CARON Cyprien BTS SIO 1ère année

Rapport de stage

Talice
SMART TRACKING SYSTEM

Campus Carlos Acutis Période de stage du 02 juin au 4 juillet 2025

Table des matières

1. Remerciements

Je tiens à remercier chaleureusement Laurent Guillot, qui m'accueilli au sein de son entreprise. Je tenais également à remercier Cédric Bordet, mon maître de stage chez Talice, pour m'avoir accompagné avec patience et bienveillance tout au long de ce stage

Un grand merci aussi à toute l'équipe, qui m'a accueilli comme un véritable membre de l'équipe. Leur gentillesse et leur soutien au quotidien ont largement contribué à faire de ce stage une expérience aussi agréable qu'enrichissante.

2. Présentation de l'entreprise Talice

2.1 Historique

Talice est une entreprise française créée en 2008 par trois experts en mobilité et traçabilité. Elle s'est rapidement imposée comme la spécialiste des solutions professionnelles RFID en France.

2.2 Activités principales

Talice propose des solutions techniques dans plusieurs domaines :

- Solutions de traçabilité et mobilité
- Technologie RFID (identification par radiofréquence)
- Développement d'applications spécifiques
- Maintenance et support technique

L'entreprise travaille principalement avec des clients de la distribution et de la logistique qui ont besoin de tracer leurs produits et d'améliorer leur productivité ;

2.3 Organisation

Talice a son siège en région parisienne et deux agences régionales (Nord et Est de la France). L'entreprise est organisée autour de trois services principaux : commercial, maintenance et développement.

Chaque client a un ingénieur commercial dédié qui coordonne tous les projets, ce qui simplifie les échanges et assure un suivi personnalisé.

3. Présentation du service d'accueil et des moyens informatiques

3.1 Moyens matériels postes de travail

Talice utilise dix serveurs SOTI MobiControl Cloud, un outil très complet de gestion des appareils mobiles (Mobile Device Management). Il permet à l'entreprise de superviser à distance environ 5

000 terminaux, principalement des smartphones ou terminaux Android, avec aussi quelques appareils sous iOS.

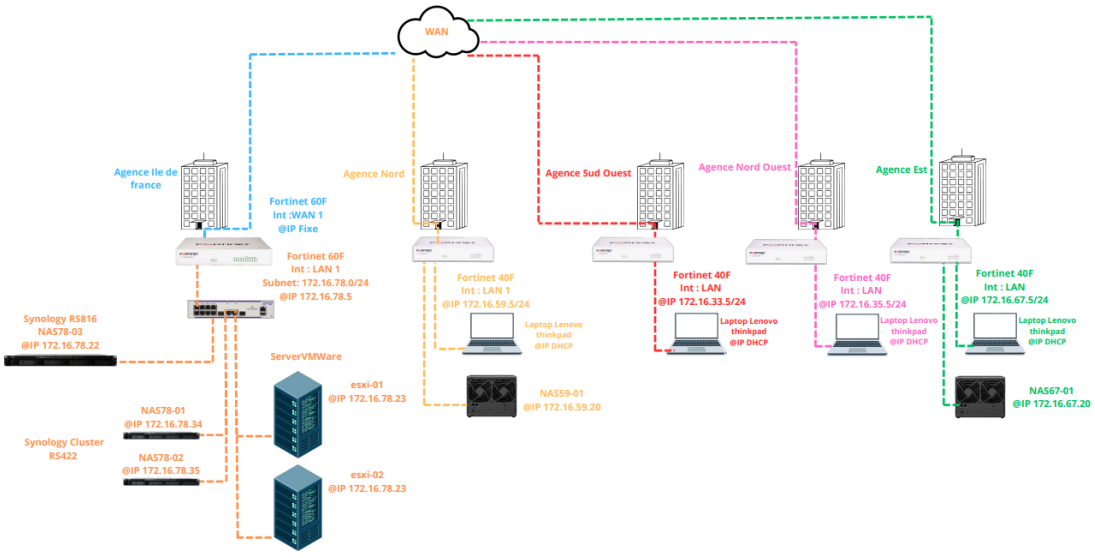
Pour la partie server Talice héberge sur deux serveurs physiques sous VMware. Ces serveurs font tourner 8 machines virtuelles :

- Un serveur de test SOTI (MDM)
- Un Active Directory
- Un serveur PRTG (monitoring)
- Un serveur Veeam (sauvegarde)
- Un serveur de développement
- Un serveur StageNow réservé à la configuration automatique des terminaux Zebra.
- Le serveur BarTender, qui permet d'imprimer des codes-barres et étiquettes pour la production ou la logistique.
- Et un server NiceLabel, qui propose des fonctionnalités similaires à BarTender.

Pour les sauvegarde deux NAS Synology RS422 sont configurer en cluster, 2 NAS Synology DS416 sont utiliser comme sauvegarde externe sur des sites distant, et 1 NAS RS816 pour du stockage de données.

Pour la sécurité des par feu Fortigate 60F, Fortigate 40F ont été configuré sur chaque site en VPN de type site to site.

(Voir Annexe 1)



3.2 Moyens logiciels

L'entreprise utilise principalement des ordinateurs sous Windows pour ses postes de travail. Les terminaux mobiles, scanners et douchettes sont à plus de 90 % sous Android. Côté logiciels, les outils utilisés incluent BarTender et NiceLabel pour l'impression d'étiquettes, ainsi que StageNow pour la configuration des terminaux Zebra.

4. Présentation du projet

Dans le cadre de la conformité au Règlement Général sur la Protection des Données (RGPD), l'entreprise Talice doit renforcer sa stratégie de sauvegarde des données. Le RGPD impose des exigences strictes concernant la protection et la sauvegarde des données personnelles,

Les précautions élémentaires pour la sauvegarde des données sont :

- *Effectuer des sauvegardes fréquentes des données, que celles-ci soient sous forme papier ou électronique. Il peut être opportun de prévoir des sauvegardes incrémentales quotidiennes et des sauvegardes complètes à intervalles réguliers*
- *Stocker au moins une sauvegarde sur un site géographiquement distinct du site d'exploitation.*
- *Isoler au moins une sauvegarde hors ligne, déconnectée du réseau de l'entreprise.*
- *Protéger les données sauvegardées au même niveau de sécurité que celles stockées sur les serveurs d'exploitation (ex. : en chiffrant les sauvegardes, en prévoyant un stockage dans un lieu sécurisé, en encadrant contractuellement une prestation d'externalisation des sauvegardes).*
- *Chiffrer le canal de transmission, si celui-ci n'est pas interne à l'organisme, lorsque les sauvegardes sont transmises par le réseau.*
- *Tester régulièrement l'intégrité des sauvegardes et la capacité de les restaurer.*

4.1 Contexte du projet

Actuellement, Talice dispose déjà de NAS (Network Attached Storage) de sauvegarde, sur ses sites mais suite à une relocalisation de ses locaux dans des espaces de coworking, ils n'ont plus la main sur l'infra réseau. Pour permettre la redondance de ces sauvegardes il faut trouver une solution afin de pouvoir effectuer une réplication de sauvegarde à distance avec une IP publique dynamique dans l'espace de coworking tout en assurant la sécurité.

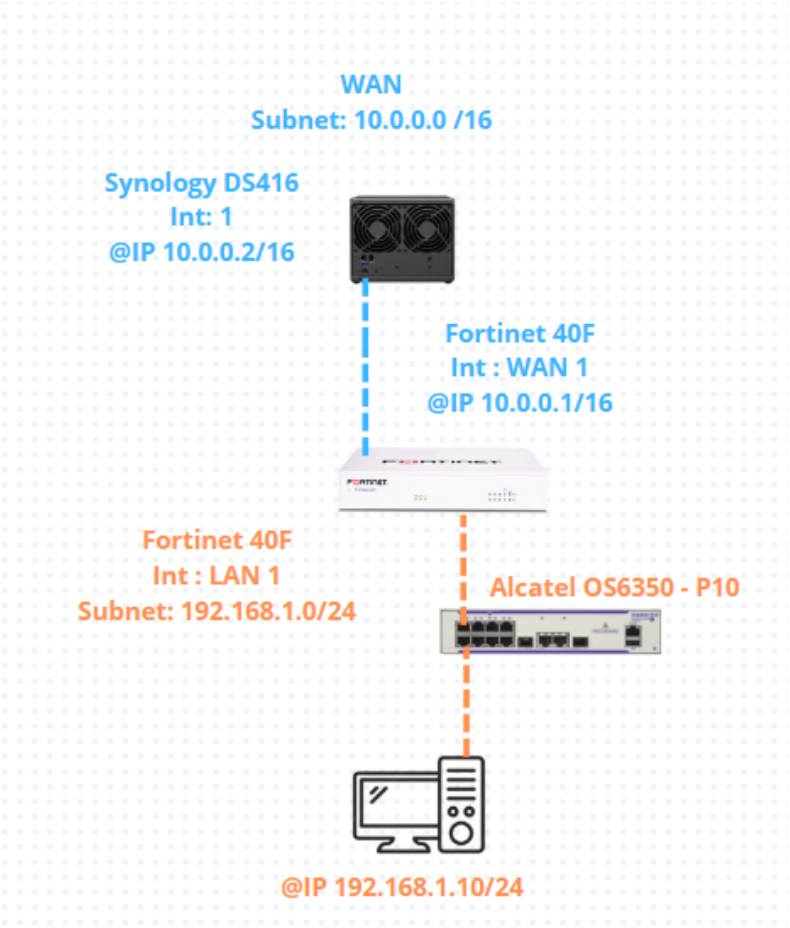
Le projet consiste donc à mettre en place un NAS de sauvegarde distante, qui permettra de créer une solution de sauvegarde redondante et sécurisée.

