easy Former
La formation à 360°

Interconnexion AD, Pfsense et OpenVPN

Ce document a pour but de décrire les étapes à réaliser pour se connecter à OpenVPN du Pfsense avec un utilisateur de l'Active Directory

Référence : EF-MS-AD&VPN

Auteur(s) :
Dorian Manzanares

Destinataire(s) :
Easyformer

Date de modification : 10/12/21

Version : 1

Sommaire

page

1 PREREQUIS ACTIVE DIRECTORY ET PFSENSE 3

1.1 GESTION DE L'ANNUAIRE 3
1.1.1 Topologie 3
1.1.2 Créations d'users 3
1.2 GESTION DE PFSENSE 4
1.2.1 Création de L'authentification avec AD 4
1.2.2 Gérer les droits et connexion au pare-feu avec un utilisateur de l'AD (facultatif) 6
1.2.3 Tests de liaison au serveur LDAP 7

2 MISE EN PLACE DE OPEN VPN 9

2.1 LES CERTIFICATS 9
2.1.1 Création d'une autorité de certification et d'un certificat pour le VPN 9
2.2 TUNNEL OPENVPN 11
2.2.1 Configuration du tunnel 11
2.3 EXPORTER LA CONFIGURATION OPENVPN 14
2.3.1 Installation du package 14
2.4 REGLES DE FIREWALL 15
2.4.1 Gestion des règles pour le VPN 15

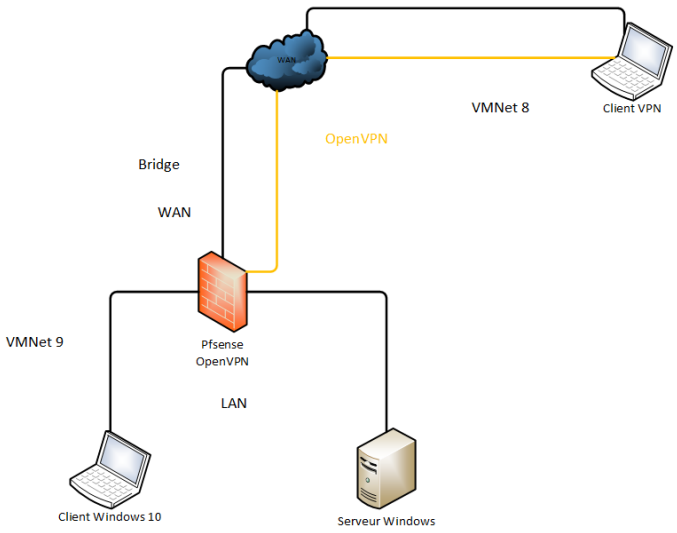
3 CONNEXION AU TUNNEL VPN 16

3.1 INSTALLATION ET TESTS 16
3.1.1 Utiliser l'assistant OpenVPN 16

1 Prérequis Active directory et Pfsense

1.1 Gestion de l'annuaire

1.1.1 Topologie



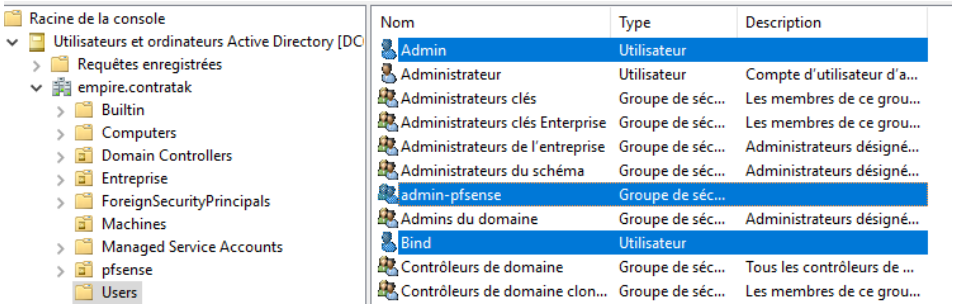
1.1.2 Créations d'users

Le but de ce TP sera de mettre en place un VPN client to site avec OpenVPN et associer pfSense à l'active directory.

Les utilisateurs créés pourront se connecter en VPN avec leurs identifiants de l'AD.

Tout d'abord, il faudra se rendre dans « Utilisateurs et ordinateurs Active Directory » au niveau de notre Windows Server, puis dans « Users ».

Ici nous allons créer deux utilisateurs et un groupe.



