

# TITAN

## Application Note 46

---

IPSEC - Server

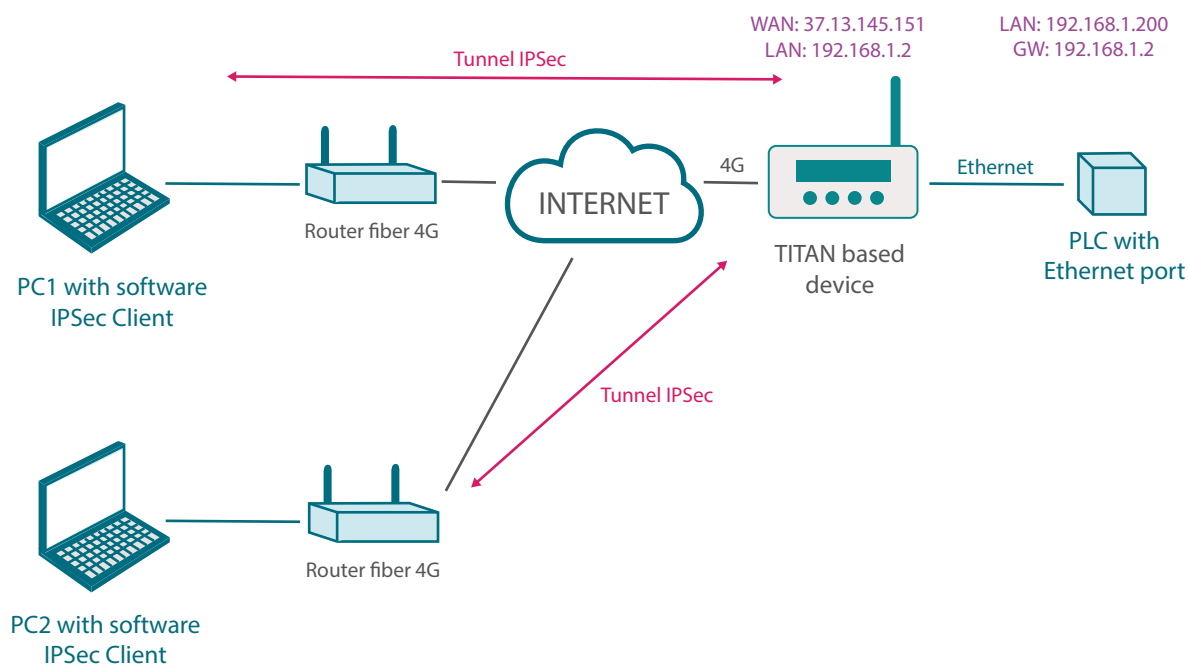
IKEv1 - Authentication Using a Certificate

# IPSEC - Server - IKEv1 - Authentication Using a Certificate

## 1. Scenario Details

We want to remotely access the configuration page of a TITAN-based device, and a PLC connected to it via Ethernet, from two locations. We also want to do this using a secure IPsec connection. We intend to use digital certificate authentication.

Example of the proposed scenario:



Basically, in this example we want to create an IPsec VPN from a pair of PCs (each of which has an IPsec Client such as TheGreenBow, which is used in this example) to a remote 4G TITAN-based device that will act as an IPsec Server, which in turn has a PLC connected to its Ethernet port. Each IPsec client must authenticate itself on the server using a valid client digital certificate.

## 2. Configurations and Prerequisites

The basic requirement for this is that the SIM card inserted in the TITAN-based device acting as the IPsec Server must have public and static IP addresses. This is necessary in order to access it remotely from a PC connected to the Internet. We must also make sure that all the devices are set to the correct time, since the generation and verification of certificates will require this.

### 3. IPSEC Configuration of the TITAN-based Device

First we must go to the “VPN > IPSEC” menu. For the planned configuration we will need the “ca-cert.pem”, and “server-cert.pem” certificates. As well as your private keys “ca-key.pem” and “server-key.pem”. We will also need a pair of client certificates with their private keys “client1-cert.pem”, “client1-key.pem”, “client2-cert.pem” and “client2-key.pem”.

