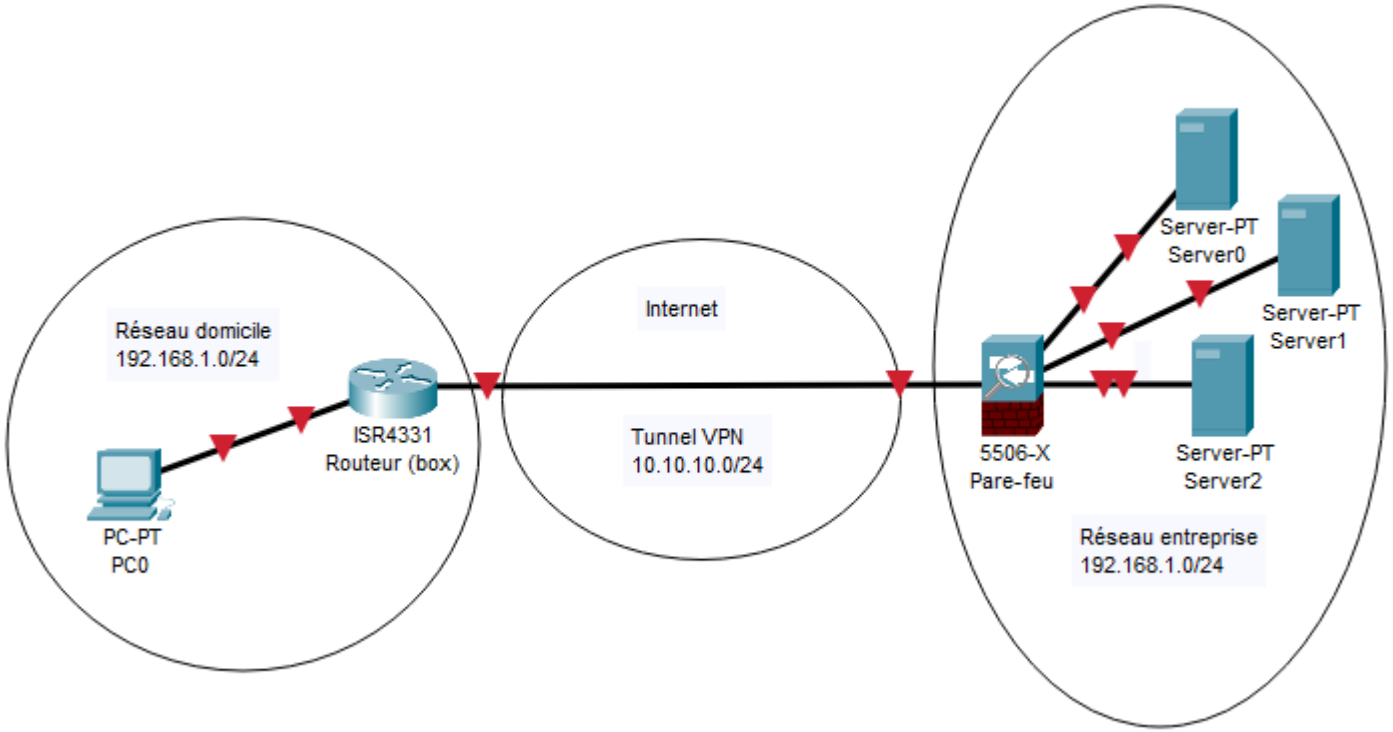
TP VPN pfSense

FLORENTIN BRACQ-FLABAT BTS 2 SIO

Qu’est-ce qu’un VPN ?

Un VPN, ou Virtual Private Network (réseau privé virtuel), est une technologie qui permet de créer une connexion sécurisée et chiffrée entre votre appareil (ordinateur, smartphone, etc.) et un serveur distant via Internet.

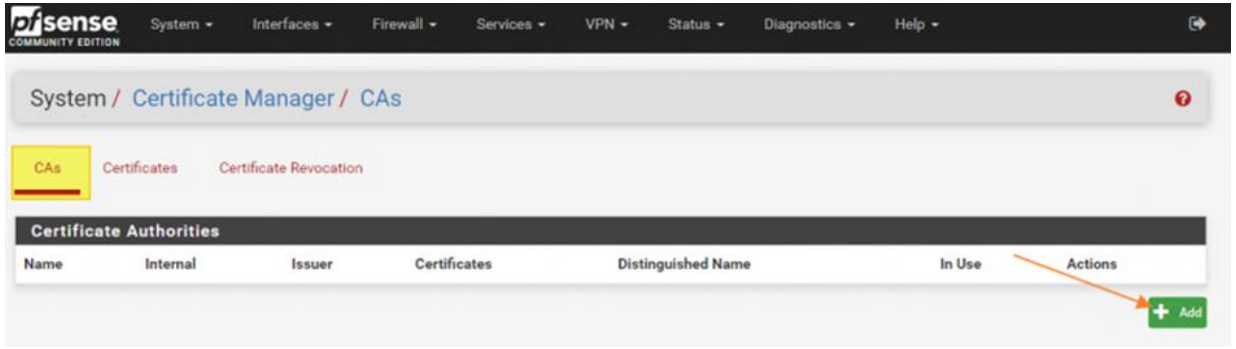
Schéma réseau

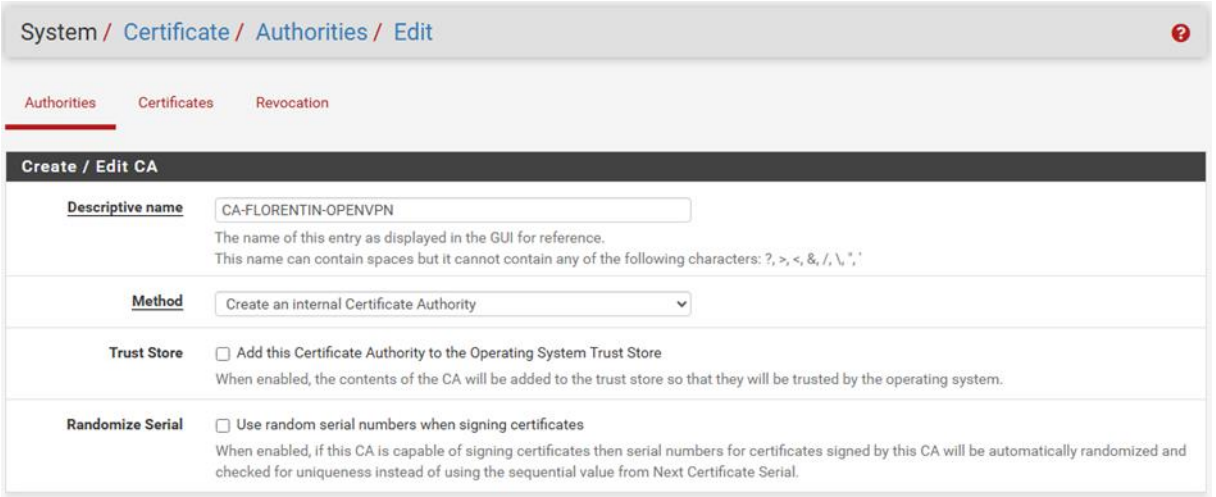


Création de l’autorité de certification

Une fois connecté à l’interface web d’administration de pfSense, cliquer sur System puis Cert. Manager (Certificates), dans l’onglet Cas, cliquer sur Add

