



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:

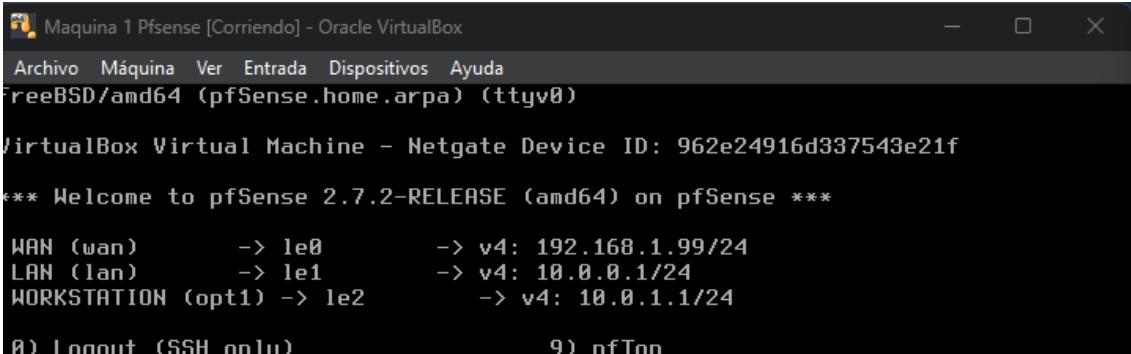
La primera en modo túnel con IPSec usando la máquina de la anterior práctica (que será la sucursal principal en Sevilla) que cuenta con 3 tarjetas de red: una en WAN, y dos LAN. Unida a otra máquina (que será la sucursal de Barcelona) donde tendremos dos tarjetas de red una en WAN y otra en LAN.

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)

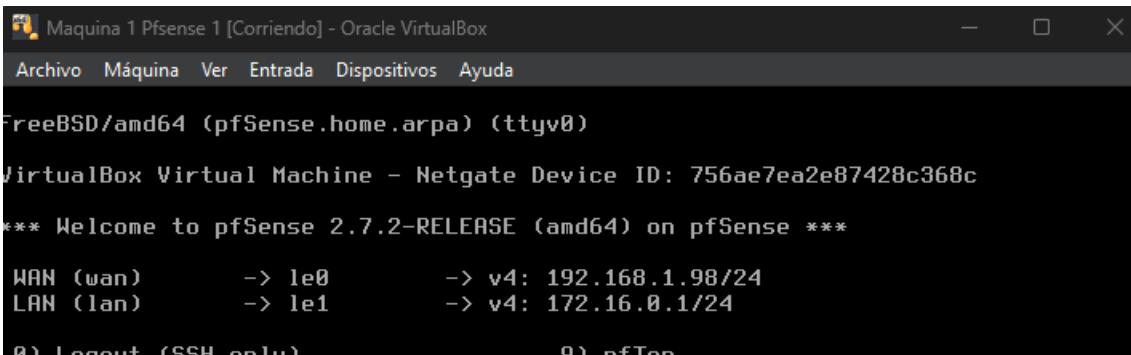
VirtualBox Virtual Machine - Netgate Device ID: 962e24916d337543e21f

*** 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

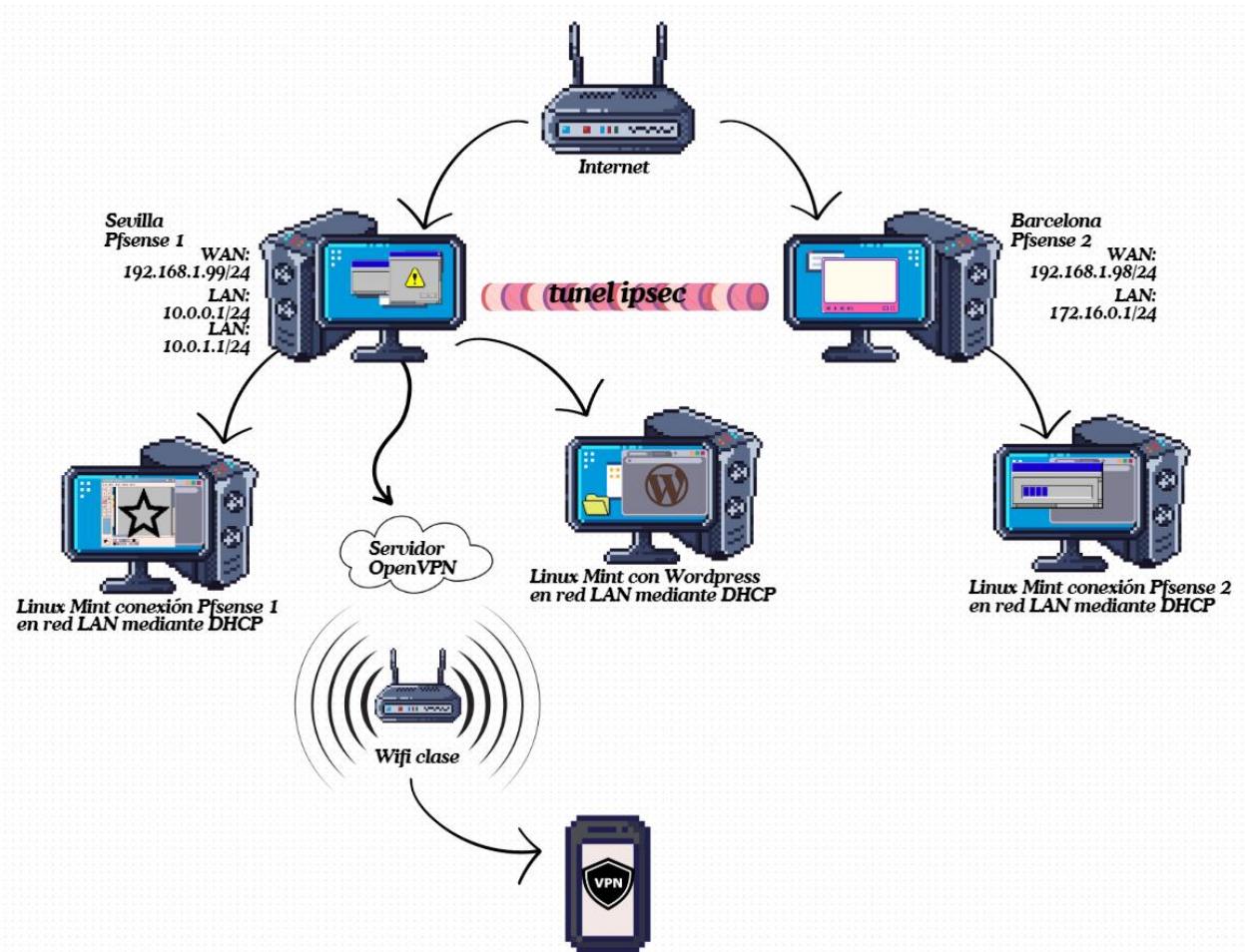
0) Logout (SSH only)         9) pfTop
```

*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	PfSense1ToPfSense2 A description may be entered here for administrative reference (not parsed).
