Berry Pierre
Option SISR
Session 2025

12/02/2025

Document Technique GSB

Mise en place d'un service VPN avec OpenVPN

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

ANNEXE 7-1-A : Fiche descriptive de réalisation professionnelle (recto)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : 1**
Nom, prénom : Berry Pierre	**N° candidat :** 01950955985
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date :** 12/02/2025

Organisation support de la réalisation professionnelle : La société GSB m'a chargé d'installer et de configurer un service de VPN disponible pour les administrateurs du réseau afin de permettre un accès sécurisé au réseau GSB en étant en dehors du site. Le serveur OpenVPN est déployé sur un des pfSense du réseau.

Intitulé de la réalisation professionnelle : Configuration d'un Serveur OpenVPN tournant sur le pfSense de notre réseau, tout en gérant l'accès aux VPN avec les certificats utilisateurs.

Période de réalisation : 2e Année **Lieu :** Sciences-U Lyon

Modalité : ☒ **Seul(e)** ☐ **En équipe**

Compétences travaillées

- ☒ Installation d'un Pare-Feu pfSense
- ☒ Gestion des Certificats utilisateurs sur pfSense
- ☒ Créer un VPN « client to site » sécurisé

Conditions de réalisation[1] (ressources fournies, résultats attendus)

Ressource : Pare-Feu pfSense

Résultat attendu : Pouvoir se connecter à l'intégralité du réseau GSB en étant à distances, via un tunnel sécurisé.

Description des ressources documentaires, matérielles et logicielles utilisées[2]

- 1 pfSense qui héberge OpenVPN
- 1 machine client test

Modalités d'accès aux productions[3] et à leur documentation[4]

Connexion au pfSense via l'ip 192.168.100.2 -> Identifiant : admin / mdp : grp3@2024

[I] En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

[I] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

[1] Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[1] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

Table des matières :

Description de l'entreprise 4
Schéma de l'infrastructure réseau de l'entreprise 4
Problématique 5
Solution proposée 5
Mise en place du VPN 6-13
Conclusion 14

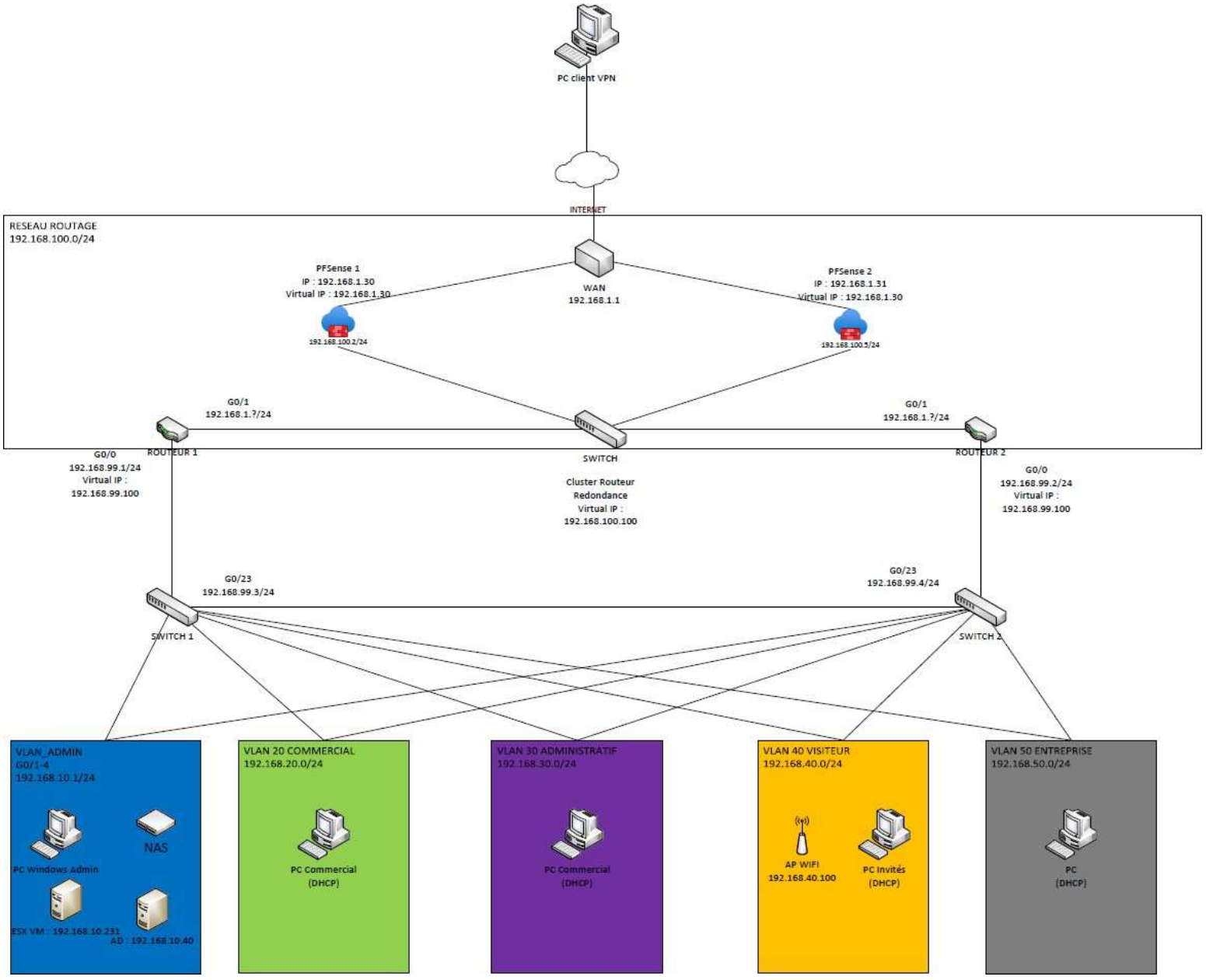
Description de l'Entreprise :

Galaxy Swiss Bourdin :

Le laboratoire Galaxy Swiss Bourdin est issu de la fusion entre le géant américain Galaxy (spécialisé dans le secteur des maladies virales dont le SIDA et les hépatites) et le conglomérat européen Swiss Bourdin (travaillant sur des médicaments plus conventionnels), lui-même déjà union de trois petits laboratoires.

En 2009, les deux géants pharmaceutiques unissent leurs forces pour créer un leader de ce secteur industriel. L'entité Galaxy Swiss Bourdin Europe a établi son siège administratif à Paris.

