



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	2
Prérequis	2
Phase 1 : Création de l'Autorité de Certification (CA) et du Certificat Serveur	2
Étape 1 : Vérification initiale	2
Étape 2 : Création de l'Autorité de Certification	2
Étape 3 : Création du Certificat Serveur	4
Phase 2 : Création des Accès Utilisateurs	4
Étape 1 : Accès au gestionnaire d'utilisateurs	4
Étape 2 : Ajout et paramétrage de l'utilisateur	5
Étape 3 : Génération du certificat lié à l'utilisateur	5
Phase 3 : Déploiement et Configuration du Serveur OpenVPN	6
Étape 1 : Lancement de l'assistant de configuration	6
Étape 2 : Type de serveur d'authentification	6
Étape 3 : Choix des certificats	7
Étape 4 : Configuration Réseau et Cryptographie	8
Étape 5 : Paramètres du Tunnel (Tunnel Settings)	9
Étape 6 : Règles de Pare-feu (Firewall Rules)	9
Phase 4 : Installation de l'Exportateur Client (Client Export)	10
Étape 1 : Installation du paquet supplémentaire	10
Étape 2 : Configuration de l'export	11
Étape 3 : Téléchargement du client	12

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

Prérequis

Avant de débiter 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.

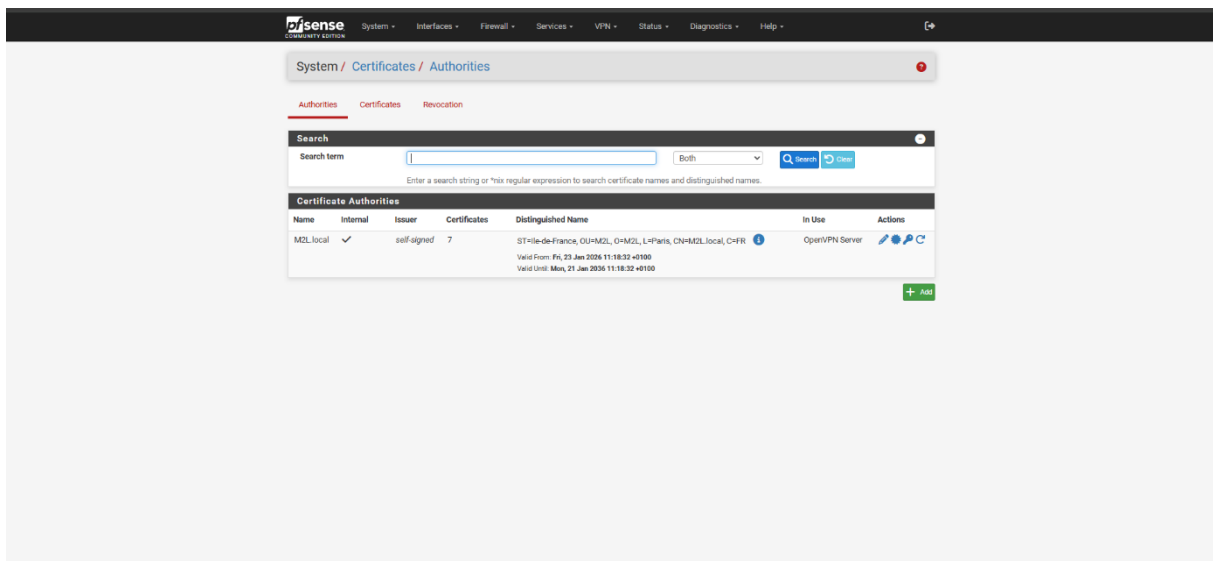
Phase 1 : Création de l'Autorité de Certification (CA) et du Certificat Serveur

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.

The screenshot shows a configuration form for an Internal Certificate Authority. The fields are as follows:

- Descriptive name:** m2l.local
- Method:** Create an internal Certificate Authority
- Trust Store:** Add this Certificate Authority to the Operating System Trust Store
- Randomize Serial:** Use random serial numbers when signing certificates
- Internal Certificate Authority:**
 - Key type:** RSA
 - Key Length:** 8192
 - Digest Algorithm:** sha512
 - Lifetime (days):** 3650
 - Common Name:** m2l.local
 - 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)

A "Save" button is located at the bottom of the form.

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.

