

TITAN

Application Note 45

IPSEC - Server
IKEv1 - PSK Authentication

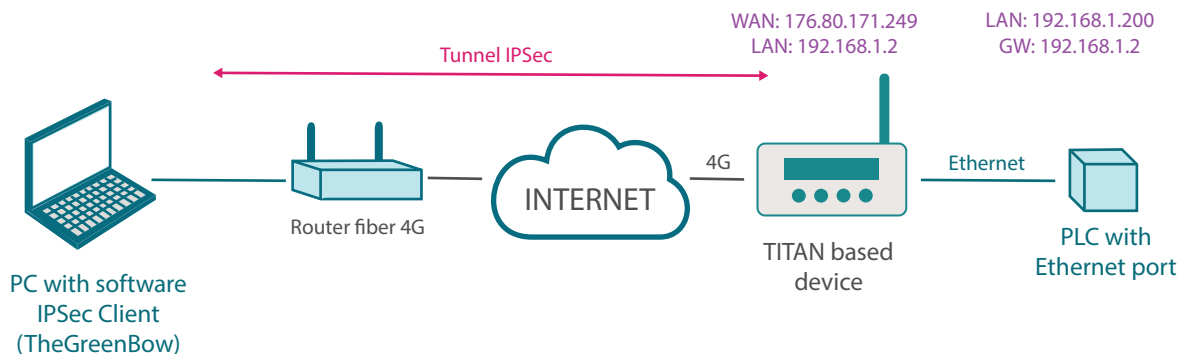
IPSEC - Server

IKEv1 - 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 IKEv1 and PSK authentication.

Example of the proposed scenario:



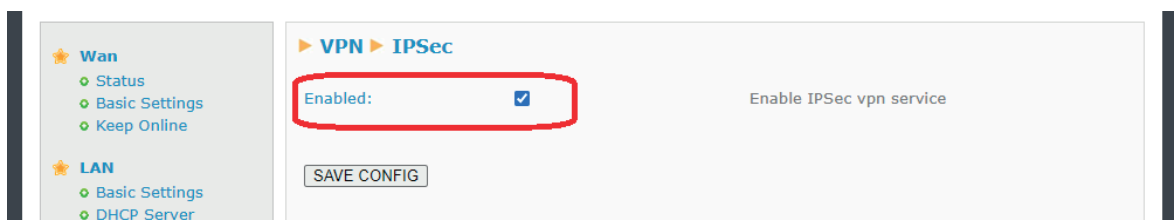
Basically, in this example we want to create an IPsec VPN from a PC (which has an IPsec Client such as TheGreenBow, which is used in this example) to a remote 4G TITAN-based device that will act as an IPsec Server, which in turn has a PLC connected to its Ethernet port.

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

Check the “Enabled” box at the top of the configuration page and click on the “SAVE CONFIG” button.



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

★ DHCP Server

★ Firewall

- ◊ NAT
- ◊ Authorized IPs

★ Serial Settings

- ◊ Serial Port1-232
- ◊ Serial Port2-232
- ◊ Serial Port3-485
- ◊ Serial Port4-TTL
- ◊ Serial Port5-USB
- ◊ SSL Certs

★ External Devices

- ◊ Logger configuration
- ◊ Temperature Sensor
- ◊ ModBus Devices
- ◊ Distance Sensor
- ◊ Wavenis Concentrator
- ◊ W-MBus Concentrator
- ◊ GPS Receiver
- ◊ Generic Serial Device
- ◊ USB Camera