Schéma de l'infrastructure réseau de l'entreprise :



Problématique :

Comment permettre aux utilisateurs avec privilèges d'accéder aux ressources du VLAN Administrateurs sur le réseau GSB avec un accès distant et sécurisé ?

Solution Retenue :

La mise en place d’un VPN (client to site) sécurisé permet de chiffrer les connexions à distance pour protéger les données sensibles. Ce VPN garantit l’accès sécurisé aux réseaux du projet de façon crypté. Pour se connecter au VPN, l’utilisateur aura besoin de s’authentifier, pour voir s’il a bien un certificat utilisateur, permettant l’accès au réseau aux personnes à qui auxquelles on souhaite donner accès au réseau.

Mise en Oeuvre :

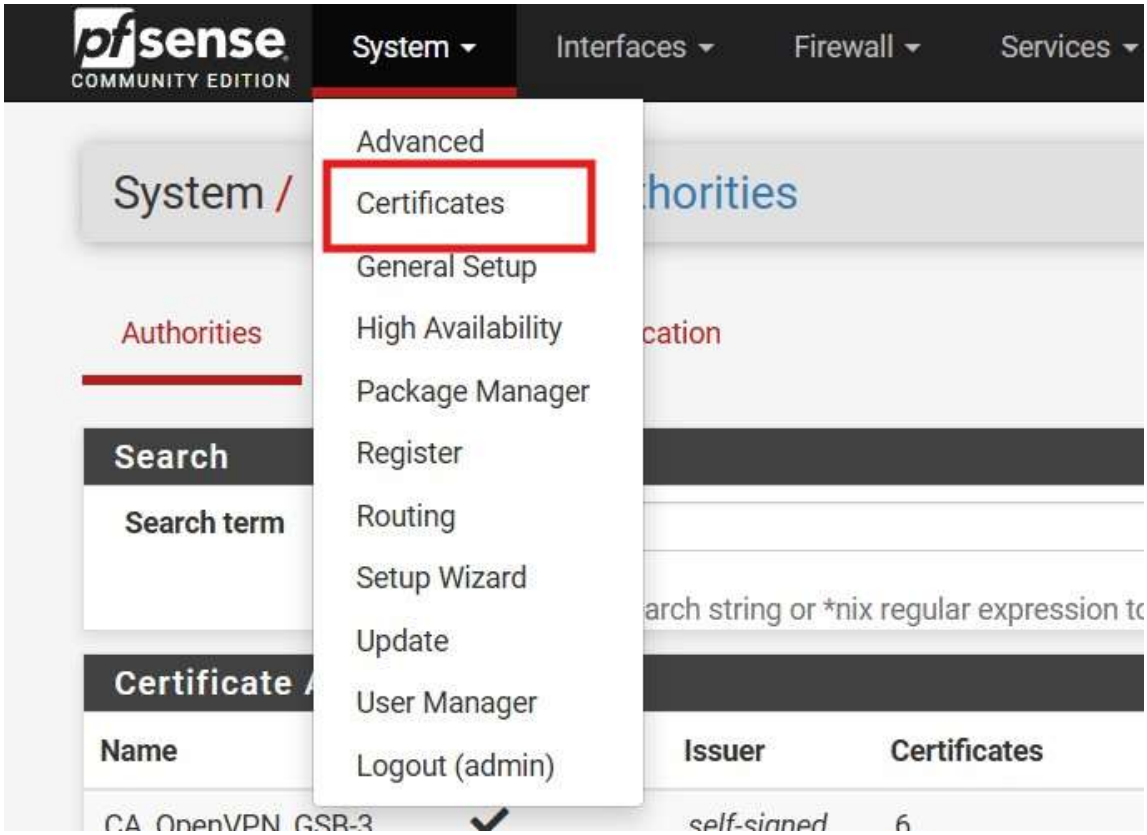
La mise en place d’un service VPN sur pfSense se déroule en trois étapes :

1- Création du Certificat d’Autorité
2- La mise en place du Serveur OpenVPN
3- Création et exportation des utilisateurs

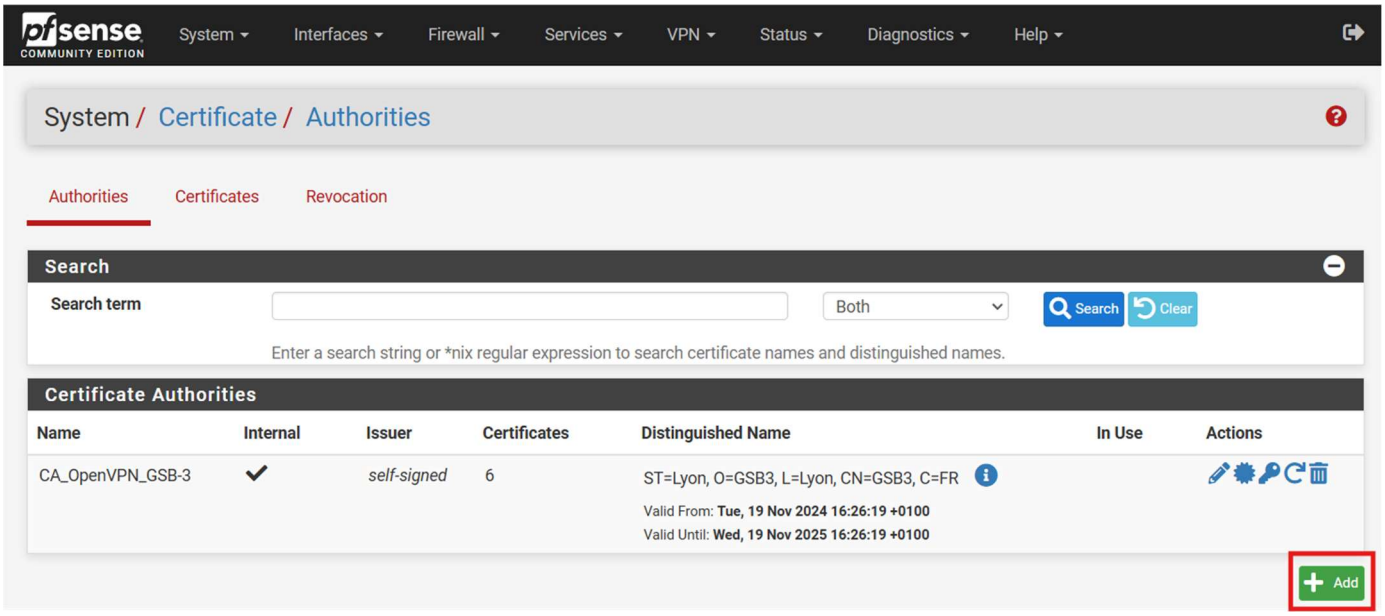
Procédure de mise en place du Service

I - Création du Certificat d'Autorité

Pour créer l'autorité de certification sur PfSense (si vous n'en possédez déjà pas une), vous devez accéder au menu : **System > Certificates**

