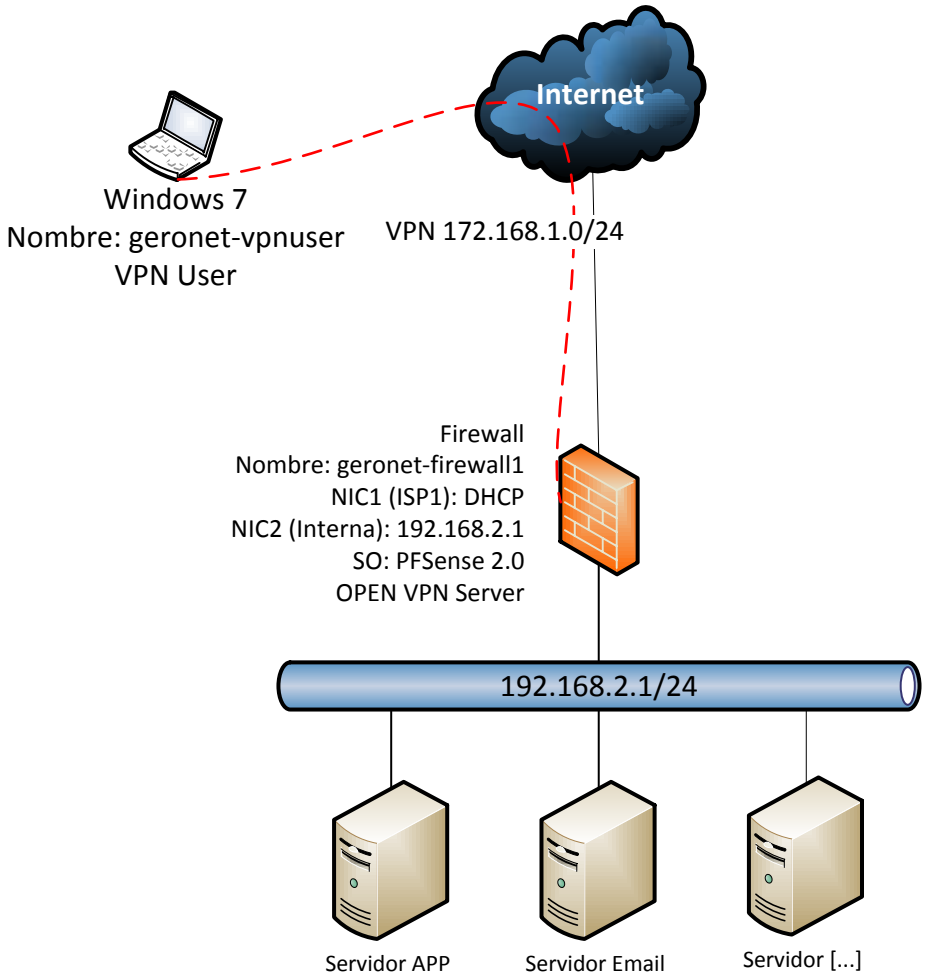
Configuración de PFSense 2.0 con OpenVPN Road Warrior.

Esta vez el escenario propuesto consiste en que un cliente requiere conectarse en forma remota a nuestra organización con una conexión VPN segura que permita acceder a todos los servicios de la red interna de nuestra empresa. Por eso a continuación describiré los pasos necesarios para realizar esta configuración implementando un firewall con PFSense 2.0.

Escenario:



Los pasos necesarios para conseguir nuestro objetivo son los siguientes:

1. Crear una autoridad certificadora.
2. Crear un tunel VPN.
3. Crear un certificado de servidor.
4. Crear un certificado de cliente.
5. Instalar el cliente en una PC.
6. Establecer la conexión VPN.

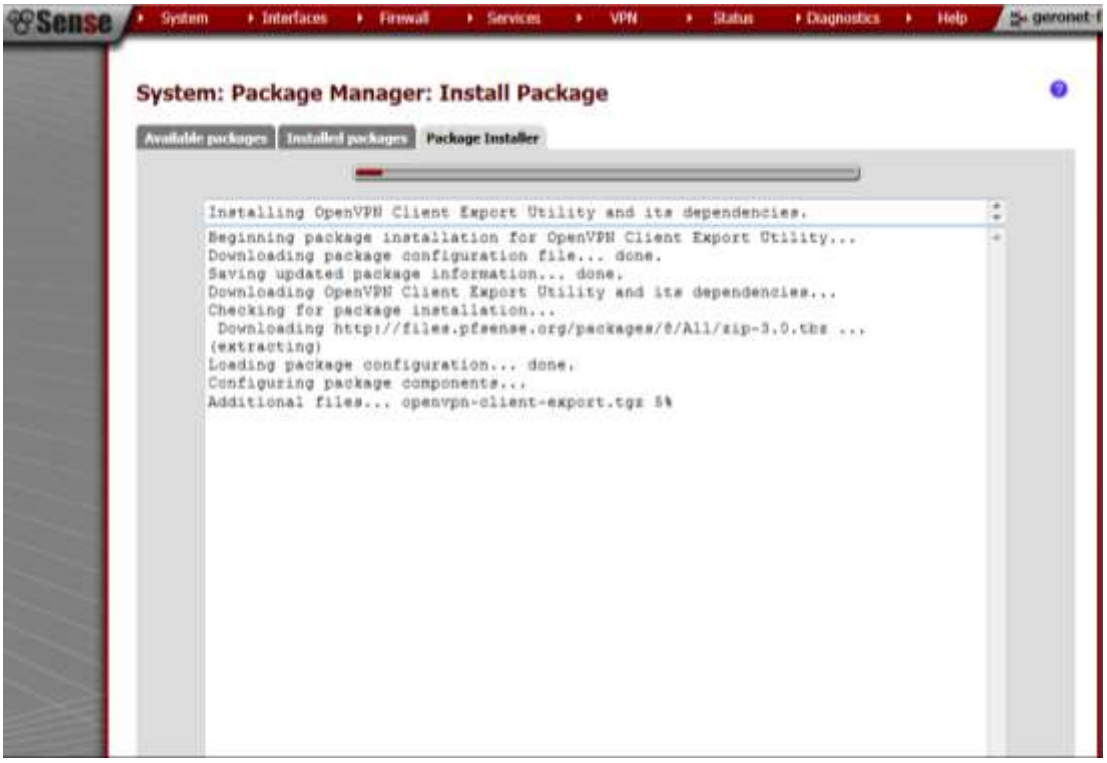
Para comenzar, una vez instalado nuestro PFSense, debemos descargar el paquete Open VPN

Client Export Utility.

Entonces vamos a **System→Packages**

Agregamos la utilidad de exportación pulsando en el símbolo (+):

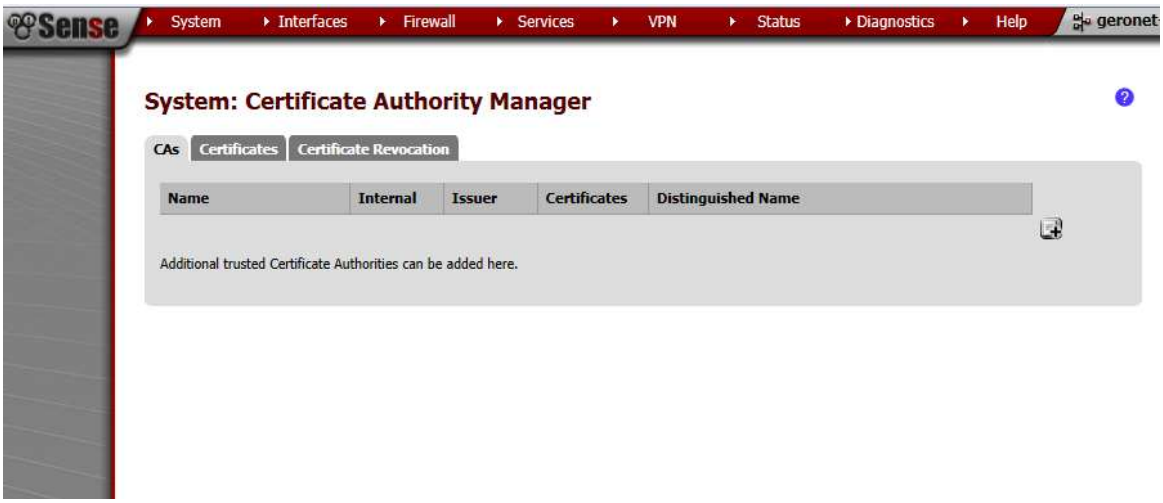
Nos muestra el progreso de la instalación y debemos verificar que termine correctamente:



Ahora crearemos en nuestro servidor la Autoridad certificadora.

