Procédure de configuration des équipements

Auteur: *Bagassien Stephen*

Référence : *Assurmer*

Date : *04/2024*

SOMMAIRE

Table des matières

Procédure de configuration des équipements

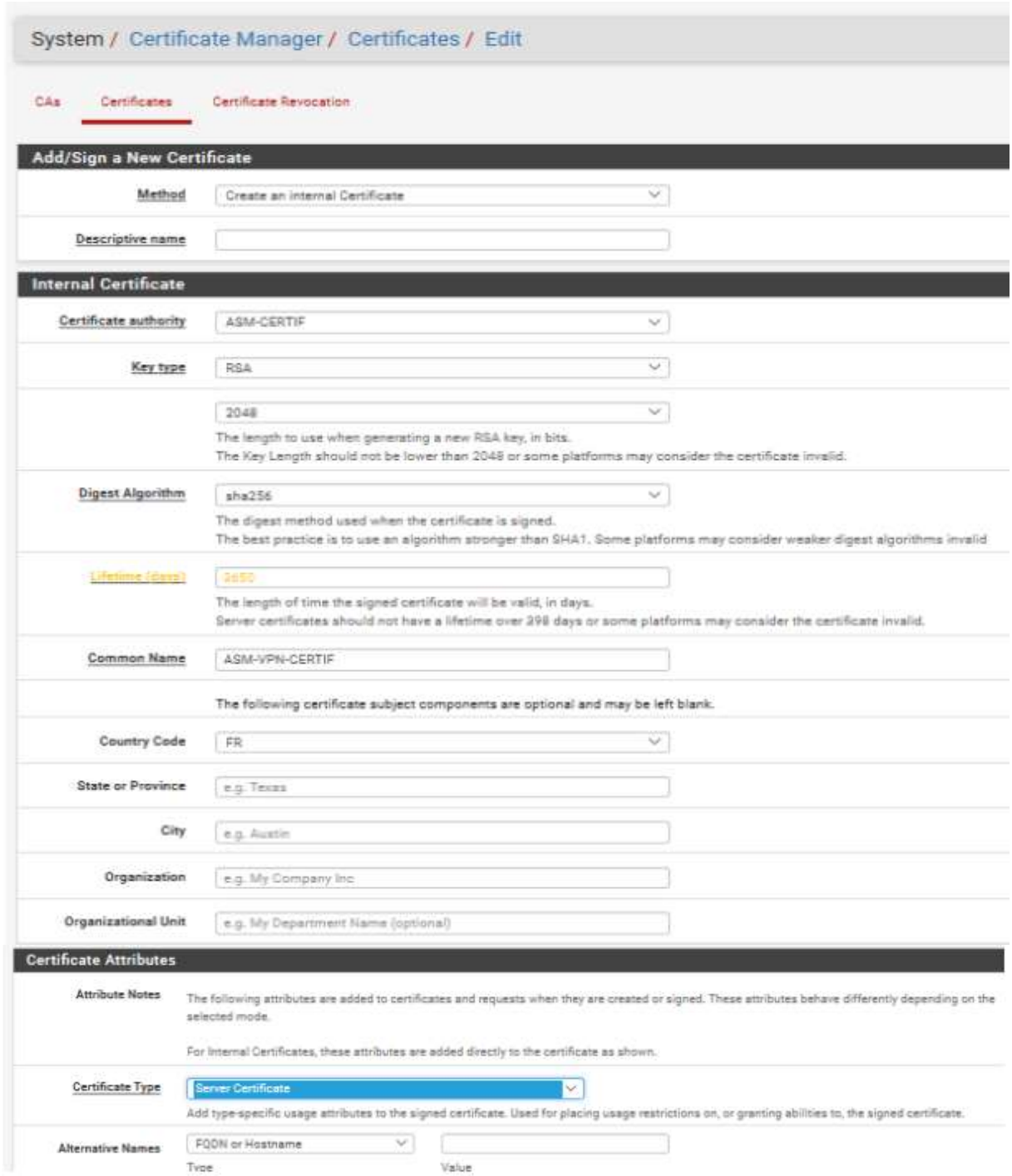
OpenVPN

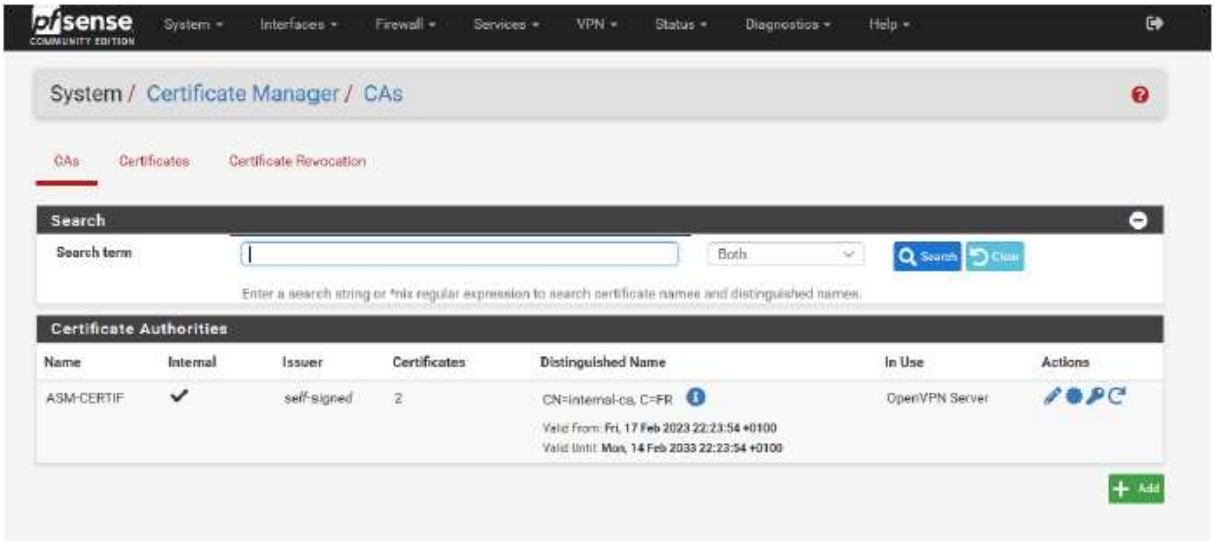
Prérequis :

