RAPPORT

BTS SIO - E6

Situation professionnelle n°1

Déploiement d'un bastion de sécurité pfSense et configuration d'un service OpenVPN avec authentification par certificats

06/02/2026

Contexte et Problématique :

Une PME possède des données dispersées sur plusieurs postes de travail, sans sauvegarde centralisée ni gestion des droits. Cette situation pose des risques critiques : perte de données en cas de panne disque, accès non autorisés à des documents confidentiels (RH, Direction), et saturation de l'espace de stockage par des fichiers personnels (vidéos, musiques). La demande : Centraliser les données sur un serveur sécurisé, garantir la redondance des disques, cloisonner les accès par service et contrôler le type de fichiers stockés.

NOM	DATE	TAMPON
CHERIF SOULEYMANE	06/02/2026	

SOMMAIRE :

1. LE CAHIER DES CHARGES :

1. Objectif principal :

L'objectif est de déployer une solution de télétravail sécurisé pour la PME. Il s'agit de permettre aux employés (Compta, Direction) d'accéder aux ressources internes (le serveur de fichiers du projet E5) depuis l'extérieur, tout en garantissant que les données ne soient pas interceptées sur Internet.

1.2. Choix techniques :

Environnement technologique :

- Pare-feu/Routeur : pfSense (Bastion de sécurité).
- Protocole VPN : OpenVPN (choisi pour sa robustesse et sa facilité de passage à travers les box internet).
- Chiffrement : SSL/TLS avec algorithme AES-256-GCM.
- Authentification : Double facteur (Certificat numérique + Identifiant/Mot de passe).

1.3. Prérequis :

- Le pare-feu pfSense opérationnel avec une interface WAN (Internet) et une interface LAN.
- Une Autorité de Certification (CA) interne créée sur le pfSense.
- Le serveur Windows Server 2022 (E5) fonctionnel dans le LAN.

1.4. Compétences :

Compétences du référentiel mises en œuvre :

- Protéger les données à travers des flux chiffrés.
- Gérer l'identité par la gestion des certificats numériques (PKI).
- Sécuriser les accès distants des utilisateurs nomades.

1.5. Déroulement :

Phase 1 : Mise en place de l'Infrastructure à Clés Publiques (PKI)

- Création d'une Autorité de Certification (CA) interne sur le bastion pfSense.
- Génération d'un certificat serveur dédié au service OpenVPN pour garantir l'identité du point d'accès.

Phase 2 : Configuration du service d'accès distant (VPN)

- Paramétrage du serveur OpenVPN (chiffrement AES-256-GCM, port UDP 1194).
- Définition du réseau de tunnel (adressage virtuel) et routage vers le réseau local (LAN).

Phase 3 : Gestion des identités et des accès nomades

- Création des comptes utilisateurs et génération des certificats clients individuels.
- Configuration des règles de pare-feu (Firewall) pour autoriser le flux VPN et filtrer les accès vers le serveur de fichiers.

Phase 4 : Déploiement client et validation

- Installation du client OpenVPN sur les postes nomades.
- Tests de connectivité et vérification du chiffrement des flux pour valider la confidentialité.

1.6. **Contraintes :**

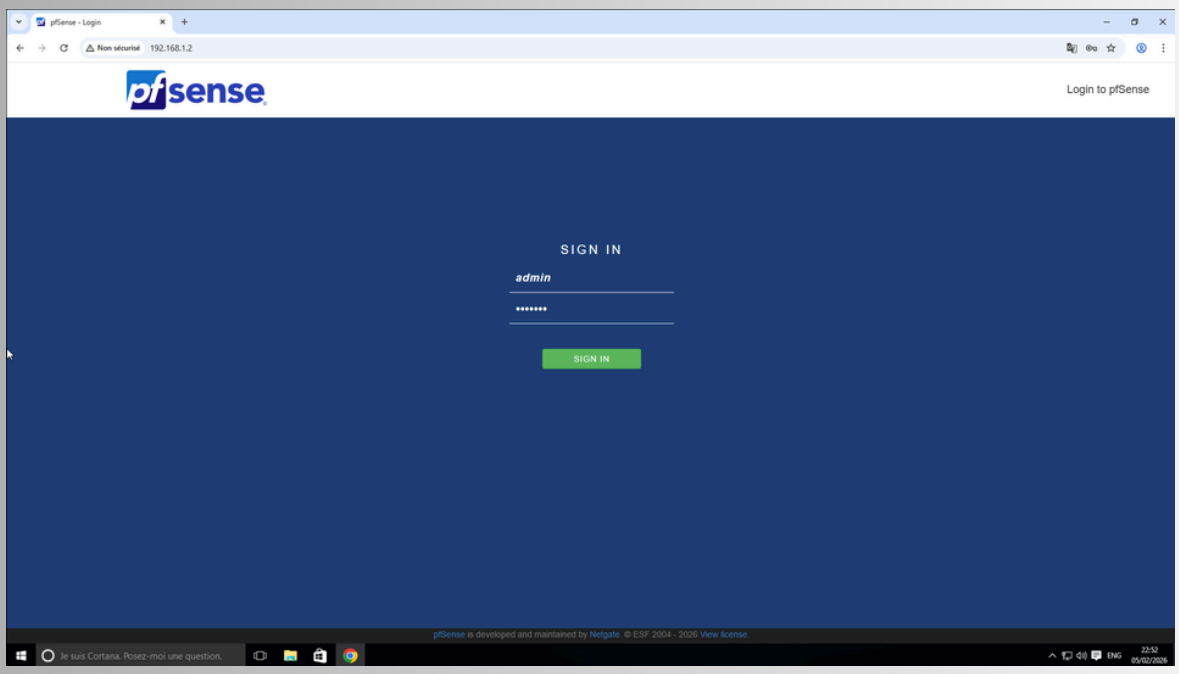
- **Contrainte de sécurité** : L'accès doit impérativement reposer sur une authentification forte (certificat + mot de passe) pour éviter toute usurpation d'identité en cas de vol de terminal.
- **Contrainte technique** : La solution VPN doit être capable de traverser les équipements réseaux domestiques (NAT des box internet) sans configuration complexe pour l'utilisateur final.
- **Contrainte de confidentialité** : Tous les flux transitant par Internet doivent être chiffrés avec un algorithme robuste pour empêcher l'interception de données sensibles de la PME.
- **Contrainte organisationnelle** : L'accès distant ne doit pas modifier les habitudes des utilisateurs ; les lecteurs réseau (Compta, Direction) configurés en E5 doivent être accessibles de la même manière via le tunnel.

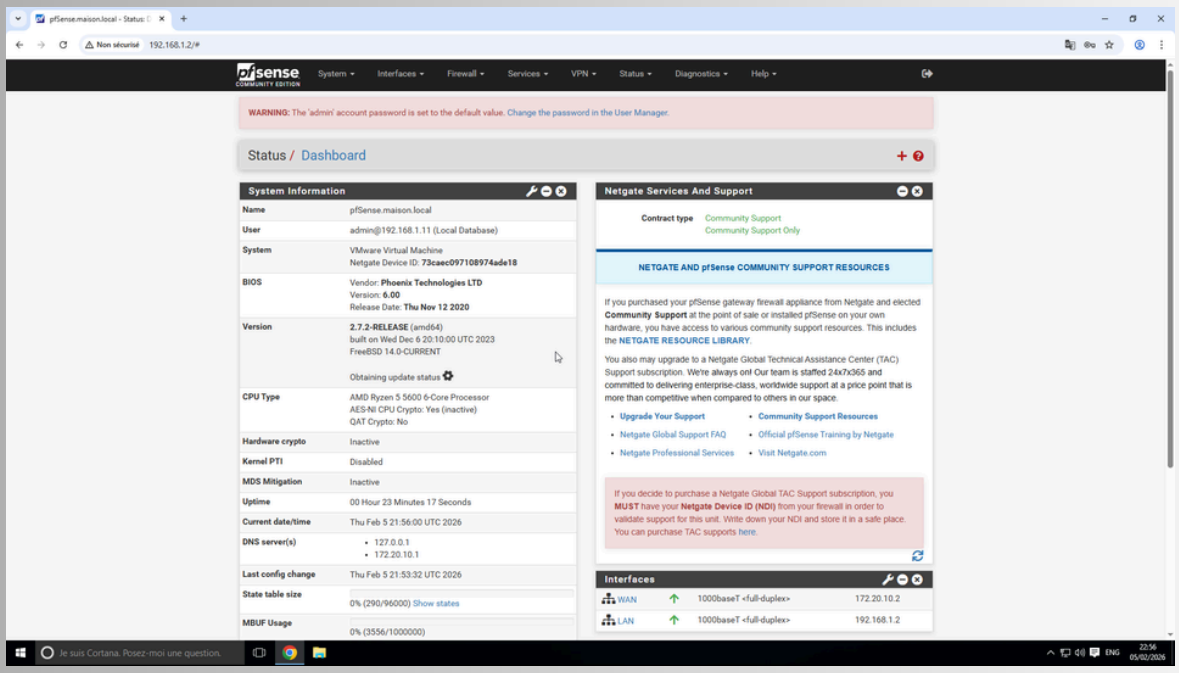
2. MISE EN OEUVRE :

2.1. Création de la PKI (Public Key Infrastructure)

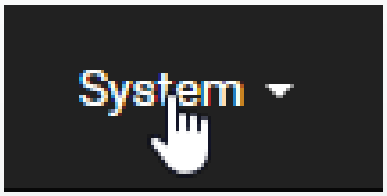
2.1.1. Création de l'Autorité de Certification (CA) interne

- Connexion au WebConfigurator de pfSense.

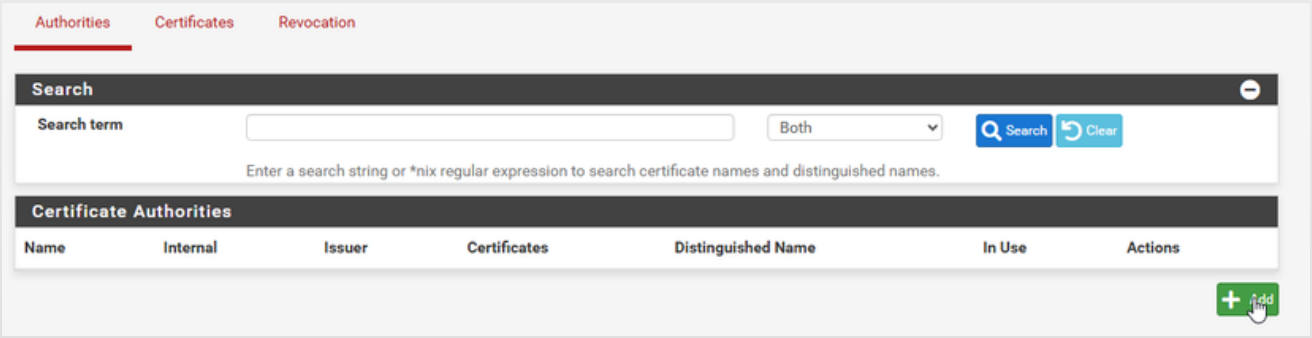




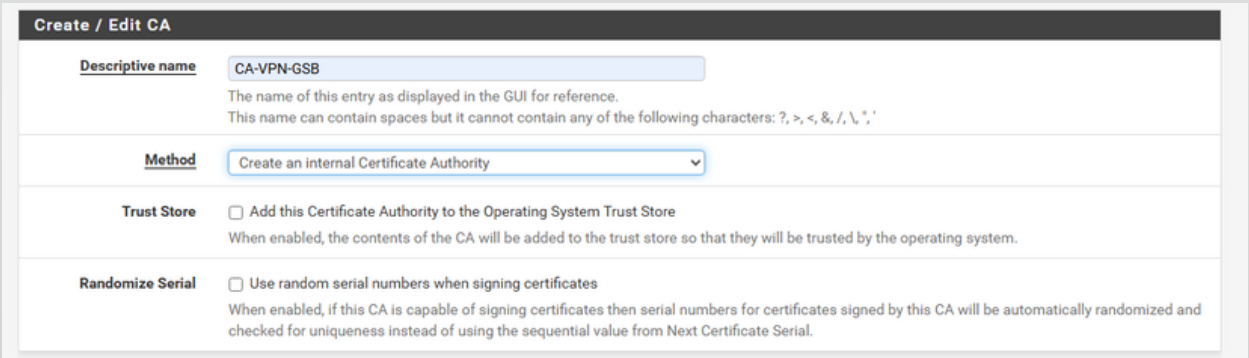
- Configuration de l'autorité de certificat interne.

