TP4 : OpenVPN Pfsense

Fait par DEPRADE ELIOTT

SOMMAIRE

But du TP

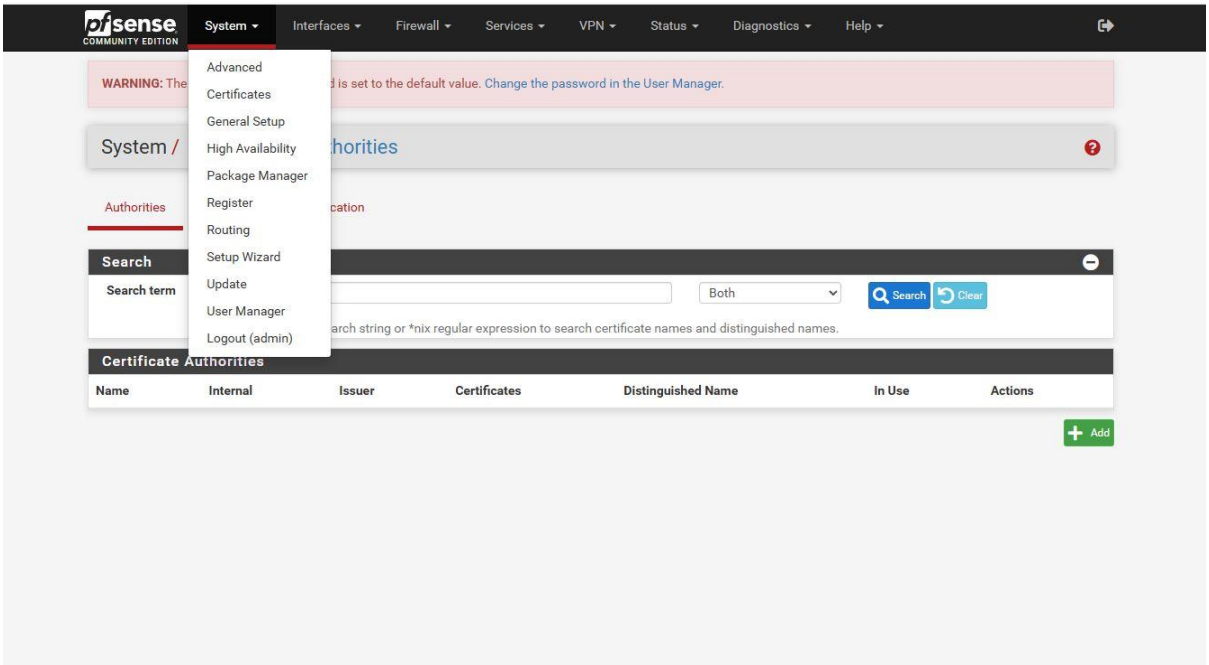
Un client nomade (ordinateur personnel) doit pouvoir se connecter à distance au réseau local derrière pfSense, comme s'il y était physiquement connecté.

La connexion doit être chiffré en UDP.

