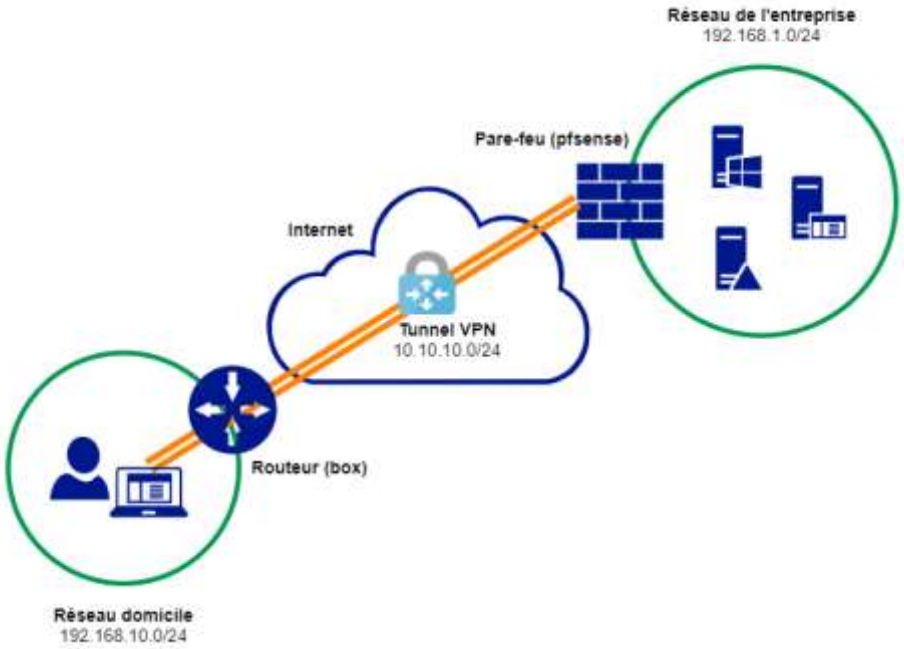
VPN-SSL client-to-site avec OpenVPN

SERIGNE KHADIM FAYE

IT Network Systeme & Security

Cyber Security Enthusiast

Fayekhadim96s@gmail.com



Mise en place d'un VPN-SSL client to Site sur Pfsense

SERIGNE KHADIM FAYE

XAM XAM DOU DOY !

VPN-SSL client-to-site avec OpenVPN

Introduction : Mise en place d'un VPN SSL/TLS sur pfSense

Avec la croissance des menaces sur Internet et la nécessité d'accéder en toute sécurité aux ressources d'un réseau à distance, la mise en place d'un VPN est devenue une solution incontournable pour les entreprises et les particuliers. Parmi les différentes technologies VPN disponibles, le **VPN SSL (Secure Sockets Layer / Transport Layer Security)** s'est imposé comme une solution fiable, flexible et hautement sécurisée.
Ce document détaille la configuration d'un VPN SSL/TLS en utilisant **pfSense**, un pare-feu open source et puissant, et fournit une compréhension approfondie du rôle du protocole SSL/TLS dans ce type de VPN.

1. Le rôle et les caractéristiques du protocole SSL/TLS

❖ Qu'est-ce que le SSL/TLS ?

Le **SSL (Secure Sockets Layer)** et son successeur, le **TLS (Transport Layer Security)**, sont des protocoles de sécurisation des communications sur Internet. Ils permettent d'établir une connexion cryptée et authentifiée entre deux parties (client et serveur).

Rôles principaux du SSL/TLS :

- **Confidentialité des données :**

  Les données échangées sont chiffrées pour qu'elles ne puissent être lues que par les parties concernées.

- **Authentification** :

  Les entités qui doivent communiquer devront s'authentifier pour s'assurer qu'il s'agit bien de l'entité légitime.

- **Intégrité des données :**

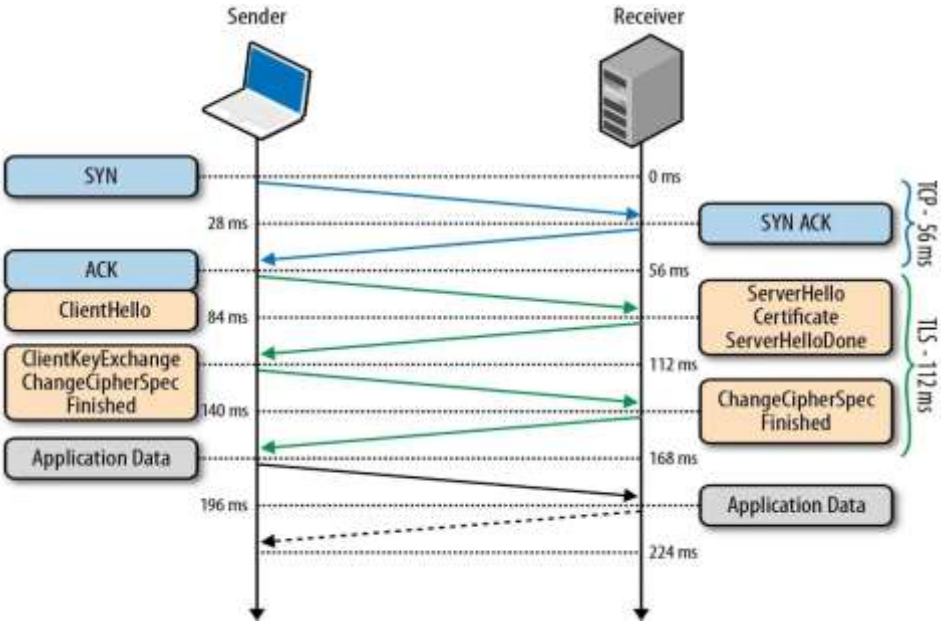
  Le protocole assure que les données n'ont pas été modifiées ou altérées pendant leur transmission a l'aide des fonctions de hachage comme SHA-256.

❖ Fonctionnement du SSL/TLS Handshake SSL/TLS :

Le TLS est un protocole de chiffrement conçu pour sécuriser les communications Internet. La négociation TLS (également nommée handshake) désigne le processus qui amorce une session de communication utilisant le chiffrement TLS.

Au cours de cette négociation, les deux parties communicantes s'échangent l'une l'autre des messages **d'authentification** et de **vérification**, établissent les algorithmes de chiffrement

qu'elles utiliseront et se mettent d'accord sur les clés de session. Cette négociation constitue un élément fondamental du **fonctionnement du protocole HTTPS.**



Que se passe-t-il lors d'une négociation TLS ?

Au cours d'une négociation TLS, le client et le serveur effectuent ensemble les opérations suivantes :

- Préciser quelle version de TLS (TLS 1.0, 1.2, 1.3, etc.) ils utiliseront.
- Décider quelles suites de chiffrement (**Ciphersuites, AES, 3DES…**) ils utiliseront.
- Authentifier l'identité du serveur à l'aide de la clé publique du serveur et de la signature numérique de l'autorité de certification SSL.
- Générer des clés de session afin d'utiliser le chiffrement symétrique une fois la négociation terminée.

❖ **Quelles sont les étapes d'une négociation TLS ?**

La négociation TLS se compose d'une série de datagrammes (ou messages) échangés par un client et un serveur. Elle implique plusieurs étapes, car le client et le serveur échangent les informations nécessaires pour terminer la négociation et rendre la conversation possible.

Les étapes exactes d'une poignée de main TLS varient en fonction du type d'algorithme d'échange de clés utilisé et des suites de chiffrement prises en charge par les deux parties. L'algorithme d'échange de clés RSA, bien que considéré aujourd'hui comme non sécurisé, était utilisé dans les versions de TLS antérieures à la version 1.3. Cela se passe à peu près comme suit :

- **« ClientHello » :** le client démarre la négociation en envoyant un message. Le message inclut la version TLS prise en charge par le client, les suites de chiffrement prises en charge (par exemple, AES-256-GCM, ChaCha20), et une chaîne d'octets aléatoires connue sous le nom de « client random », ou nombre aléatoire pour contribuer à la création de la clé de session.