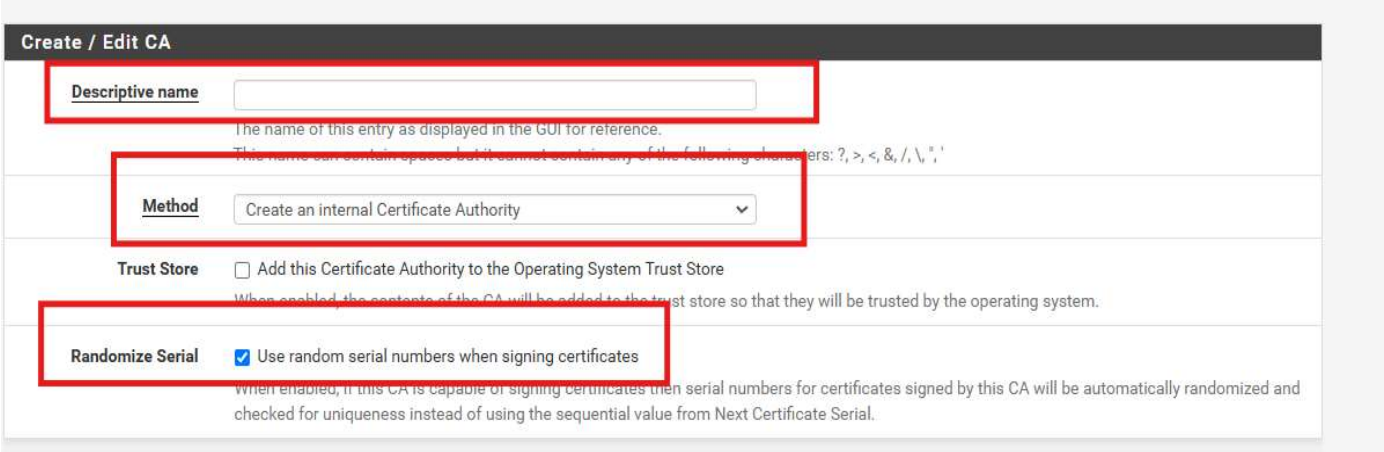


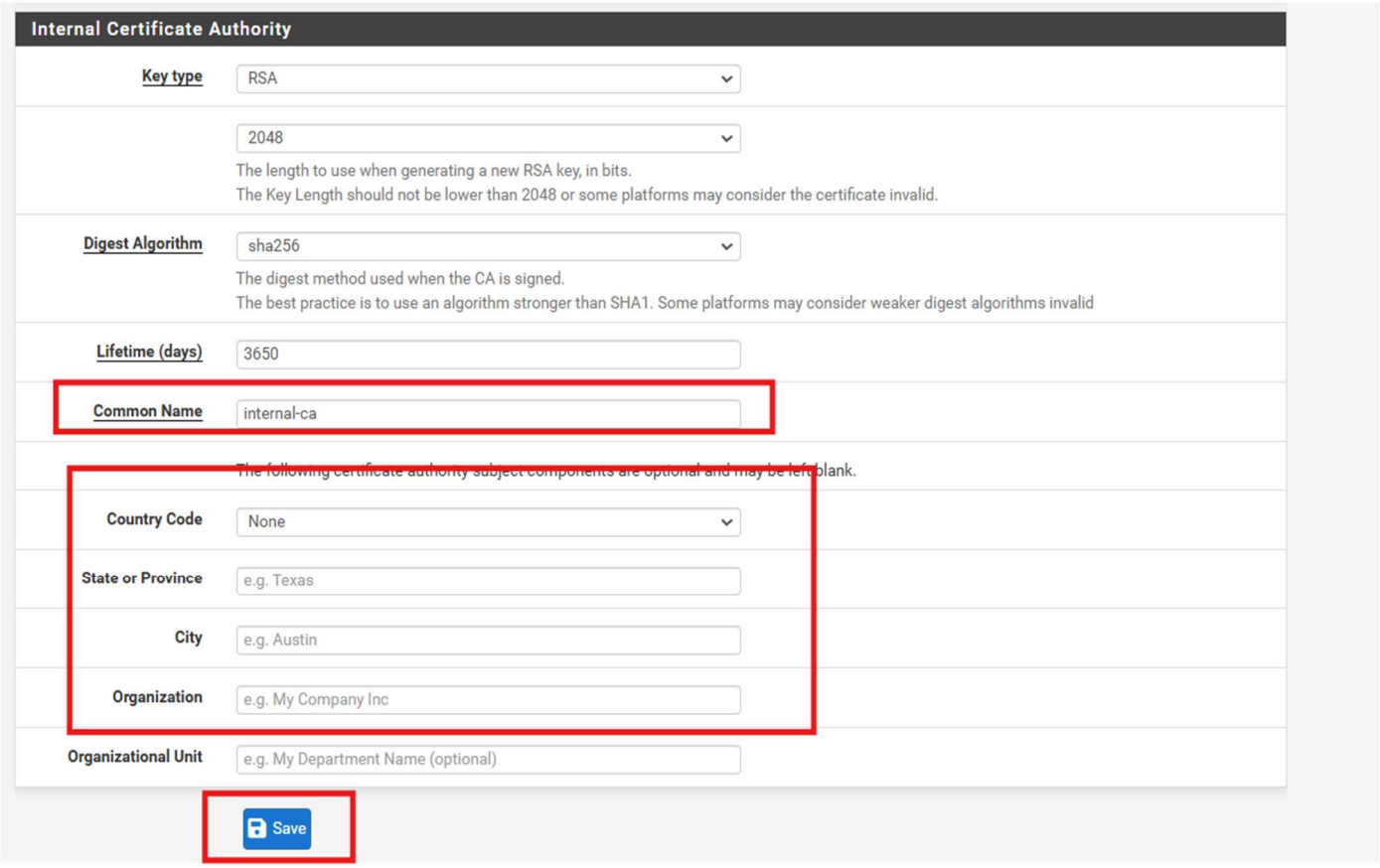
Dans l'onglet "**Authorities**", cliquez sur le bouton "**Add**".



