



TP VPN pfSense

---

FLORENTIN BRACQ-FLABAT BTS 2 SIO



# Qu'est-ce qu'un VPN ?

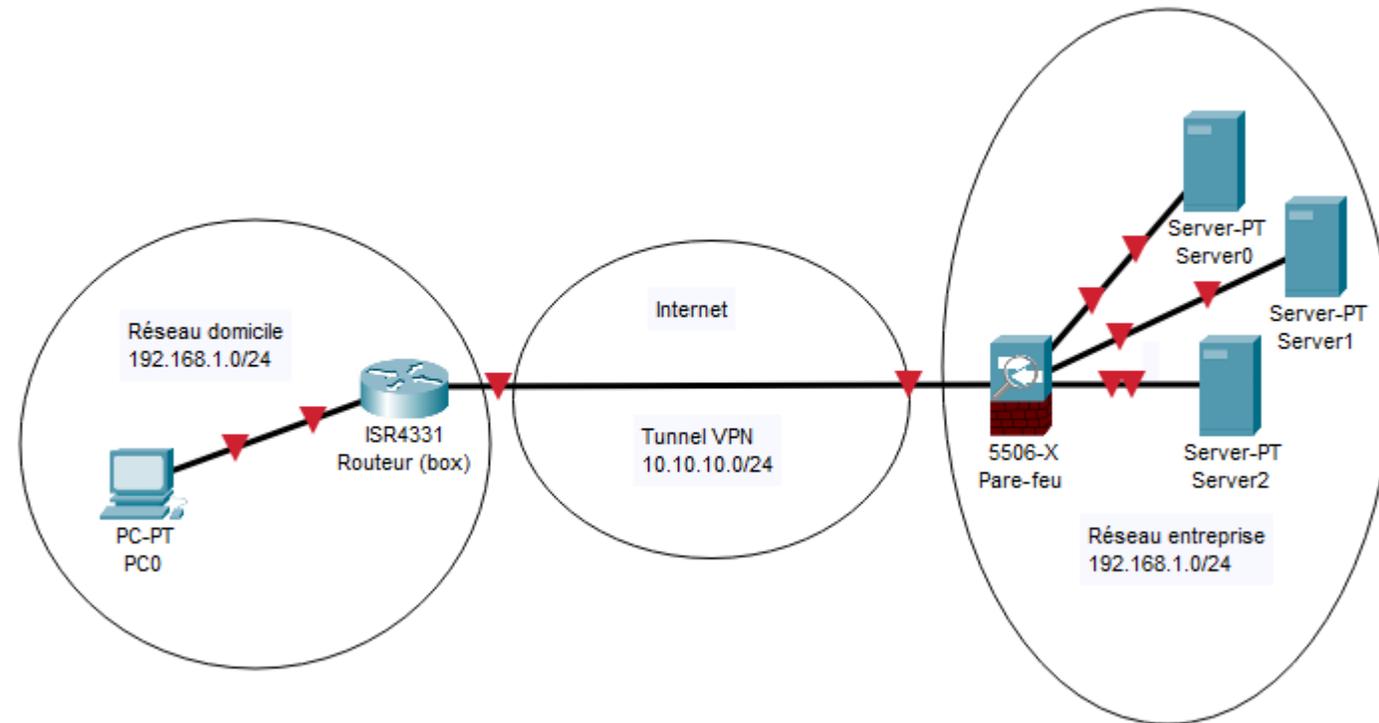
---

Un VPN, ou Virtual Private Network (réseau privé virtuel), est une technologie qui permet de créer une connexion sécurisée et chiffrée entre votre appareil (ordinateur, smartphone, etc.) et un serveur distant via Internet.