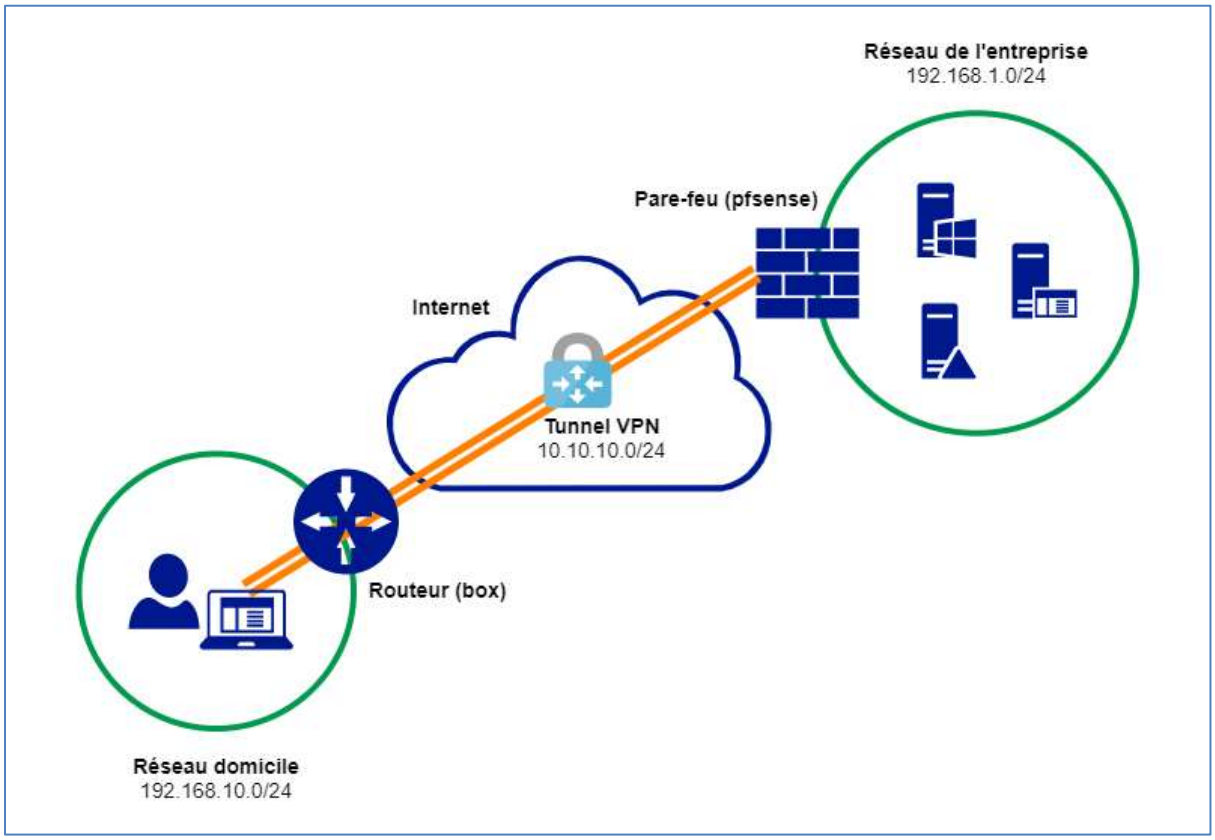
- **« ServerHello » :** en réponse au message Client Hello, le serveur envoie un message contenant **la versions du TLS choisie et compatible, Cipher suite sélectionnée** (Par exemple, AES-256-GCM), **Certificat du serveur** (Le certificat contient la clé publique du serveur, il prouve l'identité du serveur et est signé par une Autorité de Certification (CA) et le « Server random », une autre chaîne aléatoire d'octets générée par le serveur.

- **Signature numérique du serveur :** le serveur calcule une signature numérique de tous les messages jusqu'à ce point.
- **Signature numérique confirmée :** le client vérifie la signature numérique du serveur, confirmant que le serveur est bien celui qu'il prétend être.
- **Paramètre DH client** : le client envoie son paramètre DH au serveur.
- **Calcul du secret pré-maître par le client et le serveur :** plutôt que le client génère le secret pré-maître et l'envoie au serveur, comme dans une négociation RSA, le client et le serveur utilisent les paramètres DH qu'ils ont échangés pour calculer séparément un secret pré-maître correspondant.
- **Création des clés de session :** le client et le serveur calculent à présent les clés de session à partir du secret pré-maître, du client random et du server random, comme dans la négociation RSA.
- **Client prêt :** comme dans la négociation RSA.
- **Serveur prêt**
- **Chiffrement symétrique sécurisé effectué**

2. OpenVPN

OpenVPN est un protocole de **tunneling** open-source largement utilisé pour établir des connexions VPN sécurisées. Il utilise des techniques de chiffrement avancées pour créer un "tunnel" virtuel entre le client et le serveur, permettant ainsi de sécuriser le trafic réseau qui passe sur des réseaux non sécurisés, comme Internet. En tant que protocole de tunneling, **OpenVPN** encapsule les données dans un tunnel sécurisé pour garantir leur confidentialité et leur intégrité pendant leur transmission. Il prend en charge plusieurs méthodes de chiffrement, telles que AES, et utilise des mécanismes de sécurité robustes, comme l'échange de clés basé sur TLS, pour établir une connexion sécurisée entre les deux points. OpenVPN est extrêmement flexible et peut être configuré pour utiliser différents protocoles de transport (comme UDP ou TCP) et s'adapter à divers types de réseaux, ce qui en fait une solution idéale pour des connexions VPN sur des réseaux publics ou privés.

3. Architecture



4. **Gestion des Certificats Numériques :**

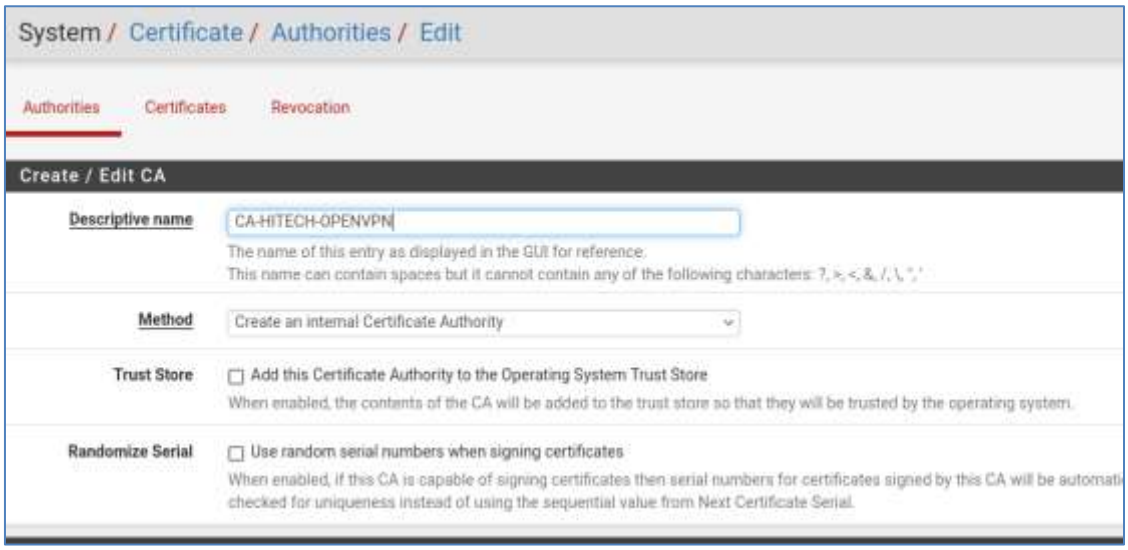
La gestion des certificats est une étape essentielle pour sécuriser un tunnel VPN SSL. Sur le firewall pfSense, nous commencerons par créer une **autorité de certification (CA)** interne, qui servira de base pour émettre et valider les certificats nécessaires.

