Déploiement d'un Serveur OpenVPN sous pfSense

Création de l'Autorité de certification locale et configuration des accès utilisateurs

Table des matières

Guide de Configuration : Serveur VPN et Gestion des Certificats sous pfSense

Prérequis

Avant de débuter la configuration, assurez-vous de réunir les éléments suivants :

- Accès à l'interface d'administration de votre pare-feu pfSense.
- Connaissance de l'adresse IP publique de votre interface WAN (ex : 88.185.203.206).
- Identification de la plage IP de votre réseau local M2L, à savoir 172.16.0.0/16.
- Définition du réseau virtuel alloué au tunnel VPN (ex : 10.87.0.0/24), en vous assurant qu'il n'entre pas en conflit avec les réseaux existants.

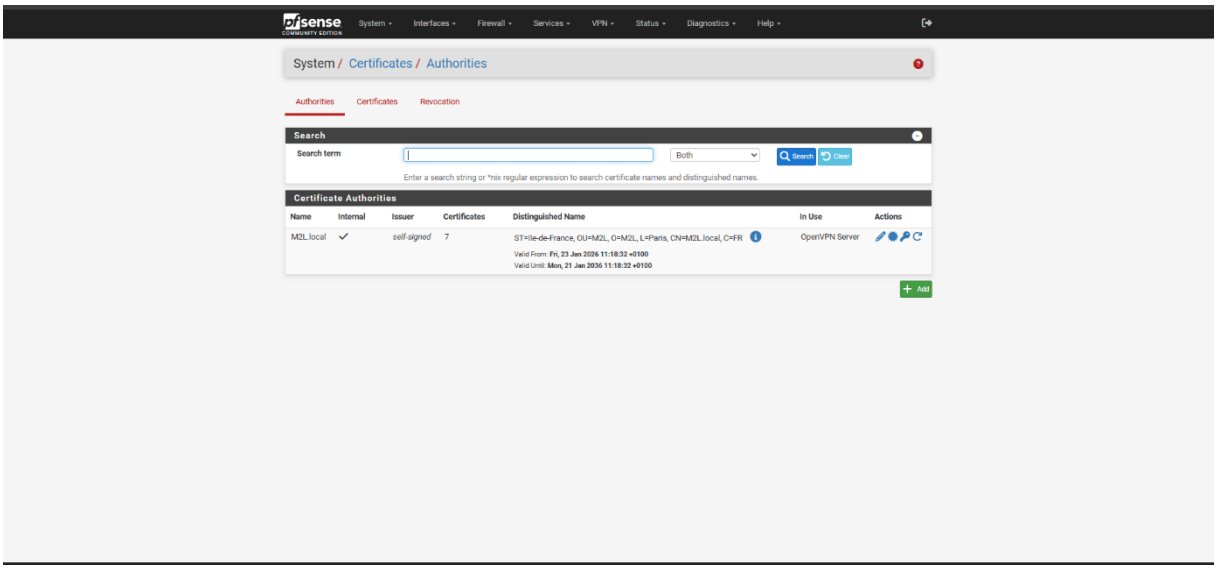
Phase 1 : Création de l'Autorité de Certification (CA) et du Certificat Serveur

Étape 1 : Vérification initiale

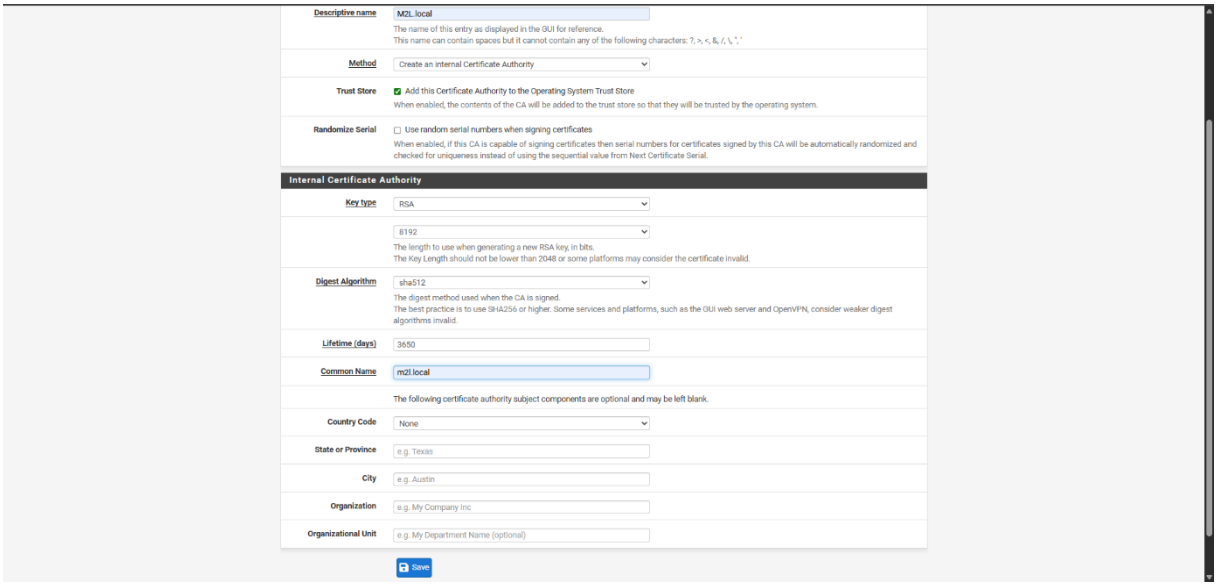
- Accédez au menu **System**, puis **Certificates**.
- Dans l'onglet *Certificates*, vérifiez les certificats déjà présents sur le système.

Étape 2 : Création de l'Autorité de Certification

- Naviguez dans l'onglet *Authorities* et cliquez sur le bouton **Add** pour créer la nouvelle autorité.



- Nommez l'autorité m2l.local.
- Cochez la case **Trust Store** pour l'ajouter au magasin de confiance du système.
- Sélectionnez le type de clé **RSA** avec une longueur de **8192** bits (ou minimum 4096).
- Sélectionnez l'algorithme **sha512** et définissez une durée de vie (Lifetime) de **3650** jours.
- Renseignez m2l.local dans le champ **Common Name** et sauvegardez.