- Un pare-Feu Netgate sg-3100
- Un accès Internet

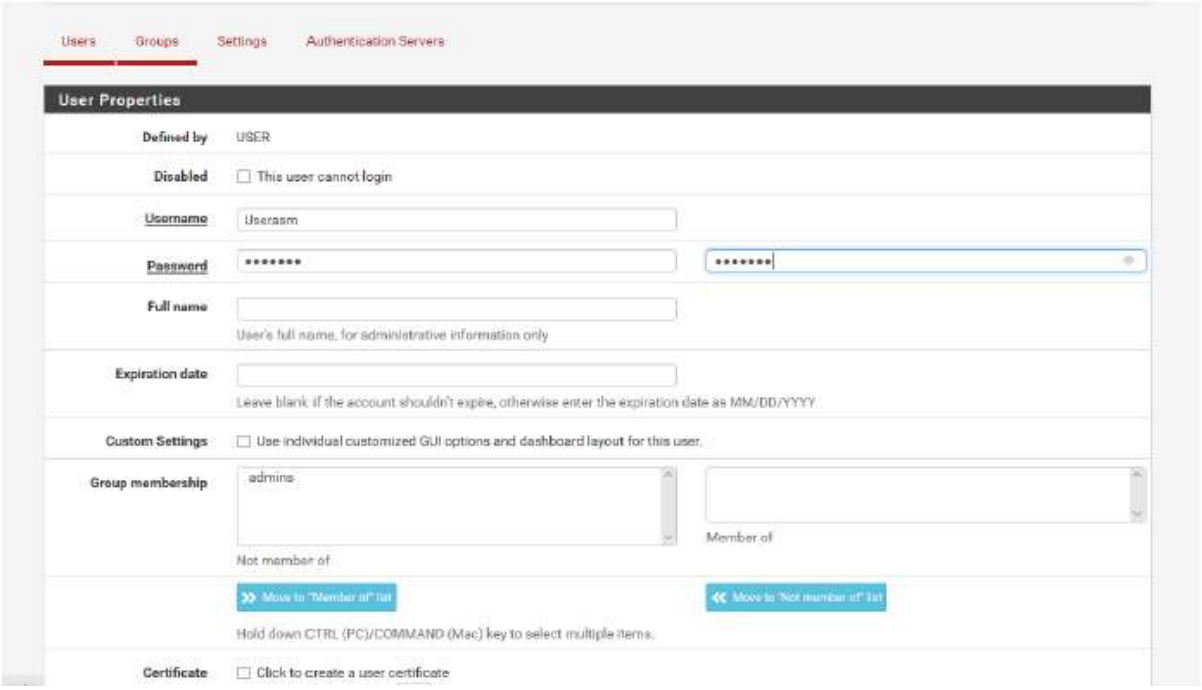
Étapes pour l'installation :

a. Génération des certificats d'autorité et de serveur.