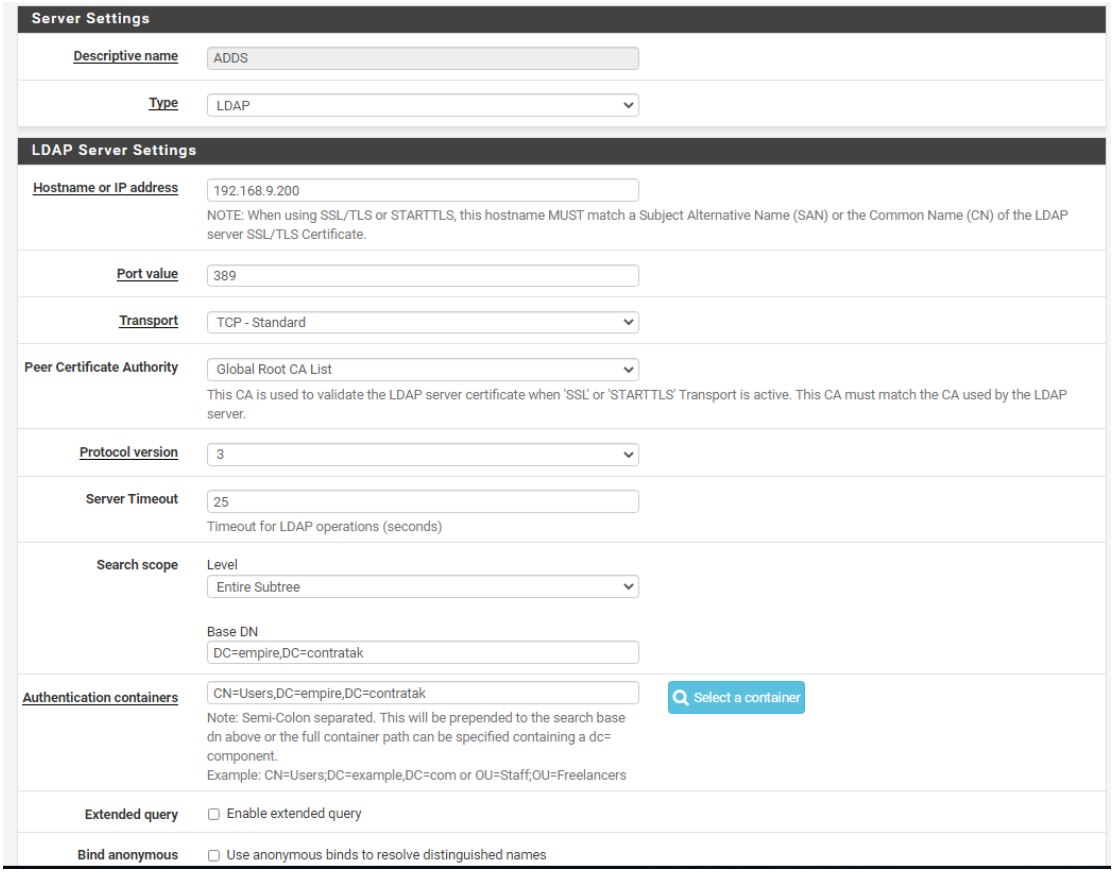
Maintenant, nous allons créer un compte grâce auquel Pfsense pourra récupérer les informations de la base de données active directory.

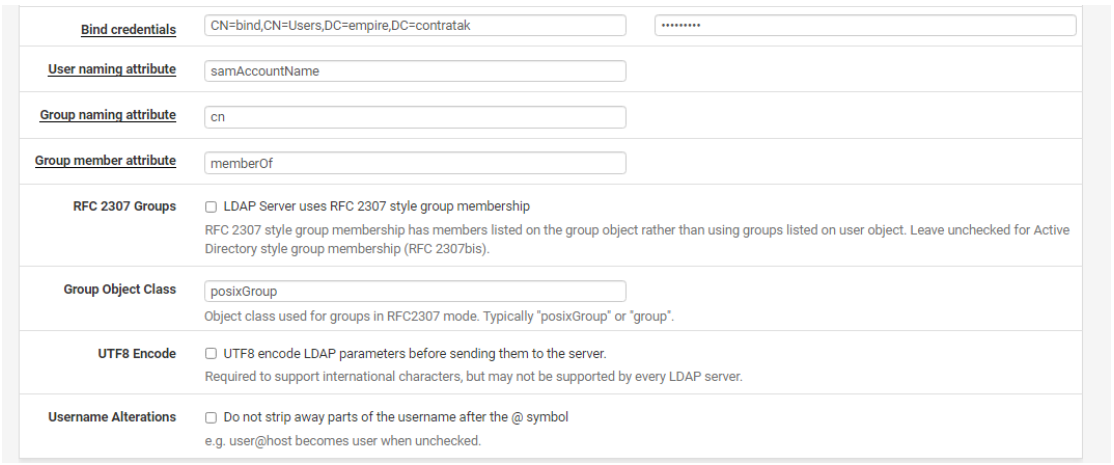
- Créer un utilisateur nommé Bind
- Créer un groupe nommé « admin-pfsense »
- Ajouter l'utilisateur « Admin » au groupe « admin-pfsense »

1.2 Gestion de Pfsense

1.2.1 Création de L'authentification avec AD

Dans pfSense on se rendra dans « System » puis « User manager » et on choisira l'onglet « authentication Server » puis, on clique sur add.





- Dans Hostname or IP address Il faut renseigner l'IP du serveur.
- La base DN signifie le nom de domaine "DC=empire,DC=contratak

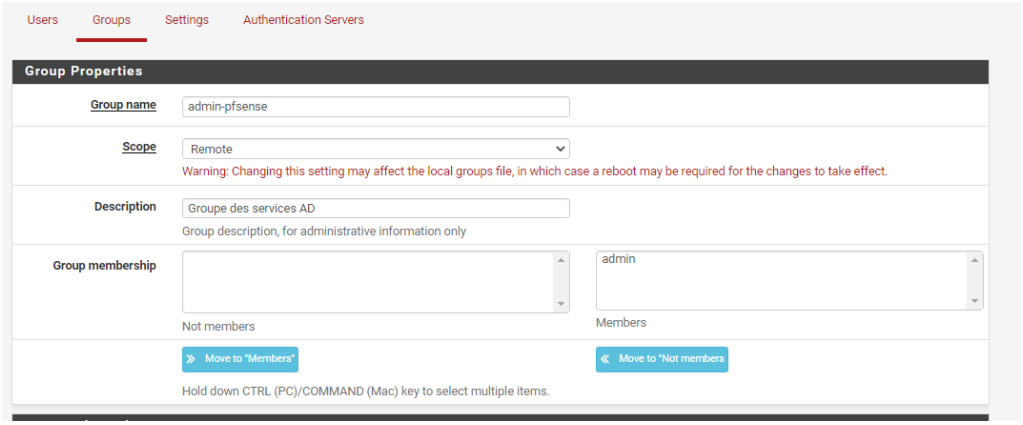
  C'est le nom de domaine que j'ai choisi pour mon Windows Server.
- Pour l'authentification containers, il faut choisir un compte dont le mot de passe n'expirera pas car sinon les authentifications ne pourront pas se faire cela peut poser de gros problèmes si ce compte devient indisponible. Donc ça sera le compte « Bind » crée plus haut.

