2022

TP_INTERCONNEXION_VPN

U4_CONCEVOIR_SOLUTION_INFRA

FEVRE & HUBER & YILMAZ

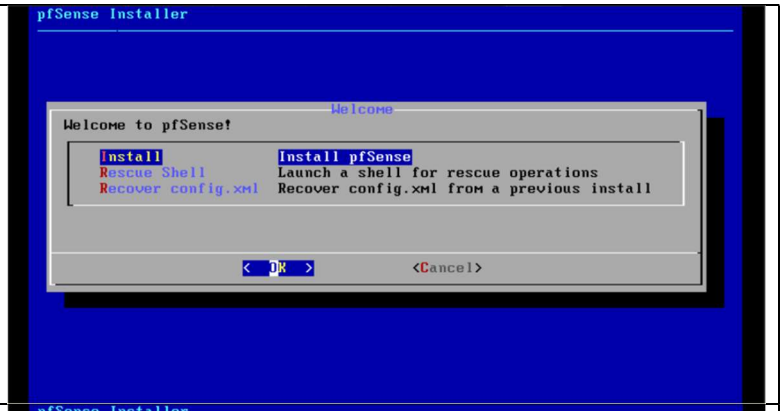
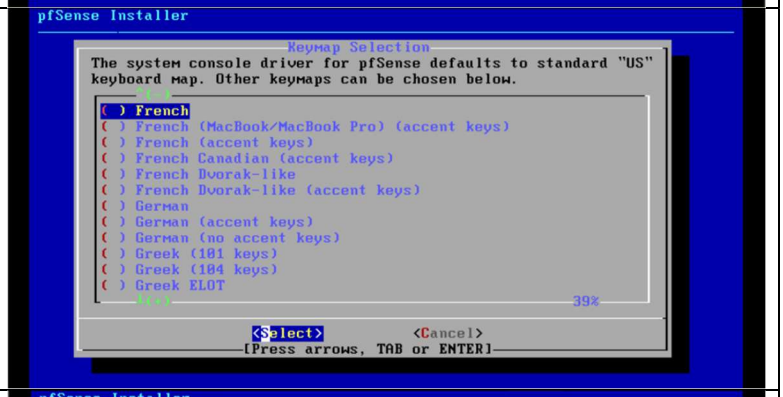
Table des matières

1. Savoir installer et configurer un serveur PfSense.

Prérequis

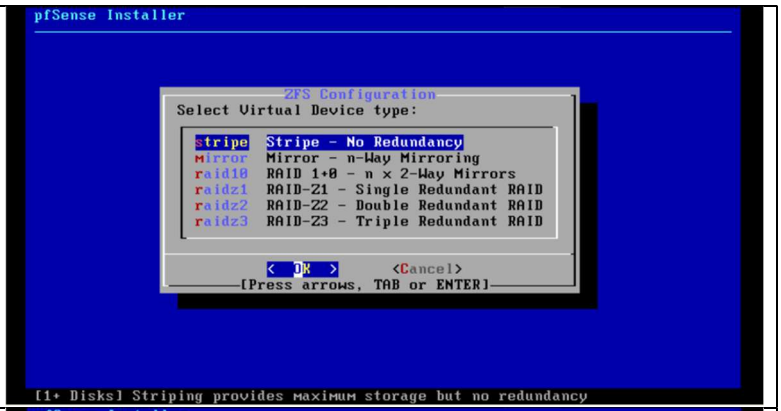
- Une vm Pfsense FreeBSD sur VMware avec 2 cartes réseaux, une pour le WAN et une pour le LAN.
- Un client Windows 10 (ici c'est un PRO)

1.1 Installation de pfsense freeBSD

L'installation peut maintenant débuter en validant l'option : `Install pfSense`	
On choisit ensuite la langue du clavier : `( ) French` Puis **Entrée.**	
Une interface qui demande de partitionner le disque se propose. Restez sur le choix : `Auto (2FS)` et appuyez sur **Entrée.**	
La configuration du partitionnement du disque va être demandé, voici le paramétrage :	

Choisir :

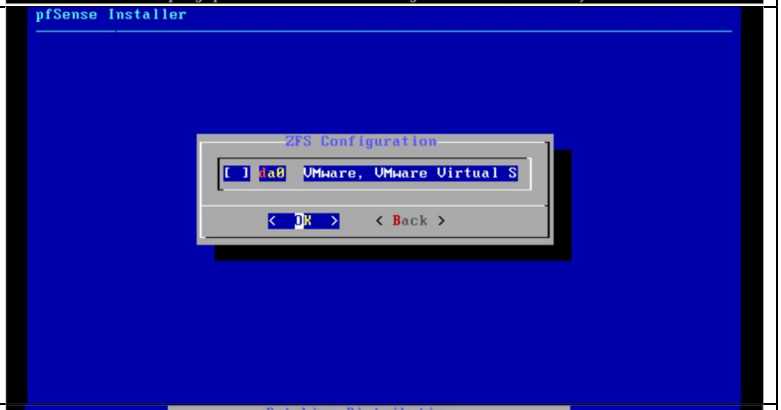
```
Stripe - No Redundancy
```



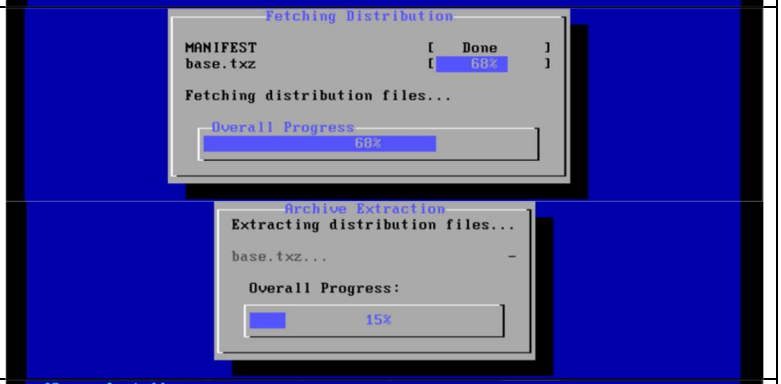
Il faut bien s'assurer à valider le choix :

```
[ ] da0 VMware,
VMware Virtual S
```

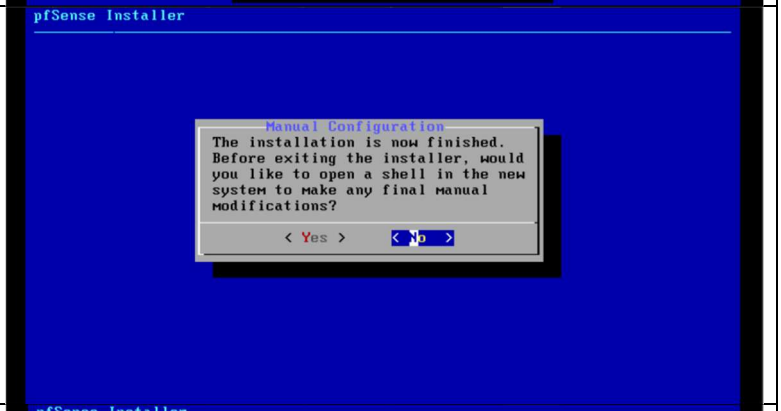
avec **Espace**, puis appuyez sur **Entrée.**



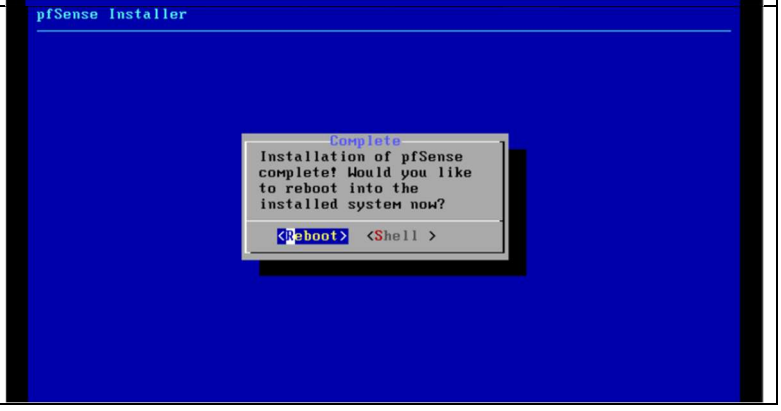
Le partitionnement du disque, puis l'installation de PFSense va alors se lancer.



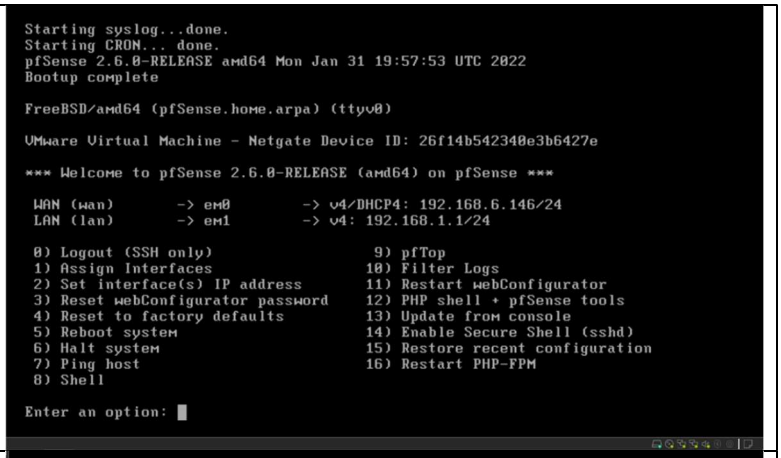
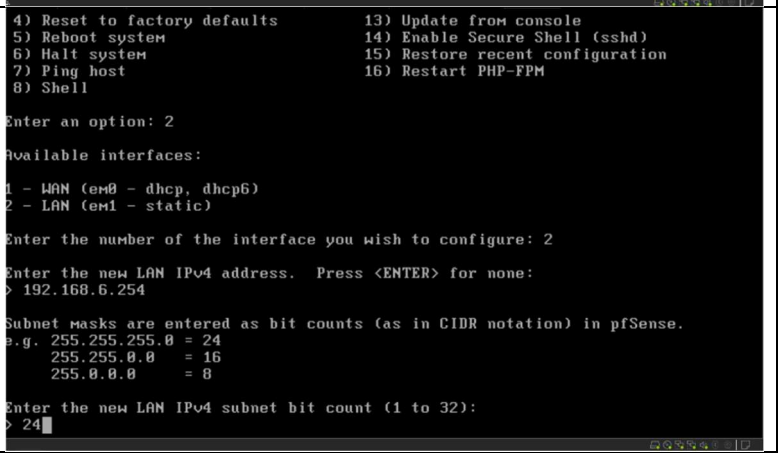
Une interface qui demande d'ouvrir un shell (terminal) se propose. Restez sur le choix « No » et appuyez sur Entrée.



L'installation est à présent terminée.
Pour finir, appuyez sur Entrée pour reboot la machine et lancer PfSense.



1.2 Configuration de PFSense

L'interface suivant sera proposée une fois la machine démarrée. A partir de ce menu, nous pouvons taper un numéro de 0 à 16 selon le besoin pour configurer la machine.	
Avant de se lancer sur PFSense, il faut d'abord assigner une adresse IP à l'interface LAN. Tapez "2 " puis **Entrée.** Il va alors proposer de choisir entre WAN ou LAN Tapez "2 " puis configurer l'IP.	
Définissez le masque de sous-réseau du réseau local, tapez 24	

1.3 Configuration depuis client Windows 10 Pro

Configuration de base = carte réseau avec l'IP sur le même réseau que pfsense et mettre l'IP de pfsense en passerelle (8.8.8.8 en dns pour internet).
Par défaut le login est : admin et le MDP est : pfsense

2. Installer et configurer un VPN site à site (IPsec)

2.1 Prérequis

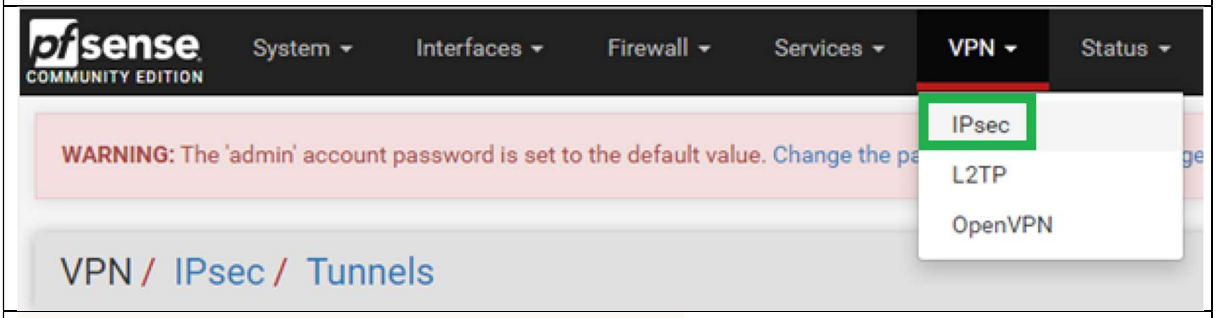
Deux machines virtuelles PFSENSE sur la même connexion (Exemple : partage de connexion) avec l'adressage IP suivant :