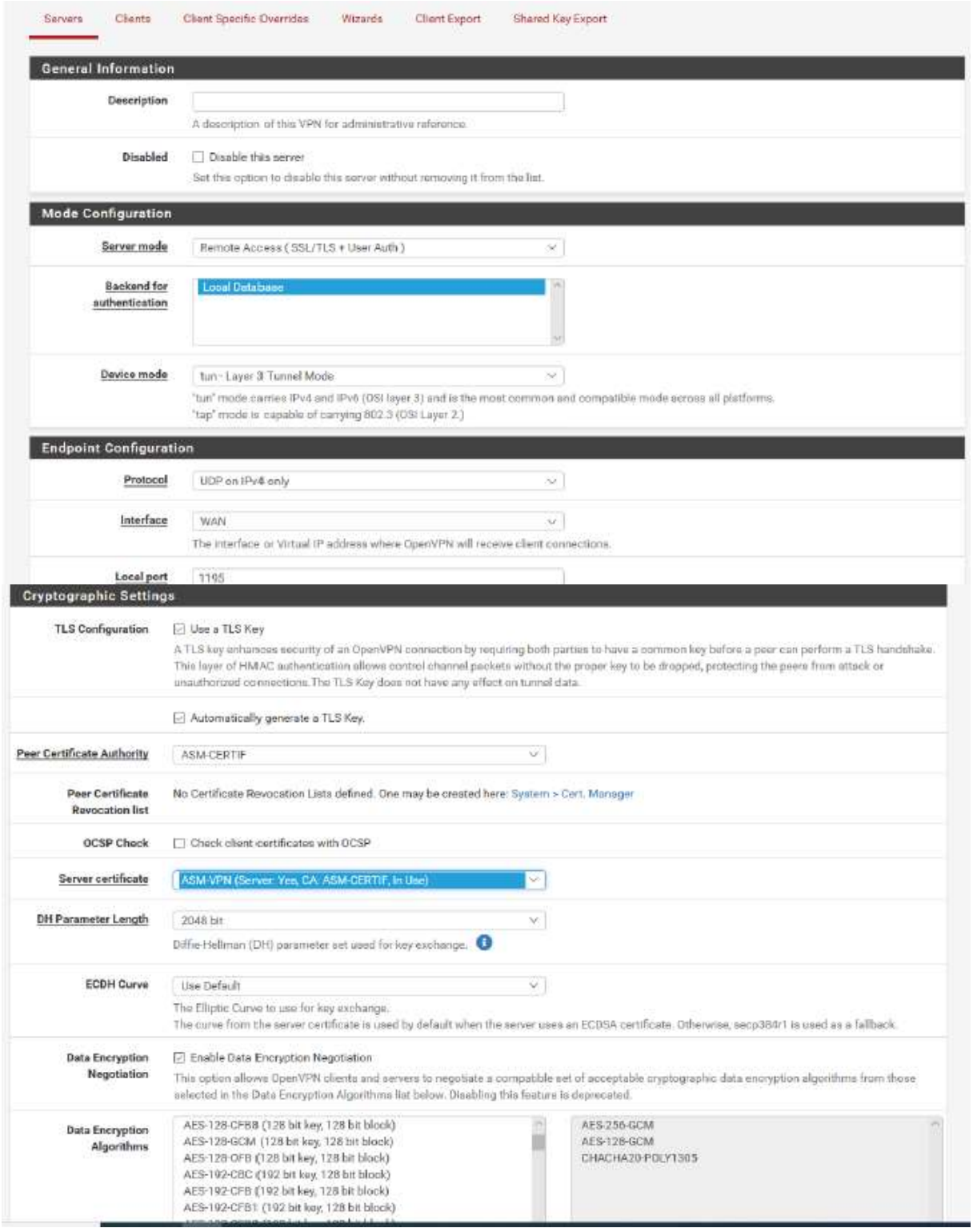


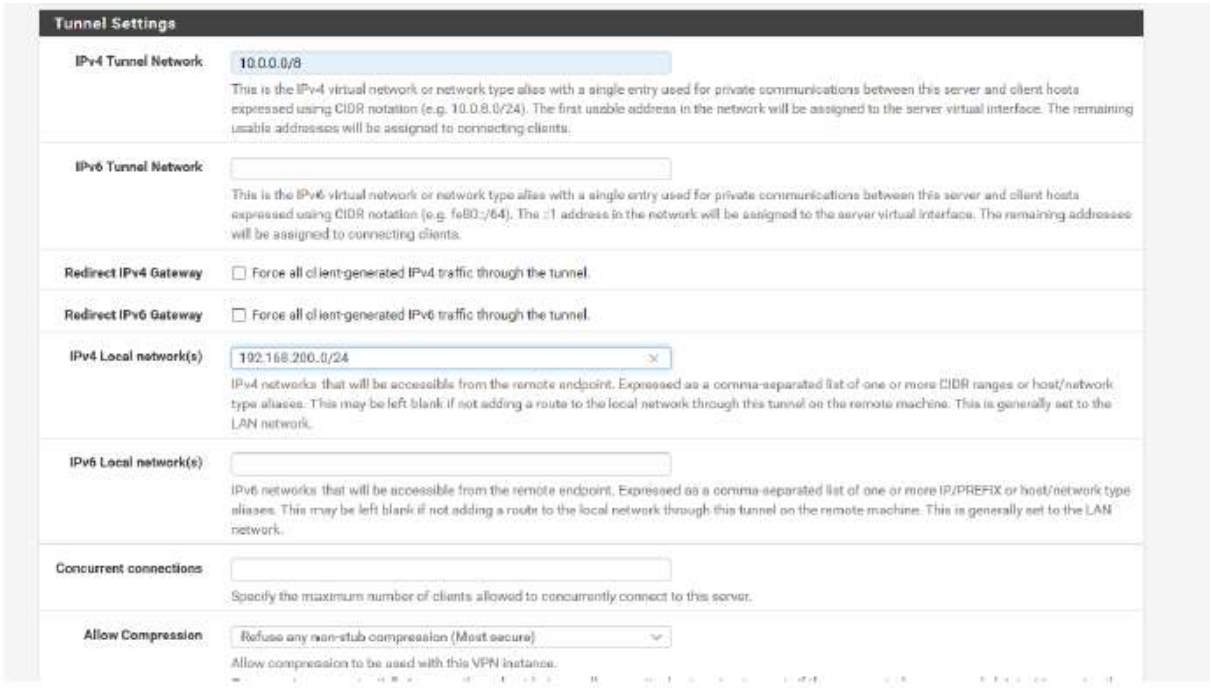


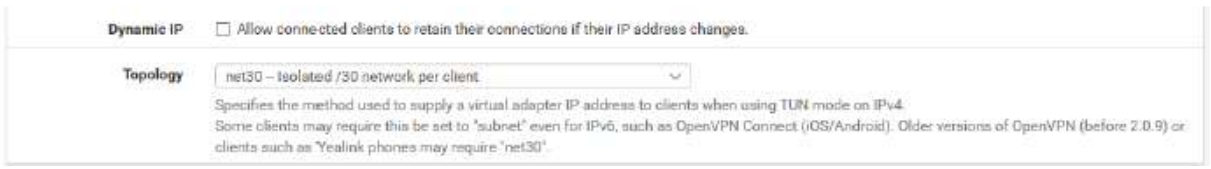
b. Création d'un utilisateur avec son certificat associé.

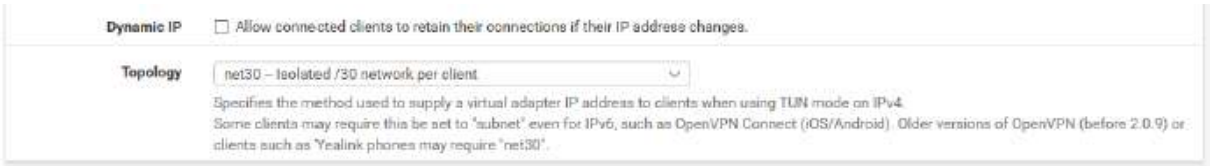


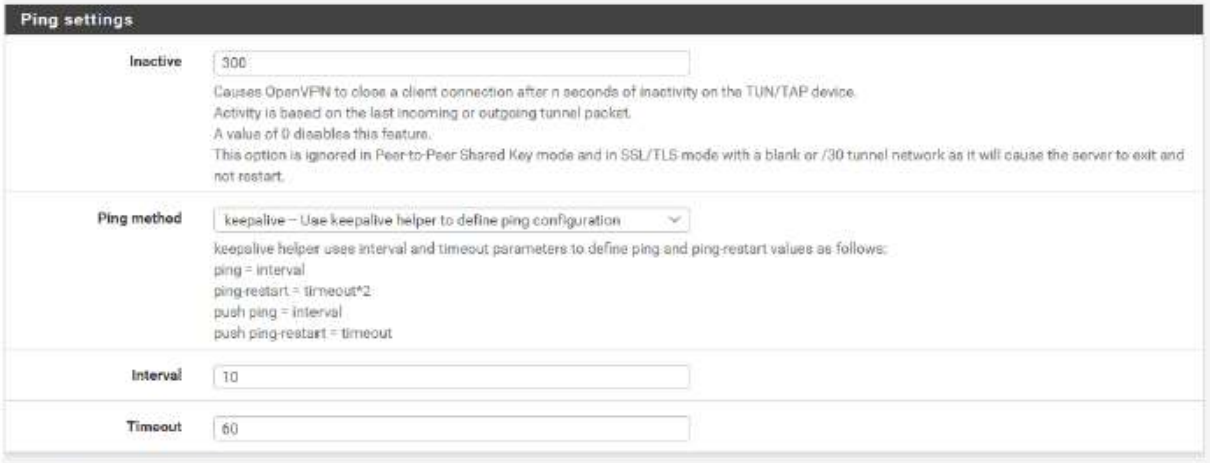
c. Mise en place d'un serveur OpenVPN




Tunnel Settings
IPv4 Tunnel Network
10.0.0.0/8
This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.
IPv6 Tunnel Network
This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.
Redirect IPv4 Gateway
Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway
Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)
192.168.200.0/24
IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. 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.
IPv6 Local network(s)
IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. 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
Specify the maximum number of clients allowed to concurrently connect to this server.
Allow Compression
Refuse any non-stub compression (Most secure)
Allow compression to be used with this VPN instance.

