DOCUMENTATION AP
(Partie B)

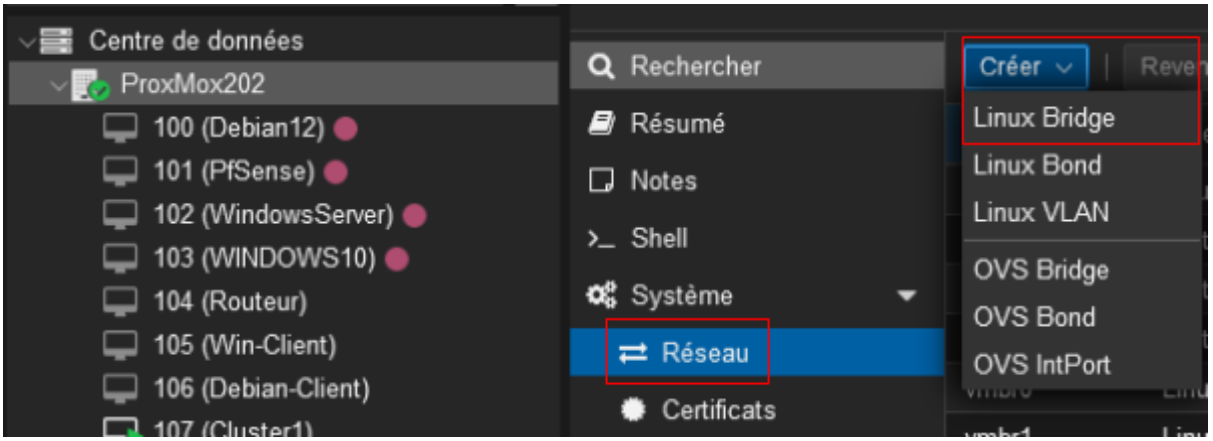
LEPINE Mattéo

BTS SIO 2

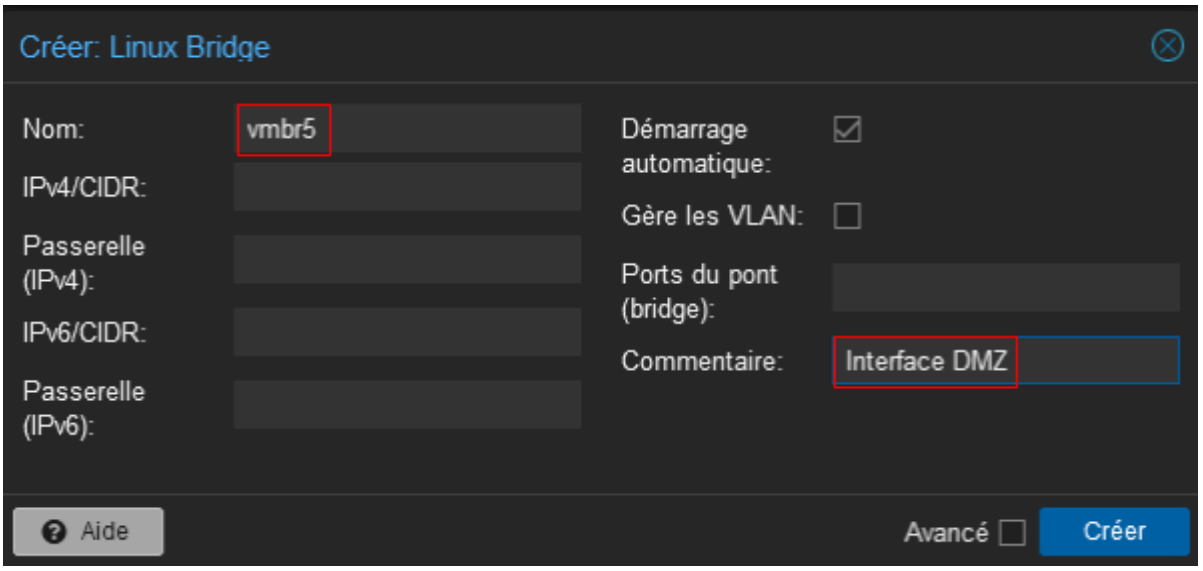
Table des matières :

1 - Création de l'interface DMZ sur Proxmox

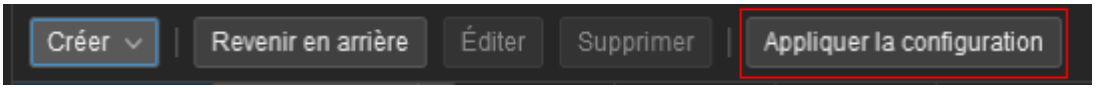
Sur ProxMox, on crée l'interface pour la DMZ :



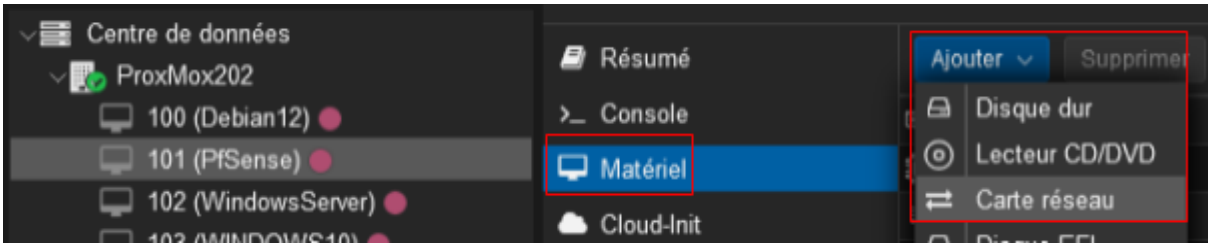
On nomme l'interface et on y ajoute un commentaire si besoin :



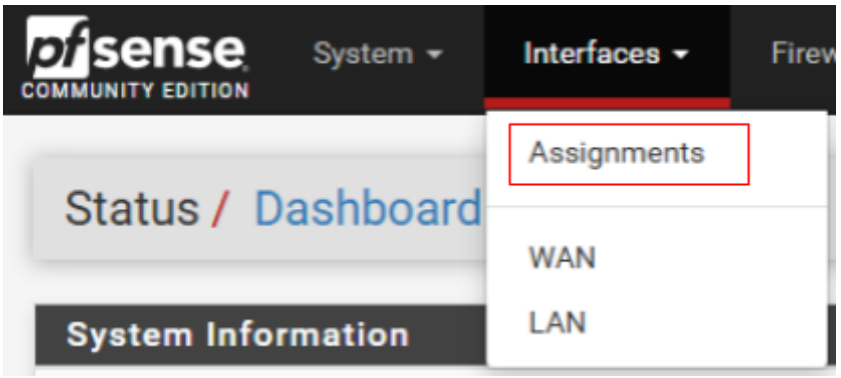
On applique la configuration pour démarrer l'interface sur le ProxMox :



