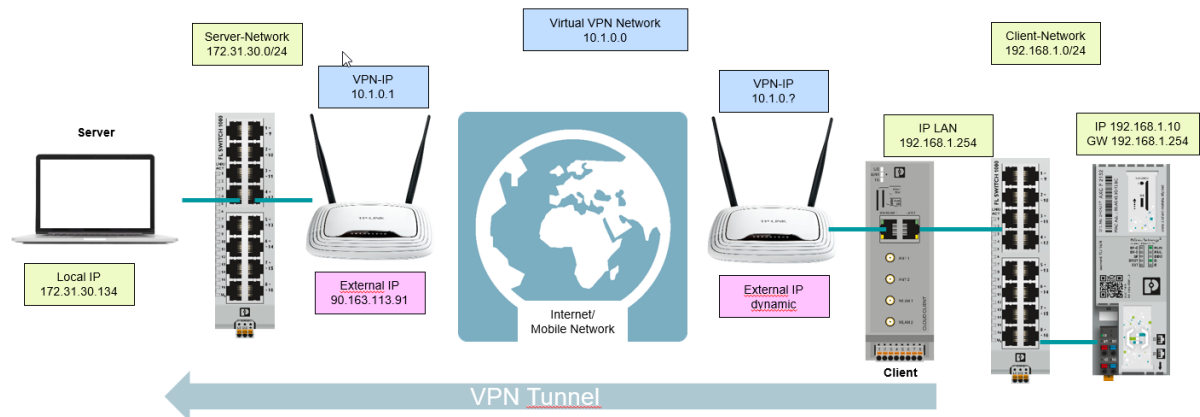


# Guía de Configuración OpenVPN Cliente con TC Router



# 1 Introducción

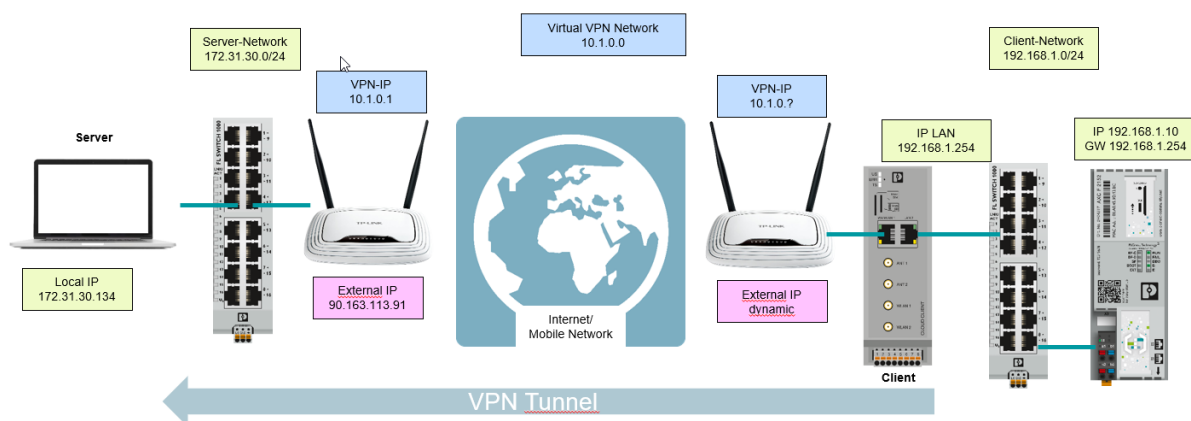
Esta guía muestra como configurar una conexión OpenVPN entre:

OpenVPN Server (Windows)

OpenVPN Client (TC Router 4102T-4G EU WLAN – 1234353)

El procedimiento es nuestros TC Router xxxx VPN.

La configuración desarrollada es la siguiente.