At this point there are two options. 1) If these certificates are available, they can be uploaded manually from the section marked in red:

OpenVPN EasyLink

- IPSec
- Plugins
  - Link
  - Nonat
  - Wifiscan
- Device Manager
  - Cervello
- Other
  - DynDns
  - Private DynDns
  - Digital Input 1
  - Digital Input 2
  - ModBus Slave
  - Titan Scripts
  - Jamming detection
  - AT Command
  - Sms control
  - Email configuration
  - Gsm Location
  - Periodic Autoreset
  - Custom Skin
  - Custom Led
  - Time Servers
  - Advanced Routing
  - Remote Console
  - Snmp
  - Tacacs+
  - Mqtt
  - Https
  - Audio
  - User Permissions
  - Passwords Web UI
  - Backup / Factory
  - Firmware Upgrade
  - Reboot
  - Logout

VPN > IPSEC > Client Certificates (files needed for "IPSec client" mode)

CA certificate: file 'ca1-cert.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Client Certificate: file 'xclient1-cert.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Client KEY: file 'xclient1-key.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded

DELETE ALL CLIENT CERTIFICATES

VPN > IPSEC > Server Certificates (files needed for "IPSec server" mode)

CA certificate: file 'ca-cert.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
CA key: file 'ca-key.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Server Certificate: file 'server-cert.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Server KEY: file 'server-key.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Client 1 Certificate: file 'client1-cert.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Client 2 Certificate: file 'client2-cert.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Client 3 Certificate: file 'client3-cert.pem'	Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded

DELETE ALL SERVER CERTIFICATES GENERATE ALL SERVER CERTIFICATES AUTOMATICALLY

2) If no certificates are available, the TITAN-based device has a button that will create them. When you press the button, all certificates will be generated automatically. The process may take up to 5 minutes to complete. Click on the “REFRESH” button to check the status of the process.

Snmp

- Tacacs+
- Mqtt
- Https
- Audio
- User Permissions
- Passwords Web UI
- Backup / Factory
- Firmware Upgrade
- Reboot
- Logout

file 'server-cert.pem'

Server KEY:  
file 'server-key.pem'

Client 1 Certificate:  
file 'client1-cert.pem'

Client 2 Certificate:  
file 'client2-cert.pem'

Client 3 Certificate:  
file 'client3-cert.pem'

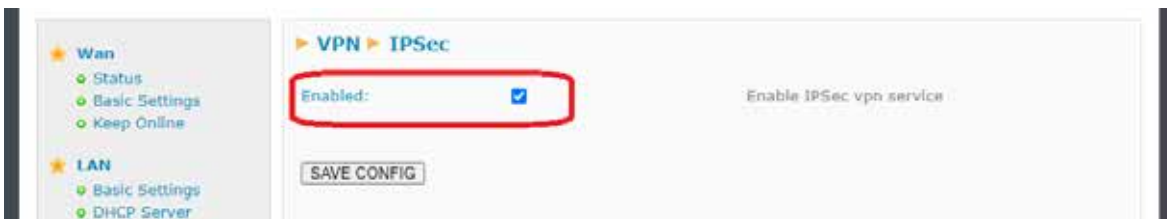
Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded
Seleccionar archivo	Ningún archivo seleccionado	Upload	not uploaded

DELETE ALL SERVER CERTIFICATES GENERATE ALL SERVER CERTIFICATES AUTOMATICALLY

In this example, we will use the second option to generate all certificates automatically. To do this, click on the “GENERATE ALL SERVER CERTIFICATES AUTOMATICALLY” button. Once the process has finished correctly, the result will be:



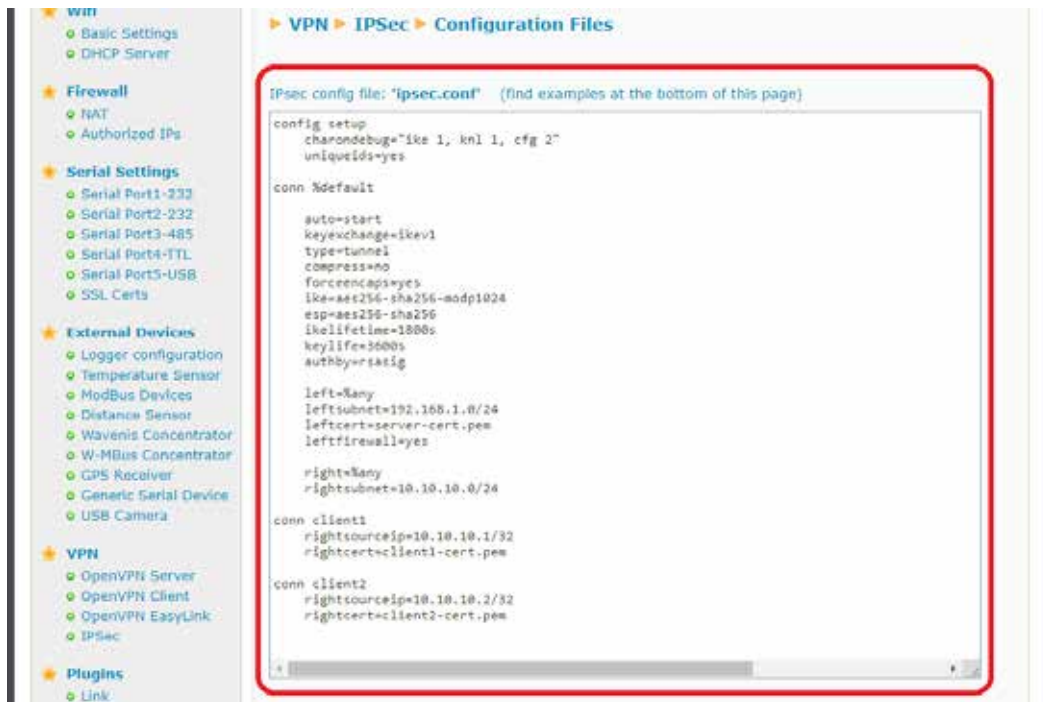
Once you have the necessary certificates, we can proceed with the actual configuration of the VPN. To do this, check the “Enabled” box at the top of the configuration page and click on the “SAVE CONFIG” button.



Lastly, since the TITAN-based device’s IPSec service is based on strongswan, the “ipsec.conf” and “ipsec.secrets” files must also be configured. The simplest solution is to go to the examples at the bottom of the page and choose the example that is closest to your configuration needs. For this application note we will choose example 6, clicking on (downloading) the corresponding “ipsec.conf” and “ipsec.secrets” files, which we will open with a notepad to extract their contents.



This content must be tailored to the example and inserted into the appropriate boxes. For “ipsec.conf”:



And for “ipsec.secrets” (you must click on the “Show/Hide” legend beforehand to display the box):



Next we click on the “SAVE CONFIG” button, which will record the contents of both files in the TITAN-based device’s internal memory. Lastly, if the IPsec service was not started when the device started (i.e. the “Enabled” box was not checked), it must be fully restarted (“Other>Reboot” menu). If the IPsec service was already started (“Enabled” box checked), you can just click on the “RESTART IPSEC” button to restart the IPsec service with the new configuration, without having to restart the device itself, which is a much faster option.

Once the TITAN-based device has been restarted or the “RESTART IPSEC” button has been pressed (if the service was already active), the IPSEC connection status will appear as shown below. If the “Status” box is blank, the service may not yet have started. Wait a few seconds and click on the “REFRESH” button.