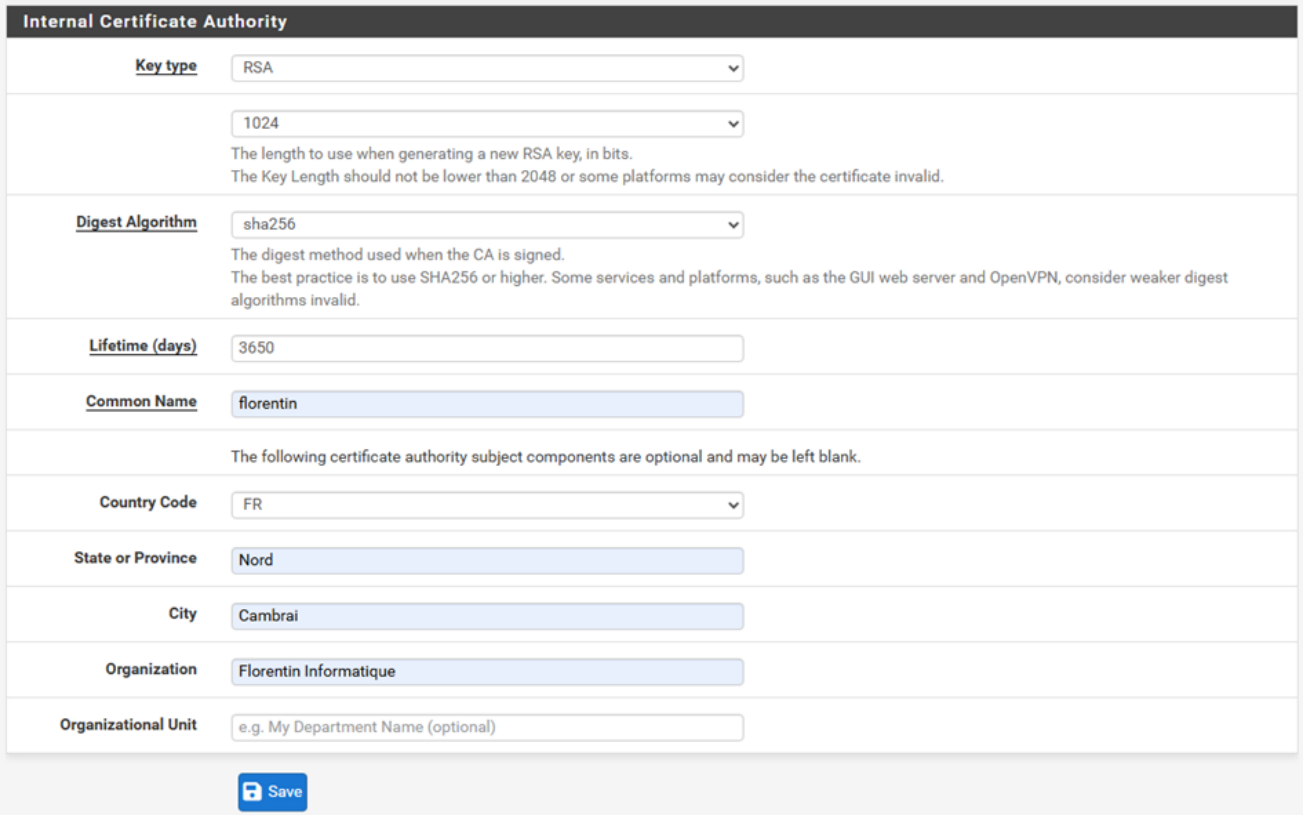
Donner un nom à l'autorité de certification CA-FLORENTIN-OPENVPN, et choisir Create an internal Certificate Authority