L'entreprise Talice a déjà un réseau fonctionnel avec des FortiGate 60F et 40F et deux NAS Synology en cluster. Le FortiGate est configurer en VPN site to site ce qui permet aux agences distantes de se connecter au réseau de Talice. Pour ne pas perturber le bon fonctionnement de l'entreprise j'ai dû crée une maquette hors réseau pour faire mes tests et pour ne pas déranger le bon fonctionnement de l'entreprise (voir schéma). Le plan de sauvegarde actuel des serveurs est classé par importance des services, celui des Laptop utilise une technologie dédier de Synology la sauvegarde en continu.

La sauvegarde des machines virtuelles est géré par **Veam**, elle est catégorisée selon l'importance des services qu'elles hébergent. Plus un service est essentiel, plus les sauvegardes sont fréquentes. C'est le cas notamment du serveur Windows qui gère l'Active Directory : il est sauvegardé tous les jours en incrémental, et une sauvegarde complète est faite tous les mois. Pour éviter une accumulation excessive, les anciennes sauvegardes sont automatiquement supprimées dès que 20 incrémentations ont été effectuées.

Machine virtuelle	Nb sauvegarde incremental	Nb full back up
Windows Server (AD)	Tous les jours de la semaine	1 fois /mois
Server Dolibarr	Tous les jours de la semaine	1 fois /mois
Server Git	Tous les jours de la semaine	1 fois /mois
Bartender	1 fois /mois	1 fois /semestre
Loftware	1 fois /mois	1 fois /semestre
Windows Server (Devs)	1 fois /mois	1 fois /semestre
Server monitoring (Prtg)	1 fois /mois	1 fois /semestre
Soti Mobil control (MDM)	1 fois /mois	1 fois /semestre

Maquette hors réseau



4.2 Objectifs

L'objectif principal est de garantir la continuité d'activité de l'entreprise et de respecter les obligations légales du RGPD.

En cas de sinistre (incendie, vol, panne majeure) touchant le site principal, l'entreprise doit pouvoir récupérer ses données critiques rapidement.

Les objectifs sont :

- Assurer la conformité aux exigences RGPD en matière de sauvegarde
- Créer une sauvegarde géographiquement distante
- Sécuriser les transferts de données via un canal chiffré
- Maintenir l'intégrité et la disponibilité des données de l'entreprise

4.3 Commanditaire

Ce projet bénéficie à l'ensemble de l'entreprise Talice, et plus particulièrement :

- À la *direction*, qui doit s'assurer de la conformité légale
- Au *service informatique*, responsable de la sécurité des données
- À tous les *collaborateurs* dont les données de travail seront protégées

Les enjeux sont multiples pour Talice :

- Légaux : Respecter les obligations du RGPD et éviter les sanctions
- Garantir la disponibilité : Garantir la continuité d'activité en cas d'incident
- Économiques : Éviter les pertes financières liées à une perte de données
- Réputation : Maintenir la confiance des clients en protégeant leurs informations

5. Développement du travail réalisé

5.1 Outils utilisés

Dans le cadre de la réalisation de la maquette, j'ai mis en œuvre les équipements suivants :

- un switch Alcatel OS6350-P10,
- un NAS Synology DS416 (avec sa version du système d'exploitation),
- un pare-feu FortiGate 40F (également avec sa version du système d'exploitation),
- un ordinateur portable Lenovo ThinkPad utilisé pour la configuration des équipements,
- un ordinateur portable HP Victus dédié aux phases de test.

Pour la communication avec les équipements via le port console, j'ai utilisé le logiciel PuTTY, en combinaison avec un câble console et un adaptateur USB vers DB9.

5.2 Méthodes de travail

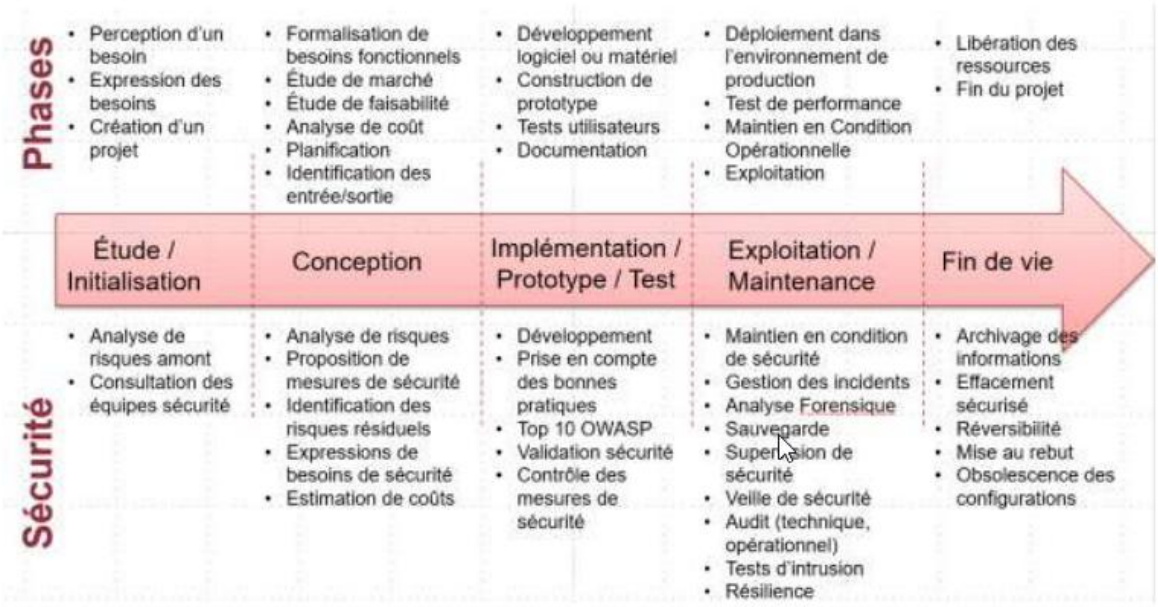
Ma méthode de travail pour ce projet était de faire mes recherches sur les solutions possible pour résoudre la problématique, documenter toutes les solutions avec les liens des tutos/site web avec

les procédures à effectuer sur le matériel ou alors de suivre la documentation officielle du matériel.

5.3 Déroulement du projet

Le projet a débuté dès la phase d'étude et d'initialisation, au cours de laquelle j'ai analysé les besoins, défini les objectifs et posé les premières bases techniques. Étant seul en charge du projet, je n'ai pas utilisé des outils de gestion du temp comme Trello ou un diagramme de Gantt.

Je tenais un journal de bord dans un cahier de brouillon, où je notais tous mes essais, qu'ils soient concluants ou non. Une fois une solution validée, je la documentais de manière plus formelle dans un fichier Word, afin de garder une trace claire et structurée de mes avancées.



5.4 Explications techniques

Le réseau de Talice était déjà en place et fonctionnait, il était donc en phase d'exploitation et de maintenance. De mon côté, pour pouvoir implémenter la nouvelle solution, j'ai dû repartir de zéro, comme si je lançais un nouveau projet. J'ai donc commencé par une phase d'étude et d'initialisation.

5.4.1 Étude / Initialisation

Après avoir reçu tous les équipements pour crée ma maquette j'ai dû les réinitialiser car ils contenaient encore des anciennes configurations.

Pour commencer, j'ai dû réinitialiser le switch Alcatel os6350 p-10 de test, qui contenait encore une ancienne configuration. Cependant, ce modèle ne dispose pas de bouton de réinitialisation externe.

J'ai alimenté le switch et connecté le câble console à l'adaptateur DB9, lui-même relié à mon PC. Dans le Gestionnaire de périphériques, le câble a été détecté sur le port COM4.

J'ai lancé PuTTY avec les bons paramètres (vitesse, port COM4, etc.), mais aucune réponse n'est apparue dans le terminal.

J'ai revérifié toutes les connexions ainsi que les paramètres de PuTTY, sans succès.

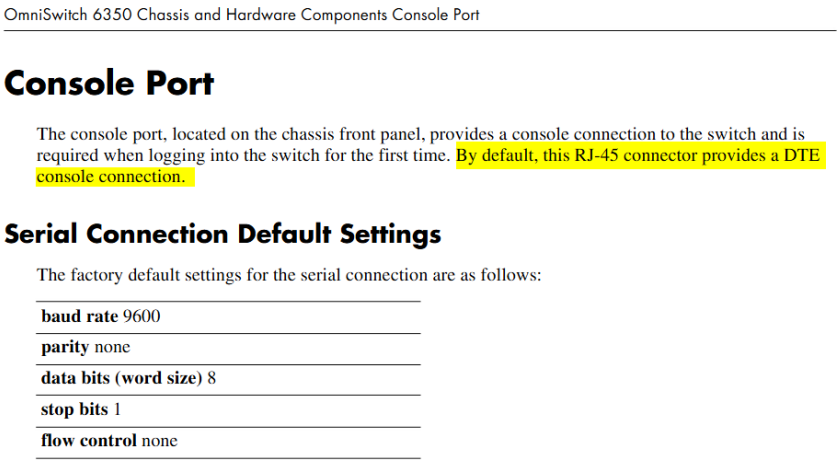
Pensant que le câble DB9 pouvait être défectueux, je l'ai remplacé par un autre, testé et fonctionnel sur un autre switch — même résultat : aucune communication.