Donnez un Nom à l'autorité de certification.

- Choisissez-la **Method : "Create an internal Certficate Authority"**
- Cochez Randomize Serial.
- Créez le "**Common Name**" de votre choix.
- Et remplissez les coordonnées de localisation pour le certificat. (Optionnel)
- Laissez les autres paramètres par défaut.
- Save

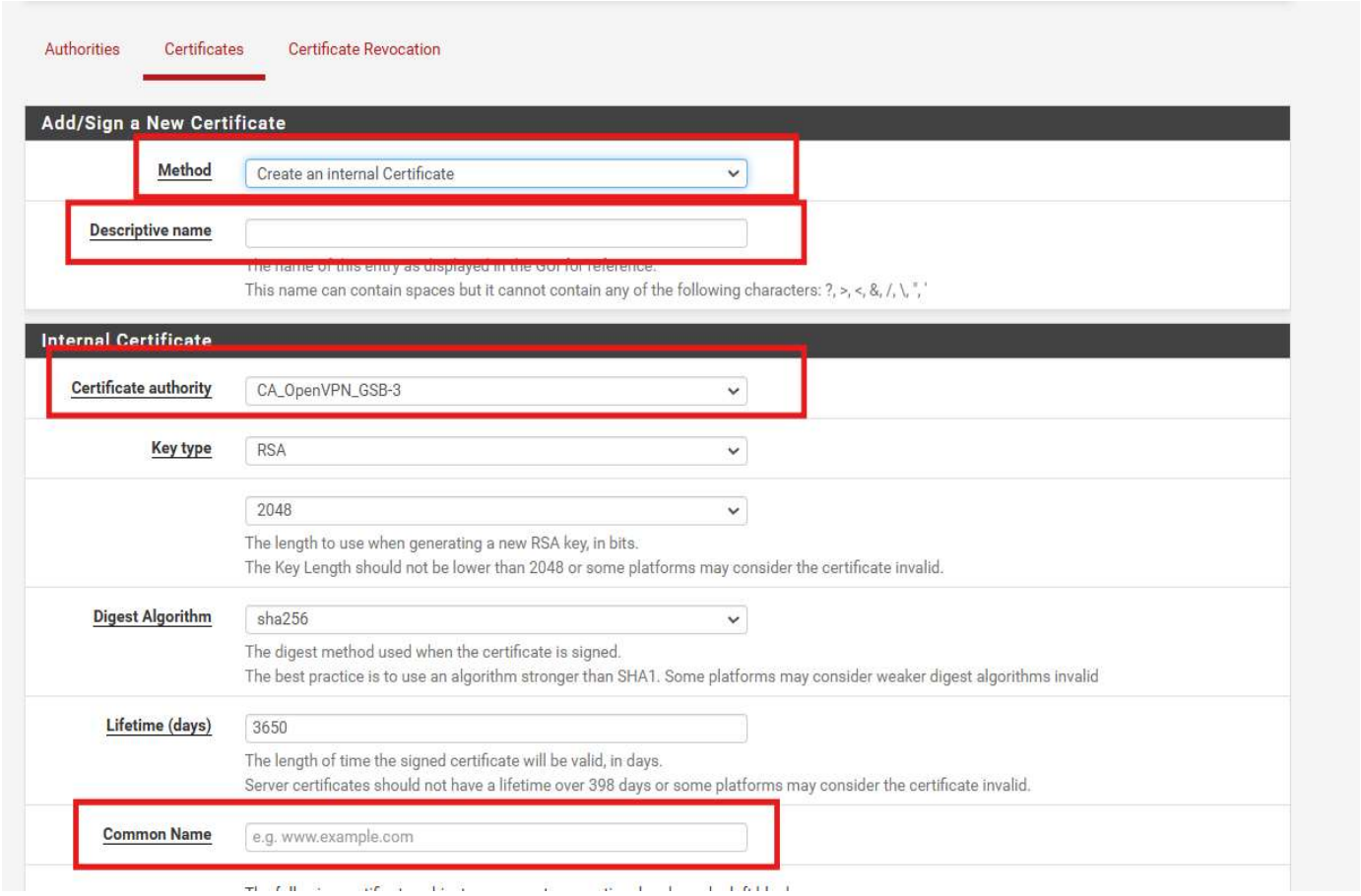


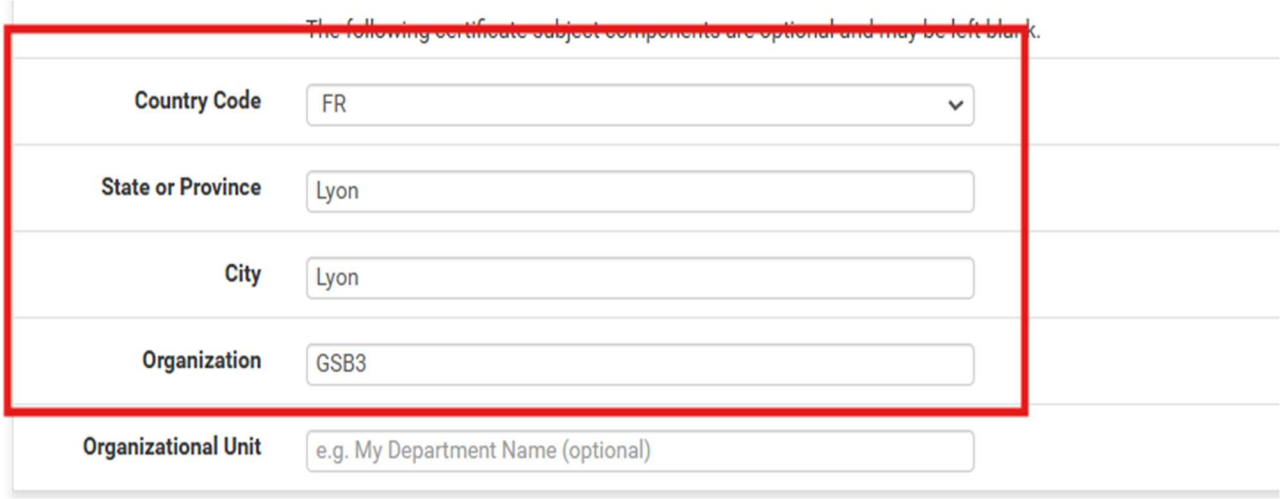


II - Mise en place du serveur OpenVPN

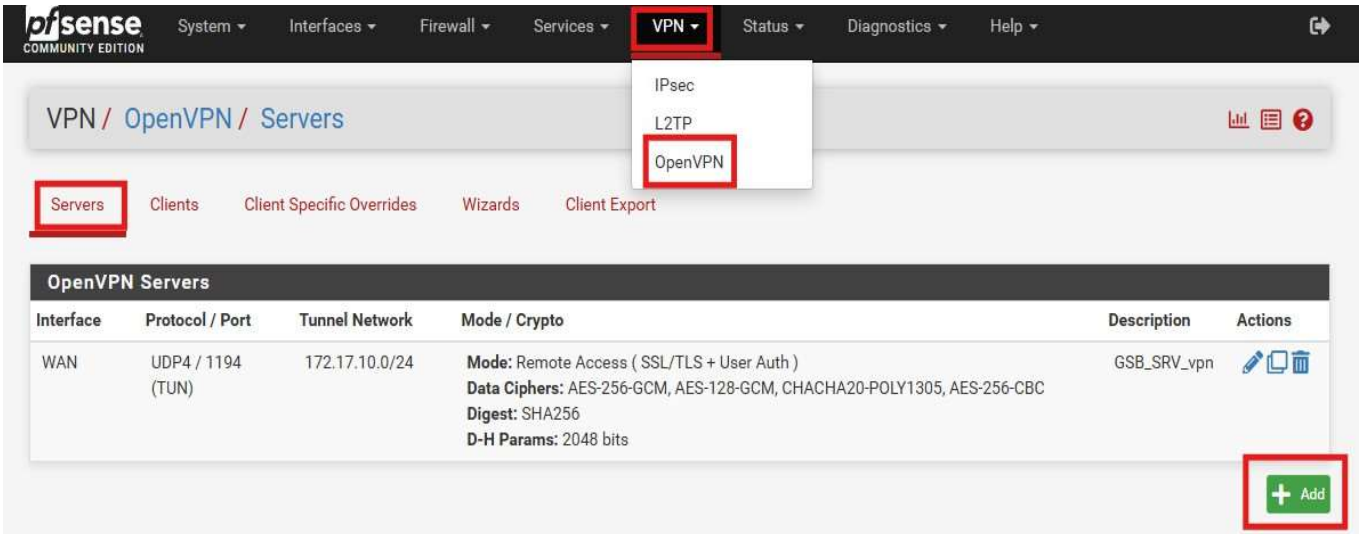
Nous devons maintenant créer un certificat "Server" en utilisant notre Autorité de certification. Il faut donc aller dans : **System > Certificates** et cette fois-ci dans l'onglet "Certificates", cliquez sur le bouton "Add/Sign" et remplissez les champs suivants :