# Schéma réseau

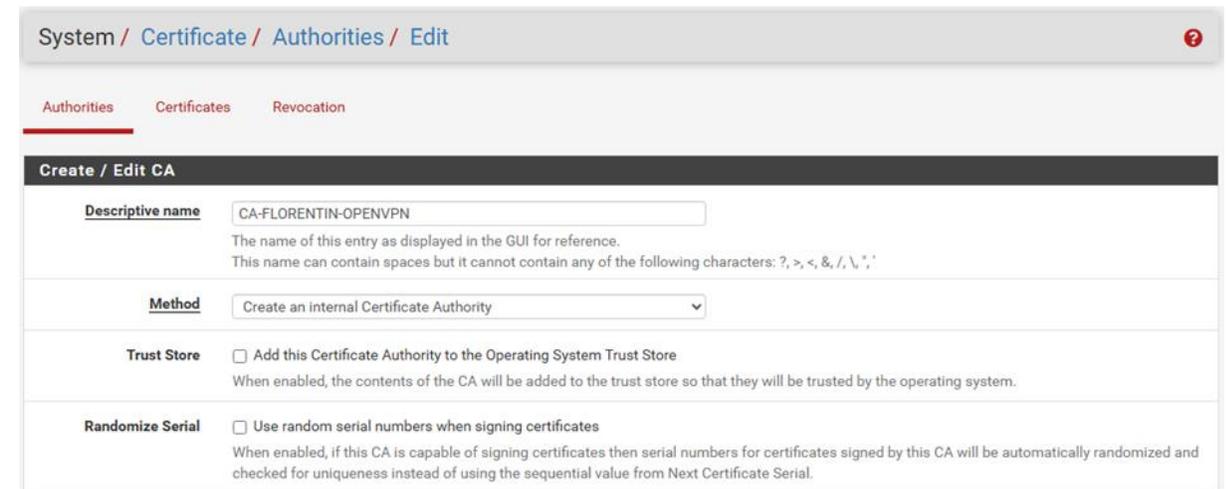
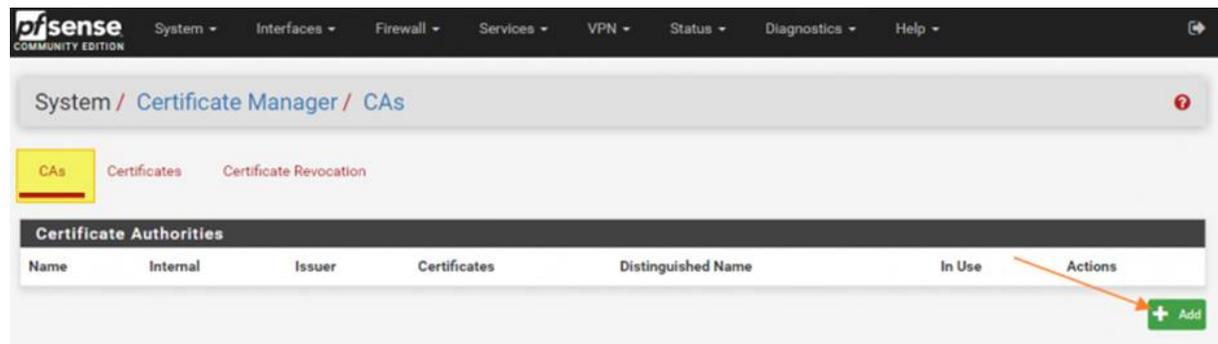
---



# Création de l'autorité de certification

Une fois connecté à l'interface web d'administration de pfSense, cliquer sur System puis Cert. Manager (Certificates), dans l'onglet Cas, cliquer sur Add

Donner un nom à l'autorité de certification CA-FLORENTIN-OPENVPN, et choisir Create an internal Certificate Authority



# Création de l'autorité de certification

Pour Common Name, mettre florentin et compléter les autres valeurs : la région, la ville, etc... et cliquez sur "Save" pour créer la CA.

**Internal Certificate Authority**

**Key type** RSA

1024  
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 CA 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

**Common Name** florentin

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

**Country Code** FR

**State or Province** Nord

**City** Cambrai

**Organization** Florentin Informatique

**Organizational Unit** e.g. My Department Name (optional)

**Save**

System / Certificate / Authorities

**Authorities** Certificates Revocation

**Search**

Search term  Both

Enter a search string or \*nix regular expression to search certificate names and distinguished names.