J'ai inspecté le câble console plus en détail. J'ai testé la continuité des fils à l'aide d'un multimètre.

Je me suis appuyé sur un schéma de câblage pour m'assurer que chaque fil établissait bien une liaison — le test s'est révélé concluant.

Je me suis alors référé à la documentation officielle du switch. J'ai découvert qu'il était possible de flasher le BIOS via le port USB, mais cela nécessite un accès au boot menu, inaccessible tant que la liaison série ne fonctionne pas.

En examinant de plus près la documentation du switch, j'ai repéré une norme de câblage spécifique propre à Alcatel, ce qui m'a orienté vers la nécessité d'un câblage console non standard pour établir une connexion correcte.



OmniSwitch 6350 Chassis and Hardware Components Console Port

Console Port

The console port, located on the chassis front panel, provides a console connection to the switch and is required when logging into the switch for the first time. By default, this RJ-45 connector provides a DTE console connection.

Serial Connection Default Settings

The factory default settings for the serial connection are as follows:

baud rate 9600
parity none
data bits (word size) 8
stop bits 1
flow control none

Je me renseigne sur le câble console et constate qu'il n'est pas compatible.

Je récupère alors le matériel nécessaire : deux connecteurs RJ45, un câble RJ45, une rallonge RJ45 et un multimètre.

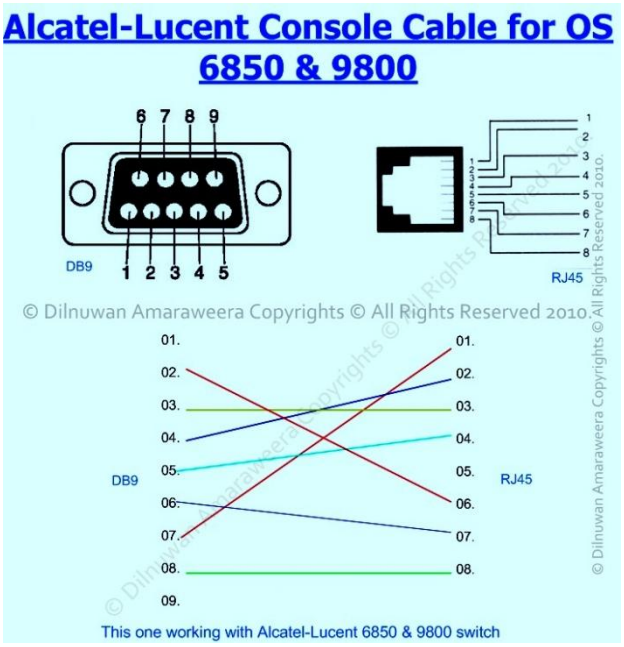
Je commence par câbler la première partie du câble, celle connectée à la rallonge RJ45, en suivant la norme T568-B.

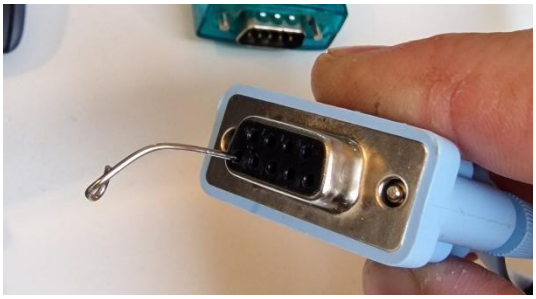
Ensuite, je recherche un schéma de câblage compatible avec les switches Alcatel, ce qui me permet d'identifier les connecteurs ainsi que l'ordre de câblage à respecter sur le connecteur.

Pour le connecteur :

Couleur indiquer sur le connecteur :	Position
Blanc Orange	3
Orange	6
Blanc Marron	7
Marron	8
Blanc Vert	1
Vert	2
Blanc Bleu	5
Bleu	4

Maintenant que j'ai identifié la correspondance entre chaque couleur et sa position sur le connecteur, il ne me reste plus qu'à insérer une extrémité de trombone dans chacune des broches du connecteur DB9 (1, 2, 3, 4, etc.), tout en respectant la norme de câblage DTE, comme illustré dans le schéma ci-dessous.





Je teste chaque câble afin d'identifier sa position dans le connecteur DB9, de repérer par où il ressort et de déterminer à quelle broche il doit être raccordé.

Par exemple pour être raccorder correctement le Blanc orange doit être raccorder à la broche numéro 6 du connecteur voici un tableau avec toutes les positions par rapport au connecteur et sa couleur

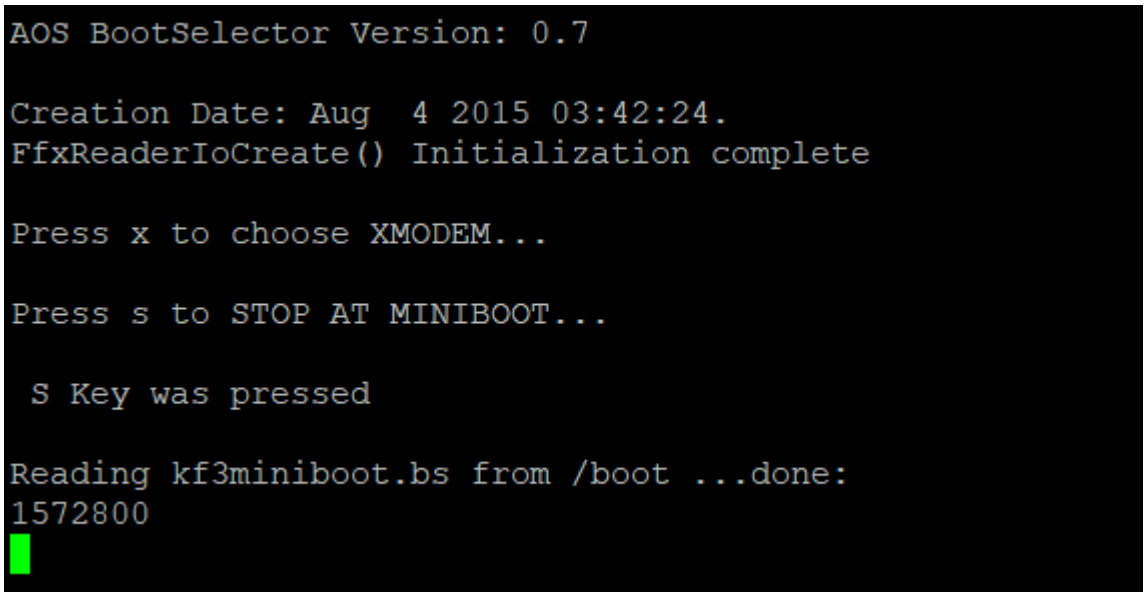
Les connecteurs que j'ai utilisés

Couleur du câble	Position dans le connecteur RJ45
Blanc Orange	6
Orange	3
Blanc Marron	2
Marron	1
Blanc Vert	8
Vert	7
Blanc Bleu	4
Bleu	Pas connecter

Après avoir réalisé des tableaux de repérage pour organiser le câblage, je procède à l'assemblage des connecteurs en respectant l'ordre défini précédemment. Je retente ensuite la connexion au switch, et cette fois, la communication fonctionne correctement.

Une fois cela fait nous pouvons accéder à l'interface via le terminal et nous pouvons aller dans le menu mini boot

Donc je peux enfin commencer la réinitialisation du switch au branchement de l'alimentation nous avons quelques seconde avant que le switch ne boot il faut appuyer très rapidement sur la touche « s » pour interrompre le boot (comme sur un ordinateur avec les touches f11, f12 ...)



Une fois cela fait nous arrivons dans une interface de mini boot il faut supprimer les anciens fichiers de configuration.

