



---

# PFSENSE: VPN CON IPSEC Y SERVIDOR OPENVPN

---

SAD



2ºASIR

I.E.S. ANTONIO MACHADO  
ANA OROZCO ASENSIO

## Contenido

Introducción.....	2
IPSec.....	4
Sevilla.....	4
Reglas Firewall.....	7
Barcelona.....	8
Reglas Firewall.....	10
Reglas Firewall IPSec.....	12
Conexión.....	12
OpenVPN.....	14
Certificados.....	14
Regla Firewall.....	19
Archivos para OpenVPN.....	20
Acceso desde dispositivo móvil.....	23
Creación usuario profesor.....	26
Conclusión.....	27

# 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:

```
Maquina 1 Pfsense [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 962e24916d337543e21f

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> le0      -> v4: 192.168.1.99/24
LAN (lan)      -> le1      -> v4: 10.0.0.1/24
WORKSTATION (opt1) -> le2      -> v4: 10.0.1.1/24

0) Logout (SSH only)      9) pfTop
```

Pfsense 2:

```
Maquina 1 Pfsense 1 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 756ae7ea2e87428c368c

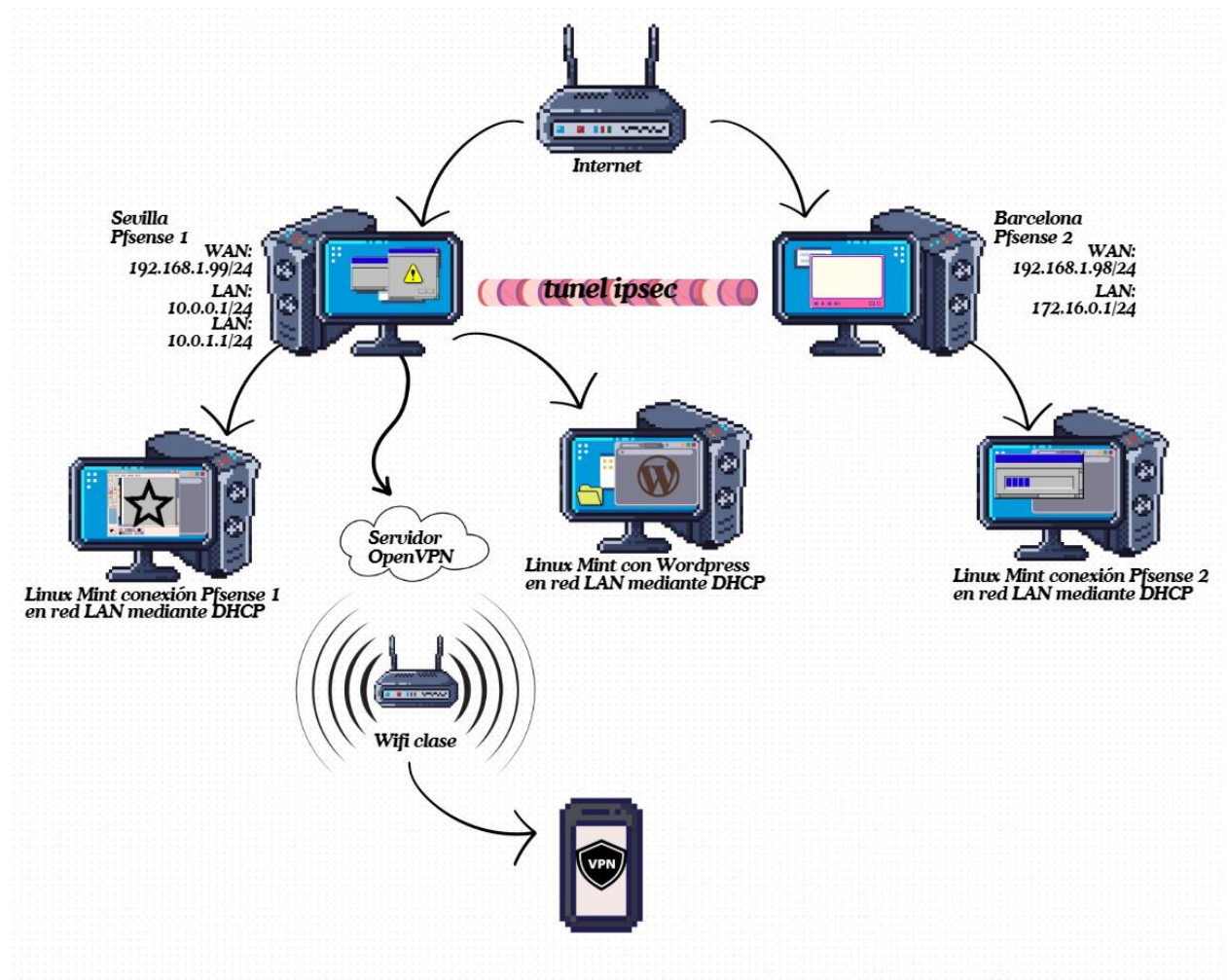
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> le0      -> v4: 192.168.1.98/24
LAN (lan)      -> le1      -> v4: 172.16.0.1/24

0) Logout (SSH only)      9) pfTop
```

\*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.

General Information	
Description	<input type="text" value="Pfsense1ToPfsense2"/> <small>A description may be entered here for administrative reference (not parsed).</small>
Disabled	<input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.

IKE Endpoint Configuration	
Key Exchange version	<input type="text" value="IKEv2"/> <small>Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and acce</small>
Internet Protocol	<input type="text" value="IPv4"/> <small>Select the Internet Protocol family.</small>
Interface	<input type="text" value="WAN"/> <small>Select the interface for the local endpoint of this phase1 entry.</small>
Remote Gateway	<input type="text" value="192.168.1.98"/> <small>Enter the public IP address or host name of the remote gateway. </small>

Phase 1 Proposal (Authentication)	
-----------------------------------	--

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.

**Phase 1 Proposal (Authentication)**

**Authentication Method** Mutual PSK  
Must match the setting chosen on the remote side.

**My identifier** My IP address

**Peer identifier** Peer IP address

**Pre-Shared Key** pfsense  
Enter the Pre-Shared Key string. This key must match on both peers.  
This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.  
[Generate new Pre-Shared Key](#)

**Phase 1 Proposal (Encryption Algorithm)**

**Encryption Algorithm** AES 128 bits SHA256 14 (2048 bit) [Delete](#)  
Algorithm Key length Hash DH Group

Note: SHA1 and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

**Add Algorithm** [+ Add Algorithm](#)

**Expiration and Replacement**

**Life Time** 28800  
Hard IKE SA life time, in seconds, after which the IKE SA will be expired. Must be larger than Rekey Time and Reauth Time. Cannot be set to the same value as Rekey Time or Reauth Time. If left empty, defaults to 110% of whichever timer is higher (reauth or rekey)

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.

10.0.0.1/vpn\_ipsec\_phase2.php?ikeid=1

**Information**

**Description** Pfsense1ToPfsense2  
A description may be entered here for administrative reference (not parsed).

**Disabled** ☐ Disable this phase 2 entry without removing it from the list.

**Mode** Tunnel IPv4

**Phase 1** Pfsense1ToPfsense2 (IKE ID 1)

**Local Network** LAN subnet / 0  
Type Address  
Local network component of this IPsec security association.

**NAT translation** None / 0  
Type Address  
If NAT/BINAT is required on this network specify the address to be translated

**Remote Network** Network 172.16.0.1 / 24  
Type Address  
Remote network component of this IPsec security association.

**Proposal (SA/Key Exchange)**

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.

10.0.0.1/vpn\_ipsec\_phase2.php?ikeid=1

**Life Time** 3600  
Hard Child SA life time, in seconds, after which the Child SA will be expired. Must be larger than Rekey Time. If left empty, defaults to 110% of Rekey Time. If both Life Time and Rekey Time are empty, default is 3600 seconds.

