

12/02/2025

Document Technique GSB

Mise en place d'un service VPN avec
OpenVPN



DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE		N° réalisation : 1
Nom, prénom : Berry Pierre		N° candidat : 01950955985
Épreuve ponctuelle <input checked="" type="checkbox"/>	Contrôle en cours de formation <input type="checkbox"/>	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 : 2 ^e Année Lieu : Sciences-U Lyon		
Modalité : <input checked="" type="checkbox"/> Seul(e) <input type="checkbox"/> En équipe		
Compétences travaillées		
<input checked="" type="checkbox"/> Installation d'un Pare-Feu pfSense		
<input checked="" type="checkbox"/> Gestion des Certificats utilisateurs sur pfSense		
<input checked="" type="checkbox"/> Créer un VPN « client to site » sécurisé		
Conditions de réalisation¹ (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 utilisées²		
- 1 pfSense qui héberge OpenVPN		
- 1 machine client test		
Modalités d'accès aux productions³ et à leur documentation⁴		
Connexion au pfSense via l'ip 192.168.100.2 -> Identifiant : admin / mdp : grp3@2024		

¹ 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.

² Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

³ 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.

⁴ 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

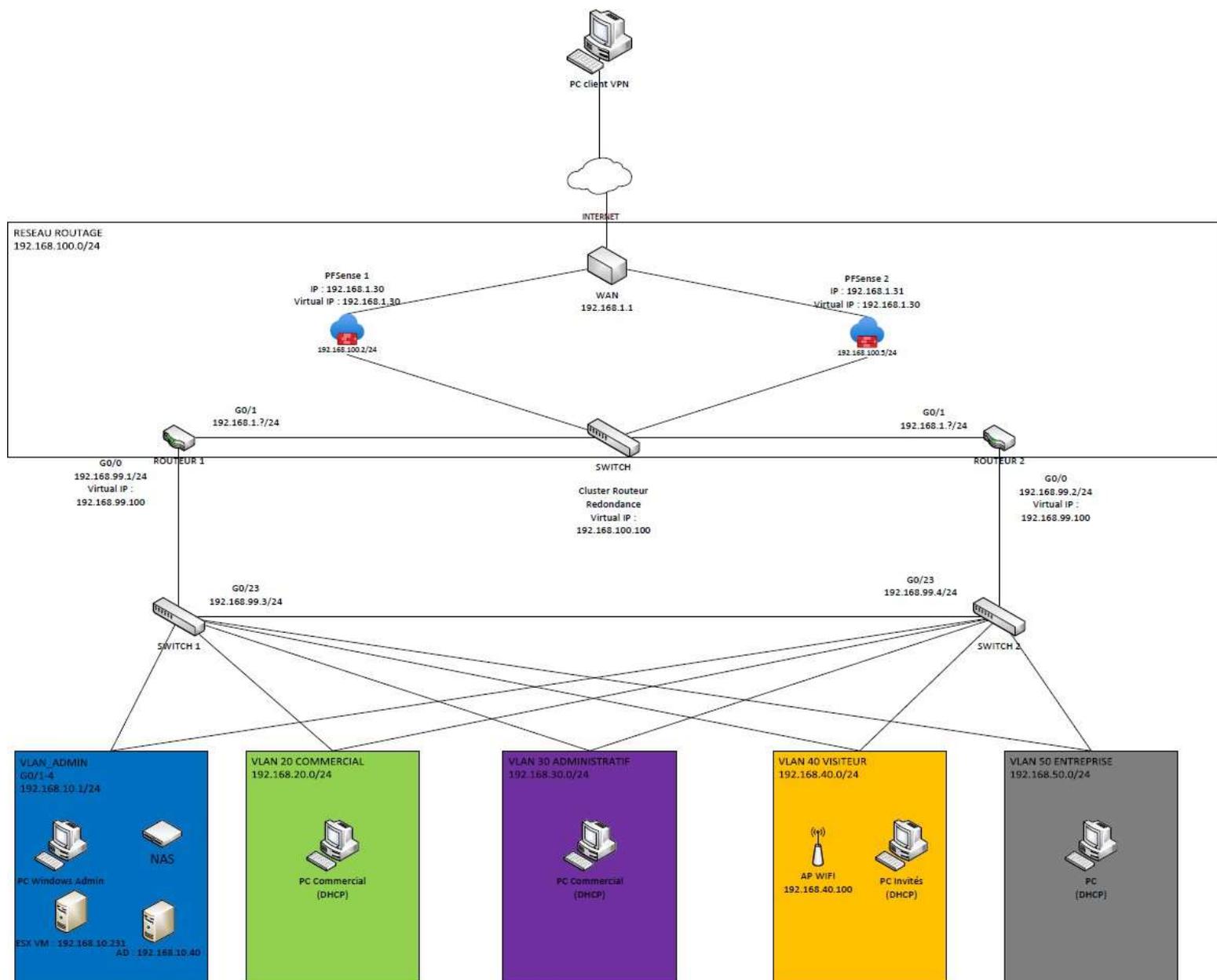
Description de l'Entreprise :