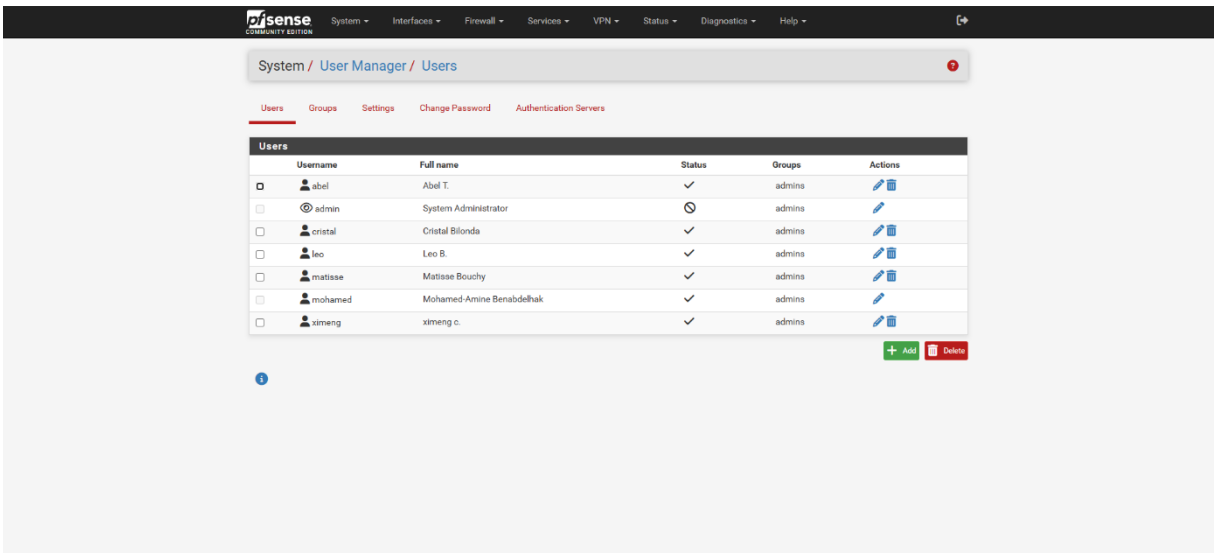
Étape 3 : Création du Certificat Serveur

- Retournez dans l'onglet *Certificates* et cliquez à nouveau sur **Add**.
- Nommez le certificat M2L.local.
- Choisissez une clé **RSA** de **4096** bits, l'algorithme **sha512** et une durée de vie de **398** jours.
- Dans *Certificate Type*, spécifiez qu'il s'agit d'un **Server Certificate**.
- Dans la section *Alternative Names*, ajoutez le FQDN ou Hostname m2l.local, puis sauvegardez.

Phase 2 : Création des Accès Utilisateurs

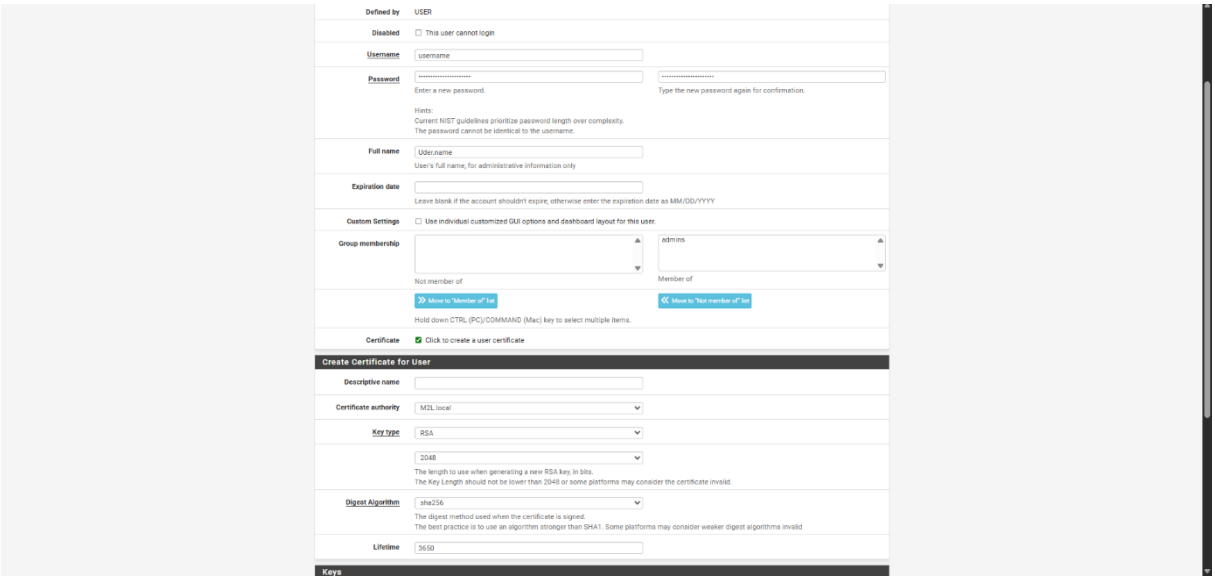
Étape 1 : Accès au gestionnaire d'utilisateurs

- Naviguez dans le menu **System**, puis sélectionnez **User Manager**.



