webdyn
flexitron group

TITAN

Application Note 43

IPSEC - Server

IKEv2 - Authentication Using a Certificate

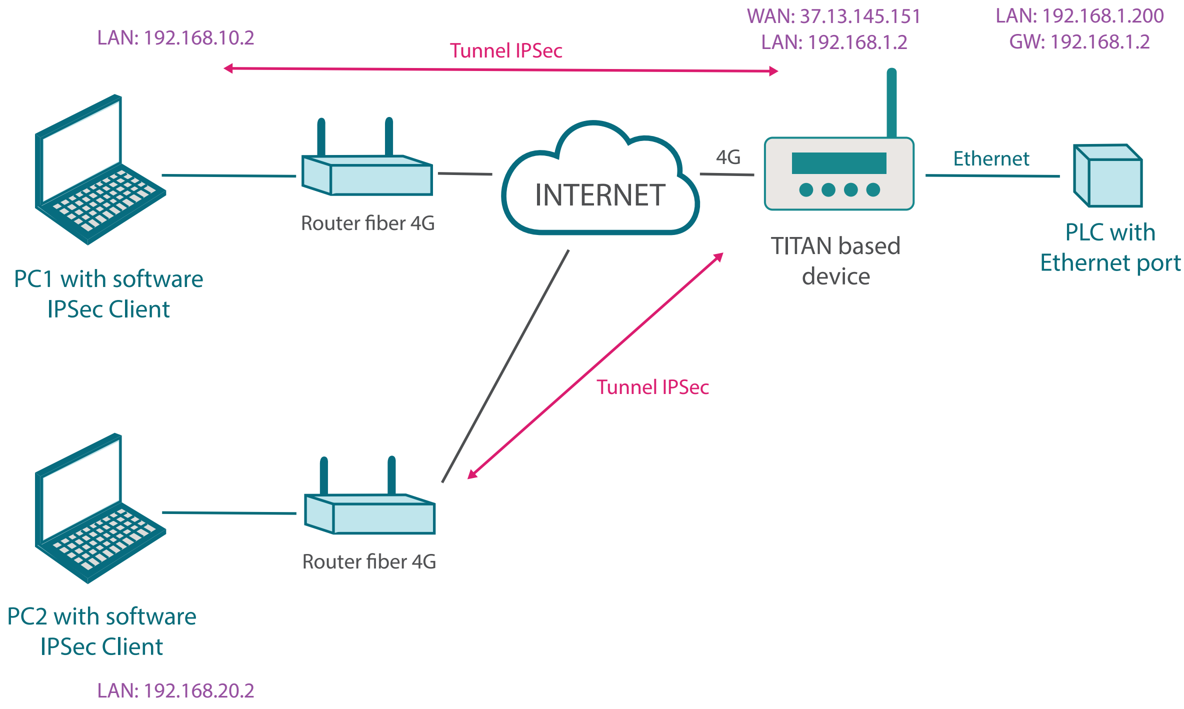
www.webdyn.com

IPSEC - Server - IKEv2 - 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.

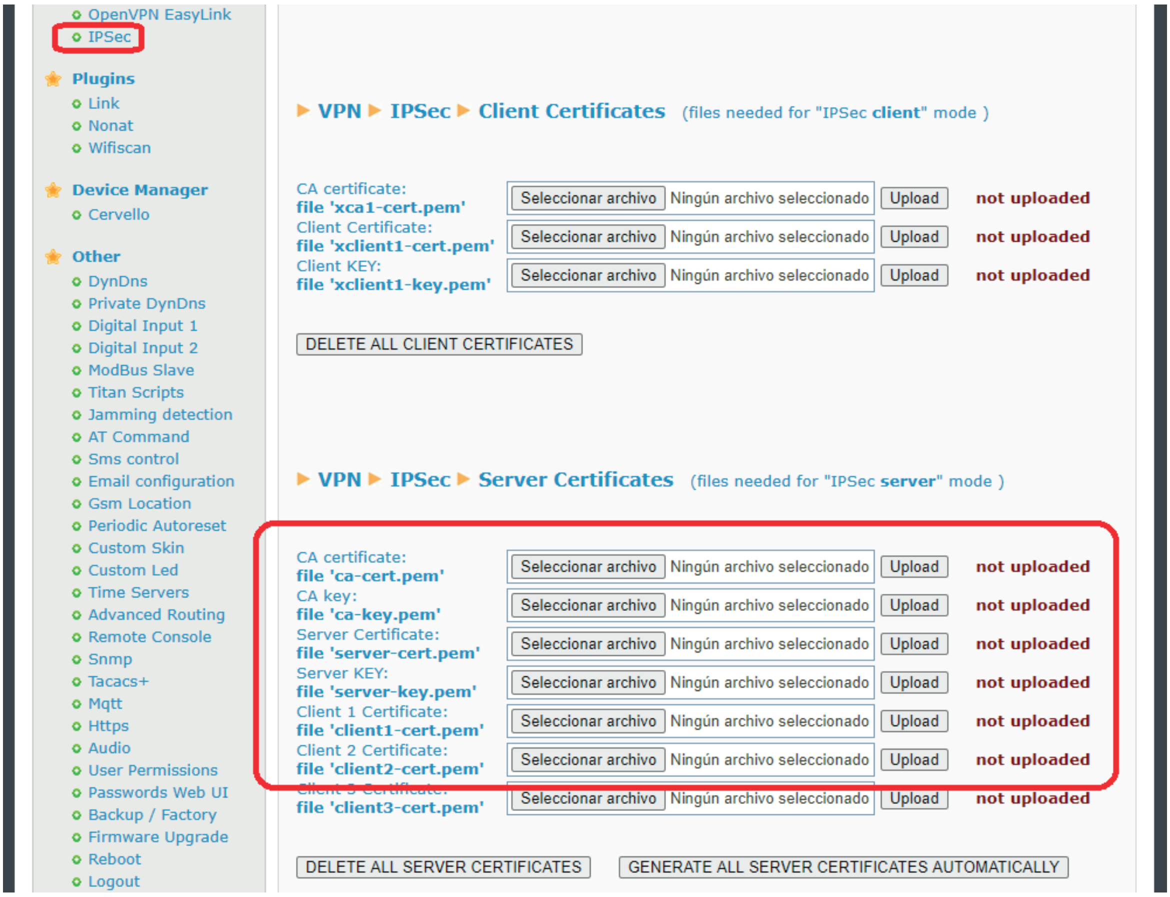
2. Configurations and Prerequisites

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

The first thing to do is to 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”, “client2-key.pem”, which will be used by the devices acting as IPSec clients to authenticate themselves.

