***Que és Open VPN?**

OpenVPN és un software de codigo libre que permite hacer conexiones de red privadas virtuales, en dispositivos a través de internet.

***Diferències entre VPN d'accés remot i VPN punt a punt, per a què serveix cada una?**

La diferencia principal es que mientras que la VPN de acceso remoto necesita un servidor intermediario para poder llegar a la red privada, la VPN punto a punto hace la conexión directa con la red. Esto permite la comunicación segura directa entre los dispositivos o redes involucradas.

***Per a què utilitza OpenSSL a Open VPN?**

Es una librería de código abierto, para la seguridad e integridad de la as VPN, usa funciones criptográficas, como la generación de llaves, encriptación i firma digital.

***Per a què utilitza TLS a Open VPN?**

Para la privacidad y la integridad de los datos que se transmiten a través de Internet, se aseguran mediante la encriptación de las comunicaciones y la autenticación de los dispositivos en la comunicación.

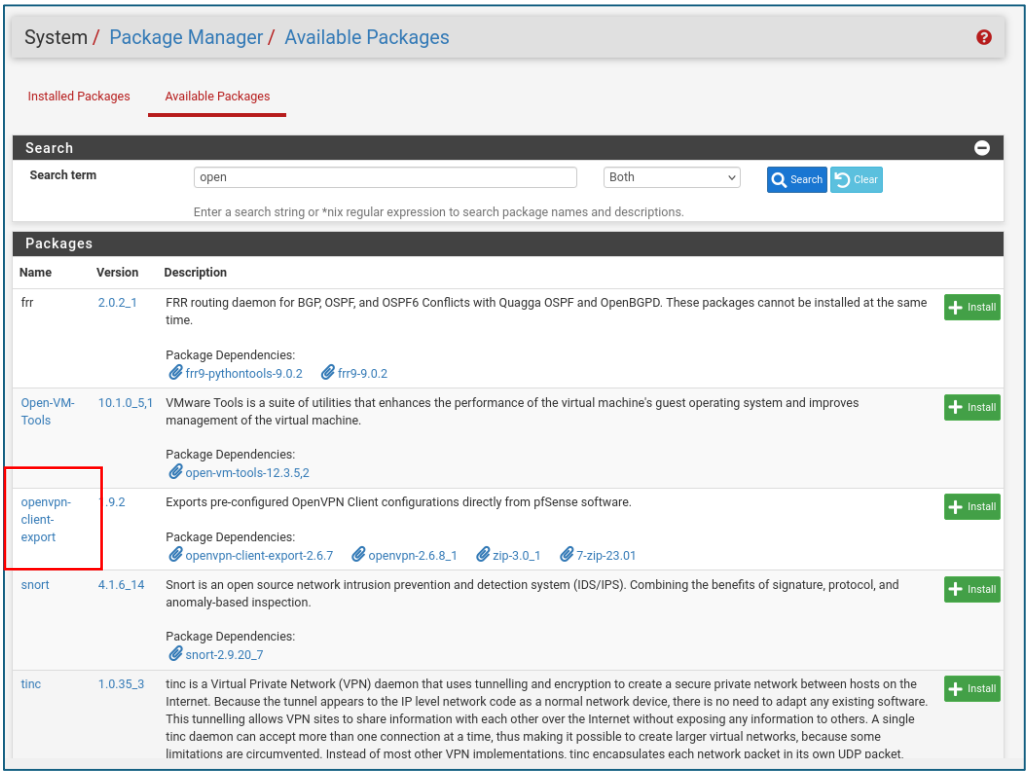
***Pera a què utilitza SSL/TLS a Open VPN?**

Para establecer un túnel seguro de un punto a otro, entre los dispositivos de la red. Es distinto al TLS, SSL protege el envío, TLS es más por el propio dato enviado.