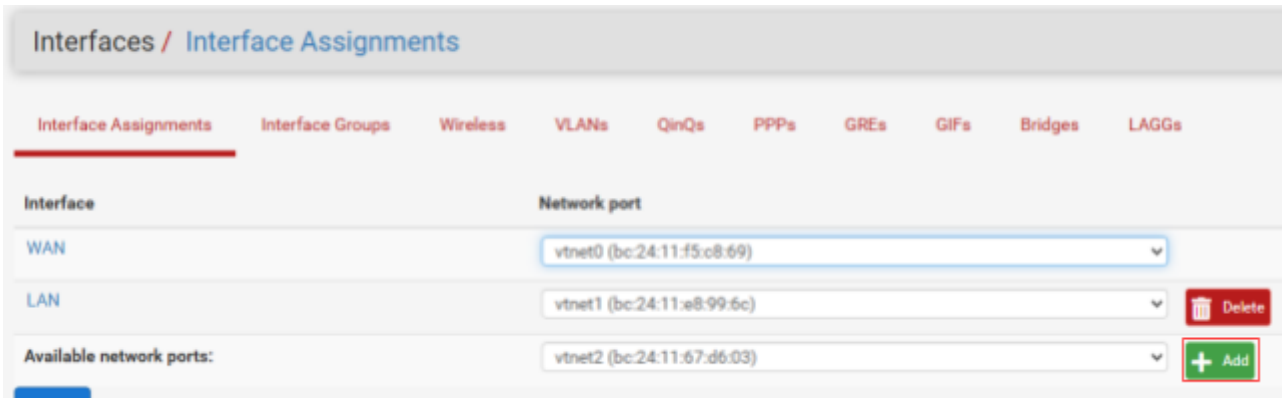
2 - Ajout de l'interface au PfSense :



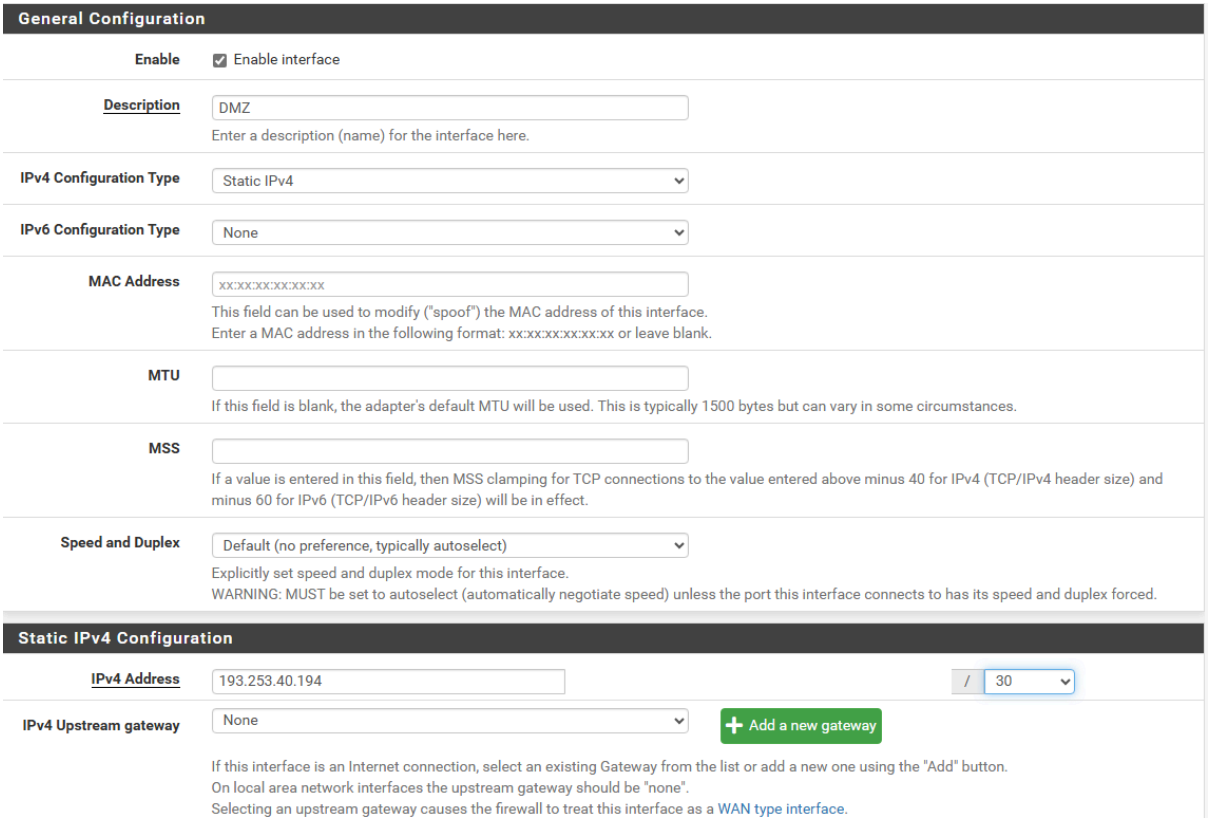
2.1 - Configuration de l'interface de la DMZ via l'interface Web du PfSense :



Ajouter l'interface :



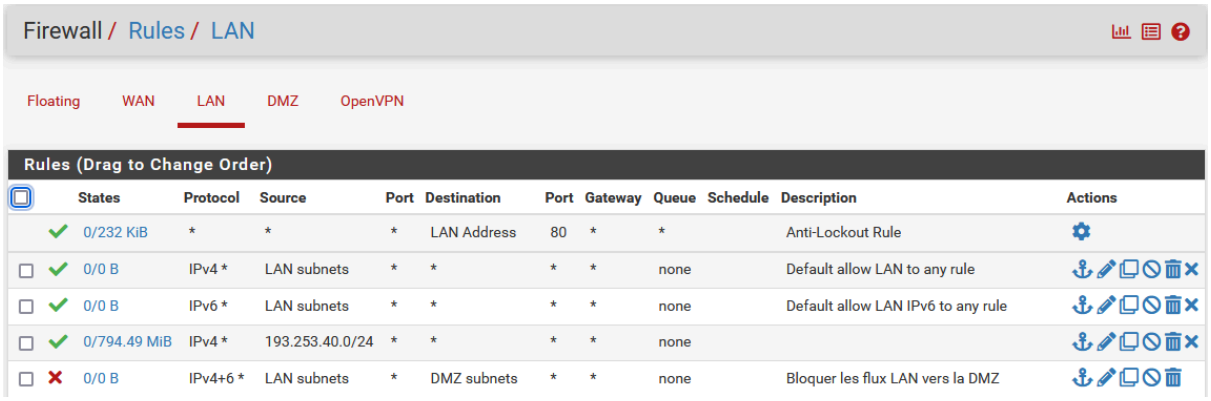
Aller sur le menu de l'interface et la configurer :



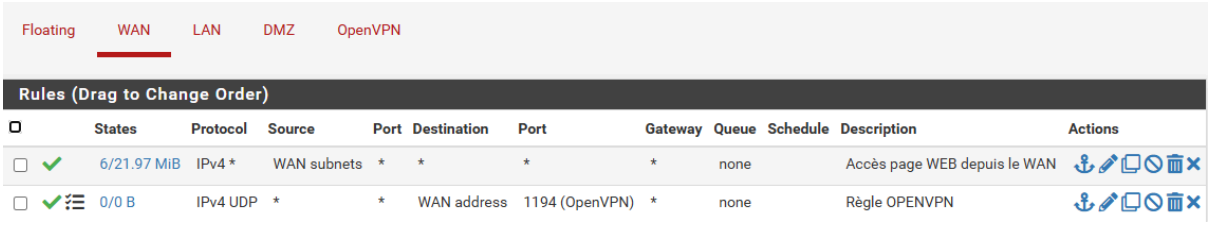
Ensuite sauvegarder la configuration et l'appliquer, la configuration est terminée.