Serveur 1: WAN : 192.168.125.113/24
LAN : 192.168.30.5

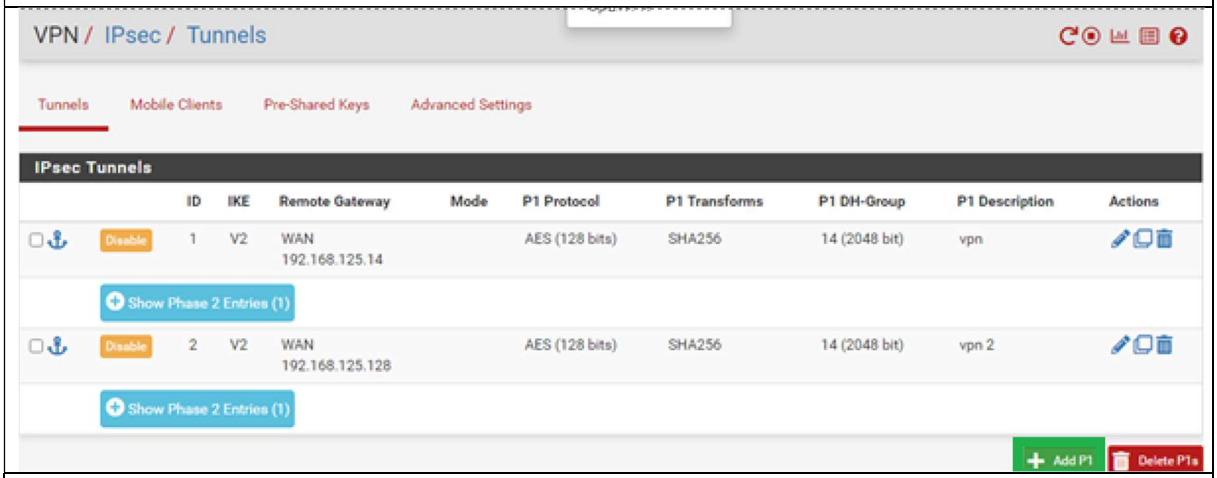
Serveur 2: WAN : 192.168.125.14/24
LAN : 192.168.20.5

2.2 IPSEC

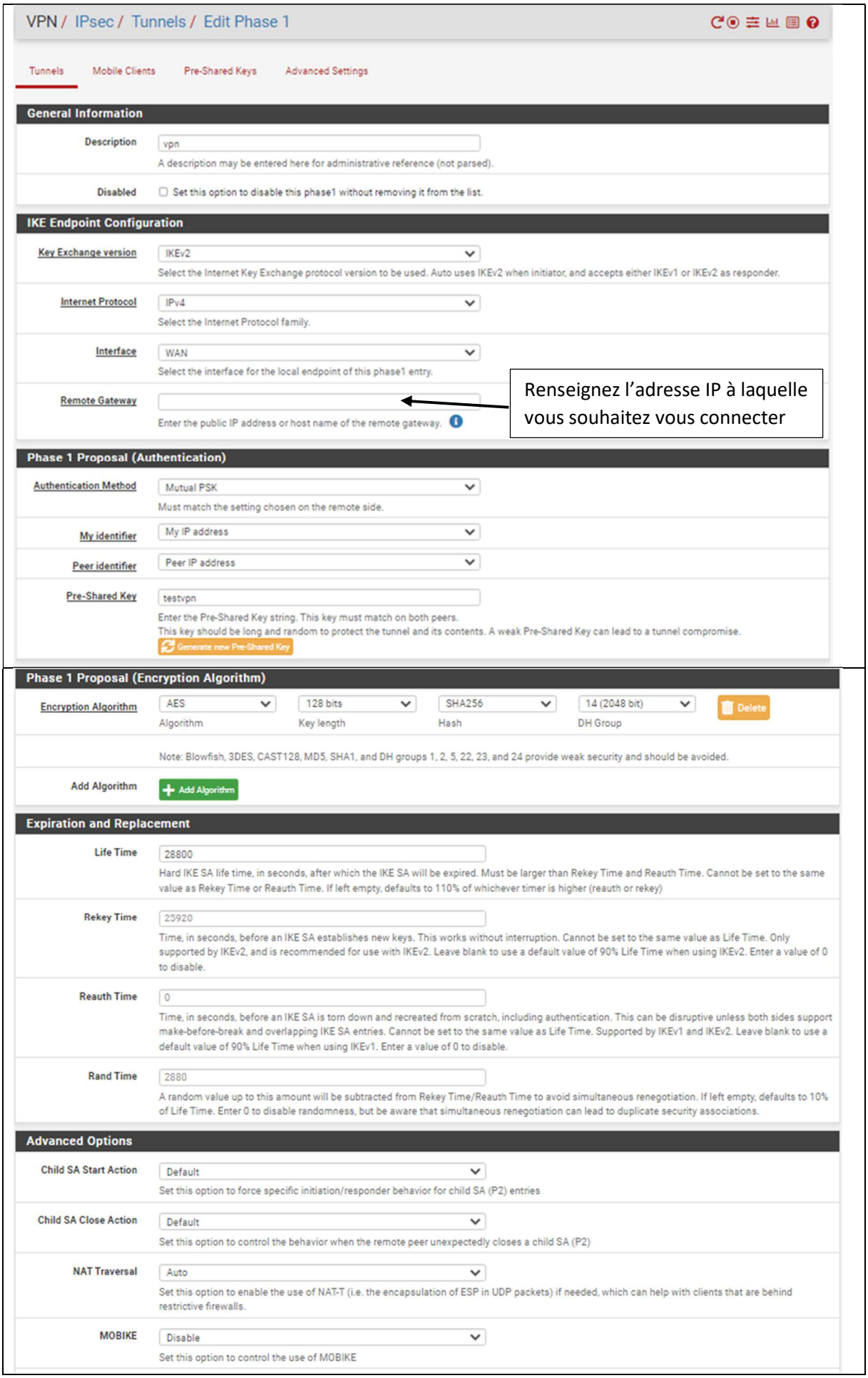
Aller dans l'onglet VPN/IPSEC



Cliquez sur le bouton « add P1 » pour ajouter la phase 1



Remplissez selon la photo ci-dessous
Dans « Remote Gateway » mettre l'addresse ip WAN du second serveur PfSense
Dans preshared key, mettez un mot (ex : test vpn) ou générez une clé (il faudra absolument configurer la meme clé sur le second serveur pfsense)


VPN / IPsec / Tunnels / Edit Phase 1
Tunnels
Mobile Clients
Pre-Shared Keys
Advanced Settings
General Information
Description
vpn
A description may be entered here for administrative reference (not parsed).
Disabled
Set this option to disable this phase1 without removing it from the list.
IKE Endpoint Configuration
Key Exchange version
IKEv2
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.
Internet Protocol
IPv4
Select the Internet Protocol family.
Interface
WAN
Select the interface for the local endpoint of this phase1 entry.
Remote Gateway
Enter the public IP address or host name of the remote gateway.
Renseignez l'adresse IP à laquelle vous souhaitez vous connecter
Phase 1 Proposal (Authentication)
Authentication Method
Mutual PSK
Must match the setting chosen on the remote side.
My identifier
My IP address
Peer identifier
Peer IP address
Pre-Shared Key
testvpn
Enter the Pre-Shared Key string. This key must match on both peers.
This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.
Generate new Pre-Shared Key
Phase 1 Proposal (Encryption Algorithm)
Encryption Algorithm
AES
Algorithm
128 bits
Key length
SHA256
Hash
14 (2048 bit)
DH Group
Delete
Note: Blowfish, 3DES, CAST128, MD5, SHA1, and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.
Add Algorithm
Add Algorithm
Expiration and Replacement
Life Time
28800
Hard IKE SA life time, in seconds, after which the IKE SA will be expired. Must be larger than Rekey Time and Reauth Time. Cannot be set to the same value as Rekey Time or Reauth Time. If left empty, defaults to 110% of whichever timer is higher (reauth or rekey)
Rekey Time
25920
Time, in seconds, before an IKE SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Only supported by IKEv2, and is recommended for use with IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv2. Enter a value of 0 to disable.
Reauth Time
0
Time, in seconds, before an IKE SA is torn down and recreated from scratch, including authentication. This can be disruptive unless both sides support make-before-break and overlapping IKE SA entries. Cannot be set to the same value as Life Time. Supported by IKEv1 and IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv1. Enter a value of 0 to disable.
Rand Time
2880
A random value up to this amount will be subtracted from Rekey Time/Reauth Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.
Advanced Options
Child SA Start Action
Default
Set this option to force specific initiation/responder behavior for child SA (P2) entries
Child SA Close Action
Default
Set this option to control the behavior when the remote peer unexpectedly closes a child SA (P2)
NAT Traversal
Auto
Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls.
MOBIKE
Disable
Set this option to control the use of MOBIKE

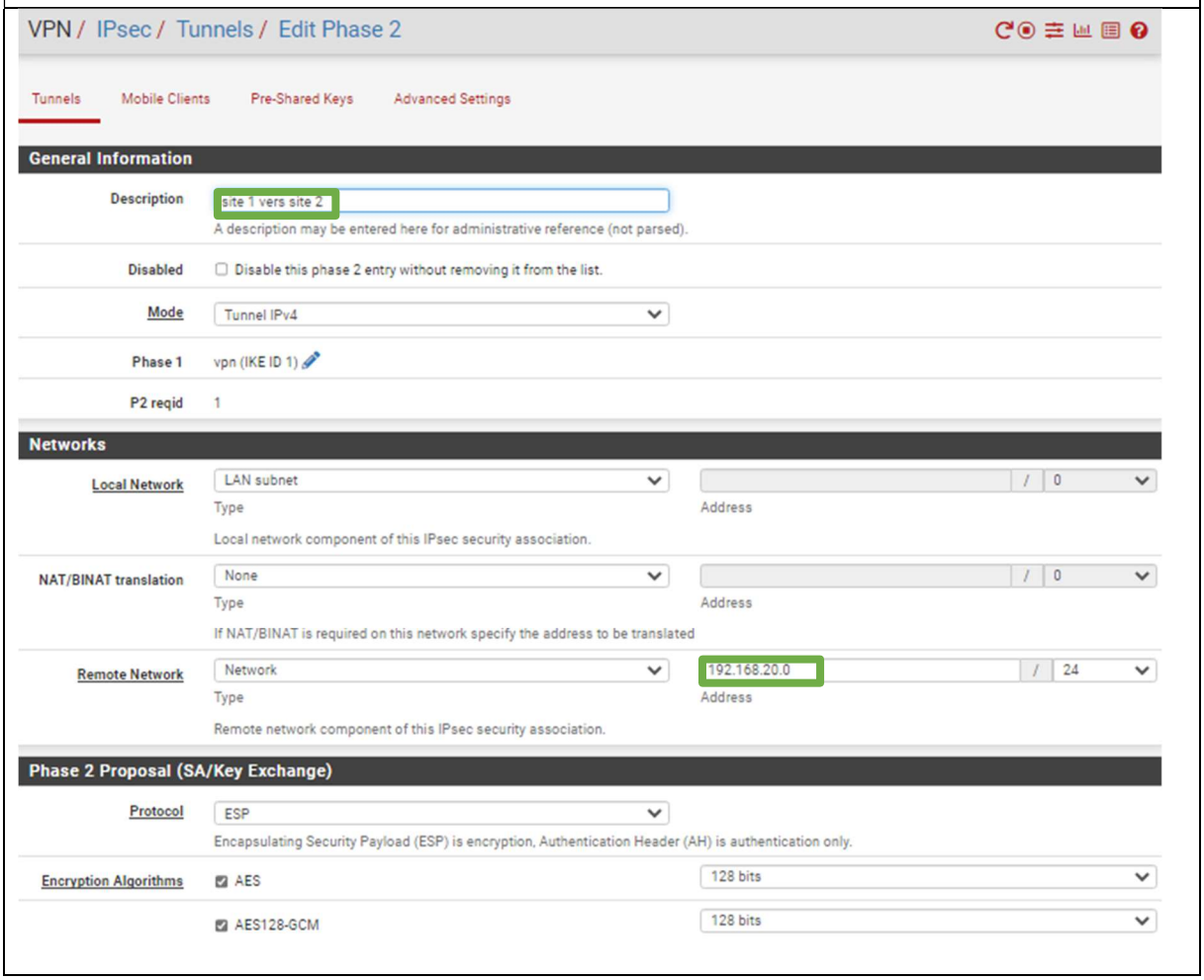
Gateway duplicates	☐ Enable this to allow multiple phase 1 configurations with the same endpoint. When enabled, pfSense does not manage routing to the remote gateway and traffic will follow the default route without regard for the chosen interface. Static routes can override this behavior.
Split connections	☐ Enable this to split connection entries with multiple phase 2 configurations. Required for remote endpoints that support only a single traffic selector per child SA.
PRF Selection	☐ Enable manual Pseudo-Random Function (PRF) selection Manual PRF selection is typically not required, but can be useful in combination with AEAD Encryption Algorithms such as AES-GCM
Custom IKE/NAT-T Ports	Remote IKE Port UDP port for IKE on the remote gateway. Leave empty for default automatic behavior (500/4500). Remote NAT-T Port UDP port for NAT-T on the remote gateway.
Dead Peer Detection	☑ Enable DPD Check the liveness of a peer by using IKEv2 INFORMATIONAL exchanges or IKEv1 R_U_THERE messages. Active DPD checking is only enforced if no IKE or ESP/AH packet has been received for the configured DPD delay.
Delay	10 Delay between sending peer acknowledgement messages. In IKEv2, a value of 0 sends no additional messages and only standard messages (such as those to rekey) are used to detect dead peers.
Max failures	5 Number of consecutive failures allowed before disconnecting. This only applies to IKEv1; in IKEv2 the retransmission timeout is used instead.