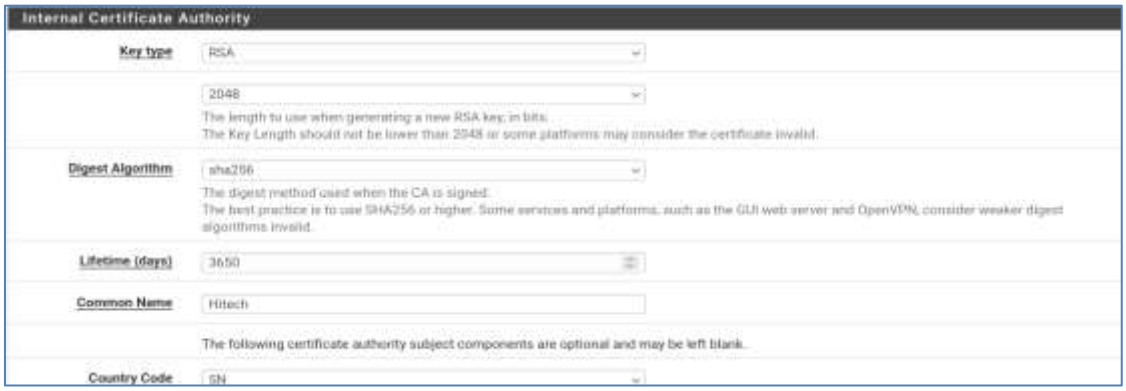
❖ **Création de l'Autorité de Certification (CA)**

L'autorité de certification agit comme une entité de confiance qui délivre des certificats numériques. Sur pfSense, une CA interne sera générée pour signer les certificats utilisés dans notre configuration VPN. Cette CA garantit que les certificats émis sont authentiques et qu'ils peuvent être vérifiés par les clients VPN.

System ➔ Certificates puis Add

Nous remplissons les informations comme la description, l'algorithme de chiffrement ici RSA, l'algorithme de hachage, et les informations concernant notre entreprise etc.





Apres on peut sauvegarder avec **Save**

❖ **Création du certificat du serveur OPENVPN**

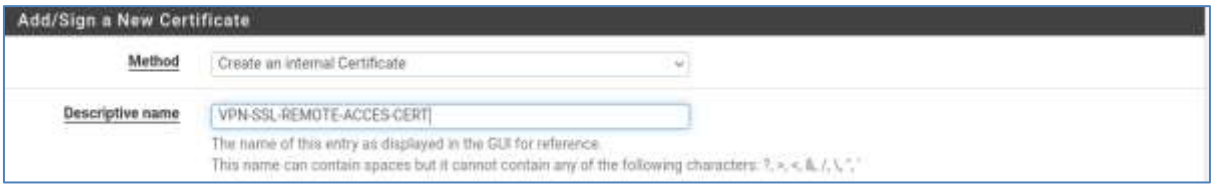
Après avoir créé **l'autorité de certification (CA),** qui, rappelons-le, sert à valider et certifier les informations contenues dans les certificats numériques (comme la clé publique) en signant ces certificats par à l'aide de sa clé publique, nous passons à la création du certificat pour le serveur OpenVPN.

Ce certificat sera utilisé par le serveur pour :

- **Authentifier** son identité auprès des clients VPN.
- **Fournir une clé publique** permettant d'établir un canal sécurisé pour l'échange des clés de session.

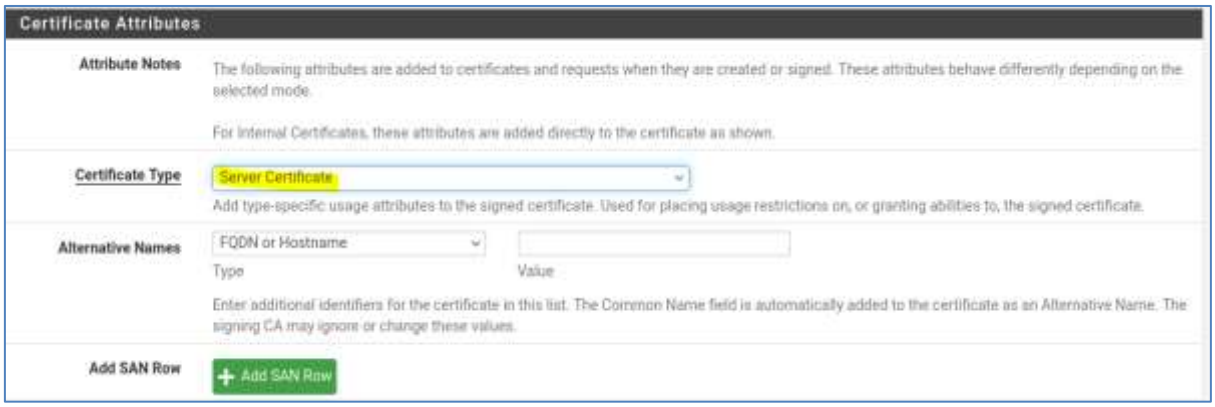
Ainsi, le certificat du serveur, signé par notre CA, garantit une communication sécurisée et de confiance entre les clients et le serveur OpenVPN.

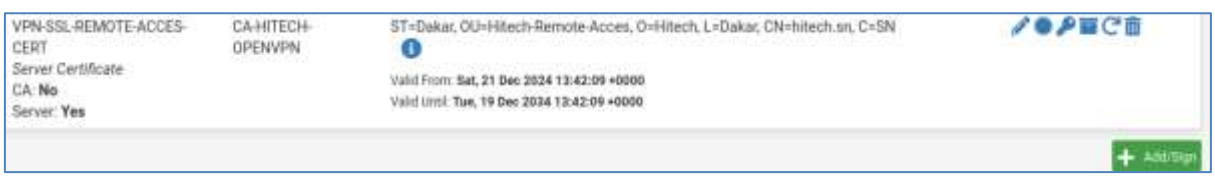
Pour cela, allons dans : **Certificates ➔ Add/Sign**



Par défaut, la validité du certificat est fixée à 3650 jours soit 10 ans. Le "Common Name" correspond là aussi au nom intégré dans le certificat, si vous souhaitez établir une connexion VPN basée sur un nom de domaine, il est préférable d'indiquer cette valeur ici. **Choisissez bien le type de certificat (Certificate Type) suivant : Server Certificate.**

Apres on peut enregistrer les con figurations ; **Save**, nous pouvons voir le certificat qui a été créé.





5. Gestion des utilisateur locaux

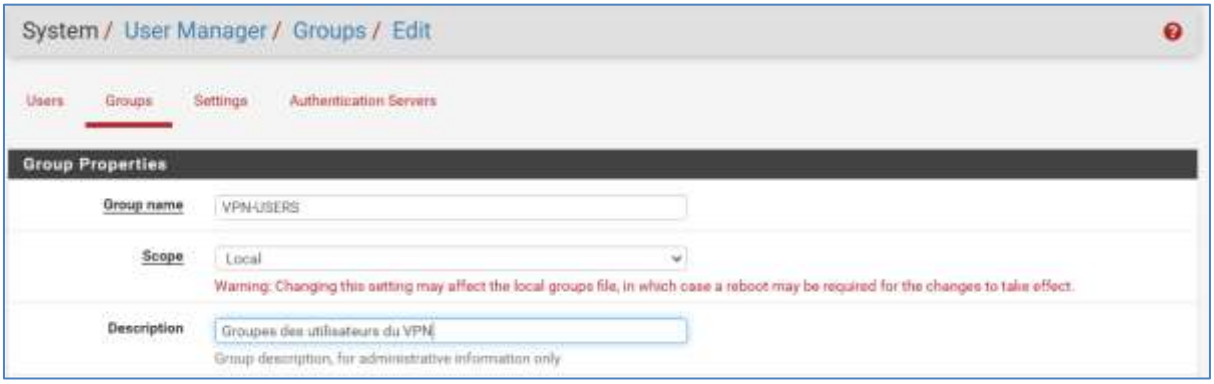
Après avoir configuré l'autorité de certification et créé le certificat du serveur, nous passons à la gestion des utilisateurs. Cette étape consiste à créer les comptes utilisateurs qui auront le droit d'accéder à notre réseau via le VPN.

Pour renforcer la sécurité et simplifier la gestion des droits d'accès, nous allons créer un groupe spécifique nommé **VPN-Users**. Ce groupe servira à regrouper tous les utilisateurs autorisés à se connecter via le VPN.

Étapes 1 : Création du groupe VPN Users :

Le groupe est défini avec des permissions spécifiques, adaptées aux besoins des utilisateurs VPN. Cela permet une gestion centralisée et homogène des droits.

