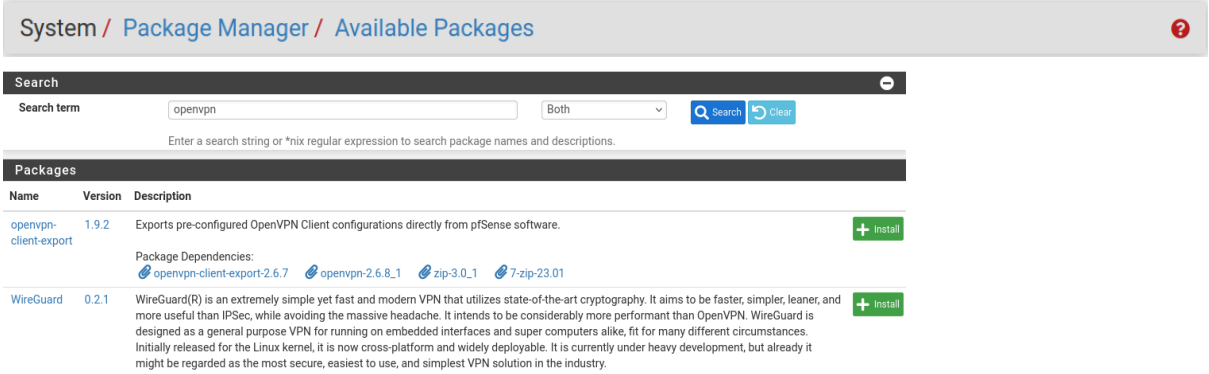
PfSense OpenVPN

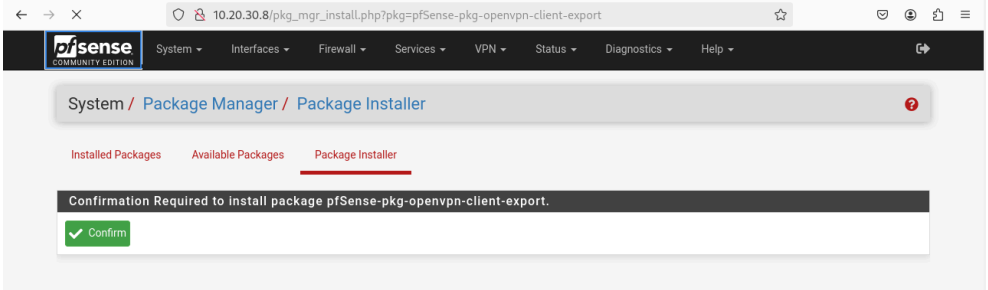
TMD

Instalación de los paquetes necesarios

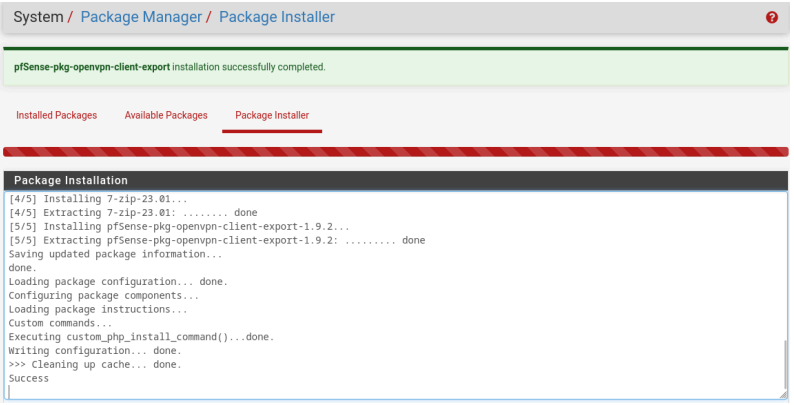
Una vez configurado el pfSense con las interfaces de red descargamos el paquete pfSense-pkg-openvpn-client-export, para acceder a la descarga vamos por la ruta siguiente: System - Package Manager - Available Packages y buscamos el paquete de instalación del openvpn.



Confirmamos la descarga.



Descarga completada.



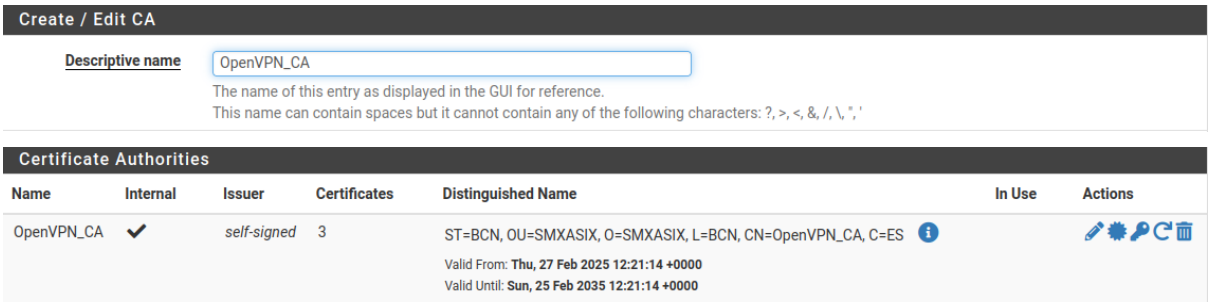
Una vez instalado el paquete deberíamos ver lo siguiente:

Creación de los certificados digitales

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 Autoridad de Certificación
Nos vamos a la ruta siguiente: System → Certificate Manager

- Creamos un certificado nuevo
- Rellenamos los datos
- Guardamos
- Creamos un certificado de servidor OpenVPN



Configurar el certificado del servidor OpenVPN

Nos vamos a la ruta siguiente:

System / Certificates / Certificates

Rellenamos todos los datos necesarios tal, como se indica a continuación:

Add/Sign a New Certificate

Method	Create an internal Certificate
Descriptive name	OpenVPN_Server_TK The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '

Internal Certificate

Certificate authority	OpenVPN_CA
Key type	RSA
	2048 The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm	sha256 The digest method used when the certificate is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.
Lifetime (days)	3650 The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.
Common Name	OpenVPN_Server_TK
	The following certificate subject components are optional and may be left blank.
Country Code	ES
State or Province	BCN
City	BCN

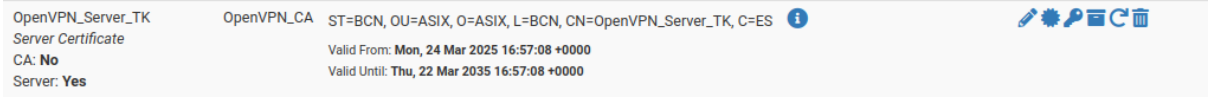
Certificate Attributes

Attribute Notes	The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode. For Internal Certificates, these attributes are added directly to the certificate as shown.
Certificate Type	Server Certificate Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.
Alternative Names	FQDN or Hostname (Type) — Value Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.
Add SAN Row	+ Add SAN Row

Guardamos

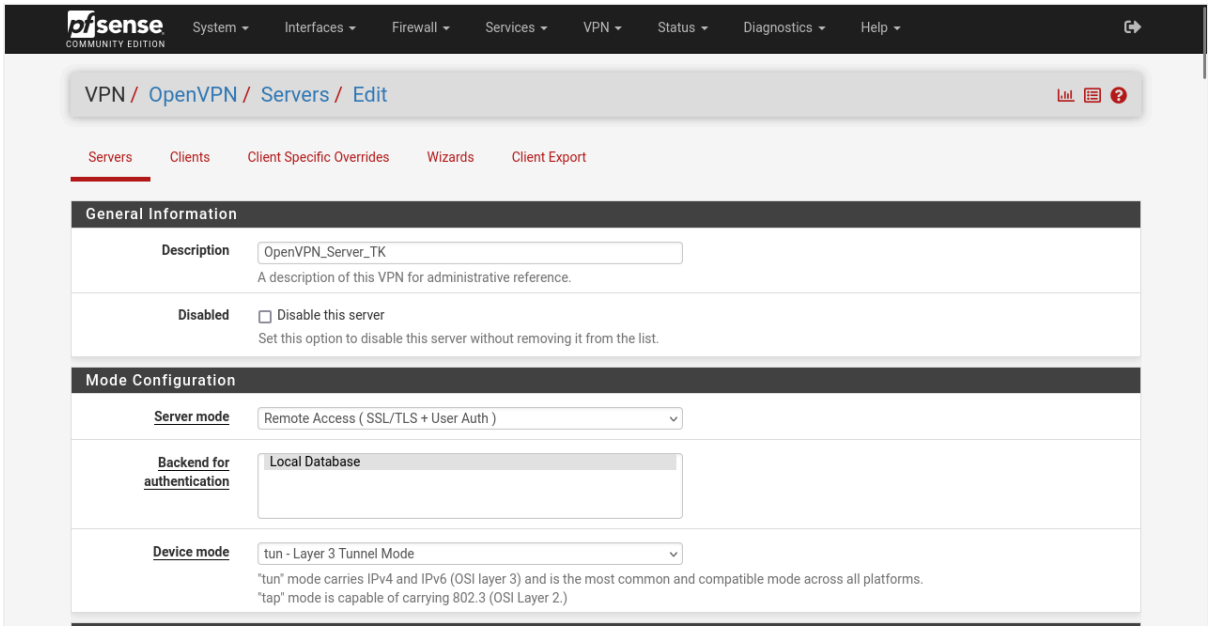
Save

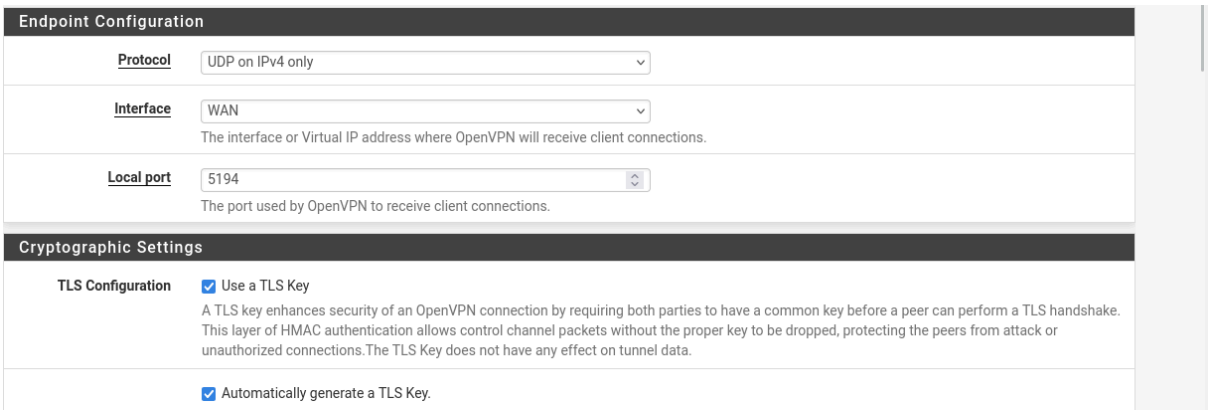
Al finalizar la configuración vemos el resultado siguiente:



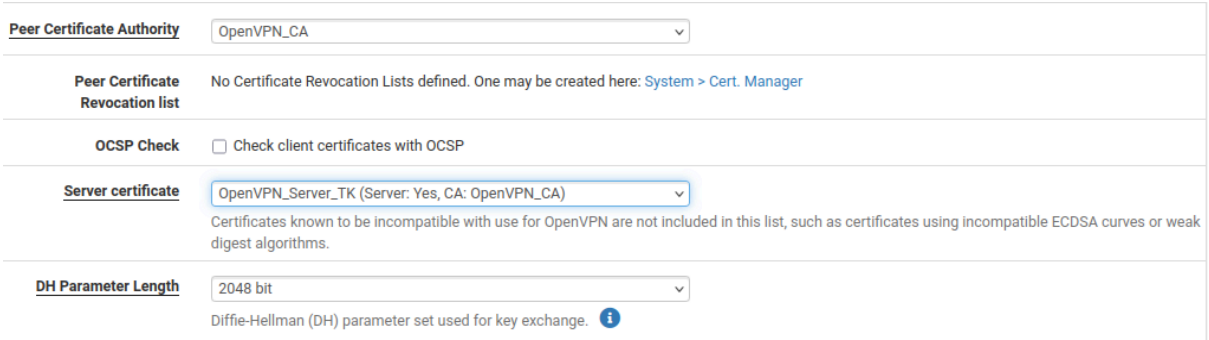
Configuramos el servidor OpenVPN

Ruta para acceder al apartado correcto: VPN - OpenVPN - Servers - Edit





Añadimos el certificado de servidor que acabamos de crear:



Tunnel Settings

IPv4 Tunnel Network	10.4.44.0/24 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.
Inter-client communication	☑ Allow communication between clients connected to this server
Duplicate Connection	☑ Allow multiple concurrent connections from the same user When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session. Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.
Duplicate Connection Limit	2 Limit the number of concurrent connections from the same user.

Advanced Client Settings

DNS Default Domain	☐ Provide a default domain name to clients
DNS Server enable	☑ Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1	1.1.1.1
DNS Server 2	8.8.8.8
DNS Server 3	
DNS Server 4	
Block Outside DNS	☐ Make Windows 10 Clients 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.
Force DNS cache update	☐ Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation. This is known to kick Windows into recognizing pushed DNS servers.
NTP Server enable	☐ Provide an NTP server list to clients
NetBIOS enable	☐ Enable NetBIOS over TCP/IP If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

Resultado de la creación del servidor OpenVPN:

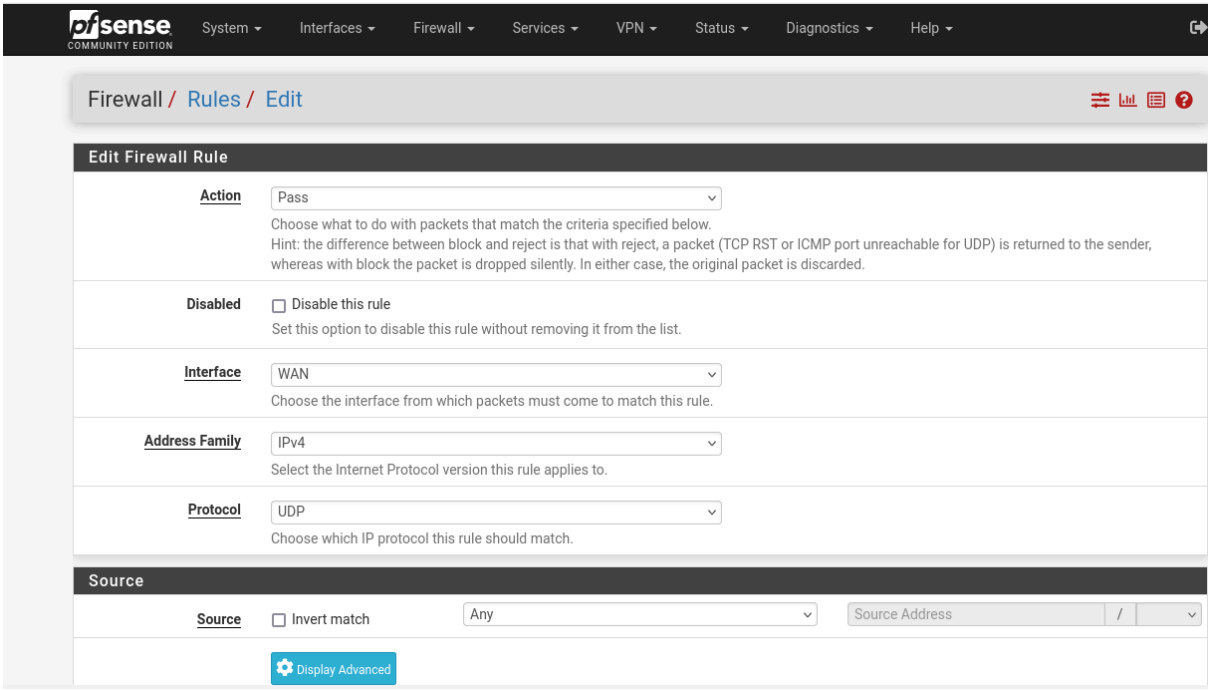
OpenVPN Servers

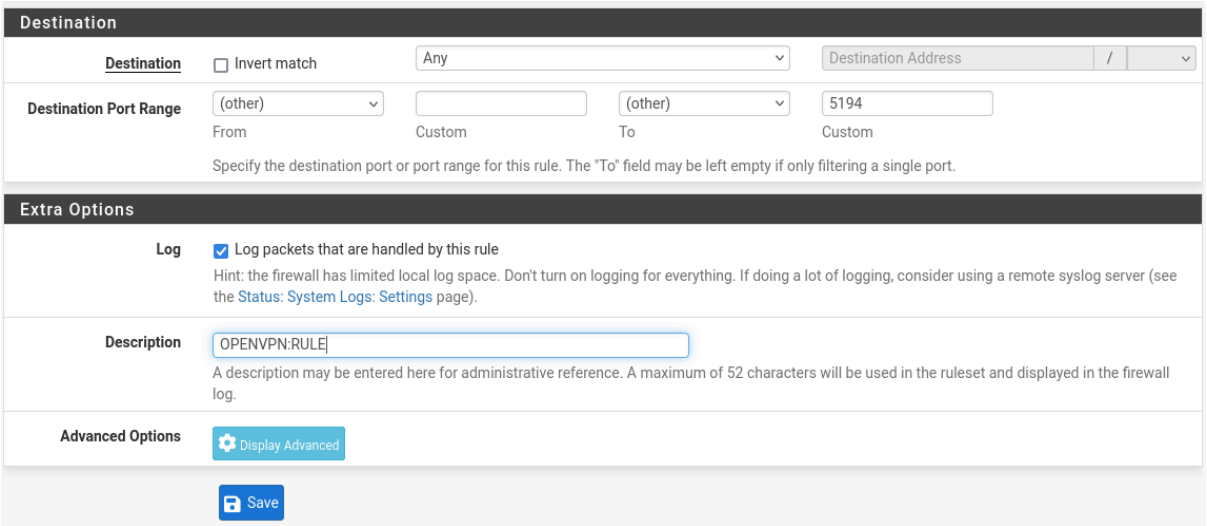
Interface	Protocol / Port	Tunnel Network	Mode / Crypto
WAN	UDP4 / 5194 (TUN)	10.4.44.0/24	**Mode:** Remote Access (SSL/TLS + User Auth) **Data Ciphers:** AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC **Digest:** SHA256 **D-H Params:** 2048 bits

Permiso al acceso al firewall desde el VPN.

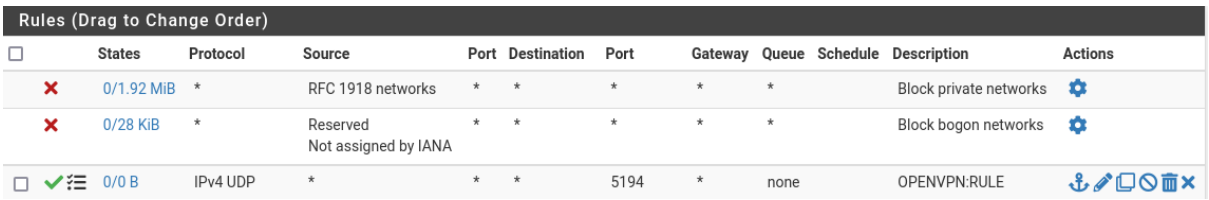
Nos vamos a la ruta siguiente: Firewall → Rules → WAN

Crearemos una nueva regla a continuación:





La regla nos quedaría así:

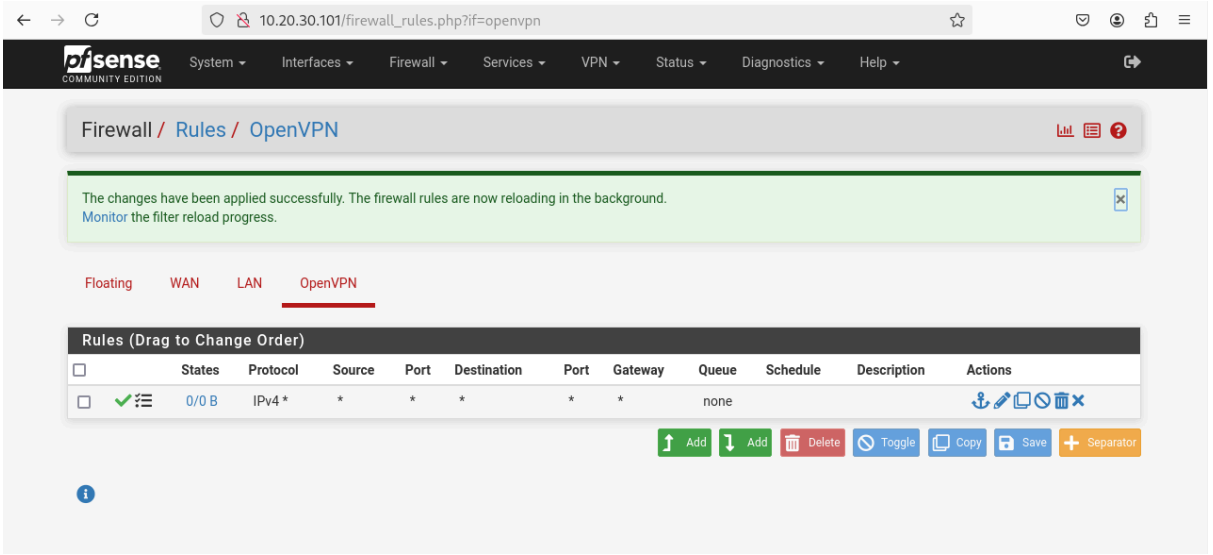


Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✕	0/1.92 MiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
✕	0/28 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
✓	0/0 B	IPv4 UDP	*	*	*	5194	*	none		OPENVPN:RULE	

Regla para permitir todo el tráfico VPN

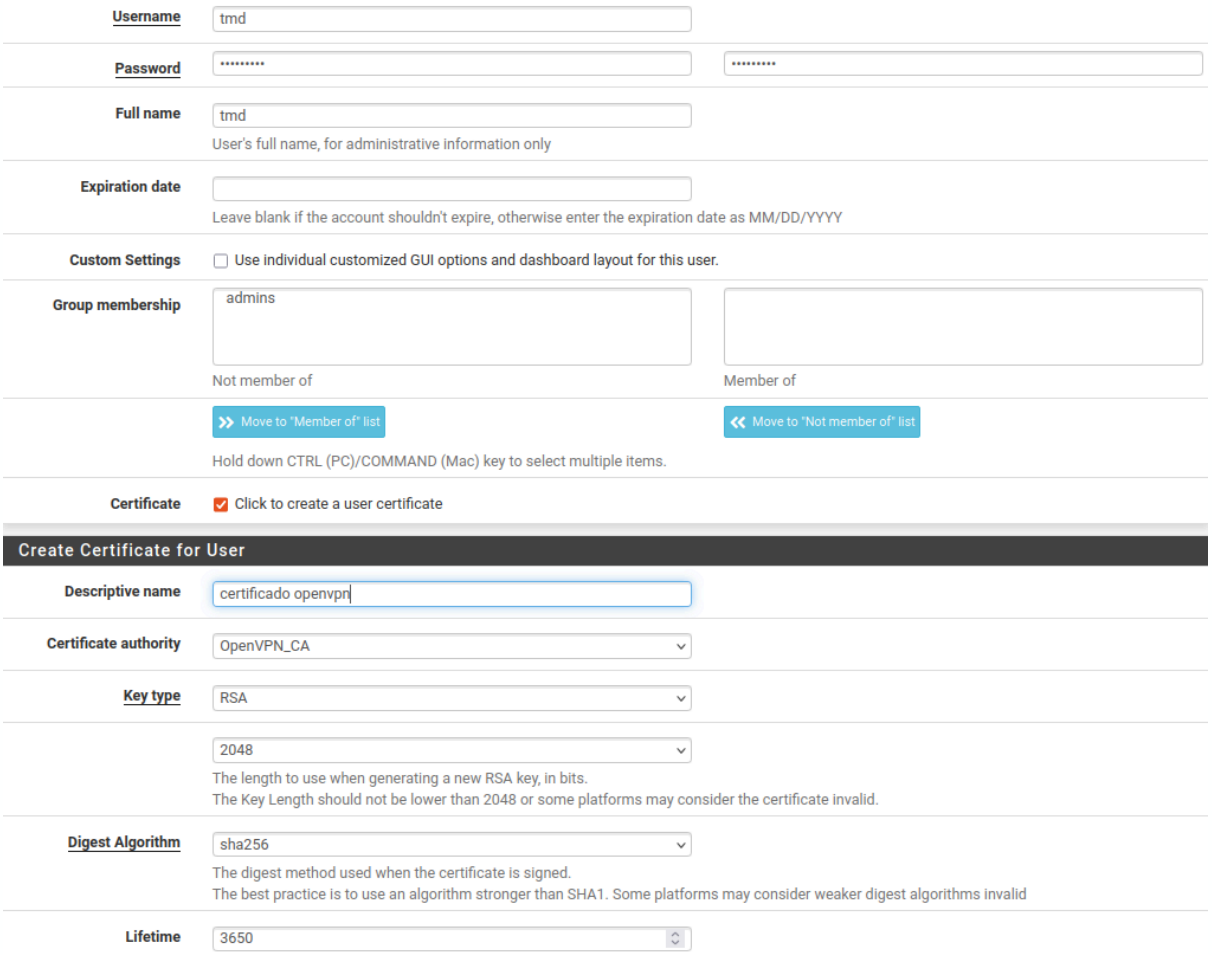
Ponemos todo a “any” y activamos la opción de los logs.



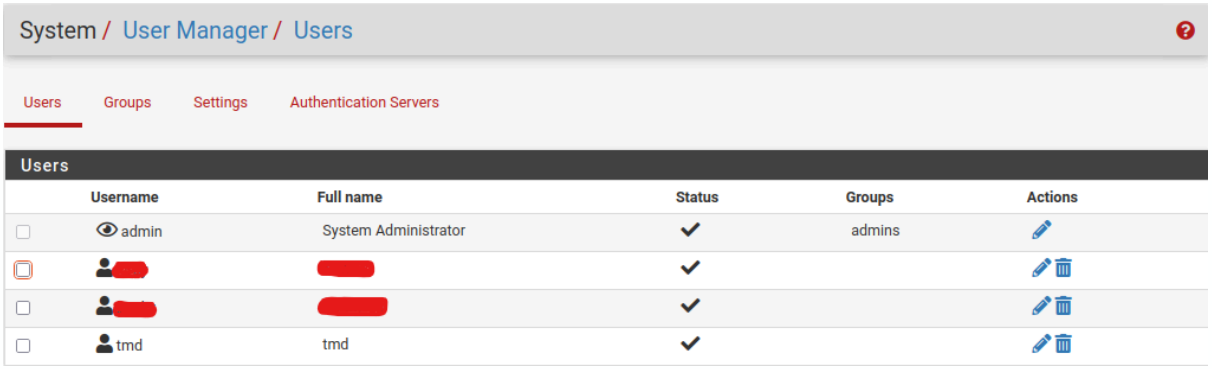
Exportar el archivo de configuración OpenVPN para los clientes

Vamos a crear un usuario nuevo. (System → User Manager → Users)

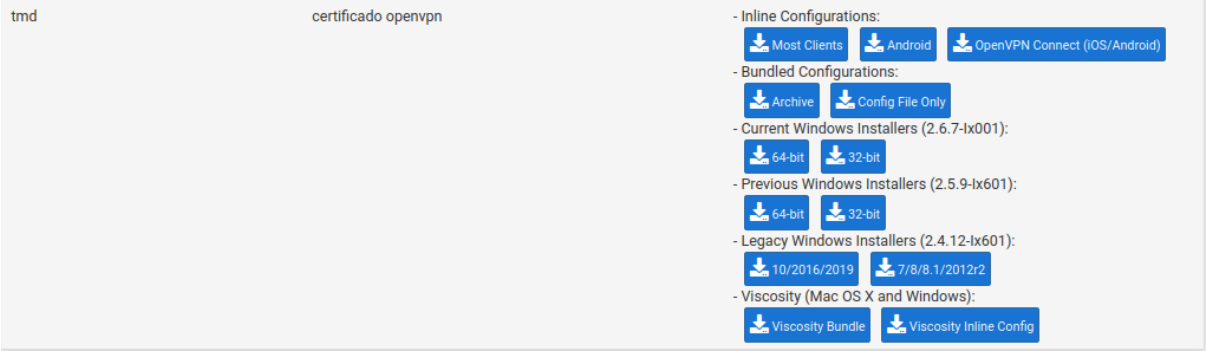
Paso importante: hacer click en la opción de hacer el certificado de usuario.



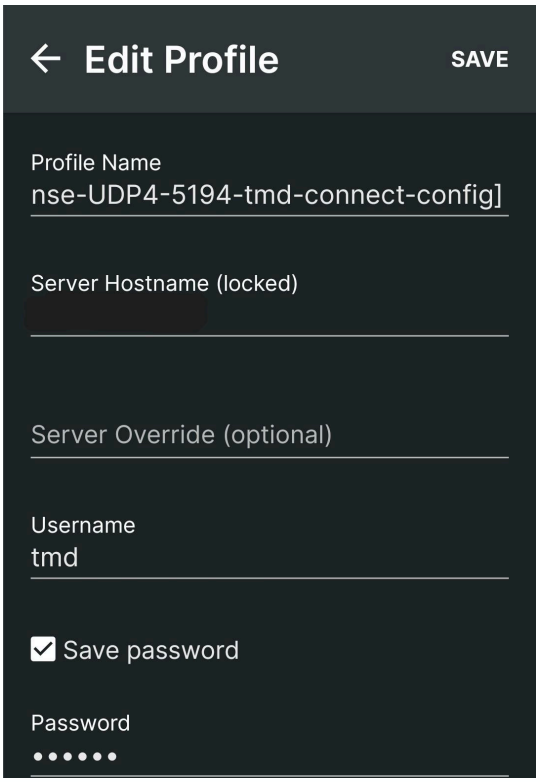
Aquí podemos ver a nuestro cliente que acabamos de crear.



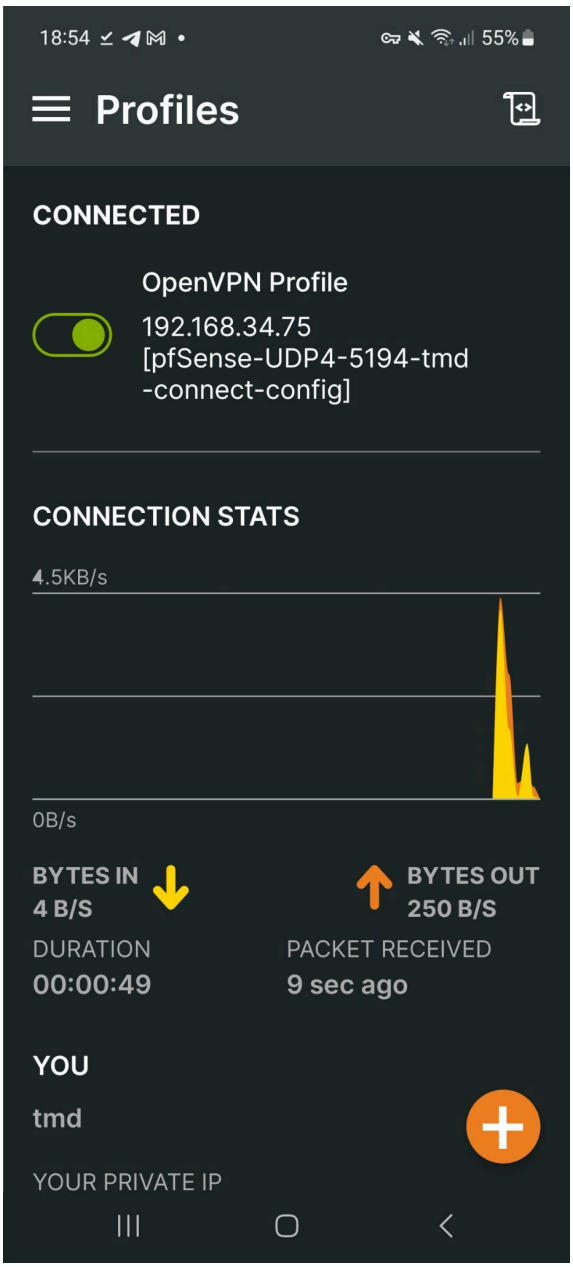
Exportamos el archivo de nuestro cliente:

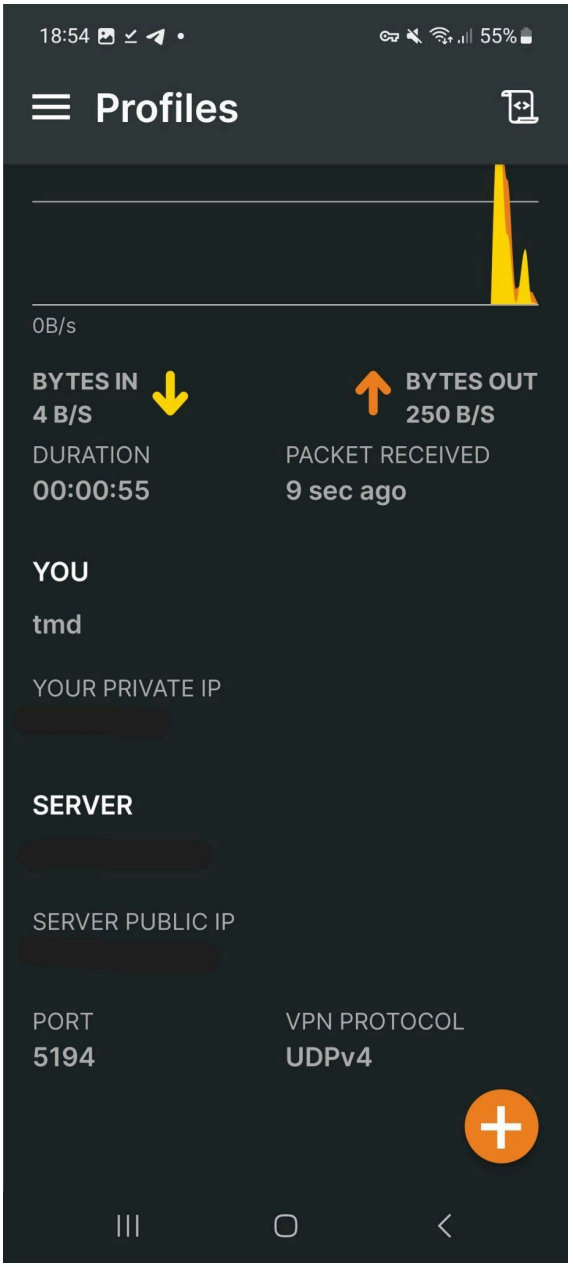


Instalamos la aplicación de OpenVPN en el dispositivo móvil y dentro de la app añadimos una nueva conexión importando el archivo que descargamos en la captura anterior.



Resultados de la conexión exitosa:





Si introducimos la IP pública en el navegador del móvil tenemos acceso a nuestro pfSense.