- Choisissez-la **Method : "Create an internal Certificate Authority"**
- Donnez un Nom au Certificat du Serveur VPN dans : **Descriptive name**
- Vérifiez dans **Certificate authority**, que notre Certificat d'Autorité est bien sélectionné.
- Choisissez le "**Common Name**" de votre choix.
- Remplissez les coordonnées de localisation pour le certificat (optionnel)
- Laissez les autres paramètres par défaut comme pour le CA.
- Save

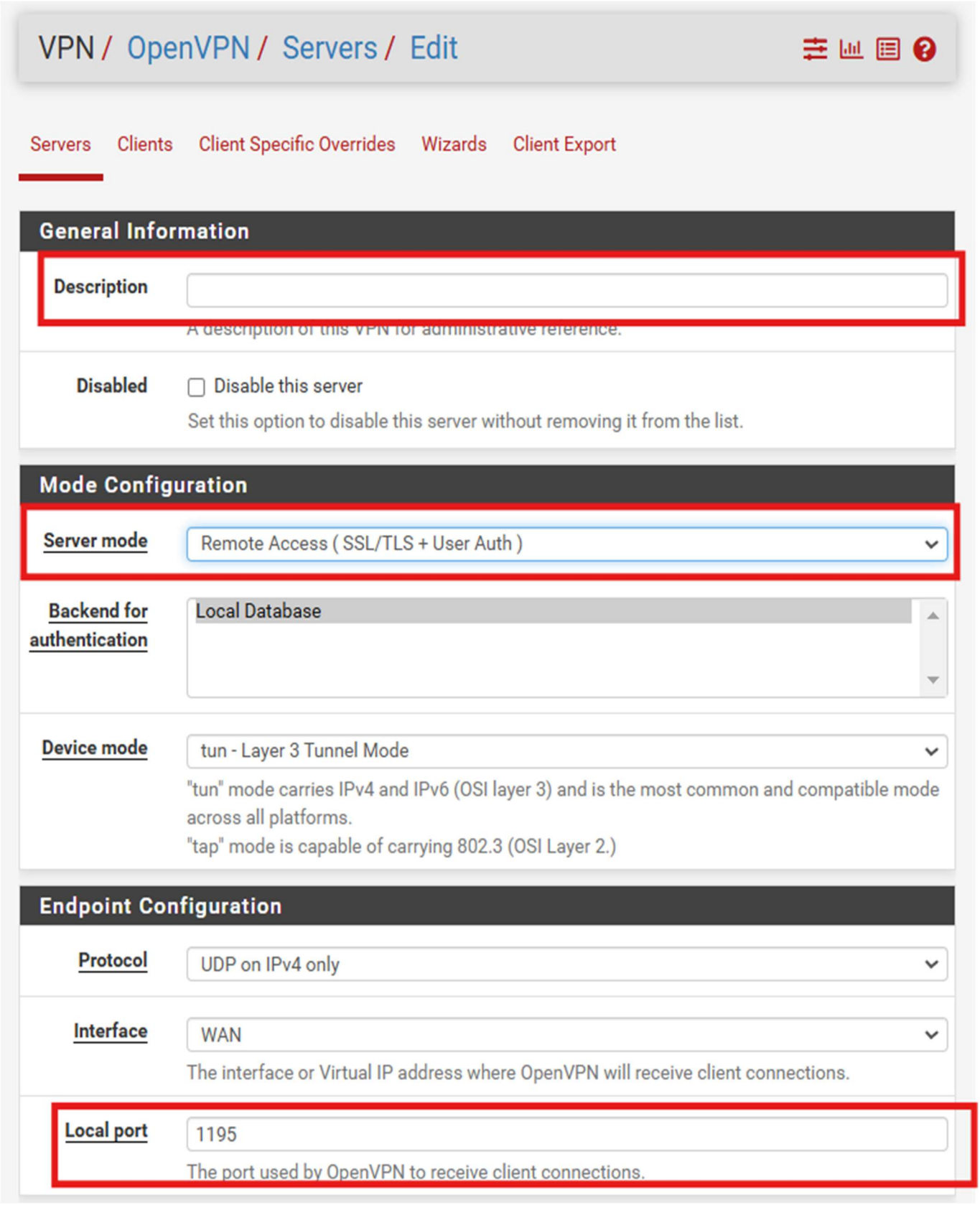




Ensuite nous pouvons aller configurer le serveur VPN en allant dans : **VPN > OpenVPN** et dans l'onglet **Serveur**, cliquer sur "**Add**".