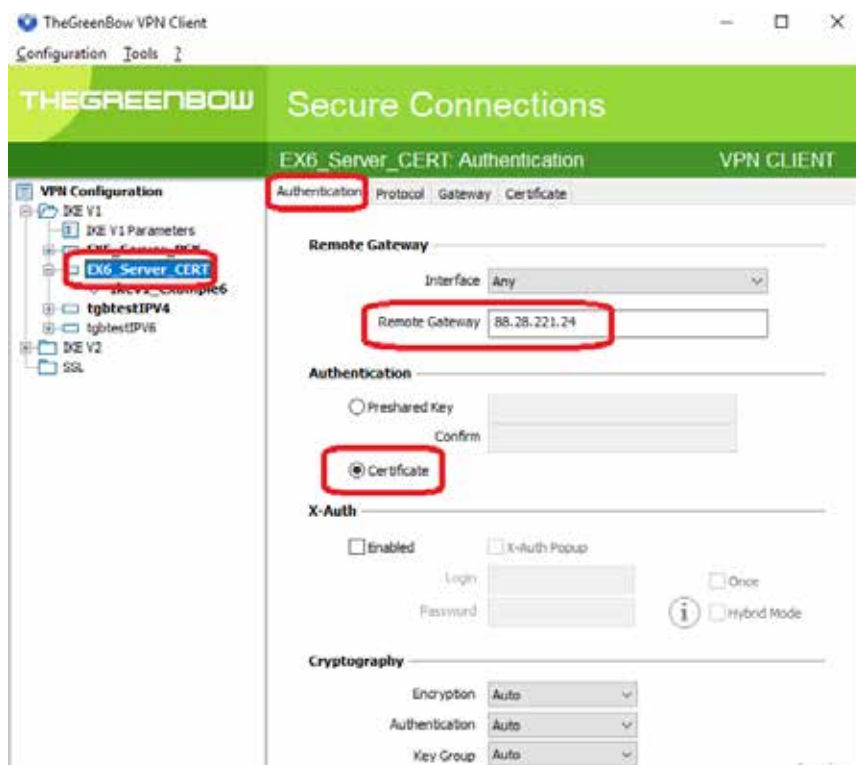


## 4. Configuring the IPSEC Client

In this example, the well-known TheGreenBow software for PCs will be used as the IPsec client when connecting to the TITAN-based device. Below you will find several screenshots showing the basic configuration of each section. This configuration refers to the IPsec client 1 PC. The configuration of the IPsec client 2 PC is entirely analogous.

### 4.1 Authentication

The TITAN-based device’s public IP address method must be entered in the “Authentication” section of the IKEv1 connection (in this example it is 88.28.221.24), the authentication method is by digital certificate.





