PFSENSE: VPN CON IPSEC Y SERVIDOR OPENVPN

SAD

2ºASIR
I.E.S. ANTONIO MACHADO
ANA OROZCO ASENSIO

Contenido

Introducción.

En esta práctica vamos a crear 2 VPNs mediante Pfsense:

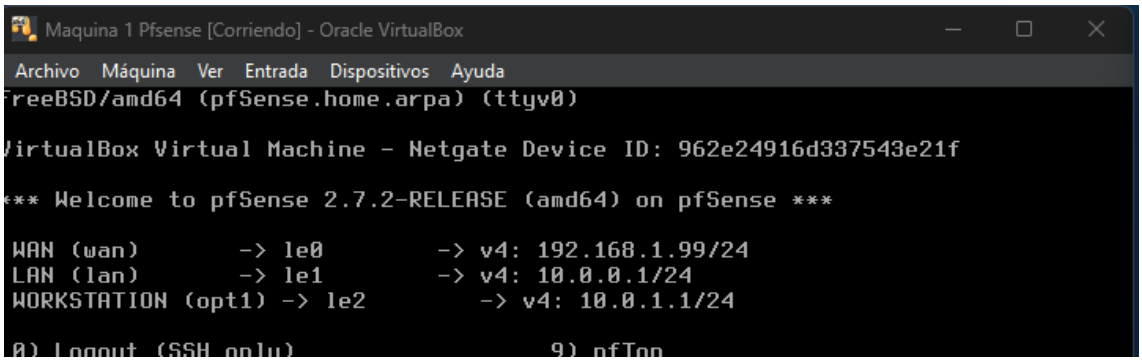
La primera en modo túnel con IPSec usando la máquina de la anterior práctica (que será la sucursal principal en Sevilla) que cuenta con 3 tarjetas de red: una en WAN, y dos LAN. Unida a otra máquina (que será la sucursal de Barcelona) donde tendremos dos tarjetas de red una en WAN y otra en LAN.

Y también tendremos esa máquina de la sucursal principal de Sevilla en modo servidor con OpenVPN que dará servicio a los clientes que añadamos, entre ellos nuestro dispositivo móvil.

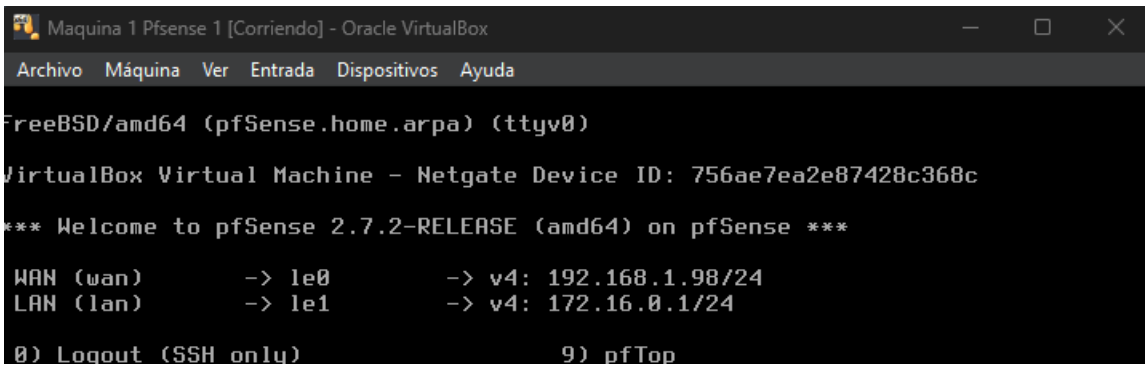
*NOTA: he clonado todas las máquinas, simplemente he adaptado las necesidades de cada, por eso los nombres son similares o solo se le añade “1”.

Por eso también se llama igual en consola, pero hago ip a para que se vea cual es cual ya que la MAC varía.

Pfsense 1:



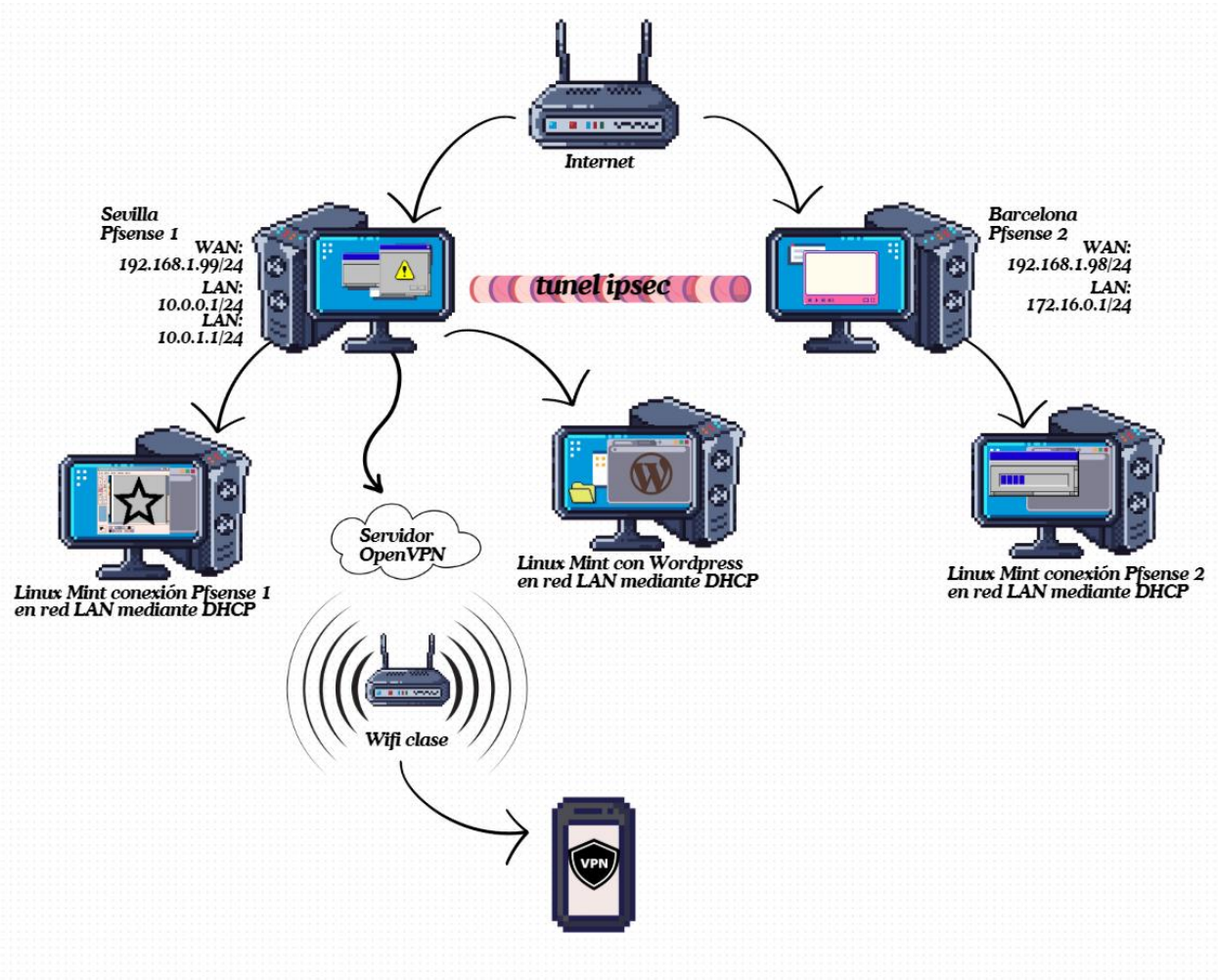
Pfsense 2:



*NOTA: las IP en clase solo varían en las redes WAN que en vez de ser
192.168.1.99 /24 → 192.168.2.99 /21

192.168.1.98 /24 → 192.168.2.98 /21

El esquema de red queda así:



*lo añadiré a parte para que se pueda observar mejor.

IPSec.

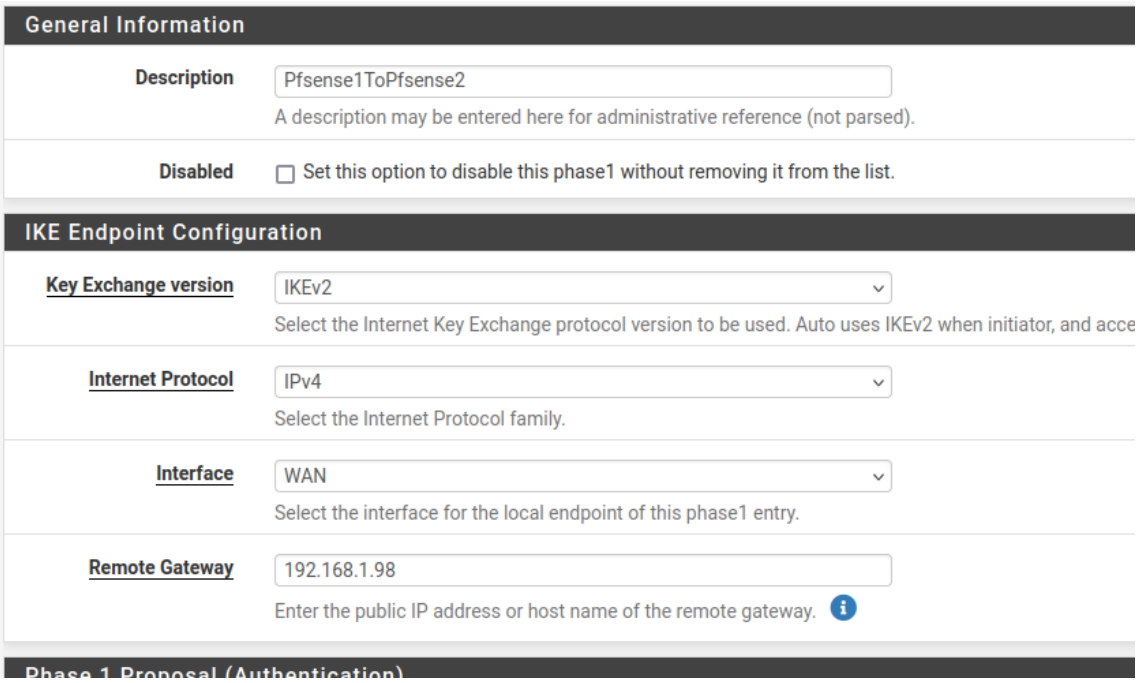
Vamos a implementar un servidor VPN con IPSec, que unirá en modo túnel (punto a punto) ambos Pfsense.

Sevilla.

Vamos a comenzar con el Pfsense que tenemos en la sucursal de Sevilla, para acceder a la configuración voy a usar un Linux mint que ya tenía creado de la anterior práctica.

Una vez estemos en la configuración iremos al menú superior y seleccionaremos la opción VPN > IPSec.

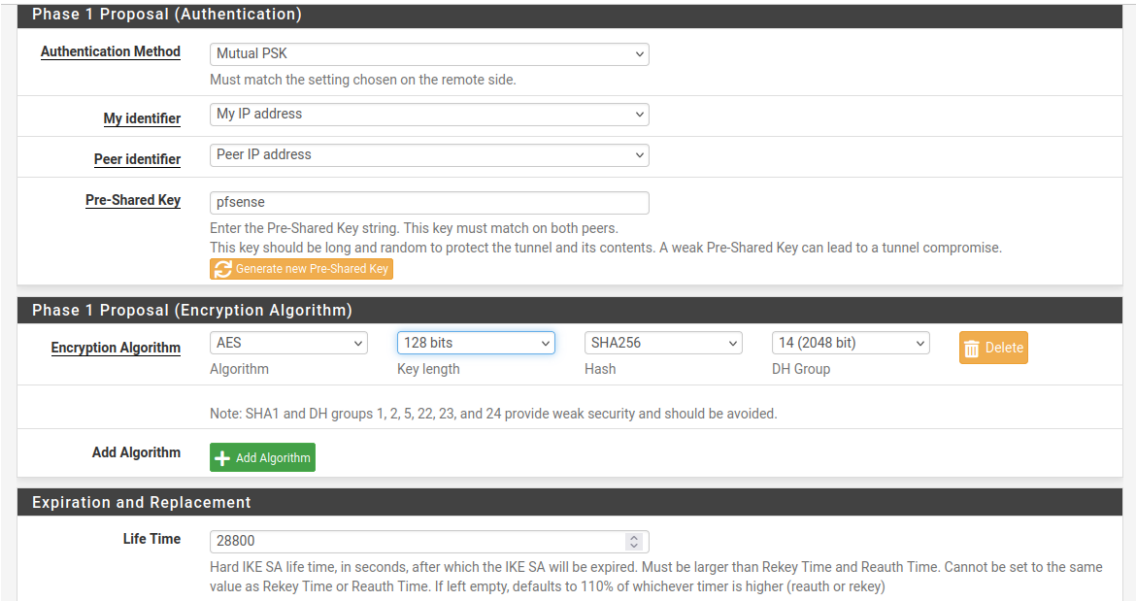
Vamos a crear el primer túnel, que nombraré Pfsense1ToPfsense2, será en la interfaz WAN del punto local final.