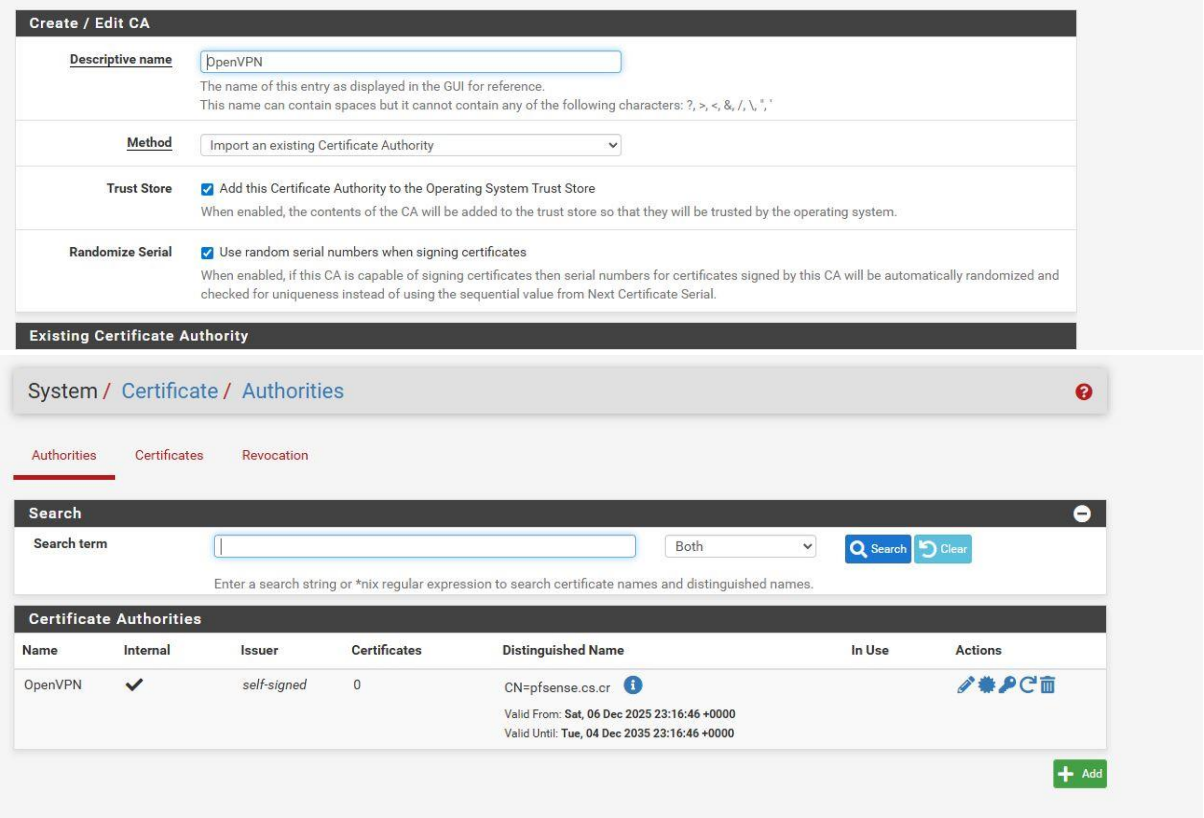
Configuration dans Pfsense

Création certificat serveur

Dans un premier temps on va créer le certificat du serveur en allant dans System > Certificates > Authorities :



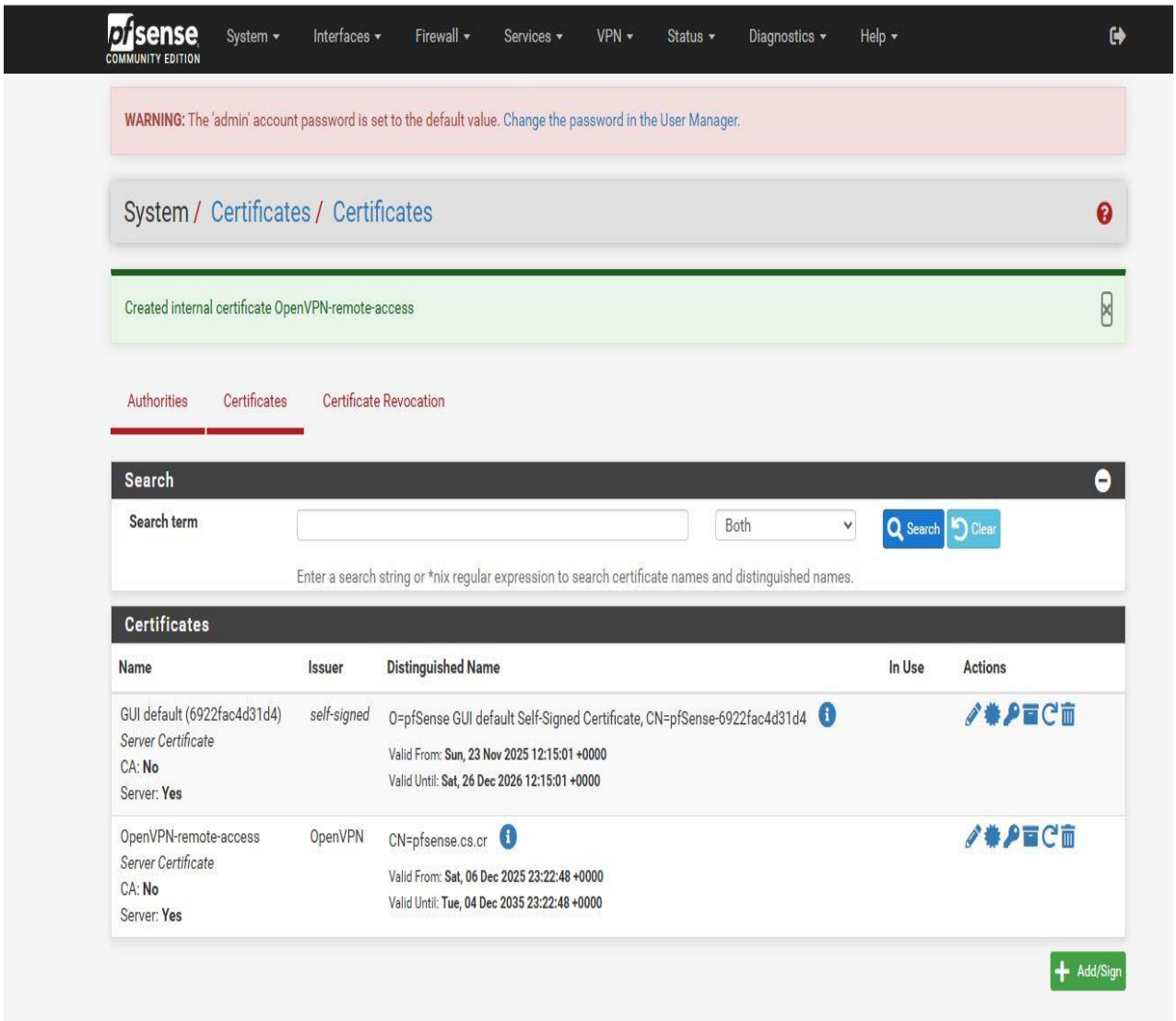
Cliquons sur “Add”.



