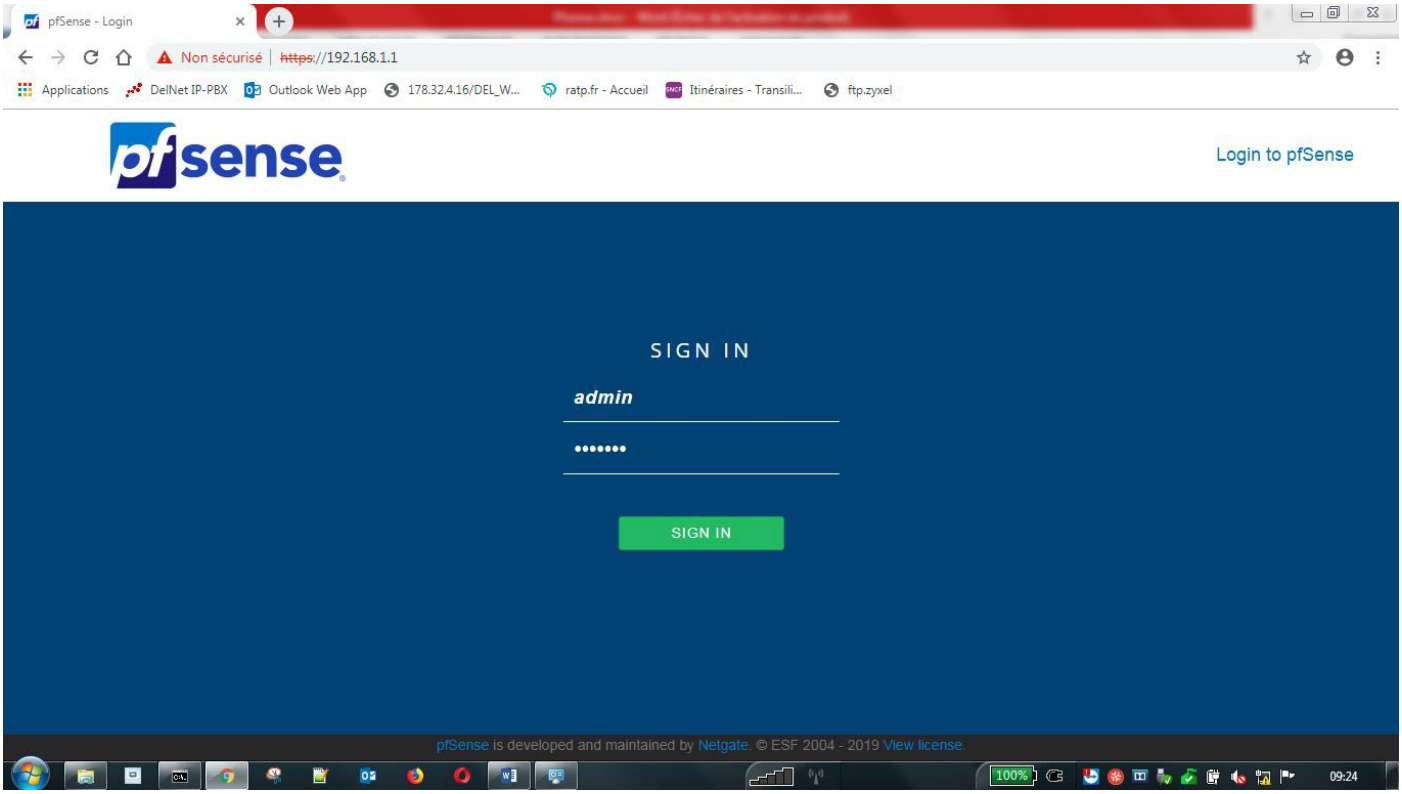
Procédure :
Configuration pfSense.

Sommaire

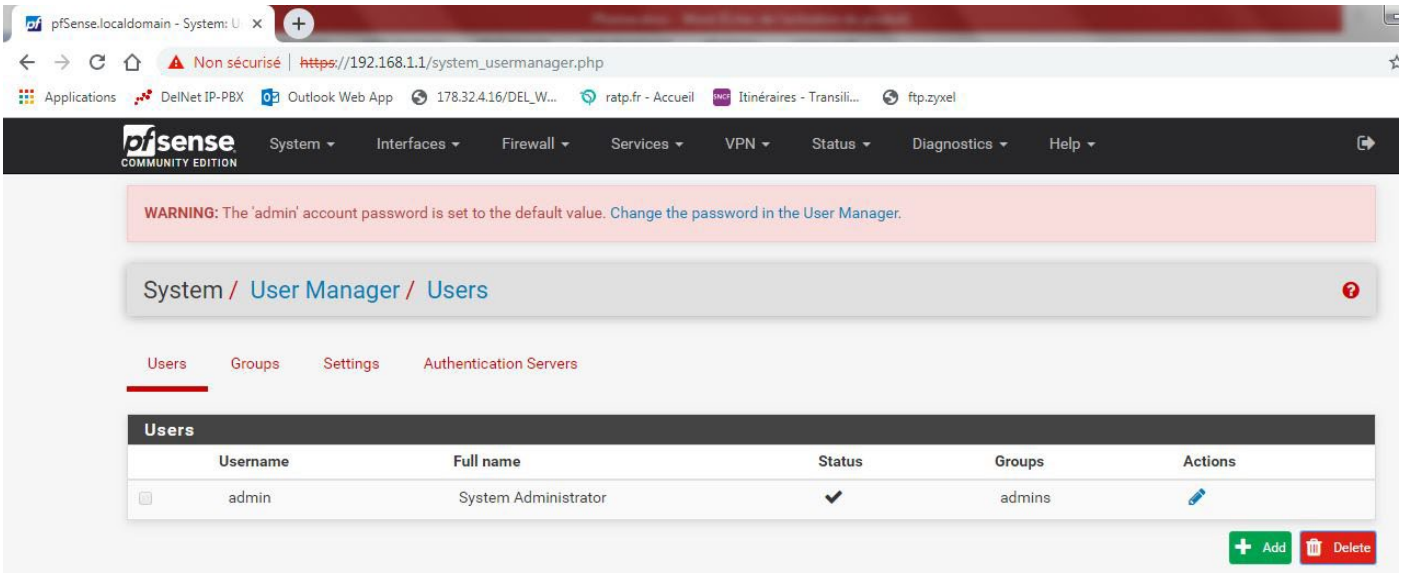
1/- Configuration du pfSense.

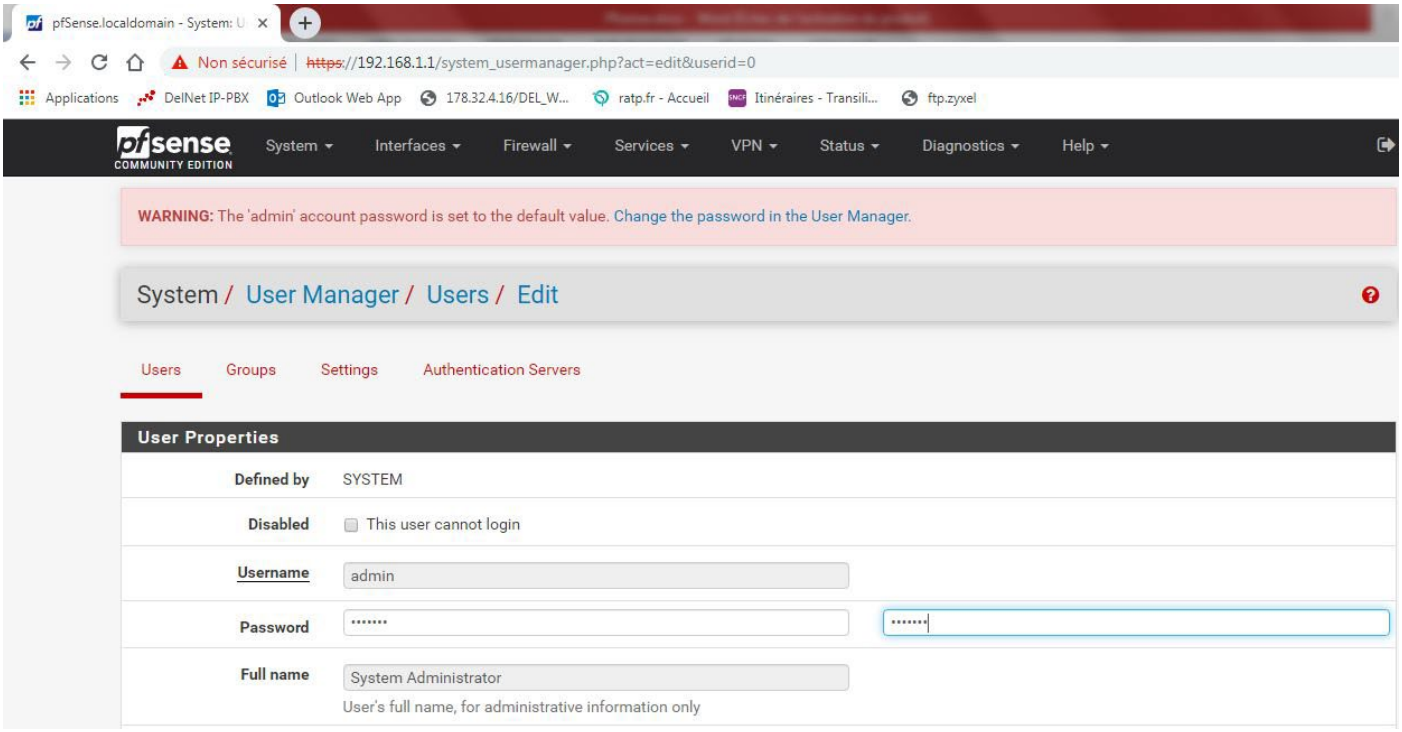
Se connecter sur la page de configuration du pfsense par défaut : https://192.168.1.1 (avec DHCP) et entrer les identifiants par défaut : admin / pfsense.



