pfSense
– GUIA DE USUARIO –

Xavi Conde

Gerard Soteras

Índice

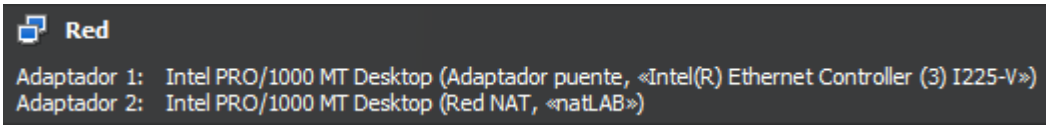
¿Qué es pfSense?

pfSense es una distribución de software basada en FreeBSD utilizada para la implementación de cortafuegos y enrutadores. Se caracteriza por su flexibilidad, seguridad y facilidad de uso, permitiendo a los administradores de red gestionar configuraciones avanzadas a través de una interfaz web intuitiva. Gracias a su amplia compatibilidad con múltiples plataformas y su soporte para plugins y extensiones, pfSense es una solución robusta para redes empresariales y domésticas.

Configuración inicial

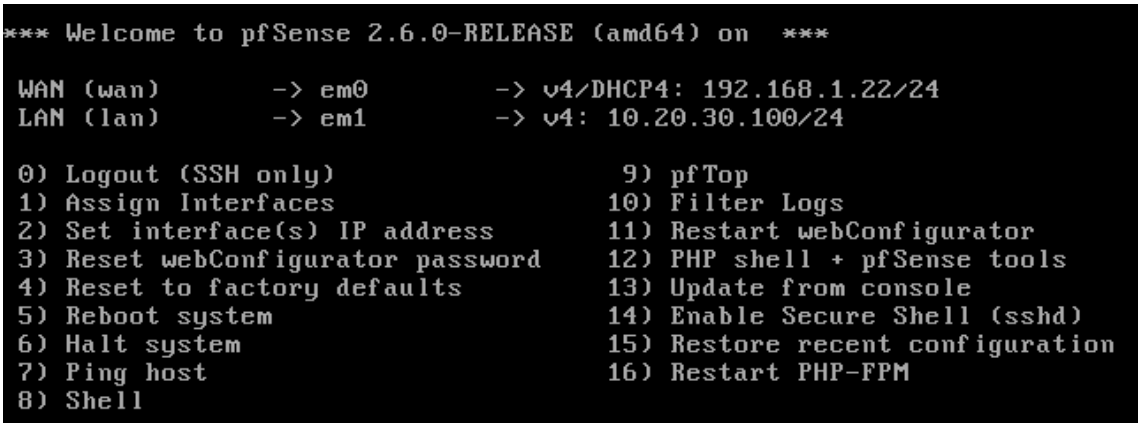
Para la instalación de pfSense utilizaremos VirtualBox. Antes de iniciar la máquina virtual, es necesario configurar los adaptadores de red. En esta configuración inicial, agregaremos dos adaptadores:

- Red WAN: Adaptador puente.
- Red LAN: Red NAT.



Configuración de las redes en pfSense

Al iniciar la máquina virtual, aparecerán las direcciones IP asignadas en ambas redes y una lista de opciones numeradas. Para poder entrar en las configuraciones del firewall de manera gráfica antes tenemos que configurar las direcciones IP de las interfaces para poder acceder desde un equipo virtual que se encuentre dentro de la misma red LAN.



Configuración de la interfaz LAN: Para entrar a la configuración LAN pulsamos **2** y nos saldrá una ventana que nos preguntará qué red queremos configurar. Pulsamos nuevamente el **2.** En esta configuración le estamos diciendo que tenga la IP 192.168.56.2, con la que accederemos más adelante desde otro equipo. También vamos a hacer que sea un servidor DHCP para la red.

