

TITAN

Application Note 42

IPSEC - Server
IKEv2 - PSK Authentication

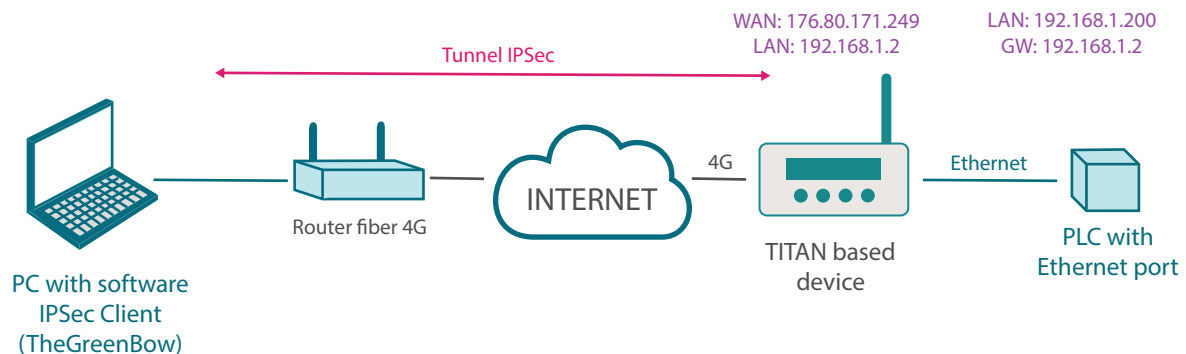
IPSEC - Server

IKEv2 - PSK Authentication

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 a PC. We also want to do this using a secure IPsec connection. We intend to use IKEv2 and PSK authentication.

Example of the proposed scenario:



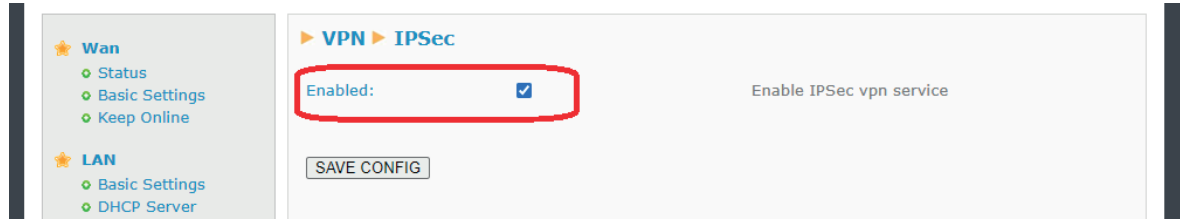
Basically, in this example we want to create an IPsec VPN from a PC (which has an IPsec Client such as TheGreenBow, which is used in this example) to a remote 4G TITAN-based device that will act as an IPsec Server, which in turn has a PLC connected to its Ethernet port.

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.

3. IPSEC Configuration of the TITAN-based Device

In the “VPN > IPsec” menu, 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 2, 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”:

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
    authby=secret

    left=%any
    leftid=@titan
    leftsubnet=192.168.1.0/24
    leftfirewall=yes

    right=%any
    rightid=%any
    rightsourceip=10.10.10.0/24
```

And for “ipsec.secrets” (you must click on the “Show/Hide” legend beforehand to display the box), we will set the password as “mypass”.

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