**Rekey Time** 3240  
Time, in seconds, before a Child SA establishes new keys. This works without interruption. (If Rekey Time is empty, it will use a default value of 90% Life Time. If both Life Time and Rekey Time are empty, default is 3240 seconds when rekey is disabled, connections can be interrupted while new Child SA entries are negotiated.)

**Rand Time** 360  
A random value up to this amount will be subtracted from Rekey Time to avoid simultaneous renegotiations. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to denial of service.

**Periodically ping host** 172.16.0.1  
Sends an ICMP echo request inside the tunnel to the specified IP Address. Can trigger initial VTI mode P2.

**Keep Alive** ☐ Enable periodic keep alive check  
Periodically check this P2 and initiate it if disconnected; does not send traffic inside the tunnel. Action\* and works for both VTI and tunnel mode P2s. For IKEv2 without split connections, this option is not applicable.

Guardaremos y aplicaremos cambios.

The changes have been applied successfully.

IPsec Tunnels									
	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/> <a href="#">Disable</a>	1	V2	WAN 192.168.1.98	Mutual PSK -	AES (128 bits)	SHA256	14 (2048 bit)	Pfsense1ToPfsense2	<a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>

	ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions
<input type="checkbox"/> <a href="#">Disable</a>	1	tunnel	LAN	172.16.0.1/24	ESP	AES (128 bits)	SHA256	Pfsense1ToPfsense2	<a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a>

[+ Add P2](#)

[+ Add P1](#) [Delete P1s](#)

**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.

Gateways can be managed by [clicking here](#).

---

### Reserved Networks

---

**Block private networks and loopback addresses** ☐

Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16, RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned off for private address space, too.

---

**Block bogon networks** ☐

Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

---

## 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.

---

**Address Family**

Select the Internet Protocol version this rule applies to.

---

**Protocol**

Choose which IP protocol this rule should match.

---

### Source

---

**Source** ☐ Invert match

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination's default value, **any**.

---

### Destination

---

**Destination** ☐ Invert match

**Destination Port Range**

From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering

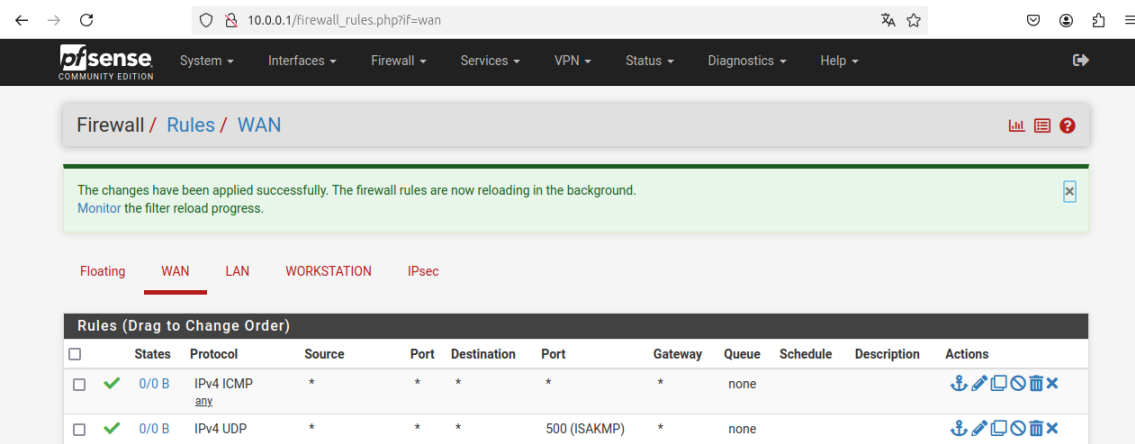
---

### Extra Options

---

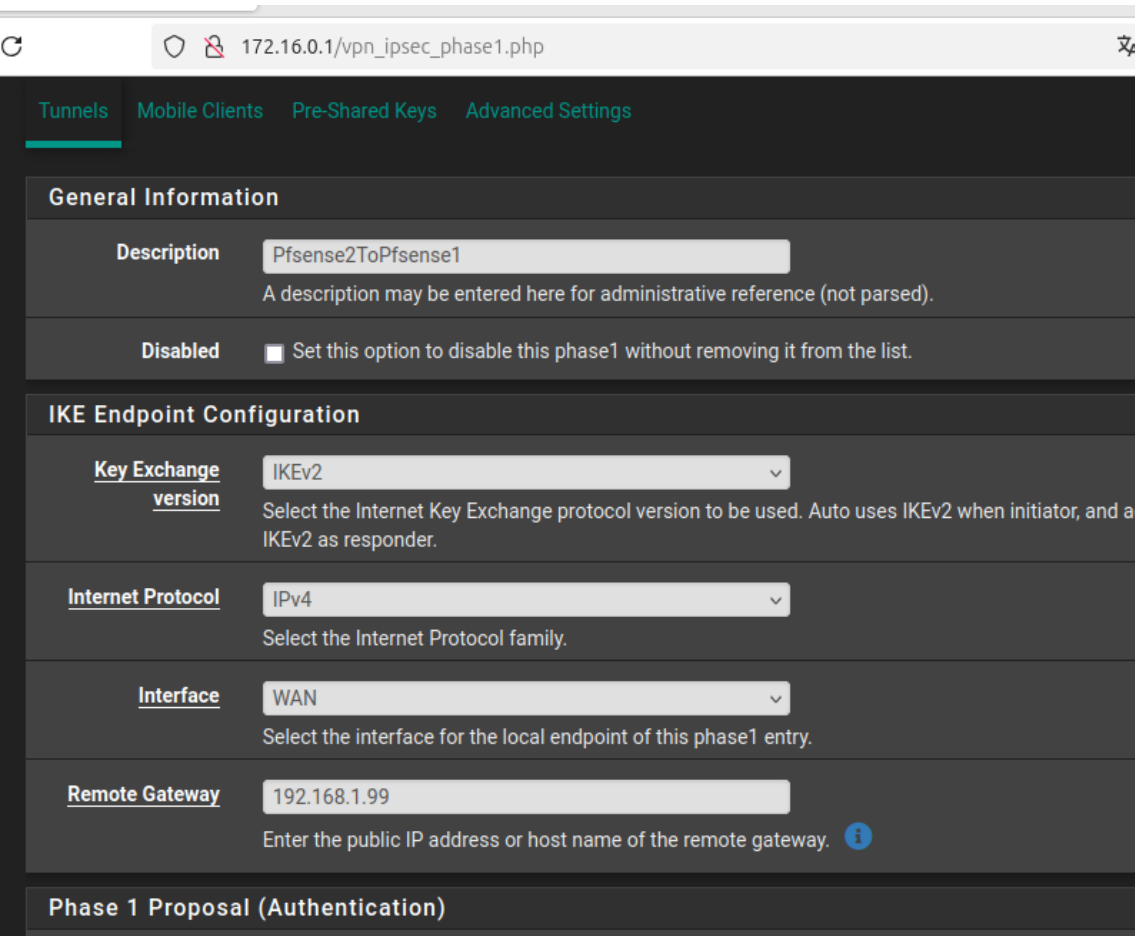


Además, añadiremos otra que permita que hagan ping, que es mediante el protocolo ICMP.



## 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:

The screenshot shows the 'Phase 2' configuration page in Pfsense. The browser address bar shows '172.16.0.1/vpn\_ipsec\_phase2.php?ikeid=1'. The page has a dark theme. At the top, there's a description field. Below it, a 'Disabled' checkbox is unchecked. The 'Mode' is set to 'Tunnel IPv4'. The 'Phase 1' is 'Pfsense2ToPfsense1 (IKE ID 1)'. The 'Networks' section has three rows: 'Local Network' with 'LAN subnet' selected, 'NAT/BINAT translation' set to 'None', and 'Remote Network' with 'Network' selected and '10.0.0.1' entered. The 'Phase 2 Proposal (SA/Key Exchange)' section has 'Protocol' set to 'ESP'. A 'Save' button is at the bottom.