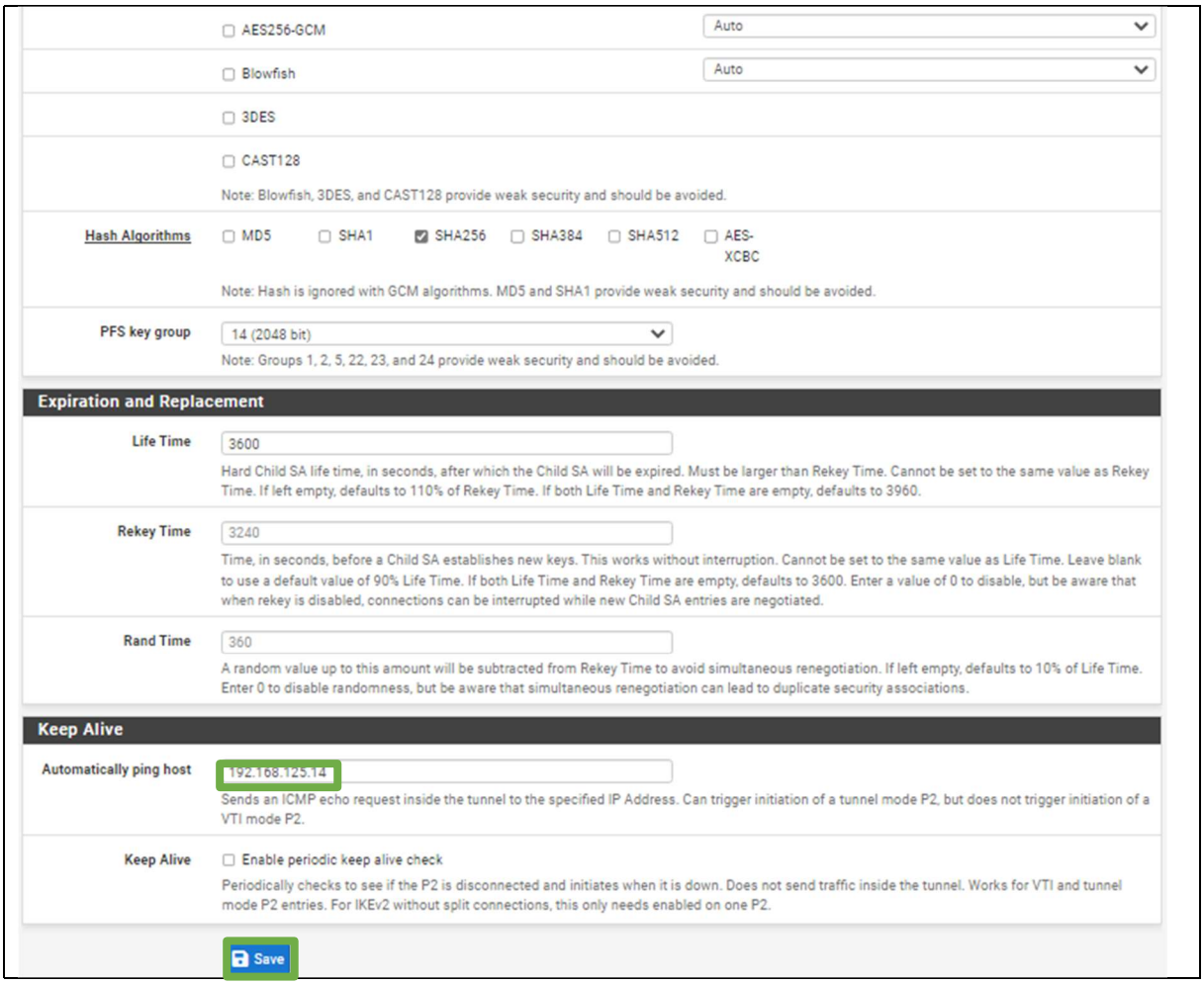
Save

2.3 Phase 2

Cliquez sur « add P2 » pour renseigner la phase 2

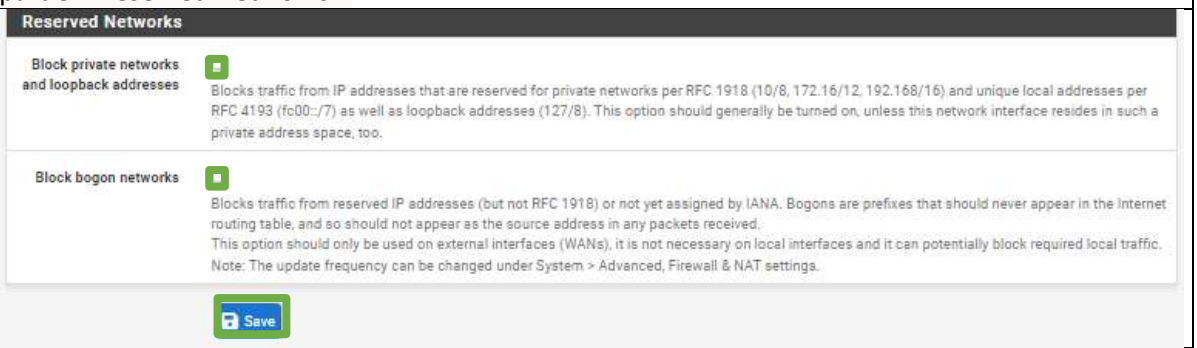
Remplir selon la photo ci-dessus. Dans le remote Network, bien renseignez l'adresse réseau de la LAN du second serveur PfSense



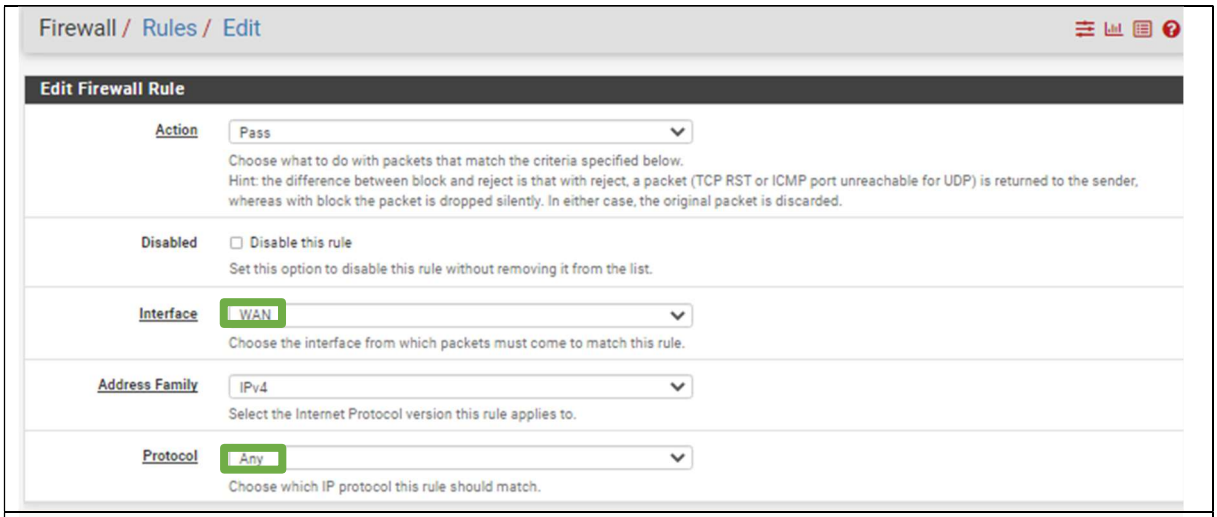


2.4 RULES

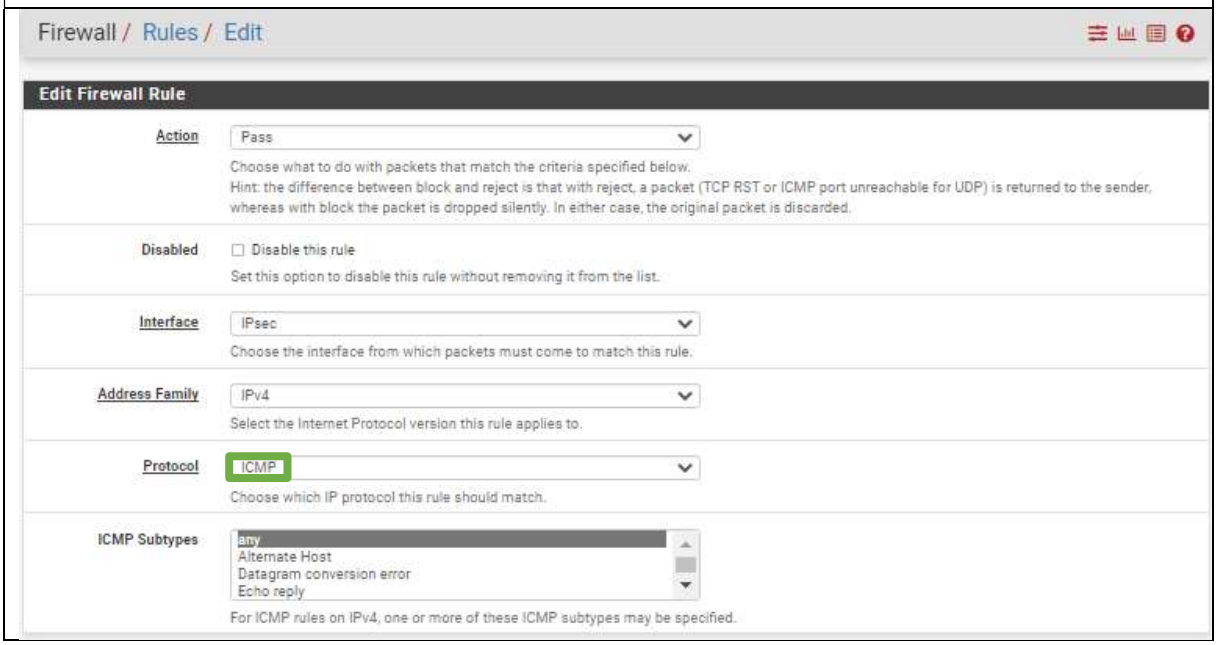
Allez dans « Interfaces/WAN » descendre tout en bas de la page puis décochez les 2 cases dans la partie « Reserved Networks »



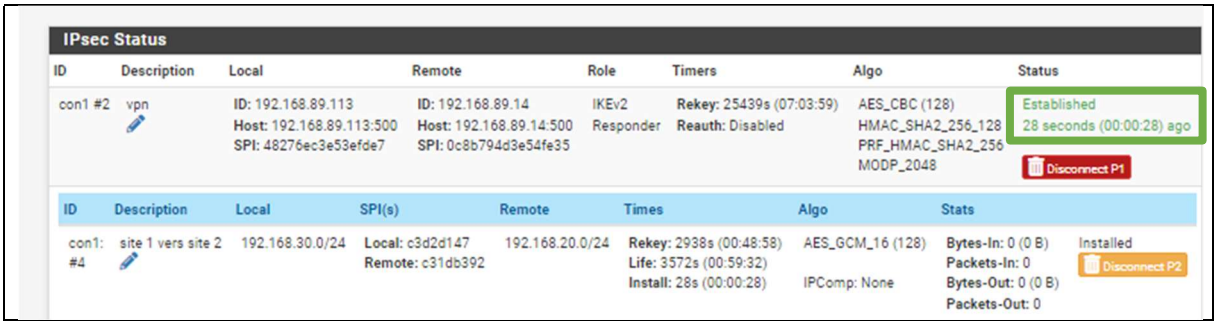
Ensuite, allez dans l'onglet « Firewall / Rules » Commencez par la partie WAN, modifier la règle en changeant le protocole par « Any » puis sauvegardez

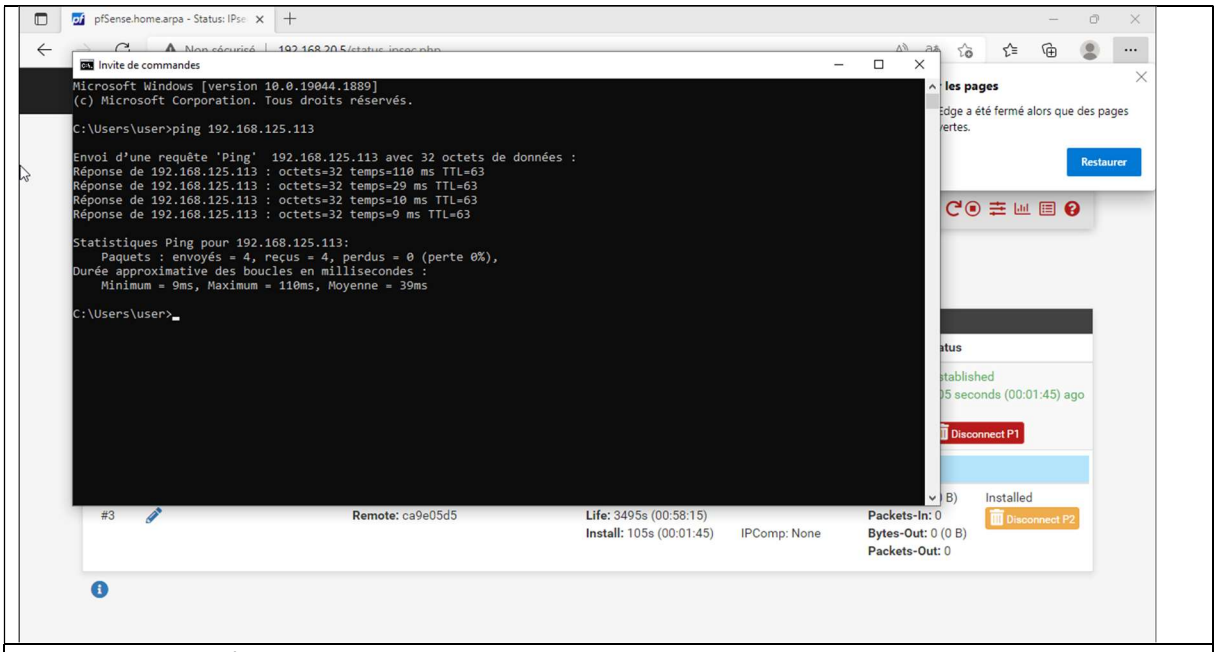


Appliquez les mêmes paramètres pour la partie LAN et IPsec puis rajoutez une règle en autorisant le protocole ICMP dans IPsec.