Une fois que tous les champs sont bien remplis,on peut cliquer sur save.

1.2.2 Gérer les droits et connexion au pare-feu avec un utilisateur de l'AD (facultatif)

Il faut ajouter le groupe « admin-pfsense » créé dans l'AD sur pfsense avec le même nom dans l'onglet System\user manager.

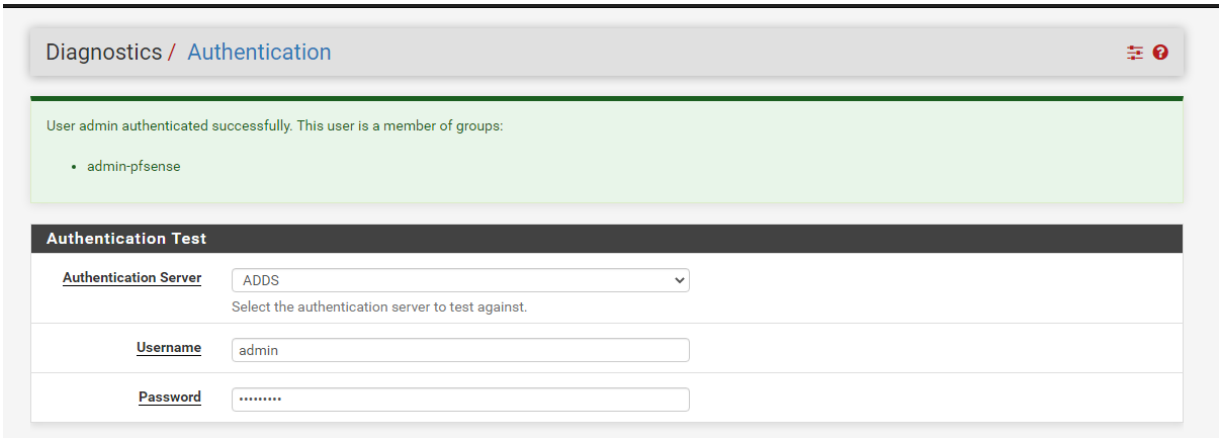
Il faut choisir un type « remote »



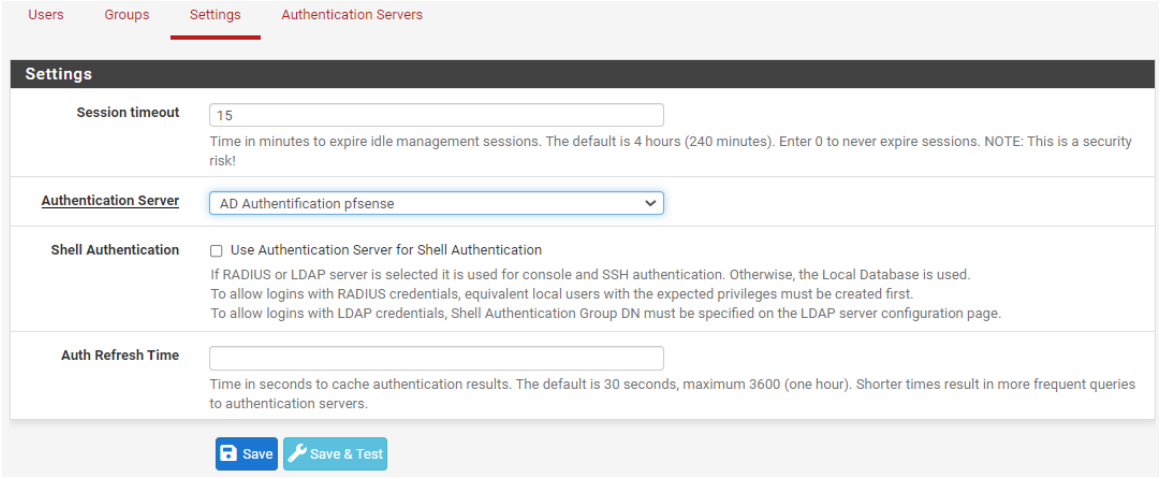
1.2.3 Tests de liaison au serveur LDAP

On peut maintenant tester l'authentification d'un utilisateur de mon domaine au niveau de Pfsense.

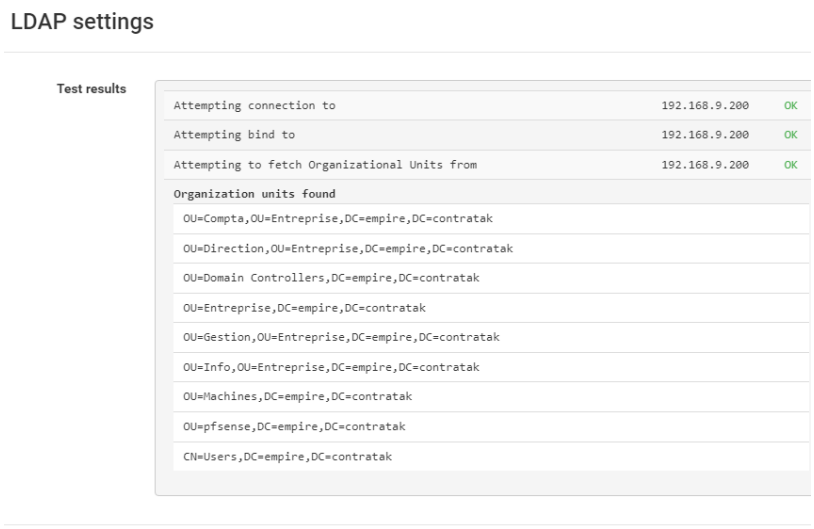
Pour cela, il faut se rendre dans l'onglet « Diagnostic » puis dans « Authentication ».