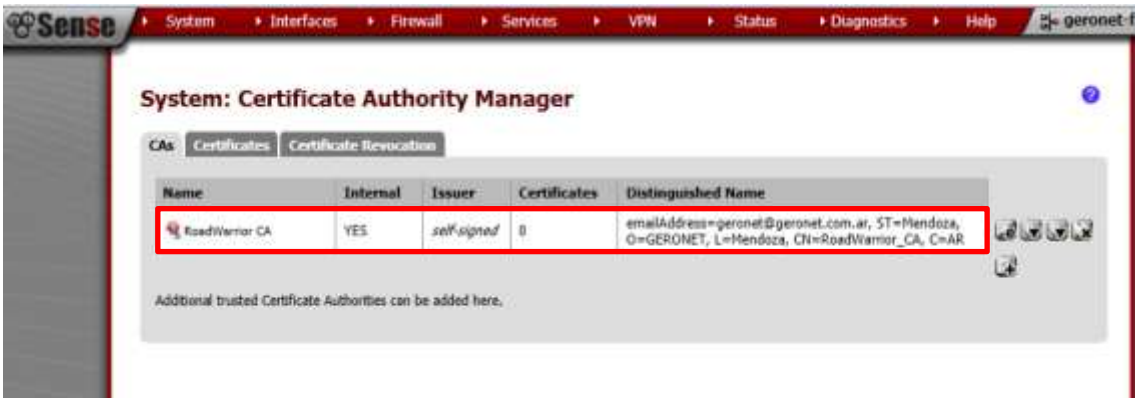
System → Cert Manager

Pulsando el botón (+) agregaremos una nueva autoridad:



Completamos los compos con los datos de nuestra empresa seleccionando en la opción Method **"Create an internal Certificate Authority"**:

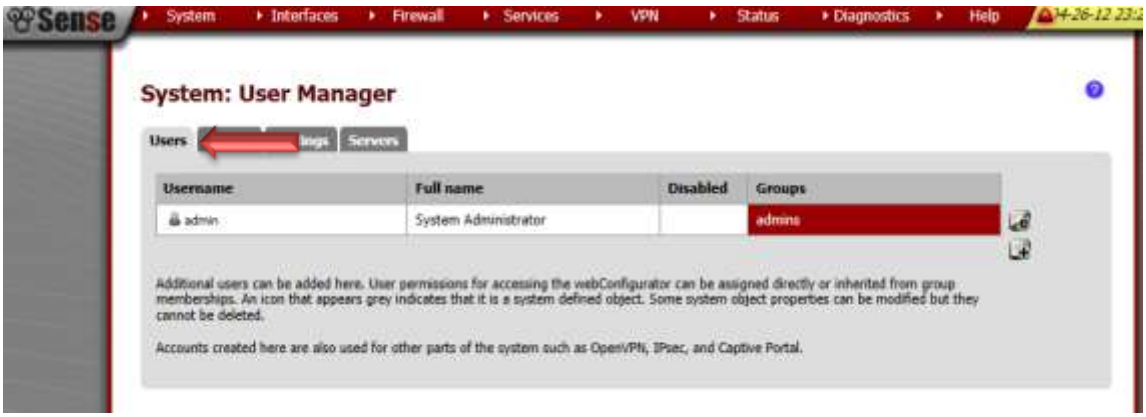
Guardando los cambios con **"Save"** podemos verificar en la pantalla anterior que ya se ha creado la autoridad certificadora:



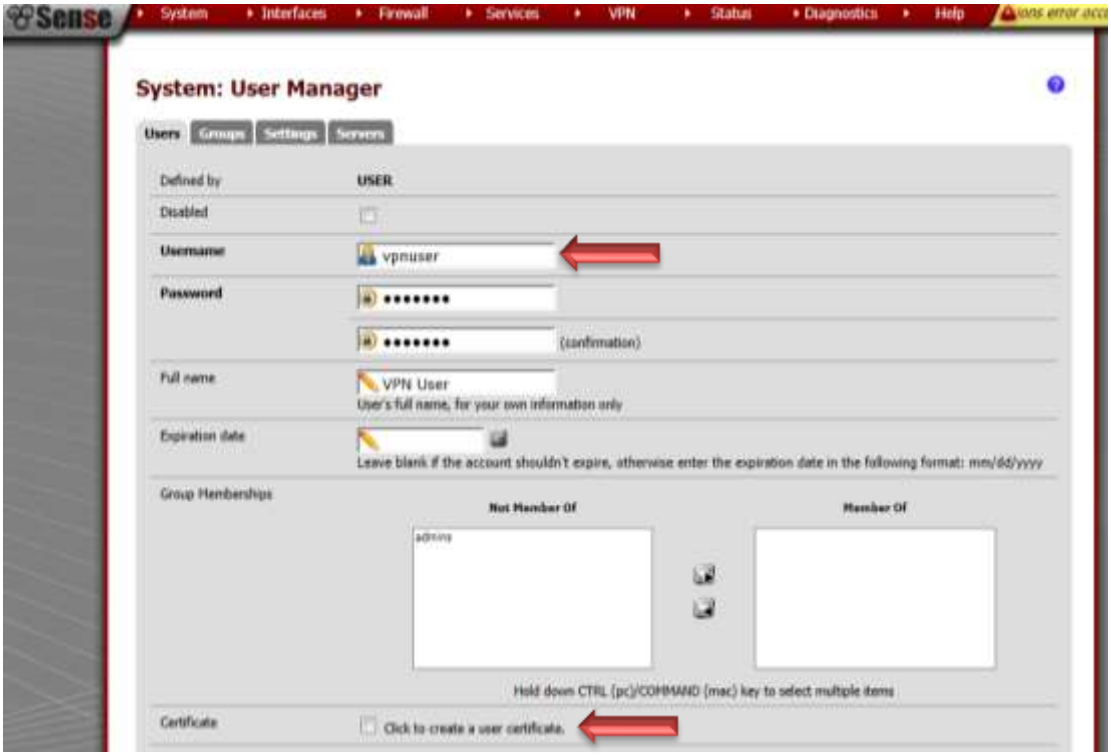
Ahora crearemos un usuario al cual le generaremos un certificado para poder conectarse a la VPN.