On choisi la méthode **Method: Create an Internal Certificate Authority**

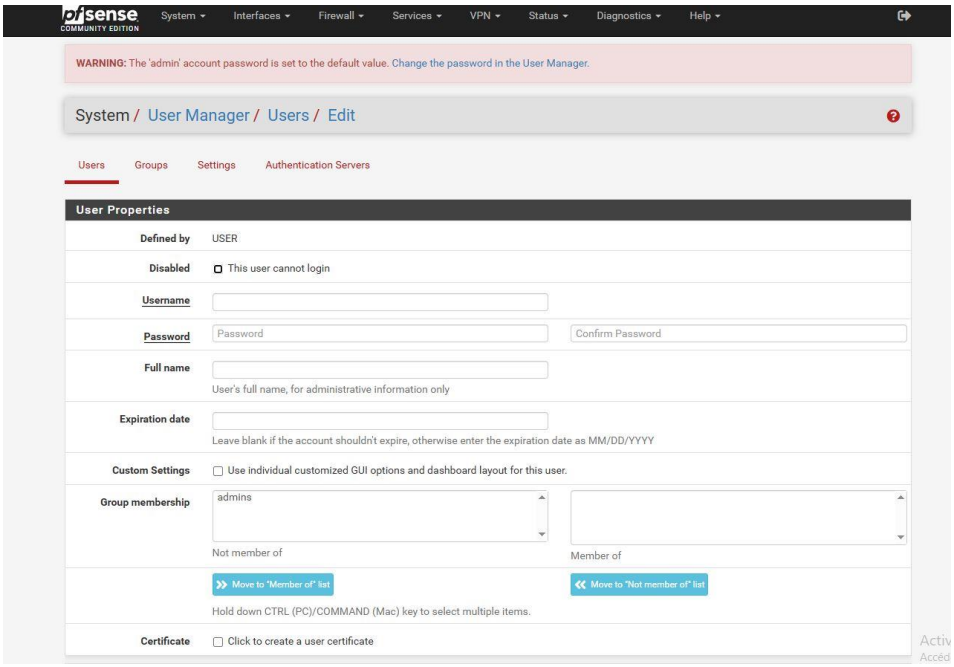
Et dans le **Common Name** on renseigne **le nom de domaine**, exemple pour ici : pfsense.cs.cr

Ensuite, passez à l’onglet **Certificates** et créez un nouveau certificat de serveur en cliquant sur Add/Sign. Choisissez Create an internal certificate, nommez-le (p.ex. OpenVPN-remote-access), sélectionnez la CA créée précédemment et entrez comme Common Name le nom du serveur (par ex. pfSense.cs.sr). Dans Certificate Type, sélectionnez Server Certificate. Cliquez sur Save.