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.20.30.100

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 10.20.30.1

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 10.20.30.150
Enter the end address of the IPv4 client address range: 10.20.30.160
Disabling IPv6 DHCPD...
```

Una vez configuradas las interfaces de red, podemos acceder a la interfaz gráfica de administración de pfSense. Para ello, es necesario utilizar una máquina con entorno gráfico conectada a la red LAN.

Si se requiere acceso desde la red WAN, es posible desactivar temporalmente las restricciones de seguridad utilizando el siguiente comando en pfSense (opción 8 para abrir el terminal):

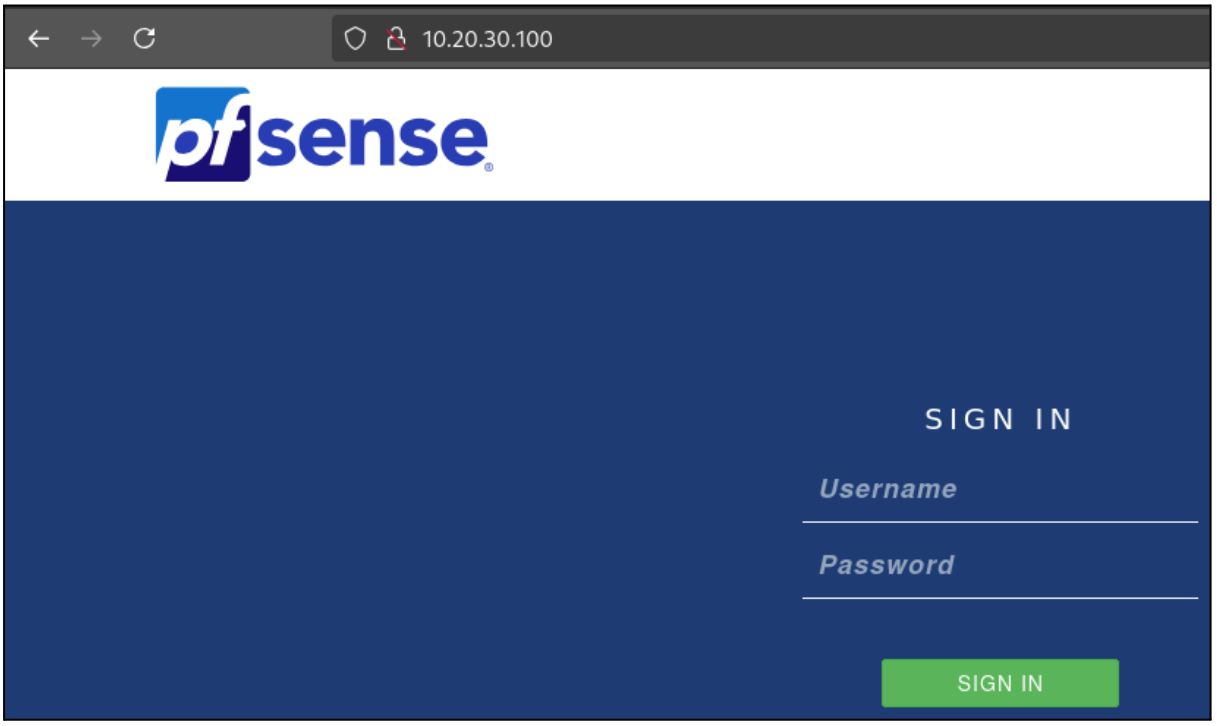
```
pfctl -d
```

Este comando permite acceder a la interfaz de configuración desde la WAN ingresando la dirección IP correspondiente. Sin embargo, esto representa un riesgo de seguridad, ya que puede abrir una puerta de acceso a usuarios no autorizados.

Desde una máquina en la red LAN, al ingresar la dirección IP de pfSense en un navegador, se mostrará la página de inicio de sesión. Por defecto, las credenciales son:

- **Usuario:** admin
- **Contraseña:** pfsense

Se recomienda cambiar la contraseña inmediatamente después del primer inicio de sesión para mejorar la seguridad del sistema.



Configuración de la red WAN PortForward

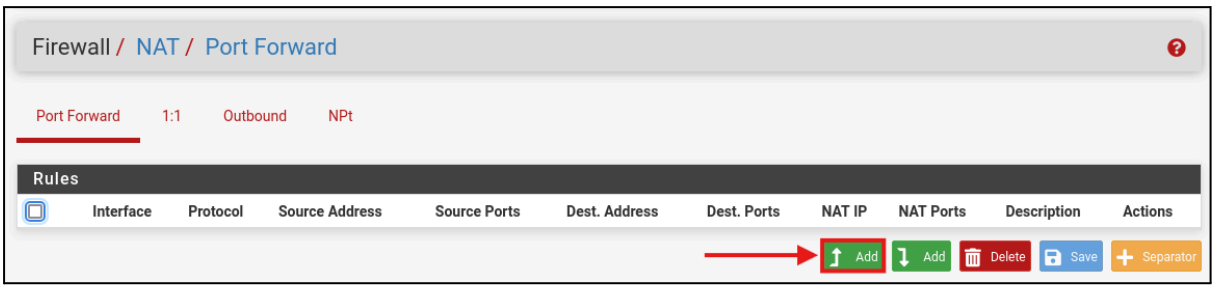
Para configurar la red WAN y poder hacer PortForward, gracias a esto podemos ver una página web alojada en un servidor de nuestra red LAN introduciendo la IP del firewall desde la WAN. Es un reenvío de puertos.

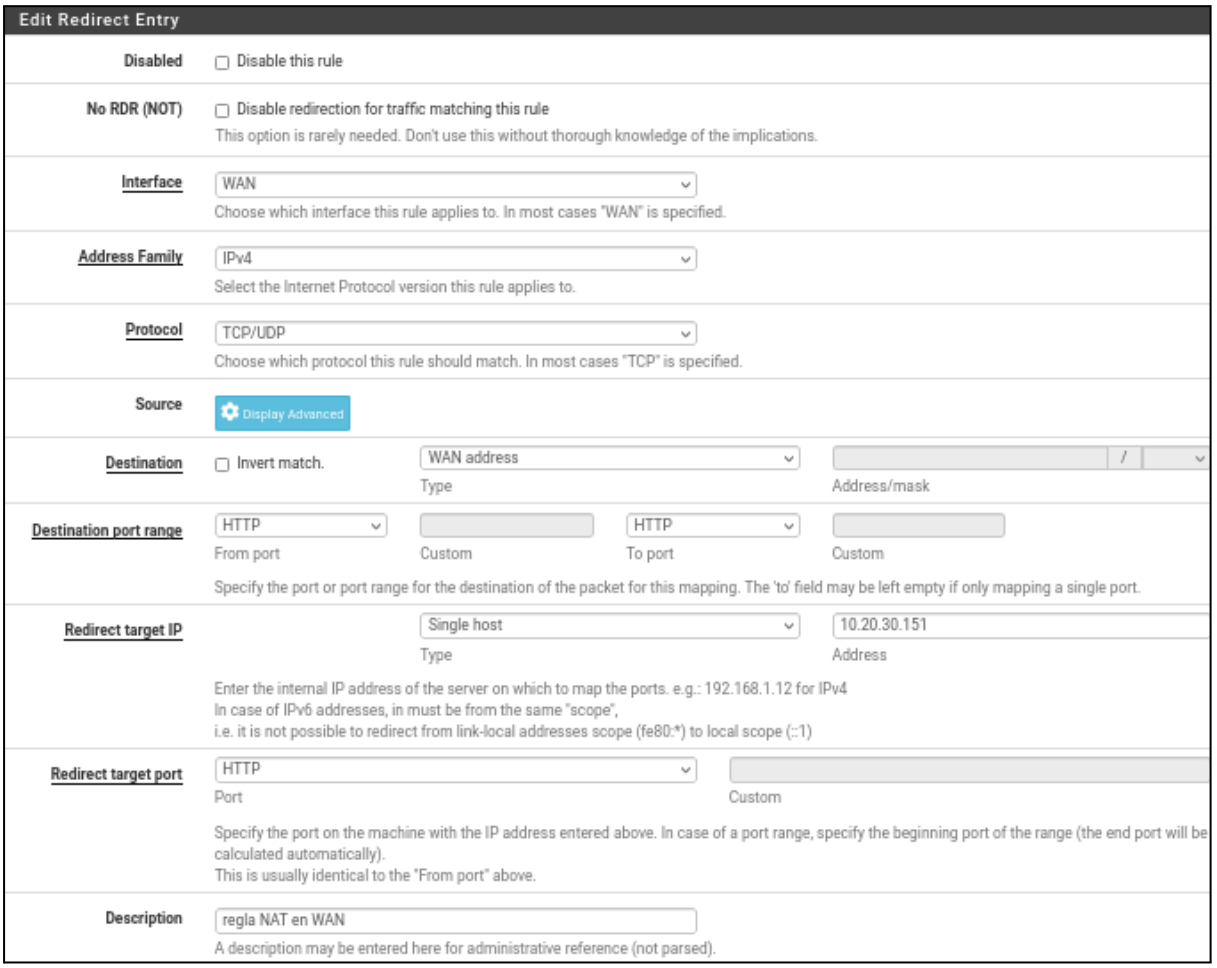
Configuración del servicio Nginx

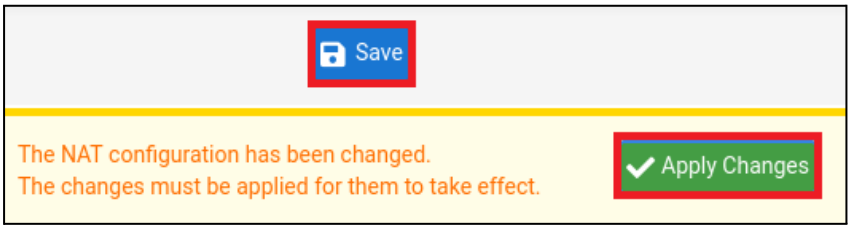
Si en la red LAN existe un servidor web con Nginx, podemos configurar pfSense para redirigir el tráfico de la WAN hacia dicho servidor. Para ello, realizamos la configuración en la sección de PortForward del firewall:

1. Accedemos a **Firewall → NAT→ PortForward**.