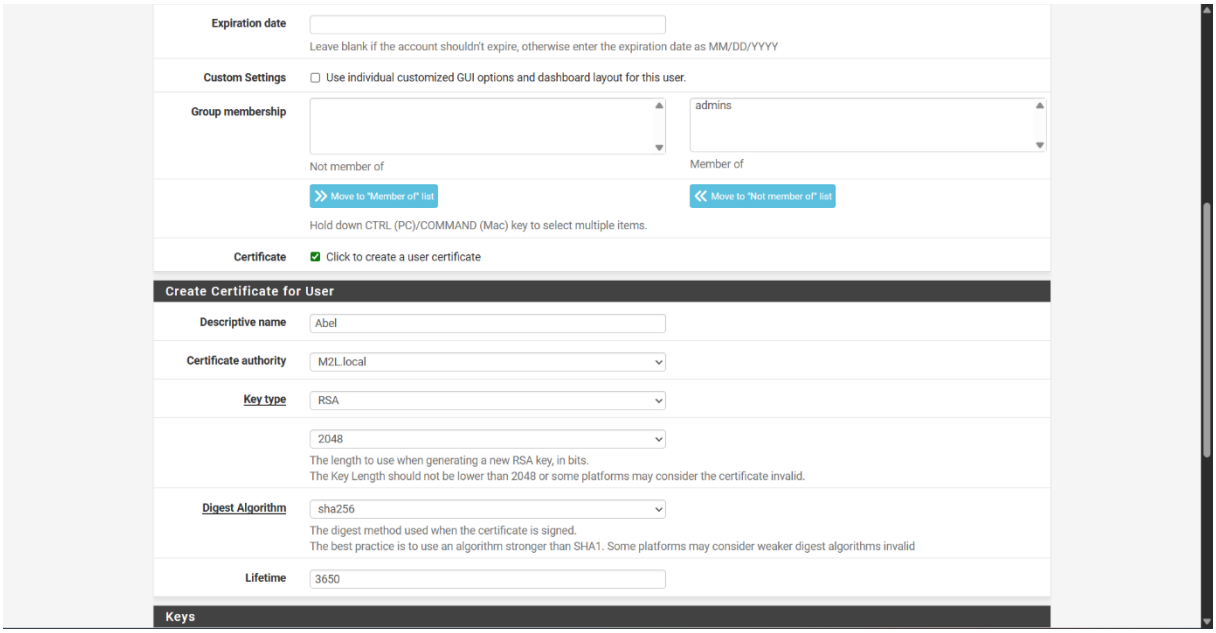
Étape 2 : Ajout et paramétrage de l'utilisateur

- Cliquez sur le bouton **Add** et remplissez les informations d'identification.
- Dans la section *Group membership*, veillez impérativement à déplacer le groupe **admins** vers la liste de droite ("Member of").



Étape 3 : Génération du certificat lié à l'utilisateur

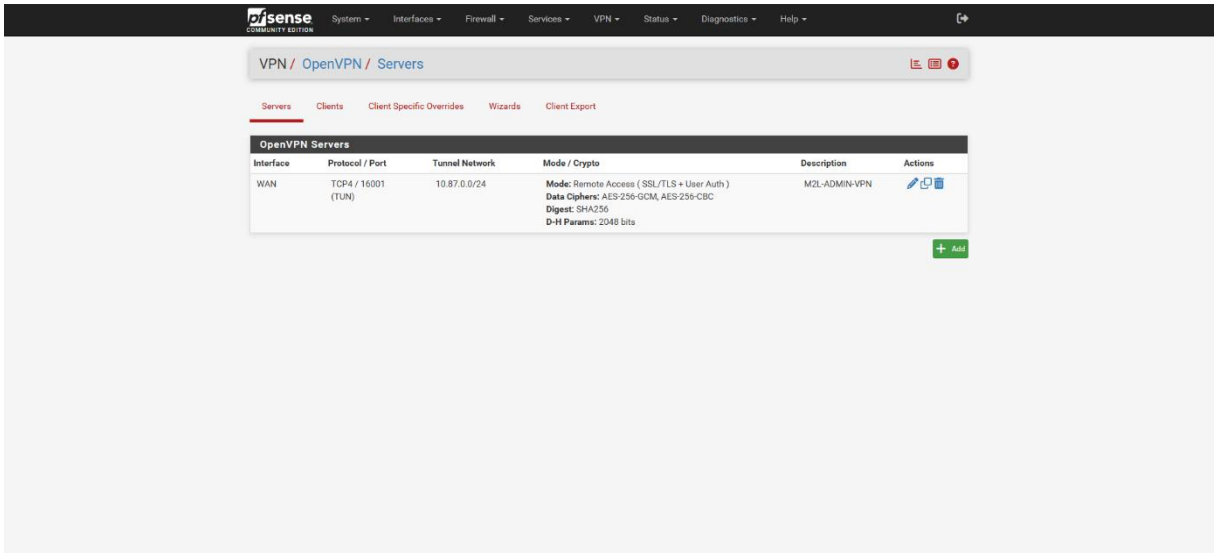
- Tout en bas du formulaire, cochez la case **Click to create a user certificate**.
- Vérifiez que l'autorité sélectionnée est bien M2L.local, avec une clé **RSA** de **2048** bits, l'algorithme **sha256** et **3650** jours de validité, puis enregistrez.