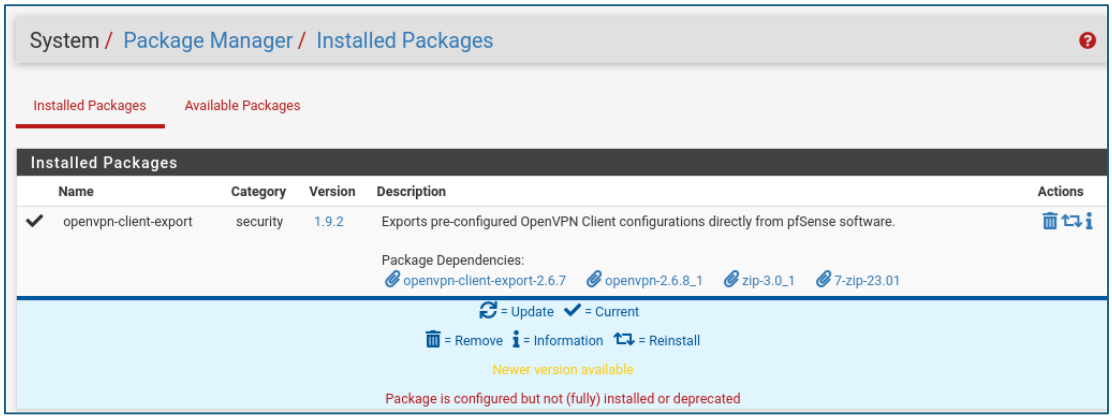
Instalación y configuración de OpenVPN en PFSense