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 :

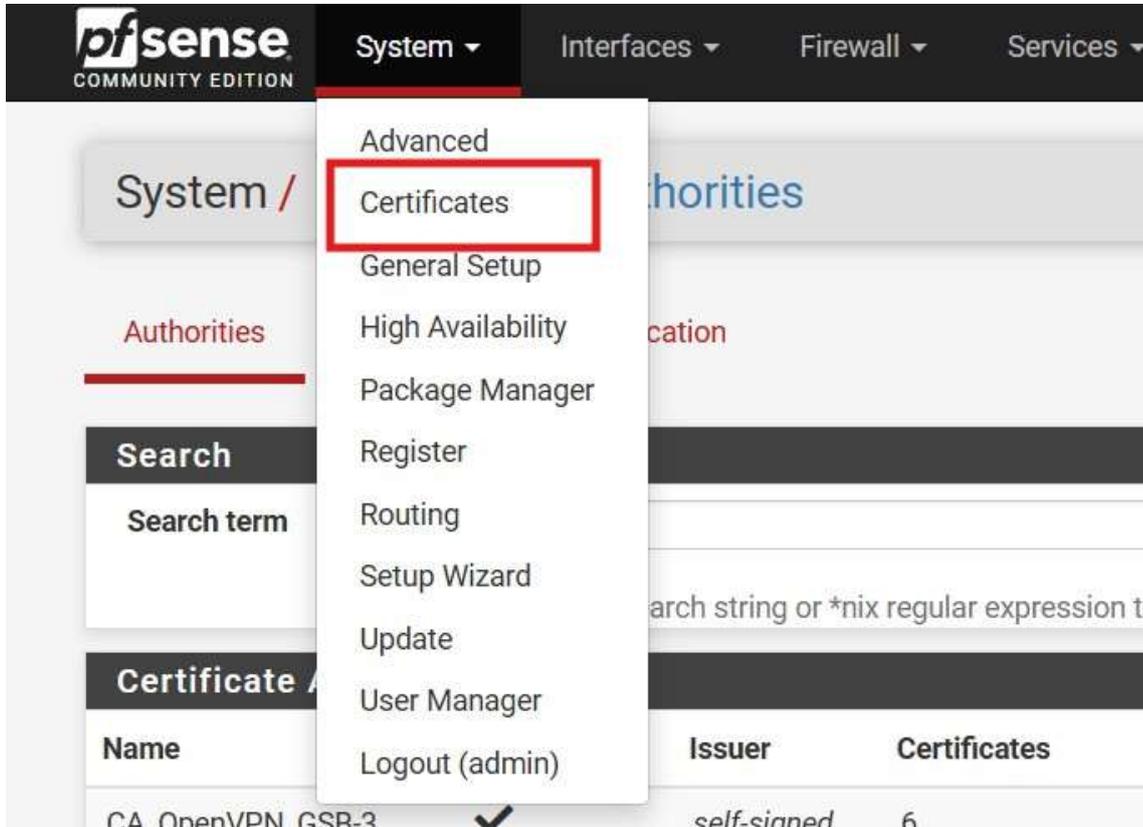
La mise en place d'un service VPN sur pfSense se déroule en trois étapes :