A description may be entered here for administrative reference (not parsed).

**Disabled** ☐ Disable this phase 2 entry without removing it from the list.

**Mode** Tunnel IPv4

**Phase 1** Pfsense2ToPfsense1 (IKE ID 1)

**Networks**

**Local Network** LAN subnet / 0  
Type Address  
Local network component of this IPsec security association.

**NAT/BINAT translation** None / 0  
Type Address  
If NAT/BINAT is required on this network specify the address to be translated

**Remote Network** Network 10.0.0.1 / 24  
Type Address  
Remote network component of this IPsec security association.

**Phase 2 Proposal (SA/Key Exchange)**

**Protocol** ESP  
Encapsulating Security Payload (ESP) performs encryption and authentication, Authentication Header (AH) is authentication only.

**Save**

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

The screenshot shows the bottom part of the 'Phase 2' configuration page. The browser address bar shows '172.16.0.1/vpn\_ipsec\_phase2.php?ikeid=1'. The 'Rekey Time' is set to '3240'. The 'Rand Time' is set to '360'. The 'Keep Alive' section has 'Automatically ping host' set to '10.0.0.1' and 'Keep Alive' checkbox checked. A 'Save' button is at the bottom.

**Rekey Time** 3240  
Time, in seconds, before a Child SA establishes new keys. This works without interruption. Cannot be less than Life Time. Leave blank to use a default value of 90% Life Time. If both Life Time and Rekey Time are set, Rekey Time will be used. Enter a value of 0 to disable, but be aware that when rekey is disabled, connections can be initiated but new SA entries are negotiated.

**Rand Time** 360  
A random value up to this amount will be subtracted from Rekey Time to avoid simultaneous renegotiations. Defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiations can create duplicate security associations.

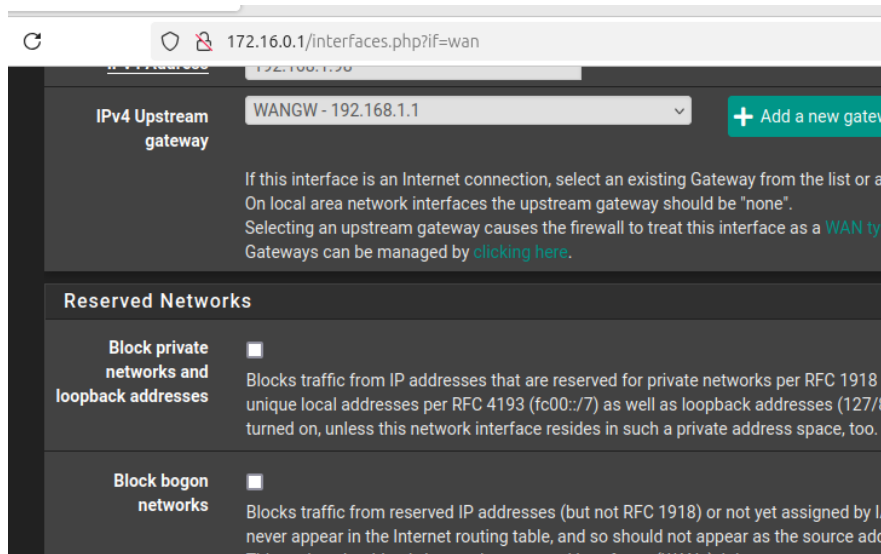
**Keep Alive**

**Automatically ping host** 10.0.0.1  
Sends an ICMP echo request inside the tunnel to the specified IP Address. Can trigger initiation of a new SA if the host does not trigger initiation of a VTI mode P2.

**Keep Alive** ☒ Enable periodic keep alive check  
Periodically check this P2 and initiate it if disconnected; does not send traffic inside the tunnel. This option "Child SA Start Action" and works for both VTI and tunnel mode P2s. For IKEv2 without split tunneling, this option needs to be enabled on one P2.

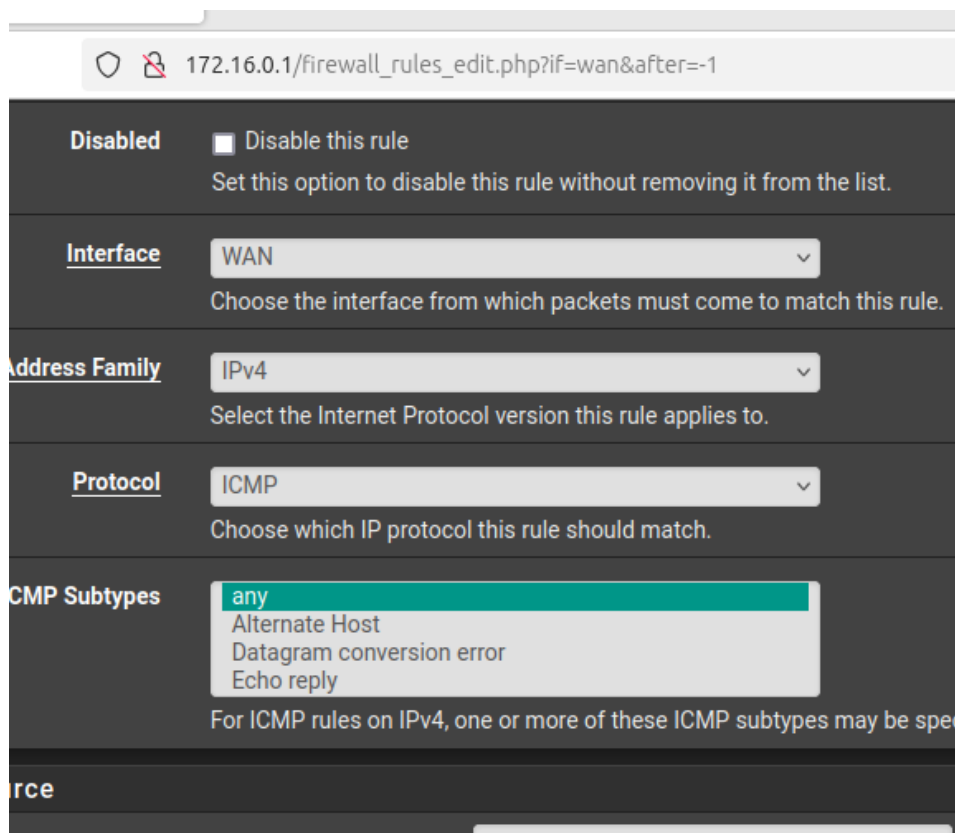
**Save**

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.



172.16.0.1/firewall\_rules\_edit.php?if=wan&after=-1

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** UDP  
Choose which IP protocol this rule should match.

**Source** ☐ Invert match Any

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In this case, this setting must remain at its default value, **any**.

**Destination** ☐ Invert match Any

**Destination Port Range** From ISAKMP (500) Custom To ISAKMP (500)

Specify the destination port or port range for this rule. The "To" field may be left empty.