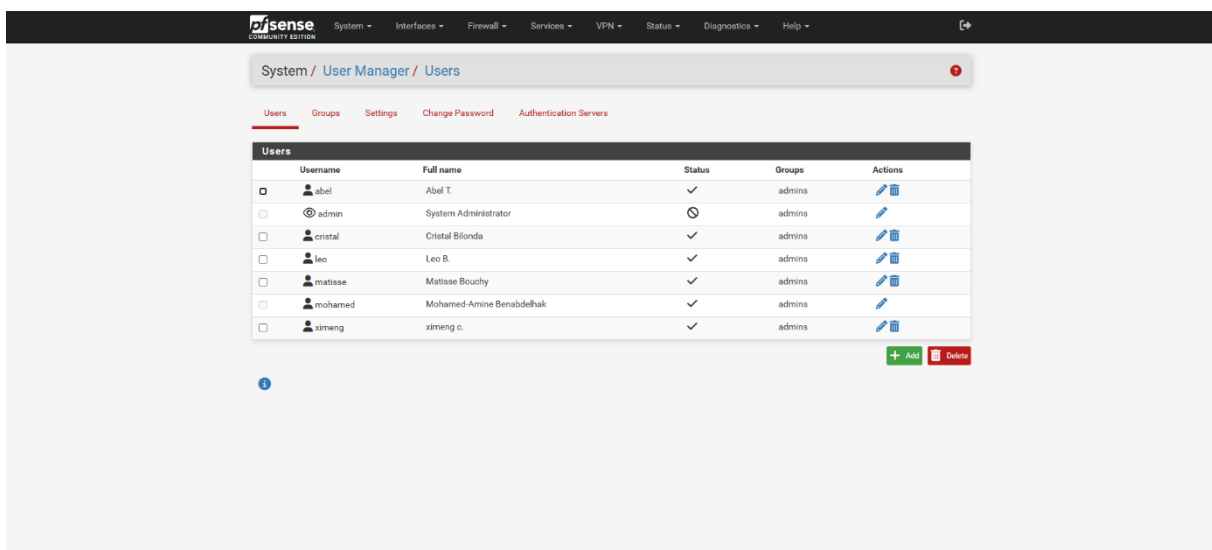
The screenshot shows the 'Create Internal Certificate' form in Mikrotik WinBox. The form is filled with the following values:

- Method:** Create Internal Certificate
- Descriptive name:** M2L.local
- Internal Certificate:**
 - Certificate authority:** M2L.local
 - Key type:** RSA
 - Key length:** 4096
 - Digest algorithm:** sha512
 - Lifetime (days):** 398
 - Common Name:** www.example.com
 - Country Code:** FR
 - State or Province:** Ile-de-France
 - City:** Paris
 - Organization:** M2L
 - Organizational Unit:** M2L
- Certificate Attributes:**
 - Attribute Notes:** The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode. For Internal Certificates, these attributes are added directly to the certificate as shown.
 - Certificate Type:** Server Certificate
 - Alternative Names:** FQDN or Hostname: m2l.local

Phase 2 : Création des Accès Utilisateurs

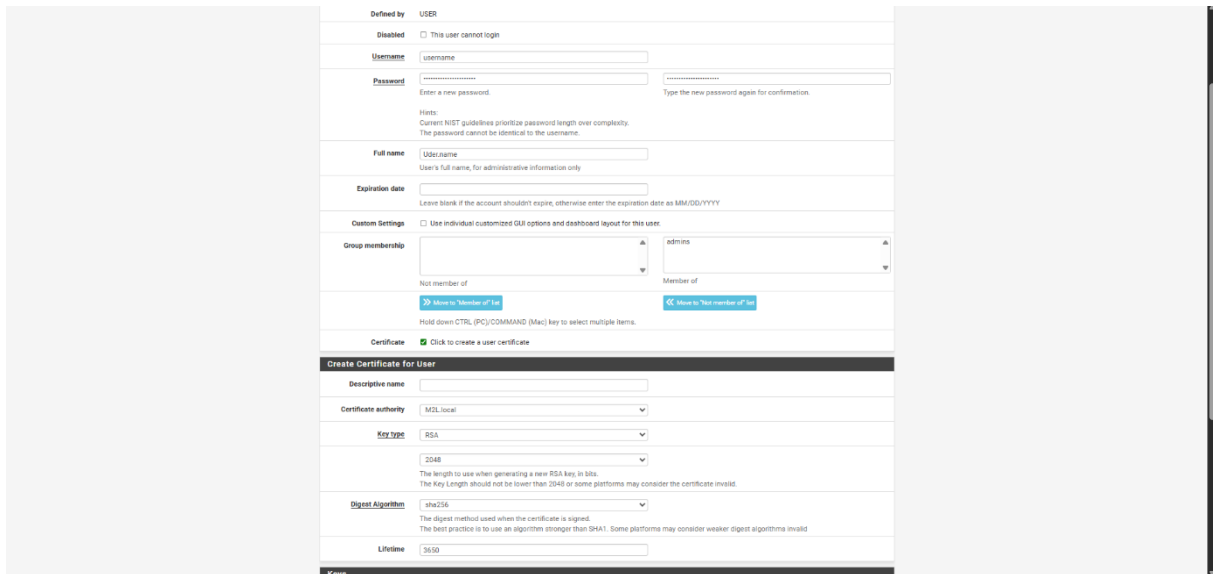
Étape 1 : Accès au gestionnaire d'utilisateurs

- 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*, veuillez impérativement à déplacer le groupe **admins** vers la liste de droite ("Member of").