En Pfsense, el apartado de ***System/Pakage Manager/Available Packages*** ->

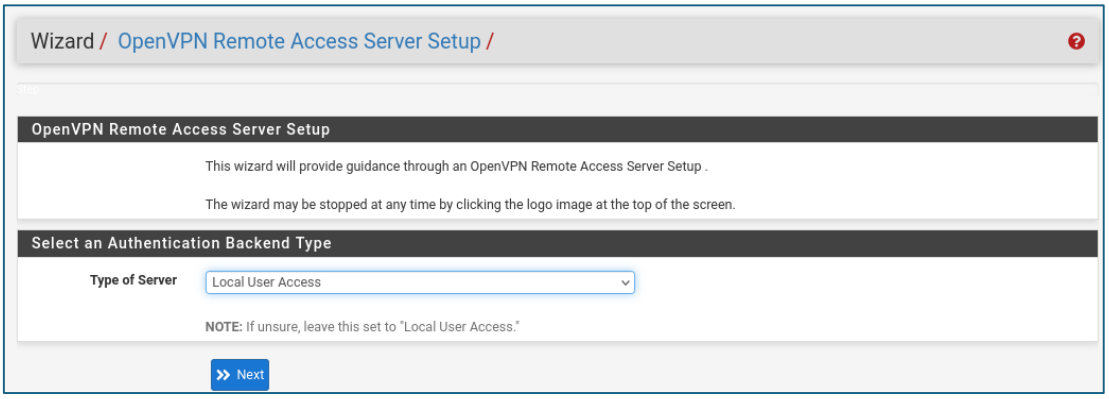
- Install openvpn-client-export



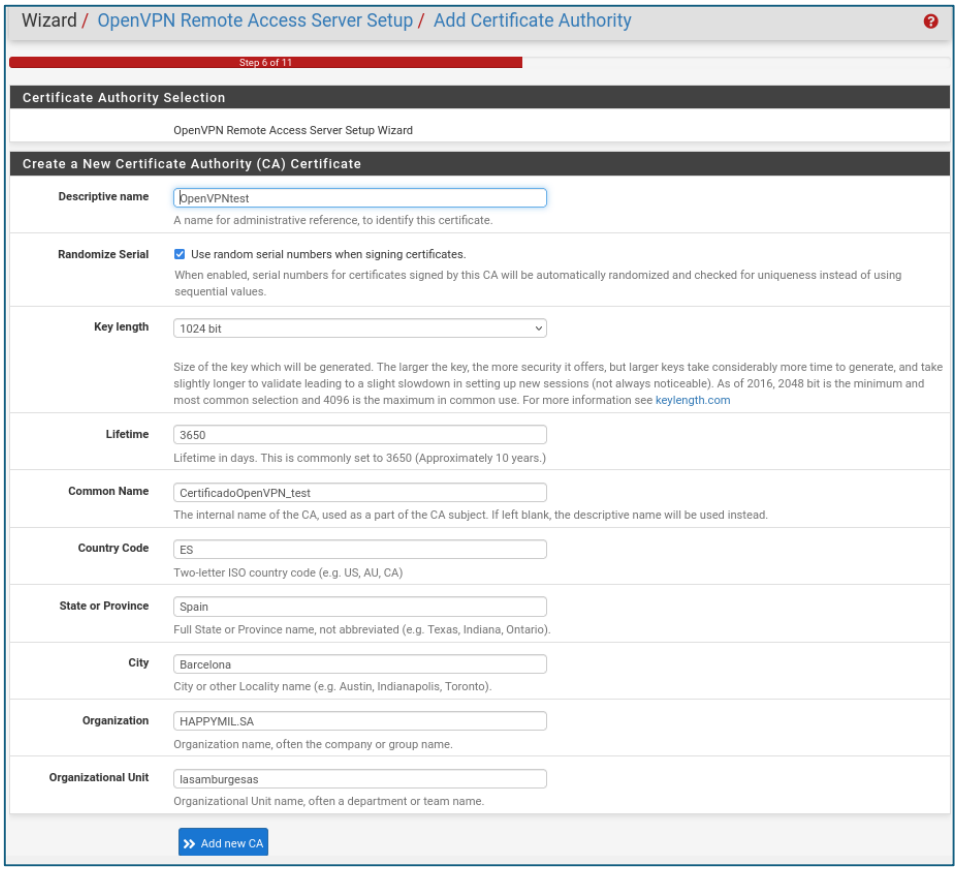
- instalado



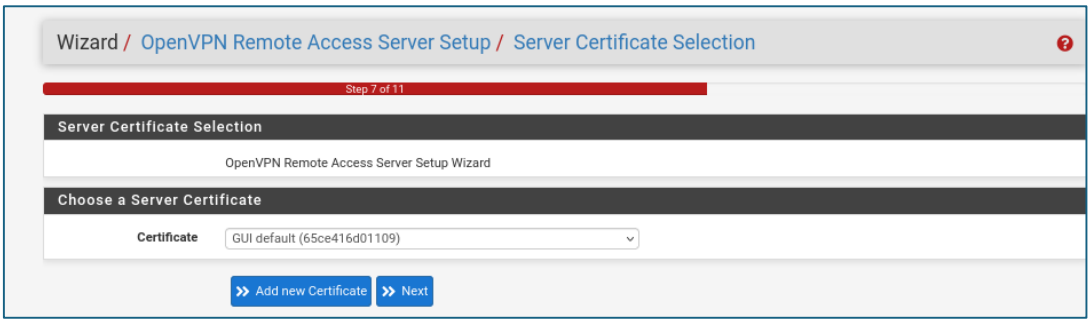
- Vamos al wizard/openVPN Remote Acces Server Setup para configurarlo
- Type of Server (lo haremos en local) -> Local User Acces -> Next