**Extra Options**

☐ Log Log packets that are handled by this rule

Así quedan las reglas WAN:

172.16.0.1/firewall\_rules.php

pfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

Firewall / Rules / WAN

Floating WAN LAN IPsec

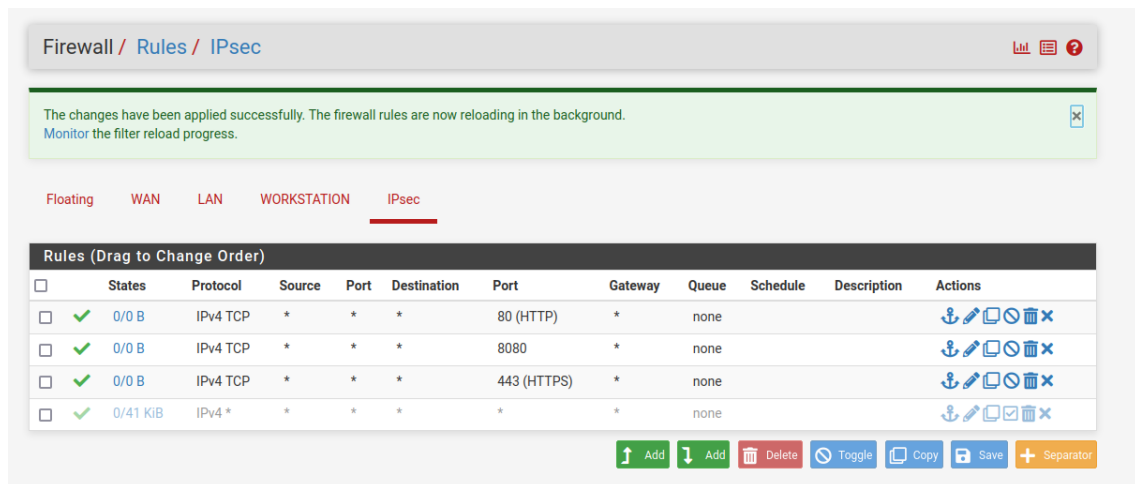
Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 ICMP	*	*	*	*	*	none			<a href="#">↓</a> <a href="#">✎</a> <a href="#">🗑</a> <a href="#">✖</a>
<input type="checkbox"/>	✓ 1/4 KiB	IPv4 UDP	*	*	*	500 (ISAKMP)	*	none			<a href="#">↓</a> <a href="#">✎</a> <a href="#">🗑</a> <a href="#">✖</a>

## Reglas Firewall IPsec.

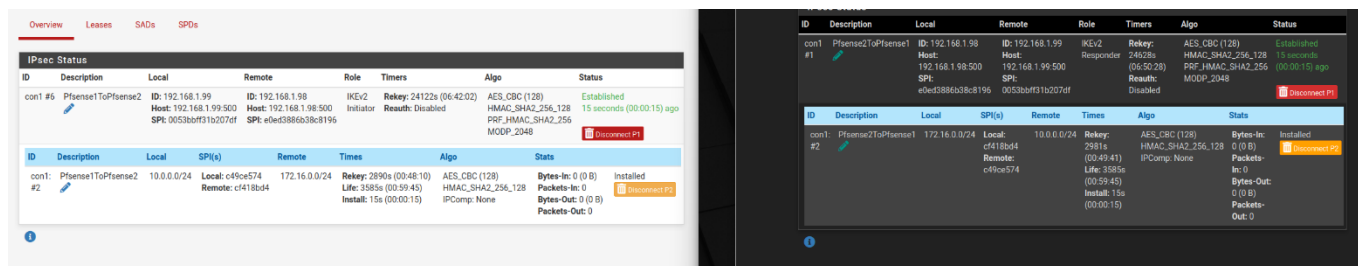
Antes de probar conexión vamos a crear una regla en el firewall de IPsec para que deje pasar todos los protocolos, una vez probada la conexión deshabilitaré esa regla y procedo a hacer reglas para que solo se permita el puerto 80 que es http, el 443 que es https y el 8080 donde tenemos el Wordpress.

\*Este paso lo realicé en ambos Pfsense.



## Conexión.

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

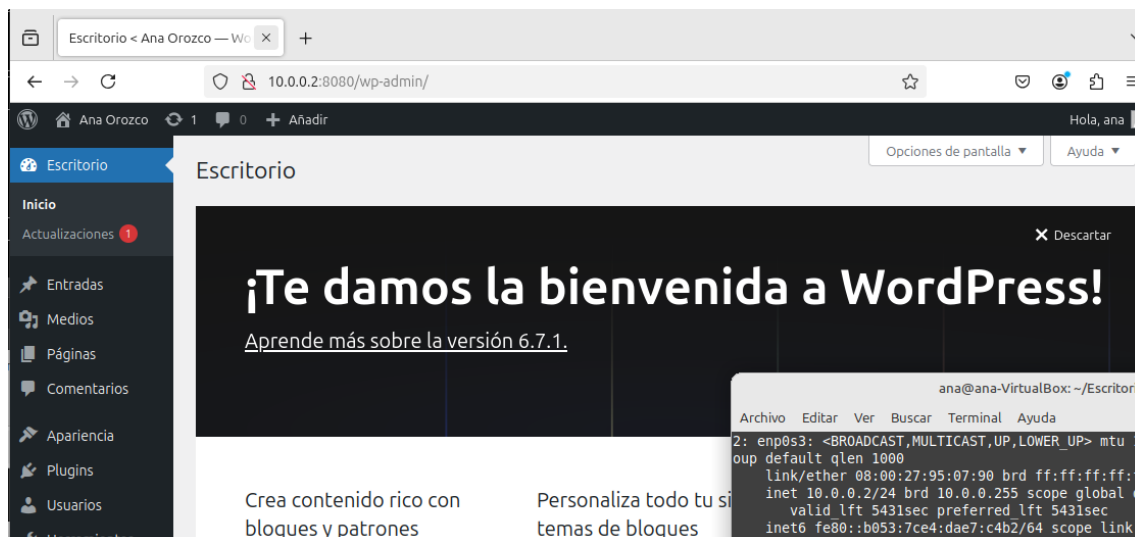


Para comprobar la conexión primero probaré a hacer ping entre ambas:

The image shows two terminal windows from a VirtualBox environment. The left window displays the output of the 'ifconfig' command for the 'enp0s3' interface, showing IP address 172.16.0.1 and other network details. It also shows the output of a 'ping' command to 172.16.0.1. The right window shows the output of the 'ifconfig' command for the 'enp0s3' interface, showing IP address 10.0.0.2 and other network details. It also shows the output of a 'ping' command to 10.0.0.1.

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:

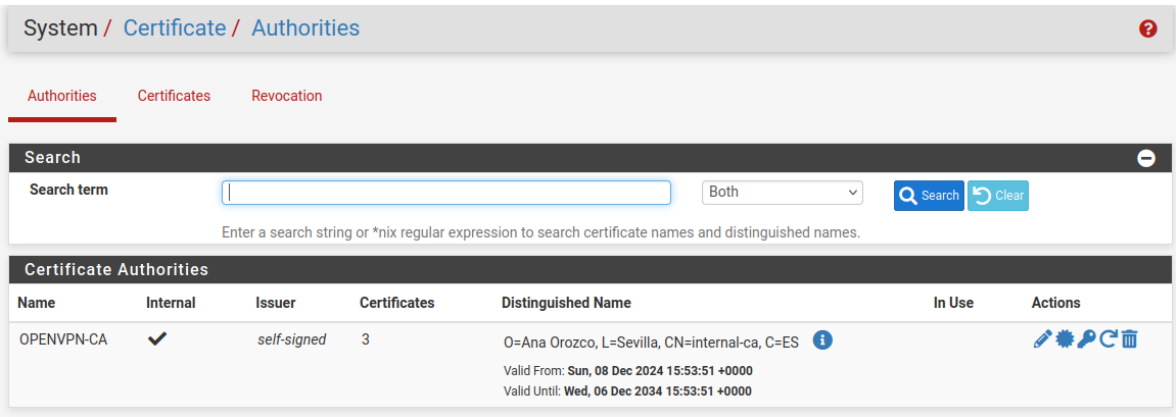


## OpenVPN.

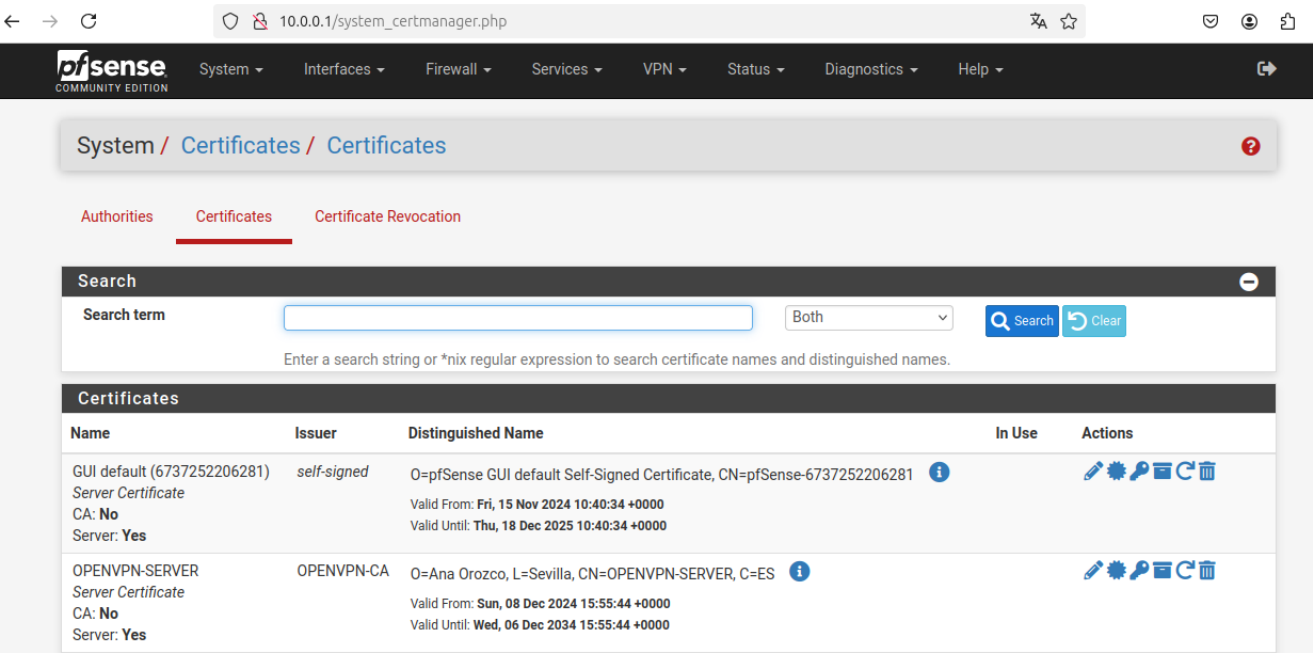
Esta parte de la práctica se hará desde el Pfsense 1 de la sucursal de Sevilla.

## Certificados.

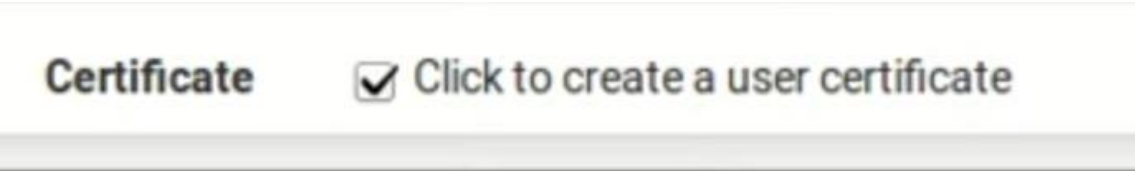
Lo primero que vamos a hacer es crear certificados, para ello iremos a System > Certificate Manager y añadiremos una autoridad certificadora con método interno.



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

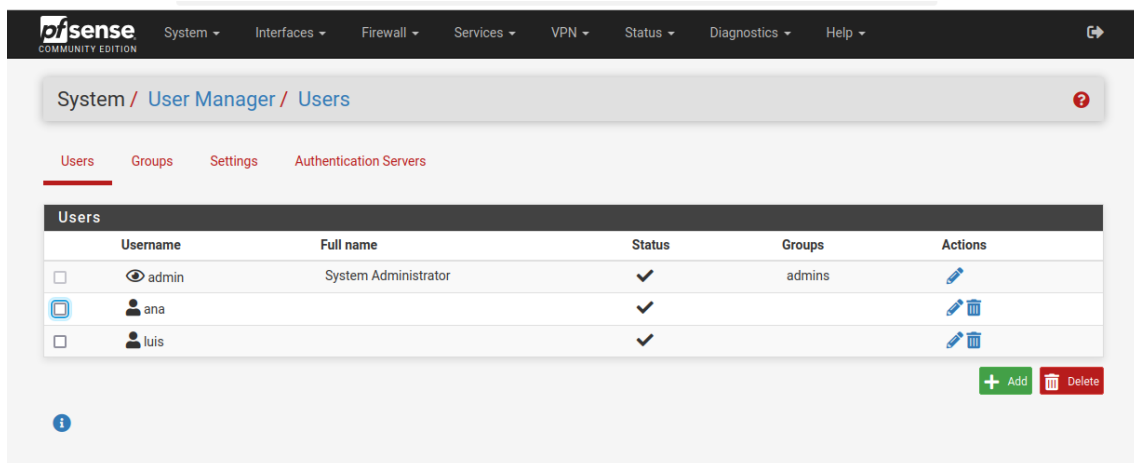


A continuación, vamos a crear las certificaciones de usuario, que para ello hay que crear los usuarios en System > User Manager, aquí crearemos los usuarios que necesitemos con contraseña, grupos, etc. Para crear la certificación solo debemos hacer clic en una opción que dice “Clic para crear certificado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

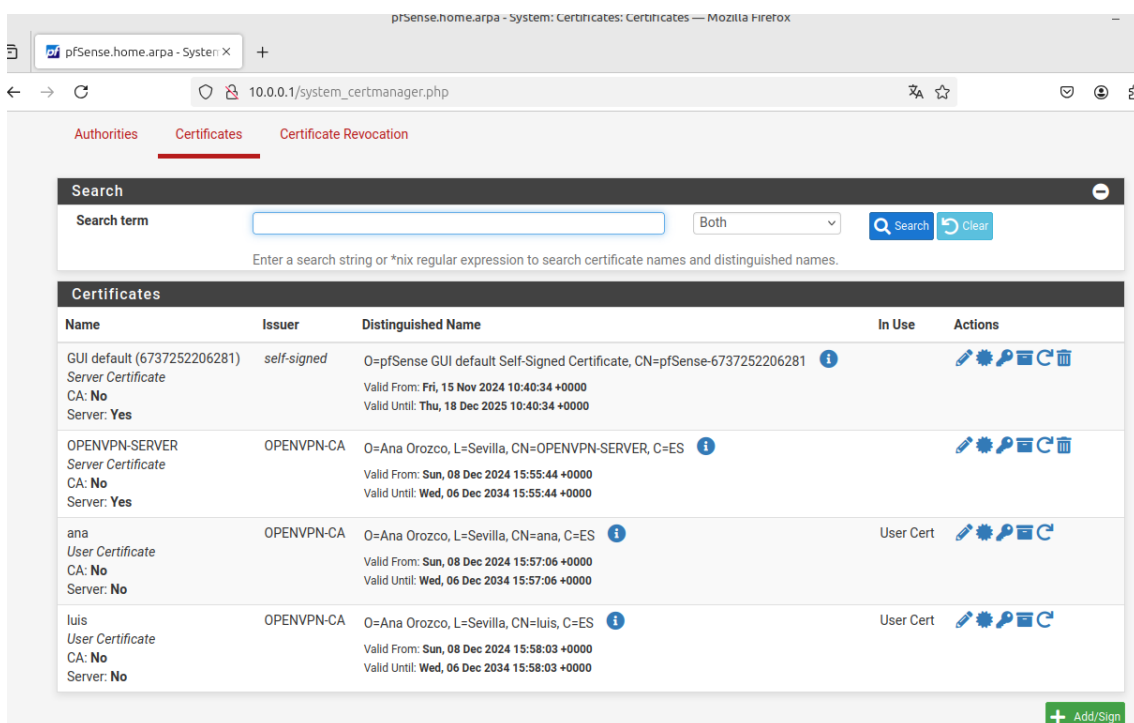


Yo he creado el usuario Ana y otro Luis (más adelante creo el usuario Bernat).