**Certificate Authorities**

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA-FLORENTIN-OPENVPN	✓	self-signed	0	ST=Nord, O=Florentin Informatique, L=Cambrai, CN=florentin, C=FR Valid From: Sun, 24 Nov 2024 15:35:14 +0100 Valid Until: Wed, 22 Nov 2034 15:35:14 +0100	<input type="checkbox"/>	

# Création du certificat interne

Cliquer ensuite sur l'onglet Certificates et cliquer sur Add

The screenshot shows the pfSense web interface for managing certificates. The breadcrumb trail is 'System / Certificates / Certificates'. There are three tabs: 'Authorities', 'Certificates' (which is selected and underlined), and 'Certificate Revocation'. Below the tabs is a search bar with a 'Search term' input field, a 'Both' dropdown menu, and 'Search' and 'Clear' buttons. A note below the search bar says 'Enter a search string or \*nix regular expression to search certificate names and distinguished names.' Below the search bar is a table titled 'Certificates' with the following columns: 'Name', 'Issuer', 'Distinguished Name', 'In Use', and 'Actions'. There is one entry in the table: 'webConfigurator default (67433b8b7d707) Server Certificate'. The 'In Use' column shows 'webConfigurator' and the 'Actions' column contains icons for edit, delete, and refresh. At the bottom right of the table area is a green '+ Add/Sign' button.

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (67433b8b7d707) Server Certificate CA: No Server: Yes	self- signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense- 67433b8b7d707 ⓘ Valid From: Sun, 24 Nov 2024 15:43:23 +0100 Valid Until: Sat, 27 Dec 2025 15:43:23 +0100	webConfigurator	  

# Création du certificat interne

Choisir la méthode Create an Internal Certificate puisqu'il s'agit d'une création, donnez-lui un nom et sélectionnez l'autorité de certification au niveau du paramètre "Certificate authority".

System / Certificates / Certificates / Edit ?

Authorities Certificates Certificate Revocation

### Add/Sign a New Certificate

**Method** Create an internal Certificate

**Descriptive name** Certificat-OpenVPN

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** CA-FLORENTIN-OPENVPN

**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** florentin-firewall

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

**Country Code** FR

**State or Province** Nord

**City** Cambrai

**Organization** Florentin Informatique

**Organizational Unit** e.g. My Department Name (optional)

# Création du certificat interne

Choisissez bien le type de certificat (Certificate Type) suivant : Server Certificate et cliquer sur save pour enregistrer les modifications.

**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

Save

Après avoir cliqué sur "Save" pour valider la création du certificat, il apparaît dans la liste des certificats du Pare-feu :

System / Certificates / Certificates

Created internal certificate Certificat-OpenVPN

Authorities Certificates Certificate Revocation

Search

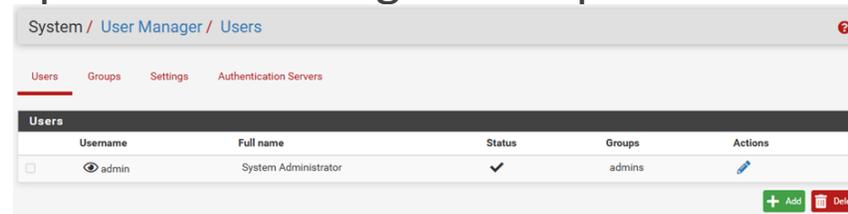
Search term Both Search Clear

Enter a search string or \*nix regular expression to search certificate names and distinguished names.

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (674236b7d707) Server Certificate CA: No Server: Yes	self-signed	OrgPSense webConfigurator Self-Signed Certificate, CN=OrgSense-674236b7d707 Valid from: Sun, 24 Nov 2024 16:43:23 +0100 Valid Until: Sat, 27 Dec 2025 15:43:23 +0100	webConfigurator	  
Certificat-OpenVPN Server Certificate CA: No Server: Yes	CA-FLORENTIN-OPENVPN	ST=Nord, O=Florentin Informatique, L=Cambrai, CN=florentin-fwwall-Ci-FR Valid from: Sun, 24 Nov 2024 16:16:01 +0100 Valid Until: Wed, 22 Nov 2034 16:16:01 +0100		  

# Création des utilisateurs locaux

Cliquer en haut dans System puis User Manager et cliquer sur Add



Donner un nom au nouvel utilisateur, définir un mot de passe et cocher la case certificate

A screenshot of the 'System / User Manager / Users / Edit' page. The page title is 'System / User Manager / Users / Edit'. Below the navigation tabs, there is a 'User Properties' section. The form includes the following fields and options:

- Defined by:** USER
- Disabled:**  This user cannot login
- Username:** florentin
- Password:** Two password input fields with masked characters.
- Full name:** (empty field) with a note: 'User's full name, for administrative information only'
- Expiration date:** (empty field) with a note: '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:** A dropdown menu showing 'admins'. Below it are two more dropdowns: 'Not member of' and 'Member of'. There are also buttons to 'Move to Member of list' and 'Move to Not member of list'.
- Certificate:**  Click to create a user certificate

# Création des utilisateurs locaux

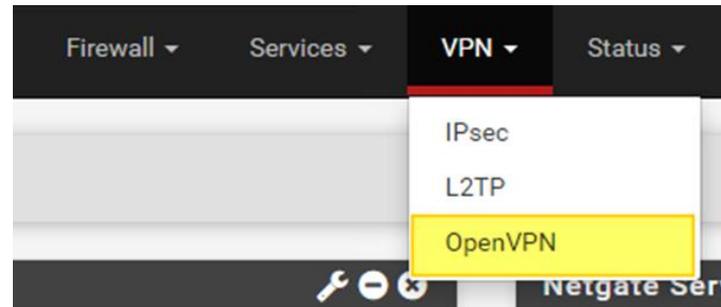
---

Donner un nom au certificat utilisateur qui va être créé et cliquer sur Save pour enregistrer les modifications :

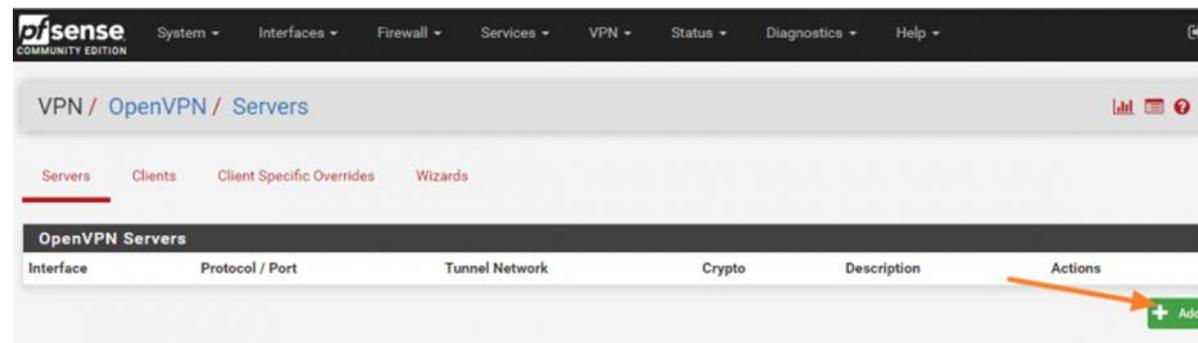
Create Certificate for User	
<b>Descriptive name</b>	<input type="text" value="Certificat-VPN-Florentin"/>
<b>Certificate authority</b>	<input type="text" value="CA-FLORENTIN-OPENVPN"/> ▼
<b>Key type</b>	<input type="text" value="RSA"/> ▼
	<input type="text" value="2048"/> ▼ The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
<b>Digest Algorithm</b>	<input type="text" value="sha256"/> ▼ 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
<b>Lifetime</b>	<input type="text" value="3650"/>

# Configurer le serveur OpenVPN

Cliquer sur le menu « VPN » puis « OpenVPN »



Dans l'onglet « Servers », cliquer sur « Add » pour créer une nouvelle configuration.



# Configurer le serveur OpenVPN

Toujours dans l'onglet Serveurs, donner une description, pour Serveur mode, choisir Remote Access (SSL/TLS + User Auth)

VPN / OpenVPN / Servers / Edit

Servers Clients Client Specific Overrides Wizards

### General Information

**Description**   
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**

**Backend for authentication**

**Device 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**

**Interface**   
The interface or Virtual IP address where OpenVPN will receive client connections.

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

# Configurer le serveur OpenVPN

Pour serveur certificate choisir le certificat serveur crée précédemment et pour Fallback Data Encryption choisir AES-256-CBC :

**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.

**Peer Certificate Authority** CA-FLORENTIN-OPENVPN

**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** Certificat-OpenVPN (Server: Yes, CA: CA-FLORENTIN-OPENVPN)  
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. [i](#)