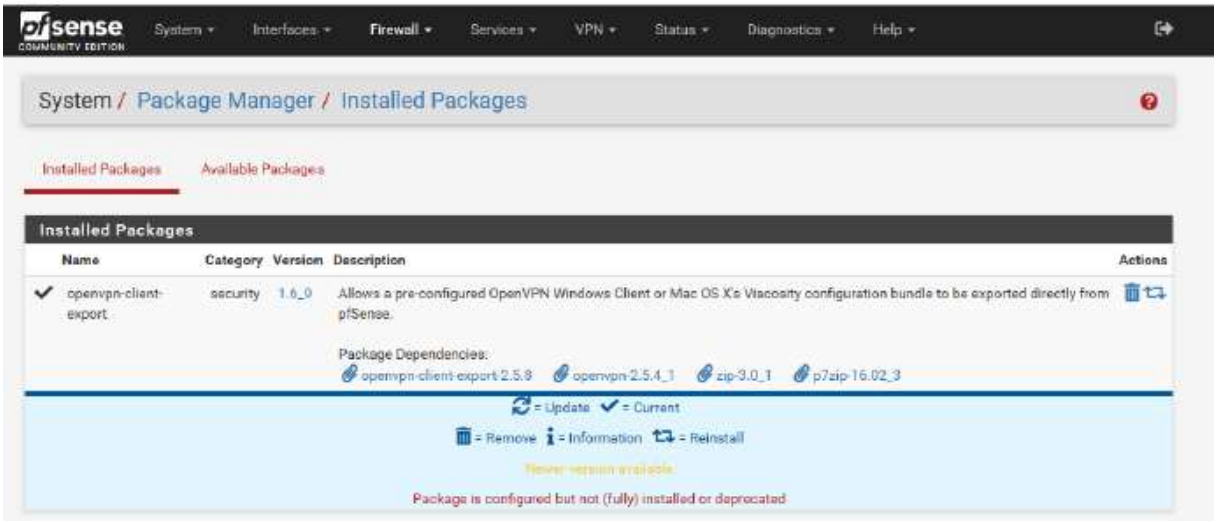

Dynamic IP
Allow connected clients to retain their connections if their IP address changes.
Topology
net30 – Isolated /30 network per client
Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4.
Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".


Dynamic IP
Allow connected clients to retain their connections if their IP address changes.
Topology
net30 – Isolated /30 network per client
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".