3 - Règles de pare-feu

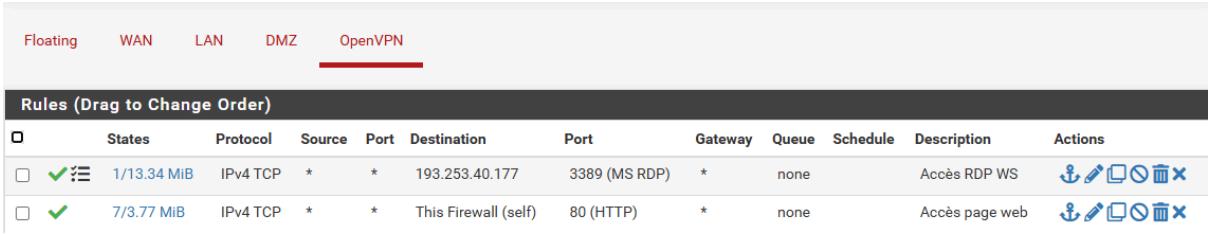
3.1 - Règles du LAN :



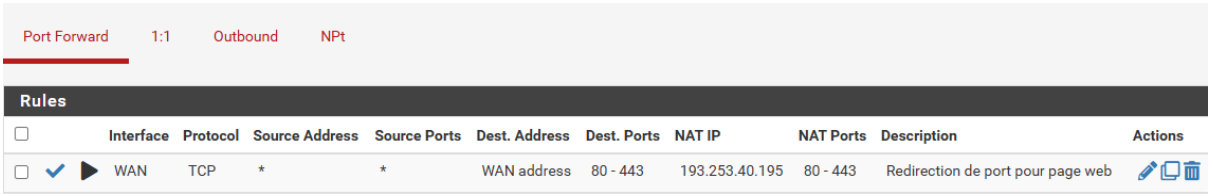
3.2 - Règles sur le WAN :



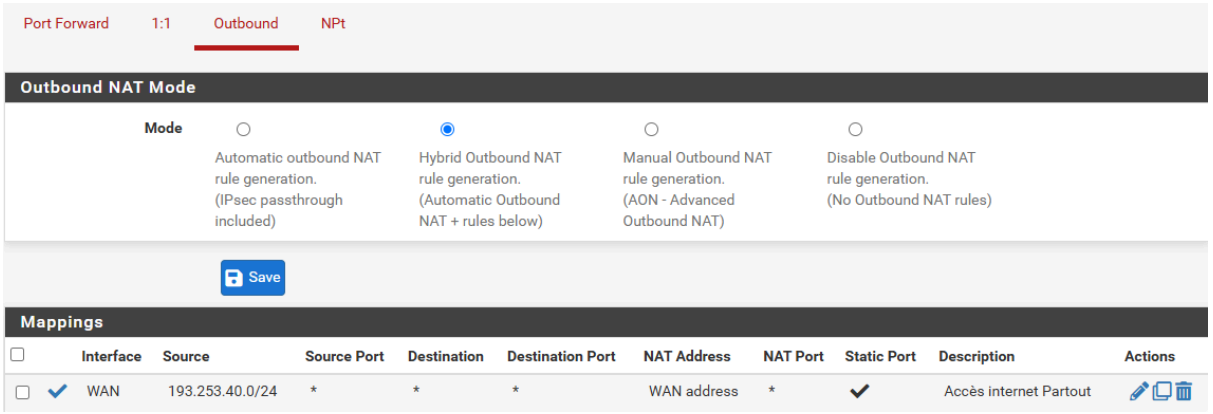
3.3 - Règles sur le VPN :



3.4 - Redirection de port DMZ pour la page web :



3.5 - Communication vers internet de chacun des sous réseaux :

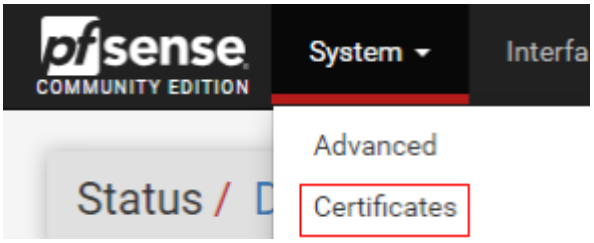


Pour des raisons de facilités, prendre la globalité du réseau est plus simple que faire chacun des sous réseaux à l'unité, à adapter suivant les besoins.

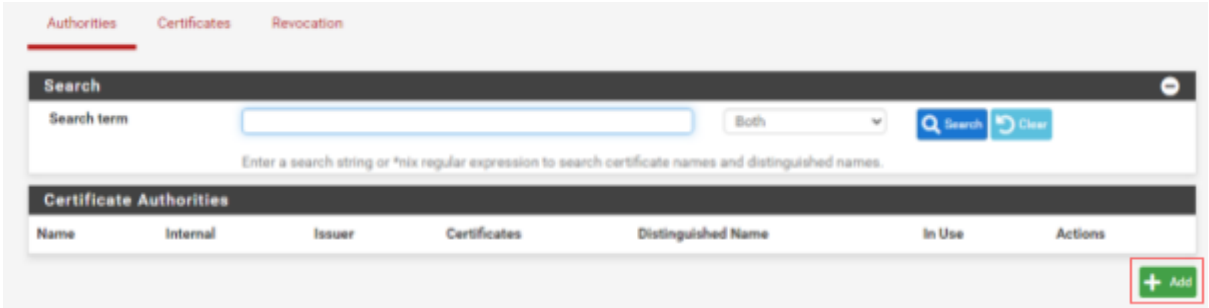
4 - Mise en place du VPN

4.1 - Création des certificats :

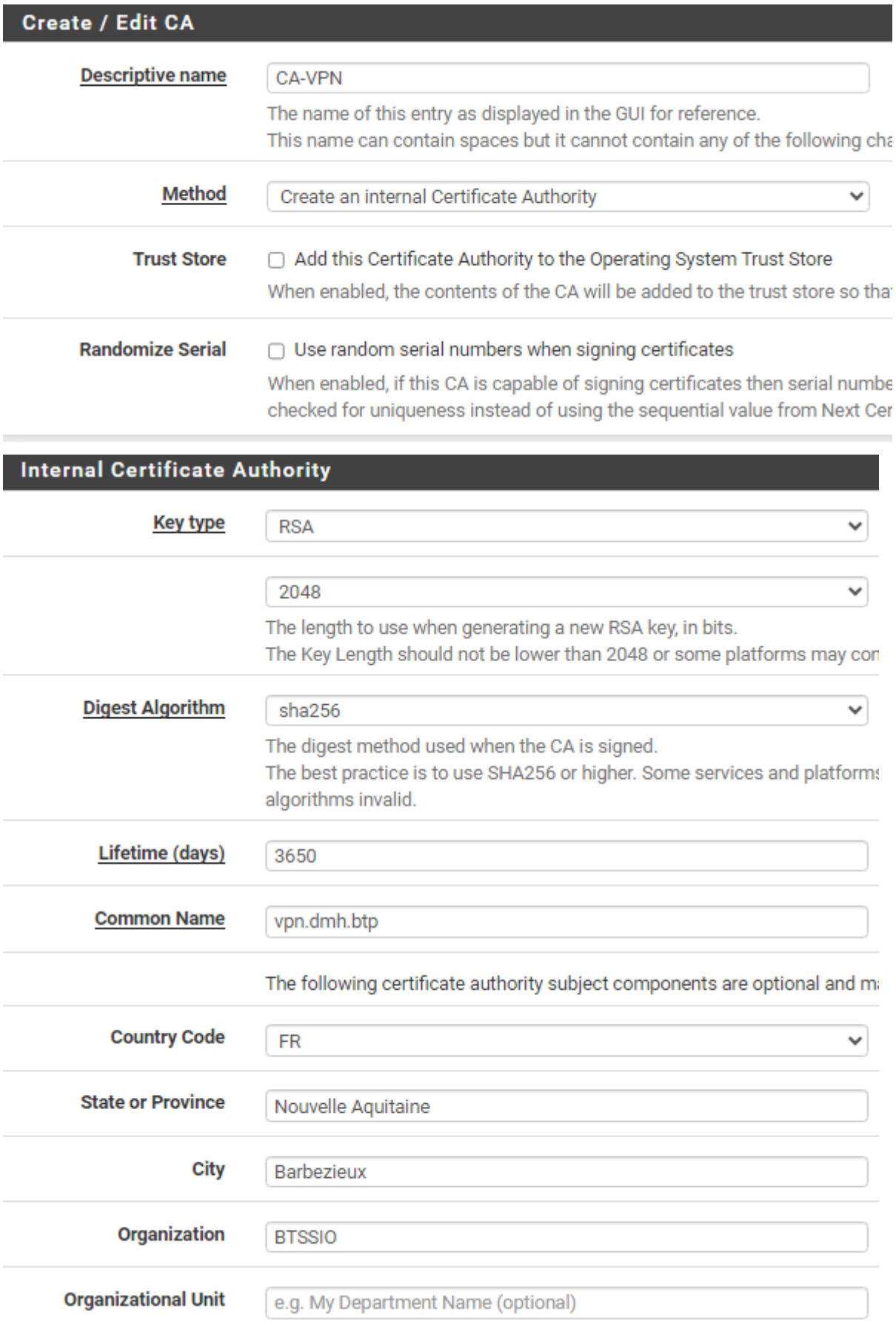
Se rendre sur la page liée aux certificats :