2. Configuramos una nueva regla con los siguientes parámetros:
    - **Interfaz**: WAN
    - **Address family**: IPv4
    - **Protocol**: TCP
    - **Destination**: WAN address
    - **Destination port**: HTTP (puerto 80 por defecto)
    - **Redirect target IP**: single host - (IP donde esté SERVIDOR WEB)
    - **Redirect target port**: HTTP (puerto 80 por defecto)
    - **Description**: regla NAT en WAN

Esta misma regla se creará automáticamente en **Firewall → Rules → WAN**
Con esta configuración, cualquier solicitud HTTP que llegue a la IP de pfSense en la WN será redirigida al servidor Nginx en la LAN.







Comprobación

Para verificar que la configuración ha salido correctamente, tendremos que ver la misma página web que se ve en la LAN introduciendo la IP del firewall en la WAN.

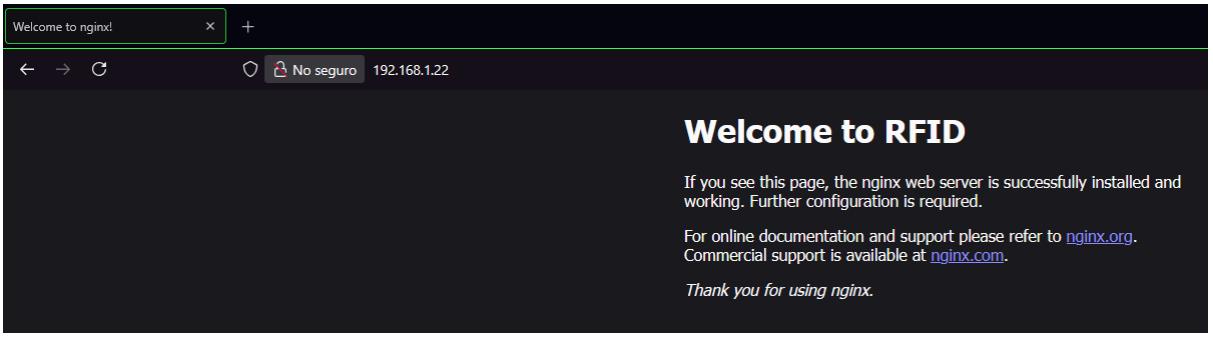
Comprobación de la IP del servidor Nginx

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e9:ff:89 brd ff:ff:ff:ff:ff:ff
    inet 10.20.30.151/24 brd 10.20.30.255 scope global dynamic enp0s3
       valid_lft 6950sec preferred_lft 6950sec
    inet6 fe80::a00:27ff:fee9:ff89/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Comprobación del servicio Nginx activo.

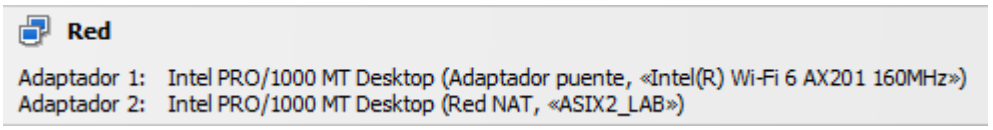
```
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/lib/systemd/system/nginx.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-03-09 18:46:06 CET; 2h 34min ago
```

Accedemos a la web desde la red WAN introduciendo la IP WAN de pfSense.



Configuración OpenVPN

Para tener OpenVPN en nuestro firewall debemos instalar el plugin correspondiente a la herramienta VPN y crear un usuario autorizado que pueda establecer conexión. Para este ejemplo cambiaremos el adaptador al del WiFi para poder conectarse por VPN desde el móvil.




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

WAN (wan)       -> em0        -> v4/DHCP4: 192.168.33.253/22
LAN (lan)       -> em1        -> v4: 10.20.30.100/24
```

