

TITAN

Application Note 41

IPSEC - Server
IKEv2 - EAP Authentication

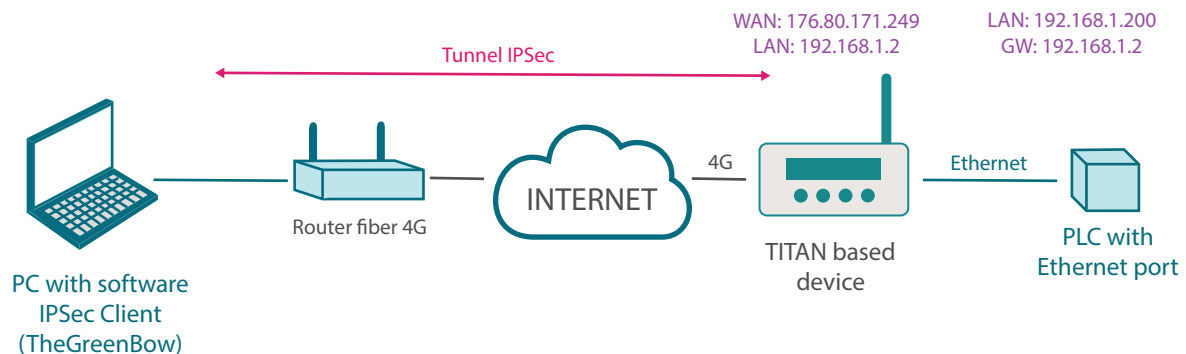
IPSEC - Server

IKEv2 - EAP Authentication

1. Scenario Details

The goal is to remotely configure a TITAN-based device, and a PLC connected to the Ethernet port of said router, from a PC. We also want to do this via a secure IPsec connection. We intend to use IKEv2 and EAP authentication.

Example of the proposed scenario:



Basically, in this example we want to create an IPsec VPN from a PC (which has an IPsec Client such as TheGreenBow, which is used in this example) to a remote TITAN-based device that will act as an IPsec Server, which in turn has a PLC connected to its Ethernet port.

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

The screenshot shows the 'VPN > IPSEC' configuration page. The left sidebar has a menu with 'IPSec' highlighted. The main content area has a breadcrumb trail 'VPN > IPSEC > Client Certificates'. Below this, there are fields for uploading certificates and keys for a client. The 'Client Certificates' section is highlighted with a red box. It contains the following fields:

Field	File Name	Choose File	No file chosen	Upload	Status
CA certificate:	file 'xca1-cert.pem'	Choose File	No file chosen	Upload	not uploaded
Client Certificate:	file 'xclient1-cert.pem'	Choose File	No file chosen	Upload	not uploaded
Client KEY:	file 'xclient1-key.pem'	Choose File	No file chosen	Upload	not uploaded

Below the upload fields, there is a 'DELETE ALL CLIENT CERTIFICATES' button. Further down, there is a section for 'Server Certificates' with a similar set of upload fields and a 'GENERATE ALL SERVER CERTIFICATES AUTOMATICALLY' button.

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. Press the “REFRESH” button to check the status of the process.

The screenshot shows the 'VPN > IPSEC' configuration page, specifically the 'Server Certificates' section. The left sidebar has a menu with 'Reboot' and 'Logout' options. The main content area has a breadcrumb trail 'VPN > IPSEC > Server Certificates'. Below this, there are fields for uploading certificates and keys for a server. The 'Server Certificates' section is highlighted with a red box. It contains the following fields:

Field	File Name	Choose File	No file chosen	Upload	Status
CA key:	file 'ca-key.pem'	Choose File	No file chosen	Upload	not uploaded
Server Certificate:	file 'server-cert.pem'	Choose File	No file chosen	Upload	not uploaded
Server KEY:	file 'server-key.pem'	Choose File	No file chosen	Upload	not uploaded
Client 1 Certificate:	file 'client1-cert.pem'	Choose File	No file chosen	Upload	not uploaded
Client 2 Certificate:	file 'client2-cert.pem'	Choose File	No file chosen	Upload	not uploaded
Client 3 Certificate:	file 'client3-cert.pem'	Choose File	No file chosen	Upload	not uploaded

Below the upload fields, there is a 'DELETE ALL SERVER CERTIFICATES' button and a 'GENERATE ALL SERVER CERTIFICATES AUTOMATICALLY' button, which is highlighted with a red box.

