Lebeau Mathéo

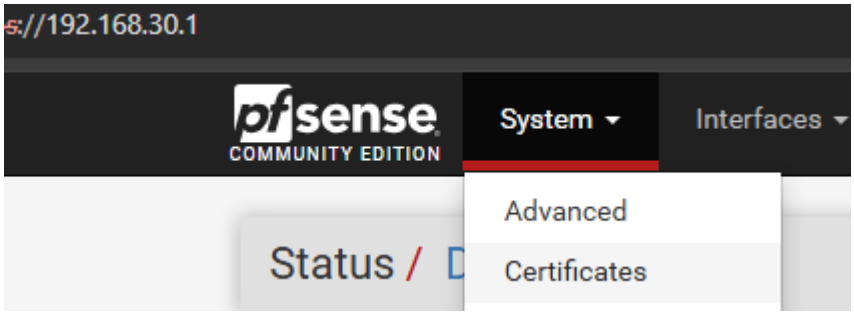
TP installation VPN SITE/client openvpn sur pfsense

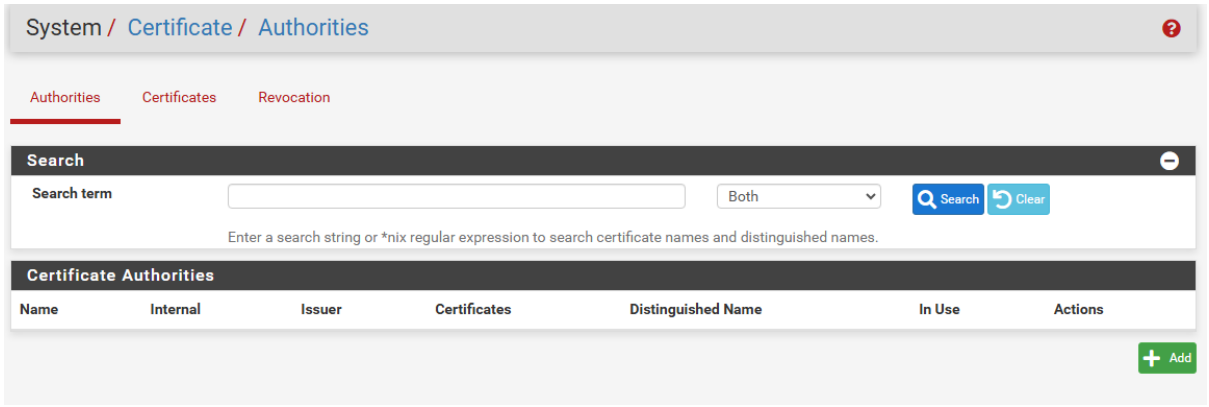
BTS SIO2

Intro :

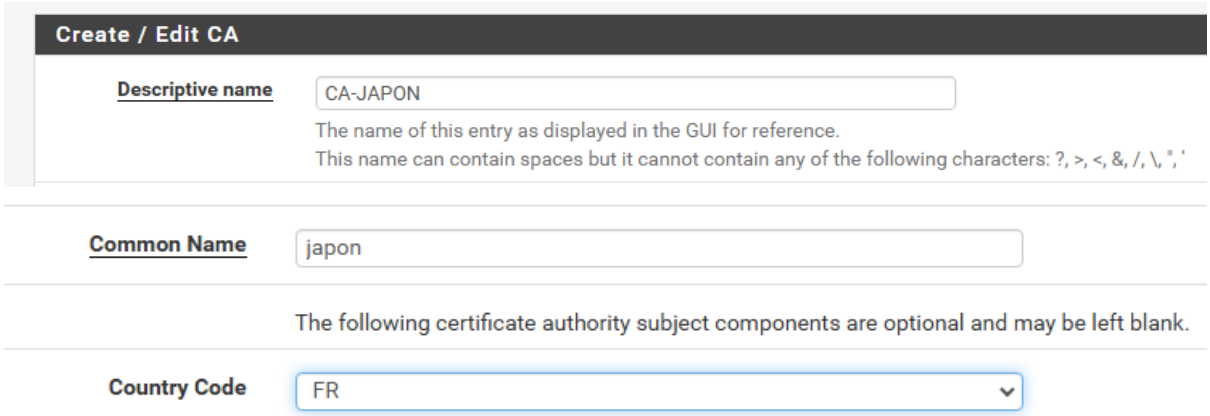
Dans ce tp nous allons utiliser la solution openvpn qui va nous permettre de sécuriser nos échanges en créant un réseau vpn sur notre pare-feu et utiliser des connexions à distance sur un réseau distant vers notre serveur.

Pour commencer nous allons nous rendre sur le pare-feu pfsense et modifier les certificats et en créer un nouveau.