Après un test réussi au niveau de notre utilisateur, nous allons pouvoir tester la bonne lisaison de Pfsense avec l'Active Directory, pour se faire, il faut se rendre dans le menu « Settings » et renseigner la base de donnée LDAP.



Save and test permet de vérifier que la synchro pfsense et AD fonctionne bien.



Le résultat du test confirmera que notre configuration est valide.

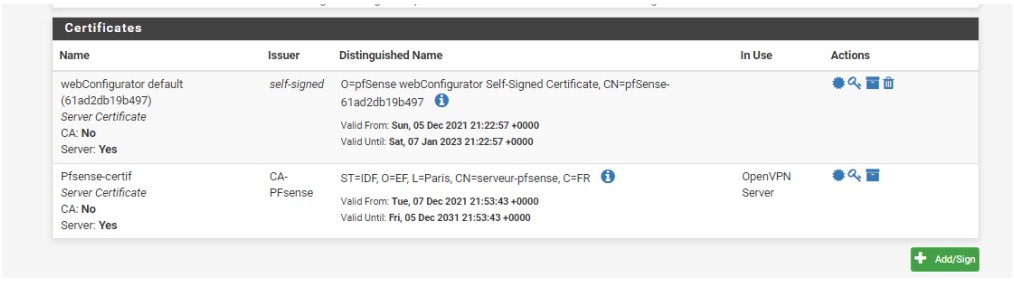
2 Mise en place de open VPN

2.1 Les certificats

2.1.1 Création d'une autorité de certification et d'un certificat pour le VPN

J'ai choisi d'appeler mon autorité de certificat CA-PFsense

Et mon certificat utilisateur pour OpenVPN nommé Pfsense-certif



Bien que j'utilise l'annuaire LDAP pour me connecter au VPN, il faut tout de même créer un utilisateur.

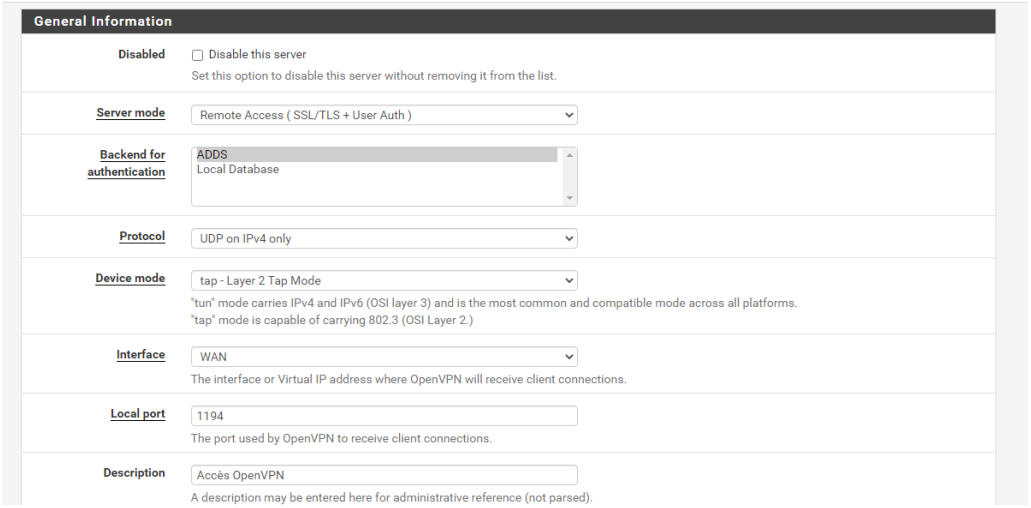
Dans User certificat, il faudra cliquer sur add, on sera alors redirigé vers une page pour créer un certificat.

Il faudra ensuite uniquement vérifier que le type de certificat « User » soit bien sélectionné.