Disabled	<input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.
IKE Endpoint Configuration	
<u>Key Exchange version</u>	IKEv2 Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and acce
<u>Internet Protocol</u>	IPv4 Select the Internet Protocol family.
<u>Interface</u>	WAN Select the interface for the local endpoint of this phase1 entry.
<u>Remote Gateway</u>	192.168.1.98 Enter the public IP address or host name of the remote gateway. i

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 Algorithm	128 bits Key length	SHA256 Hash	14 (2048 bit) DH Group	Delete
-----------------------------	------------------	------------------------	----------------	---------------------------	------------------------

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	<input type="checkbox"/> Disable this phase 2 entry without removing it from the list.
Mode	Tunnel IPv4
Phase 1	Pfsense1ToPfsense2 (IKE ID 1) Edit

Local Network

Type	LAN subnet	Address
------	------------	---------

Local network component of this IPsec security association.

Network Translation

Type	None	Address
------	------	---------

If NAT/BINAT is required on this network specify the address to be translated

Remote Network

Type	Network	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.

The screenshot shows the configuration page for an IPsec tunnel. The URL is 10.0.0.1/vpn_ipsec_phase2.php?ikeid=1. The configuration includes:

- Life Time:** 3600 seconds. Description: 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 seconds. Description: Time, in seconds, before a Child SA establishes new keys. This works without interruption. Can be left empty to use a default value of 90% Life Time. If both Life Time and Rekey Time are empty, default is 3600 seconds. If rekey is disabled, connections can be interrupted while new Child SA entries are negotiated.
- Rand Time:** 360 seconds. Description: 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 duplicate traffic.
- Tunnel IP:** 172.16.0.1. Description: Sends an ICMP echo request inside the tunnel to the specified IP Address. Can trigger initiation in VTI mode P2.
- Keep Alive:** Enable periodic keep alive check. Description: 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 action is disabled.

Guardaremos y aplicaremos cambios.

The screenshot shows the IPsec Tunnels configuration table. It displays one main tunnel entry and a detailed view of its P2 settings. The main table columns are: ID, IKE, Remote Gateway, Auth/Mode, P1 Protocol, P1 Transforms, P1 DH-Group, P1 Description, and Actions. The detailed view table columns are: ID, Mode, Local Subnet, Remote Subnet, P2 Protocol, P2 Transforms, P2 Auth Methods, Description, and P2 actions.

ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
1	V2	WAN 192.168.1.98	Mutual PSK	AES (128 bits)	SHA256	14 (2048 bit)	Pfsense1ToPfsense2	

ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions
1	tunnel	LAN	172.16.0.1/24	ESP	AES (128 bits)	SHA256	Pfsense1ToPfsense2	

[+ Add P2](#) [+ Add P1](#) [Delete P1s](#)

NOTA: será importante en el Firewall de la interfaz WAN que desmarquemos las opciones que bloquean el tráfico 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	
<input type="checkbox"/> Block private networks	<input type="checkbox"/>
<input type="checkbox"/> Block loopback addresses	Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned off as it may interfere with private address space, too.
<input type="checkbox"/> Block bogon networks	<input type="checkbox"/>
	Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are typically listed in the 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	<input type="button" value="IPv4"/>					
Select the Internet Protocol version this rule applies to.						
Protocol	<input type="button" value="UDP"/>					
Choose which IP protocol this rule should match.						
Source						
Source	<input type="checkbox"/> Invert match	<input type="button" value="Any"/>				
<input type="button" value="Display Advanced"/>						
The Source Port Range for a connection is typically random and almost never equal to the destination port. Use the dropdown menu to select its default value, any.						
Destination						
Destination	<input type="checkbox"/> Invert match	<input type="button" value="Any"/>				
Destination Port Range	<input type="button" value="ISAKMP (500)"/>	<input type="button" value="From"/>	<input type="button" value="Custom"/>	<input type="button" value="To"/>	<input type="button" value="ISAKMP (500)"/>	<input type="button" value="To"/>
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering on the source port.						