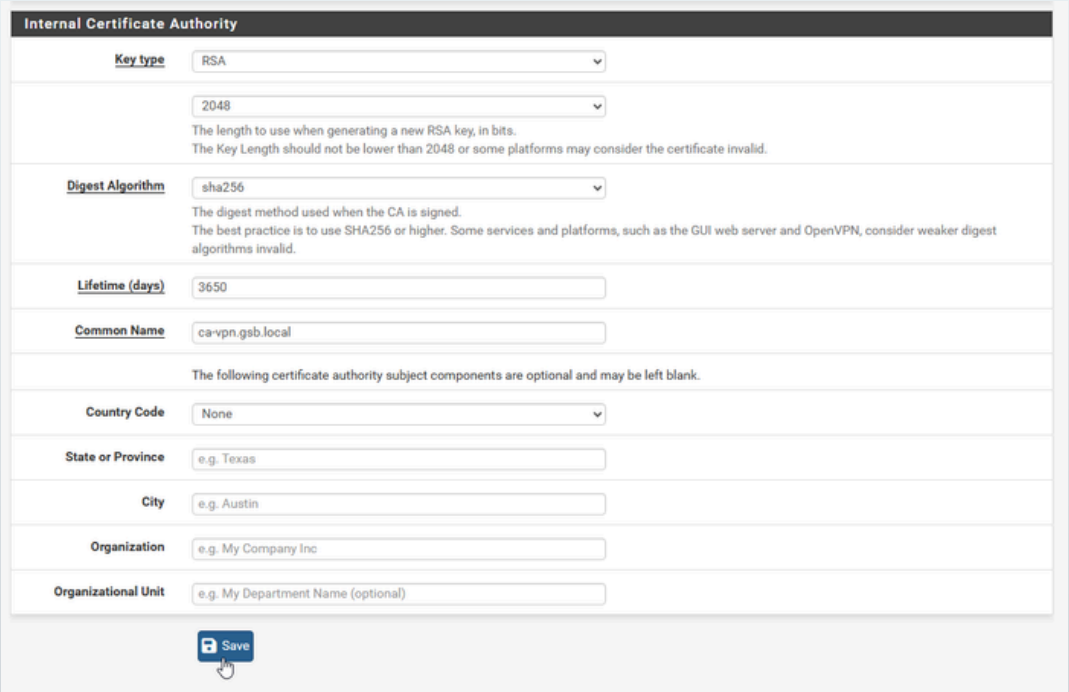


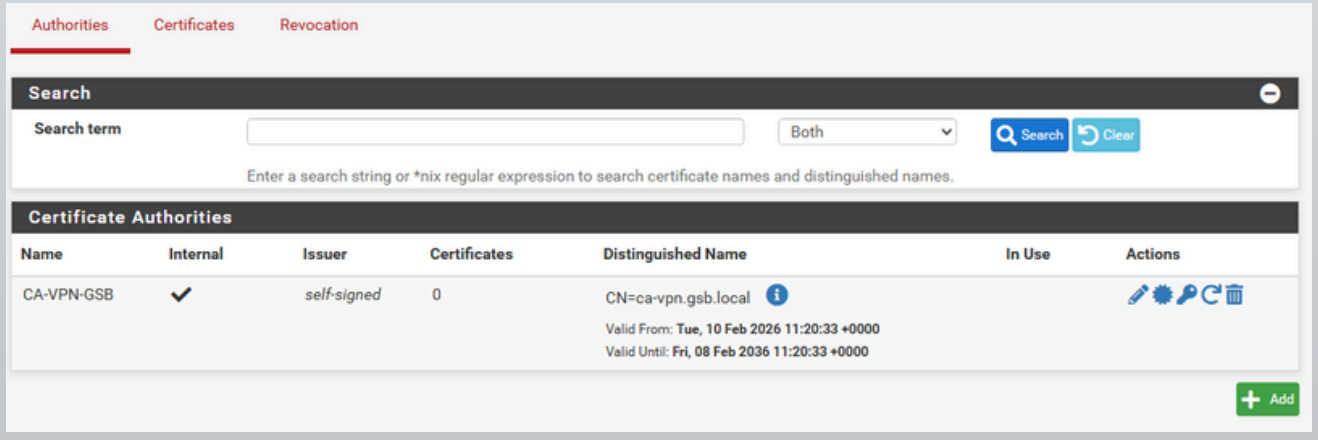
- Cette autorité va signer tous les futurs certificats. Elle est la base de notre chaîne de confiance.



- Définition des paramètres nécessaires a l'autorité.



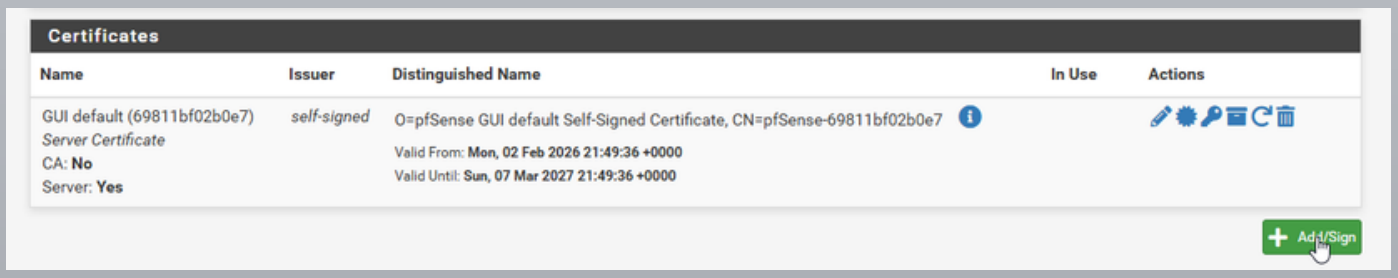


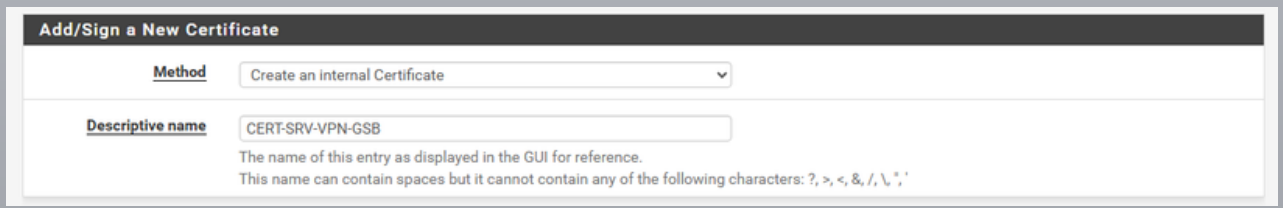


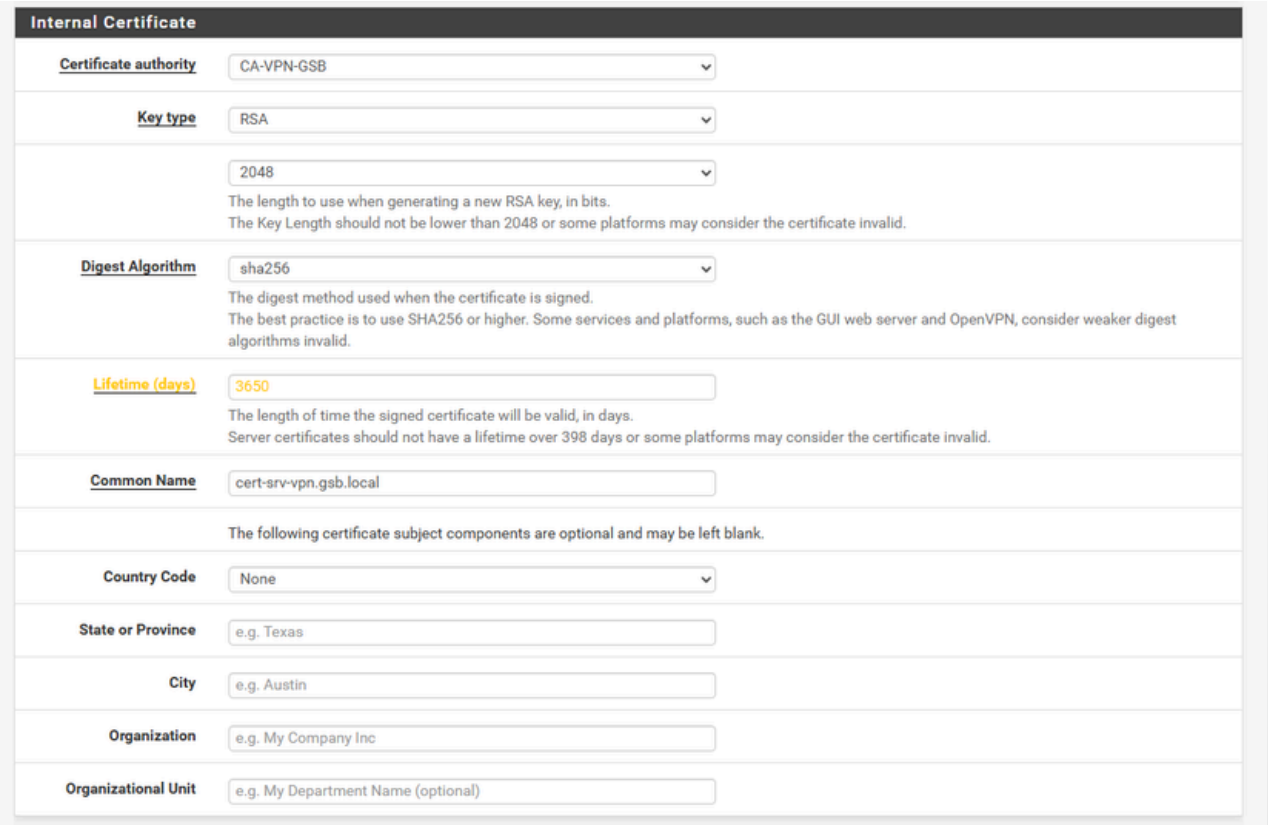
- Autorité de certificat créée.

2.1.2. **Création du Certificat Serveur**

- Configuration du certificat serveur.

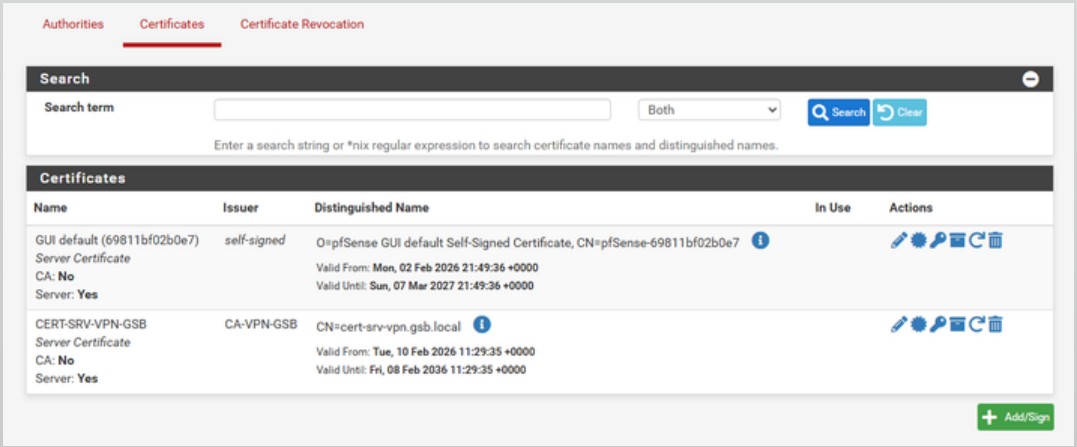






- Définition du certificat en 'Server Certificate'

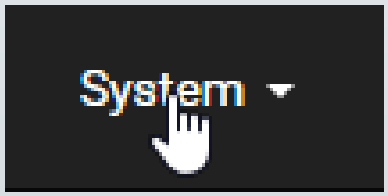
- Certificat de serveur créé.

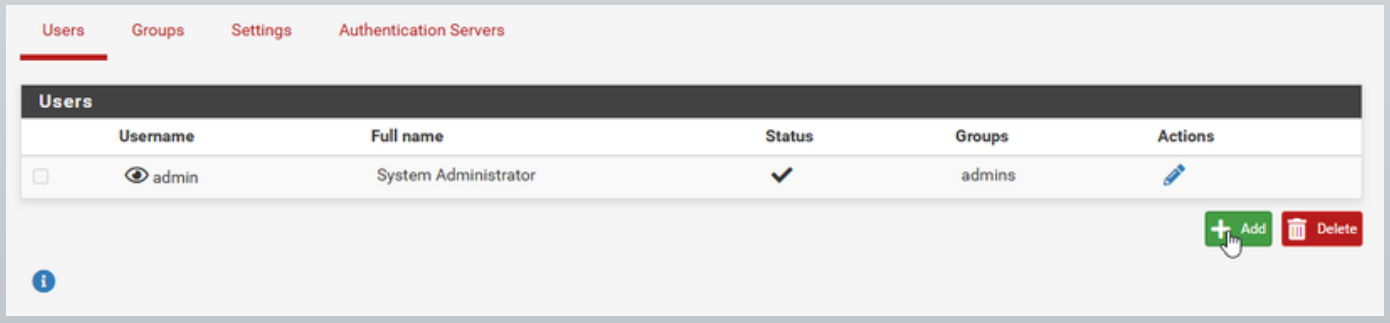


- Ce certificat permet au pfSense de prouver son identité aux clients qui tentent de se connecter

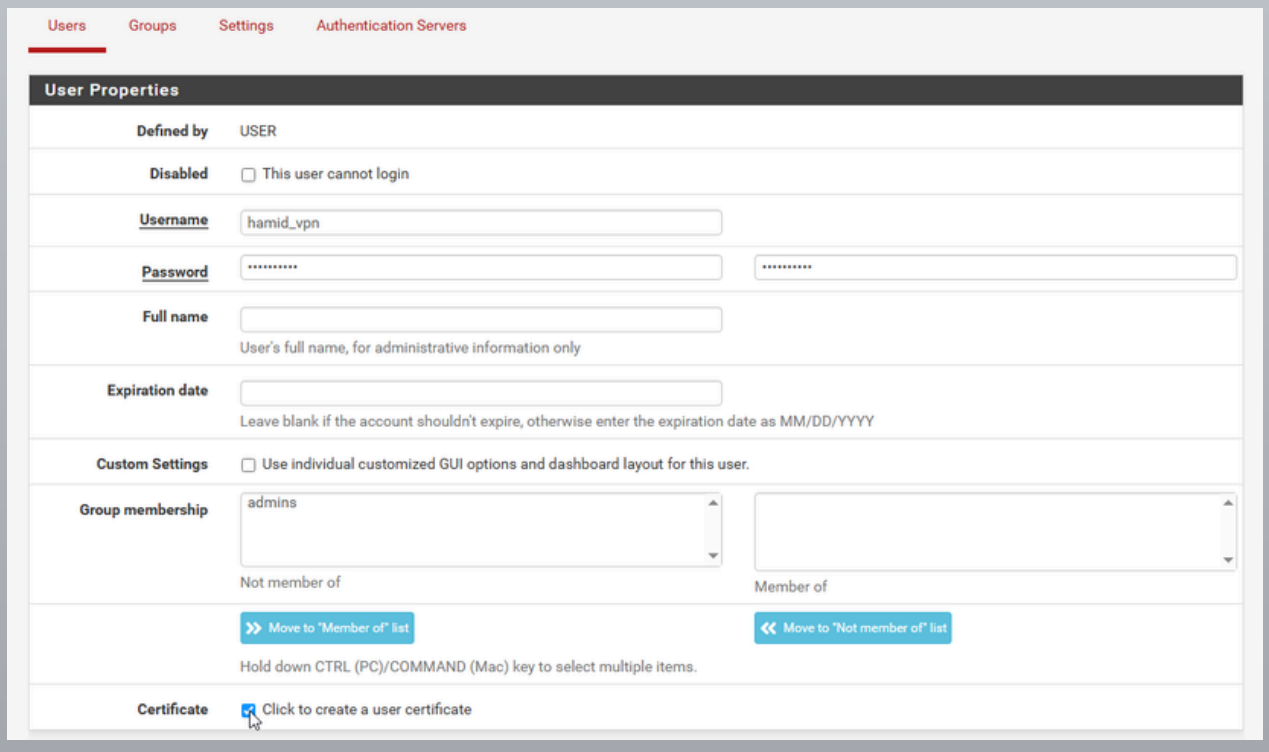
2.1.3. **Création de l'Utilisateur et de son Certificat Client**