## 2 Instalación de OpenVPN en Windows

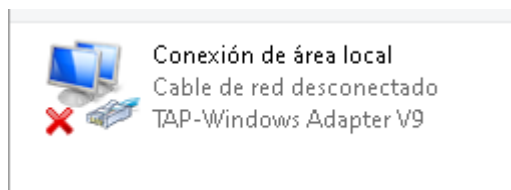
Descarga la versión actual desde este link:

[Community Downloads | OpenVPN](https://openvpn.net/community-downloads/)

<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 Creación de certificados

Los certificados son necesarios en una conexión segura OpenVPN. Se pueden crear con el correspondiente software. En esta guía los certificados se crean con el programa XCA.

En esta guía no se detalla como crear y exportar los certificados. Phoenix Contact tiene una guía de como hacerlo con XCA.

El programa XCA se puede descargar desde:

[Download \(hohnstaedt.de\)](https://www.hohnstaedt.de/download/)

Para una conexión OpenVPN se necesitan:

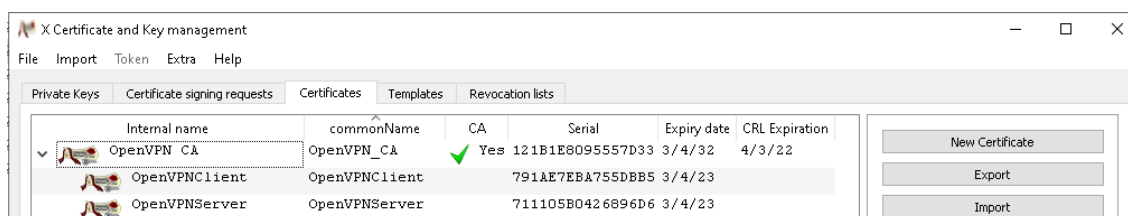
2 x certificados de máquina.p12 (para cliente y servidor)

1 x certificado CA CA.crt

1 x certificado de parámetros Diffie-Hellmann dh2048.pem (guardado en la configuración de OpenVPN)

Una vez creados los certificados tenemos el certificado de la autoridad certificadora (OpenVPN\_CA), el certificado de cliente (OpenVPNClient) y el certificado del servidor (OpenVPNServer).

Es importante que en los certificados de cliente y servidor el "Internal Name" sea el mismo que el "commonName".



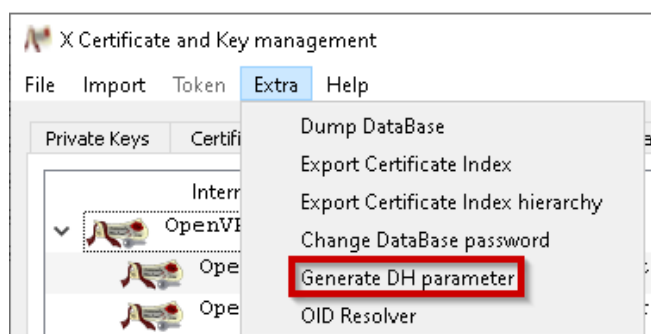
Exporta los certificados OpenVPNCClient y OpenVPNServer con el formato “p12” o “pfx”.

Ambos formatos son la copia de seguridad del certificado con su clave privada.

Guarda certificado exportado “OpenVPNServer.pfx” o .p12 en el directorio “C:\Program Files\OpenVPN\config”.

### 3.1 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.

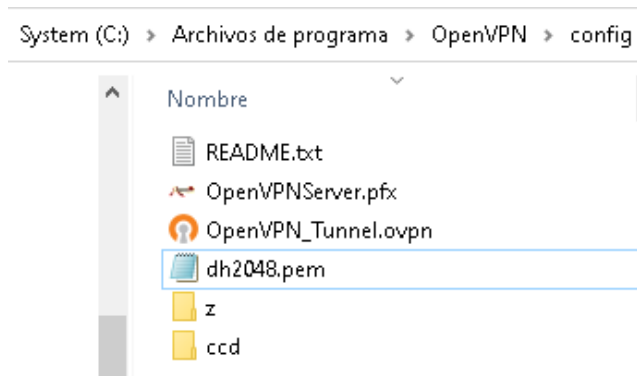


Guarda con el nombre “dh2048.pem” en el directorio “C:\Program Files\OpenVPN\config”.

