



# Document d'exploitation

---

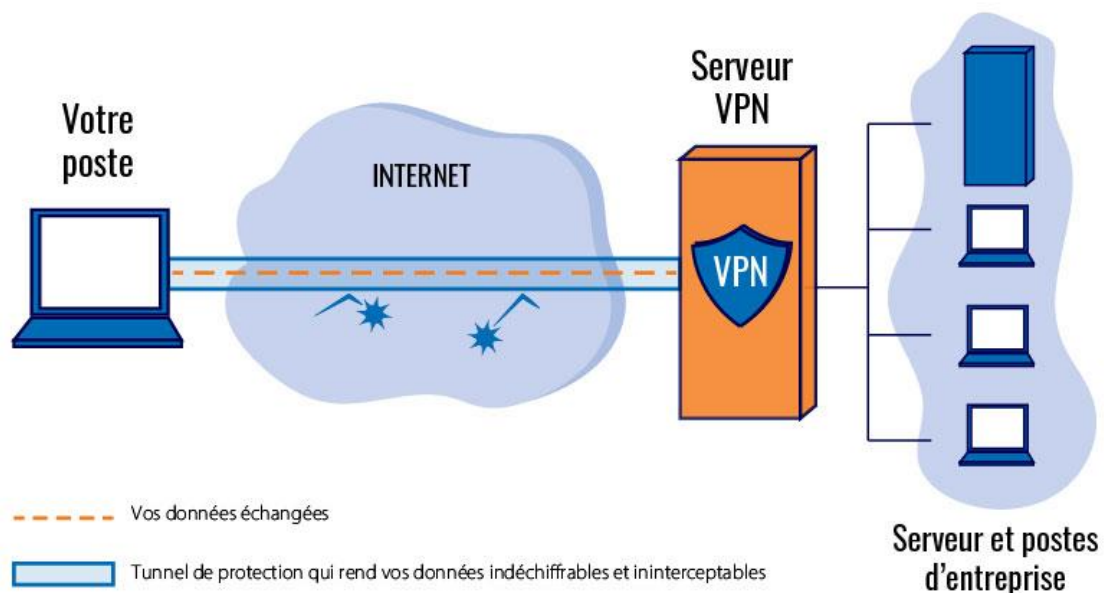
- I. Qu'est-ce qu'un vpn ?**
- II. La gestion des certificats**
  - A. Créer l'autorité de certification**
  - B. Créer le certificat Server**
- III. Créer les utilisateurs locaux**
- IV. Configurer le serveur OpenVPN**
- V. Exporter la configuration OpenVPN**
- VI. Créer les règles de firewall pour OpenVPN**
- VII. Tester l'accès distant depuis un poste client**

# I. Qu'est-ce qu'un vpn ?

Je vais vous montrer comment configurer un VPN SSL client à client avec PfSense en utilisant OpenVPN afin que nos ordinateurs puissent accéder à des serveurs distants.

Ce type de VPN sert à établir une connexion directe entre un ordinateur et un réseau d'entreprise grâce à un tunnel crypté et sécurisé.

Dans cet exemple, j'utilise la base d'utilisateurs locale du pare-feu.



## B. Créer le certificat Server

Nous devons créer un certificat de type "Server" en nous basant sur notre nouvelle autorité de certification. Toujours dans "*Certificate Manager*", cette fois-ci dans l'onglet "*Certificates*", cliquez sur le bouton "*Add/Sign*".

The screenshot shows a web browser window with the URL `192.168.10.1/system_certmanager.php?act=new`. The page title is "System / Certificate Manager / Certificates / Edit". The breadcrumb navigation shows "CAs", "Certificates", and "Certificate Revocation". The main heading is "Add/Sign a New Certificate".

The form contains the following fields:

- Method:** A dropdown menu with "Create an internal Certificate" selected.
- Descriptive name:** A text input field containing "certificat openvpn".
- Internal Certificate:**
  - Certificate authority:** A dropdown menu with "iccmn-sqy" selected.
  - Key type:** A dropdown menu with "RSA" selected.
  - Key length:** A dropdown menu with "2048" selected. Below it, a note states: "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:** A dropdown menu with "sha256" selected. Below it, a note states: "The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider".