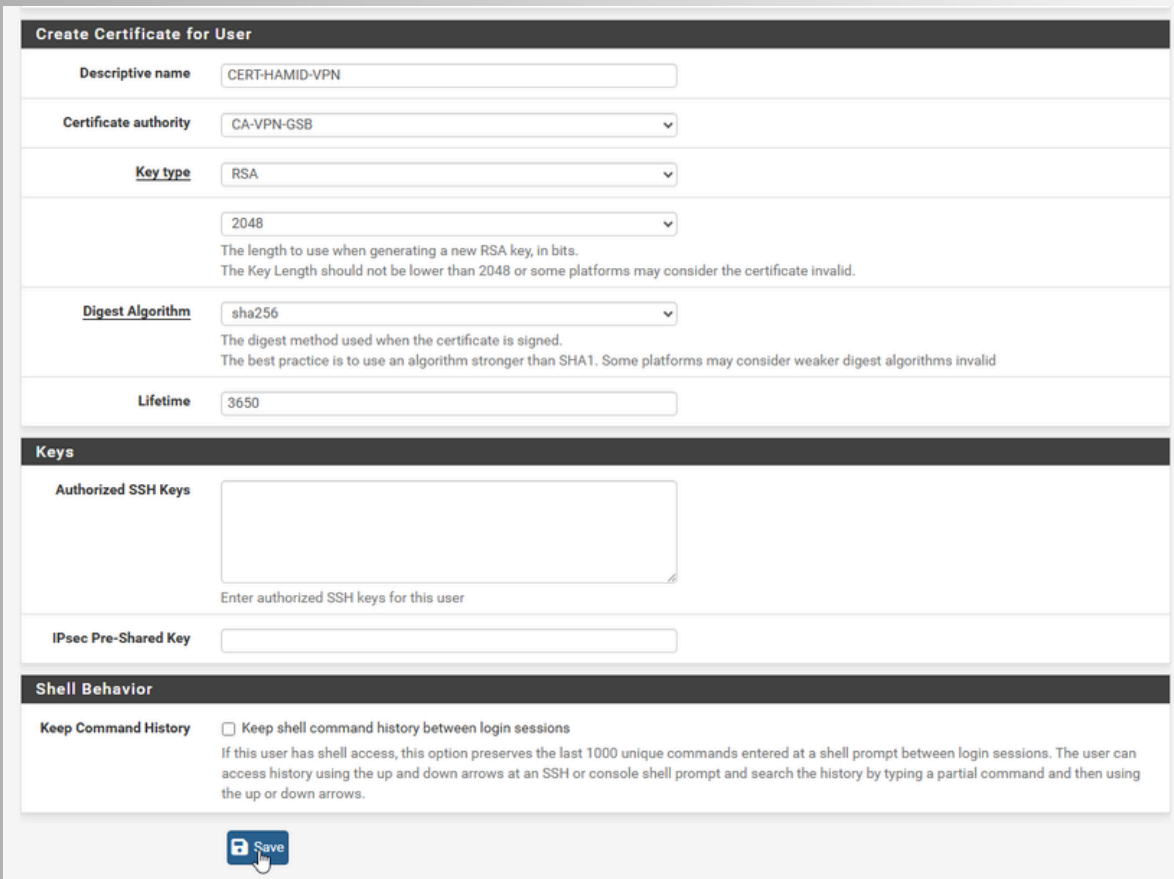
- Configuration de l'utilisateur "hamid_vpn" ainsi que de la liaison avec l'autorité de certificat



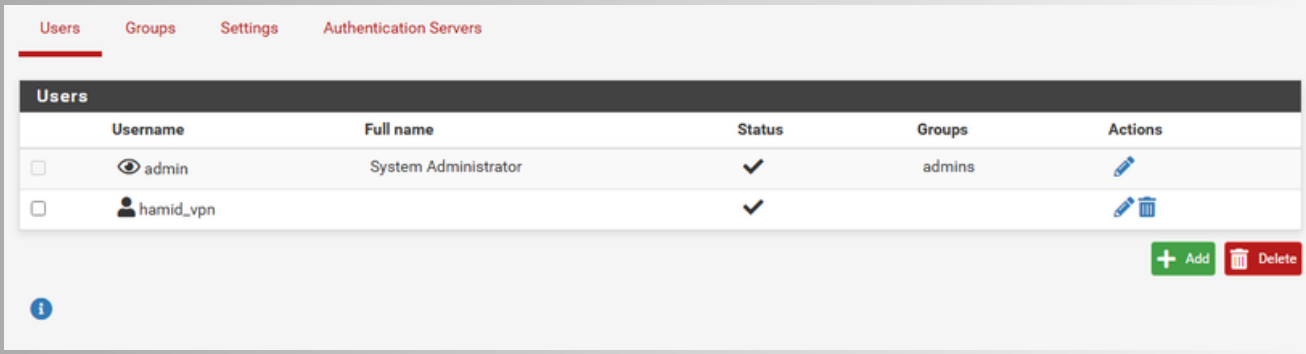


- Bien cocher le case "Certificate" pour que la liaison utilisateur autorité soit faite.



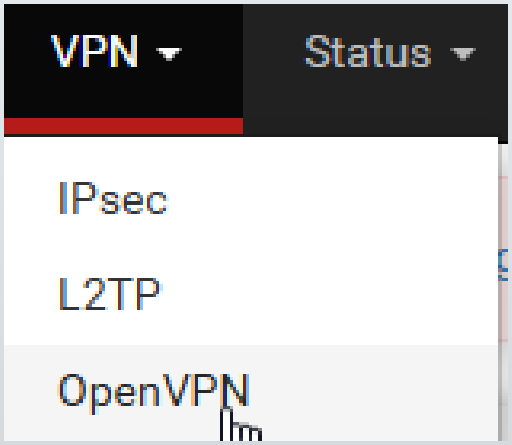


- Utilisateur bien créé.



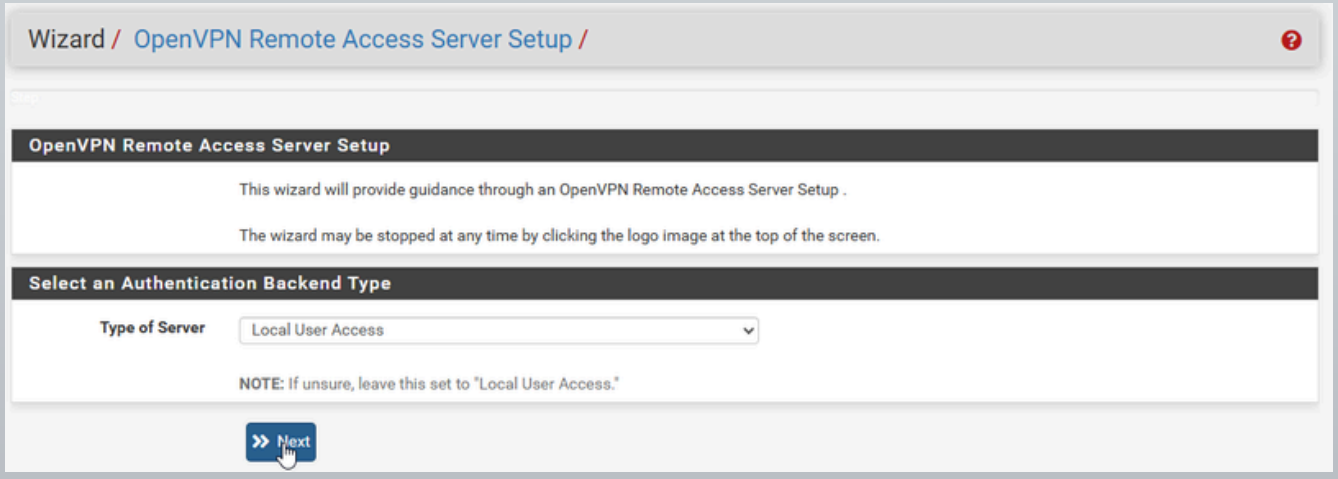
- Chaque utilisateur possède son propre certificat X.509. Si un employé quitte l'entreprise, on peut révoquer son certificat sans bloquer les autres.

2.2. **Configuration du Serveur OpenVPN**

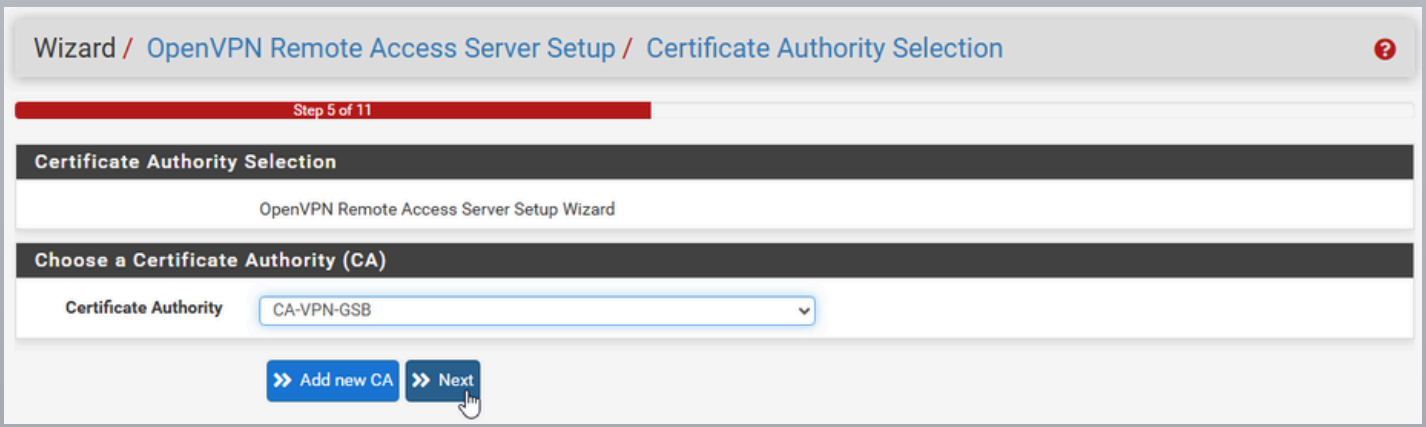


- Accéder au menu “Wizard” dans OpenVPN et configurer l’accès a distance.

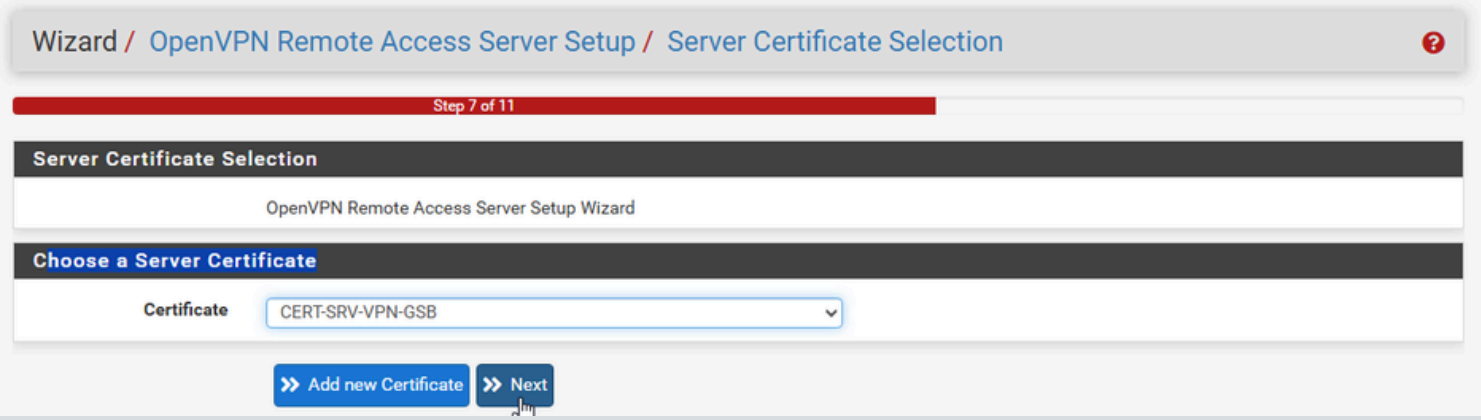
- Choisir “Local User Access”.



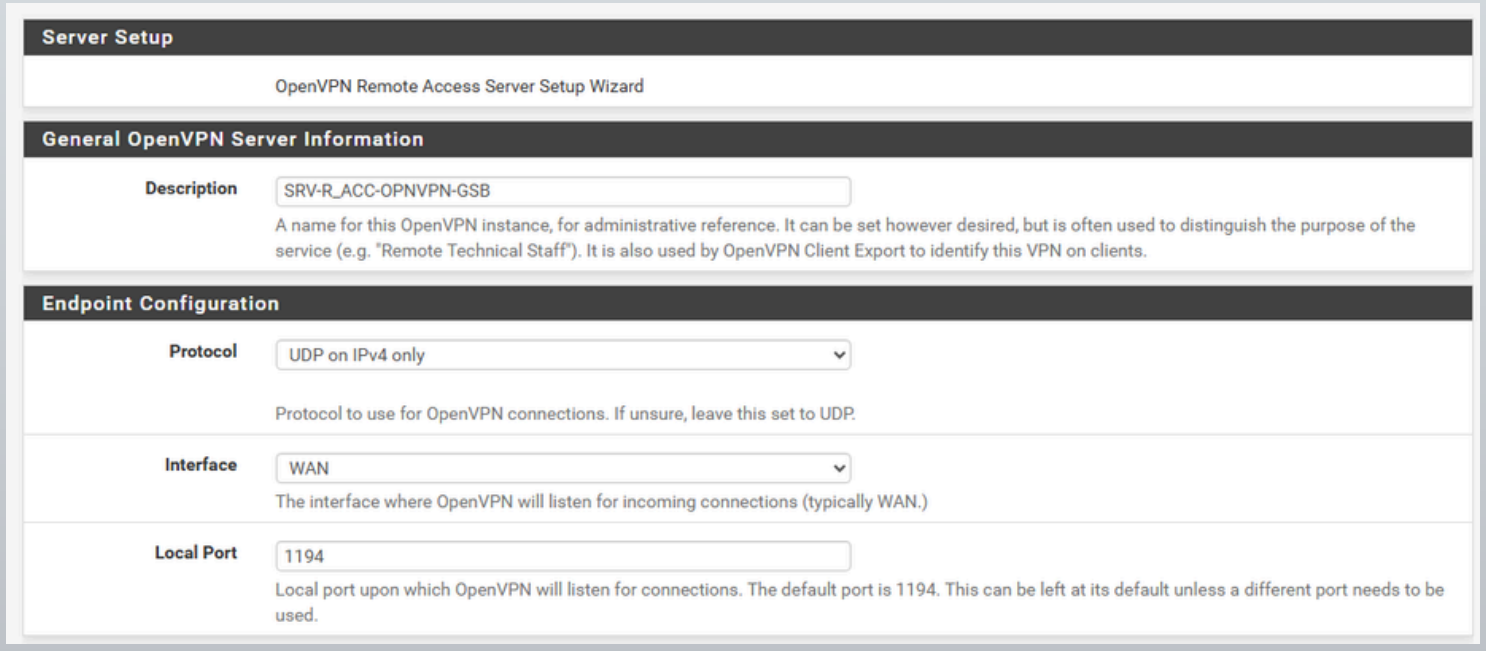
- Sélectionner l’autorité de certificat.



