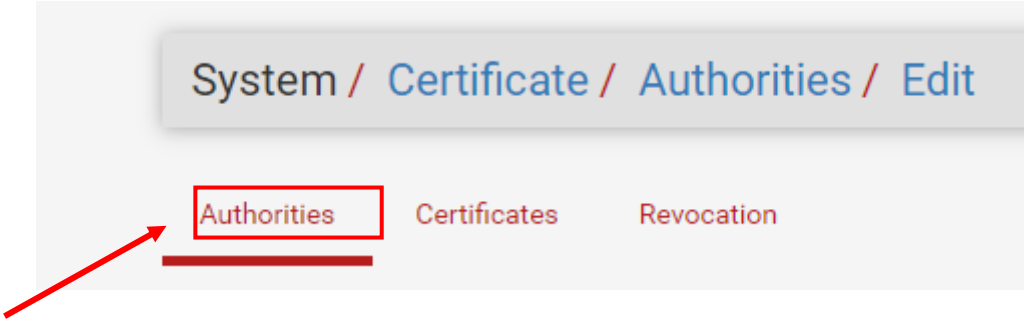
Configuration d’OpenVPN

Matthis LAPULY
REALISATION PERSONELLE

I. Créations des certificats

Etape 1 : On va se rendre sur l'interface Pfsense pour aller sur System < Certificates < Authorities pour ajouter une autorité

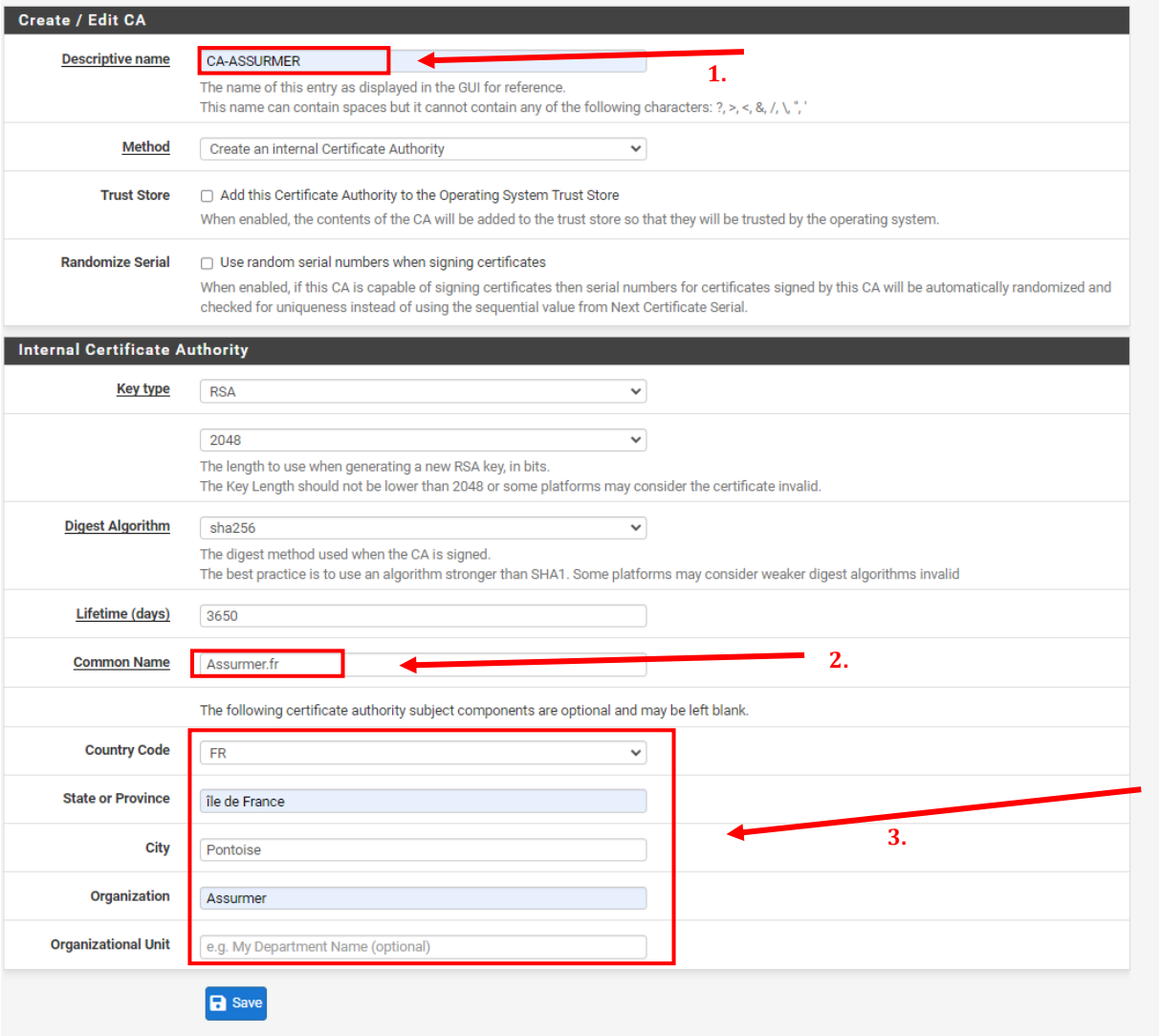
Nous devons commencer par crée une autorité de certification



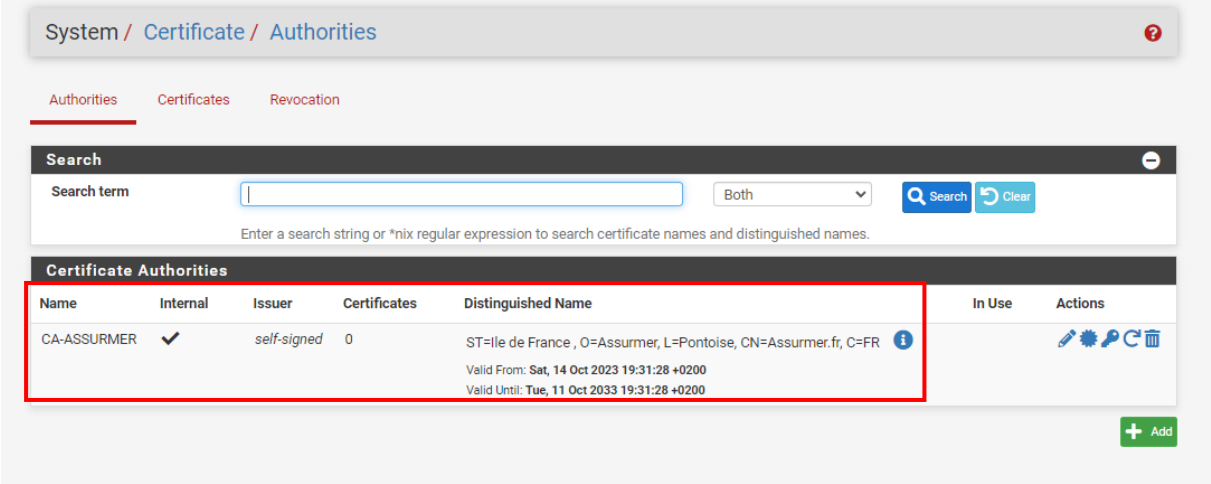
Etape 2 : Nous allons remplir les champs correspondants :

- Description Name : On nomme l'autorité de certification
- Common Name : Cela sera le nom des certificats généré par cette autorité
- Nous devons indiquer des informations concernant notre entreprise pour les champs restant

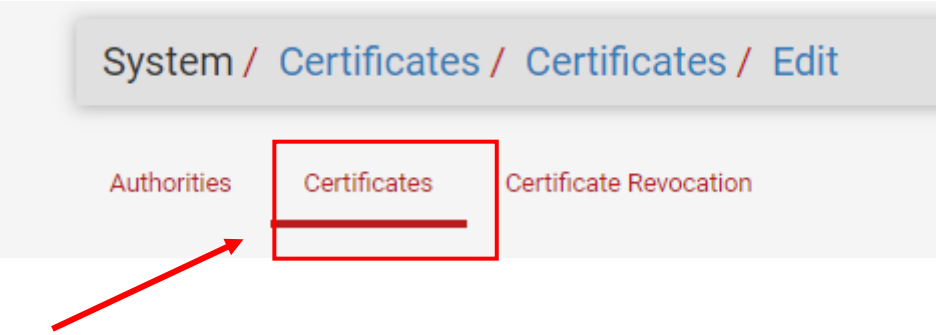
Nous laissons les autres champs par défaut