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

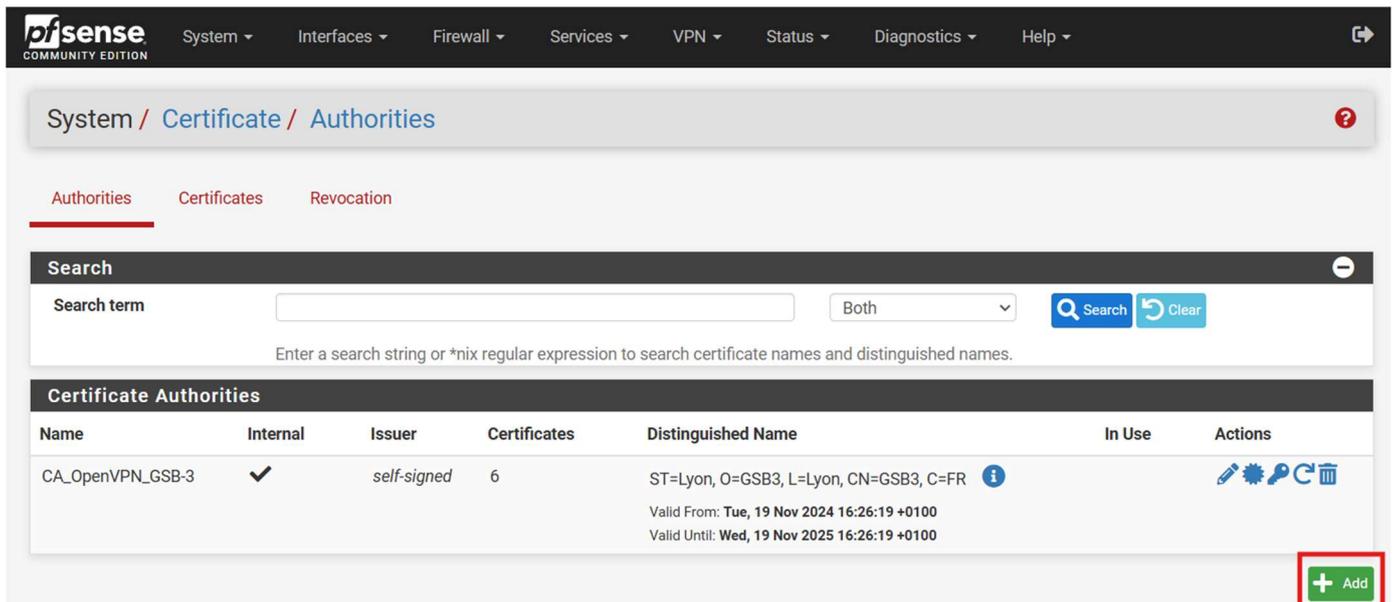
Procédure de mise en place du Service

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 Certificate 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

Create / Edit CA

Descriptive name []
The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ' , "

Method Create an internal Certificate Authority

Trust Store Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority

Key type RSA

2048
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm sha256
The digest method used when the CA is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Lifetime (days) 3650

Common Name internal-ca
The following certificate authority subject components are optional and may be left blank.

Country Code None

State or Province e.g. Texas

City e.g. Austin

Organization e.g. My Company Inc

Organizational Unit e.g. My Department Name (optional)

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

The screenshot shows the OpenVPN web interface with the 'Certificates' tab selected. The 'Add/Sign a New Certificate' form is displayed. The 'Method' dropdown is set to 'Create an internal Certificate'. The 'Descriptive name' field is empty. The 'Certificate authority' dropdown is set to 'CA_OpenVPN_GSB-3'. The 'Key type' dropdown is set to 'RSA'. The 'Key length' dropdown is set to '2048'. The 'Digest Algorithm' dropdown is set to 'sha256'. The 'Lifetime (days)' field is set to '3650'. The 'Common Name' field is set to 'e.g. www.example.com'. Red boxes highlight the 'Method', 'Descriptive name', 'Certificate authority', and 'Common Name' fields.

The following certificate subject components are optional and may be left blank.

Country Code	FR
State or Province	Lyon
City	Lyon
Organization	GSB3
Organizational Unit	e.g. My Department Name (optional)

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

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards Client Export

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	172.17.10.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	GSB_SRV_vpn	

+ 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.

[Servers](#) [Clients](#) [Client Specific Overrides](#) [Wizards](#) [Client Export](#)

General Information

Description

A description of this VPN for administrative reference.

Disabled Disable this server

Set this option to disable this server without removing it from the list.