2.2 Tunnel OpenVPN

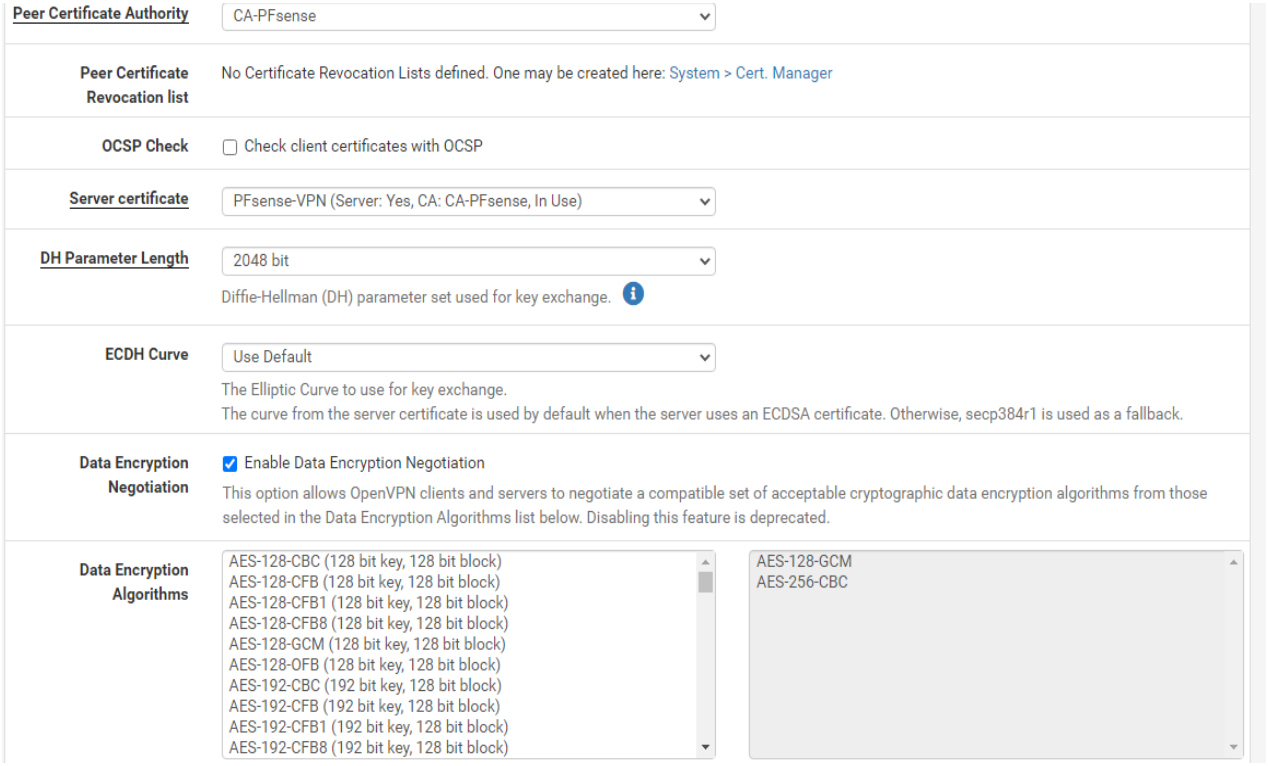
2.2.1 Configuration du tunnel

Nous allons maintenant configurer le tunnel VPN, c'est-à-dire paramétrer le serveur (Pfsense).

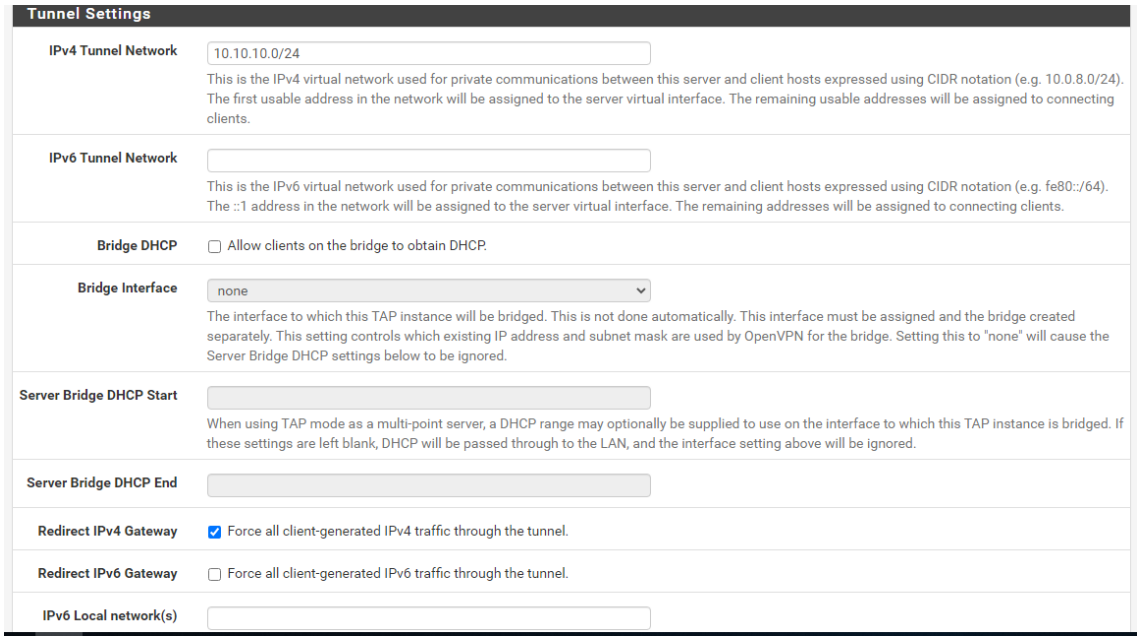


Ci-dessus il faut préciser que le VPN recevra ses clients depuis l'interface WAN et que le port de réception sera le port 1194, il est important de donner une description.

Là j'ai choisi l'autorité de certificat que j'ai créé auparavant pour les échanges sécurisés.

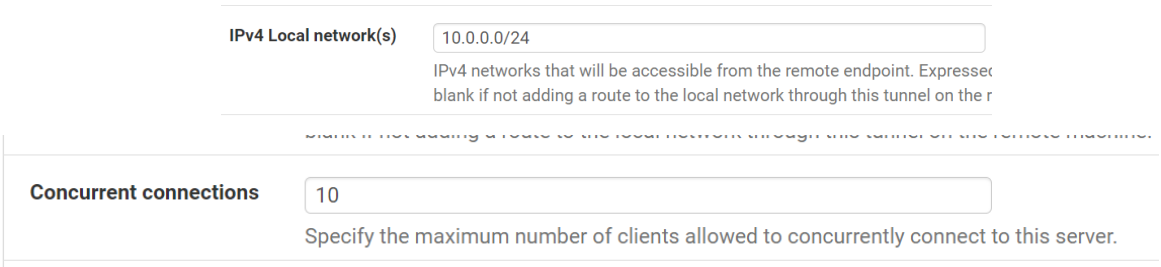


Là le réseau IPV4 du tunnel VPN et renseigné en tant que : 10.10.10.0/24 c'est-à-dire que lorsque quelqu'un se connectera en VPN, il fera partie de ce réseau.