★ VPN

- ◊ OpenVPN Server
- ◊ OpenVPN Client

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

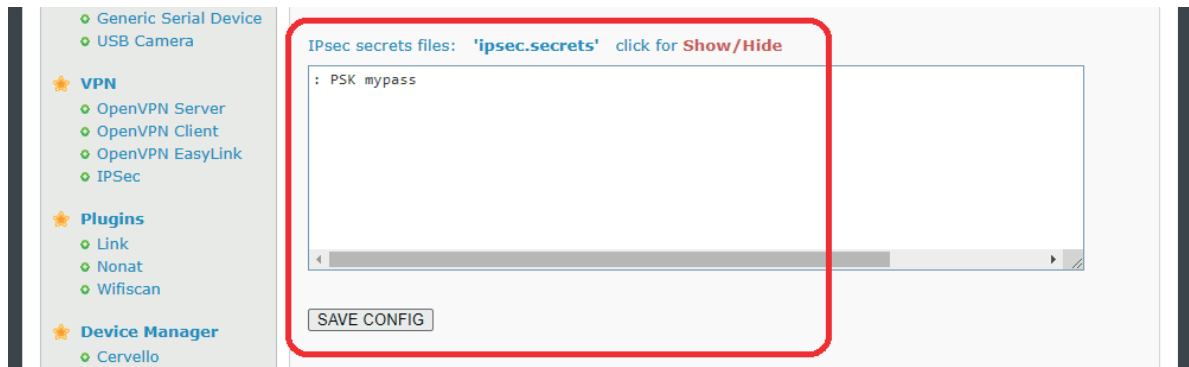
```
config setup
    charondebug="ike 1, knl 1, cfg 2"
    uniqueids=no

conn server

    auto=add
    keyexchange=ikev1
    type=tunnel
    compress=no
    forceencaps=yes
    dpdaction=clear
    dpddelay=300s
    rekey=no
    ike=aes256-sha256-modp1024
    esp=aes256-sha256
    authby=secret

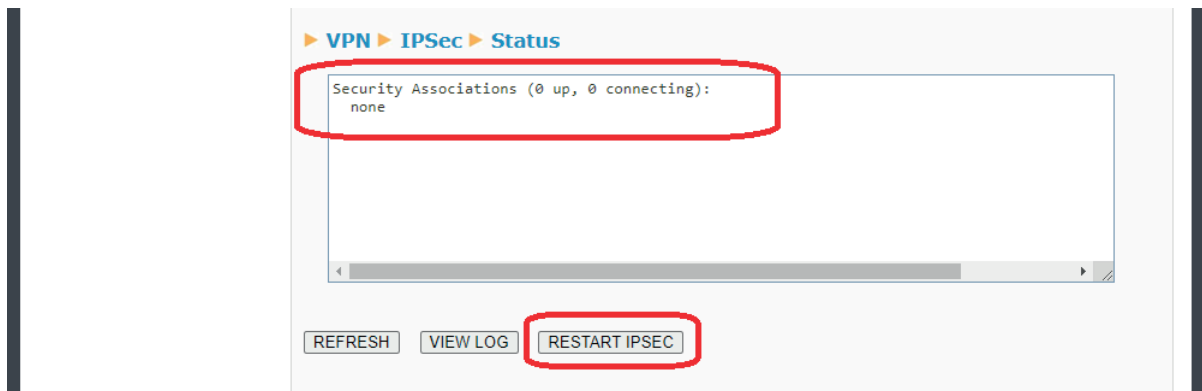
    left=%any
    leftid=@titan
    leftsubnet=192.168.1.0/24
    leftfirewall=yes
    right=%any
    rightid=%any
    #rightsourceip=10.10.10.1/32
    rightsubnet=10.10.10.0/24
```

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.

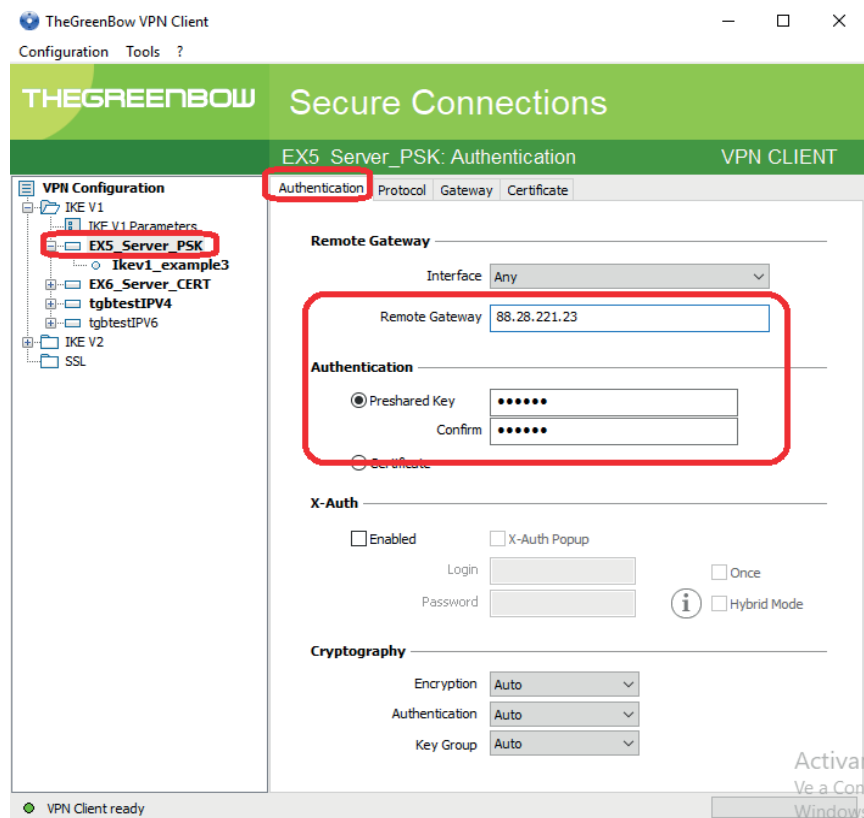


4. Configuring the IPSEC Client

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 are some screenshots showing the basic configurations for each section.