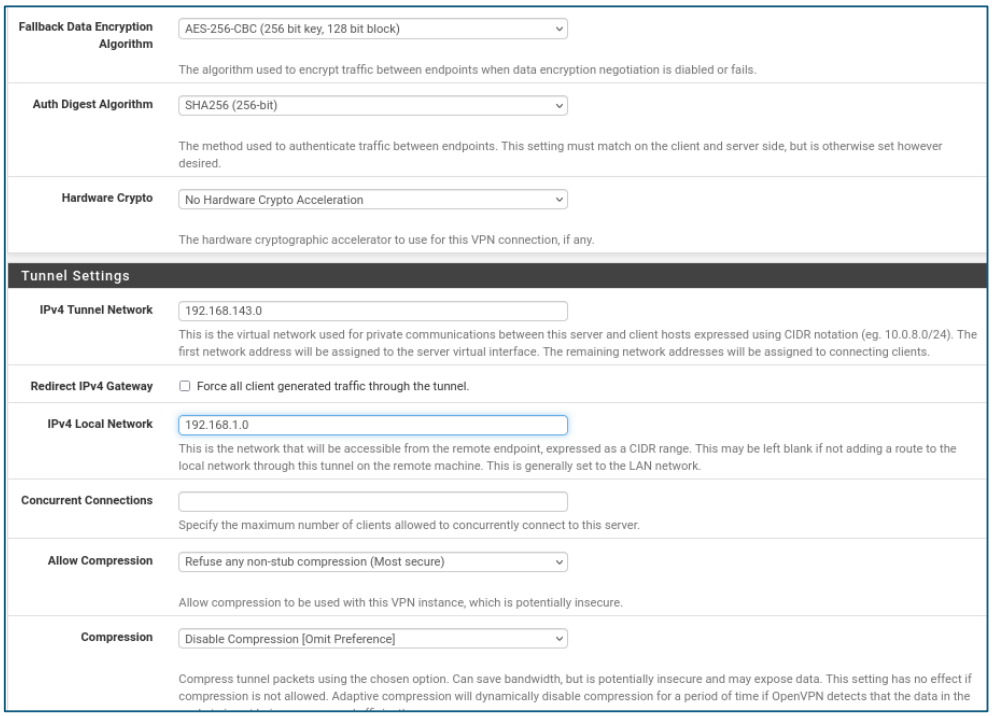
- Agregamos un certificado para La VPN
- Nombre descriptivo, Tamaño de la key, tiempo de vida de este, el nombre y datos variados opcionales de la empresa (ficticia en este caso).



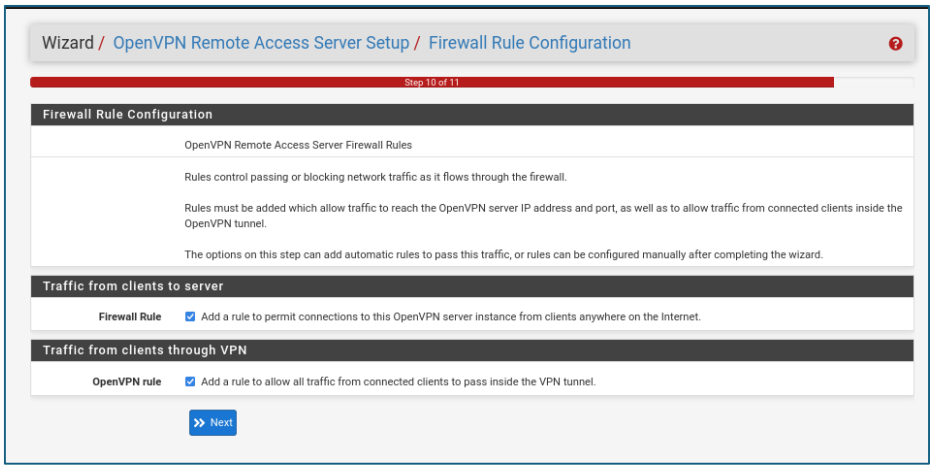
- Escogemos servidor default del certificado.