Para ello vamos a **System → User Manager**

En la pestaña **Users** pulsamos en el botón (+) para agregar un usuario:

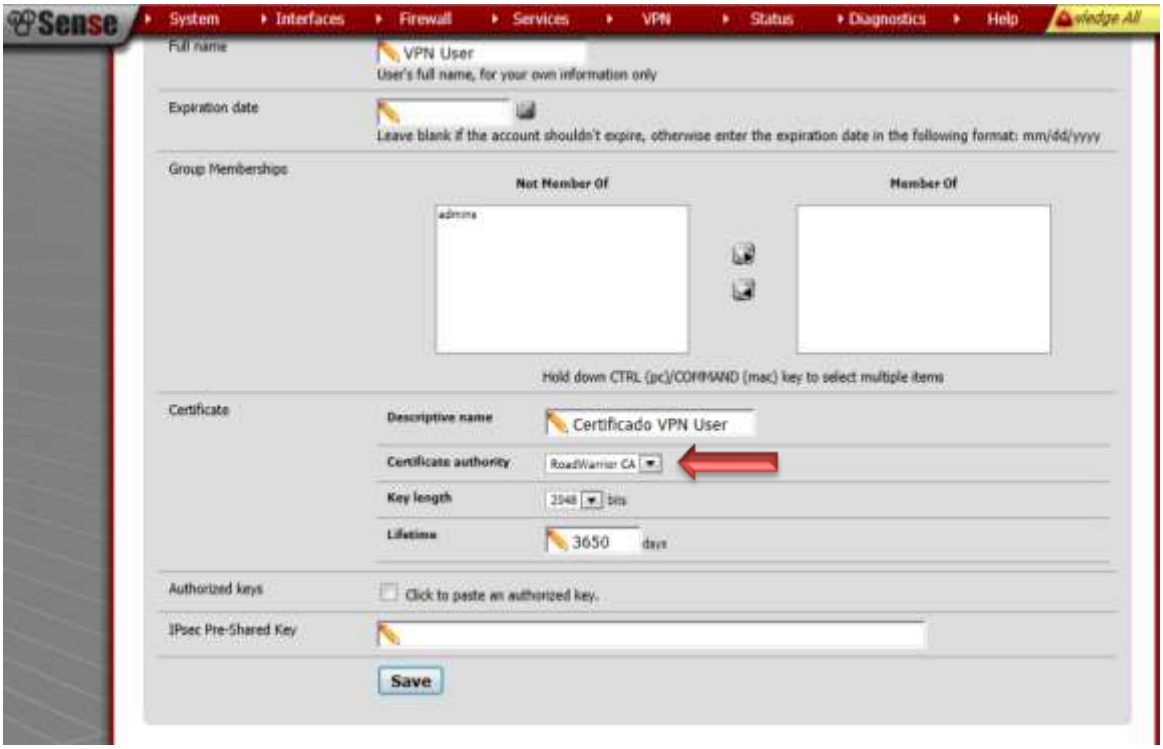


En nuestro caso crearemos el usuario “vpnuser” y le asignaremos un password.

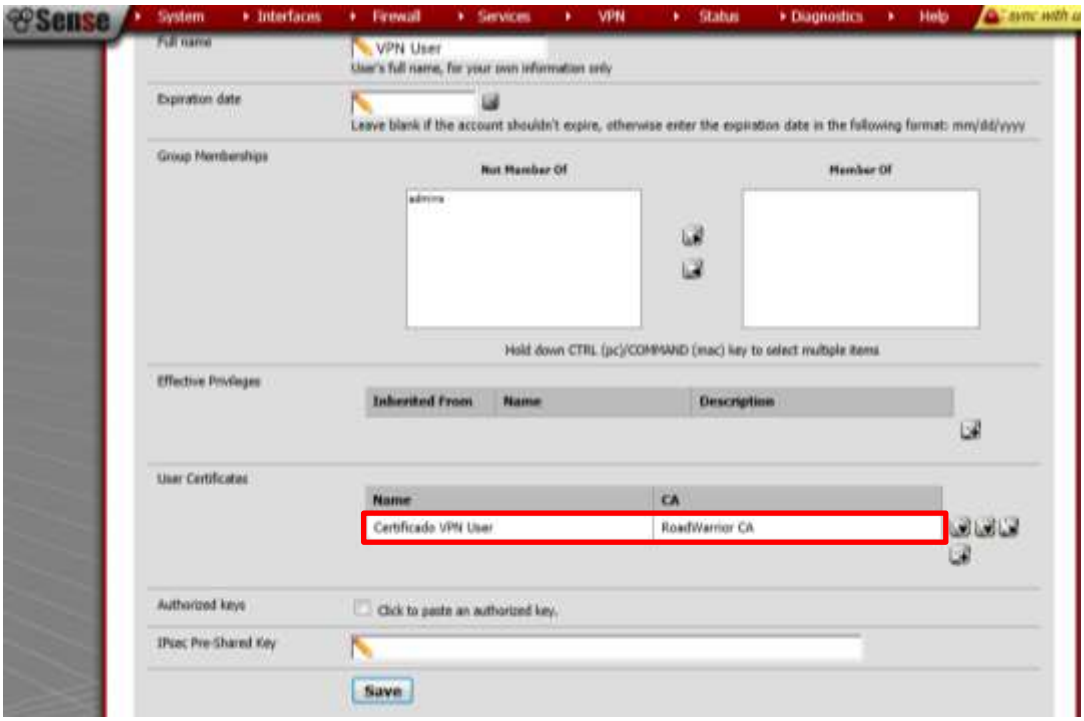


Debemos tildar la opción “**Click to créate a user certificate**” para que al momento de crear el usuario, también nos genere el certificado.

Debemos seleccionar la Autoridad de Certificación creada anteriormente y podemos definir un tiempo de vida para el certificado:



Luego guardando los cambios con **Save** y volviendo a ingresar a los datos del usuario veremos el certificado creado:



Nuestro próximo paso será crear el servidor.

Para esto vamos al menú **VPN→OpenVPN**:

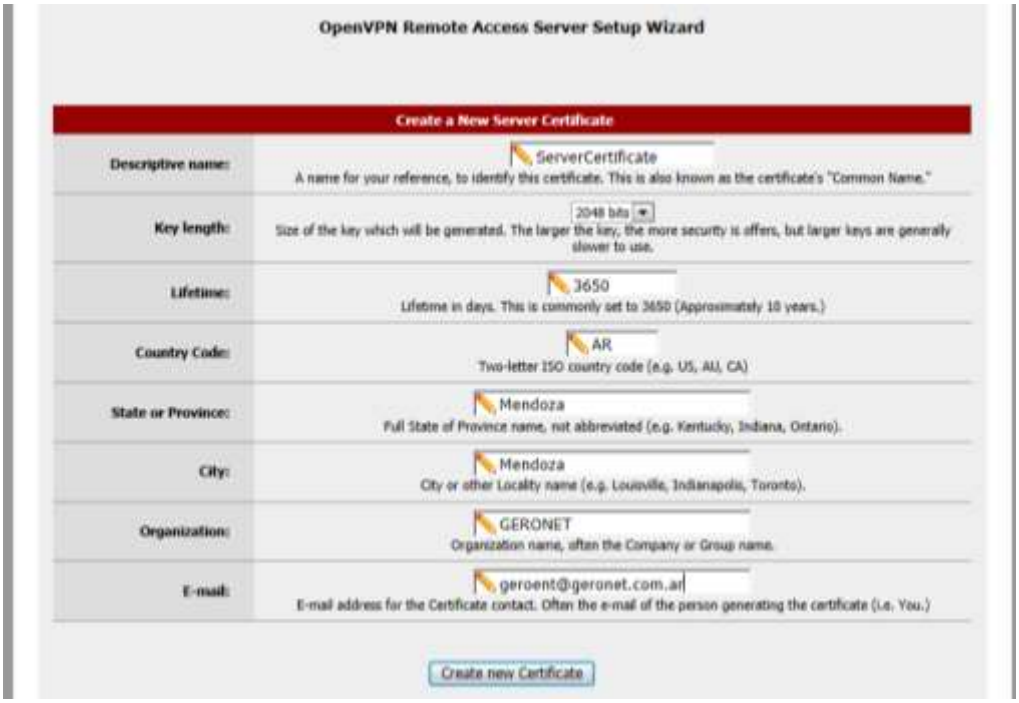
Utilizaremos un Wizard llendo a la pestaña del mismo nombre y pulsadon el botón (+):

En **Type of Server**, seleccionaremos **Local User Access**, ya que nuestros usuarios se crearán desde el firewall:

Pulsamos **Next**, y seleccionamos la autoridad de certificación creada:

Pulsando Next, generaremos nuestro certificado de Servidor, pulsando el botón **Add new Certificate**

En esta pantalla generaremos el certificado que estará en nuestro server. Completamos con los datos de nuestra empresa y pulsamos en "**Create New Certificate**"



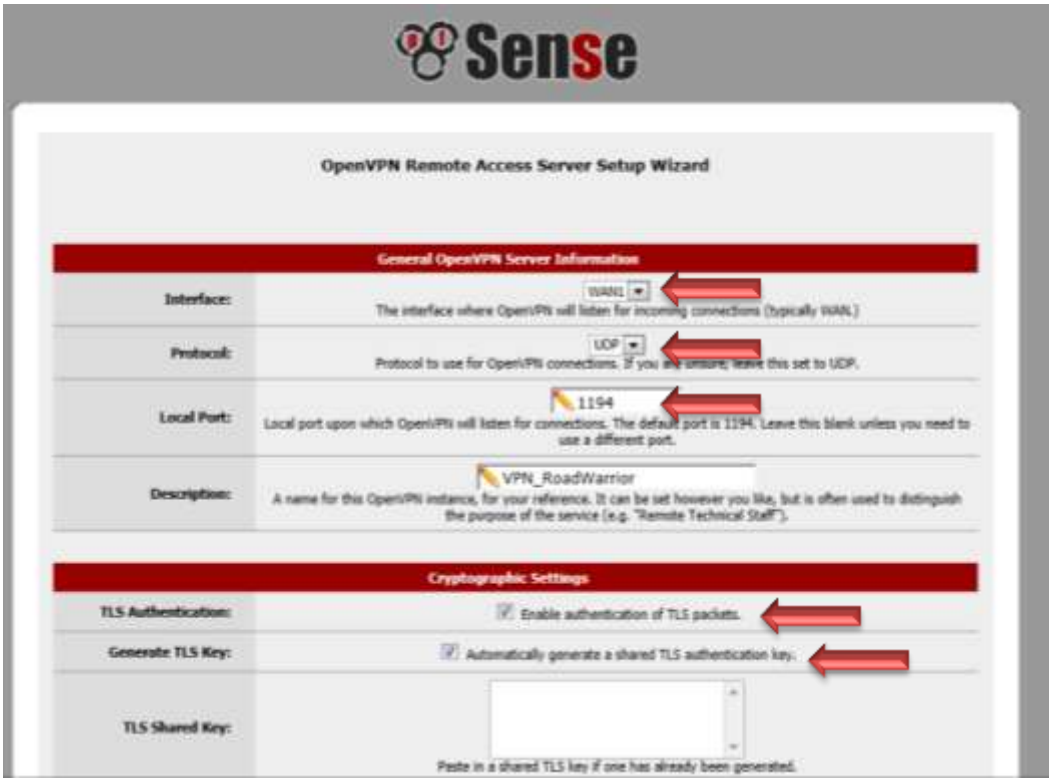
Luego configuraremos los siguientes campos:

Inteface: Será la placa que estará escuchando las conexiones entrantes de la VPN. Por lo general es nuestra WAN.

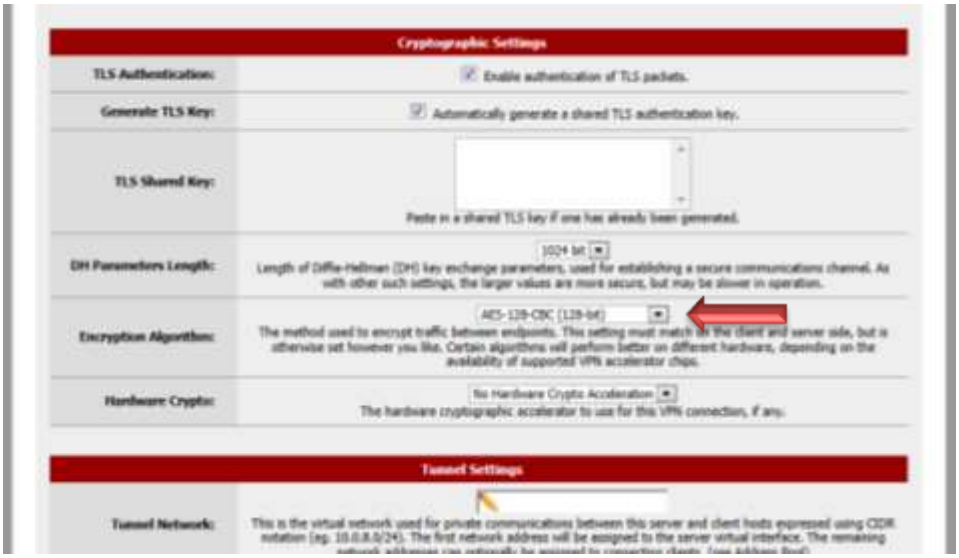
Protocol: Seleccionaremos UPD en este ejemplo.

Local Port: por defecto OpenVPN utiliza el 1194. Y lo dejaremos así. Aunque si se cambia no hay problemas.

Tildar la opción **TLS Autentication** y **Generate TLS Key**.



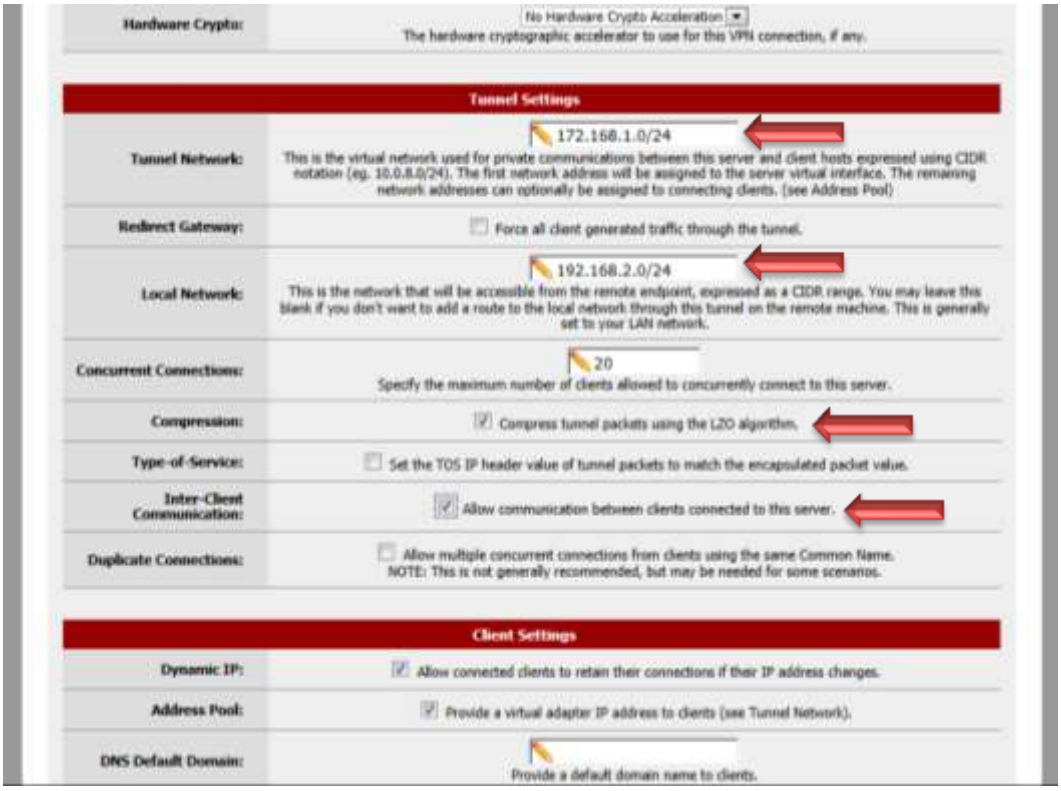
Seleccionamos un algoritmo de encriptación. Ej: AES-128:



En la misma pantalla tambien configuraremos la red que se utilizará en nuestro tunel:

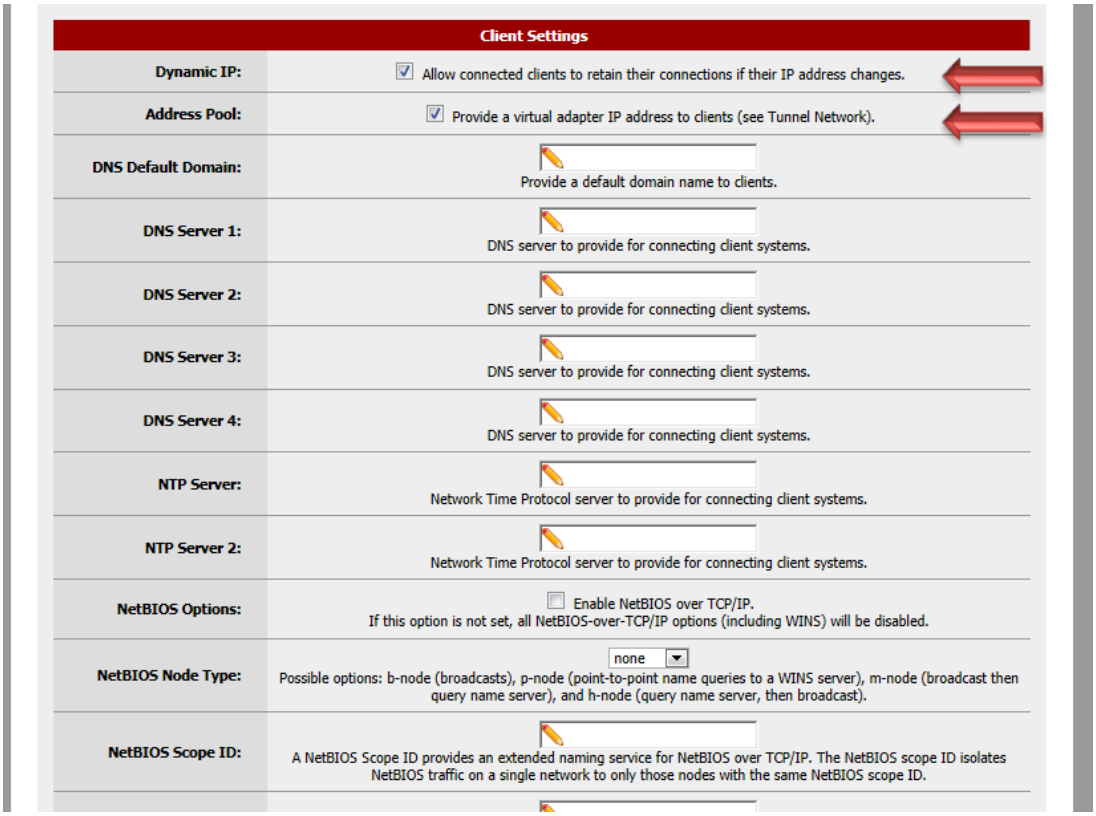
Tunnel Network: de acuerdo al ejemplo del primer gráfico ingresamos la red: 172.168.1.0/24

En **Local Network** debemos configurar la red de nuestra LAN Interna, en este caso: 192.168.2.0/24

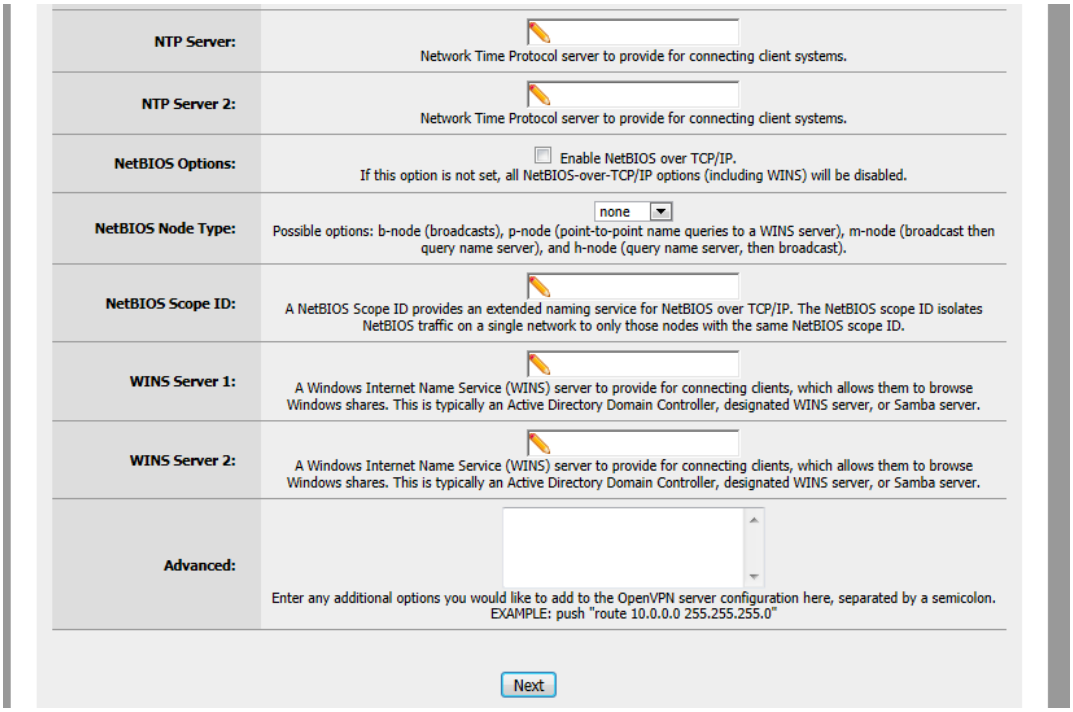


También habilitamos la compresión del tunel.

Tildamos la opción **Dynamic IP** y **Adddress Pool**:



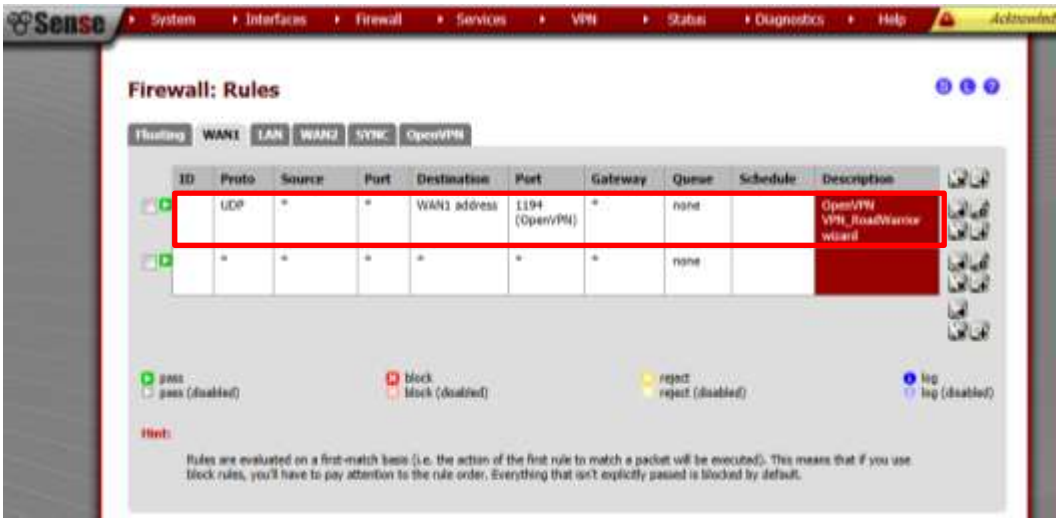
El resto de las configuraciones por ahora no las modificaremos, y pulsamos **Next**:



En este paso seleccionamos las opcines **Firewall Rule** y **OpenVPN rule** para que el asistene nos genere las reglas para permitir la conexión con la VPN en el firewall:

Pulsando **NEXT**, finaliza la configuración:

Ahora verificamos en **Firewall → Rules** que se hayan creados las reglas correspondientes en las interfaces WAN y OpenVPN:



El siguiente paso consiste en exportar desde nuestro firewall el paquete de instalación de OpenVPN y la configuración para nuestro cliente. Básicamente el paquete instalado en el primer paso nos permitirá obtener el instalador del Cliente VPN y su configuración para cada usuario generado en el sistema. En el ejemplo es nuestro **usrvpn** creado anteriormente.