Une fois fini on va cliquer sur « Save » pour visualiser notre autorité de certification

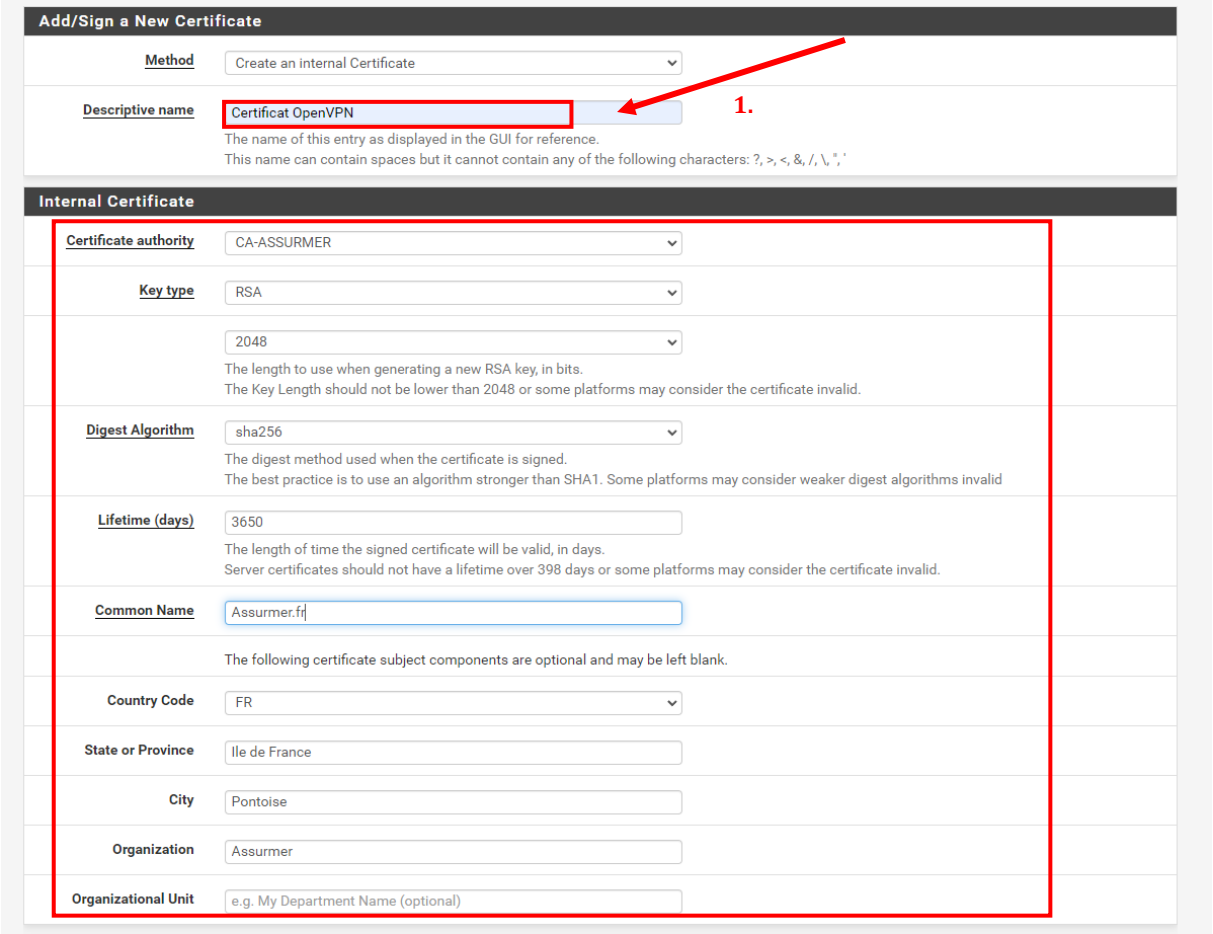


Etape 3 : On va maintenant aller sur Certificate pour crée un certificat pour notre serveur

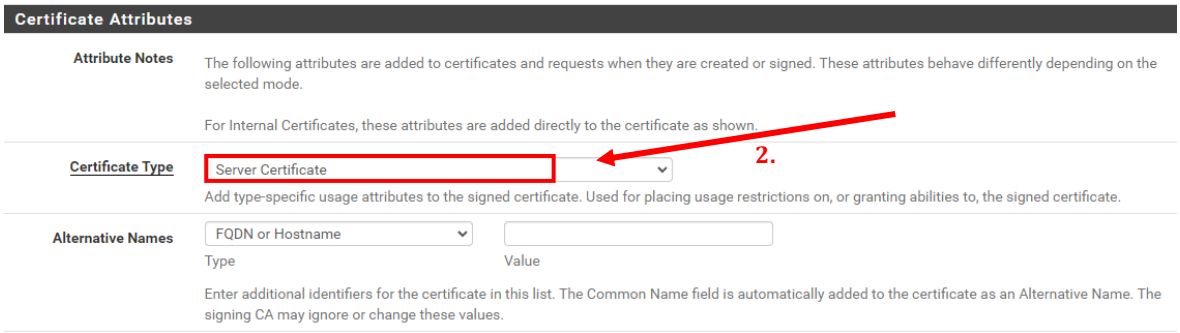


Etape 4 : On va remplir les champs correspondants :

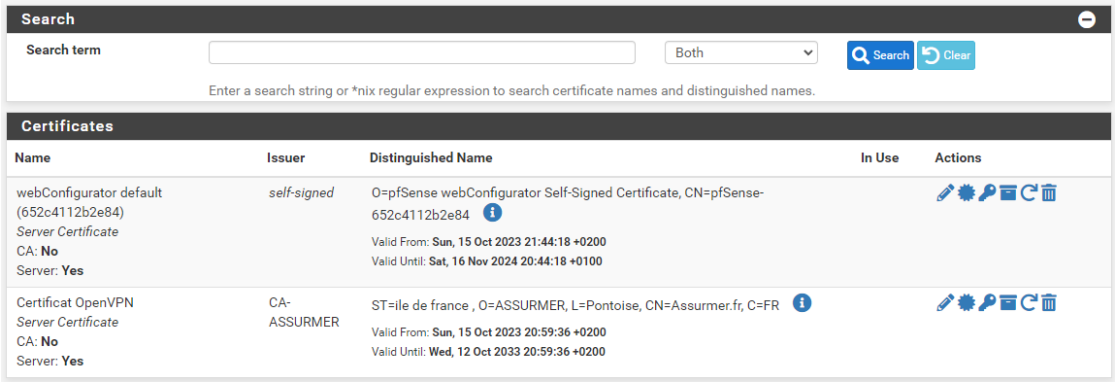
- Descriptive Name : Description de notre certificat
- Internal Certificat : Ici, nous retrouvons les informations de notre autorité de certificat crée précédemment