Mot de passe :

Changer le mot de passe administrateur dans System > User Manager > Users.

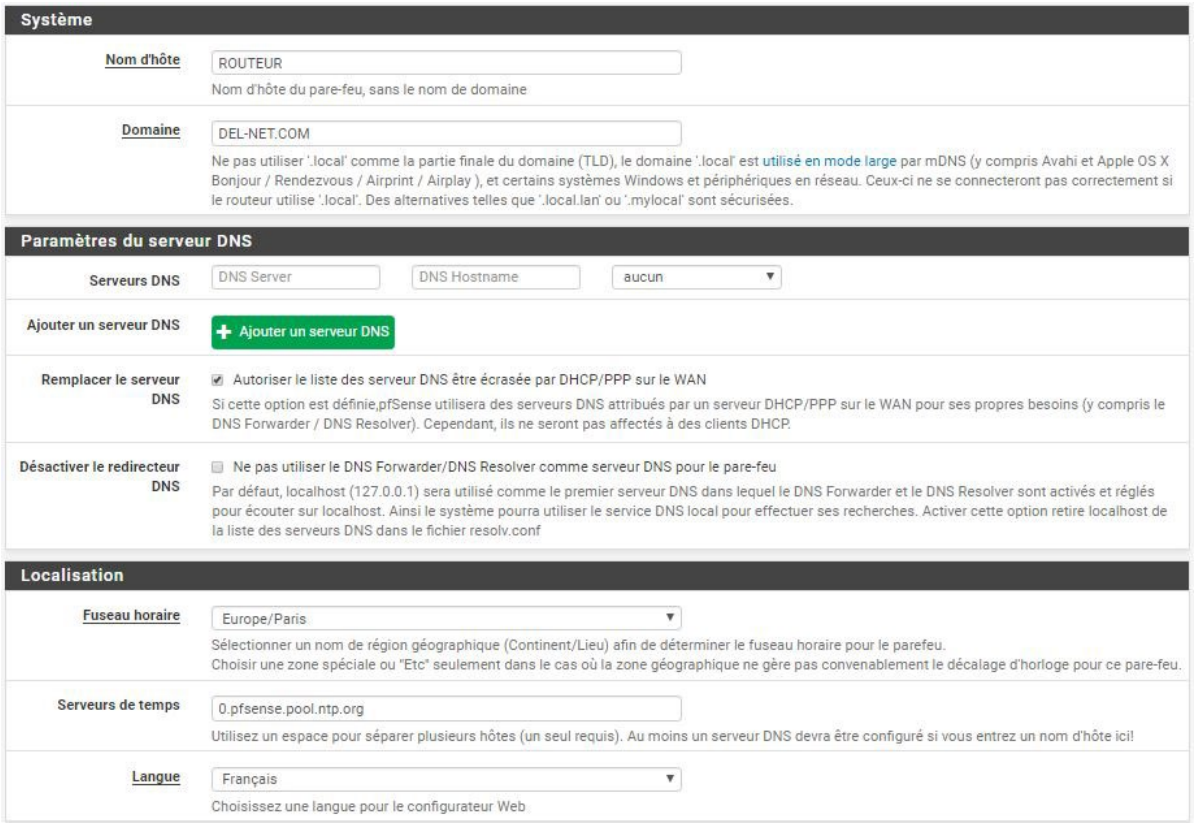




Enregistrer le mot de passe en cliquant sur Save en bas de la page.

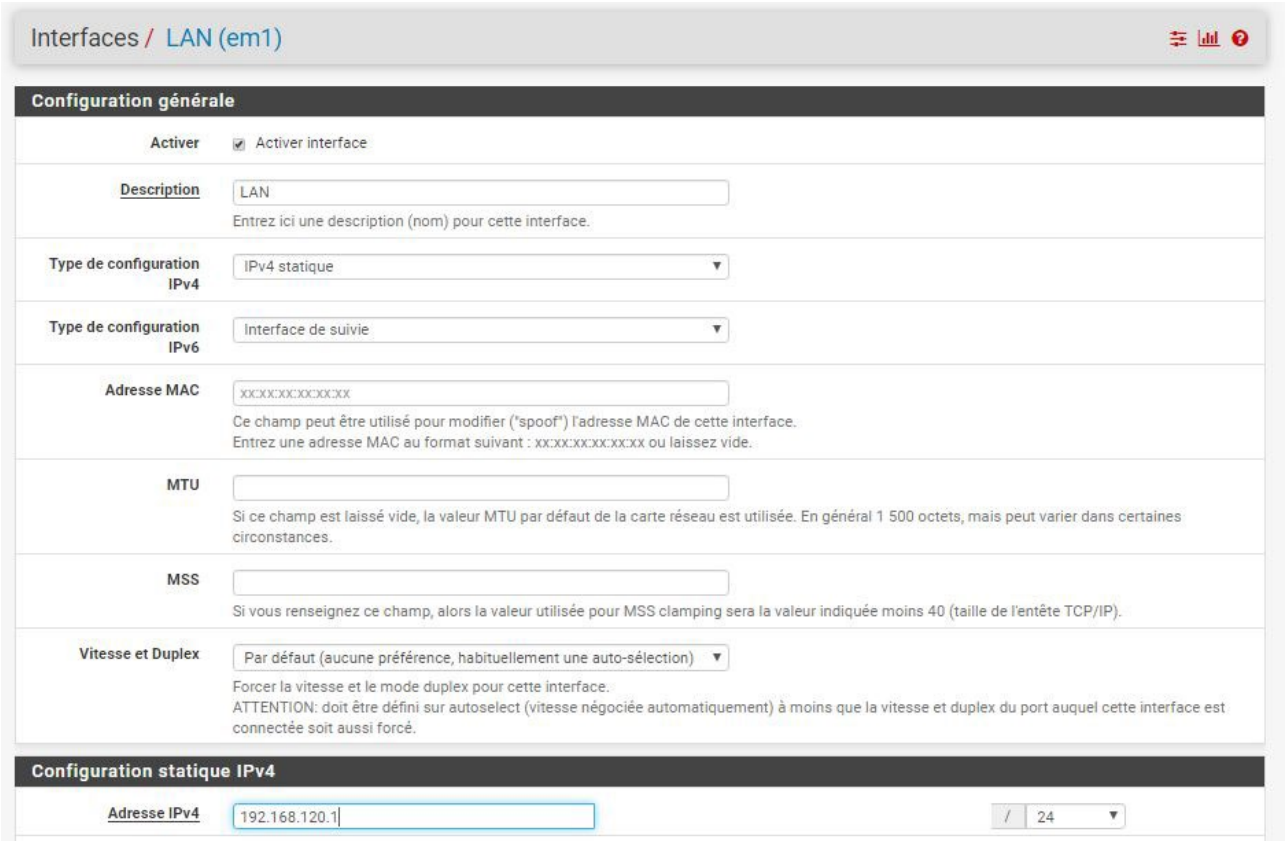
Configuration de base :

Aller dans System > General setup et donner un nom, une zone de temps et choisir une langue pour votre routeur.