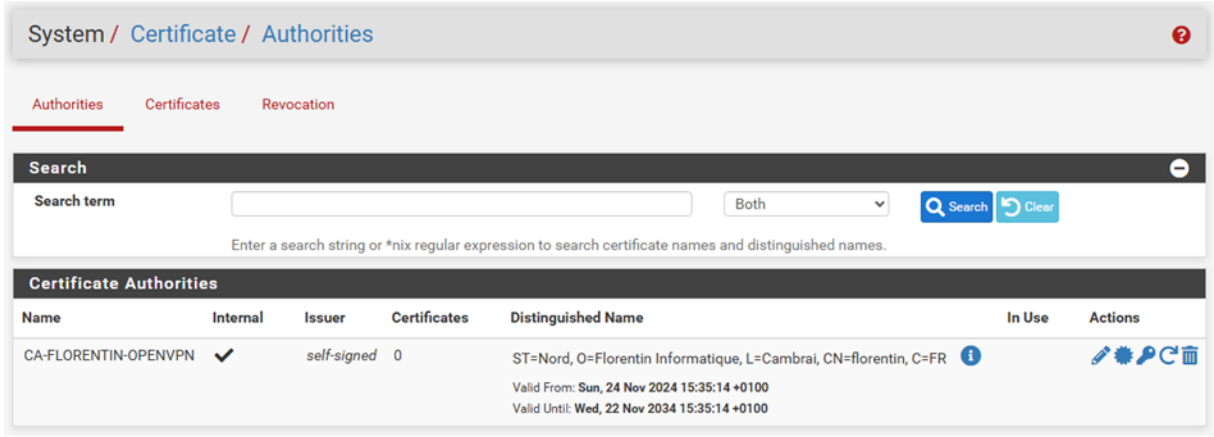




Création de l’autorité de certification

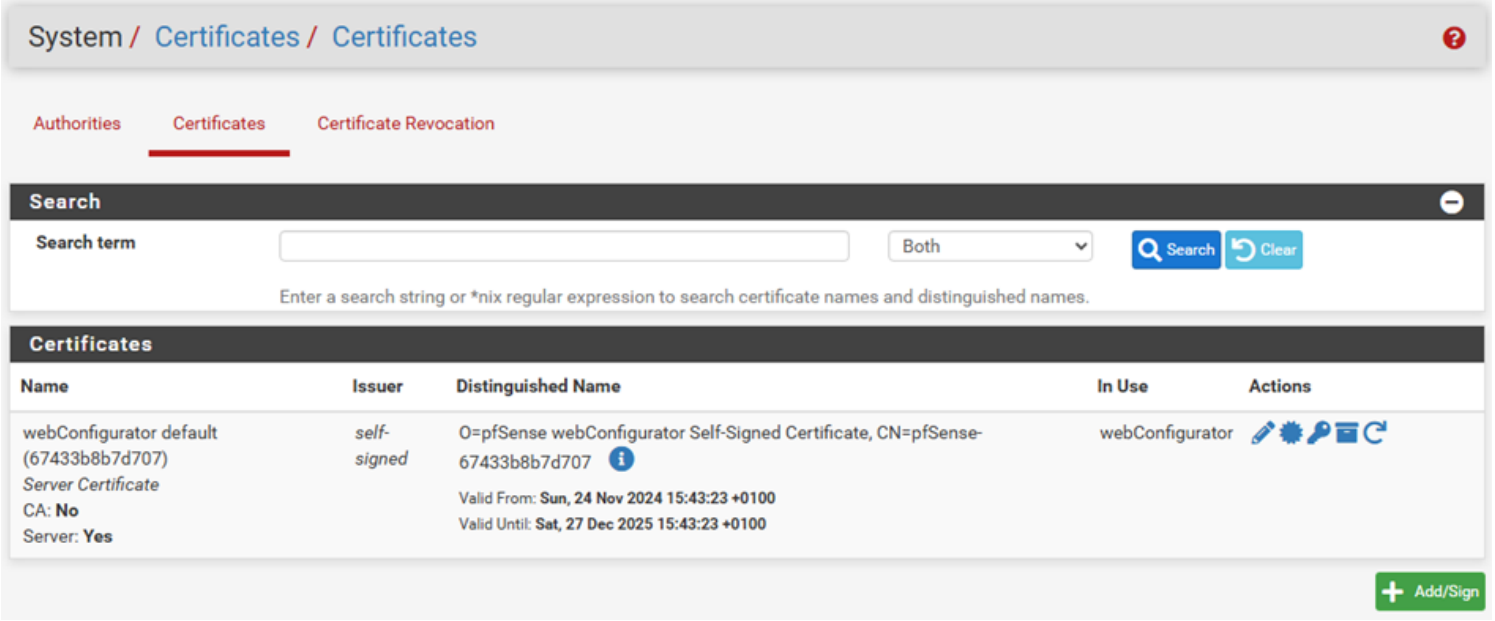
Pour Common Name, mettre florentin et compléter les autres valeurs : la région, la ville, etc... et cliquez sur "Save" pour créer la CA.





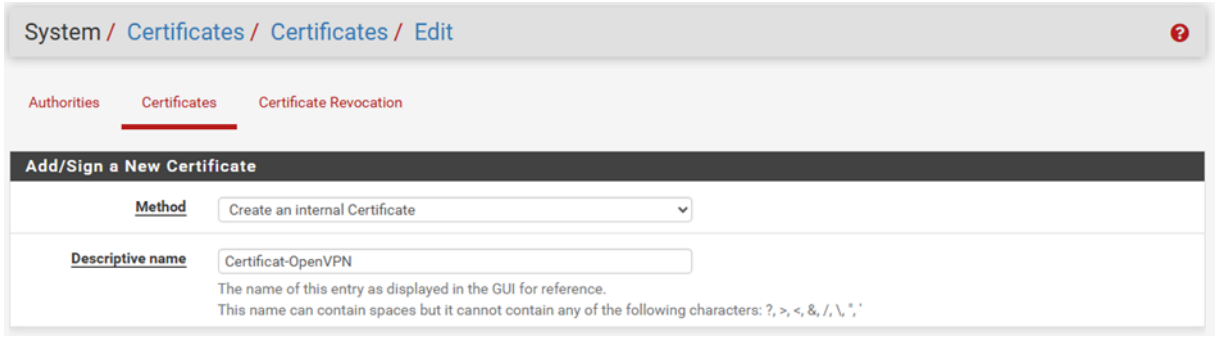
Création du certificat interne

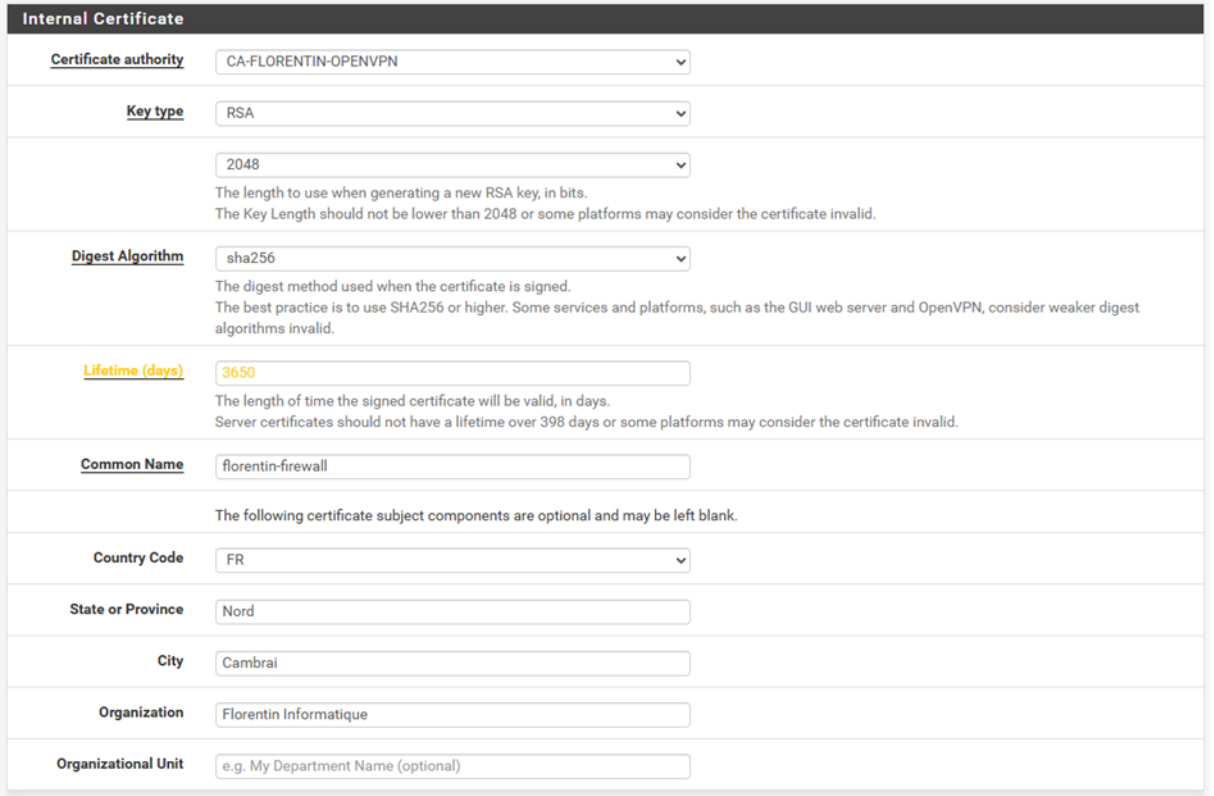
Cliquer ensuite sur l'onglet Certificates et cliquer sur Add