System ➔User Managers➔Group après Add pour creer le groupe VPN-USERS



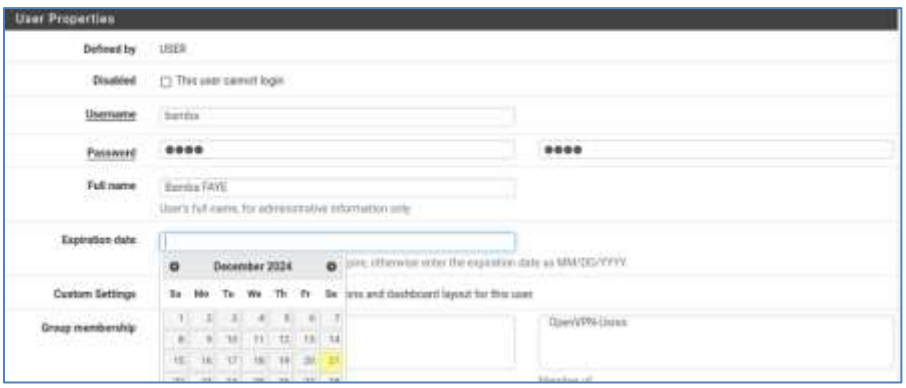
Etape2 : Ajout des utilisateurs :

Chaque utilisateur est créé avec des identifiants uniques (nom d'utilisateur et mot de passe).

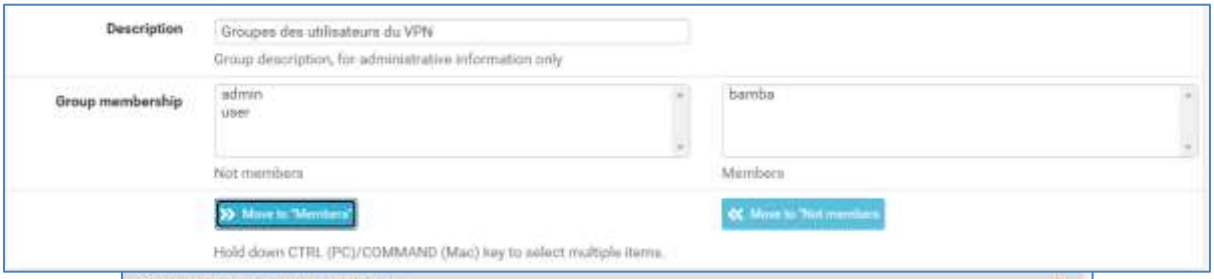
Un certificat personnel est également généré pour chaque utilisateur, signé par l'autorité de certification. Ce certificat garantit leur identité et sécurise la connexion. Si nous avons plusieurs utilisateurs qui doivent utiliser le vpn, c'est mieux par la suite de choisi l'authentification base sur **un serveur LDAP ou RADIUS** pour centraliser le tout.

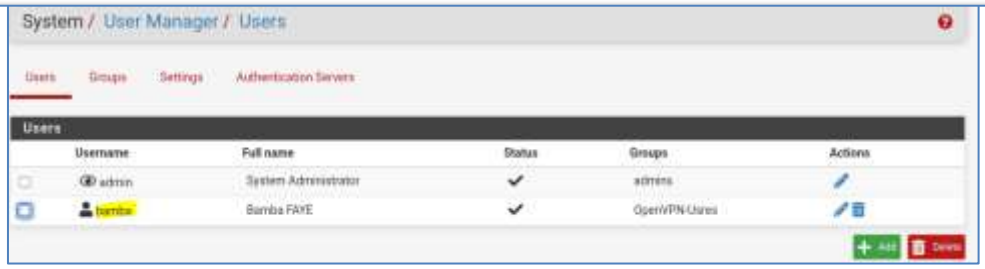
Grâce à cette organisation par groupe, il est plus facile de gérer les accès et de modifier les permissions globales en cas de besoin, tout en maintenant un haut niveau de sécurité.

Il est aussi possible de définir la date d'expiration du compte créer, ce qui est aussi très utile et présent un avantage de sécurité.



Apres, nous pouvons voir l'utilisateur déjà crée.



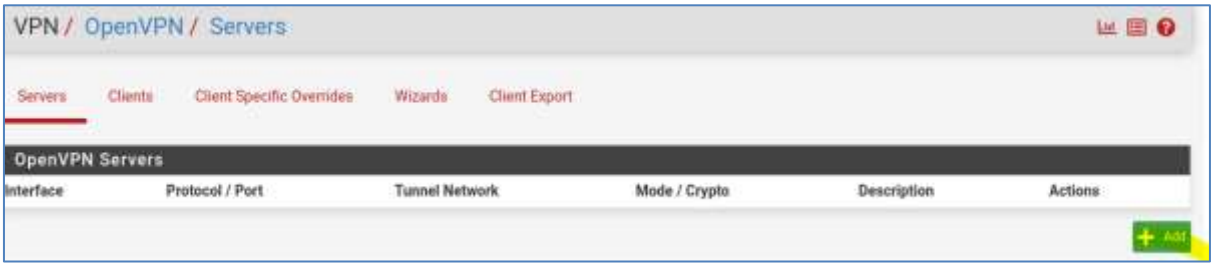


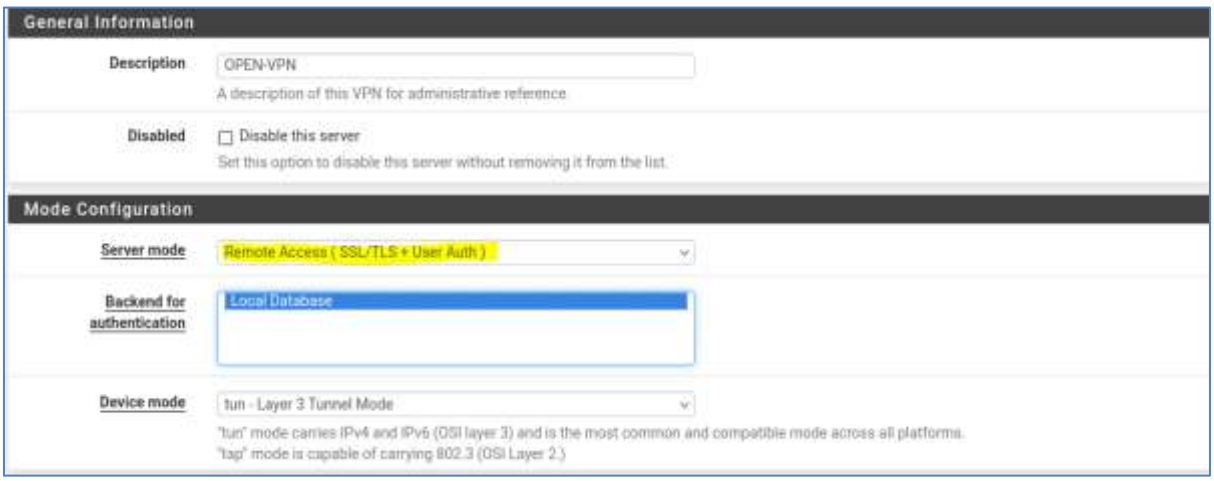
6. Configuration de OpenVPN

Maintenant que la gestion des certificats est fonctionnelle et que nous avons créé un compte utilisateur (ou un groupe d'utilisateurs pour une meilleure organisation), nous pouvons passer à la configuration proprement dite du VPN. Cette étape consiste à définir les paramètres nécessaires pour établir un tunnel sécurisé entre les clients et le réseau de l'entreprise. Pour ce faire, accédez au menu **"VPN"** dans l'interface de PfSense, puis sélectionnez **"OpenVPN"**. Vous y trouverez les options pour configurer le serveur OpenVPN, spécifier les protocoles, les ports, et les paramètres de chiffrement adaptés à vos besoins.