A watermark "Activer Windows" is visible on the right side of the form.

The screenshot shows the "Certificate Attributes" section of the form. It contains the following fields:

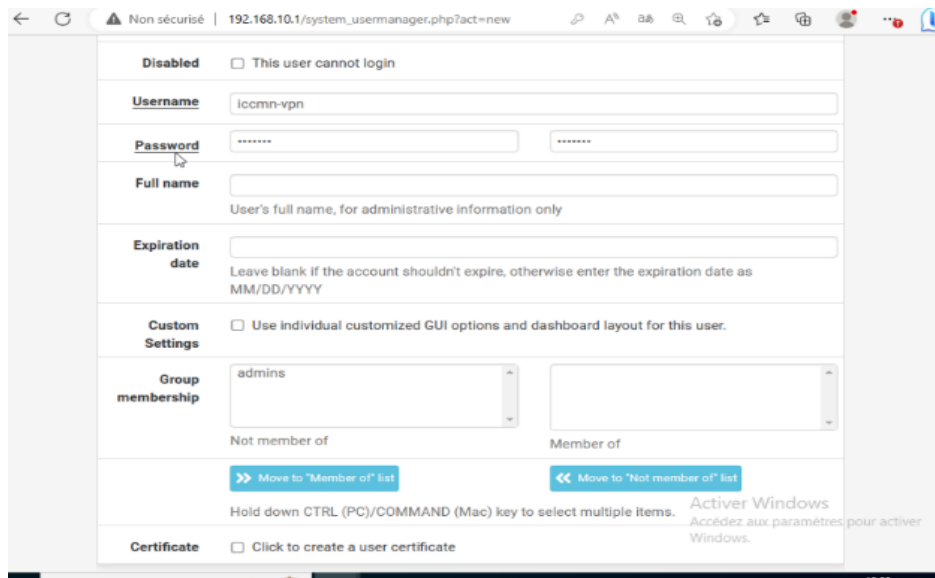
- State or Province:** A text input field with a blurred value.
- City:** A text input field with a blurred value.
- Organization:** A text input field with a blurred value.
- Organizational Unit:** A text input field containing "e.g. My Department Name (optional)".
- Certificate Attributes:**
  - Attribute Notes:** A text area containing the text: "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:** A dropdown menu with "Server Certificate" selected. Below it, a note states: "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:** A dropdown menu with "FQDN or Hostname" selected.
    - Value:** A text input field.
    - A note below states: "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."

A watermark "Activer Windows" is visible on the right side of the form.

### III. Créer les utilisateurs locaux

Il faut créer un utilisateur ainsi qu'un certificat de type "User" pour l'authentification VPN.

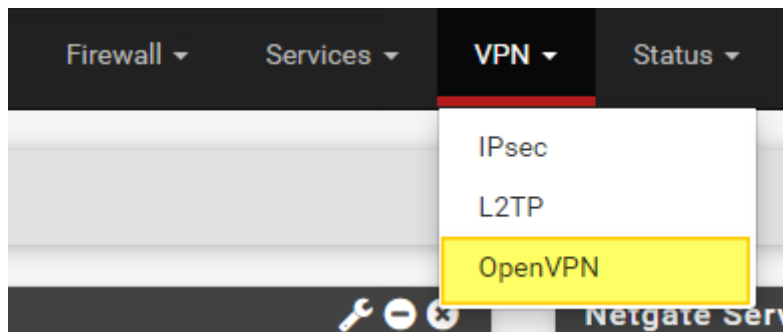
Pour créer l'utilisateur, il faut indiquer un identifiant, un mot de passe... Ainsi que cocher l'option **"Click to create a user certificate"** : cela va ajouter le formulaire de création du certificat juste en dessous. Pour créer le certificat, on se base sur notre autorité de certification



### IV. Configurer le serveur OpenVPN

Maintenant que la partie certificat est opérationnelle et que nous disposons d'un compte utilisateur, on peut s'attaquer à la configuration du VPN.

Cliquez sur le menu "VPN" puis "OpenVPN"



Ensuite, j'ai choisi le **"Server Mode"** suivant : **Remote Access (SSL/TLS + User Auth)**.