Extra Options						

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

The screenshot shows the pfSense Firewall Rules configuration. The WAN tab is selected. A message at the top states: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress." Below this, there are tabs for Floating, WAN, LAN, WORKSTATION, and IPsec. The WAN tab is active. A table titled "Rules (Drag to Change Order)" lists two rules:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 ICMP any	*	*	*	*	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	*	*	*	500 (ISAKMP)	*	none			

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.

The screenshot shows the pfSense VPN IPsec Phase 1 configuration. The Tunnels tab is selected. The General Information section includes a Description field set to "Pfsense2ToPfsense1" and a note: "A description may be entered here for administrative reference (not parsed)." The Disabled checkbox is unchecked. The IKE Endpoint Configuration section includes fields for Key Exchange version (IKEv2), Internet Protocol (IPv4), Interface (WAN), and Remote Gateway (192.168.1.99). The Phase 1 Proposal (Authentication) section is also visible.

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

Ahora vamos con la fase dos:

The screenshot shows the configuration for Phase 2 of the IPsec security association. It includes fields for Mode (Tunnel IPv4), Local Network (LAN subnet), NAT/BINAT translation (None), Remote Network (Network 10.0.0.1/24), and Protocol (ESP). A note indicates that ESP performs encryption and authentication, while AH is authentication only.

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

The screenshot shows advanced configuration options for the IPsec Phase 2. It includes fields for Rekey Time (3240 seconds), Rand Time (360 seconds), and Keep Alive settings. Under 'Automatically ping host', the IP address 10.0.0.1 is specified. Under 'Keep Alive', the 'Enable periodic keep alive check' option is selected. A 'Save' button is at the bottom.

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

The screenshot shows the 'interfaces.php?if=wan' page. At the top, it says 'IPv4 Upstream gateway' and 'WANGW - 192.168.1.1'. A button '+ Add a new gateway' is visible. Below this, there is a note about selecting an upstream gateway for an Internet connection. Under the heading 'Reserved Networks', two options are listed: 'Block private networks and loopback addresses' (unchecked) and 'Block bogon networks' (unchecked). Both descriptions mention RFC 1918 and RFC 4193.

Reglas Firewall.

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

The screenshot shows the 'firewall_rules_edit.php?if=wan&after=-1' page. It displays a form for creating a new rule. The 'Disabled' section has a checkbox 'Disable this rule' with the note 'Set this option to disable this rule without removing it from the list.' The 'Interface' dropdown is set to 'WAN'. The 'Address Family' dropdown is set to 'IPv4'. The 'Protocol' dropdown is set to 'ICMP'. In the 'ICMP Subtypes' section, 'any' is selected, and a dropdown menu shows 'Alternate Host', 'Datagram conversion error', and 'Echo reply'. A note at the bottom states 'For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.'

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

Source Invert match Any

Display Advanced
The **Source Port Range** for a connection is typically random and almost never equals the port number specified in the source port field. For this reason, this setting must remain at its default value, **any**.

destination

Destination Invert match Any

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

Specify the destination port or port range for this rule. The "To" field may be left empty if you want to accept all traffic to the specified port.

extra Options

Log Log packets that are handled by this rule

Así quedan las reglas WAN:

172.16.0.1/firewall_rules.php

Firewall / Rules / WAN

Floating **WAN** LAN IPsec

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0/0 B	IPv4 ICMP	*	*	*	*	*	none		 	
<input checked="" type="checkbox"/>	✓ 1/4 KIB	IPv4 UDP	*	*	*	500 (ISAKMP)	*	none		 	

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.

ID	Description	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	HTTP	IPv4 TCP	*	*	*	80 (HTTP)	*	none			