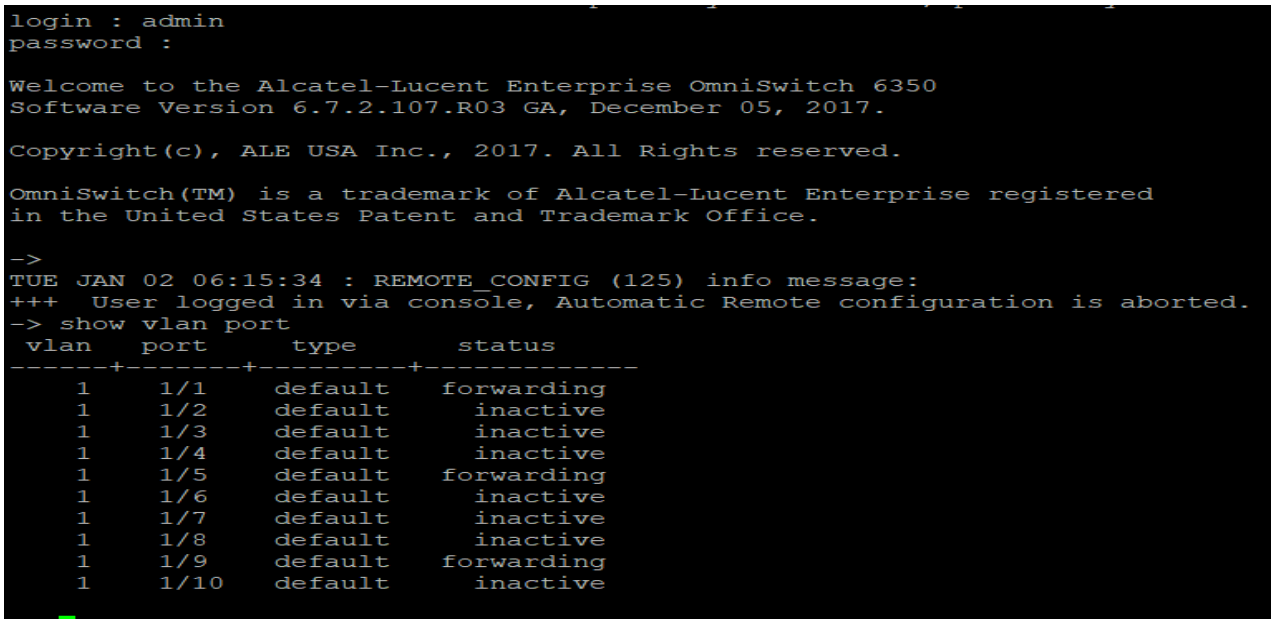
```
[Miniboot]->cd "/flash/working"
value = 0 = 0x0
[Miniboot]->pwd
/flash/working
value = 15 = 0xf
[Miniboot]->rm boot.cfg
invalid number: .c
[Miniboot]->rm "boot.cfg"
value = 0 = 0x0
[Miniboot]->cd ..
invalid number: ..
[Miniboot]->cd ".."
value = 0 = 0x0
[Miniboot]->cd "certified"
value = 0 = 0x0
[Miniboot]->rm "boot.cfg"
value = 0 = 0x0
[Miniboot]->reload
```

Une fois les fichiers de configuration supprimés, il suffit de tenter un accès au switch pour vérifier s'il reste une configuration active.

Les identifiants par défaut sont :

Identifiant : admin

Mot de passe : switch



L'absence de VLAN attribué à l'ensemble des ports confirme que le switch a été correctement réinitialisé.

Ensuite, je procède à la réinitialisation du Fortinet 40F. Pour cela, je connecte le câble console à l'équipement, puis j'accède à l'interface CLI après avoir saisi le mot de passe, j'exécute la commande « **execute factoryreset** » pour restaurer les paramètres d'usine.

Le NAS avait déjà été réinitialisé par mon tuteur de stage avant qu'il ne me le confie.

5.4.2 Conception

Une fois tous les équipements réinitialisés, j'ai pu tester des solutions potentielles.

Dans les locaux de Talice, un pare-feu FortiGate 60F est déjà installé et permet la création de connexions VPN.

J'ai d'abord envisagé d'utiliser cette solution en installant le logiciel FortiClient VPN sur le NAS Synology DS416 distant, avec un compte spécifique pour qu'il puisse accéder au réseau de l'entreprise via le VPN.

Malheureusement, cette option n'a pas pu aboutir, car FortiClient n'est pas disponible sur l'App Center de Synology.

En cherchant une alternative, je me suis tourné vers une solution proposée directement par Synology : l'application VPN Server.

Celle-ci permet de transformer un NAS en serveur VPN.

L'idée étais donc de configurer sur l'un des deux NAS (par exemple, celui situé chez Talice) comme serveur VPN, et de faire en sorte que le NAS distant s'y connecte en tant que client.

Cela aurait permis de créer un tunnel sécurisé entre les deux appareils, garantissant une transmission chiffrée des données pendant les sauvegardes.

Le principal problème étant que Talice avec son Fortigate déjà présent utilise déjà la fonction VPN avec les deux VPN cela pourrait crée un conflit de VPN par rapport au port d'ouvertures des protocoles et donc gêner le bon fonctionnement de l'entreprise.

En réfléchissant un peu plus j'ai trouvé une autre solution en ajoutant le NAS client sur le VPN FortiGate car le NAS permet de crée ses configurations VPN avec trois protocoles de disponible :

-PPTP

-OPENVPN

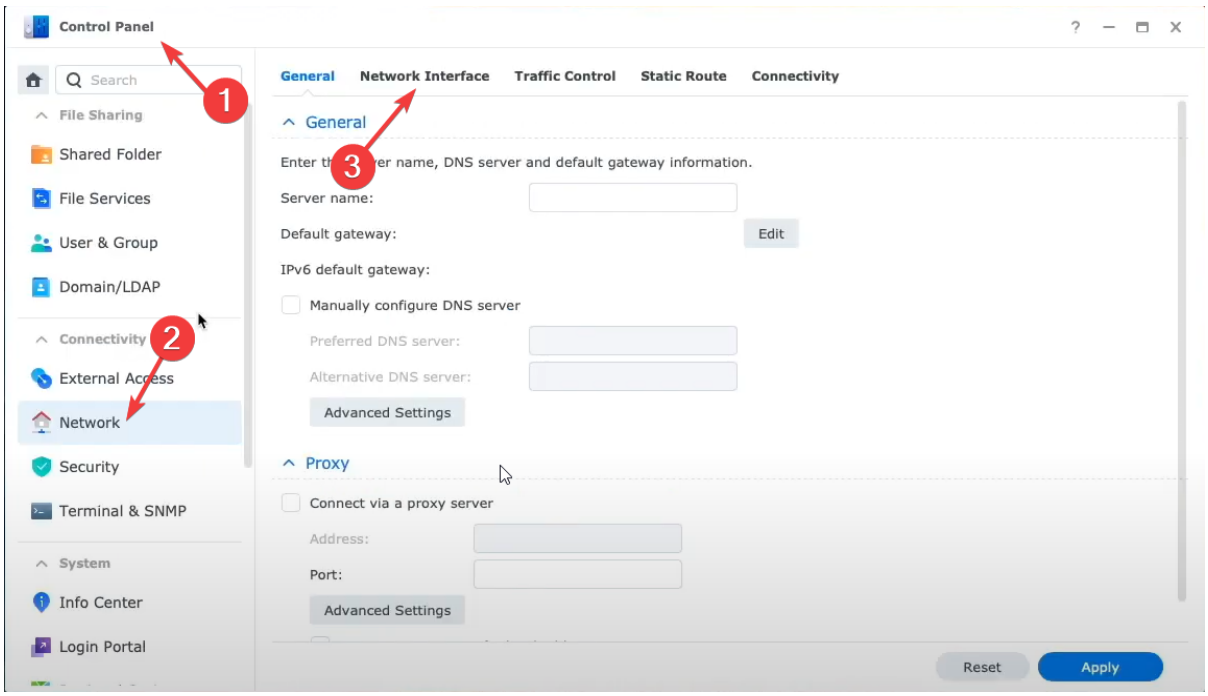
-L2TP/IPsec

La configuration des clients VPN actuel sur le FortiGate 60F est en IPsec. J'ai donc essayé de configurer le NAS avec la procédure suivante en choisissant le protocole L2TP/IPSEC

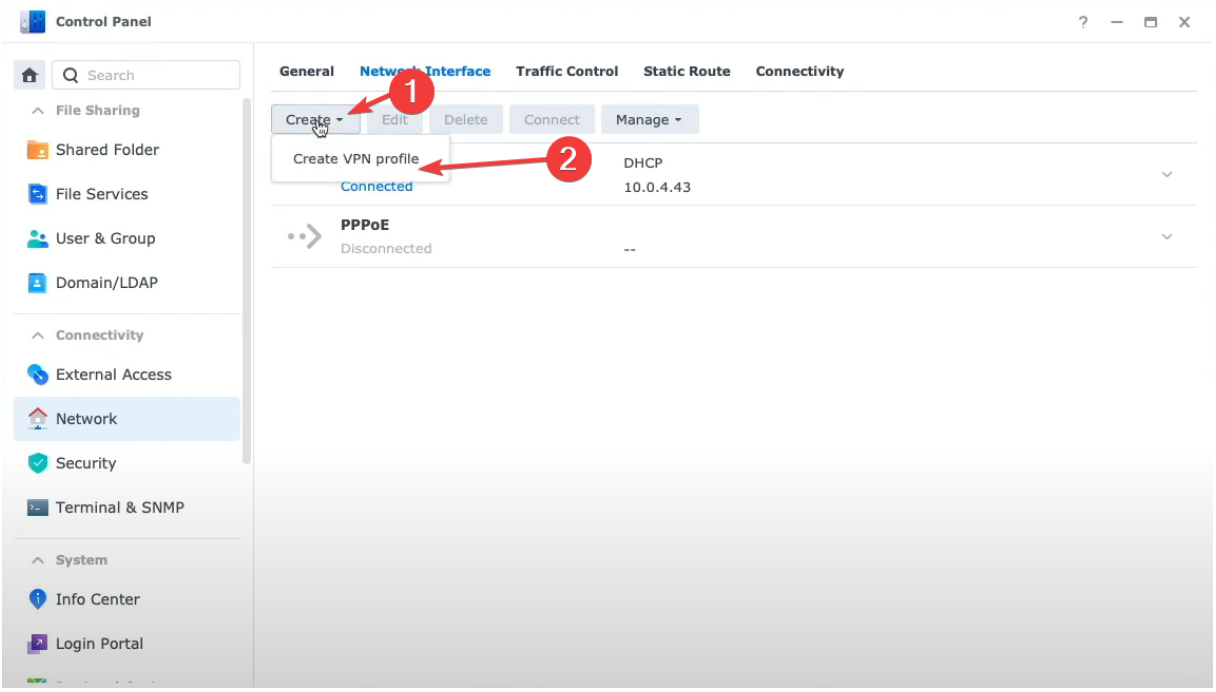
Procédure :