Mode Configuration

Server mode

Remote Access (SSL/TLS + User Auth)

**Backend for authentication**

Local Database

**Device mode**

tun - Layer 3 Tunnel Mode



"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.

"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

Endpoint Configuration

Protocol

UDP on IPv4 only

**Interface**

WAN



The interface or Virtual IP address where OpenVPN will receive client connections.

Local port

1195

The port used by OpenVPN to receive client connections.

- 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.

Cryptographic Settings

TLS Configuration Use a TLS Key
 A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

Automatically generate a TLS Key.

Peer Certificate Authority CA_OpenVPN_GSB-3

- 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.

Tunnel Settings

IPv4 Tunnel Network
 This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.

IPv6 Tunnel Network
 This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

Redirect IPv4 Gateway Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway Force all client-generated IPv6 traffic through the tunnel.

IPv6 Local network(s)
 IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

Concurrent connections
 Specify the maximum number of clients allowed to concurrently connect to this server.

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

Client Settings

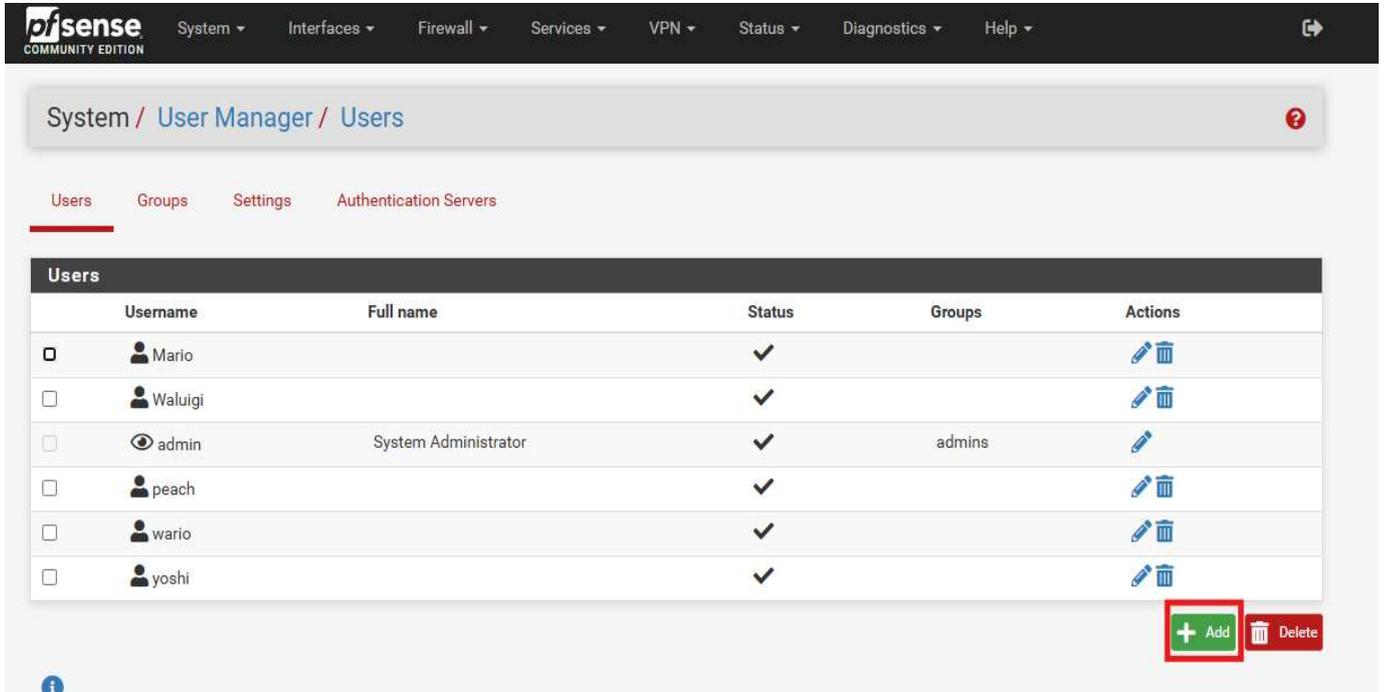
Dynamic IP Allow connected clients to retain their connections if their IP address changes.

