

## Introduction

Pour ce type de VPN c'est assez simple il faut créer une autorité de certification sur Pfsense ensuite un certificat de serveur et créer un utilisateur plus un certificat utilisateur pour ce dernier.

Ensuite il faudra créer la config du serveur Openvpn sur le pfsense

Puis il faudra installer un paquet sur le Pfsense qui permettra d'exporter une config toute prête pour mes différents clients.

## Autorité de certification



Voilà on souhaite créer une autorité de certification interne on définit le nom

pfSense COMMUNITY EDITION

Système - Interfaces - Pare-feu - Services - VPN - État - Diagnostics - Aide

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Système / Gestionnaire de certificats / ACs / Modifier

ACs Certificats Révocation de certificat

**Créer / Modifier l'AC**

Nom descriptif CA-VPN

Méthode Créer une autorité de certification interne

Trust Store  Add this Certificate Authority to the Operating System Trust Store  
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial  Use random serial numbers when signing certiffices  
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

**Autorité de certification interne**

Key type RSA

4096  
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.

Algorithme de hachage sha256  
The digest method used when the CA is signed.  
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.

Activer Windows  
Accédez aux paramètres pour activer Windows.

Voilà les paramètres basique du certificat durée de vie pays etc

Durée de vie (jours) 3650

Nom commun internal-ca

Les composantes suivantes de l'autorité de certification sont facultatives et peuvent être laissées vides.

Code du pays Aucun

État ou province FR

Ville Paris

Organisation sadek-info

Unité organisationnelle e.g. My Department Name (optional)

Enregistrer

Activer Windows  
Accédez aux paramètres pour activ

## Un petit récapitulatif

The screenshot shows the 'Gestionnaire de certificats / ACs' page. At the top, there are navigation tabs for 'ACs', 'Certificats', and 'Révocation de certificat'. Below this is a search bar labeled 'Recherche' with a text input field, a dropdown menu set to 'Les deux', and buttons for 'Recherche' and 'Effacer'. 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 'Autorités de certification' with columns: 'Nom', 'Interne', 'Émetteur', 'Certificats', 'Nom distinctif', 'En cours d'utilisation', and 'Actions'. The table contains one entry for 'CA-VPN' with a checkmark in the 'Interne' column, 'auto-signé' as the issuer, '0' certificates, and a distinguished name 'ST=FR, O=sadek-info, L=Paris, CN=internal-ca'. It also shows validity dates from Saturday, 04 Nov 2023 01:48:43 +0000 to Tuesday, 01 Nov 2033 01:48:43 +0000. An 'Ajouter' button is at the bottom right.

## Certificat serveur

Ensuite créer le certificat serveur qui permettra d'authentifier le serveur.

The screenshot shows the 'Gestionnaire de certificats / Certificats' page. At the top, there are navigation tabs for 'ACs', 'Certificats', and 'Révocation de certificat'. Below this is a search bar labeled 'Recherche' with a text input field, a dropdown menu set to 'Les deux', and buttons for 'Recherche' and 'Effacer'. 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 'Certificats' with columns: 'Nom', 'Émetteur', 'Nom distinctif', 'En cours d'utilisation', and 'Actions'. The table contains one entry for 'webConfigurator default (653454e4aa50f) Server Certificate' with 'auto-signé' as the issuer, a distinguished name 'O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-653454e4aa50f', and 'webConfigurator' as the usage. It also shows validity dates from Saturday, 21 Oct 2023 22:47:00 +0000 to Friday, 22 Nov 2024 22:47:00 +0000. An 'Ajouter/Signer' button is at the bottom right.

ACs   Certificats   Révocation de certificat

### Ajouter/Signer un nouveau certificat

**Méthode** Créer un certificat interne

**Nom descriptif** VPN-PFSENSE

#### Certificat interne

**Autorité de certification** CA-VPN

**Key type** RSA

**Key length** 4096  
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.

**Algorithme de hachage** 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.

**Durée de vie (jours)** 365  
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.

**Nom commun** vpn.sadek.info

Les éléments suivants sont facultatifs et peuvent être laissés vides.

**Code du pays** Aucun

**État ou province** FR

**Ville** Paris

**Organisation** sadek-info

**Unité organisationnelle** e.g. My Department Name (optional)

Activer Windows  
Accédez aux paramètres Windows.

On a bien précisé l'autorité de certification.

Ensuite définir type de certificat etc

### Attributs de certificat

**Notes d'attributs** Les attributs suivants sont ajoutés aux certificats et aux requêtes lorsqu'ils sont créés ou signés. Ces attributs se comportent différemment en fonction du mode sélectionné.  
 Pour les certificats internes, ces attributs sont ajoutés directement au certificat comme indiqué.

**Type de certificat** Server Certificate  
 Ajoutez les attributs d'utilisation spécifiques au certificat signé. Utilisé pour placer les restrictions d'utilisation ou l'octroi de capacités au certificat signé.