Création du certificat interne

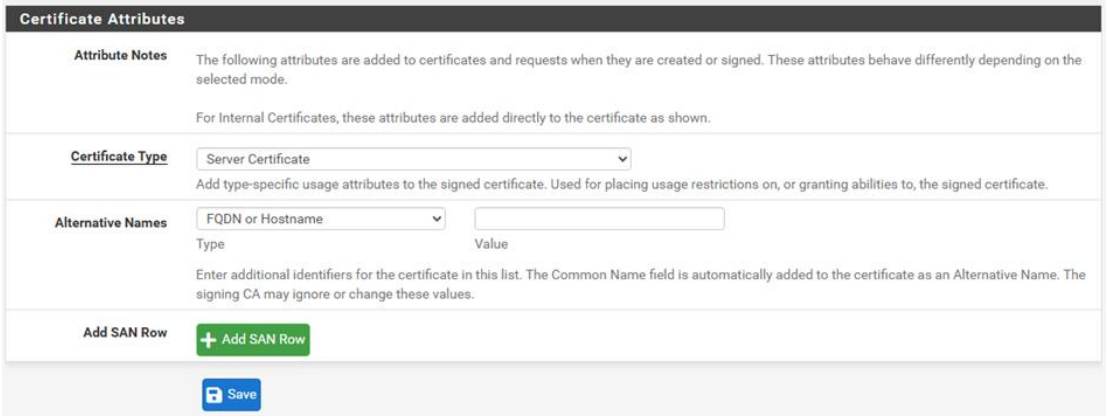
Choisir la méthode Create an Internal Certificate puisqu'il s'agit d'une création, donnez-lui un nom et sélectionnez l'autorité de certification au niveau du paramètre "Certificate authority".



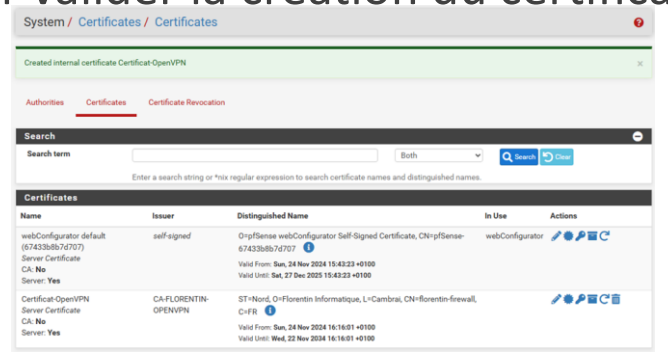


Création du certificat interne

Choisissez bien le type de certificat (Certificate Type) suivant : Server Certificate et cliquer sur save pour enregistrer les modifications.

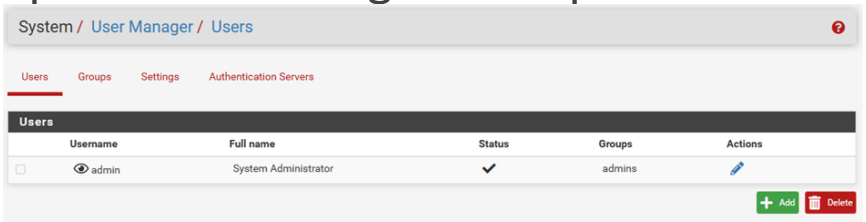


Après avoir cliqué sur "Save" pour valider la création du certificat, il apparaît dans la liste des certificats du Pare-feu :