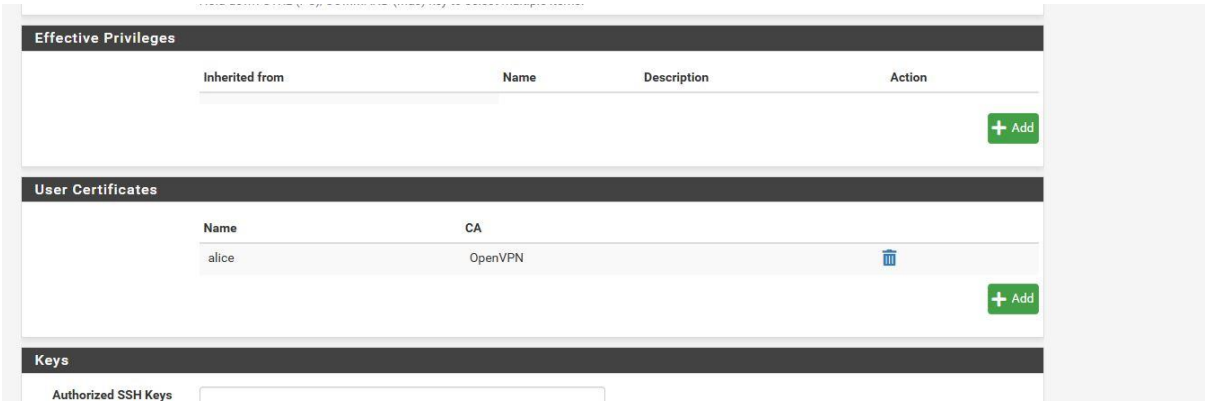

pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
System / Certificates / Certificates
Created internal certificate OpenVPN-remote-access
Authorities
Certificates
Certificate Revocation
Search
Search term
Both
Search
Clear
Enter a search string or *nix regular expression to search certificate names and distinguished names.
Certificates
Name
Issuer
Distinguished Name
In Use
Actions
GUI default (6922fac4d31d4)
Server Certificate
CA: No
Server: Yes
self-signed
O=pfSense GUI default Self-Signed Certificate, CN=pfSense-6922fac4d31d4
Valid From: Sun, 23 Nov 2025 12:15:01 +0000
Valid Until: Sat, 26 Dec 2026 12:15:01 +0000
OpenVPN-remote-access
Server Certificate
CA: No
Server: Yes
OpenVPN
CN=pfsense.cs.cr
Valid From: Sat, 06 Dec 2025 23:22:48 +0000
Valid Until: Tue, 04 Dec 2035 23:22:48 +0000
Add/Sign

Création d’un utilisateur

Allez ensuite dans System>User Manager>Users>Edit.

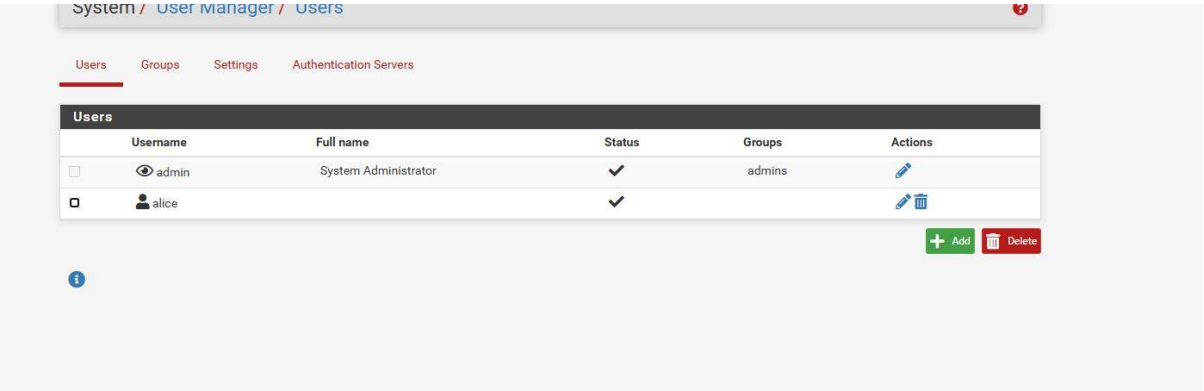


Créer votre utilisateur et cochez la case “Create User Certificate”.



Utilisez le CA que vous venez de créer.