2.5 Test de connexion



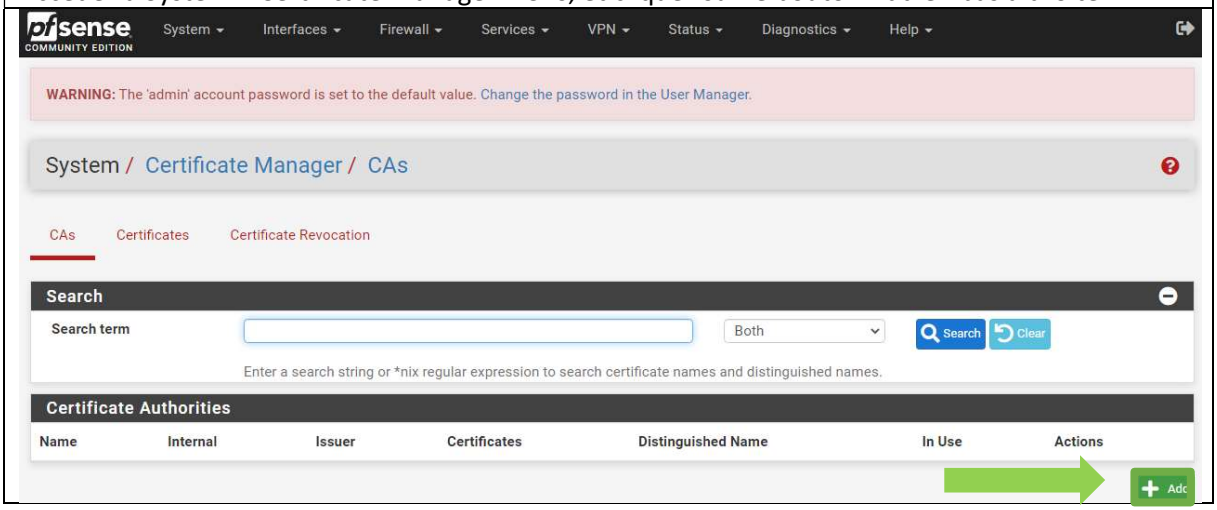


La connexion est établie et le ping passe.

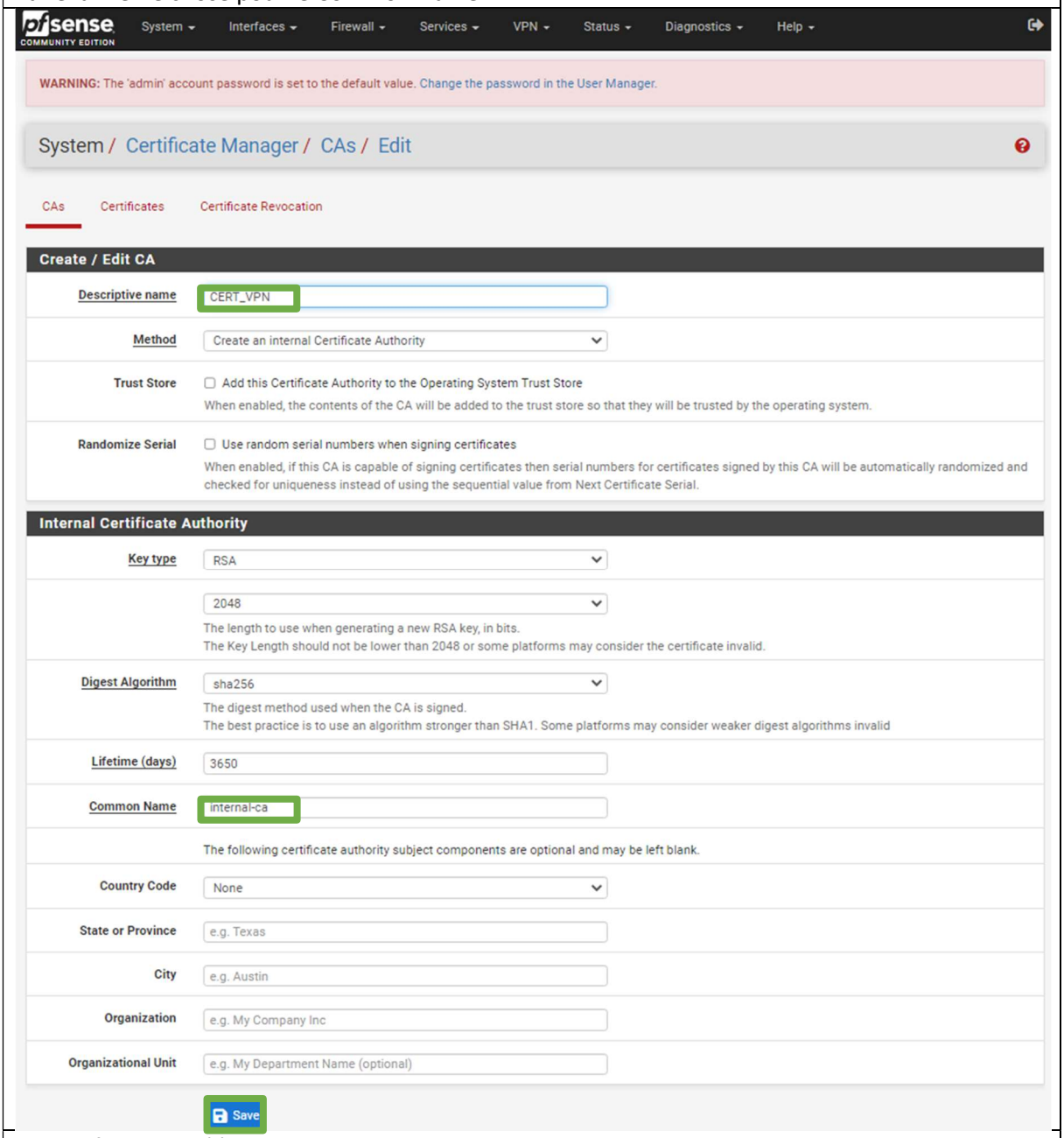
3. Installer et configurer un VPN distant (OpenVPN)

3.1 Création de l'Autorité de Certification – CA

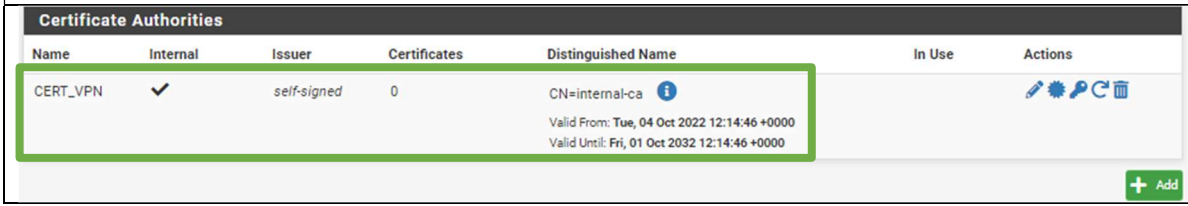
Accédez à System > Certificate Manager > CAs, et cliquez sur le bouton Add en bas à droite.



Remplir le « Descriptive name » (sans espaces, ni caractères spéciaux)
Faire la même chose pour le Common Name