Dans l'onglet 'Autorité', créer le certificat auto-signé de l'autorité de certification :

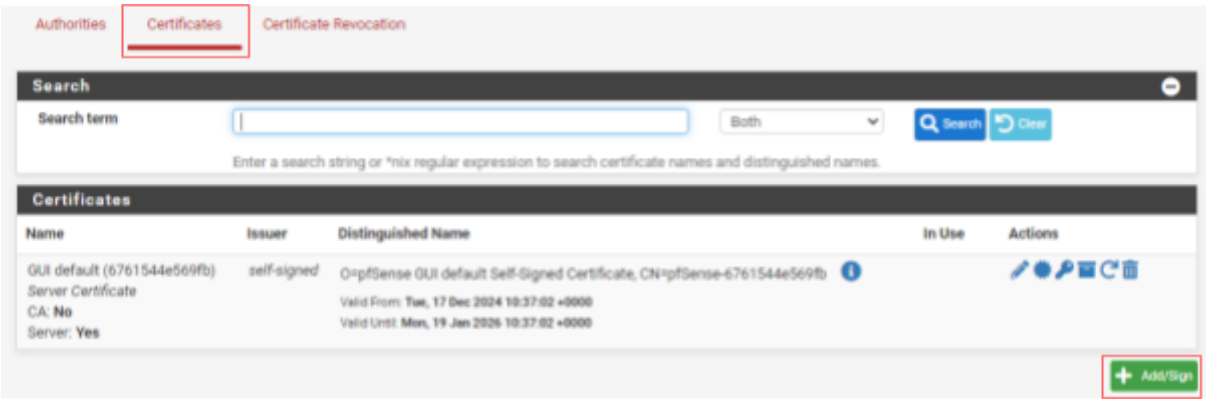


Entrer les informations dont on a besoin pour créer le certificat :