La dirección IP de puerta de enlace usaremos la IP del Pfsense 2.

La “pre-shared key” es recomendable poner una complicada, pfsense tiene el botón justo abajo para generar una, pero en este caso usaremos una para la prueba.

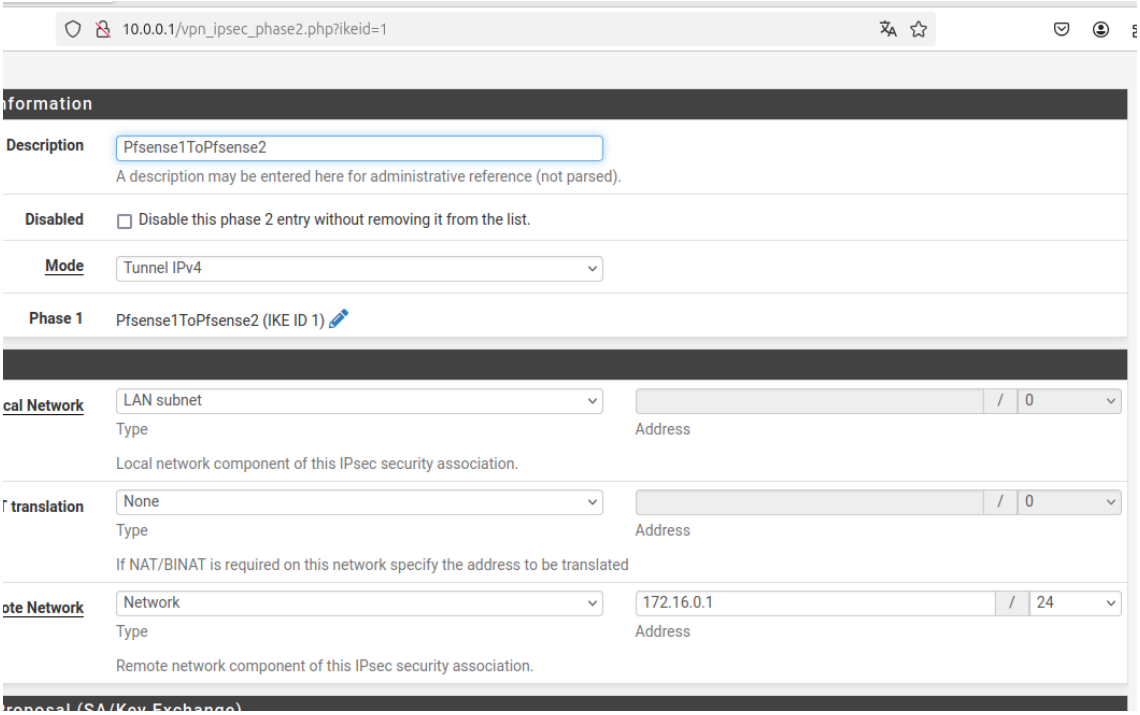
El algoritmo de encriptación mientras más bits tenga la llave de longitud más consumirá de CPU por lo que mayores requisitos necesitaremos y más tiempo tardará, pero será más seguro.



El resto de opciones se quedan por predeterminado, bajaremos y lo añadiremos.

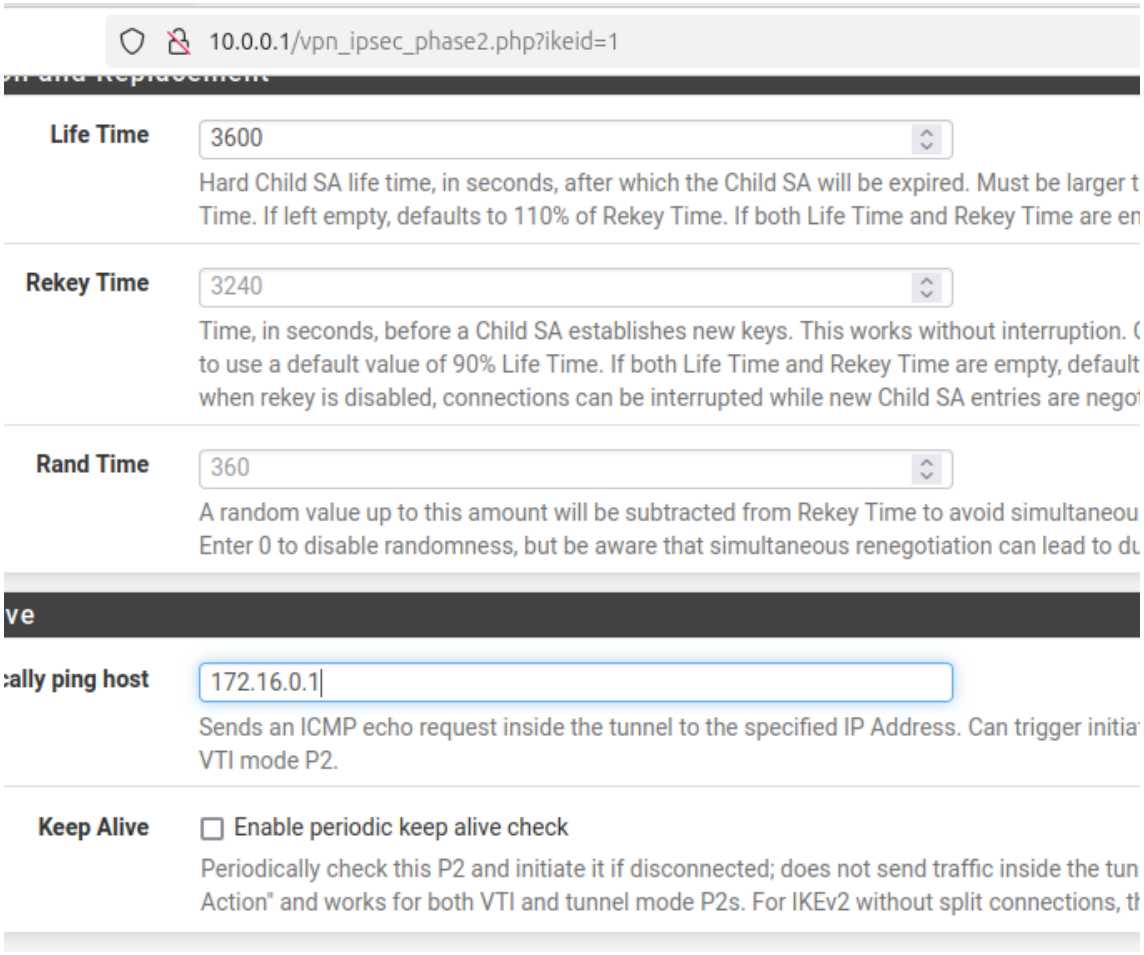
Antes de aplicar los cambios vamos a añadir la Fase dos haciendo clic en Add P2.

Le pondré el mismo nombre, en red remota pondremos la IP de LAN del Pfsense 2.

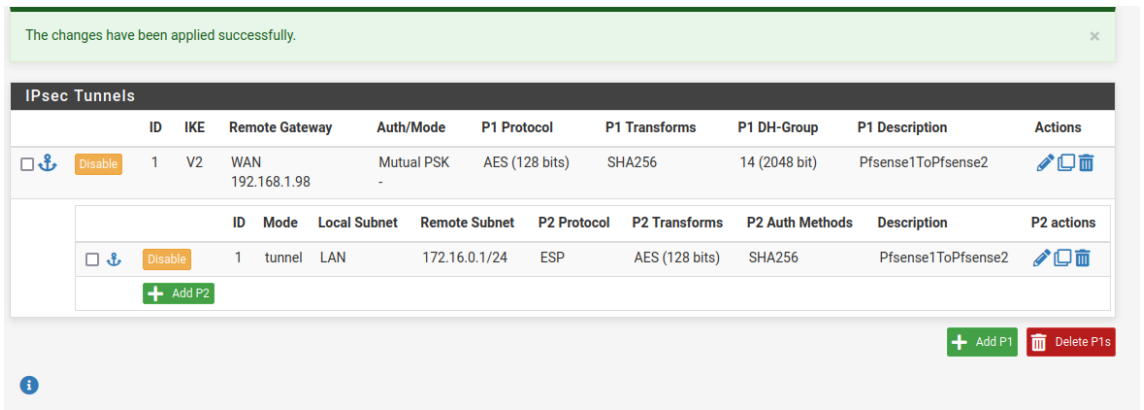


Como estamos probando solo dejaremos la encriptación AES a 128bits, las demás opciones las desmarcamos. Y lo demás por default.

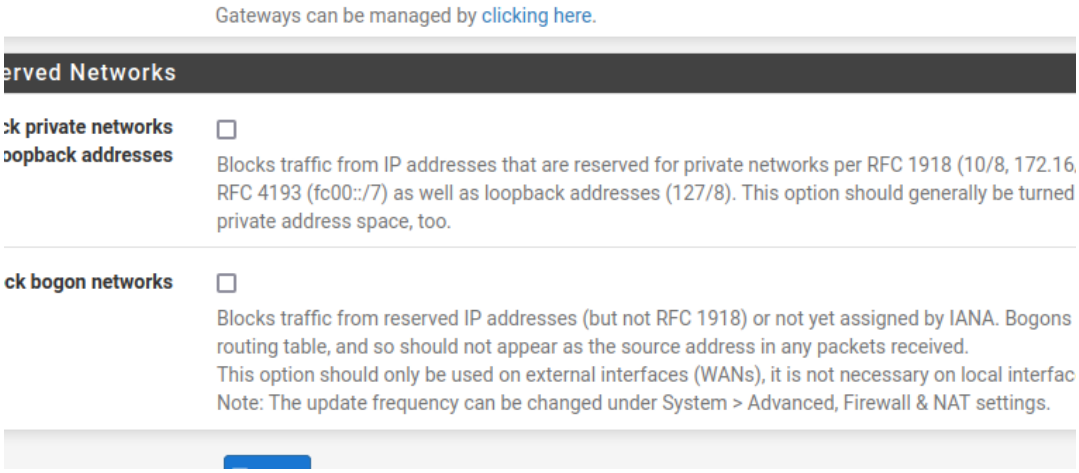
En el host ping pondremos la IP de la LAN de Pfsense 2.



Guardaremos y aplicaremos cambios.

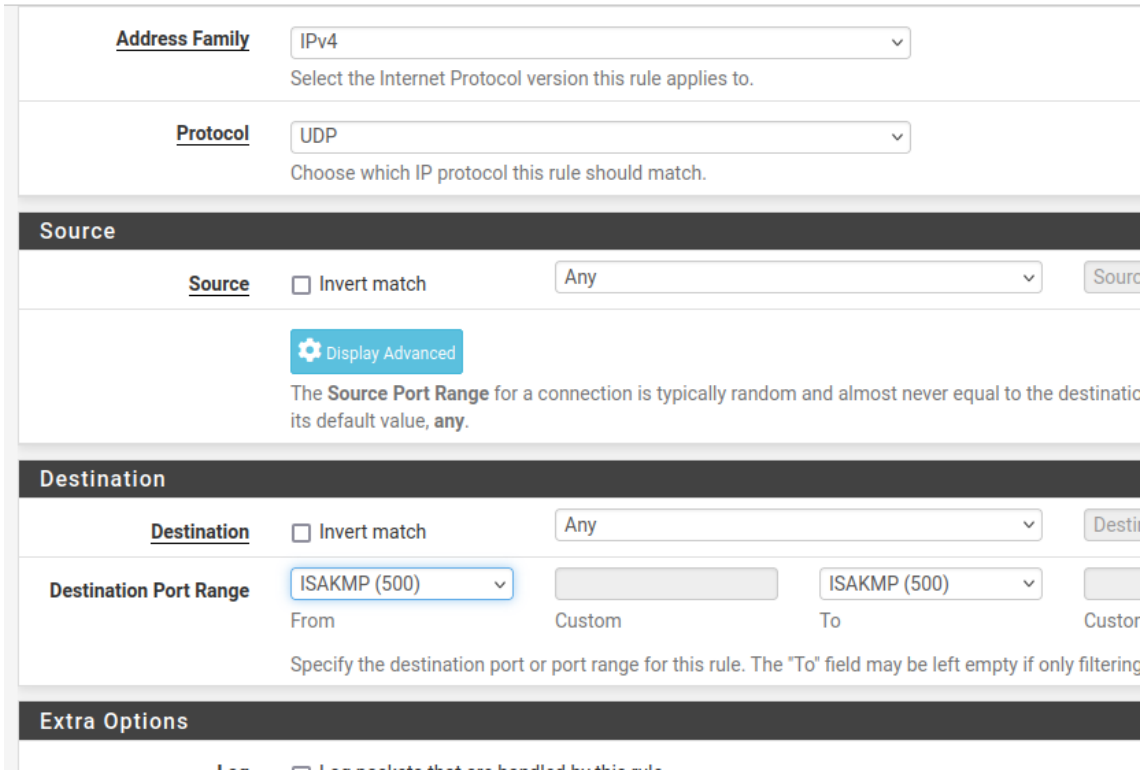


NOTA: será importante en el Firewall de la interfaz WAN que desmarquemos las opciones que bloquean el trafico de redes privadas y redes loopback, además si queremos probar esto desde Windows también desactivar el Firewall de Windows o del programa que tengamos.