**Noms alternatifs** FQDN ou nom d'hôte

Type Valeur

Entrez des identifiants supplémentaires pour le certificat dans cette liste. Le champ Nom commun est automatiquement ajouté au certificat en tant que nom alternatif. La signature CA peut ignorer ou modifier ces valeurs.

Ajouter + Ajouter

E Enregistrer

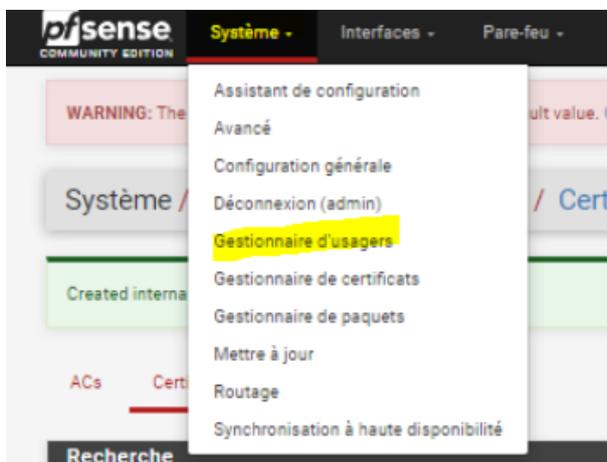
Activer Windows  
Accédez aux paramètres Windows.

Ensuite un petit récapitulatif

Certificats				
Nom	Émetteur	Nom distinctif	En cours d'utilisation	Actions
webConfigurator default (653454e4aa50f) Server Certificate CA: No Serveur: Yes	auto-signé	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-653454e4aa50f ⓘ	webConfigurator	   
<b>VPN-PFSense</b> Server Certificate CA: No <b>Serveur: Yes</b>	CA-VPN	ST=FR, O=sadek-info, L=Paris, CN=vpn.sadek.info ⓘ		   

[+ Ajouter/Signer](#)

Créer un user local et lui créer un certificat



Système / Gestionnaire d'utilisateurs / Utilisateurs / Modifier

Utilisateurs    Groupes    Paramètres    Serveurs d'authentification

### Propriétés utilisateur

Défini par: USER

Désactivé:  Cet utilisateur ne peut pas s'authentifier

Nom d'utilisateur: asadek

Mot de passe: \*\*\*\*\*

Nom complet: Adel Sadek vpn  
Nom complet de l'utilisateur, à des fins administratives uniquement

Date d'expiration:   
Laissez vide si le compte ne doit pas expirer, sinon entrez la date d'expiration sous la forme MM/JJ/AAAA

Paramètres personnalisés:  Utilisez les options GUI individuelles personnalisées et la disposition du tableau de bord pour cet utilisateur.

Appartenance à un groupe: admins

Pas un membre de:

Membre de:

» Déplacer vers la liste "Membre de"    « Déplacer vers la liste "Non membre de"

Maintenez la touche CTRL (PC)/COMMAND (Mac) enfoncée pour sélectionner plusieurs éléments.

Certificat:  Cliquez pour créer un certificat client.

### Créer un certificat pour l'utilisateur

Nom descriptif: USER-VPN

Autorité de certification: CA-VPN

Key type: RSA

4096  
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.

Algorithme de hachage: 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

Durée de vie: 3650

### Clés

Clés SSH autorisées:   
Entrez les clés SSH autorisées pour cet utilisateur

Clé pré-partagée IPsec:

Enregistrer

Il faut cliquer sur l'option Créer un certificat et un onglet s'affichera pour définir les paramètres de ce certificat la date d'expiration, Nom, autorité de certification, combien de bits possèdera la taille de clé de chiffrement RSA.

Utilisateurs					
	Nom d'utilisateur	Nom complet	État	Groupes	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input checked="" type="checkbox"/>	asadek	Adel Sadek vpn	✓		

+ Ajouter
Supprimer

## Configuration du serveur VPN

VPN / OpenVPN / Serveurs

Serveurs Clients Ré-écritures spécifiques au client Assistants

Serveurs OpenVPN					
Interface	Protocole / Port	Réseau tunnel	Mode / Crypto	Description	Actions
<span style="background-color: green; color: white; padding: 2px 5px;">+ Ajouter</span>					

Les différents mode de server

Server Mode : ici, nous avons cinq possibilités :

Peer to peer (SSL/TLS) : pour monter un VPN site-à-site en utilisant une authentification par certificat.

Peer to peer (Shared Key) : pour monter un VPN site-à-site en utilisant une authentification par clé partagée.

Remote Access (SSL/TLS) : pour monter un accès distant pour clients nomades en utilisant une authentification par certificat.

Remote Access (User Auth) : pour monter un accès distant pour clients nomades en utilisant une authentification par login/password.