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. After finishing the process correctly, this will be the result

Connectivity tools
Digital I/O
Custom Skin
Led Config
Syslog
Backup / Factory
Firmware Upgrade
Reboot
Logout

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

CA certificate:
file 'ca-cert.pem'

Choose File No file chosen Upload **uploaded**

Download ca-cert.pem

CA key:
file 'ca-key.pem'

Choose File No file chosen Upload **uploaded**

Server Certificate:
file 'server-cert.pem'

Choose File No file chosen Upload **uploaded**

Server KEY:
file 'server-key.pem'

Choose File No file chosen Upload **uploaded**

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

Choose File No file chosen Upload **uploaded**

Download client1-cert.pem client1-key.pem

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

Choose File No file chosen Upload **uploaded**

Download client2-cert.pem client2-key.pem

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

Choose File No file chosen Upload **uploaded**

Download client3-cert.pem client3-key.pem

DELETE ALL SERVER CERTIFICATES GENERATE ALL SERVER CERTIFICATES AUTOMATICALLY

VPN > IPsec > Status

REFRESH VIEW LOG RESTART IPSEC

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.

Wan
Status
Basic Settings
Keep Online

LAN
Basic Settings
DHCP Server

VPN > IPsec

Enabled: ☒ Enable IPsec vpn service

SAVE CONFIG

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

VPN ► IPSec ► Examples		
Example1:	<code>ipsec.conf</code> <code>ipsec.secrets</code>	IPSec configured as IPSec Server - EAP authentication (user and password) - IKEV2
Example2:	<code>ipsec.conf</code> <code>ipsec.secrets</code>	IPSec configured as IPSec Server - authentication with PSK Key - IKEV2
Example3:	<code>ipsec.conf</code> <code>ipsec.secrets</code>	IPSec configured as IPSec Server - authentication with Certificate - IKEV2
Example4:	<code>ipsec.conf</code> <code>ipsec.secrets</code>	IPSec configured as IPSec Client - authentication with Certificate - IKEV2
Example5:	<code>ipsec.conf</code> <code>ipsec.secrets</code>	IPSec configured as IPSec Server - authentication with PSK Key - IKEV1
Example6:	<code>ipsec.conf</code> <code>ipsec.secrets</code>	IPSec configured as IPSec Server - authentication with Certificate - IKEV1
Example7:	<code>ipsec.conf</code> <code>ipsec.secrets</code>	IPSec configured as IPSec Client - authentication with PSK Key - IKEV1

This content must be tailored to the specific scenario of the application note and inserted into the appropriate boxes. For “ipsec.conf”:

★ **Firewall**

◆ NAT

◆ Authorized IPs

★ **Serial Settings**

◆ Serial Port1-232

◆ Serial Port2-485

◆ SSL Certificates

★ **External Devices**

◆ Logger configuration

◆ ModBus Devices

◆ Generic Serial Device

◆ Temperature Sensor

◆ IEC102 Meter

◆ W-MBus

◆ GPS Receiver

★ **VPN**

◆ IPsec

◆ OpenVPN Client

◆ OpenVPN Server

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

```
config setup
    charondebug="ike 1, knl 1, cfg 0"
    uniqueids=no

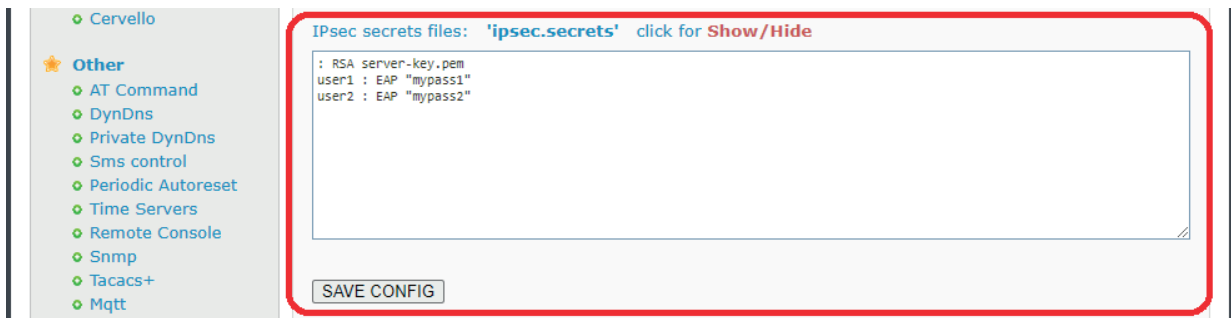
conn server

    auto=add
    keyexchange=ikev2
    type=tunnel
    compress=no
    forceencaps=yes
    dpdaction=clear
    dpddelay=300s
    rekey=no
    eap_identity=%identity

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

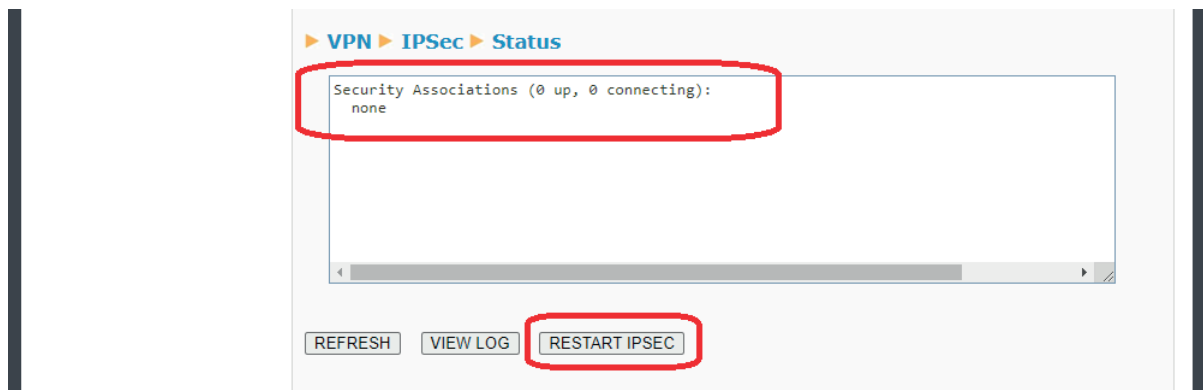
    right=%any
    rightid=%any
    rightsourceip=10.10.10.0/24
    rightsendcert=never
    rightauth=eap-mschapv2
```

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 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.