## 4 Configuración del OpenVPN Server

Utiliza un editor de texto para crear un fichero de configuración con el nombre "OPENVPN\_Tunnel.opvn". Asegúrate 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.

```
# This is a sample configuration for an OpenVPN server
# Parameters to be filled in

server 10.1.0.0 255.255.255.0      # IP address pool of the OpenVPN server
pkcs12 OpenVPNServer.pfx          # Container with the necessary certificates
dh dh2048.pem                     # File with the Diffie Hellmann parameter set

# Fix Parameters
proto udp                         # Protocol used for the tunnel
rport 1194                       # Port to be used on the remote station
lport 1194                       # Local port
comp-lzo                         # LZO compression
cipher AES-256-CBC              # Encryption algorithm used
tun-mtu 1500                    # Maximum size of the data packets
reneg-sec 3600                  # Interval for key renewal (in seconds)
ping 30                         # Connection check after 30 seconds without data traffic
ping-restart 60                 # Restart connection after 60 seconds without ping from the remote
station
verb 3                          # Detailedness of the log message
dev tun                         # OpenVPN network device
float                           # Accept packages from all computers (float)

# Create a route for the client
push "route 172.31.30.0 255.255.255.0" # Real server network
# Define the routes for the clients
client-config-dir ccd           # Directory for the client network
# Add Windows routes
route 192.168.1.0 255.255.255.0 # Client IP address space
```

## 4.1 Enrutamiento

Requerimientos:

El programa OpenVPN instalado en el ordenador que debe correr el servidor.

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 172.31.30.0/24.

```
# Create a route for the client
push "route 172.31.30.0 255.255.255.0" # Real server
network
```

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

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

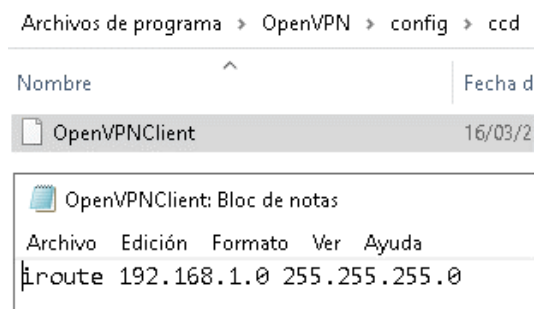
```
# Define the routes for the clients
client-config-dir ccd                # Directory for the client network
```

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

Ten 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.

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 TC Router... como cliente

Habilita el servicio OpenVPN

Pestaña VPN -> OpenVPN -> Administration -> Administrative Status: Enabled

Home Interfaces Routing Network Security **VPN** Services System Logout

TC ROUTER  
1234353



OpenVPN

[Administration](#)

[Tunnel Configuration](#)

### OpenVPN Administration

Administrative status:	<input checked="" type="radio"/> enabled <input type="radio"/> disabled
Restart on link change:	<input checked="" type="checkbox"/>
Multipath TCP support:	<input type="checkbox"/>
Restart OpenVPN:	<input type="button" value="Restart"/>

Configuración del cliente OpenVPN. Se pueden configurar hasta 4 tuneles OpenVPN

Pestaña VPN -> OpenVPN -> Tunnel Configuration -> Tunnel 1

*Operation mode:* Client. Standard

*Peer selection:* single. Server: < direccion IP pública del OpenVPN Server >. Port: 1194