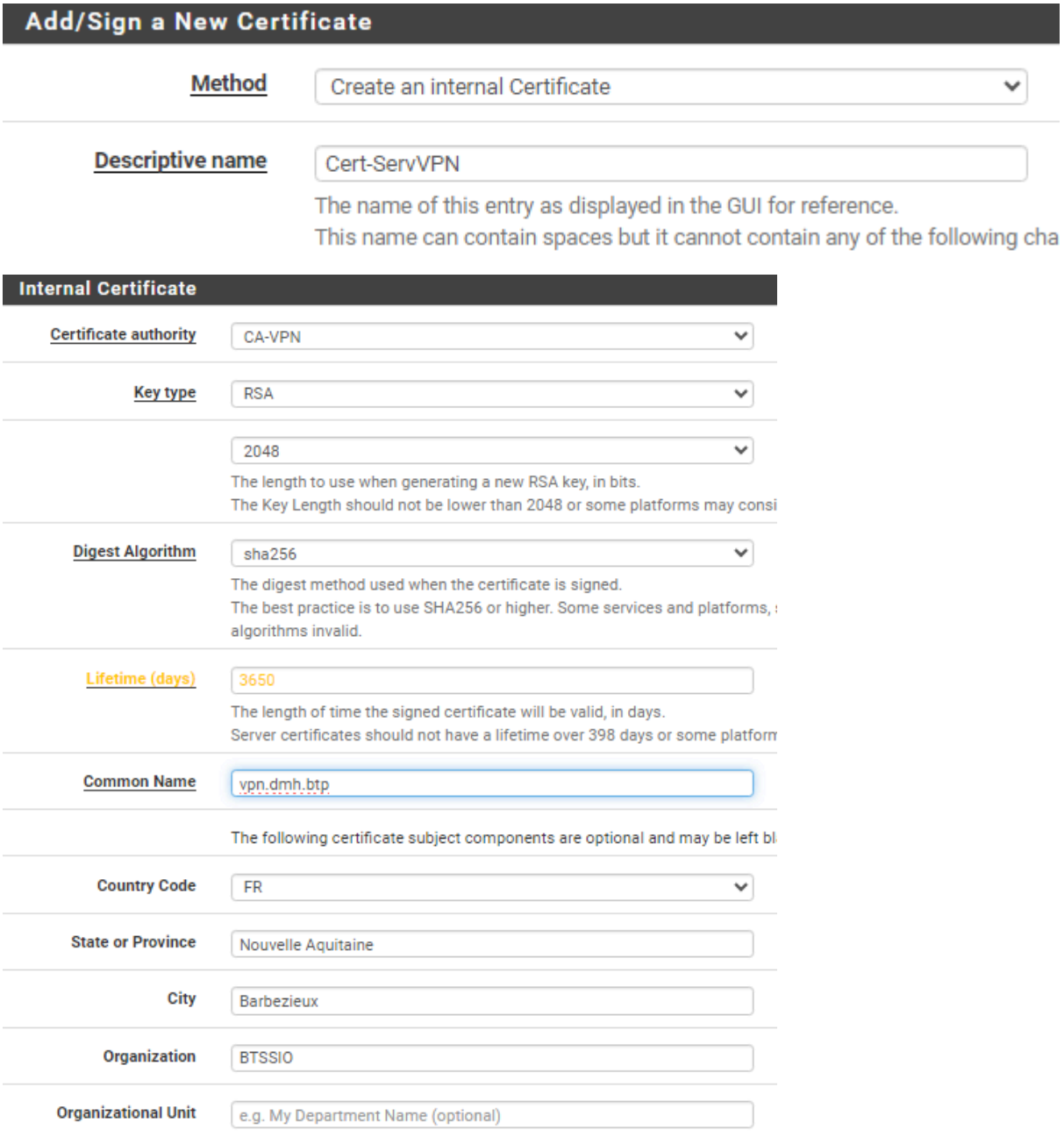


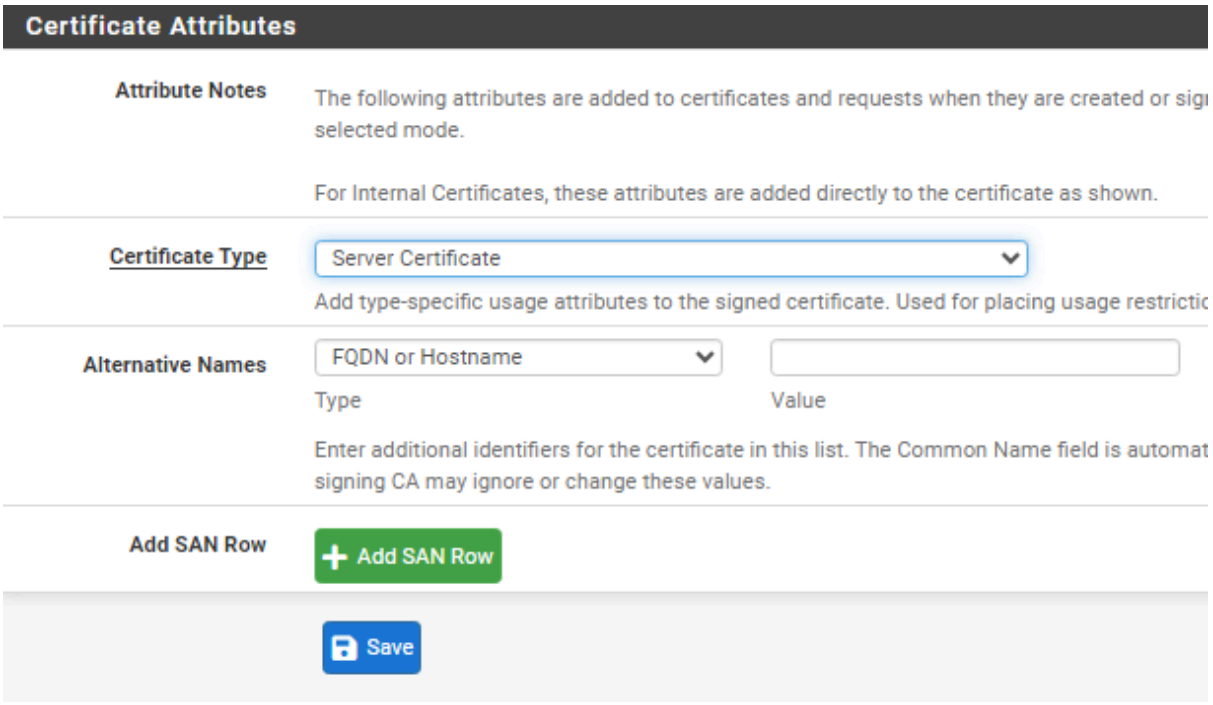
Ensuite on appuie sur "Sauvegarder", notre certificat est donc créé.

Création du certificat du serveur VPN :



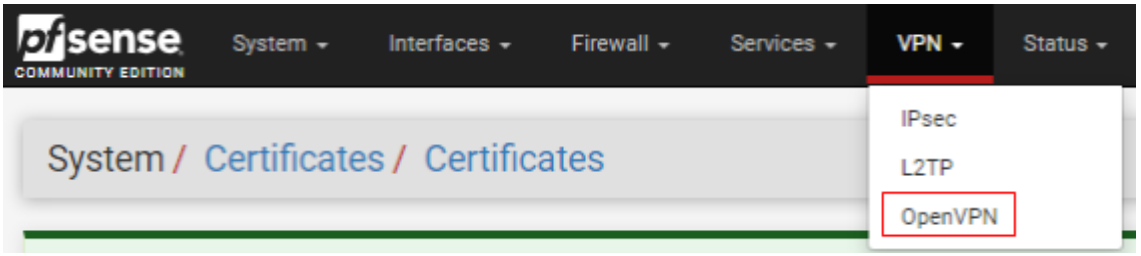
On appuie sur add pour créer le certificat du serveur :



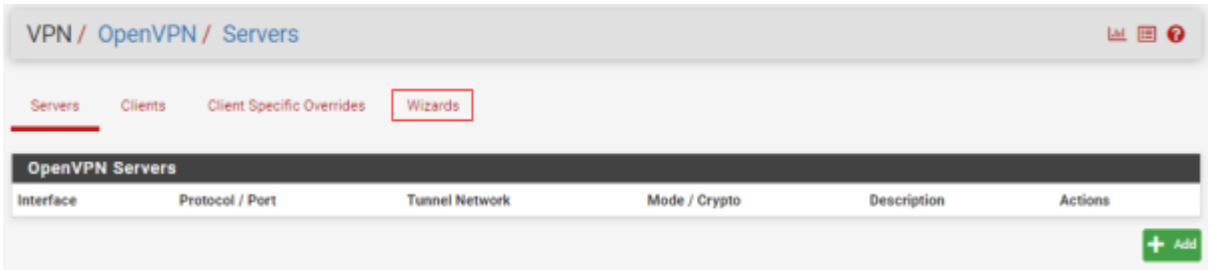


Et on sauvegarde le certificat du serveur.

4.2 - Configuration du serveur VPN :

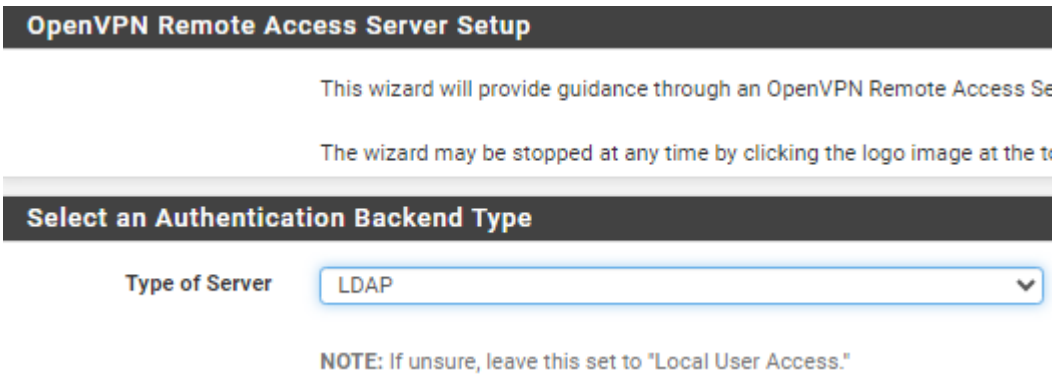


Pour une configuration plus simple et rapide on utilise l'onglet "Wizards" :

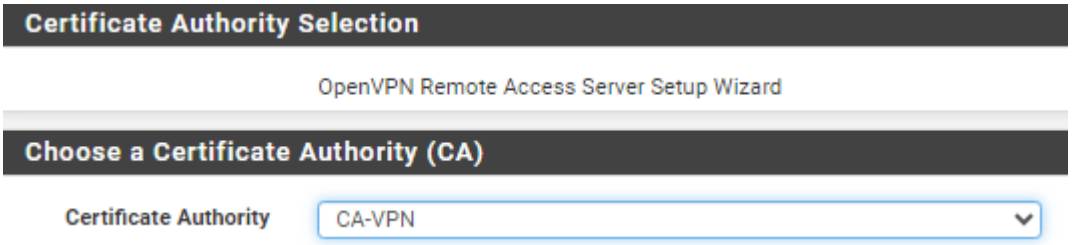


et ensuite on suit les étapes de la configuration :