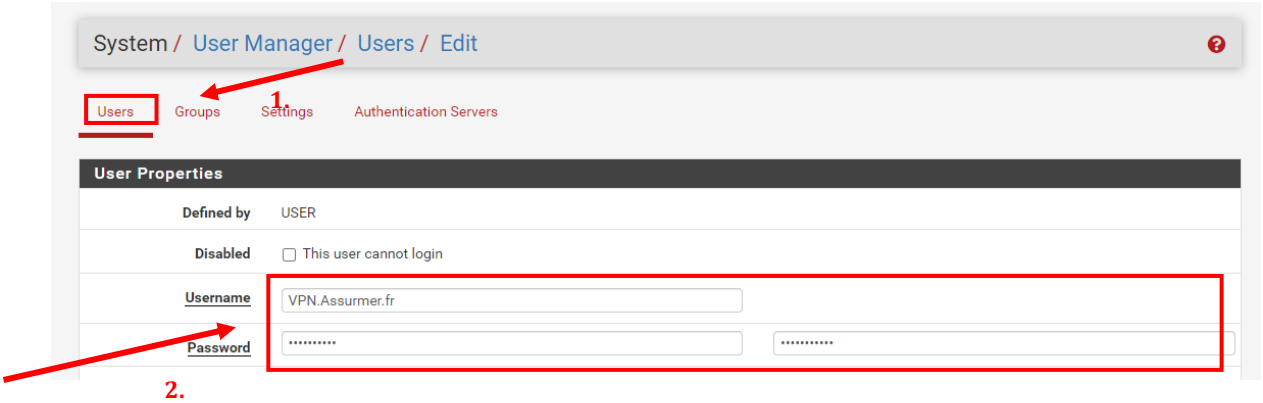
Certificat Type : Nous devons mettre « Server Certificate » car cela est un certificat pour notre serveur qui va permettre d'authentifier le serveur et de déchiffrer les données



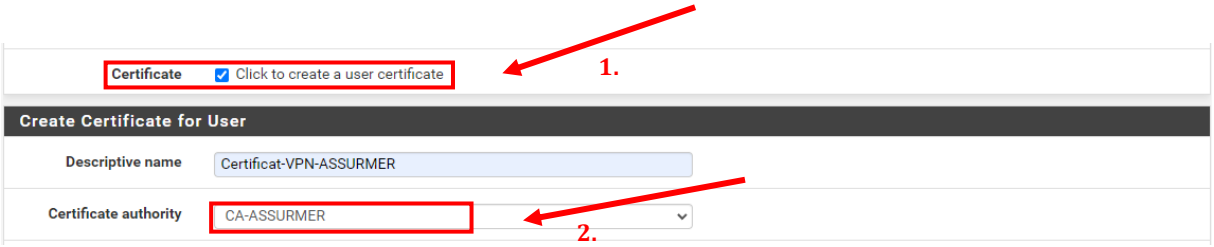
Certificat Crée



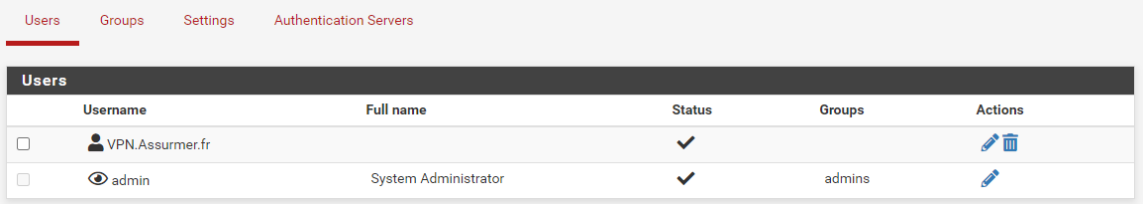
Etape 4 : Ici, on va se rendre sur system < user manager pour crée un utilisateur pour générer un certificat de type utilisateur



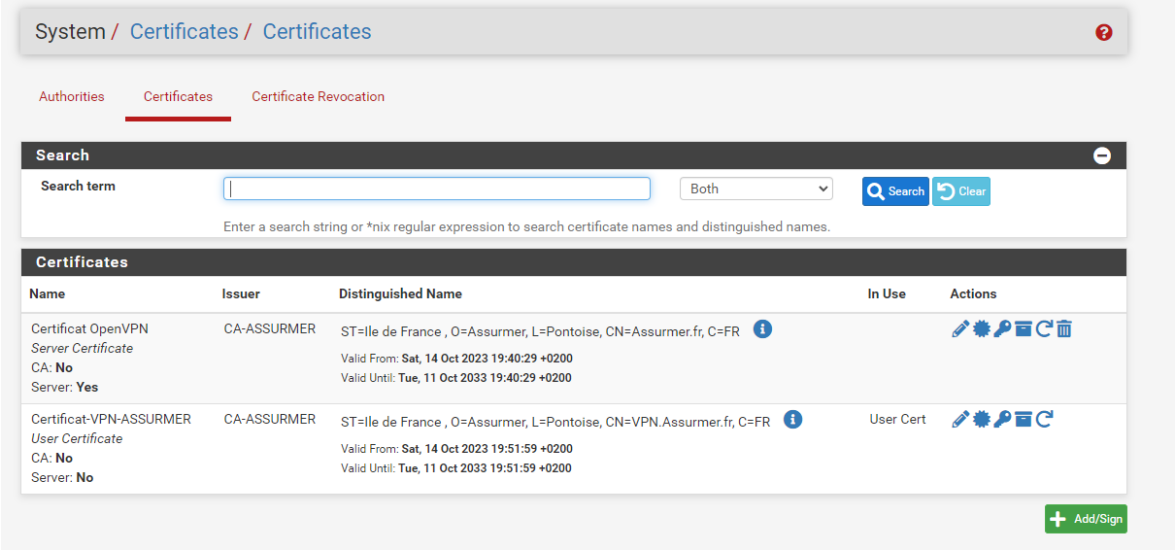
Nous allons penser à cocher la case « Click to create a user certificate » pour que cela générer notre certificat utilisateur qui va permettre de chiffrer les données envoyé par les utilisateurs . On pourra nommer ce certificat



L’utilisateur a bien été crée



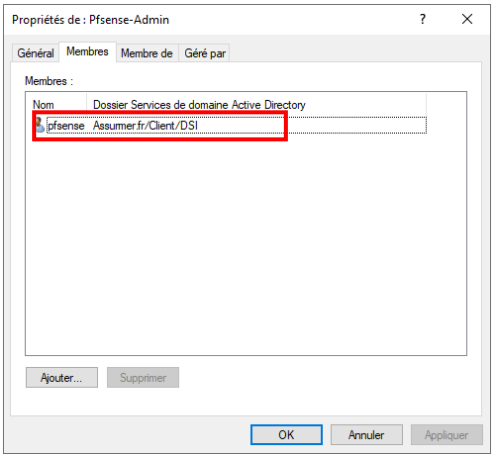
Le certificat utilisateur a bien été générer



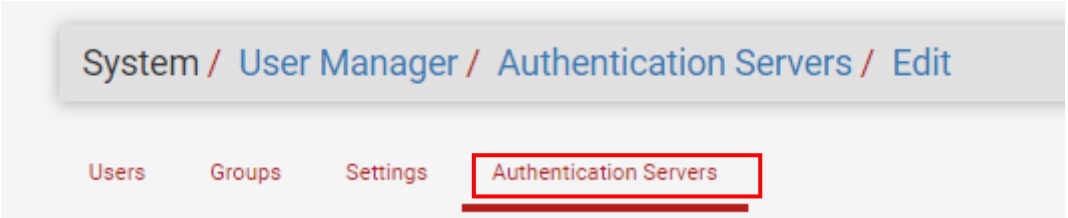
II. Configuration de la liaison LDAP

Etape 1 : On va créer un utilisateur « pfsense » spécialisé pour la liaison LDAP qu'on va ajouter dans un groupe AD crée spécialement pour le LDAP qu'on va appelé « pfsense-admin »

Cela va être essentiel car Pfsense va utiliser cet utilisateur pour lire notre Active directory



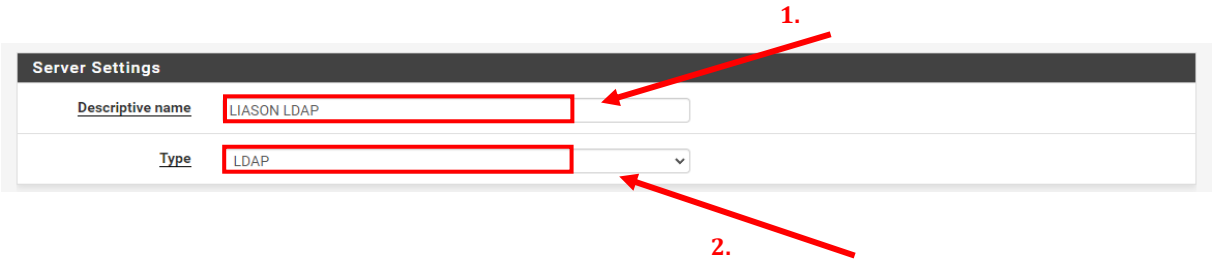
Etape 2 : Sur l'interface Pfsense , on va se rendre sur Authentification Servers pour crée notre liason LDAP



