webdyn
flexitron group

TITAN

Nota de aplicación 45

IPSEC - Server

IKEv1 - PSK Authentication

www.webdyn.com

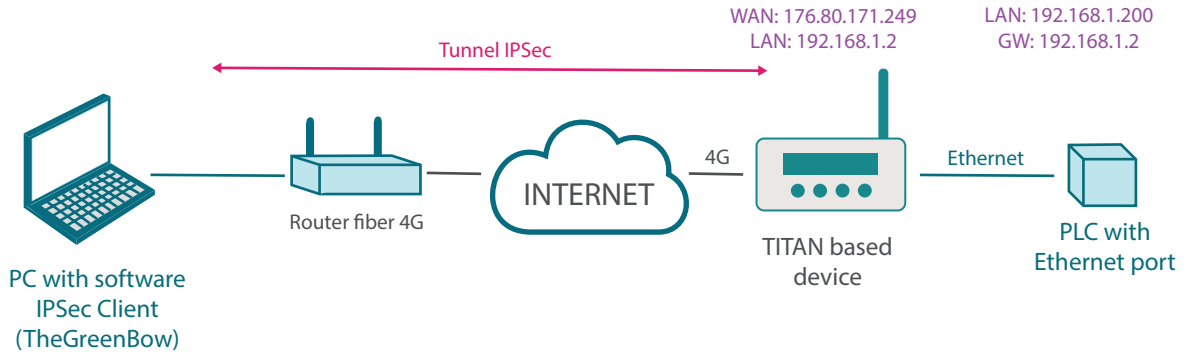
IPSEC - Server

IKEv1 - PSK Authentication

1. Detalles del escenario

Desde un PC se pretende acceder remotamente a la configuración de un equipo basado en TITAN y a la configuración de un PLC conectado vía Ethernet. Todo ello a través de una conexión segura de tipo IPSec. Se pretende utilizar IKEv1 y autenticación PSK.

Ejemplo del escenario planteado:



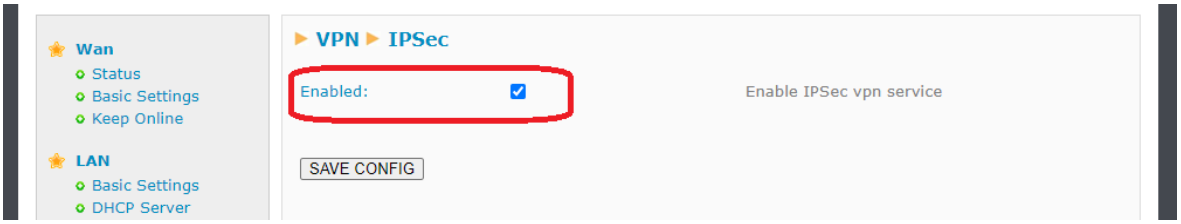
Básicamente con este ejemplo se pretende crear una VPN IPSec desde un PC (el cual dispone de un software de Cliente IPSec como puede ser TheGreenBow el cual es utilizado en este ejemplo) contra un equipo basado en TITAN 4G remoto que actuará como Servidor IPSec el cual tiene a su vez conectado un PLC a su puerto Ethernet.

2. Configuraciones y requisitos previos

El requisito básico para poder llevar a cabo la aplicación es que la tarjeta SIM introducida en el equipo basado en TITAN que actuará como IPSec Server debe disponer de una dirección IP pública y estática. Ello es necesario para poder acceder remotamente desde un PC conectado a la internet pública.