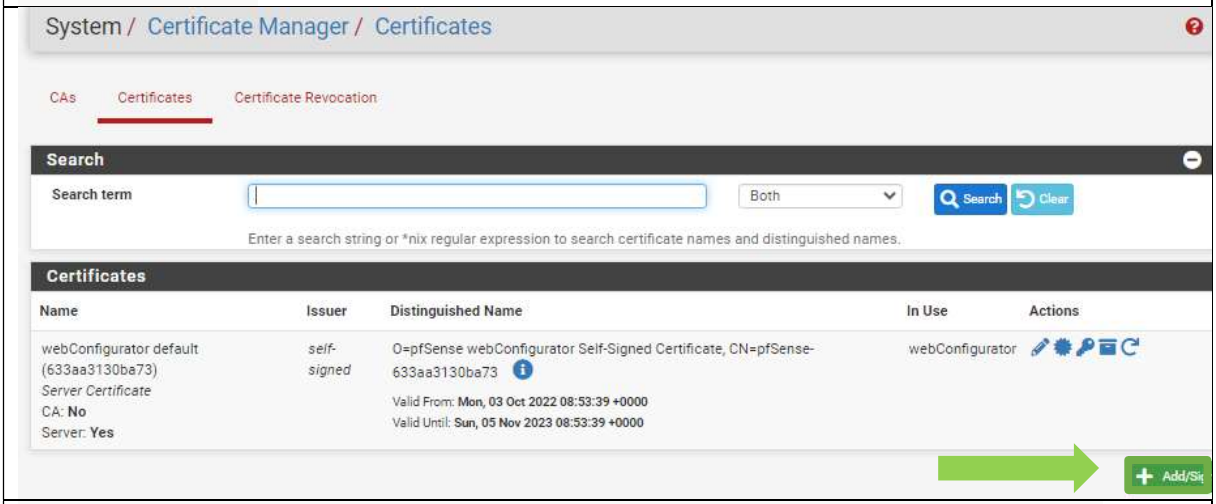


Le certificat est créé

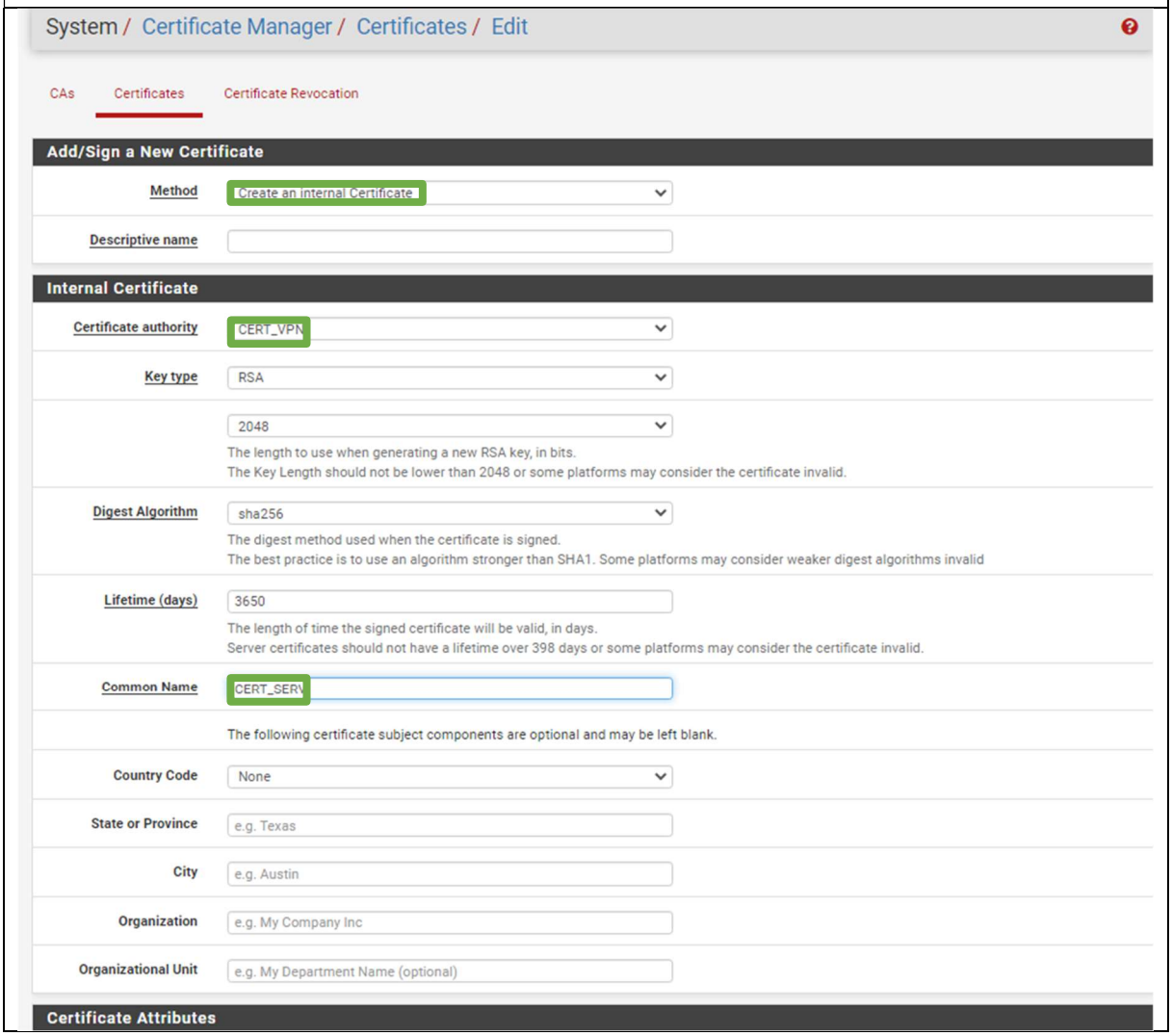


3.2 Création Certificat Serveur

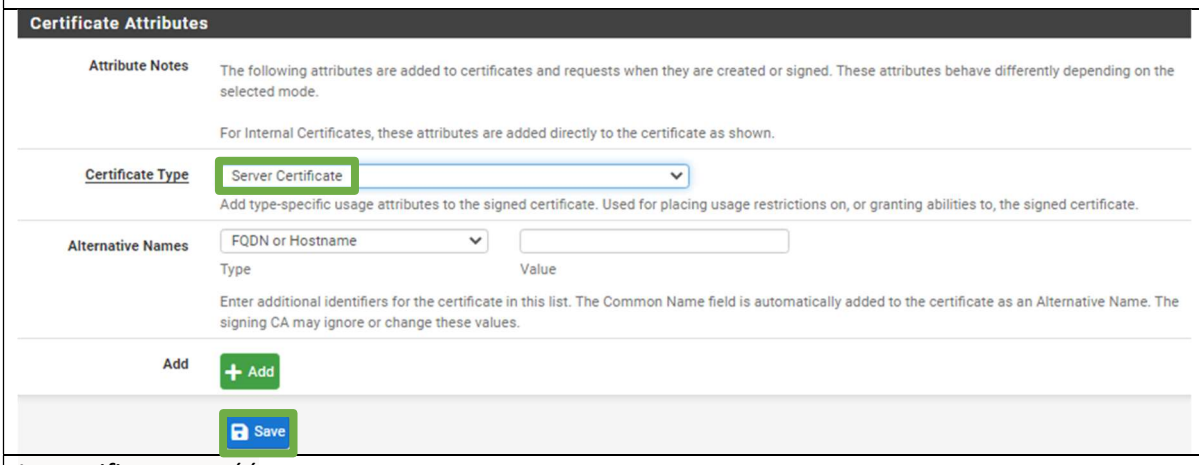
Dans la même rubrique Certificate Manager, accédez à l'onglet Certificat et cliquez sur le bouton Add en bas à droite.



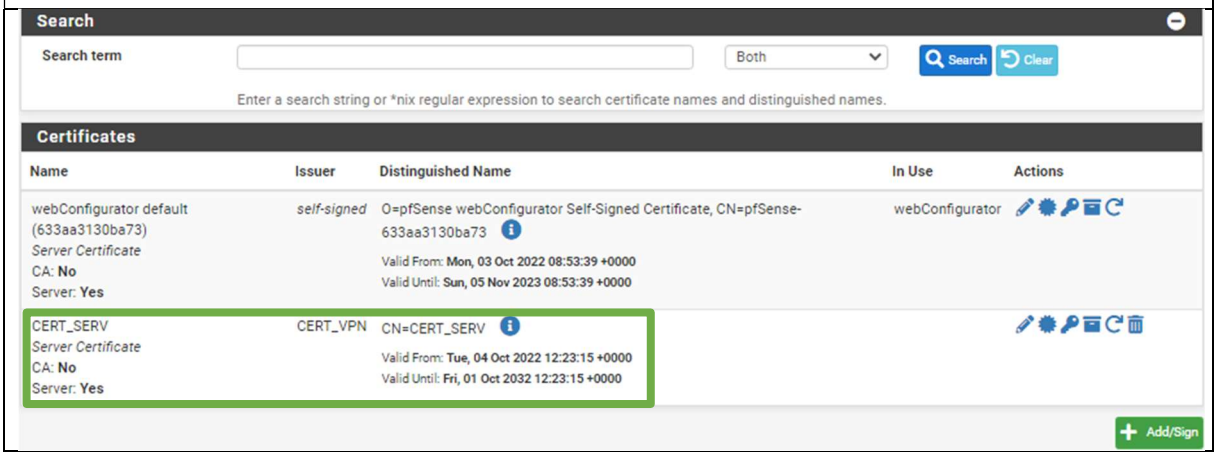
Définir « Method » sur « Create an Internal Certificate« , donner un Nom « CERT_SERV » et sélectionner l'autorité de certification « Certificate authority » créé précédemment « CERT_VPN »



Sélectionnez « Server Certificate » et sauvegardez

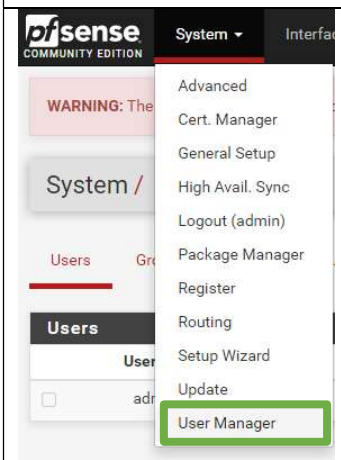


Le certificat est créé

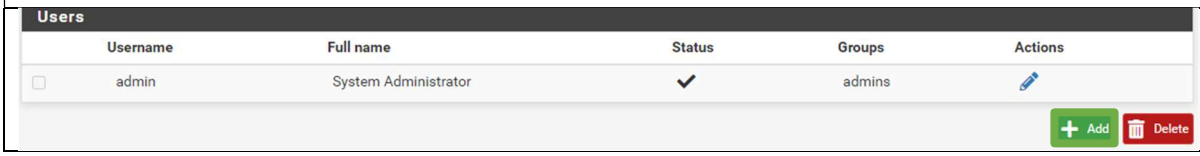


3.3 Création utilisateur VPN

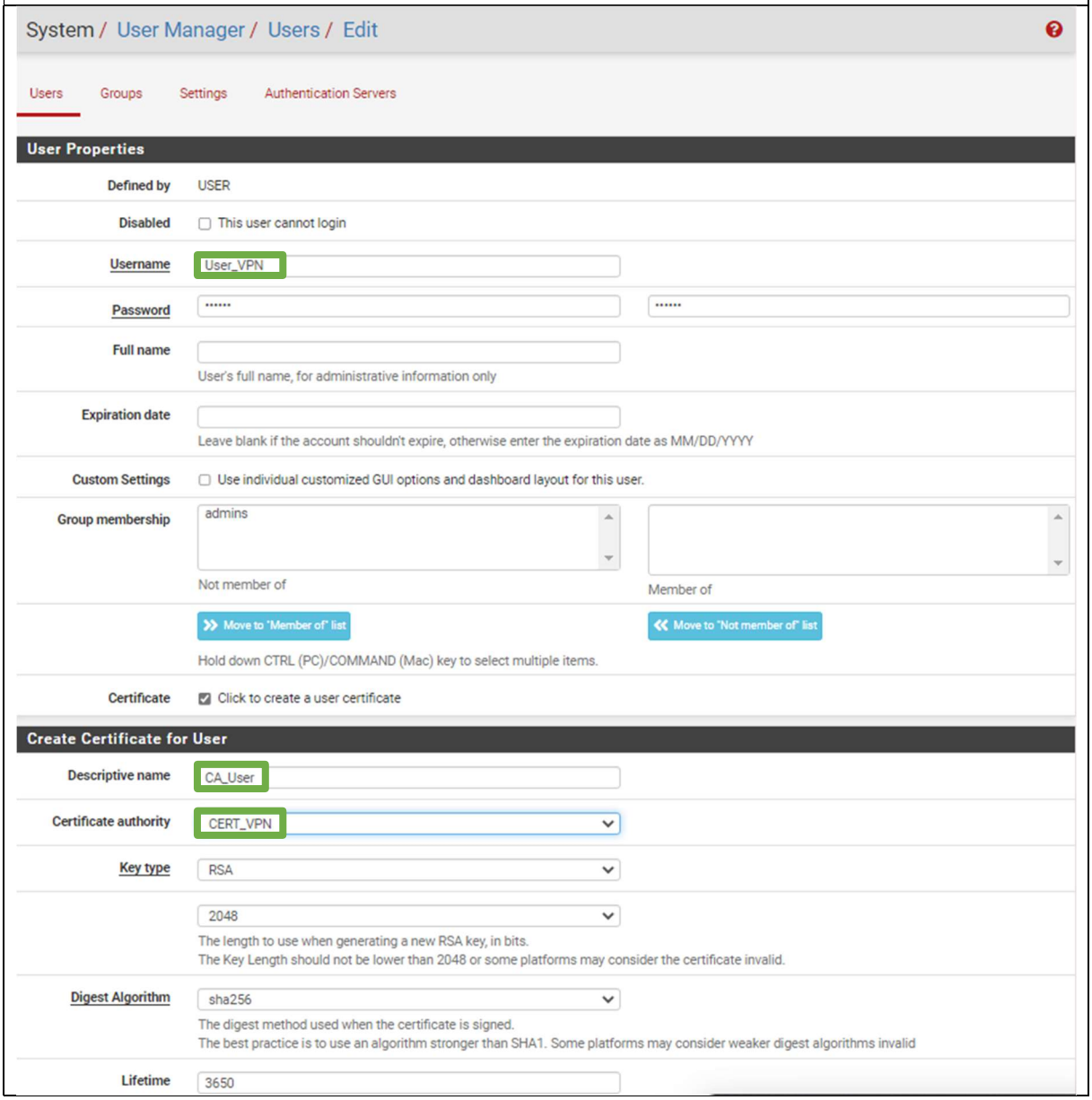
Sélectionnez : System > User Manager



Cliquez sur « Add »

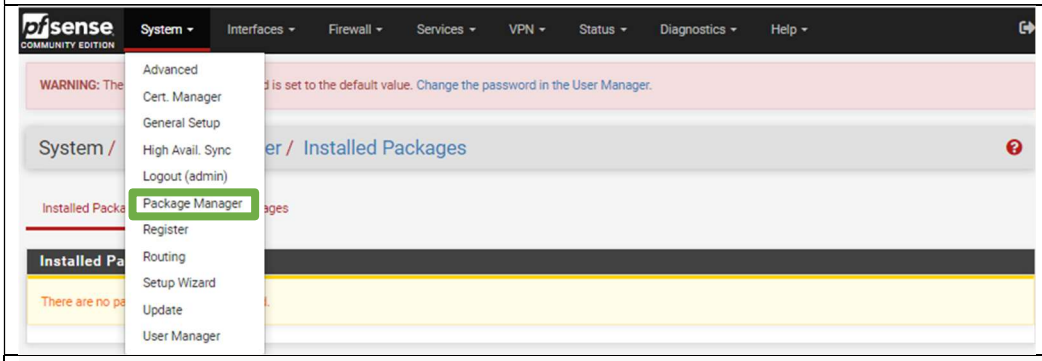


Rentrez le nom « User_vpn » et un mot de passe puis cochez la case « Click to create a user certificate » entrez le nom « CA_User » et sélectionnez le « Certificare authority » « CERT_VPN » puis « save »

