2026

MISE EN PLACE D'UNE CONNEXION DISTANTE

TECHNICIEN SYSTEME ET RESEAU

MARC VOUA

EXPERIS FRANCE

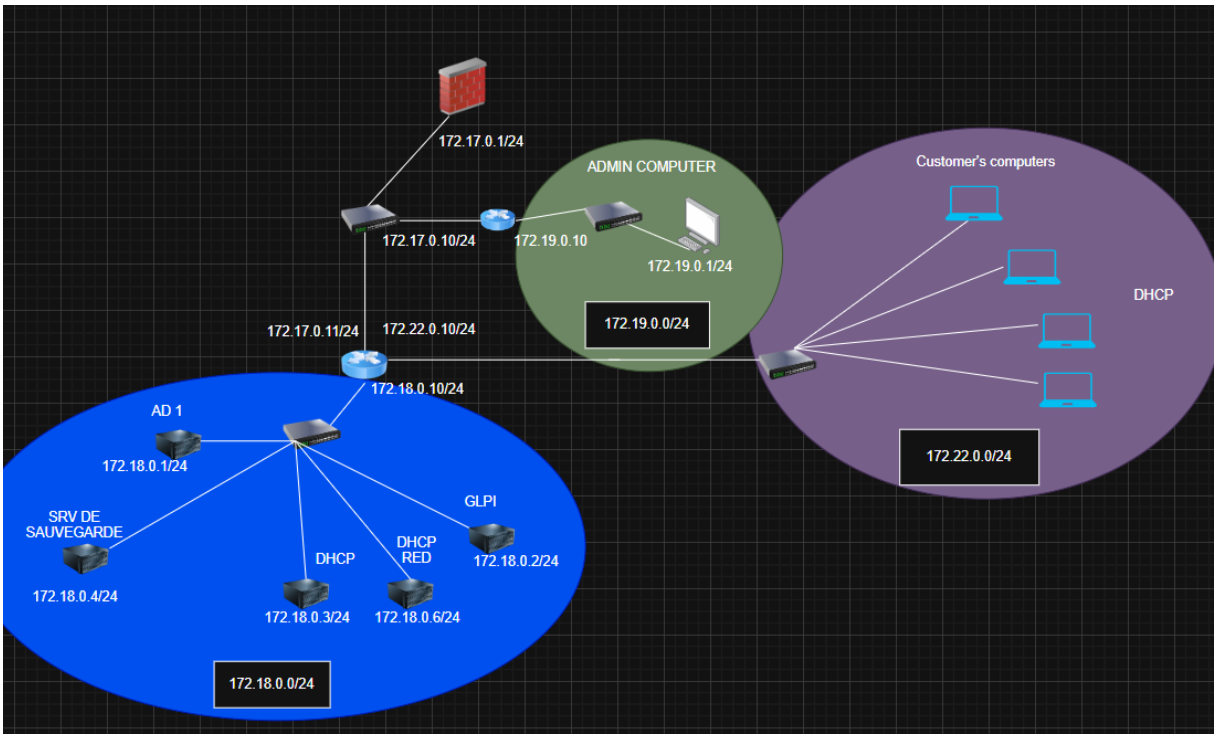
Table des matières

I- Cahier des charges – Expression des besoins

1) Descriptif de l'existant.

Le client avait d'ores et déjà réalisé en amont une partie du travail afin d'obtenir une vision claire des tâches à effectuer. Possédant déjà une infrastructure réseau fonctionnelle, il nous présente… :

a) Schéma



Un schéma avec les différentes adresses IP des machines ainsi que leurs noms

b) Tableau d'adressage

Network	Mask	First address	Last address	Broadcast	pfsesne	AD 1	GLPI	DHCP	BACKUP	DHCP RED	Admin post
172.17.0.0/24 (vlan1)	255.255.255.0	172.17.0.1/24	172.17.0.254/24	172.17.0.255/24	172.17.0.1/24						
172.18.0.0/24 (vlan2)	255.255.255.0	172.18.0.1/24	172.18.0.254/24	172.18.0.255/24		172.18.0.1/24	172.18.0.2/24	172.18.0.3/24	172.18.0.4/24	172.18.0.6/24	
172.19.0.0/24 (vlan3)	255.255.255.0	172.19.0.1/24	172.19.0.254/24	172.19.0.255/24							172.19.0.1/24
172.22.0.0/24 (vlan 5)(dhcp)	255.255.255.0	172.22.0.1/24	172.22.0.254/24	172.22.0.255/24							

Un tableau d'adressage contenant les différents réseaux, les masques, premières et dernières adresses utilisables ainsi que les adresses de broadcast

2) Besoin

Le client nous sollicite à la suite de la déclaration d'un prestataire externe intervenant en qualité de technicien support exclusivement en télétravail. Il souhaite disposer d'une solution permettant à l'ensemble des prestataires d'accéder aux différents outils à distance

3) Contraintes

Un délai particulièrement court, justifié par l'indisponibilité de certains outils de travail, notamment le pare-feu.

II- Analyse

1) Descriptifs des solutions et choix des solutions

Après un échange approfondi avec le client et une définition rigoureuse de ses exigences, nous avons analysé les différentes solutions susceptibles de répondre à ses contraintes techniques et organisationnelles. Au regard des ressources déjà disponibles et des limites identifiées, le choix s'est orienté vers la mise en place d'un VPN à accès restreint, ce dispositif offrant un niveau de sécurité élevé, une isolation efficace des services sensibles et une maîtrise renforcée des accès distants.

En retenant cette option d'accès VPN (OpenVPN), l'entreprise adopte une approche garantissant à la fois la simplicité opérationnelle et un haut niveau de sécurité : le VPN restreint permet aux prestataires d'accéder uniquement aux ressources strictement nécessaires, sans exposer l'ensemble du réseau interne, grâce à des règles d'accès finement contrôlées. Ce choix renforce la segmentation du système d'information, réduit significativement les risques d'intrusion, facilite l'audit des connexions externes et constitue une solution robuste, évolutive et conforme aux bonnes pratiques de sécurité pour l'accès distant des prestataires.