Instalar el plugin OpenVPN client

Para instalar el paquete tenemos que ir a **System** → **Package Manager** → **Available Packages**. Aquí buscaremos el paquete llamado: **openvpn-client-export**

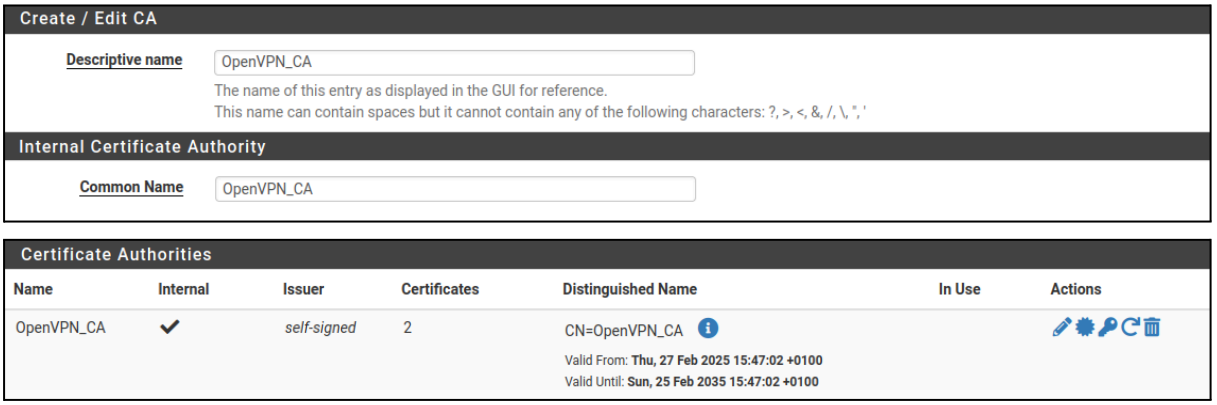
Una vez instalado, tendremos que crear certificados digitales para los usuarios.

Certificados digitales propios de pfSense

Para que un usuario pueda acceder por VPN a la red, tendremos que crear unos certificados digitales y configurar una serie de reglas.

Creación de CA (Autoridad de Certificación)

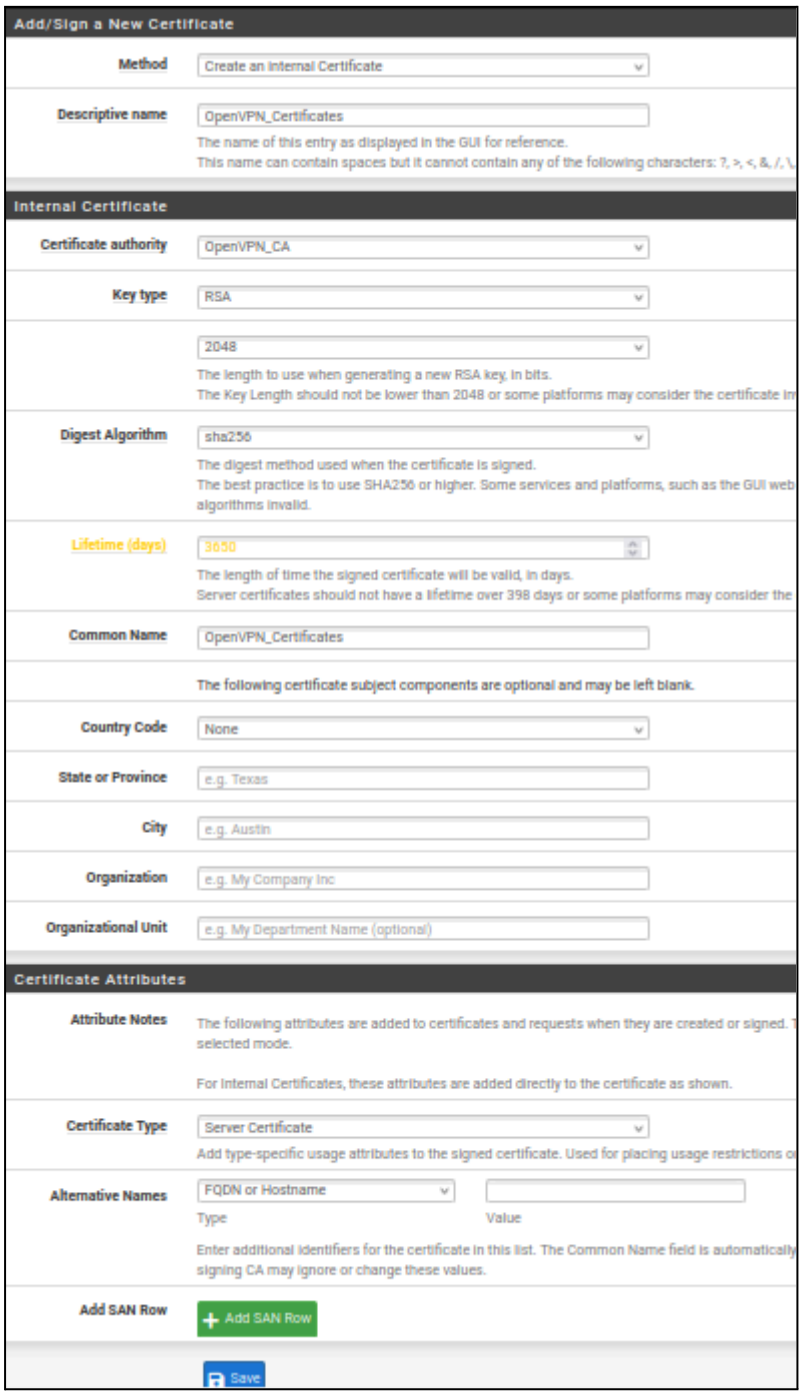
- Nos dirigimos a: **System** → **Certificate Manager**
- Creamos un certificado nuevo
- Rellenamos los datos
- Guardamos

