

MISE EN PLACE D'UNE CONNEXION DISTANTE

TECHNICIEN SYSTEME ET RESEAU
MARC VOUA



Table des matières

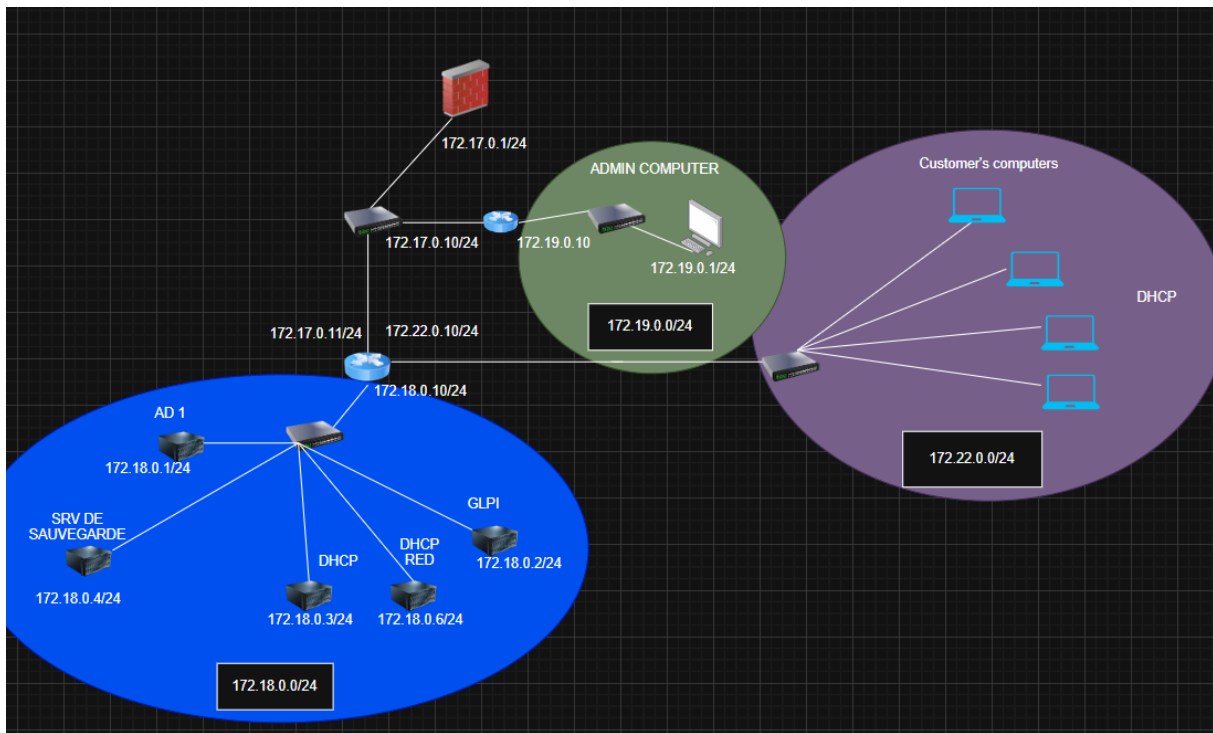
I- Cahier des charges – Expression des besoins.....	2
1) Descriptif de l'existant.	2
a) Schéma	2
b) Tableau d'adressage	2
2) Besoin	2
3) Contraintes	2
II- Analyse	3
1) Descriptifs des solutions et choix des solutions	3
2) Prévisions des tests de validation.....	3
III- Mise en place	4
1) Schéma, Tableau d'adressage et Table de routage.....	4
a) Nouveau schéma	4
b) Tableau d'adressage	4
c) Table de routage.....	4
2) Méthodologie.....	5

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

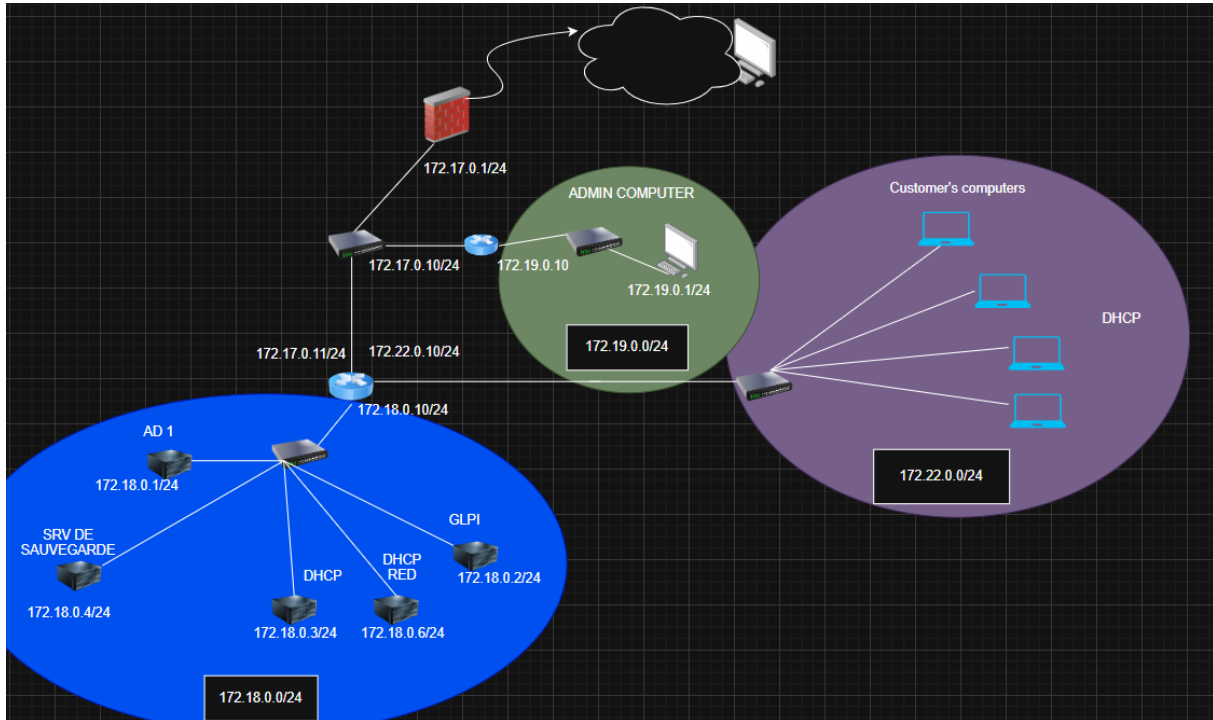
Les tests seront effectués une fois la mise en place du VPN réalisée et consisteront à vérifier la conformité des accès depuis un environnement extérieur au réseau de confiance. Une première série d'essais visera à établir une connexion depuis une machine située sur un réseau externe en utilisant le 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	pfesne	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.

⇄ Carte réseau (net0)	e1000=BC:24:11:0B:BF:52,bridge=vibr0
⇄ Carte réseau (net1)	e1000=BC:24:11:1B:51:F8,bridge=z3vl1

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

```
*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 172.16.32.11/24
LAN (lan) -> em1 -> v4: 172.17.0.1/24
```

Maintenant que les différentes cartes sont configurées nous allons accéder à l'interface graphique du pare-feu 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.

```
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::2c0a:ff44:322c:fbfa%3
IPv4 Address. . . . . : 172.17.0.30
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.17.0.1
```

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 parefeu nous pouvons commencer la configuration.

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

Authorities Certificates Revocation

Create / Edit CA

Descriptive name CA-VPN
The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, %, ' "

Method Create an internal Certificate Authority

Trust Store Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

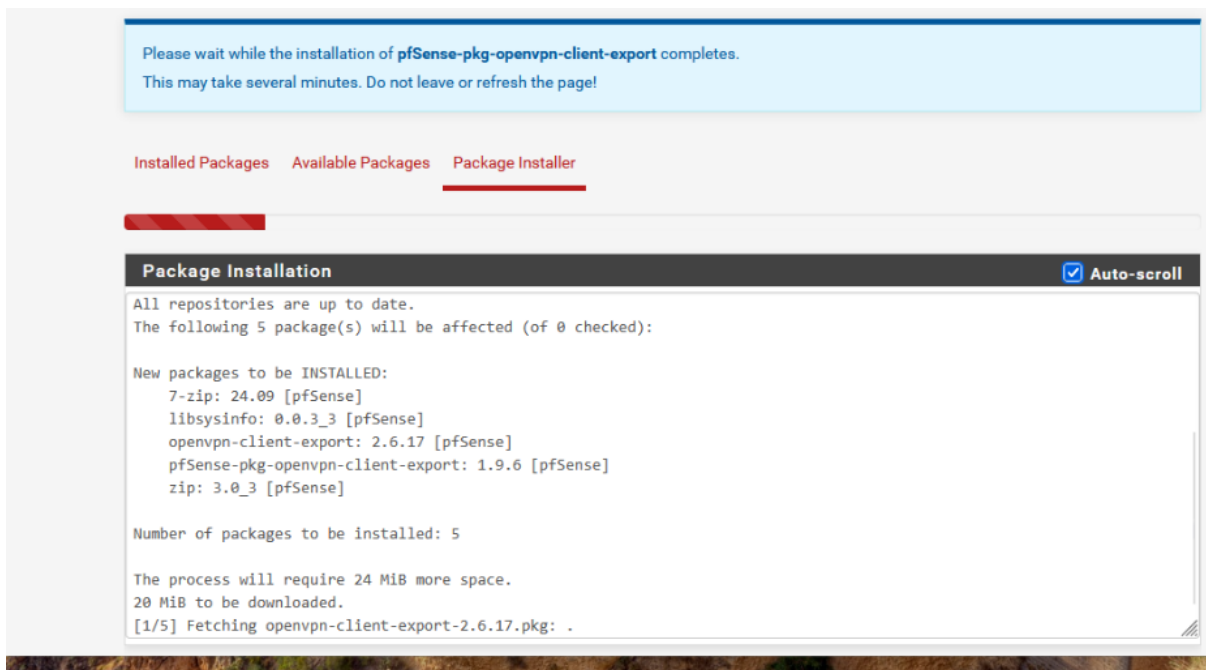
Randomize Serial Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority

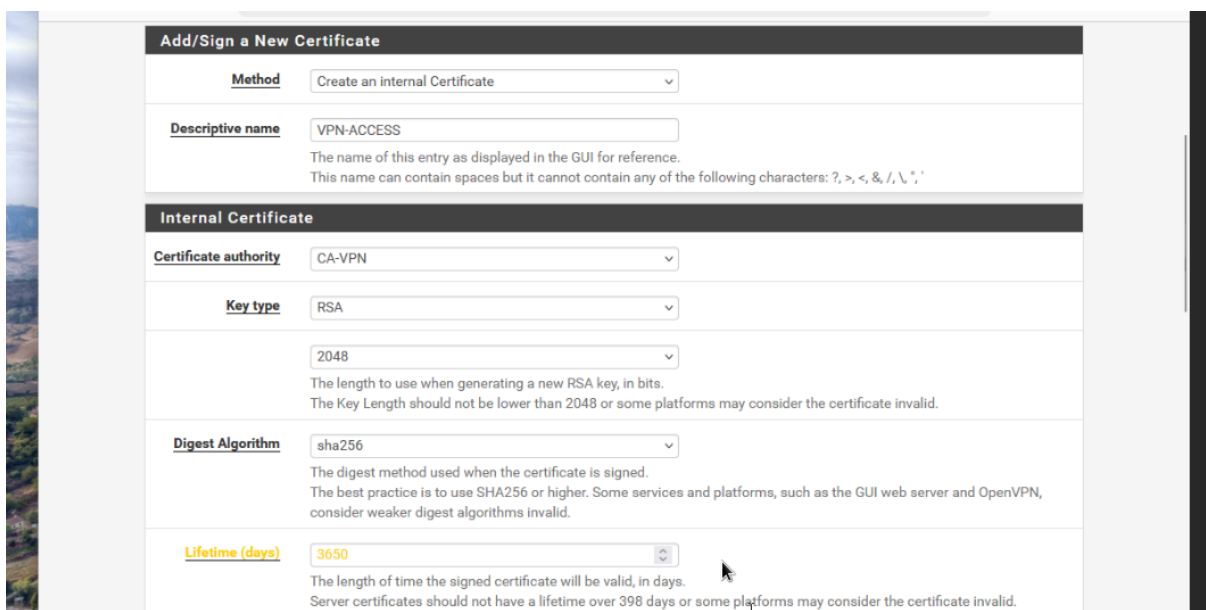
Key type RSA

2048
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 as some platforms may consider the certificate invalid.

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

User Properties	
Defined by	USER
Disabled	<input type="checkbox"/> This user cannot login
Username	<input type="text" value="client"/>
Password	<input type="password" value="••••"/> <input type="password" value="••••"/> <p>Enter a new password. Type the new password again for confirmation.</p> <p>Hints: Current NIST guidelines prioritize password length over complexity. The password cannot be identical to the username.</p>
Full name	<input type="text" value="client externe"/> User's full name, for administrative information only
Expiration date	<input type="text"/> Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.
Group membership	<input type="text" value="admins"/>

Create Certificate for User	
Descriptive name	<input type="text" value="user certificate"/>
Certificate authority	<input type="text" value="CA-VPN"/>
Key type	<input type="text" value="RSA"/>
	<input type="text" value="2048"/> The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm	<input type="text" value="sha256"/> The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.
Lifetime	<input type="text" value="3650"/>

Configuration du serveur OpenVPN

General Information

Description

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

Backend for authentication

Device 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

Interface

The interface or Virtual IP address where OpenVPN will receive client connections.

Local port

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

Peer Certificate Revocation list No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

Server certificate

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

Diffie-Hellman (DH) parameter set used for key exchange. 

ECDH Curve

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)

Available Data Encryption Algorithms
Click to add or remove an algorithm from the list

The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode.

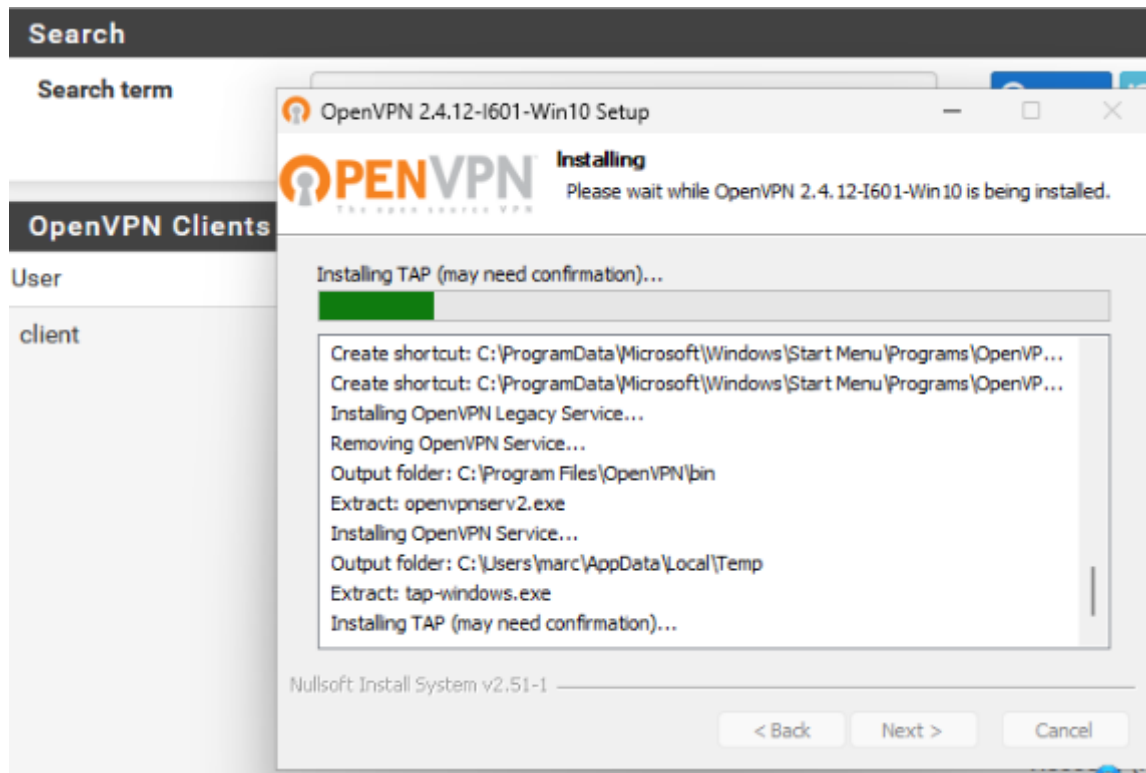
AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305
AES-256-CBC (256 bit key, 128 bit block)

Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list

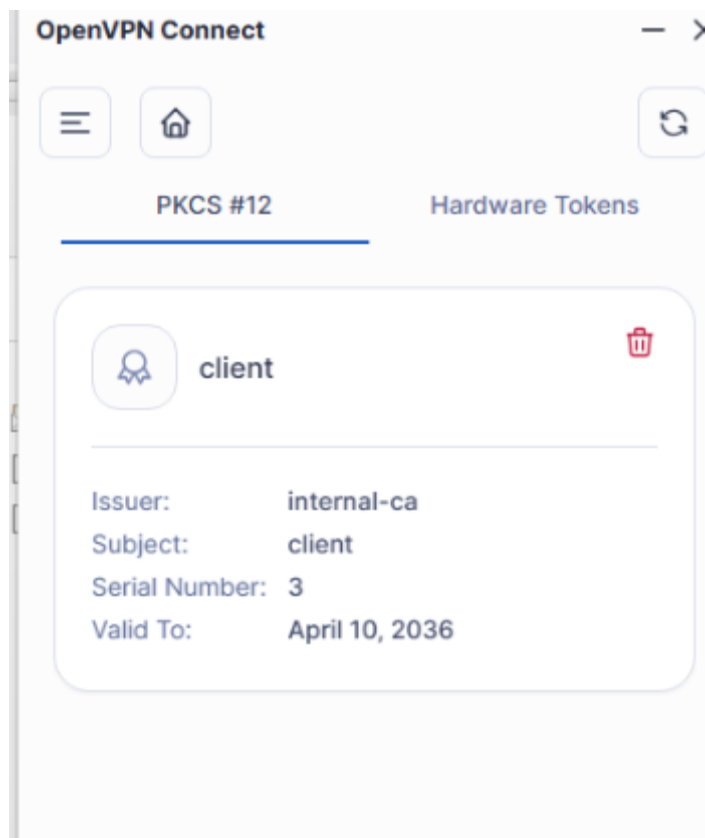
Tunnel Settings	
IPv4 Tunnel Network	<input type="text" value="10.10.10.0/24"/> This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in 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	<input type="text"/> 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	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	<input checked="" type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)	<input type="text" value="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	<input checked="" type="checkbox"/> Provide a default domain name to clients
DNS Default Domain	<input type="text" value="voua.local"/>
DNS Server enable	<input checked="" type="checkbox"/> Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
DNS Server 1	<input type="text" value="172.18.0.1"/>
DNS Server 2	<input type="text"/>
DNS Server 3	<input type="text"/>
DNS Server 4	<input type="text"/>
Block Outside DNS	<input type="checkbox"/> 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	<input type="checkbox"/> 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	<input type="checkbox"/> Provide an NTP server list to clients

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



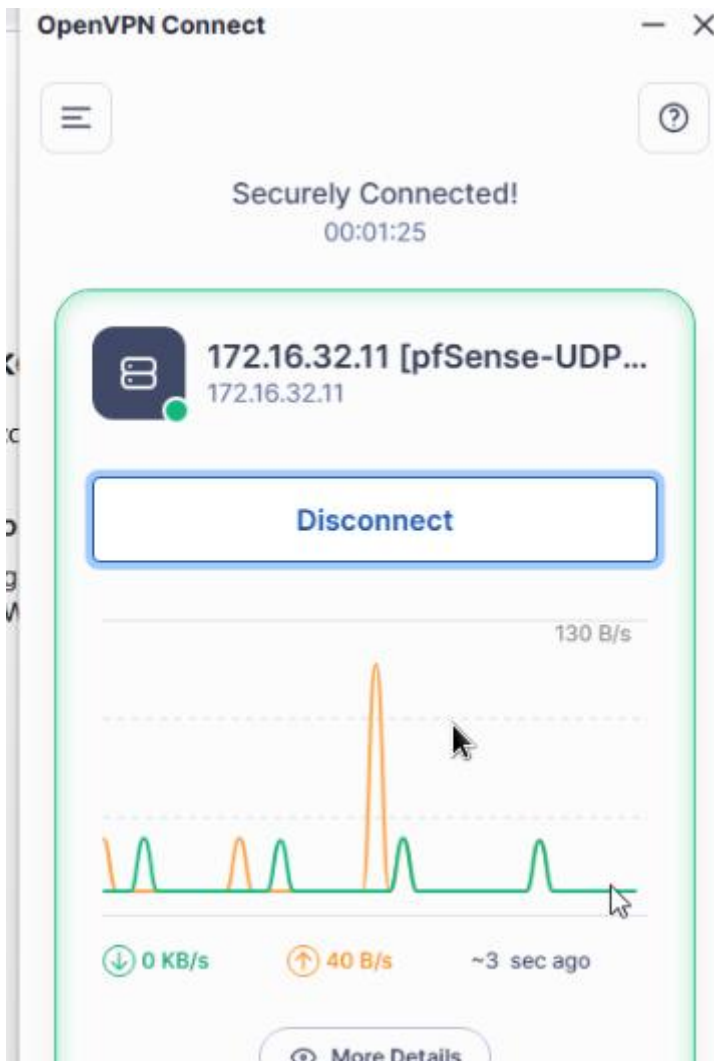
Importation du certificat et de la configuration cliente



Règle de parefeu



Tentative de connexion vpn sur machine cliente externe



OpenVPN Connecté avec succès

Nous tentons de ping sur un serveur interne

```
C:\Users\marc>ping 172.18.0.1

Pinging 172.18.0.1 with 32 bytes of data:
Reply from 172.18.0.1: bytes=32 time=1ms TTL=126
Reply from 172.18.0.1: bytes=32 time=1ms TTL=126
Reply from 172.18.0.1: bytes=32 time=1ms TTL=126
Reply from 172.18.0.1: bytes=32 time=1ms TTL=126
```

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

The screenshot shows the Nagios web interface in a browser window. The address bar shows 'http://172.18.0.5/nagios4/'. The interface includes a left sidebar with navigation links like 'General', 'Current Status', 'Problems', and 'Reports'. The main content area displays 'Current Network Status' with a last update of 'Mon Apr 20 10:47:54 CEST 2026'. It also features 'Host Status Totals' and 'Service Status Totals' summary boxes. Below these, there is a 'Host Status Details For All Host Groups' table with columns for Host, Status, Last Check, Duration, and Status Information. The table lists two hosts: 'Serveur-GLPI' and 'localhost', both with a status of 'UP'. A 'Quick Search' input field is visible below the table. The bottom right corner of the page has an 'Activate Windows' watermark.

Host	Status	Last Check	Duration	Status Information
Serveur-GLPI	UP	04-20-2026 10:43:30	6d 23h 56m 26s	PING OK - Packet loss = 0%, RTA = 0.32 ms
localhost	UP	04-20-2026 10:43:58	20d 2h 30m 33s	PING OK - Packet loss = 0%, RTA = 0.03 ms