Adresse IP routeur :

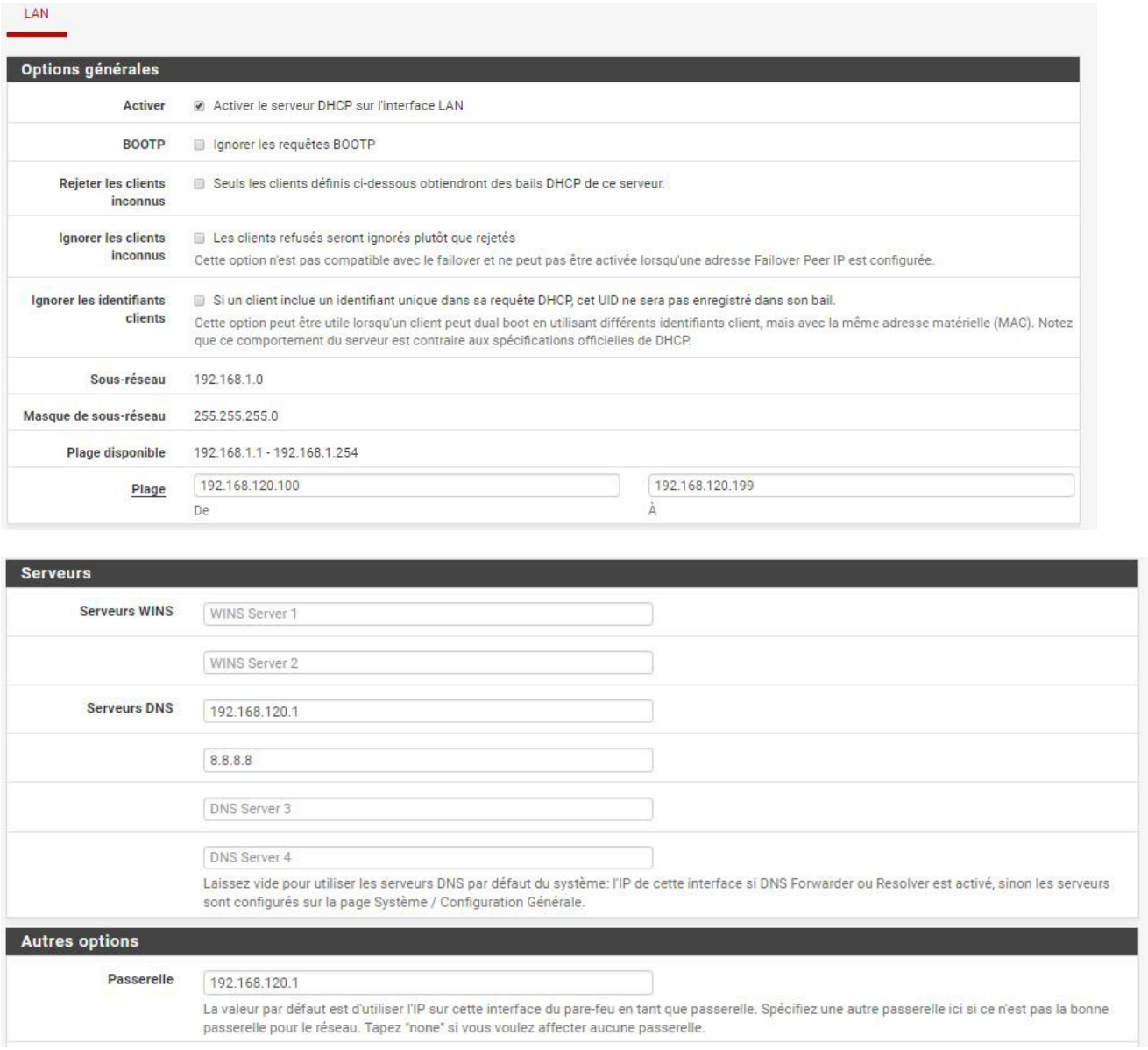
Allers dans Interface > LAN puis changer l'adresse IP du routeur sans appliquer les modifications.



DHCP :

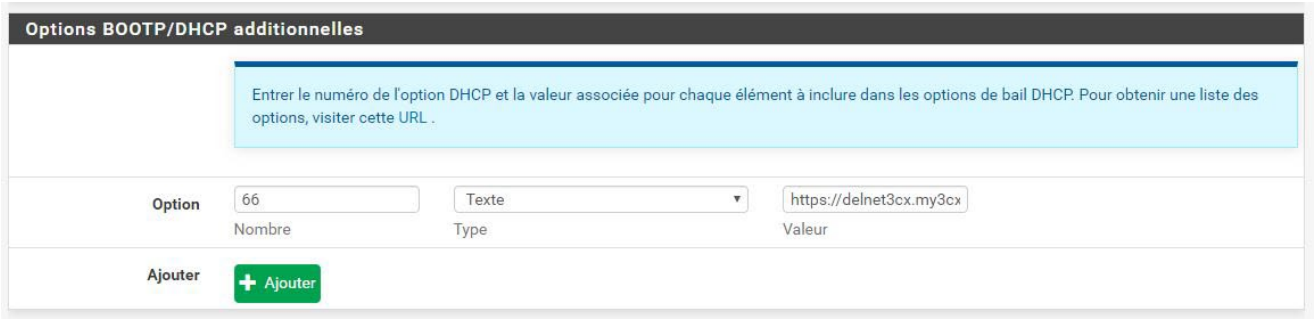
Aller dans Services > Serveur DHCP

Configurer la plage DHCP et renseigner passerelle et DNS.



Option 66 – VOIP :

Dans Services > Serveur DHCP vous pouvez configurer des options.



Appliquer les modifications puis se connecter sur la nouvelle adresse IP :

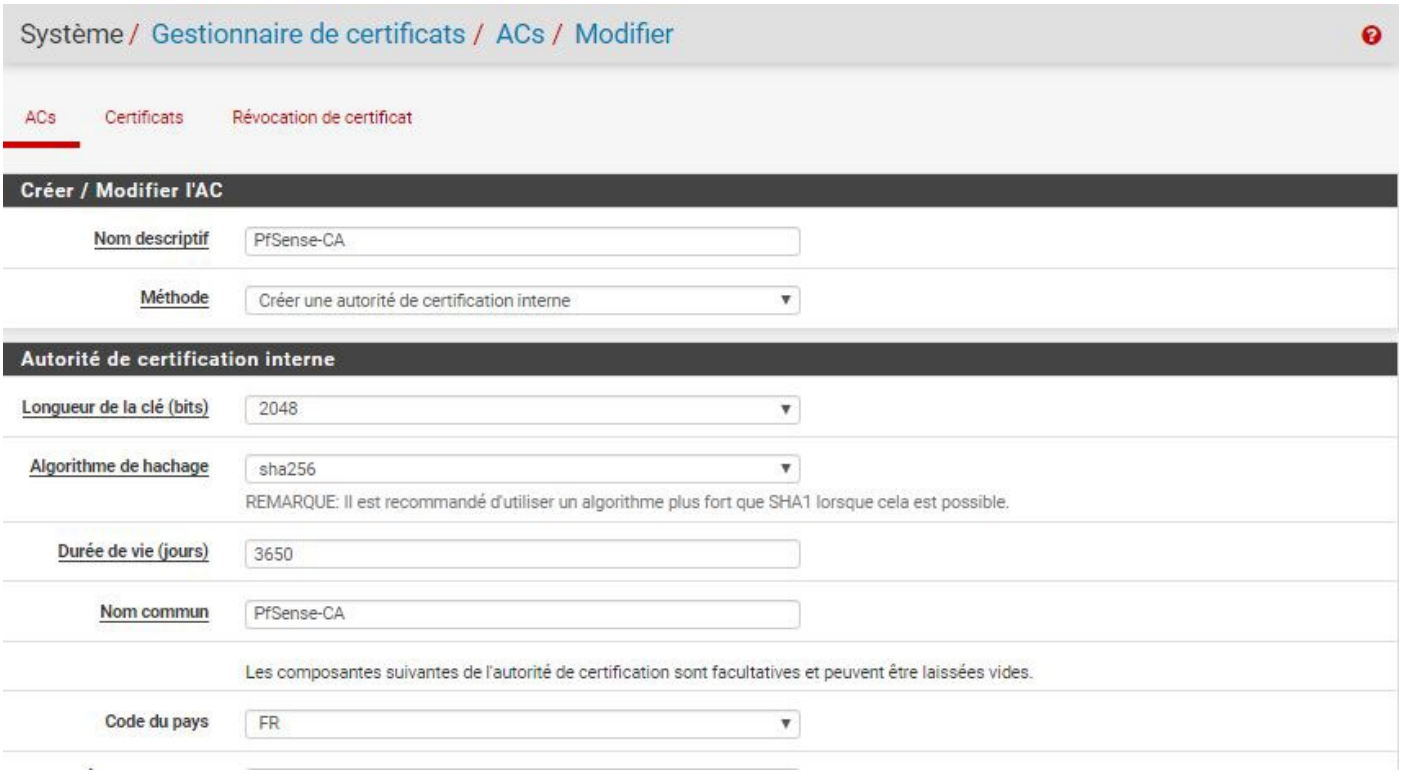
Changer port :