Phase 3 : Déploiement et Configuration du Serveur OpenVPN

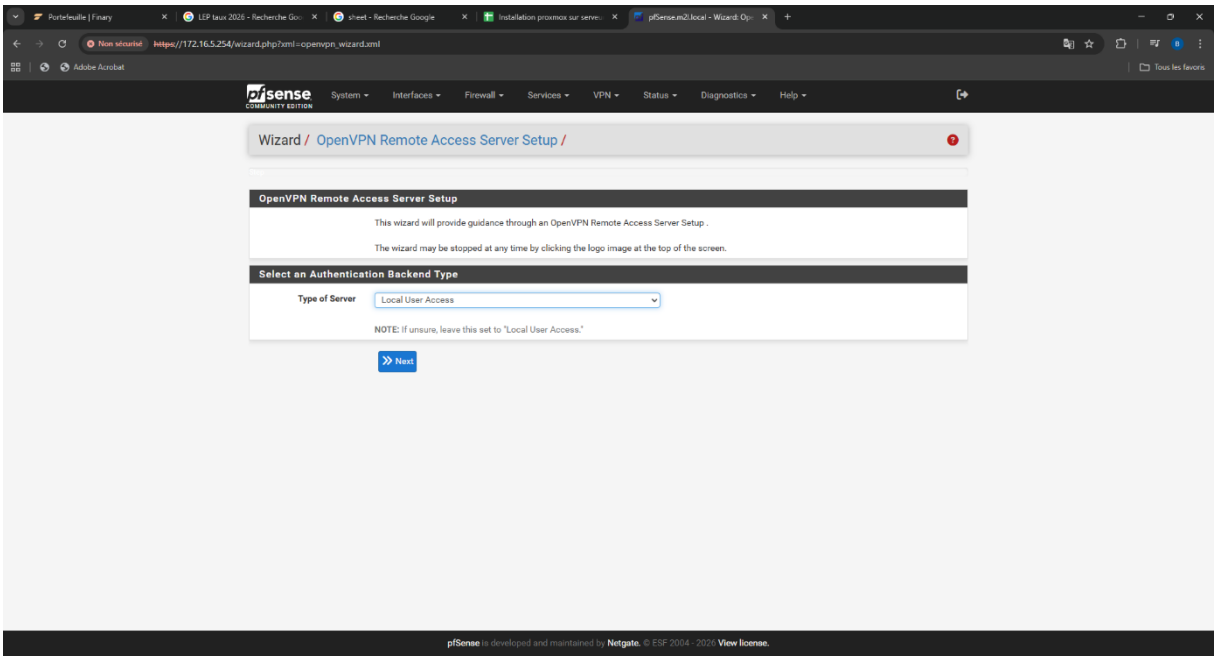
Étape 1 : Lancement de l'assistant de configuration

- Allez dans le menu **VPN**, puis **OpenVPN**, et cliquez sur l'onglet **Wizard**.



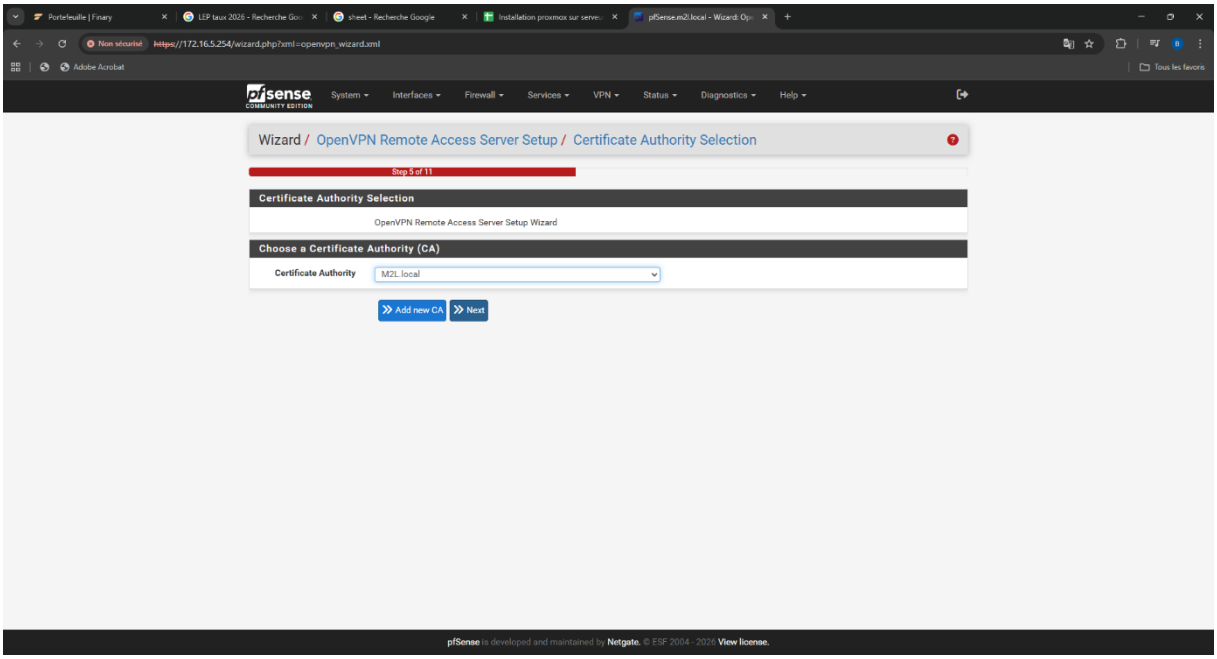
Étape 2 : Type de serveur d'authentification

- Dans *Type of Server*, choisissez **Local User Access** et cliquez sur **Next**.