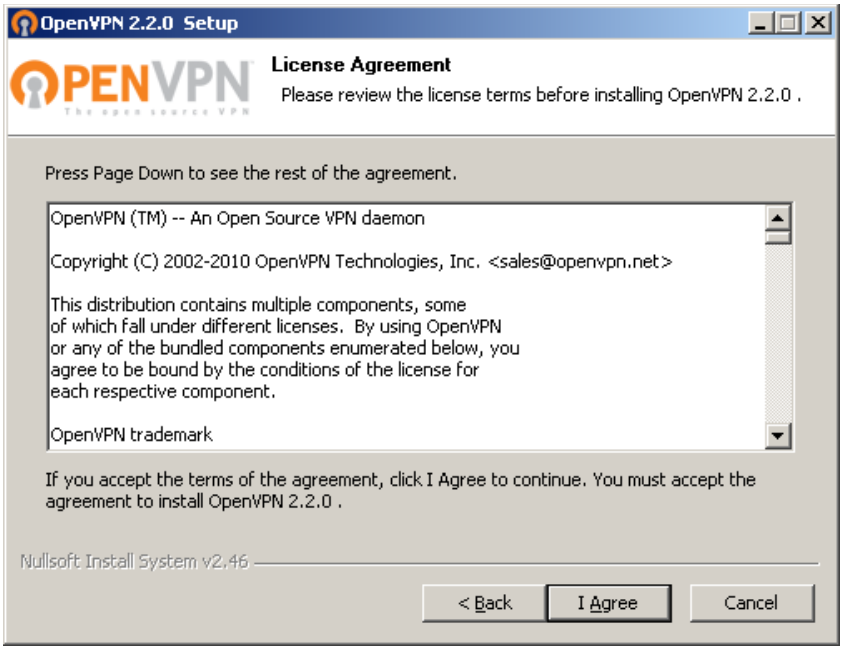
Para hacer esto vamos al menú **VPN→OpenVPN→Client Export**

Seleccionamos nuestro servidor y hacemos un clic en el link **Windows Installer:**

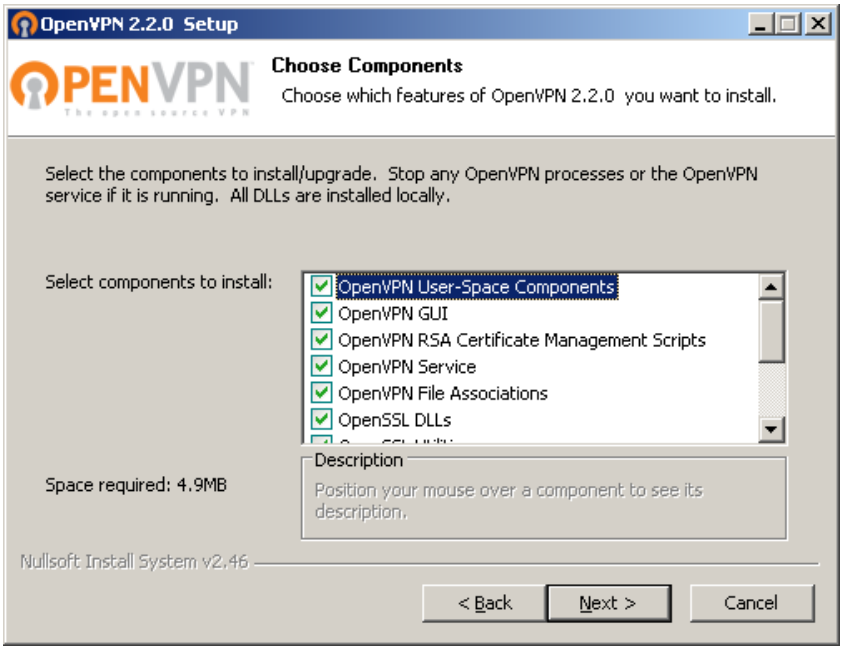
Guardamos el paquete generado para nuestro usuario y luego lo instalaremos en la PC que se conectará remotamente a nuestra red.

Ejecutamos el instalador:

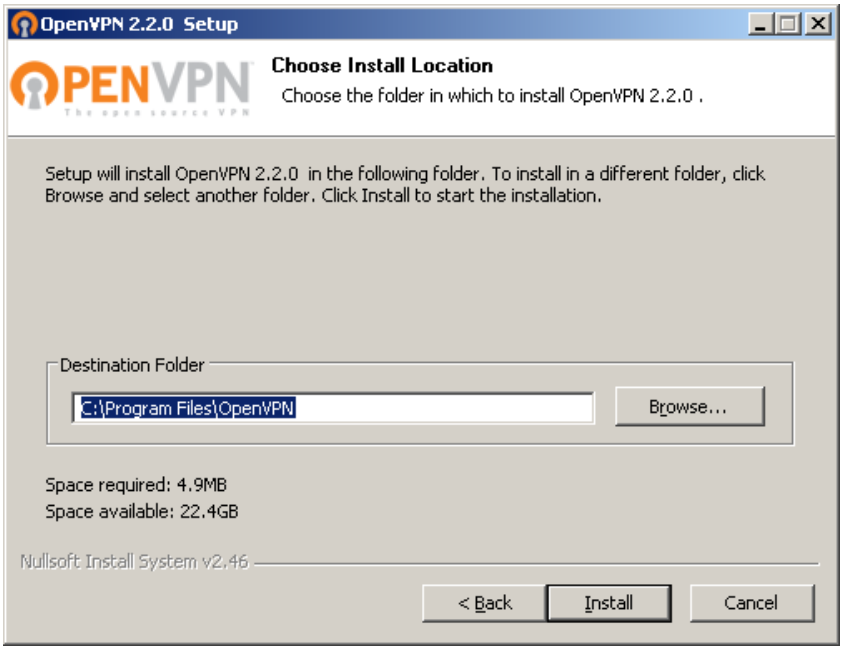
Pulsamos Next



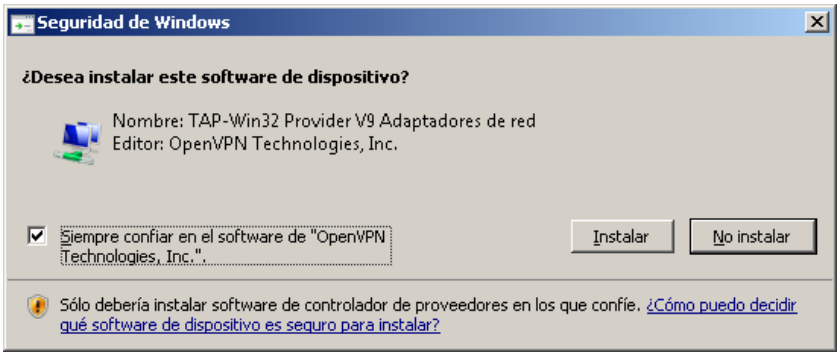
Aceptamos el acuerdo.