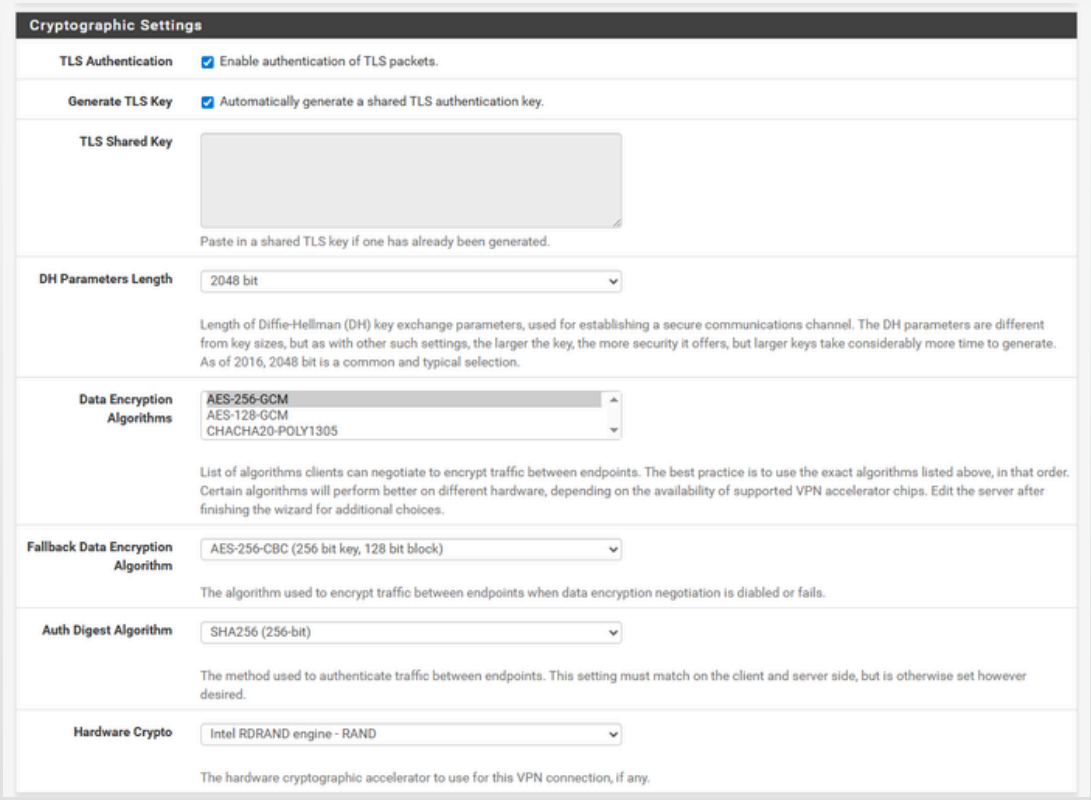
- Ensuite sélectionner le certificat de serveur.



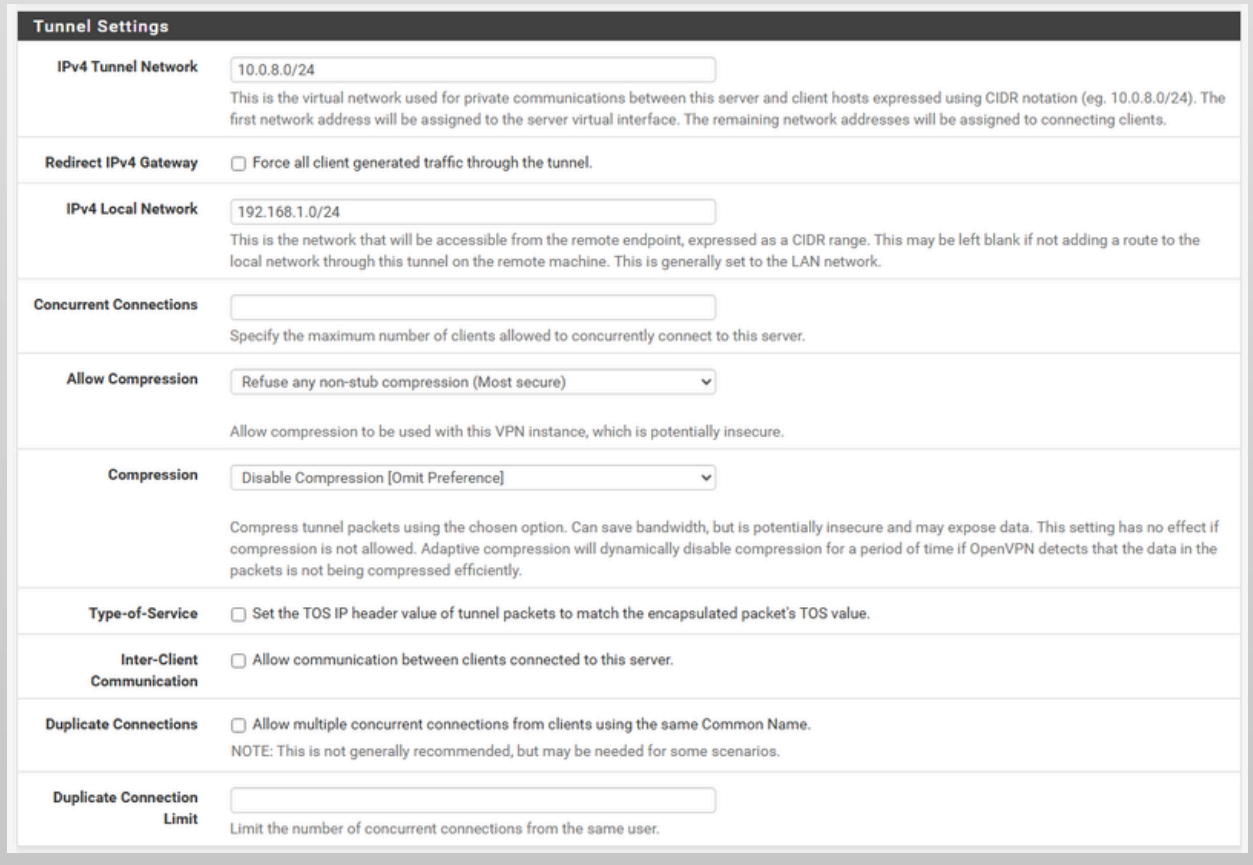
- Choix du Protocol “UDP” pour plus de performances.

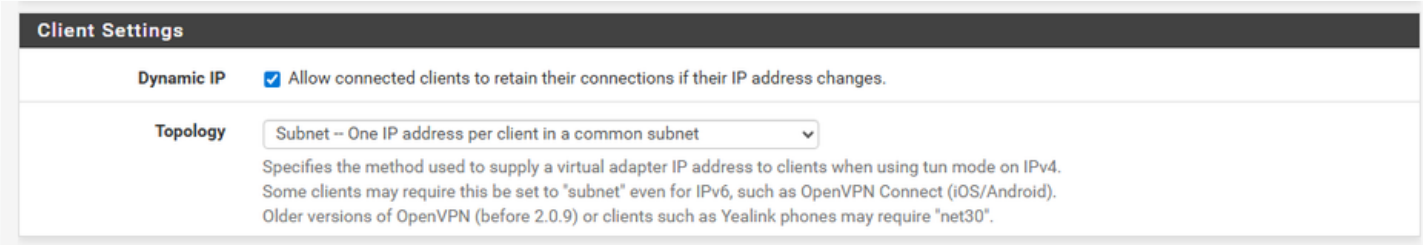


- Pour garantir la confidentialité des flux, j'ai implémenté l'algorithme de chiffrement AES-256-GCM. Ce choix permet d'allier une sécurité de niveau industriel à une haute performance de transfert, essentielle pour l'accès aux dossiers partagés du serveur GSB.

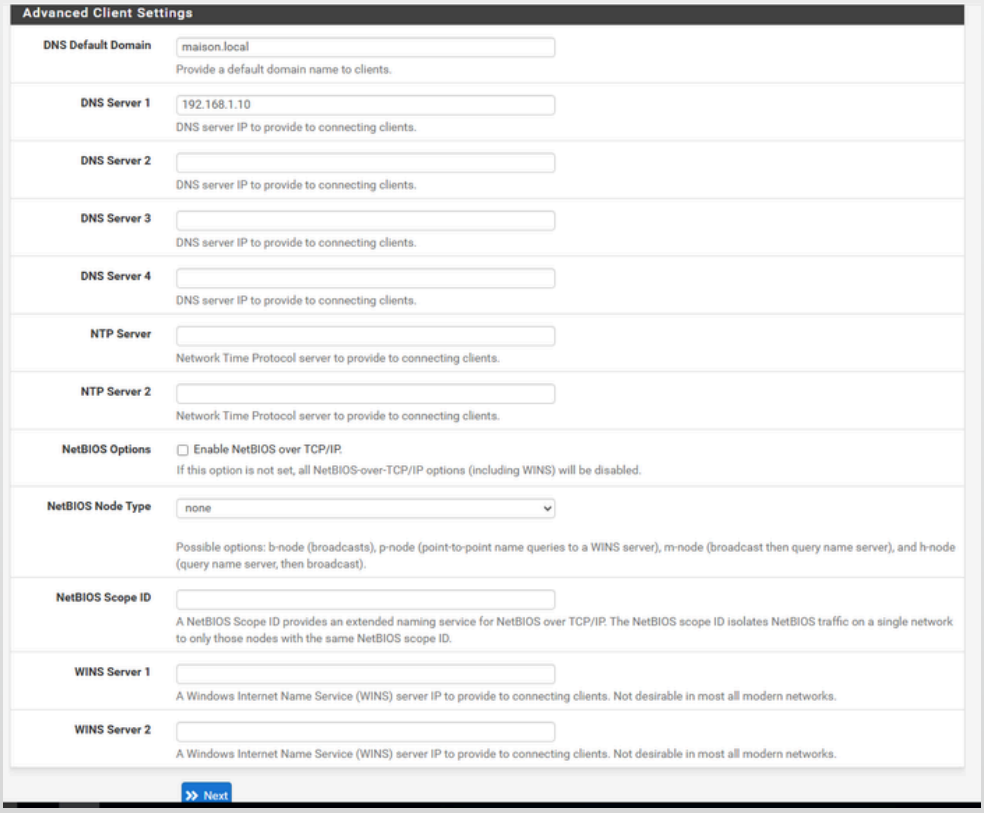


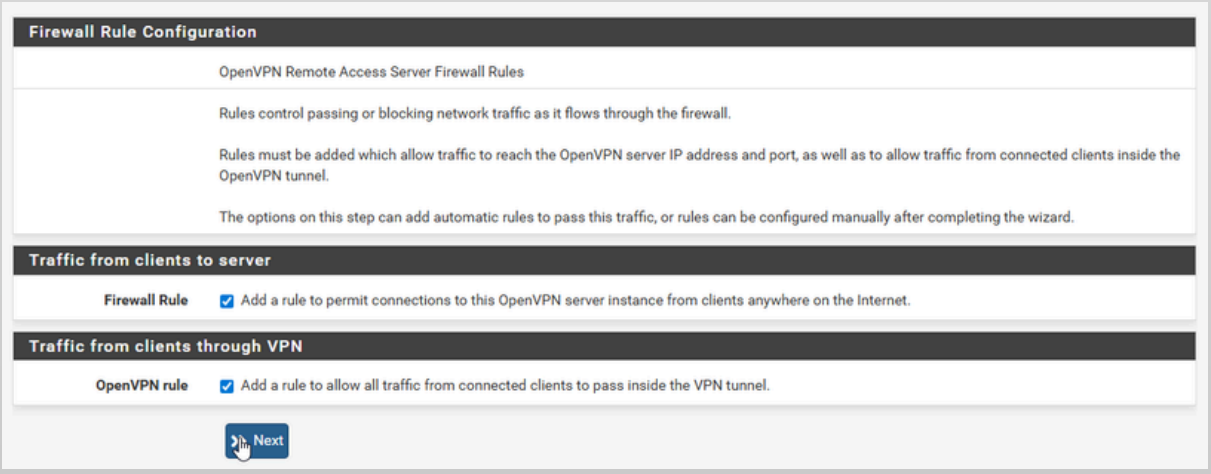
- Paramétrage des paramètres tunnel (liaison vers le pfsense).