Se rendre sur le NAS Synology :

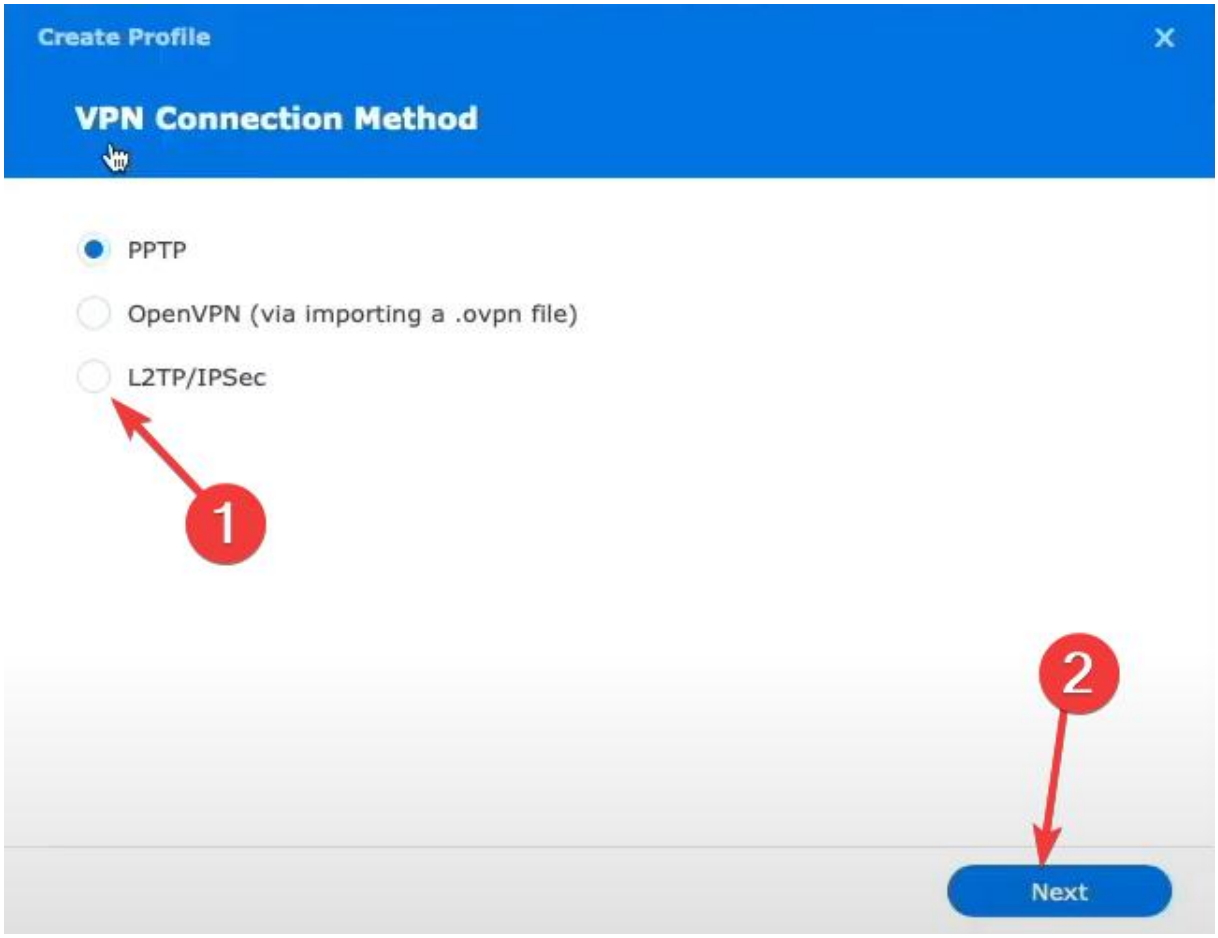
Aller dans **control Panel**->**network**-> **network interface**



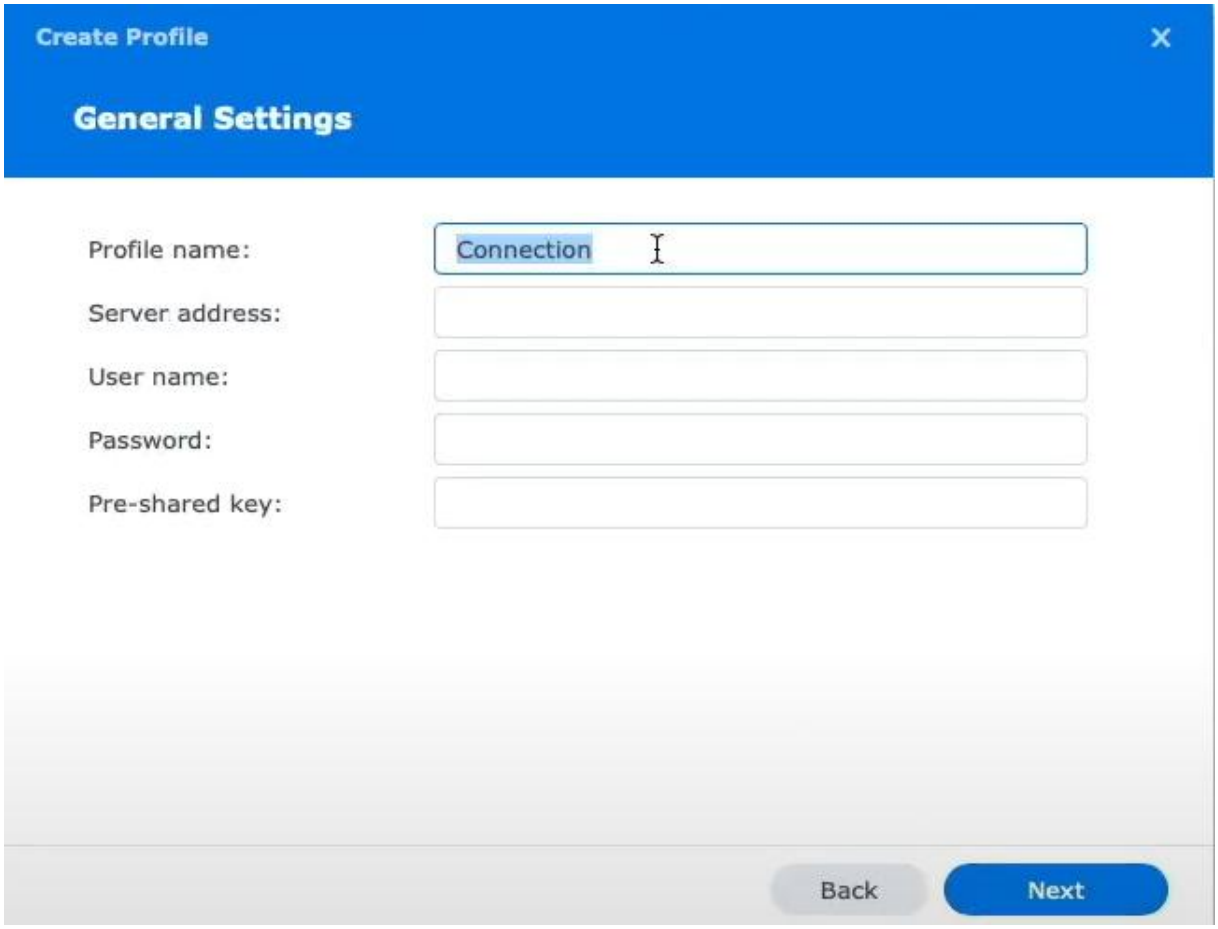
Puis aller dans : **create** -> **create a VPN Profile**