Aller dans Système > Avancé > Accès Administrateur et changer le port de connexion au routeur.

4/- Configuration d'une connexion nomade - OpenVPN.

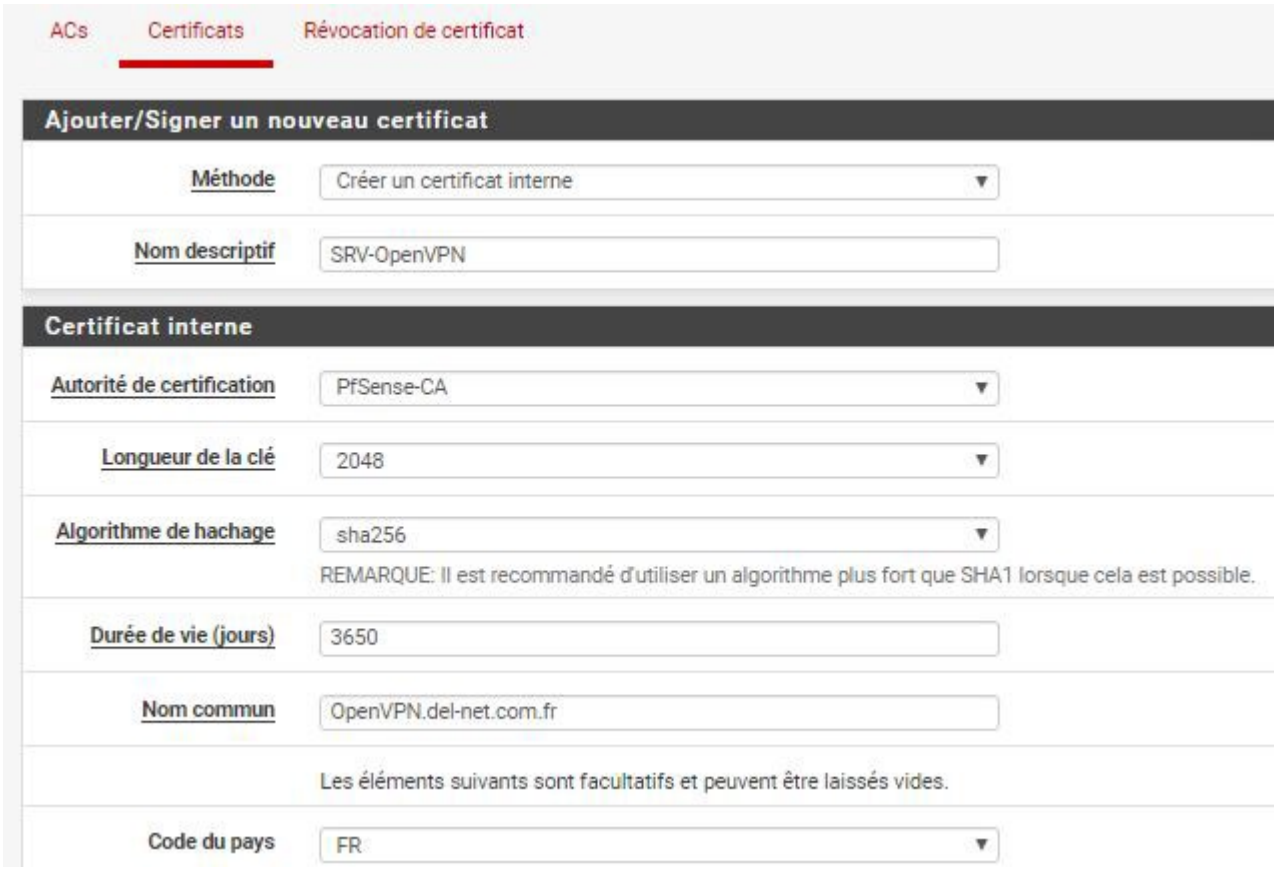
Création d'une Autorité de certification :

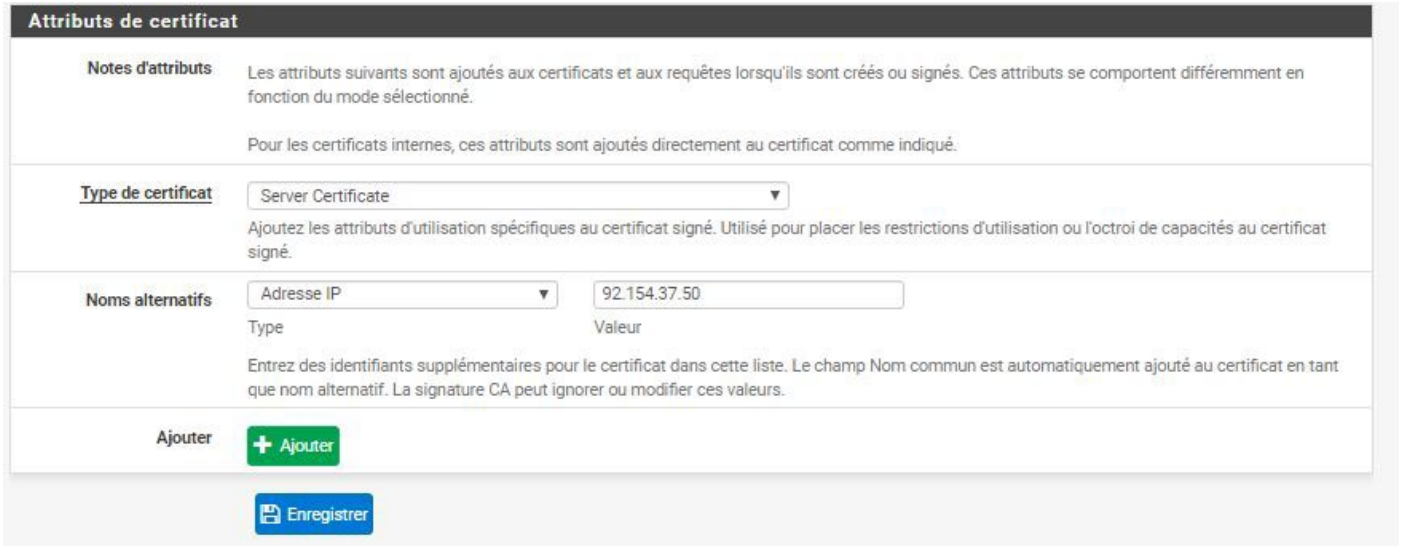
Donner un nom à l'autorité de certification.