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



▶ VPN ▶ IPSec ▶ Client Certificates (files needed for "IPSec **client**" mode)

CA certificate: **file 'xca1-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**

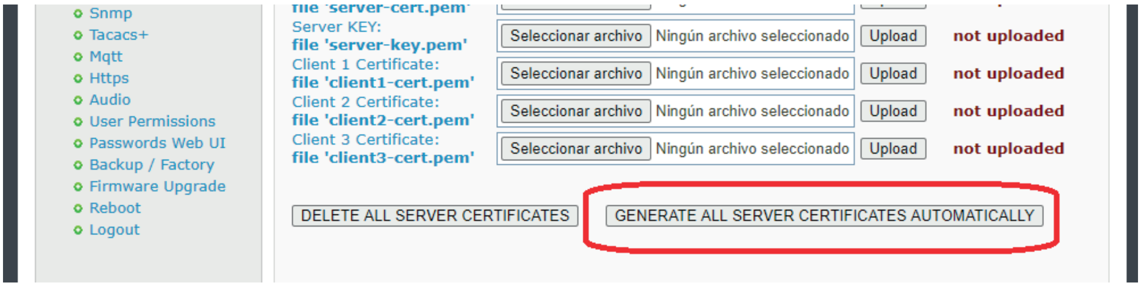
DELETE ALL CLIENT CERTIFICATES

▶ 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 to 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.



file 'server-cert.pem'

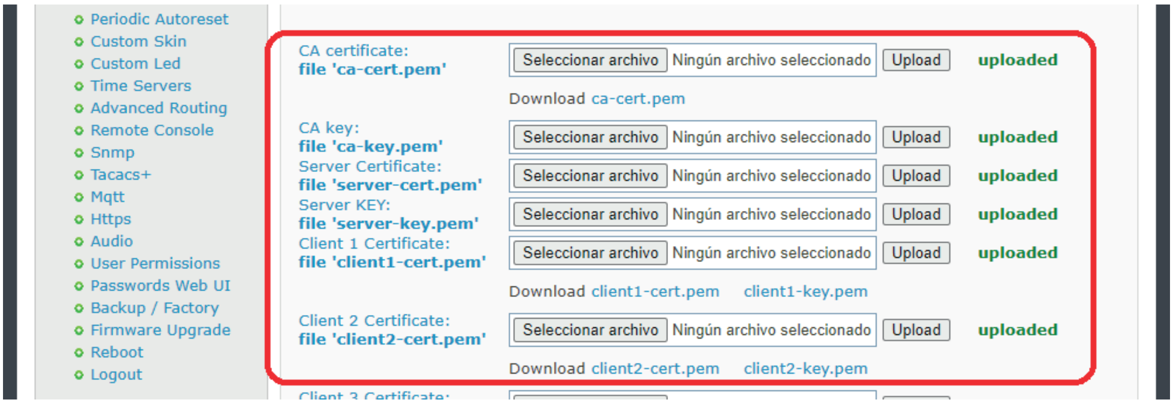
Server KEY: **file 'server-key.pem'**	Seleccionar archivo	Ningún archivo seleccionado	Upload	**not uploaded**
Client 1 Certificate: **file 'client1-cert.pem'**	Seleccionar archivo	Ningún archivo seleccionado	Upload	**not uploaded**
Client 2 Certificate: **file 'client2-cert.pem'**	Seleccionar archivo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

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.

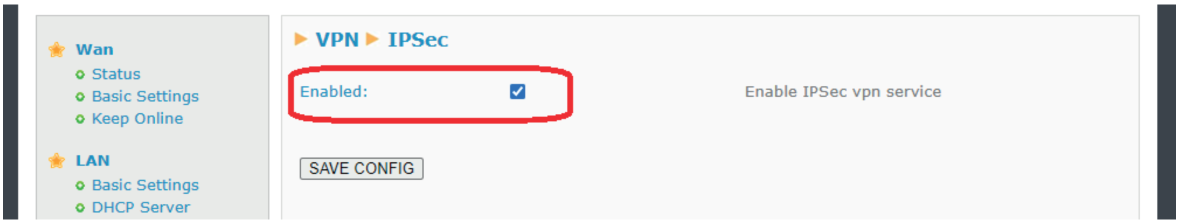
NB: Make sure the router has been updated before generating the certificates.