**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 as a fallback.

**Data Encryption Algorithms**

<ul style="list-style-type: none"><li>AES-128-CBC (128 bit key, 128 bit block)</li><li>AES-128-CFB (128 bit key, 128 bit block)</li><li>AES-128-CFB1 (128 bit key, 128 bit block)</li><li>AES-128-CFB8 (128 bit key, 128 bit block)</li><li>AES-128-GCM (128 bit key, 128 bit block)</li><li>AES-128-OFB (128 bit key, 128 bit block)</li><li>AES-192-CBC (192 bit key, 128 bit block)</li><li>AES-192-CFB (192 bit key, 128 bit block)</li><li>AES-192-CFB1 (192 bit key, 128 bit block)</li><li>AES-192-CFB8 (192 bit key, 128 bit block)</li></ul>	<ul style="list-style-type: none"><li>AES-256-GCM</li><li>AES-128-GCM</li><li>CHACHA20-POLY1305</li></ul>
---	---

Available Data Encryption Algorithms  
Click to add or remove an algorithm from the list

Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list

The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode. [i](#)

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

# Configurer le serveur OpenVPN (Tunnel VPN)

Donner l'adresse IP du tunnel 10.10.10.0/24

Donner l'adresse IP du réseau local 192.168.1.0/24

Et définir le nombre de connexion simultanée maximum par exemple 10

Tunnel Settings	
<b>IPv4 Tunnel Network</b>	<input type="text" value="10.10.10.0/24"/> <small>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.</small>
<b>IPv6 Tunnel Network</b>	<input type="text"/> <small>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.</small>
<b>Redirect IPv4 Gateway</b>	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
<b>Redirect IPv6 Gateway</b>	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
<b>IPv4 Local network(s)</b>	<input type="text" value="192.168.1.0/24"/> <small>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.</small>
<b>IPv6 Local network(s)</b>	<input type="text"/> <small>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.</small>
<b>Concurrent connections</b>	<input type="text" value="10"/> <small>Specify the maximum number of clients allowed to concurrently connect to this server.</small>

# Configurer le serveur OpenVPN

---

Pour la partie Client Settings

Activer le Dynamic IP si les clients sont nomades et que leur adresse IP publique change pour maintenir la connexion VPN, activer le protocole net30 qui permettra à chaque client connecté de se trouver dans un sous réseau sans pouvoir communiquer avec les autres clients en VPN.



The screenshot shows the 'Client Settings' configuration panel. It features a dark header with the title 'Client Settings'. Below the header, there are two main sections. The first section, 'Dynamic IP', includes a checked checkbox and the text 'Allow connected clients to retain their connections if their IP address changes.' The second section, 'Topology', contains a dropdown menu currently set to 'net30 - Isolated /30 network per client'. Below the dropdown is a descriptive paragraph: 'Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".'

# Configurer le serveur OpenVPN

---

Et pour Advanced Configuration, dans Custom options activer l'option `auth-nocache` qui permettra d'empêcher la mise en cache de l'authentification pour éviter une fuite des authentifications. Cliquer sur save pour enregistrer les modifications.