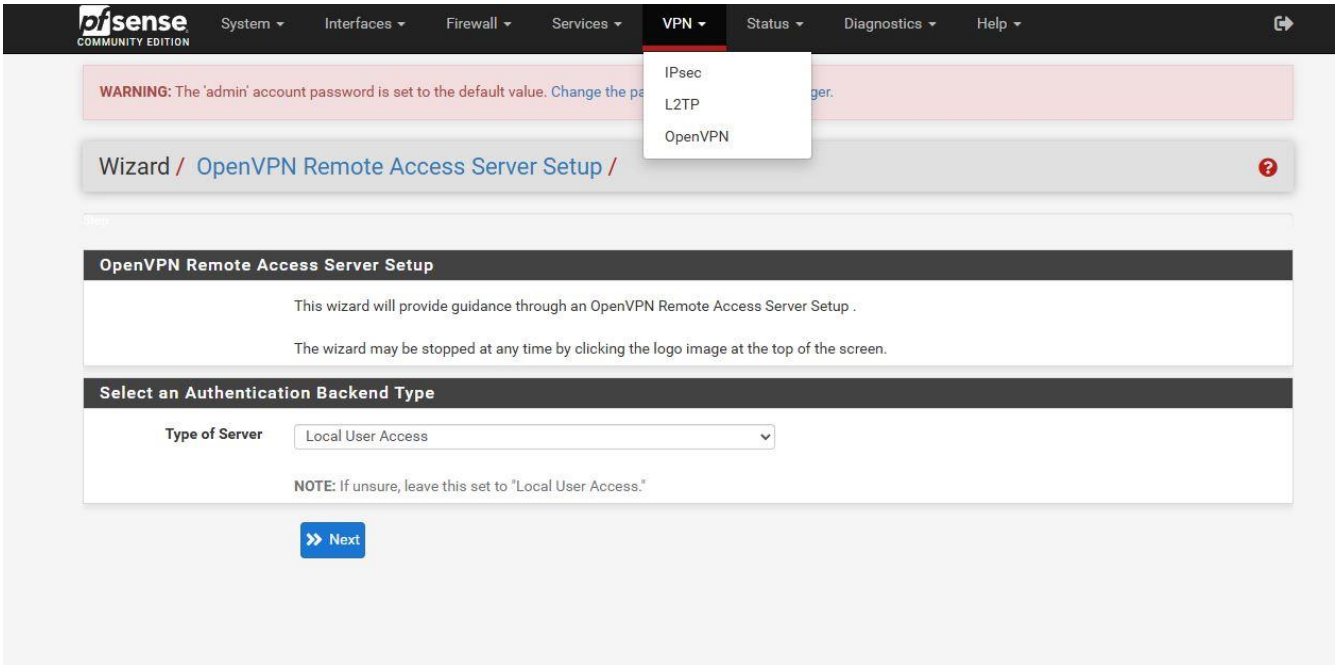
Parfait, votre utilisateur devrait être maintenant visible dans vos Users.



Passons à la configuration du VPN

Configuration du VPN

Allez dans VPN > OpenVPN > Wizard



Type of serveur = Local User Access

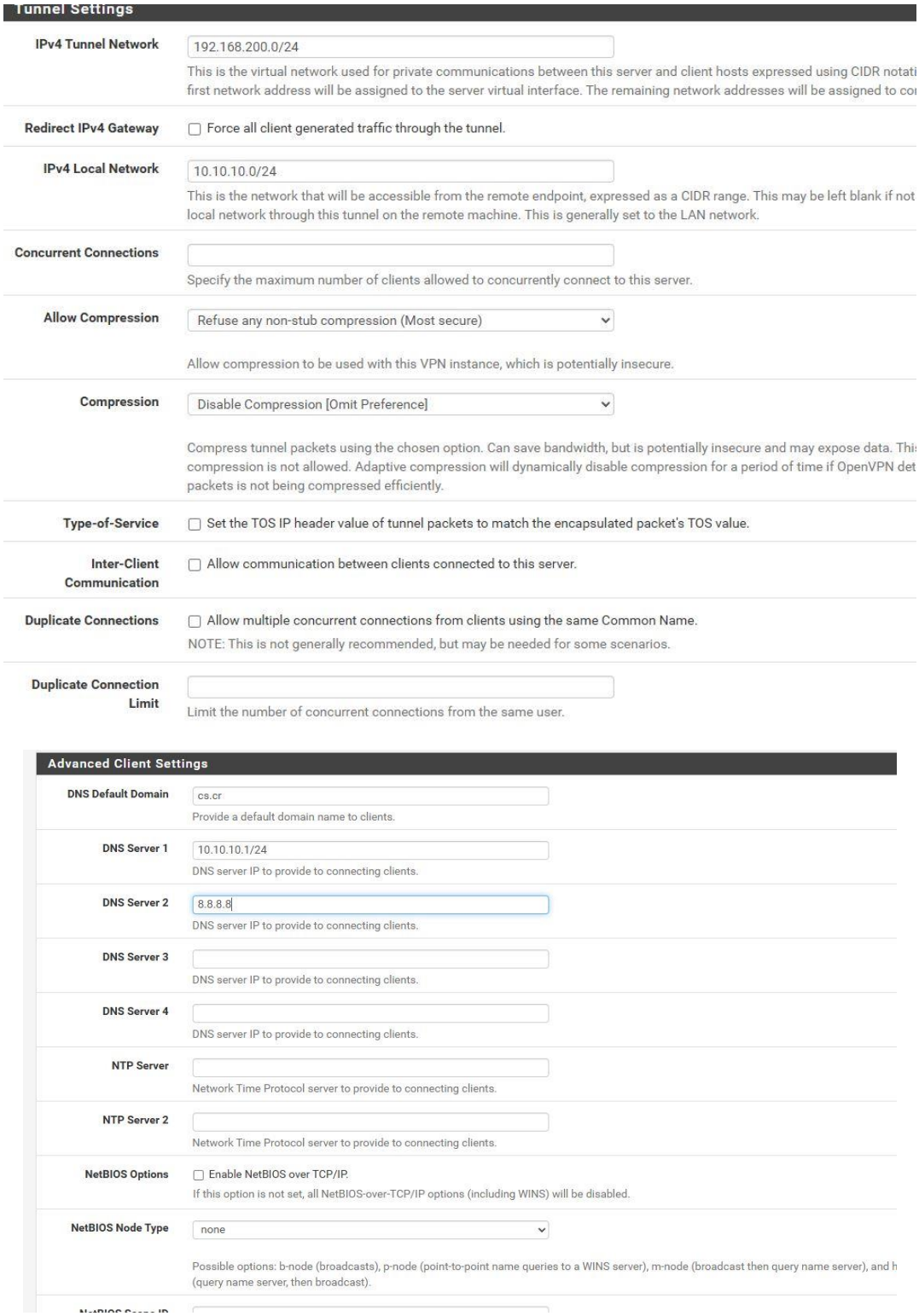
Autorité CA et certificat serveur = choisissez la CA interne créée et le certificat serveur (OpenVPNremote-access) déjà générés.