Once the process has finished correctly, the result will be:



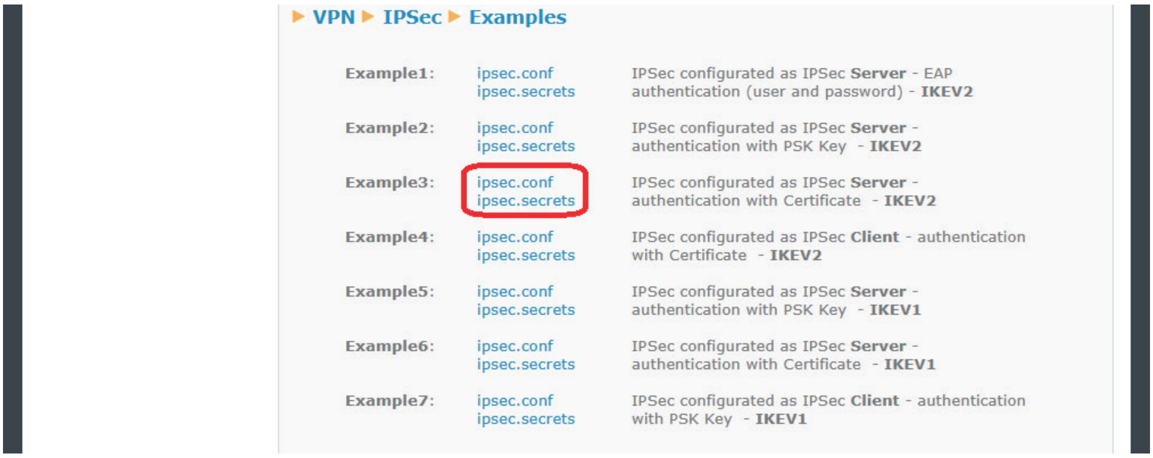
CA certificate: file 'ca-cert.pem'	Seleccionar archivo Ningún archivo seleccionado	Upload	uploaded
	Download ca-cert.pem		
CA key: file 'ca-key.pem'	Seleccionar archivo Ningún archivo seleccionado	Upload	uploaded
Server Certificate: file 'server-cert.pem'	Seleccionar archivo Ningún archivo seleccionado	Upload	uploaded
Server KEY: file 'server-key.pem'	Seleccionar archivo Ningún archivo seleccionado	Upload	uploaded
Client 1 Certificate: file 'client1-cert.pem'	Seleccionar archivo Ningún archivo seleccionado	Upload	uploaded
	Download client1-cert.pem client1-key.pem		
Client 2 Certificate: file 'client2-cert.pem'	Seleccionar archivo Ningún archivo seleccionado	Upload	uploaded
	Download client2-cert.pem client2-key.pem		
Client 3 Certificate:			

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.



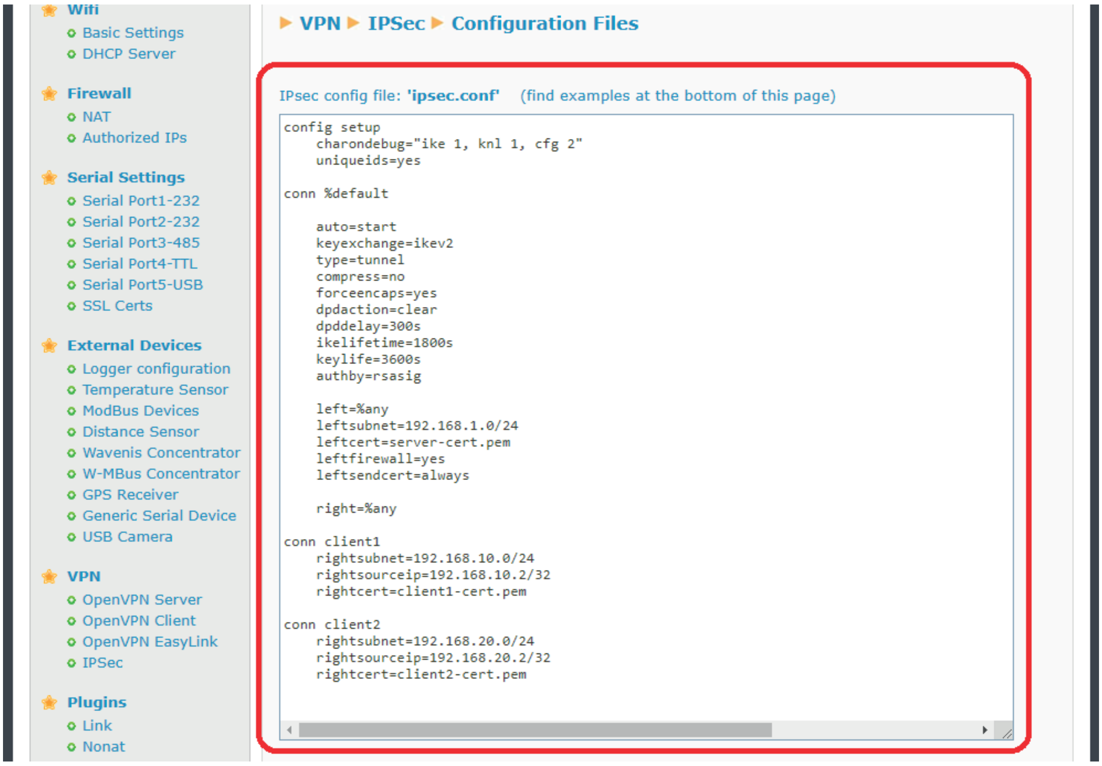
Enabled: ☑ Enable IPSec vpn service

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 3, clicking on (downloading) the corresponding “ipsec.conf” and “ipsec.secrets” files, which we will open with a notepad to extract their contents.