```
: PSK mypass
```

SAVE CONFIG

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.

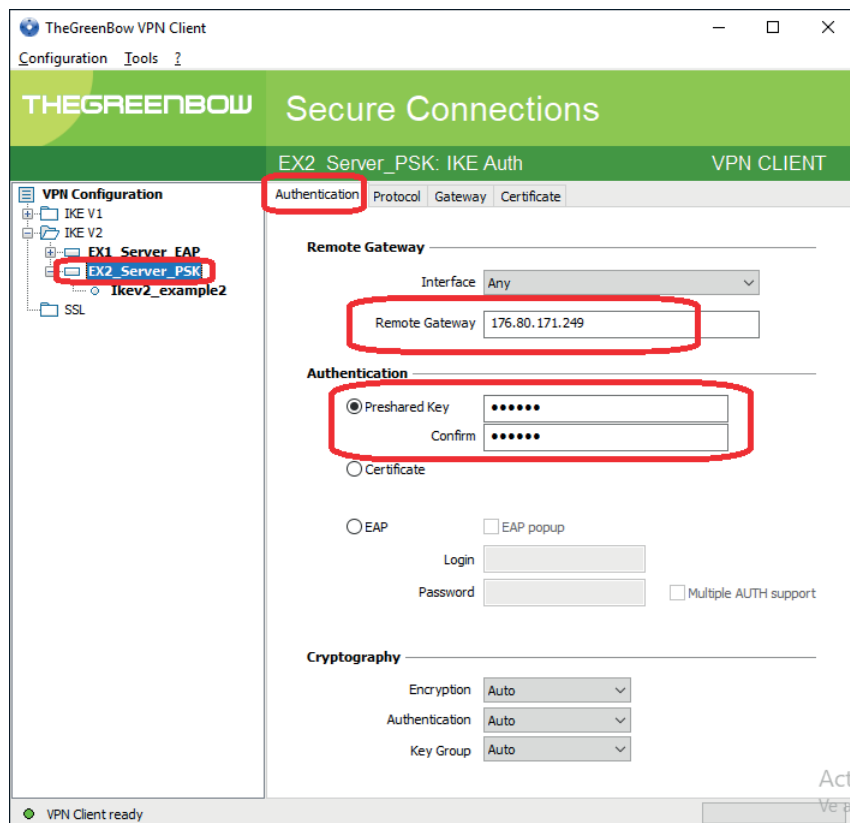


4. Configuring the IPSEC Client

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.

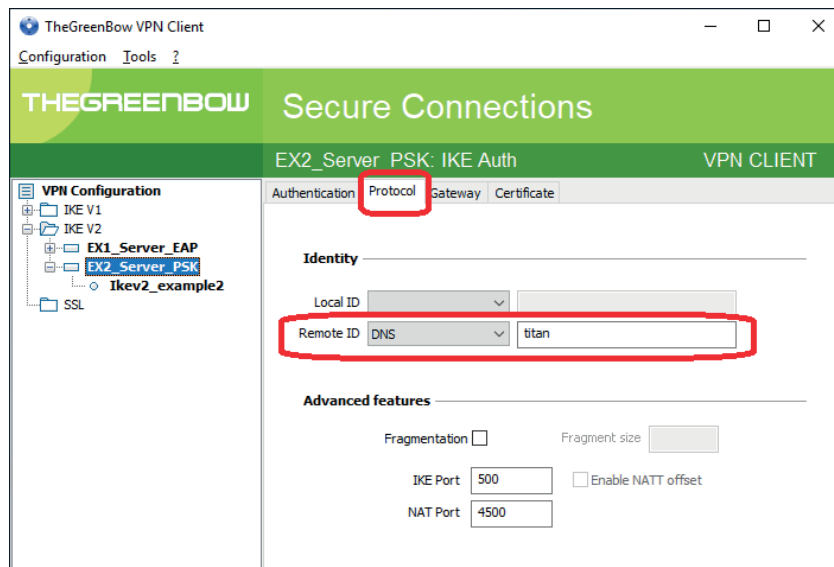
4.1 Authentication

The TITAN-based device's public IP address (which in this example is 176.80.171.249) and the PSK (Preshared Key) authentication method, with password “mypass” as specified in the “ipsec.secrets” file, must be entered in the “Authentication” section of the IKEv2 connection.



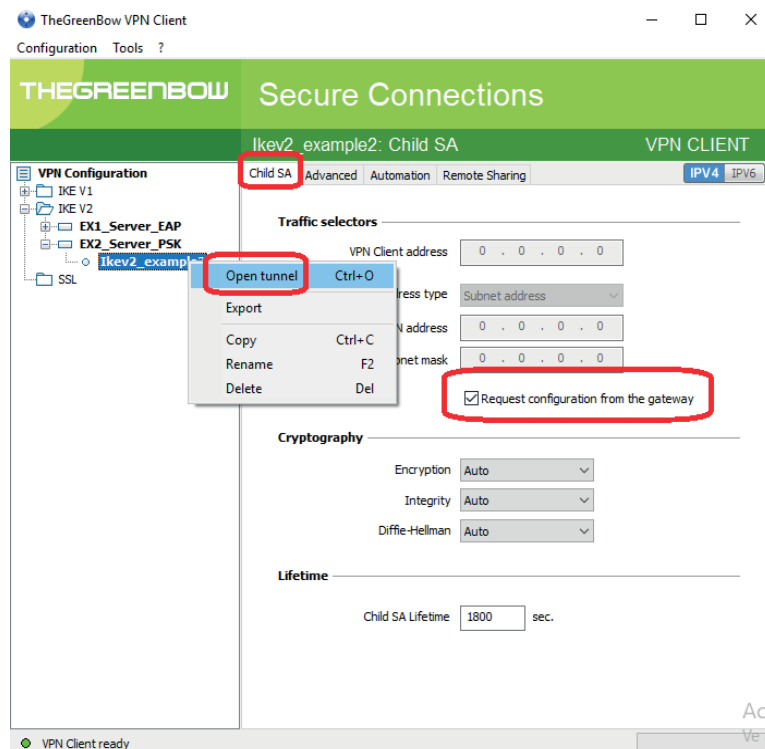
4.2 Protocol

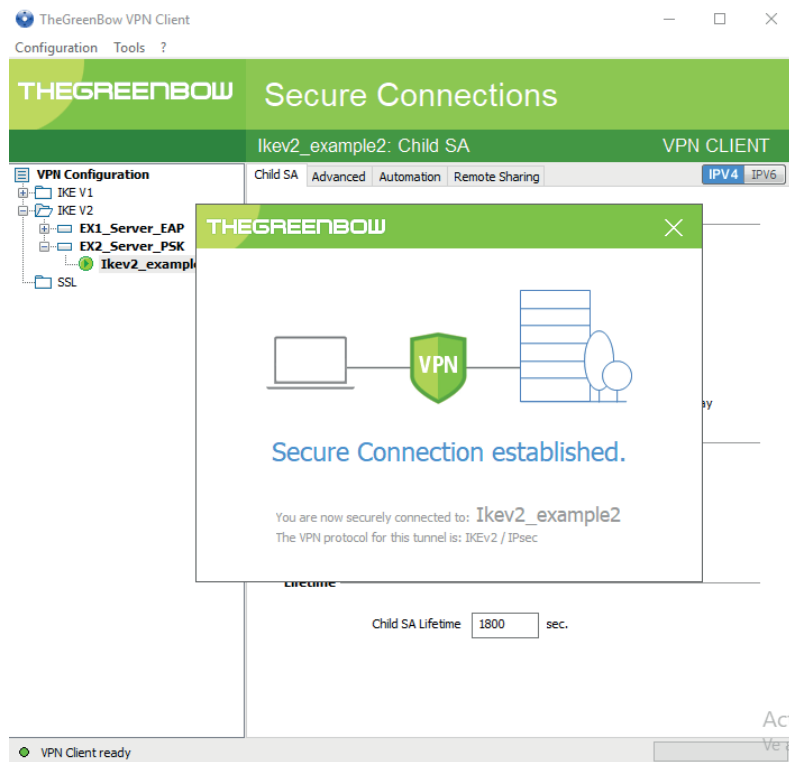
We must configure DNS and enter the remote ID as “titan” in the “Protocol” section, as this is the name given