TITAN

Application Note 47

IPSEC - Client-Server

IKEv1 - PSK Authentication

www.webdyn.com

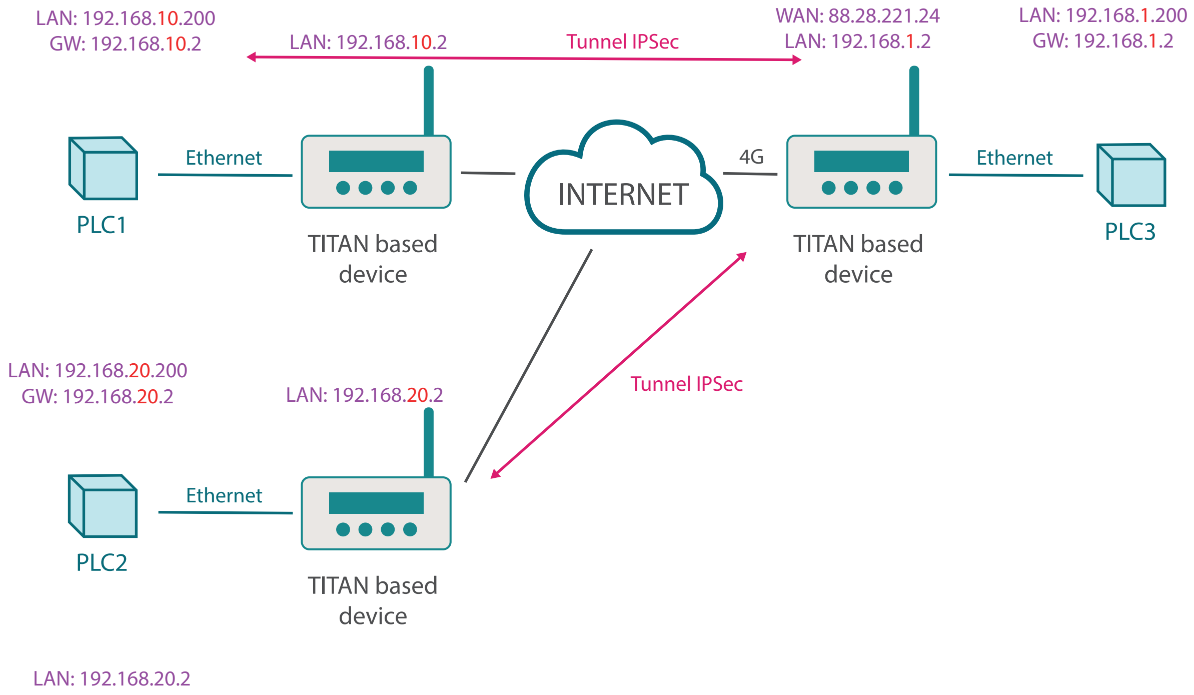
IPSEC - Client-Server

IKEv1 - PSK Authentication

1. Scenario Details

We need to implement a secure network between 3 PLCs to enable them to communicate with each other. To do this we will create an IPSec tunnel in which a TITAN-based device connected to the PLC3 will act as the IPSec Master. The device will have a SIM card with a fixed IP address of 88.28.221.24. The TITAN-based device connected to PLC2 and PLC3 will act as the IPSec Client. The following diagram shows the connection diagram with the relevant IP addresses of all devices.

Example of the proposed scenario:



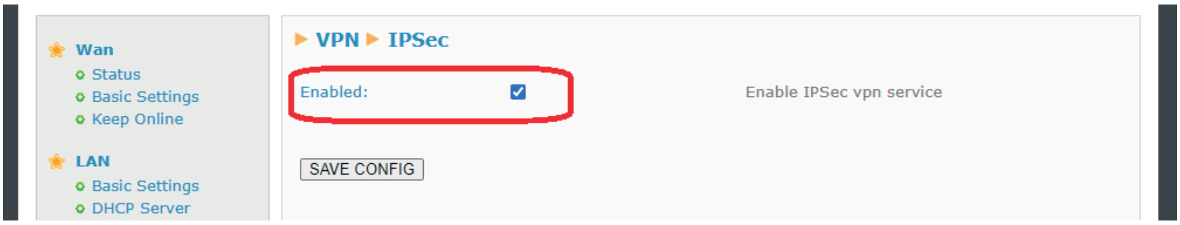
In this example, authentication using a secret key (PSK) will be used.