Puis appuyer sur l'option : **L2TP/IPSec**



Rentrer les informations de connexion du serveur VPN

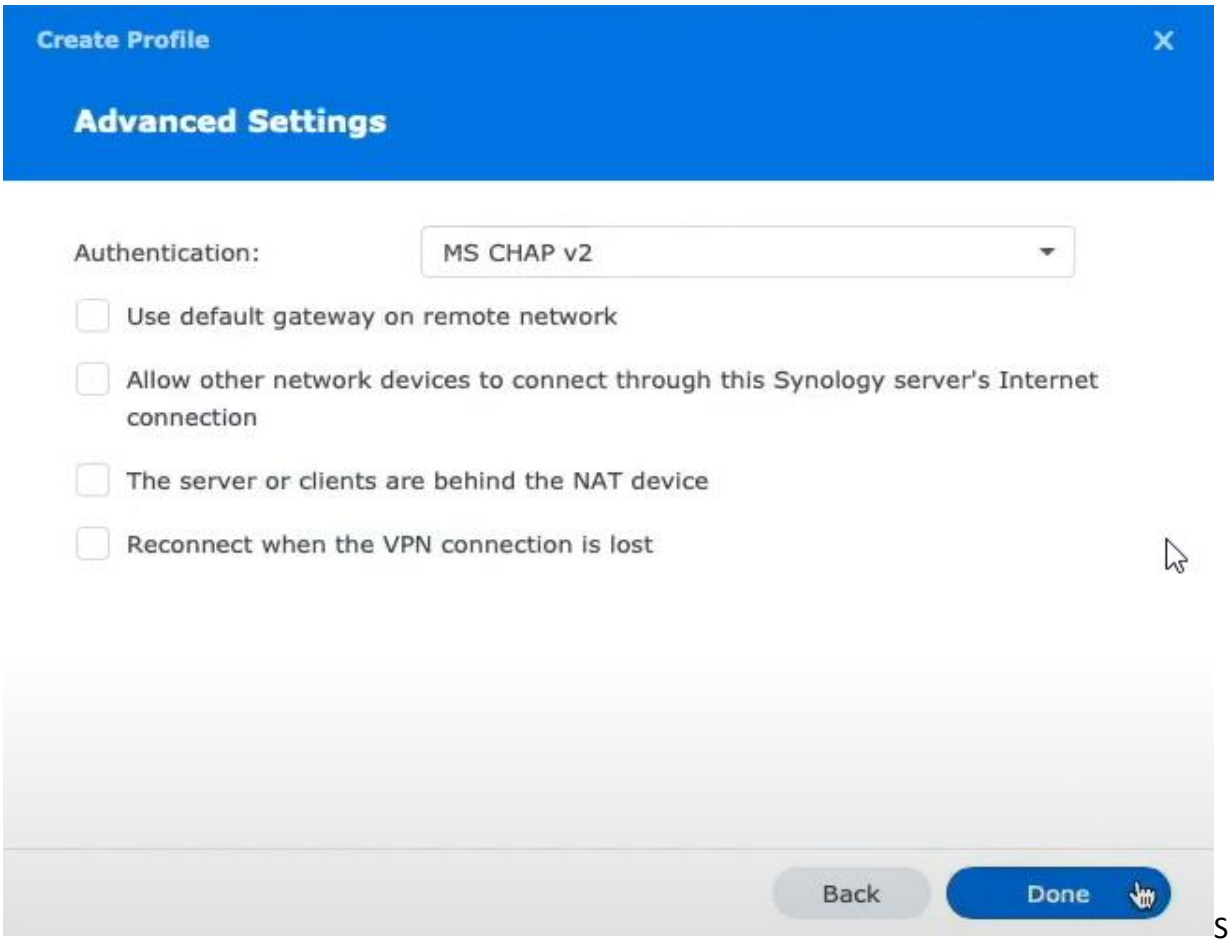


Puis cocher les options suivantes :

-The server or clients are behind the NAT device

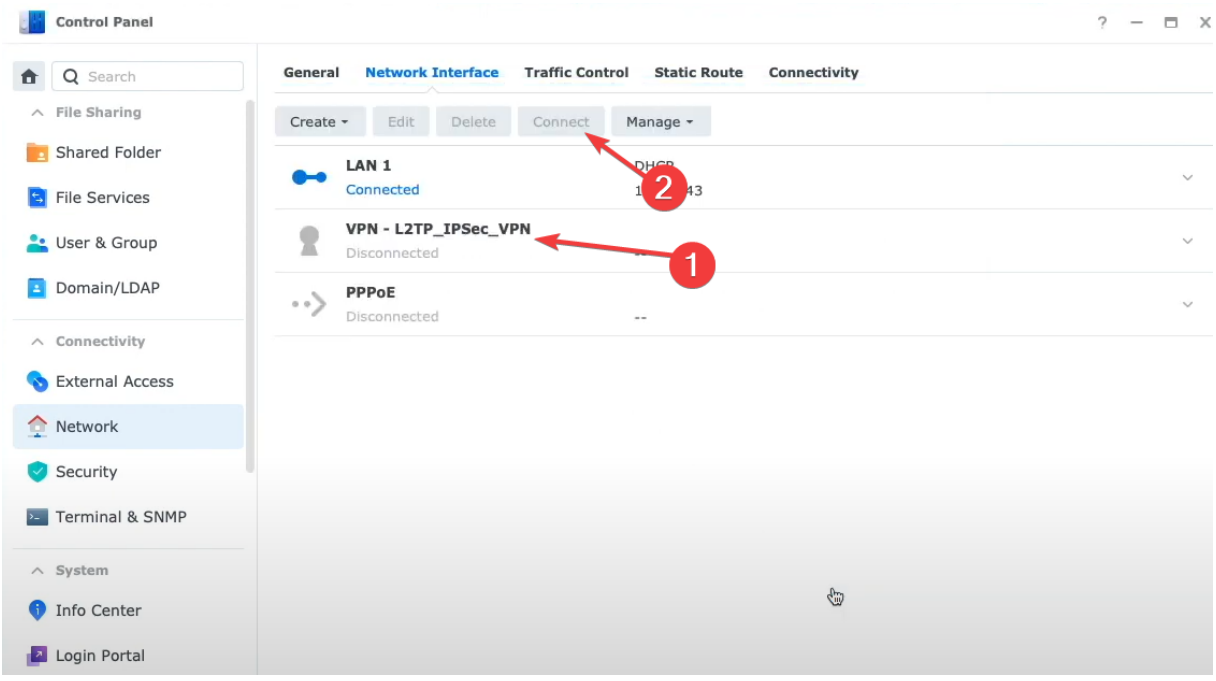
-Reconnect when the VPN connection is lost

Puis Cliquer sur terminer



S

Sélectionner la configuration précédemment créée et cliquer sur **Connect**



Après un essai je me suis aperçu que la configuration ne fonctionnait pas. Puis j'ai douté sur la compatibilité des protocoles L2TP/IPSEC et IPsec. Pour comprendre l'erreur je me suis renseigner sur ces protocoles :

IPsec :

Le sigle IPsec signifie (Internet Protocol Secure), IPsec n'est pas un protocole mais une suite de protocole qui permet de chiffre la charge utile du paquet en mode transport ou tout le paquet en mode tunnel. L'IPsec est composé de tous ces protocoles

- AH (Authentication Header)
  Le rôle de ce protocole est d'assurer l'authenticité et l'intégrité des données
- ESP (Encapsulating Security Protocol)
- SA (Security Association)

L2TP/IPsec :

Le sigle L2TP signifie (Layer 2 Tunneling Protocol), ce protocole ne se charge que de la création du tunnel (il ne chiffre pas les données).

C'est l'IPsec (en mode transport) qui s'occupe de chiffrer la charge utile des paquets.

Donc après ces courtes recherches j'ai compris que les protocoles n'était pas compatible. J'ai donc cherché dans la documentation de Fortinet / Synology, à ce moment-là j'avais potentiellement trouvé une solution le « L2TP over IPSEC ».

Cette option permet de garder le tunnel IPsec déjà existant en implémentant le L2TP ce qui pour notre usage est parfait.

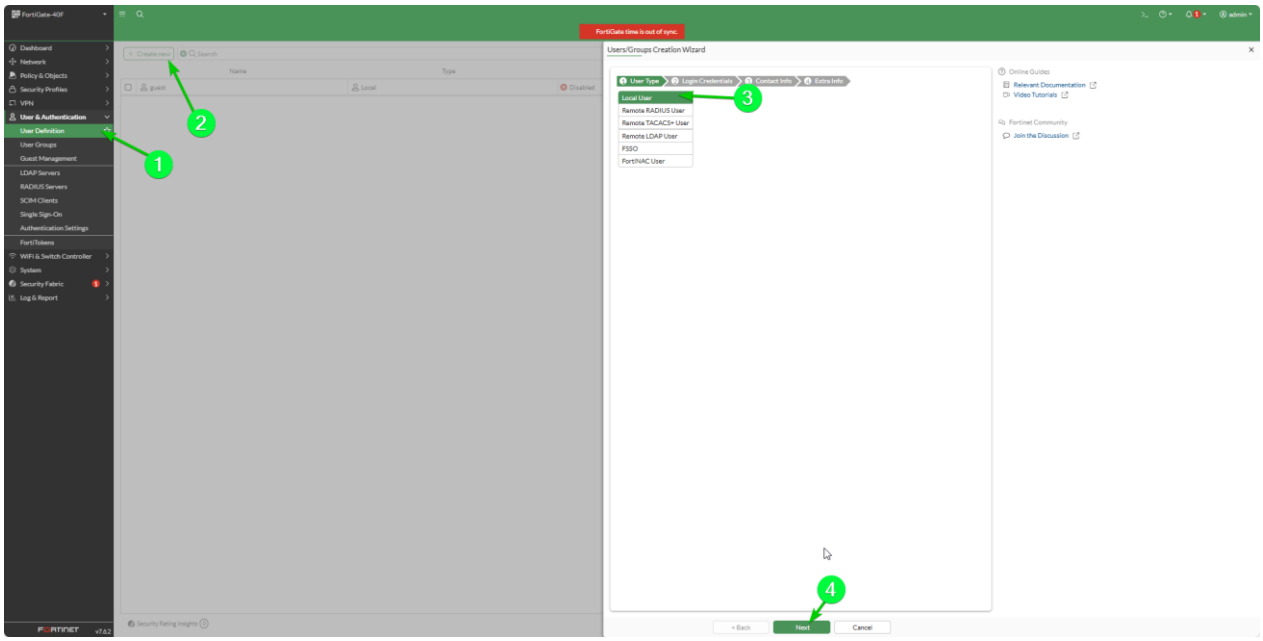
5.4.3 Implémentation / Prototype / Tests