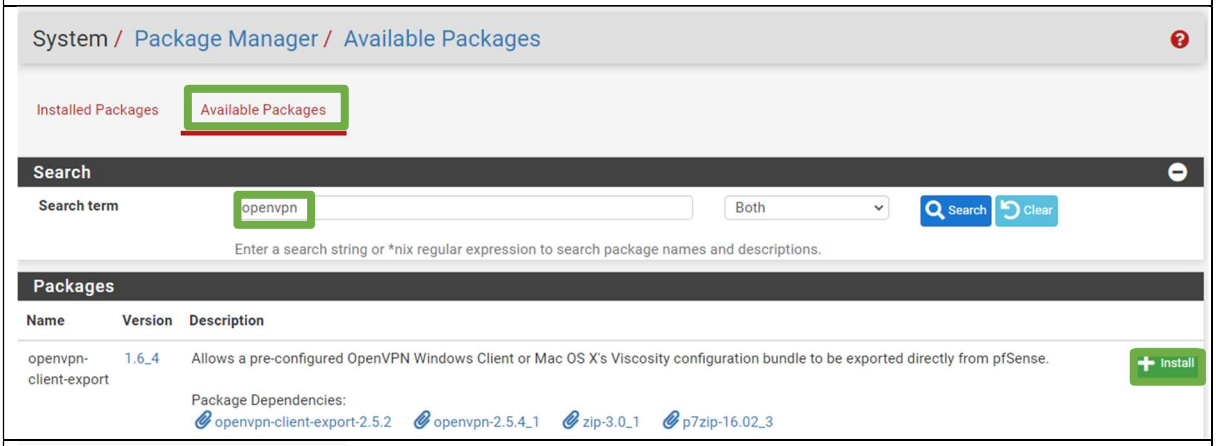


3.4 Installation du package « OpenVPN-Client-Export »

Sélectionnez : System > Package Manager

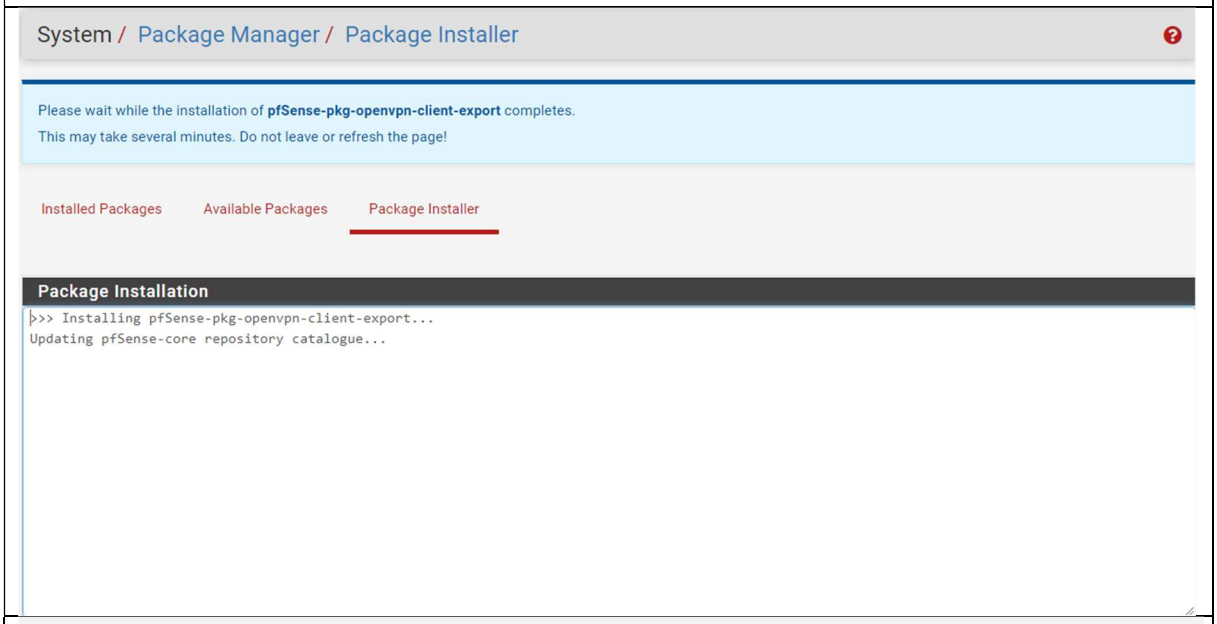


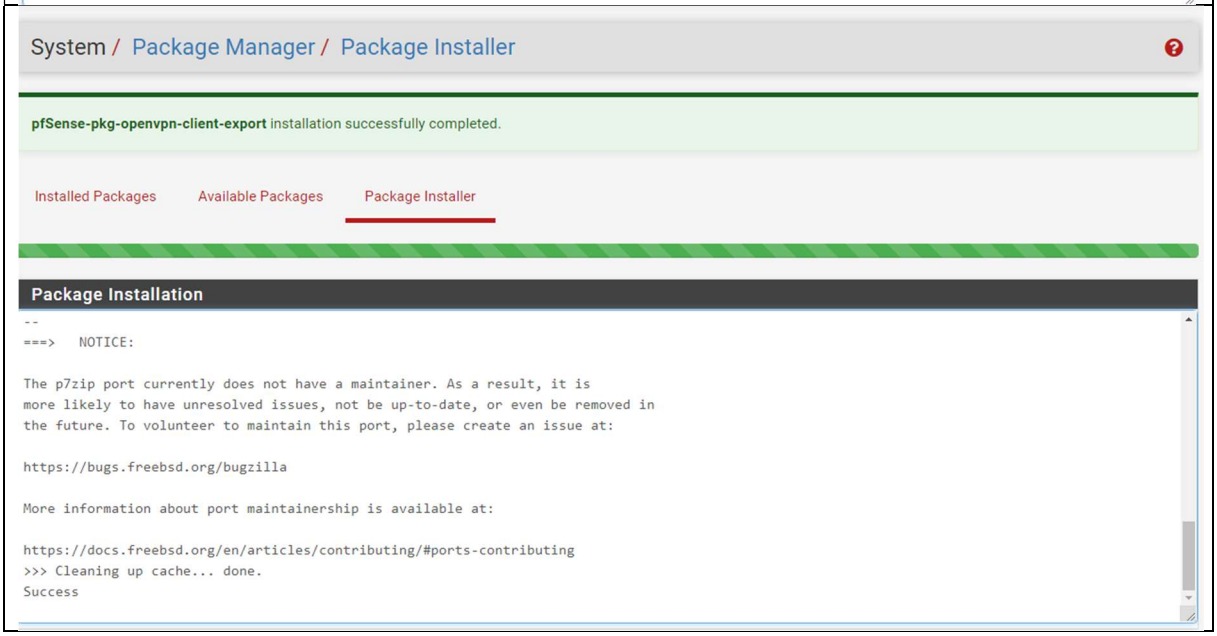
Sélectionnez « Available Packages« , rechercher « openvpn » et installer « openvpn-client-export »



Puis cliquez sur « Confirm »

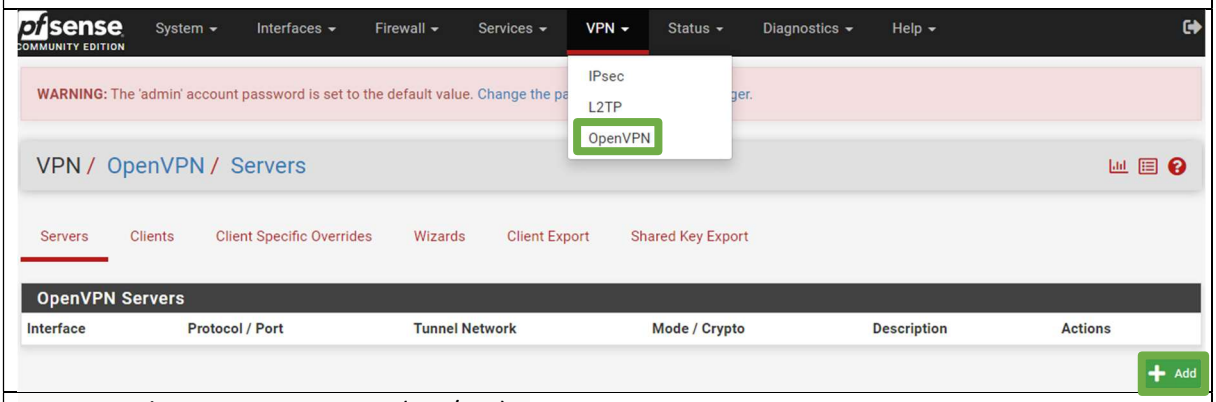
Patientez le temps de l'installation



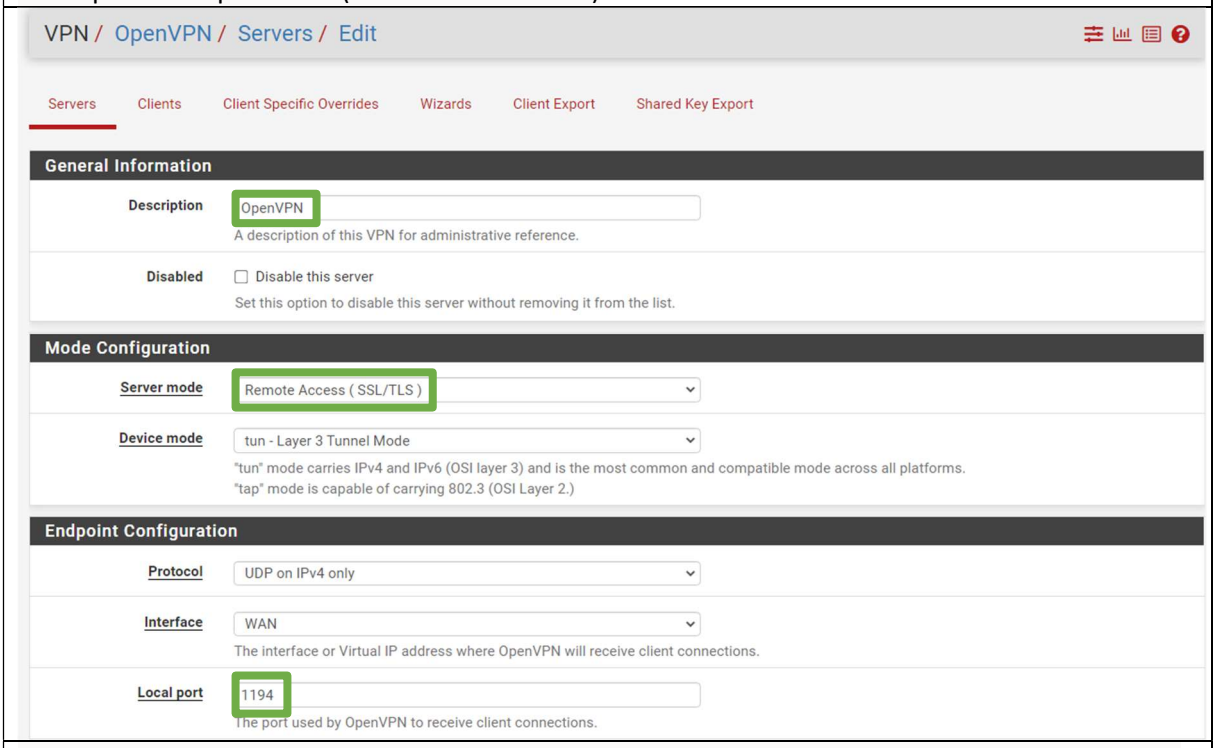


3.5 Configurer OpenVPN

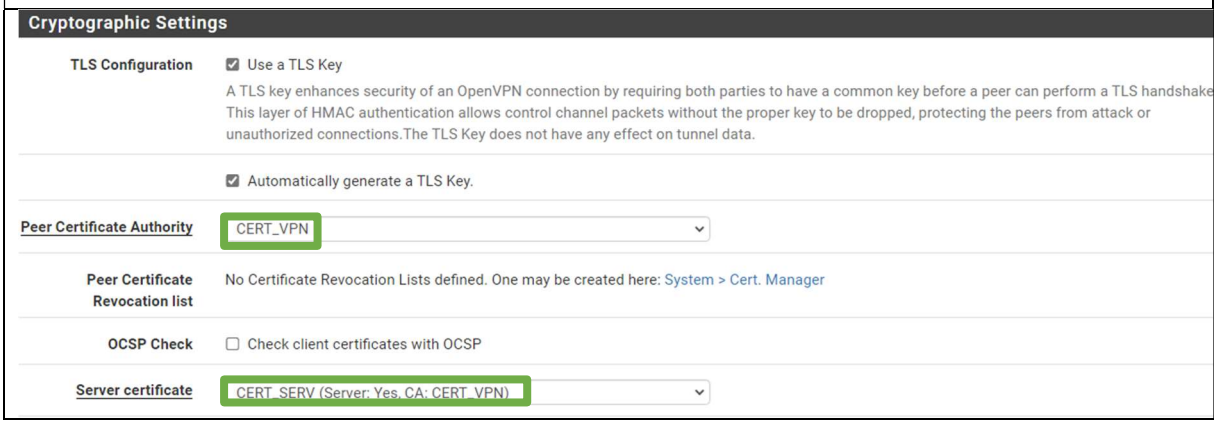
Sélectionnez « VPN » > « OpenVPN » et cliquer sur « + Add »



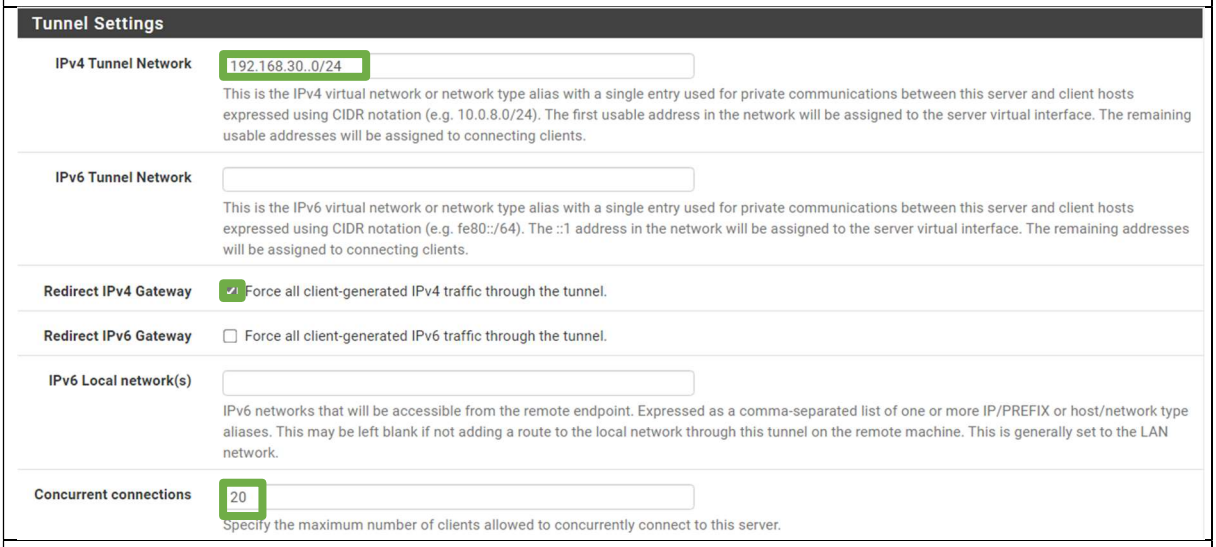
Server mode : « Remote Access (SSL/TLS) »
Local port : 1194 (Port par Défaut)
Description : « OpenVPN » (Nom du Tunnel VPN)



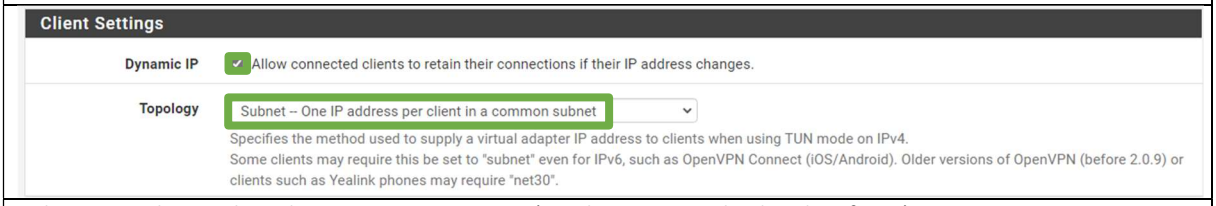
Sélectionnez votre autorité de certification « CERT_VPN » dans « Peer Certificate Authority » et le certificat Server « CERT_SERV» dans « Server certificate ».