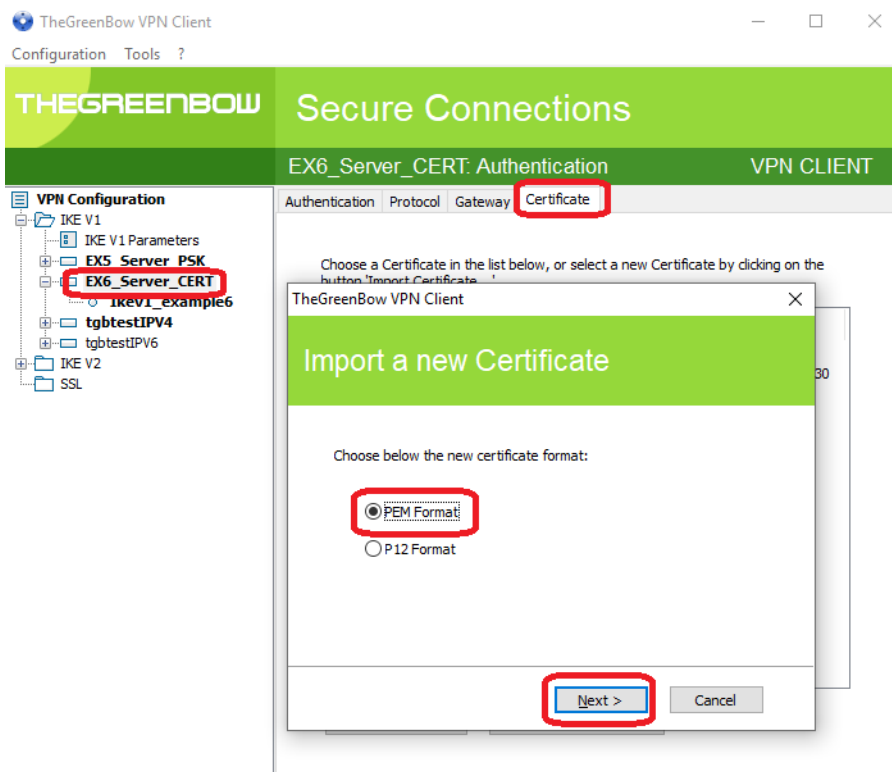
## 4.2 Certificate

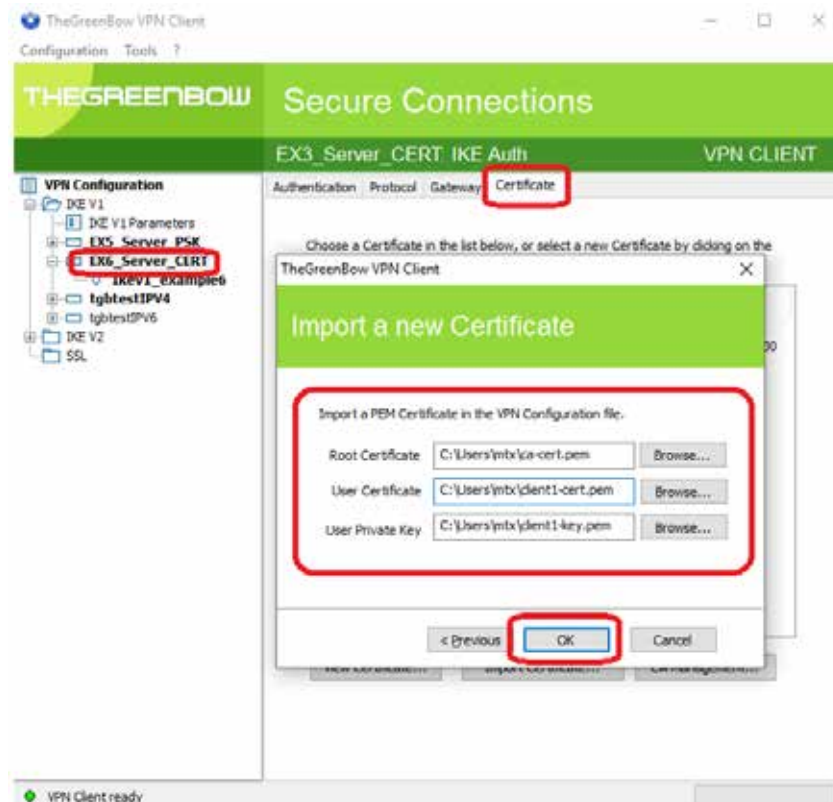
You must specify the client certificate and CA certificate to be used in the "Certificate" section. These certificates can be downloaded from the TITAN-based device itself, as they were generated in the previous step.



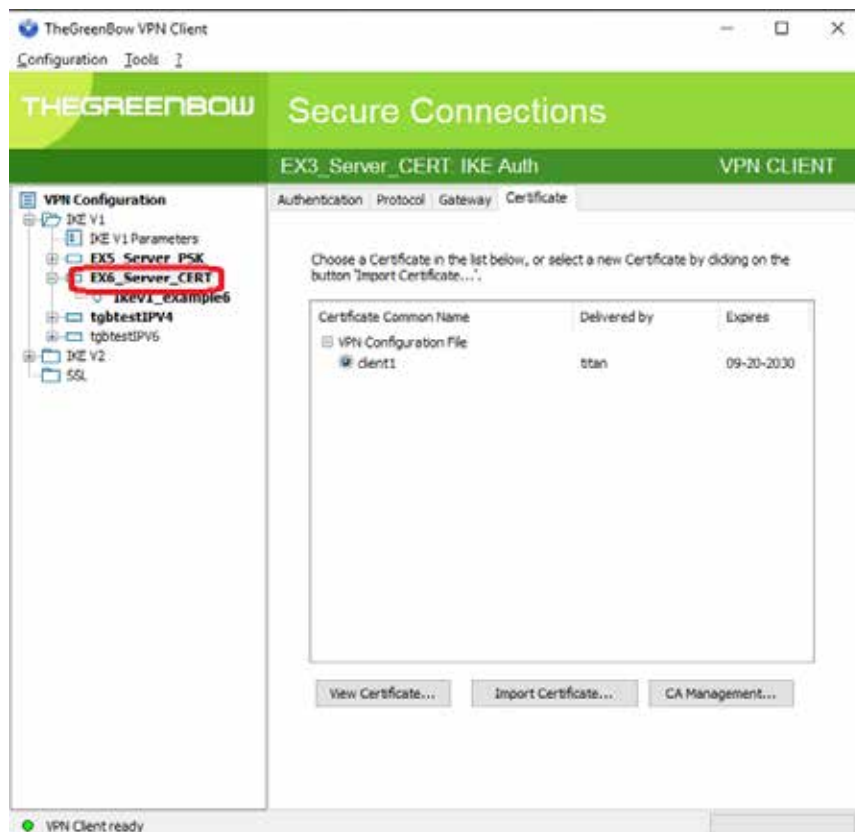
You will first need to download the “ca-cert.pem”, “client1-cert.pem” and “client1-key.pem” files for PC1, and the “ca-cert.pem”, “client2-cert. pem” and “client2-key.pem” files for PC2.