Así se verán los certificados cuando creamos 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 + autenticación de usuario

10.0.0.1/vpn\_openvpn\_server.php?act=new

**Servers** Clients Client Specific Overrides Wizards

### General Information

**Description** VPNsevilla para clientes  
A description of this VPN for administrative reference.

**Disabled** ☐ Disable this server  
Set this option to disable this server without removing it from the list.

### Mode Configuration

**Server mode** Remote Access ( SSL/TLS + User Auth )

**Backend for authentication** Local Database

**Device mode** tun - Layer 3 Tunnel Mode  
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.  
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

### Endpoint Configuration

**Protocol** UDP on IPv4 only

**Interface** WAN  
The interface or Virtual IP address where OpenVPN will receive client connections.

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

10.0.0.1/vpn\_openvpn\_server.php?act=new

This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting them from unauthorized connections. The TLS Key does not have any effect on tunnel data.

☒ Automatically generate a TLS Key.

**Certificate Authority** OPENVPN-CA

**Peer Certificate Revocation list** No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

**OCSP Check** ☐ Check client certificates with OCSP

**Server certificate** OPENVPN-SERVER (Server: Yes, CA: OPENVPN-CA)  
Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using insecure digest algorithms.

**H Parameter Length** 2048 bit  
Diffie-Hellman (DH) parameter set used for key exchange. ⓘ

**ECDH Curve** Use Default  
The Elliptic Curve to use for key exchange.  
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used.

**Data Encryption** AES-128-CBC (128 bit key, 128 bit block) || AES-256-GCM (256 bit key, 128 bit block)  
AES-128-CFB (128 bit key, 128 bit block) || AFS-128-GCM

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

→ 10.0.0.1/vpn\_openvpn\_server.php?act=new

Tunnel Settings

IPv4 Tunnel Network

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.

IPv6 Tunnel Network

This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

Redirect IPv4 Gateway

☐ Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway

☐ Force all client-generated IPv6 traffic through the tunnel.

IPv4 Local network(s)

IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

IPv6 Local network(s)

IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

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

expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

Redirect IPv4 Gateway

☐ Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway

☐ Force all client-generated IPv6 traffic through the tunnel.

IPv4 Local network(s)

IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

IPv6 Local network(s)

IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

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

← → 10.0.0.1/vpn\_openvpn\_server.php

pfSense

COMMUNITY EDITION

System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help

VPN / OpenVPN / Servers

Servers

Clients

Client Specific Overrides

Wizards

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.34.87.0/24	<b>Mode:</b> Remote Access ( SSL/TLS + User Auth ) <b>Data Ciphers:</b> AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC <b>Digest:</b> SHA256 <b>D-H Params:</b> 2048 bits	VPNsevilla para clientes	<div><div></div><div></div><div></div></div>

+

 Add

## 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.

Firewall / Rules / WAN

The changes have been applied successfully. The firewall rules are now reloading in the background. [Monitor the filter reload progress.](#)

Floating **WAN** LAN WORKSTATION IPsec OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 ICMP any	*	*	*	*	*	none			<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a> <a href="#">Toggle</a>
<input type="checkbox"/>	0/81 KIB	IPv4 UDP	*	*	*	500 (ISAKMP)	*	none			<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a> <a href="#">Toggle</a>
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	*	*	10.0.0.24	8080	*	none		NAT	<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a> <a href="#">Toggle</a>
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	192.168.1.32	*	10.0.0.24	22 (SSH)	*	none		NAT	<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a> <a href="#">Toggle</a>
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	10.0.0.24	80 (HTTP)	*	none		NAT	<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a> <a href="#">Toggle</a>
<input type="checkbox"/>	0/0 B	IPv4 UDP	*	*	*	1194 (OpenVPN)	*	none		Servicio OPENVPN	<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a> <a href="#">Toggle</a>

[Add](#) [Add](#) [Delete](#) [Toggle](#) [Copy](#) [Save](#) [Separator](#)

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.

Firewall / Rules / OpenVPN

The changes have been applied successfully. The firewall rules are now reloading in the background. [Monitor the filter reload progress.](#)

Floating WAN LAN WORKSTATION IPsec **OpenVPN**

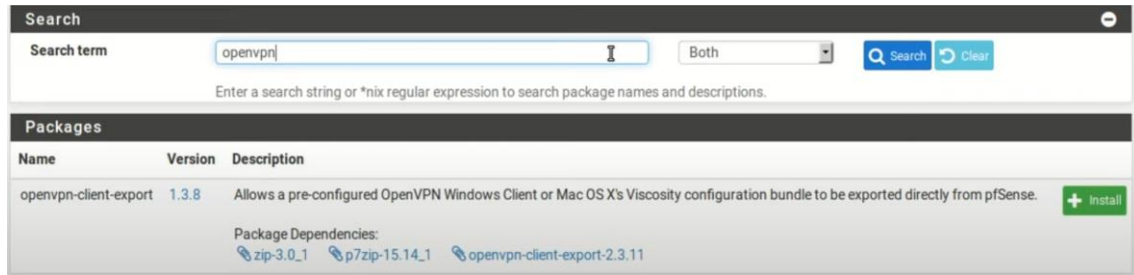
Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 *	*	*	*	*	*	none		Permitir trafico total en OPENVPN	<a href="#">Anchor</a> <a href="#">Edit</a> <a href="#">Copy</a> <a href="#">Delete</a> <a href="#">Toggle</a>

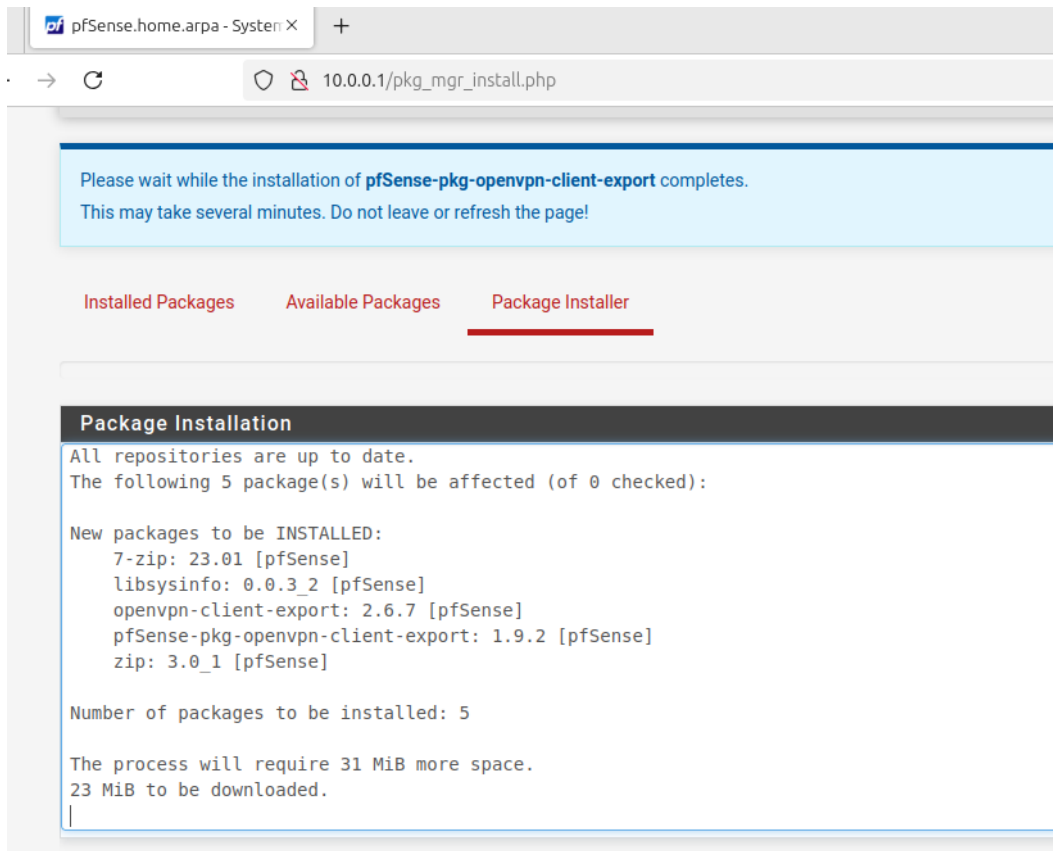
[Add](#) [Add](#) [Delete](#) [Toggle](#) [Copy](#) [Save](#) [Separator](#)