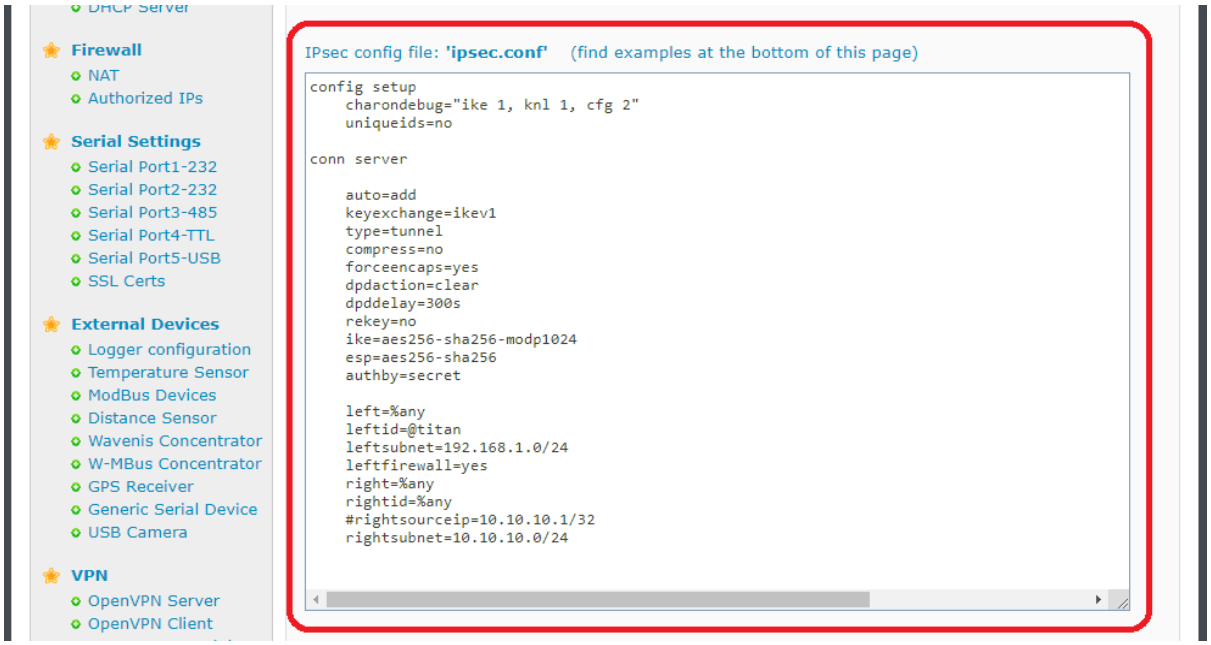
3. Configuración IPSEC del equipo basado en TITAN

Debe activarse la casilla “Enabled” que se encuentra en el inicio de esta página de configuración y pulsar el botón “SAVE CONFIG”.

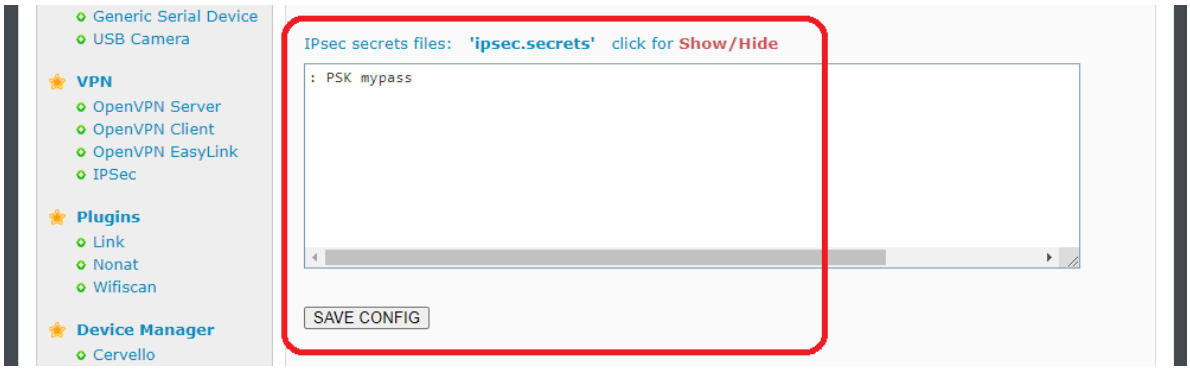


Por último, al estar basado el servicio IPSec del equipo basado en TITAN en strongswan, deben configurarse los ficheros “ipsec.conf” e “ipsec.secrets”. Lo más sencillo es acudir a los ejemplos de la parte inferior de la página y obtener el ejemplo más parecido a lo que se pretende configurar. En el caso de esta nota de aplicación se escoge el Ejemplo 5, haciendo click (descargando) los ficheros “ipsec.conf” e “ipsec.secrets” correspondientes, los cuales abriremos con un block de notas para obtener su contenido.