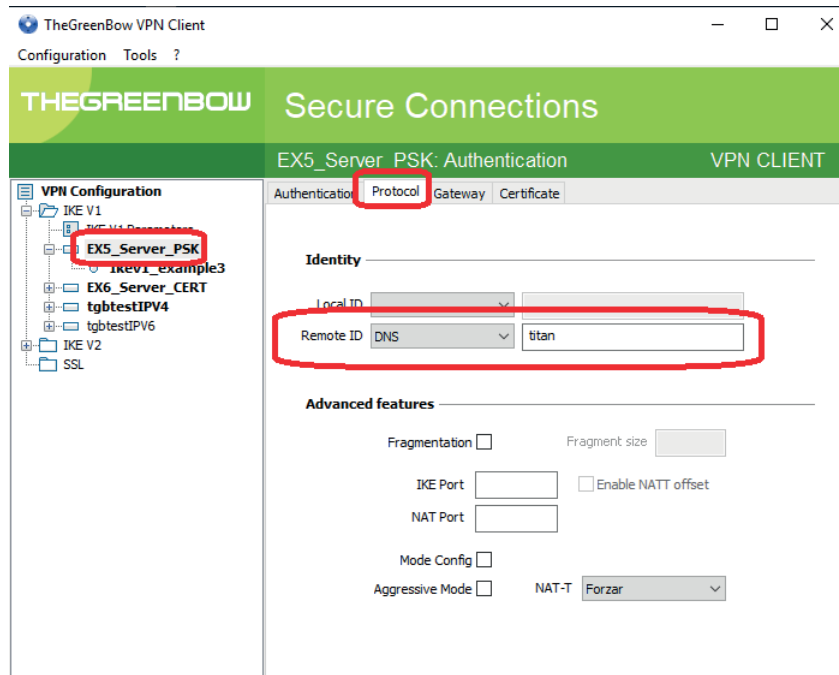
4.1 Authentication

The TITAN-based device's public IP address (which in this example is 88.28.221.23) 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 IKEv1 connection.



