

***Que és Open VPN?**

OpenVPN és un software de código libre que permite hacer conexiones de red privadas virtuales, en dispositivos a través de internet.

***Diferències entre VPN d'accés remot i VPN punt a punt, per a què serveix cada una?**

La diferencia principal es que mientras que la VPN de acceso remoto necesita un servidor intermediario para poder llegar a la red privada, la VPN punto a punto hace la conexión directa con la red. Esto permite la comunicación segura directa entre los dispositivos o redes involucradas.

***Per a què utilitza OpenSSL a Open VPN?**

Es una librería de código abierto, para la seguridad e integridad de la as VPN, usa funciones criptográficas, como la generación de llaves, encriptación i firma digital.

***Per a què utilitza TLS a Open VPN?**

Para la privacidad y la integridad de los datos que se transmiten a través de Internet, se aseguran mediante la encriptación de las comunicaciones y la autenticación de los dispositivos en la comunicación.

***Pera a què utilitza SSL/TLS a Open VPN?**

Para establecer un túnel seguro de un punto a otro, entre los dispositivos de la red. Es distinto al TLS, SSL protege el envío, TLS es más por el propio dato enviado.

Instalación y configuración de OpenVPN en PFSense

En Pfsense, el apartado de **System/Package Manager/Available Packages** ->

- Install openvpn-client-export

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term: open Both Search Clear

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

Name	Version	Description	Actions
frr	2.0.2_1	FRR routing daemon for BGP, OSPF, and OSPF6 Conflicts with Quagga OSPF and OpenBGPD. These packages cannot be installed at the same time. Package Dependencies: frr9-pythontools-9.0.2 frr9-9.0.2	+ Install
Open-VM-Tools	10.1.0.5.1	VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine. Package Dependencies: open-vm-tools-12.3.5.2	+ Install
openvpn-client-export	9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software. Package Dependencies: openvpn-client-export-2.6.7 openvpn-2.6.8_1 zip-3.0_1 7-zip-23.01	+ Install
snort	4.1.6_14	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. Package Dependencies: snort-2.9.20_7	+ Install
tinc	1.0.35_3	tinc is a Virtual Private Network (VPN) daemon that uses tunnelling and encryption to create a secure private network between hosts on the Internet. Because the tunnel appears to the IP level network code as a normal network device, there is no need to adapt any existing software. This tunnelling allows VPN sites to share information with each other over the Internet without exposing any information to others. A single tinc daemon can accept more than one connection at a time, thus making it possible to create larger virtual networks, because some limitations are circumvented. Instead of most other VPN implementations, tinc encapsulates each network packet in its own UDP packet.	+ Install

- instalado

System / Package Manager / Installed Packages

Installed Packages Available 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. Package Dependencies: openvpn-client-export-2.6.7 openvpn-2.6.8_1 zip-3.0_1 7-zip-23.01	Update Current Remove Information Reinstall

Newer version available

Package is configured but not (fully) installed or deprecated

- Vamos al wizard/openVPN Remote Acces Server Setup para configurarlo
- Type of Server (lo haremos en local) -> Local User Acces -> Next

Wizard / OpenVPN Remote Access Server Setup /

OpenVPN Remote Access Server Setup

This wizard will provide guidance through an OpenVPN Remote Access Server Setup .

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

Select an Authentication Backend Type

Type of Server: Local User Access

NOTE: If unsure, leave this set to "Local User Access."

Next

- Agregamos un certificado para La VPN
- Nombre descriptivo, Tamaño de la key, tiempo de vida de este, el nombre y datos variados opcionales de la empresa (ficticia en este caso).

Wizard / OpenVPN Remote Access Server Setup / Add Certificate Authority

Step 6 of 11

Certificate Authority Selection

OpenVPN Remote Access Server Setup Wizard

Create a New Certificate Authority (CA) Certificate

Descriptive name: OpenVPNTest
A name for administrative reference, to identify this certificate.

Randomize Serial: ☒ Use random serial numbers when signing certificates.
When enabled, serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using sequential values.

Key length: 1024 bit
Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com

Lifetime: 3650
Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)

Common Name: CertificadoOpenVPN_test
The internal name of the CA, used as a part of the CA subject. If left blank, the descriptive name will be used instead.

Country Code: ES
Two-letter ISO country code (e.g. US, AU, CA)

State or Province: Spain
Full State or Province name, not abbreviated (e.g. Texas, Indiana, Ontario).