Remote Access (SSL/TLS + User Auth) : pour monter un accès distant pour clients nomades en utilisation une authentification par certificat et par login/password.

Je vais utiliser SSL/TLS+User auth pour me simplifier la vie

**Informations Générales**

**Désactivé**  Désactiver ce serveur  
Définissez cette option pour désactiver ce serveur sans le retirer de la liste.

**Mode serveur** Accès à distance (SSL/TLS + Authentification utilisateur)

**Backend pour l'authentification** Local Database

**Protocole** UDP on IPv4 only

**Mode dispositif** tun - Layer 3 Tunnel Mode  
Le mode "tun" porte IPv4 et IPv6 (couche OSI 3) et est le mode le plus courant et compatible sur toutes les plates-formes.  
Le mode "tap" est capable de transporter 802.3 (couche OSI 2.)

**Interface** WAN  
L'interface ou l'adresse IP virtuelle où OpenVPN recevra les connexions des clients

**Port local** 1194  
Le port utilisé par OpenVPN pour recevoir des connexions client.

**Description**   
Une description peut être saisie ici à des fins de référence administrative (non analysée).

Active Windows

Je définis le port + interface d'écoute sur quel support ce basera l'authentification ici « local » car je n'ai pas joint mon pfSense au domaine AD

Au niveau du chiffrement j'utilise du AES 256

**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

The order of the selected Data Encryption Algorithms is respected by OpenVPN. **i**

**Fallback Data Encryption Algorithm** AES-256-CBC (256 bit key, 128 bit block)  
The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation. This algorithm is automatically included in the Data Encryption Algorithms list.

**Algorithme de hachage d'authentification** SHA256 (256-bit)  
The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.  
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.  
The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.

**Chiffrement matériel** Pas d'accélération cryptographique matérielle

Active Windows

Accédez aux paramètres pour activer Windows.

Ensuite les paramètres du tunnel IPV4

**Paramètres du tunnel**

**Réseau Tunnel IPv4**   
Il s'agit du réseau virtuel IPv4 utilisé pour les communications privées entre ce serveur et les hôtes clients exprimés à l'aide de la notation CIDR (par exemple, 10.0.8.0/24). La première adresse utilisable dans le réseau sera affectée à l'interface virtuelle du serveur. Les autres adresses utilisables seront affectées à la connexion des clients.

**Tunnel réseau IPv6**   
Il s'agit du réseau virtuel IPv6 utilisé pour les communications privées entre ce serveur et les hôtes clients exprimés en utilisant la notation CIDR (par exemple, fe80 :: / 64). L'adresse :: 1 dans le réseau sera affectée à l'interface virtuelle du serveur. Les adresses restantes seront affectées à la connexion des clients.

**Rediriger la passerelle IPv4**  Force all client-generated IPv4 traffic through the tunnel.

**Rediriger la passerelle IPv6**  Force all client-generated IPv6 traffic through the tunnel.

**Réseau(x) local/locaux IPv6**   
Les réseaux IPv6 qui seront accessibles depuis le point d'extrémité distant. Exprimé sous la forme d'une liste séparée par des virgules d'un ou plusieurs IP / PREFIX. Cela peut être laissé vide si vous n'ajoutez pas d'itinéraire au réseau local via ce tunnel sur la machine distante. Ceci est généralement défini sur le réseau LAN.

**Connexions simultanées**   
Spécifier le nombre maximum de clients autorisés à se connecter en même temps à ce serveur.

**Allow Compression**

Je définis l'ip dans le tunnel

Ensuite je redirige tout le trafic vers mon vpn du côté client de sorte à ce que tout type de flux passe par le vpn si je veux simplement donner l'accès à un réseau sans rediriger tout le flux je décoche cette option et je renseigne les réseaux locaux juste en bas.

Je définis ensuite le nom de connexion simultanés

Ensuite ici

**Paramètres du client**

**IP dynamique**  Autoriser les clients connectés à conserver leurs connexions si leur adresse IP change.

**Topologie**   
Spécifie la méthode utilisée pour fournir une adresse IP d'adaptateur virtuel aux clients lors de l'utilisation du mode TUN sur IPv4.  
Certains clients peuvent exiger que cela soit mis en «sous-réseau» même pour IPv6, par exemple OpenVPN Connect (iOS / Android). Les anciennes versions d'OpenVPN (avant 2.0.9) ou les clients tels que les téléphones Yealink peuvent nécessiter "net30".

Une IP par client dans le sous réseau je ne souhaite pas isoler chaque client dans un sous-réseau simplement pour les faire communiquer entre eux et ne pas me rajouter de contrainte

Je renseigne comme serveur DNS mon srv AD

Ensuite je valide

avec tous les paramètres et les configurations avec la mise en œuvre de votre serveur OpenVPN.