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 needed to enable remote access from other TITAN-based devices 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.

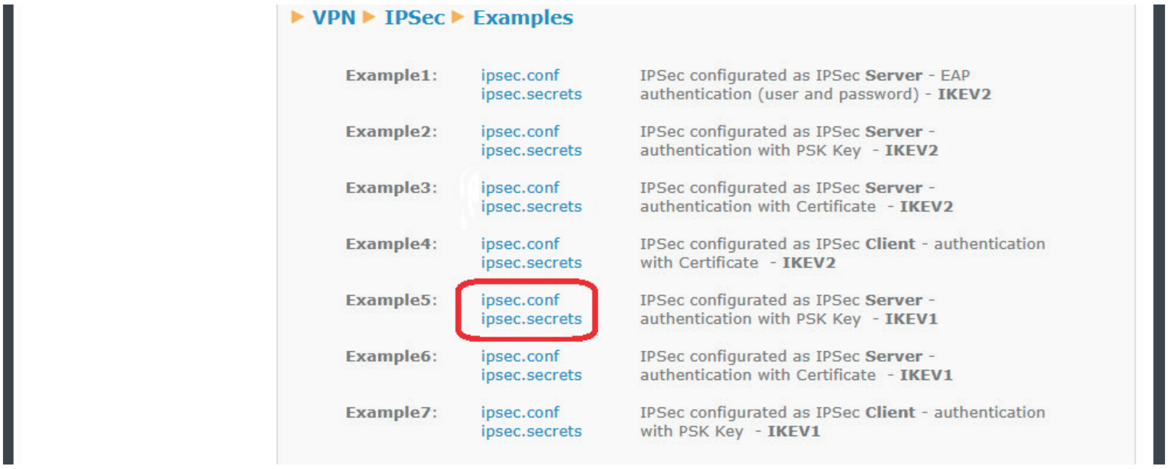
3. IPSEC configuration of the TITAN-based device (SERVER)