Example1:	ipsec.conf ipsec.secrets	IPSec configurated as IPSec **Server** - EAP authentication (user and password) - **IKEV2**
Example2:	ipsec.conf ipsec.secrets	IPSec configurated as IPSec **Server** - authentication with PSK Key - **IKEV2**
Example3:	ipsec.conf ipsec.secrets	IPSec configurated as IPSec **Server** - authentication with Certificate - **IKEV2**
Example4:	ipsec.conf ipsec.secrets	IPSec configurated as IPSec **Client** - authentication with Certificate - **IKEV2**
Example5:	ipsec.conf ipsec.secrets	IPSec configurated as IPSec **Server** - authentication with PSK Key - **IKEV1**
Example6:	ipsec.conf ipsec.secrets	IPSec configurated as IPSec **Server** - authentication with Certificate - **IKEV1**
Example7:	ipsec.conf ipsec.secrets	IPSec configurated as IPSec **Client** - authentication with PSK Key - **IKEV1**

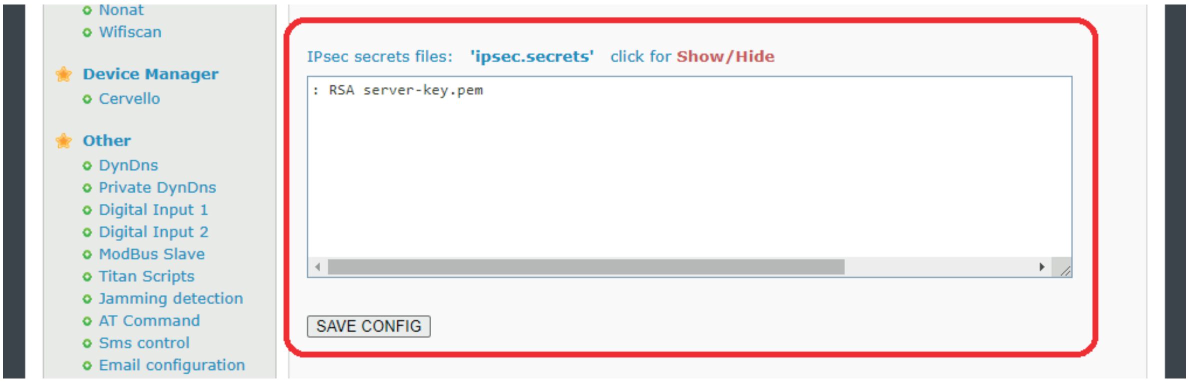
This content must be tailored to the example and inserted into the appropriate boxes. For “ipsec.conf”:



IPsec config file: **'ipsec.conf'** (find examples at the bottom of this page)

```
config setup
    charondebug="ike 1, knl 1, cfg 2"
    uniqueids=yes

conn %default

    auto=start
    keyexchange=ikev2
    type=tunnel
    compress=no
    forceencaps=yes
    dpdaction=clear
    dpddelay=300s
    ikelifetime=1800s
    keylife=3600s
    authby=rsasig

    left=%any
    leftsubnet=192.168.1.0/24
    leftcert=server-cert.pem
    leftfirewall=yes
    leftsendcert=always

    right=%any

conn client1
    rightsubnet=192.168.10.0/24
    rightsourceip=192.168.10.2/32
    rightcert=client1-cert.pem

conn client2
    rightsubnet=192.168.20.0/24
    rightsourceip=192.168.20.2/32
    rightcert=client2-cert.pem
```

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

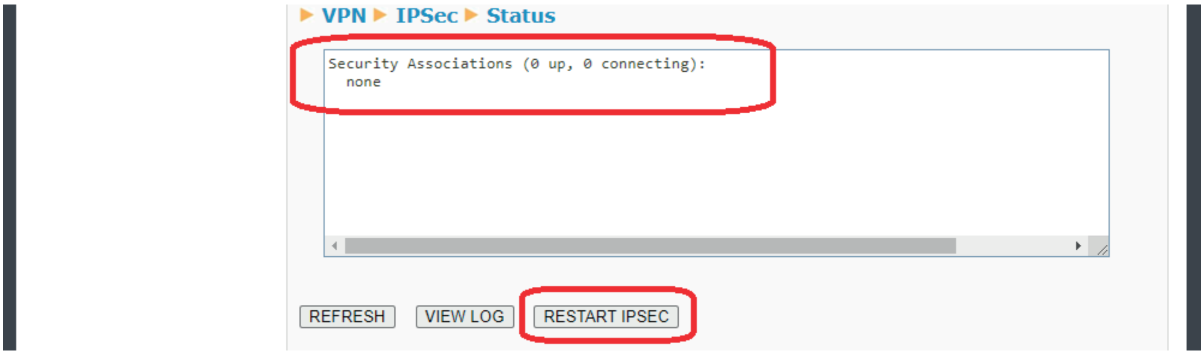


IPsec secrets files: **'ipsec.secrets'** click for **Show/Hide**

```
: RSA server-key.pem
```

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 equipment 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.



▶ VPN ▶ IPSec ▶ Status

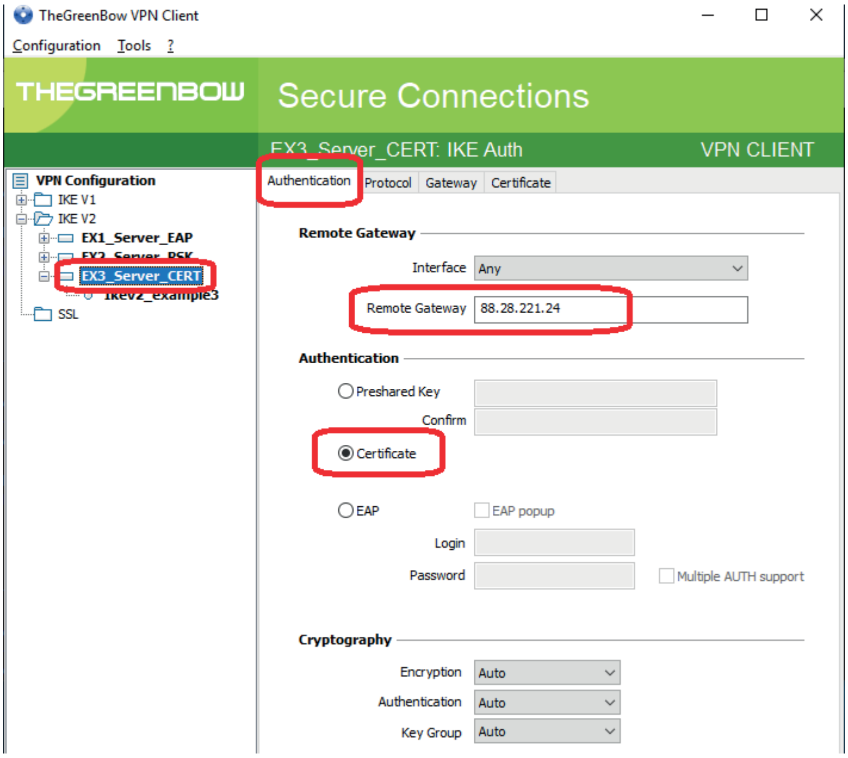
```
Security Associations (0 up, 0 connecting):
  none
```

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 must be entered in the “Authentication” section of the IKEv2 connection (in this example it is 88.28.221.24), the authentication method is by digital certificate.