Adresse WAN du serveur = indiquez l'IP WAN actuelle du pfSense (ici 192.168.1.130)

Choisissez une adresse différente de votre Wan ou Lan pour votre **Tunnel**

Local Network = spécifiez le réseau LAN local à rendre accessible par le VPN

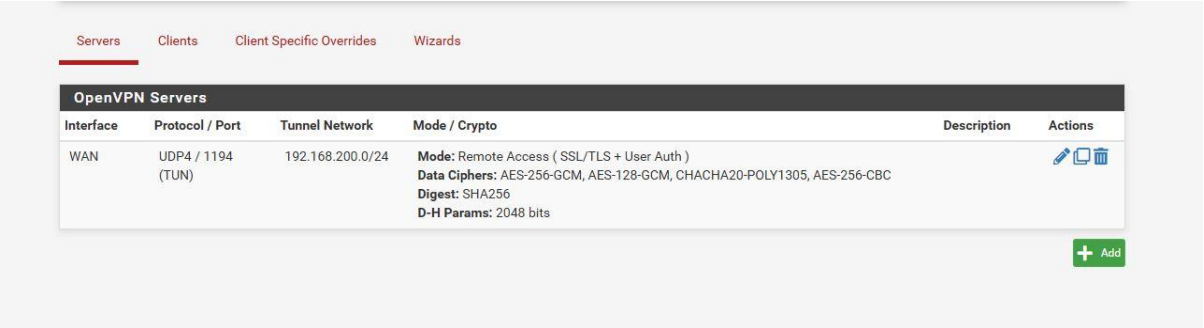
Advanced Client Settings = entrez DNS Default Domain = votre domaine, DNS Server 1 = (IP LAN) et DNS Server 2 = (IP WAN/pfSense)



Le Wizard propose ensuite d'ajouter automatiquement des règles de pare-feu. Validez les options Add a firewall rule et Add an OpenVPN rule pour autoriser le trafic VPN entrant. Terminez le Wizard. Un serveur OpenVPN est alors créé, mais nous devons affiner certains réglages.

