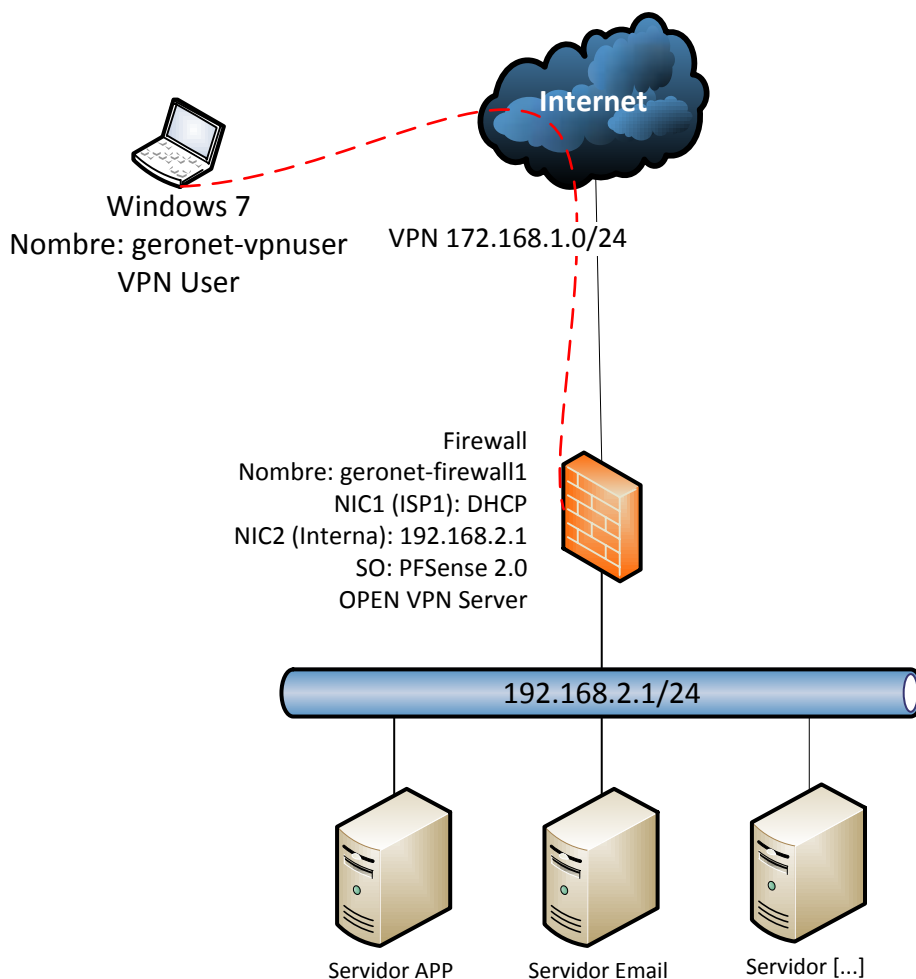


## Configuración de PFSense 2.0 con OpenVPN Road Warrior.

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.

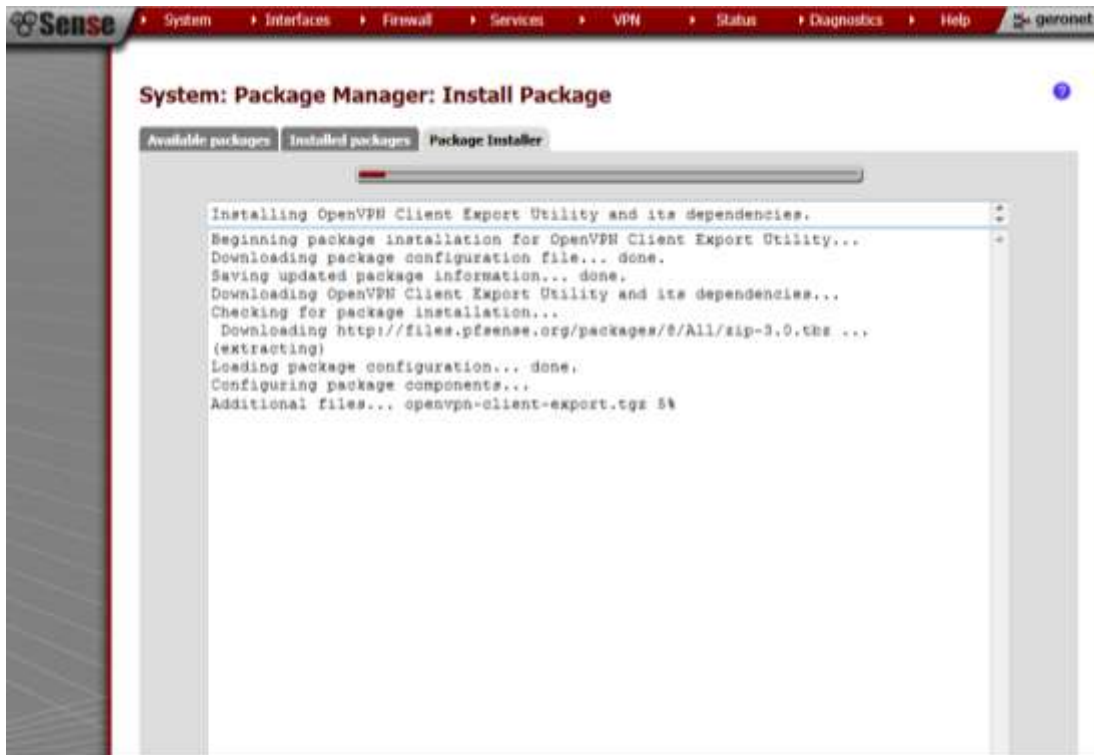
Para comenzar, una vez instalado nuestro PFSense, debemos descargar el paquete Open VPN