<b>Exit Notify</b>	<input type="text" value="Désactivé"/>
Send an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately disconnect rather than waiting for a timeout. In SSL/TLS Server modes, clients may be directed to reconnect or use the next server. In Peer-to-Peer Shared Key or with a /30 Tunnel Network, this value controls how many times this instance will attempt to send the exit notification.	
<b>Tampon d'envoi/réception</b>	<input type="text" value="Par défaut"/>
Configurez une taille de mémoire tampon d'envoi et de réception pour OpenVPN. La taille de la mémoire tampon par défaut peut être trop faible dans de nombreux cas, selon les vitesses de liaison montante du matériel et du réseau. Trouver la meilleure taille de mémoire tampon peut faire quelques expériences. Pour tester la meilleure valeur pour un site, commencez à 512KIB et testez des valeurs plus élevées et plus faibles.	
<b>Création d'une passerelle</b>	<input checked="" type="radio"/> Les deux <input type="radio"/> IPv4 uniquement <input type="radio"/> IPv6 uniquement
If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.	
<b>Niveau de verbosité</b>	<input type="text" value="défaut"/>
Chaque niveau affiche toutes les informations des niveaux précédents. Le niveau 3 est recommandé pour un bon résumé de ce qui se passe sans être submergé par la sortie.  Aucun: Seules les erreurs fatales Défaut à 4: Plage d'utilisation normale 5: Caractères R et W sur la console pour chaque paquet lu et écrit. Les majuscules sont utilisées pour les paquets TCP/UDP et les minuscules sont utilisées pour les paquets TUN/TAP. 6-11: plage d'informations de débogage	

Activer Windows  
Accédez aux paramètres pour activer Windows

On a un petit résumé ici

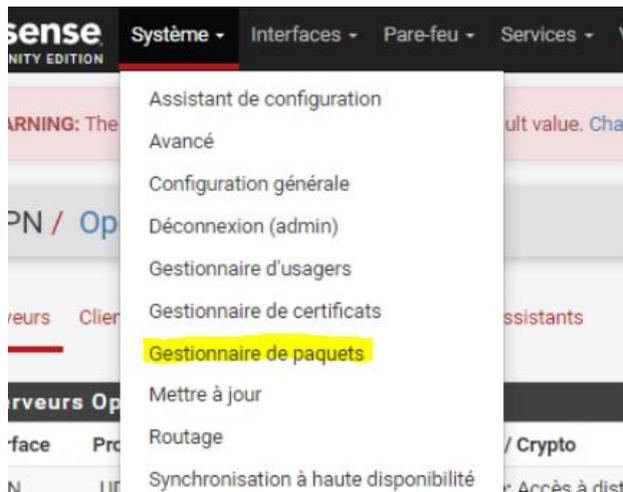
Serveurs Clients Ré-écritures spécifiques au client Assistants

Serveurs OpenVPN					
Interface	Protocole / Port	Réseau tunnel	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	20.0.0.0/24	<b>Mode:</b> Accès à distance (SSL/TLS + Authentification utilisateur) <b>Data Ciphers:</b> AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC <b>Digest:</b> SHA256 <b>D-H Params:</b> 2048 bits		  

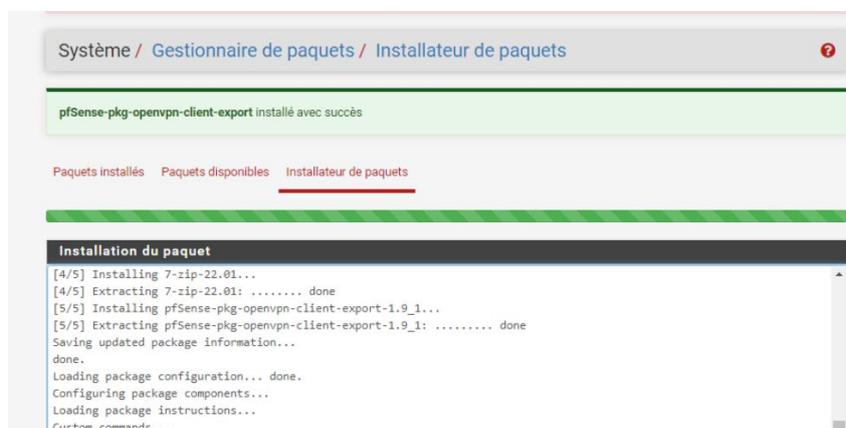
## Exporter la config aux clients

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.