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



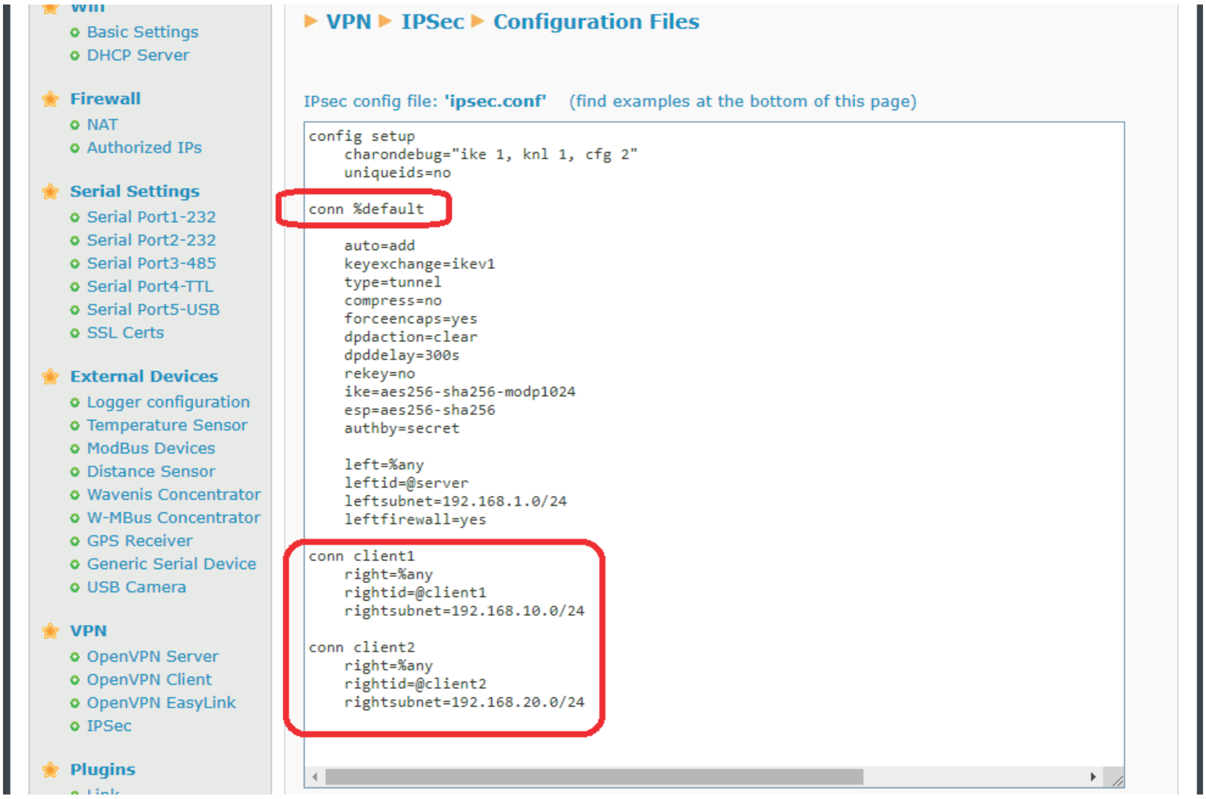
Enabled: ☑ Enable IPSec vpn service

Next, 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 5 (as we are configuring the server), 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 scenario and inserted into the appropriate box. For “ipsec.conf”:

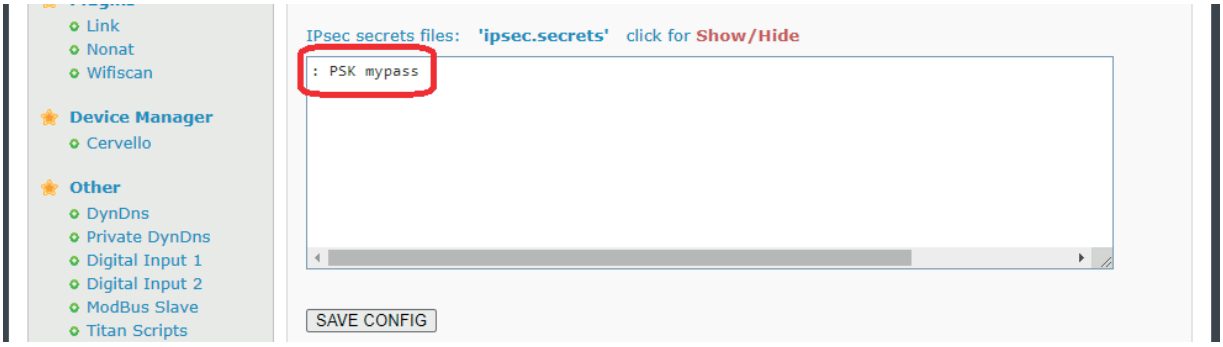


IPsec config file: **'ipsec.conf'** (find examples at the bottom of this page)

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

conn %default

    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=@server
    leftsubnet=192.168.1.0/24
    leftfirewall=yes