Entonces vamos a **System→Packages**



| pSense                         |                    |     |                                                                |                          | System                                                                                                                                                                                                                                                                                                                                                                                | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help | geronet-f |
|--------------------------------|--------------------|-----|----------------------------------------------------------------|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|----------|----------|-----|--------|-------------|------|-----------|
| OpenBGPD                       | NET                | 1.2 | STABLE<br>0.5.2<br>platform:<br>1.3                            | Package<br>Info          | OpenBGPD is a FREE implementation of the Border Gateway Protocol, Version 4. It allows ordinary machines to be used as routers exchanging routes with other systems speaking the BGP protocol.                                                                                                                                                                                        |            |          |          |     |        |             |      |           |
| OpenOSPFD                      | Routing            |     | BETA<br>0.5.2<br>platform:<br>1.2.1                            | No info, check the forum | OSPF routing protocol                                                                                                                                                                                                                                                                                                                                                                 |            |          |          |     |        |             |      |           |
| Open-VPN-Tools                 | Services           |     | Stable<br>8.7.0-3046<br>(build-<br>313025)<br>platform:<br>2.0 | Package<br>Info          | VMware Tools                                                                                                                                                                                                                                                                                                                                                                          |            |          |          |     |        |             |      |           |
| Open-VPN-Tools-8.8.1           | Services           |     | RC<br>528969<br>platform:<br>2.0                               | Package<br>Info          | VMware Tools                                                                                                                                                                                                                                                                                                                                                                          |            |          |          |     |        |             |      |           |
| OpenVPN Client Export Utility  | Security           |     | BETA<br>0.9.9<br>platform:<br>2.0                              | No info, check the forum | Allows a pre-configured OpenVPN Windows Client or Mac OSX's Viscosity configuration bundle to be exported directly from pSense.                                                                                                                                                                                                                                                       |            |          |          |     |        |             |      |           |
| OpenVPN tap Bridging Fix       | System             |     | BETA<br>0.3<br>platform:<br>2.0<br>2.1                         | No info, check the forum | Patch to fix OpenVPN tap bridging on 2.0.x. WARNING! Cannot be uninstalled.                                                                                                                                                                                                                                                                                                           |            |          |          |     |        |             |      |           |
| pBlocker                       | Firewall           |     | Release<br>1.0.2<br>platform:<br>2.0                           | Package<br>Info          | Introduce Enhanced Aliasable Feature to pfsense. Assign many IP url lists from sites like I-blocklist to a single alias and then choose rule action to take. This package also block countries and IP ranges. pBlocker replaces Countryblock and IPblocklist.                                                                                                                         |            |          |          |     |        |             |      |           |
| Proxy Server with mod_security | Network Management |     | ALPHA<br>0.1.2<br>platform:<br>1.2.3                           | Package<br>Info          | ModSecurity is a web application firewall that can work either embedded or as a reverse proxy. It provides protection from a range of attacks against web applications and allows for HTTP traffic monitoring, logging and real-time analysis. In addition this package allows URL forwarding which can be convenient for hosting multiple websites behind pSense using 1 IP address. |            |          |          |     |        |             |      |           |

Gerónimo Manso

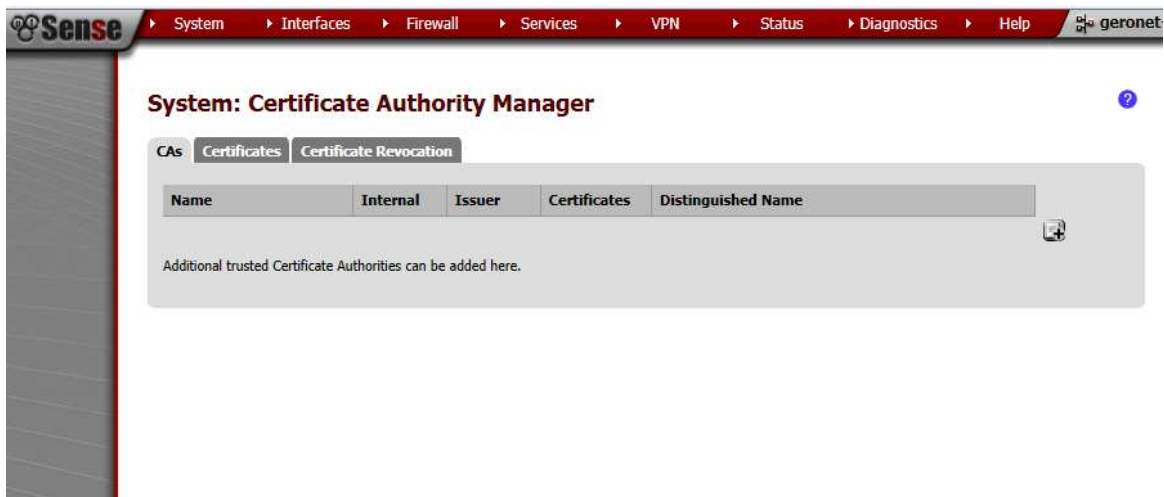


Ahora crearemos en nuestro servidor la Autoridad certificadora.

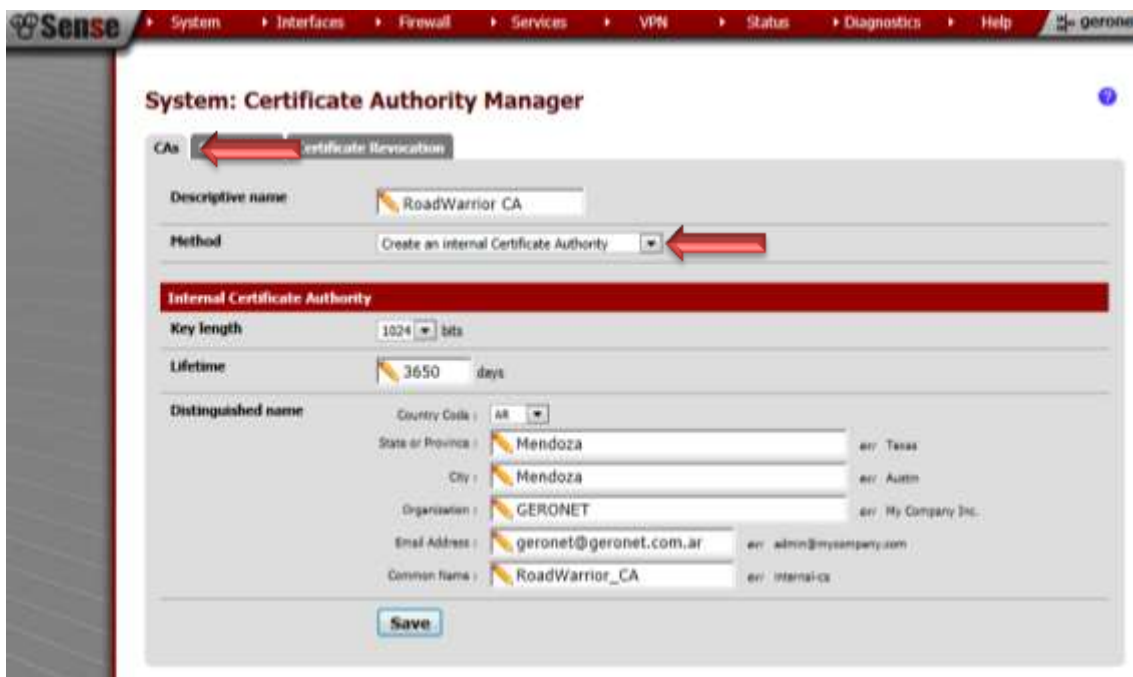
**System → Cert Manager**



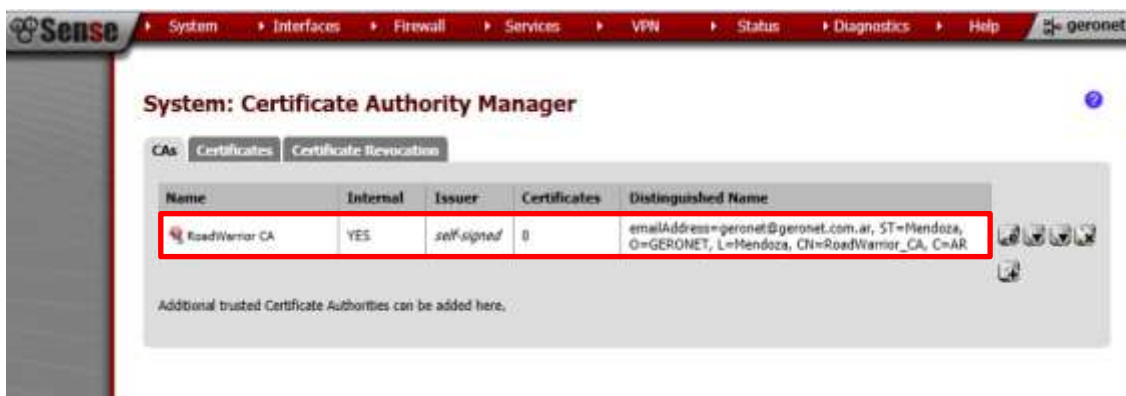
Pulsando el botón (+) agregaremos una nueva autoridad:



Completamos los campos 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:

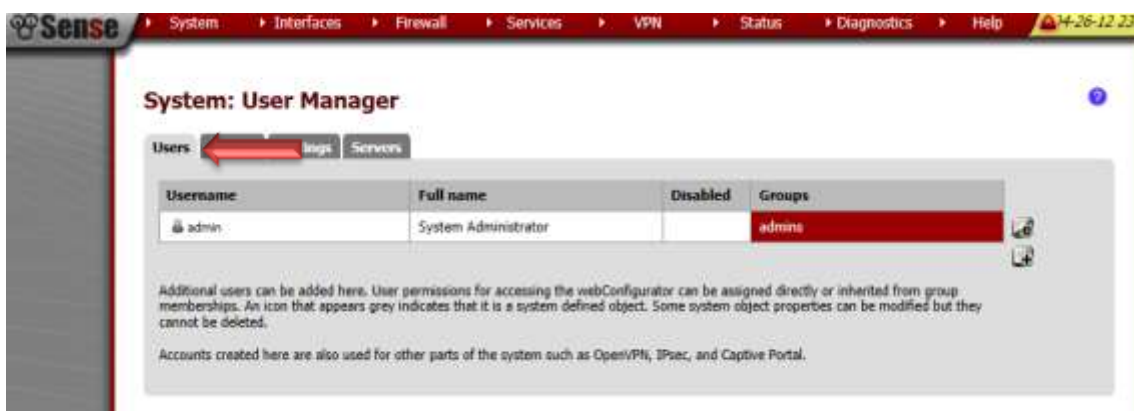


Ahora crearemos un usuario al cual le generaremos un certificado para poder conectarse a la VPN.

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



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

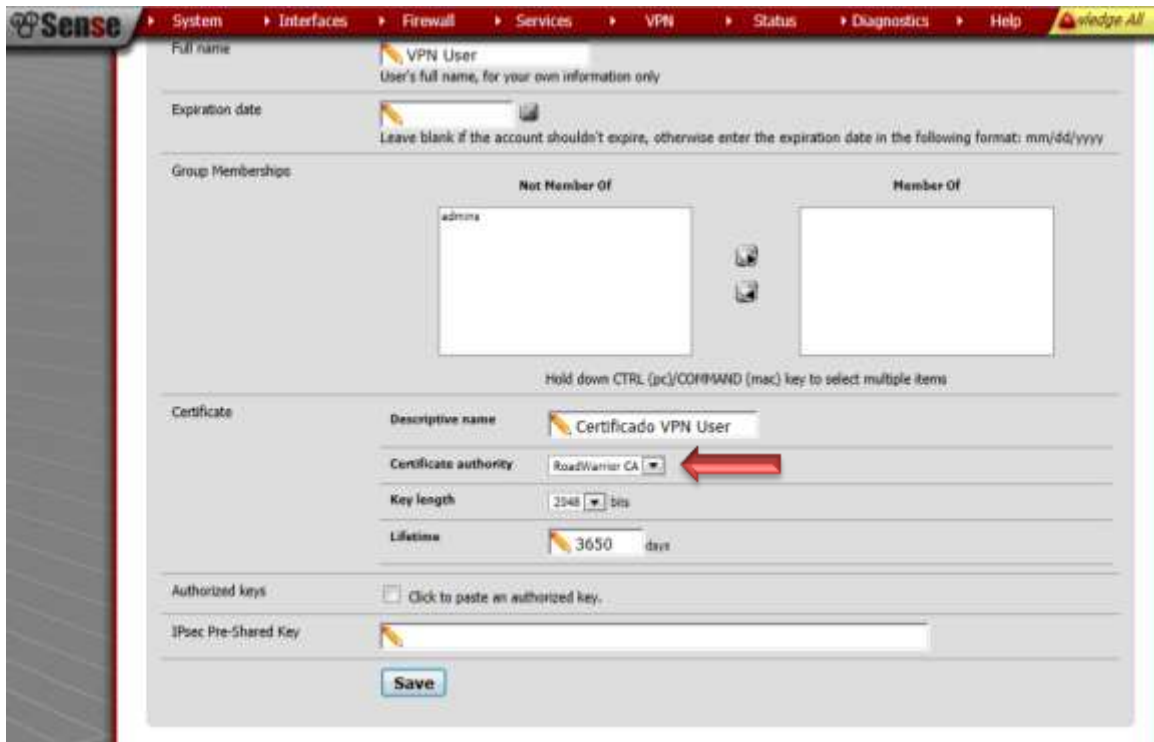


En nuestro caso crearemos el usuario “vpnuser” y le asignaremos un password.

The screenshot shows the 'System: User Manager' interface in the Sense web management tool. The 'Users' tab is selected. The 'Defined by' dropdown is set to 'USER'. The 'Disabled' checkbox is unchecked. The 'Username' field contains 'vpnuser' and is highlighted with a red arrow. The 'Password' field contains masked characters (dots) and is also highlighted with a red arrow. The 'Full name' field contains 'VPN User' with a subtext 'User's full name, for your own information only'. The 'Expiration date' field is empty with a subtext 'Leave blank if the account shouldn't expire, otherwise enter the expiration date in the following format: mm/dd/yyyy'. Below this, there are two empty boxes for 'Group Memberships' labeled 'Not Member Of' and 'Member Of'. At the bottom, the 'Certificate' section has a checkbox labeled 'Click to create a user certificate', which is also highlighted with a red arrow.

Debemos tildar la opción “**Click to create 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:

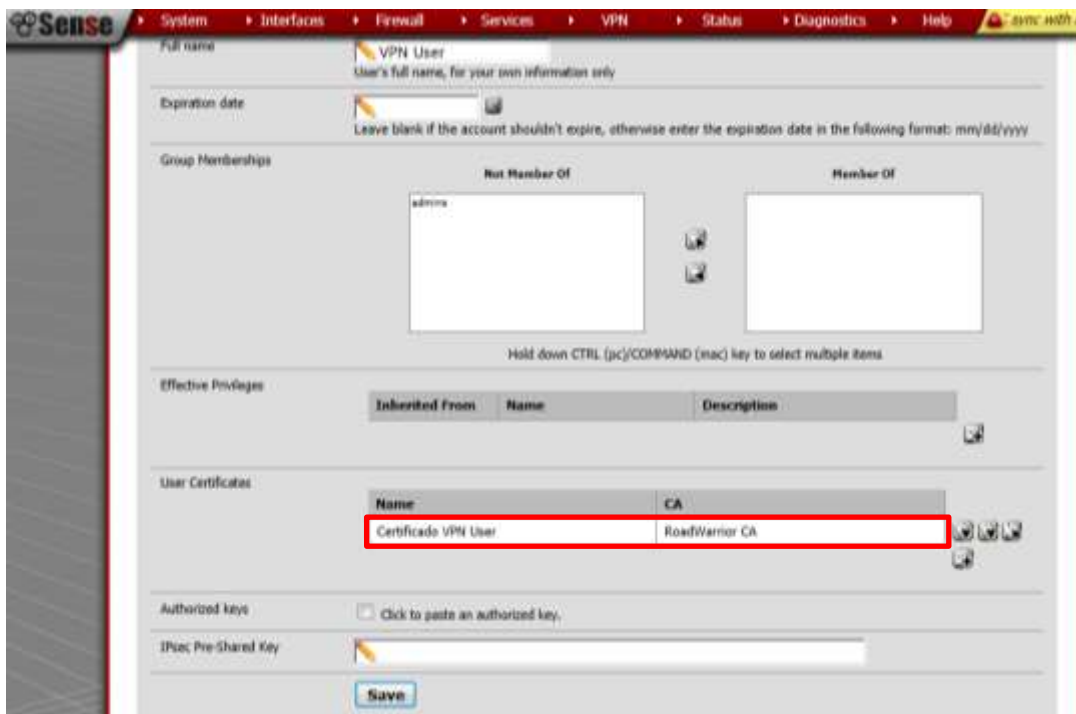


The screenshot shows the 'VPN User' configuration page in the Sense interface. The 'Certificate' section is expanded, showing the following fields:

- Descriptive name: Certificado VPN User
- Certificate authority: RoadWarrior CA (indicated by a red arrow)
- Key length: 2548 bits
- Lifetime: 3650 days

Below the certificate fields, there are sections for 'Authorized keys' and 'IPsec Pre-Shared Key'. A 'Save' button is located at the bottom of the form.

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



The screenshot shows the 'VPN User' configuration page in the Sense interface, specifically the 'User Certificates' section. The 'Certificado VPN User' certificate is listed with 'RoadWarrior CA' as the authority, highlighted by a red box.

| Name                 | CA             |
|----------------------|----------------|
| Certificado VPN User | RoadWarrior CA |

Below the certificate list, there are sections for 'Effective Privileges', 'Authorized keys', and 'IPsec Pre-Shared Key'. A 'Save' button is located at the bottom of the form.

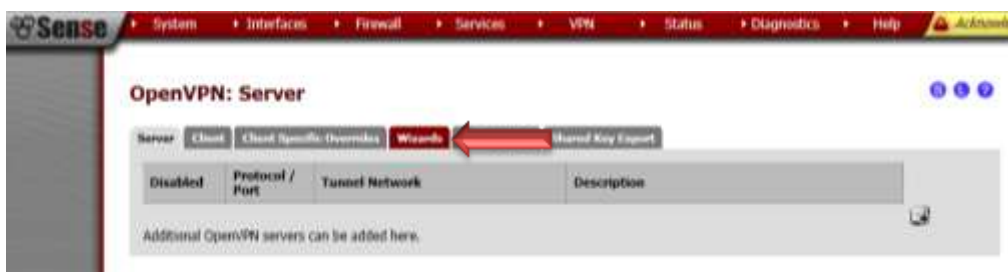


Nuestro próximo paso será crear el servidor.

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



Utilizaremos un Wizard llenando a la pestaña del mismo nombre y pulsando 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”**

**OpenVPN Remote Access Server Setup Wizard**

---

**Create a New Server Certificate**

|                           |                                                                                                                                                     |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Descriptive name:</b>  | ServerCertificate<br>A name for your reference, to identify this certificate. This is also known as the certificate's "Common Name."                |
| <b>Key length:</b>        | 2048 bits<br>Size of the key which will be generated. The larger the key, the more security it offers, but larger keys are generally slower to use. |
| <b>Lifetime:</b>          | 3650<br>Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)                                                                    |
| <b>Country Code:</b>      | AR<br>Two-letter ISO country code (e.g. US, AU, CA)                                                                                                 |
| <b>State or Province:</b> | Mendoza<br>Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).                                                          |
| <b>City:</b>              | Mendoza<br>City or other Locality name (e.g. Louisville, Indianapolis, Toronto).                                                                    |
| <b>Organization:</b>      | GERONET<br>Organization name, often the Company or Group name.                                                                                      |
| <b>E-mail:</b>            | geroent@geronet.com.ar<br>E-mail address for the Certificate contact. Often the e-mail of the person generating the certificate (i.e. You.)         |

[Create new Certificate](#)

Luego configuraremos los siguientes campos:

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

**Protocol:** Seleccionaremos UDP 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 Authentication** y **Generate TLS Key**.

**Sense**

OpenVPN Remote Access Server Setup Wizard

**General OpenVPN Server Information**

|              |                 |
|--------------|-----------------|
| Interface:   | WAN1            |
| Protocol:    | UDP             |
| Local Port:  | 1194            |
| Description: | VPN_RoadWarrior |

**Cryptographic Settings**

|                     |                                                                                             |
|---------------------|---------------------------------------------------------------------------------------------|
| TLS Authentication: | <input checked="" type="checkbox"/> Enable authentication of TLS packets.                   |
| Generate TLS Key:   | <input checked="" type="checkbox"/> Automatically generate a shared TLS authentication key. |
| TLS Shared Key:     |                                                                                             |

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

**Cryptographic Settings**

|                       |                                                                                             |
|-----------------------|---------------------------------------------------------------------------------------------|
| TLS Authentication:   | <input checked="" type="checkbox"/> Enable authentication of TLS packets.                   |
| Generate TLS Key:     | <input checked="" type="checkbox"/> Automatically generate a shared TLS authentication key. |
| TLS Shared Key:       |                                                                                             |
| DH Parameters Length: | 1024 bit                                                                                    |
| Encryption Algorithm: | AES-128-CBC (128-bit)                                                                       |
| Hardware Crypto:      | No Hardware Crypto Acceleration                                                             |

**Tunnel Settings**

|                 |  |
|-----------------|--|
| Tunnel Network: |  |
|-----------------|--|