Defined by USER

Disabled This user cannot login

Username

Password
Enter a new password.
Type the new password again for confirmation.

Hints:
Current NIST guidelines prioritize password length over complexity.
The password cannot be identical to the username.

Full name
User's full name, for administrative information only

Expiration date
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings Use individual customized GUI options and dashboard layout for this user.

Group membership
Not member of
Member of
[Move to "Member of" list](#) [Move to "Not member of" list](#)

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Certificate Click to create a user certificate

Create Certificate for User

Descriptive name

Certificate authority

Key type
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.

Key length

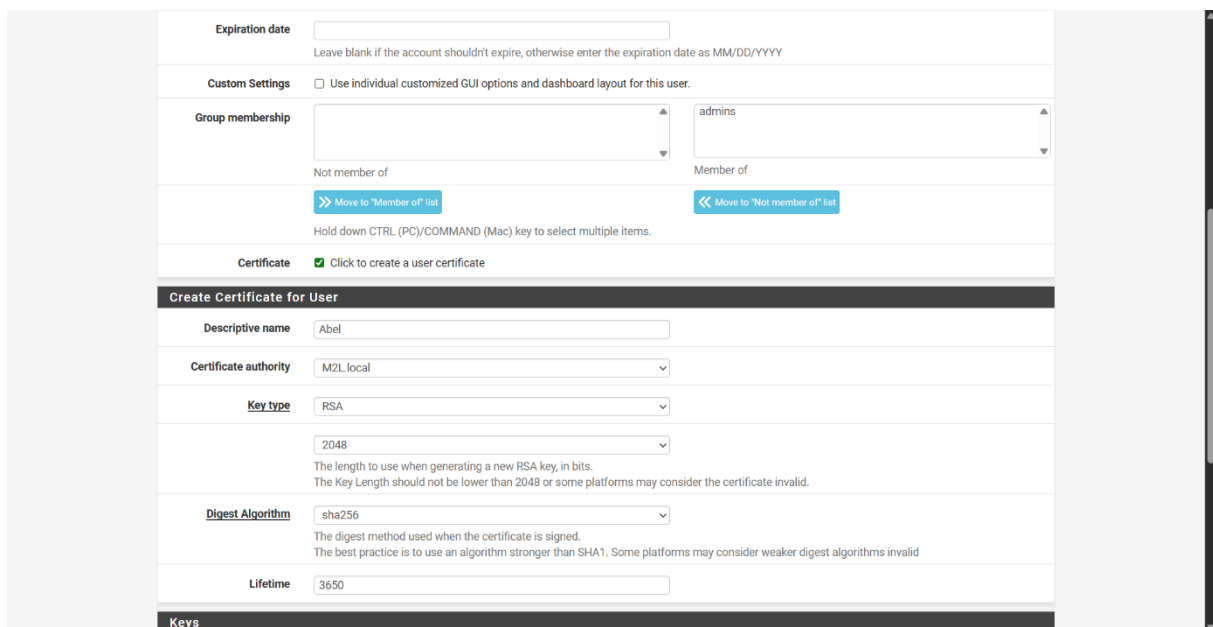
Digest Algorithm
The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.

Lifetime

Keys

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.



Expiration date
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings Use individual customized GUI options and dashboard layout for this user.

Group membership
Not member of
Member of
[Move to "Member of" list](#) [Move to "Not member of" list](#)

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Certificate Click to create a user certificate

Create Certificate for User

Descriptive name

Certificate authority

Key type
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.

Key length

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.