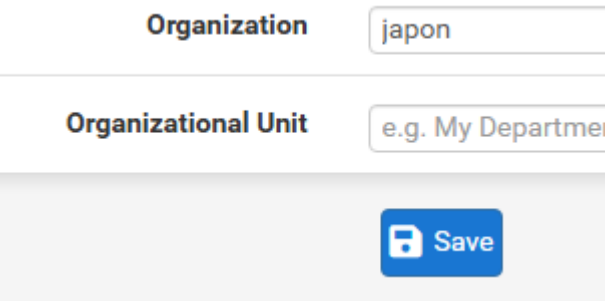




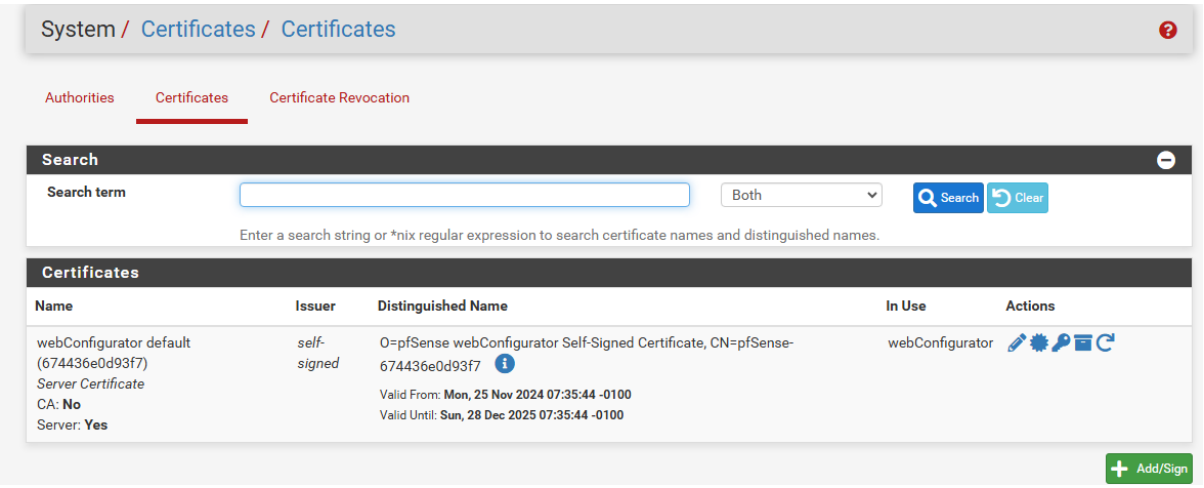
Puis quelques modifications suffisent avec le nom du certificat son nom commun et la langue FR ici



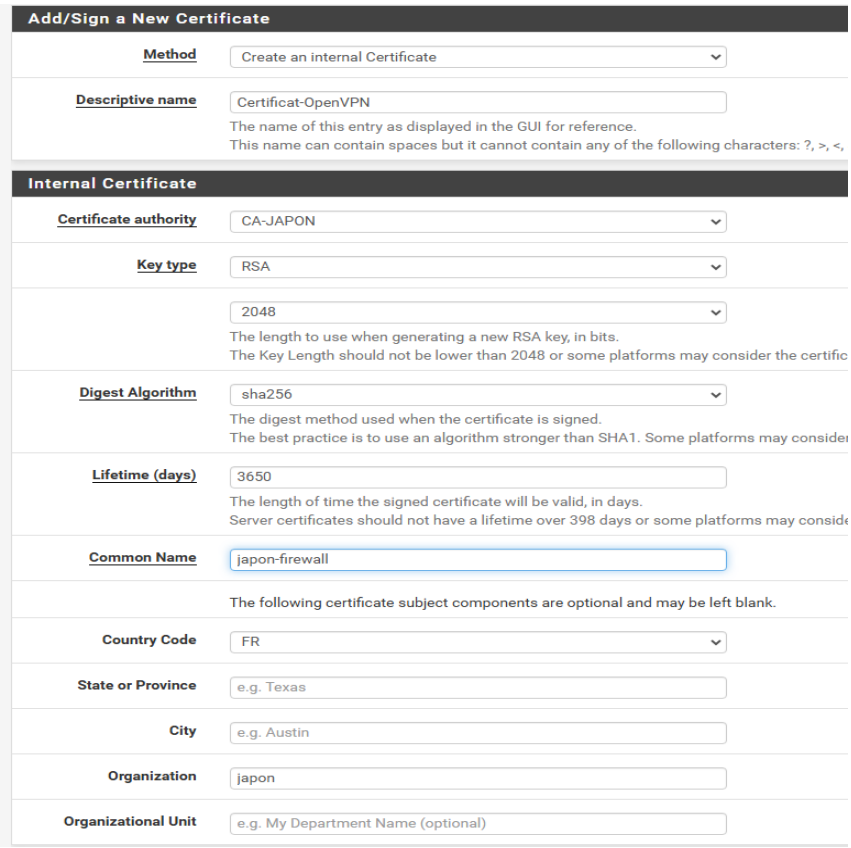
Enfin dans organisation également et on peut faire save



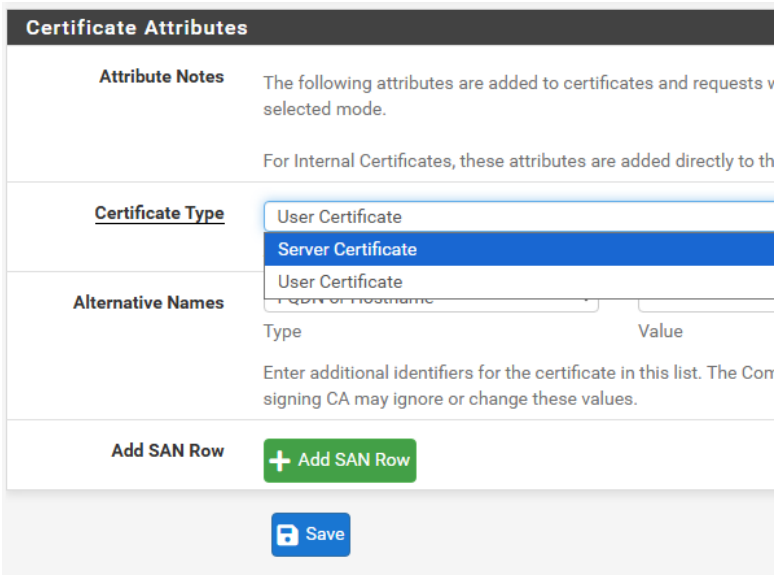
Puis dans l'onglet certificates on va aussi ajouter un autre certificat pour OpenVPN



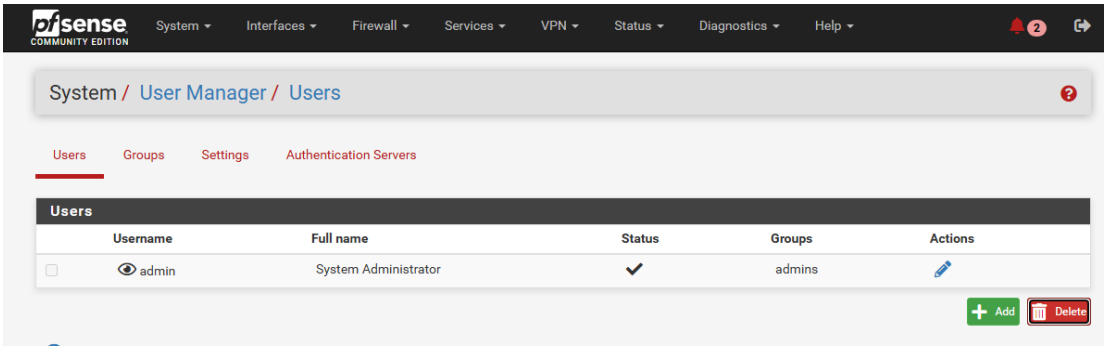
Le paramétrage de nom est quasi identique.