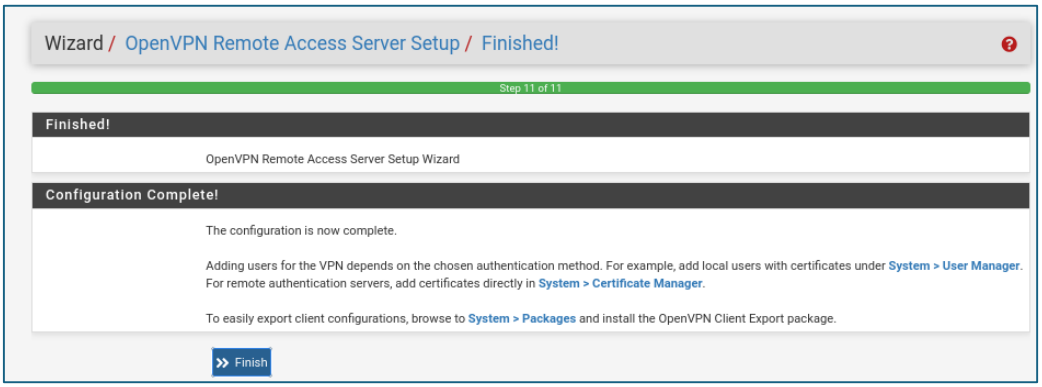
- Aquí vamos a modificar el tunnel network, y el local network,
- El *tunnel network*, por así decirlo es el que sale hacia afuera, por que es el que va a hacer el túnel, el local network es la red interna, estas ip las sacaremos de la configuración previa del PFSense (WAN, LAN) vamos a pillar el rango ->
- WAN (túnel) 192.168.143.0/24
- LAN (Local) 192.168.1.0/24
- Next ->



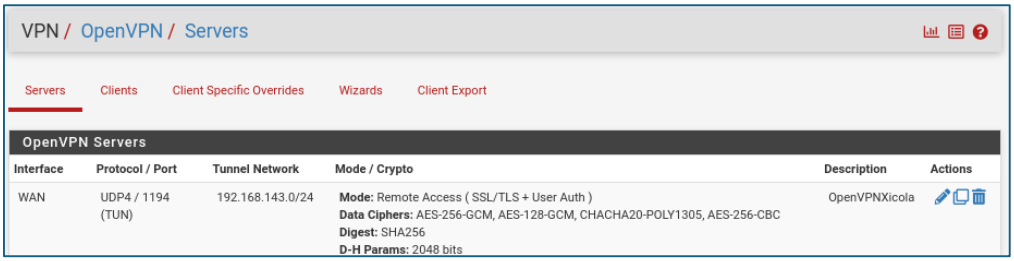
- Vamos a agregar las reglas del firewall que permita las conexiones a OpenVPN de los usuarios de internet, y vamos a agregar una regla que permita el tráfico en el túnel VPN.