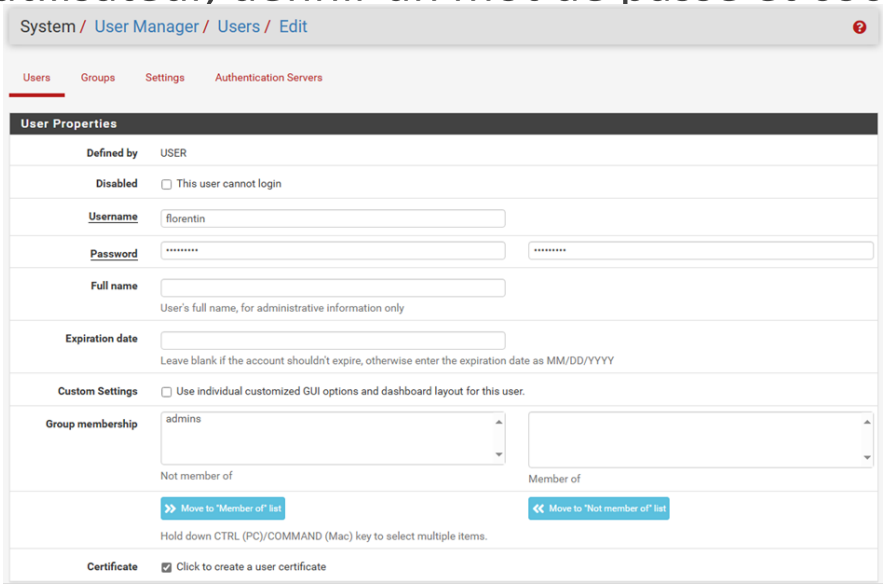


Création des utilisateurs locaux

Cliquer en haut dans System puis User Manager et cliquer sur Add

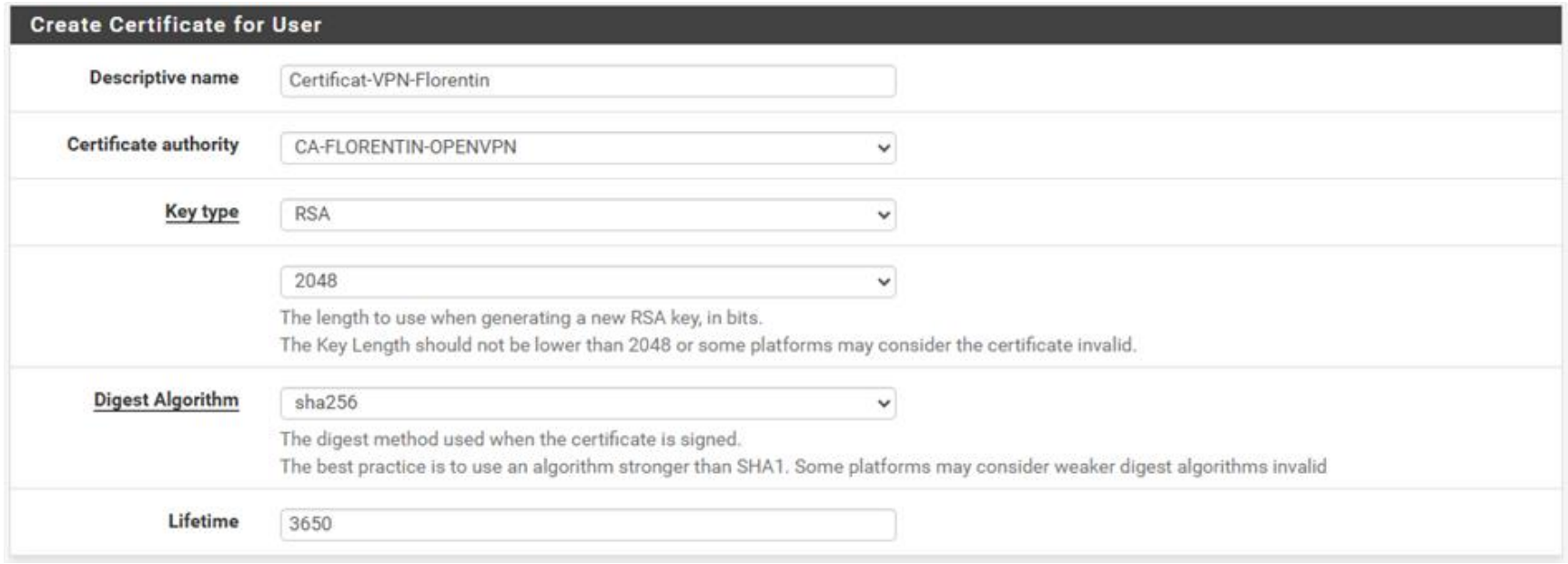


Donner un nom au nouvel utilisateur, définir un mot de passe et cocher la case certificate



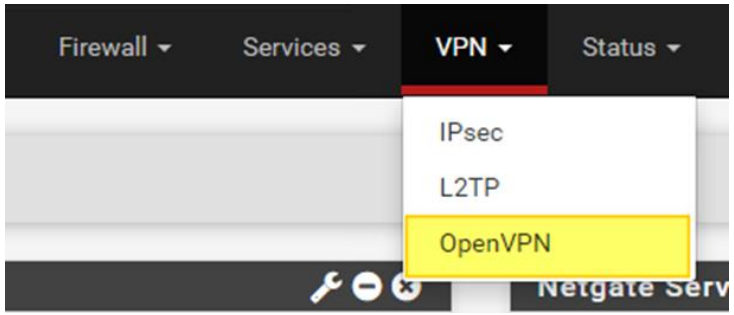
Création des utilisateurs locaux

Donner un nom au certificat utilisateur qui va être crée et cliquer sur Save pour enregistrer les modifications :

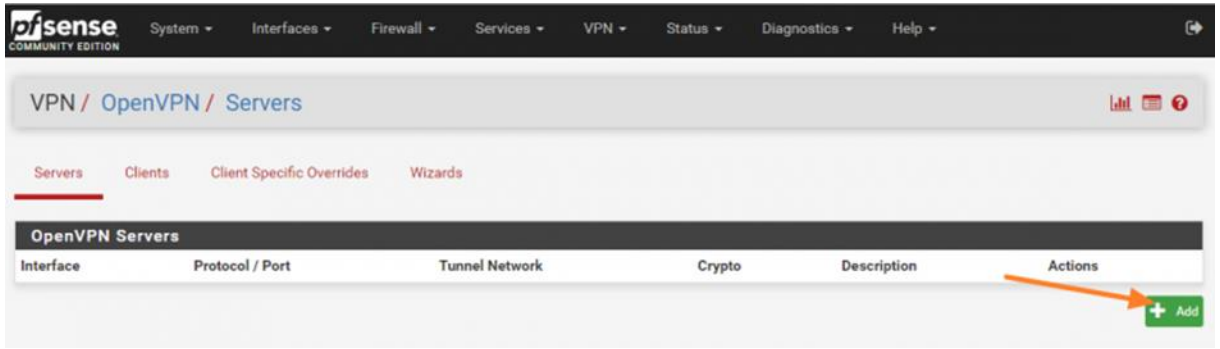


Configurer le serveur OpenVPN

Cliquer sur le menu « VPN » puis « OpenVPN »

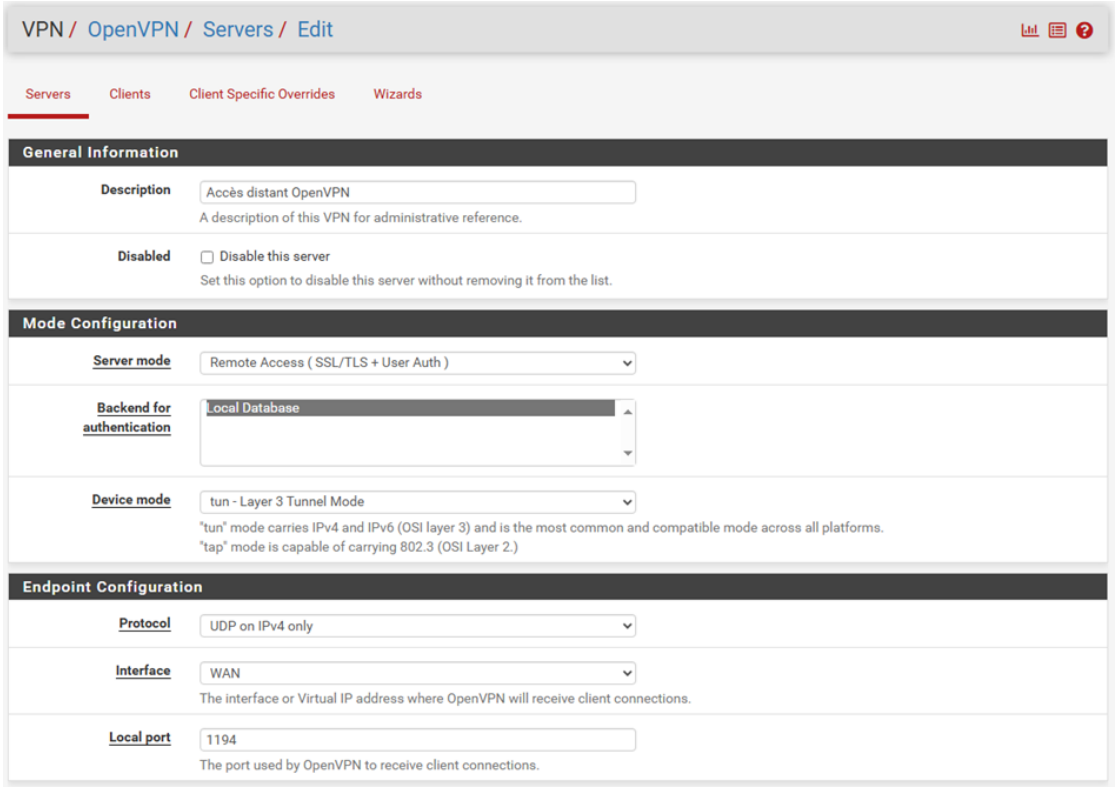


Dans l'onglet « Servers », cliquer sur « Add » pour créer une nouvelle configuration.