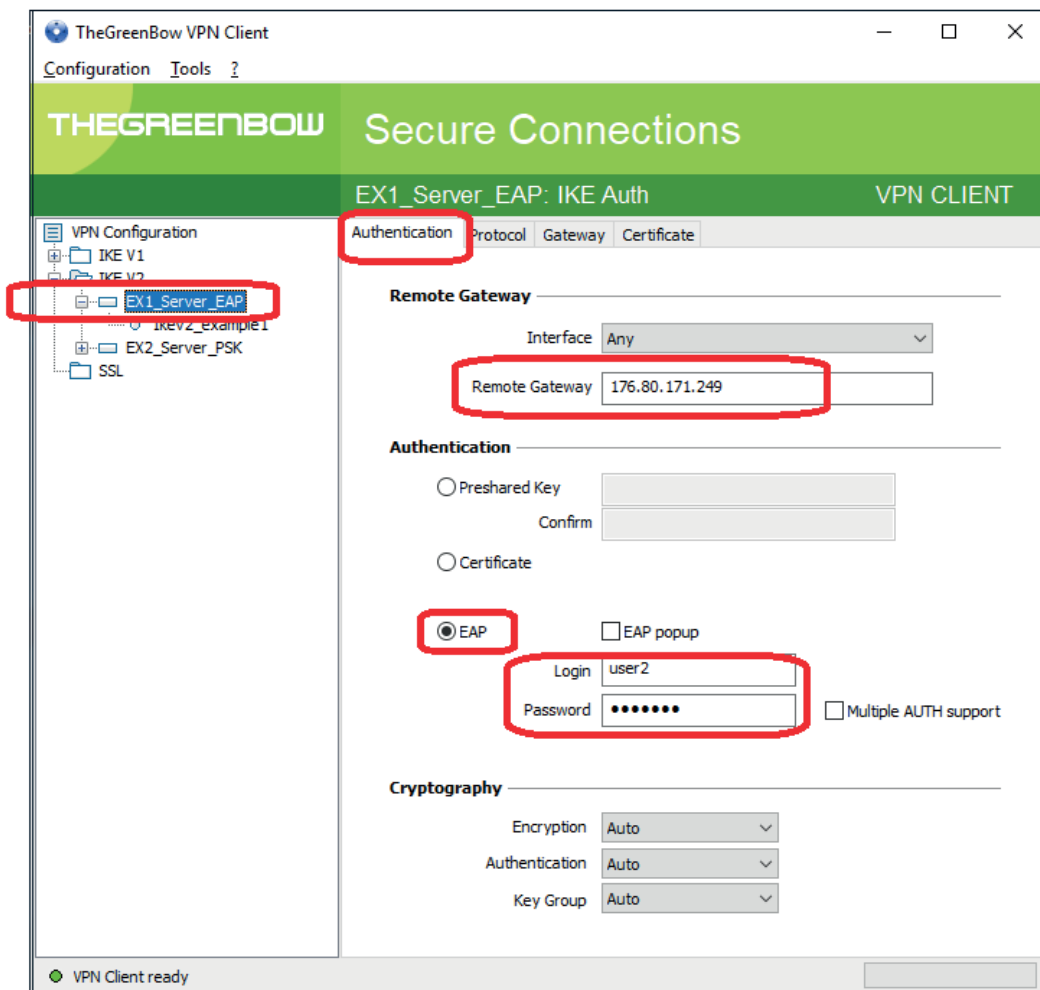
4. Configuring the IPSEC Client

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.

4.1 Authentication

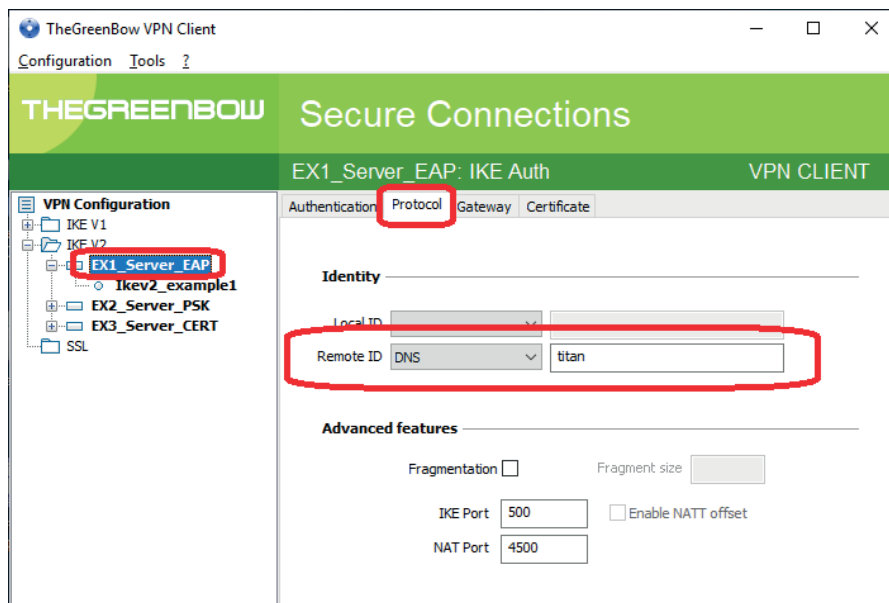
The TITAN-based device's public IP address and the EAP authentication method must be entered in the "Authentication" section of the IKEv2 connection (in this example it is 176.80.171.249). We will then add one of the two users that we specified in the "ipsec.secrets" file:

Login: "user2", Password: "mypass2".