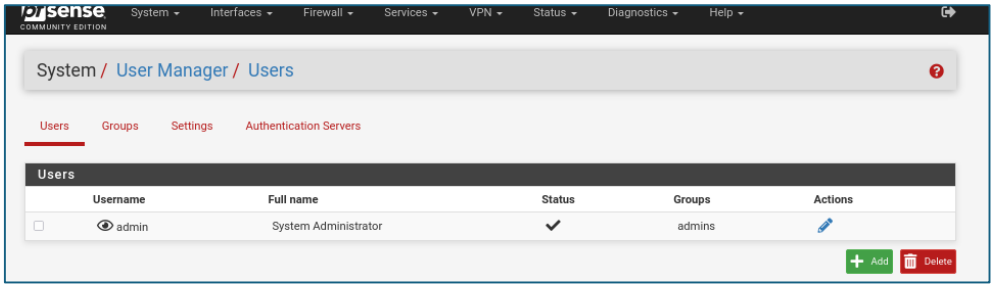
- Y ya estaría. Open >VPN configurado



- Tenemos aquí el servidor con el certificado hecho



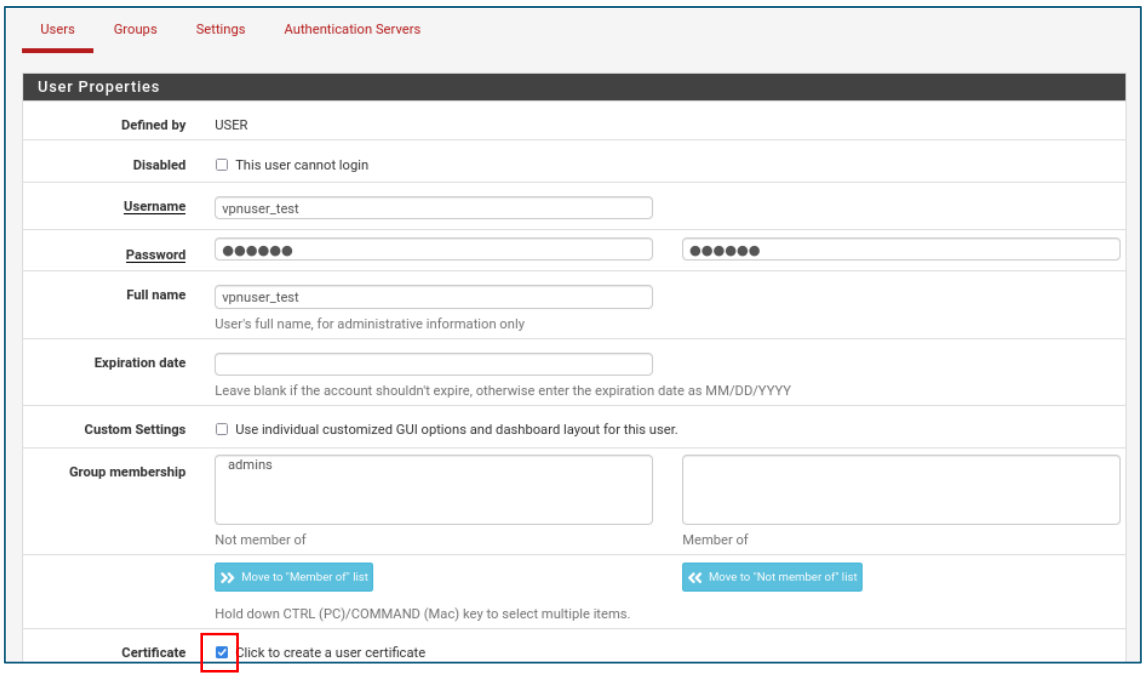
- Ahora Creo el usuario, Nos vamos a:
  System > User manager > Users



- Y agregamos usuario nuevo (add)
- Rellenamos los datos siguientes:

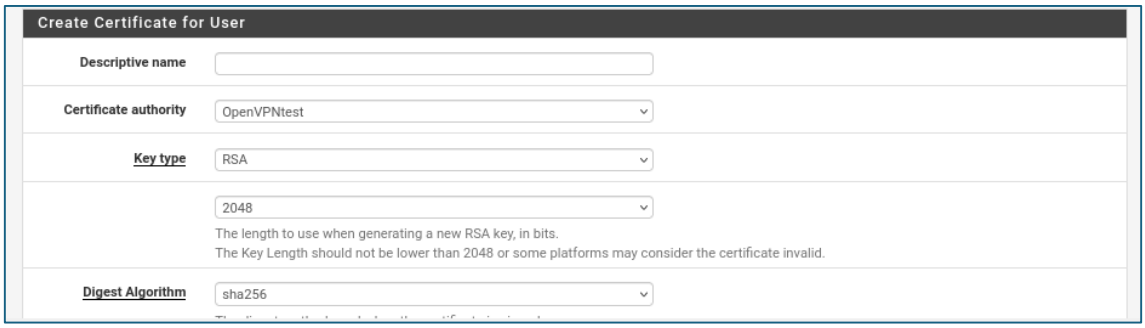
Nombre, fullname, Passwrd

- Y el certificado para el usuario (le damos ok a la checkbox)



- Completamente necesario hacer y rellenar el certificado para el usuario.