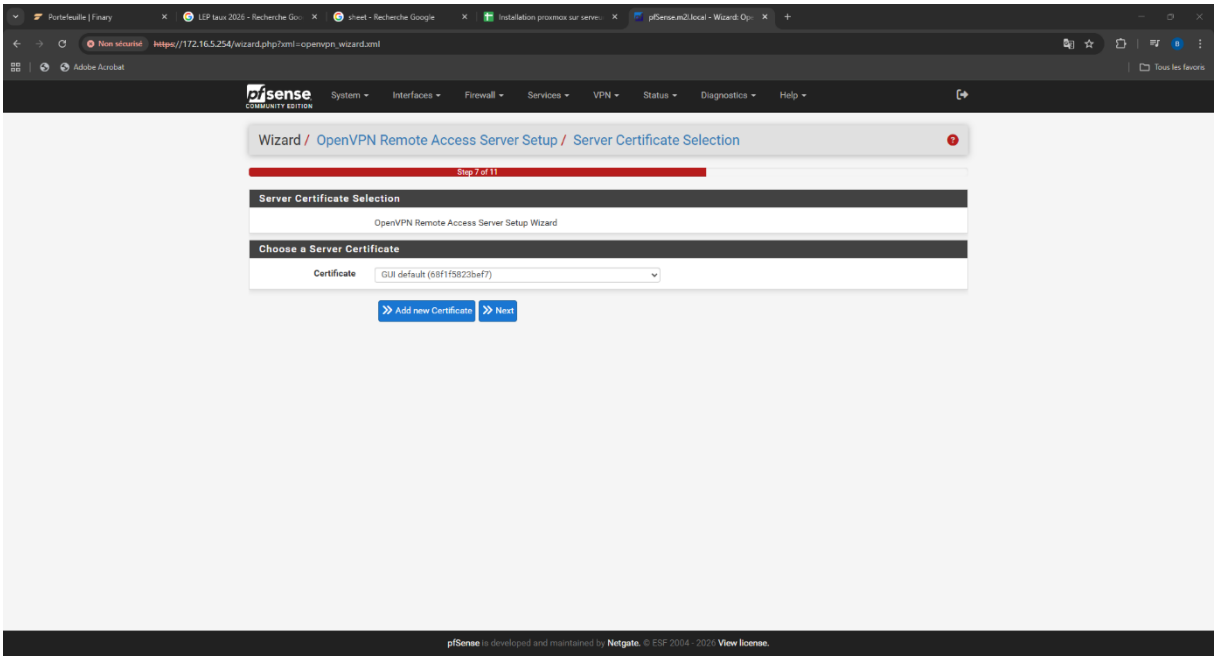


Étape 3 : Choix des certificats

- Sélectionnez l'autorité de certification M2L.local et faites **Next**.

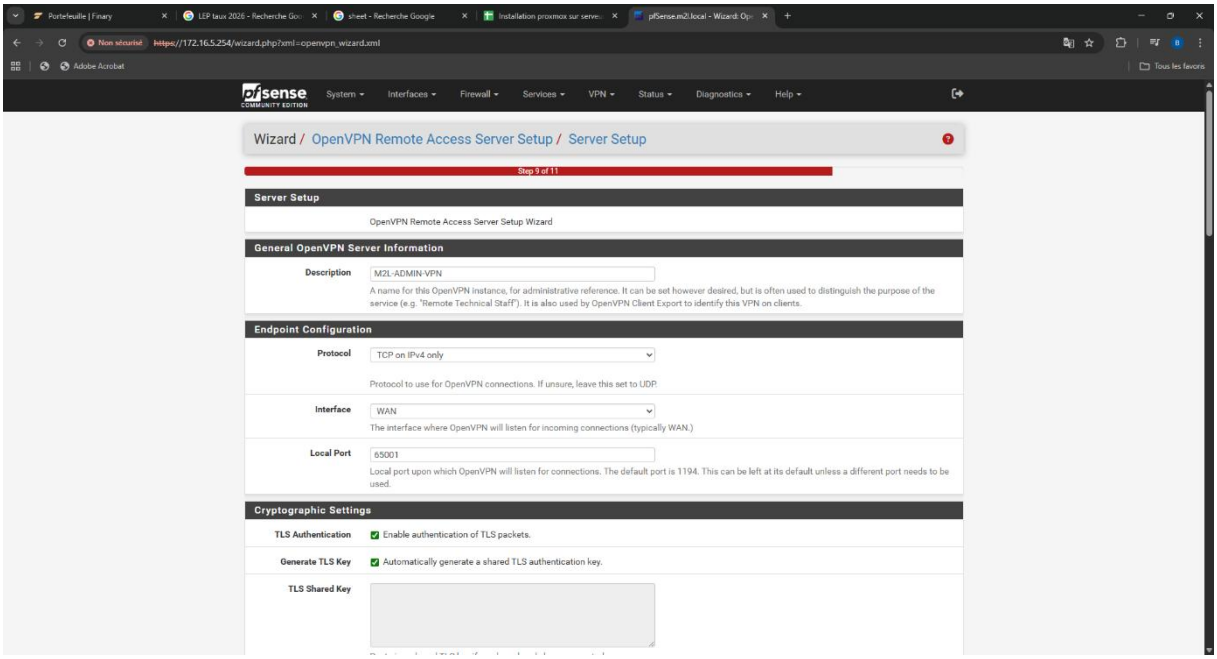


- Sélectionnez ensuite le certificat serveur M2L.local et faites **Next**.

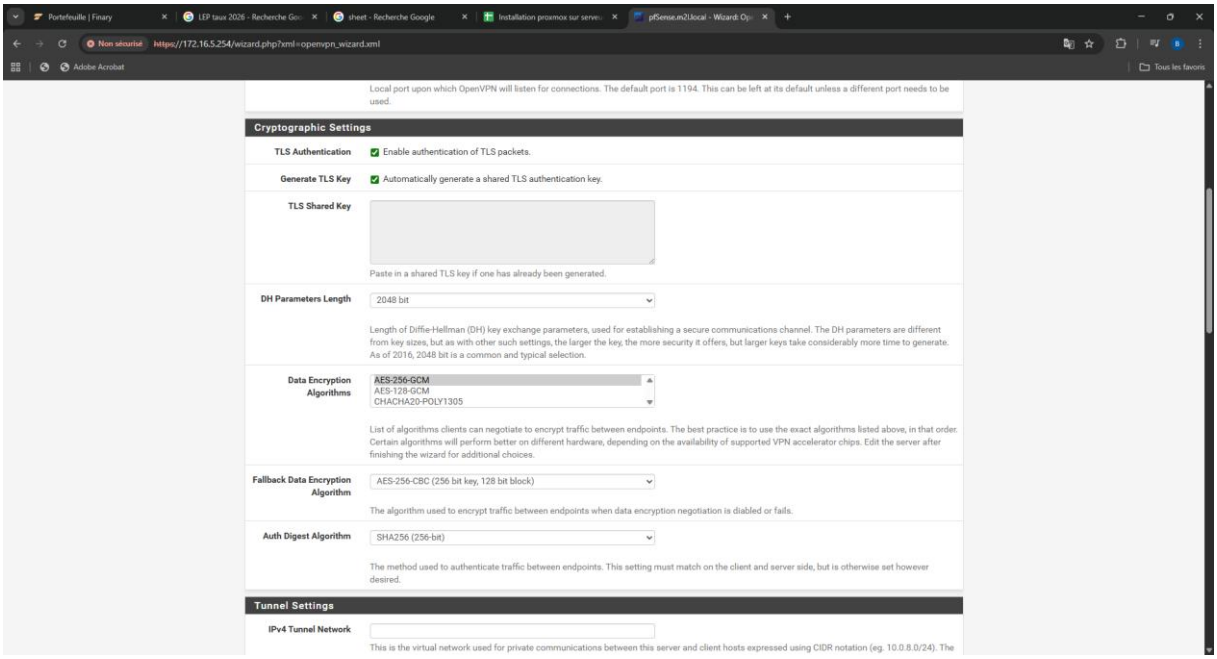


Étape 4 : Configuration Réseau et Cryptographie

- Dans la description, saisissez M2L-ADMIN-VPN.
- Sélectionnez le protocole **TCP on IPv4 only**, l'interface d'écoute **WAN**, et le port local **65001**.