**Advanced Configuration**

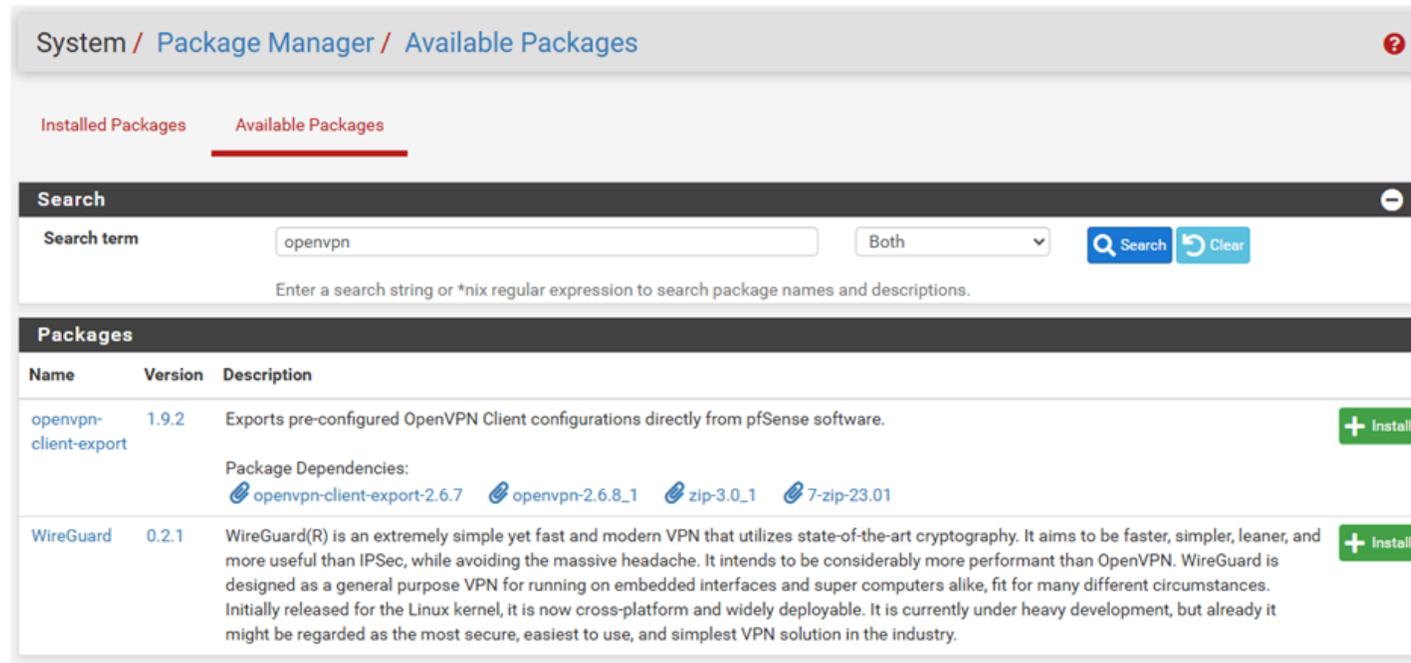
**Custom options**

```
auth-nocache
```

Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.  
EXAMPLE: push "route 10.0.0.0 255.255.255.0"

# Installer le paquet client export

Dans la barre en haut, cliquer sur System puis Package Manager, puis cliquer sur l'onglet Available Package rechercher openvpn et installer le paquet openvpn-client-export



The screenshot shows the pfSense Package Manager interface. At the top, the breadcrumb navigation reads "System / Package Manager / Available Packages". Below this, there are two tabs: "Installed Packages" and "Available Packages", with the latter being the active tab. A search bar is present with the search term "openvpn" and a dropdown menu set to "Both". There are "Search" and "Clear" buttons. Below the search bar, a message says "Enter a search string or \*nix regular expression to search package names and descriptions." The main content area is titled "Packages" and contains a table with the following data:

Name	Version	Description	
openvpn-client-export	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software.  Package Dependencies: <a href="#">openvpn-client-export-2.6.7</a> <a href="#">openvpn-2.6.8_1</a> <a href="#">zip-3.0.1</a> <a href="#">7-zip-23.01</a>	<a href="#">+ Install</a>
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.	<a href="#">+ Install</a>

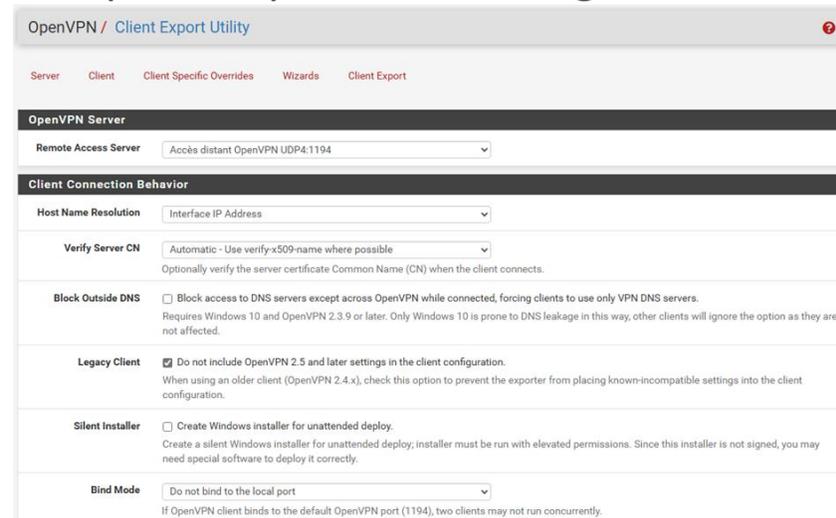
# Exporter la configuration utilisateur

Dans la barre en haut cliquer sur VPN, puis OpenVPN et cliquer sur l'onglet Client Export

Choisir pour Host Name Resolution Interface IP Address et cocher la case Legacy Client pour les utilisateurs qui utilisent une version antérieure d'Open VPN.

