PFsense : VPN client to site

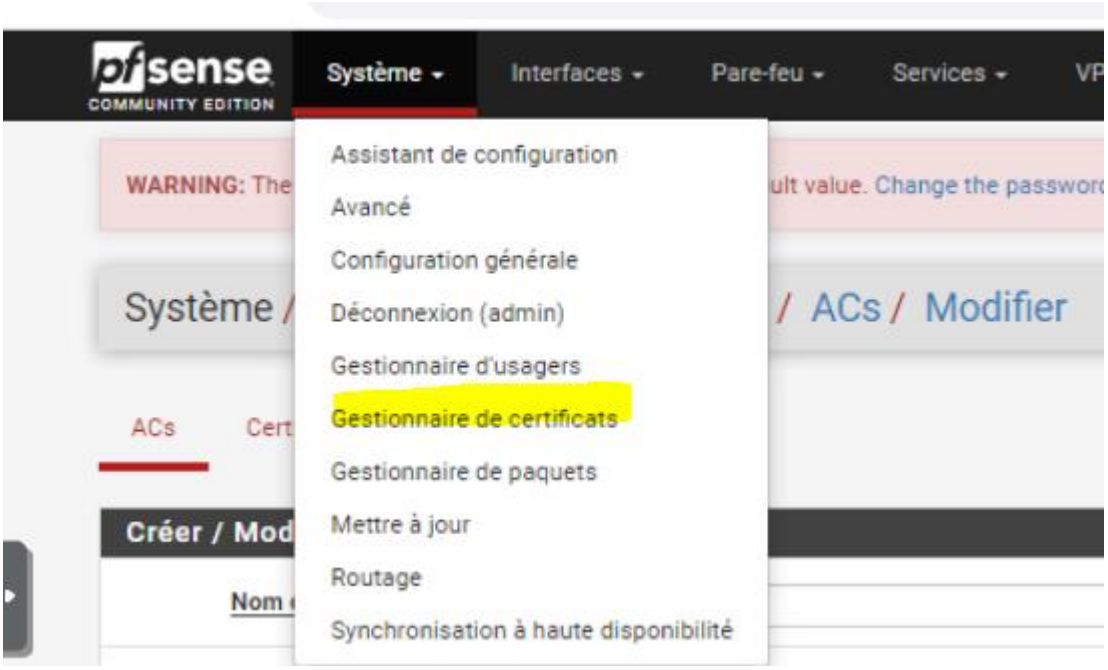
Introduction

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.

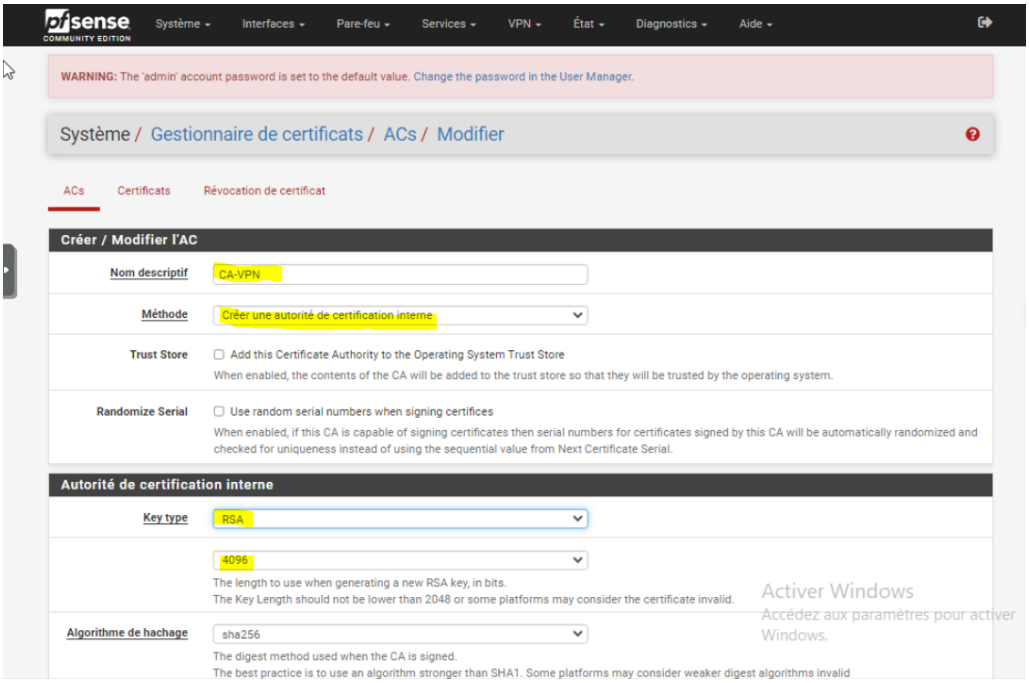
Ensuite il faudra créer la config du serveur Openvpn sur le pfsense

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

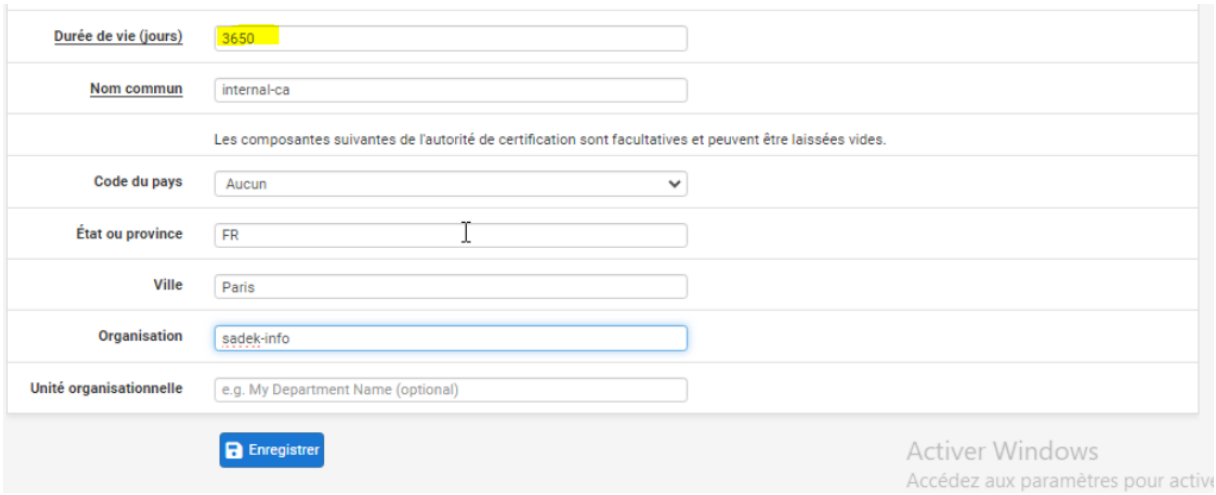
Autorité de certification



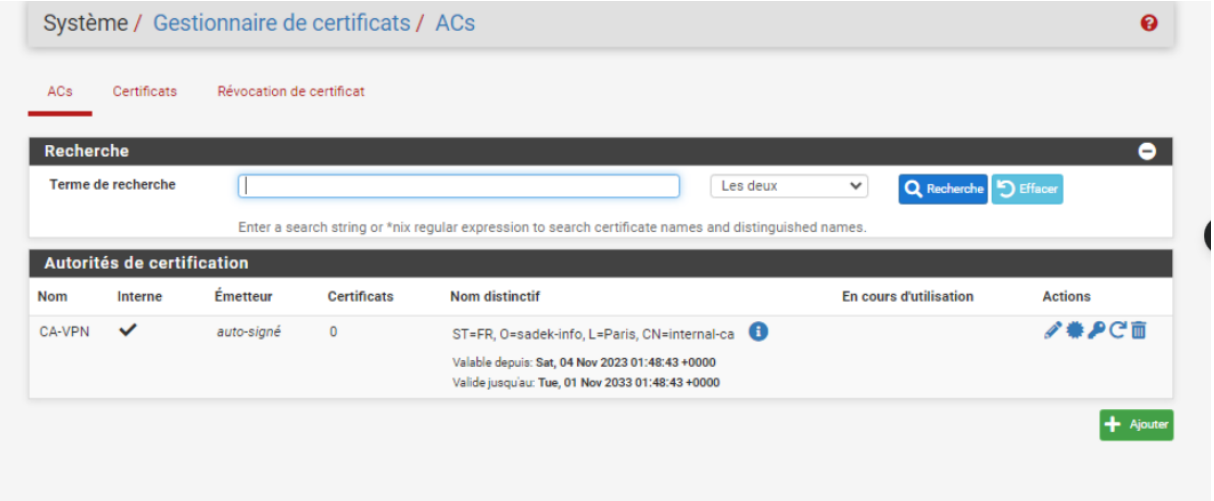
Voila on souhaite créer une autorité de certification interne on définit le nom