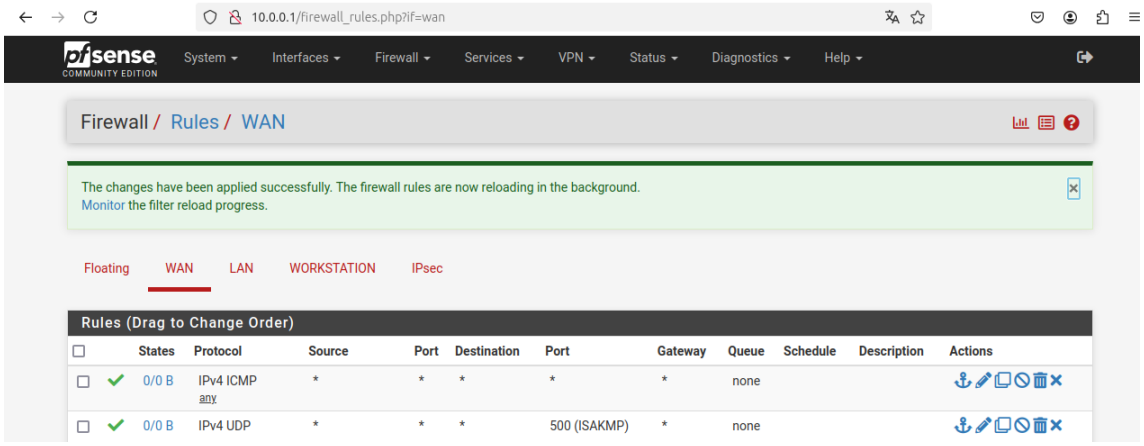


Reglas Firewall.

Vamos a ir Firewall > Rules > WAN y aquí crearemos una regla que permita el protocolo ISAKMP el cual proporciona comunicaciones seguras a través de redes IP porque negocia los parámetros de seguridad, entre otras cosas.

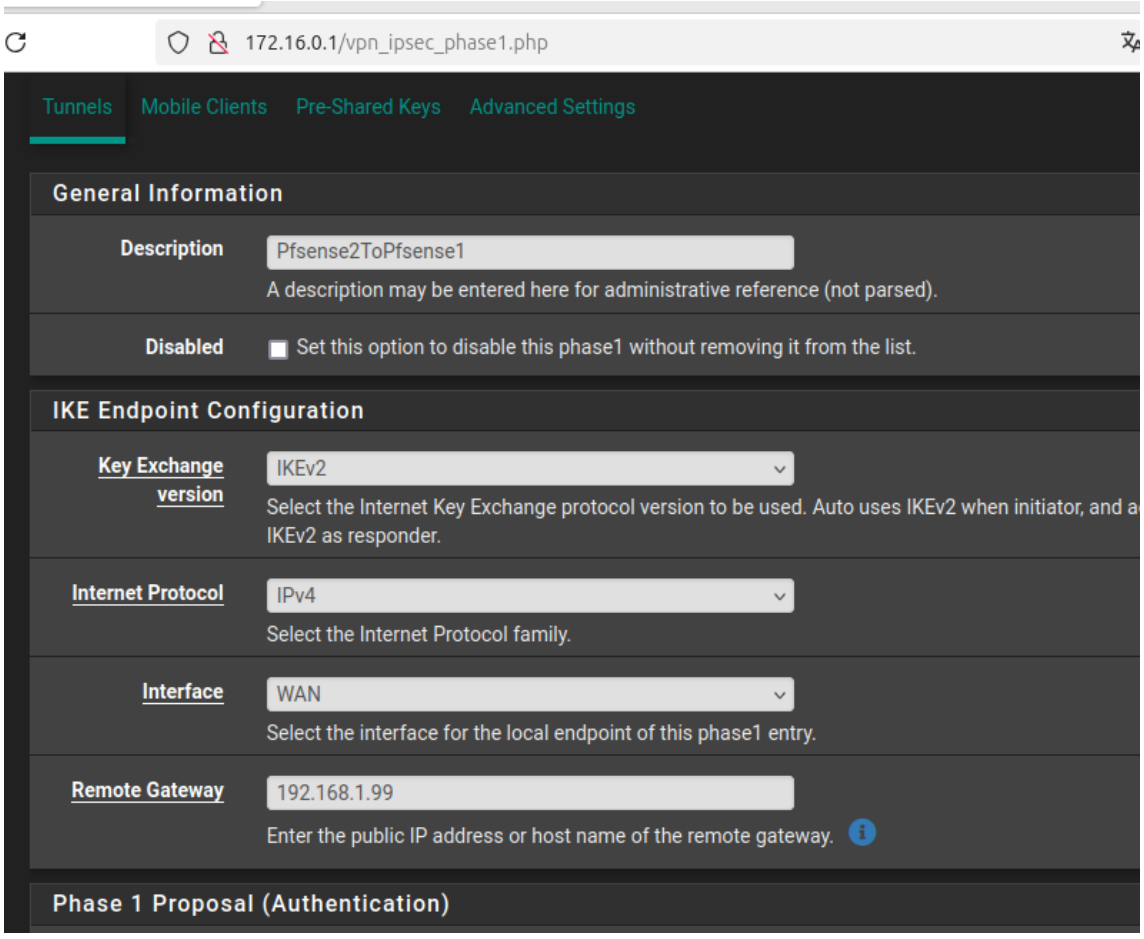


Además, añadiremos otra que permita que hagan ping, que es mediante el protocolo ICMP.



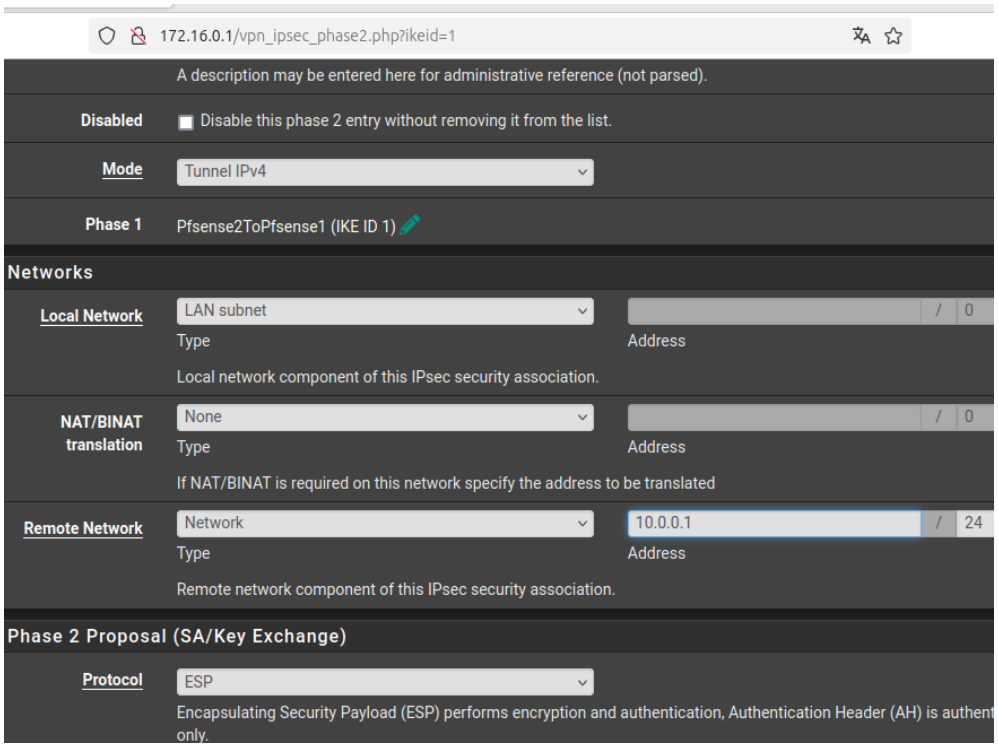
Barcelona.

Pasamos ahora a la configuración del Pfsense de la sucursal de Barcelona, para ello iremos al menú superior VPN> Ipsec y aquí añadiremos el túnel igual que en Sevilla, esta vez se llamará Pfsense2ToPfsense1.

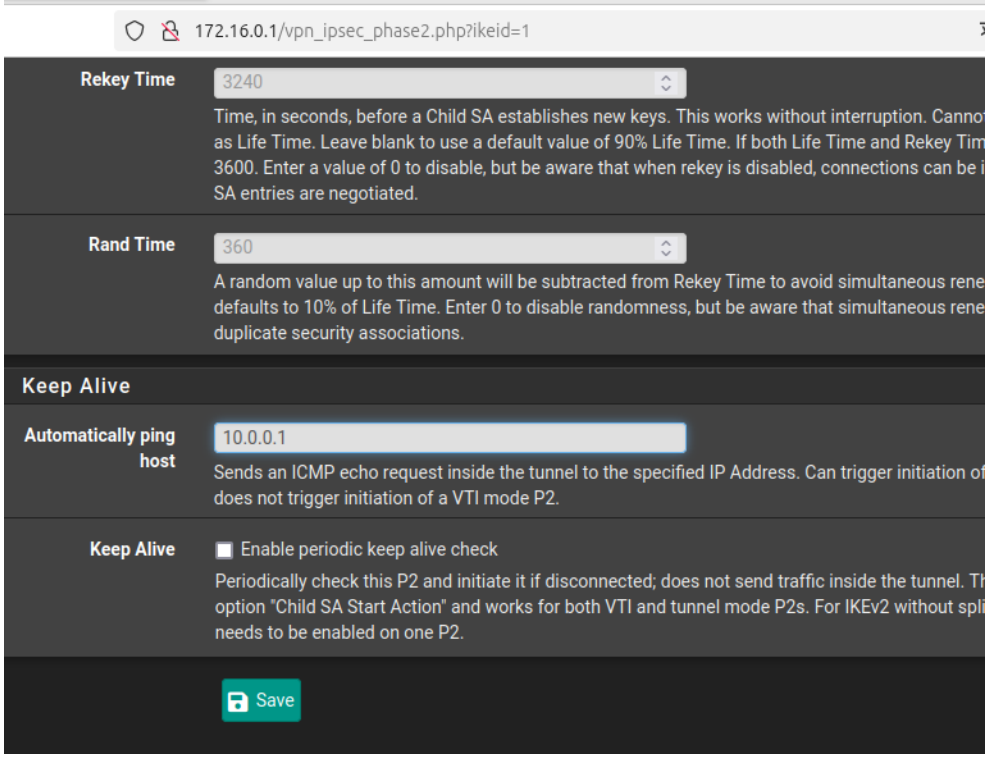


Seguiremos los mismos pasos que en Sevilla y guardaremos pero no aplicaremos la configuración.

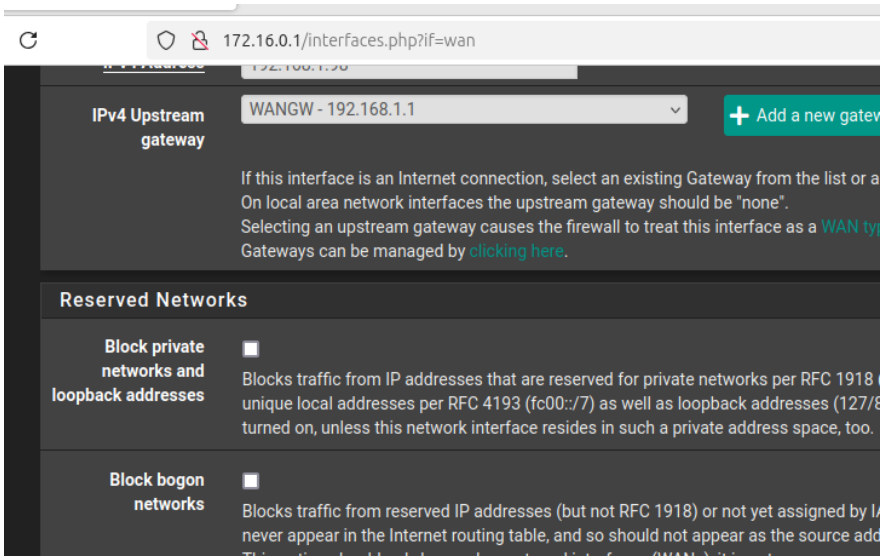
Ahora vamos con la fase dos:



Esta vez las IPs serán de la LAN del Pfsense 1.