2) Prévisions des tests de validation

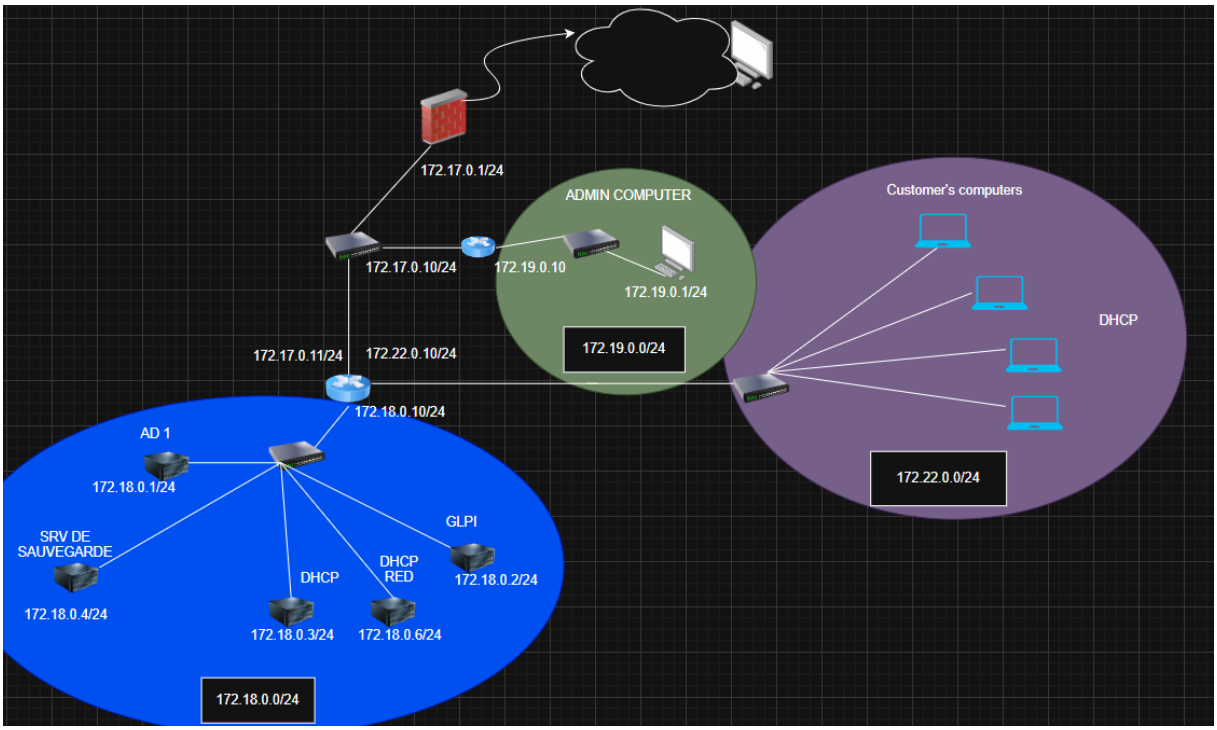
Les tests seront effectués une fois la mise en place du VPN réalisée et consisteront à vérifier la conformité des accès depuis un environnement extérieur au réseau de confiance. Une première série d'essais visera à établir une connexion depuis une machine située sur un réseau externe en utilisant le VPN déployé, afin de s'assurer que l'accès aux ressources autorisées est correctement attribué et strictement limité au périmètre défini.

Une seconde série de tests sera menée, toujours depuis une machine externe, en tentant cette fois d'atteindre des ressources non autorisées, dans le but de confirmer que ces accès sont effectivement refusés et que l'isolation du système d'information est pleinement opérationnelle.

III- Mise en place

1) Schéma, Tableau d'adressage et Table de routage

a) Nouveau schéma



Nous avons ajouté un poste externe afin d'illustrer la connexion distante requise, lequel servira de support pour vérifier le bon fonctionnement des différentes opérations mises en œuvre.

b) Tableau d'adressage

Network	Mask	First address	Last address	Broadcast	pfsesne	AD 1	GLPI	DHCP	BACKUP	DHCP RED	Admin post
172.17.0.0/24 (vlan1)	255.255.255.0	172.17.0.1/24	172.17.0.254/24	172.17.0.255/24	172.17.0.1/24						
172.18.0.0/24 (vlan2)	255.255.255.0	172.18.0.1/24	172.18.0.254/24	172.18.0.255/24		172.18.0.1/24	172.18.0.2/24	172.18.0.3/24	172.18.0.4/24	172.18.0.6/24	
172.19.0.0/24 (vlan3)	255.255.255.0	172.19.0.1/24	172.19.0.254/24	172.19.0.255/24							172.19.0.1/24
172.22.0.0/24 (vlan 5)(dhcp)	255.255.255.0	172.22.0.1/24	172.22.0.254/24	172.22.0.255/24							

c) Table de routage

Parfeu :

@Réseau Destination	Masque	@Passerelle	@Interface
172.18.0.0/24	255.255.255.0	172.17.0.10/24	172.17.0.1/24
172.19.0.0/24	255.255.255.0	172.17.0.11/24	172.17.0.1/24
172.22.0.0/24	255.255.255.0	172.17.0.11/24	172.17.0.1/24

Routeur 1 :

@Réseau Destination	Masque	@Passerelle	@Interface
0.0.0.0	255.255.255.255	172.17.0.1/24	172.17.0.10/24
172.18.0.0/24	255.255.255.0	172.17.0.11/24	172.17.0.10/24
172.19.0.0/24	255.255.255.0	172.19.0.10/24	172.19.0.10/24
172.22.0.0/24	255.255.255.0	172.17.0.11/24	172.17.0.10/24

Routeur 2 :

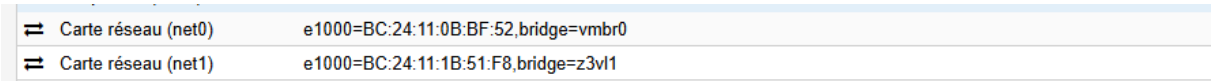
@Réseau Destination	Masque	@Passerelle	@Interface
0.0.0.0	255.255.255.255	172.17.0.10/24	172.17.0.11/24
172.17.0.0/24	255.255.255.0	172.17.0.10/24	172.17.0.11/24
172.19.0.0/24	255.255.255.0	172.17.0.10/24	172.17.0.11/24
172.22.0.0/24	255.255.255.0	172.22.0.10/24	172.22.0.10/24