Etape 3 : Remplir les champs correspondants

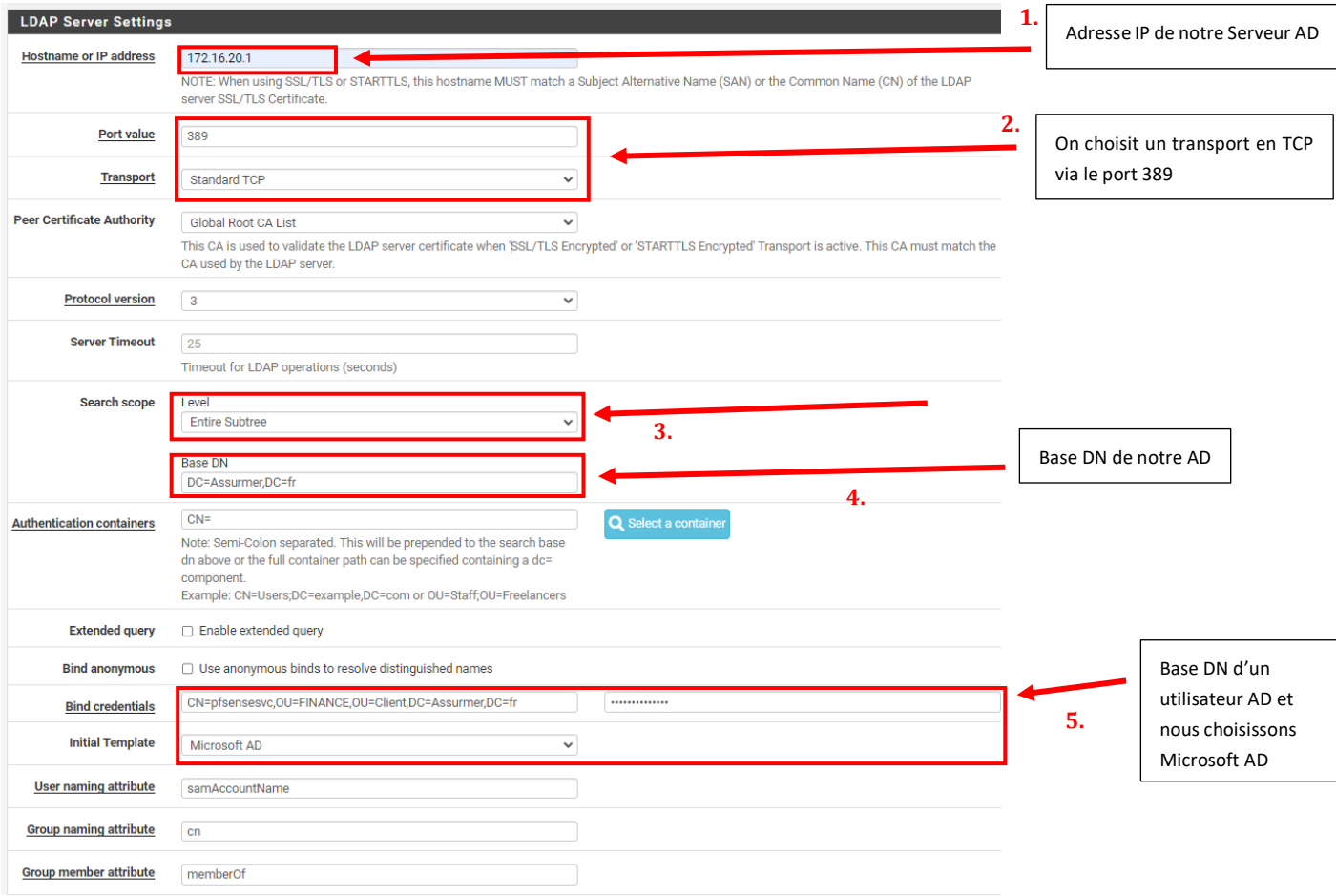
Server Settings :

- **Descriptive Name :** On va nommer nos paramètres
- **Type :** On Sélectionne "LDAP".



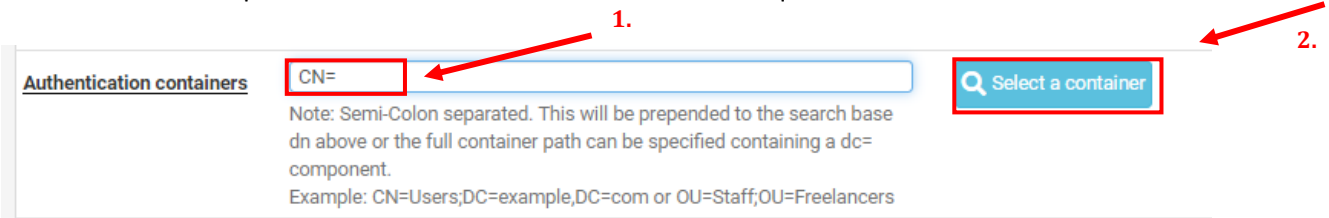
LDAP Server Settings :

- **Bind credentials :** Nous devons ici entrez le nom d'utilisateur (sous forme de DN complet) et le mot de passe du compte AD que nous avons préparé pour la lecture des informations AD.



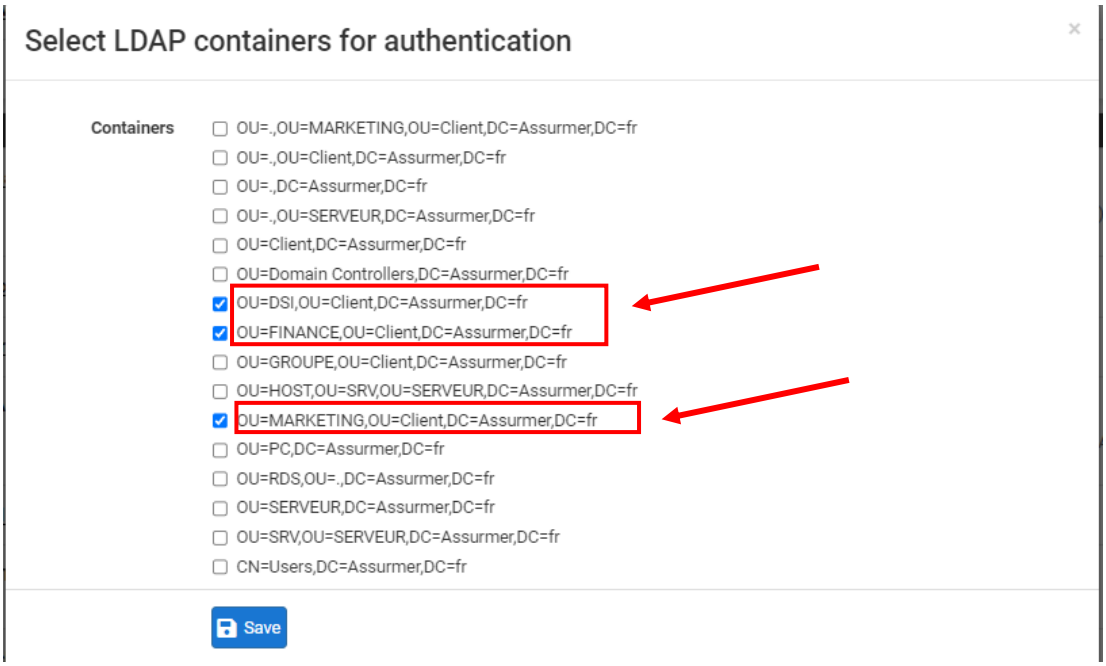
A cette étape nous pouvons remplir le champs « **Authentification containers** » car grâce a notre user « pfsense » , notre serveur pfsense est capable de lire notre annuaire active directory dans son intégralité .