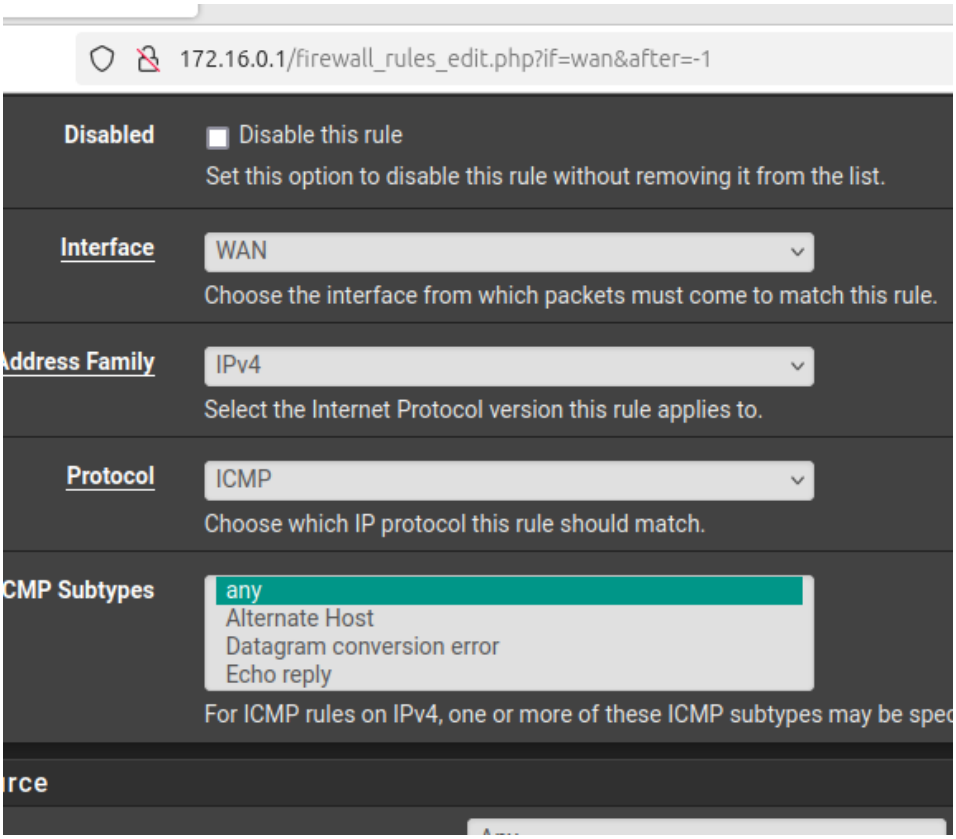


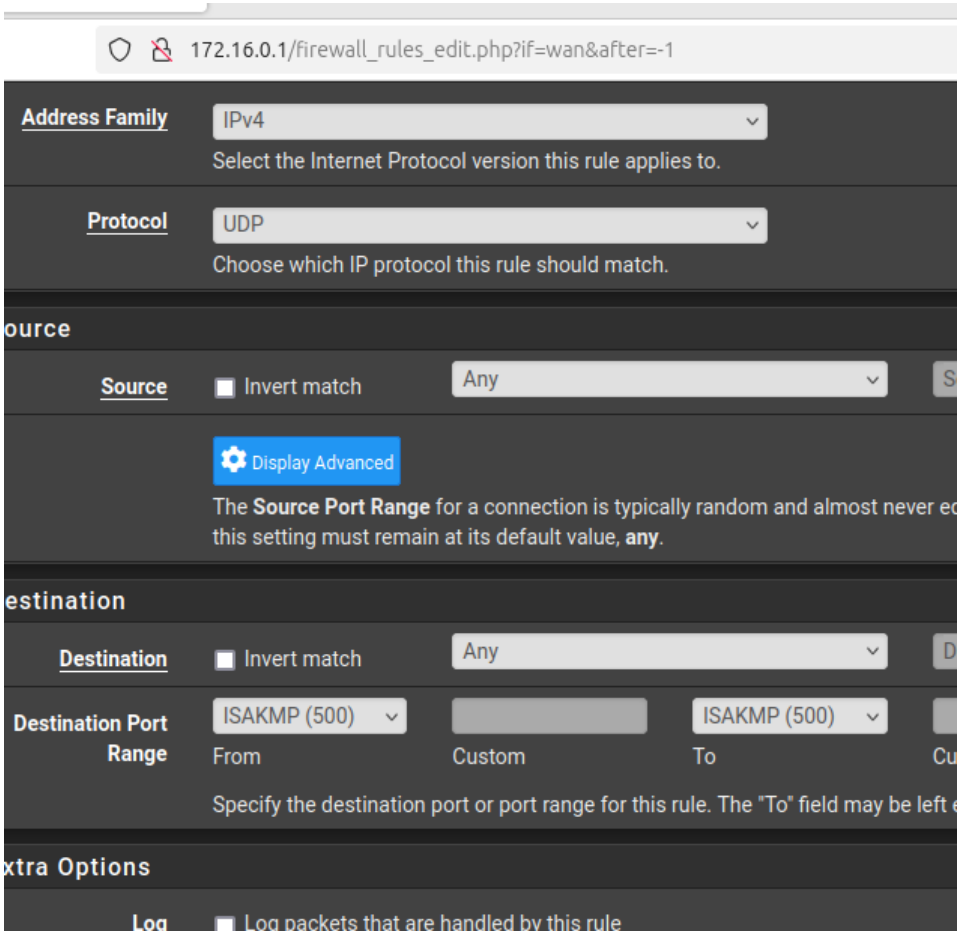
De nuevo comprobaremos que tenemos estas opciones desactivadas en la interfaz WAN:



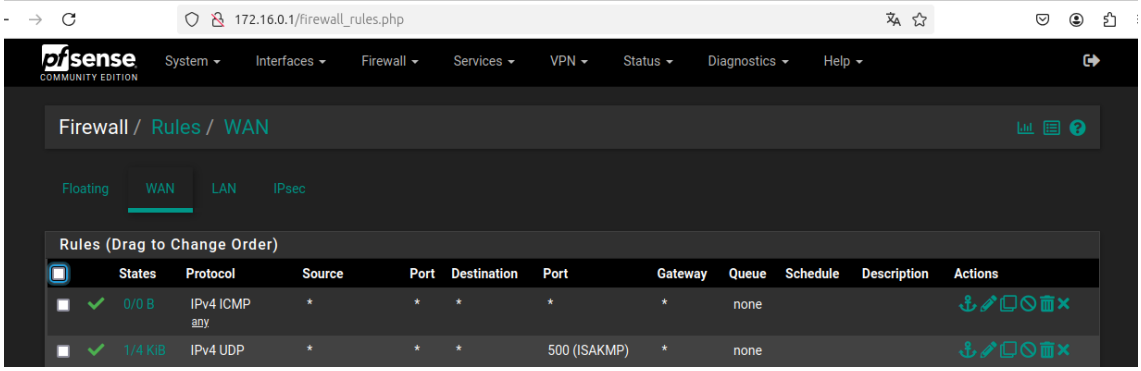
Reglas Firewall.

Esta vez vamos a crear las mismas redes firewall que en Sevilla, que son la de ISAKMP y la de ICMP.





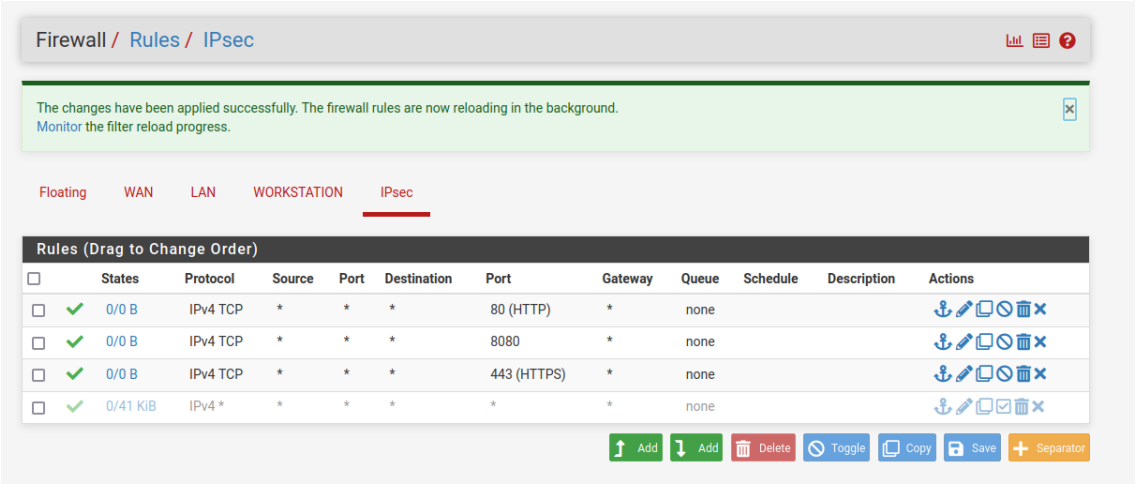
Así quedan las reglas WAN:



Reglas Firewall IPSec.

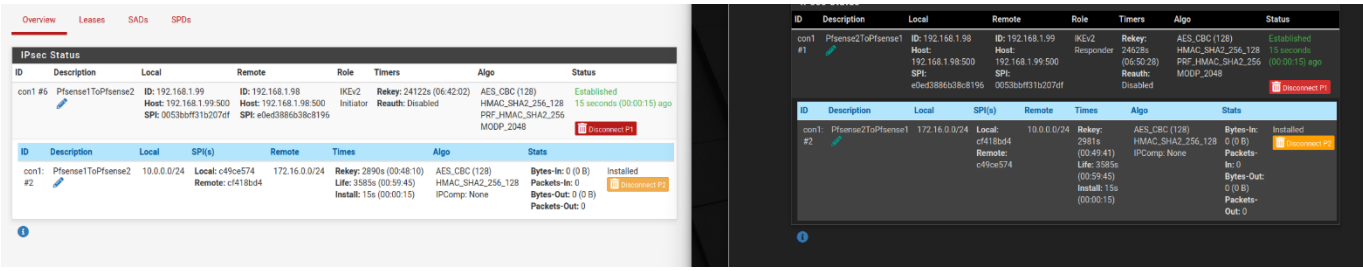
Antes de probar conexión vamos a crear una regla en el firewall de IPSec para que deje pasar todos los protocolos, una vez probada la conexión deshabilitaré esa regla y procedo a hacer reglas para que solo se permita el puerto 80 que es http, el 443 que es https y el 8080 donde tenemos el Wordpress.

*Este paso lo realicé em ambos Pfsense.

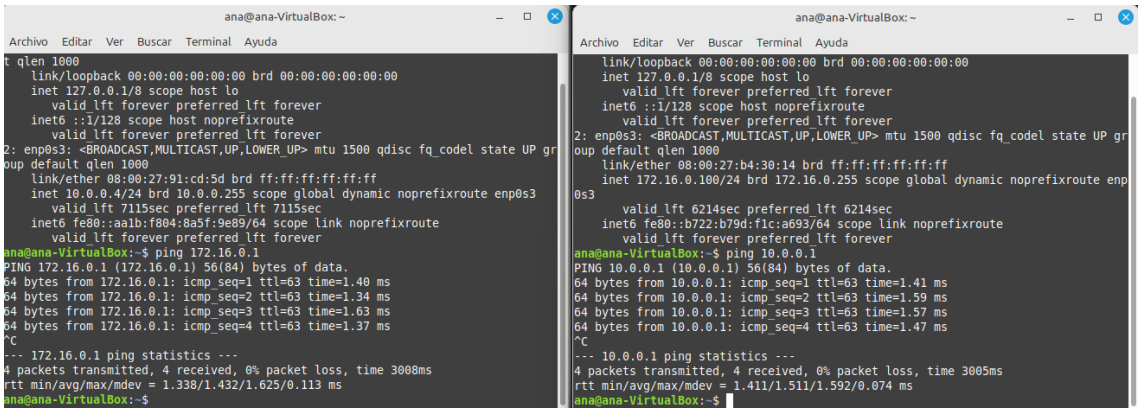


Conexión.

Voy a comprobar el status y para ello iré Status > IPSec.



Para comprobar la conexión primero probaré a hacer ping entre ambas:



Lo segundo que haré será montar un servidor Wordpress igual que en la anterior práctica (tuve que crearlo ya que tuve que migrar lados de un SSD a otro por un fallo del SO y algunos archivos parece que se corrompieron o se perdieron y no funcionaban muchas máquinas).