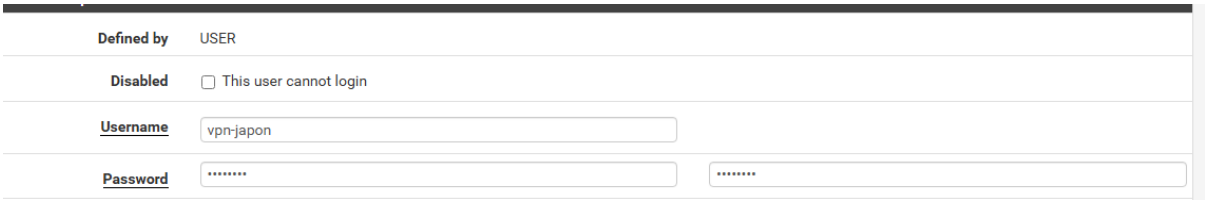
Puis la partie en dessous est à modifier pour un certificat serveur et on save.



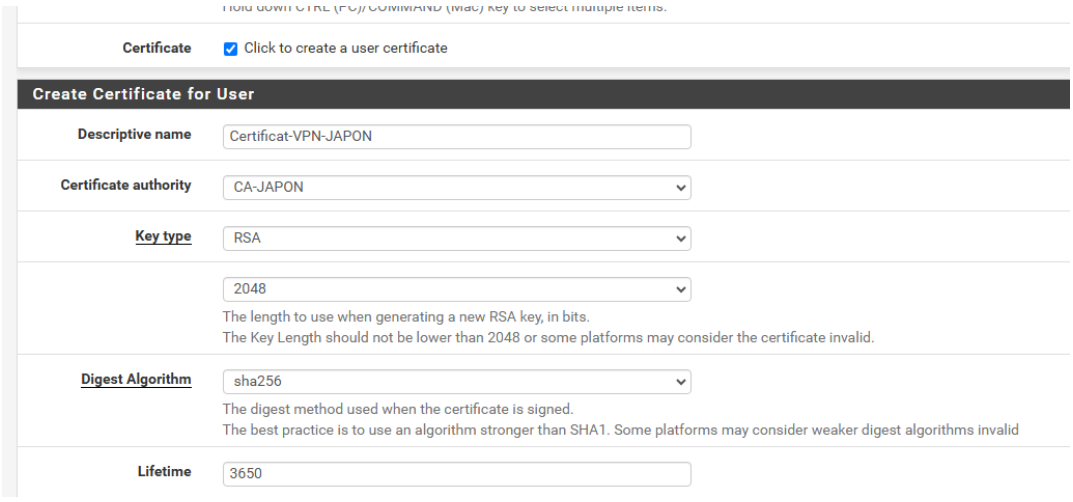
On va maintenant créer un utilisateur pfsense.



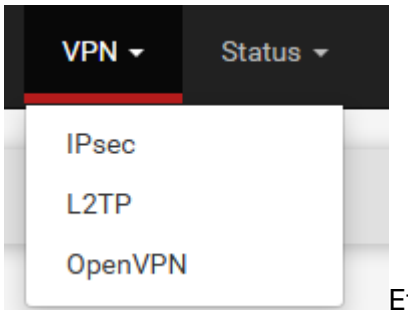
Pour la première partie on va simplement créer un identifiant mot de passe et cocher la case en dessous créer un certificat utilisateur pour la suite



Puis on renseignera juste un nom et on peut enregistrer

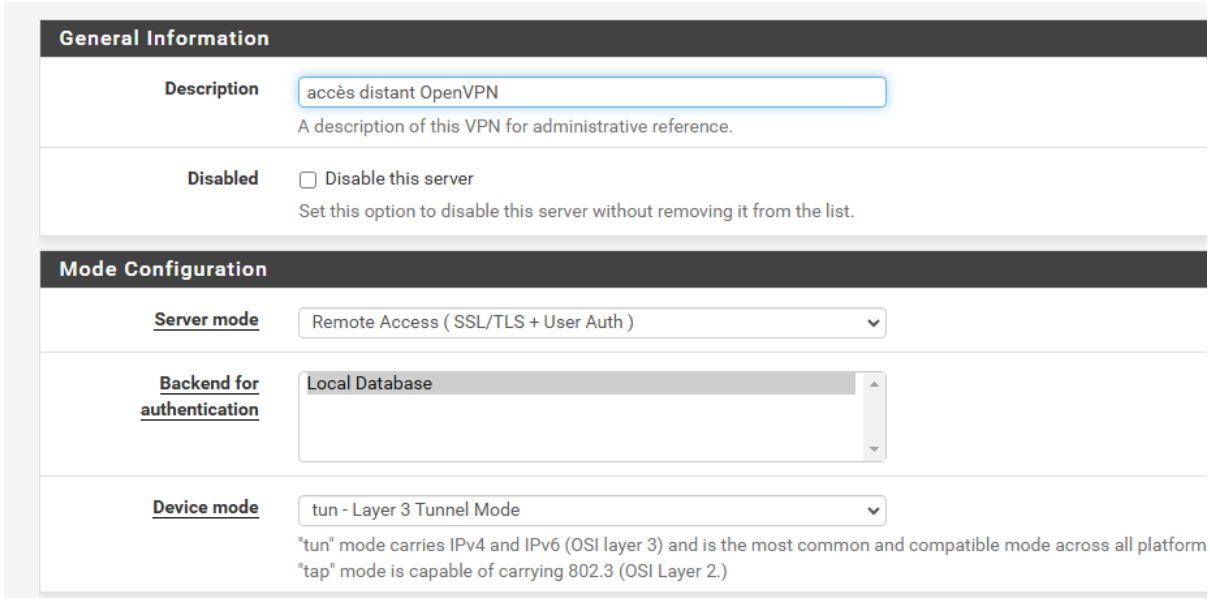


Maintenant que cette préparation est faite on va passer à la configuration open vpn