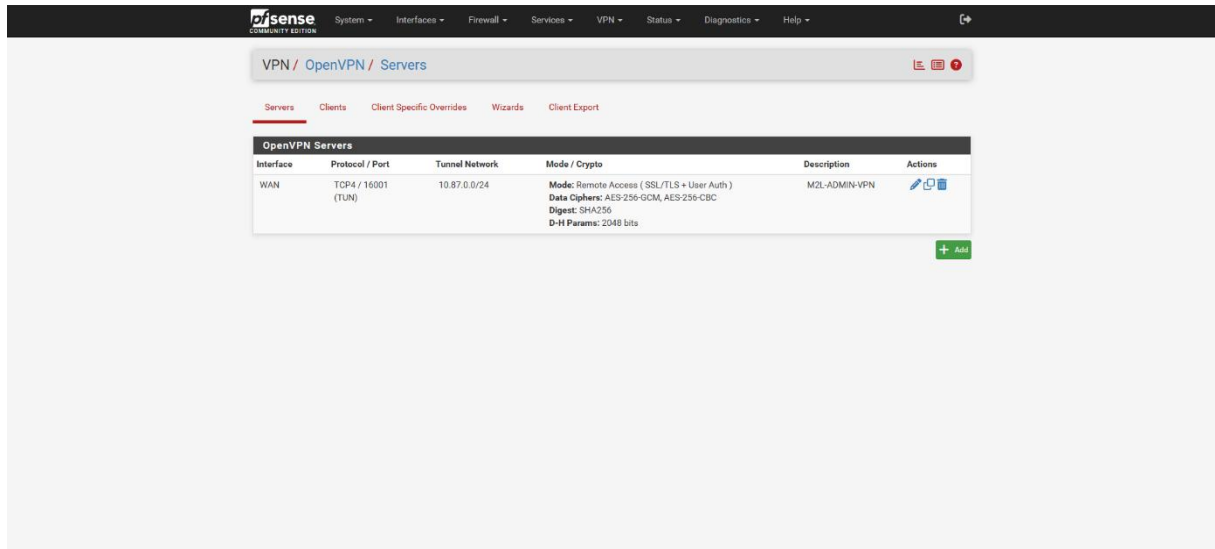
Lifetime

Keys

Phase 3 : Déploiement et Configuration du Serveur OpenVPN

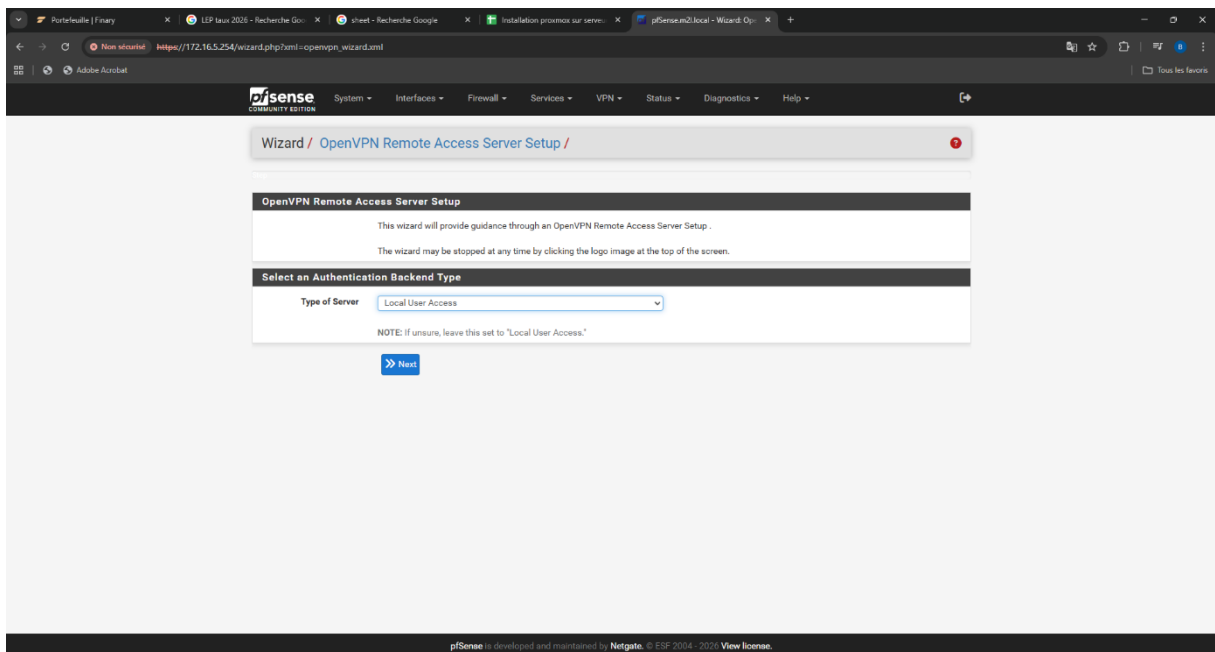
Étape 1 : Lancement de l'assistant de configuration