Voila les paramètres basique du certificat durée de vie pays etc

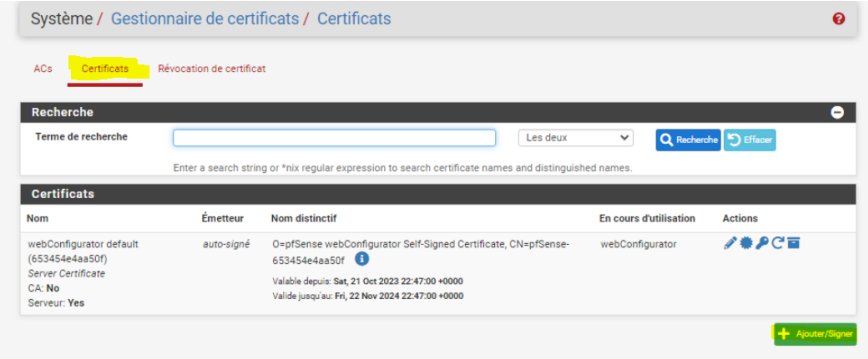


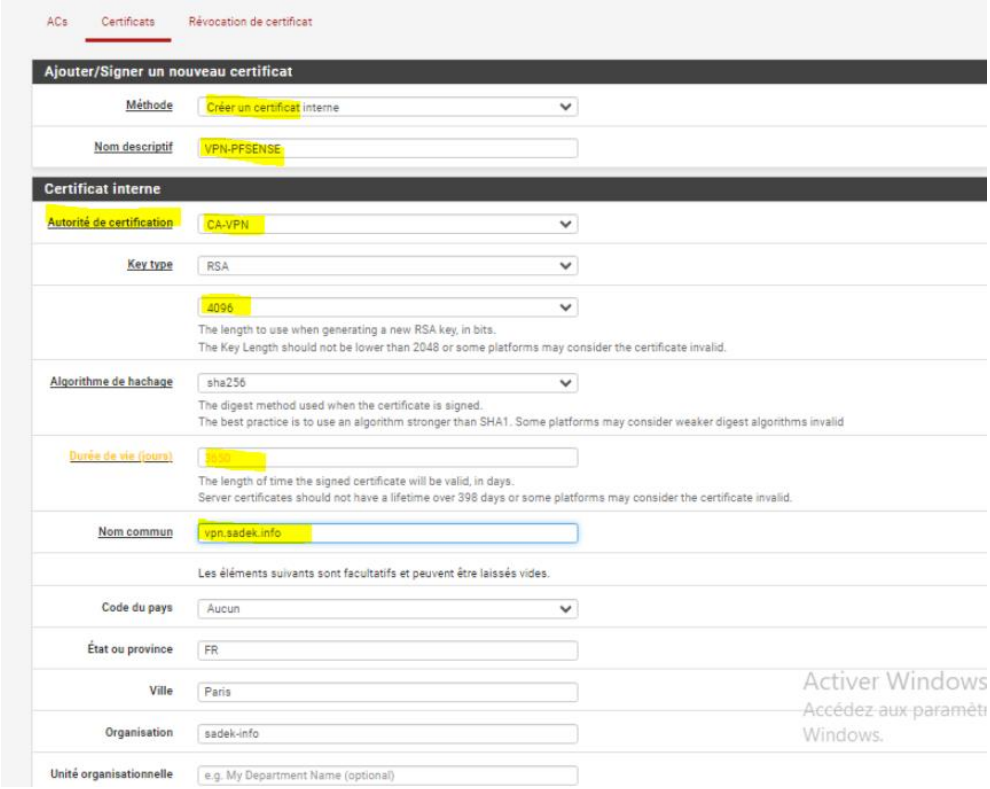
Un petit récapitulatif



Certificat serveur

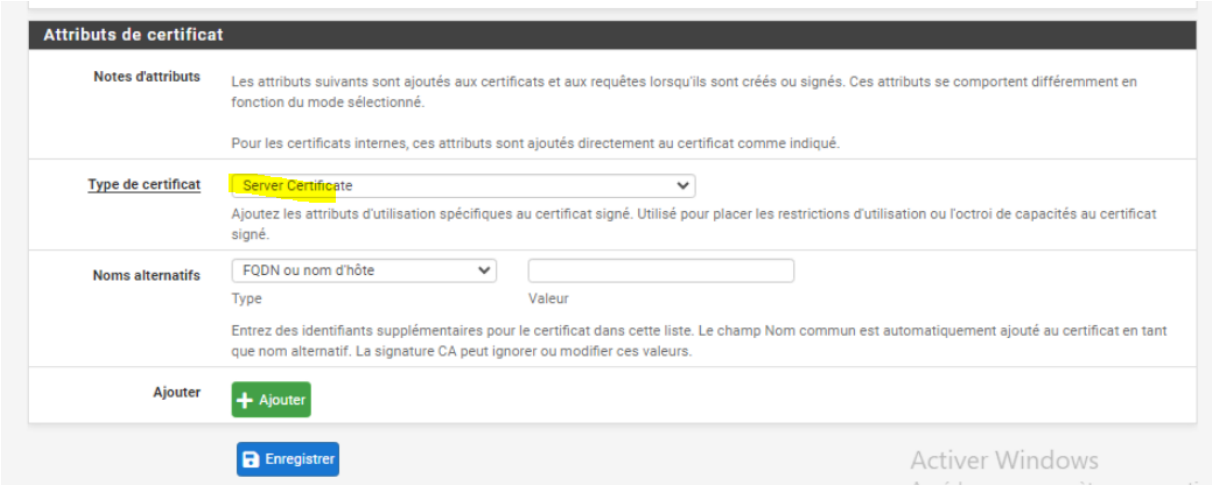
Ensuite créer le certificat serveur qui permettra d'authentifier le serveur.



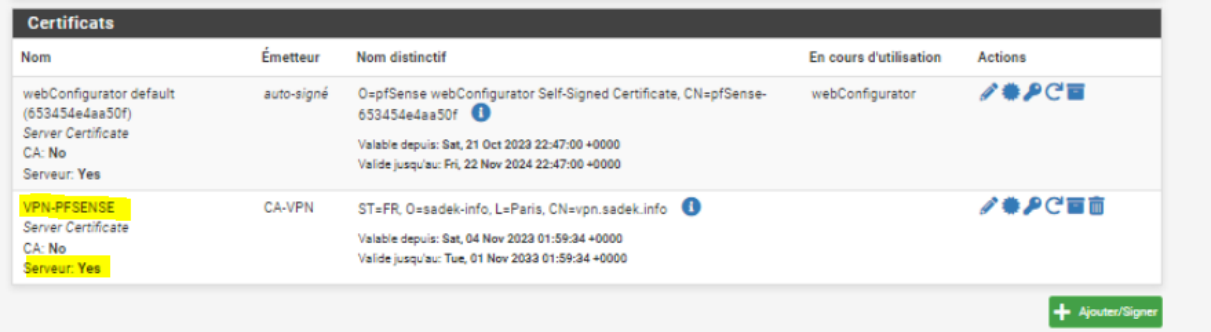


On a bien précisé l'autorité de certification.