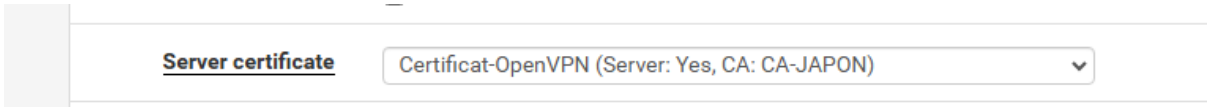


Et on fait ajouter comme les fois précédentes.

Pour les paramètres on sélectionnera remote acces avec le TLS et l'authentification utilisateur.

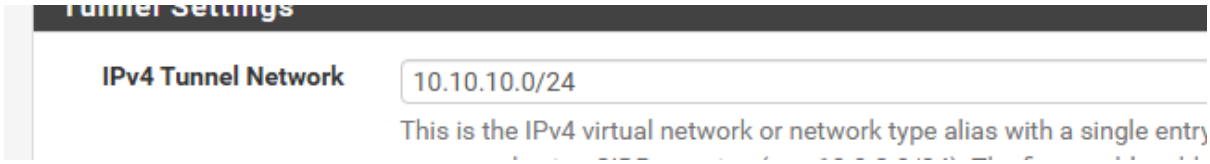


Ensuite on modifiera le certificat serveur.

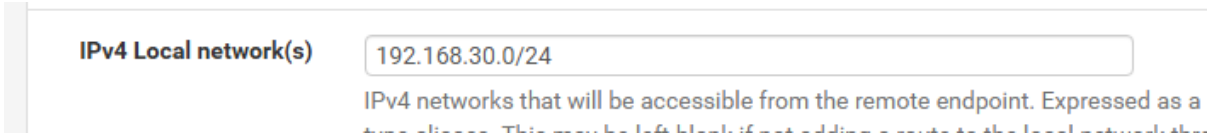


Et on va passer aux paramètres de tunnel et ip

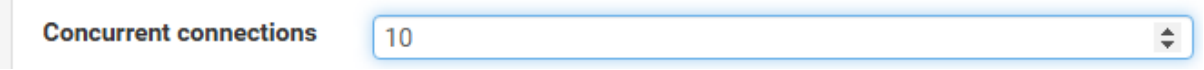
En premier on spécifiera l'adresse qui sera donné pour le tunnel VPN



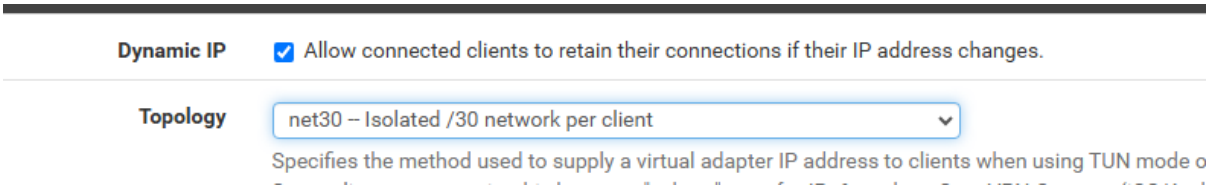
Puis notre réseau pour indiquer la zone d'effet



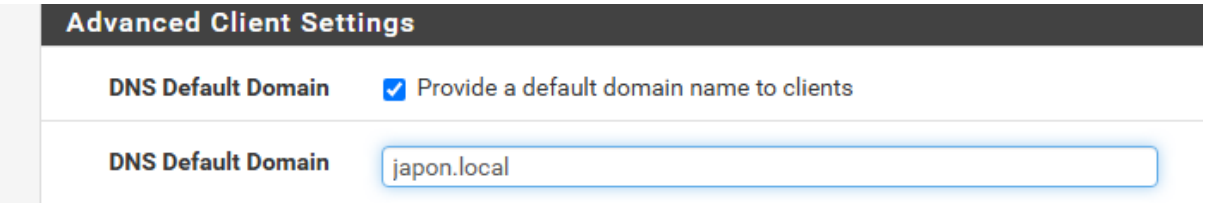
On peut également limiter le nombre d'accès simultané au VPN



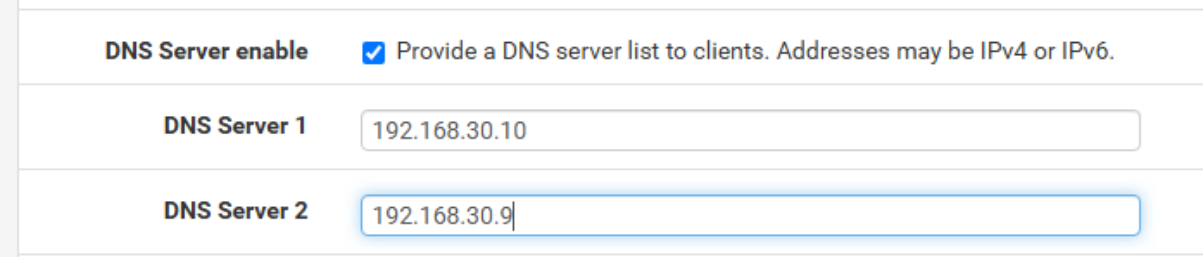
Puis en dessous on va cocher une case et sélectionner la topologie net30 la case permet de maintenir une stabilité pour les postes nomades et la topologie elle met chaque utilisateur dans un sous réseau en /30 pour plus de sécurité