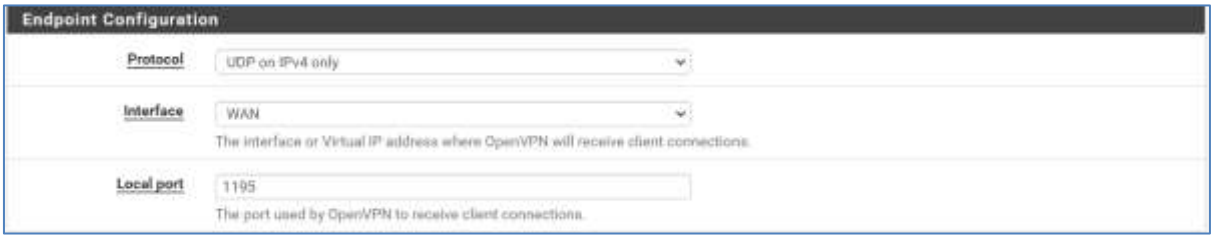
Il est possible d'utiliser Wizards pour avoir un assistant pour la configuration, mais je préférer faire la configuration sans l'utiliser ! **Genre Geek lol**

Pour cela, allons dans Server➔Add

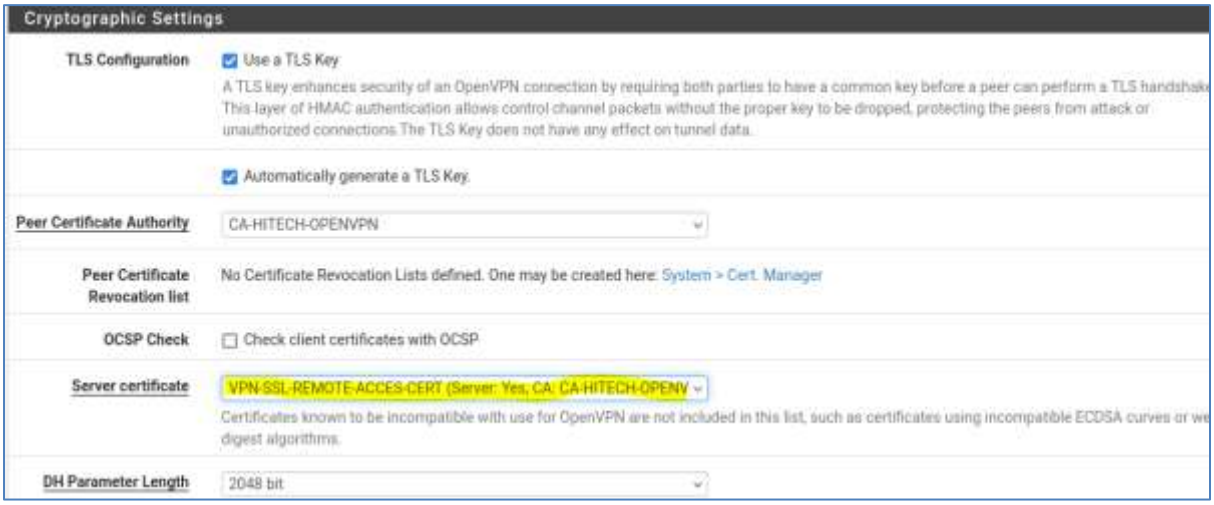




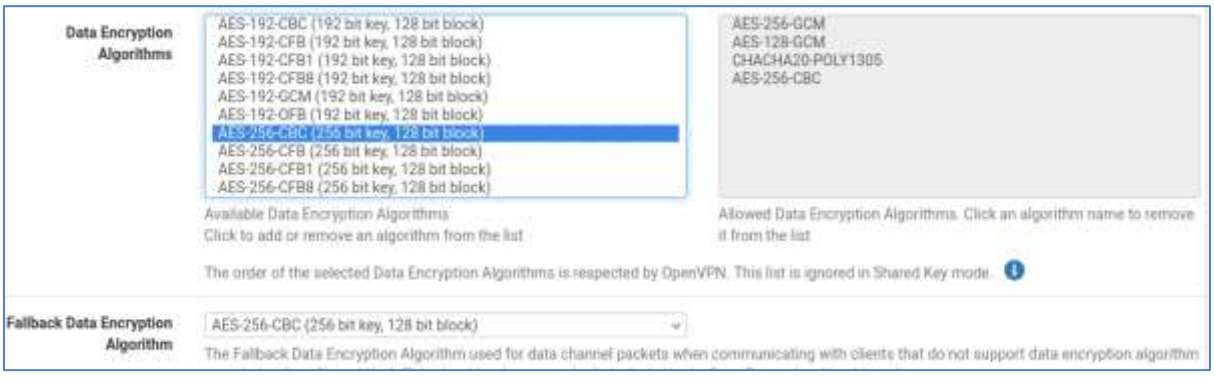
Sur la partie Endpoint Configuration, choisissons le protocole, l'interface et le port (par défaut 1194)



Cryptograpic Settings nous permet de choisir les paramètres cryptographiques qui seront utilisés comme l'algorithme ce chiffrement, l'algorithme de hachage etc.



Il faudra bien choisir sur la partie Server Mode : Remote Acces (SSL/TLS + User Auth)
Le port par défaut est le **1194 en UDP**. C'est possible de changer ce port aussi pour garantir un peu l'anonymat. Sur la partie des paramètres cryptographiques, il faudra bien l'autorité de certificat précédent créer.



Passons maintenant à la configuration détaillée de notre tunnel VPN. Cette étape est cruciale pour définir les paramètres réseau nécessaires à la communication entre les clients et le réseau de l'entreprise. Voici les principales options à configurer :

1. IPv4 Tunnel Network

- Cette option définit l'adresse du réseau dédié au VPN. Lorsqu'un client se connecte via le VPN, il se voit attribuer une adresse IP de ce réseau.
- **Exemple** : Si vous spécifiez 10.10.10.0/24, les clients auront des adresses IP comprises entre 10.10.10.1 et 10.10.10.254.

2. Redirect IPv4 Gateway

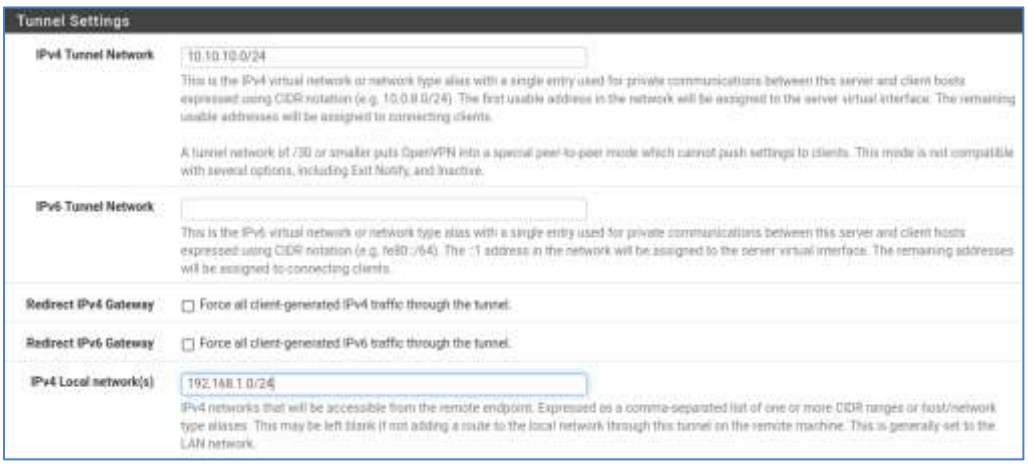
- En cochant cette option, vous activez le mode **full tunnel**. Cela signifie que tout le trafic réseau de l'utilisateur distant transitera par le VPN.
- Si cette option n'est pas cochée, vous êtes en mode **split-tunnel**, où seuls les flux destinés au réseau distant passeront par le VPN, tandis que le reste du trafic (par exemple, vers Internet) utilisera directement la connexion locale de l'utilisateur.
- **Astuce** : Utilisez le full tunnel pour un maximum de sécurité, mais privilégiez le split-tunnel pour une meilleure performance et réduction de la bande passante utilisée.

3. IPv4 Local Network

- Spécifiez ici les adresses des réseaux locaux (LAN) que vous souhaitez rendre accessibles via le VPN.
- **Exemple** : Si vous voulez permettre l'accès au réseau interne 192.168.1.0/24, vous entrez cette adresse ici. Pour plusieurs réseaux, séparez-les par une virgule (e.g., 192.168.1.0/24,192.168.2.0/24).