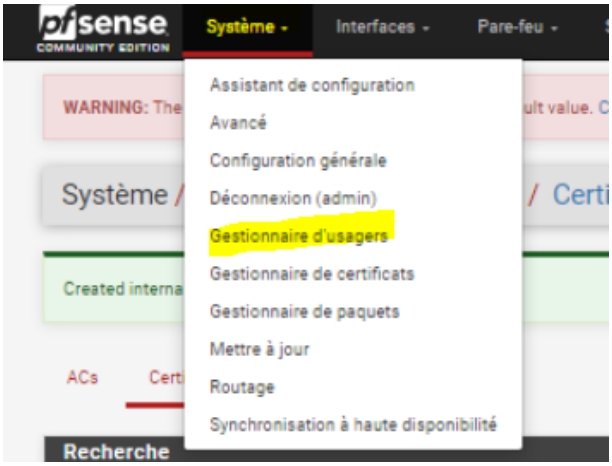
Ensuite définir type de certificat etc

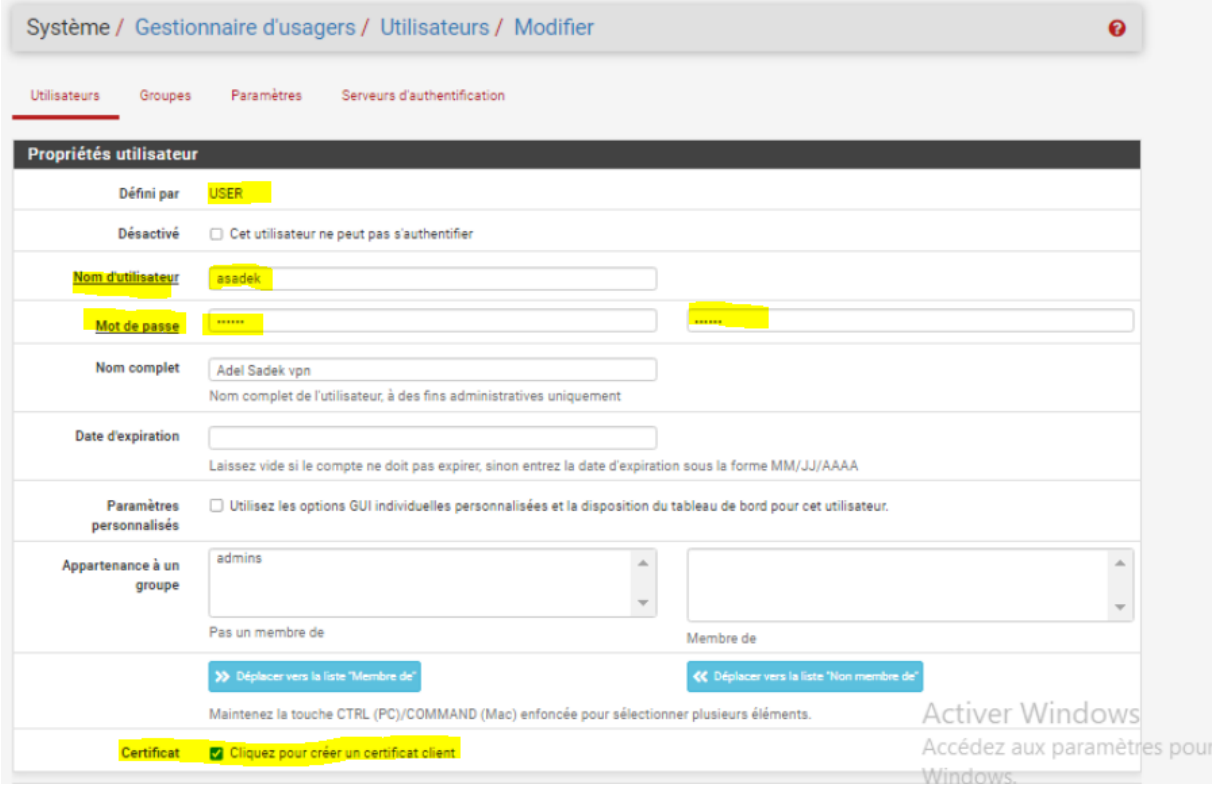


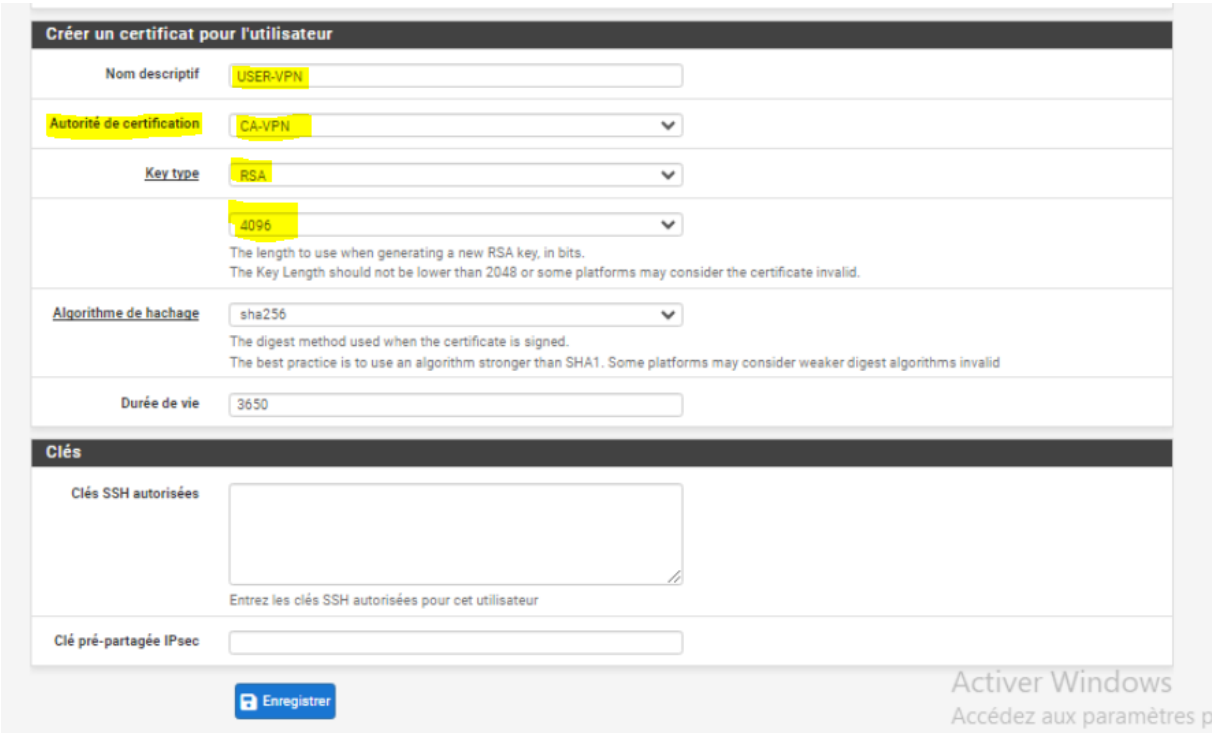
Ensuite un petit récapitulatif



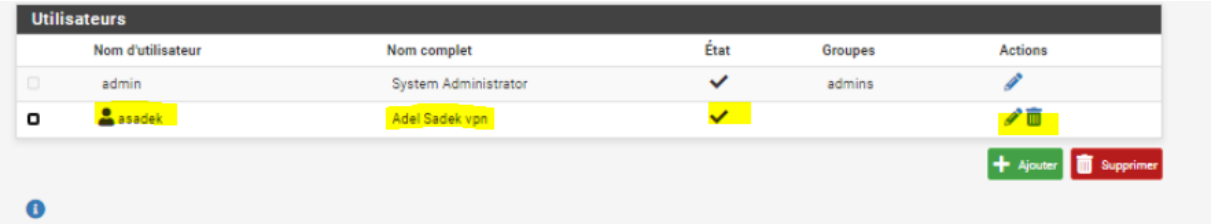
Créer un user local et lui créer un certificat