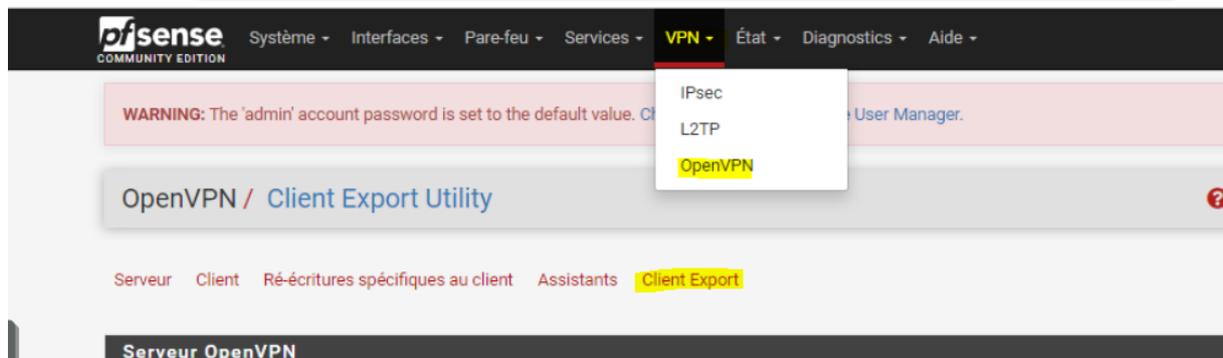
Recherchez "openvpn" et installez le paquet : openvpn-client-export.



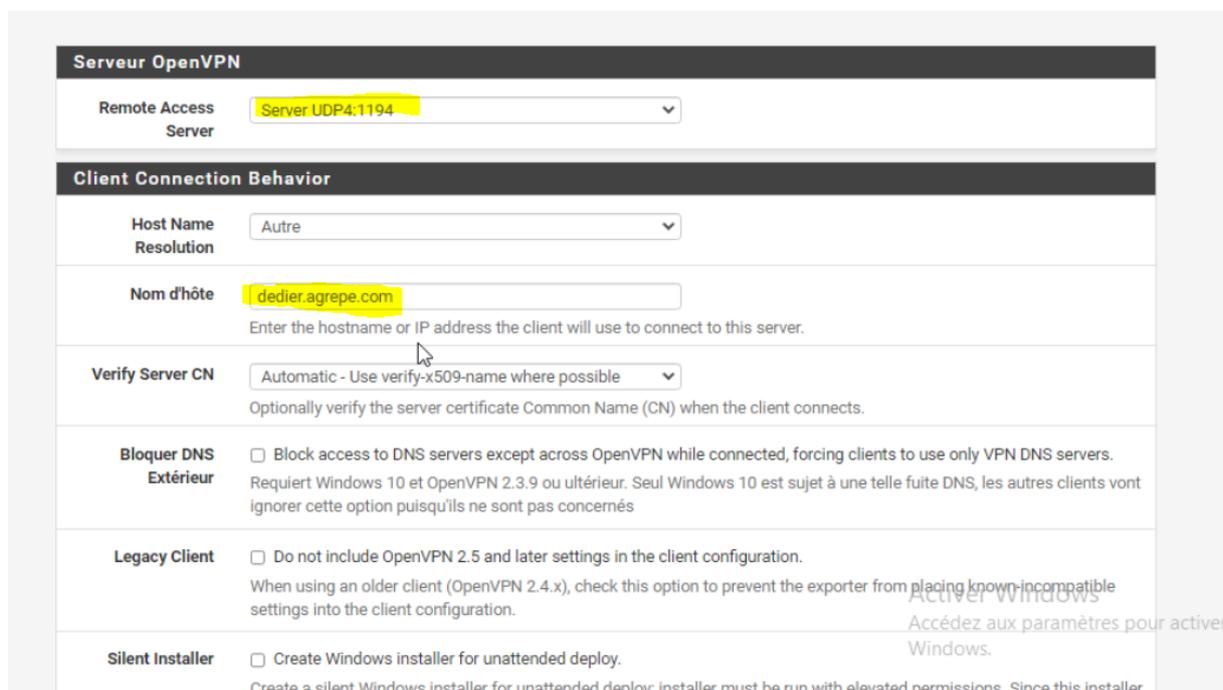
Cet écran s'affiche je patiente



Ensuite partir ici



Comme mon vpn est derrière un routeur et c'est une règle de PAT qui sera utiliser pour renvoyer vers le port 1194 de mon pare feu je dois modifier un parametre dans la config du client à exporter



**Certificate Export Options**

<b>PKCS#11 Certificate Storage</b>	<input type="checkbox"/> Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files.
<b>Microsoft Certificate Storage</b>	<input type="checkbox"/> Use Microsoft Certificate Storage instead of local files.
<b>Password Protect Certificate</b>	<input type="checkbox"/> Use a password to protect the PKCS#12 file contents or key in Viscosity bundle.
<b>PKCS#12 Encryption</b>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">High: AES-256 + SHA256 (pfSense Software, FreeBSD) ▼</div> Select the level of encryption to use when exporting a PKCS#12 archive. Encryption support varies by Operating System and program

**Proxy Options**

<b>Use A Proxy</b>	<input type="checkbox"/> Use proxy to communicate with the OpenVPN server.
--------------------	--