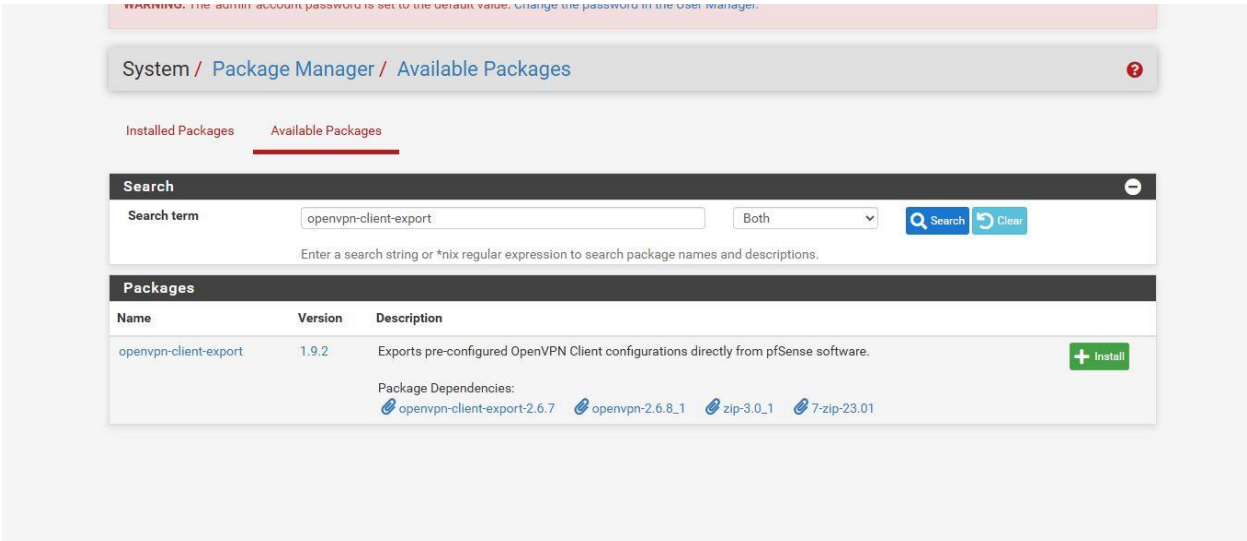
Dans "**advanced configuration**" ajoutez la ligne push "route LAN MASK" dans Custom Option

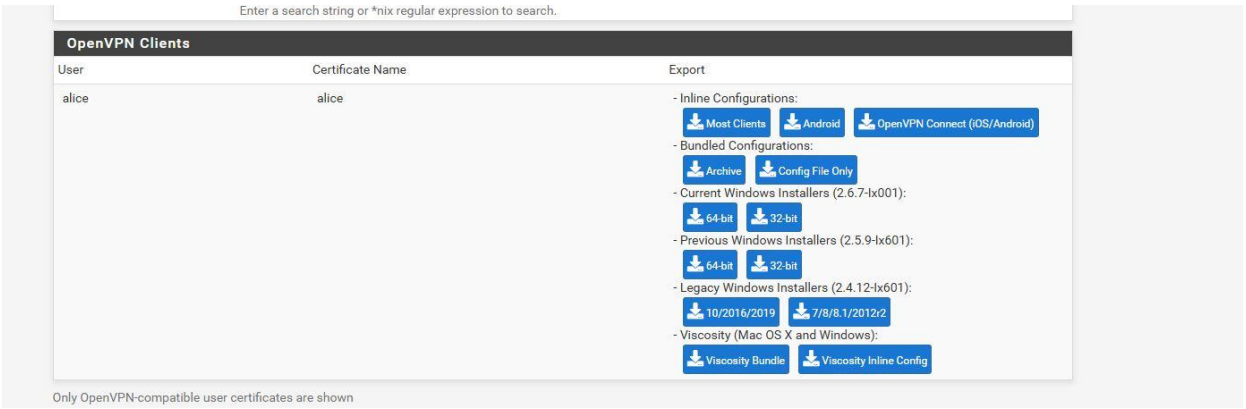
Votre VPN est normalement fin prêt :



Export de la configuration

Installez le paquet **openvpn-client-export** via **System > Packages**. Ensuite, retournez dans VPN > OpenVPN, onglet Client Export. Sélectionnez l'utilisateur alice et cliquez sur **Most Clients** pour générer un fichier .ovpn (il contient automatiquement le certificat utilisateur et la CA) . Téléchargez ce profil sur le poste client.





Configuration du client VPN (machine physique)

Sur la machine physique (située sur le réseau WAN), installez un client OpenVPN adapté à l'OS

Sous Windows, installez OpenVPN Connect puis importez le fichier .ovpn :

Vous serez ensuite connecté à votre pfSense grâce aux identifiants de l'utilisateur crée précédement.

Derniers tests

Essayez de pinger votre LAN depuis votre machine en WAN :

```
Microsoft Windows [version 10.0.19045.6575]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\depra>ping 10.10.10.10

Envoi d'une requête 'Ping'  10.10.10.10 avec 32 octets de données :
Réponse de 10.10.10.10 : octets=32 temps<1ms TTL=63
Réponse de 10.10.10.10 : octets=32 temps=1 ms TTL=63
Réponse de 10.10.10.10 : octets=32 temps=1 ms TTL=63
Réponse de 10.10.10.10 : octets=32 temps=1 ms TTL=63

Statistiques Ping pour 10.10.10.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C:\Users\depra>
```

Si ce test ne fonctionne pas, vérifiez votre pare-feu psSense voir s'il n'y a pas de règles trop strictes.