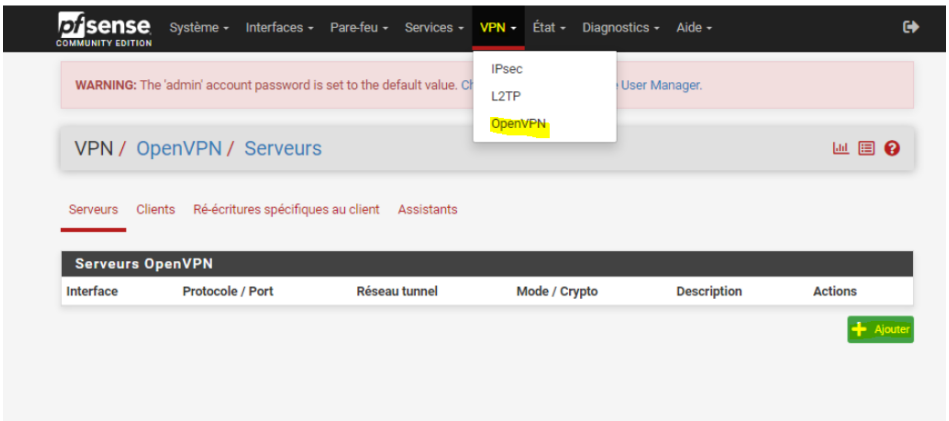




Il faut cliquer sur l'option Créer un certificat et un onglet s'affichera pour définir les paramètres de ce certificat la date d'expiration, Nom, autorité de certification, combien de bits possèdera la taille de clé de chiffrement RSA.



Configuration du serveur VPN



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.

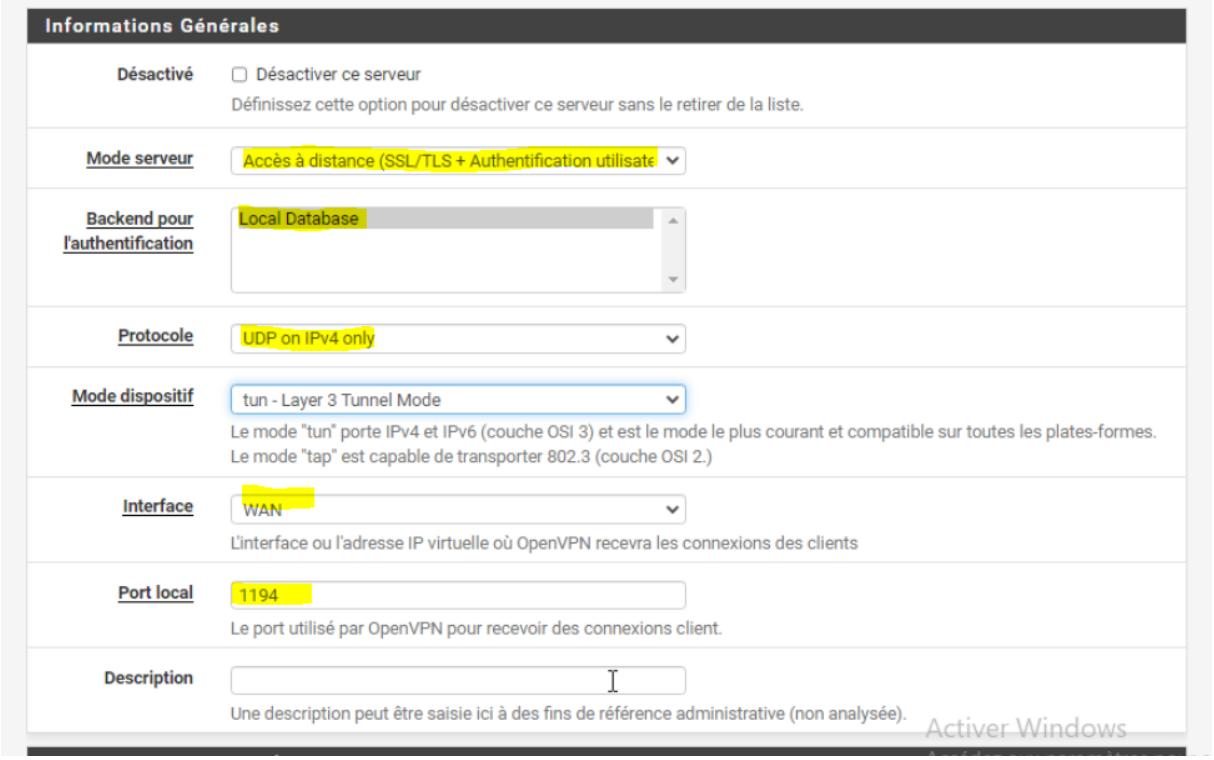
Peer to peer (Shared Key) : pour monter un VPN site-à-site en utilisant une authentification par clé partagée.

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.

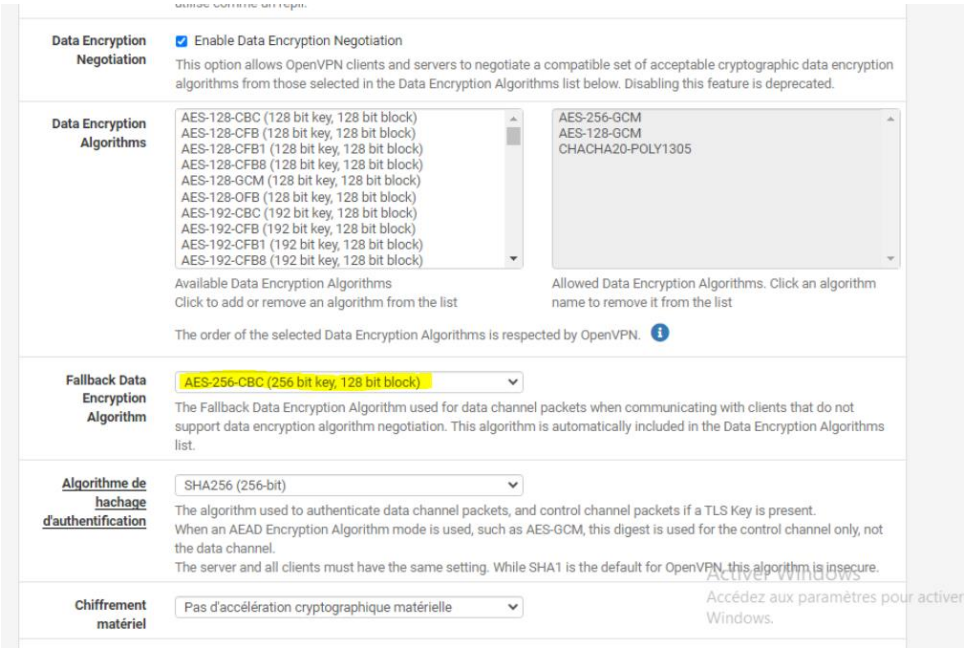
Remote Access (SSL/TLS + User Auth) : pour monter un accès distant pour clients nomades en utilisation une authentification par certificat et par login/password.