**Avancé**

<b>Additional configuration options</b>	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <p style="font-size: small;">Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon.</p> <p style="font-size: x-small;">EXAMPLE: remote-random;</p>
---	---

Save as default

Je télécharge ce fichier de conf ovpn qui contient tout le certificat + la clé privée du certificat

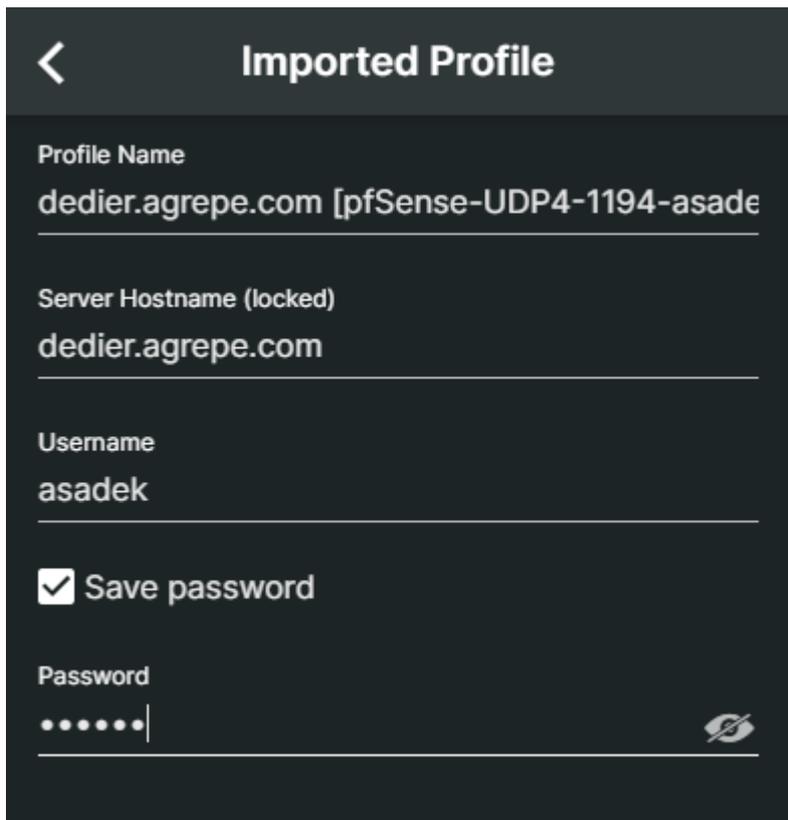
**Clients OpenVPN**

Utilisateur	Nom du certificat	Export
asadek	USER-VPN	- Inline Configurations: <div style="display: flex; gap: 5px;"> <span style="background-color: #28a745; color: white; padding: 2px 5px;">Most Clients</span> <span style="background-color: #007bff; color: white; padding: 2px 5px;">Android</span> </div> <div style="background-color: #007bff; color: white; padding: 2px 5px; margin-top: 2px;">OpenVPN Connect (iOS/Android)</div> - Bundled Configurations: <div style="display: flex; gap: 5px;"> <span style="background-color: #007bff; color: white; padding: 2px 5px;">Archive</span> <span style="background-color: #007bff; color: white; padding: 2px 5px;">Config File Only</span> </div> - Current Windows Installers (2.6.5-ix001): <div style="display: flex; gap: 5px;"> <span style="background-color: #007bff; color: white; padding: 2px 5px;">64-bit</span> <span style="background-color: #007bff; color: white; padding: 2px 5px;">32-bit</span> </div> - Previous Windows Installers (2.5.9-ix601): <div style="display: flex; gap: 5px;"> <span style="background-color: #007bff; color: white; padding: 2px 5px;">64-bit</span> <span style="background-color: #007bff; color: white; padding: 2px 5px;">32-bit</span> </div> - Legacy Windows Installers (2.4.12-ix601): <div style="display: flex; gap: 5px;"> <span style="background-color: #007bff; color: white; padding: 2px 5px;">10/2016/2019</span> <span style="background-color: #007bff; color: white; padding: 2px 5px;">7/8/8.1/2012r2</span> </div> - Viscosity (Mac OS X and Windows): <div style="display: flex; gap: 5px;"> <span style="background-color: #007bff; color: white; padding: 2px 5px;">Viscosity Bundle</span> <span style="background-color: #007bff; color: white; padding: 2px 5px;">Viscosity Inline Config</span> </div>