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

|                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hardware Crypto:</b> <span>No Hardware Crypto Acceleration ▼</span><br>The hardware cryptographic accelerator to use for this VPN connection, if any. |                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Tunnel Settings</b>                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Tunnel Network:</b>                                                                                                                                   | This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients. (see Address Pool)<br><input type="text" value="172.168.1.0/24"/> |
| <b>Redirect Gateway:</b>                                                                                                                                 | <input type="checkbox"/> Force all client generated traffic through the tunnel.                                                                                                                                                                                                                                                                                                   |
| <b>Local Network:</b>                                                                                                                                    | This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. You may leave this blank if you don't want to add a route to the local network through this tunnel on the remote machine. This is generally set to your LAN network.<br><input type="text" value="192.168.2.0/24"/>                                                              |
| <b>Concurrent Connections:</b>                                                                                                                           | Specify the maximum number of clients allowed to concurrently connect to this server.<br><input type="text" value="20"/>                                                                                                                                                                                                                                                          |
| <b>Compression:</b>                                                                                                                                      | <input checked="" type="checkbox"/> Compress tunnel packets using the LZO algorithm.                                                                                                                                                                                                                                                                                              |
| <b>Type-of-Service:</b>                                                                                                                                  | <input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet value.                                                                                                                                                                                                                                                                    |
| <b>Inter-Client Communication:</b>                                                                                                                       | <input checked="" type="checkbox"/> Allow communication between clients connected to this server.                                                                                                                                                                                                                                                                                 |
| <b>Duplicate Connections:</b>                                                                                                                            | <input type="checkbox"/> Allow multiple concurrent connections from clients using the same Common Name.<br>NOTE: This is not generally recommended, but may be needed for some scenarios.                                                                                                                                                                                         |
| <b>Client Settings</b>                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Dynamic IP:</b>                                                                                                                                       | <input checked="" type="checkbox"/> Allow connected clients to retain their connections if their IP address changes.                                                                                                                                                                                                                                                              |
| <b>Address Pool:</b>                                                                                                                                     | <input checked="" type="checkbox"/> Provide a virtual adapter IP address to clients (see Tunnel Network).                                                                                                                                                                                                                                                                         |
| <b>DNS Default Domain:</b>                                                                                                                               | <input type="text"/><br>Provide a default domain name to clients.                                                                                                                                                                                                                                                                                                                 |

También habilitamos la compresión del tunel.

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

| Client Settings     |                                                                                                                                                                                                                               |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dynamic IP:         | <input checked="" type="checkbox"/> Allow connected clients to retain their connections if their IP address changes.                                                                                                          |
| Address Pool:       | <input checked="" type="checkbox"/> Provide a virtual adapter IP address to clients (see Tunnel Network).                                                                                                                     |
| DNS Default Domain: | <input type="text"/><br>Provide a default domain name to clients.                                                                                                                                                             |
| DNS Server 1:       | <input type="text"/><br>DNS server to provide for connecting client systems.                                                                                                                                                  |
| DNS Server 2:       | <input type="text"/><br>DNS server to provide for connecting client systems.                                                                                                                                                  |
| DNS Server 3:       | <input type="text"/><br>DNS server to provide for connecting client systems.                                                                                                                                                  |
| DNS Server 4:       | <input type="text"/><br>DNS server to provide for connecting client systems.                                                                                                                                                  |
| NTP Server:         | <input type="text"/><br>Network Time Protocol server to provide for connecting client systems.                                                                                                                                |
| NTP Server 2:       | <input type="text"/><br>Network Time Protocol server to provide for connecting client systems.                                                                                                                                |
| NetBIOS Options:    | <input type="checkbox"/> Enable NetBIOS over TCP/IP.<br>If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.                                                                         |
| NetBIOS Node Type:  | <input type="text" value="none"/><br>Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast). |
| NetBIOS Scope ID:   | <input type="text"/><br>A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID. |

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

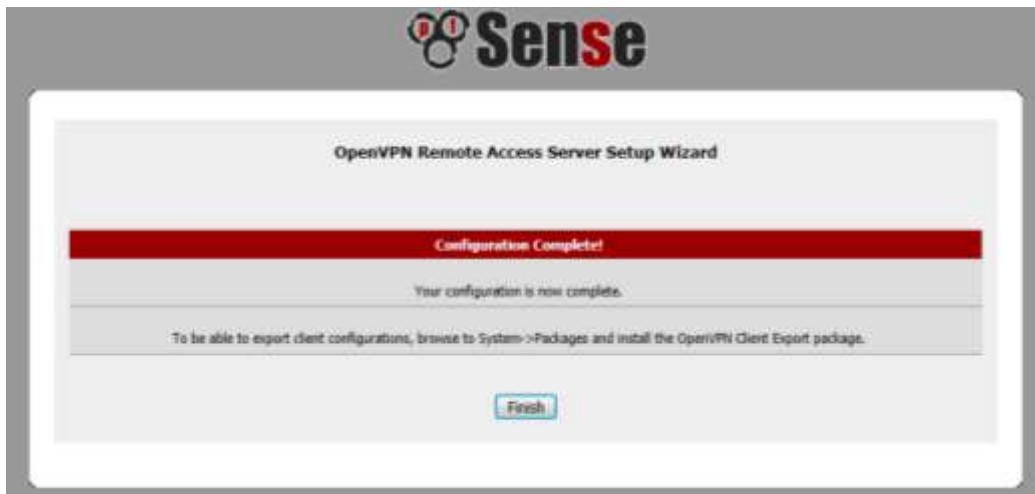
|                    |                                                                                                                                                                                                                                                        |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NTP Server:        | <input type="text"/><br>Network Time Protocol server to provide for connecting client systems.                                                                                                                                                         |
| NTP Server 2:      | <input type="text"/><br>Network Time Protocol server to provide for connecting client systems.                                                                                                                                                         |
| NetBIOS Options:   | <input type="checkbox"/> Enable NetBIOS over TCP/IP.<br>If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.                                                                                                  |
| NetBIOS Node Type: | <input type="text" value="none"/><br>Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).                          |
| NetBIOS Scope ID:  | <input type="text"/><br>A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID.                          |
| WINS Server 1:     | <input type="text"/><br>A Windows Internet Name Service (WINS) server to provide for connecting clients, which allows them to browse Windows shares. This is typically an Active Directory Domain Controller, designated WINS server, or Samba server. |
| WINS Server 2:     | <input type="text"/><br>A Windows Internet Name Service (WINS) server to provide for connecting clients, which allows them to browse Windows shares. This is typically an Active Directory Domain Controller, designated WINS server, or Samba server. |
| Advanced:          | <input type="text"/><br>Enter any additional options you would like to add to the OpenVPN server configuration here, separated by a semicolon.<br>EXAMPLE: push "route 10.0.0.0 255.255.255.0"                                                         |

[Next](#)

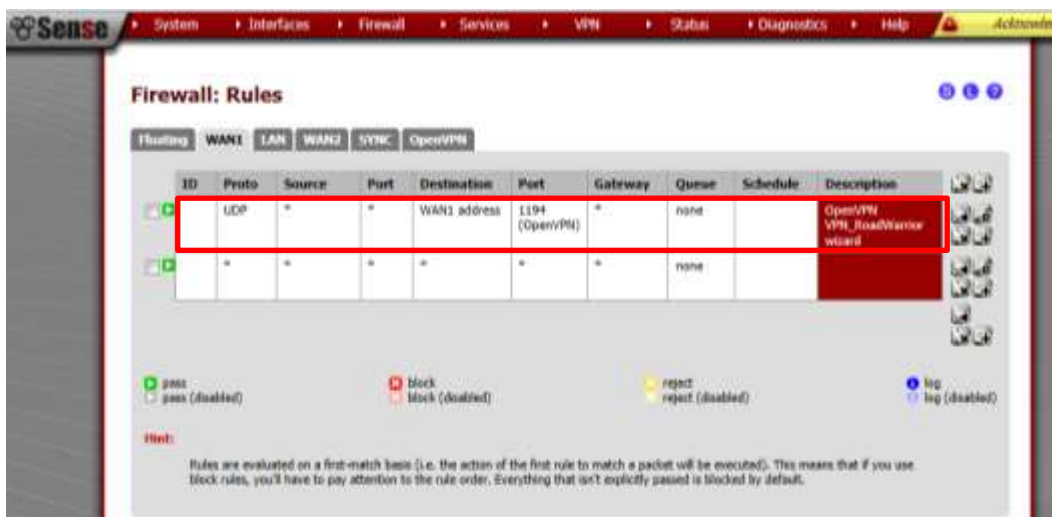
En este paso seleccionamos las opciones **Firewall Rule** y **OpenVPN rule** para que el asistente nos genere las reglas para permitir la conexión con la VPN en el firewall:



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**:



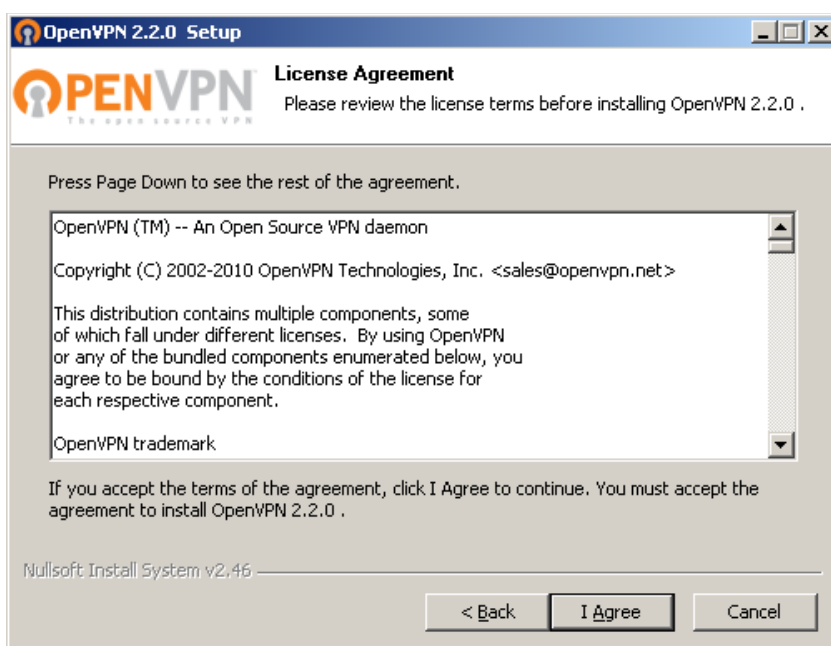
Guardamos el paquete generado para nuestro usuario y luego lo instalaremos en la PC que se conectará remotamente a nuestra red.



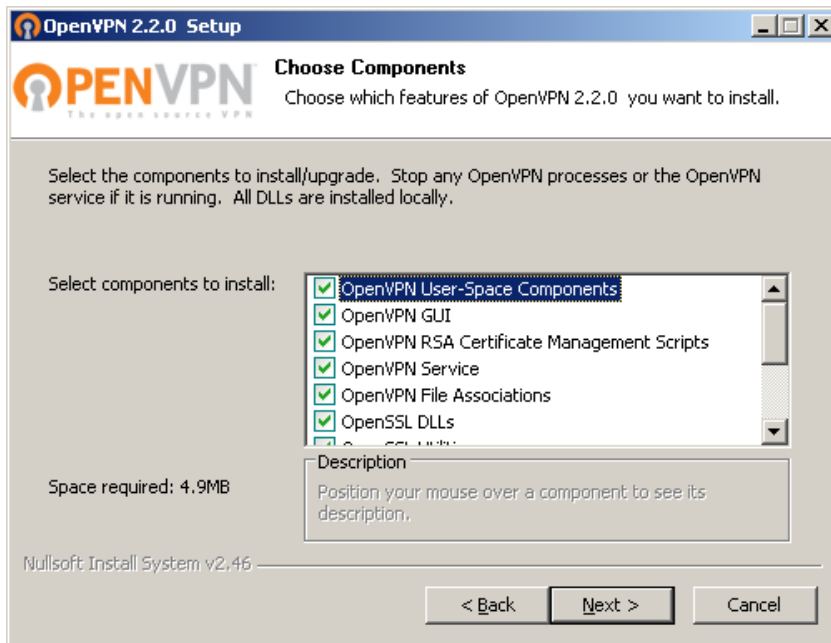
Ejecutamos el instalador:



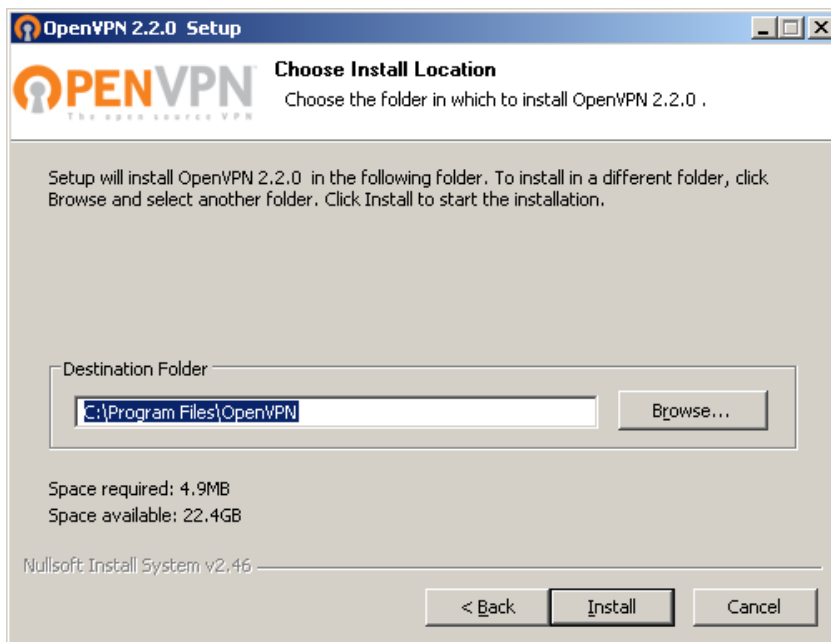
Pulsamos Next



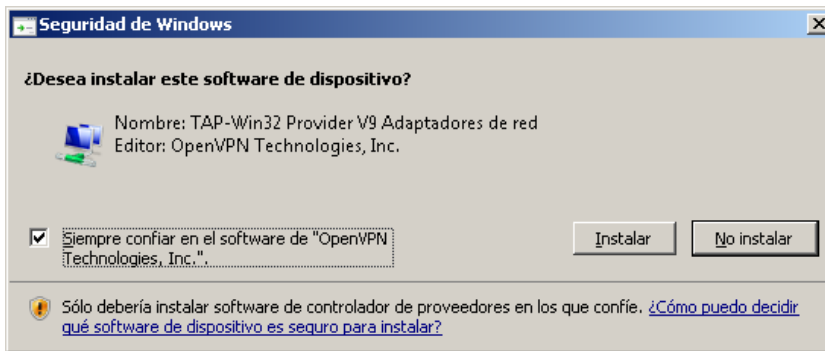
Aceptamos el acuerdo.