Dans ce champ nous allons écrire seulement « CN= » et cliquer sur « Select a container »



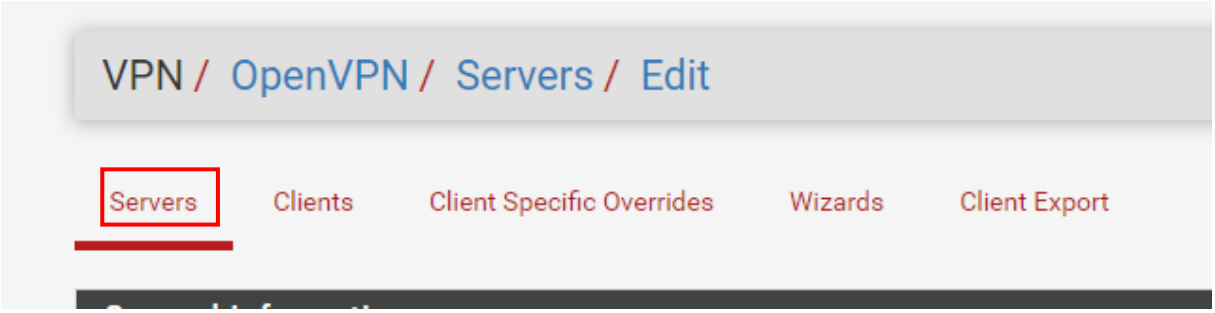
Cette page va s'ouvrir dans lequel on va sélectionner toutes nos OU un par un contenant nos utilisateurs.

Cette page nous affiche toutes notre annuaire active directory grâce au nom DN d'une utilisateur AD



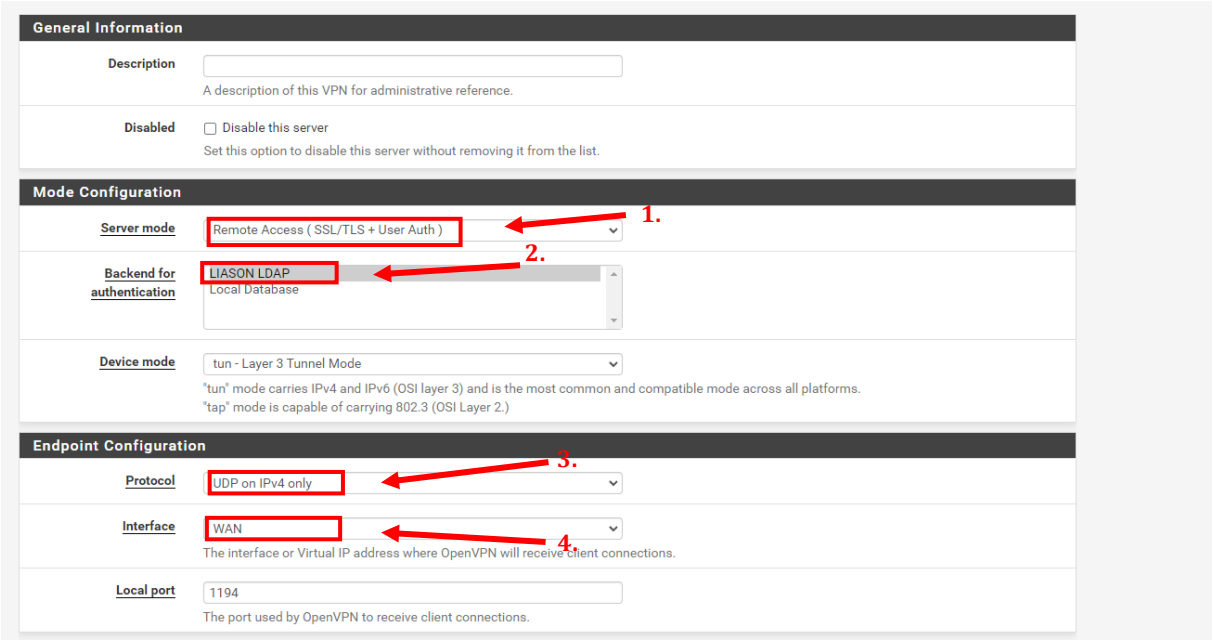
III. Paramétrage du VPN

Etape 1 : Nous allons rendre sur VPN < OpenVPN < Server pour configurer notre VPN



Etape 2 : Remplir les champs correspondants

- **Server mode** : On sélectionne Remote Acess . On va se baser sur notre certificat crée juste avant et sur une authentification par utilisateurs
- **Backend for Authentifcation** : On va sélectionner notre Annuaire LDAP
- **Protocol** : Pour le VPN, le protocole s'appuie sur de l'UDP, avec **le port 1194 par défaut. Nous pouvons le changer mais pour l'instant nous allons rester comme ça**
- **Interface :** Pour l'interface, nous allons conserver "WAN" puisque c'est bien par cette interface que l'on va se connecter en accès distant.



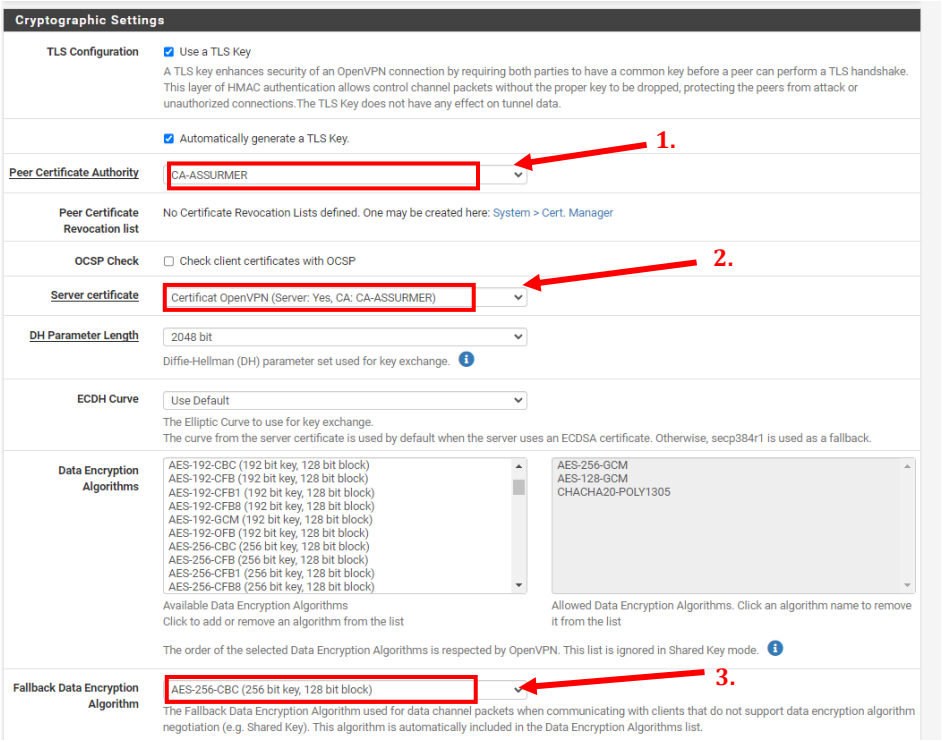
- **Peer Certificate Authority** : On retrouve notre certificat d'autorité

- **Server certificate :** On va sélectionner notre certificat serveur crée précédemment

- **Falback Data Encryption Algorithm :** On va choisir AES-256-CBC (256 bit key , 128 bit block) .