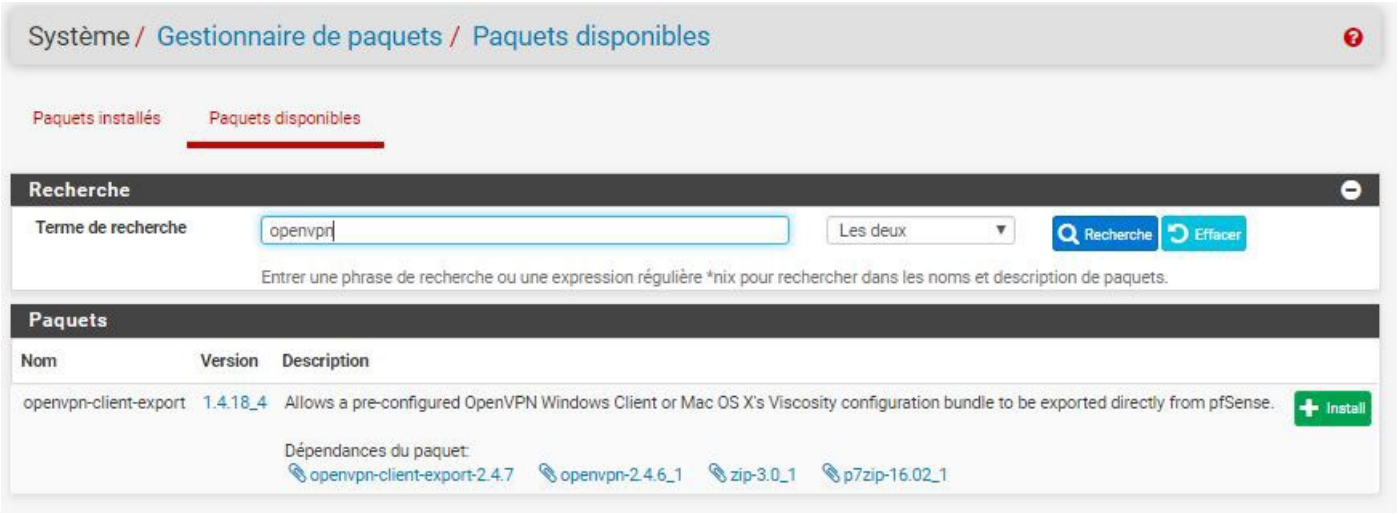
Création d'un certificat pour le serveur VPN :

Donner un nom à notre certificat, sélectionner l'autorité de certification précédemment créée, choisir le type de certificat (serveur) et indiquer le nom et/ou adresse IP de la connexion WAN.





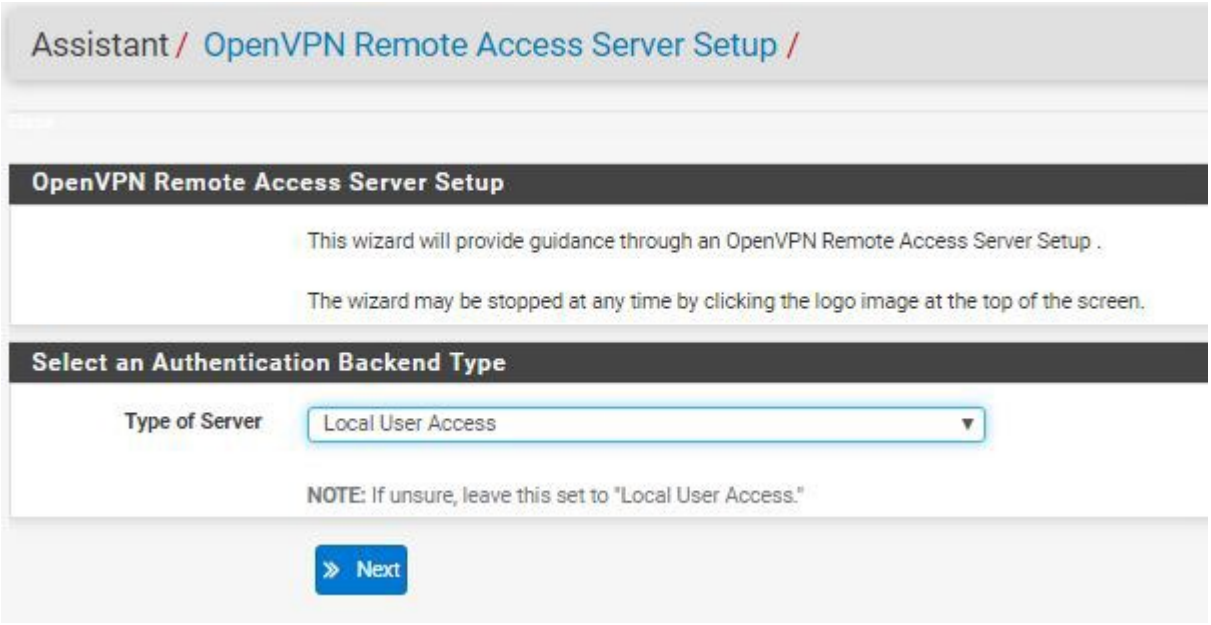
Installation du paquet OpenVPN-Client-Export :



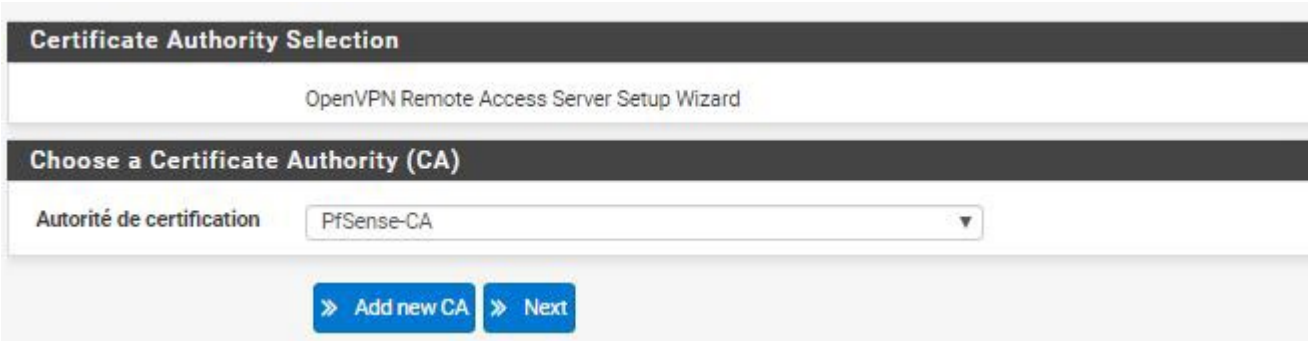
Lancement de l'assistant :

VPN > OpenVPN > Assistant :

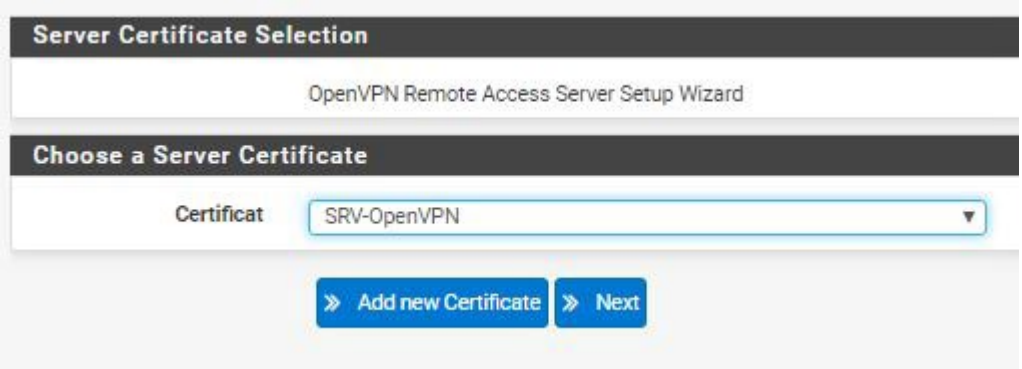
Laisser Local User Access.