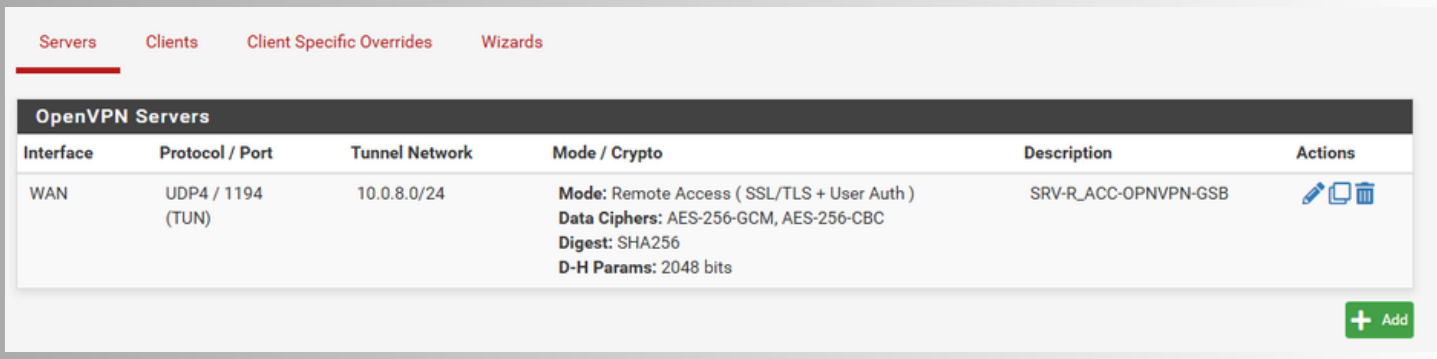


- Paramétrage des paramètres clients avancés (liaison vers le serveur).
- En renseignant le suffixe DNS et l'adresse du contrôleur de domaine dans les paramètres du serveur VPN, je permets aux utilisateurs nomades de bénéficier de la résolution de noms interne, exactement comme s'ils étaient au bureau.



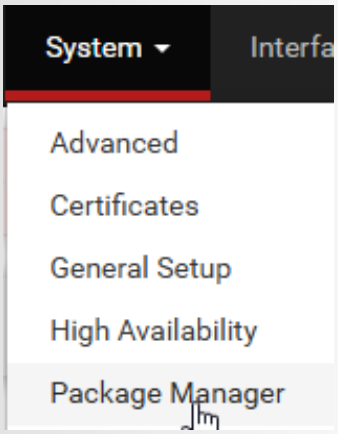


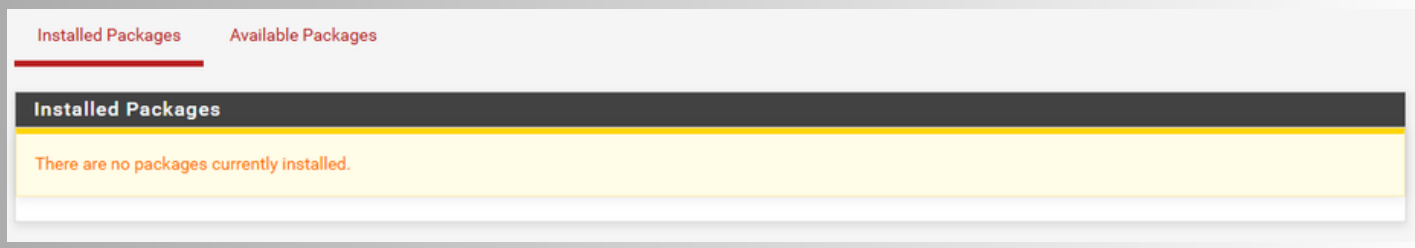
- Server OpenVPN créé.



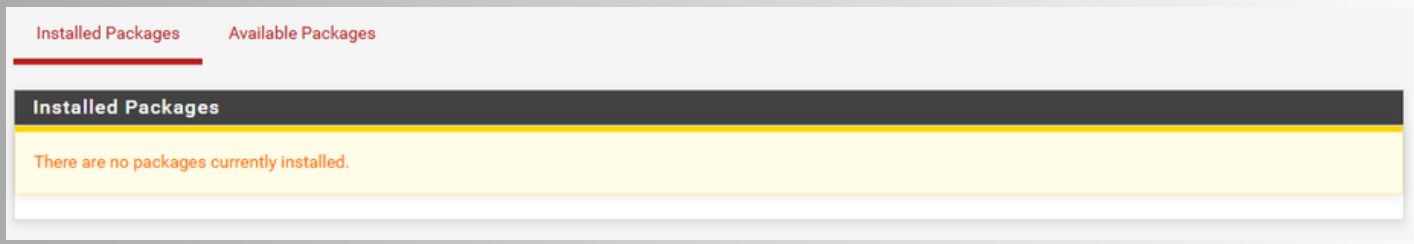
2.3. Gestion des accès utilisateurs

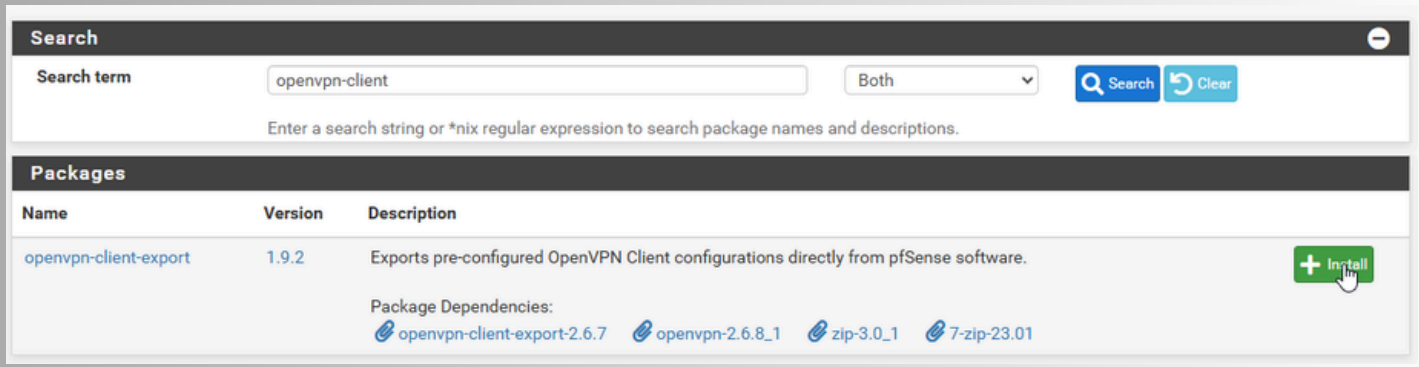
2.3.1. Installation de l'outil d'exportation.

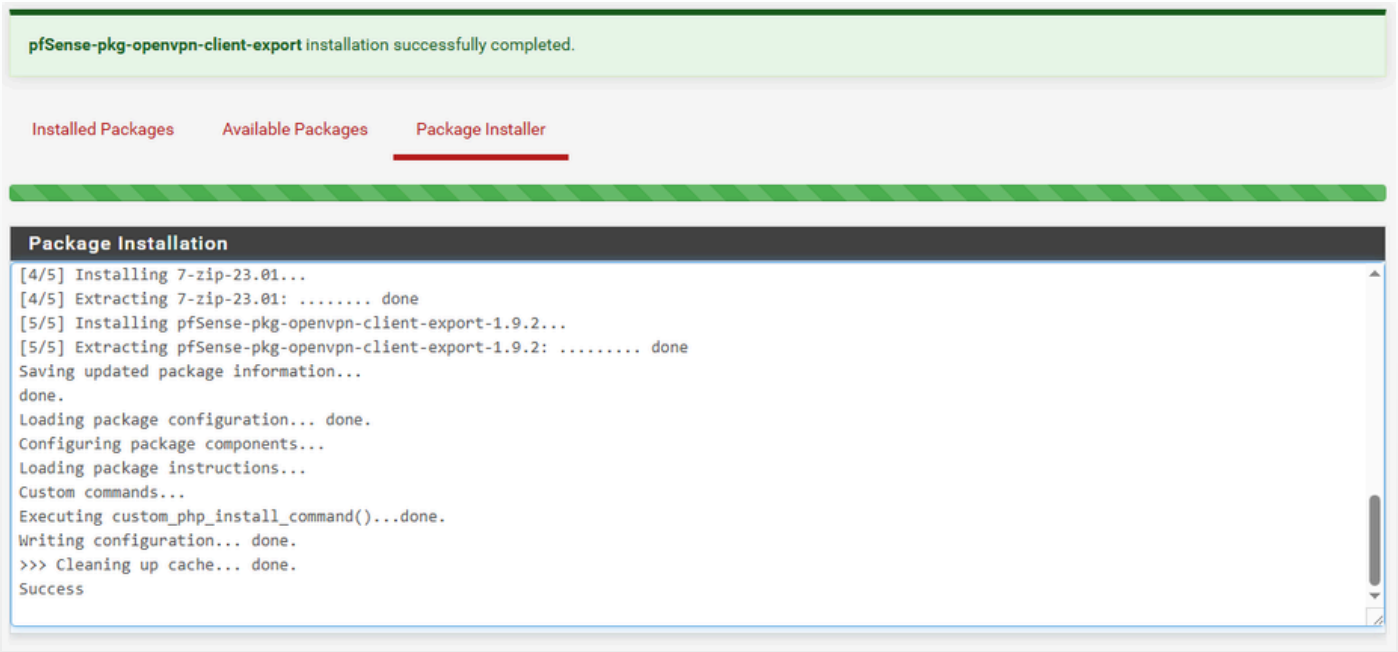


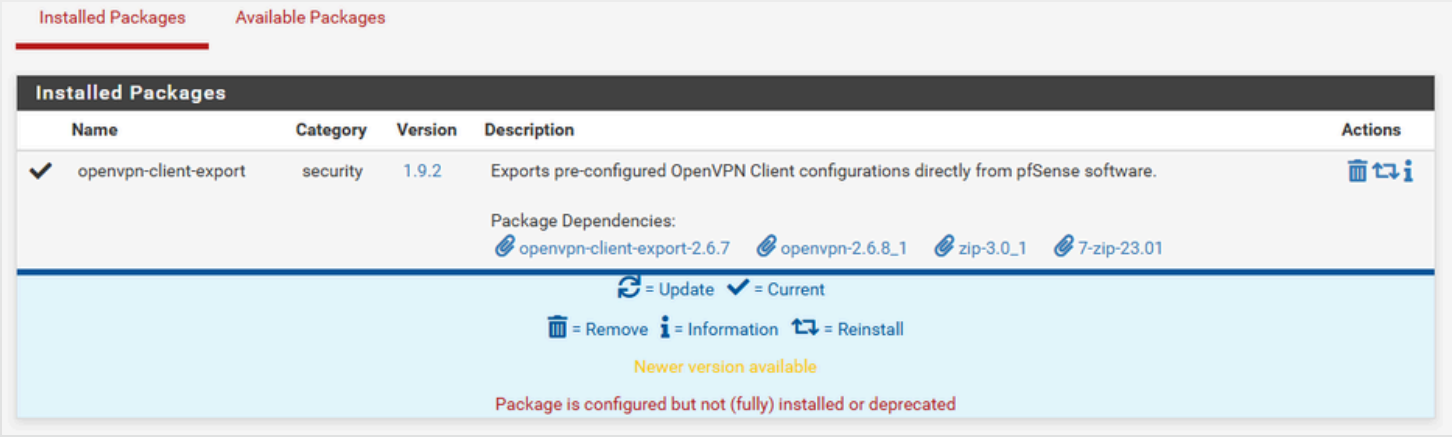


- Installation du packet “openvpn-client-export”