Remote Gateway

Interface: Any

Remote Gateway: 88.28.221.24

Authentication

○ Preshared Key

Confirm

● Certificate

○ EAP　□ EAP popup

Login

Password　□ Multiple AUTH support

Cryptography

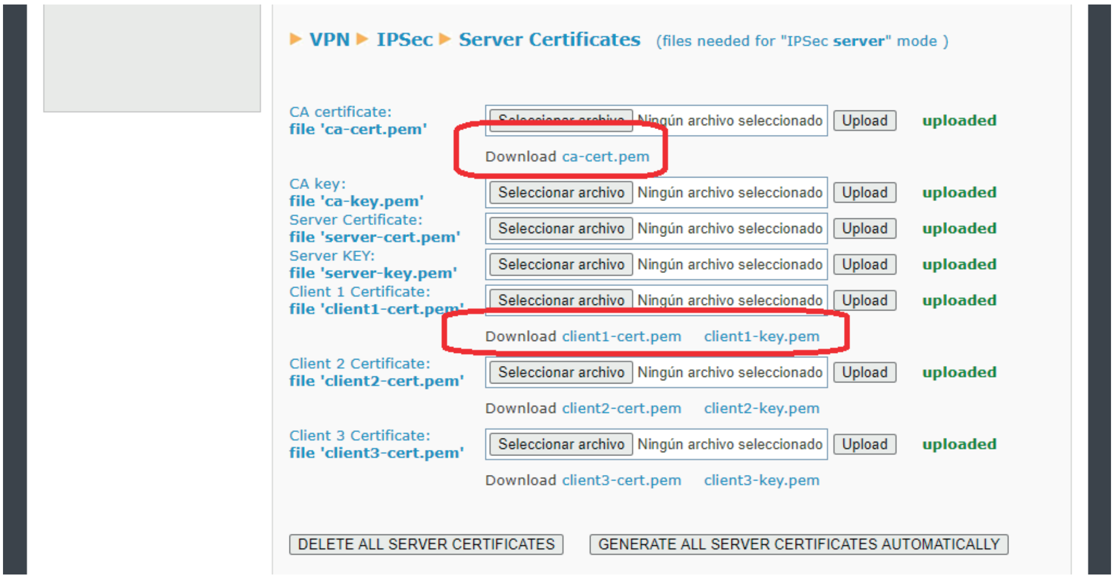
Encryption: Auto

Authentication: Auto

Key Group: Auto

4.2 Certificate

You must specify the client certificate and CA certificate to be used in the "Certificate" section. These certificates can be downloaded here:



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

CA certificate: file 'ca-cert.pem' — Seleccionar archivo | Ningún archivo seleccionado | Upload — uploaded
Download ca-cert.pem

CA key: file 'ca-key.pem' — Seleccionar archivo | Ningún archivo seleccionado | Upload — uploaded

Server Certificate: file 'server-cert.pem' — Seleccionar archivo | Ningún archivo seleccionado | Upload — uploaded

Server KEY: file 'server-key.pem' — Seleccionar archivo | Ningún archivo seleccionado | Upload — uploaded

Client 1 Certificate: file 'client1-cert.pem' — Seleccionar archivo | Ningún archivo seleccionado | Upload — uploaded
Download client1-cert.pem client1-key.pem

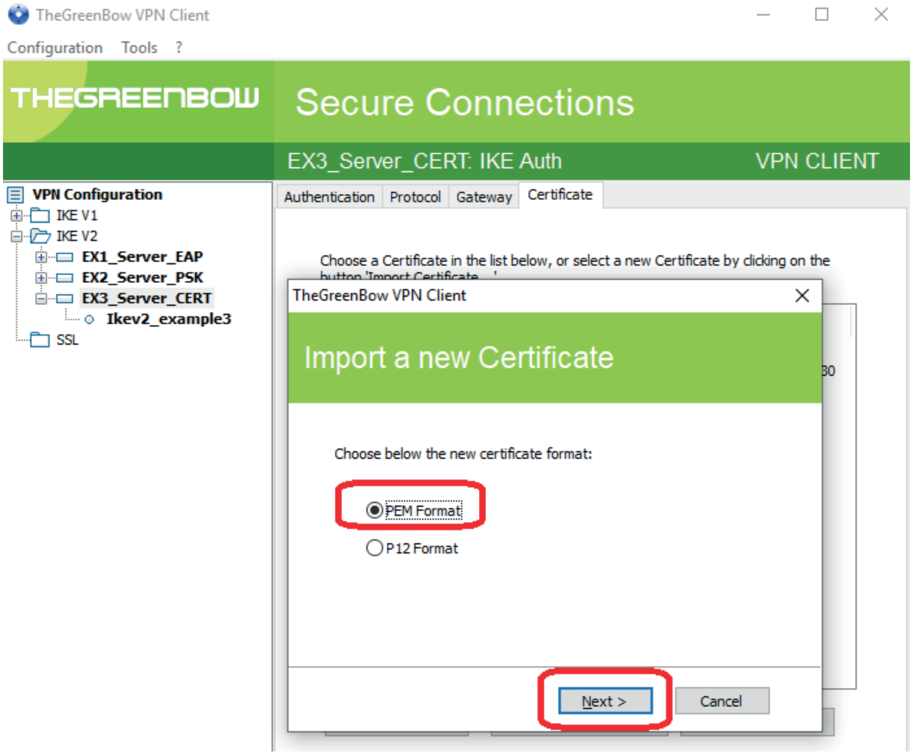
Client 2 Certificate: file 'client2-cert.pem' — Seleccionar archivo | Ningún archivo seleccionado | Upload — uploaded
Download client2-cert.pem client2-key.pem

Client 3 Certificate: file 'client3-cert.pem' — Seleccionar archivo | Ningún archivo seleccionado | Upload — uploaded
Download client3-cert.pem client3-key.pem

DELETE ALL SERVER CERTIFICATES
GENERATE ALL SERVER CERTIFICATES AUTOMATICALLY

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.