8080		IPv4 TCP	*	*	*		*	none			
443	HTTPS	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			
0/41 KIB	All traffic	IPv4	*	*	*	*	*	none			

Buttons at the bottom: Add, Add, Delete, Toggle, Copy, Save, Separator.

Conexión.

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

ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #1	Pfsense1ToPfsense2	ID: 192.168.1.99 Host: 192.168.1.99.500 SPI: 0053bbf51b207df	ID: 192.168.1.98 Host: 192.168.1.98.500 SPI: e0ed388693b8c8196	Initiator	Rekey: 24122s (06:42:02) Established 15 seconds (00:00:15 ago)	AES_CBC (128) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	Established
con2 #2	Pfsense2ToPfsense1	10.0.0.0/24 Local: c49ce574 Remote: cf418bd4	172.16.0.0/24 Host: 172.16.0.1.99.500 SPI: 0053bbf51b207df	Responder	Rekey: 2890s (00:48:10) Established 15s (00:00:15 ago)	AES_CBC (128) HMAC_SHA2_256_128 IPComp: None	Established

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

```

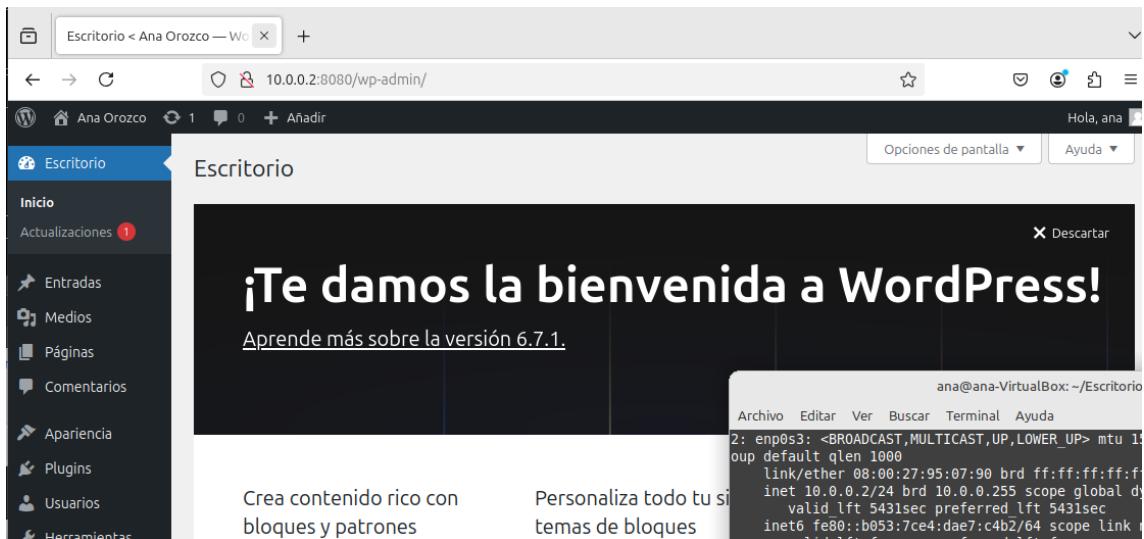
ana@ana-VirtualBox:~ Archivo Editar Ver Buscar Terminal Ayuda
t qlen 1000
link/Loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
    valid lft forever preferred lft forever
inet6 ::1/128 scope host noprefixroute
    valid lft forever preferred lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
link/ether 08:00:27:91:cd:5d brd ff:ff:ff:ff:ff:ff
inet 10.0.0.4/24 brd 10.0.0.255 scope global dynamic noprefixroute enp0s3
    valid lft 7115sec preferred lft 7115sec
inet6 fe80::aabb:1804%enp0s3/64 scope link noprefixroute
    valid lft forever preferred lft forever
ana@ana-VirtualBox:~$ ping 172.16.0.1
PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data.
64 bytes from 172.16.0.1: icmp_seq=1 ttl=63 time=1.40 ms
64 bytes from 172.16.0.1: icmp_seq=2 ttl=63 time=1.34 ms
64 bytes from 172.16.0.1: icmp_seq=3 ttl=63 time=1.63 ms
64 bytes from 172.16.0.1: icmp_seq=4 ttl=63 time=1.37 ms
^C
--- 172.16.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 1.338/1.432/1.625/0.113 ms
ana@ana-VirtualBox:~$
```

```

ana@ana-VirtualBox:~ Archivo Editar Ver Buscar Terminal Ayuda
link/Loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
    valid lft forever preferred lft forever
inet6 ::1/128 scope host noprefixroute
    valid lft forever preferred lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
link/ether 08:00:27:b4:30:14 brd ff:ff:ff:ff:ff:ff
inet 172.16.0.100/24 brd 172.16.0.255 scope global dynamic noprefixroute enp
0s3
    valid lft 6214sec preferred lft 6214sec
inet6 fe80::b722:b79d:fic:a693/64 scope link noprefixroute
    valid lft forever preferred lft forever
ana@ana-VirtualBox:~$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=63 time=1.41 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=63 time=1.59 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=63 time=1.57 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=63 time=1.47 ms
^C
--- 10.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.411/1.511/1.592/0.074 ms
ana@ana-VirtualBox:~$
```

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 parecen 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:

The screenshot shows a web browser window with two tabs: 'pfSense.home.arpa - Status' and 'Ana Orozco'. The 'Ana Orozco' tab displays a blog post by Ana Orozco titled 'Blog'. The post content is: '¡Hola, mundo!' followed by the text 'Te damos la bienvenida a WordPress. ¡Luego empieza a escribir!'. Below the post is the date '7 de diciembre de 2024'. To the right of the browser is a terminal window titled 'ana@ana-VirtualBox: ~' showing the output of the command 'ip a'. The terminal output includes details about interfaces lo, enp0s3, and enp0s3:0s3.

```
ana@ana-VirtualBox:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 0.0.0.0 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 brd 0.0.0.0 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
    qlen 1000
        link/ether 08:00:27:b4:30:14 brd ff:ff:ff:ff:ff:ff
        inet 172.16.0.106/24 brd 172.16.0.255 scope global dynamic nop
            valid_lft 7031sec preferred_lft 7031sec
            inet6 fe80::b722:b79d:f1c:a693/64 brd fe80::ff:ffff:ffff:ffff scope link noprefixroute
                valid_lft forever preferred_lft forever
ana@ana-VirtualBox:~$
```

OpenVPN.