Este es mi Wordpress:

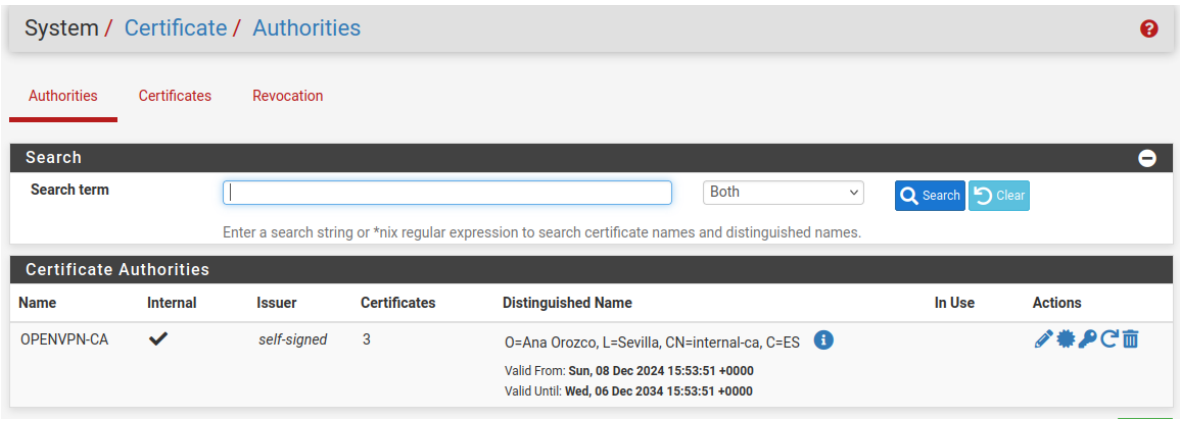
Y esta es la conexión desde la LAN del Pfsense 2:

OpenVPN.

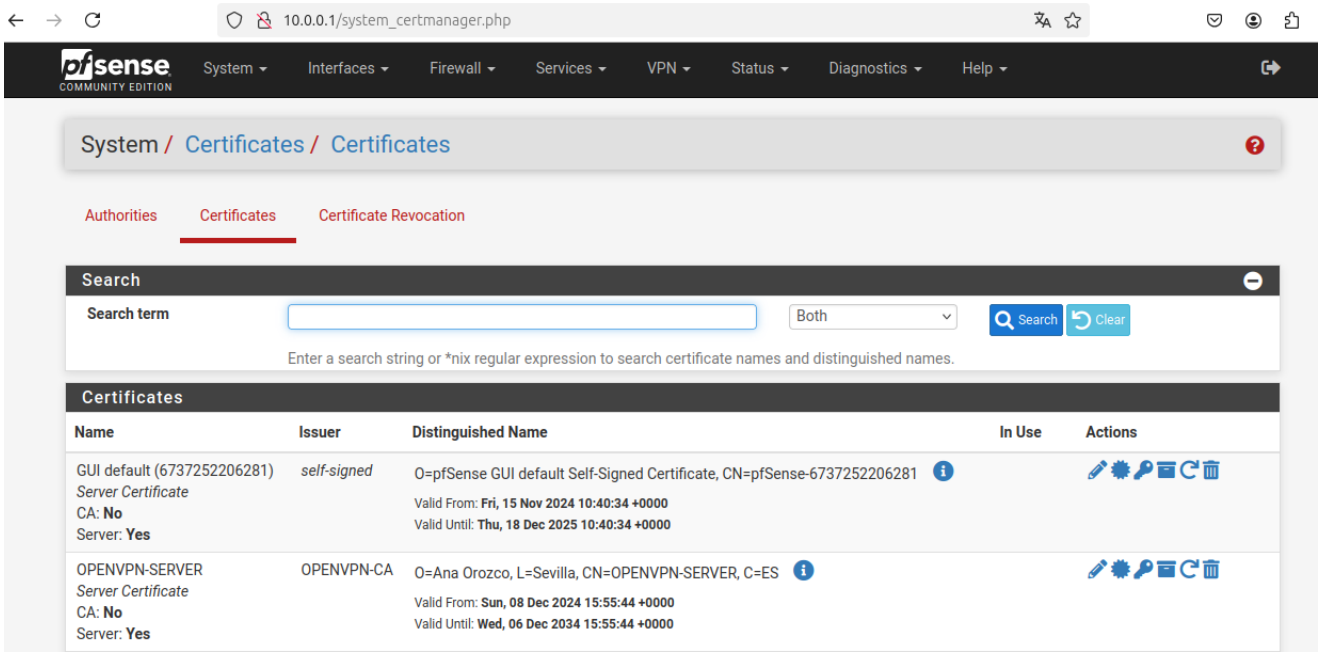
Esta parte de la práctica se hará desde el Pfsense 1 de la sucursal de Sevilla.

Certificados.

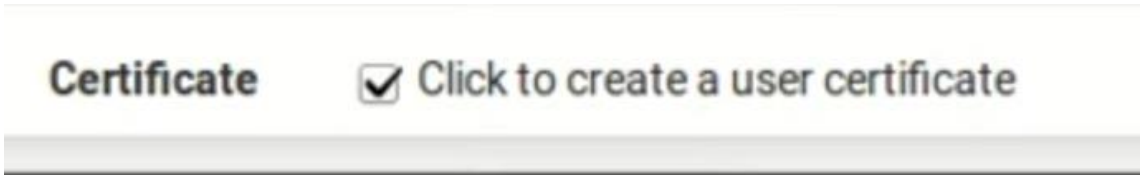
Lo primero que vamos a hacer es crear certificados, para ello iremos a System > Certificate Manager y añadiremos una autoridad certificadora con método interno.



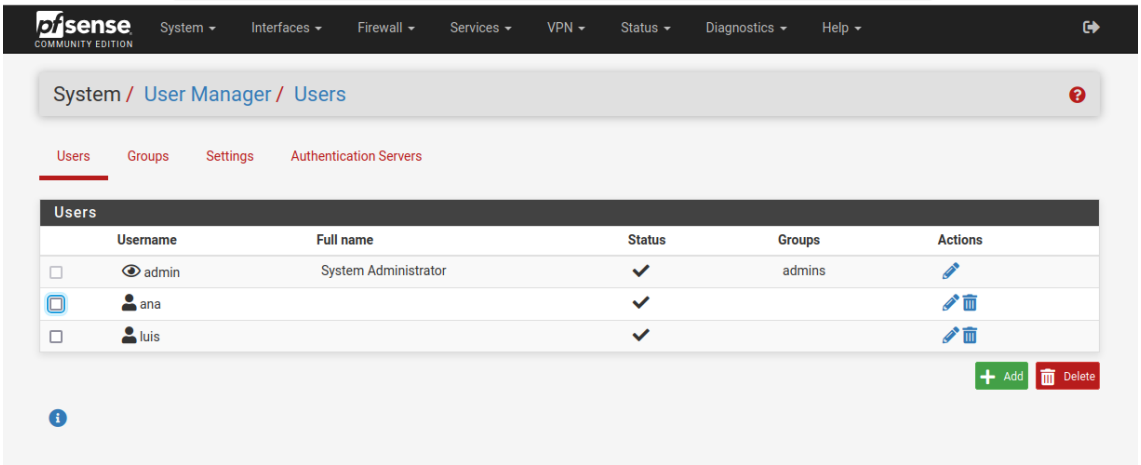
Ahora en esta misma ventana seleccionaremos Certificates donde crearemos un certificado de tipo servidor:



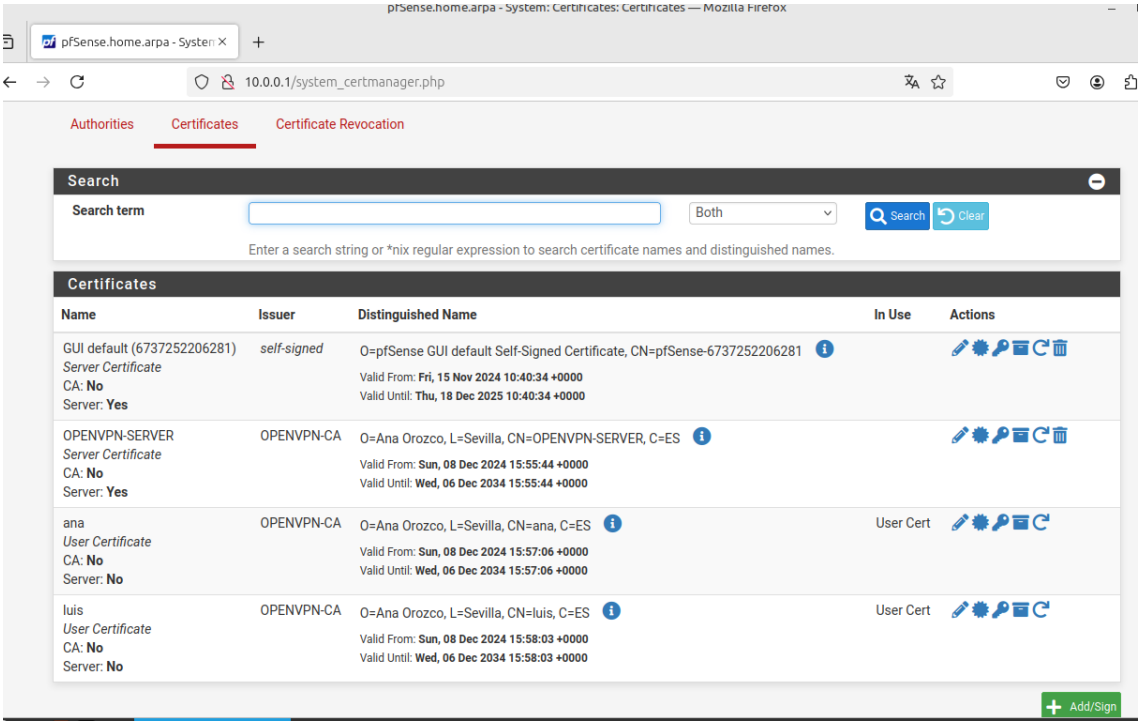
A continuación, vamos a crear las certificaciones de usuario, que para ello hay que crear los usuarios en System > User Manager, aquí crearemos los usuarios que necesitemos con contraseña, grupos, etc. Para crear la certificación solo debemos hacer clic en una opción que dice “Clic para crear certificado de usuario” desde la misma zona de la creación de cada usuario:



Yo he creado el usuario Ana y otro Luis (más adelante creo el usuario Bernat).



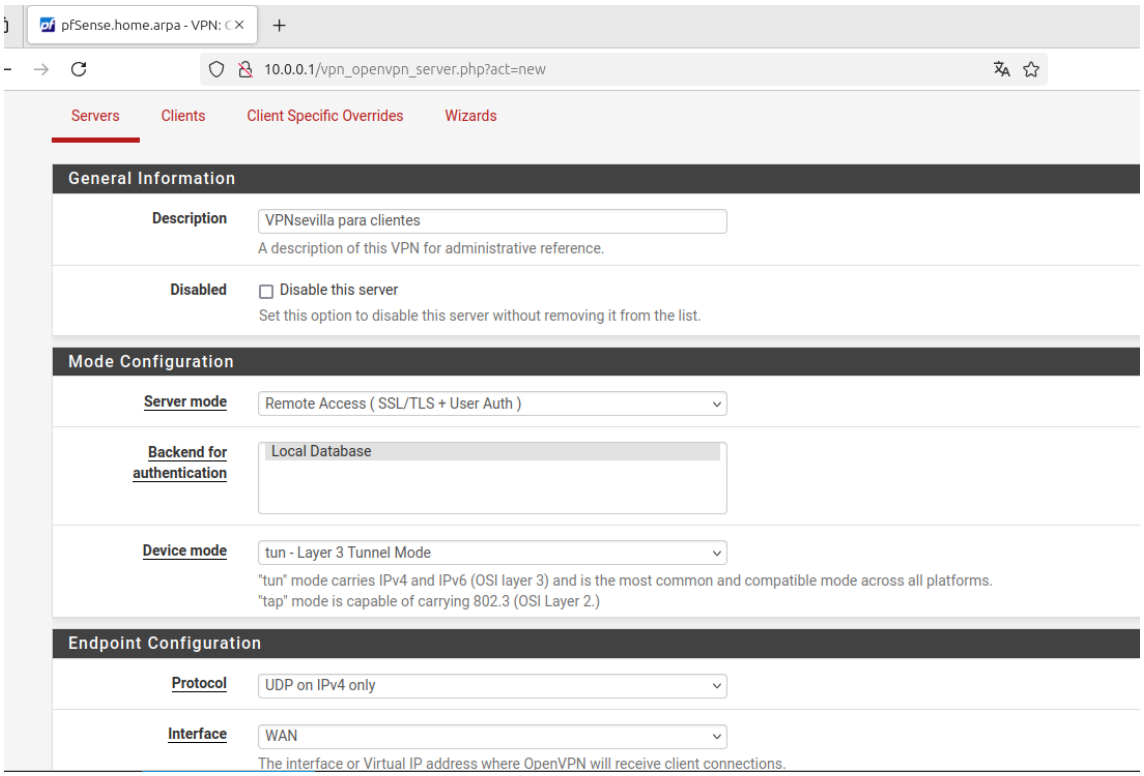
Así se verán los certificados cuando creemos los usuarios:



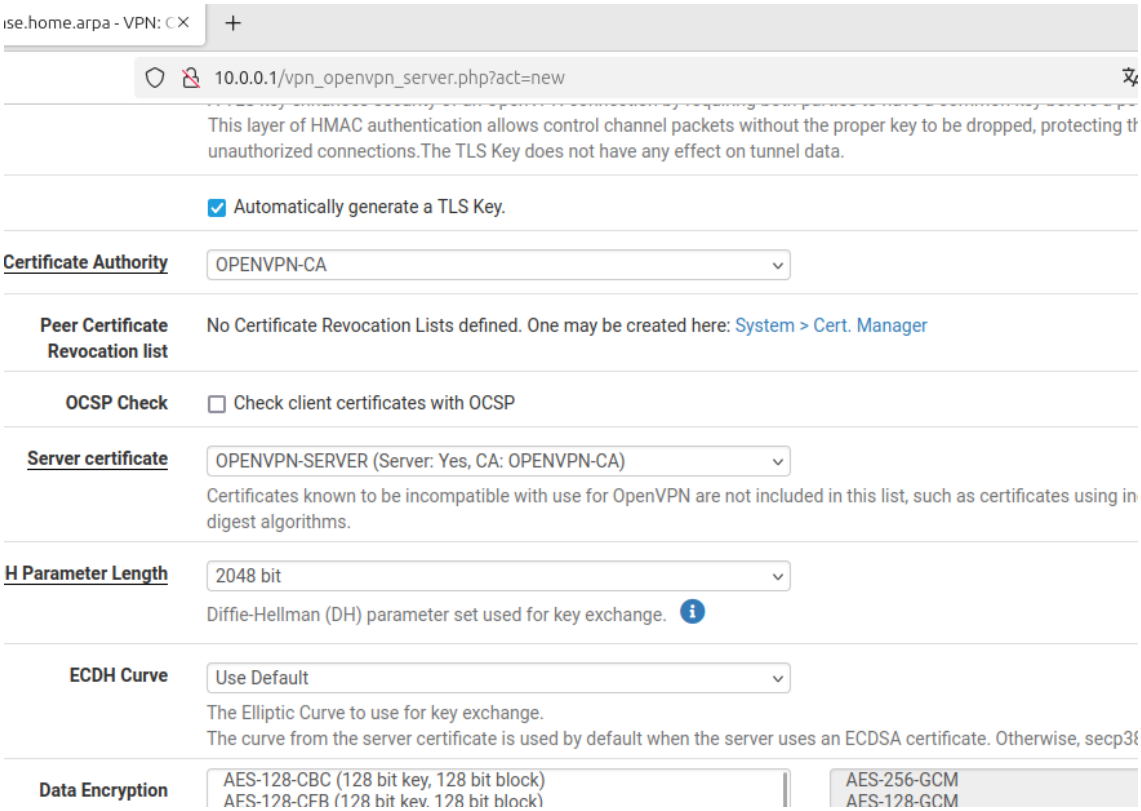
Una vez tengamos los usuarios que necesitamos vamos a crear el servicio de OpenVPN, para ello iremos a VPN > OpenVPN.

Y Añadiremos un servidor con las siguientes configuraciones:

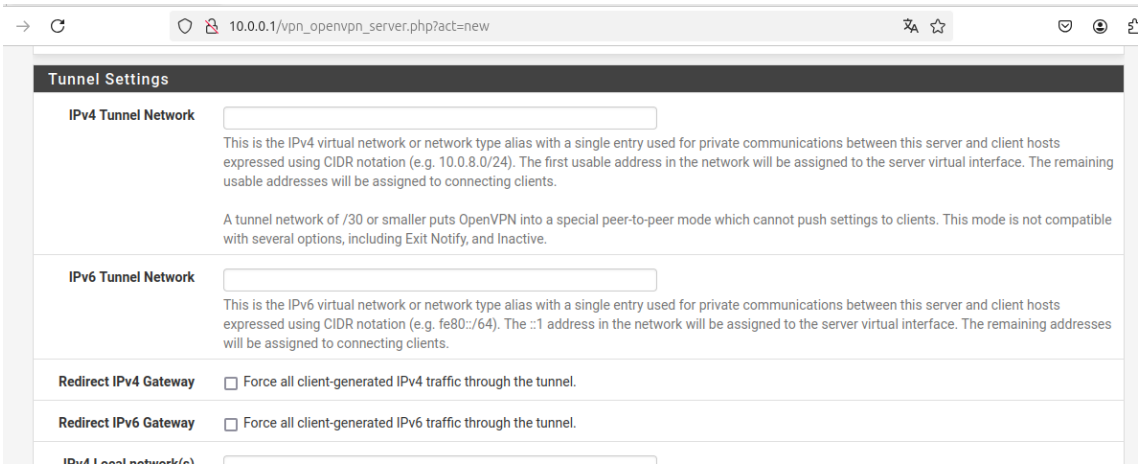
El modo de servidor será de acceso remoto SSL/TLS + autentificación de usuario



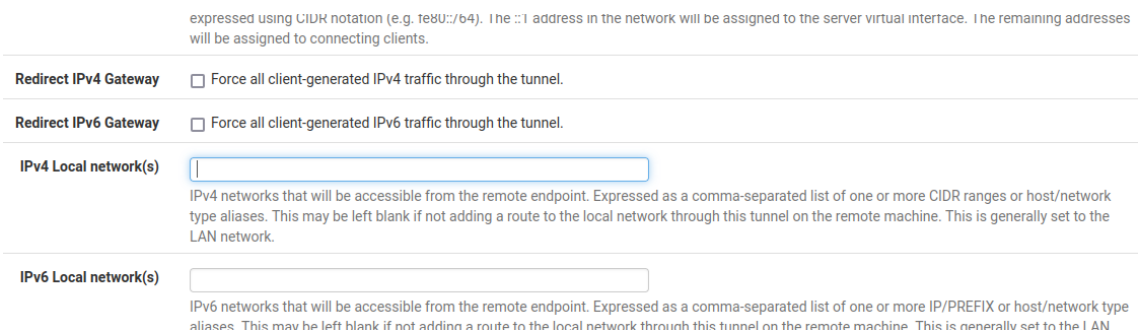
Vamos a seleccionar los certificados que ya creamos en el paso anterior, lo demás lo dejaré por predeterminado.



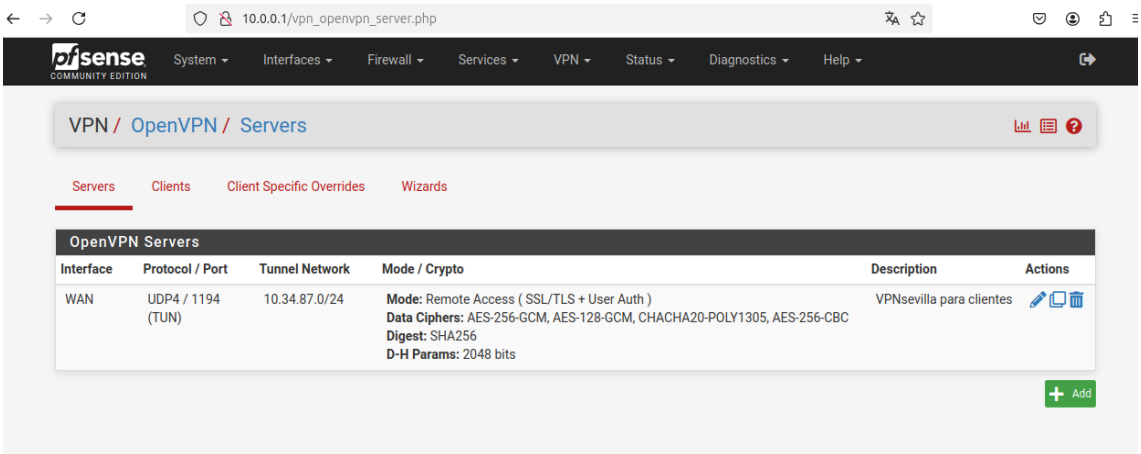
Como Red Tunnel esta es la que tendrán los usuarios que se conectarán, pondré la 10.34.87.0/24



Y en Local Networks pondremos la IPs que queremos que sean accesibles, como dice la práctica serán las LANs del Pfsense .

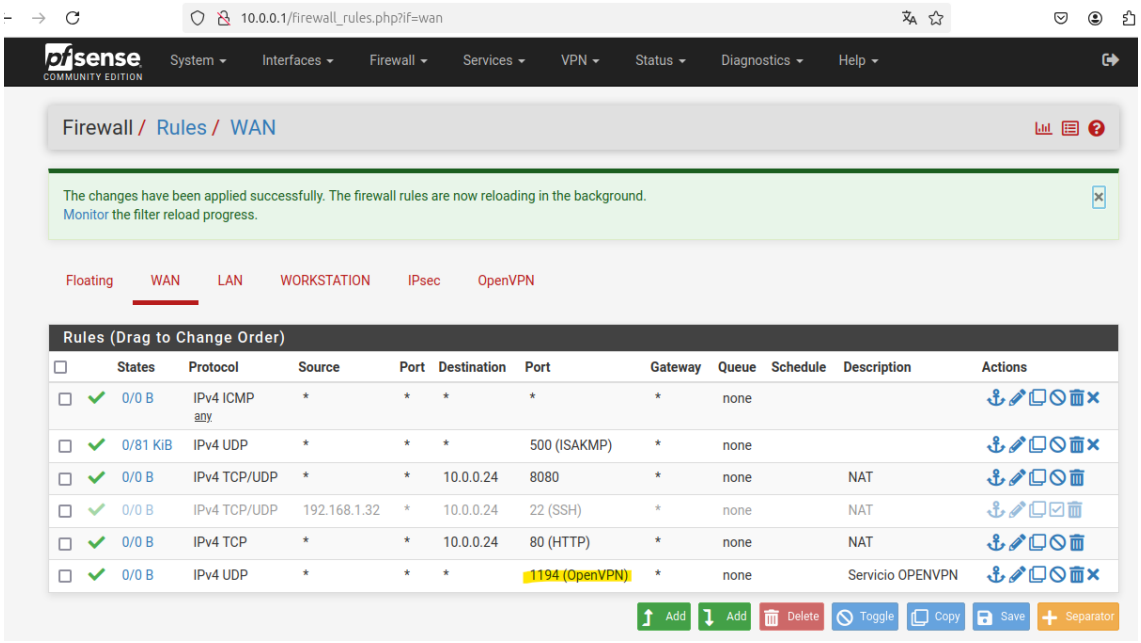


Por último, casi al final de la configuración pondremos nivel 3 de registro de Logs y guardaremos el servidor.

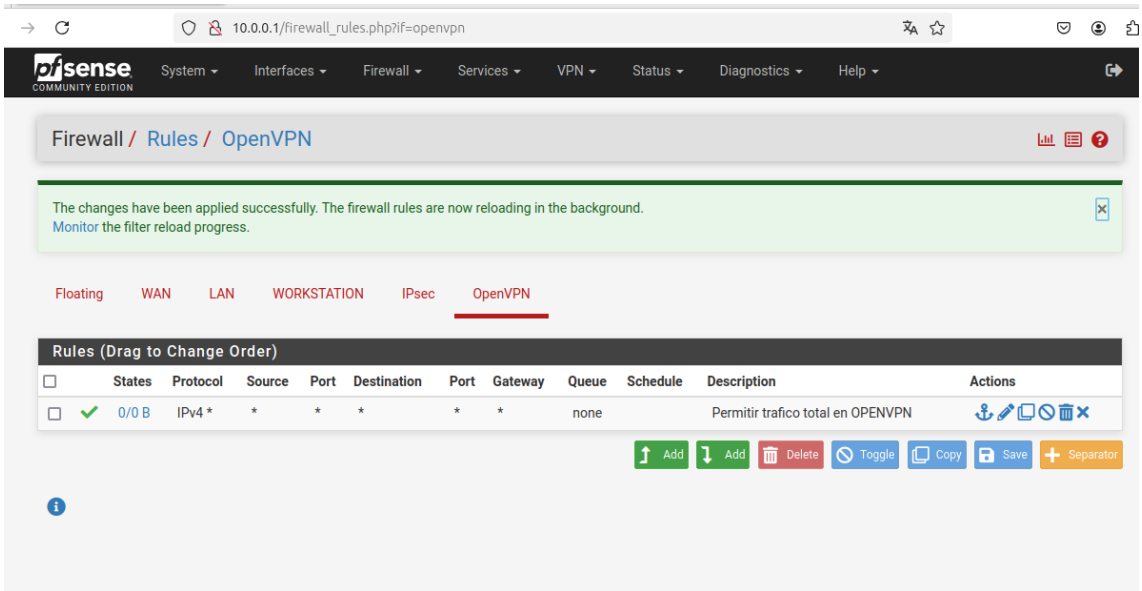


Regla Firewall

Será necesario hacer una regla firewall para que permita el puerto 1194 de tipo UDP en la interfaz WAN, en la imagen sale abajo del todo, pero decidí subirla más delante de la configuración ya que es muy importante el orden en el que disponemos las reglas firewall.