Cliquer enfin sur Save as default

Et télécharger la version archive pour exporter la configuration VPN pour un utilisateur.



The screenshot shows the 'OpenVPN / Client Export Utility' window. The 'Client Export' tab is active. The 'OpenVPN Server' section has 'Remote Access Server' set to 'Accès distant OpenVPN UDP4:1194'. The 'Client Connection Behavior' section has 'Host Name Resolution' set to 'Interface IP Address' and 'Verify Server CN' set to 'Automatic - Use verify-x509-name where possible'. The 'Legacy Client' checkbox is checked, with the label 'Do not include OpenVPN 2.5 and later settings in the client configuration.' The 'Block Outside DNS' checkbox is unchecked. The 'Silent Installer' checkbox is unchecked. The 'Bind Mode' dropdown is set to 'Do not bind to the local port'.

# Modifier les règles de parefeu

Dans la barre en haut, cliquer sur Firewall, Rules, cliquer sur Add.

Créer une 1ère règle pour autoriser la connexion VPN

Cliquer sur save et appliquer les modifications

The screenshot shows the 'Edit Firewall Rule' configuration page in Mikrotik WinBox. The breadcrumb navigation at the top reads 'Firewall / Rules / Edit'. The main configuration area is divided into several sections:

- Action:** Set to 'Pass'. A note explains that 'Pass' allows packets, while 'block' or 'reject' would discard or return them to the sender.
- Disabled:** A checkbox for 'Disable this rule' is unchecked.
- Interface:** Set to 'WAN'.
- Address Family:** Set to 'IPv4'.
- Protocol:** Set to 'UDP'.

The **Source** section includes an 'Invert match' checkbox (unchecked), a dropdown for 'Any', and a 'Source Address' field. A 'Display Advanced' button is visible. A note states: '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.'

The **Destination** section includes an 'Invert match' checkbox (unchecked), a dropdown for 'WAN address', and a 'Destination Address' field. The **Destination Port Range** is configured with 'From' set to '1194' (Custom) and 'To' set to '1194' (Custom). A note at the bottom states: 'Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.'

# Modifier les règles de parefeu

Cliquer sur l'onglet OpenVPN et créer une nouvelle règle dans le Firewall, par exemple autoriser à utiliser le protocole RDP pour se connecter sur une machine distante

### Destination

**Destination**  Invert match Address or Alias 192.168.1.100 /

**Destination Port Range** (other) 3389 (other) 3389  
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** Autoriser RDP vers PC Windows 10  
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

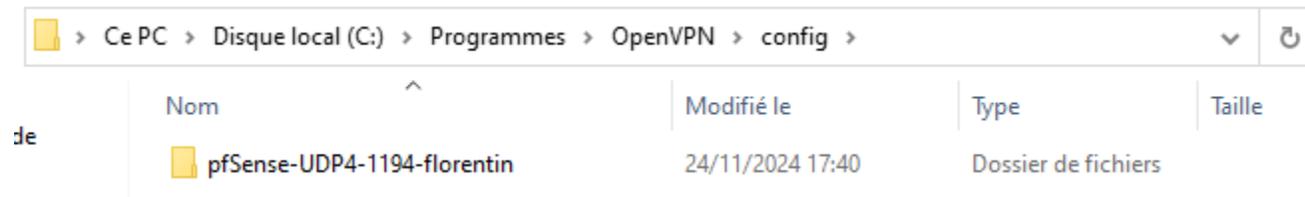
Save

# Connexion en VPN

---

Installer OpenVPN sur une machine cliente

Copier le dossier dans l'archive téléchargée précédemment dans  
C:\Programmes\OpenVPN\config



Se connecter avec OpenVPN à l'aide des identifiants de connexion de l'utilisateur

# Sources

---

<https://www.it-connect.fr/pfsense-configurer-un-vpn-ssl-client-to-site-avec-openvpn/>

<https://www.youtube.com/watch?v=QDaRpaIH4GE>