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

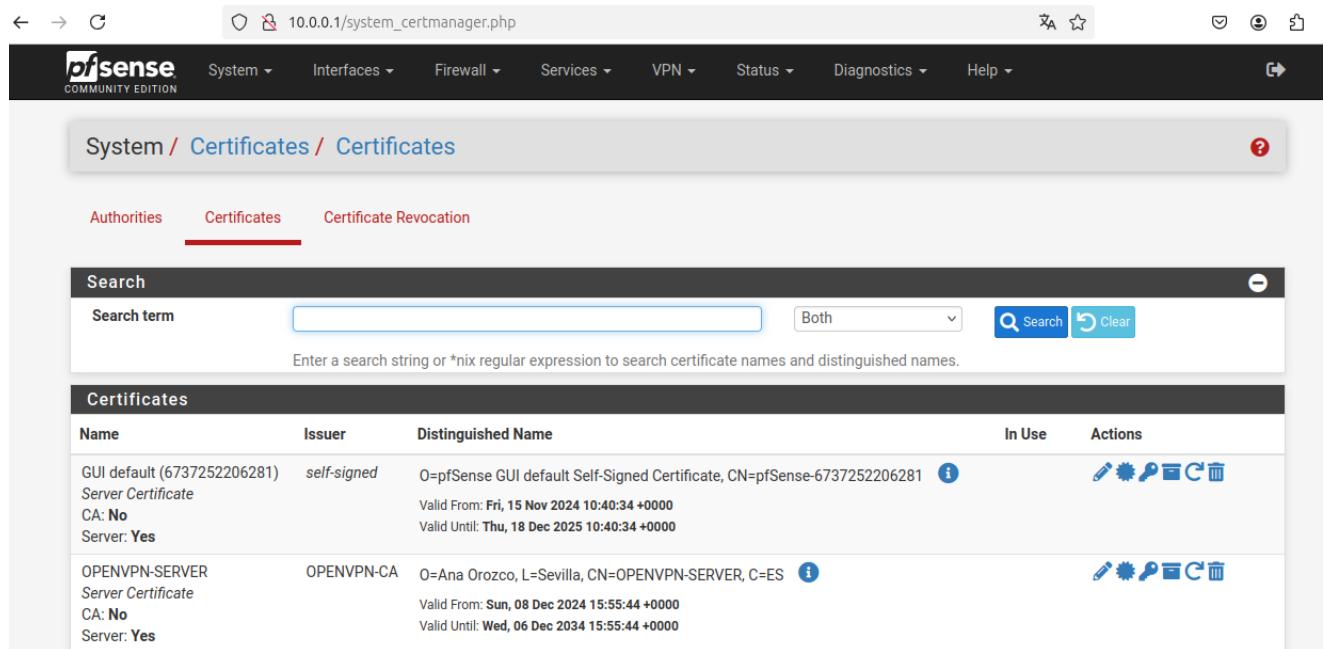
Certificados.

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

The screenshot shows the 'System / Certificate / Authorities' page. The 'Authorities' tab is selected. At the top, there is a search bar with fields for 'Search term' and 'Both'. Below the search bar is a table titled 'Certificate Authorities' with columns: Name, Internal, Issuer, Certificates, Distinguished Name, In Use, and Actions. One row is visible: 'OPENVPN-CA' (Internal), 'self-signed' (Issuer), 3 (Certificates), 'O=Ana Orozco, L=Sevilla, CN=internal-ca, C=ES' (Distinguished Name), 'In Use' (status), and 'Edit, Delete, Recycle' (Actions).

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
OPENVPN-CA	✓	self-signed	3	O=Ana Orozco, L=Sevilla, CN=internal-ca, C=ES	i	

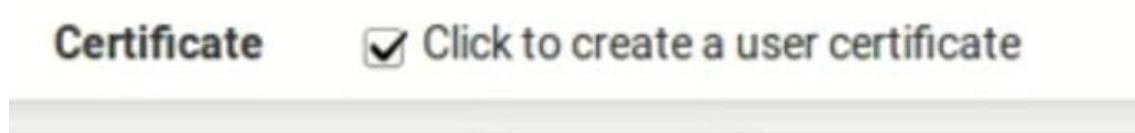
Ahora en esta misma ventana seleccionaremos Certificates donde crearemos un certificado de tipo servidor:



The screenshot shows the pfSense web interface at the URL 10.0.0.1/system_certmanager.php. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main title is "System / Certificates / Certificates". Below the title, there are three tabs: Authorities, Certificates (which is selected), and Certificate Revocation. A search bar allows for searching by "Search term" and "Both" (file and database). The main table lists two certificates:

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (6737252206281) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-6737252206281	<small>i</small>	<small>edit</small> <small>key</small> <small>cert</small> <small>ca</small>
OPENVPN-SERVER Server Certificate CA: No Server: Yes	OPENVPN-CA	O=Ana Orozco, L=Sevilla, CN=OPENVPN-SERVER, C=ES	<small>i</small>	<small>edit</small> <small>key</small> <small>cert</small> <small>ca</small>

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).

The screenshot shows the pfSense User Manager interface. At the top, there are navigation links: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the header, the path is System / User Manager / Users. There are tabs for Users, Groups, Settings, and Authentication Servers, with 'Users' being the active tab. A table lists three users:

Username	Full name	Status	Groups	Actions
admin	System Administrator	✓	admins	Edit Delete
ana		✓		Edit Delete
luis		✓		Edit Delete

At the bottom right of the table are buttons for '+ Add' and 'Delete'.

Así se verán los certificados cuando creamos los usuarios:

The screenshot shows the pfSense Certificates manager interface. The URL is 10.0.0.1/system_certmanager.php. The 'Certificates' tab is selected. A search bar at the top allows searching by 'Search term' and 'Both' (certificates or distinguished names). Below is a table of certificates:

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (6737252206281) <i>Server Certificate</i> CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-6737252206281	Info	Edit Delete Import Export
OPENVPN-SERVER <i>Server Certificate</i> CA: No Server: Yes	OPENVPN-CA	O=Ana Orozco, L=Sevilla, CN=OPENVPN-SERVER, C=ES	Info	Edit Delete Import Export
ana <i>User Certificate</i> CA: No Server: No	OPENVPN-CA	O=Ana Orozco, L=Sevilla, CN=ana, C=ES	User Cert Info	Edit Delete Import Export
luis <i>User Certificate</i> CA: No Server: No	OPENVPN-CA	O=Ana Orozco, L=Sevilla, CN=luis, C=ES	User Cert Info	Edit Delete Import Export

At the bottom right of the table is a button for '+ Add/Sign'.