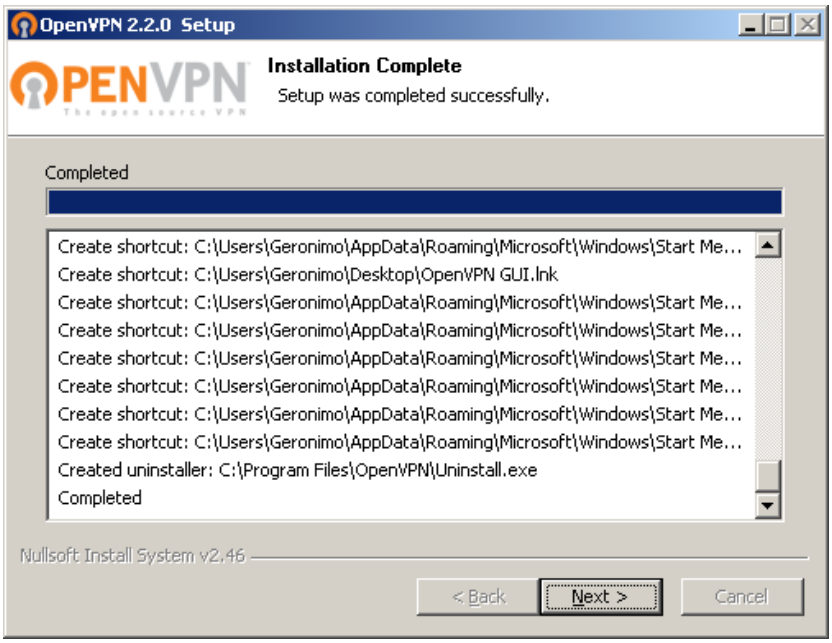
Dejamos tildada todas las opciones y **NEXT**



Pulsamos **Install**

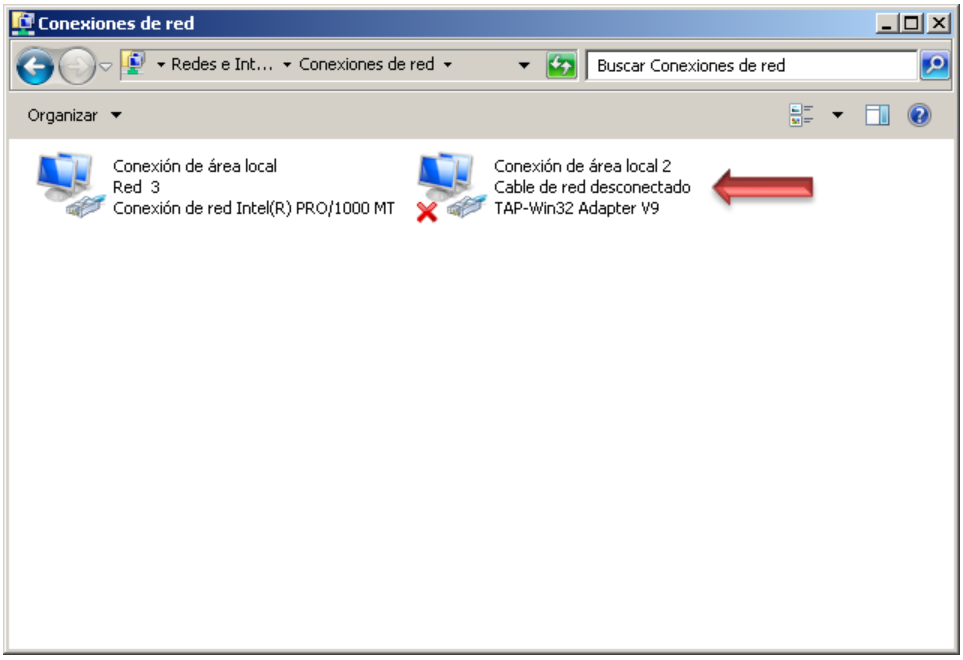


Se nos muestra el mensaje de que se quiere añador un dispositivo, al cual **tildamos la opción Siempre confiar en el Software de OpenVPN Technologies INC** y pulsamos **Instalar**.



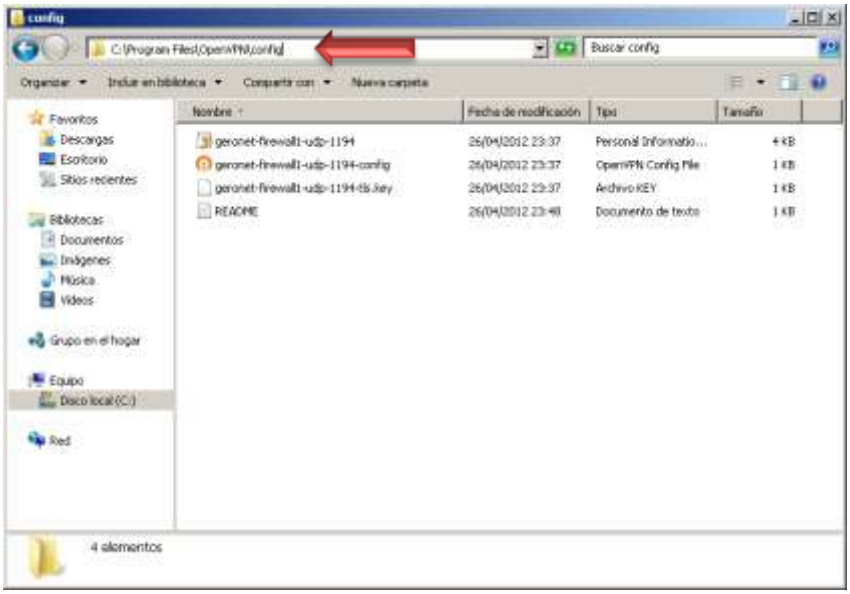
Una vez completada la opción pulsamos **Next** para finalizar.

Si nos vamos al administrador de dispositivos de red, podremos comprobar que se ha agregado un nuevo adaptador de red:

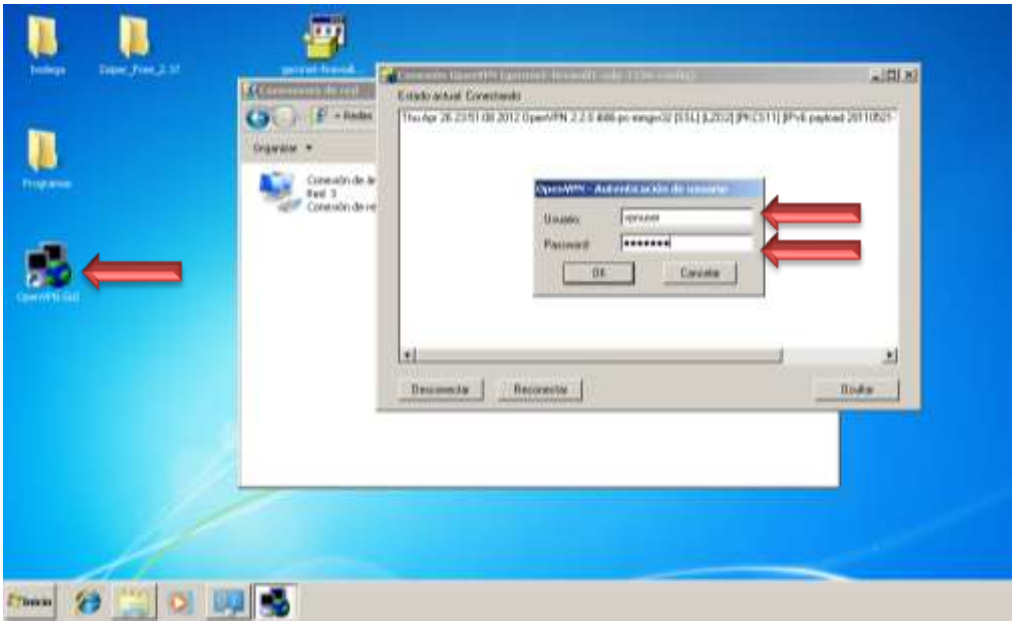


Este es quien controlará nuestra conexión.