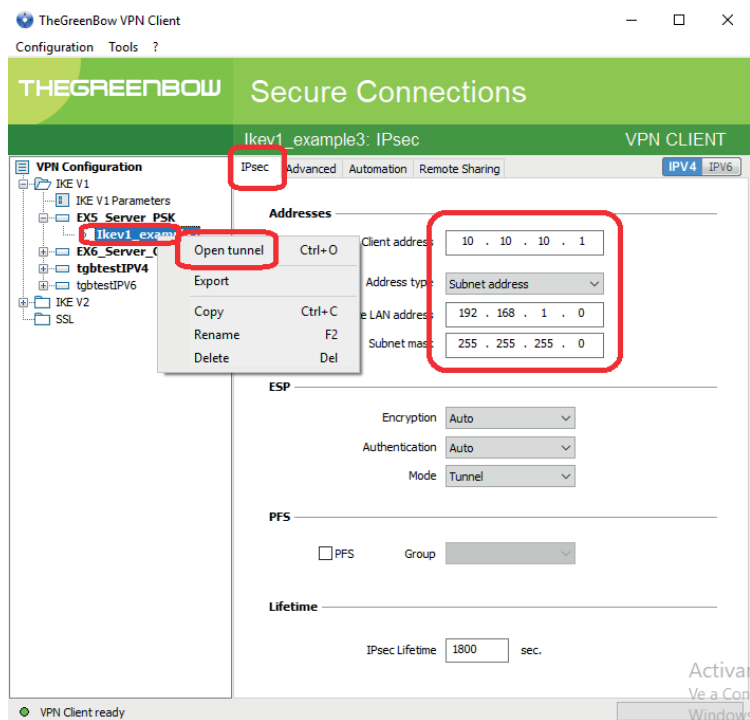
4.2 Protocol

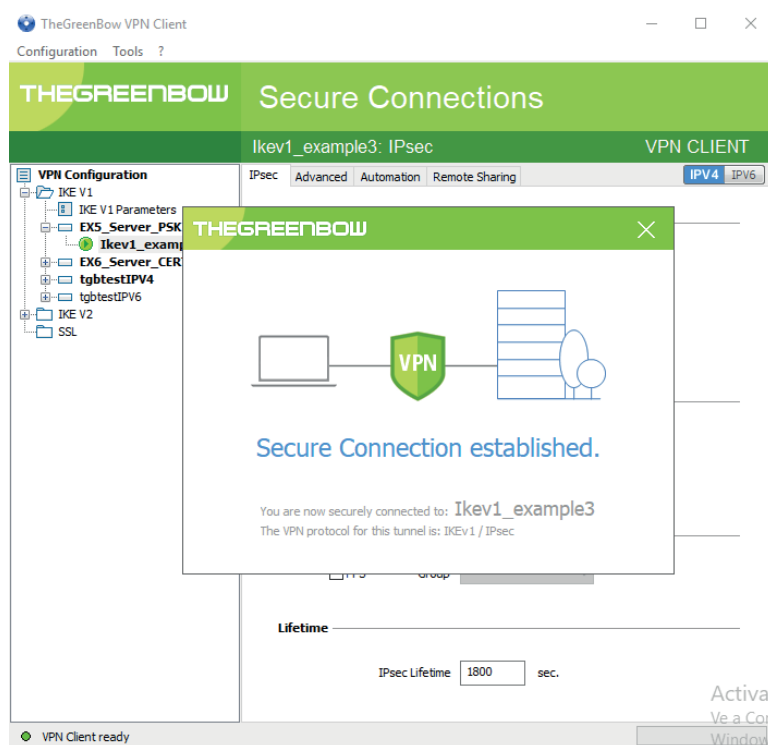
We must configure DNS and enter the remote ID as “titan” in the “Protocol” section, as this corresponds to the configured in the “leftid” field of the “ipsec.conf” file.



4.3 Child SA

Lastly, indicate the Virtual IP address that you are going to use in the “Child SA” tab (in this case 10.10.10.1 and the subnet of the TITAN server-based device 192.168.1.0 / 255.255.255.0). When this is configured we can open the IPsec tunnel by right-clicking on the connection and clicking on the “Open tunnel” option, as 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

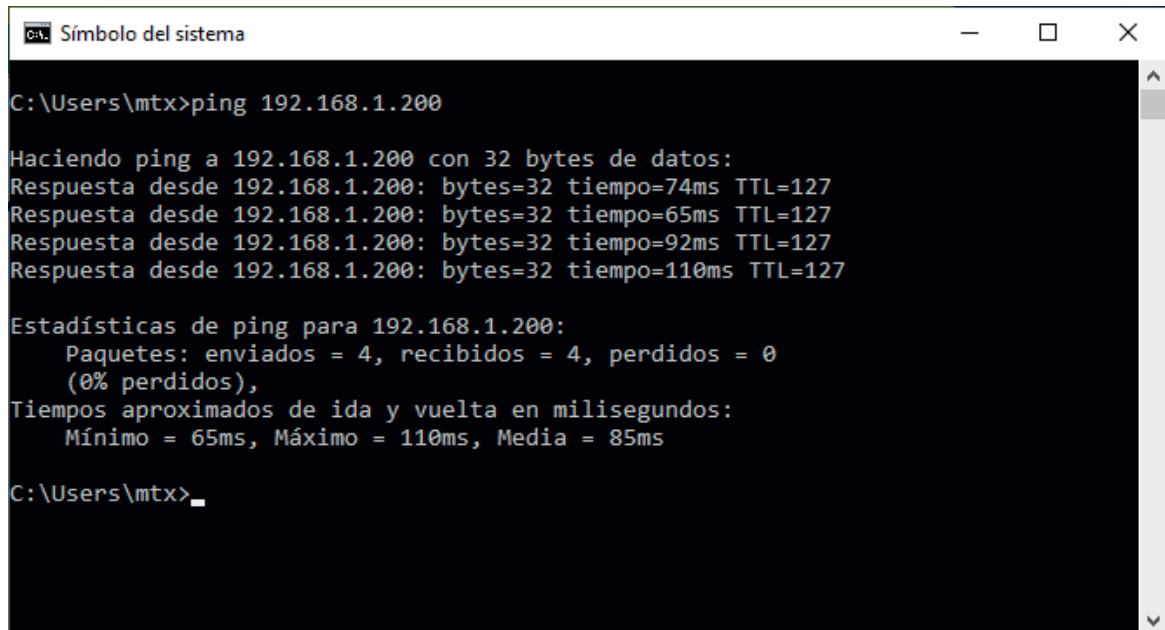
Haciendo ping a 192.168.1.2 con 32 bytes de datos:
Respuesta desde 192.168.1.2: bytes=32 tiempo=91ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=75ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=95ms TTL=64
Respuesta desde 192.168.1.2: bytes=32 tiempo=102ms TTL=64

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>_
```