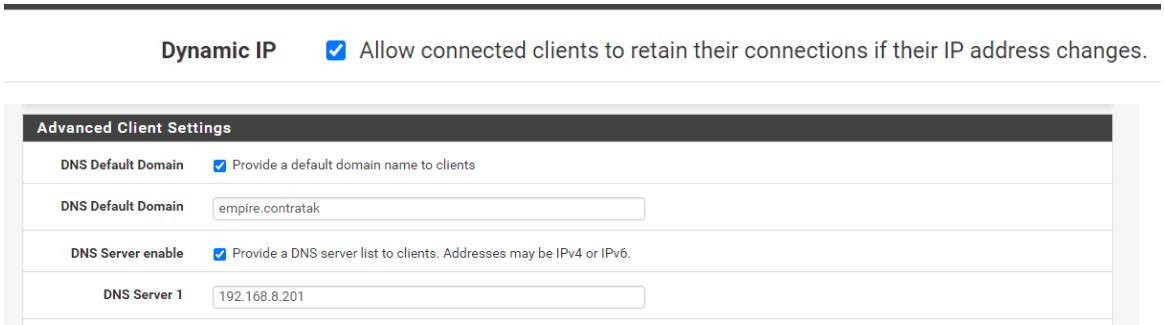


Là précise que lorsque l'utilisateur sera connecté en VPN il aura accès au réseau inscrit pour ajouter un autre réseau il suffit de rajouter un point-virgule.

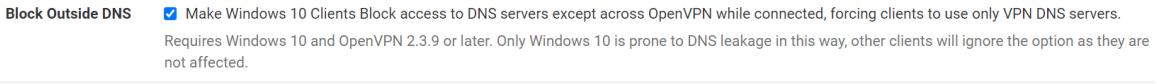
Ce champ renseigne la limitation connexion simultanée avec un compte en VPN



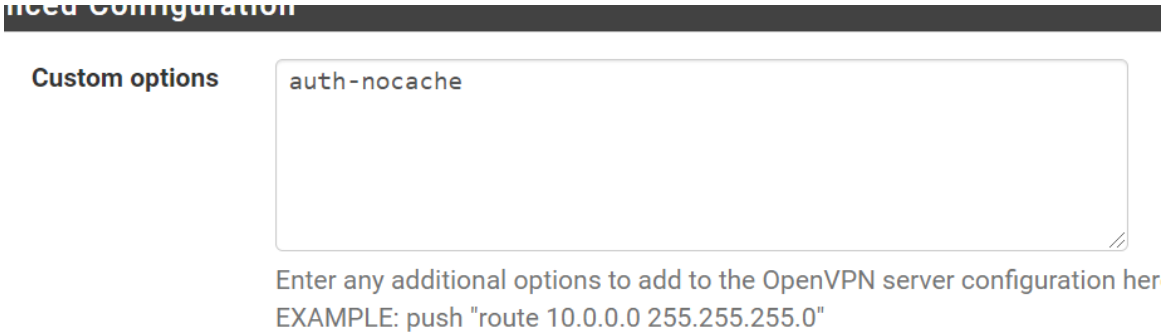
Ce champ facilite le changement d'adresse IP du client lorsqu'ils se connectent en VPN en effet cela peut causer certains problèmes lorsque le client se connectent plusieurs fois avec plusieurs adresses IP publique différentes ce champ remédie à ce problème.



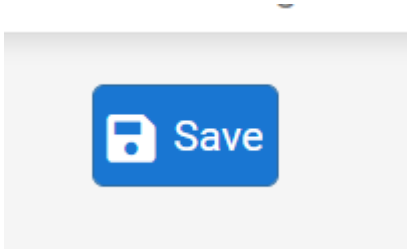
L'option suivante permet de résoudre un bug Windows qui empêche la résolution de nom DNS lorsque que le VPN est activé, en effet il utilise DNS local au lieu du VPN.



Cette option permet de supprimer le cache de connexion ce qui limite les risques d'attaque.



Une fois la configuration effectuée, il est temps de la sauvegarder.



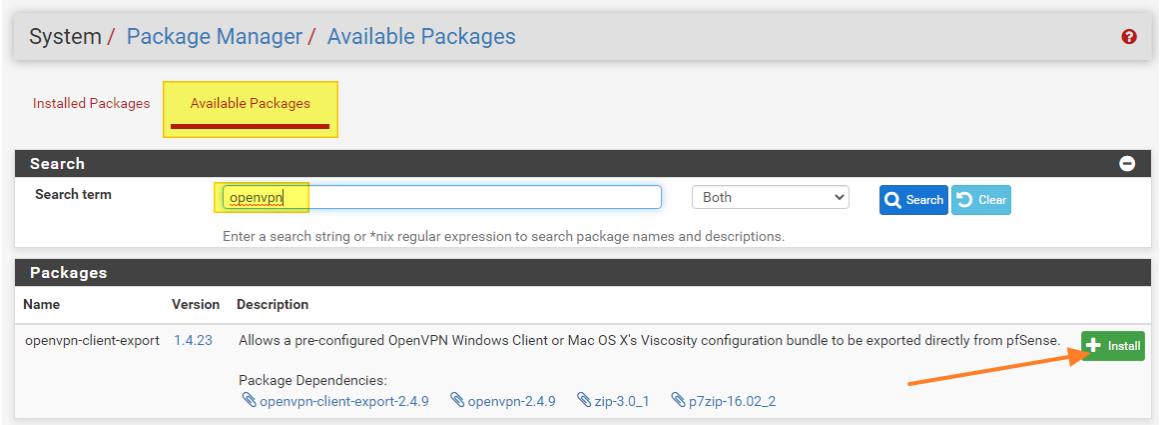
2.3 Exporter la configuration OpenVPN

2.3.1 Installation du package

Pour télécharger la configuration, il est nécessaire d'installer un paquet supplémentaire sur notre pare-feu.