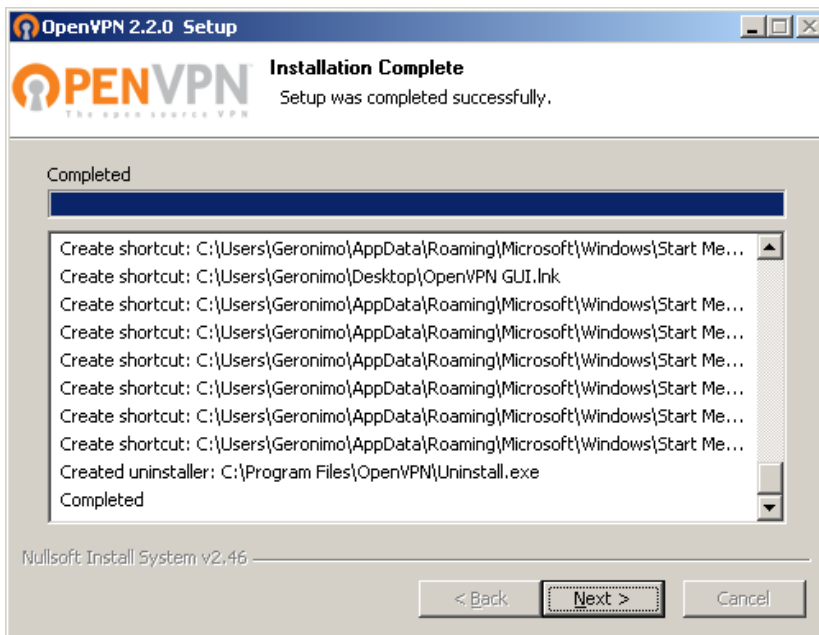
Dejamos tildada todas las opciones y **NEXT**



Pulsamos **Install**

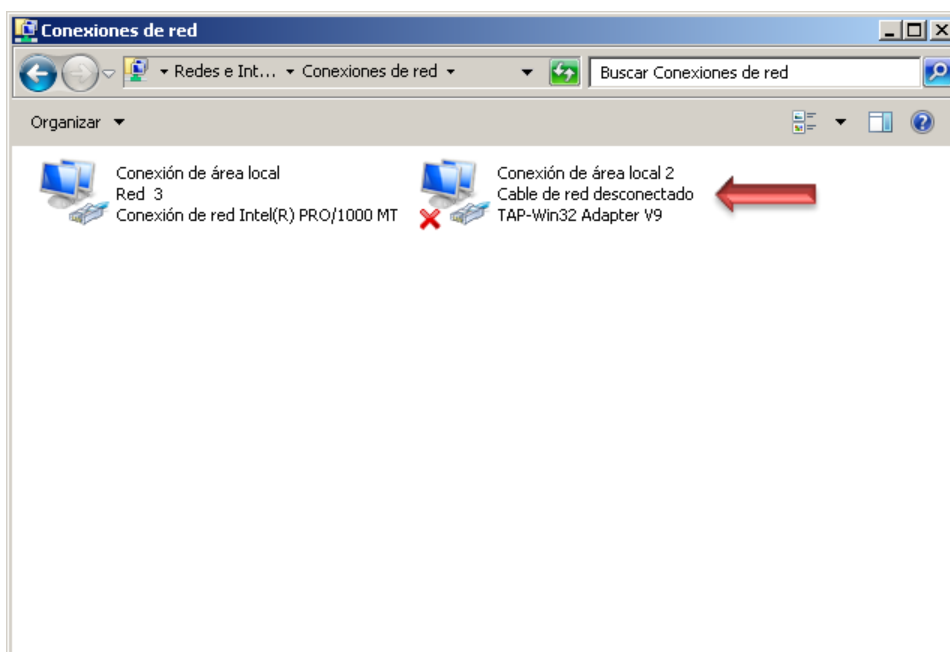


Se nos muestra el mensaje de que se quiere añadir un dispositivo, al cual **tildamos la opción Siempre confiar en el Software de OpenVPN Technologies INC** y pulsamos **Instalar**.



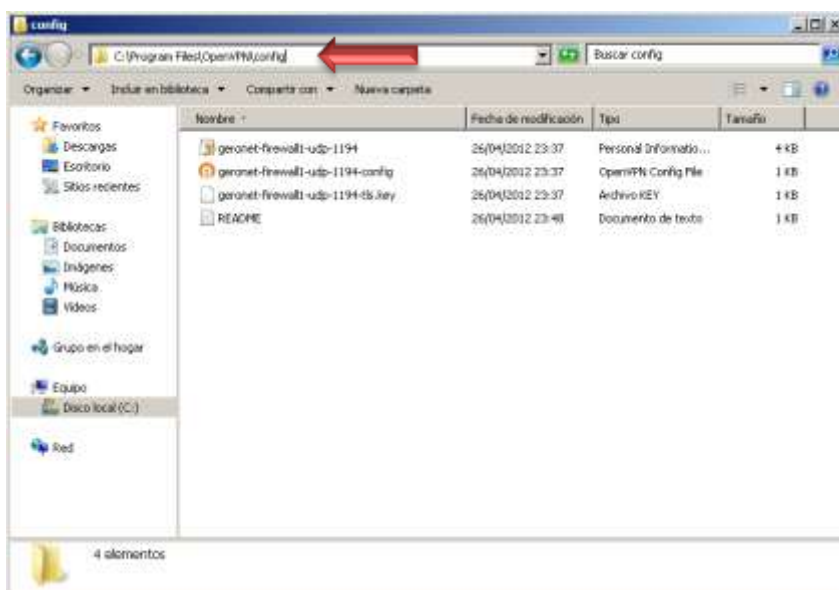
Una vez completada la opción pulsamos **Next** para finalizar.

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

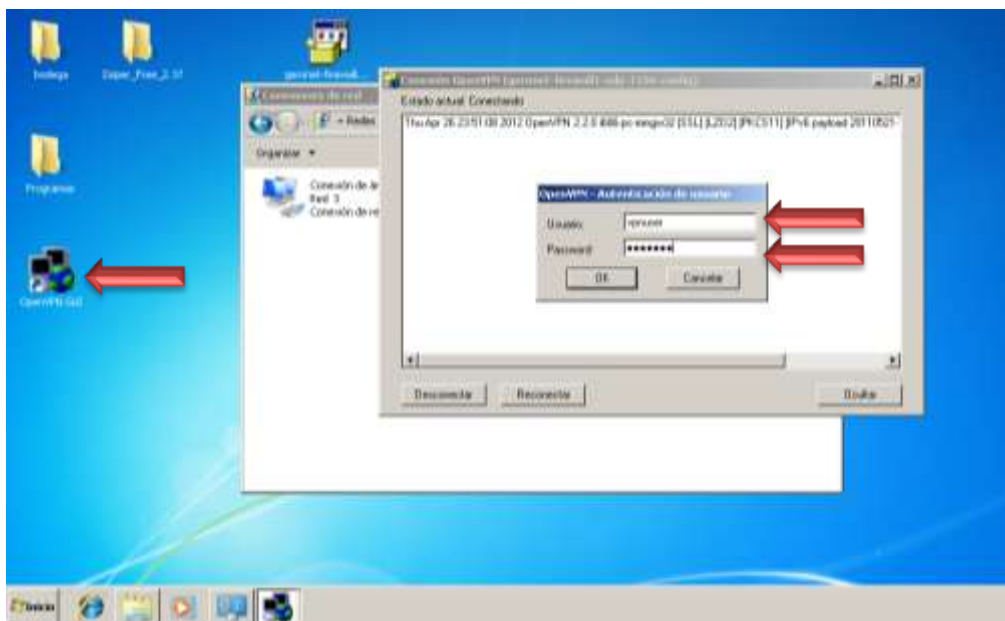


Este es quien controlará nuestra conexión.