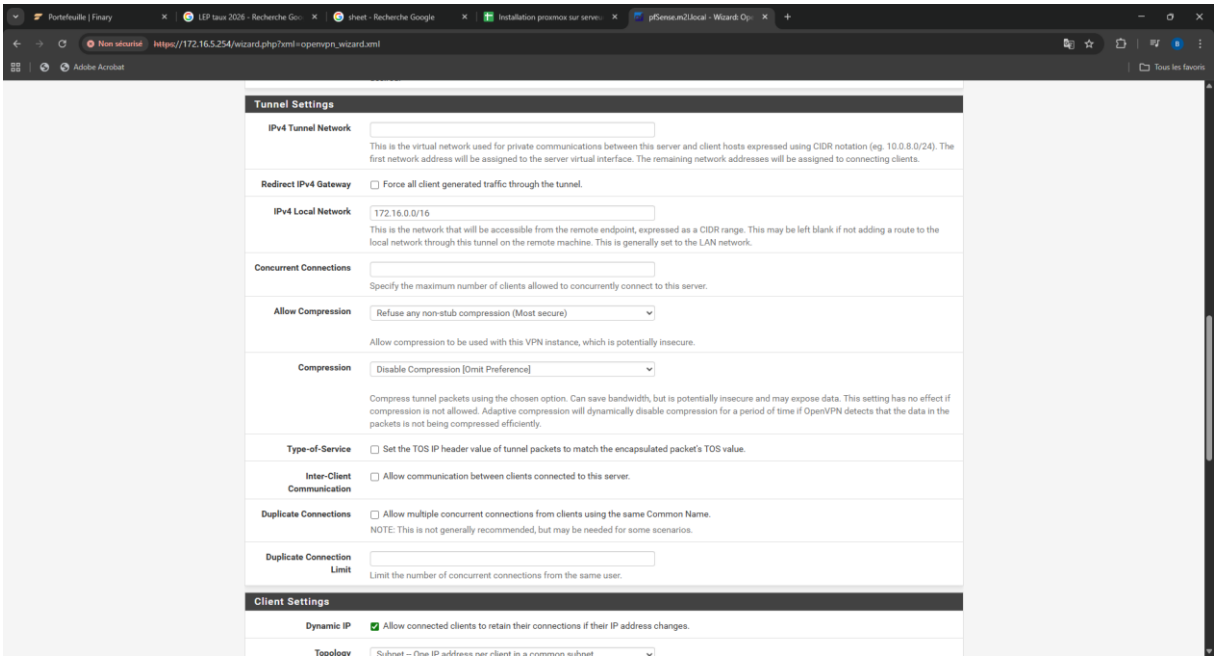


- Pour le chiffrement (Data Encryption), ne conservez que l'algorithme à **256** bits (ex: AES-256-GCM).



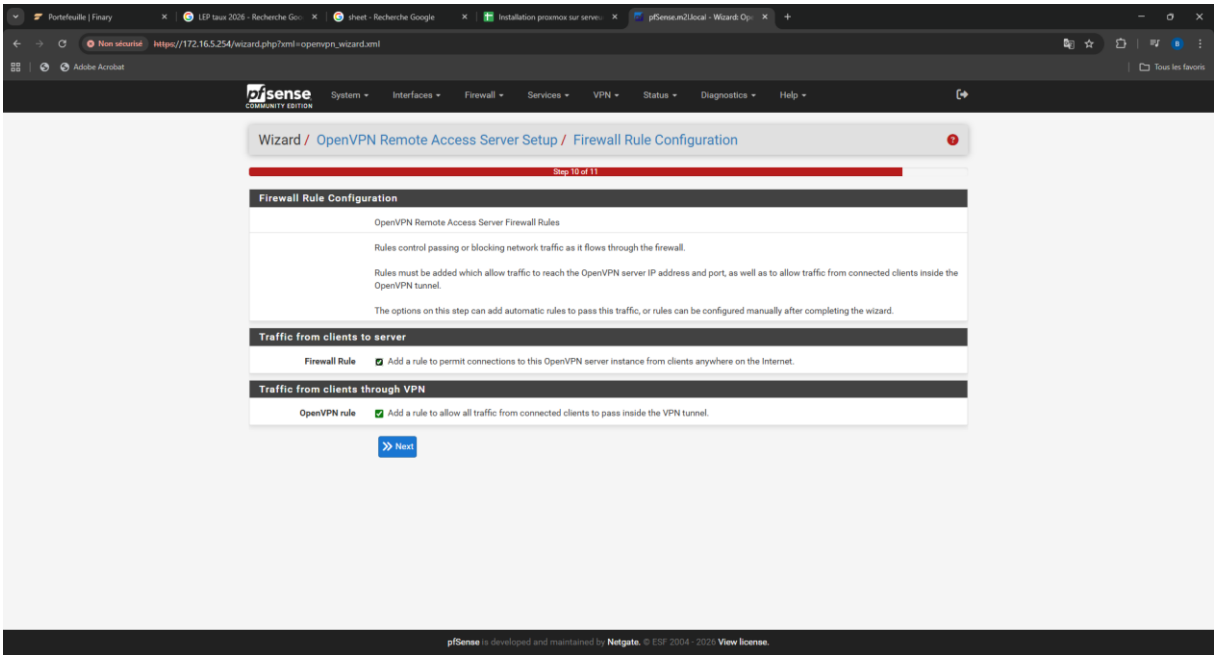
Étape 5 : Paramètres du Tunnel (Tunnel Settings)

- Renseignez l'**IPv4 Tunnel Network** avec la plage 10.87.0.0/24.
- Renseignez l'**IPv4 Local Network** avec la plage de M2L : 172.16.0.0/16.
- Dans *Client Settings*, réglez le paramètre **Topology** sur Subnet.