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

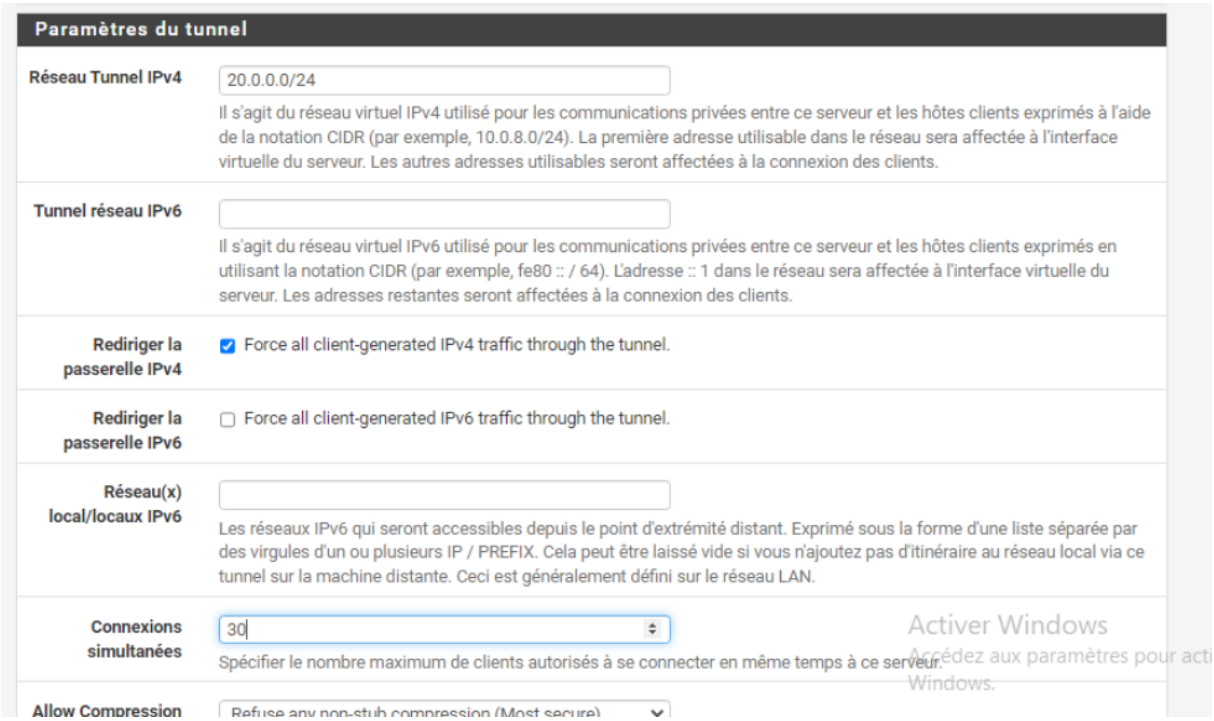


Je définis le port + interface d'écoute sur quel support ce basera l'authentification ici « local » car je n'ai pas joint mon pfsense au domaine AD

Au niveau du chiffrement j'utilise du AES 256



Ensuite les paramètres du tunnel IPV4



Je définis l'ip dans le tunnel

Ensuite je redirige tout le trafic vers mon vpn du coté 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.

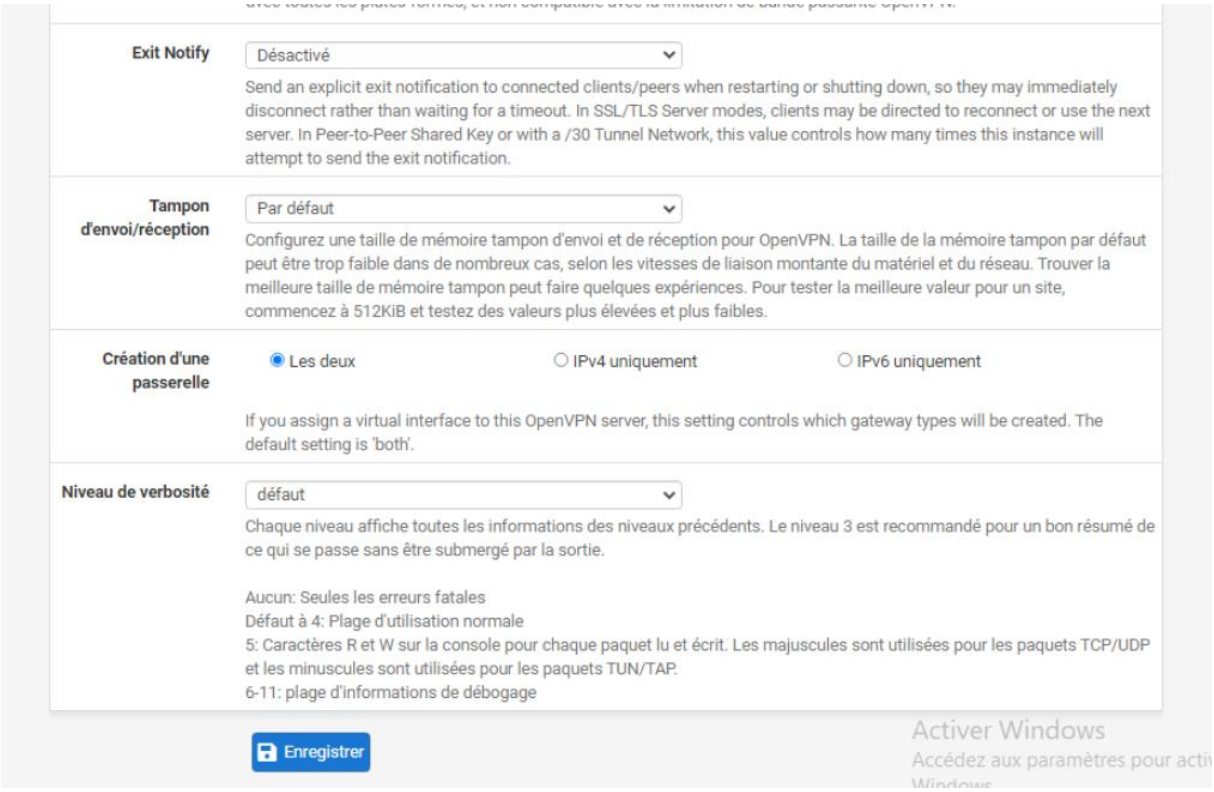
Je définis ensuite le nom de connexion simultanés

Ensuite ici

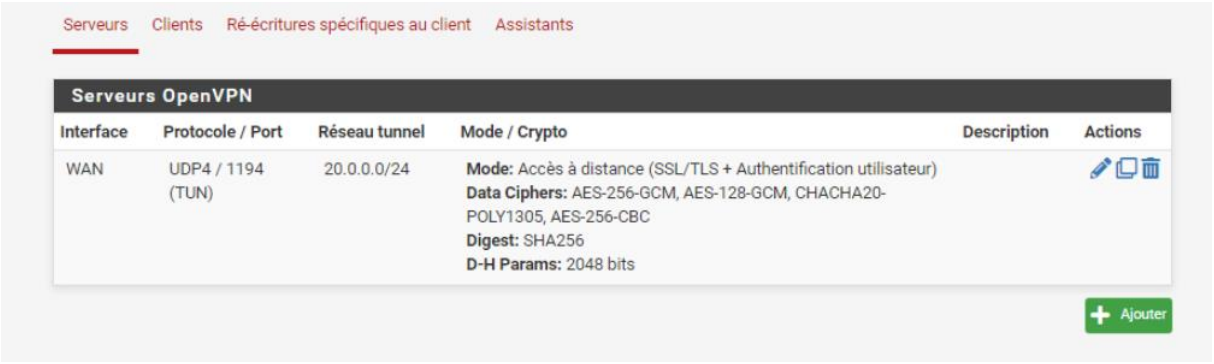
Une IP par client dans le sous réseau je ne souhaite pas isoler chaque client dans un sous-réseau simplement pour les faire communiquer entre eux et ne pas me rajouter de contrainte