The certificates (in “PEM” format) are selected in the “Certificate” tab.



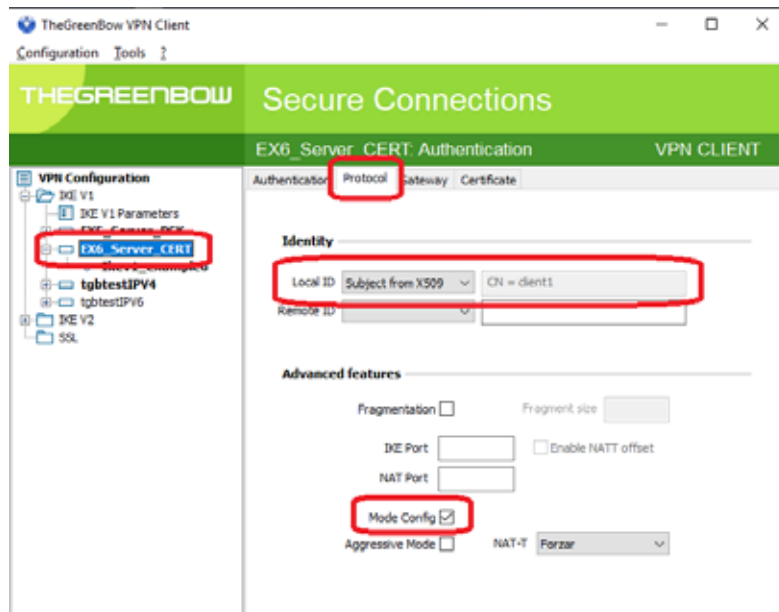


The certificate will be displayed as long as it was imported correctly.