4. Concurrent Connections

- Définit le nombre maximum de connexions VPN simultanées autorisées.
- **Exemple** : Si vous limitez à 10 connexions, seuls 10 utilisateurs pourront être connectés au VPN en même temps.



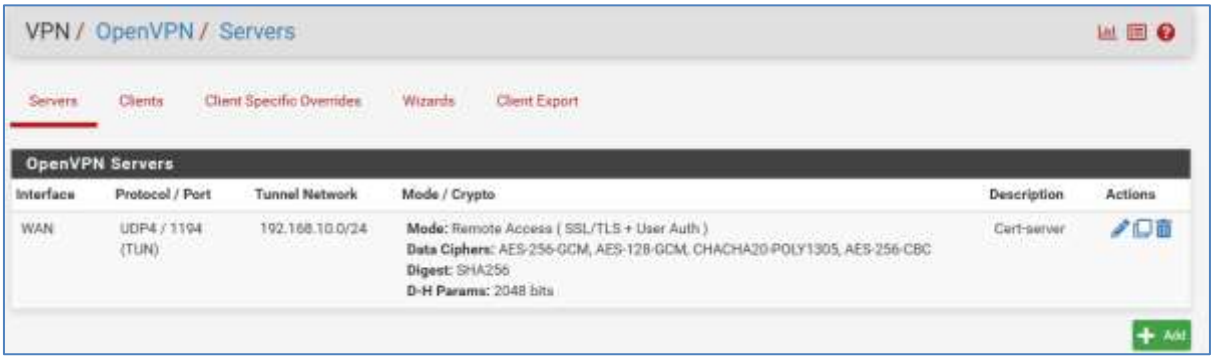
Pour les paramètres des clients, il est recommandé de cocher l'option **"Dynamic IP"**, afin de permettre aux utilisateurs en mobilité, notamment ceux connectés via une connexion 4G, de maintenir leur connexion VPN même si leur adresse IP publique change.

Au niveau de la **"Topology"**, il est crucial, pour des raisons de sécurité, de choisir la topologie **"net30 - isolated /30 network per client"**. Cette configuration garantit que chaque client est isolé dans un sous-réseau dédié (de la plage réseau VPN), empêchant ainsi toute communication directe entre les clients.

Si vous souhaitez permettre aux clients d'utiliser la résolution DNS interne de votre entreprise, vous pouvez configurer la diffusion d'un serveur DNS via le VPN. Pour cela :

1. **Cochez** l'option **"Provide a DNS server list to clients. Addresses may be IPv4 or IPv6"** et renseignez les adresses IP de vos serveurs DNS internes dans les champs prévus à cet effet.
2. **Cochez également** l'option **"Provide a default domain name to clients"** pour indiquer le nom de domaine local de votre entreprise, ce qui permettra aux clients de résoudre facilement les noms internes du réseau.

Apres, on peut sauvegarder la configuration.



7. **Exporter la configuration OpenVPN**

Pour permettre à vos utilisateurs de se connecter à votre serveur OpenVPN, il est nécessaire d'exporter la configuration du client au format «. ovpn". Cette configuration sera utilisée sur les appareils clients pour établir la connexion sécurisée au VPN. Pour cela, il est nécessaire d'installer un paquet supplémentaire sur votre pare-feu PfSense. Suivez les étapes suivantes :

1. Allez dans le menu **System** > **Package Manager** > **Available Packages**.
2. Dans la barre de recherche, tapez "openvpn".
3. Localisez et installez le paquet **openvpn-client-export**.

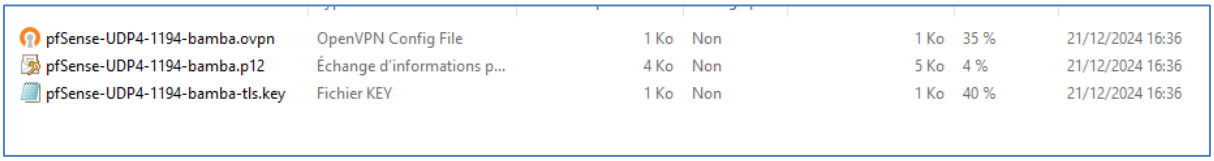
Une fois le paquet installé, vous pourrez exporter facilement la configuration du client OpenVPN et la distribuer à vos utilisateurs.

Installer Openvpn-cleint-export

Une fois installe, nous allons retourner sur l'onglet openvpn pour export la configuration. Pour cela, on part sur OpenVPN ➔Client Export et on descend tout à fait en bas de la page ; on peut voir d'ailleurs l'utilisateur que nous avons créé.

On export le fichier de configuration en cliquant sur : Archive (Bundled configuration)

Il contient le fichier de configuration pour la connexion (.ovpn), le certificat et la clé.



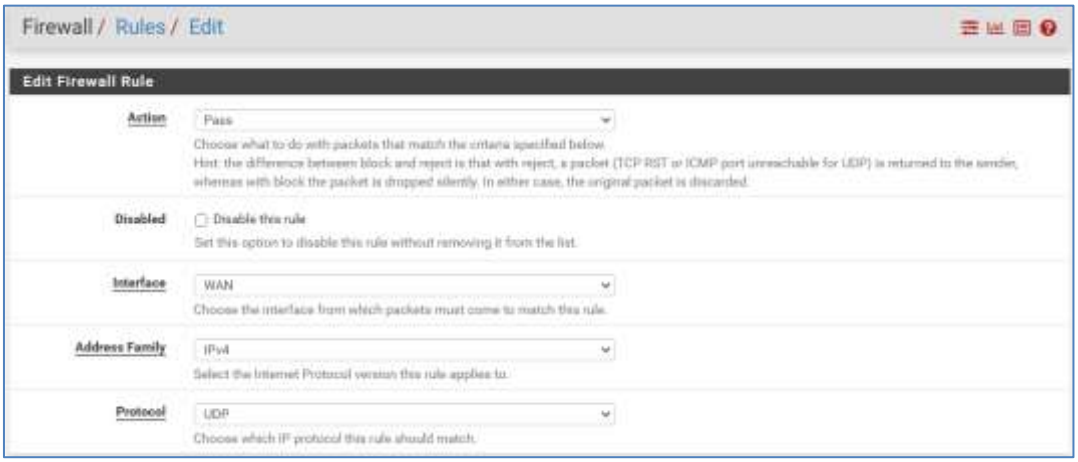
Nous pouvons en même temps cliquer sur un des liens en bas pour télécharger le client OpenVPN, ici je télécharge la version pour Windows.

8. Création de règles

Il nous faudra crée deux règles sur le pare-feu :

L'une va permettre aux clients d'établir une connexion avec notre serveur (cette règle sera créée au niveau de l'interface WAN) et l'autre va autoriser le trafic a l'intérieur du tunnel (cette règle sera créée au niveau de l'interface openVPN).

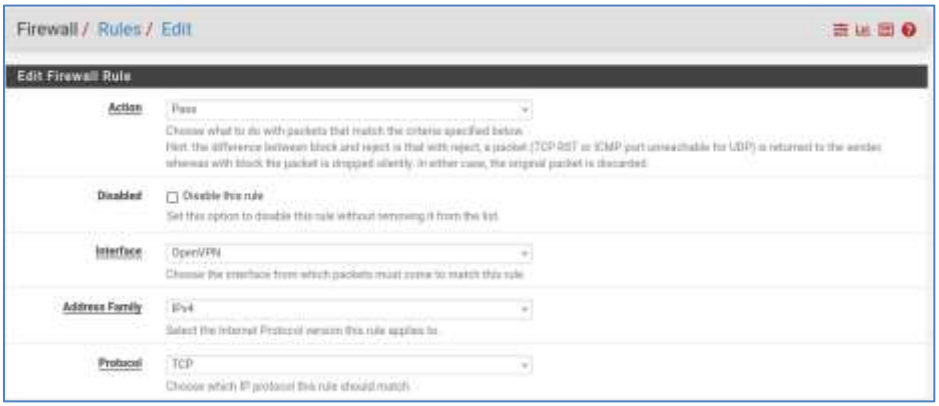
Pour cela, allons sur **Firewall➔Rules et ajoutons la règle.** Elle va autoriser le trafic sur l'interface WAN en UDP.