## 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:

10.0.0.1/vpn\_openvpn\_export.php

**OpenVPN / Client Export Utility**

Server Client **Client Specific Overrides** Wizards **Client Export**

**OpenVPN Server**

Remote Access Server VPNsevilla para clientes UDP4:1194

**Client Connection Behavior**

Host Name Resolution Interface IP Address

**Verify Server CN** Automatic - Use verify-x509-name where possible  
Optionally verify the server certificate Common Name (CN) when the client connects.

**Block Outside DNS** ☐ Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.  
Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

**Legacy Client** ☐ Do not include OpenVPN 2.5 and later settings in the client configuration.  
When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.

**Silent Installer** ☐ Create Windows installer for unattended deploy.

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

pfSense.home.arpa - OpenVPN

10.0.0.1/vpn\_openvpn\_export.php

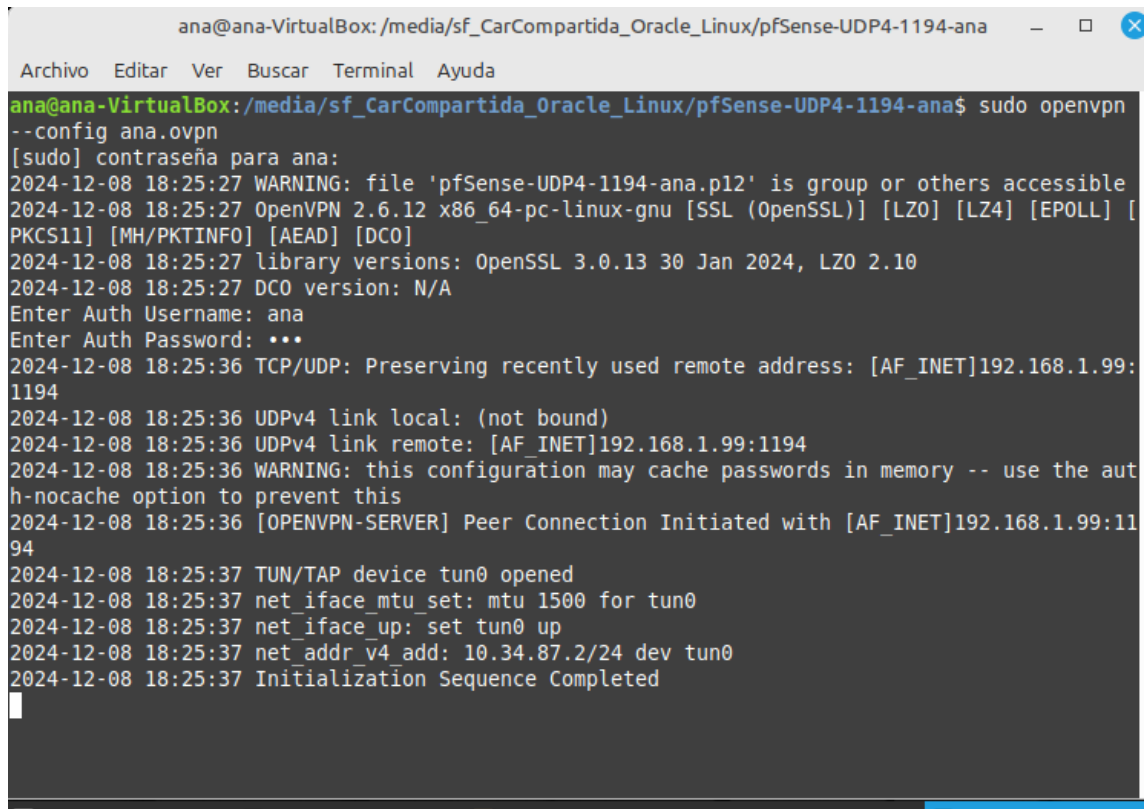
Enter a search string or \*nix regular expression to search.

**OpenVPN Clients**

User	Certificate Name	Export
ana	ana	<p><b>Inline Configurations:</b></p> <p>Most Clients Android OpenVPN Connect (iOS/Android)</p> <p><b>Bundled Configurations:</b></p> <p>Archive Config File Only</p> <p><b>Current Windows Installers (2.6.7-lx001):</b></p> <p>64-bit 32-bit</p> <p><b>Previous Windows Installers (2.5.9-lx601):</b></p> <p>64-bit 32-bit</p> <p><b>Legacy Windows Installers (2.4.12-lx601):</b></p> <p>10/2016/2019 7/8/8.1/2012r2</p> <p><b>Viscosity (Mac OS X and Windows):</b></p> <p>Viscosity Bundle Viscosity Inline Config</p>
luis	luis	<p><b>Inline Configurations:</b></p> <p>Most Clients Android OpenVPN Connect (iOS/Android)</p> <p><b>Bundled Configurations:</b></p> <p>Archive Config File Only</p> <p><b>Current Windows Installers (2.6.7-lx001):</b></p> <p>64-bit 32-bit</p> <p><b>Previous Windows Installers (2.5.9-lx601):</b></p> <p>64-bit 32-bit</p> <p><b>Legacy Windows Installers (2.4.12-lx601):</b></p> <p>10/2016/2019 7/8/8.1/2012r2</p> <p>2 actualizaciones disponibles</p>

dom 8 de dic, 18:02

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.