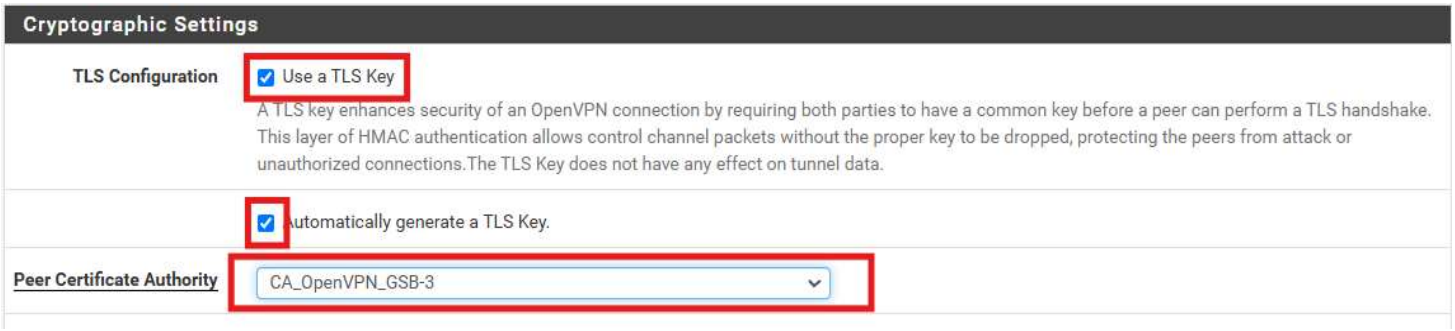


- Donnez un Nom au Serveur VPN dans : **Description**
- Sélectionnez dans "**Server mode**": **Remote Access (SSL/TLS+User Auth)**
- Choisissez le "**Common Name**" de votre choix.
- Renseignez le Port ou passera le VPN, (port par défaut OpenVPN : 1194) vous pouvez personnaliser le port que vous voulez utiliser.

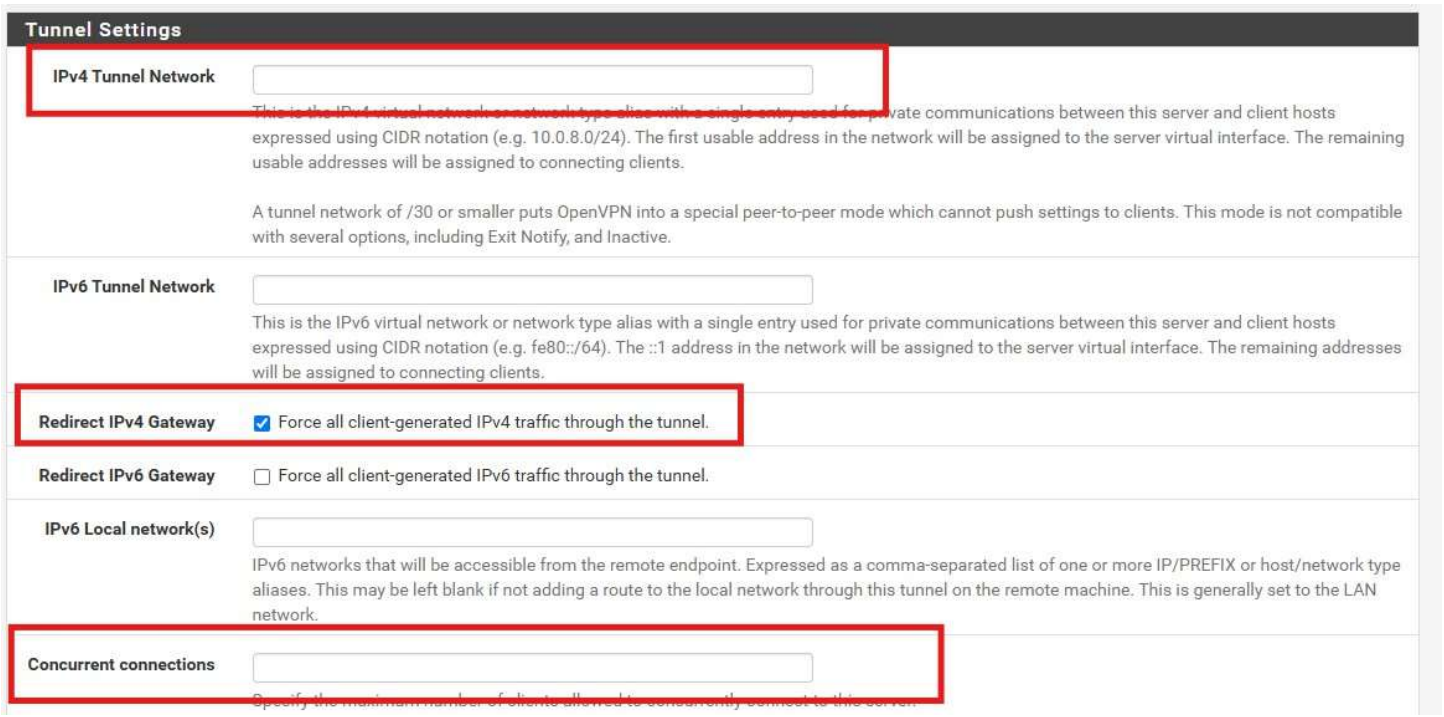


- Vérifiez que les cases **Use a TLS Key et / automatically generate a TLS Key** est bien coché.

- Dans "**Peer Certificate Authority**" sélectionnez le **Certificat d'Autorité** que nous avons créé.