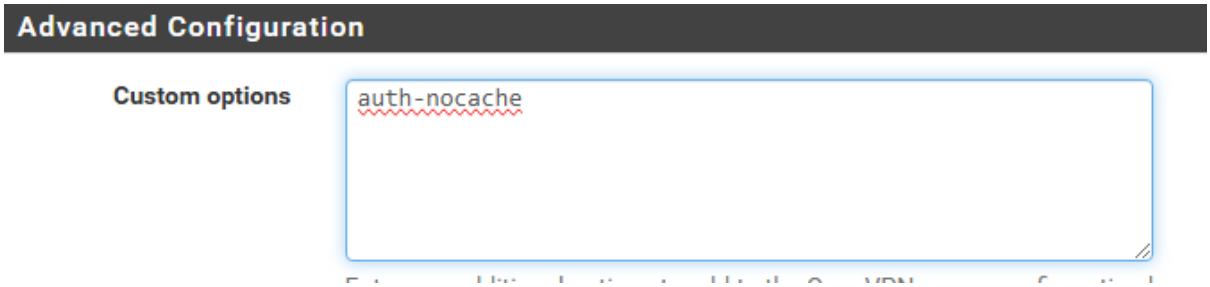
On va ensuite ajouter un domaine par défaut aux clients qui est notre domaine de contexte



Ainsi que nos dns

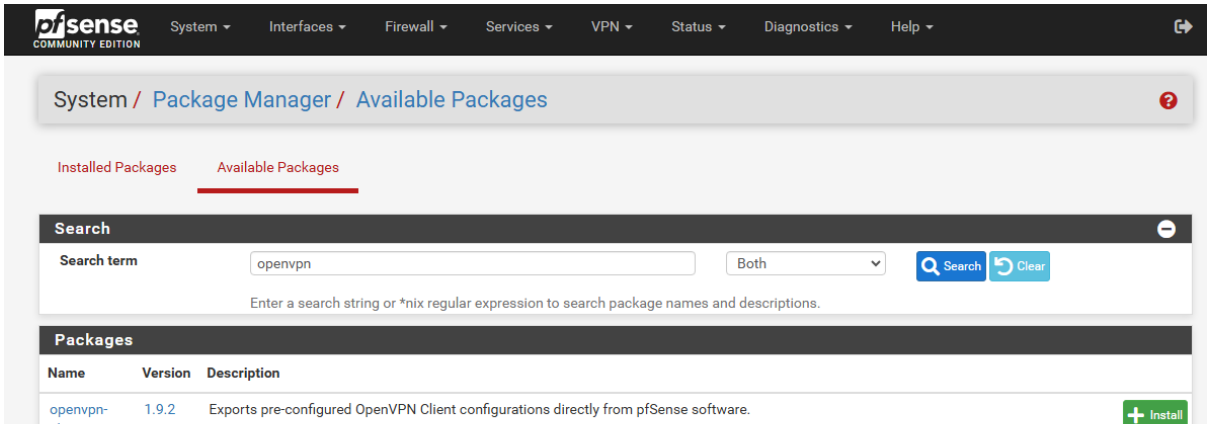


Juste avant de sauvegarder

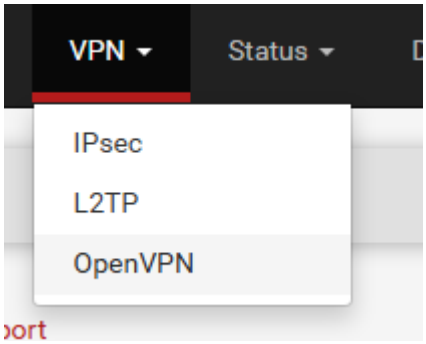


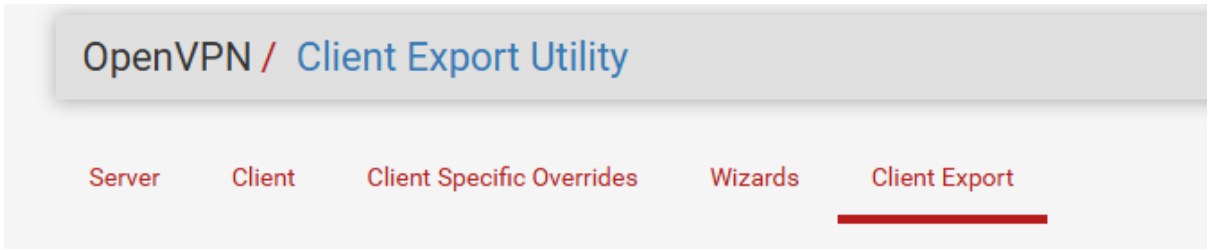
Cette option offre une protection supplémentaire contre le vol des identifiants en refusant la mise en cache.