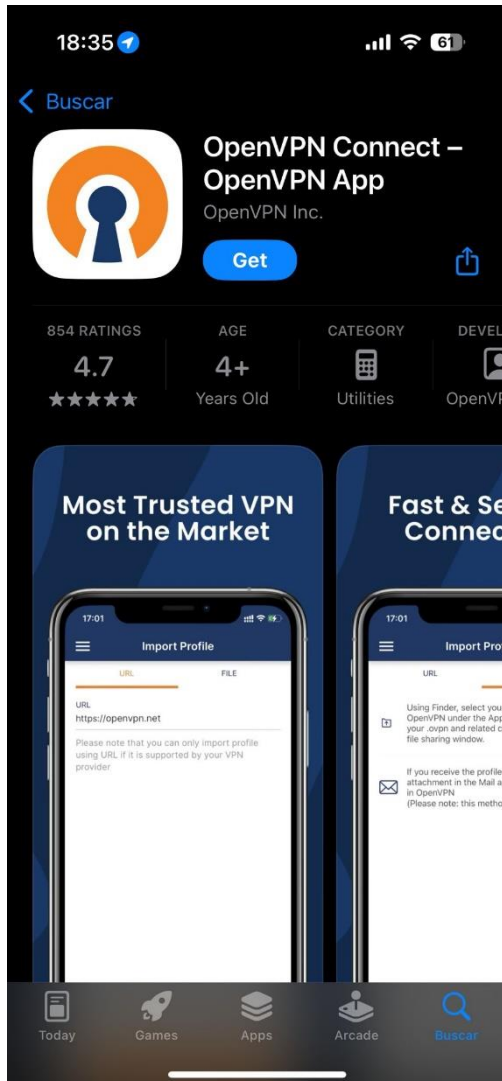


```
ana@ana-VirtualBox: /media/sf_CarCompartida_Oracle_Linux/pfSense-UDP4-1194-ana
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
ana@ana-VirtualBox:/media/sf_CarCompartida_Oracle_Linux/pfSense-UDP4-1194-ana$ sudo openvpn
--config ana.ovpn
[sudo] contraseña para ana:
2024-12-08 18:25:27 WARNING: file 'pfSense-UDP4-1194-ana.p12' is group or others accessible
2024-12-08 18:25:27 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [
PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2024-12-08 18:25:27 library versions: OpenSSL 3.0.13 30 Jan 2024, LZ0 2.10
2024-12-08 18:25:27 DCO version: N/A
Enter Auth Username: ana
Enter Auth Password: ***
2024-12-08 18:25:36 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.1.99:
1194
2024-12-08 18:25:36 UDPv4 link local: (not bound)
2024-12-08 18:25:36 UDPv4 link remote: [AF_INET]192.168.1.99:1194
2024-12-08 18:25:36 WARNING: this configuration may cache passwords in memory -- use the aut
h-nocache option to prevent this
2024-12-08 18:25:36 [OPENVPN-SERVER] Peer Connection Initiated with [AF_INET]192.168.1.99:11
94
2024-12-08 18:25:37 TUN/TAP device tun0 opened
2024-12-08 18:25:37 net_iface_mtu_set: mtu 1500 for tun0
2024-12-08 18:25:37 net_iface_up: set tun0 up
2024-12-08 18:25:37 net_addr_v4 add: 10.34.87.2/24 dev tun0
2024-12-08 18:25:37 Initialization Sequence Completed
```

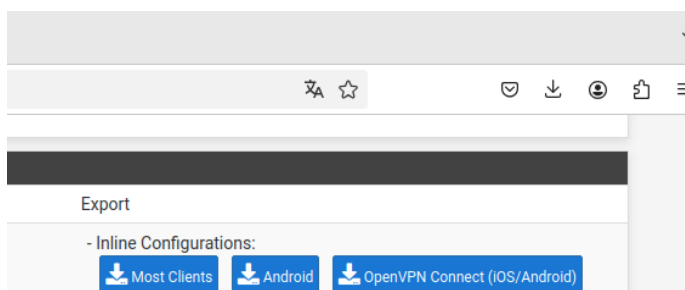
En este caso me pasé el archivo mediante una carpeta compartida existente y al archivo le cambié el nombre para facilitarme la escritura.

## 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:

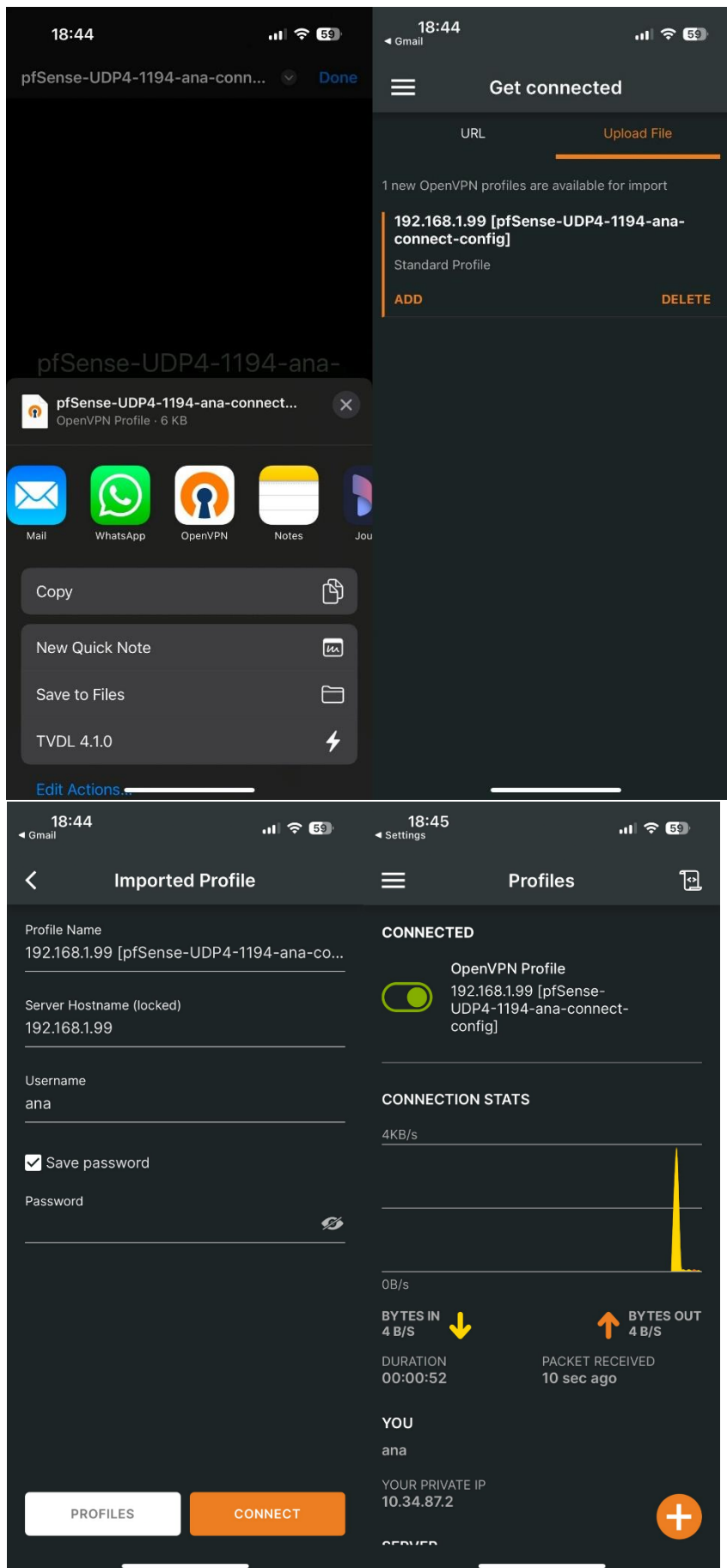


Además necesitaremos el archivo correspondiente al usuario y haremos clic en “OpenVPN Connect (iOS/Android)”:



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.

User Properties

Defined by

USER

Disabled

☐ This user cannot login

Username

bernat

Password

\*\*\*\*\*

\*\*\*\*\*

Full name

User's full name, for administrative information only

Expiration date

Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings

☐ Use individual customized GUI options and dashboard layout for this user.

Group membership

admins

Not member of

Member of

>> Move to "Member of" list

<< Move to "Not member of" list

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Certificate

☒ Click to create a user certificate

Create Certificate for User

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

bernat

bernat

- Inline Configurations:

Most Clients

Android

OpenVPN Connect (iOS/Android)

- Bundled Configurations:

Archive

Config File Only

- Current Windows Installers (2.6.7-lx001):

64-bit

32-bit

- Previous Windows Installers (2.5.9-lx601):

64-bit

32-bit

- Legacy Windows Installers (2.4.12-lx601):

10/2016/2019

7/8/8.1/2012r2

- Viscosity (Mac OS X and Windows):

Viscosity Bundle

Viscosity Inline Config

## 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.