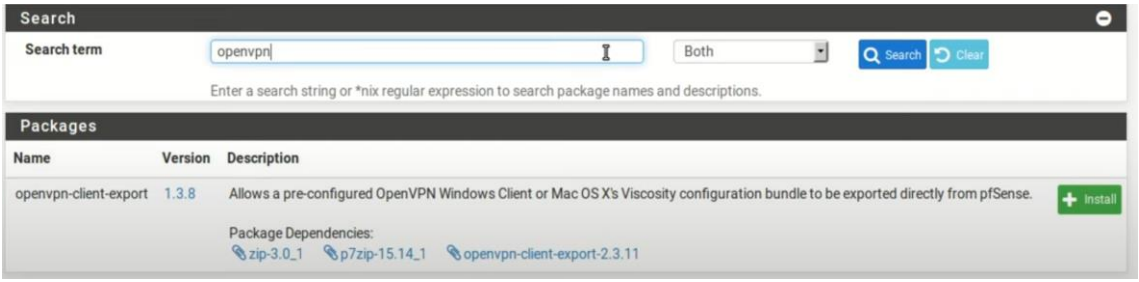


Además, en la interfaz del OpenVPN haremos una regla que de permiso total, esto podemos editarlo más adelante pero como en la práctica no se menciona ningún requisito especial pues decidí dejarlo así.

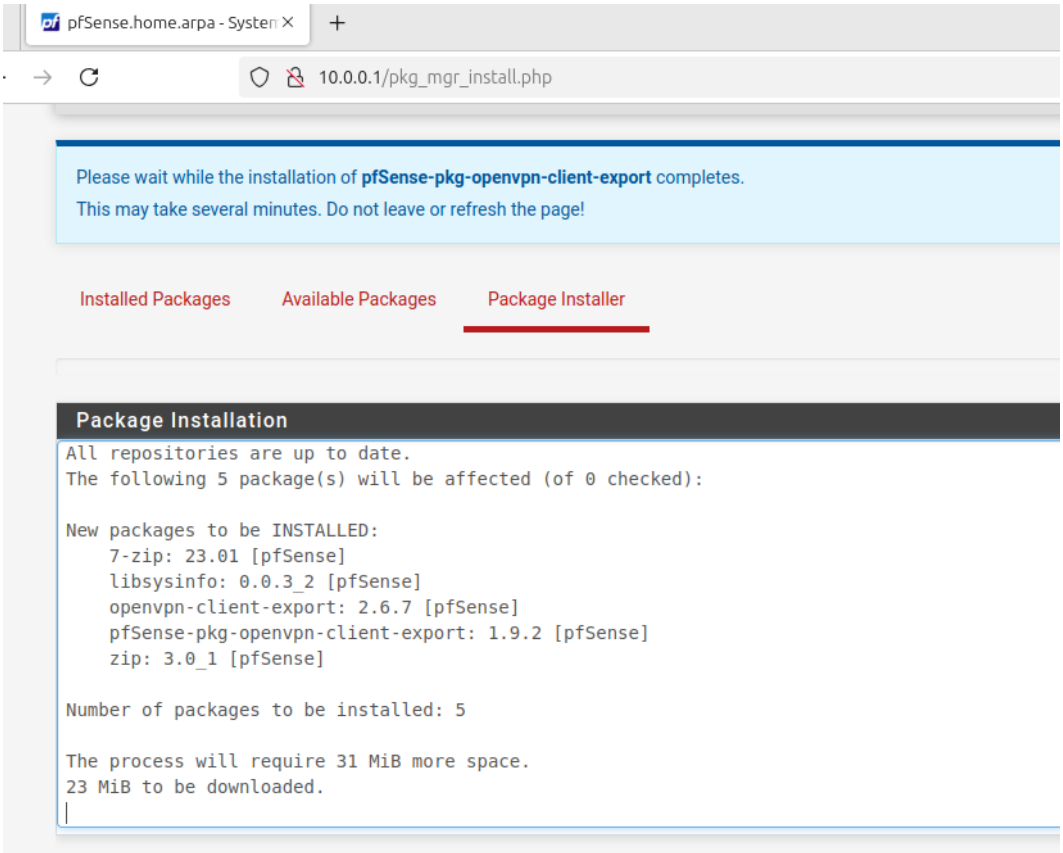


Archivos para OpenVPN.

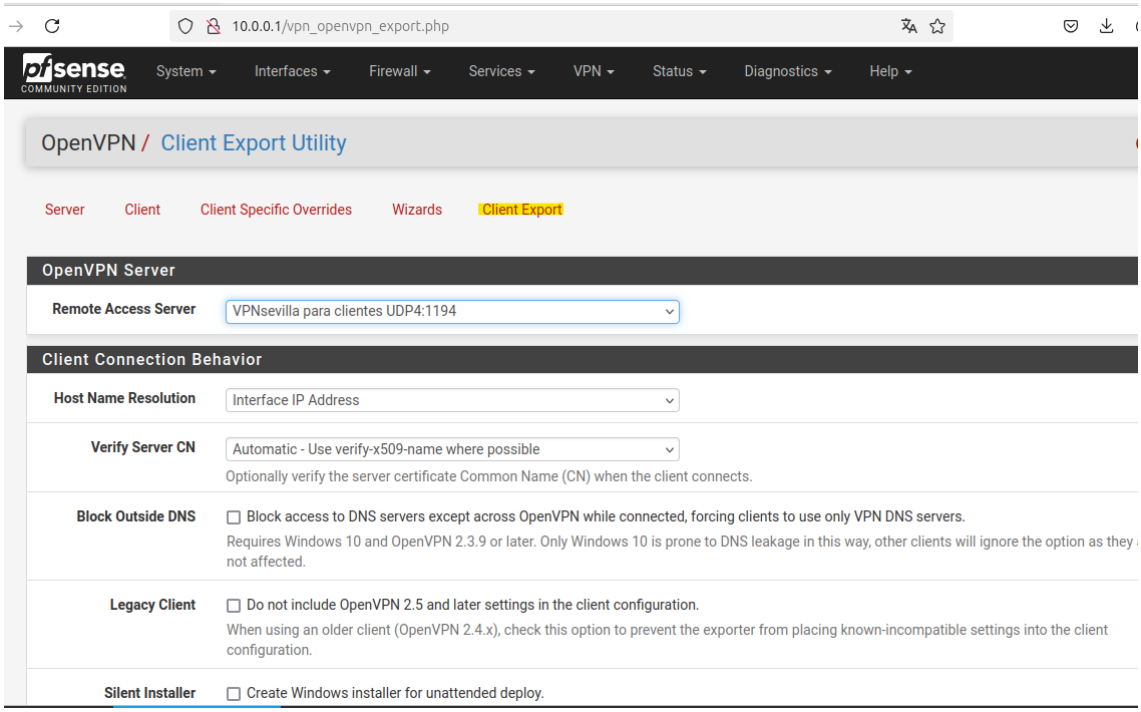
Para poder realizar esta parte de la práctica necesitamos añadirle un paquete al Pfsense, por lo cual iremos a System > Package Manager y ahí buscaremos “openvpn” en el cuadro de búsqueda y nos saldrá este paquete que instalaremos:



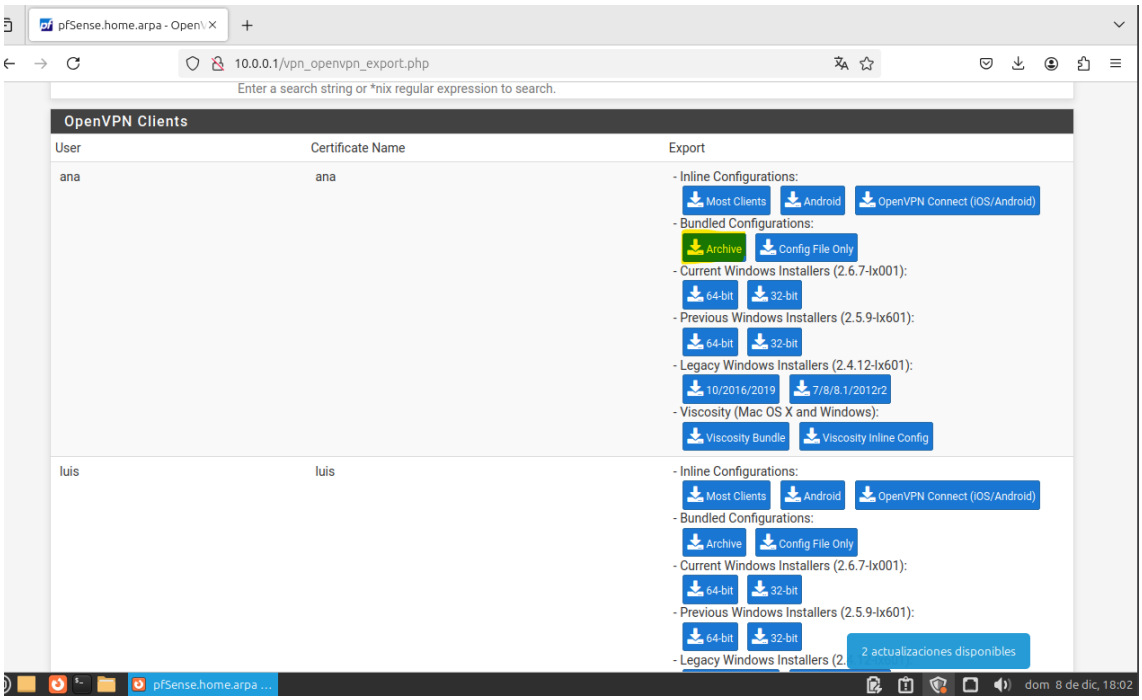
Comenzará la descarga e instalación:



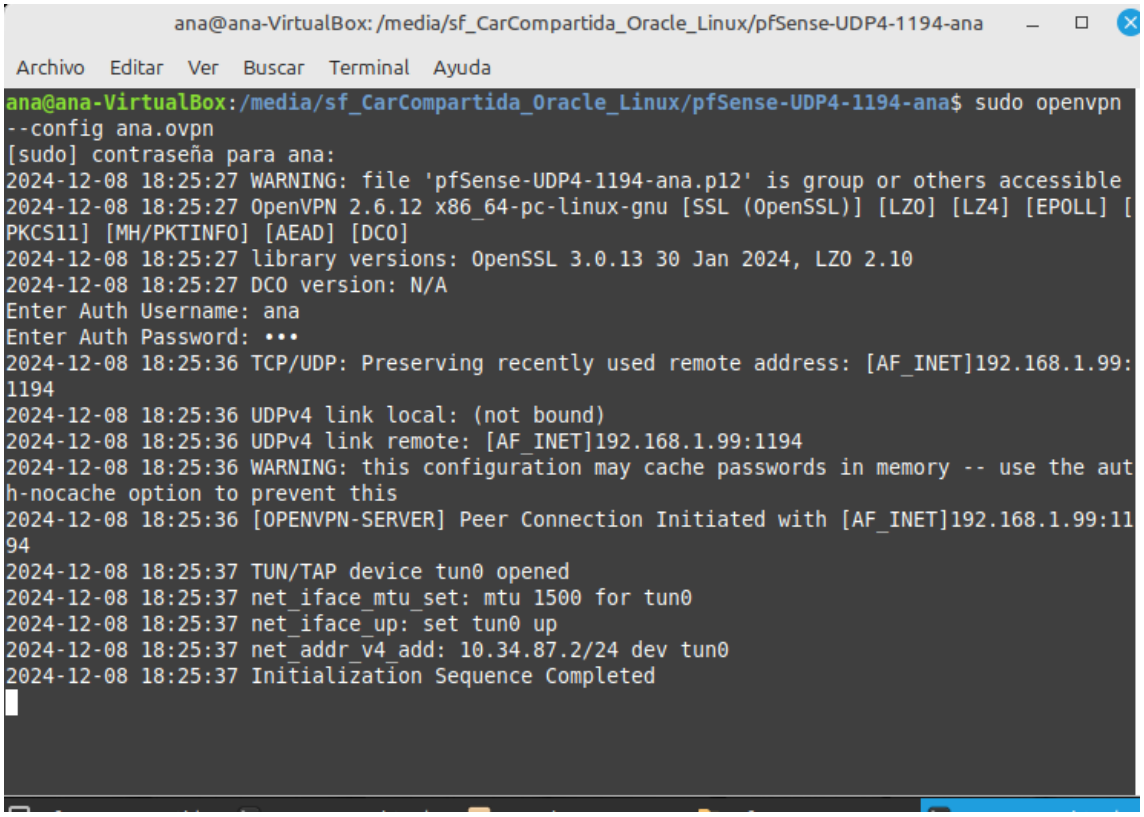
Esto añadirá en el menú OpenVPN una pestaña adicional que subrayo en la imagen de abajo:



Bajaremos y tendremos una lista con los usuarios y sus archivos para conexión:



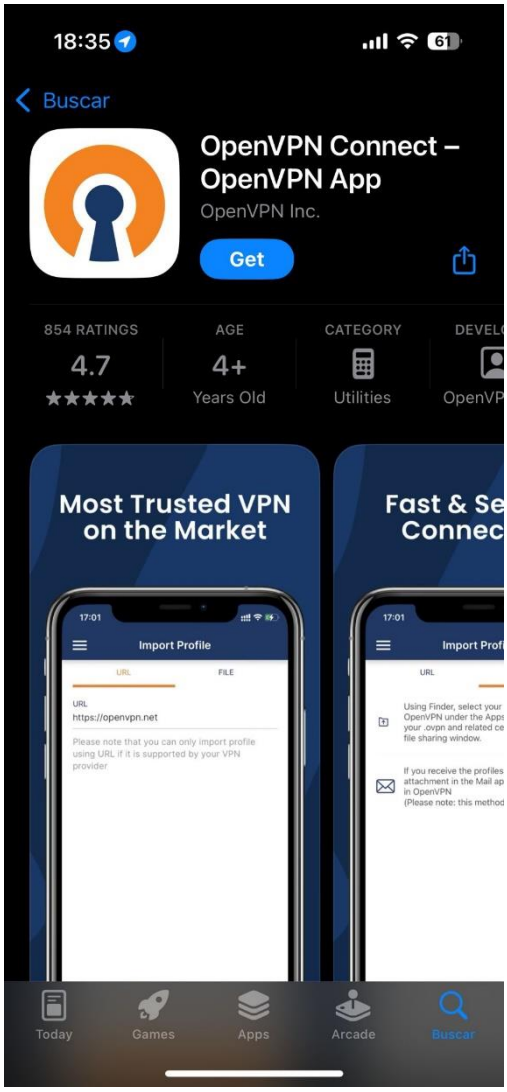
Podemos conectarnos desde Windows, lo cual requiere un programa y el archivo del usuario correspondiente, también podemos conectarnos mediante un dispositivo móvil que ahora probaremos y por último mediante Linux que es la manera más fácil, ya que solo necesitamos poner un comando y el archivo.



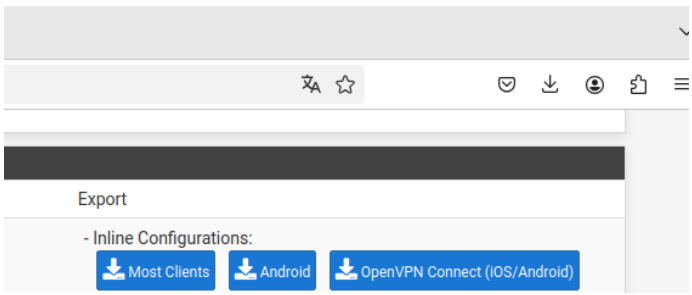
En este caso me pasé el archivo mediante una carpeta compartida existente y al archivo le cambié el nombre para facilitarme la escritura.

Acceso desde dispositivo móvil.

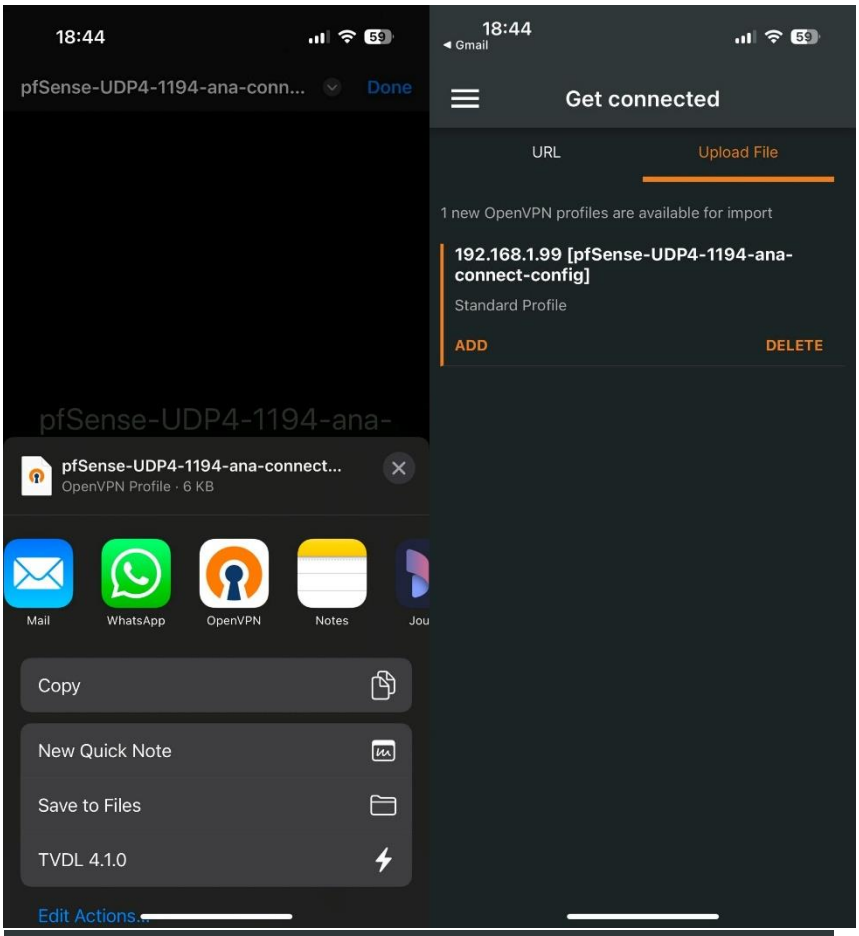
En mi caso voy a acceder desde un dispositivo Apple, un iPhone, por lo que iremos a la App Store y buscaremos esta app:

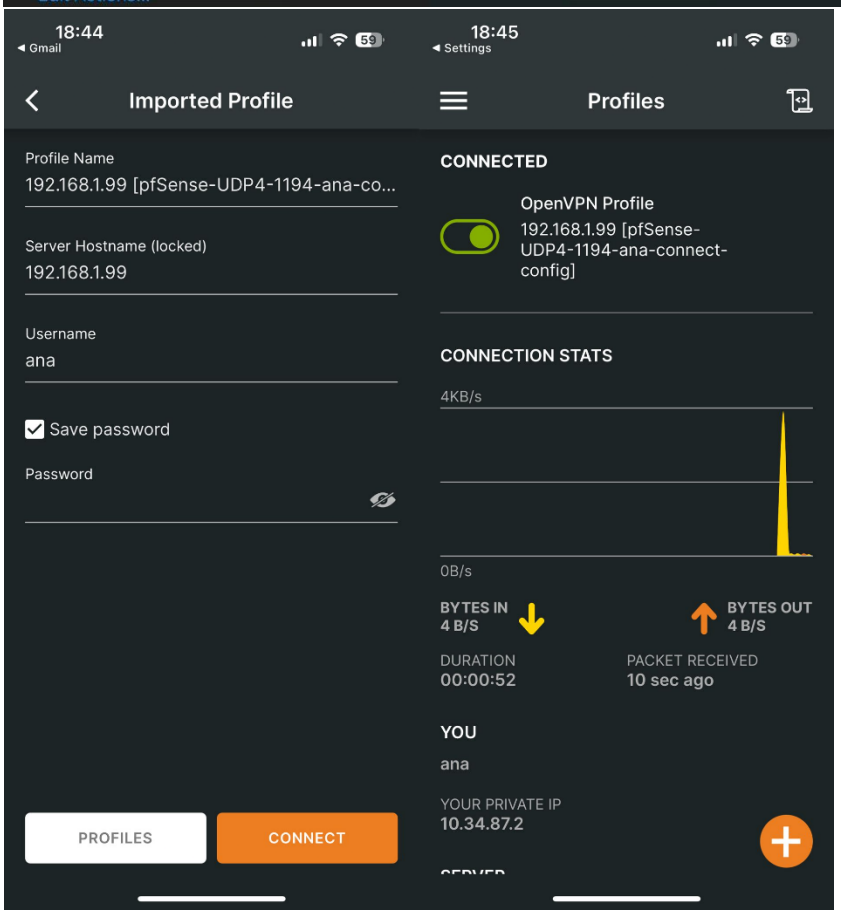


Además necesitaremos el archivo correspondiente al usuario y haremos clic en "OpenVPN Connect (iOS/Android)":



Este archivo me lo enviaré por correo y le daré a compartir > OpenVPN, esto abrirá la aplicación y nos saldrá esta ventana donde pone la IP. Le daremos a añadir.





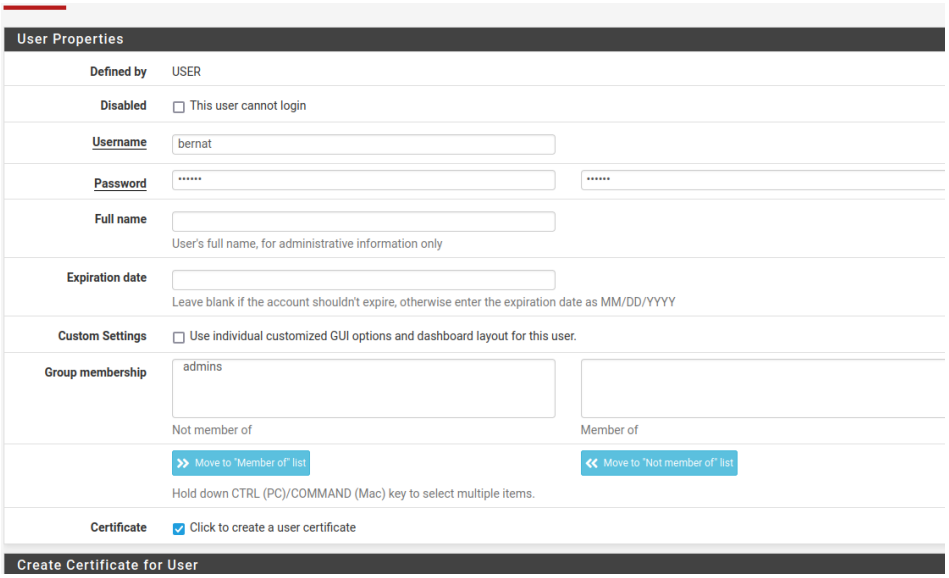
Aquí tendremos que poner nuestras credenciales, las mismas que pusimos en la creación de usuarios.

Una vez conectados tendremos esta ventana donde nos saldrá nuestra IP privada que coincide con la que pusimos, bytes usados en la conexión, etc.

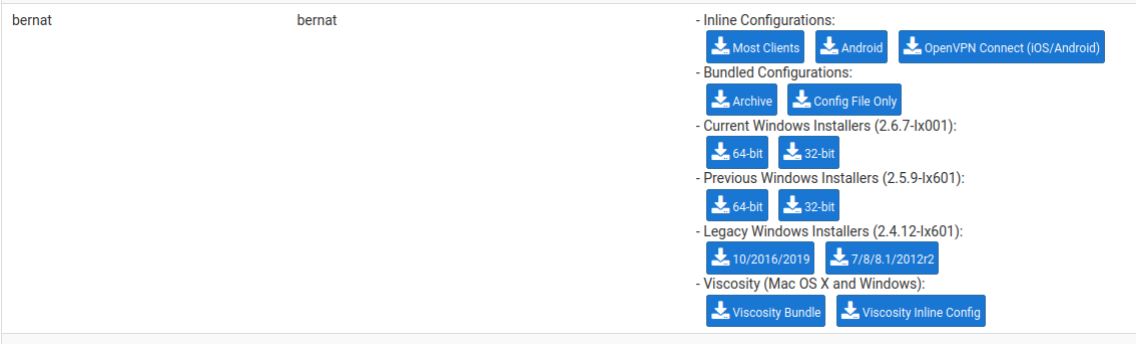
Ahora llega el momento de intentar conectarnos con la IP de la LAN que pusimos que podíamos acceder desde el servidor openVPN:

Creación usuario profesor.

Una vez comprobado que todo funciona vamos a crear un usuario con la contraseña que especifica la práctica y descargaré los archivos.



*NOTA: la contraseña la cambié después al comprobar los requisitos de la práctica.



Conclusión.

Es mi primera vez usando vpn que no sean de pago, me ha parecido algo chulo de hacer sobre todo pensando en una empresa, sería más seguro tener una vpn de todos los trabajadores para que se conecten desde allí mientras teletrabajan desde casa, es mucho más seguro y se podrían enviar archivos de maneras “local” incluso.

También en caso de ser personas que usáramos wifis públicos, sería una manera de mejorar la seguridad personal de nuestras conexiones desde el teléfono móvil/portátil en estas situaciones.