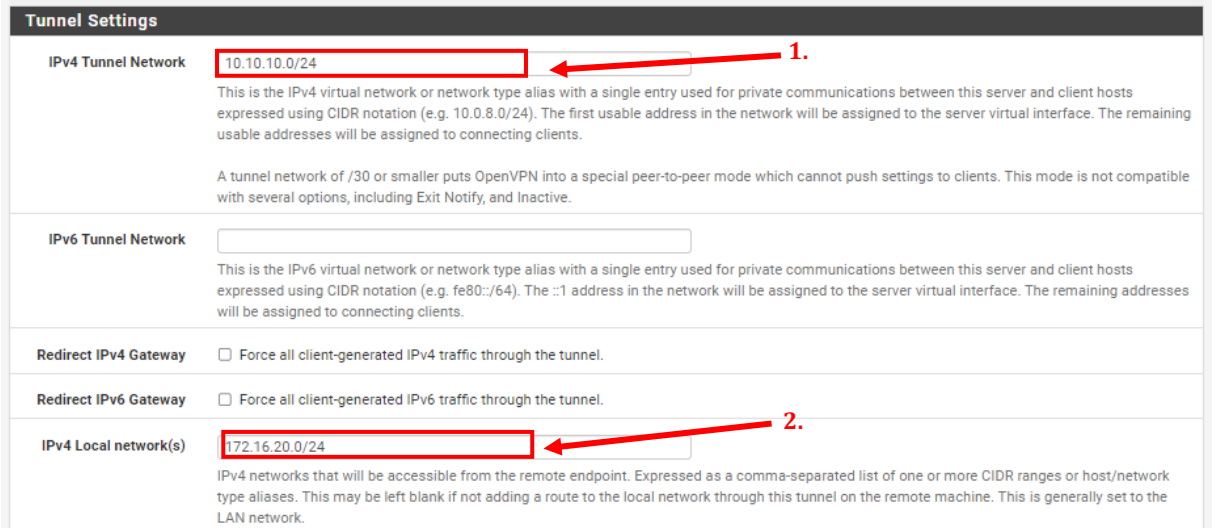
En faisant cela , la sécurité sera renforcée, mais cela impact légèrement les performances, car le processus de chiffrement est alourdi : il sera toujours possible de modifier cette valeur.

Le reste des paramètres on va les laisser par défaut



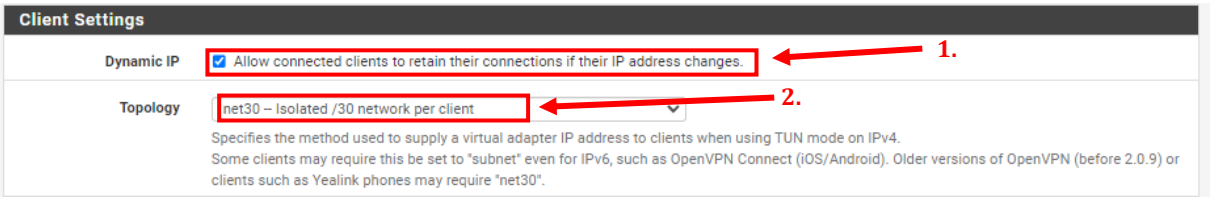
- **IPv4 Tunnel Network :** On va choisir une adresse du réseau VPN, c'est-à-dire que lorsqu'un client va se connecter en VPN il obtiendra une adresse IP dans ce réseau au niveau de la carte réseau locale du PC

- **IPv4 Local network :** On indique notre adresse réseau de notre LAN serveur que nous souhaitons rendre accessible via le tunnel VPN



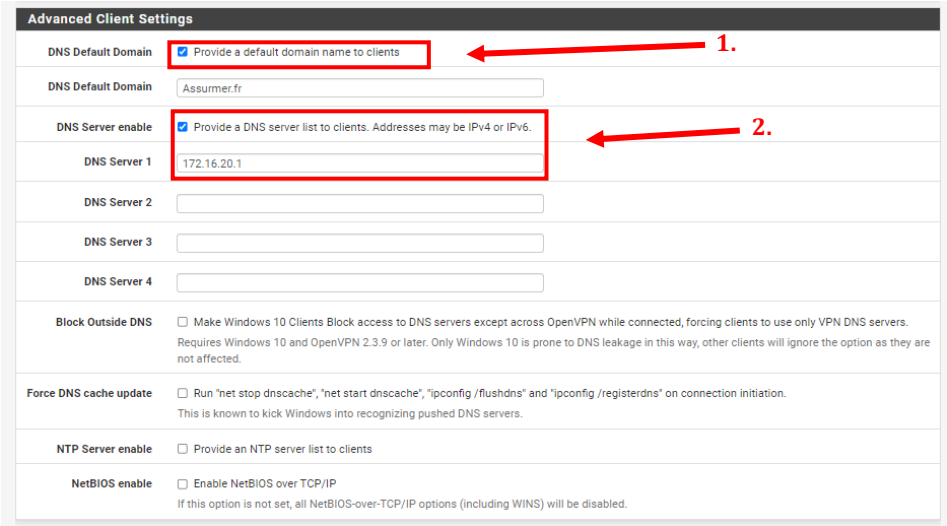
- **Dynamic IP** : On va cocher cette option. Cela peut être utile dans le cas où l'adresse IP publique d'un client change, il pourra maintenir sa connexion VPN.
  C'est surtout utile car nous avons des collaborateurs qui se connectent via une connexion 4G et en mobilité via leurs appareils nomades.

- **Topology :** On va choisir Net30-Isolated /30 network per client pour que chaque client soit isolé dans un sous-réseau (de la plage réseau VPN) afin que les clients ne puissent pas communiquer entre eux pour des réseaux de sécurité



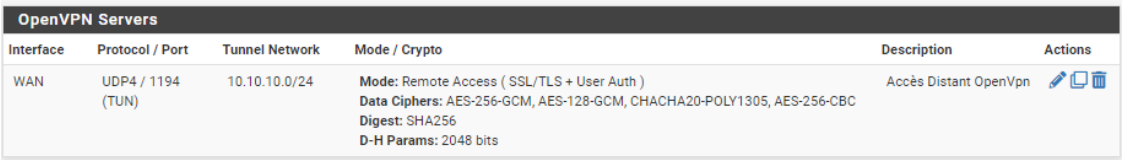
- **DNS default Domain :** On va cocher cette case et mettre le nom de notre domaine

- **DNS Server enable :** On va cocher cette case pour indiquer l'adresse IP de notre serveur DNS



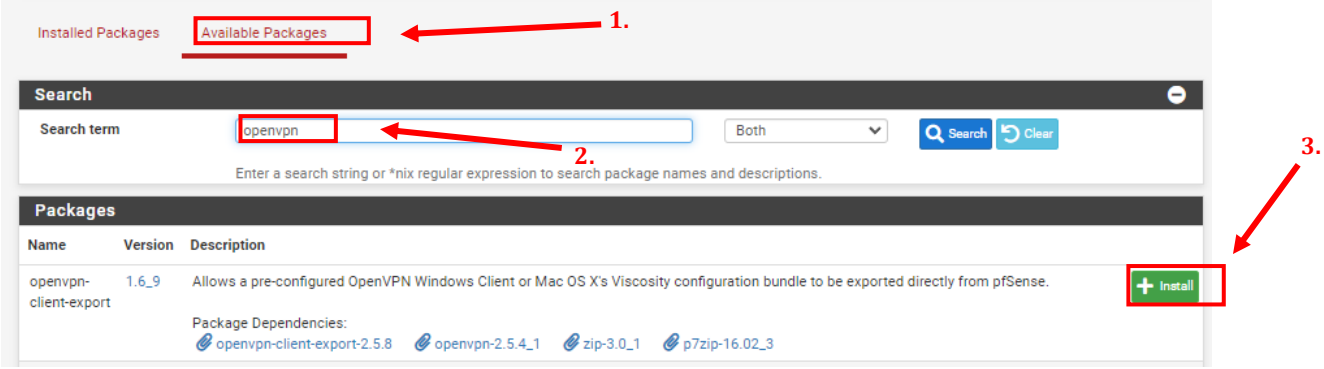
- **Custom Options :** Nous allons rajouter l'option « auth-nocache ». Cette option offre une protection supplémentaire contre le vol des identifiants en refusant la mise en cache.