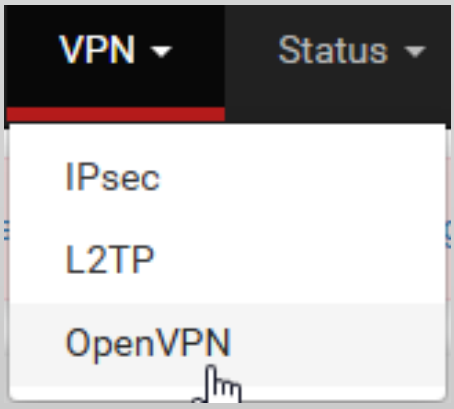




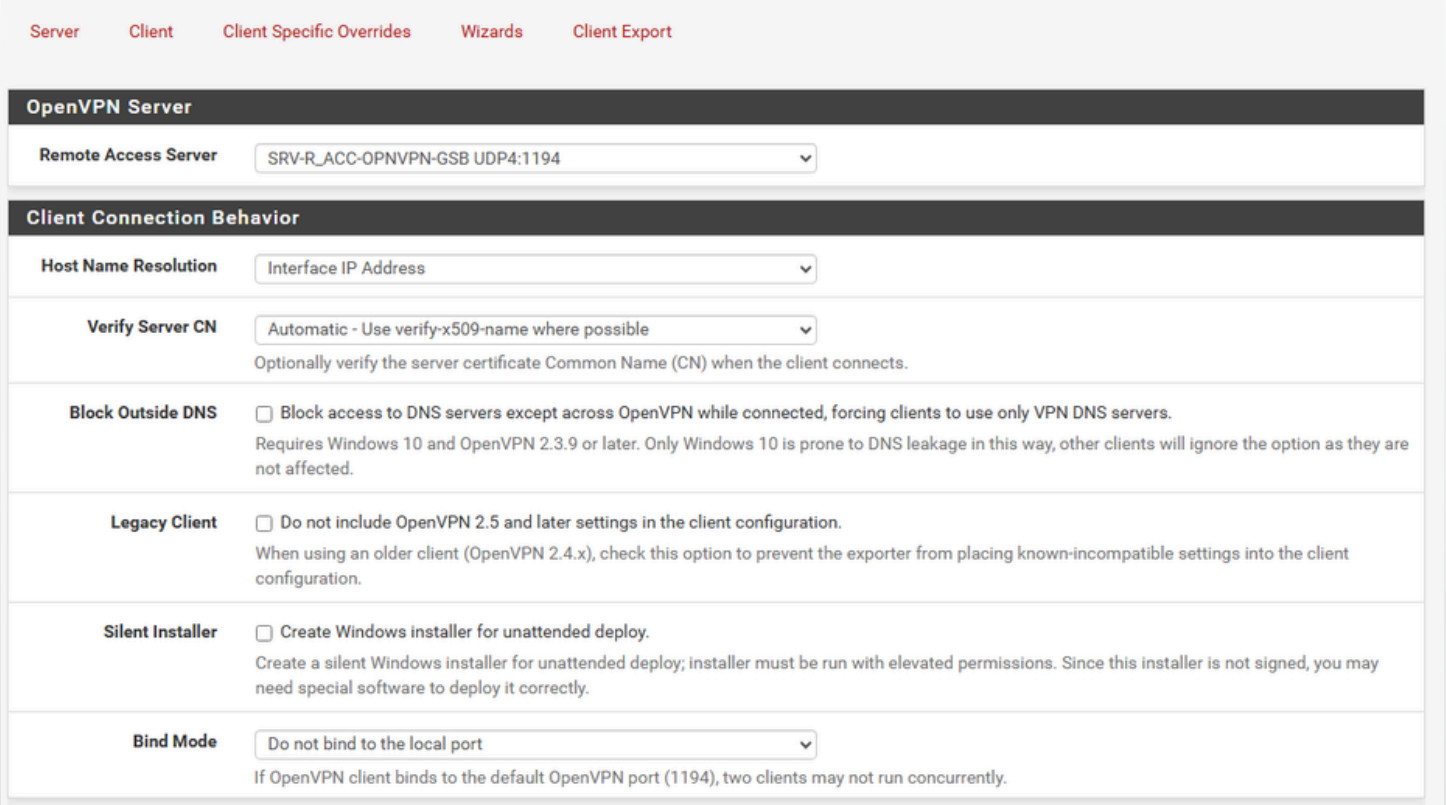


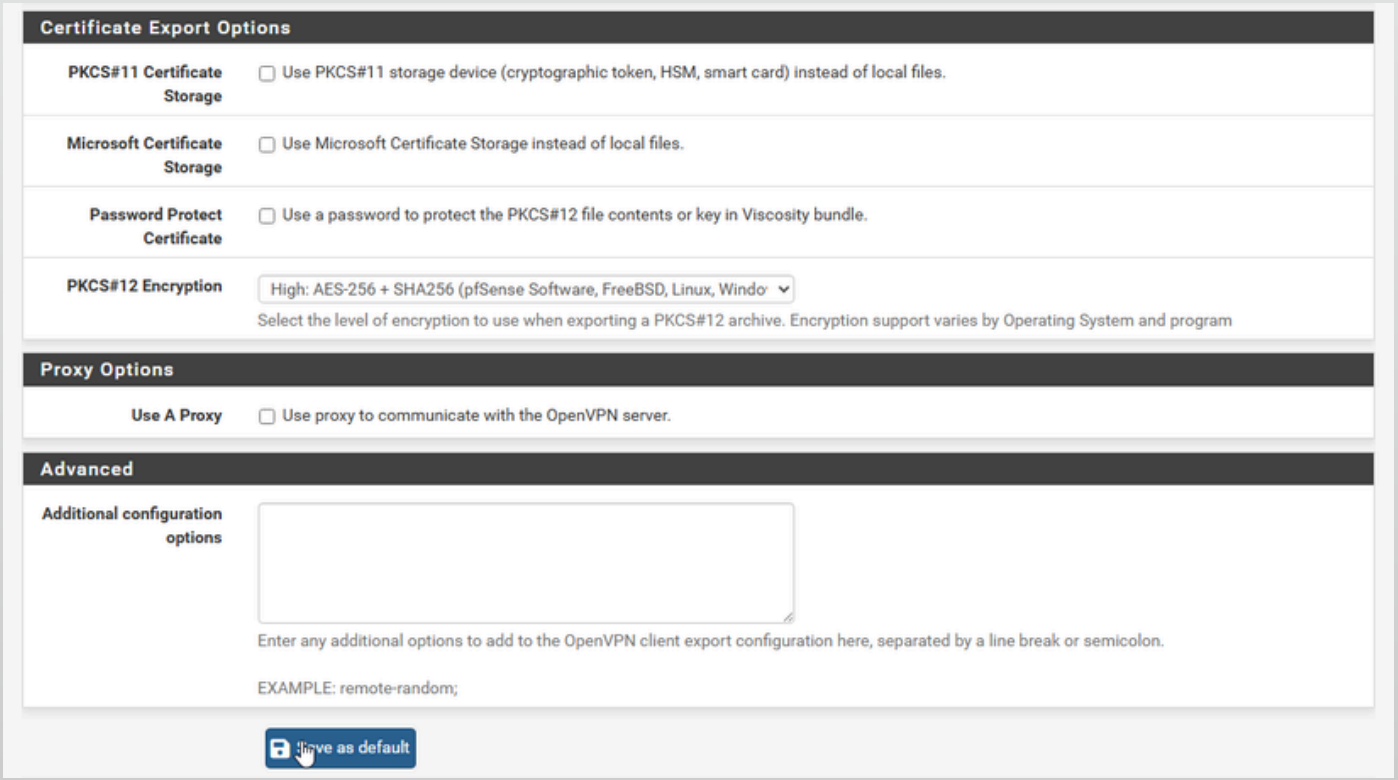
2.3.2. **Configuration de l'exportation**

- Configuration du Client Export

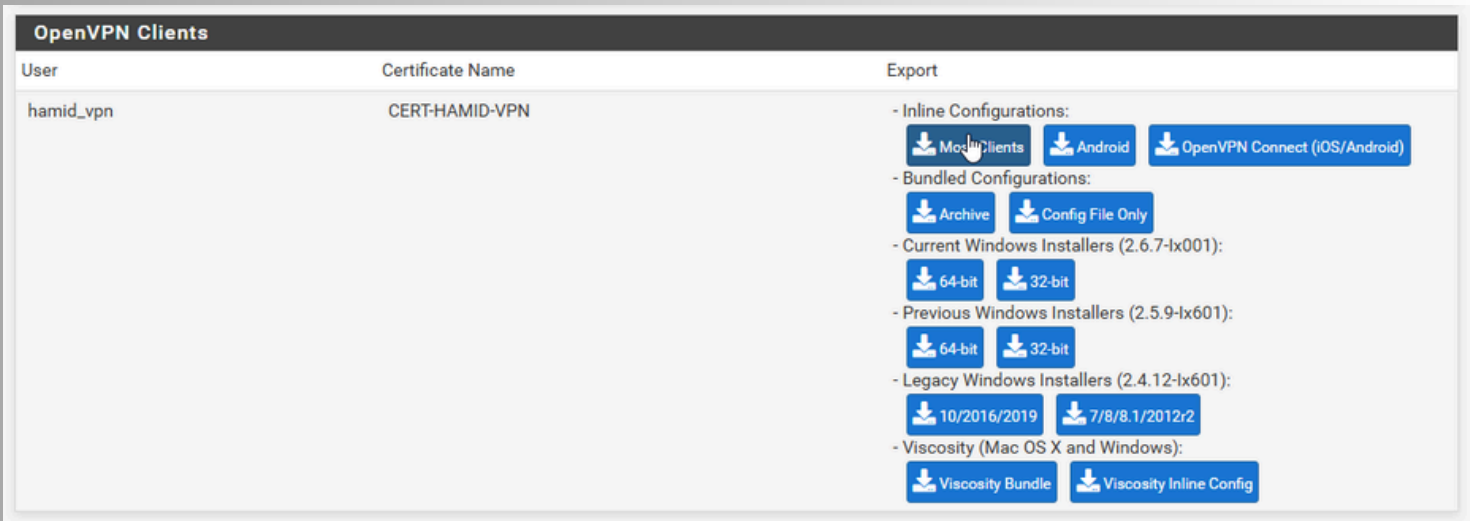


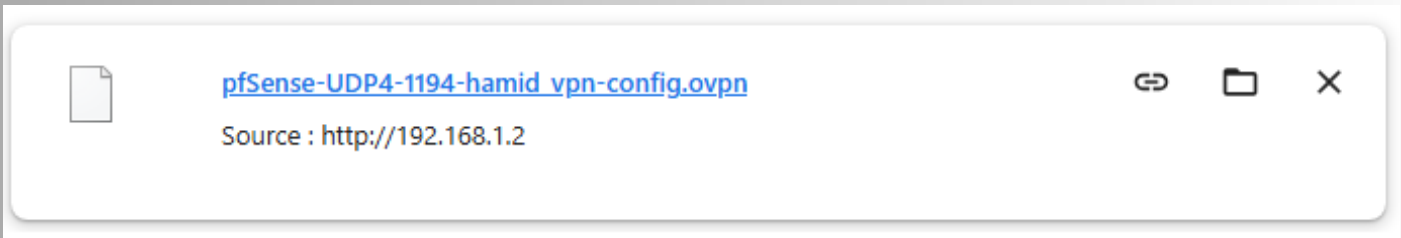
- Mise en relation avec l'interface WAN du pfSense (là où le VPN ira chercher l'internet)





2.3.3. **Téléchargement du fichier pour l'utilisateur**

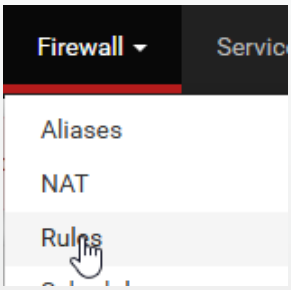


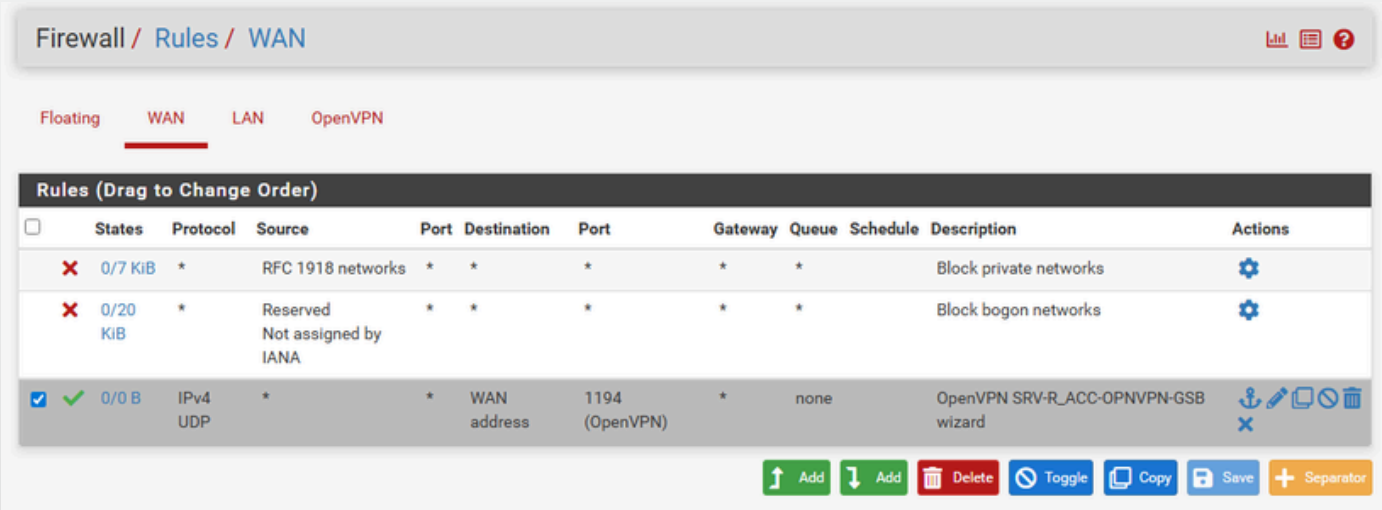


- L'exportation du client permet de regrouper en un seul fichier sécurisé la configuration du tunnel, l'adresse de la passerelle et le certificat X.509 de l'utilisateur. Ce procédé simplifie le déploiement sur les postes nomades tout en garantissant que seul l'utilisateur possédant ce fichier et son mot de passe peut initier la connexion.