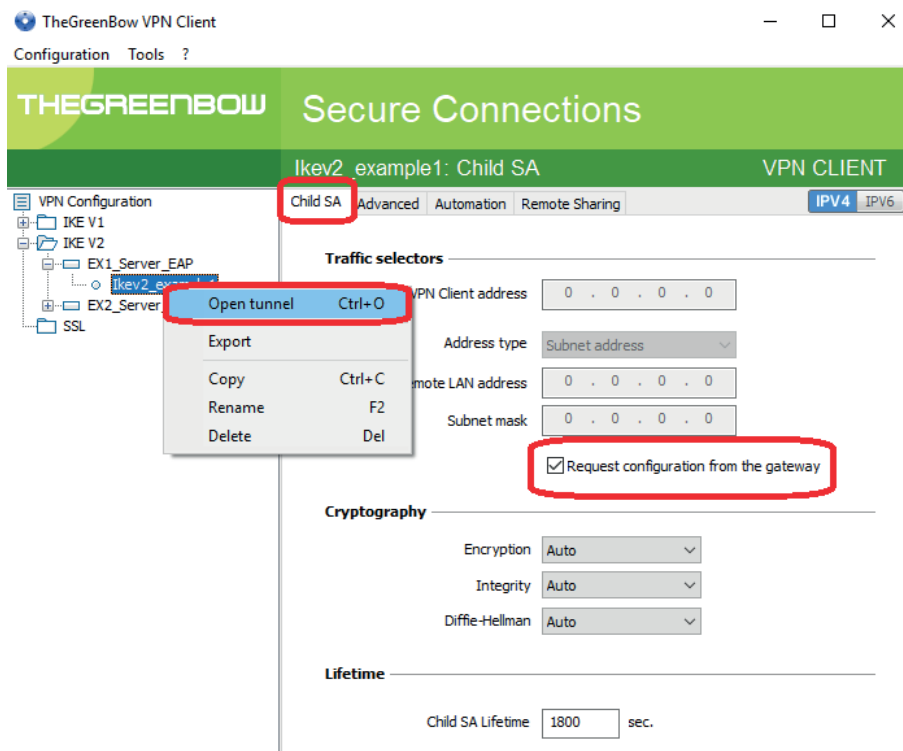
4.2 Protocol

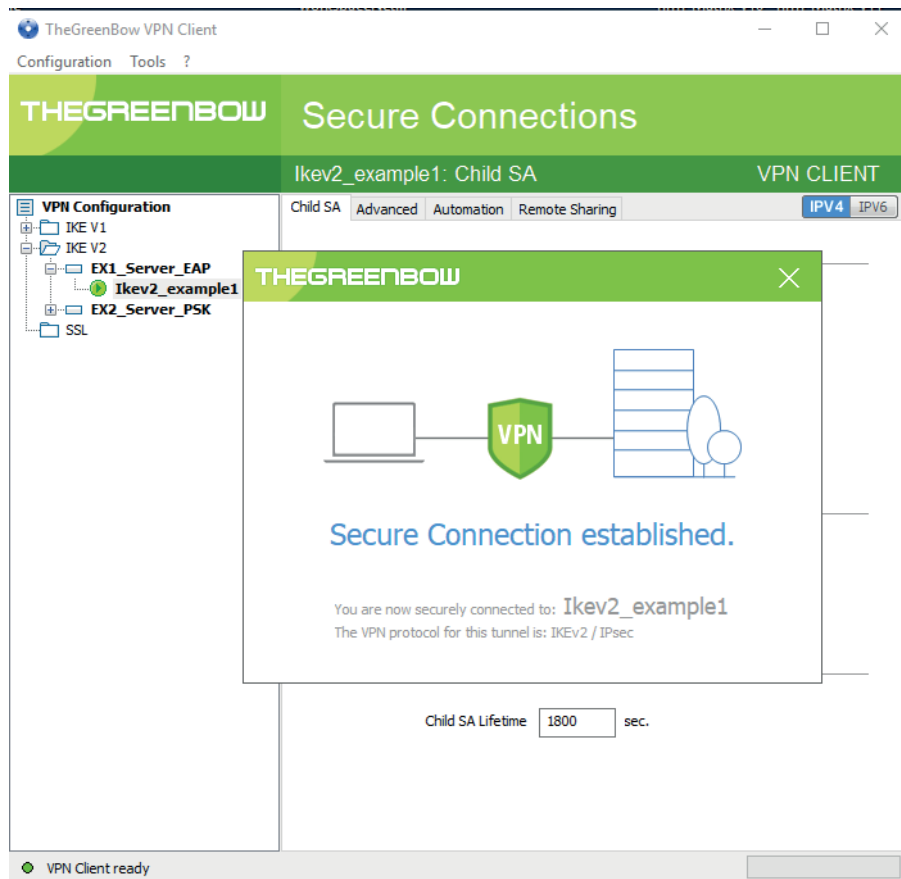
The “Protocol” section it must be configured as shown below.



4.3 Child SA

Lastly, in the "Child SA" tab, we indicate that we want to get the configuration of the TITAN-based device itself. We can now open the IPsec tunnel by right-clicking on the connection and pressing the “Open tunnel” option, as is shown in the following screen.