Pour le VPN, le protocole s'appuie sur de l'UDP, avec le port 1194 par défaut or nous en avons choisis un différent pour soucis de sécurité. Pour l'interface, nous allons conserver "WAN" puisque c'est bien par cette interface que l'on va se connecter en accès distant.

**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** 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

Pour l'algorithme de chiffrement (**Encryption Algorithm**), nous pouvons passer sur de l'**AES-256-CBC** plutôt que de l'**AES-128-CBC**. La sécurité sera renforcée, mais cela impact légèrement les performances, car le processus de chiffrement est alourdi : il sera toujours

**certificate**

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

**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 Negotiation** ☒ Enable Data Encryption Negotiation   
 This option allows OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic data encryption algorithms from those selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.

**Data Encryption Algorithms**

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

AES-128-GCM (128 bit key, 128 bit block)  
 AES-128-OFB (128 bit key, 128 bit block)  
 AES-192-CBC (192 bit key, 128 bit block)  
 AES-192-CFB (192 bit key, 128 bit block)  
 AES-192-CFB1 (192 bit key, 128 bit block)  
 AES-192-CFB8 (192 bit key, 128 bit block)  
 AES-192-GCM (192 bit key, 128 bit block)  
 AES-192-OFB (192 bit key, 128 bit block)  
 AES-256-CBC (256 bit key, 128 bit block)  
 AES-256-CFB (256 bit key, 128 bit block)  
 AES-256-CFB1 (256 bit key, 128 bit block)  
 AES-256-CFB8 (256 bit key, 128 bit block)


AES-256-CBC

possible de modifier cette valeur. Enfin on rentre l'adresse du tunnel vpn que l'on souhaite choisir puis les adresses à laquelle l'on souhaite donner accès.

<b>IPv4 Tunnel Network</b>	<input type="text" value="10.50.50.0/29"/>
<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.</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="10.74.0.202/24, 192.168.10.0/24, 172.20.0.0/27, 172.30.0.0/28, 192.168.40.0/26, 10.50.50.0/29"/>
<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"/>

Active Windows  
Accédez aux paramètres pour Windows



<b>TLS Configuration</b>	<input checked="" type="checkbox"/> 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.
	<input checked="" type="checkbox"/> Automatically generate a TLS Key.
<b>Peer Certificate Authority</b>	<div>iccmn-sqy</div>
<b>Peer Certificate Revocation list</b>	No Certificate Revocation Lists defined. One may be created here: <a href="#">System &gt; Cert. Manager</a>
<b>OCSP Check</b>	<input type="checkbox"/> Check client certificates with OCSP
<b>Server certificate</b>	<div>certificat openvpn (Server: Yes, CA: iccmn-sqy)</div>
<b>DH Parameter Length</b>	<div>2048 bit</div> <div>Diffie-Hellman (DH) parameter set used for key exchange. </div>
<b>ECDH Curve</b>	<div>Use Default</div>

## V. Exporter la configuration OpenVPN

Pour télécharger la configuration au format ".ovpn", il est nécessaire d'installer un paquet supplémentaire sur notre pare-feu. Rendez-vous dans le menu suivant : **System > Package Manager > Available Packages**.

Recherchez "openvpn" et installez le paquet : **openvpn-client-export**.