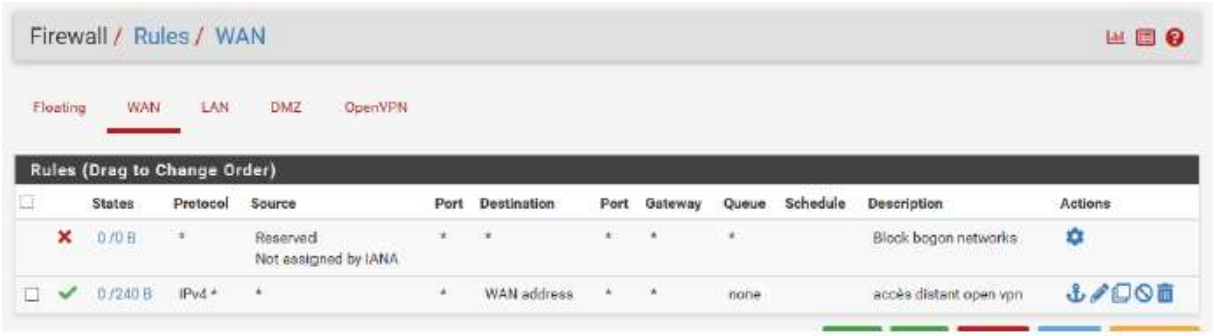

Ping settings
Inactive
300
Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device.
Activity is based on the last incoming or outgoing tunnel packet.
A value of 0 disables this feature.
This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.
Ping method
keepalive – Use keepalive helper to define ping configuration
keepalive helper uses interval and timeout parameters to define ping and ping-restart values as follows:
ping = interval
ping-restart = timeout*2
push ping = interval
push ping-restart = timeout
Interval
10
Timeout
60


Advanced Client Settings
DNS Default Domain
Provide a default domain name to clients
DNS Default Domain
assurmer.fr
DNS Server enable
Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1
172.16.0.1

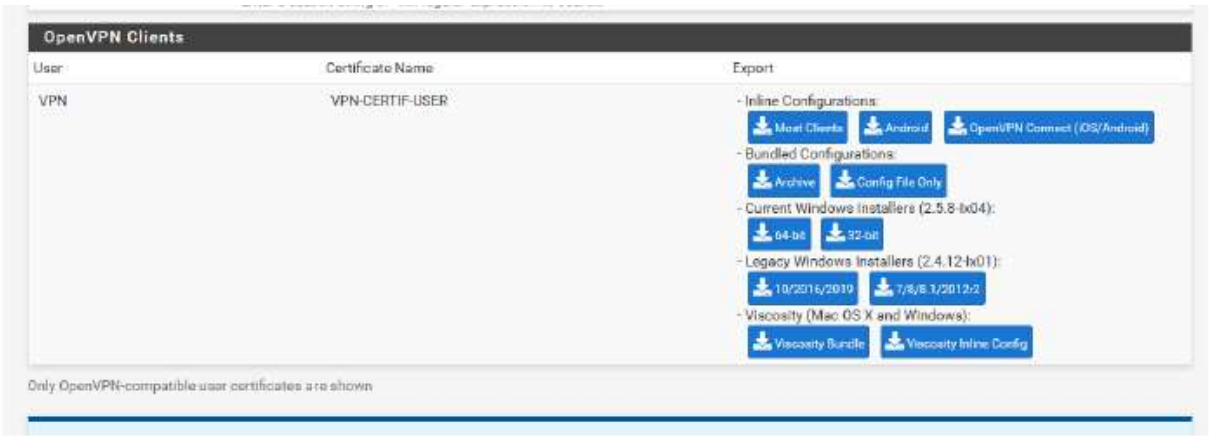
d. Installation du package « openvpn-client-export »