Je renseigne comme serveur DNS mon srv AD

Ensuite je valide



On a un petit résumé ici

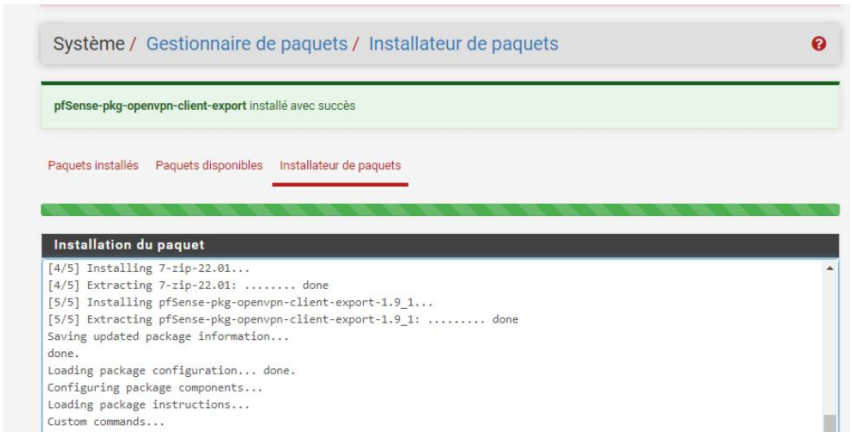


Exporter la config aux clients

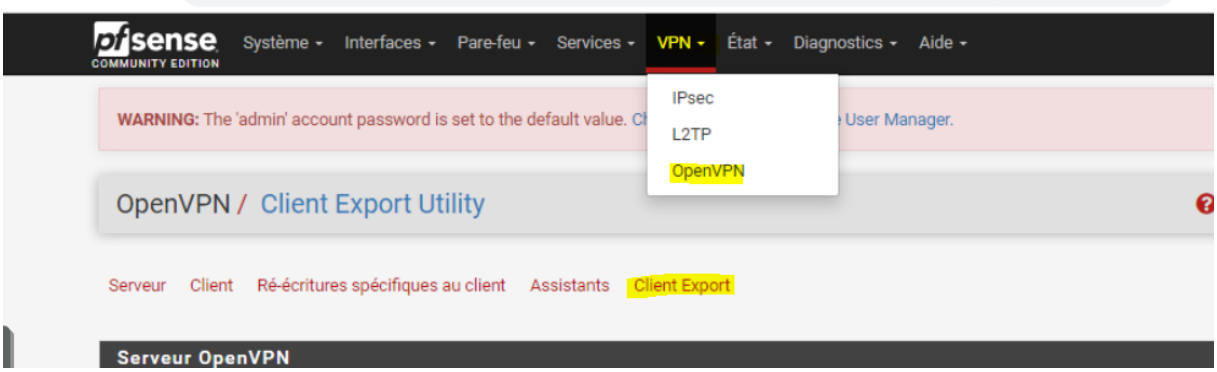
Pour télécharger la configuration au format ".ovpn", il est nécessaire d'installer un paquet supplémentaire sur notre pare-feu. Rendez-vous dans le menu suivant : System > Package Manager > Available Packages.