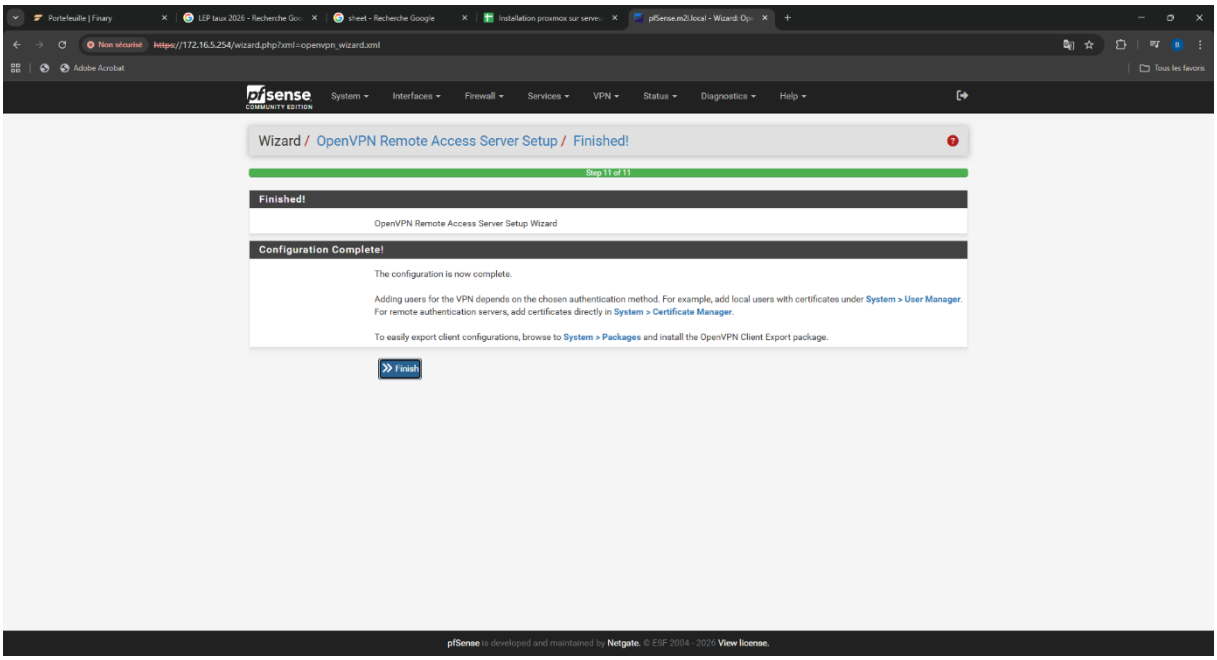


Étape 6 : Règles de Pare-feu (Firewall Rules)

- Cochez impérativement les deux cases **Firewall Rule** et **OpenVPN Rule** afin d'autoriser les flux de connexion extérieurs et internes au tunnel.



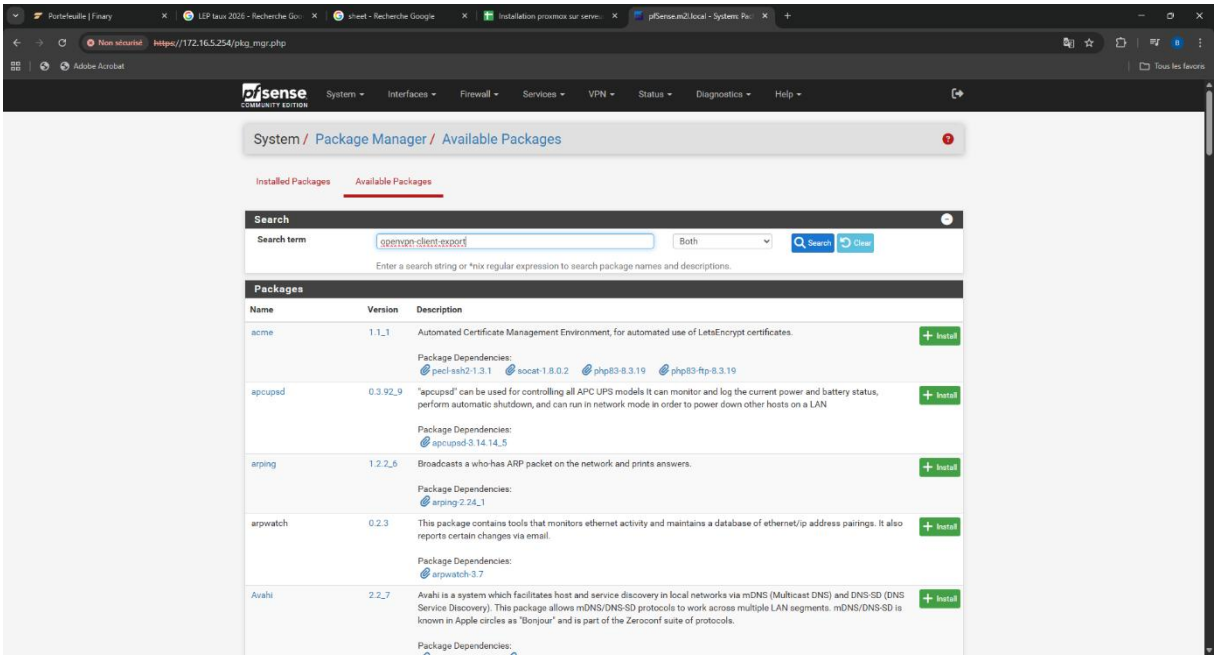
- Cliquez sur **Next**, puis sur **Finish** pour achever la configuration du serveur.