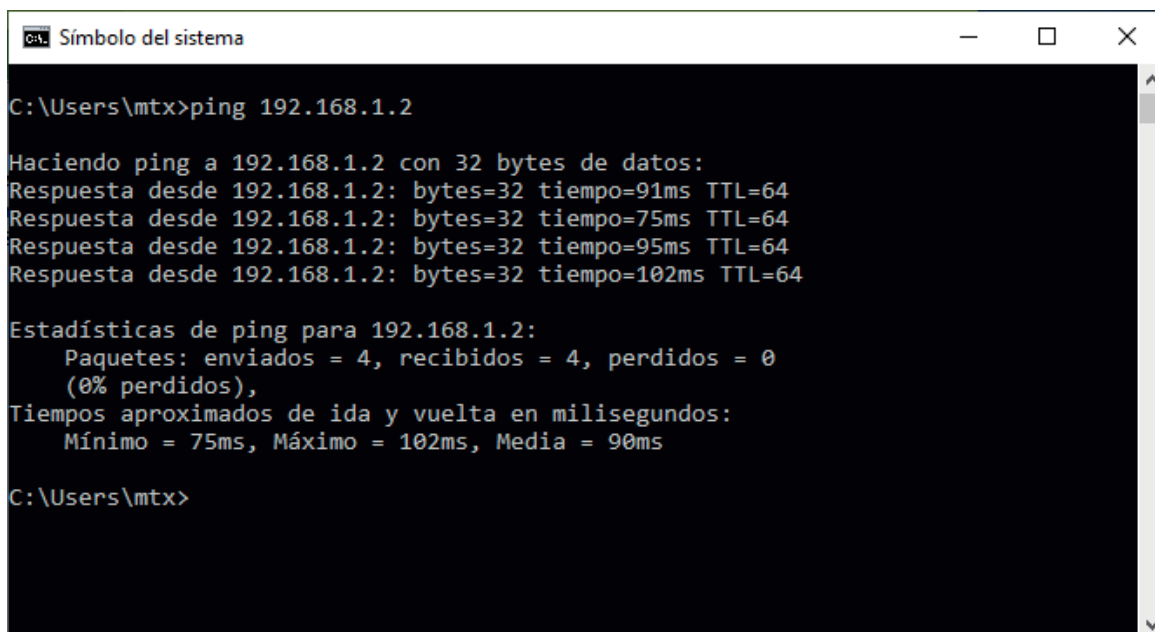




5. Checking Connectivity

If the connection process was successful, we just need to check the connectivity, i.e. that the IPSec client 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 PC to the TITAN-based device via the IPSec VPN:



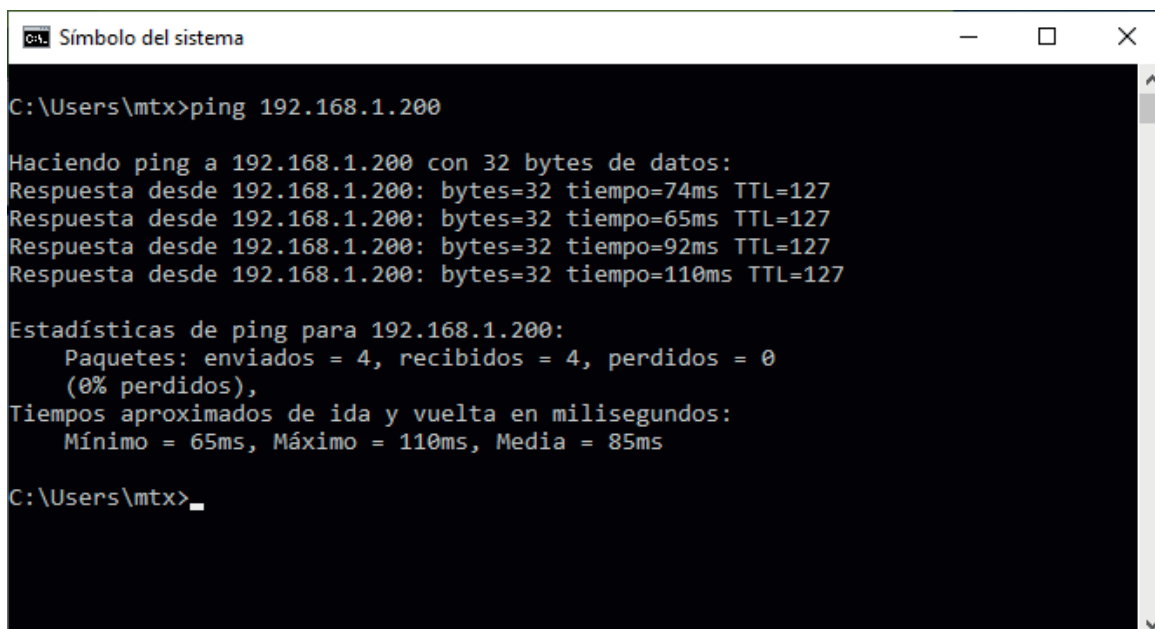
```
C:\Users\mtx>ping 192.168.1.2

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 PC 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>
```