conn client1
    right=%any
    rightid=@client1
    rightsubnet=192.168.10.0/24

conn client2
    right=%any
    rightid=@client2
    rightsubnet=192.168.20.0/24
```

Note that the final file has been changed with respect to example 5, adding 2 connections for “client1” and “client2” and their corresponding subnets. The default connection parameters have also been changed to “conn %default”.

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

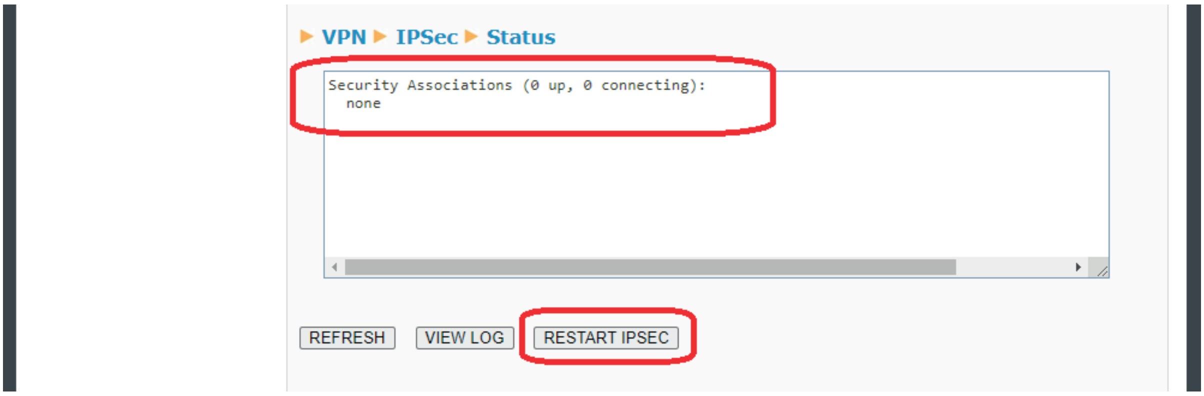


IPsec secrets files: **'ipsec.secrets'** click for **Show/Hide**

```
: PSK mypass
```

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.

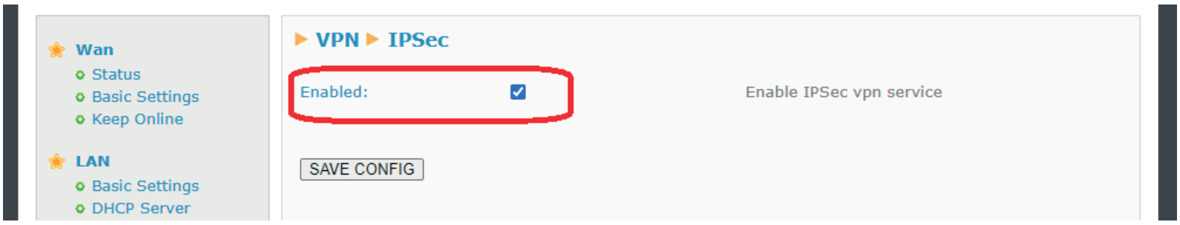