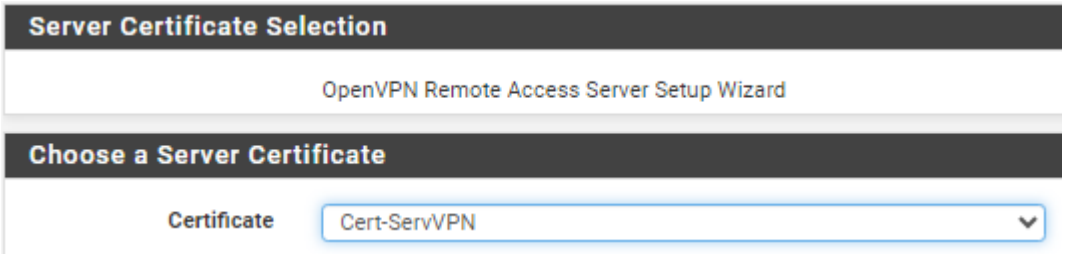
J'ai au préalable configuré un serveur d'Authentification pour pouvoir utiliser les utilisateurs de mon AD lors de la connexion au VPN via le protocole LDAP.



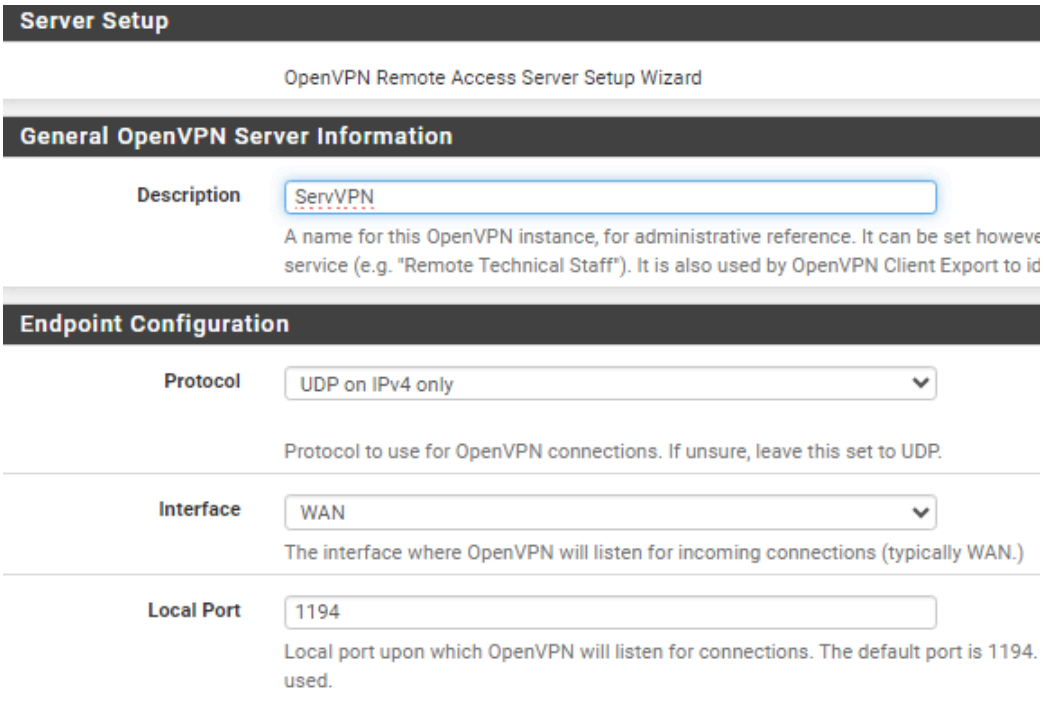
On choisit le certificat de son autorité :



On choisit le certificat de son serveur VPN :



On configure le serveur : (à adapter suivant les besoins)



Cryptographic Settings

TLS Authentication — ☑ Enable authentication of TLS packets.

Generate TLS Key — ☑ Automatically generate a shared TLS authentication key.

TLS Shared Key

Paste in a shared TLS key if one has already been generated.

DH Parameters Length — 2048 bit

Length of Diffie-Hellman (DH) key exchange parameters, used for establishing
from key sizes, but as with other such settings, the larger the key, the more se
As of 2016, 2048 bit is a common and typical selection.

Data Encryption Algorithms

AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305

List of algorithms clients can negotiate to encrypt traffic between endpoints. T
Certain algorithms will perform better on different hardware, depending on the
finishing the wizard for additional choices.

Fallback Data Encryption Algorithm — AES-256-CBC (256 bit key, 128 bit block)

The algorithm used to encrypt traffic between endpoints when data encryptior

Auth Digest Algorithm — SHA256 (256-bit)

The method used to authenticate traffic between endpoints. This setting must
desired.

Hardware Crypto — No Hardware Crypto Acceleration

The hardware cryptographic accelerator to use for this VPN connection, if any

Tunnel Settings

IPv4 Tunnel Network — 10.10.10.0/24 — Adresse réseau du tunnel

This is the virtual network used for private communications between this serv
first network address will be assigned to the server virtual interface. The rema

Redirect IPv4 Gateway — ☐ Force all client generated traffic through the tunnel.

IPv4 Local Network — 192.168.50.0/24 — Réseau dont on veut avoir accès

This is the network that will be accessible from the remote endpoint, expresse
local network through this tunnel on the remote machine. This is generally set

Concurrent Connections — 10 — Nombre connexions max en simultanées

Specify the maximum number of clients allowed to concurrently connect to th

Allow Compression — Refuse any non-stub compression (Most secure)

Allow compression to be used with this VPN instance, which is potentially ins

Compression — Disable Compression [Omit Preference]

Compress tunnel packets using the chosen option. Can save bandwidth, but is
compression is not allowed. Adaptive compression will dynamically disable c
packets is not being compressed efficiently.

Type-of-Service — ☐ Set the TOS IP header value of tunnel packets to match the encapsulated p

Inter-Client Communication — ☐ Allow communication between clients connected to this server.

Duplicate Connections — ☑ Allow multiple concurrent connections from clients using the same Comm

NOTE: This is not generally recommended, but may be needed for some scen

Duplicate Connection Limit — 10 — Utilisation du même utilisateur pour se connecter au vpn et combien de fois max

Limit the number of concurrent connections from the same user.

Advanced Client Settings

DNS Default Domain
192.168.50.182
Provide a default domain name to clients.

DNS Server 1
DNS server IP to provide to connecting clients.

DNS Server 2
DNS server IP to provide to connecting clients.

DNS Server 3
DNS server IP to provide to connecting clients.

DNS Server 4
DNS server IP to provide to connecting clients.

NTP Server
Network Time Protocol server to provide to connecting clients.

NTP Server 2
Network Time Protocol server to provide to connecting clients.

NetBIOS Options
☐ Enable NetBIOS over TCP/IP.
If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will

NetBIOS Node Type
none
Possible options: b-node (broadcasts), p-node (point-to-point name queries to
(query name server, then broadcast).

NetBIOS Scope ID
A NetBIOS Scope ID provides an extended naming service for NetBIOS over T
to only those nodes with the same NetBIOS scope ID.