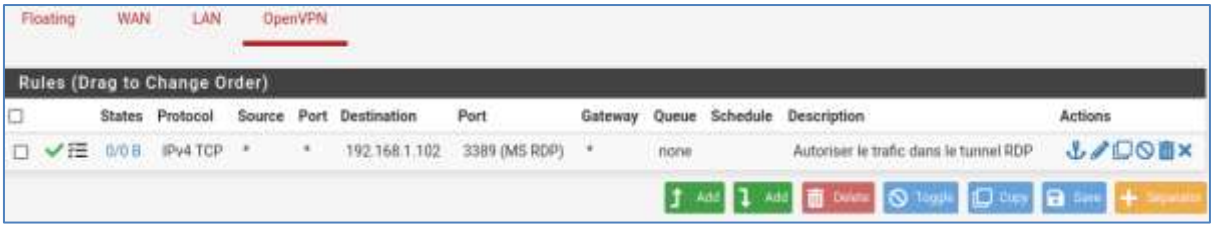


La source sera n'importe quel réseau comme internet, mais la destination sera sur l'interface WAN et uniquement sur le port 1194 sur lequel tourne le service OpenVPN.

On peut aussi Consigner les paquets gérés par cette règle en cochant l'option **: Log packets that are handled by this rule**

A ce stade, notre serveur OpenVPN est bien configure et permet aux clients de se connecter mais le trafic a l'intérieur du tunnel est bloquer ; donc il faudra aussi crée une règle pour autoriser le trafic dans le tunnel vpn. Pour ce lab, je mets en place une règle qui va autoriser le trafic dans le tunnel pour avoir accès a mon contrôleur de domaine (Windows Serveur 2019) via RDP (Remote Desktop Protocol).

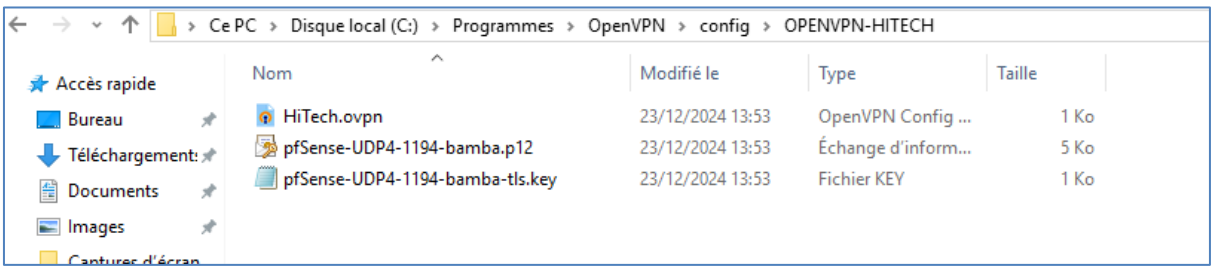




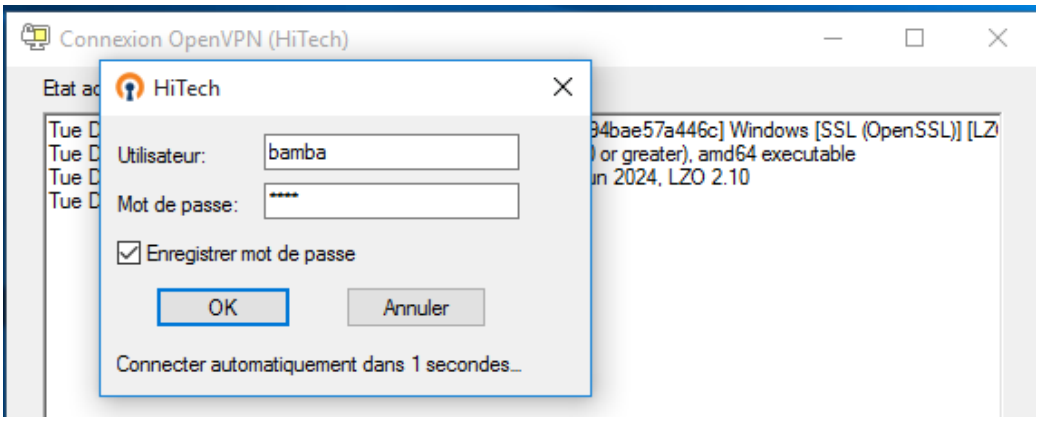
9. Installation de OpenVPN sur le client Windows

Passons s sur le client pour installer openVPN client et importer le fichier de configuration. Apres avoir téléchargé le client openVPN, l'installation est très simple : Suivant, suivant et installer.

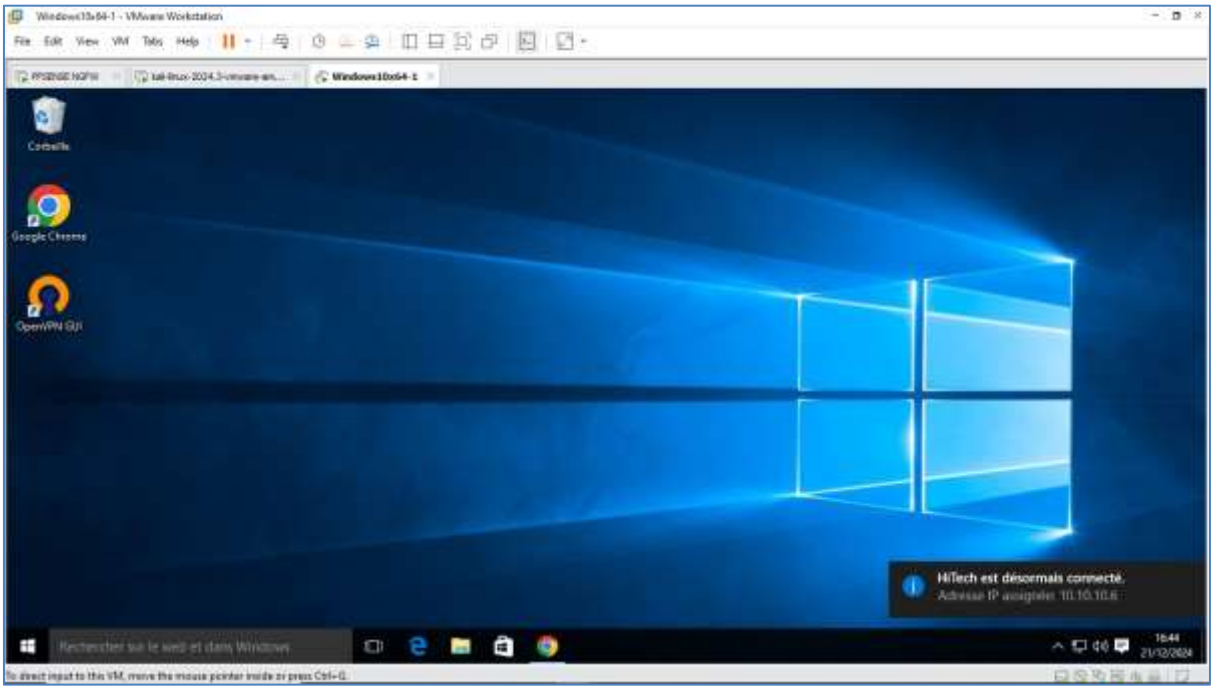
Apres l'installation, nous allons copier les trois sur fichier sur **C:\Users\Bamba-FAYE\OpenVPN\config ou C:\Program Files\OpenVPN\config**



Apres cela, faisons une clique droite sur le cadenas ➔connecter pour entrer le login et le mot de passe de 'utilisateur.



La connexion est établie avec succès et on peut même voir la nouvelle adresse ip assignée à notre client ; ici le 10.10.10.6.