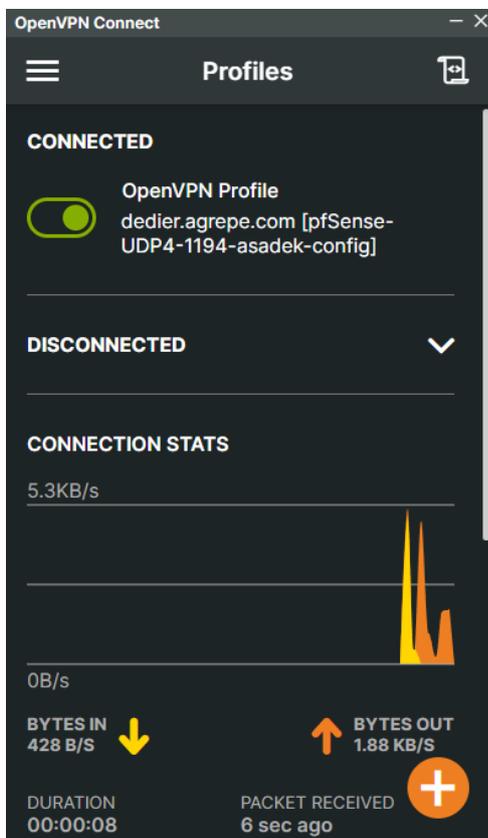
Only OpenVPN-compatible user certificates are shown

Voila le fichier .ovpn

Je passe au test



Connexion établis dans openvpnConnect



Je teste avec un ipconfig si j'ai une ip dans le tunnel

```
Carte inconnue Connexion au réseau local :
Suffixe DNS propre à la connexion. . . :
Adresse IPv6 de liaison locale. . . . : fe80::2a55:ff47:155f:72bf%20
Adresse IPv4. . . . . : 20.0.0.2
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . :
```

## Modification règles

Je vais modifier les règles du pare-feu pour permettre à tout le flux dans le vpn de passer et ne pas être bloqué car par défaut tout est bloqué



Je crée cette règle qui autorise tout le but n'est pas de restreindre pour le moment pour vérifier que tout fonctionne

**Modifier la règle de Pare-Feu**

**Action**    
 Choisissez que faire des paquets qui correspondent aux critères ci-dessous.   
 Aide : La différence entre bloquer et rejeter est qu'avec 'Rejeter', un paquet (TCP, RST ou ICMP port unreachable pour UDP) est retourné à l'expéditeur, alors qu'avec 'Bloquer', le paquet est supprimé silencieusement. Dans tous les cas, le paquet est supprimé.

**Désactivé**  Désactiver cette règle   
 Choisissez cette option pour désactiver cette règle sans la supprimer de la liste.

**Interface**    
 Choisissez l'interface d'où les paquets doivent provenir pour correspondre à cette règle.

**Famille d'adresse**    
 Choisissez la version du protocole IP à laquelle cette règle s'applique.

**Protocole**    
 Choisissez quel protocole IP cette règle devrait correspondre.

**Source**  Invert match   /    
  /

**Destination**  Invert match    
  /

**Options additionnelles**   
  Journaliser les paquets gérés par cette règle   
  Journaliser les paquets gérés par cette règle

Activer Windows   
 Accédez aux paramètres pour activer Windows.

Ensuite j'effectue un test

C'est parfait ça fonctionne

```
C:\Users\PC>ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=92 ms TTL=112
Réponse de 8.8.8.8 : octets=32 temps=94 ms TTL=112
Réponse de 8.8.8.8 : octets=32 temps=92 ms TTL=112
Réponse de 8.8.8.8 : octets=32 temps=94 ms TTL=112

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 92ms, Maximum = 94ms, Moyenne = 93ms

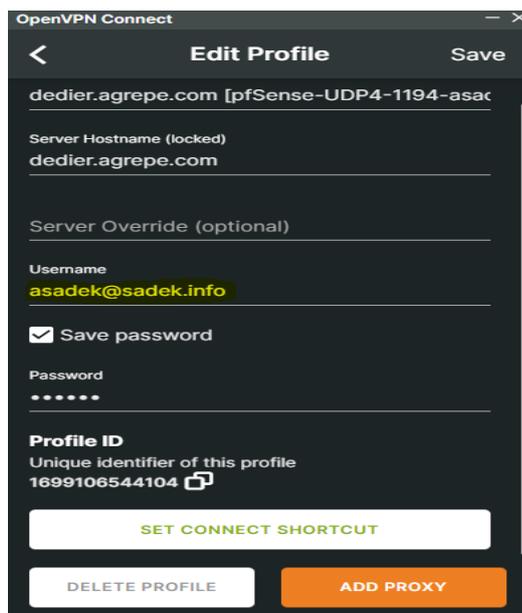
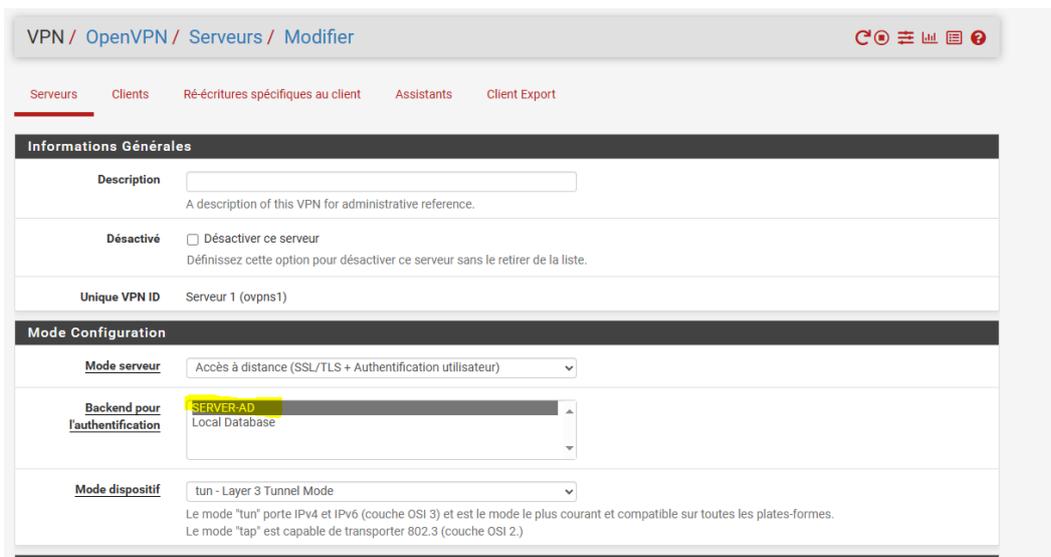
C:\Users\PC>
```