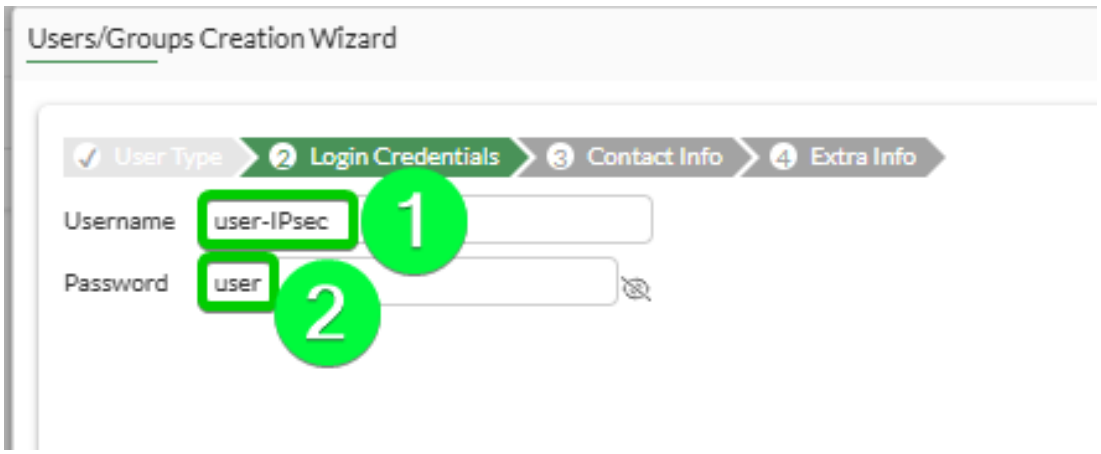
5.4.3.1 Création du user et du Tunnel IPsec

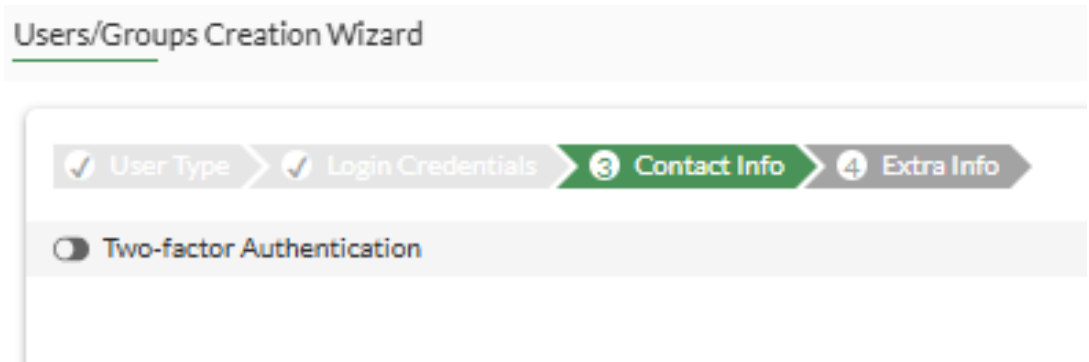
J'ai voulu tester le bon fonctionnement de cette solution donc en premier lieu il fallait que je créé un VPN IPsec.

Avec ma maquette j'avais démarré la passerelle puis j'avais créé un compte utilisateur local pour l'IPsec.

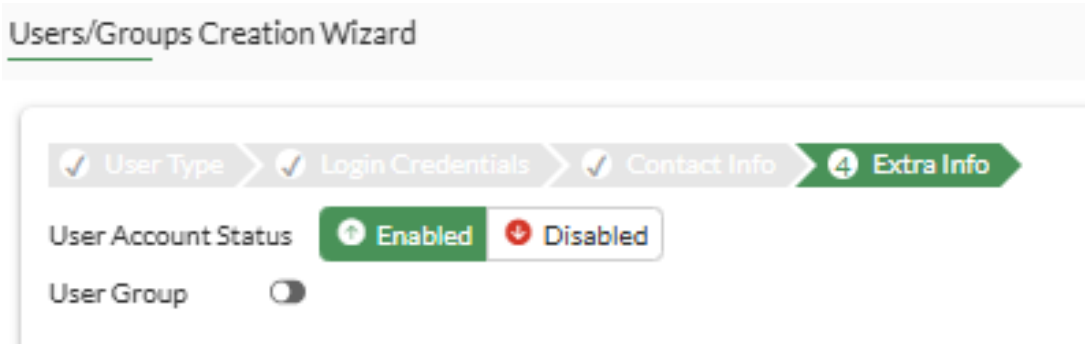
Se rendre dans **User Definition** -> **Create user** -> **Local user** ->**Next**





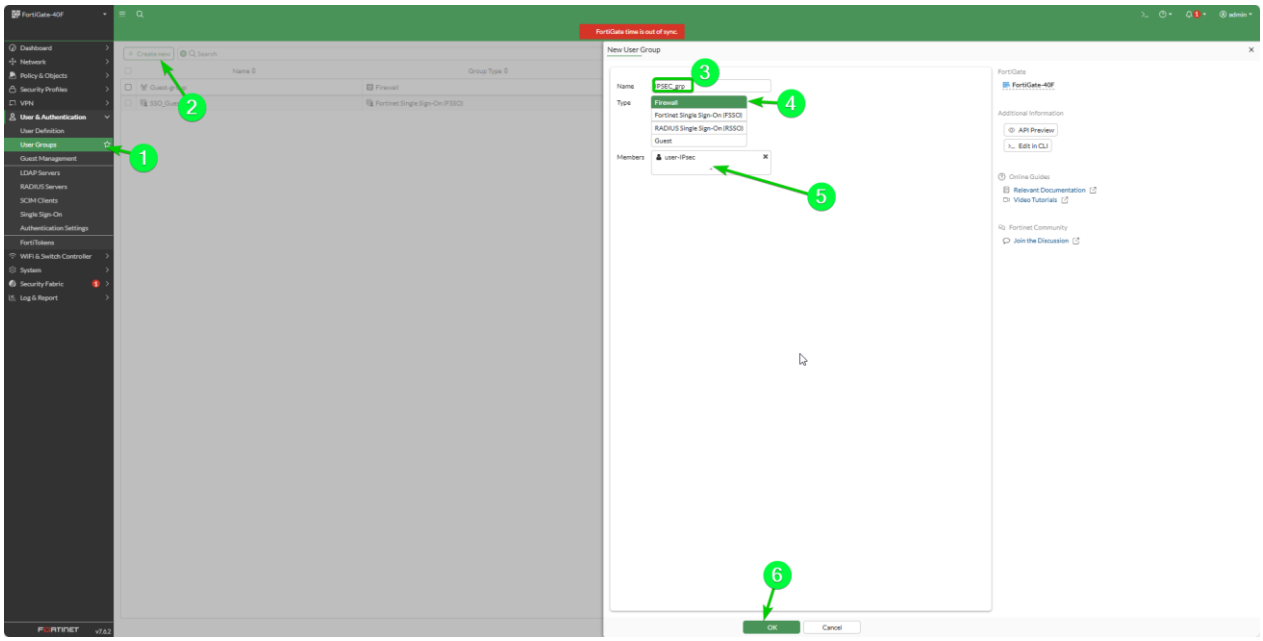


Désactiver l'authentification à double facteur pour la connexion de **l'utilisateur**