to the router in the “leftid” field of the “ipsec.conf” file.



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.

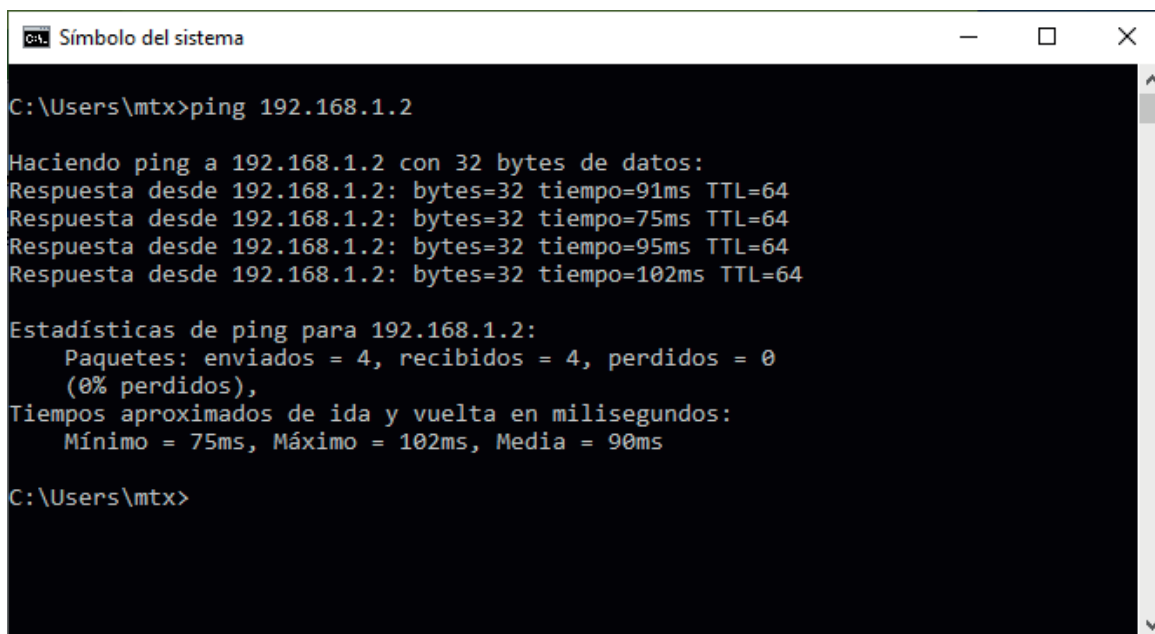




5. Checking Connectivity

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:



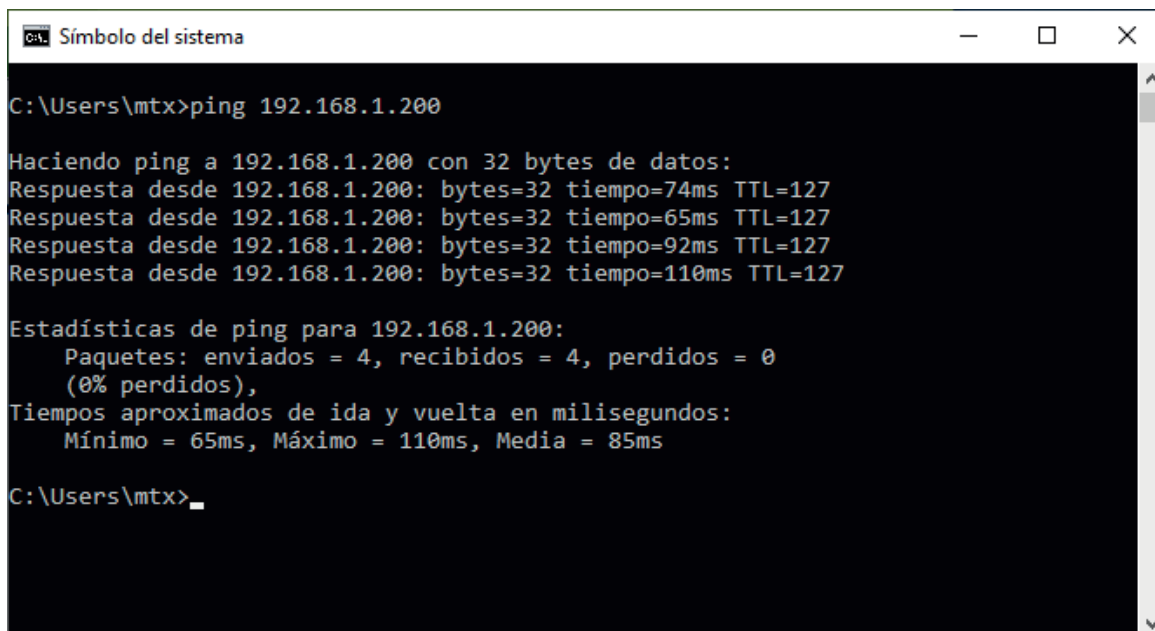
```
C:\Users\mtx>ping 192.168.1.2

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>
```