Prochaine étape installer un package lié à openVPN

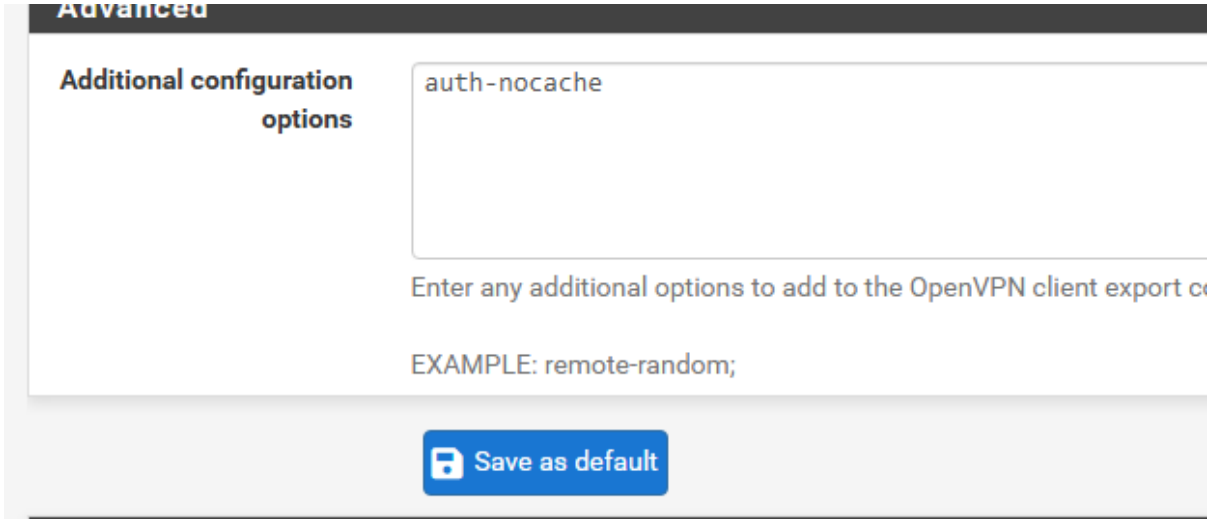


Nous allons maintenant passer à l'export de la configuration openVPN serveur.

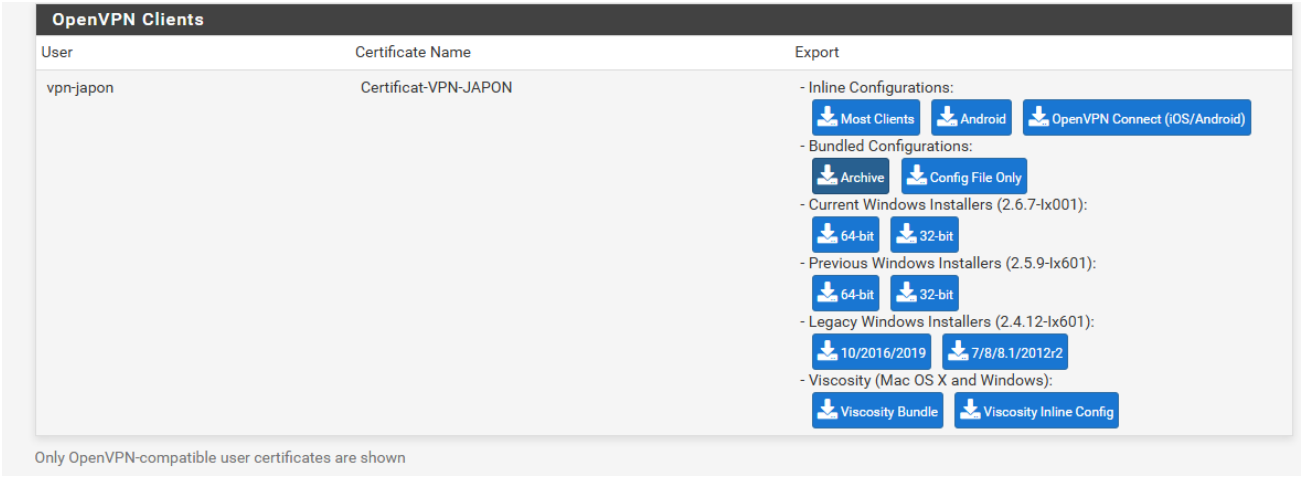




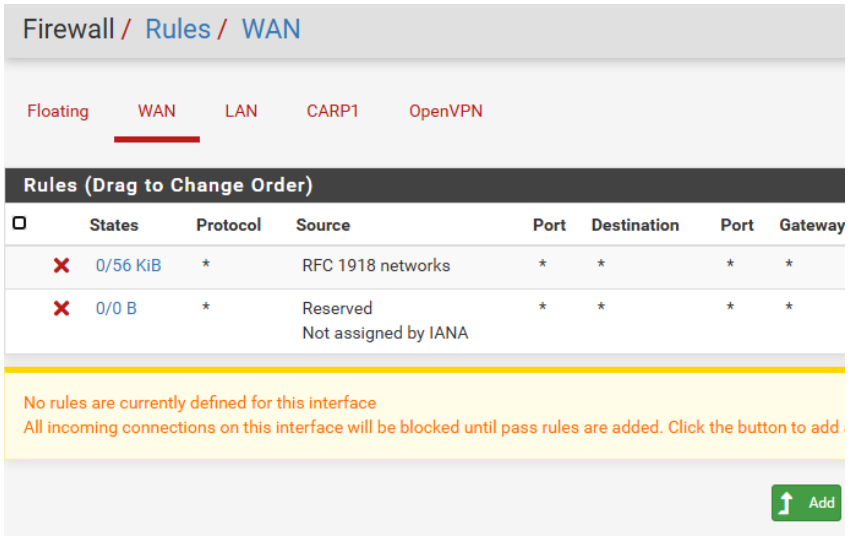
Pour la partie haute on sauvegarde sans rien changer.