WINS Server 1
192.168.50.182
A Windows Internet Name Service (WINS) server IP to provide to connecting c

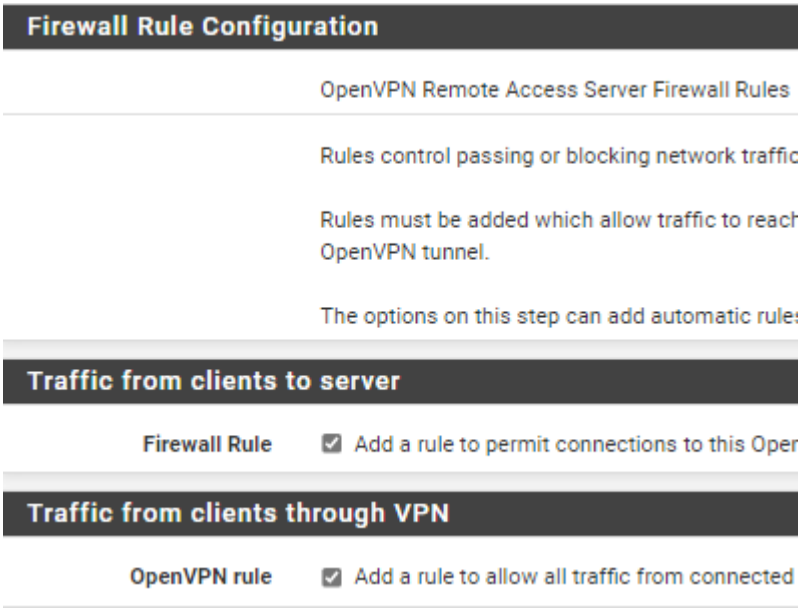
WINS Server 2

Settings

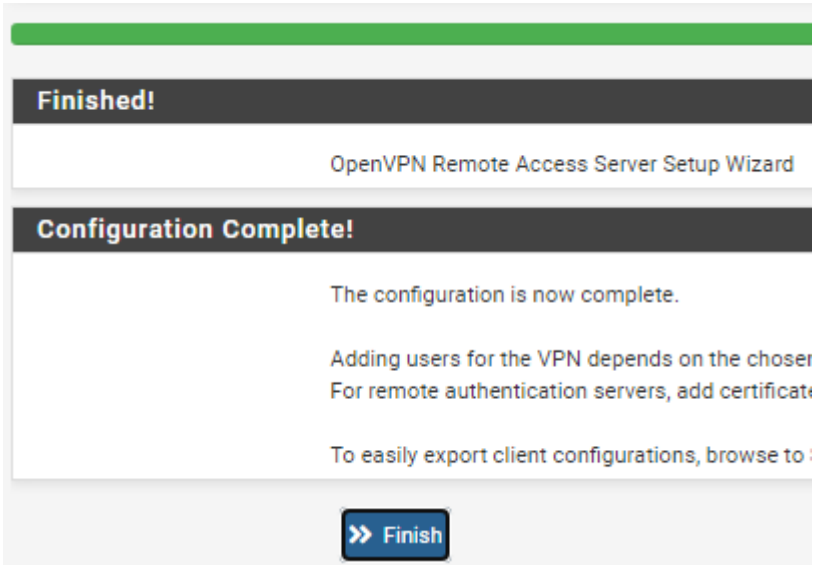
Dynamic IP
☑ Allow connected clients to retain their connections if their IP address changes.

Topology
Subnet -- One IP address per client in a common subnet
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".

Et enfin pour finir la configuration, on ajoute si on le souhaite, les règles (créées automatiquement) :



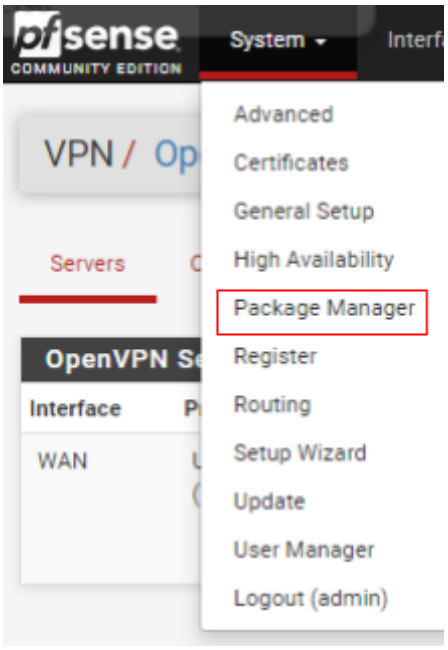
On clique sur "Next", et notre configuration est enfin terminée !



4.3 - Exportation de la configuration du VPN :

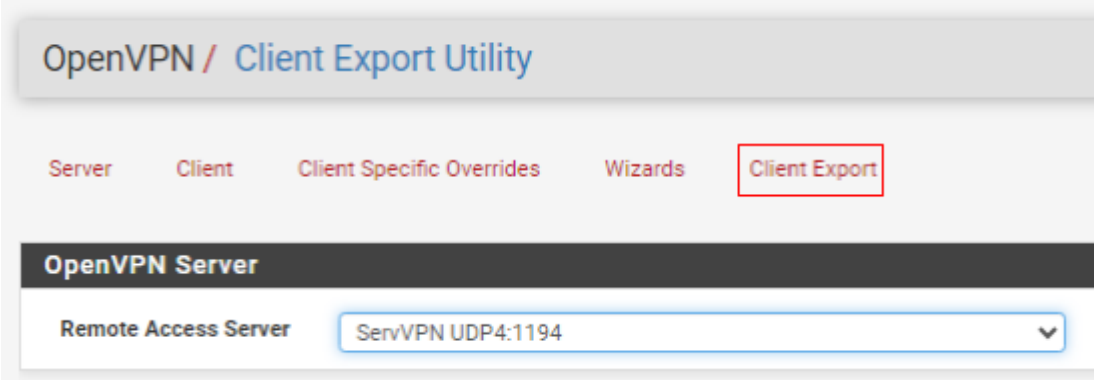
Pour exporter la configuration du VPN, on doit installer un paquet nommé "openvpn-client-export"

Pour l'installer on se rend sur la page faites pour :

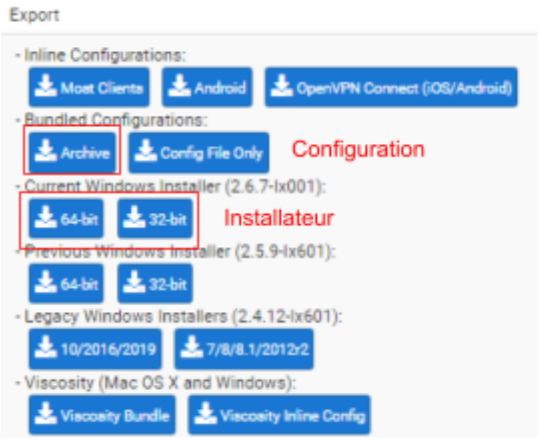


Et on installe le paquet.