El certificado creado agragamos



Ahora Nos vamos a VPN > OpenVPN > Client Export

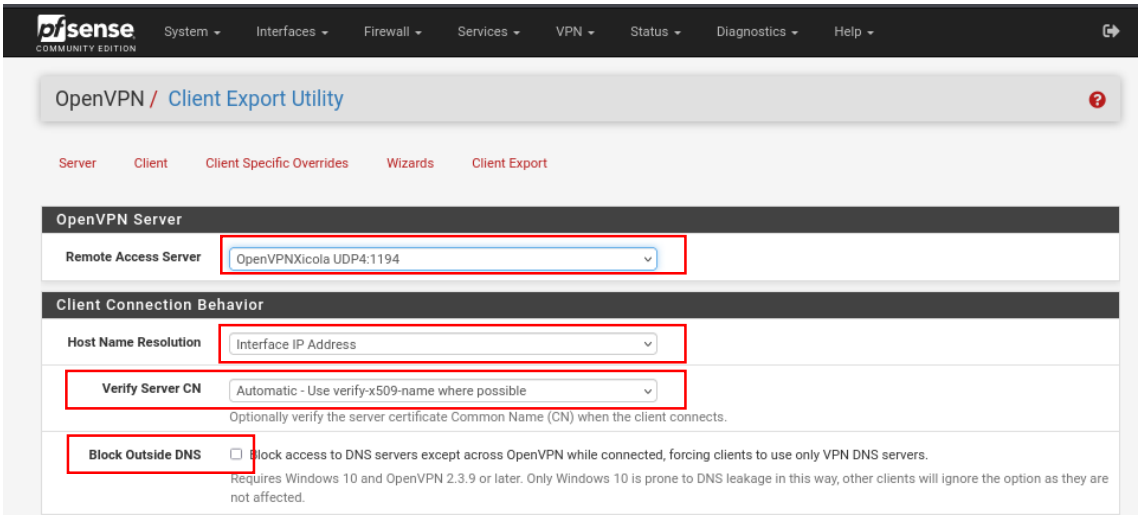
• Seleccionamos la VPN en RAS Sever

• En Host Name Resolution hemos de escoger la IP que este expuesta en mi caso la de la interficie

• Verify server CN: lo dejamos

• Block outside DNS: para prevenir las filtraciones de DNS Win10, Pero lo dejamos como esta, no usamos win10