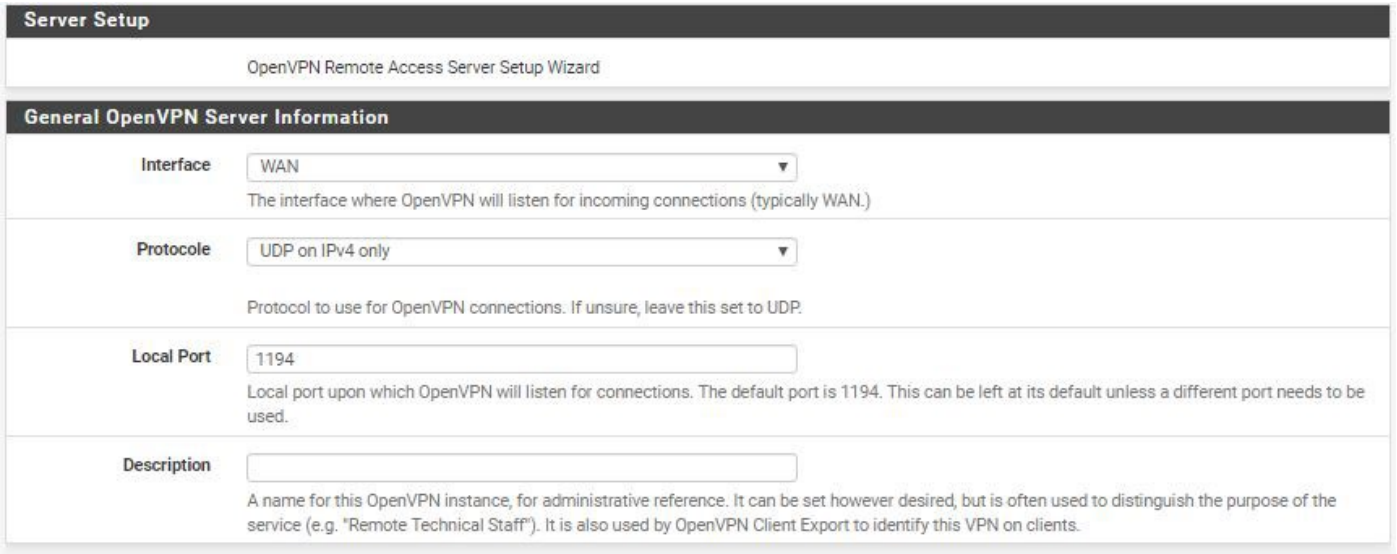
Indiquer l'autorité de certification que nous avons créé.



Indiquer le certificat serveur que nous avons créé.



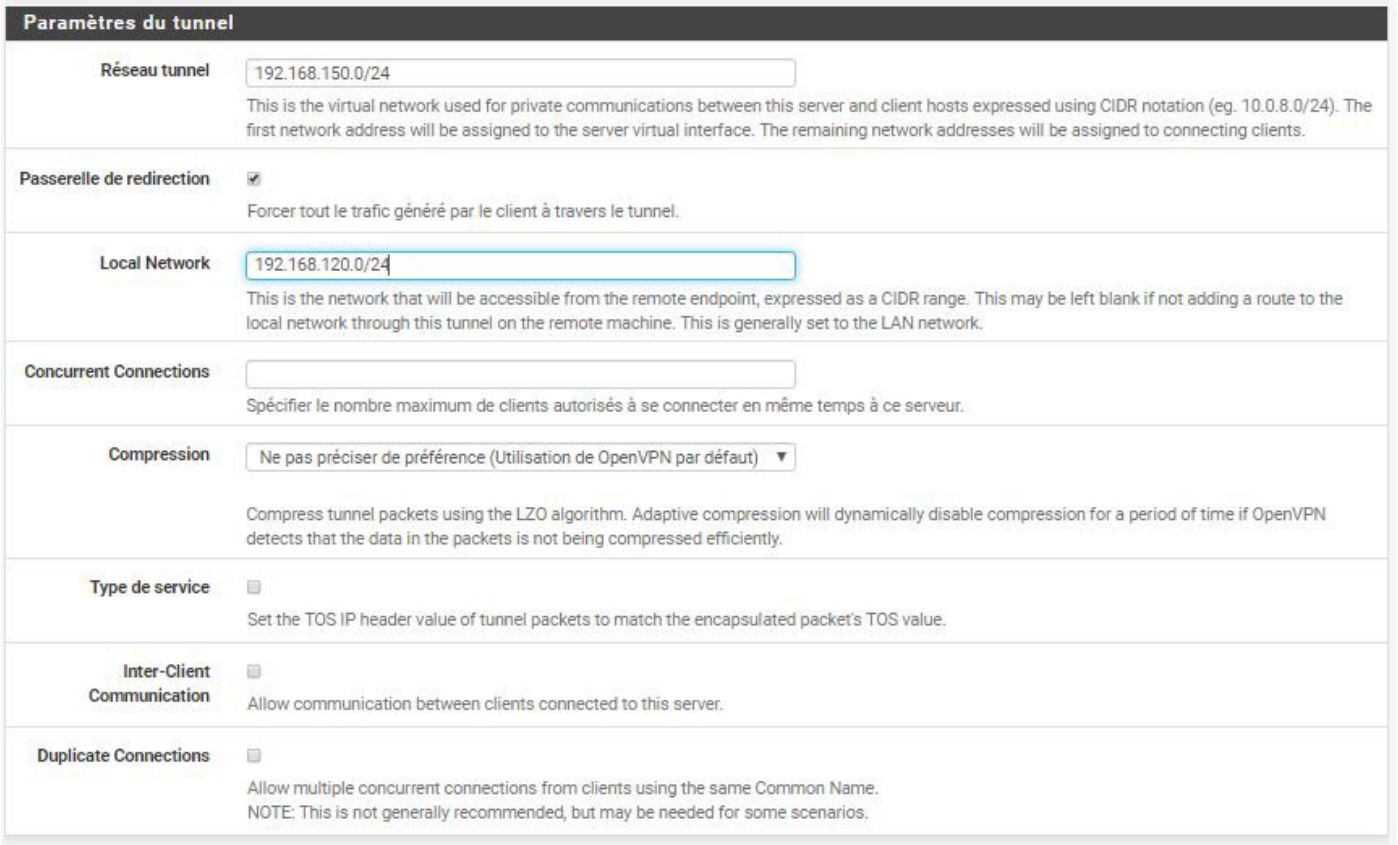
Indiquer un port à utiliser pour le VPN qu'il faudra ouvrir dans le pare-feu.



Renseigner une adresse réseau pour le VPN.

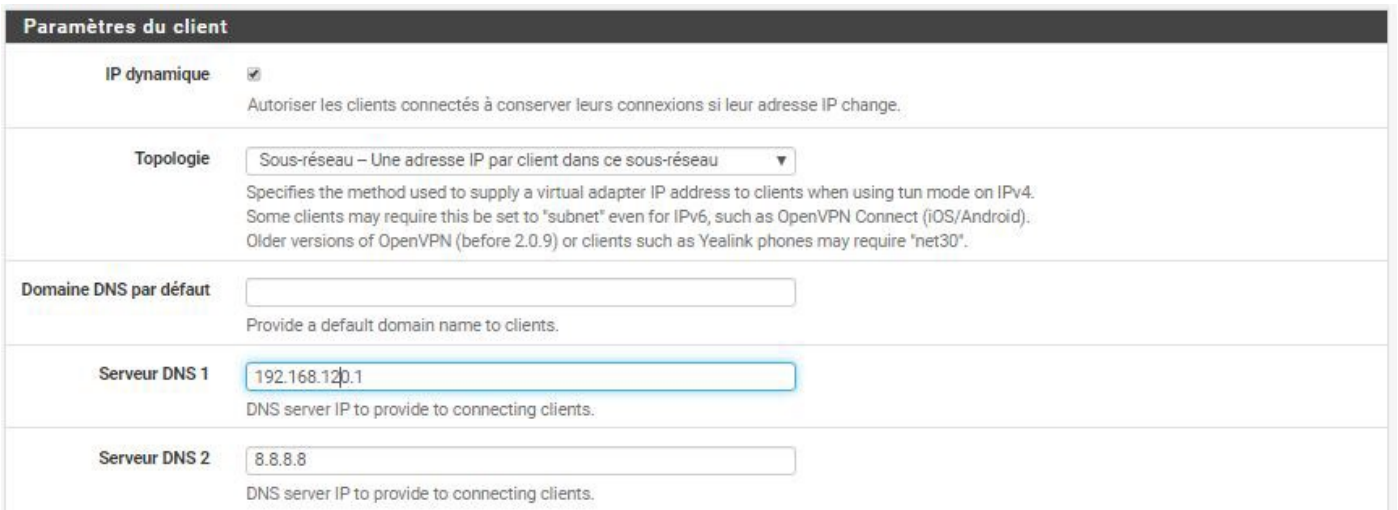
Cocher la redirection du trafic.
Renseigner l'adresse réseau local à laquelle le VPN aura accès.