Après l'installation on retourne sur la page précédente du service VPN et on va sur l'onglet "Client Export" :

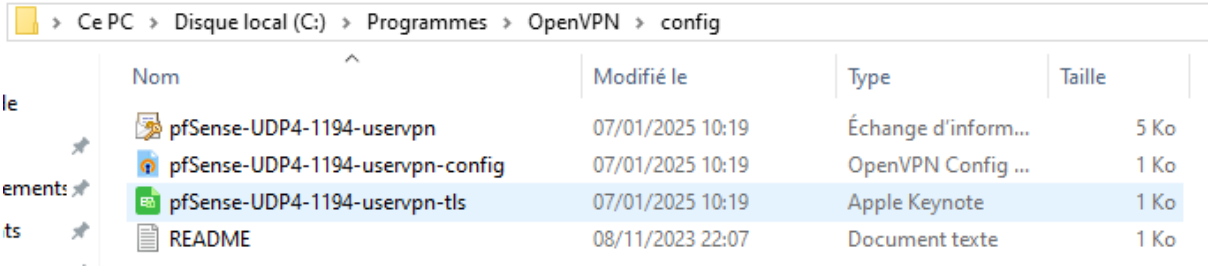


On descend tout en bas, et on récupère la configuration pour un client, et si on veut, même récupérer l'installateur de l'application pour le client :

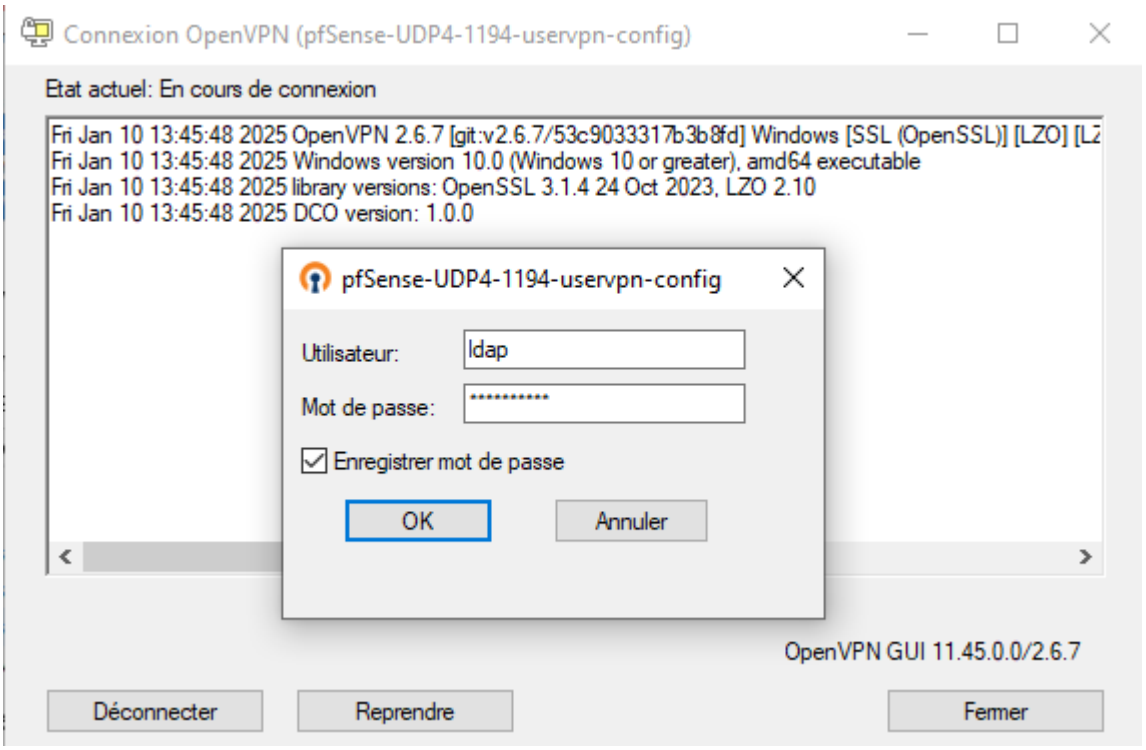


4.4 - Tests du VPN :

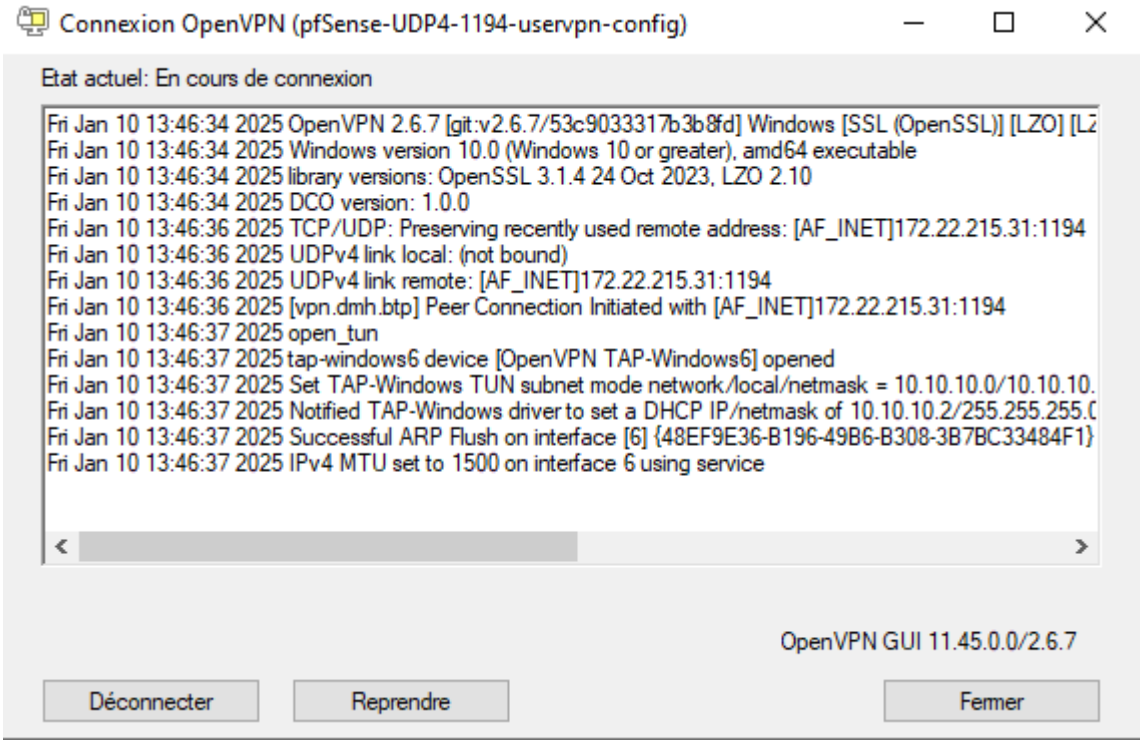
Sur mon hôte, après installation du client OpenVPN, il faut mettre les fichiers téléchargés juste avant, pour ainsi mettre la configuration :

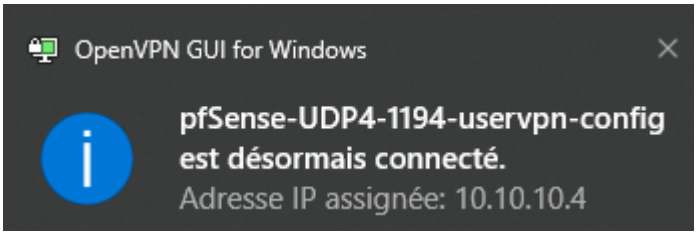


On essaie ensuite la connexion au VPN :

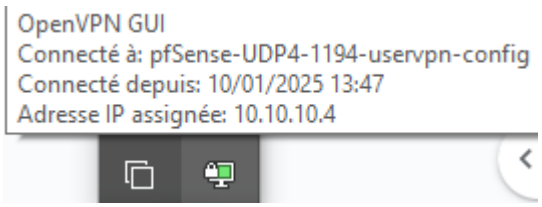


On utilisateur un des utilisateurs adapté pour la connexion :





On est bien implanté dans le sous-réseau créé exprès.



Nous sommes bien connectés.