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 debe modificar nada, es solo para comprobar que se encuentren estos archivos:

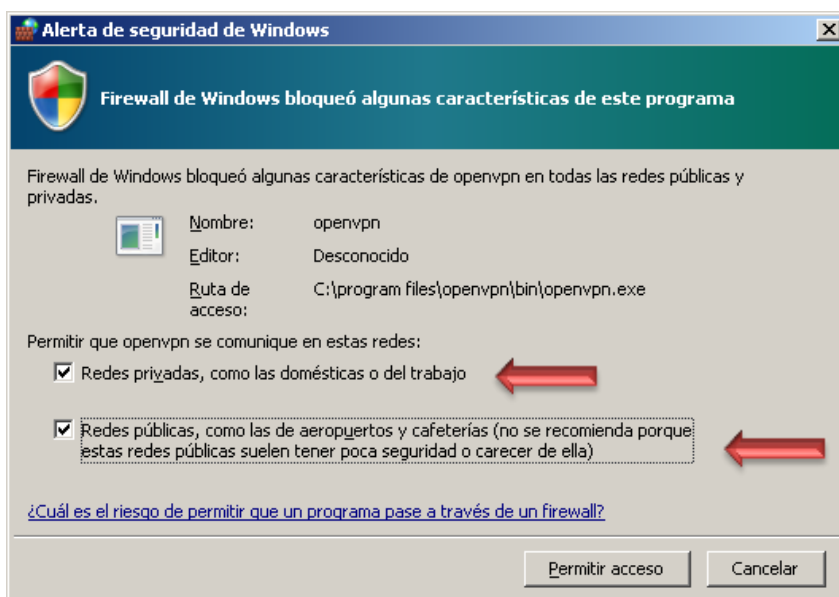


En nuestro escritorio se generó un acceso directo a la interfaz de usuario del cliente VPN, al cual accederemos e ingresaremos nuestro usuario y clave generados en nuestro firewall:

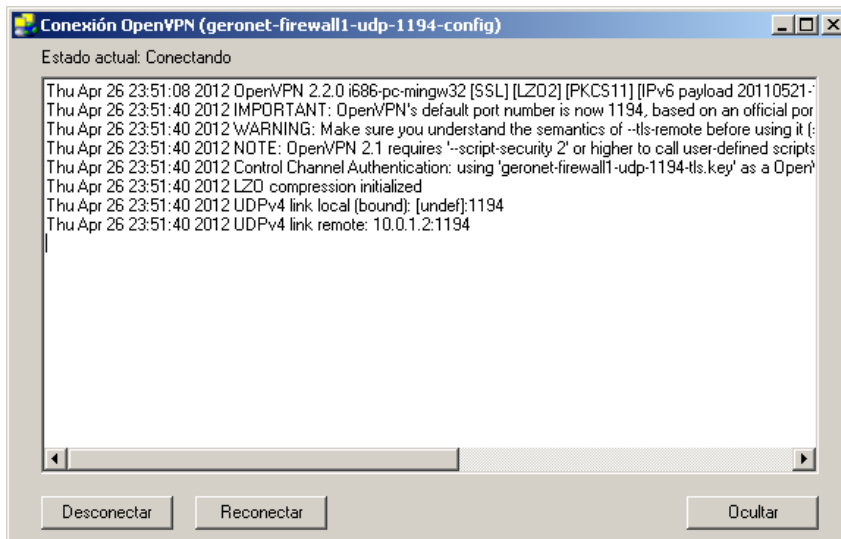


Pulsando OK, el sistema tratará de conectarse.

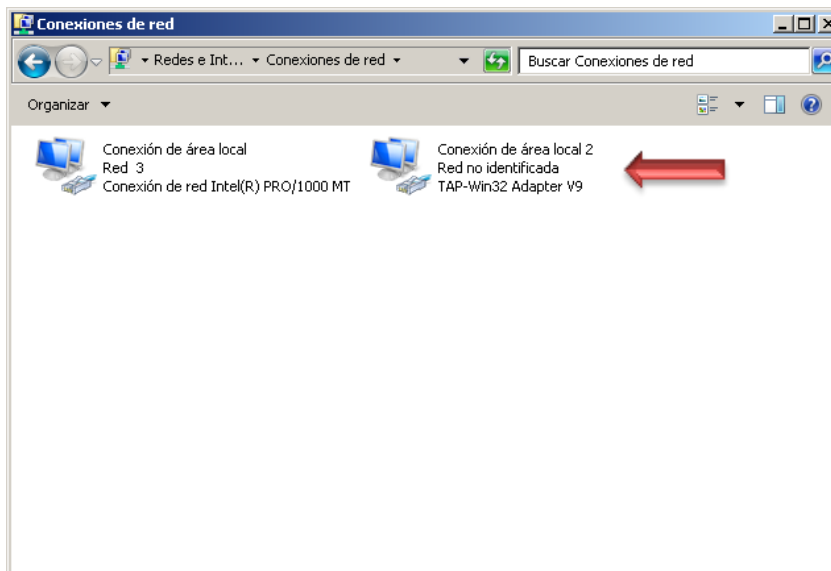
Debemos agregar estas excepciones al firewall de Windows si es que lo tenemos activado:



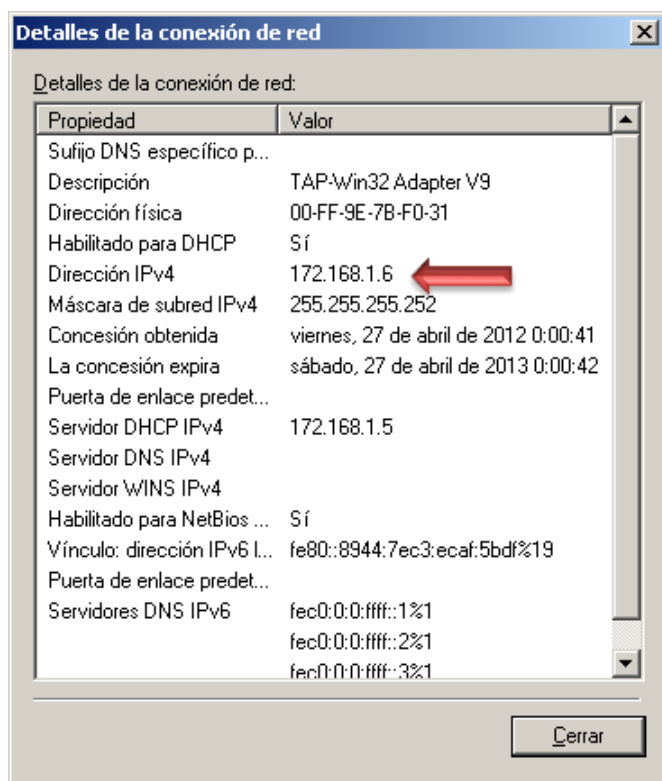
El sistema genera la conexión segura:



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.