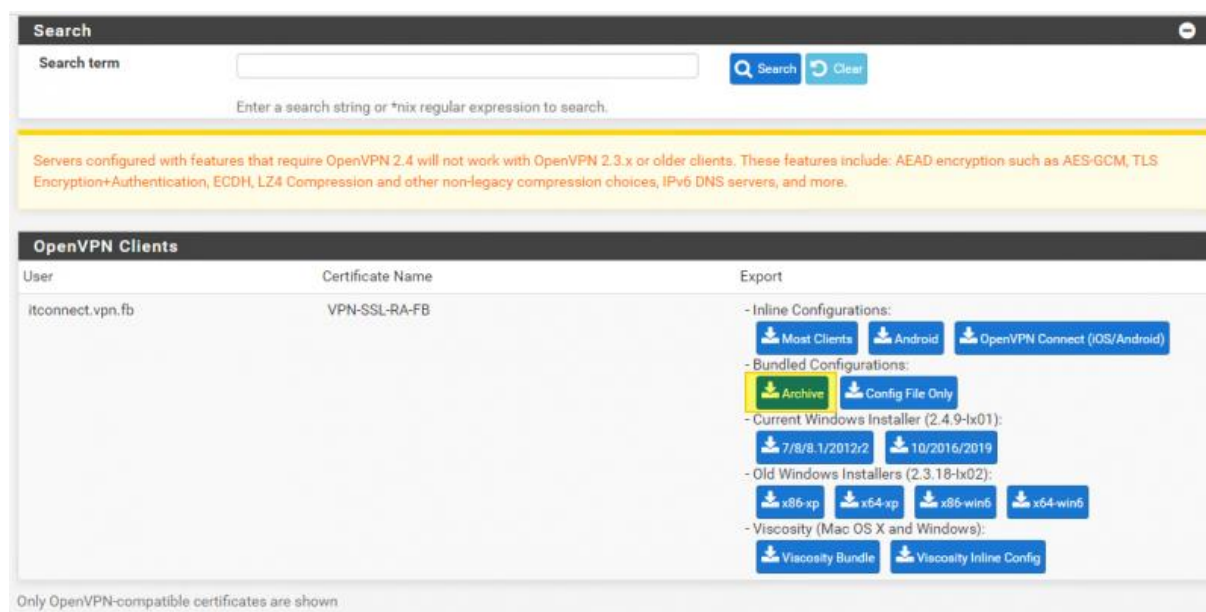


Lorsque c'est fait, retournez dans le menu "OpenVPN" puis dans l'onglet "Client Export".

Si vous souhaitez utiliser l'adresse IP publique pour vous connecter, utilisez l'option "Interface IP Address" pour l'option "Host Name Resolution". Il y a d'autres options possibles, notamment par nom de domaine. De plus, Il y a seulement notre option "auth-nocache" à reporter dans la section des options additionnelles.

.

En dessous de la part configuration, vous avez la possibilité de télécharger la configuration. Pour utiliser OpenVPN Community, il faudra prendre la configuration "Bundled Configuration", au format archive pour récupérer tous les fichiers nécessaires.



Il faut ensuite décompresser le fichier archive dans le dossier config d'openvpn.

Téléchargements > FW-PFSENSE-UDP4		-config.zip > FW-PFSENSE-UDP4		-vpn.fb	
Nom	Type	Taille compressée	Protégé		
FW-PFSENSE-UDP4	b.ovpn	Fichier OVPN	1 Ko	Non	
FW-PFSENSE-UDP4	b.p12	Échange d'informations p...	4 Ko	Non	
FW-PFSENSE-UDP4	tls.key	Fichier KEY	1 Ko	Non	

## VI. Créer les règles de firewall pour OpenVPN

D'une part, nous devons créer une règle pour autoriser les clients à monter la connexion VPN, et d'autre part nous devons créer une ou plusieurs règles pour autoriser l'accès aux ressources : serveur en RDP, serveur de fichiers, application web, etc.

Cliquez sur le menu "Firewall" > "WAN". Il est nécessaire de créer une nouvelle règle pour l'interface WAN, en sélectionnant le protocole UDP.

La destination ce sera notre adresse IP publique donc sélectionnez "WAN address". Pour le port, prenez OpenVPN dans la liste ou alors indiquez votre port personnalisé.

Validez la création de la règle et appliquez la configuration.

À partir de ce moment-là, il est possible de monter le tunnel VPN sur un PC, mais les ressources de votre entreprise seront inaccessibles.

Ajoutez une nouvelle règle, cette fois-ci sur l'interface OpenVPN.

La règle qui suit sert à autoriser l'accès en RDP à l'hôte 192.168.1.30 (qui fait bien parti du réseau autorisé dans la configuration du VPN) au travers du tunnel VPN. Vous devez créer une ou plusieurs règles en fonction des ressources auxquelles vos utilisateurs doivent accéder via le VPN, en limitant les flux au maximum.

## VII. Tester l'accès distant depuis un poste client

Puis se connecter au vpn à l'aide des identifiants et mot de passes de l'utilisateur créés.