*Interface type:* TUN

*Protocol:* UDP


*Network mode:* routed

*Authentication:* certificate-based. HMAC digest: SHA1

*Encryption:* AES-256-CBC

*Options:* use compression: on. use keepalive: on

TC ROUTER  
1234353



OpenVPN

Administration

**Tunnel Configuration**

IPsec

Administration

Tunnel Configuration

PPTP

Administration

Tunnel Configuration

Home Interfaces Routing Network Security VPN Services System Logout

Tunnel 1

Tunnel 2

Tunnel 3

Tunnel 4

OpenVPN Tunnel 1 Configuration

Operation mode:

☐ disabled
☒ client
☐ server
☒ standard
☐ expert

Peer selection:

single

Server: 90.163.113.91 Port: 1194

Interface type:

TUN

Protocol:

UDP

Network mode:

☒ routed MTU:
☐ bridged

Authentication:

certificate-based

HMAC digest: SHA1

Encryption:

AES-256-CBC

Options:

☒ use compression
☐ redirect gateway
☒ use keepalive
☐ negotiate DNS

Apply

Erase


Download

Pulsa el botón *Apply*.

Al seleccionar la autenticación basada en certificados aparece el siguiente link, al cual pulsaremos para subir los certificados del cliente al TC Router.

Pulsamos en *< Manage keys and certificates >*

TC ROUTER  
1234353



OpenVPN

Administration

**Tunnel Configuration**

IPsec

Administration

Tunnel Configuration

PPTP

Administration

Tunnel Configuration

GRE

Home Interfaces Routing Network Security VPN Services System Logout

Tunnel 1

**Tunnel 2**

Tunnel 3

Tunnel 4

OpenVPN Tunnel 2 Configuration

Operation mode:

☐ disabled
☒ client
☐ server
☒ standard
☐ expert

Peer selection:

single

Server: 92.163.91.91 Port: 1194

Interface type:

TUN

Protocol:

UDP

Network mode:

☒ routed MTU:
☐ bridged

Authentication:

certificate-based

HMAC digest: SHA1

root certificate, client certificate and client key are missing

Manage keys and certificates

Encryption:

AES-256-CBC

Options:

☒ use compression
☐ redirect gateway
☒ use keepalive
☐ negotiate DNS

Apply

Erase

Download

Action: upload files

**Select file:** Pulsamos el botón y elegimos el certificado anteriormente creado para el cliente (pfx or p12 extension)

**Passphrase:** escribimos la contraseña del certificado.

Pulsamos el botón **RUN**.



[Home](#) [Interfaces](#) [Routing](#) [Network Security](#) [VPN](#) [Services](#) [System](#) [Logout](#)

#### OpenVPN2

The certificates used for authenticating OpenVPN Tunnel 2 running in client mode

CA certificate	missing
Client certificate	missing
Client key	missing

Action:

Select file:  OpenVPNClient.pfx

Passphrase:

Los certificados CA de cliente y la llave privada se instalan en el TC Router.



[Home](#) [Interfaces](#) [Routing](#) [Network Security](#) [VPN](#) [Services](#) [System](#) [Logout](#)

#### OpenVPN1

The certificates used for authenticating OpenVPN Tunnel 1 running in client mode

CA certificate	installed	<a href="#">view</a>
Client certificate	installed	<a href="#">view</a>
Client key	installed	<a href="#">view</a>

Action:

X.509 attributes: C=DE, ST=Germany, L=Blomberg, O=PHOENIX CONTACT GmbH & Co. KG, OU=Communication Interfaces, CN=TC-ROUTER/emailAddress=info@phoenixcontact.de

## 6 Port Forwarding puerto OpenVPN

En el Router de internet de la parte del servidor se debe configurar el port forwarding 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 172.31.30.134

	OpenVPN	1194	1194	UDP	172.31.30.134	
---	---------	------	------	-----	---------------	---

## 7 Requisitos para la conexión cliente con el TC Router

Alguno de los interfaces del TC Router debe estar conectado a internet o la red móvil.

En este ejemplo la interfaz cableada LAN 1 está conectada a internet.