En faisant ipconfig/all votre pc devrait avoir une interface dans la plage de l'IP choisie plus tôt :

Vérification de l'interface

136	215.404181	fe80::7188:e82b:b58a:55c3	ff02::fb	MDNS	102 Standard query 0x0000 PTR _g
137	215.405430	192.168.200.2	224.0.0.251	MDNS	82 Standard query 0x0000 PTR _g
138	215.405844	fe80::7188:e82b:b58a:55c3	ff02::fb	MDNS	102 Standard query 0x0000 PTR _g
139	218.962569	00:ff:4f:97:78:42	Broadcast	ARP	42 Who has 192.168.200.1? Tell
140	218.962579	00:ff:50:97:78:42	00:ff:4f:97:78:42	ARP	60 192.168.200.1 is at 00:ff:50
141	219.418510	fe80::7188:e82b:b58a:55c3	ff02::1:2	DHCPv6	147 Solicit XID: 0xbd2570 CID: 0
142	224.280377	192.168.200.2	192.168.200.255	STEAMDISCOVER	280 Client Status from THOOR[Mal
143	224.699103	192.168.200.2	10.10.10.10	ICMP	74 Echo (ping) request id=0x00
144	224.699994	10.10.10.10	192.168.200.2	ICMP	74 Echo (ping) reply id=0x00
145	225.701332	192.168.200.2	10.10.10.10	ICMP	74 Echo (ping) request id=0x00
146	225.702304	10.10.10.10	192.168.200.2	ICMP	74 Echo (ping) reply id=0x00
147	226.703242	192.168.200.2	10.10.10.10	ICMP	74 Echo (ping) request id=0x00
148	226.704277	10.10.10.10	192.168.200.2	ICMP	74 Echo (ping) reply id=0x00
149	227.706576	192.168.200.2	10.10.10.10	ICMP	74 Echo (ping) request id=0x00
150	227.707607	10.10.10.10	192.168.200.2	ICMP	74 Echo (ping) reply id=0x00
151	235.419577	fe80::7188:e82b:b58a:55c3	ff02::1:2	DHCPv6	147 Solicit XID: 0xbd2570 CID: 0

On peut voir que j'utilise bien l'interface 192.168.200.2 (le tunnel)

Et sur l'interface wan cela se traduit par du traffic en UDP chiffré :

81	3.532075	192.168.1.33	192.168.1.4	WireGuard	138	Transport Data, receiver=0xADDFC7C4, counter=657, datal
82	3.532637	192.168.1.4	192.168.1.33	WireGuard	138	Transport Data, receiver=0xD24E9E01, counter=415, datal
83	3.533000	192.168.1.33	192.168.1.4	WireGuard	122	Transport Data, receiver=0xADDFC7C4, counter=658, datal
84	3.533354	192.168.1.33	192.168.1.4	WireGuard	1354	Transport Data, receiver=0xADDFC7C4, counter=659, datal
85	3.533367	192.168.1.33	192.168.1.4	WireGuard	682	Transport Data, receiver=0xADDFC7C4, counter=660, datal
86	3.533878	192.168.1.4	192.168.1.33	WireGuard	122	Transport Data, receiver=0xD24E9E01, counter=416, datal
87	3.535471	192.168.1.4	192.168.1.33	WireGuard	1354	Transport Data, receiver=0xD24E9E01, counter=417, datal
88	3.535471	192.168.1.4	192.168.1.33	WireGuard	714	Transport Data, receiver=0xD24E9E01, counter=418, datal
89	3.535687	192.168.1.33	192.168.1.4	WireGuard	122	Transport Data, receiver=0xADDFC7C4, counter=661, datal
90	3.535845	192.168.1.33	192.168.1.4	WireGuard	154	Transport Data, receiver=0xADDFC7C4, counter=662, datal
91	3.535890	192.168.1.33	192.168.1.4	WireGuard	122	Transport Data, receiver=0xADDFC7C4, counter=663, datal
92	3.536220	192.168.1.4	192.168.1.33	WireGuard	122	Transport Data, receiver=0xD24E9E01, counter=419, datal
93	3.536409	192.168.1.33	192.168.1.4	WireGuard	122	Transport Data, receiver=0xADDFC7C4, counter=664, datal