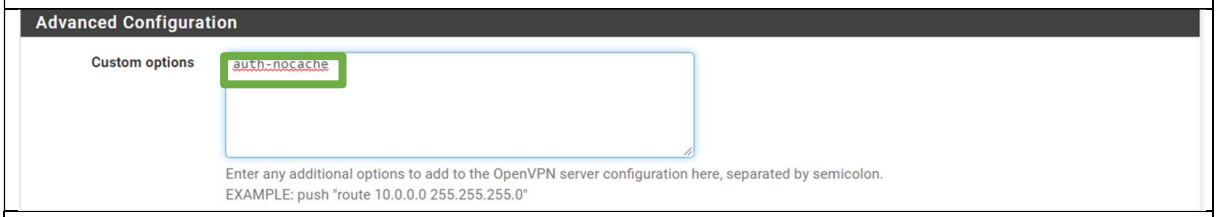
IPv4 Tunnel Network : 192.168.89.0/24 (Adresse du tunnel VPN CIDR. Nous pouvons utiliser n'importe quel adresse IP privé sauf celles définies par la RFC 1918)
Cocher « Redirect IPv4 Gateway » pour passer en mode full tunnel
Concurrent connections : Nombre de connexions VPN simultanées (ici 20)



Cocher « Dynamic IP » et laisser « Topology » sur « Subnet – One IP address per client… »



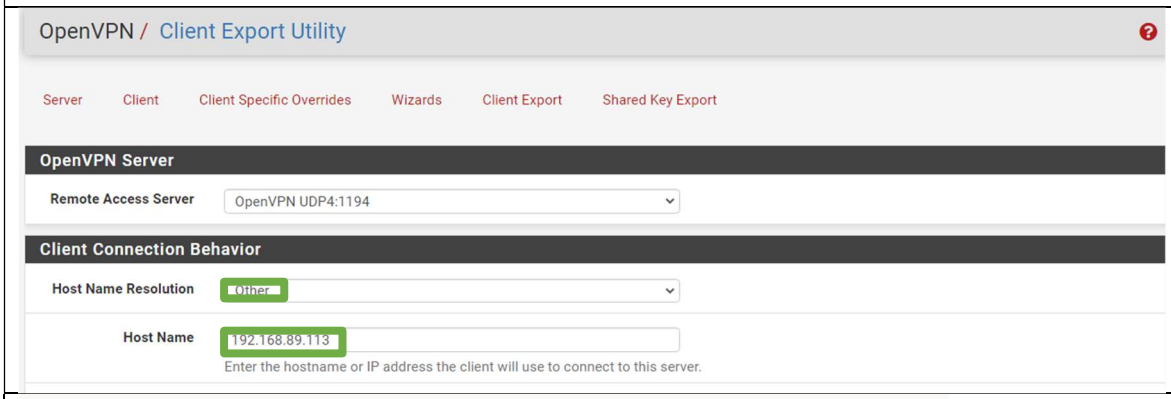
Indiquez « auth-nocache » dans « Custom options« . (Pas de mise en cache des identifiants)



Puis cliquez sur « save », Le serveur vpn est créé.

3.6 Exporter la configuration VPN pour un Client

Menu « Client Export » , Sélectionnez « Other » pour « Host Name Resolution » et renseigner votre IP WAN Publique dans « Host Name »



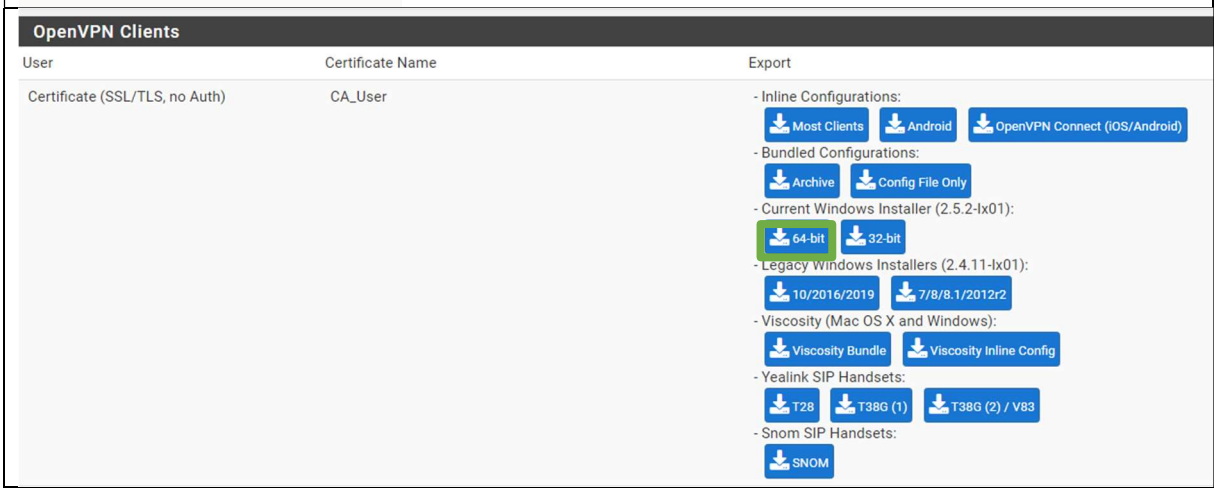
Indiquez « auth-nocache » dans « Additional configuration options » puis save

Toujours dans le Menu « Client Export« , en bas de page, « OpenVPN Clients », 2 Solutions pour l'installation des postes Clients :

-1ère solution : Cliquez sur « Most Clients » pour télécharger uniquement la configuration du Client a importer sur son ordinateur

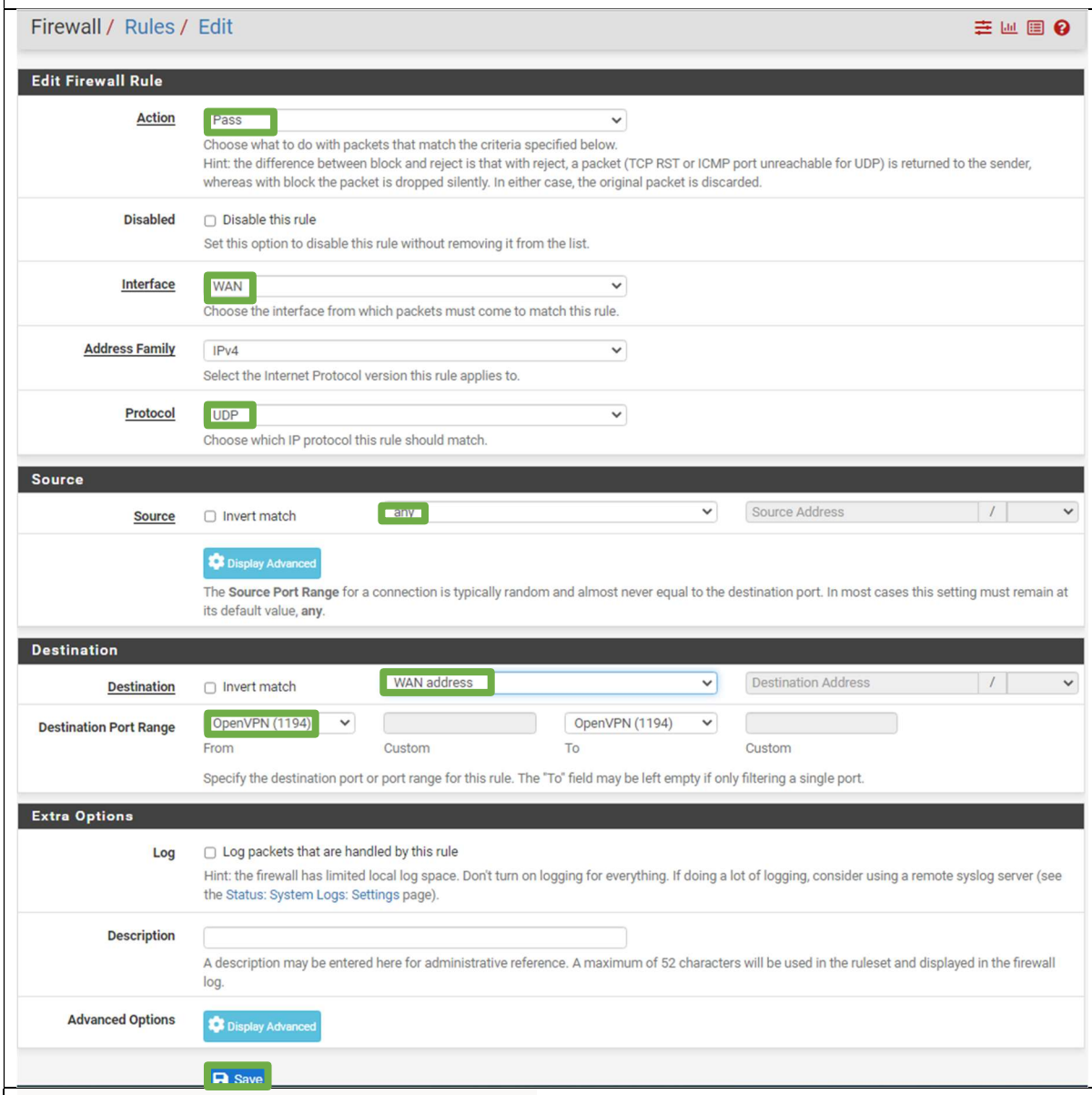
- 2ème solution : Sélectionnez « 64-bit » pour télécharger le Package OpenVPN (Logiciel + fichiers de configuration)

Nous allons choisir la solution 2.

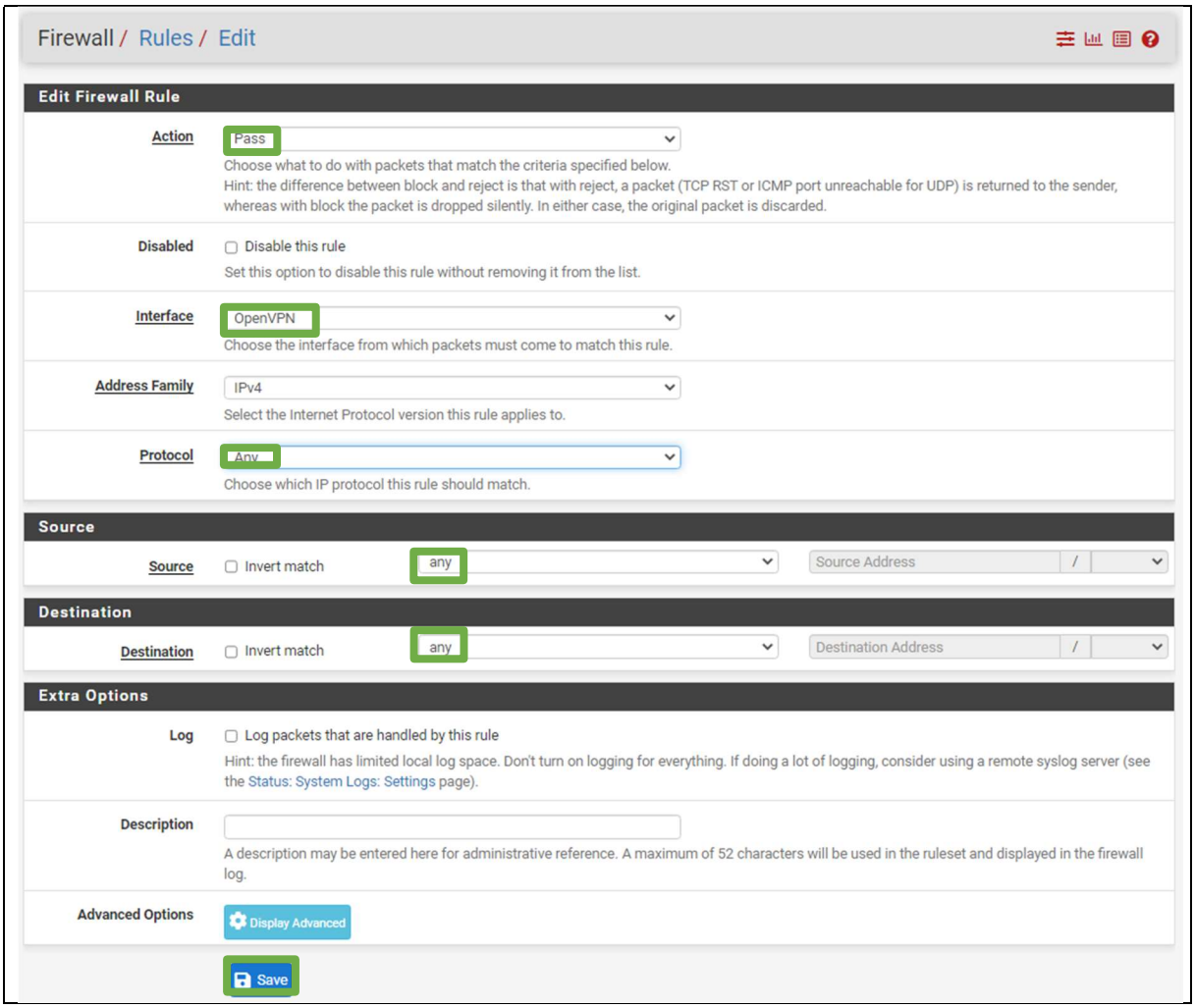


3.7 Configurer les règles du Pare-Feu pfSense

Firewall > Rules > WAN : cliquez sur “+ Add” et renseignez :
Action: Pass
Interface: WAN
Protocol: UDP
Source: any
Destination: WAN address
Destination Port Range: OpenVPN (1194)
Puis cliquez sur “Sauvegarder”