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

pfSense.home.arpa - VPN: Cx

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	<input type="checkbox"/> 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.

ise.home.arpa - VPN: Cx

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

Certificate Authority	OPENVPN-CA
-----------------------	------------

Peer Certificate Revocation list

Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
----------------------------------	---

OCSP Check

OCSP Check	<input type="checkbox"/> Check client certificates with OCSP
------------	--

Server certificate

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 in digest algorithms.	

H Parameter Length

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

ECDH Curve

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

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

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

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)

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.

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards

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

+ 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.

The screenshot shows the pfSense Firewall Rules configuration page for the WAN interface. The title bar indicates the URL is 10.0.0.1/firewall_rules.php?if=wan. The main content area displays a table of rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 ICMP any	*	*	*	*	*			none	
0/81 KIB	IPv4 UDP	*	*	*	500 (ISAKMP)	*			none	
0/0 B	IPv4 TCP/UDP	*	*	10.0.0.24	8080	*			NAT	
0/0 B	IPv4 TCP/UDP	192.168.1.32	*	10.0.0.24	22 (SSH)	*			NAT	
0/0 B	IPv4 TCP	*	*	10.0.0.24	80 (HTTP)	*			NAT	
0/0 B	IPv4 UDP	*	*	*	1194 (OpenVPN)	*			Servicio OPENVPN	

At the bottom of the table, there are several action buttons: Add, Delete, Toggle, Copy, Save, and 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.

The screenshot shows the pfSense Firewall Rules configuration page for the OpenVPN interface. The title bar indicates the URL is 10.0.0.1/firewall_rules.php?if=openvpn. The main content area displays a table of rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 *	*	*	*	*	*	*		Permitir tráfico total en OPENVPN	

At the bottom of the table, there are several action buttons: Add, Delete, Toggle, Copy, Save, and 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:

The screenshot shows the pfSense Package Manager interface. In the search bar, 'openvpn' is typed. Below the search bar, there's a message: 'Enter a search string or *nix regular expression to search package names and descriptions.' The main area is titled 'Packages' and contains a table with columns: Name, Version, and Description. One row is shown for 'openvpn-client-export' version 1.3.8, which is described as allowing a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense. It has dependencies on 'zip-3.0_1', 'p7zip-15.14_1', and 'openvpn-client-export-2.3.11'. A green 'Install' button is visible next to the package name.

Comenzará la descarga e instalación:

The screenshot shows a browser window on a pfSense system. The address bar shows the URL '10.0.0.1/pkg_mgr_install.php'. The page content indicates that the installation of 'pfSense-pkg-openvpn-client-export' is in progress, with a note: 'Please wait while the installation of pfSense-pkg-openvpn-client-export completes. This may take several minutes. Do not leave or refresh the page!'. Below this, there are tabs for 'Installed Packages', 'Available Packages', and 'Package Installer', with 'Package Installer' being the active tab. The main area is titled 'Package Installation' and displays the following information: 'All repositories are up to date.', 'The following 5 package(s) will be affected (of 0 checked):', 'New packages to be INSTALLED:', and a list of packages: '7-zip: 23.01 [pfSense]', 'libsysinfo: 0.0.3_2 [pfSense]', 'openvpn-client-export: 2.6.7 [pfSense]', 'pfSense-pkg-openvpn-client-export: 1.9.2 [pfSense]', and 'zip: 3.0_1 [pfSense]'. It also states 'Number of packages to be installed: 5' and 'The process will require 31 MiB more space. 23 MiB to be downloaded.'

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

The screenshot shows the pfSense OpenVPN Client Export Utility interface. At the top, there are tabs for Server, Client, Client Specific Overrides, Wizards, and Client Export (which is highlighted). Below this, the 'OpenVPN Server' section is visible, showing a dropdown for 'Remote Access Server' set to 'VPNsevilla para clientes UDP4:1194'. The 'Client Connection Behavior' section contains several configuration options:

- Host Name Resolution:** Set to 'Interface IP Address'.
- Verify Server CN:** Set to 'Automatic - Use verify-x509-name where possible'. A note below says: 'Optionally verify the server certificate Common Name (CN) when the client connects.'
- Block Outside DNS:** An unchecked checkbox with a note: '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:** An unchecked checkbox with a note: '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:** An unchecked checkbox with a note: 'Create Windows installer for unattended deploy.'

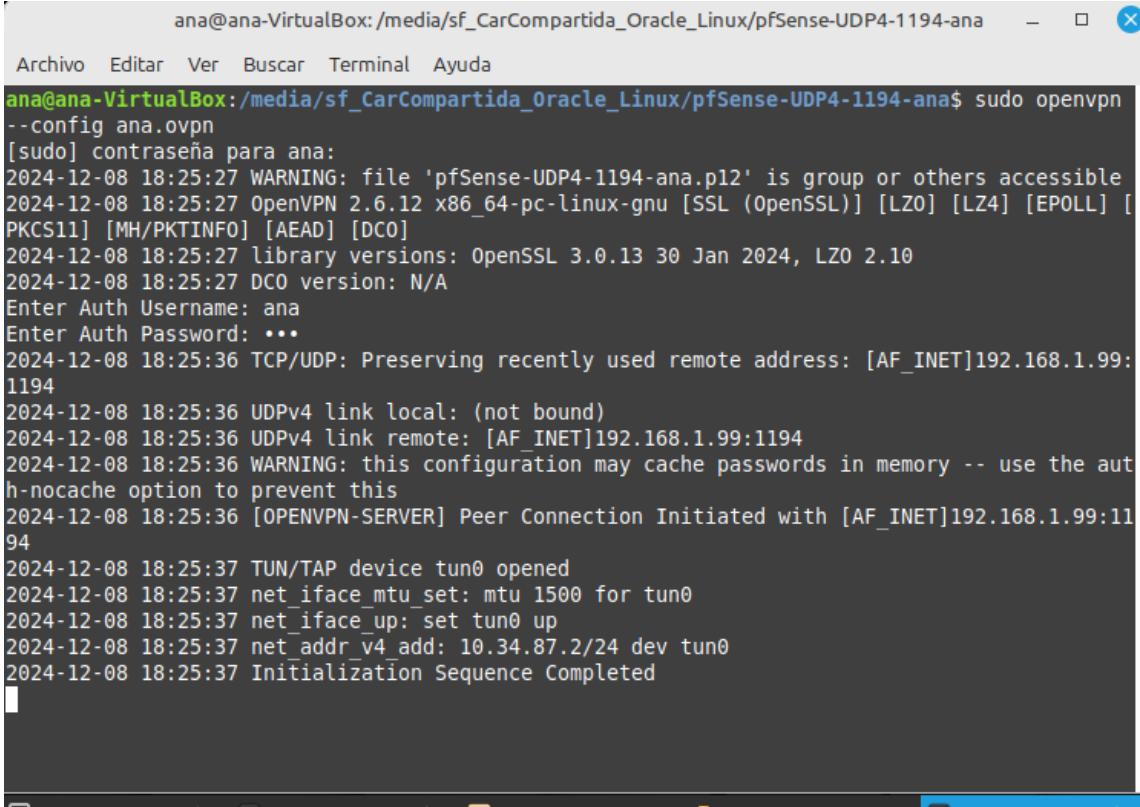
Bajaremos y tendremos una lista con los usuarios y sus archivos para conexión:

The screenshot shows the pfSense OpenVPN Clients interface. It lists two users: 'ana' and 'luis'. For each user, it shows their 'User' name and 'Certificate Name'. To the right, there is a 'Export' section with several download links:

- ana:**
 - 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](#), [7/8/8.1/2012/r2](#)
 - Viscosity (Mac OS X and Windows): [Viscosity Bundle](#), [Viscosity Inline Config](#)
- luis:**
 - 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](#), [7/8/8.1/2012/r2](#)
 - Viscosity (Mac OS X and Windows): [Viscosity Bundle](#), [Viscosity Inline Config](#)

A blue box highlights the '2 actualizaciones disponibles' link at the bottom right of the luis section.

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.

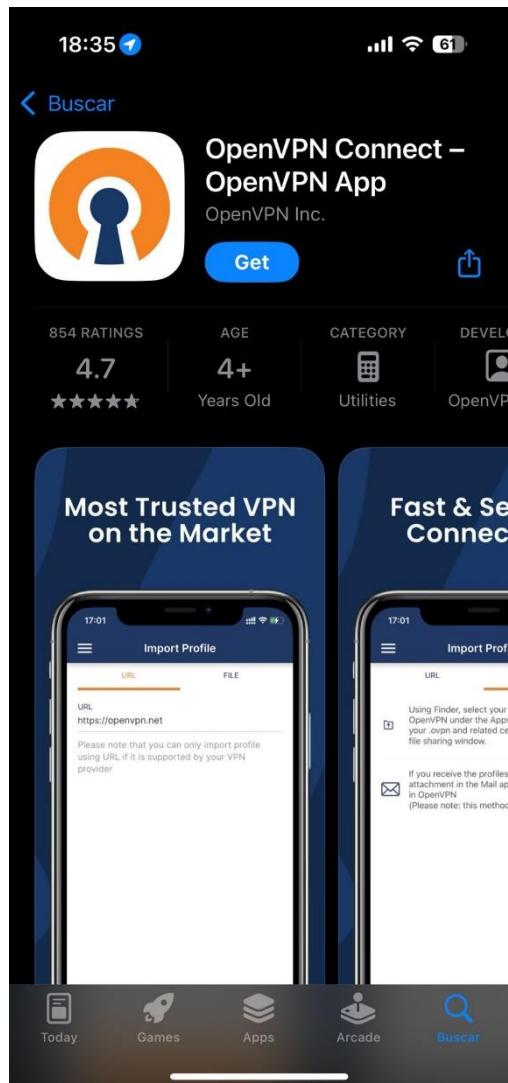


```
ana@ana-VirtualBox:/media/sf_CarCompartida_Oracle_Linux/pfSense-UDP4-1194-ana - □ X
Archivo Editar Ver Buscar Terminal Ayuda
ana@ana-VirtualBox:/media/sf_CarCompartida_Oracle_Linux/pfSense-UDP4-1194-ana$ sudo openvpn
--config ana.ovpn
[sudo] contraseña para ana:
2024-12-08 18:25:27 WARNING: file '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, LZO 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 auth-nocache option to prevent this
2024-12-08 18:25:36 [OPENVPN-SERVER] Peer Connection Initiated with [AF_INET]192.168.1.99:1194
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
```

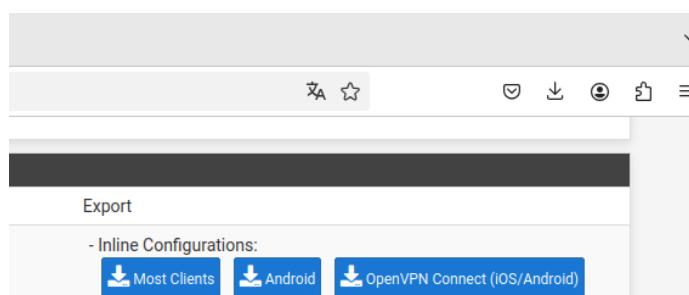
En este caso me pasé el archivo mediante una carpeta compartida existente y al archivo le cambié el nombre para facilitarme la escritura.