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



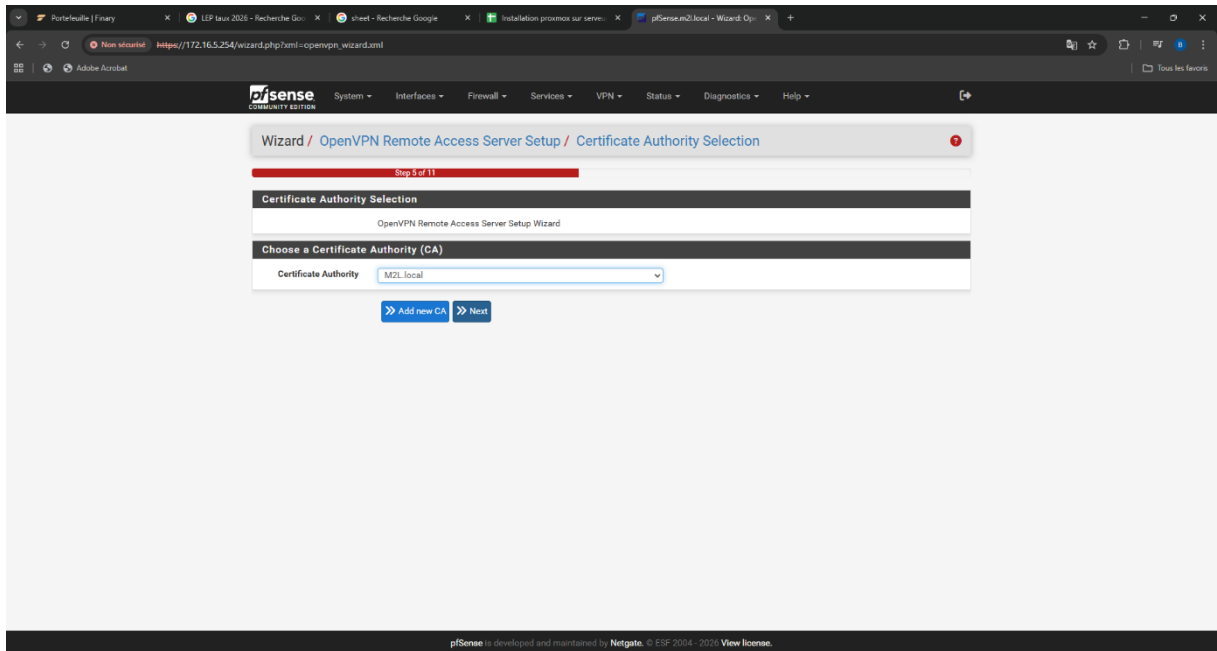
Étape 2 : Type de serveur d'authentification

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

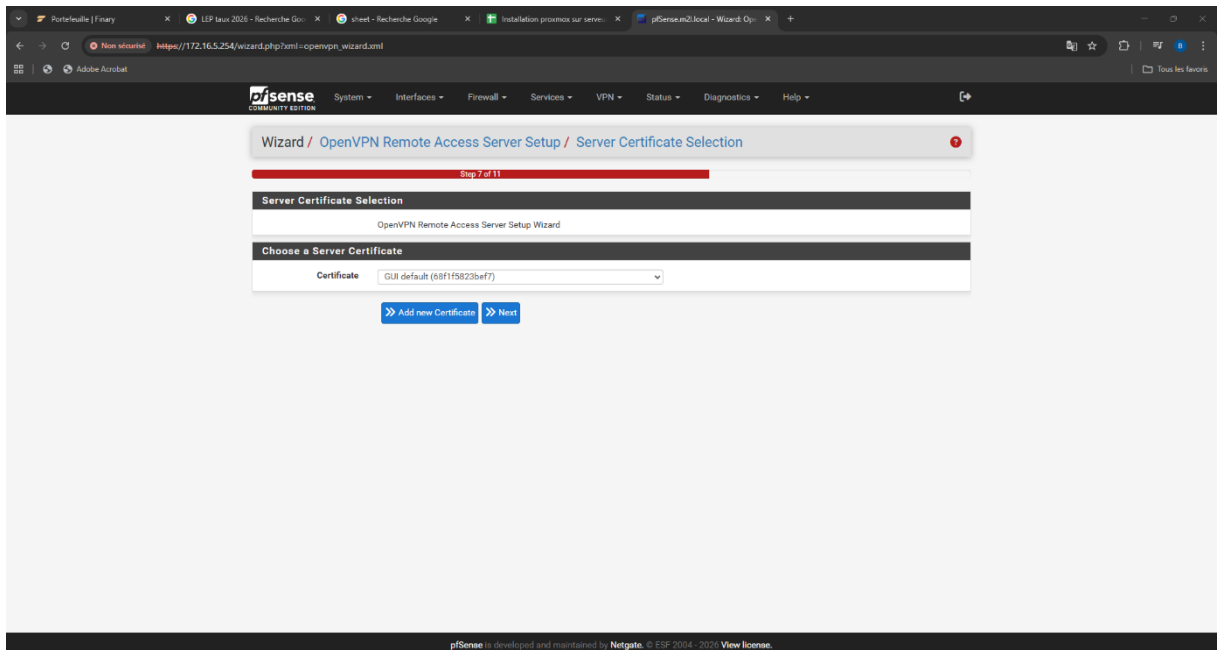


Étape 3 : Choix des certificats

- 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**.

The screenshot shows the 'Server Setup' page of the OpenVPN Remote Access Server Setup wizard. The 'General OpenVPN Server Information' section has the 'Description' field set to 'M2L-ADMIN-VPN'. The 'Endpoint Configuration' section has 'Protocol' set to 'TCP on IPv4 only', 'Interface' set to 'WAN', and 'Local Port' set to '65001'. The 'Cryptographic Settings' section has 'TLS Authentication' and 'Generate TLS Key' checked, and the 'TLS Shared Key' field is empty.