Home -> Summary

Home [Interfaces](#) [Routing](#) [Network Security](#) [VPN](#) [Services](#) [System](#)

**Summary**

Description	Administrative Status	Operational Status
Hotlink		<a href="#">LAN1</a>
LAN1	enabled	up
OpenVPN1	enabled, client	up

TC ROUTER  
1234353




Status

[Summary](#)

Interfaces -> Ethernet -> IP Settings

Home Interfaces Routing Network Security VPN Services System Logout



TC ROUTER  
1234353

WAN

[Link Management](#)

[Supervision](#)

[Settings](#)

Ethernet

[Port Setup](#)

[VLAN Management](#)

[IP Settings](#)

IP Address Management

Network Interface	Mode	IP Address Mode	IP Address	Netmask	
LAN1	WAN	DHCP mode	172.31.31.105	24	
LAN2	LAN	Static IP	192.168.1.254	24	

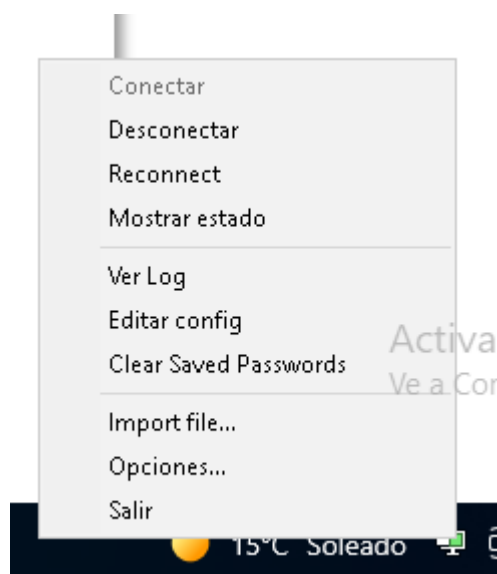
El firewall tanto del servidor como del TC Router no debe impedir la comunicación por el puerto UDP 1194.

## 8 Conexión de la OpenVPN

Ejecutar la aplicación OpenVPN GUI.

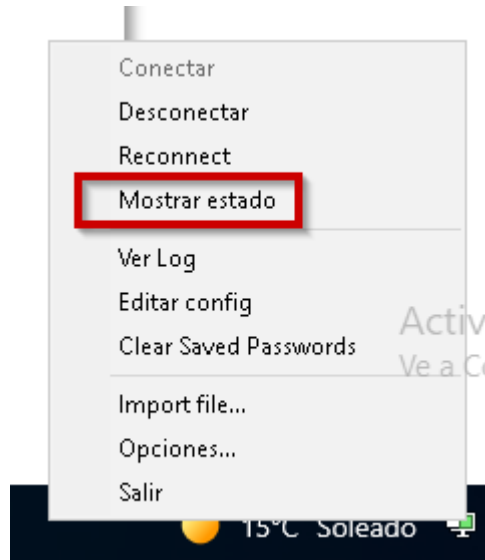
En la barra inferior de Windows aparece un icono de la aplicación.