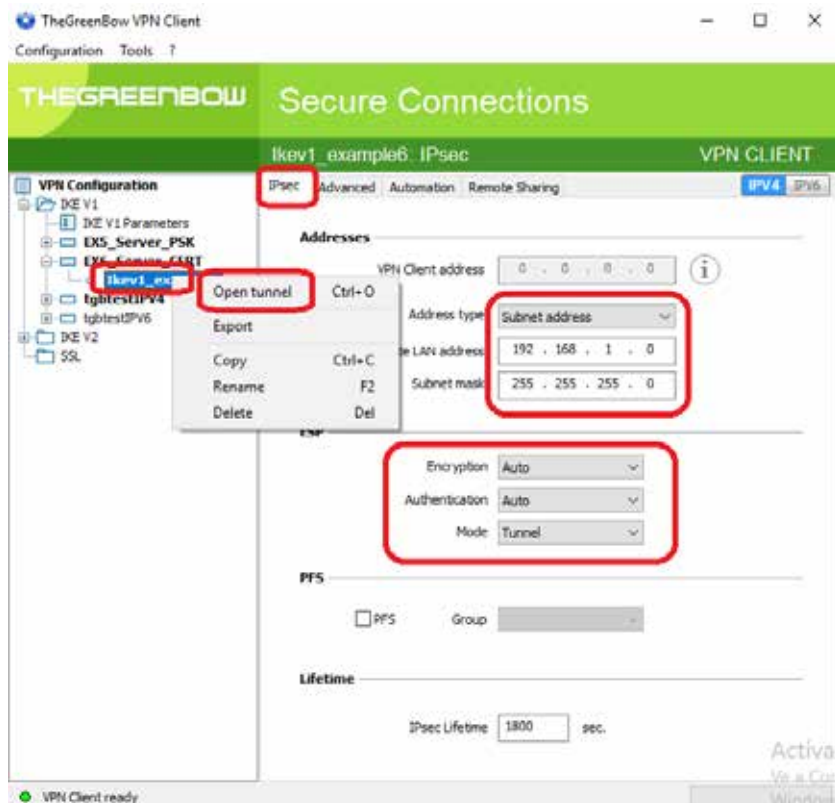


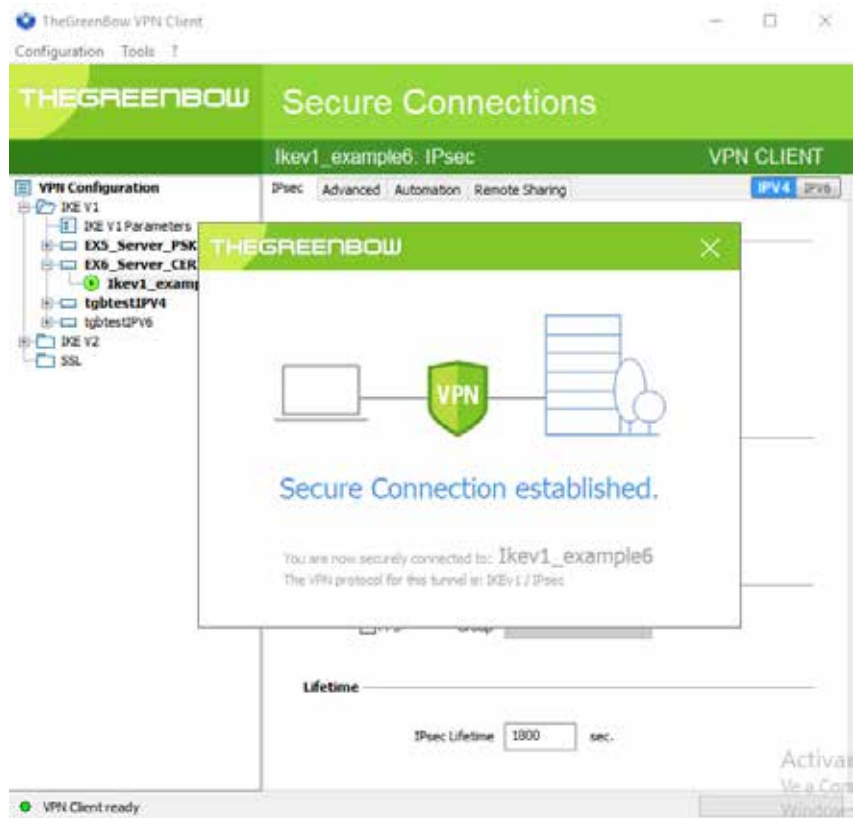


The Local ID with the CN that has just been imported will automatically be displayed as selected in the “Protocol” tab. In this example, the TITAN-based device (IPSec Server) is supposed to assign the IP address to the clients (as can be seen in the “ipsec.conf” file, where PC1 will be assigned the IP 10.10.10.1). You must therefore select the “Mode Config” option.



We can now open the IPSec tunnel by right-clicking on the connection and clicking on the “Open tunnel” option, as shown in the following screen, where we configure the network used by the TITAN-based device IPSec Server (192.168.1.0 / 255.255.255.0).