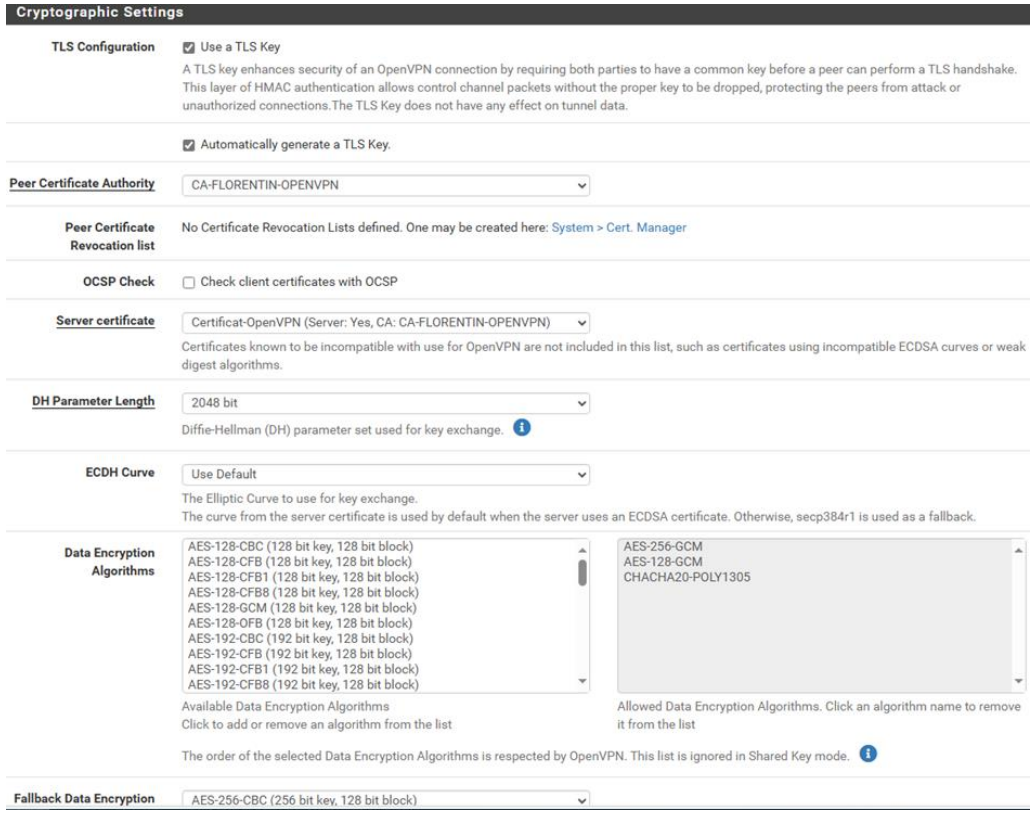
Configurer le serveur OpenVPN

Toujours dans l'onglet Serveurs, donner une description, pour Serveur mode, choisir Remote Access (SSL/TLS + User Auth)



Configurer le serveur OpenVPN

Pour serveur certificate choisir le certificat serveur crée précédemment et pour Fallback Data Encryption choisir AES-256-CBC :

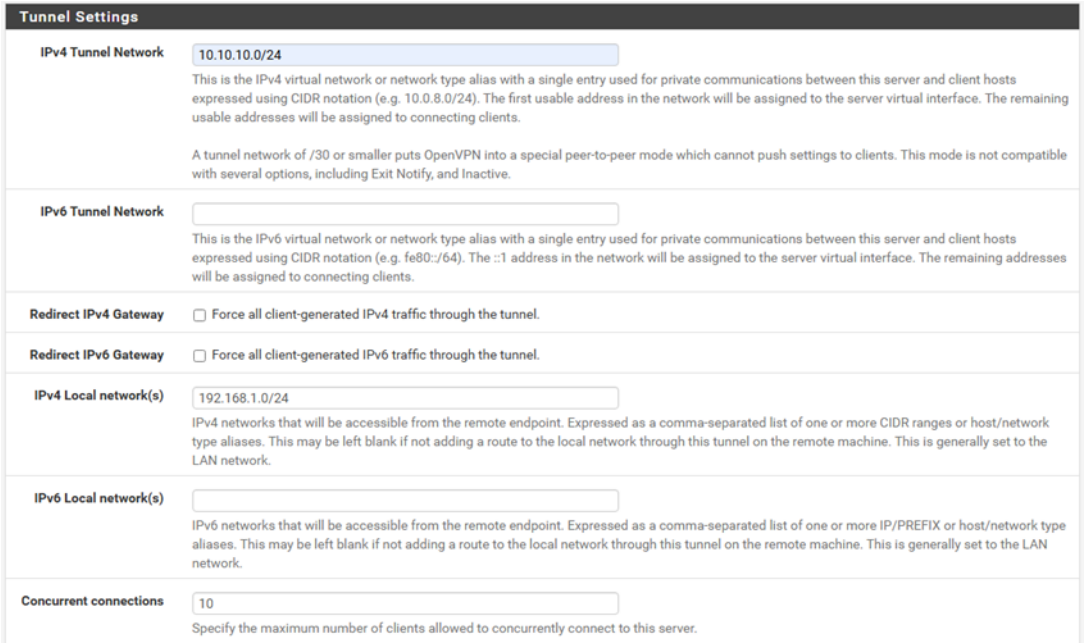


Configurer le serveur OpenVPN (Tunnel VPN)

Donner l’adresse IP du tunnel 10.10.10.0/24

Donner l’adresse IP du réseau local 192.168.1.0/24

Et définir le nombre de connexion simultané maximum par exemple 10



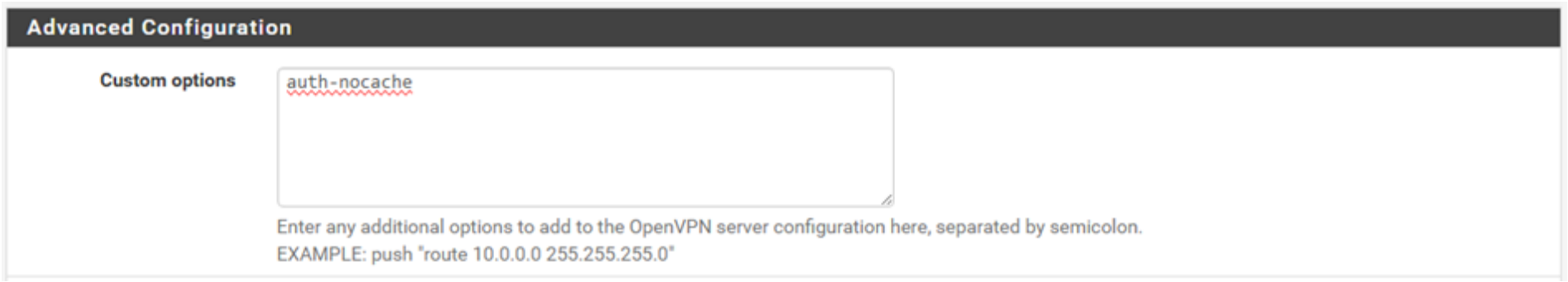
Configurer le serveur OpenVPN

Pour la partie Client Settings

Activer le Dynamic IP si les clients sont nomades et que leur adresse IP publique change pour maintenir la connexion VPN, activer le protocole net30 qui permettra à chaque client connecté de se trouver dans un sous réseau sans pouvoir communiquer avec les autres clients en VPN.