City: Barcelona
City or other Locality name (e.g. Austin, Indianapolis, Toronto).

Organization: HAPPYMILSA
Organization name, often the company or group name.

Organizational Unit: lasamburgesas
Organizational Unit name, often a department or team name.

Add new CA

- Escogemos servidor default del certificado.

Wizard / OpenVPN Remote Access Server Setup / Server Certificate Selection

Step 7 of 11

Server Certificate Selection

OpenVPN Remote Access Server Setup Wizard

Choose a Server Certificate

Certificate: GUI default (65ce416d01109)

Add new Certificate Next

- Aquí vamos a modificar el tunnel network, y el local network,
- El *tunnel network*, por así decirlo es el que sale hacia afuera, por que es el que va a hacer el túnel, el local network es la red interna, estas ip las sacaremos de la configuración previa del PFSense (WAN, LAN) vamos a pillar el rango ->
- WAN (túnel) 192.168.143.0/24
- LAN (Local) 192.168.1.0/24
- Next ->

Fallback Data Encryption Algorithm: AES-256-CBC (256 bit key, 128 bit block)

The algorithm used to encrypt traffic between endpoints when data encryption negotiation is disabled or fails.

Auth Digest Algorithm: SHA256 (256-bit)

The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.

Hardware Crypto: No Hardware Crypto Acceleration

The hardware cryptographic accelerator to use for this VPN connection, if any.

Tunnel Settings

IPv4 Tunnel Network: 192.168.143.0

This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.

Redirect IPv4 Gateway: ☐ Force all client generated traffic through the tunnel.

IPv4 Local Network: 192.168.1.0

This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. 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.

Concurrent Connections: 1

Specify the maximum number of clients allowed to concurrently connect to this server.

Allow Compression: Refuse any non-stub compression (Most secure)

Allow compression to be used with this VPN instance, which is potentially insecure.

Compression: Disable Compression [Omit Preference]

Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may expose data. This setting has no effect if compression is not allowed. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the

- Vamos a agregar las reglas del firewall que permita las conexiones a OpenVPN de los usuarios de internet, y vamos a agregar una regla que permita el tráfico en el túnel VPN.

Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration

Step 10 of 11

Firewall Rule Configuration

OpenVPN Remote Access Server Firewall Rules

Rules control passing or blocking network traffic as it flows through the firewall.

Rules must be added which allow traffic to reach the OpenVPN server IP address and port, as well as to allow traffic from connected clients inside the OpenVPN tunnel.

The options on this step can add automatic rules to pass this traffic, or rules can be configured manually after completing the wizard.

Traffic from clients to server	
Firewall Rule	<input checked="" type="checkbox"/> Add a rule to permit connections to this OpenVPN server instance from clients anywhere on the Internet.

Traffic from clients through VPN	
OpenVPN rule	<input checked="" type="checkbox"/> Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

[» Next](#)

- Y ya estaría. Open >VPN configurado

Wizard / OpenVPN Remote Access Server Setup / Finished!

Step 11 of 11

Finished!

OpenVPN Remote Access Server Setup Wizard

Configuration Complete!

The configuration is now complete.

Adding users for the VPN depends on the chosen authentication method. For example, add local users with certificates under [System > User Manager](#). For remote authentication servers, add certificates directly in [System > Certificate Manager](#).

To easily export client configurations, browse to [System > Packages](#) and install the OpenVPN Client Export package.

[» Finish](#)

- Tenemos aquí el servidor con el certificado hecho

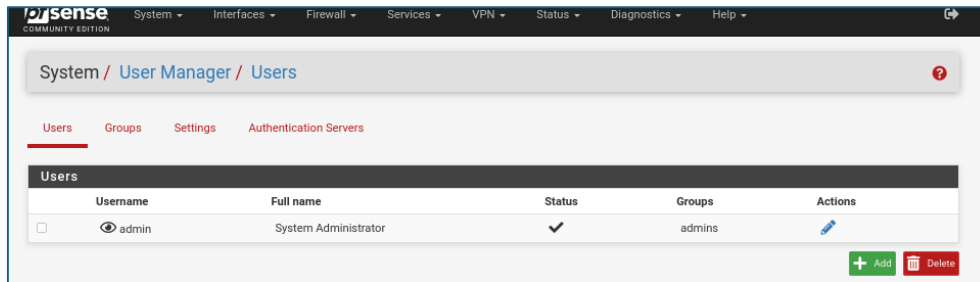
VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards Client Export