- Dans "**IPv4 Tunnel Network**" renseignez l'adresse réseau avec son IDR que vous voulez donner à votre réseau VPN. ATTENTION : L'adresse réseau ne doit pas correspondre à celles déjà présentes dans votre réseau.
- Cochez "**Redirect IPv4 Gateway**"
- Dans "Concurrent connections" définissez le nombre de clients qui pourront se connecter simultanément.

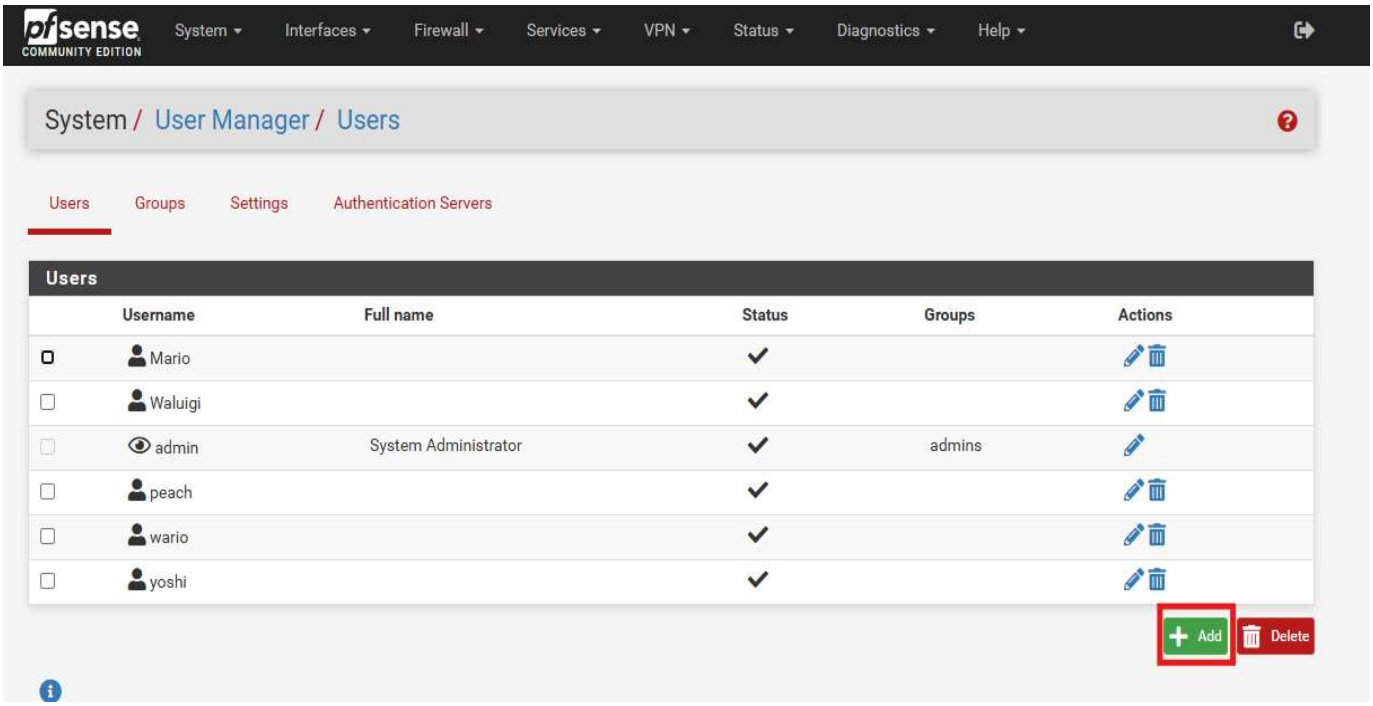


- Cochez "**Dynamic IP**"
- Dans "**Topology**" sélectionnez : **net30 - Isolated /30 network per client**

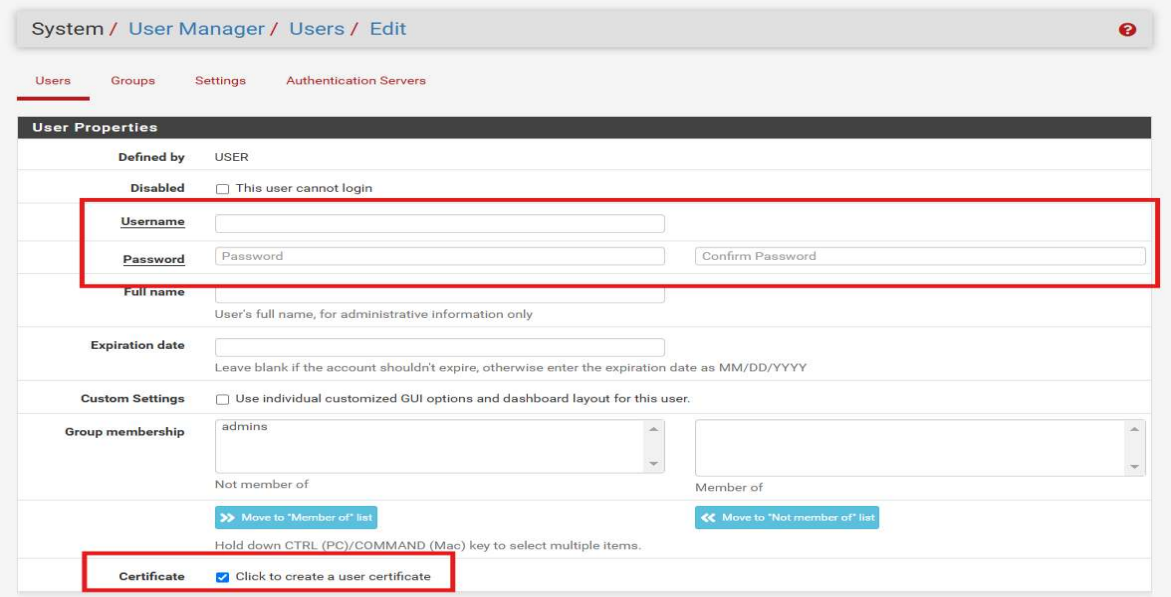
- Si vous en avez un DNS, vous pouvez remplir les paramètres DNS.
- Save