Renseigner les serveurs DNS.



Paramètres du tunnel

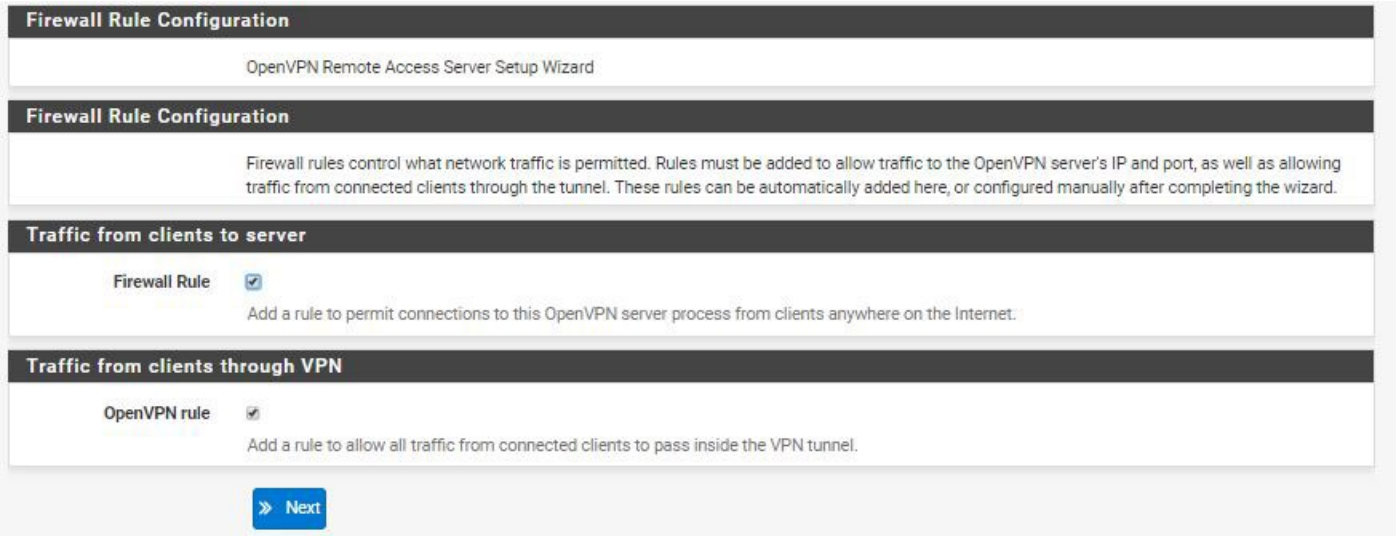
Réseau tunnel	192.168.150.0/24 This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.
Passerelle de redirection	☑ Forcer tout le trafic généré par le client à travers le tunnel.
Local Network	192.168.120.0/24 This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. 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	 Spécifier le nombre maximum de clients autorisés à se connecter en même temps à ce serveur.
Compression	Ne pas préciser de préférence (Utilisation de OpenVPN par défaut) Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.
Type de service	☐ Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
Inter-Client Communication	☐ Allow communication between clients connected to this server.
Duplicate Connections	☐ Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.



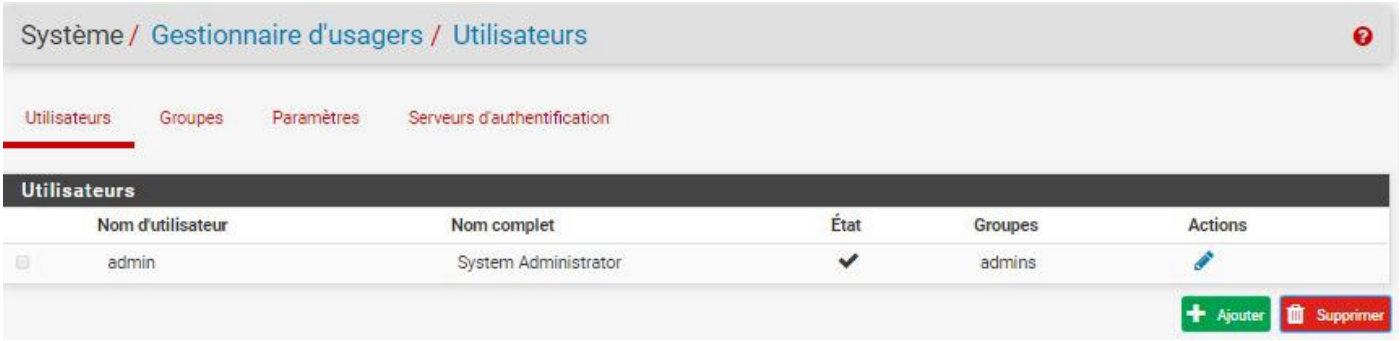
Paramètres du client

IP dynamique	☑ Autoriser les clients connectés à conserver leurs connexions si leur adresse IP change.
Topologie	Sous-réseau – Une adresse IP par client dans ce sous-réseau 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".
Domaine DNS par défaut	 Provide a default domain name to clients.
Serveur DNS 1	192.168.120.1 DNS server IP to provide to connecting clients.
Serveur DNS 2	8.8.8.8 DNS server IP to provide to connecting clients.

Cocher la configuration automatique des règles de pare-feu.