En la carpeta: **c:\Program Files\OpenVPN\config** podremos encontrar que se encuentran los certificados para la conexión y la configuración necesaria para establecer la VPN. Aquí no de debe modificar nada, es solo para comprobar que se encuentren estos archivos:

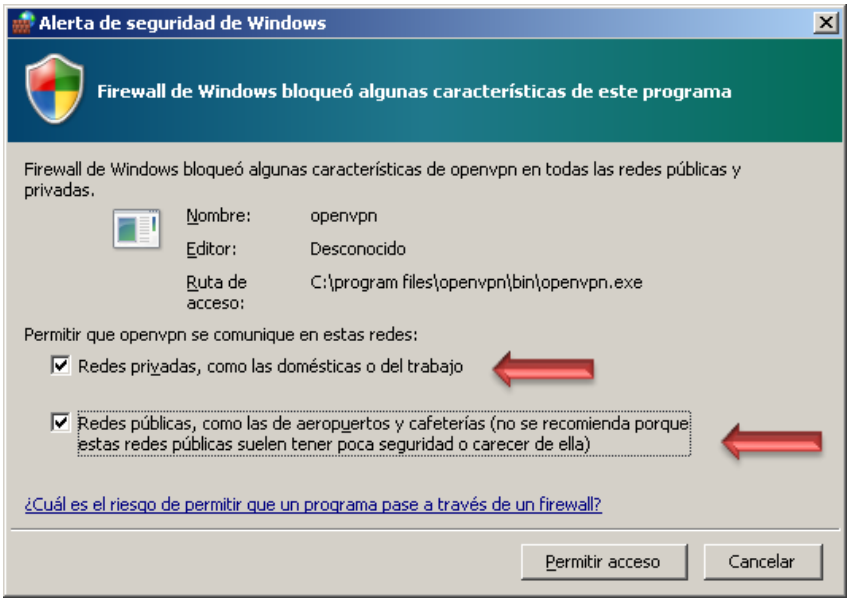


En nuestro escritorio se generó un acceso directo a la interfaz de usuario del cliente VPN, al cual accederemos e ingresaremos nuestro usuario y clave generados en nuestro firewall:

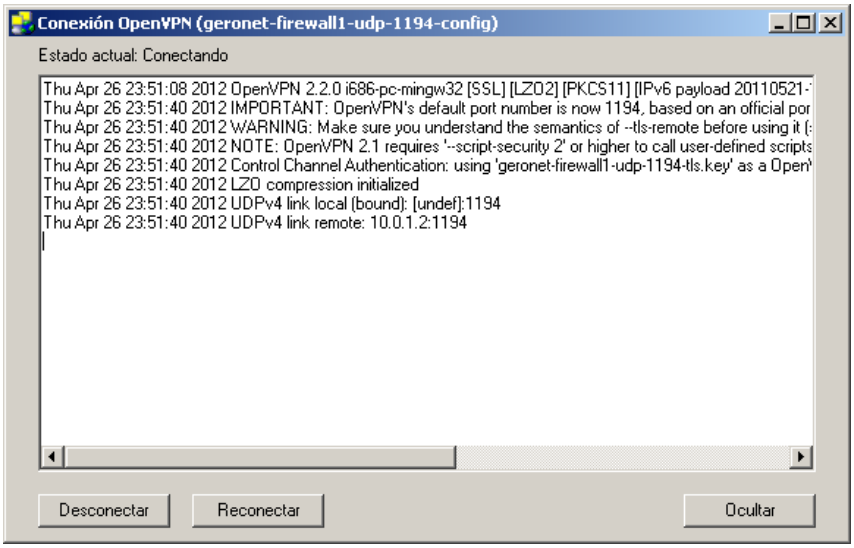


Pulsando OK, el sistema tratará de conectarse.

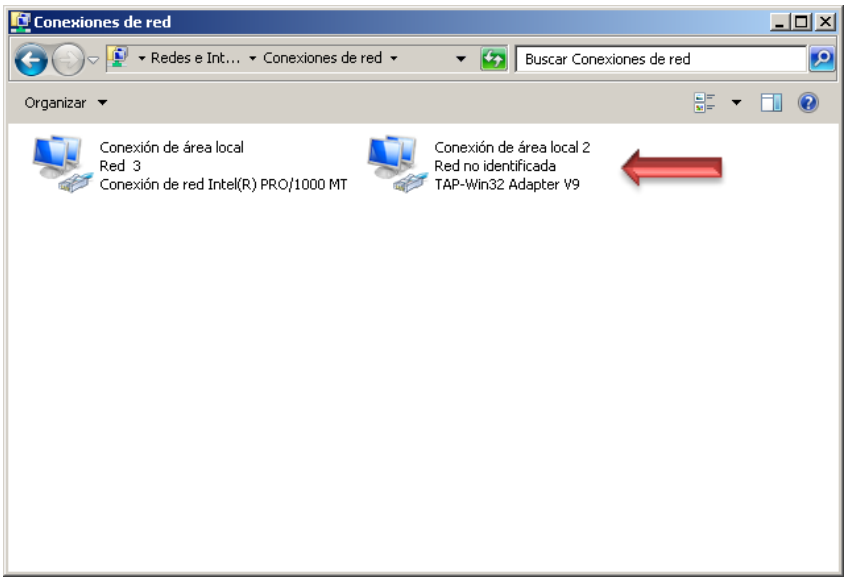
Debemos agregar estas excepciones al firewall de Windows si es que lo tenemos activado:



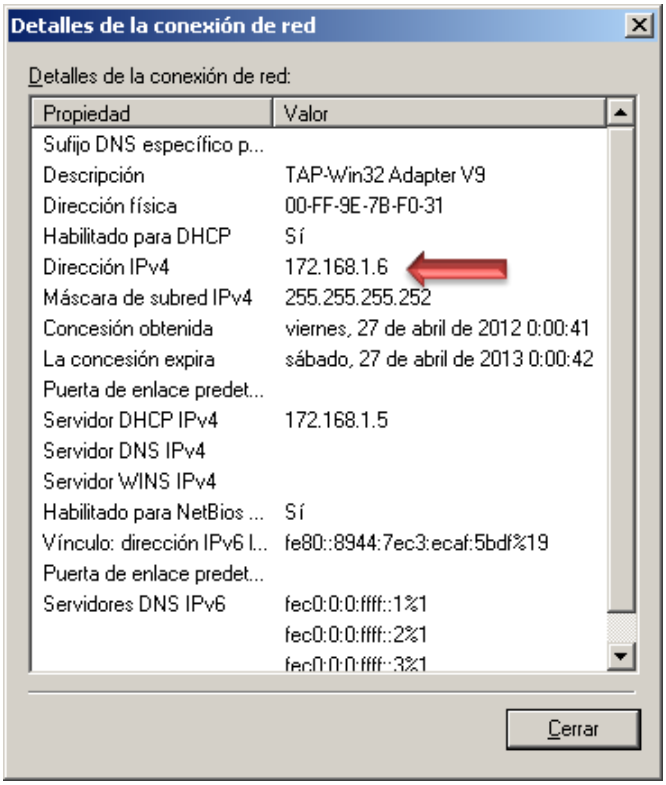
El sistema genera la conexión segura:



Y una vez establecida, podremos ver en nuestro adaptador de red de OpenVPN que ya se encuentra conectado:



Si entramos a las propiedades de la placa corroboraremos que se nos ha asignado una IP del rango que habíamos definido para nuestra VPN:



Finalmente ya estamos conectados a nuestra red interna desde cualquier parte del mundo con internet y podremos hacer uso de todos los servicios de lo que nuestra LAN disponga.

Saludos.