Topology net30 - Isolated /30 network per client
 Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

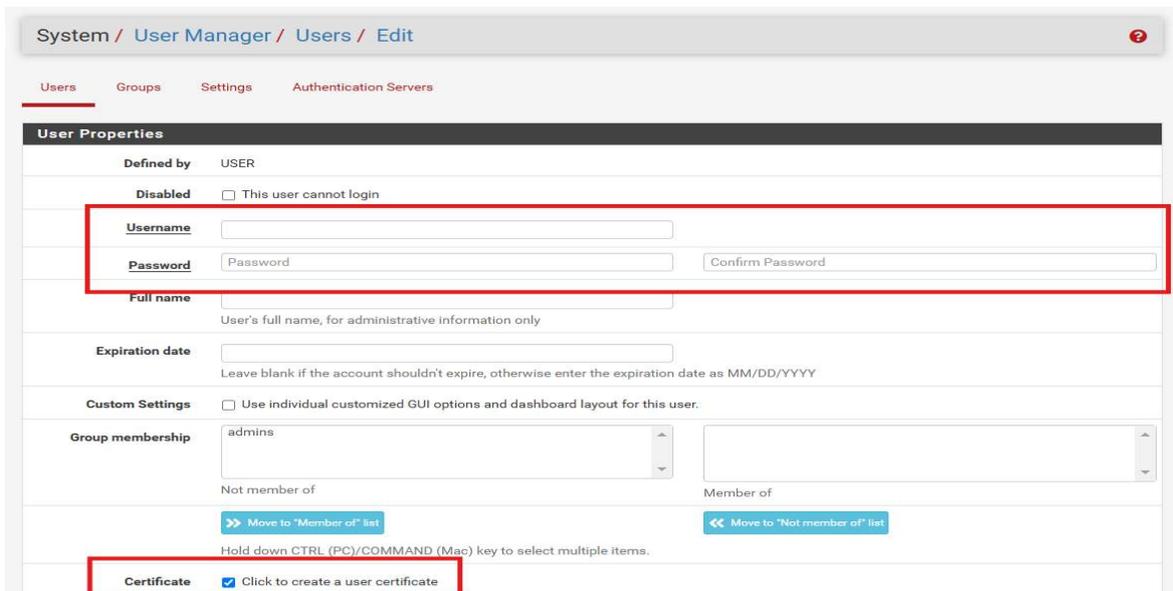
- Si vous en avez un DNS, vous pouvez remplir les paramètres DNS.
- Save

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

Create Certificate for User

Descriptive name:

Certificate authority:

Key type:

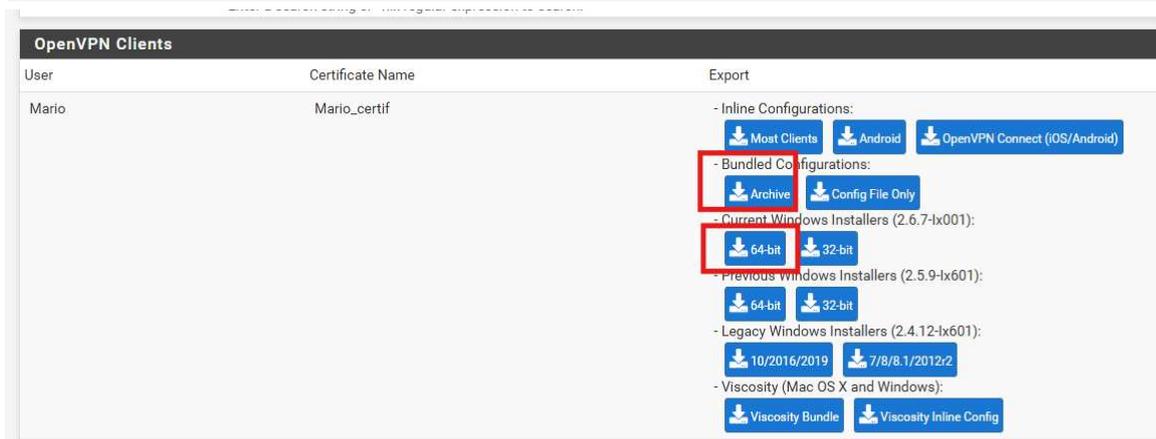
Key length:
The length to use when generating a new RSA key, in bits.
 The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm:
The digest method used when the certificate is signed.
 The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Lifetime:

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.