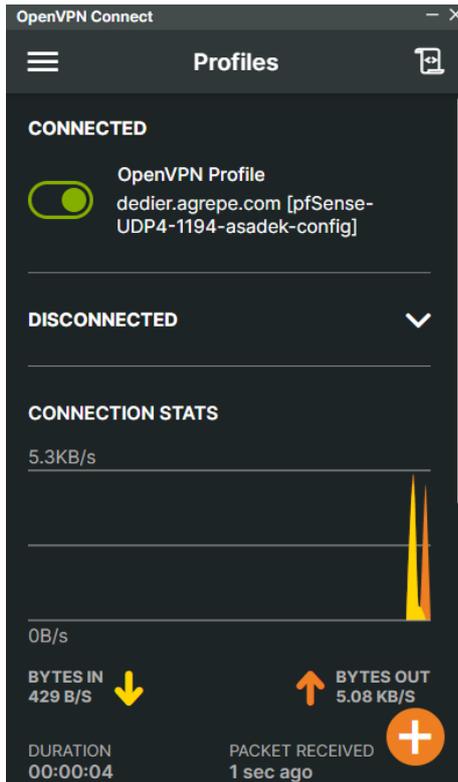
# Bonus

## Authentification via AD

Entre temps j'ai configuré une authentification via l'active directory une fois configuré il ne suffit plus que de sélectionner le serveur AD dans backend pour authentification.

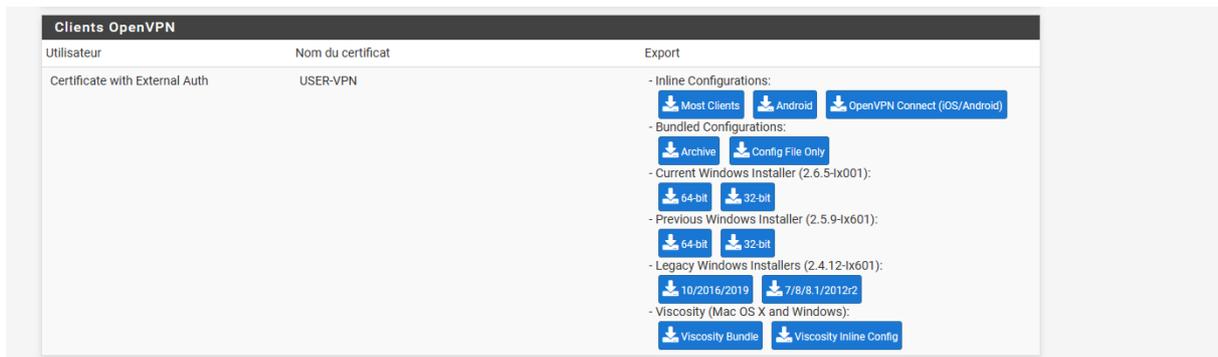
Néanmoins il faut quand même au début créer un user local pour avoir un certificat client à moins de ne faire une authentification seulement via « user ».





C'est parfait cela fonctionne à mon avis OpenVpn est une solution adaptée à de nombreuses entreprise qui souhaite pratiquer le télétravail ou autre.

Ne pas oublier de télécharger le nouveau fichier de conf client openvpn pour les users AD



Probleme à résoudre plusieurs user ne peuvent pas se connecter en même temps

La solution est de modifier l'authentification de SSL/authUser à seulement authUser avec une clé TLS qui viendra on va dire remplacer le certificat coté user.