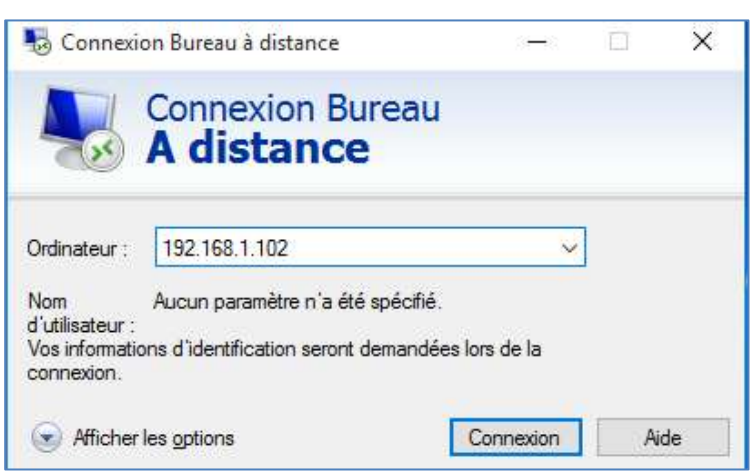
Depusi notre pare-feu, on peut voir le client qui s'est connecte avec son adresse ip reel et celui attrirbué par le serveur vpn

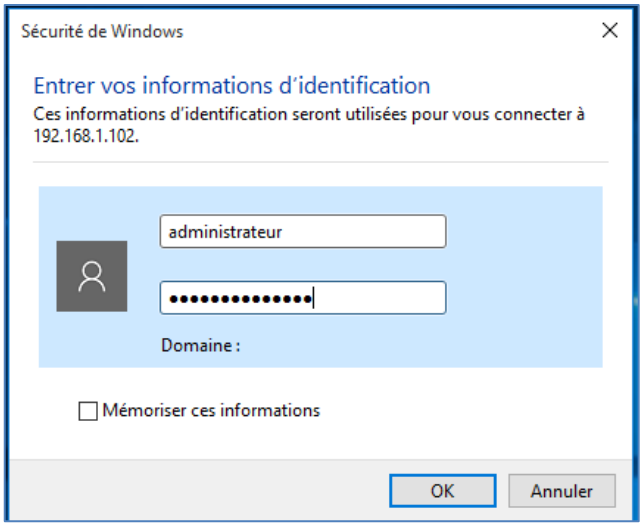
Status➔OpenVPN

Sur le client on peut6 aussi noter une nouvelle carte réseau avec l'adresse 10.10.10.6

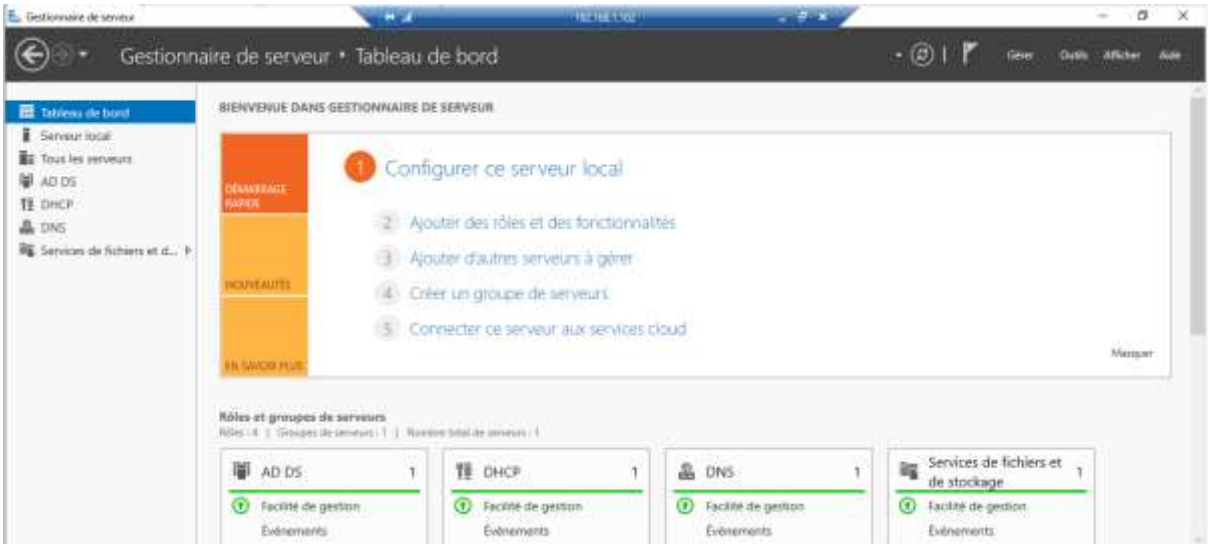
```
Carte Ethernet Ethernet 2 :

   Suffixe DNS propre à la connexion. . . : localdomain
   Adresse IPv6 de liaison locale. . . . .: fe80::4063:a974:902d:f2eb%4
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.86.131
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.86.2

Carte inconnue OpenVPN TAP-Windows6 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::ac3a:e1f7:62c:d332%9
   Adresse IPv4. . . . . . . . . . . . . .: 10.10.10.6
   Masque de sous-réseau. . . . . . . . . : 255.255.255.252
   Passerelle par défaut. . . . . . . . . :
```

10. Connexion en RDP depuis le client

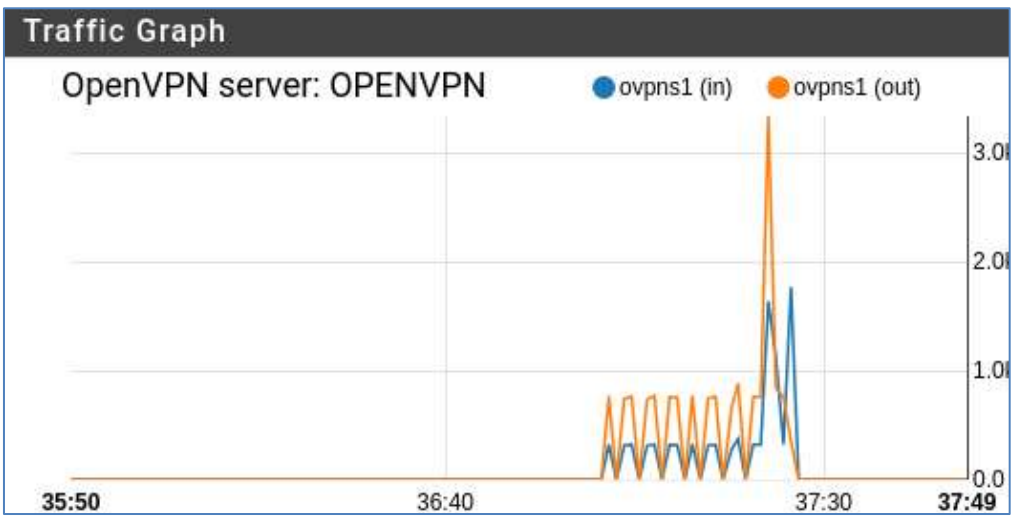




On constate que la connexion est bien établie et que j'ai accès a mon contrôleur de domaine.



On note aussi du trafic au niveau de l'interface OpenVPN



Conclusion

La mise en place d'un serveur VPN sous pfSense avec OpenVPN, basé sur le protocole SSL/TLS, offre une solution robuste et sécurisée pour protéger les communications réseau. En combinant une autorité de certification interne, des certificats numériques pour les serveurs et les clients, ainsi qu'une configuration minutieuse des paramètres de tunnel, cette architecture garantit la confidentialité, l'intégrité et l'authenticité des données échangées entre les utilisateurs et le réseau.

Cependant, lorsque le nombre d'utilisateurs VPN augmente, la gestion locale des comptes peut devenir lourde et difficile à administrer. Pour simplifier cette gestion tout en renforçant la sécurité, il est recommandé de centraliser l'authentification des utilisateurs à l'aide de protocoles tels que **LDAP** ou **RADIUS**. Ces solutions permettent de gérer efficacement les droits d'accès, d'automatiser l'intégration des utilisateurs, et de s'intégrer facilement avec les annuaires d'entreprise comme Active Directory.

En adoptant cette approche centralisée, les administrateurs bénéficient d'une meilleure flexibilité et d'un contrôle plus granulaire sur l'accès au réseau, tout en simplifiant les tâches d'administration. Ainsi, pfSense et OpenVPN, combinés à une authentification centralisée, deviennent une solution complète pour répondre aux besoins d'une infrastructure réseau moderne, sécurisée et évolutive.