2.4. Règles de Pare-feu (Firewall Rules)

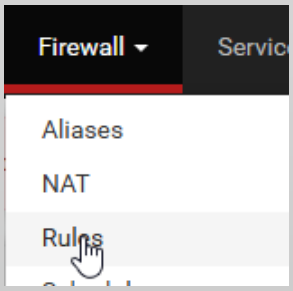
2.4.1. La règle sur l'interface WAN



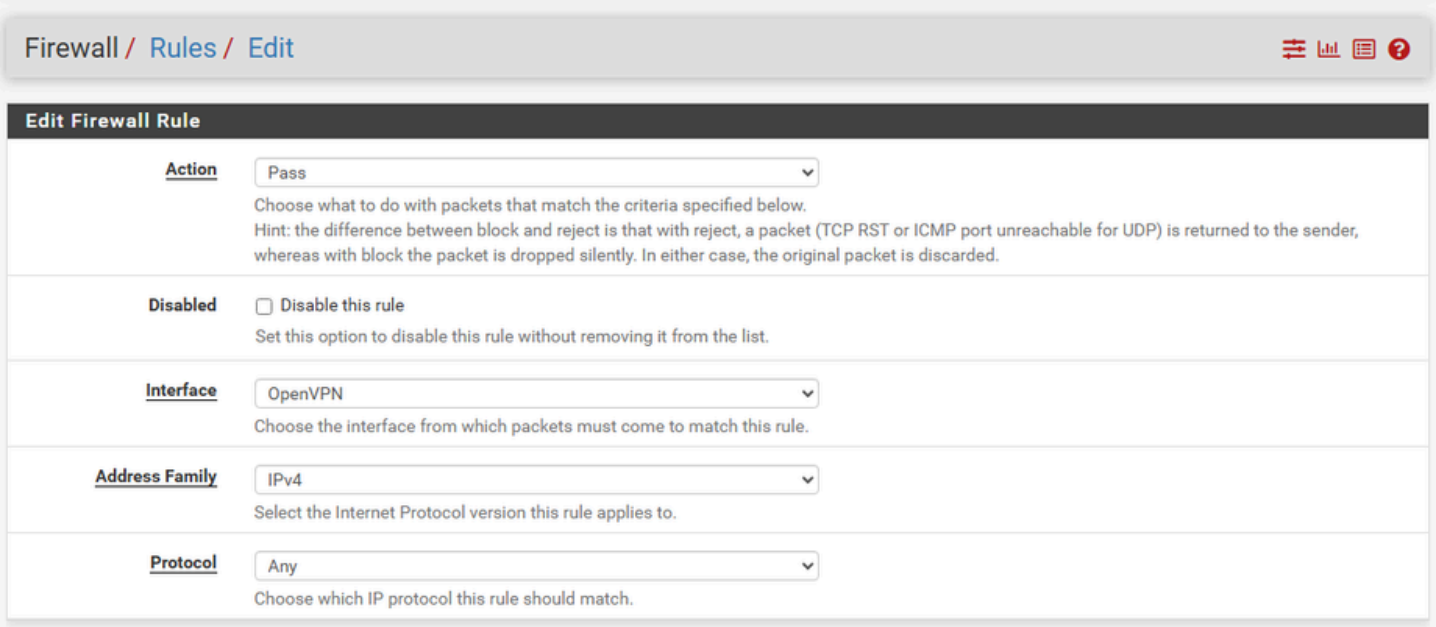


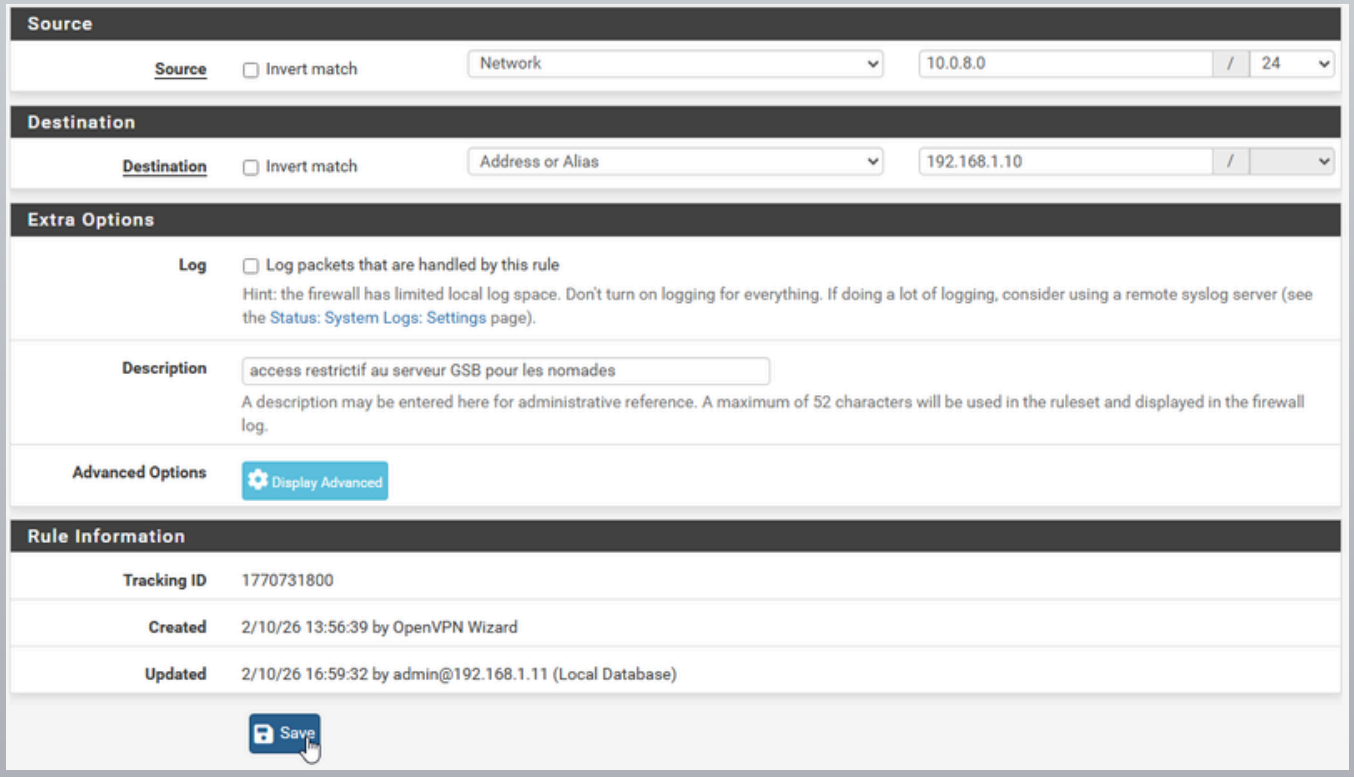
- La règle a bien été créée.
- Cette règle est indispensable pour permettre aux paquets chiffrés venant d'Internet d'atteindre le service OpenVPN du bastion.

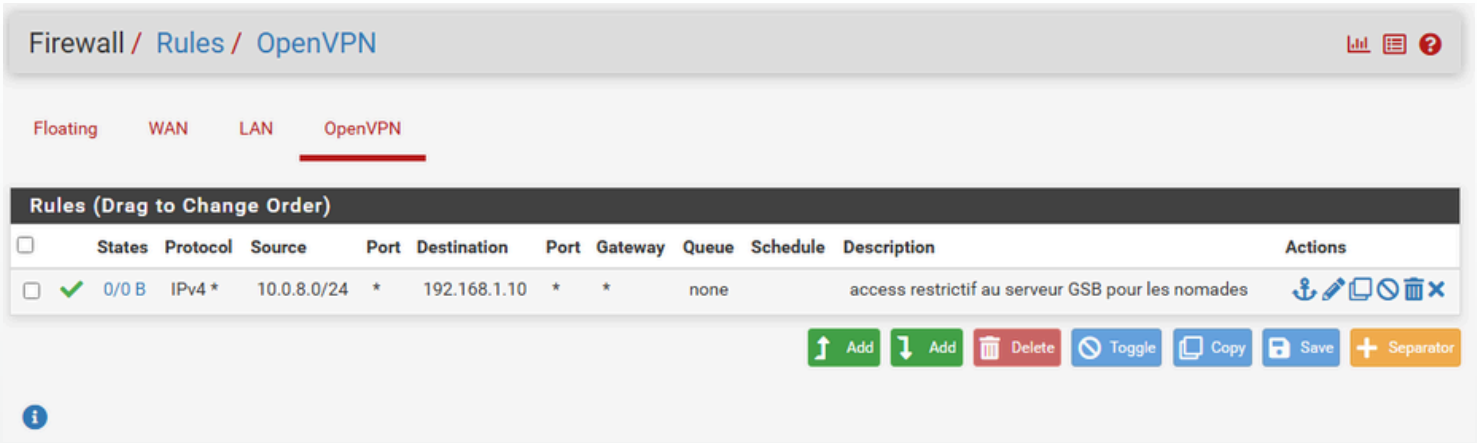
2.4.2. La règle sur l'interface OpenVPN (Le contrôle interne)



- Pour renforcer la sécurité, le filtrage sur l'interface OpenVPN restreint les flux des utilisateurs nomades vers les seules ressources nécessaires (serveur de fichiers), interdisant ainsi l'accès à l'administration du pare-feu ou aux autres équipements du LAN.







- OpenVPN finaliser.

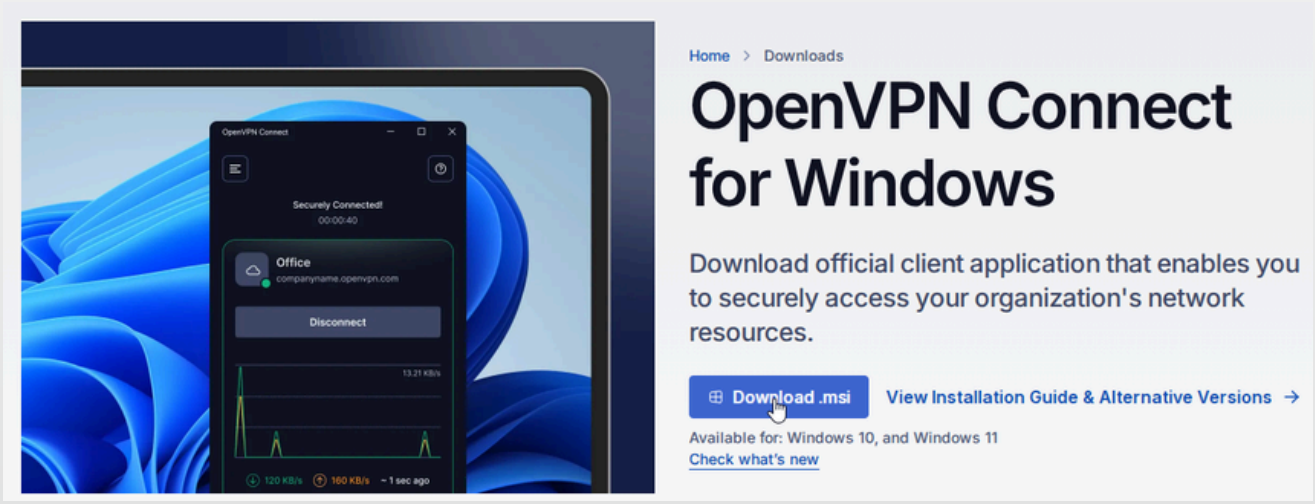
3. TESTS ET RECETTES :

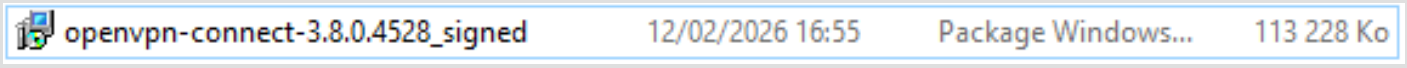
3.1. TESTS ET VÉRIFICATIONS

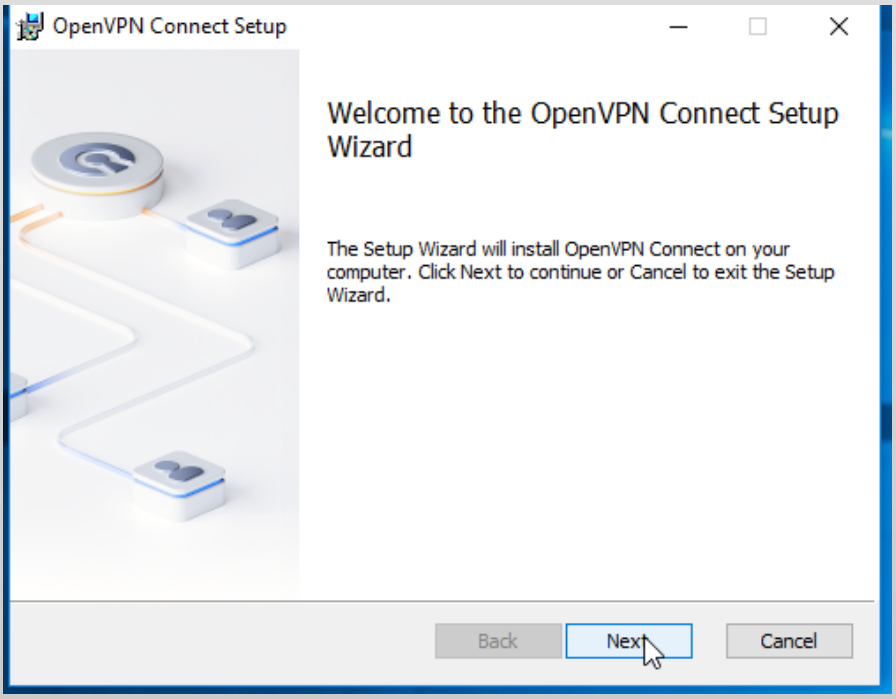
3.1.1. Vérification de l'établissement du tunnel

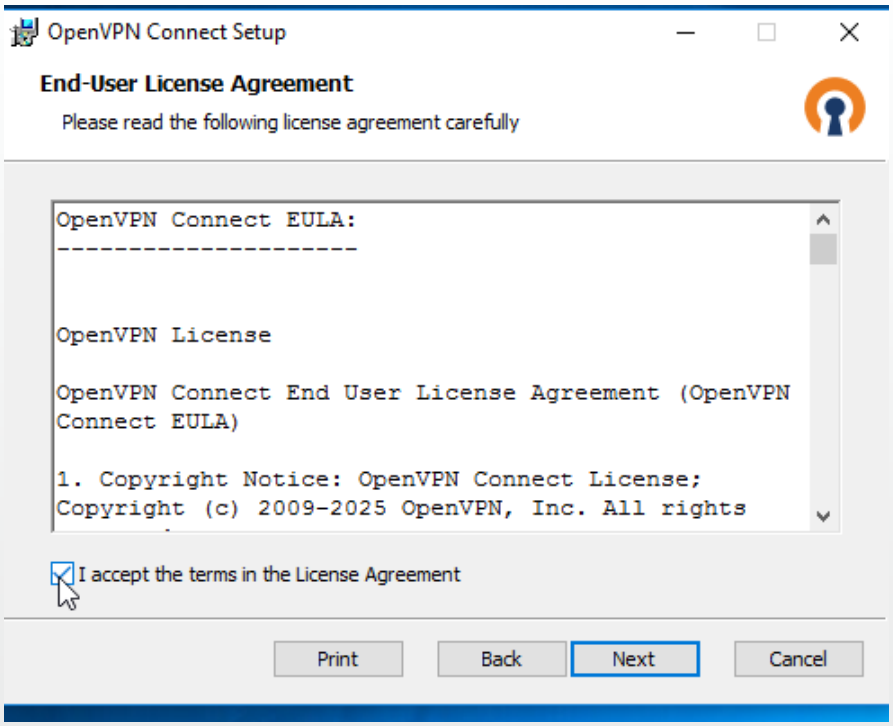
- Côté client :

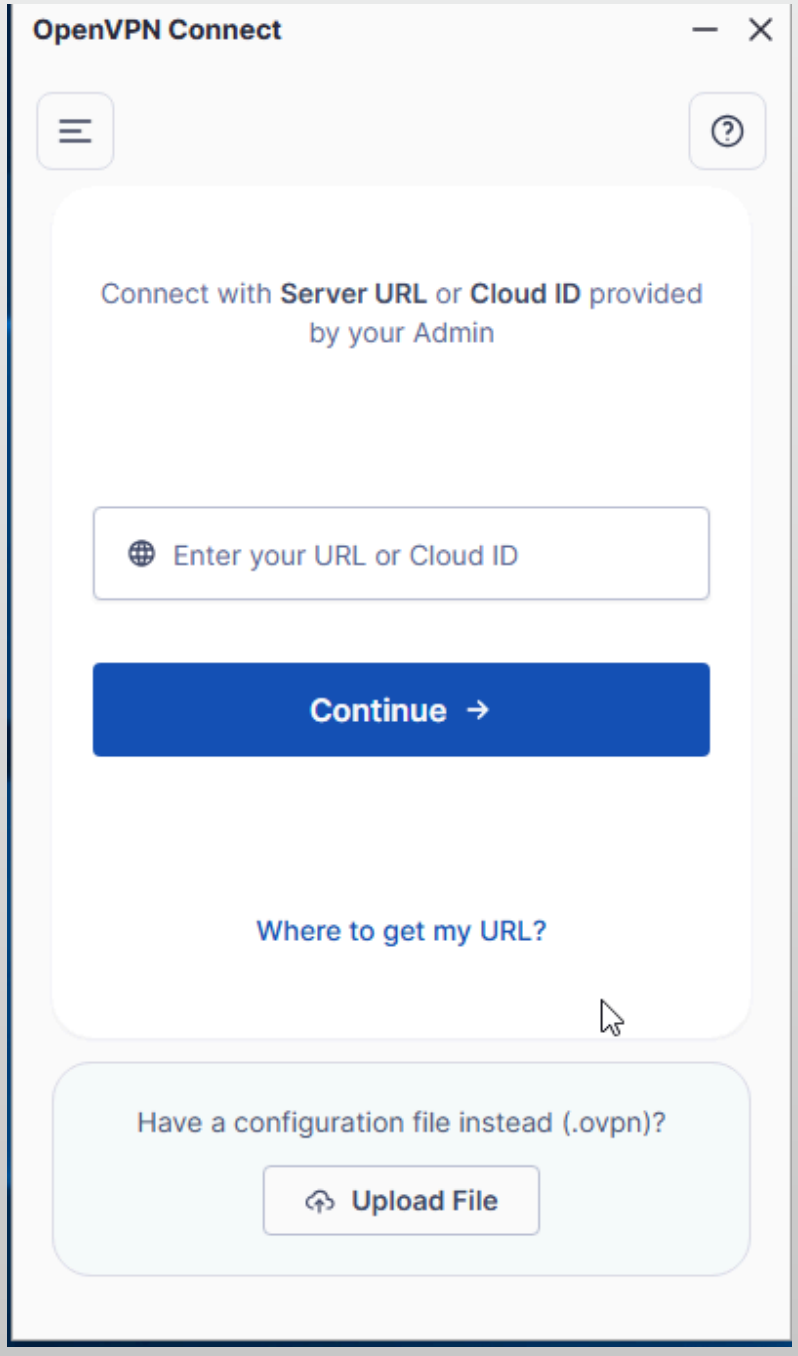
→ Installer OpenVPN Connect sur la machine Windows 10



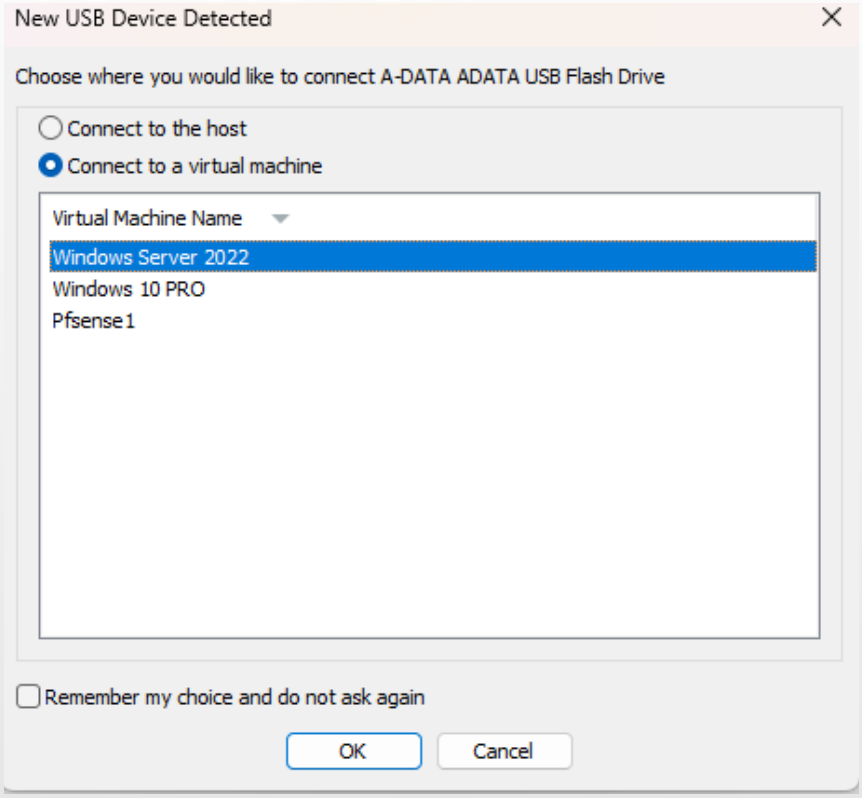


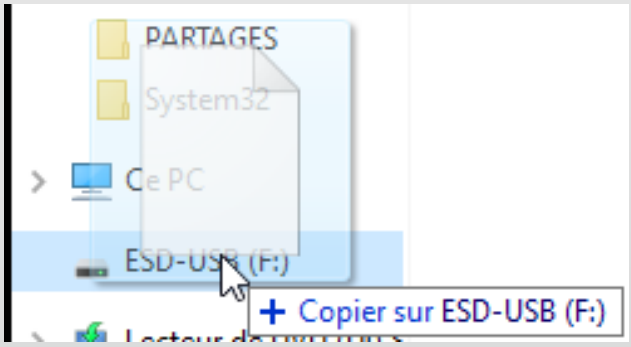



OpenVPN Connect Setup
End-User License Agreement
Please read the following license agreement carefully
OpenVPN Connect EULA:
OpenVPN License
OpenVPN Connect End User License Agreement (OpenVPN Connect EULA)
1. Copyright Notice: OpenVPN Connect License; Copyright (c) 2009-2025 OpenVPN, Inc. All rights
I accept the terms in the License Agreement
Print
Back
Next
Cancel

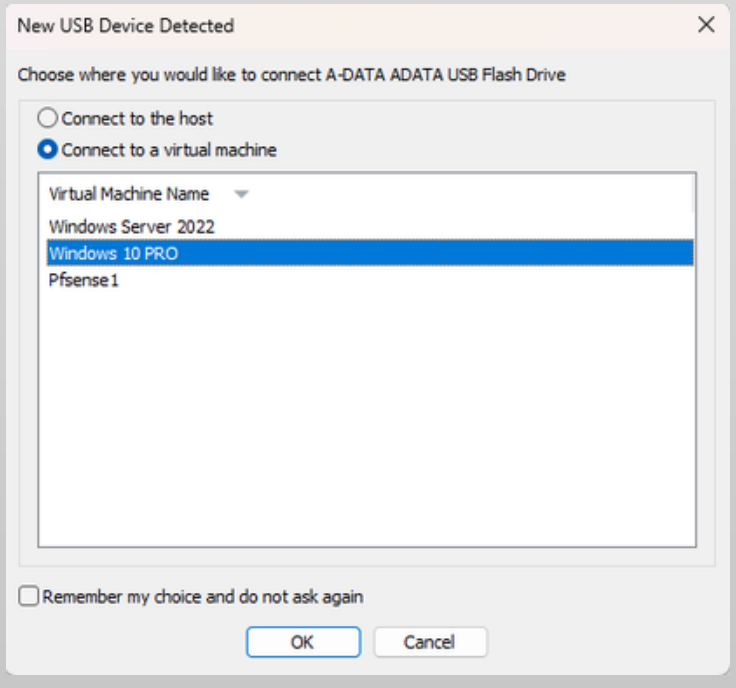

OpenVPN Connect
Connect with Server URL or Cloud ID provided by your Admin
Enter your URL or Cloud ID
Continue →
Where to get my URL?
Have a configuration file instead (.ovpn)?
Upload File

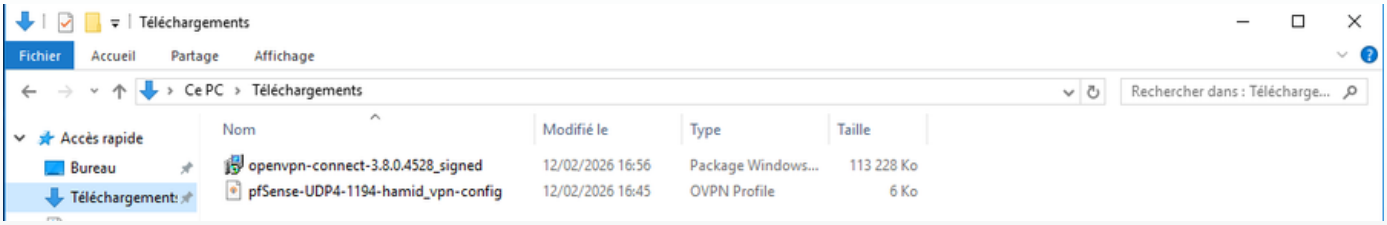
→ Importer le fichier .ovpn depuis le serveur



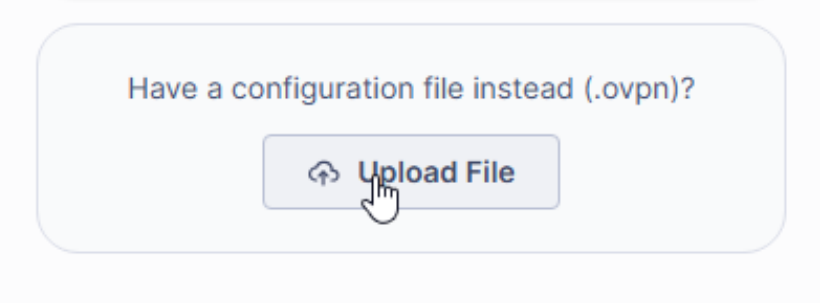


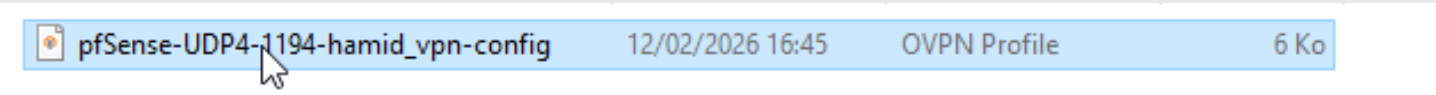
→ Importer le fichier .ovpn sur le windows



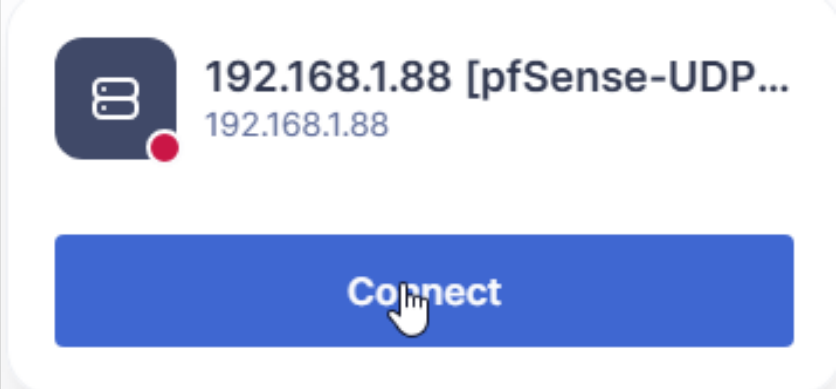


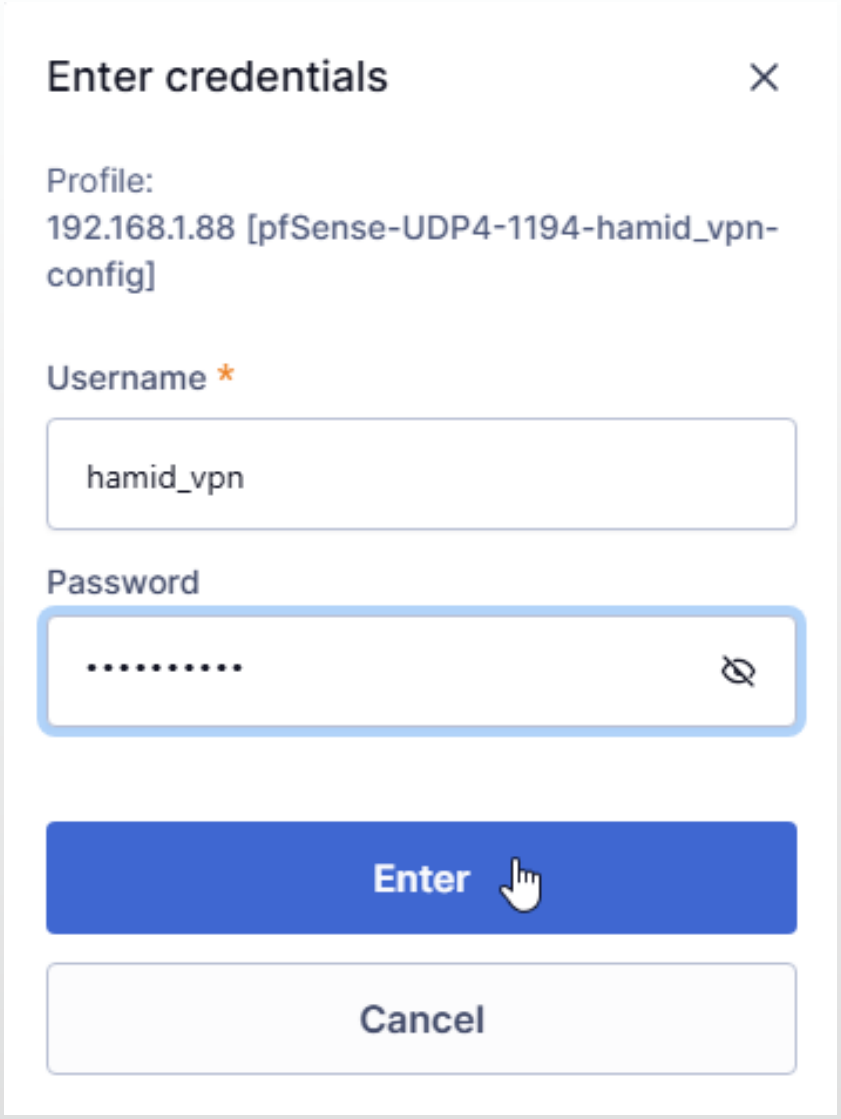
→ Importer le fichier .ovpn sur OpenVPN Connect





→ Connexion au VPN




Enter credentials
Profile:
192.168.1.88 [pfSense-UDP4-1194-hamid_vpn-config]
Username *
hamid_vpn
Password
Enter
Cancel