La configuration serveur d'OpenVPN est terminé



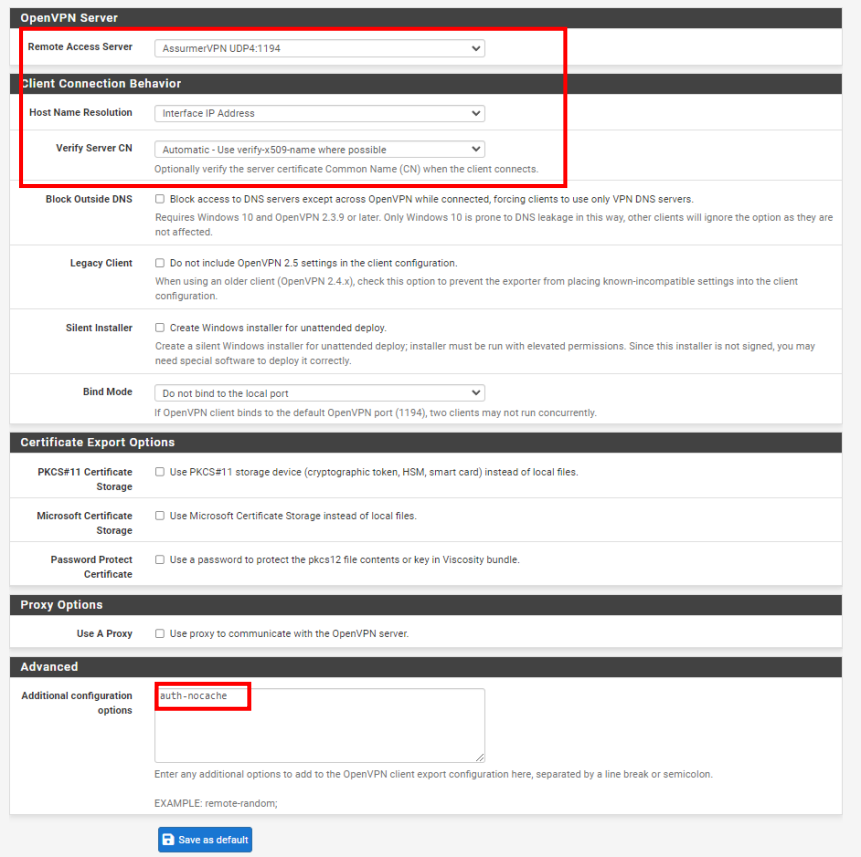
IV. Exportation de nos configuration VPN

Etape 1 : On va aller dans system < package maneger < Available packages pour recherche le package OpenVpn et l'installer

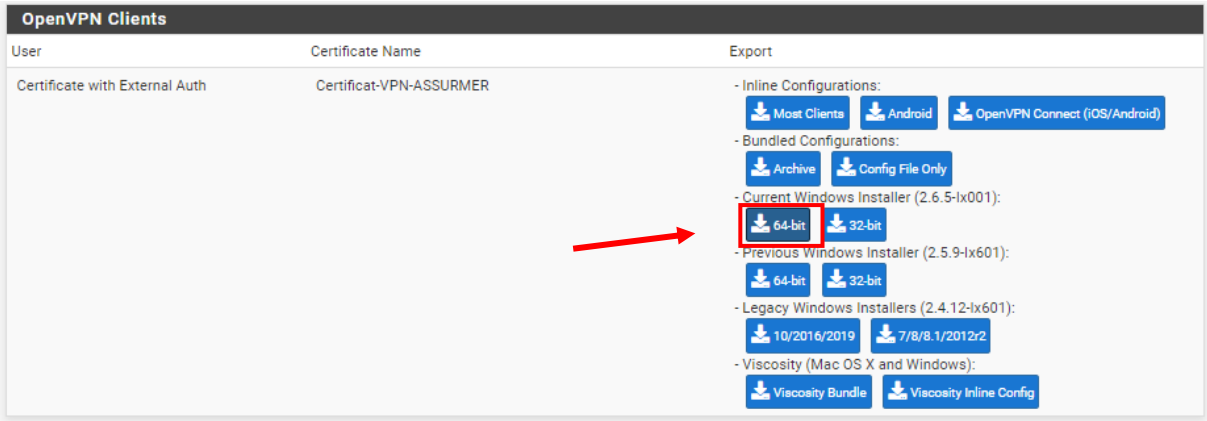


Nous devons installer ce package pour pouvoir exporter les configurations faites précédemment pour les importer sur les machines clientes

Etape 2 : Après cela, nous nous rendons sur VPN < OpenVPN < Client Export . Nous pouvons voir les résultats de nos configurations faites juste avant



Etape 3 : En dessous de la part configuration, on a la possibilité de télécharger la configuration. Pour utiliser OpenVPN il faudra prendre la configuration "Bundled Configuration", au format archive pour récupérer tous les fichiers nécessaires. Il faudra aussi installer OpenVPN client sur nos pc client

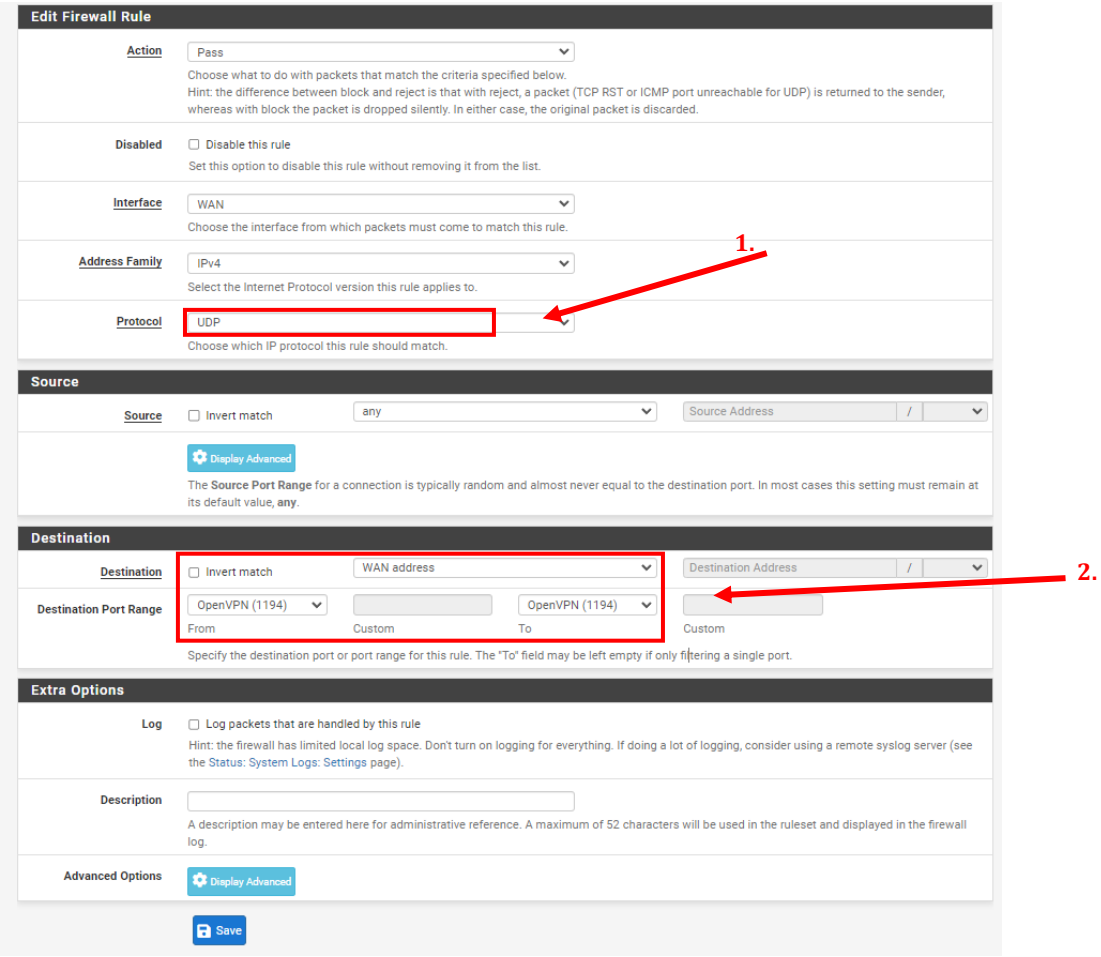

OpenVPN Clients
User
Certificate Name
Export
Certificate with External Auth
Certificat-VPN-ASSURMER
- Inline Configurations:
Most Clients
Android
OpenVPN Connect (iOS/Android)
- Bundled Configurations:
Archive
Config File Only
- Current Windows Installer (2.6.5-Ix001):
64-bit
32-bit
- Previous Windows Installer (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

V. Configuration des règles de pare-feu

Etape 1 : On va se rendre sur Firewall > Rules pour crée une règle au niveau du WAN de notre pfsense. Il est nécessaire de créer une nouvelle règle pour l'interface WAN, en sélectionnant le protocole UDP.