Dicho contenido debe adaptarse al ejemplo insertarse en las casillas apropiadas. Para “ipsec.conf”:



Y para “ipsec.secrets” (previamente debe hacerse click en la leyenda “Show/Hide” para mostrar la casilla):



Y seguidamente se pulsará el botón “SAVE CONFIG”, que grabará el contenido de ambos ficheros en la memoria interna del equipo basado en TITAN. Por último, si al arrancar el equipo no estaba iniciado el servicio IPSec (es decir, la casilla “Enabled” no estaba activa) debe reiniciarse completamente (menú “Other>Reboot”). Si ya estaba iniciado el servicio IPSec (casilla “Enabled” activa), puede pulsarse únicamente el botón “RESTART IPSEC” para reiniciar el servicio IPSec con la nueva configuración sin necesidad de reiniciar el equipo completamente, opción mucho más rápida.

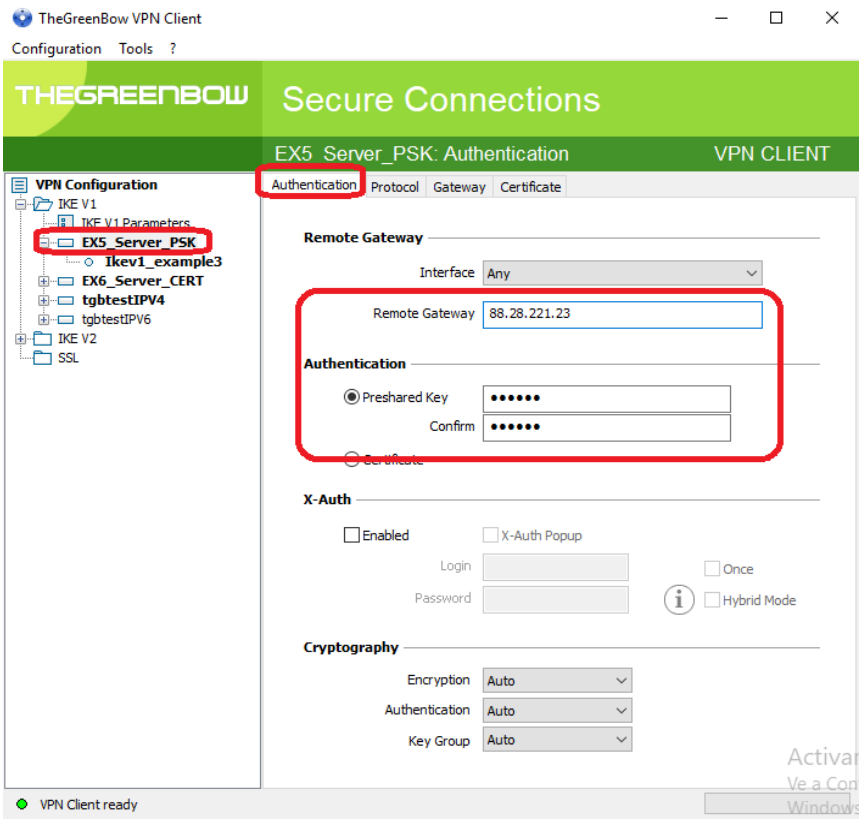
Una vez reiniciado el equipo basado en TITAN o pulsado el botón “RESTART IPSEC” (si el servicio ya estaba activo), aparecerá el estado de la conexión IPSEC como se indica a continuación. Si la casilla “Status” aparece en blanco es que quizás todavía no se ha iniciado el servicio. Espere unos segundos y pulse el botón “REFRESH”.

4. Configuración IPSEC cliente

En este ejemplo se utilizará el conocido software TheGreenBow para PC como software IPSec cliente para conectarse contra el equipo basado en TITAN. A continuación, se muestran unos pantallazos con la configuración básica de cada sección que debe configurarse.