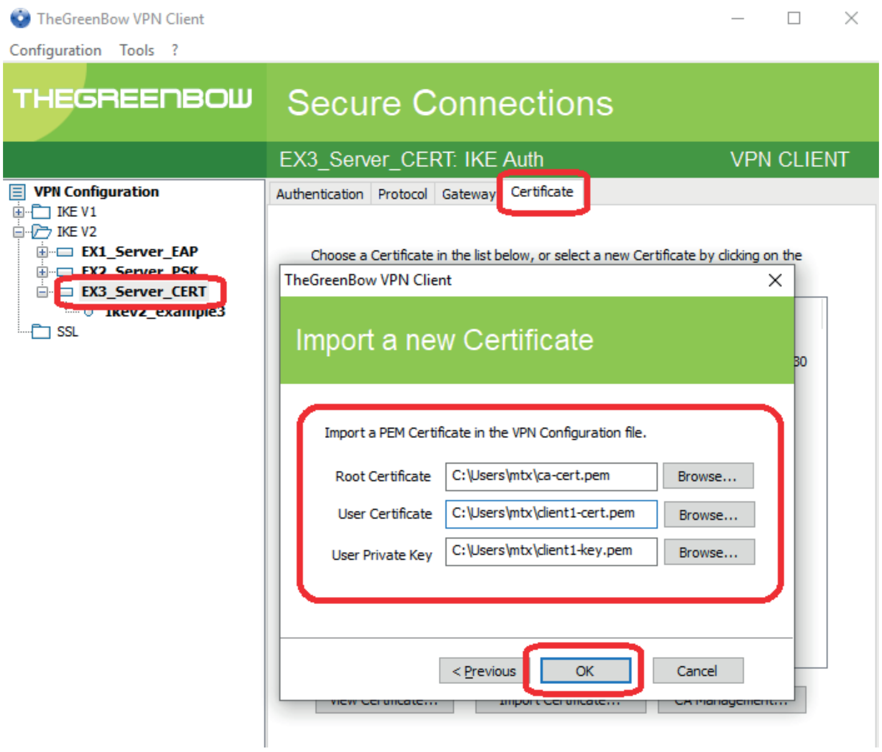
Choose a Certificate in the list below, or select a new Certificate by clicking on the button 'Import Certificate...'

TheGreenBow VPN Client

Import a new Certificate

Choose below the new certificate format:

● PEM Format
○ P12 Format

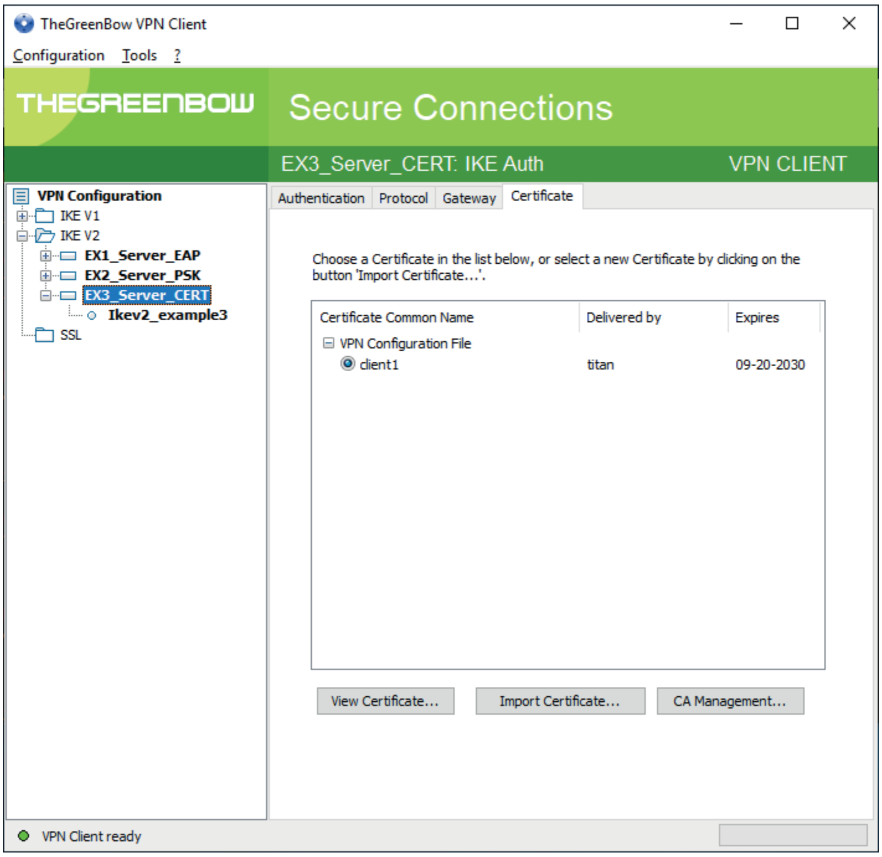


Choose a Certificate in the list below, or select a new Certificate by clicking on the

Import a PEM Certificate in the VPN Configuration file.