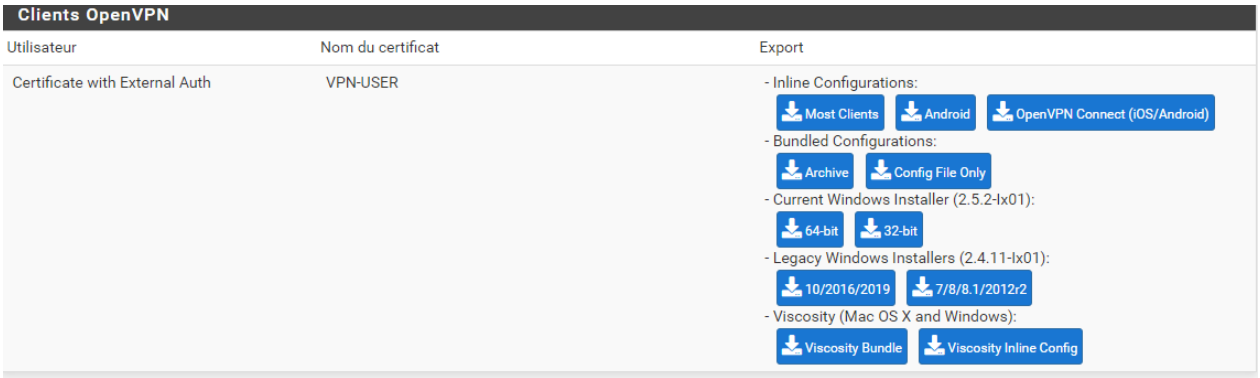
Rendez-vous dans le menu suivant : System > Package Manager > Available Packages.

Il faudra ici installer le paquet « openvpn-client-export ».



Il faudra ensuite se rendre dans : VPN/OpenVPN/Servers puis dans client export

Cliquez sur archive qui téléchargera la configuration tu certificats open VPN de fichier sera un zip à décompresser, le lien de téléchargement est disponible choisir en fonction de son système d'exploitation. Et lancer les fichiers avec open VPN.



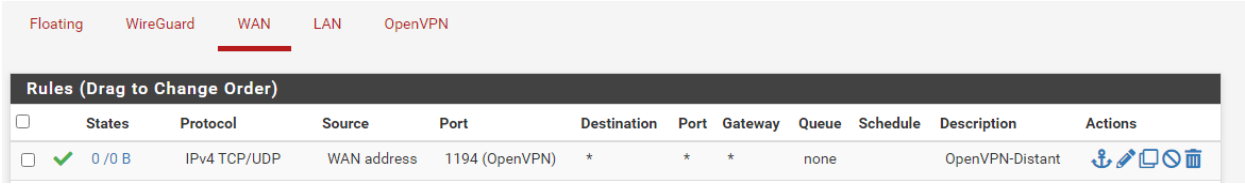
On peut voir ici que Pfsense considère mon authentification comme « externe » soit l'ADDS.

Il faut télécharger et installer « Current Windows Installer 64 bits », sur la machine Windows.

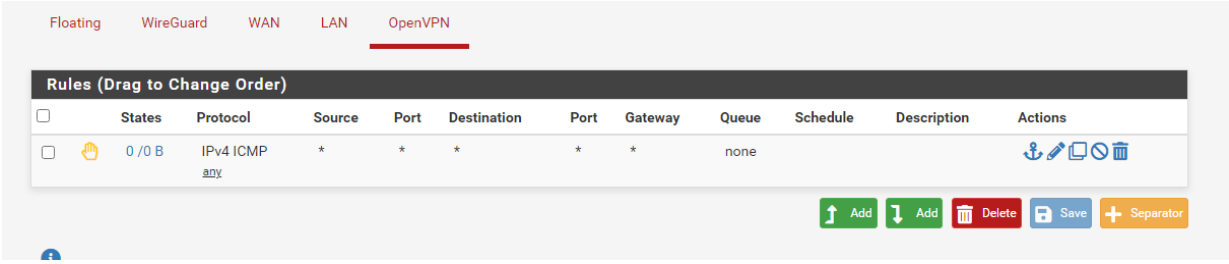
2.4 Règles de firewall

2.4.1 Gestion des règles pour le VPN

Les règles de firewall sont à fixer en fonction de vos besoins ou de ceux de l'entreprise.



Et ensuite sur l'onglet OpenVPN :



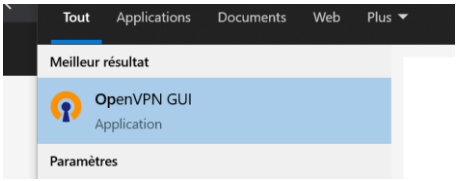
On peut par exemple ici remarquer que pour l'interface OpenVPN (qui est créée automatiquement lors de la création du VPN), je vais bloquer l'ICMP.