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	192.168.143.0/24	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	OpenVPNXicola	Edit Clone Delete

- Ahora Creo el usuario, Nos vamos a:
System > User manager > Users



- Y agregamos usuario nuevo (add)
- Rellenamos los datos siguientes:

Nombre, fullname, Passwrđ

- Y el certificado para el usuario (le damos ok a la checkbox)

A screenshot of the 'User Properties' form in the PfSense User Manager interface. The form is titled 'User Properties' and has tabs for 'Users', 'Groups', 'Settings', and 'Authentication Servers'. The 'Users' tab is active. The form contains several fields: 'Defined by' (USER), 'Disabled' (checkbox), 'Username' (vpnuser_test), 'Password' (masked), 'Full name' (vpnuser_test), 'Expiration date' (empty), 'Custom Settings' (checkbox), 'Group membership' (admins), and 'Certificate' (checkbox). The 'Certificate' checkbox is checked and highlighted with a red box. Below the 'Certificate' checkbox is a link 'Click to create a user certificate'. There are also buttons for 'Move to "Member of" list' and 'Move to "Not member of" list'.

- Completamente necesario hacer y rellenar el certificado para el usuario.

El certificado creado agragamos

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

Ahora Nos vamos a VPN > OpenVPN > Client Export

- Seleccionamos la VPN en RAS Sever
- En Host Name Resolution hemos de escoger la IP que este expuesta en mi caso la de la interficie
- Verify server CN: lo dejamos
- Block outside DNS: para prevenir las filtraciones de DNS Win10, Pero lo dejamos como esta, no usamos win10

, abajo nos aparecerán los usuarios, en mi caso lo usaré con Most Clients, que nos exporta un .ovpn:

PfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

OpenVPN / Client Export Utility

Server Client Client Specific Overrides Wizards Client Export

OpenVPN Server

Remote Access Server

Client Connection Behavior

Host Name Resolution

Verify Server CN
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.

- Marcamos create Certificate y rellenamos los datos, es necesario para conectarnos:

Method -> Create an internal Certificate

Y dejamos todo por default.

The screenshot shows the PfSense web interface for managing certificates. The breadcrumb trail is 'System / Certificates / Certificates / Edit'. There are three tabs: 'Authorities', 'Certificates' (selected), and 'Certificate Revocation'. The main section is titled 'Add/Sign a New Certificate'. A red box highlights the 'Method' dropdown menu, which is set to 'Create an internal Certificate'. Below this, the 'Descriptive name' field is filled with 'vpnuser_test'. The 'Internal Certificate' section contains several fields: 'Certificate authority' is set to 'OpenVPNtest'; 'Key type' is set to 'RSA'; 'Key length' is set to '2048'; 'Digest Algorithm' is set to 'sha256'; 'Lifetime (days)' is set to '3650'; and 'Common Name' is set to 'e.g. www.example.com'. At the bottom, there are optional fields for 'Country Code' (set to 'ES'), 'State or Province' (set to 'Spain'), and 'City' (set to 'Barcelona').

System / Certificates / Certificates / Edit

Authorities Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create an internal Certificate

Descriptive name vpnuser_test

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 OpenVPNtest

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 e.g. www.example.com

The following certificate subject components are optional and may be left blank.

Country Code ES

State or Province Spain

City Barcelona

- Guardamos, y ya podemos descargar

Organizational Unit

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
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names
Type Value

Add SAN Row [+ Add SAN Row](#)

[Save](#)

- Le damos a Most Clients y descargaria ja el fitxer

Search

Search term [Search](#) [Clear](#)

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

OpenVPN Clients

User	Certificate Name	Export
vpnuser_test	vpnuser_test	<div><p>- Inline Configurations:</p><p>Most Clients Android OpenVPN Connect (iOS/Android)</p><p>- Bundled Configurations:</p><p>Archive Config File Only</p><p>- Current Windows Installers (2.6.7-ix001):</p><p>64-bit 32-bit</p><p>- Previous Windows Installers (2.5.9-ix601):</p><p>64-bit 32-bit</p><p>- Legacy Windows Installers (2.4.12-ix601):</p><p>10/2016/2019 7/8/8.1/2012x2</p><p>- Viscosity (Mac OS X and Windows):</p><p>Viscosity Bundle Viscosity Inline Config</p></div>

Only OpenVPN-compatible user certificates are shown