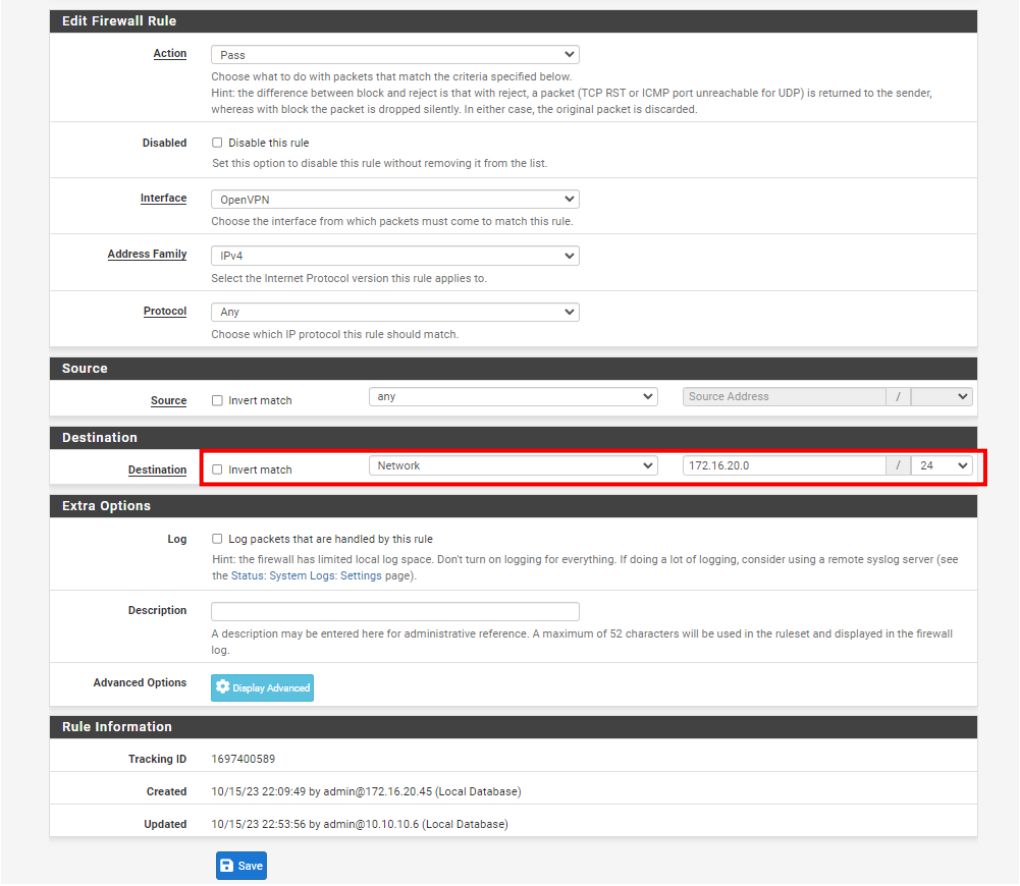
On crée une règle pour autoriser les connection avec le VPN. On va remplir les champs correspondants :

- Action : Pass
- Interface : WAN
- Protocol : UDP
- Source : On laisse en Any pour les réseaux externes
- Destination : On met WAN adresse et on indique le port de notre VPN choisit précédemment



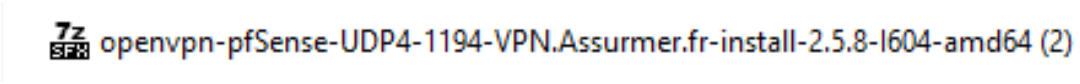
- Etape 2 : On va créer une autre règle pour autoriser les flux vers les ressources.

On va se rendre dans l'interface OpenVpn est créé une nouvelle règle. Nous devons créer une ou plusieurs règles en fonction des ressources auxquelles vos utilisateurs doivent accéder via le VPN, en limitant les flux au maximum mais ici nous allons autoriser le flux de tout le LAN serveur pour l'instant



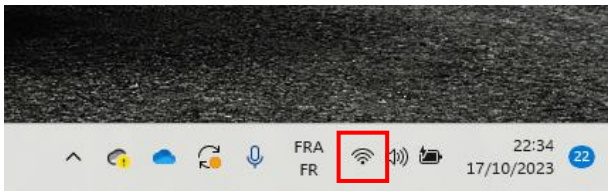
A. Importation des configurations sur le poste client

Etape 1 : Sur le pc client, on récupère le client OpenVPN proposé directement dans pfsense

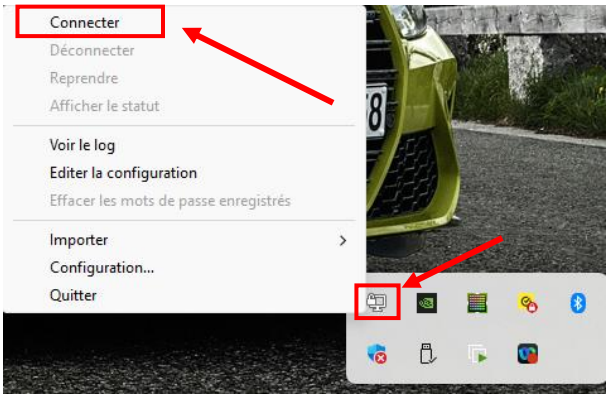


VI. TEST

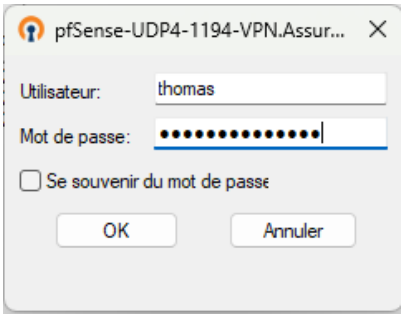
Nous sommes bien connectés à un Wifi domestique pour effectuer ce test



On va tester une connexion en faisant un clic droit sur l'icône VPN et cliquer sur « Connecter »



On se connecte avec un utilisateur du domaine

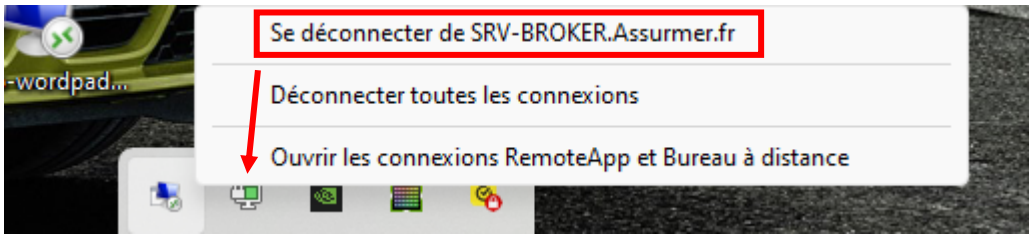


Une fois connecter on récupère bien la configuration réseau du tunnel VPN

```
Carte inconnue OpenVPN TAP-Windows6 :

   Suffixe DNS propre à la connexion. . . : Assurmer.fr
   Adresse IPv6 de liaison locale. . . . .: fe80::a15:44d:9541:3755%61
   Adresse IPv4. . . . . . . . . . . . . .: 10.10.10.6
   Masque de sous-réseau. . . . . . . . . : 255.255.255.252
   Passerelle par défaut. . . . . . . . . :
```

Nous pouvons voir que nous avons réussie à se connecter à nos serveur RDS depuis un réseau externe en utilisant le VPN d'entreprise



Résultat : La connexion externe a fonctionné avec une liaison LDAP actif