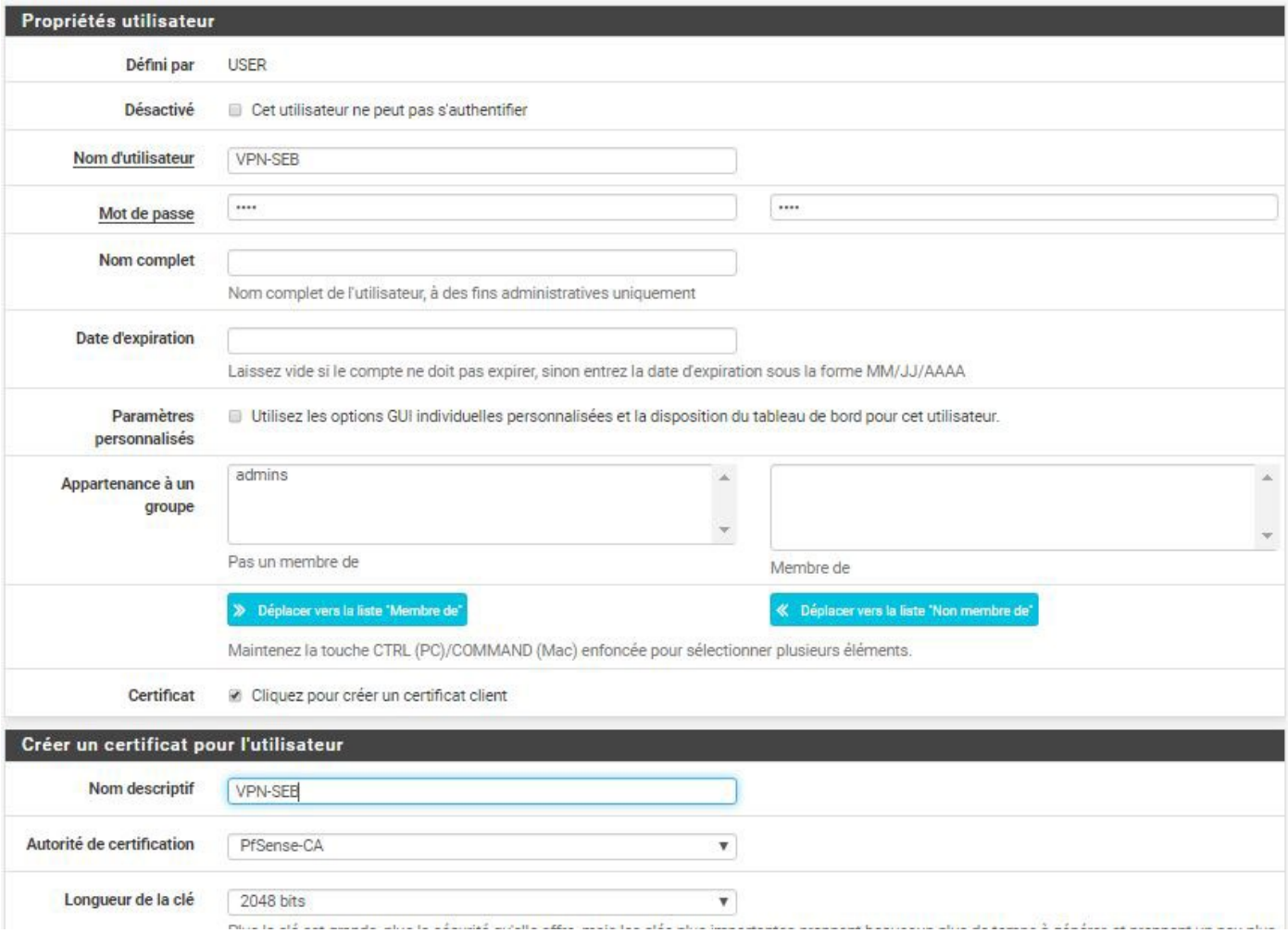


Création d'un utilisateur pour l'accès au VPN :

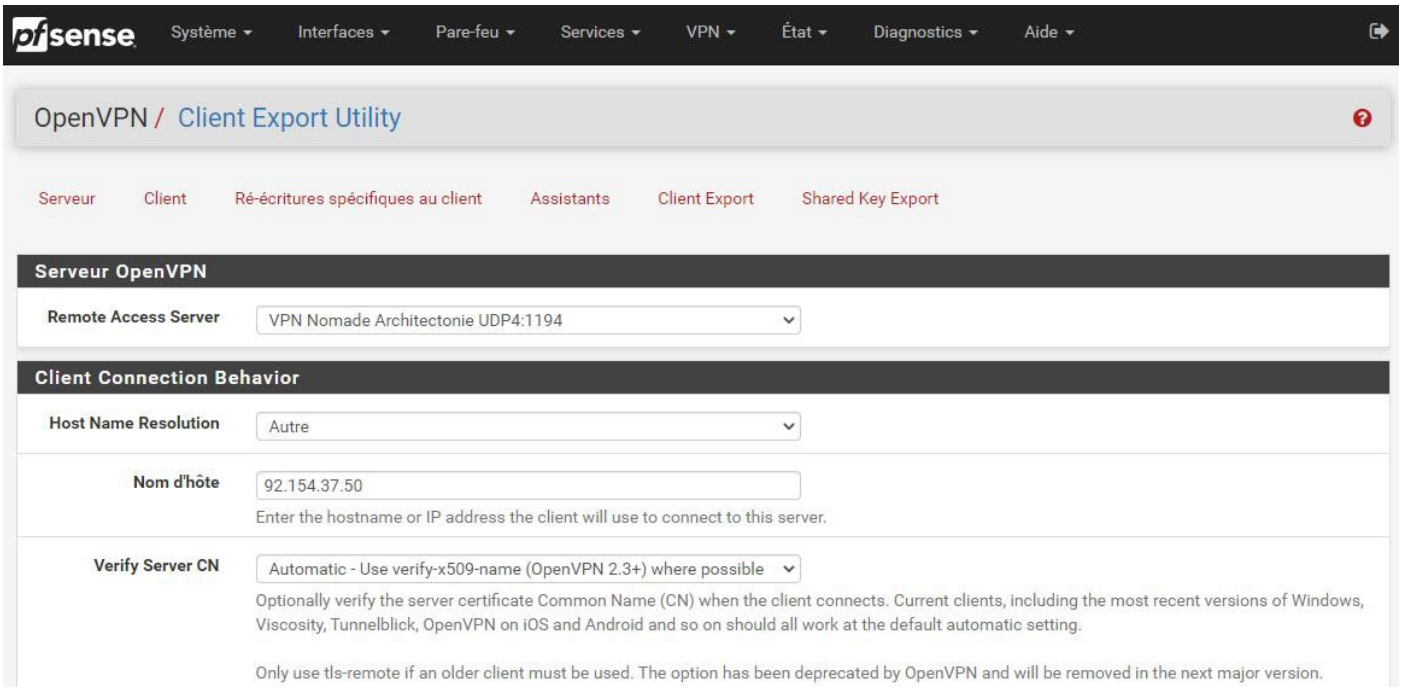


Donner un nom à votre utilisateur et un mot de passe.

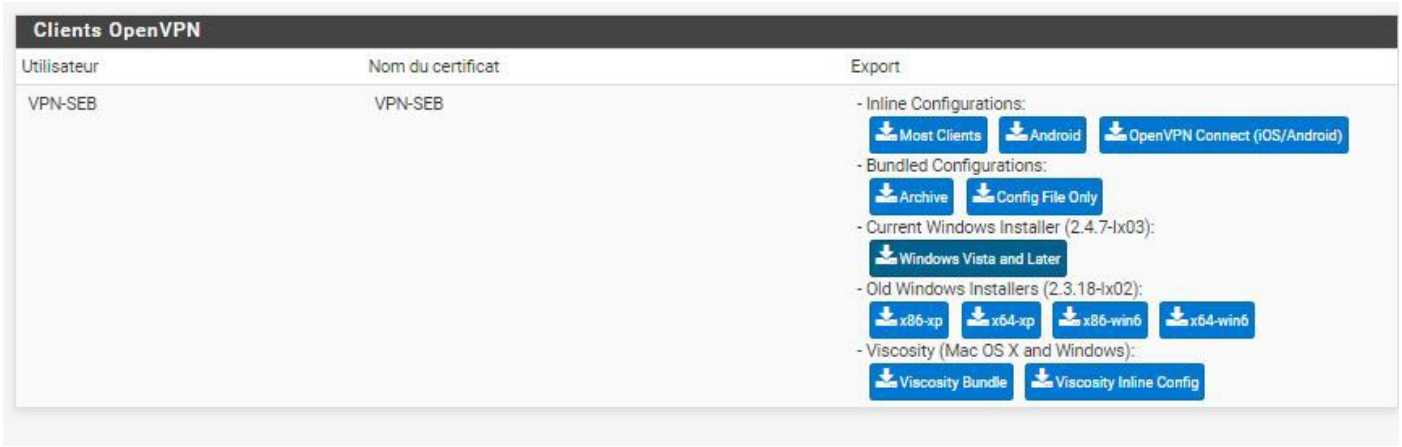
Cocher la création d'un certificat et choisir l'autorité de certification.


Propriétés utilisateur
Défini par
USER
Désactivé
Cet utilisateur ne peut pas s'authentifier
Nom d'utilisateur
VPN-SEB
Mot de passe
Nom complet
Nom complet de l'utilisateur, à des fins administratives uniquement
Date d'expiration
Laissez vide si le compte ne doit pas expirer, sinon entrez la date d'expiration sous la forme MM/JJ/AAAA
Paramètres personnalisés
Utilisez les options GUI individuelles personnalisées et la disposition du tableau de bord pour cet utilisateur.
Appartenance à un groupe
admins
Pas un membre de
Membre de
Déplacer vers la liste "Membre de"
Déplacer vers la liste "Non membre de"
Maintenez la touche CTRL (PC)/COMMAND (Mac) enfoncée pour sélectionner plusieurs éléments.
Certificat
Cliquez pour créer un certificat client
Créer un certificat pour l'utilisateur
Nom descriptif
VPN-SEB
Autorité de certification
PfSense-CA
Longueur de la clé
2048 bits

Dans la partie OpenVPN > Client Export Utility, choisir Autre au niveau "Host Name Résolution" et renseigner l'adresse IP de votre interface WAN.



Vous pouvez ensuite exporter votre configuration.



5- Configuration d'une protection sur la page d'administration.

Aller dans Système > Avancé

Puis dans la partie Login Protection, définir le seuil de tentative avant blocage à 10, le Blocktime à 300 et le Detection time à 1800.