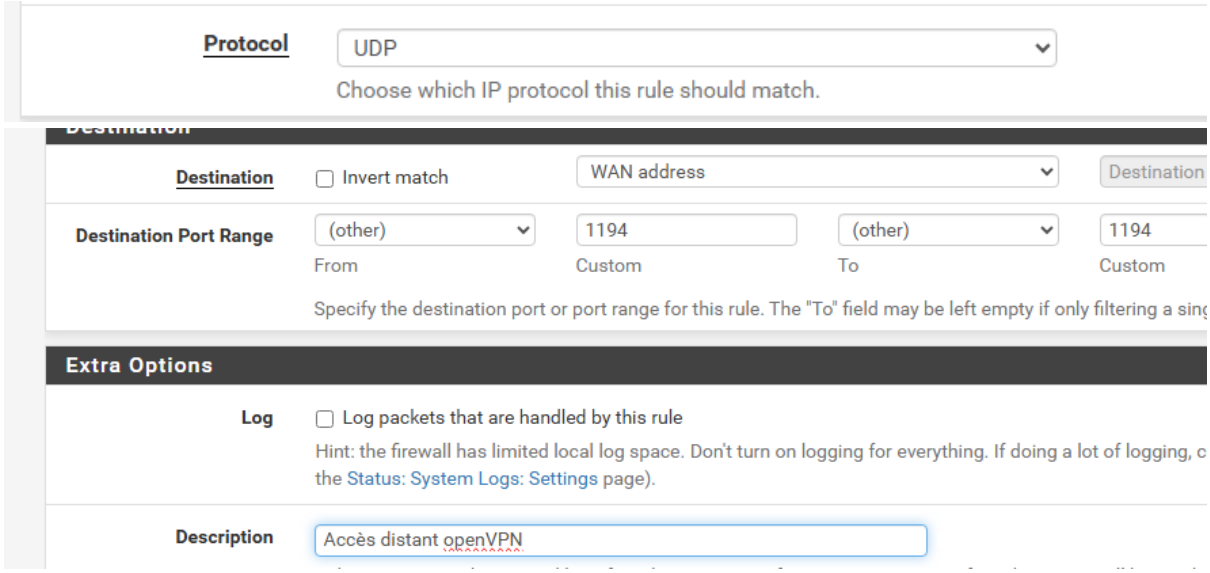


Puis en dessous du bouton sauvegarder on va télécharger l'archive bundled configuration

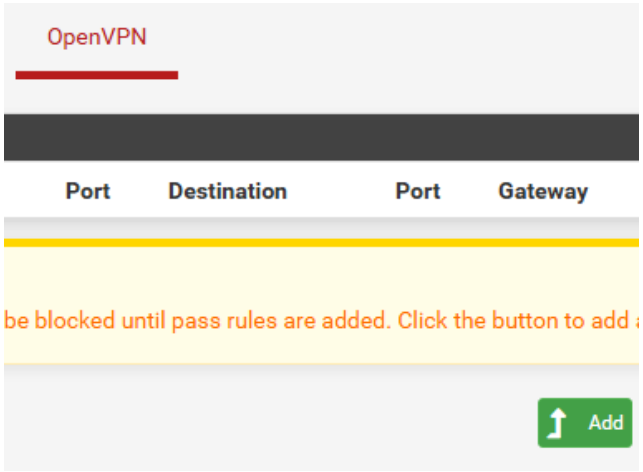

OpenVPN Clients
User
Certificate Name
Export
vpn-japon
Certificat-VPN-JAPON
- Inline Configurations:
Most Clients
Android
OpenVPN Connect (iOS/Android)
- Bundled Configurations:
Archive
Config File Only
- Current Windows Installers (2.6.7-Ix001):
64-bit
32-bit
- Previous Windows Installers (2.5.9-Ix601):
64-bit
32-bit
- Legacy Windows Installers (2.4.12-Ix601):
10/2016/2019
7/8/8.1/2012r2
- Viscosity (Mac OS X and Windows):
Viscosity Bundle
Viscosity Inline Config
Only OpenVPN-compatible user certificates are shown

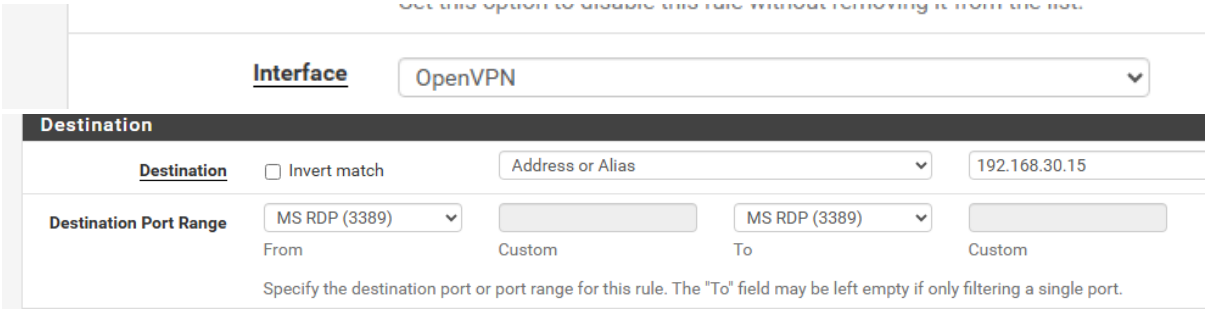
On va ajouter une règle dans le WAN sur le firewall pour autoriser les connections open vpn avec quelques changements