Phase 4 : Installation de l'Exportateur Client (Client Export)

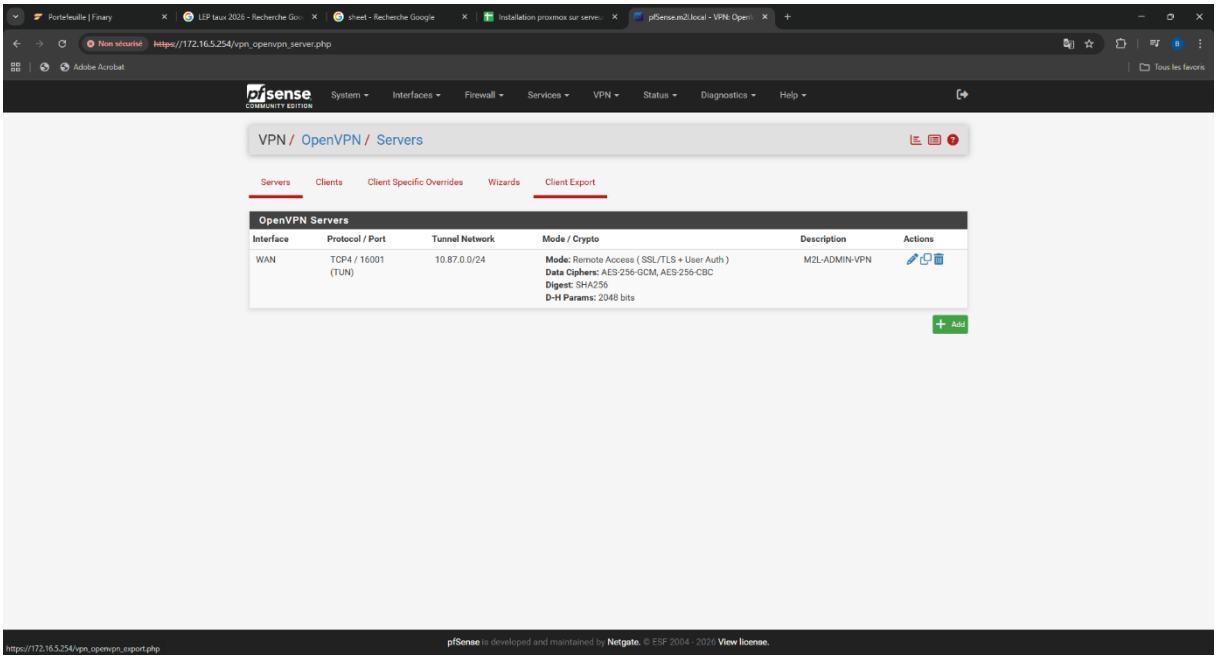
Étape 1 : Installation du paquet supplémentaire

- Allez dans le menu **System**, **Package Manager**, puis dans l'onglet **Available Packages**.
- Recherchez et installez le paquet nommé openvpn-client-export.

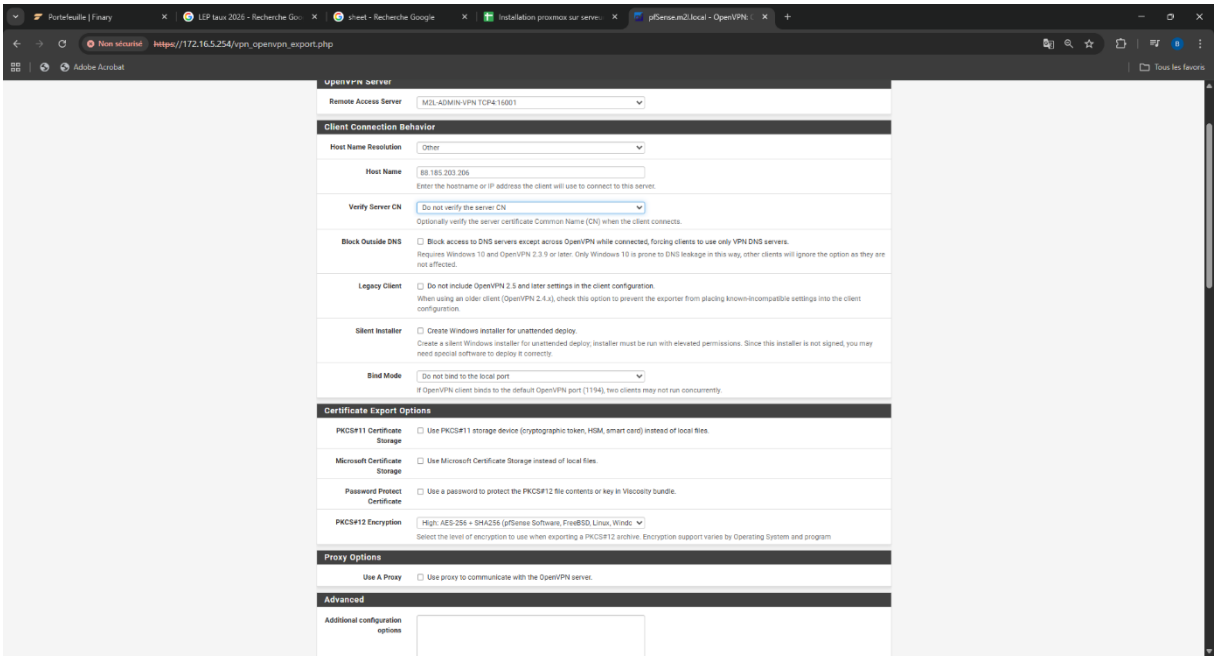


Étape 2 : Configuration de l'export

- Naviguez dans le menu **VPN**, **OpenVPN**, et cliquez sur le nouvel onglet **Client Export**.



- Réglez **Host Name Resolution** sur Other.
- Saisissez votre IP publique dans **Host Name** : 88.185.203.206.
- Réglez **Verify Server CN** sur Do not verify.
- Descendez pour cliquer sur **Save as default**.



Étape 3 : Téléchargement du client

- En bas de cette même page, repérez l'utilisateur souhaité (ex: mohamed) et cliquez sur le bouton correspondant au format d'export voulu (Windows Installer, Inline, ou Archive) pour configurer la machine cliente.