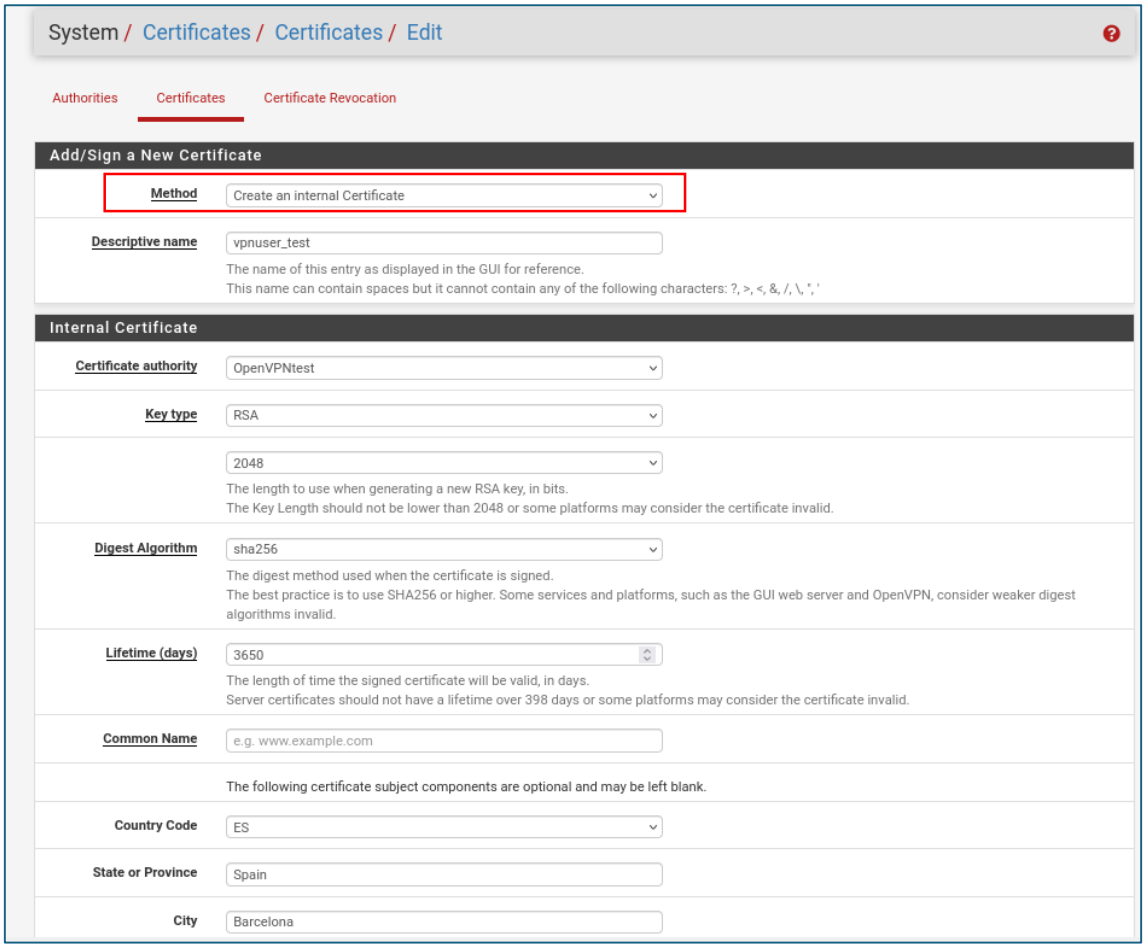
, abajo nos aparecerán los usuarios, en mi caso lo usaré con Most Clients, que nos exporta un .ovpn:



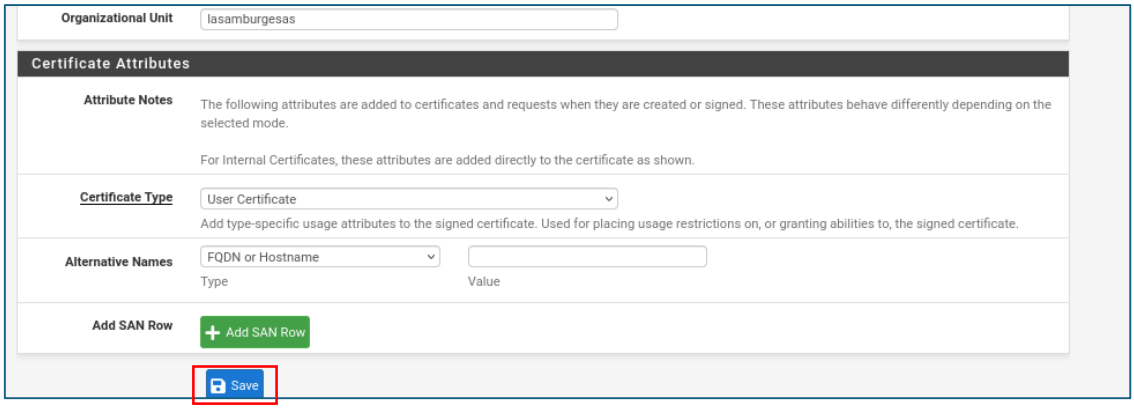
- Marcamos create Certificate y rellenamos los datos, es necesario para conectarnos:

Method -> Create an internal Certificate

Y dejamos todo por default.



- Guardamos, y ya podemos descargar



- Le damoas a Most Clients y descrgaria ja el fitxer