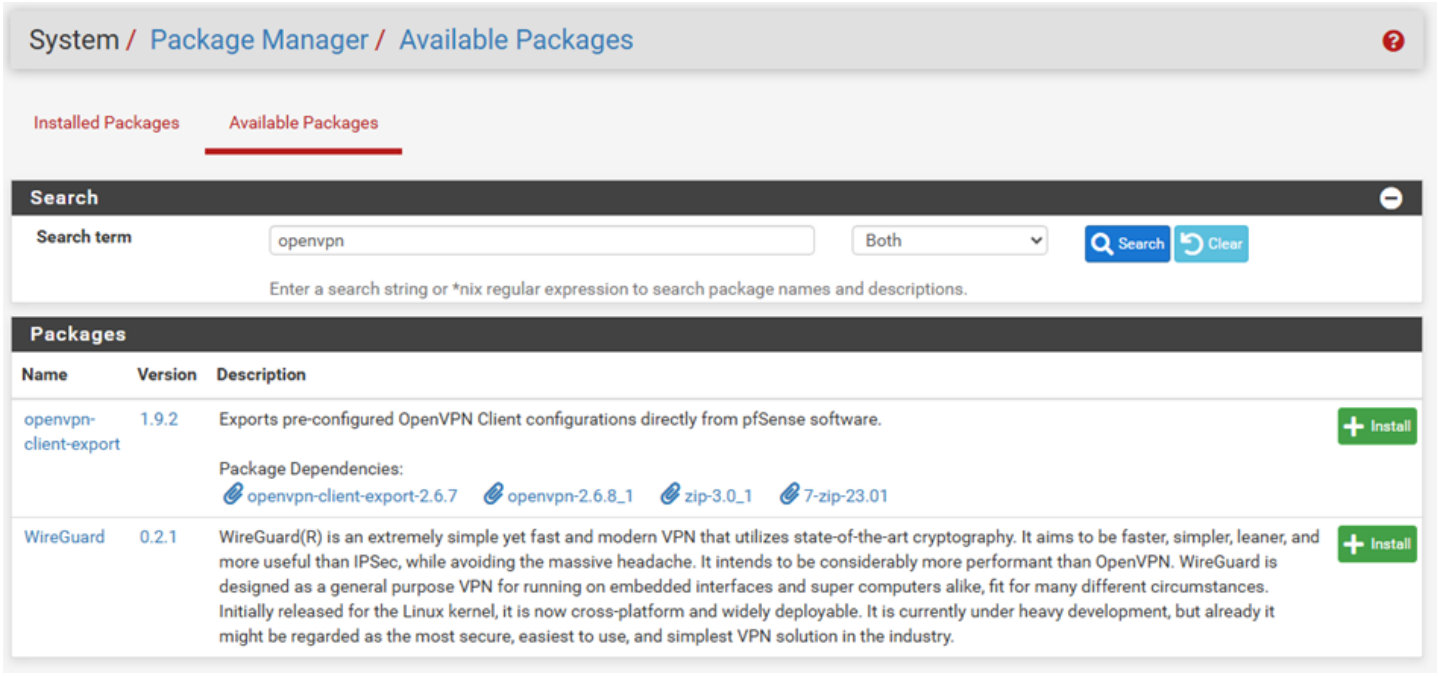
Configurer le serveur OpenVPN

Et pour Avanced Configuration, dans Custom options activer l'option auth-nocache qui permettra d'empêcher la mise en cache de l'authentification pour éviter une fuite des authentifications. Cliquer sur save pour enregistrer les modifications.



Installer le paquet client export

Dans la barre en haut, cliquer sur System puis Package Manager, puis cliquer sur l'onglet Available Package rechercher openvpn et installer le paquet openvpn-client-export



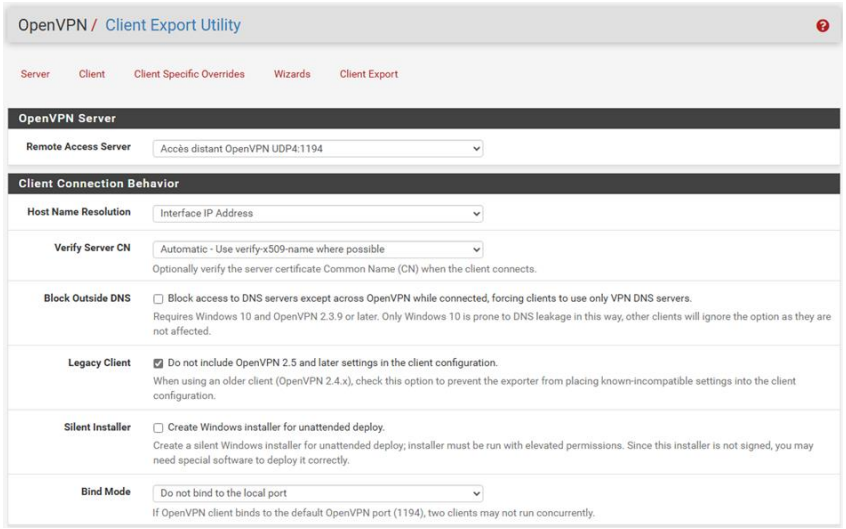
Exporter la configuration utilisateur

Dans la barre en haut cliquer sur VPN, puis OpenVPN et cliquer sur l'onglet Client Export

Choisir pour Host Name Resolution Interface IP Address et cocher la case Legacy Client pour les utilisateurs qui utilisent une version antérieure d'Open VPN.

Cliquer enfin sur Save as default

Et télécharger la version archive pour exporter la configuration VPN pour un utilisateur.