2) Méthodologie

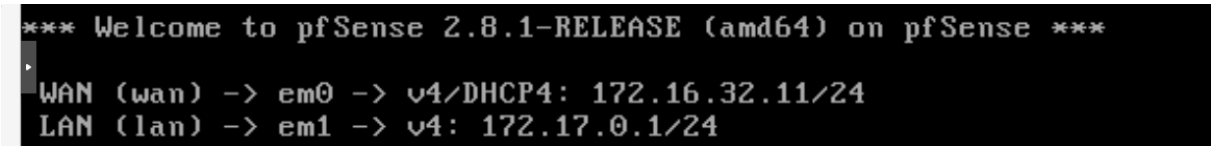
Nous avons décomposé notre travail en plusieurs étapes à savoir :

- **Configuration IP**

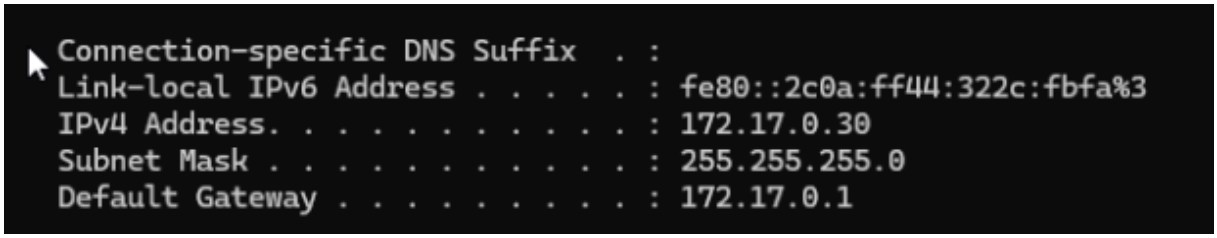
Cette étape consiste à configurer le pare-feu en lui ajoutant une interface réseau, laquelle sera utile pour le LAN.



Maintenant que la carte réseau a été ajoutée, nous passons à sa configuration



Maintenant que les différentes cartes sont configurées nous allons accéder à l'interface graphique du parfeu pour configurer les règles de filtrages Pour ce faire, nous configurons un poste situé sur le même réseau que le pare-feu, afin de pouvoir accéder à l'interface graphique de pfSense.

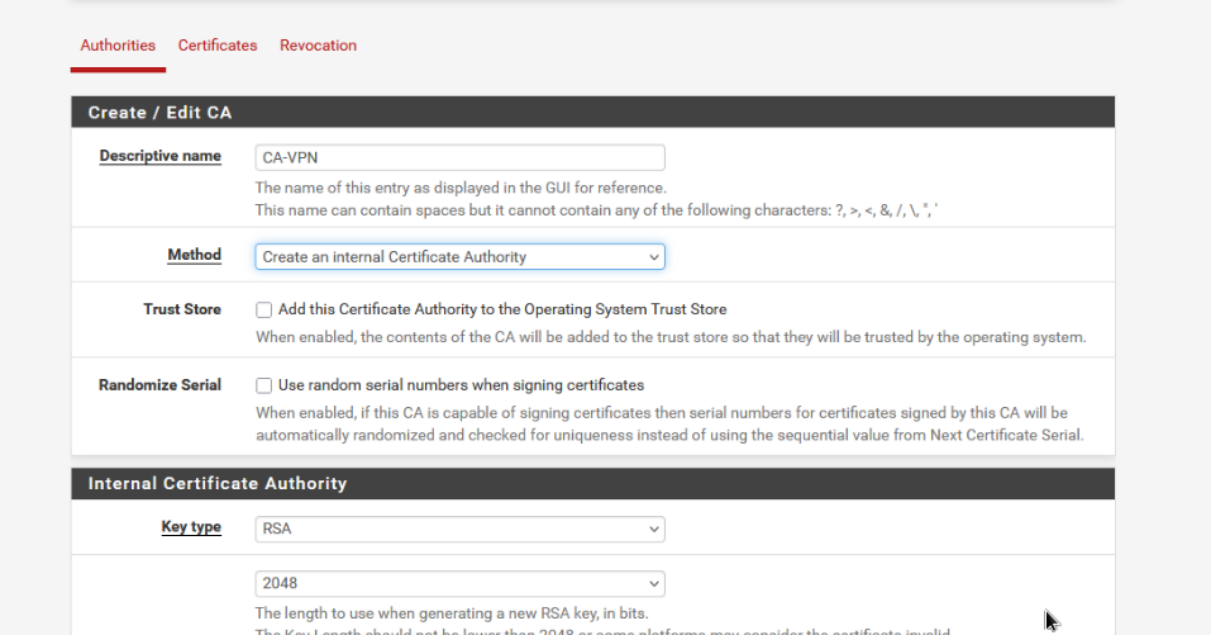


Configuration terminée on s'assure du ping…

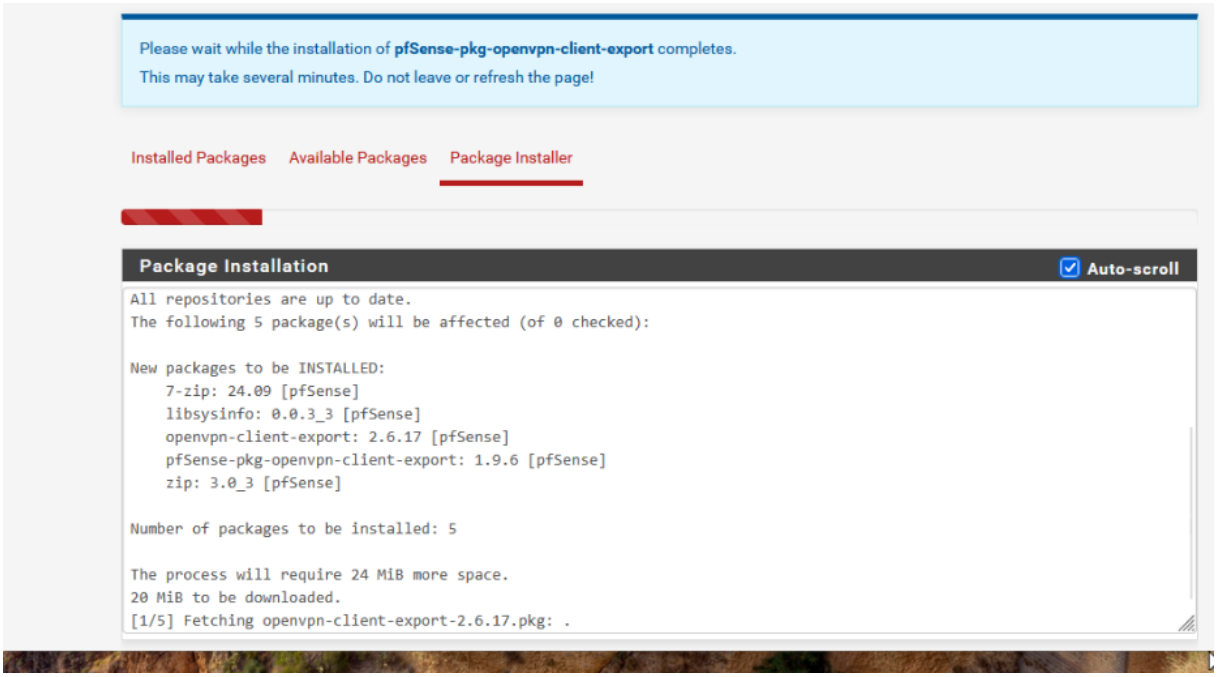
```
C:\Users\marc>ping 172.17.0.1

Pinging 172.17.0.1 with 32 bytes of data:
Reply from 172.17.0.1: bytes=32 time<1ms TTL=64
Reply from 172.17.0.1: bytes=32 time<1ms TTL=64
Reply from 172.17.0.1: bytes=32 time<1ms TTL=64
Reply from 172.17.0.1: bytes=32 time=1ms TTL=64

Ping statistics for 172.17.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Nous avons maintenant accès à l'interface graphique du parfeu nous pouvons commencer la configuration.

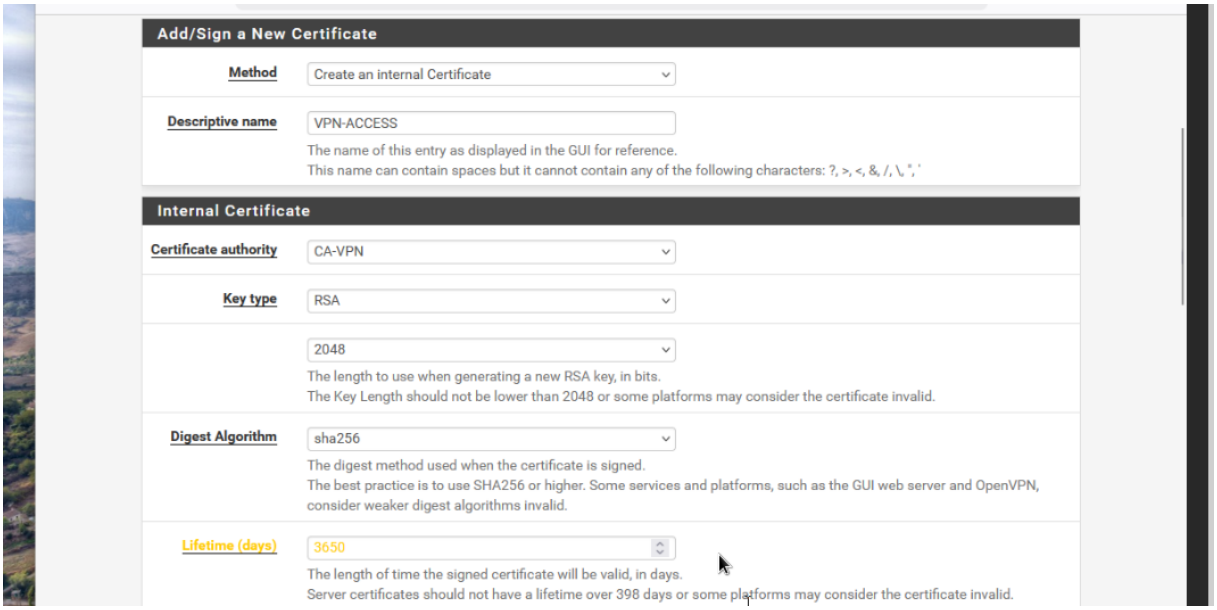
Dans un premier temp nous passons à la création d'une CA



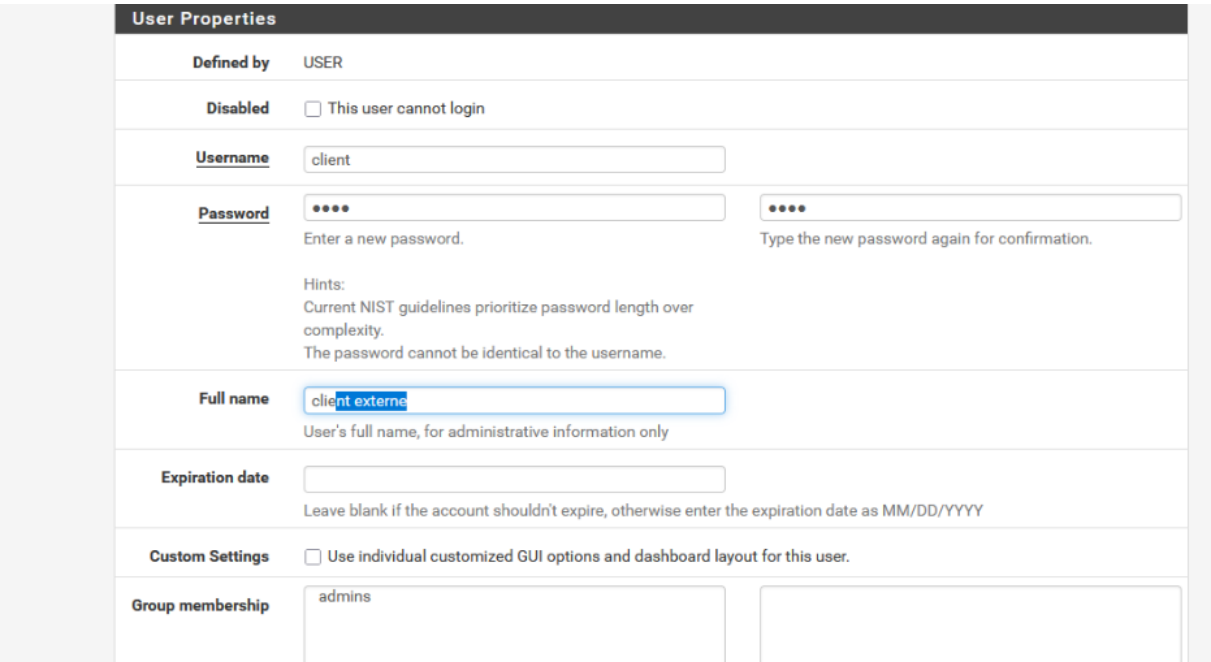
Nous passons ensuite à l'installation du module client export

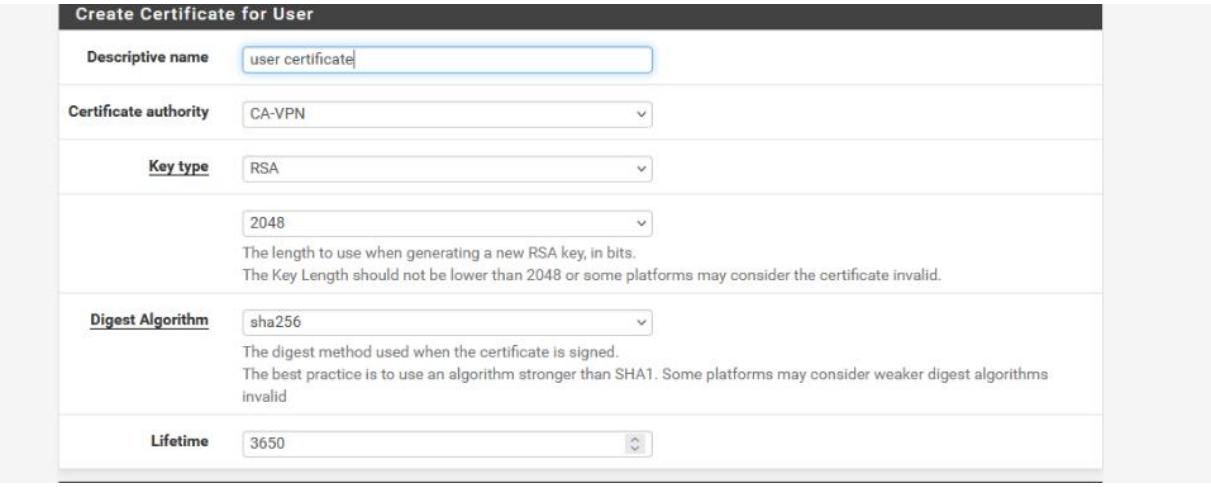


En parallèle, nous créons un certificats serveur

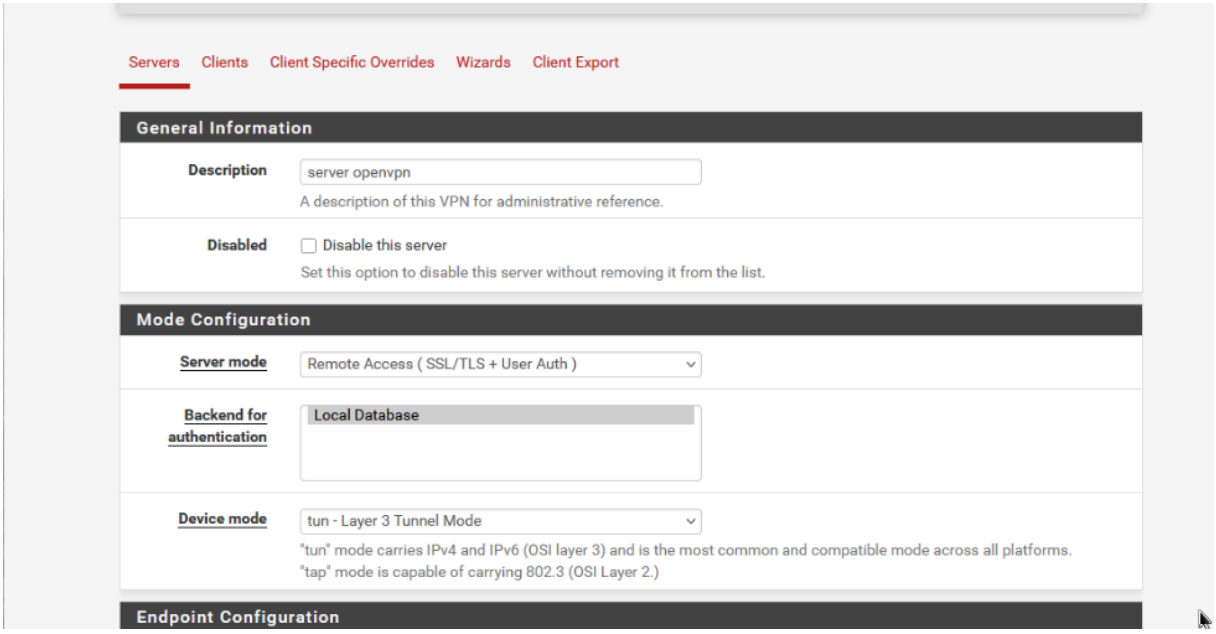


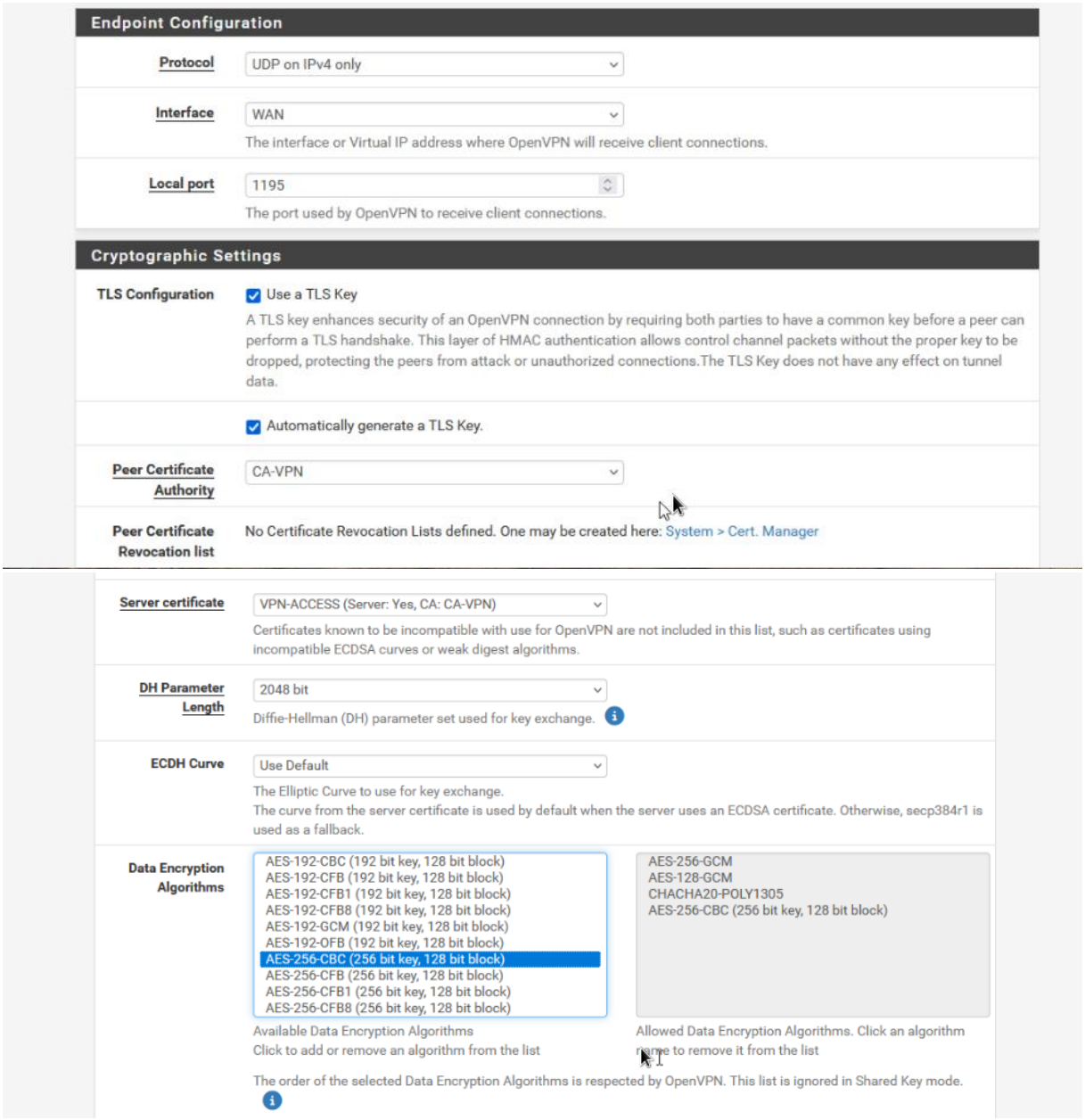
Création d'un utilisateur avec lequel l'on se connectera pour le test

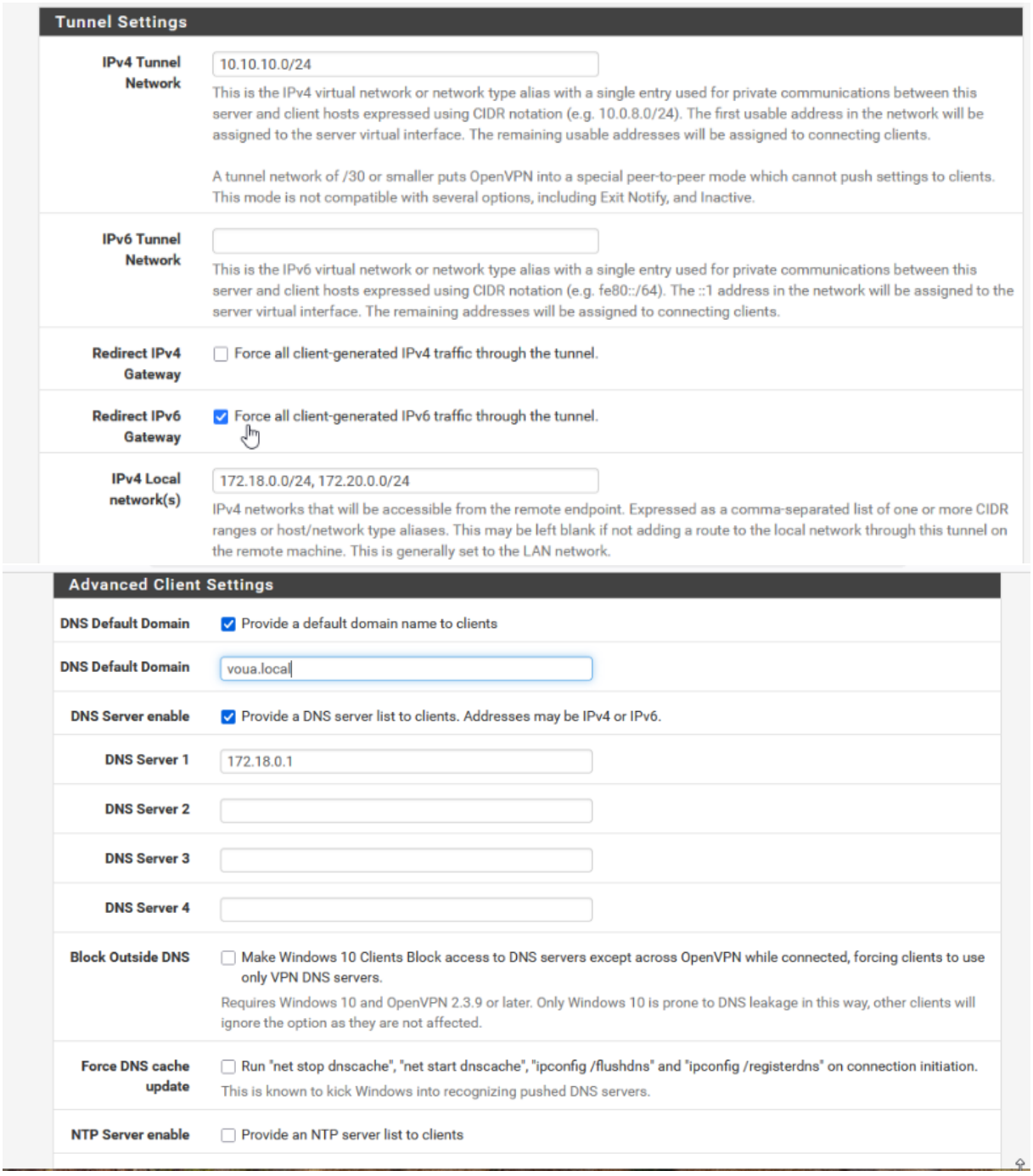




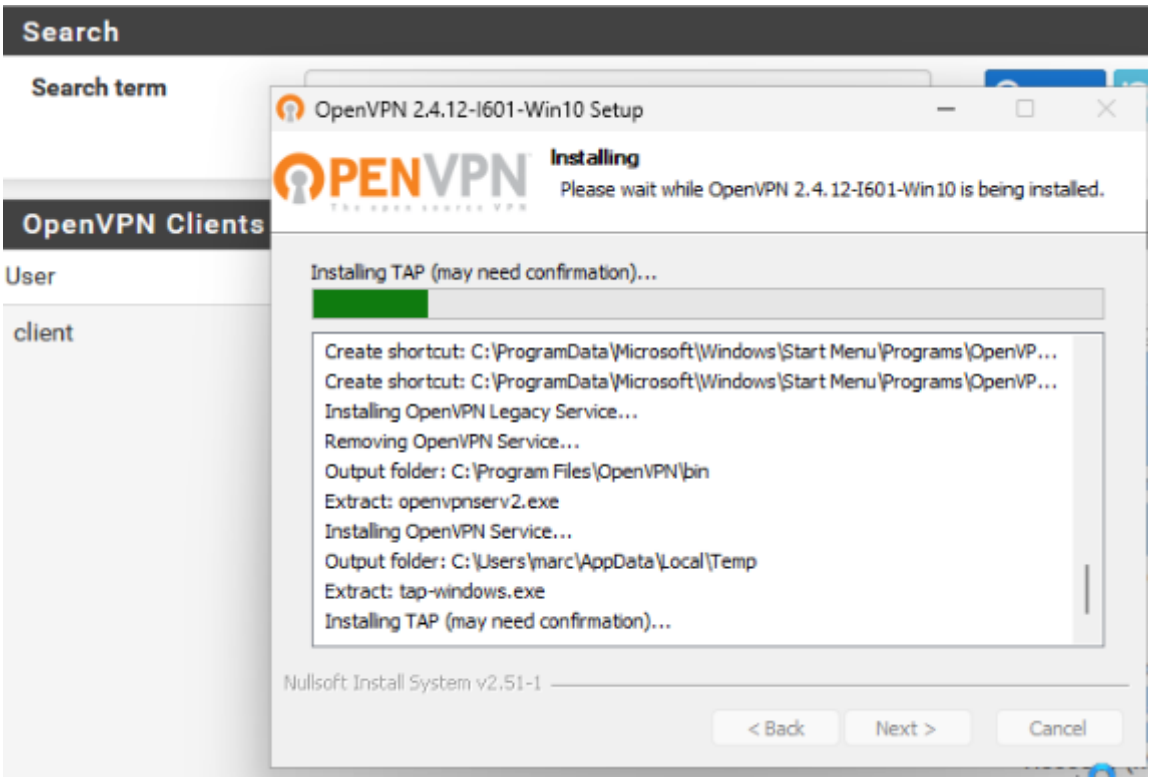
Configuration du serveur OpenVPN


Servers
Clients
Client Specific Overrides
Wizards
Client Export
General Information
Description
server openvpn
A description of this VPN for administrative reference.
Disabled
Disable this server
Set this option to disable this server without removing it from the list.
Mode Configuration
Server mode
Remote Access (SSL/TLS + User Auth)
Backend for authentication
Local Database
Device mode
tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)
Endpoint Configuration

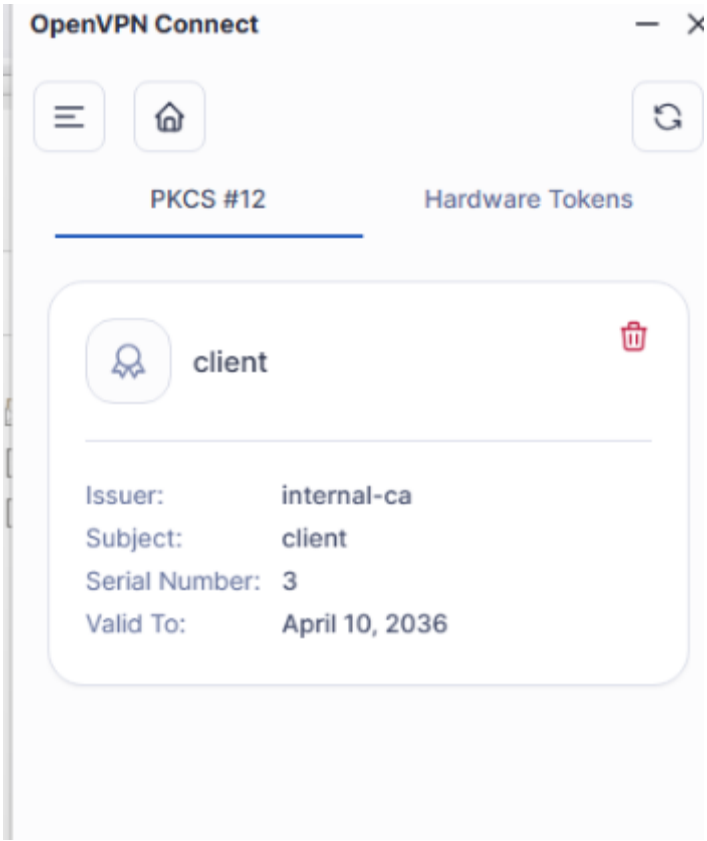

Endpoint Configuration
Protocol
UDP on IPv4 only
Interface
WAN
The interface or Virtual IP address where OpenVPN will receive client connections.
Local port
1195
The port used by OpenVPN to receive client connections.
Cryptographic Settings
TLS Configuration
Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections.The TLS Key does not have any effect on tunnel data.
Automatically generate a TLS Key.
Peer Certificate Authority
CA-VPN
Peer Certificate Revocation list
No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
Server certificate
VPN-ACCESS (Server: Yes, CA: CA-VPN)
Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.
DH Parameter Length
2048 bit
Diffie-Hellman (DH) parameter set used for key exchange.
ECDH Curve
Use Default
The Elliptic Curve to use for key exchange.
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.
Data Encryption Algorithms
AES-192-CBC (192 bit key, 128 bit block)
AES-192-CFB (192 bit key, 128 bit block)
AES-192-CFB1 (192 bit key, 128 bit block)
AES-192-CFB8 (192 bit key, 128 bit block)
AES-192-GCM (192 bit key, 128 bit block)
AES-192-OFB (192 bit key, 128 bit block)
AES-256-CBC (256 bit key, 128 bit block)
AES-256-CFB (256 bit key, 128 bit block)
AES-256-CFB1 (256 bit key, 128 bit block)
AES-256-CFB8 (256 bit key, 128 bit block)
AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305
AES-256-CBC (256 bit key, 128 bit block)
Available Data Encryption Algorithms
Click to add or remove an algorithm from the list
Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list
The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode.


Tunnel Settings
IPv4 Tunnel Network
10.10.10.0/24
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.
A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.
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)
172.18.0.0/24, 172.20.0.0/24
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.
Advanced Client Settings
DNS Default Domain
Provide a default domain name to clients
DNS Default Domain
voua.local
DNS Server enable
Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1
172.18.0.1
DNS Server 2
DNS Server 3
DNS Server 4
Block Outside DNS
Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.
Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.
Force DNS cache update
Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation.
This is known to kick Windows into recognizing pushed DNS servers.
NTP Server enable
Provide an NTP server list to clients

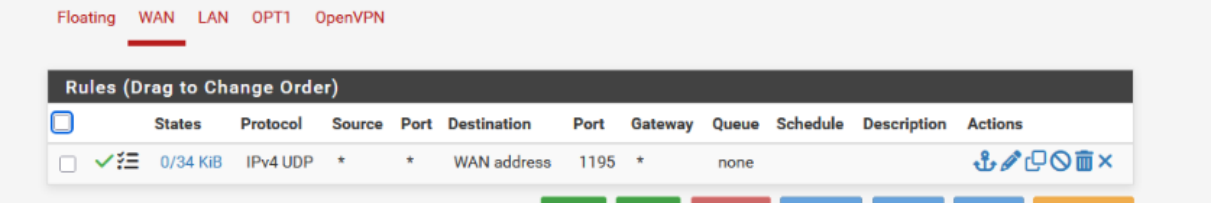
Téléchargement du fichier de configuration openvpn client puis installation de openVPN connect sur machine cliente



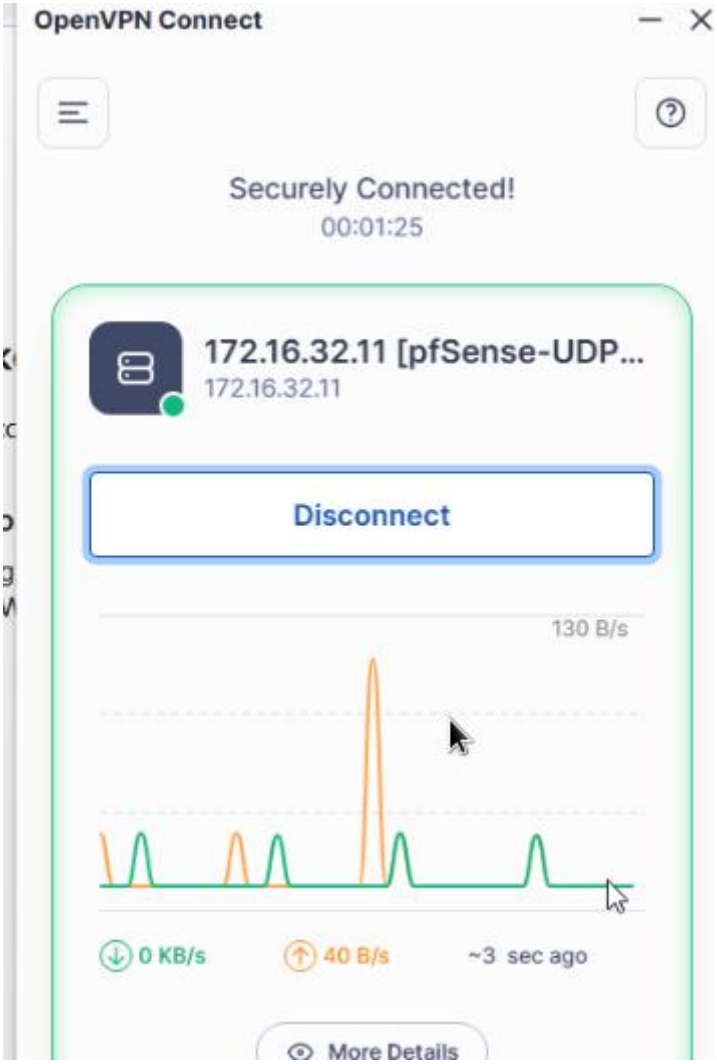
Importation du certificat et de la configuration cliente



Règle de parfeu

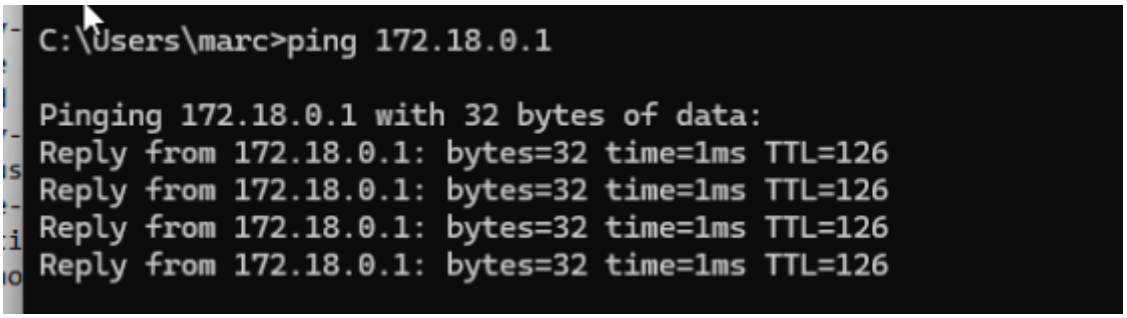


Tentative de connexion vpn sur machine cliente externe



OpenVPN Connecté avec succès

Nous tentons de ping sur un serveur interne



Nous tentons d'accéder à l'interface du serveur de supervision