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

The screenshot shows the 'Cryptographic Settings' and 'Tunnel Settings' sections of the wizard. In 'Cryptographic Settings', 'DH Parameters Length' is set to '2048 bit', 'Data Encryption Algorithms' is set to 'AES-256-GCM', 'Fallback Data Encryption Algorithm' is set to 'AES-256-CBC (256 bit key, 128 bit block)', and 'Auth Digest Algorithm' is set to 'SHA256 (256-bit)'. The 'Tunnel Settings' section has the 'IPv4 Tunnel Network' field empty.

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.

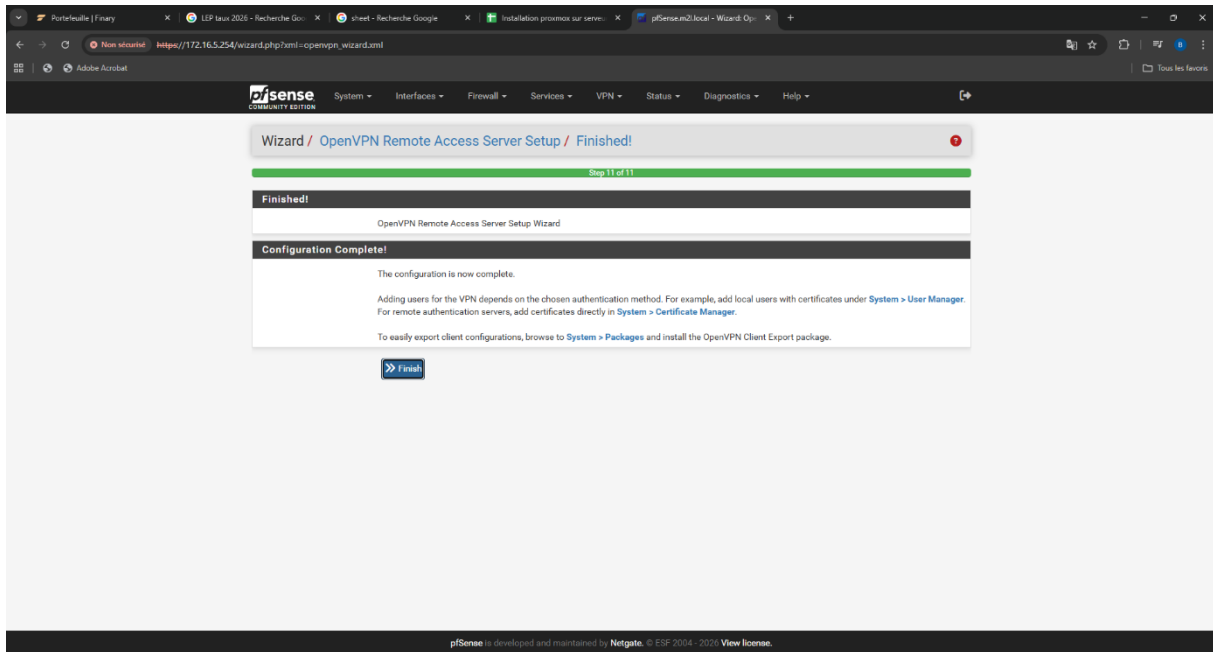
The screenshot shows the 'Tunnel Settings' section of the OpenVPN wizard. The 'IPv4 Tunnel Network' field is empty. The 'Redirect IPv4 Gateway' checkbox is unchecked. The 'IPv4 Local Network' field contains '172.16.0.0/16'. The 'Concurrent Connections' field is empty. The 'Allow Compression' dropdown is set to 'Refuse any non-stub compression (Most secure)'. The 'Compression' dropdown is set to 'Disable Compression [Omit Preference]'. The 'Type-of-Service' checkbox is unchecked. The 'Inter-Client Communication' checkbox is unchecked. The 'Duplicate Connections' checkbox is unchecked. The 'Duplicate Connection Limit' field is empty. The 'Client Settings' section is partially visible, showing 'Dynamic IP' checked and 'Topology' set to 'Subnet - One IP address per client in a common 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.

The screenshot shows the 'Firewall Rule Configuration' step of the OpenVPN wizard. The page title is 'Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration'. A progress bar indicates 'Step 10 of 11'. The 'Firewall Rule Configuration' section explains that rules control passing or blocking network traffic. Under 'Traffic from clients to server', the 'Firewall Rule' checkbox is checked. Under 'Traffic from clients through VPN', the 'OpenVPN rule' checkbox is checked. A 'Next' button is visible at the bottom.