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

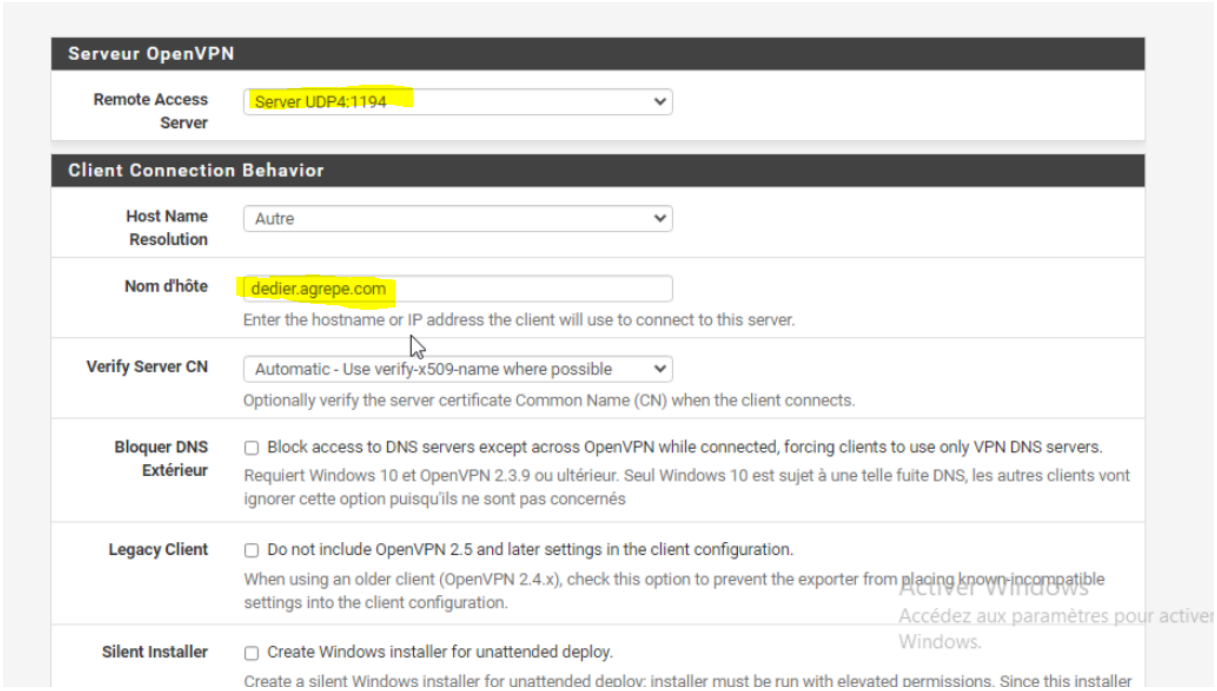
Cet écran s'affiche je patiente

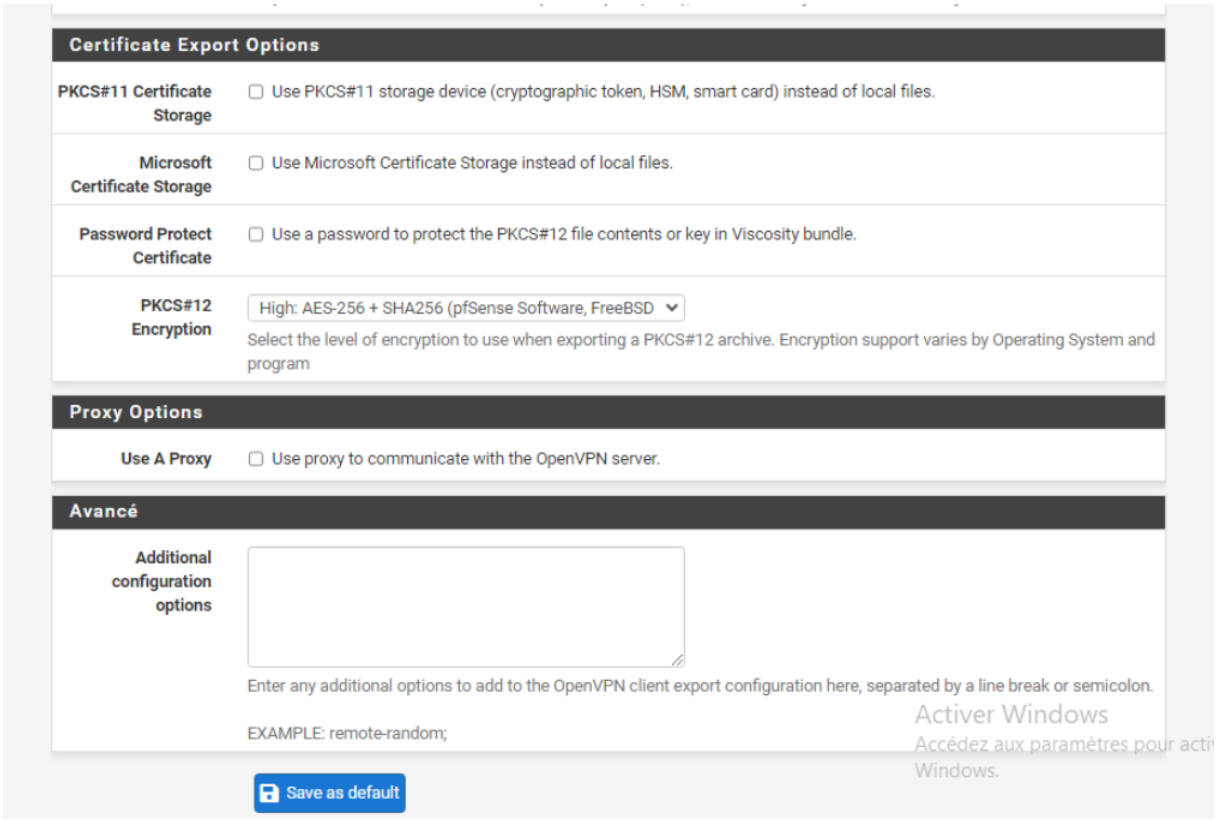


Ensuite partir ici

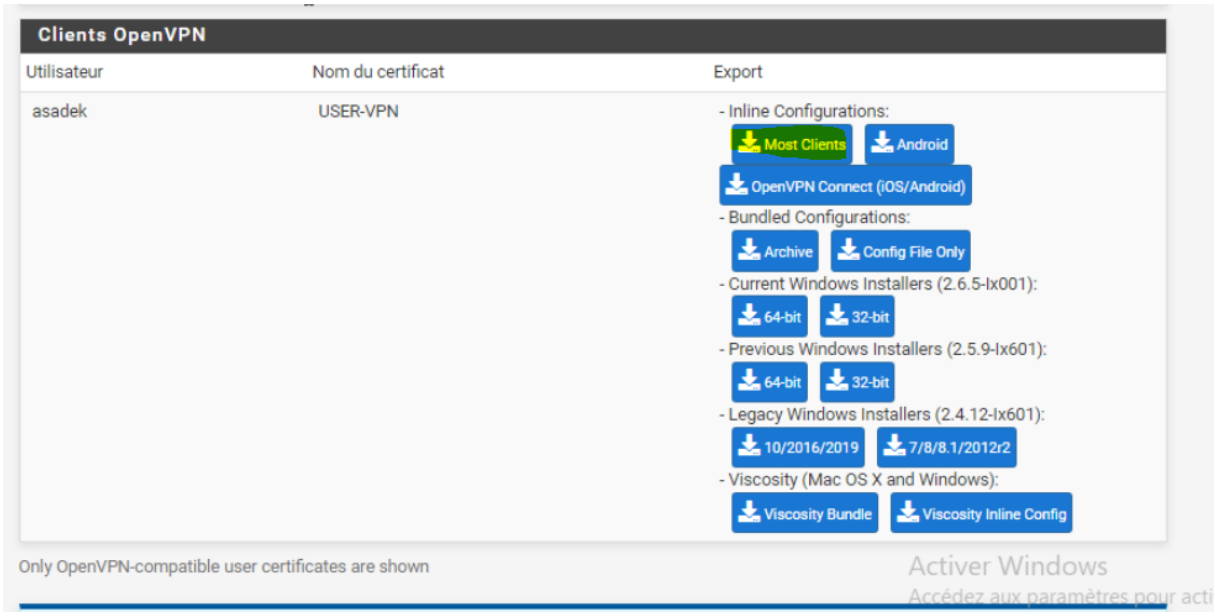


Comme mon vpn est derrière un routeur et c'est une regle de PAT qui sera utiliser pour renvoyer vers le port 1194 de mon pare feu je dois modifier un parametre dans la config du client à exporter

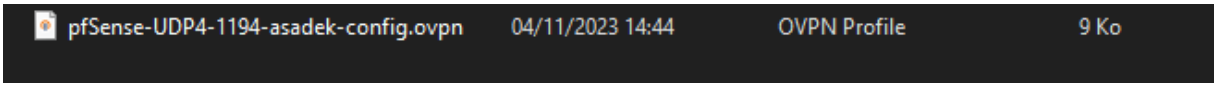




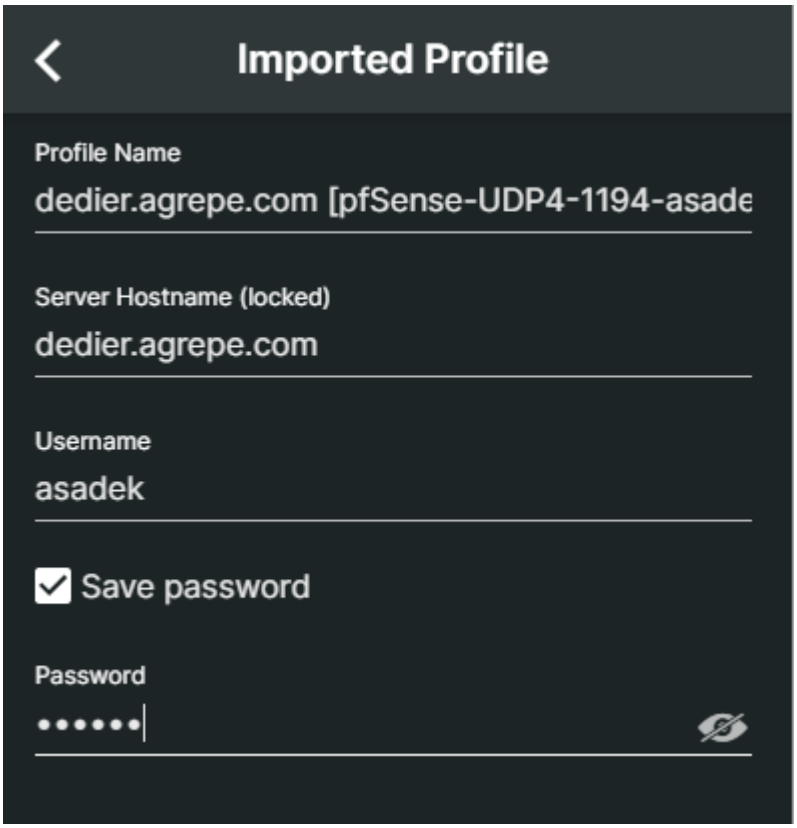
Je télécharge ce fichier de conf ovpn qui contient tout le certificat + la clé privée du certificat