Root Certificate	C:\Users\mtx\ca-cert.pem
User Certificate	C:\Users\mtx\client1-cert.pem
User Private Key	C:\Users\mtx\client1-key.pem

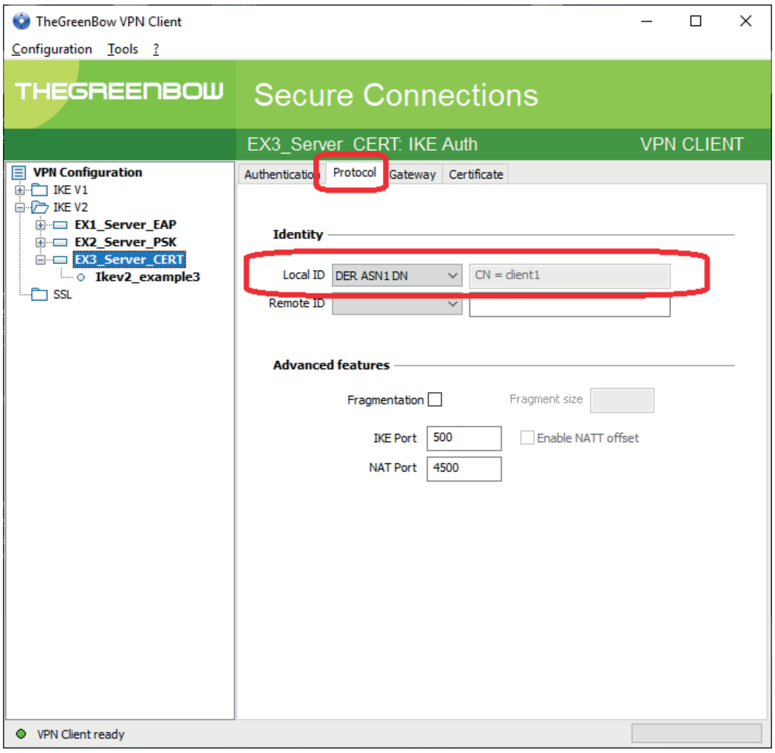
The certificate will be displayed as long as it was imported correctly.



Choose a Certificate in the list below, or select a new Certificate by clicking on the button 'Import Certificate...'.

Certificate Common Name	Delivered by	Expires
VPN Configuration File		
client1	titan	09-20-2030

The Local ID with the CN that has just been imported will automatically be displayed as selected in the “Protocol” tab.



Local ID: DER ASN1 DN — CN = client1

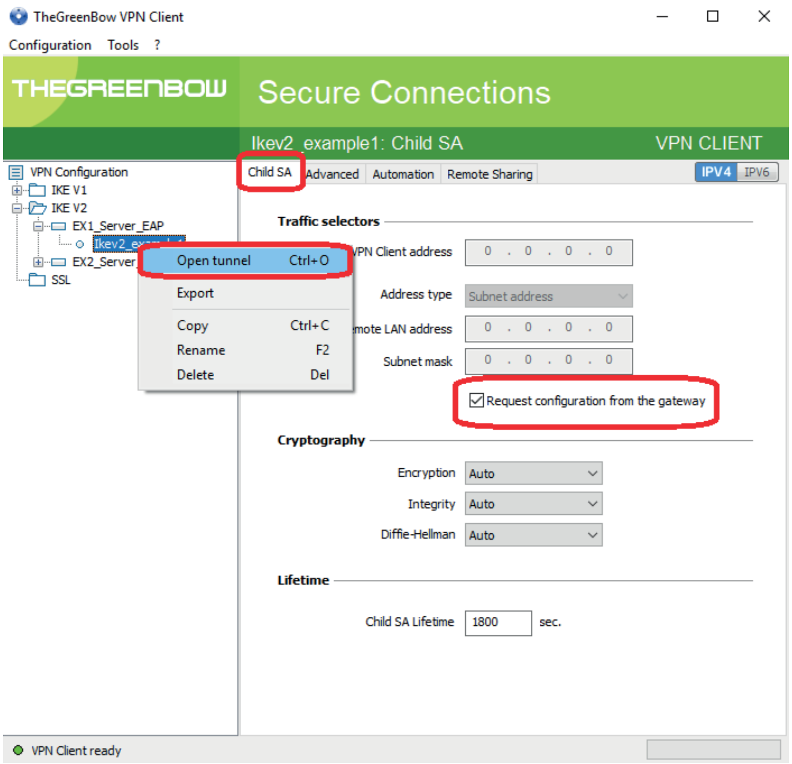
Remote ID:

Fragmentation ☐ Fragment size

IKE Port: 500 ☐ Enable NATT offset

NAT Port: 4500

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.