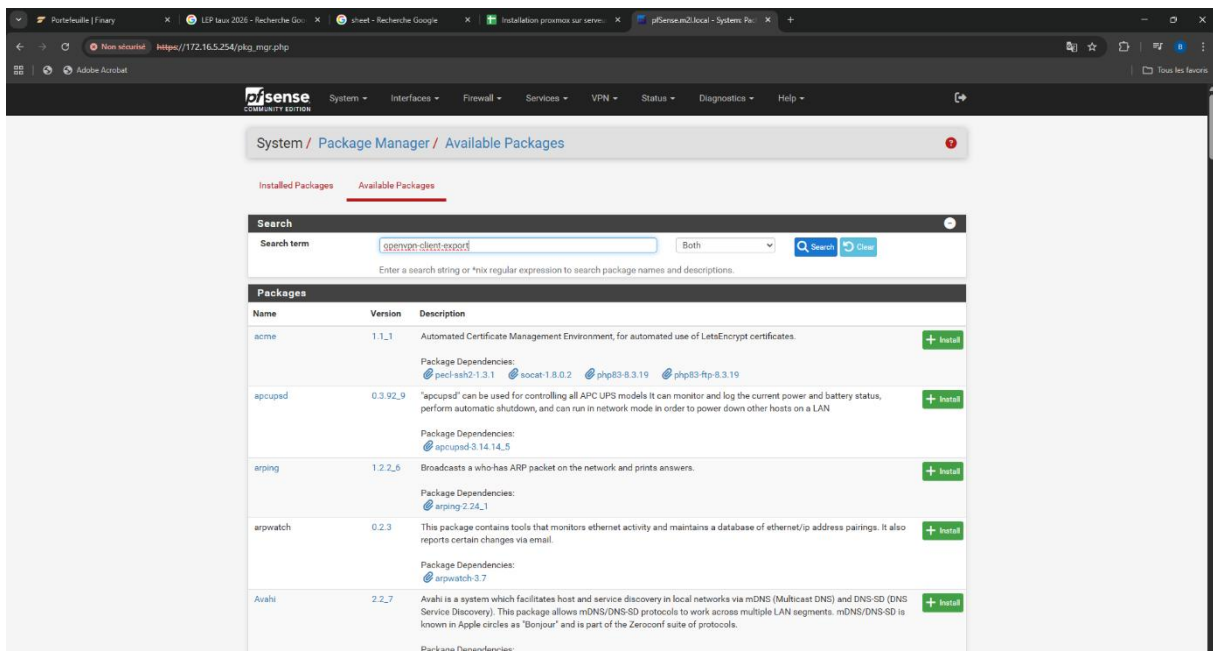
- Cliquez sur **Next**, puis sur **Finish** pour achever la configuration du serveur.



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

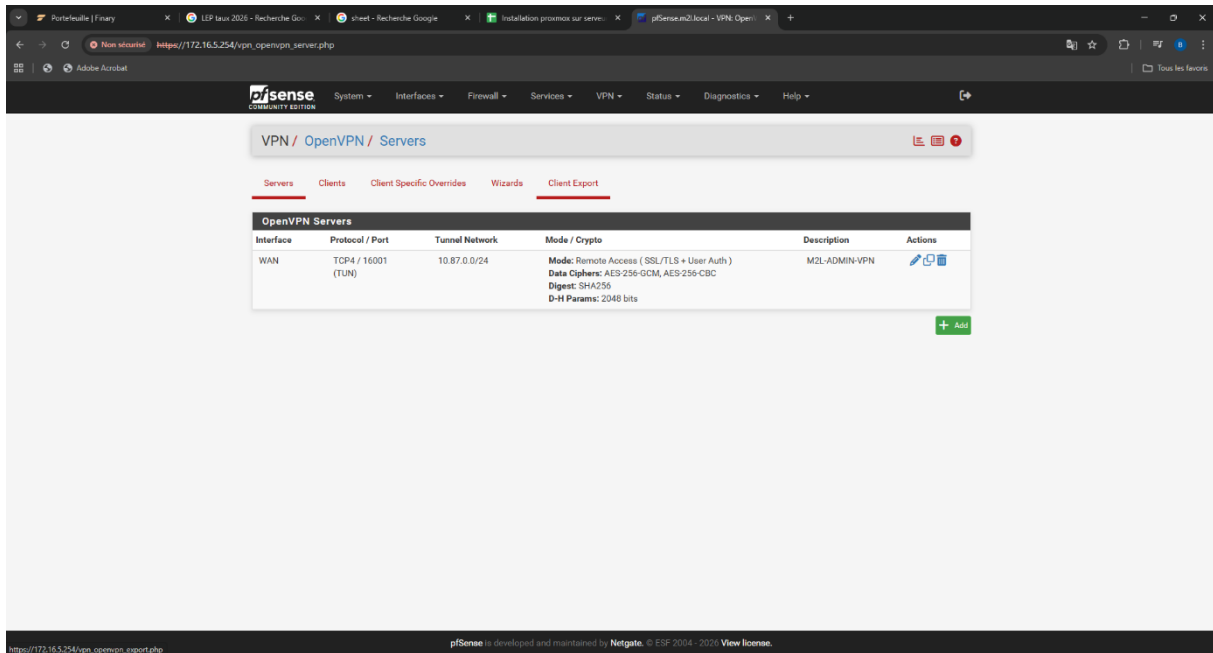
Étape 1 : Installation du paquet supplémentaire