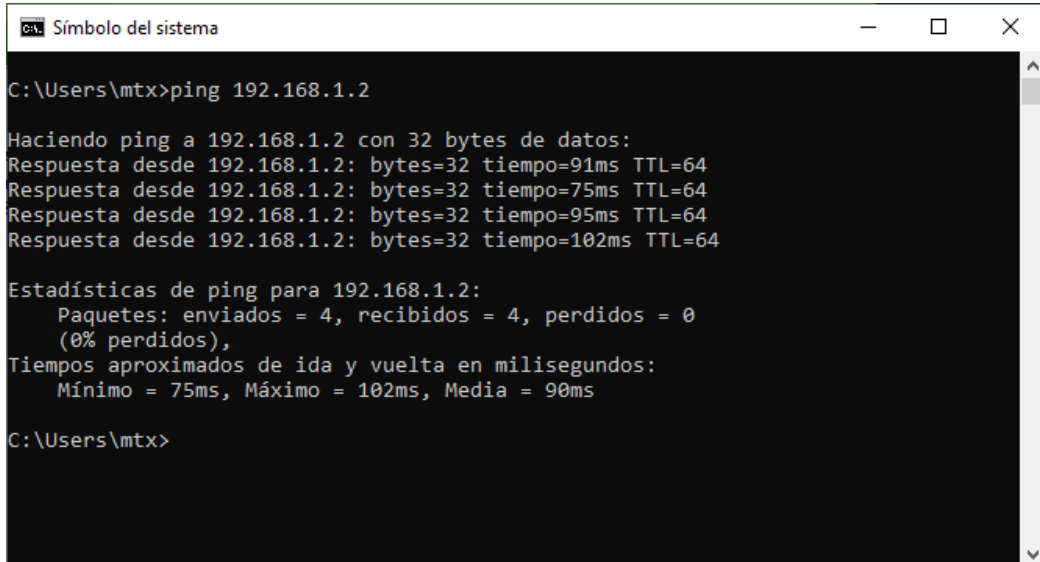




## 5. Checking Connectivity

If the connection process was successful, we just need to check the connectivity, i.e. that the IPSec client 1 PC can access both the TITAN-based device (IP: 192.168.1.2) and the PLC connected to it (IP: 192.168.1.200). This can be done with a couple of PINGS.

A Ping sent from the PC1 to the TITAN-based device via the IPSec VPN:



```
Símbolo del sistema

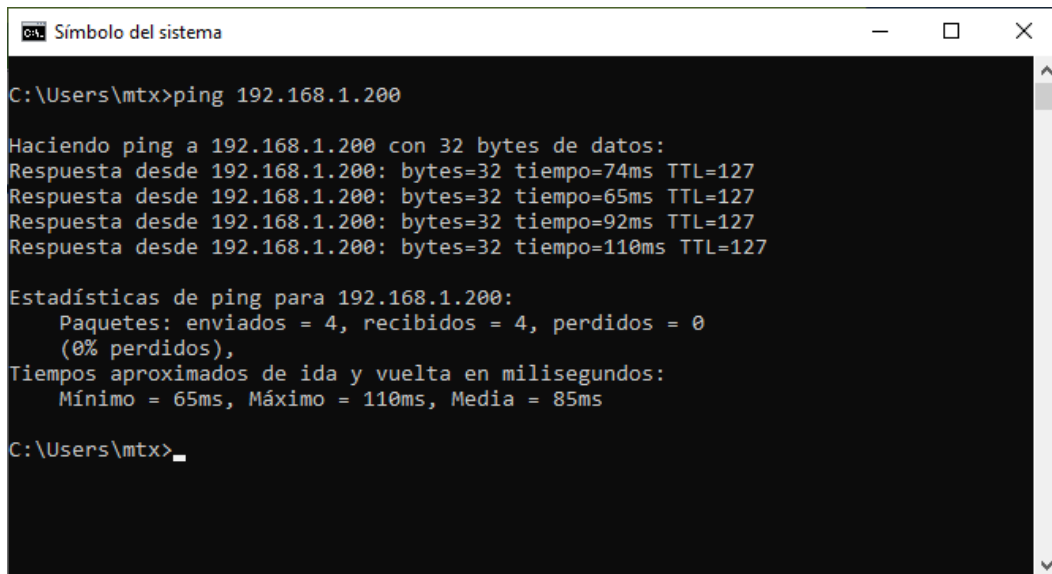
C:\Users\mtx>ping 192.168.1.2

Haciendo ping a 192.168.1.2 con 32 bytes de datos:
Respuesta desde 192.168.1.2: bytes=32 tiempo=91ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=75ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=95ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=102ms TTL=64

Estadísticas de ping para 192.168.1.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 75ms, Máximo = 102ms, Media = 90ms

C:\Users\mtx>
```

A Ping sent from the PC1 to the PLC via the IPSec VPN:



```
Símbolo del sistema

C:\Users\mtx>ping 192.168.1.200

Haciendo ping a 192.168.1.200 con 32 bytes de datos:
Respuesta desde 192.168.1.200: bytes=32 tiempo=74ms TTL=127
Respuesta desde 192.168.1.200: bytes=32 tiempo=65ms TTL=127
Respuesta desde 192.168.1.200: bytes=32 tiempo=92ms TTL=127
Respuesta desde 192.168.1.200: bytes=32 tiempo=110ms TTL=127

Estadísticas de ping para 192.168.1.200:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 65ms, Máximo = 110ms, Media = 85ms

C:\Users\mtx>
```