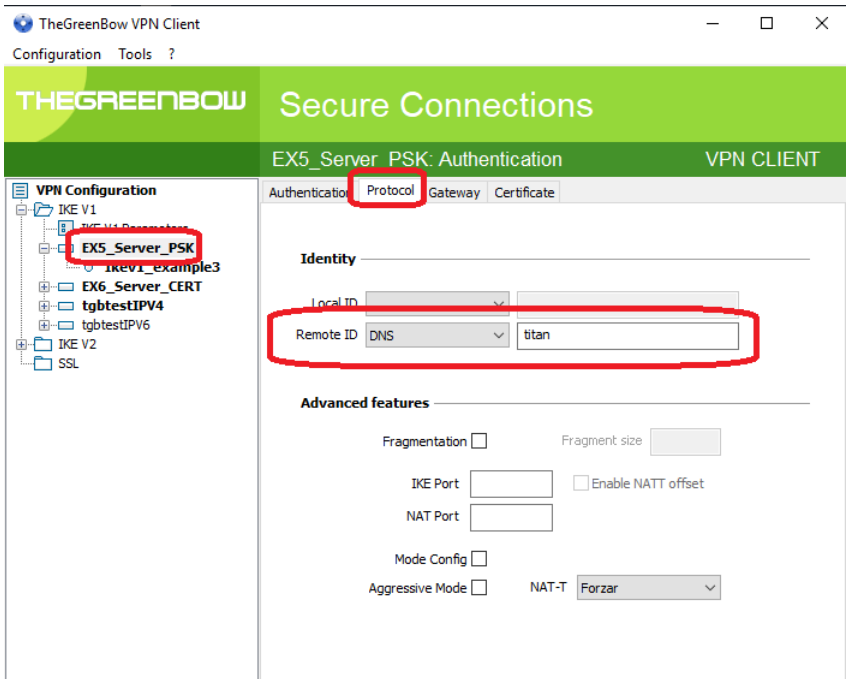
4.1 Autenticación

En la sección "Authentication" de la conexión de tipo IKEv1 debe indicarse la dirección IP pública del equipo basado en TITAN (en el caso de este ejemplo es 88.28.221.23) y el método de autenticación por "Preshared Key" (PSK), con clave "mypass" como se ha especificado en el fichero "ipsec.secrets" que se configuró en el equipo basado en TITAN en el punto anterior.