Acceso desde dispositivo móvil.

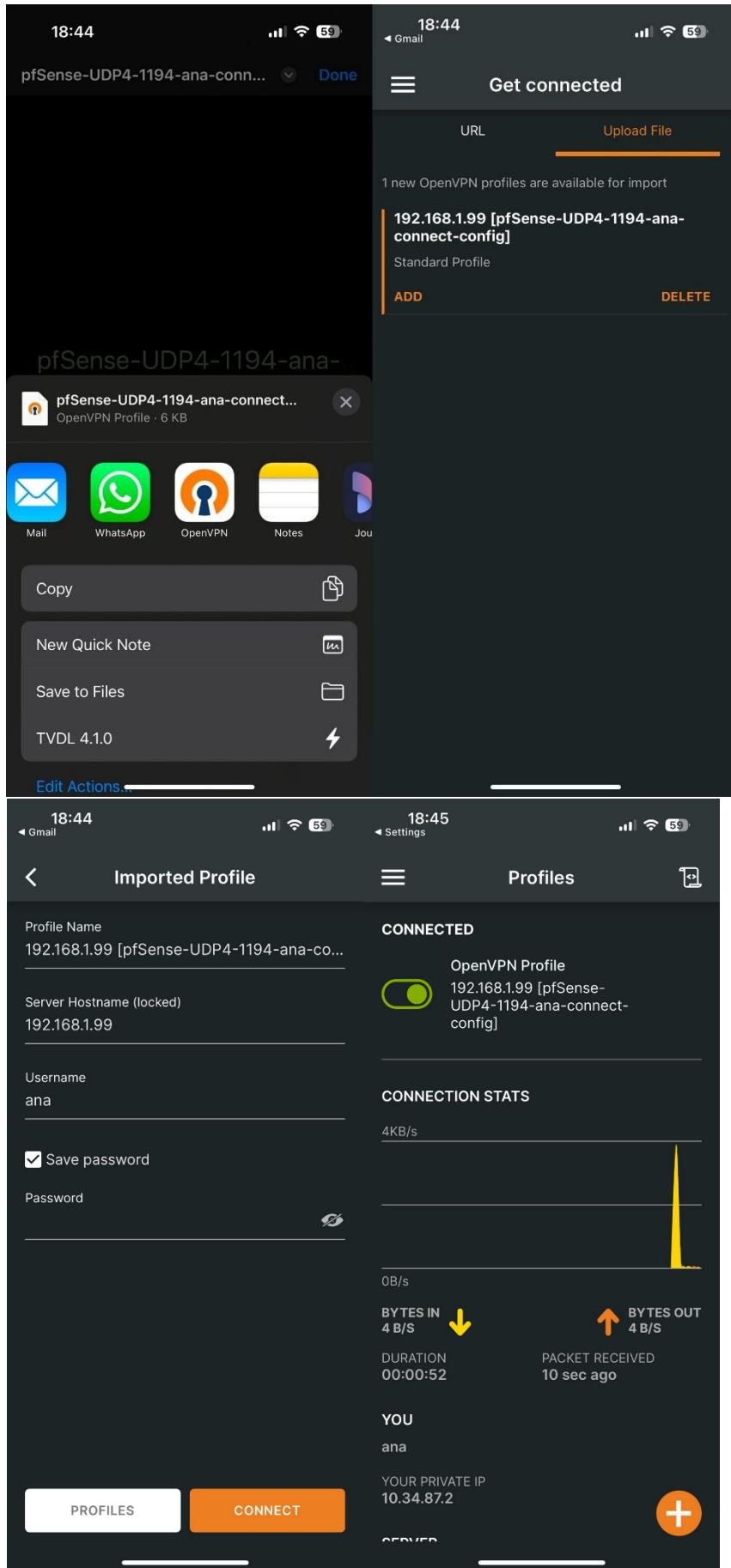
En mi caso voy a acceder desde un dispositivo Apple, un iPhone, por lo que iremos a la App Store y buscaremos esta app:



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:

18:46 11:58

Ana Orozco ≡

Blog

¡Hola, mundo!

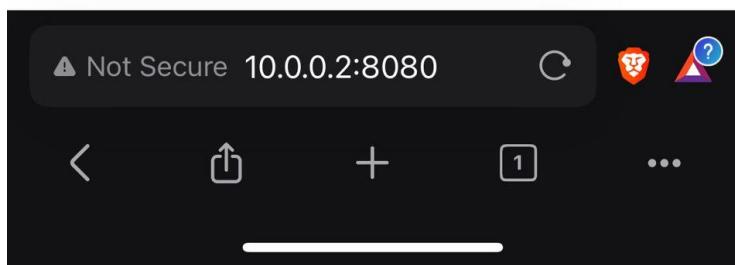
Te damos la bienvenida a WordPress. Esta es tu primera entrada. Edítala o bórrala, ¡luego empieza a escribir!

7 de diciembre de 2024

Ana Orozco

Blog

Eventos



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	<input type="checkbox"/> 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	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.
Group membership	admins
Not 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	<input checked="" type="checkbox"/> 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-ix001): 64-bit 32-bit
		- Previous Windows Installers (2.5.9-ix601): 64-bit 32-bit
		- Legacy Windows Installers (2.4.12-ix601): 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.