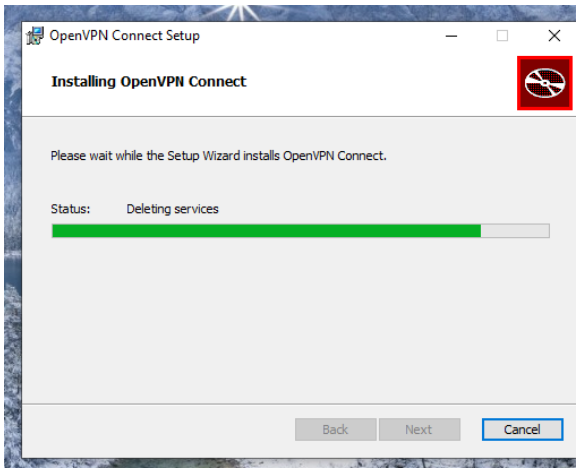


Ainsi qu'une deuxième dans la partie openVPN

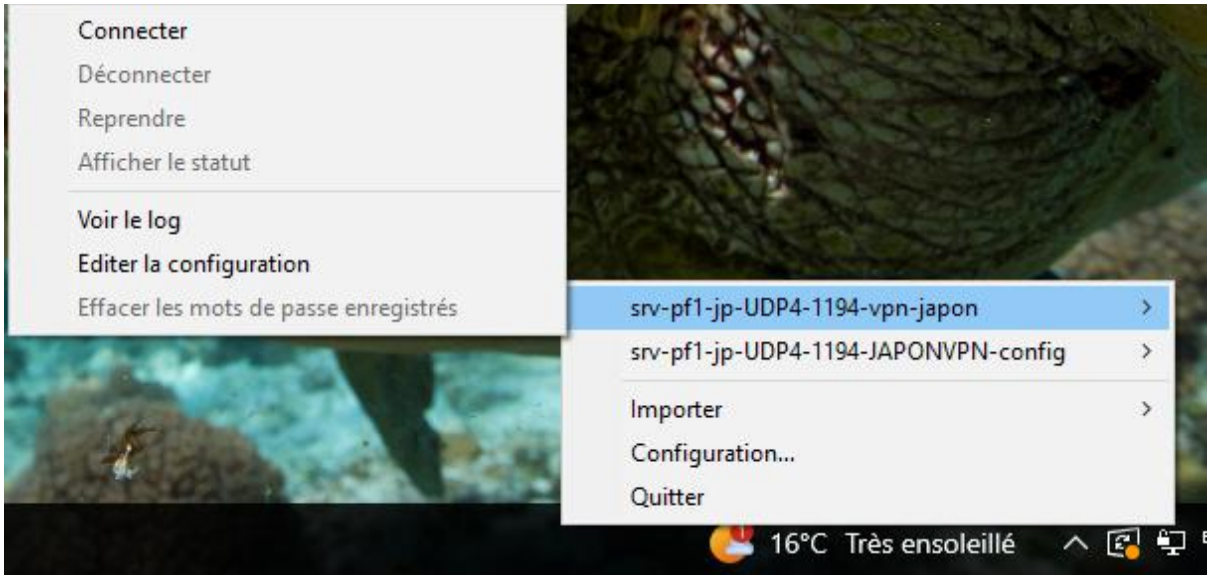




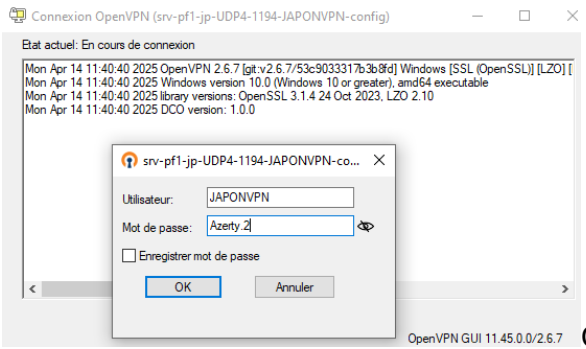
On va maintenant se connecter via le post client avec tout d'abord l'installation du client vpn



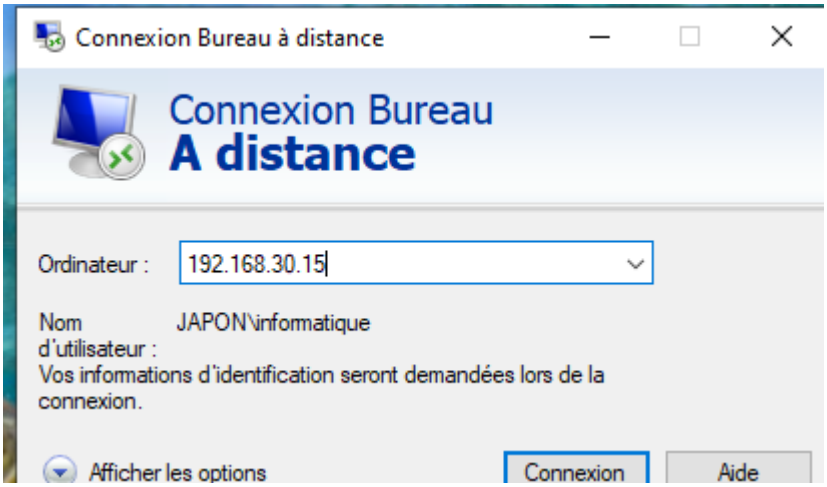
Puis en bas à droite on va sur la petite icône qui est apparue et on fait connecter sur le profil crée récemment.

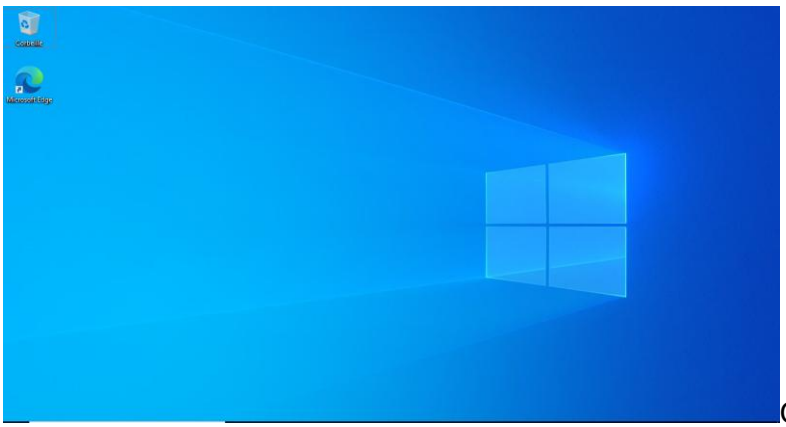


Puis on rentre les identifiants.



On peut ensuite tenter la connexion à notre serveur RDS




On arrive bien sur une session vierge du serveur RDS le VPN fonctionne bel et bien.

Voilà qui conclue notre tp ou nous avons désormais un vpn pour notre infrastructure accessible sur les postes clients pour qu'ils puissent avoir accès à une session à distance prévu pour le travail via VPN. Avec des utilisateurs pour la gestion d'accès on va dans le prochain tp lié les utilisateurs active directory avec les utilisateurs pfsense.