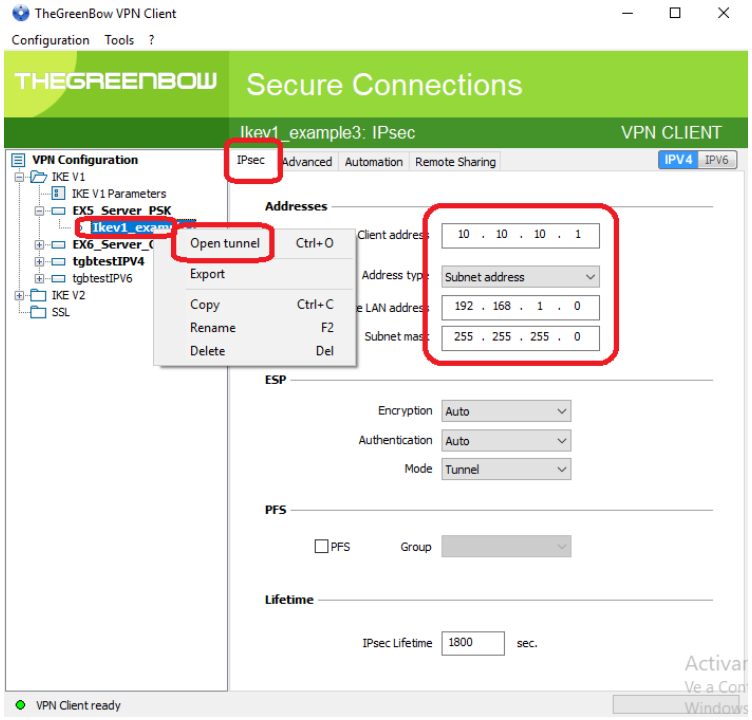
4.2 Protocol

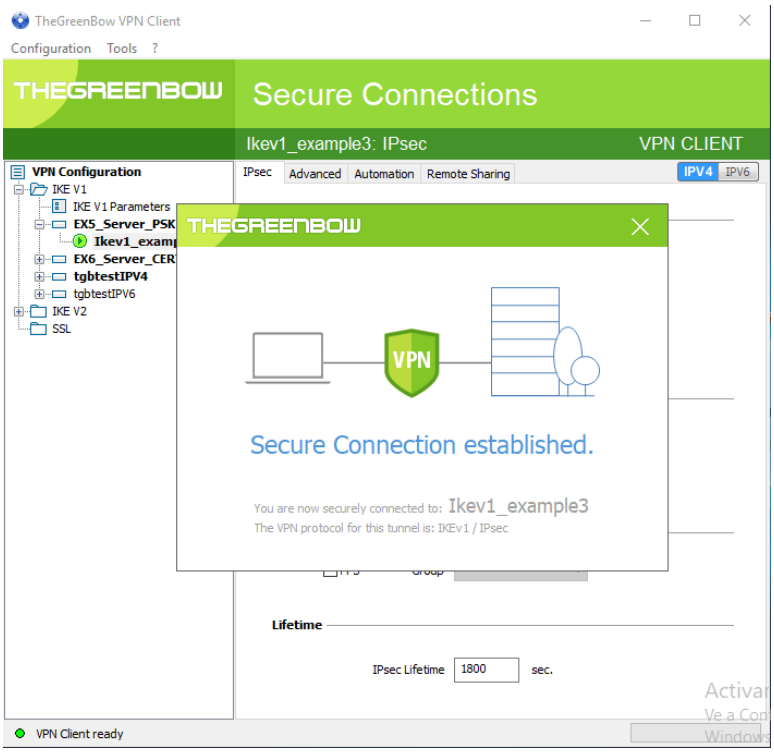
En la sección “Protocol” configuramos como DNS e introducimos el ID del remoto como “titan”, pues corresponde con lo configurado en el campo “leftid” del fichero “ipsec.conf”.



4.3 Child SA

Y, por último, simplemente, en la pestaña “Child SA” indicamos la dirección IP Virtual que vamos a tomar (en este caso 10.10.10.1 y la subred del equipo basado en TITAN servidor 192.168.1.0 / 255.255.255.0). Configurado ello ya es posible abrir el túnel IPSec haciendo click con el botón derecho del ratón sobre la conexión y pulsando la opción “Open tunnel” como se muestra en la siguiente pantalla.