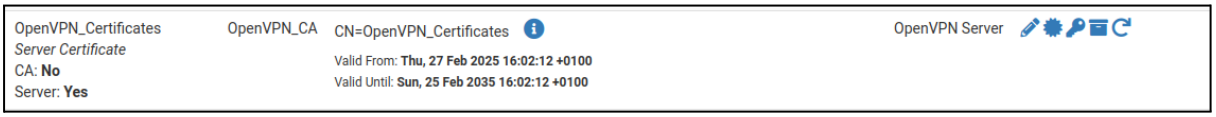


Creación de Certificado del servidor OpenVPN

- Nos dirigimos a: **System** → **Certificate Manager** → **Certificates**
- Creamos uno nuevo

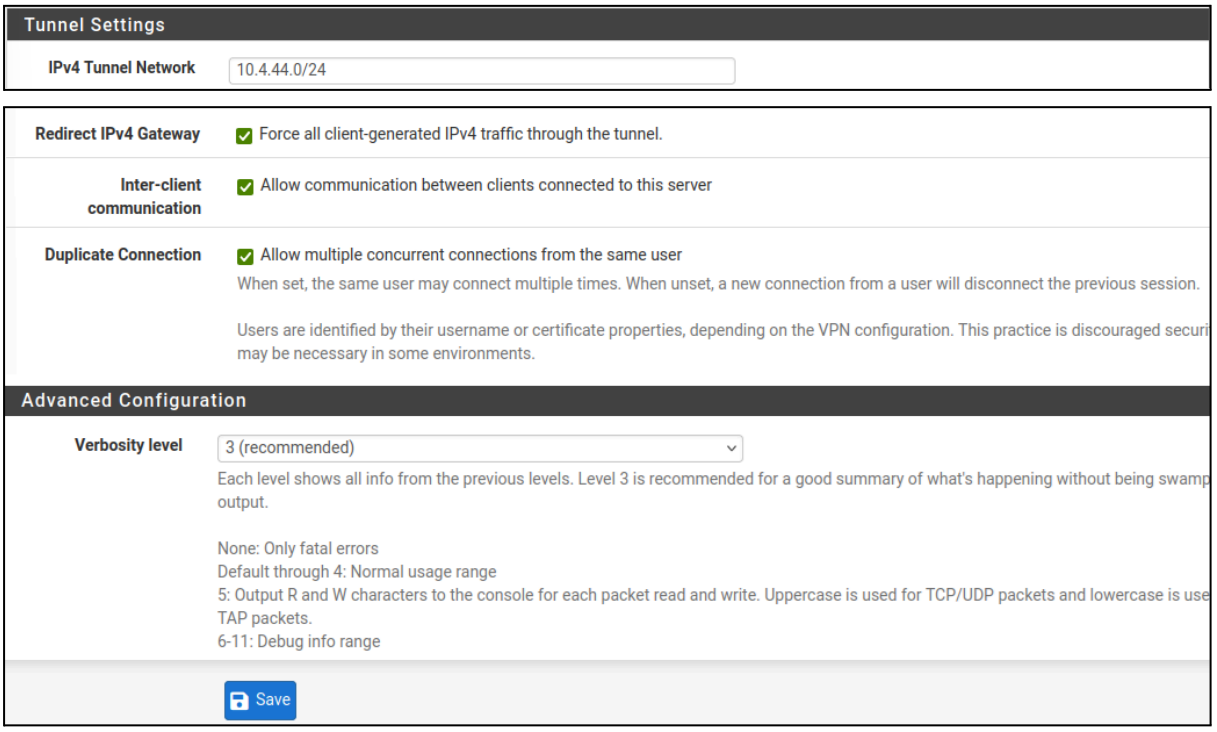
- Rellenamos los datos (los de ubicación no son obligatorios)
- Guardamos



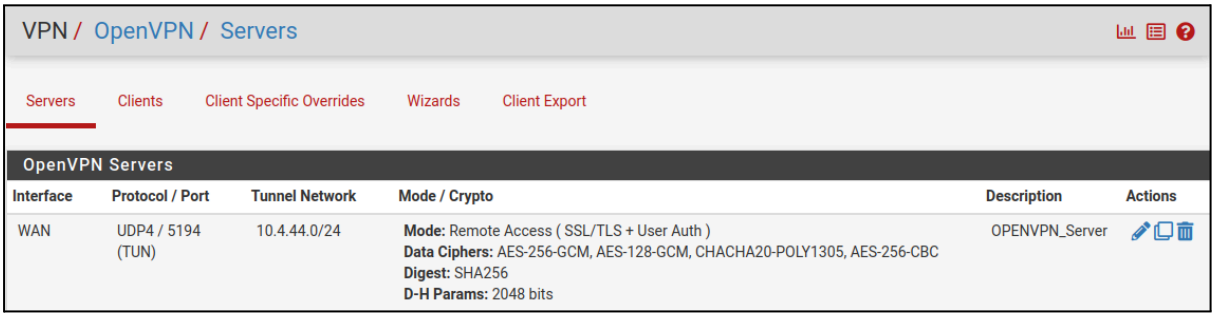


Configuración del servidor OpenVPN

Nos dirigimos a **VPN → OpenVPN → Servers**
Añadimos un nuevo certificado.

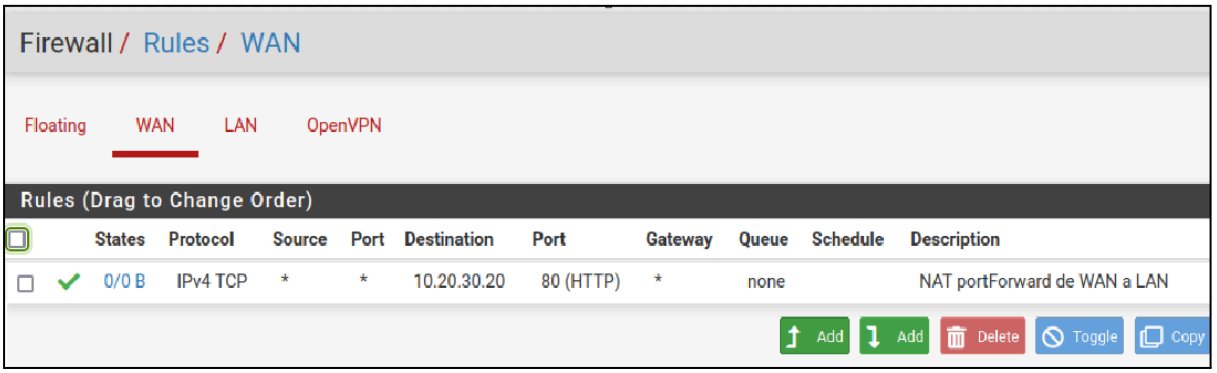


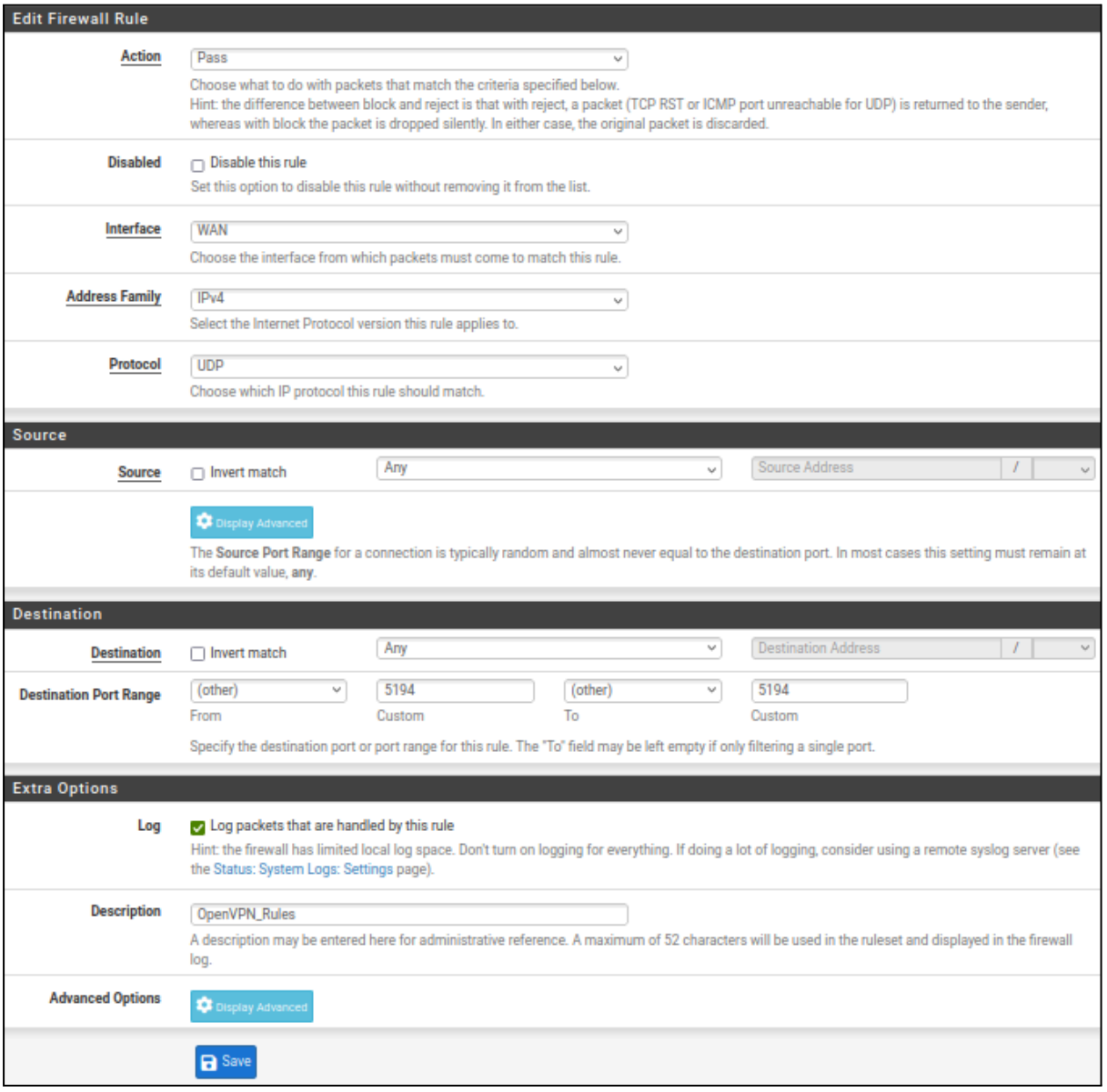
Una vez configurado, se debe ver algo así:



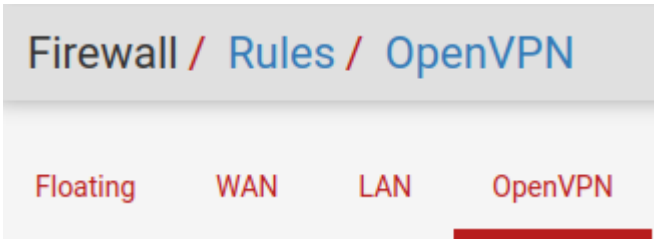
Reglas que permitan el acceso al firewall desde el VPN

Nos dirigimos a **Firewall** → **Rules** → **WAN** y creamos una nueva regla.

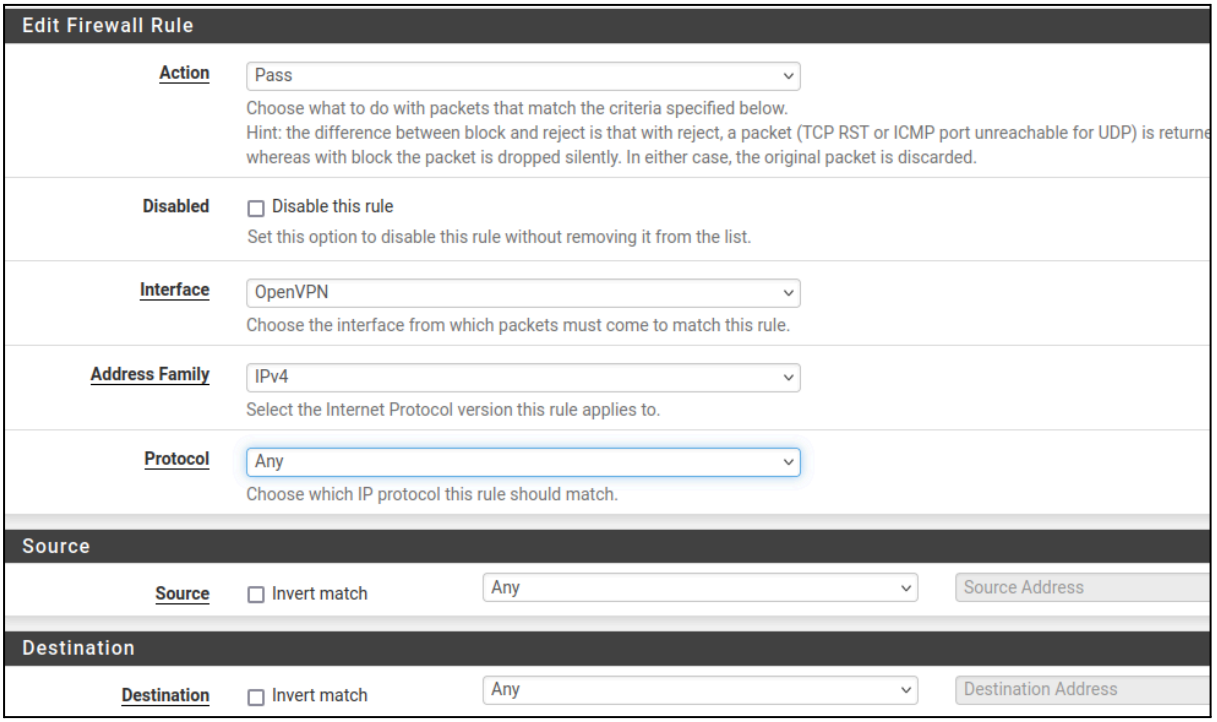

Firewall / Rules / WAN
Floating
WAN
LAN
OpenVPN
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
0/0 B
IPv4 TCP
*
*
10.20.30.20
80 (HTTP)
*
none
NAT portForward de WAN a LAN
Add
Add
Delete
Toggle
Copy


Edit Firewall Rule
Action
Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
WAN
Choose the interface from which packets must come to match this rule.
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
Source Address
Display Advanced
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.
Destination
Destination
Invert match
Any
Destination Address
Destination Port Range
(other)
5194
From
Custom
(other)
5194
To
Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.
Extra Options
Log
Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description
OpenVPN_Rules
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options
Display Advanced
Save

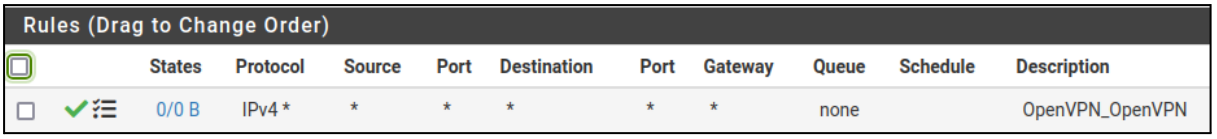
Ahora debemos crear otra regla para que se permita todo el tráfico de la VPN.
Para ello nos dirigimos al apartado de **OpenVPN**



Añadimos una nueva regla.



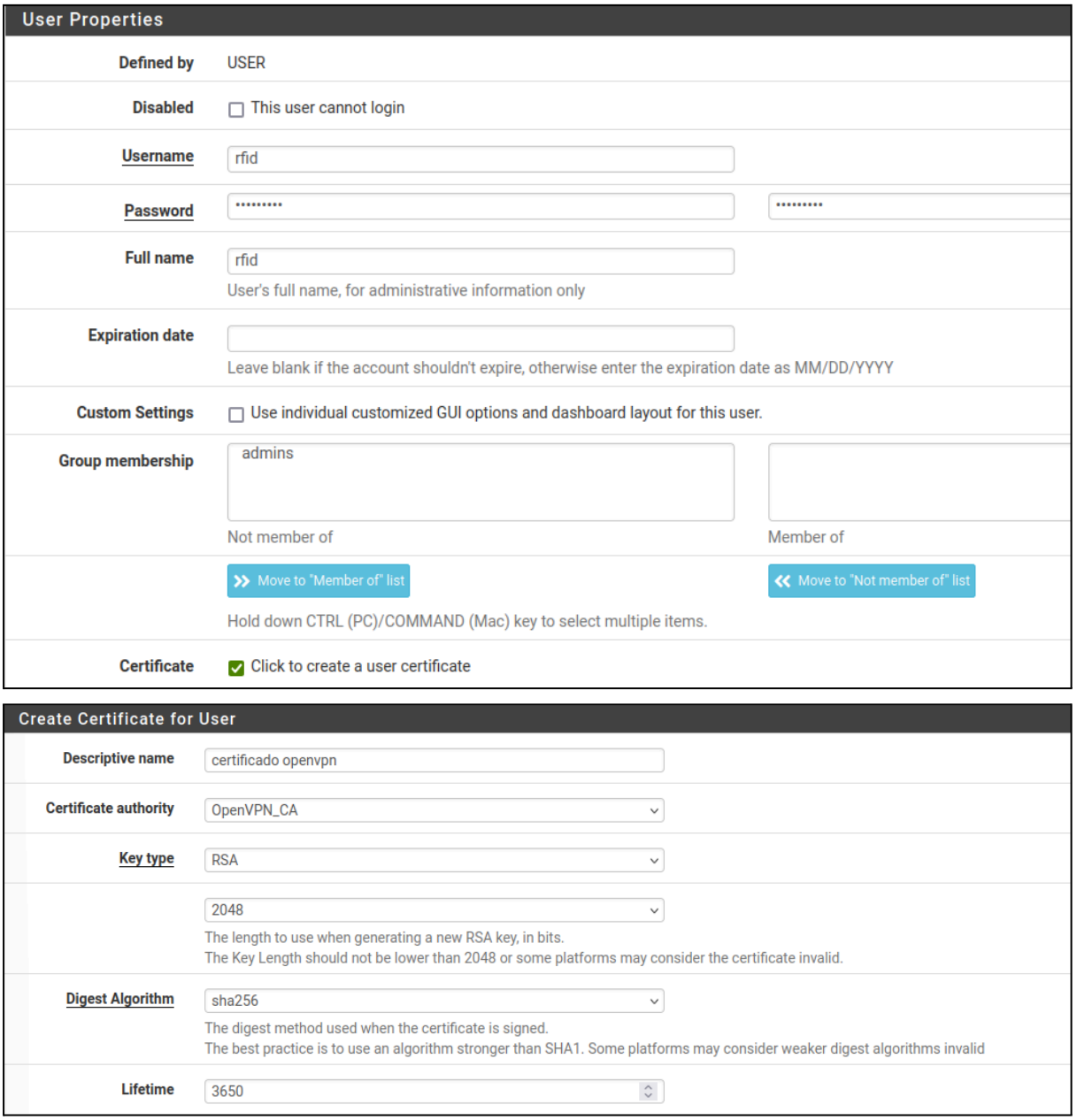
Veremos algo así:



Clientes autorizados para usar la VPN

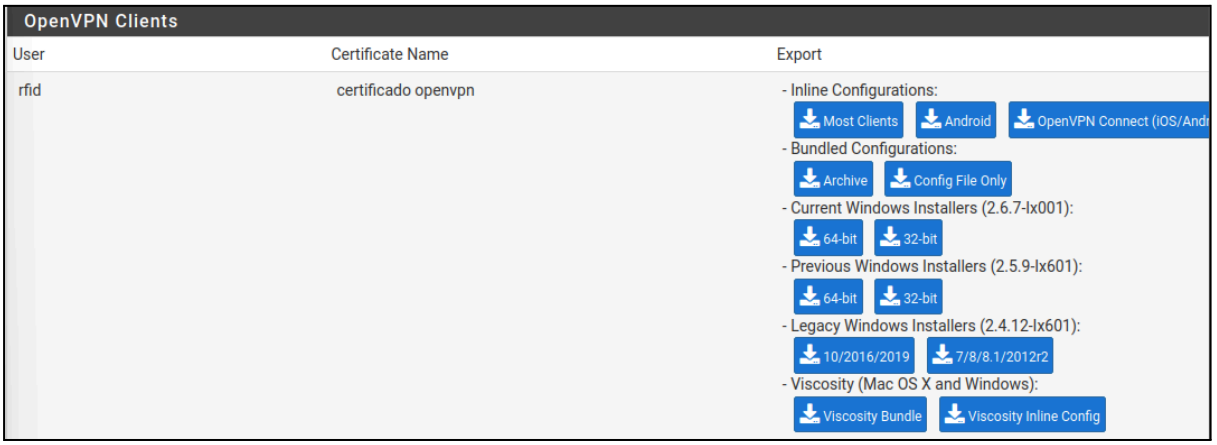
Para crear usuarios autorizados nos dirigimos a:
System → User Manager

Lo más importante de este paso es activar la opción:
- Click to create a user certificate



Una vez creado el usuario, tendremos que exportar el archivo del cliente.
Para ello nos dirigimos **VPN → OpenVPN → Client Export**

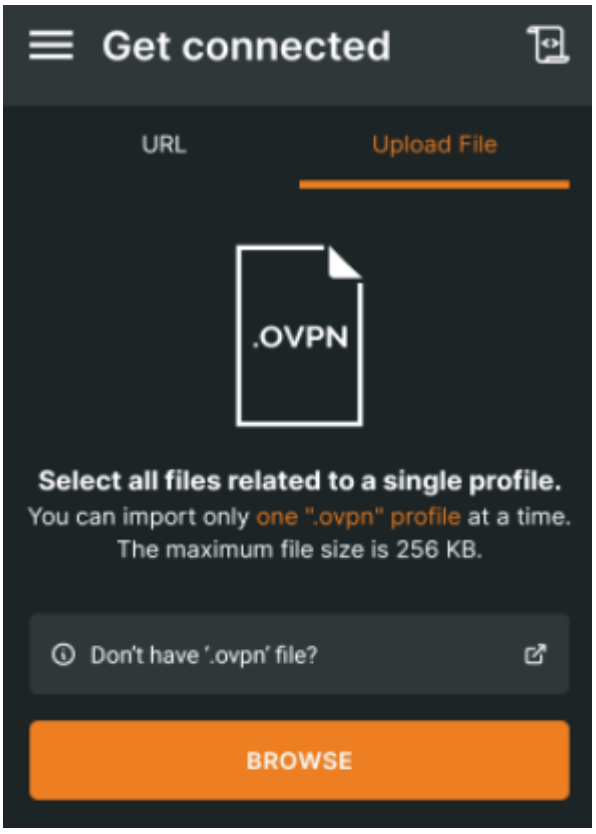
Buscamos por el final de la página hasta el apartado **OpenVPN Clients**



Descargamos el archivo que más convenga. En este caso descargamos el de Android y haremos la conexión a través del móvil. Para ello tendremos que descargar en el dispositivo la aplicación **OpenVPNConnect**.

Conexión VPN desde móvil

Una vez pasamos el archivo que se nos descarga al móvil e instalamos la aplicación, importamos el archivo en el apartado **Upload File** → **Browse**



Cuando añadimos el archivo, introducimos el nombre y contraseña del usuario autorizado. Para verificar que todo funciona correctamente, podemos buscar la IP WAN de pfsense. Si logramos ver la pantalla de acceso del firewall, podremos concluir con las configuraciones.