```
Security Associations (0 up, 0 connecting):
  none
```

4. IPSEC configuration of the TITAN-based device (CLIENT)

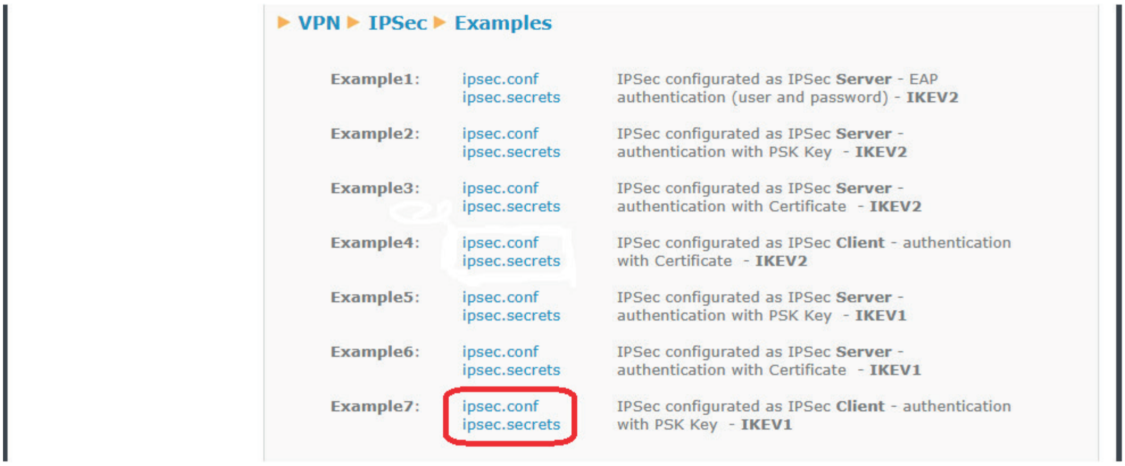
In this section we can configure the TITAN-based device acting as the IPSec client and connected to PLC1. Configuring the second Titan connected to PLC2 follows the same process.

Check the “Enabled” box at the top of the configuration page in the “VPN>IPSec” section and click on the “SAVE CONFIG” button.



Enabled: ☑ Enable IPSec vpn service

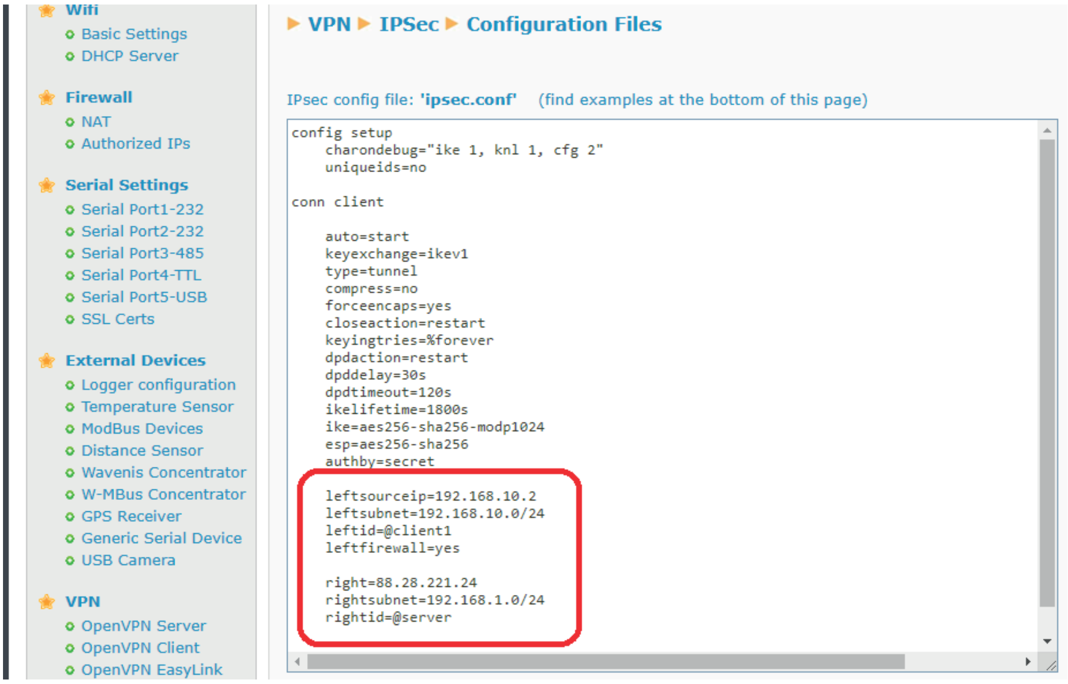
Next, since the TITAN-based device’s IPSec service is based on strongswan, the “ipsec.conf” and “ipsec. secrets” files must also be configured. The simplest solution is to go to the examples at the bottom of the page and choose the example that is closest to your configuration needs. We will choose example 7 for this application note (as we are configuring the Client), clicking on (downloading) the corresponding “ipsec.conf” and “ipsec.secrets” files, which we will open with Notepad to extract their contents.



▶ VPN ▶ IPSec ▶ Examples

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 scenario and inserted into the appropriate box. For “ipsec.conf”:



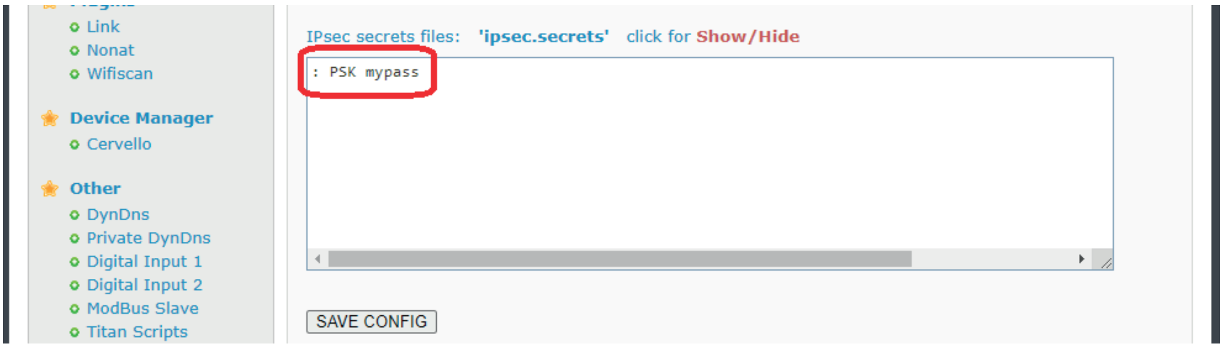
▶ VPN ▶ IPSec ▶ Configuration Files

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 client

    auto=start
    keyexchange=ikev1
    type=tunnel
    compress=no
    forceencaps=yes
    closeaction=restart
    keyingtries=%forever
    dpdaction=restart
    dpddelay=30s
    dpdtimeout=120s
    ikelifetime=1800s
    ike=aes256-sha256-modp1024
    esp=aes256-sha256
    authby=secret

    leftsourceip=192.168.10.2
    leftsubnet=192.168.10.0/24
    leftid=@client1
    leftfirewall=yes

    right=88.28.221.24
    rightsubnet=192.168.1.0/24
    rightid=@server
```