VPN Client address: 0 . 0 . 0 . 0

Address type: Subnet address

Remote LAN address: 0 . 0 . 0 . 0

Subnet mask: 0 . 0 . 0 . 0

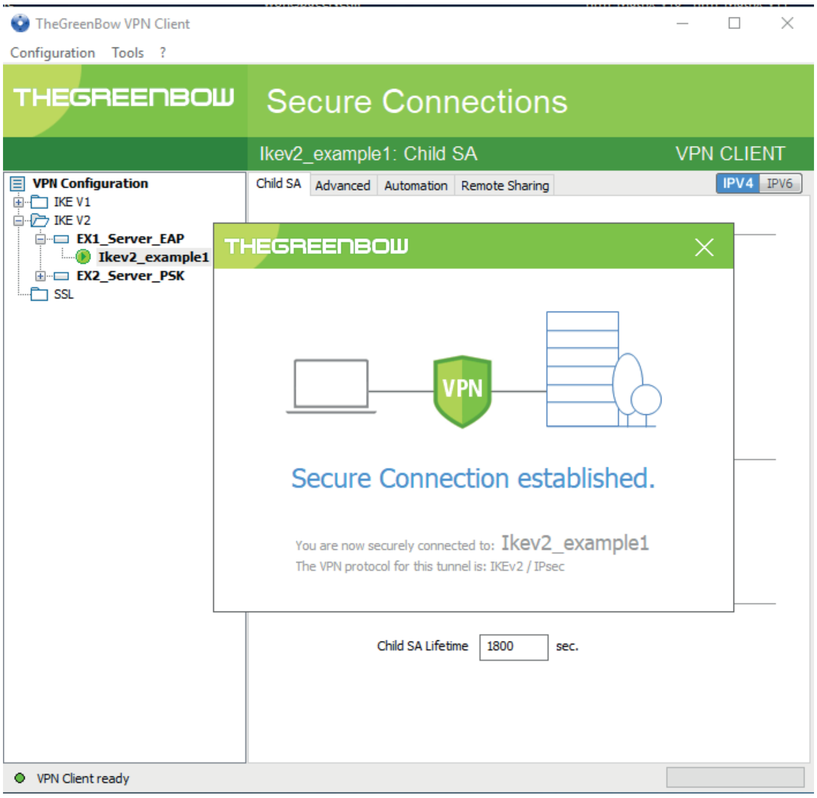
☑ Request configuration from the gateway

Encryption: Auto

Integrity: Auto

Diffie-Hellman: Auto

Child SA Lifetime: 1800 sec.



Secure Connection established.

You are now securely connected to: Ikev2_example1

The VPN protocol for this tunnel is: IKEv2 / IPsec

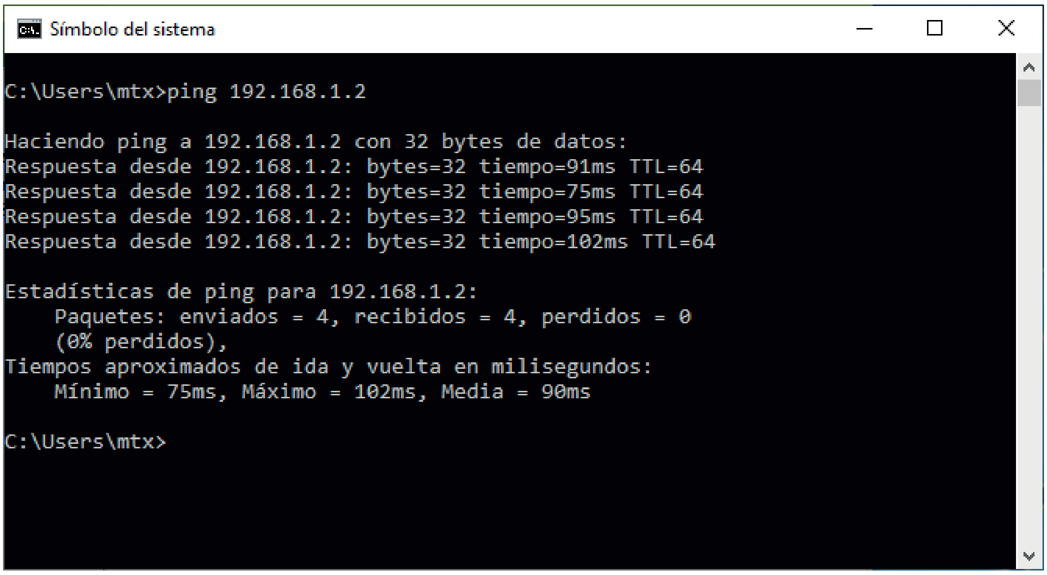
Child SA Lifetime 1800 sec.

VPN Client ready

5. Checking Connectivity

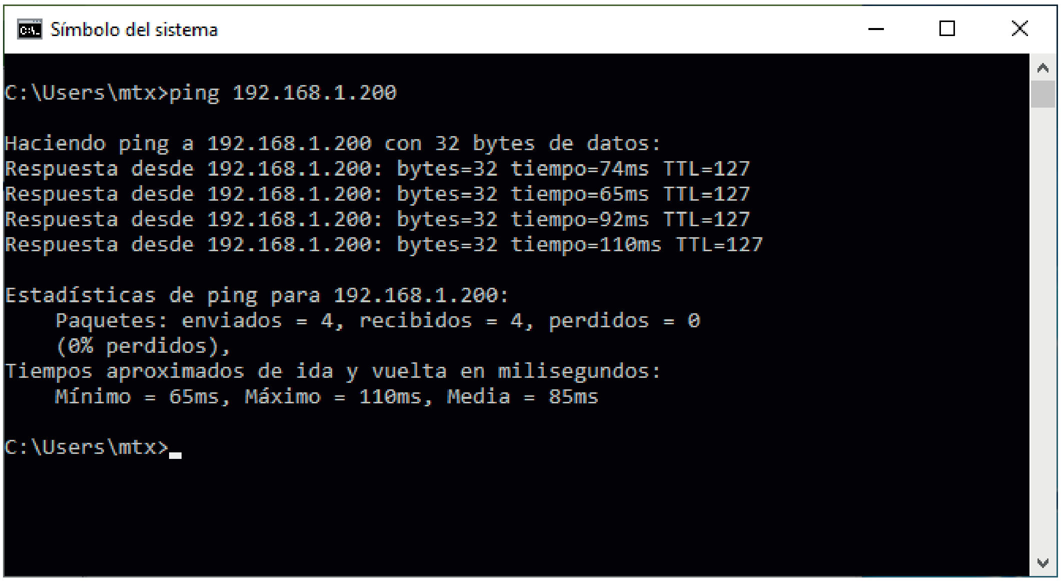
If the connection process was successful, we just need to check the connectivity, i.e. that the IPSec client 1 PC can access both the TITAN-based device (IP: 192.168.1.2) and the PLC connected to it (IP: 192.168.1.200). This can be done with a couple of PINGs.

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



```
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:



```
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>_
```