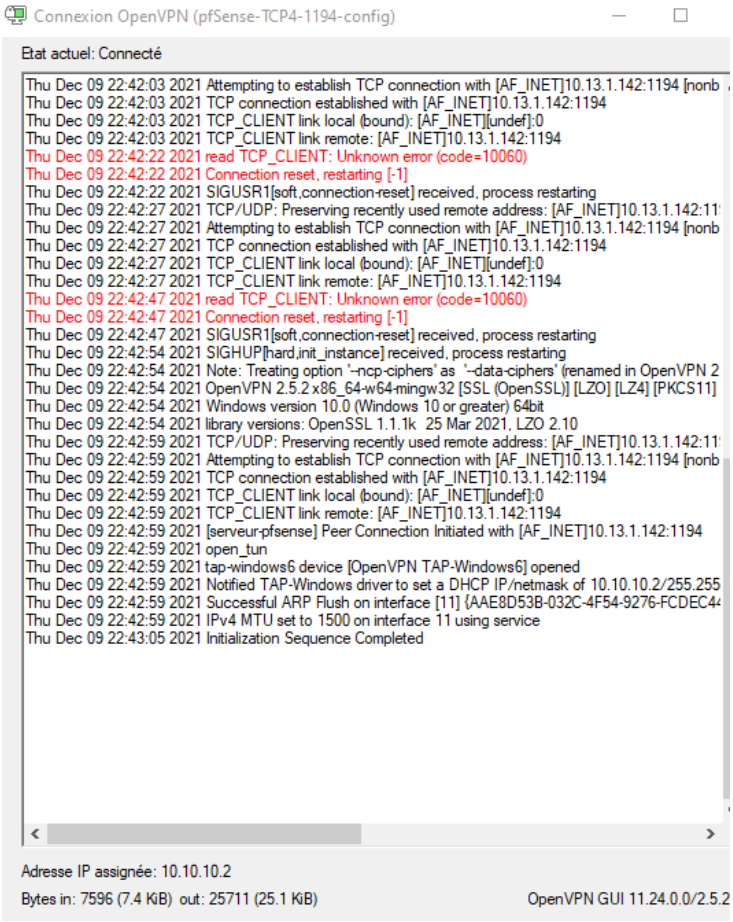
3 Connexion au tunnel VPN

3.1 Installation et tests

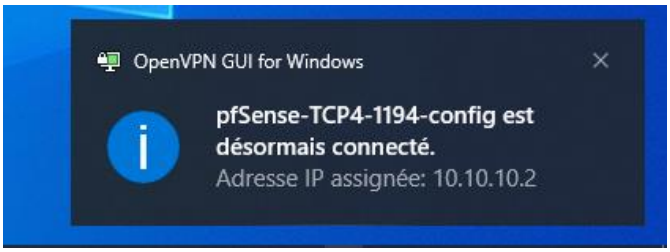
3.1.1 Utiliser l'assistant OpenVPN

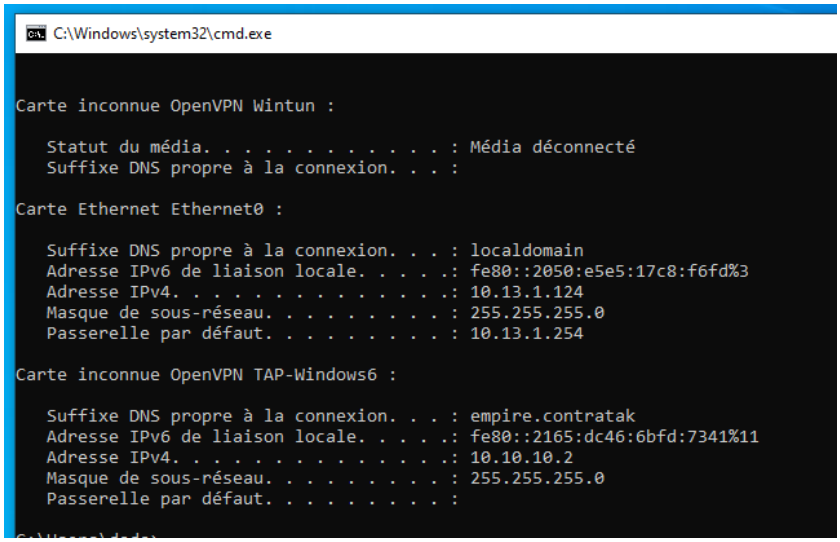
On lance OPENVPN, on va ici se connecter avec l'utilisateur « Admin » créée sur notre Active Directory.



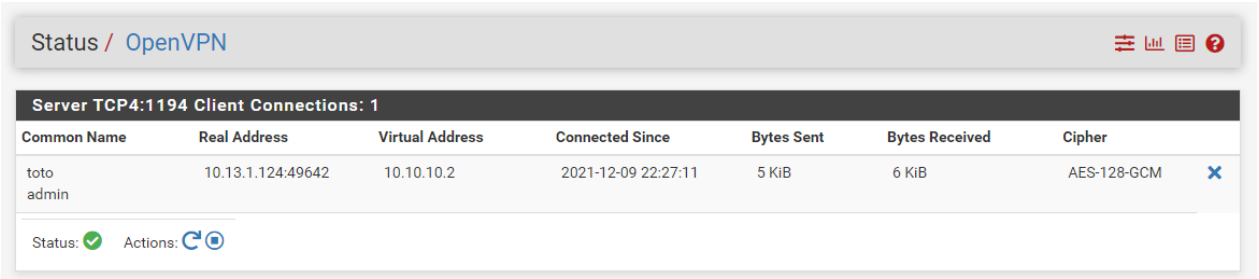


On on peut voir que j'ai une adresse IP en 10.10.10.0/24 comme défini au préalable, le DHCP du pfSense m'a bien fourni une adresse IP.





Sur pfsense, on peut voir le tunnel créé via « Status/OpenVPN »



Voilà, votre tunnel est configuré, et vous vous êtes connecté avec un utilisateur du domaine