Boton derecho -> Conectar

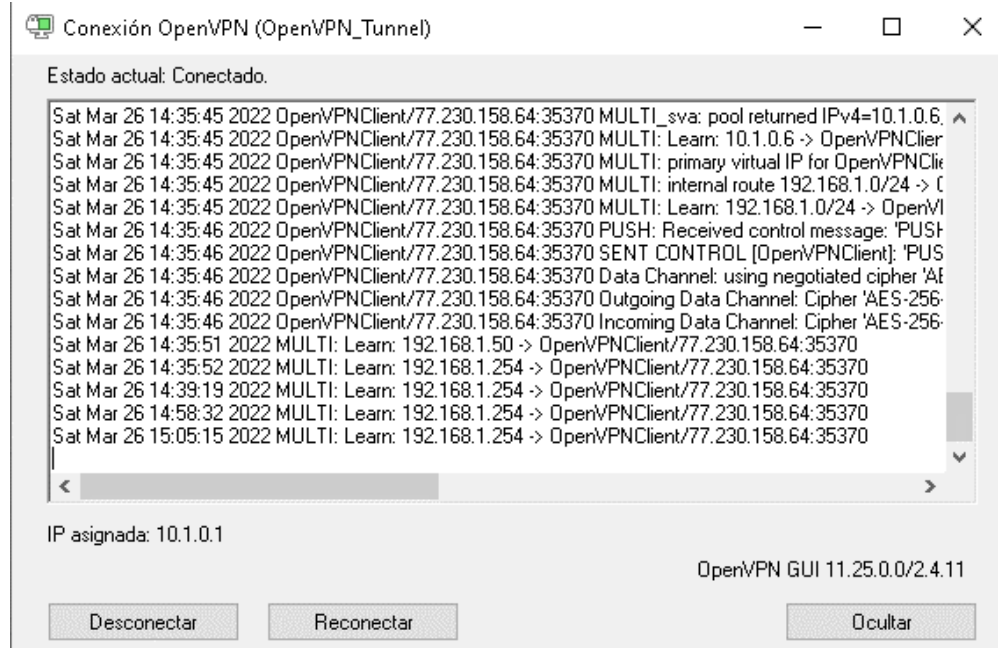


Una vez conectado la parte del servidor el icono de la aplicación aparece en verde.

## 9 Chequeo de la conexión



Se observa en log la conexión con la parte del cliente TC Router.




## 10 Conexión remota via OpenVPN con TC Router y PLC

Se observa como desde el servidor OpenVPN se tiene conexión a los dispositivos en la parte del cliente.

No seguro | <https://192.168.1.10/wbm/>

Deutsch
English



Please login with your username and password.

Username
Enter Username

Password
Enter Password

Login

Hinweis:

Dieses Gerät darf nur von autorisierten Benutzern für autorisierte Zwecke verwendet werden. Ihre Anmeldeinformationen und alle Benutzeraktionen auf diesem Gerät können überwacht, aufgezeichnet, kopiert und auditiert werden.


Durch die weitere Verwendung dieses Geräts erklären Sie sich mit diesen Bedingungen einverstanden.

Notice:

This device may only be used by authorized users for authorized purposes. Your credentials and all user actions on this device can be monitored, recorded, copied and audited. By continuing to use this device, you agree to these terms.


TC ROUTER
x
+

<https://192.168.1.254/admin/status.php>



Home
Interfaces
Routing
Network Security
VPN
Services
System
Logout

TC ROUTER  
1234353



Status
Summary
Mobile
VLAN
LAN
Ports
Bridges
DHCP
OpenVPN
Firewall
General Info

PHOENIX CONTACT  
Hostname: TC-ROUTER  
Firmware Version: 4.5.72.104  
©2021, PHOENIX CONTACT GmbH & Co. KG


2022-03-25 14:03
Successfully installed key/certificate

2022-03-25 14:02
No files have been imported

Summary

Description	Administrative Status	Operational Status
Hotlink		LAN1
LAN1	enabled	up
OpenVPN1	enabled, client	up

Guía de Configuración



15

## Tabla de contenido

1	Introducción .....	2
	.....	3
2	Instalación de OpenVPN en Windows .....	3
3	Creación de certificados .....	3
3.1	Creación de fichero de parámetros Diffie Hellmann .....	4
4	Configuración del OpenVPN Server .....	5
4.1	Enrutamiento.....	6
5	Configuración del TC Router... como cliente.....	9
6	Port Forwarding puerto OpenVPN .....	12
7	Requisitos para la conexión cliente con el TC Router .....	12
8	Conexión de la OpenVPN.....	13
9	Chequeo de la conexión .....	14
10	Conexión remota via OpenVPN con TC Router y PLC.....	15