Remember that in “right” you must indicate the public IP of the TITAN-based device acting as the IPSec Master, in this example it is 88.28.54.84. Also note that the value in leftid must be “@client1”, as that is how it is configured for Client1 in the Titan IPSec server’s “ipsec.conf” file.

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

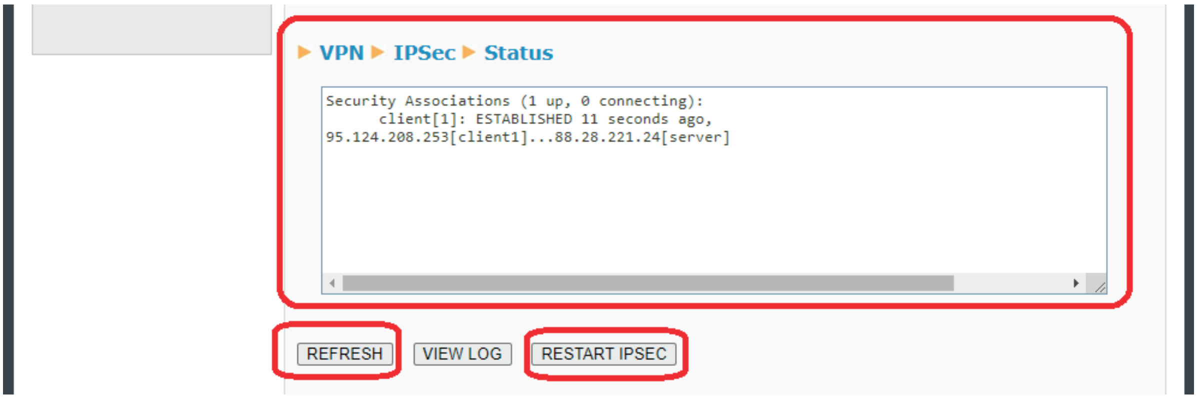


IPsec secrets files: 'ipsec.secrets' click for Show/Hide

```
: PSK mypass
```

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. If everything works fine, you should see a screen like the one below:



```
Security Associations (1 up, 0 connecting):
      client[1]: ESTABLISHED 11 seconds ago,
95.124.208.253[client1]...88.28.221.24[server]
```

At this point, PLC1 (client) and PLC3 (server) can already interact with each other through a secure IPSec tunnel. For example, you could PING PLC3 from PLC1 and vice versa. Repeat the same configuration procedure for the TITAN-based device connected to PLC2.