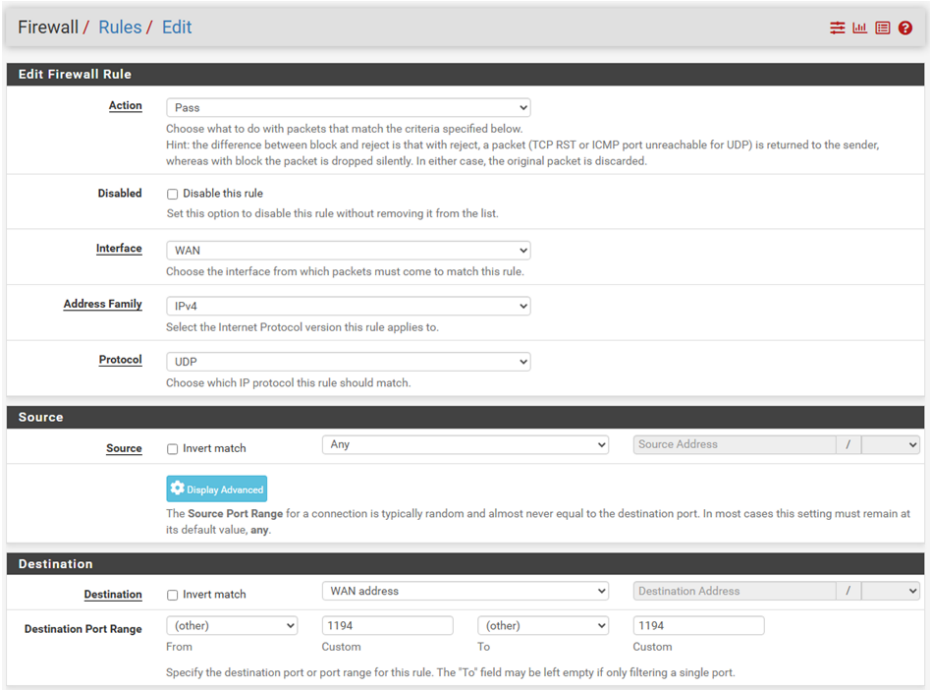


Modifier les règles de parfeu

Dans la barre en haut, cliquer sur Firewall, Rules, cliquer sur Add.

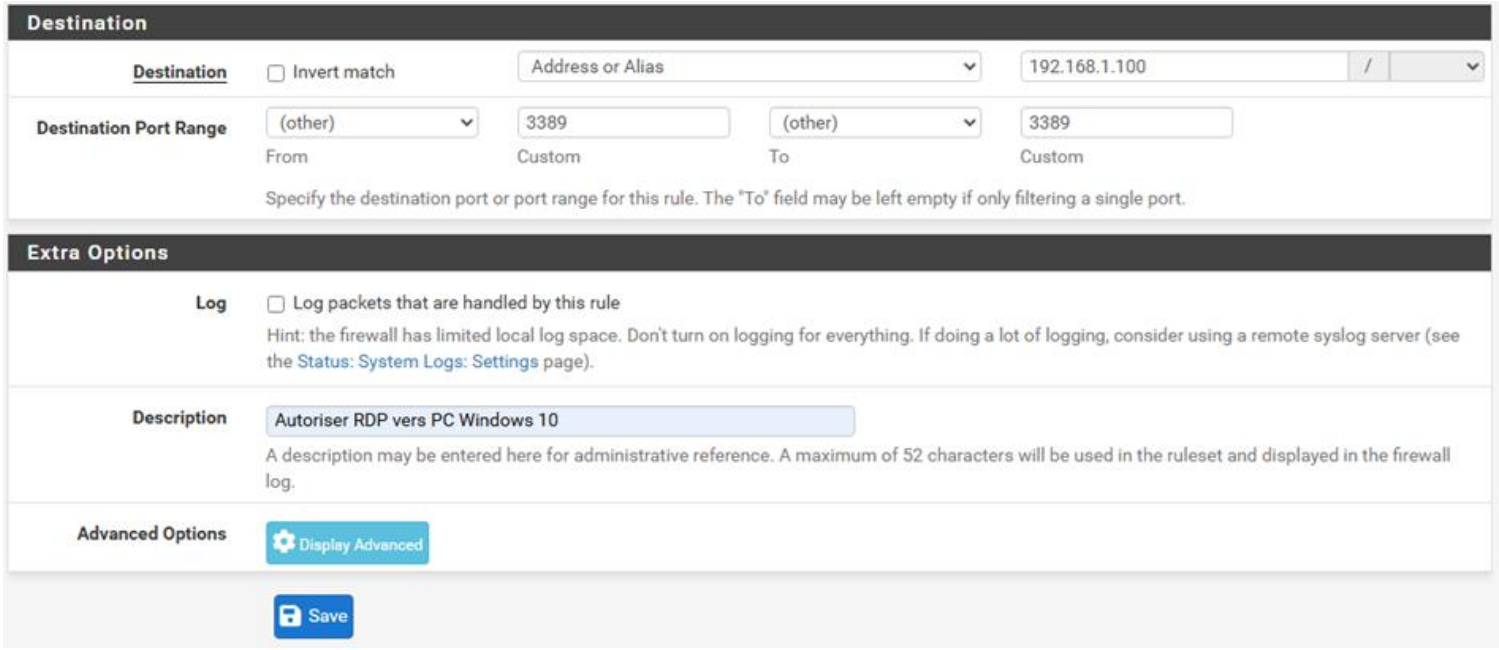
Créer une 1ère règle pour autoriser la connexion VPN

Cliquer sur save et appliquer les modifications



Modifier les règles de parfeu

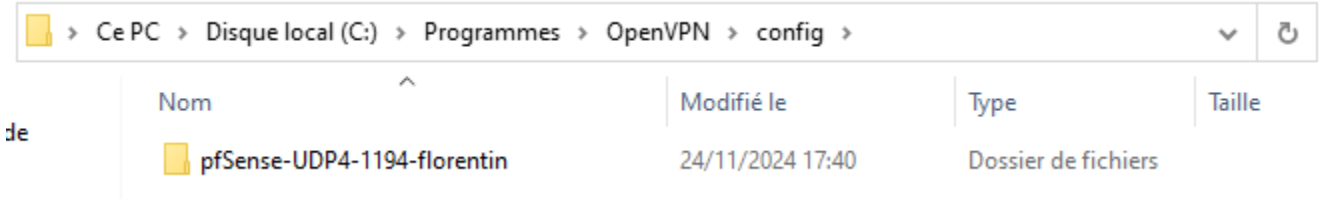
Cliquer sur l'onglet OpenVPN et créer une nouvelle règle dans le Firewall, par exemple autoriser à utiliser le protocole RDP pour se connecter sur une machine distante



Connexion en VPN

Installer OpenVPN sur une machine cliente

Copier le dossier dans l'archive téléchargée précédemment dans C:\Programmes\OpenVPN\config



Se connecter avec OpenVPN à l'aide des identifiants de connexion de l'utilisateur

Sources

https://www.it-connect.fr/pfsense-configurer-un-vpn-ssl-client-to-site-avec-openvpn/

https://www.youtube.com/watch?v=QDaRpaIH4GE