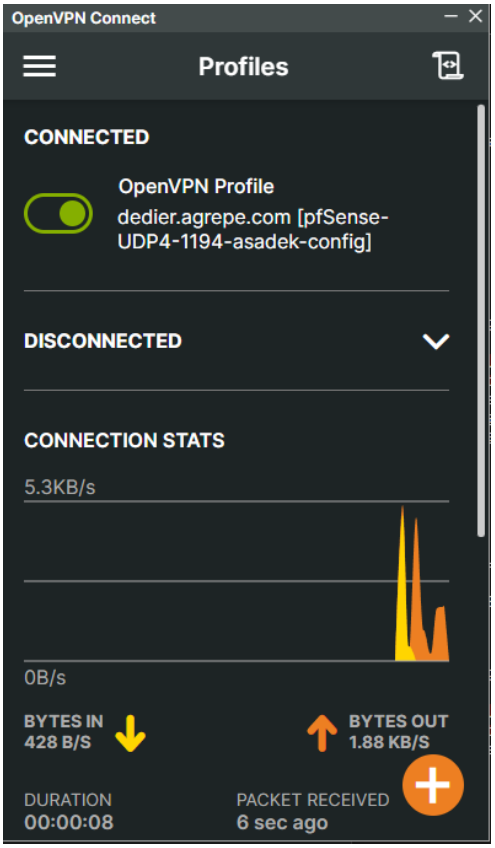
Voila le fichier .ovpn



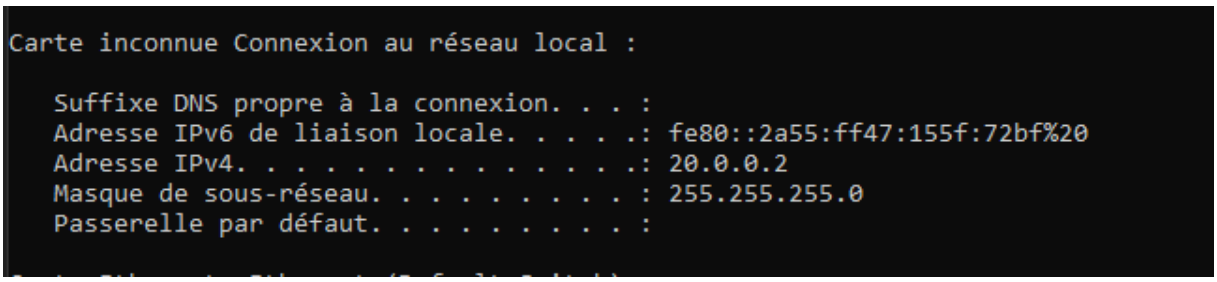
Je passe au test



Connexion établis dans openvpnConnect

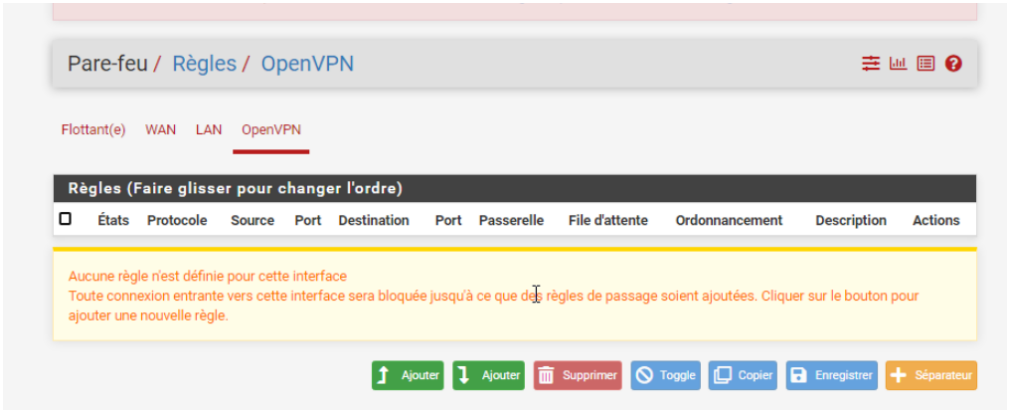


Je teste avec un ipconfig si j'ai une ip dans le tunnel



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 bloquer 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

Ensuite j'effectue un test

C'est parfait ça fonctionne

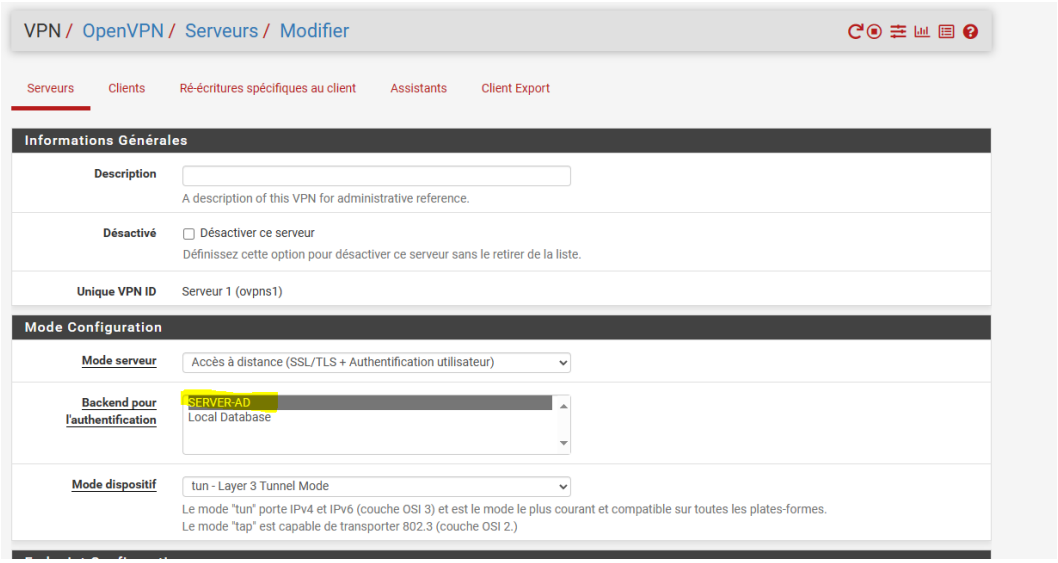
```
C:\Users\PC>ping 8.8.8.8

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>
```

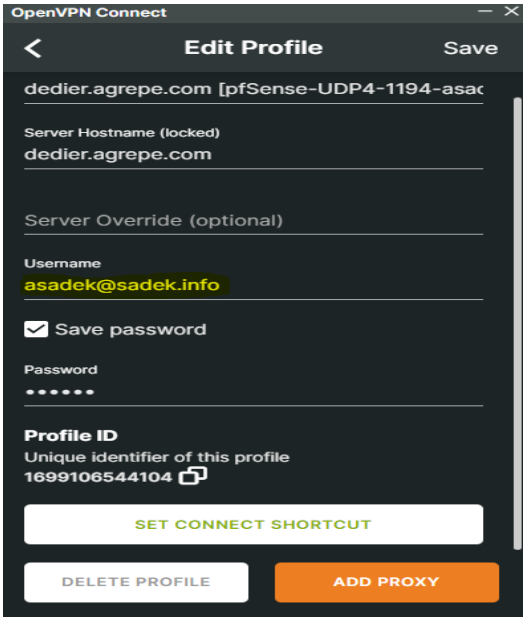
Bonus

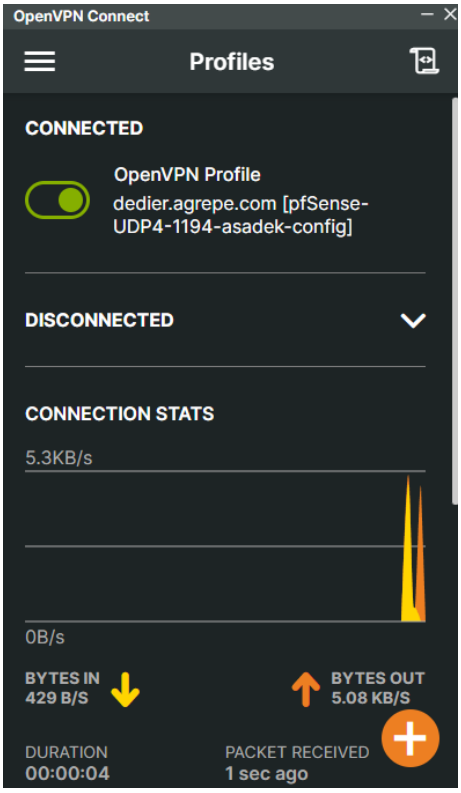
Authentification via AD

Entre temps j'ai configuré une authentification via l'active directory une fois confgiuré 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 ».

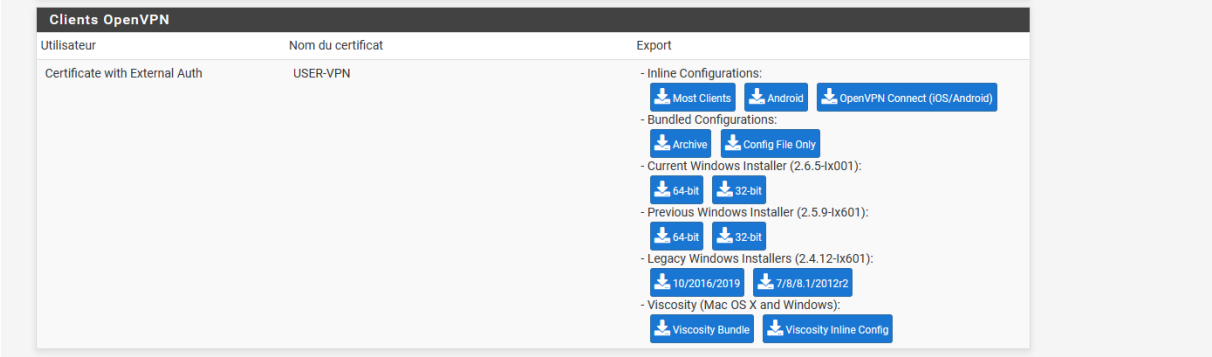






C’est parfait cela fonctionne à mon avis OpenVpn est une solution adaptée à de nombreuses entreprise qui souhaite pratiquer le télétravail ou autre.

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 clée TLS qui viendra on va dire remplacer le certificat coté user.