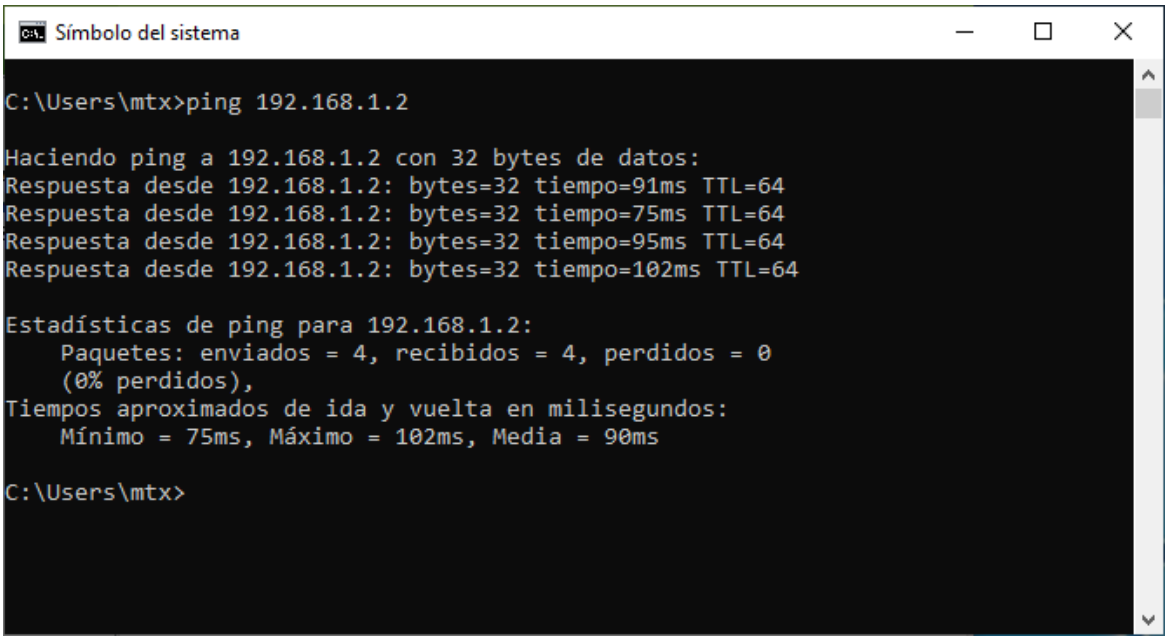
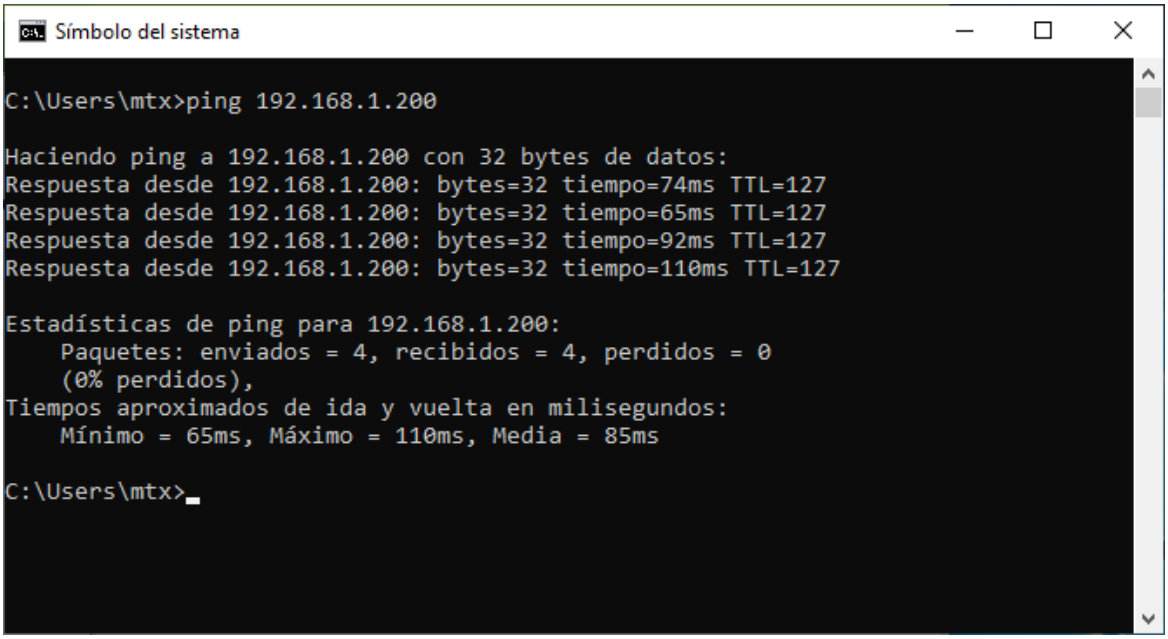




5. Comprobando la conectividad

Si la conexión se ha realizado con éxito, tan solo resta comprobar la conectividad, es decir, que desde el PC IPSec cliente sea posible acceder tanto al equipo basado en TITAN (IP: 192.168.1.2) como al PLC que cuelga del él (IP: 192.168.1.200). Para ello es posible realizar unos simples PING.

Ping al equipo basado en TITAN a través de la VPN IPSec desde el PC:



Ping al PLC a través dela VPN IPSec desde el PC: