

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.

System / Package Manager / Available Packages

Search

Search term: openvpn Both Search Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Name	Version	Description	
openvpn-client-export	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software.	+ Install
Package Dependencies: openvpn-client-export-2.6.7 openvpn-2.6.8_1 zip-3.0_1 7-zip-23.01			
WireGuard	0.2.1	WireGuard(R) is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. It aims to be faster, simpler, leaner, and more useful than IPsec, while avoiding the massive headache. It intends to be considerably more performant than OpenVPN. WireGuard is designed as a general purpose VPN for running on embedded interfaces and super computers alike, fit for many different circumstances. Initially released for the Linux kernel, it is now cross-platform and widely deployable. It is currently under heavy development, but already it might be regarded as the most secure, easiest to use, and simplest VPN solution in the industry.	+ Install

Confirmamos la descarga.

System / Package Manager / Package Installer

Installed Packages Available Packages Package Installer

Confirmation Required to install package pfSense-pkg-openvpn-client-export.

[Confirm](#)

Descarga completada.

System / Package Manager / Package Installer

pfSense-pkg-openvpn-client-export installation successfully completed.

Installed Packages Available Packages Package Installer

Package Installation

```
[4/5] Installing 7-zip-23.01...
[4/5] Extracting 7-zip-23.01: ..... done
[5/5] Installing pfSense-pkg-openvpn-client-export-1.9.2...
[5/5] Extracting pfSense-pkg-openvpn-client-export-1.9.2: ..... done
Saving updated package information...
done.
Loading package configuration... done.
Configuring package components...
Loading package instructions...
Custom commands...
Executing custom_php_install_command()...done.
Writing configuration... done.
>>> Cleaning up cache... done.
Success
```

Una vez instalado el paquete deberíamos ver lo siguiente:

System /
[Package Manager](#) /
[Installed Packages](#)

Installed Packages
Available Packages

Installed Packages

Installed Packages				
Name	Category	Version	Description	Actions
✓ openvpn-client-export	security	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software.	<div> <div></div> <div></div> </div>
<div> Package Dependencies: <div> openvpn-client-export-2.6.7 openvpn-2.6.8_1 zip-3.0_1 7-zip-23.01 </div> </div>				

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

Create / Edit CA






Descriptive name

OpenVPN_CA

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: '?', '>', '<', '&', '/', '\\', ' ', ''

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
OpenVPN_CA	✓	self-signed	3	ST=BCN, OU=SMXASIX, O=SMXASIX, L=BCN, CN=OpenVPN_CA, C=ES Valid From: Thu, 27 Feb 2025 12:21:14 +0000 Valid Until: Sun, 25 Feb 2035 12:21:14 +0000		    

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 <small>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: ?, >, <, &, /, \, ", '.</small>				
Internal Certificate					
Certificate authority	OpenVPN_CA				
Key type	RSA				
	2048 <small>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.</small>				
Digest Algorithm	sha256 <small>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.</small>				
Lifetime (days)	3650 <small>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.</small>				
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	<p>The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.</p> <p>For Internal Certificates, these attributes are added directly to the certificate as shown.</p>				
Certificate Type	Server Certificate <small>Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.</small>				
Alternative Names	<table><tr><td>FQDN or Hostname</td><td></td></tr><tr><td>Type</td><td>Value</td></tr></table> <small>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.</small>	FQDN or Hostname		Type	Value
FQDN or Hostname					
Type	Value				
Add SAN Row	<button>+ Add SAN Row</button>				

Guardamos




Al finalizar la configuración vemos el resultado siguiente:

OpenVPN_Server_TK Server Certificate CA: No Server: Yes	OpenVPN_CA ST=BCN, OU=ASIX, O=ASIX, L=BCN, CN=OpenVPN_Server_TK, C=ES Valid From: Mon, 24 Mar 2025 16:57:08 +0000 Valid Until: Thu, 22 Mar 2035 16:57:08 +0000		    
--	---	--	---

Configuramos el servidor OpenVPN

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


System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

VPN / OpenVPN / Servers / Edit

Servers Clients Client Specific Overrides Wizards Client Export

General Information

Description
OpenVPN_Server_TK
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.

Local port
5194
The port used by OpenVPN to receive client connections.

Cryptographic Settings

TLS Configuration
☒ Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

☒ Automatically generate a TLS Key.

Añadimos el certificado de servidor que acabamos de crear:

Peer 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_TK (Server: Yes, CA: OpenVPN_CA)
Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.

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

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:

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Rules / Edit

Edit Firewall Rule

Action
 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
 Choose the interface from which packets must come to match this rule.

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](#)

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 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
 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](#)

La regla nos quedaría así:

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/1.92 MiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	Settings
<input checked="" type="checkbox"/>	0/28 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	Settings
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 UDP	*	*	*	5194	*	none		OPENVPN:RULE	Settings Edit Copy Delete Refresh

Regla para permitir todo el tráfico VPN

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

The screenshot shows the pfSense web interface for configuring Firewall Rules. The breadcrumb trail is "Firewall / Rules / OpenVPN". A green notification bar 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", and "OpenVPN", with "OpenVPN" being the active tab. The main section is titled "Rules (Drag to Change Order)". It contains a table with the following columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. A single rule is listed with the following values: States is checked, Protocol is "0/0 B", Source is "IPv4 *", Port is "*", Destination is "*", Port is "*", Gateway is "*", Queue is "none", and Description is empty. To the right of the rule are icons for anchor, edit, copy, delete, and refresh. Below the table are buttons for "Add", "Add", "Delete", "Toggle", "Copy", "Save", and "Separator". An information icon is located at the bottom left of the rule configuration area.

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 OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 *	*	*	*	*	none			Anchor Edit Copy Delete Refresh

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

[i](#)

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.

Username

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
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

Descriptive name

Certificate authority

Key type

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
The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Lifetime

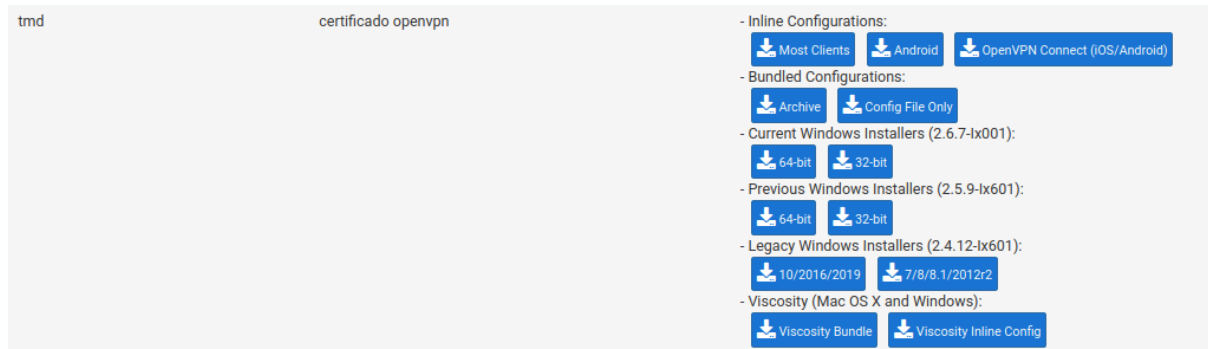
Aquí podemos ver a nuestro cliente que acabamos de crear.

System / [User Manager](#) / [Users](#) ?

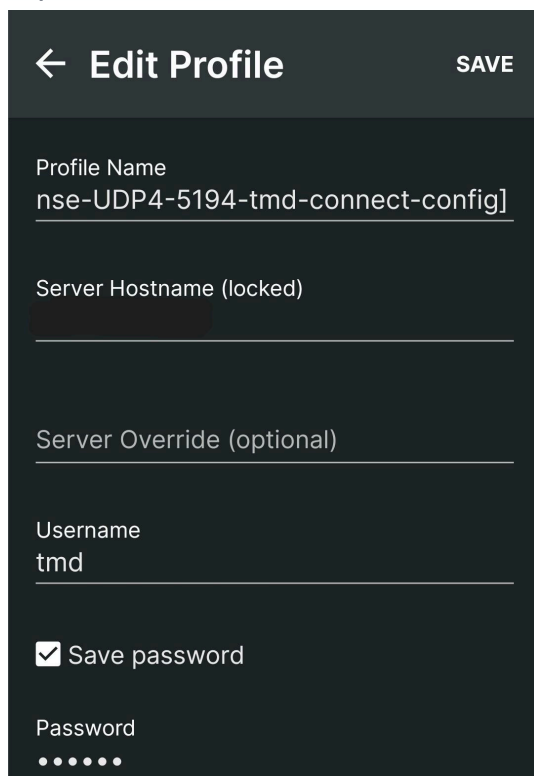
[Users](#) [Groups](#) [Settings](#) [Authentication Servers](#)

Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	 admin	System Administrator	✓	admins	
<input type="checkbox"/>	 		✓		 
<input type="checkbox"/>	 		✓		 
<input type="checkbox"/>	 tmd	tmd	✓		 

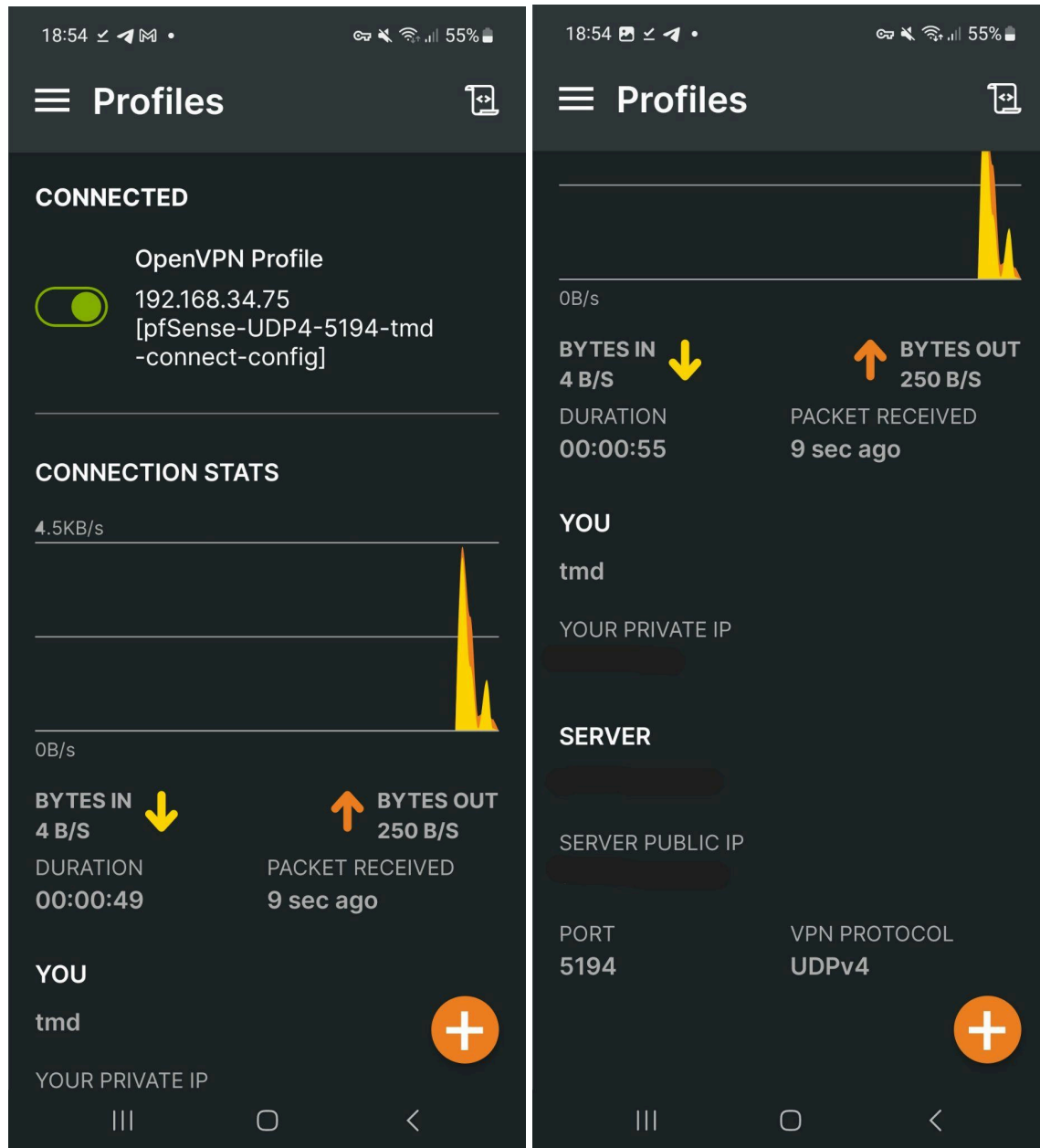
Exportamos el archivo de nuestro cliente:



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.