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

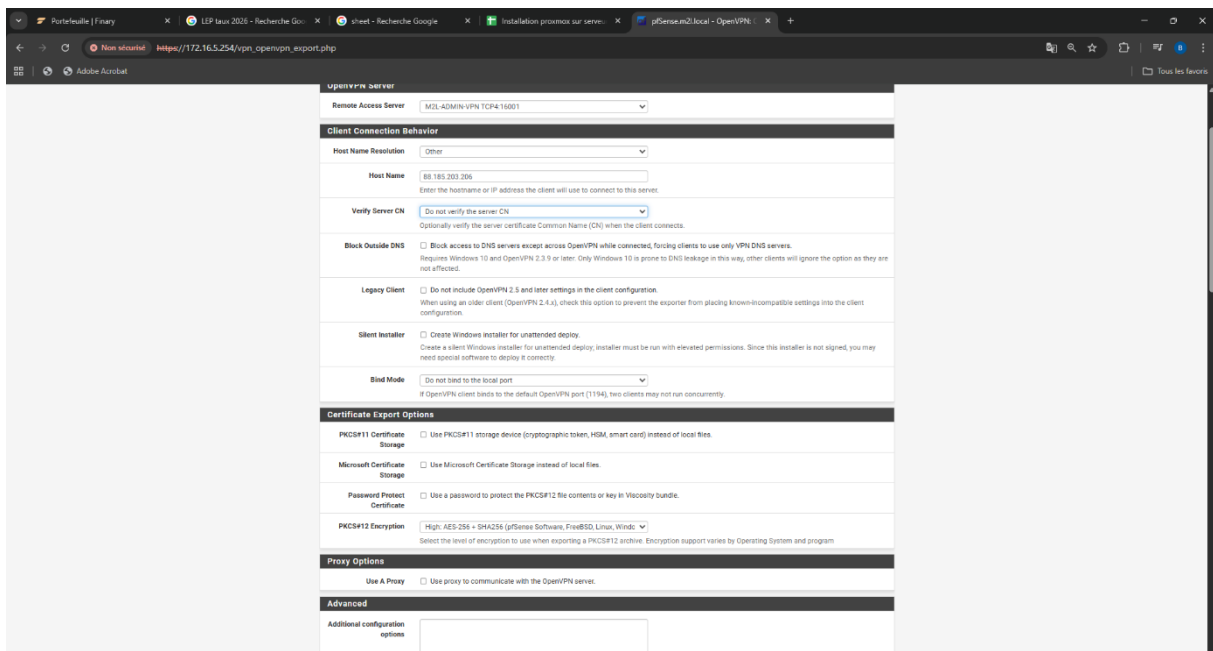


Étape 2 : Configuration de l'export

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

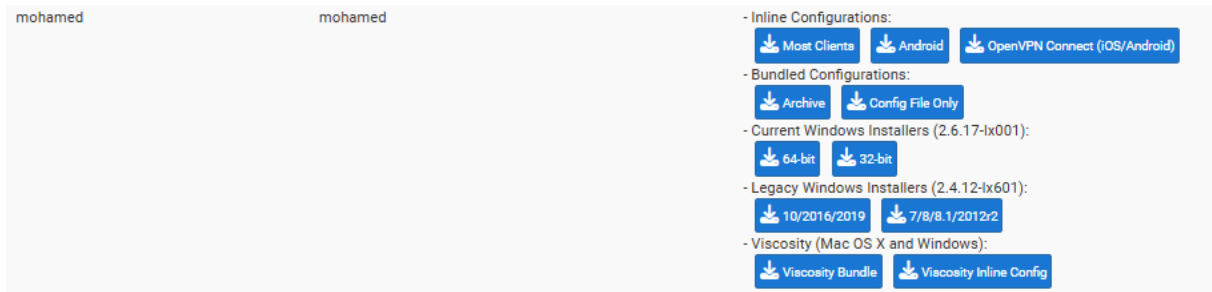


- Réglez **Host Name Resolution** sur Other.
- Saisissez votre IP publique dans **Host Name** : 88.185.203.206.
- Réglez **Verify Server CN** sur Do not verify.
- Descendez pour cliquer sur **Save as default**.



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.



The screenshot displays a user interface for downloading configurations. At the top, the name 'mohamed' is shown on both the left and right sides. Below this, there are several sections of download options, each with a minus sign icon and a title:

- Inline Configurations:** Includes three buttons: 'Most Clients', 'Android', and 'OpenVPN Connect (iOS/Android)'.
- Bundled Configurations:** Includes two buttons: 'Archive' and 'Config File Only'.
- Current Windows Installers (2.6.17-ix001):** Includes two buttons: '64-bit' and '32-bit'.
- Legacy Windows Installers (2.4.12-ix601):** Includes two buttons: '10/2016/2019' and '7/8/8.1/2012r2'.
- Viscosity (Mac OS X and Windows):** Includes two buttons: 'Viscosity Bundle' and 'Viscosity Inline Config'.