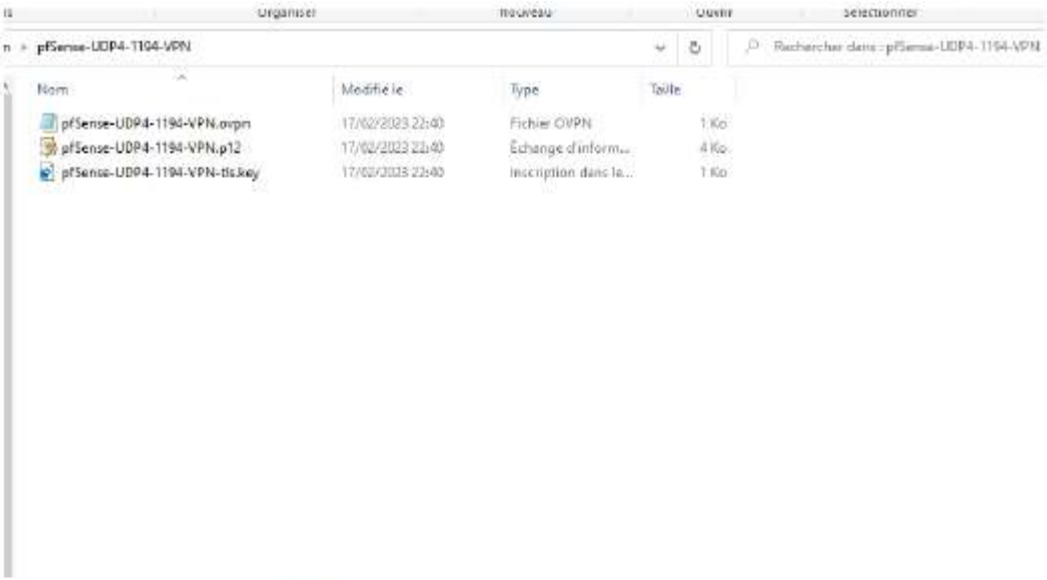


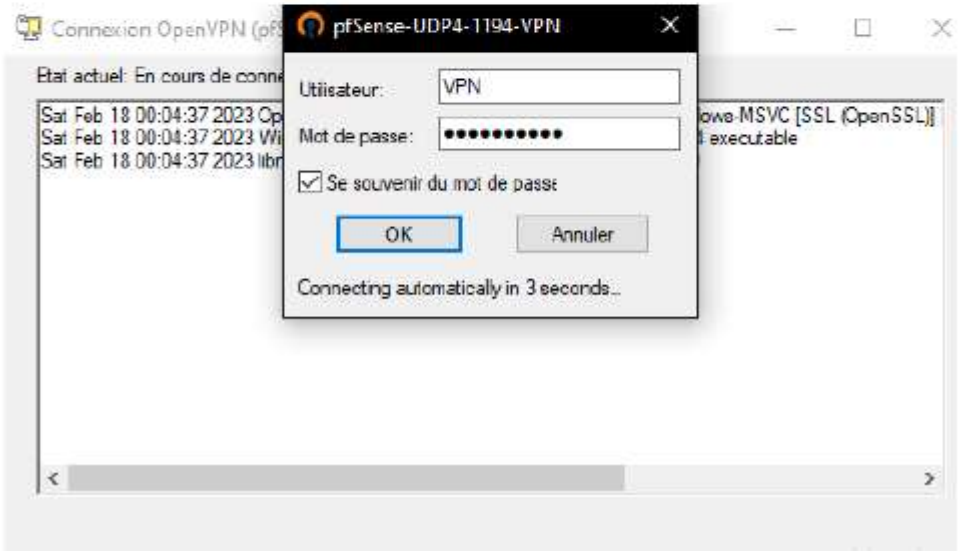
e. Configuration des règles de pare-feu pour permettre l'accès à la DMZ depuis le VPN



Exportation et déploiement du client sur l'utilisateur distant




Organiser
Nouveau
Ouvrir
Sélectionner
pfSense-UDP4-1194-VPN
Rechercher dans : pfSense-UDP4-1194-VPN
Nom
Modifié le
Type
Taille
pfSense-UDP4-1194-VPN.ovpn
17/02/2023 22:40
Fichier OVPN
1 Ko
pfSense-UDP4-1194-VPN.p12
17/02/2023 22:40
Échange d'inform...
4 Ko
pfSense-UDP4-1194-VPN-tls.key
17/02/2023 22:40
Inscription dans le...
1 Ko


Connexion OpenVPN (pf
Etat actuel: En cours de conne
Sat Feb 18 00:04:37 2023 Op
Sat Feb 18 00:04:37 2023 Wi
Sat Feb 18 00:04:37 2023 libr
owe-MSVC [SSL (OpenSSL)]
executable
pfSense-UDP4-1194-VPN
Utilisateur:
VPN
Mot de passe:
Se souvenir du mot de passe
OK
Annuler
Connecting automatically in 3 seconds...