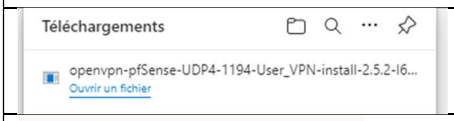


Firewall > Rules > OpenVPN: cliquez sur “+ Add”
Action: Pass
Interface: OpenVPN
Protocol: Any
Source: any
Destination: any

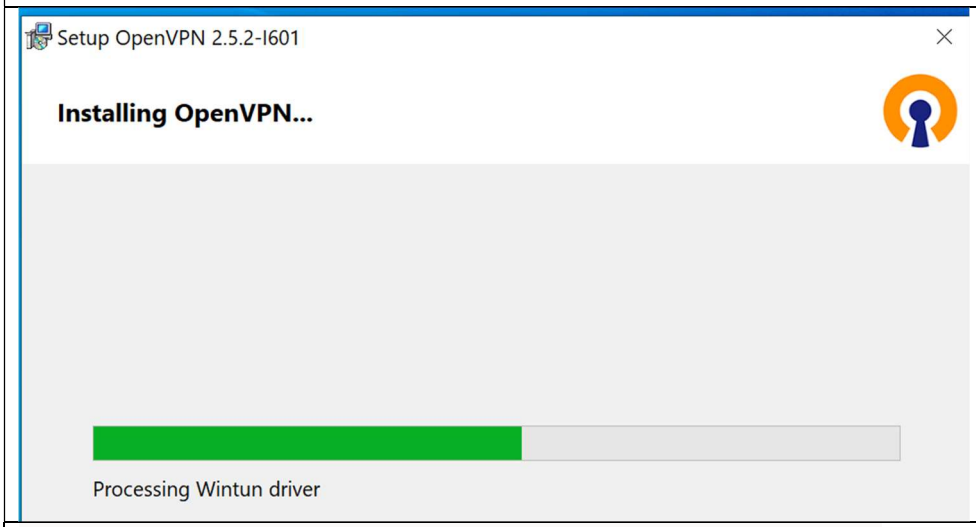


3.8 Test openvpn

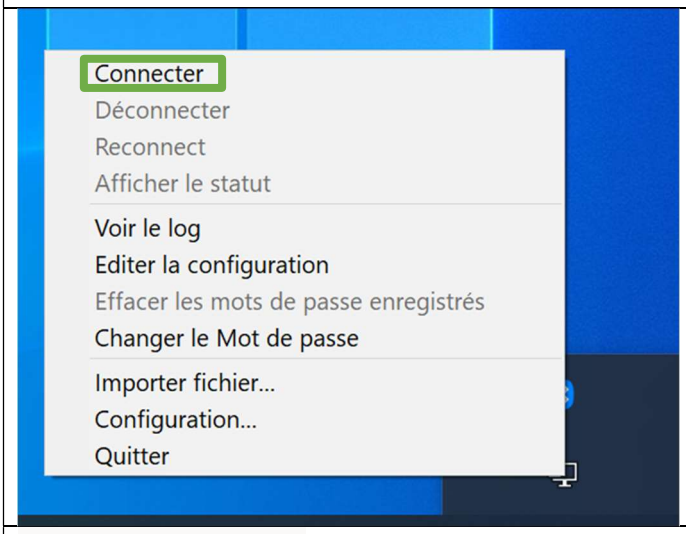
Tout d'abord téléchargez le paquet « x64 » dans l'onglet « vpn/openvpn/client export »



Installez-le sur le poste client



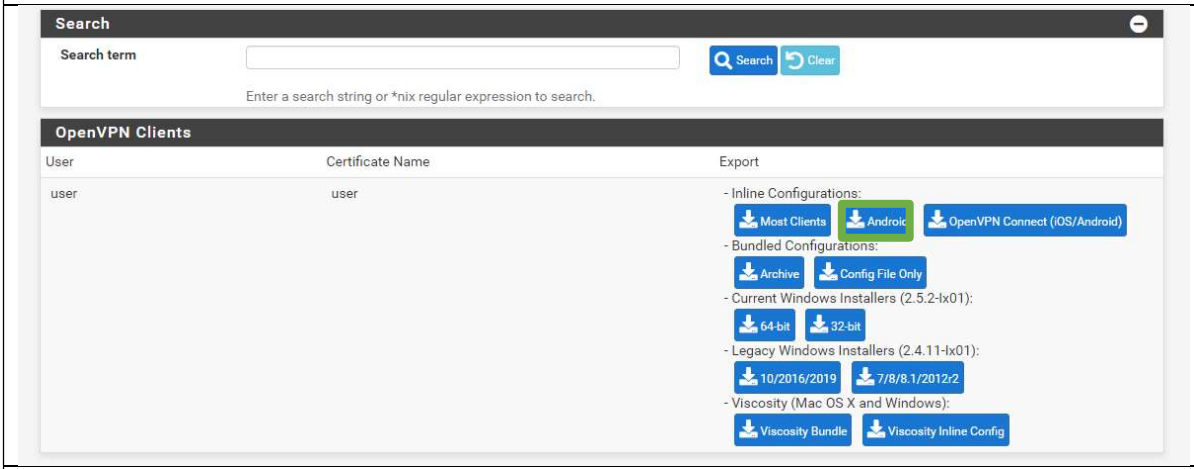
Une fois installé aller faire un clic droit sur l'icone vpn puis « connecter »



La connexion est établie

3.9 Test OpenVPN sur mobile

Tout d'abord, télécharger le paquet "Inline Configuration Android" ou "Android/IOS".



Ensuite, Archiver ce fichier avec Winrar ou 7-zip et envoyer le sur votre mobile via un mail.
Une fois le .zip réceptionné, téléchargez l'application RAR pour le désarchiver sur votre mobile.

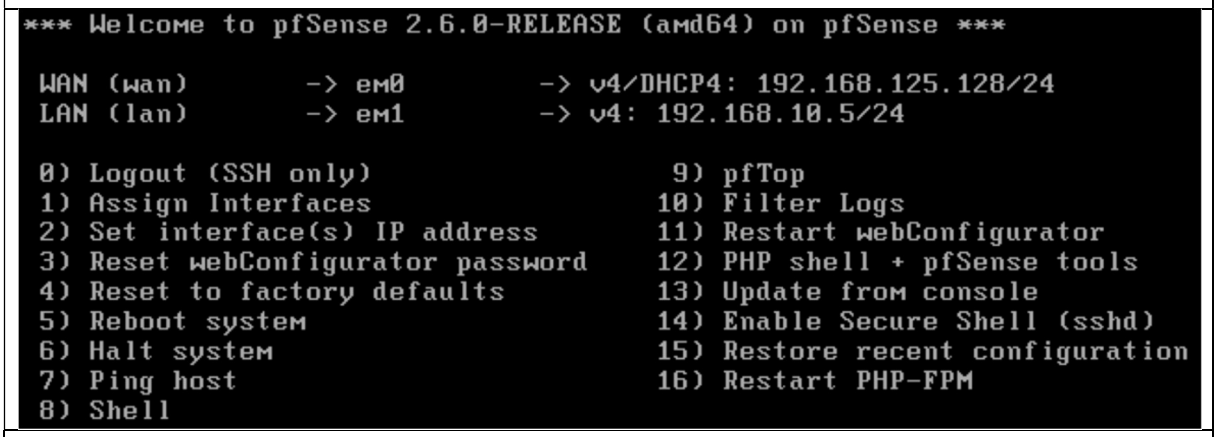
Pour finir, installez l'application Openvpn sur le PlayStore de votre mobile et ouvrez-la, une page d'import de profil va s'afficher. Importez le fichier importé.

Une fois l'import effectuer, connecter vous avec les identifiants de l'utilisateur que vous avez créer préalablement sur PfSense.

4. Problèmes / Résolutions

4.1 Connexion

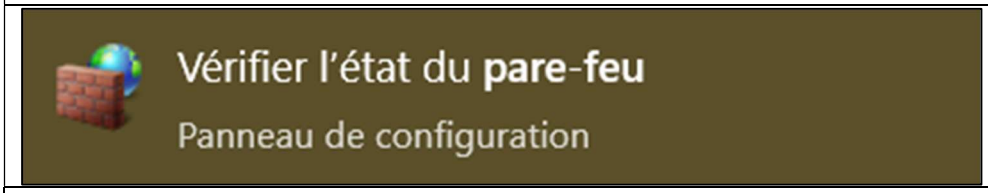
Les VPN ne s'interconnecterons pas tant qu'ils n'ont pas des IP WAN sous le même réseau. L'idéal pour résoudre ce problème, est de connecter les VM sur la même connexion internet
Ensuite, accédez au terminal de votre serveur PfSense.



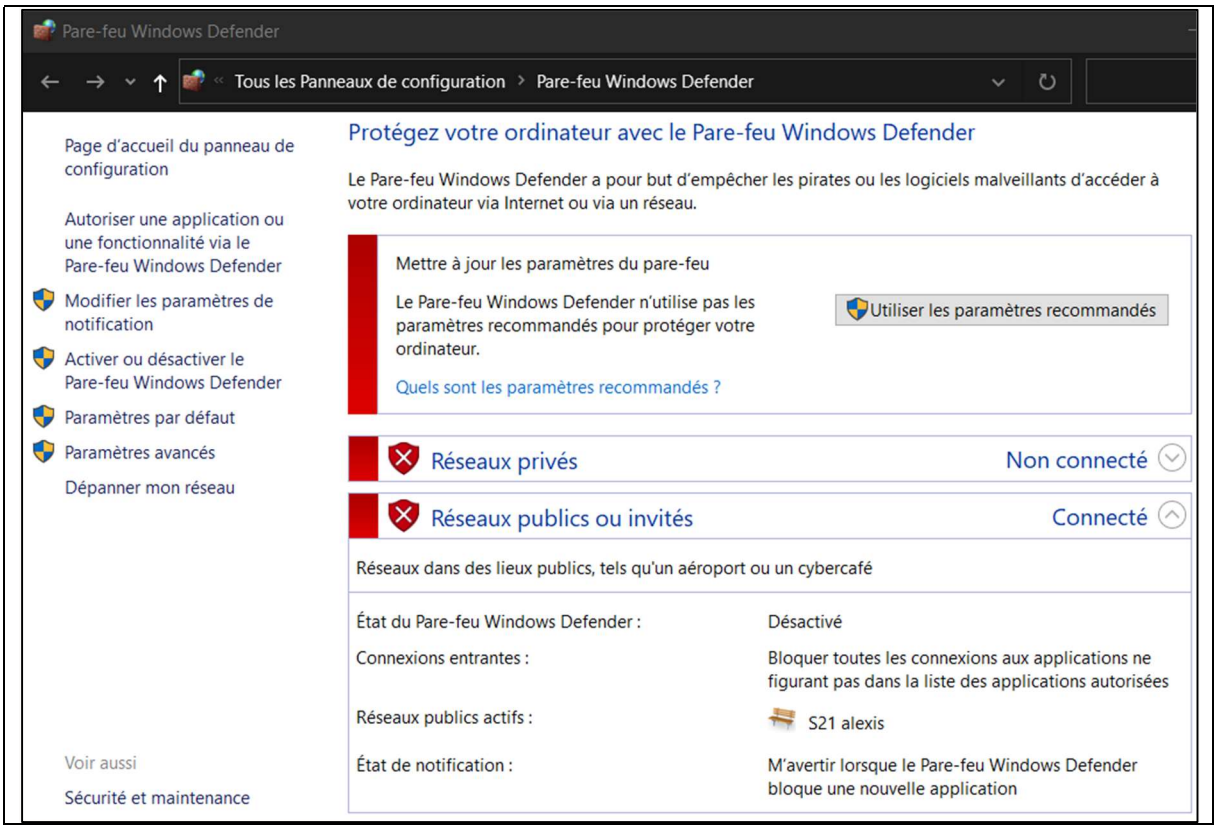
Tapez 2 "Set interface(s) IP address"
Configurez l'adresse et sélectionnez DHCP
Tapez 5 « Reboot system »
Une fois que vos VM ont redémarré, ils prendront une adresse IP WAN sous le même réseaux (192.168.125…)

4.2 Connexion des serveurs en site-à-site

Les deux VPN peuvent ne pas se connecter, pour cela il faut désactivez les pares-feux du PC hôte et des VMs.
Pour cela, tapez « pare-feu » sur la barre de recherche Windows.



Une fenêtre concernant l'état des pares-feux va apparaitre, de la il est possible de les désactiver.



4.3 Problème rencontrés

Absence de ping	Paramétrer correctement les règles pare-feu sur PFSense
Absence de connexion Phase 2	Lors de la configuration, mettre l'adresse réseau de l'adresse LAN et non l'adresse LAN directement Exemple : Adresse IP LAN : 192.168.125.93 Adresse réseau : 192.168.125.0