III - Création et exportations des Utilisateurs

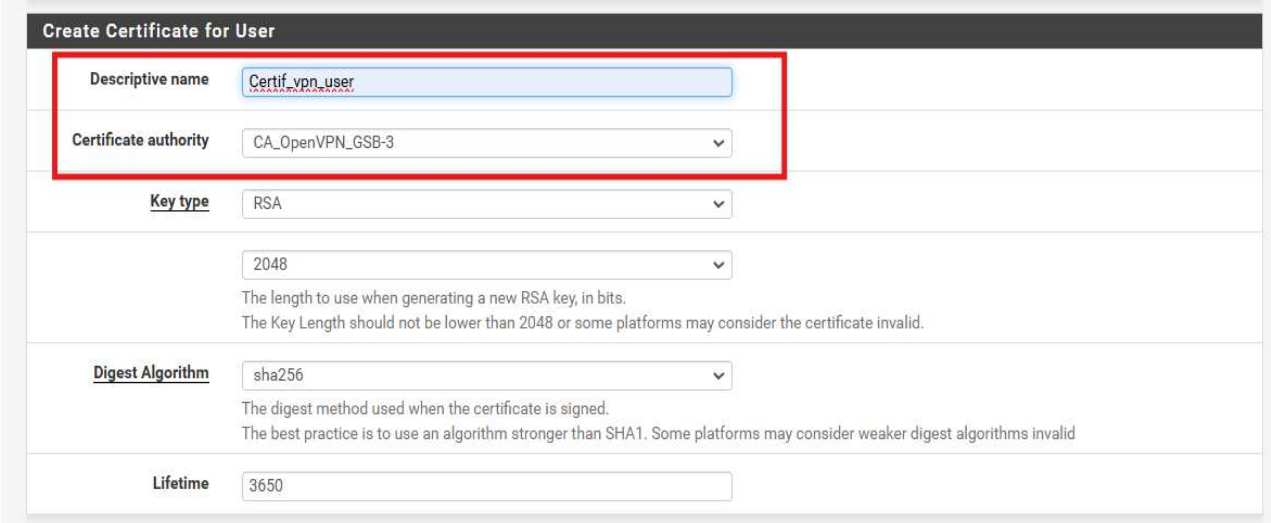
Nous devons maintenant créer les certificats de nos utilisateurs. Il faut donc aller dans : **System > User Manager** et dans l'onglet "Users", cliquez sur le bouton "Add".



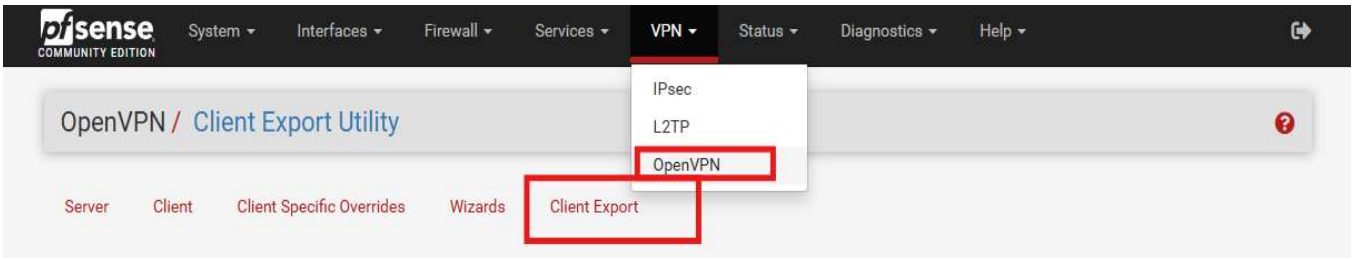
- Remplissez les champs “**Username**” et “**Password**”
- Cochez “**Certificate**” pour créer un certificat.

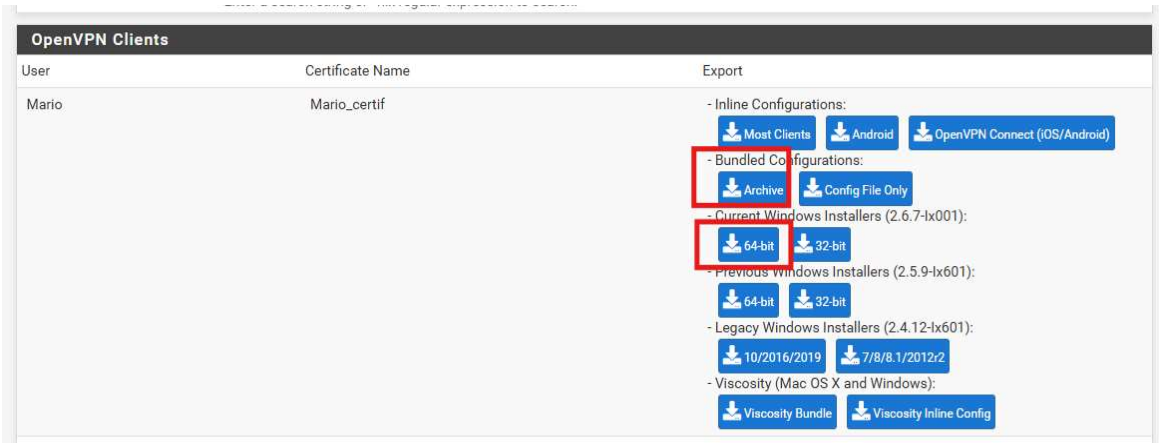


- Donnez un nom à votre certificat dans “**Descriptive Name**”
- Vérifiez que le CA est bien sélectionné dans “**Certificate authority**”
- Vous pouvez sauvegarder



Ensuite nous pouvons aller exporter le Profil utilisateur en allant dans :
VPN > OpenVPN > Client Export “Add”





Allez tout en bas de la page et sélectionner pour l’utilisateur le **fichier d’installation** et le **dossier archive** avec la configuration à exporter sur le pc client.

Vous pouvez maintenant procéder à l’installation du VPN sur le PC client de l’utilisateur.

Fin de la Procédure

Conclusion :

Grâce à sa robustesse, sa capacité à chiffrer les communications et sa flexibilité de configuration, OpenVPN s'impose comme une solution VPN fiable et sécurisée. Bien qu'il puisse sembler complexe au premier abord en raison de certaines configurations spécifiques (comme la création de certificats, l'authentification SSL/TLS ou la gestion des clients), il demeure en réalité accessible et adaptable.

Il convient aussi bien aux petites infrastructures qu'aux grands réseaux d'entreprise, notamment grâce à la possibilité de créer des accès sécurisés pour des utilisateurs distants ou de déployer des connexions site-à-site.

Les paramètres de sécurité, les règles d'authentification et les options de chiffrement sont entièrement personnalisables. De plus, la communauté OpenVPN est particulièrement active, offrant une documentation complète et de nombreux guides pour faciliter la mise en place et l'optimisation de la solution.