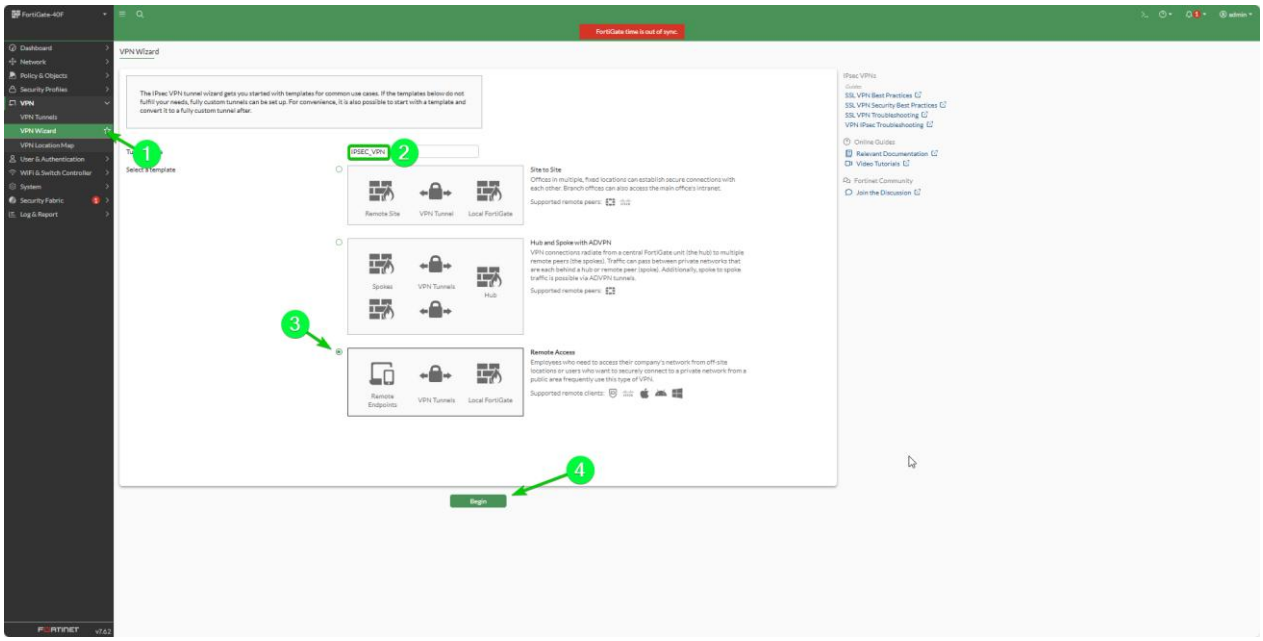


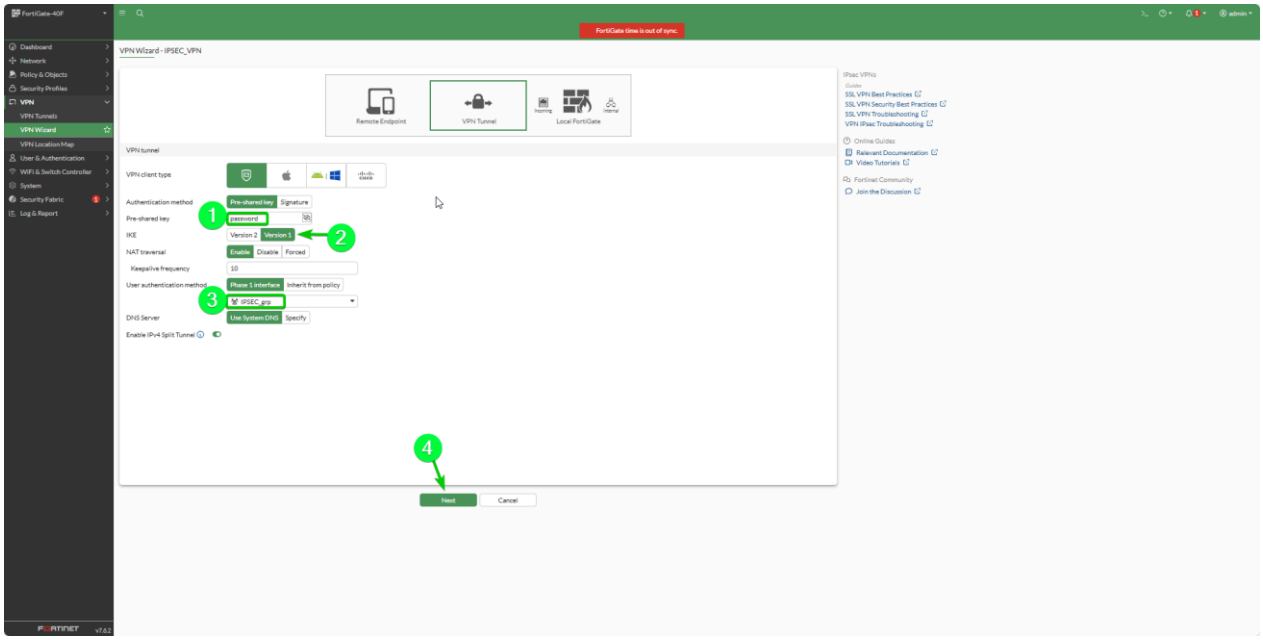
Activer le compte puis cliquer sur **submit**

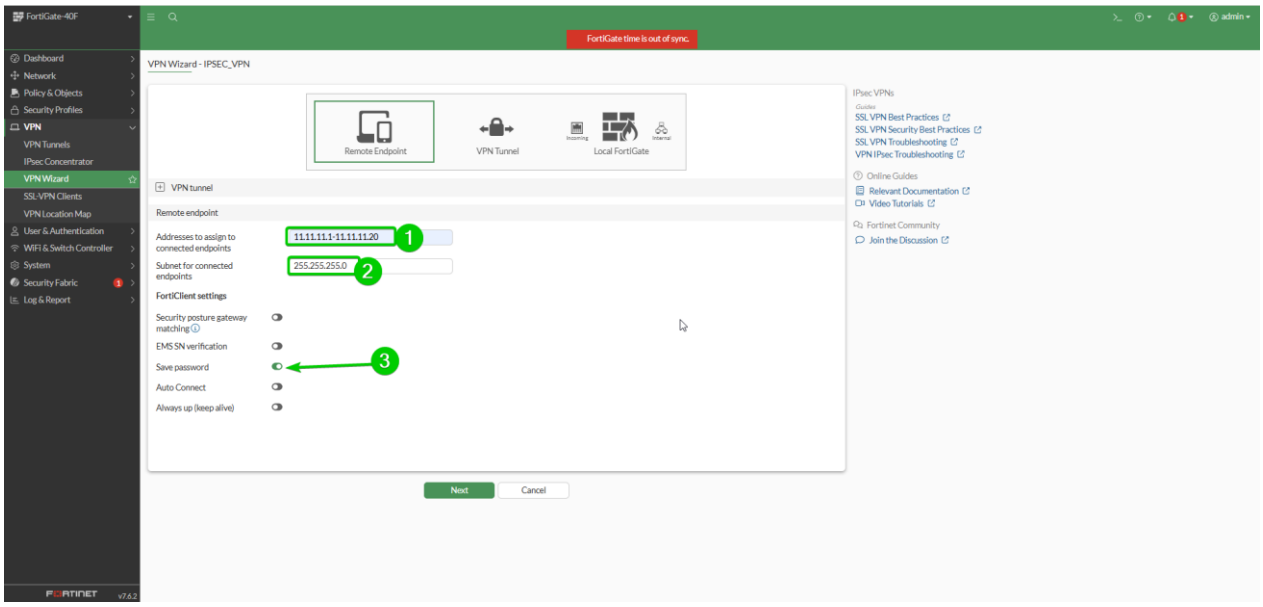
Se rendre dans **User Groups** -> **Create New** -> puis rentrer les informations -> **OK**

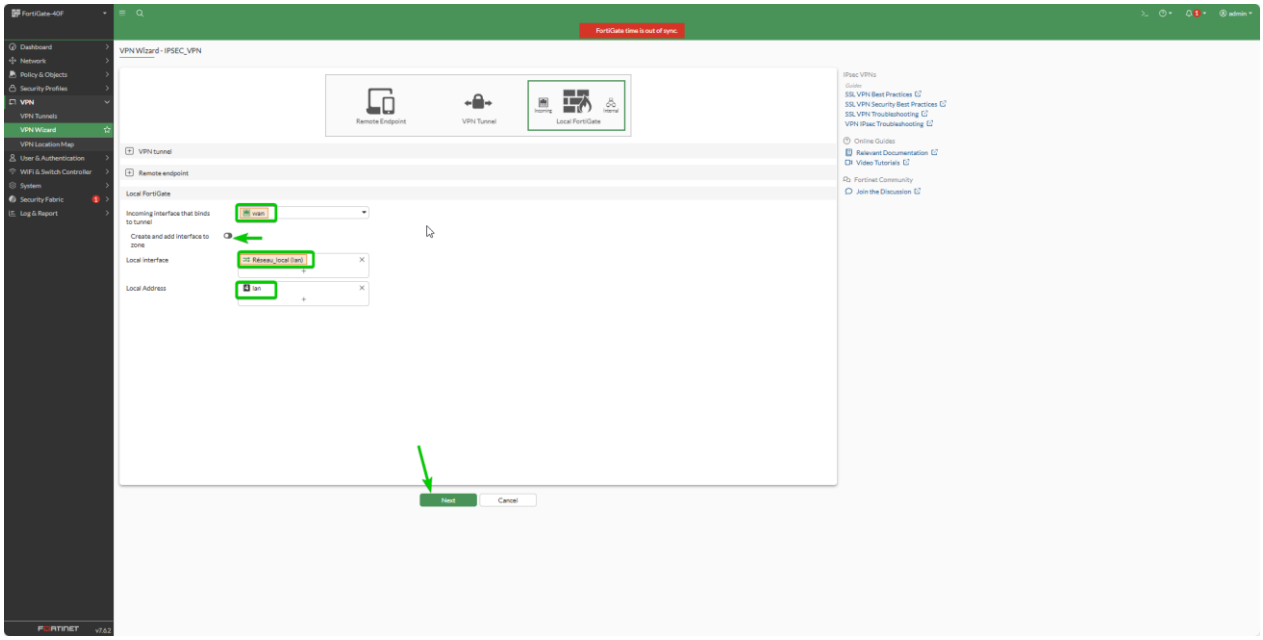


Puis se rendre dans **VPN Wizard**

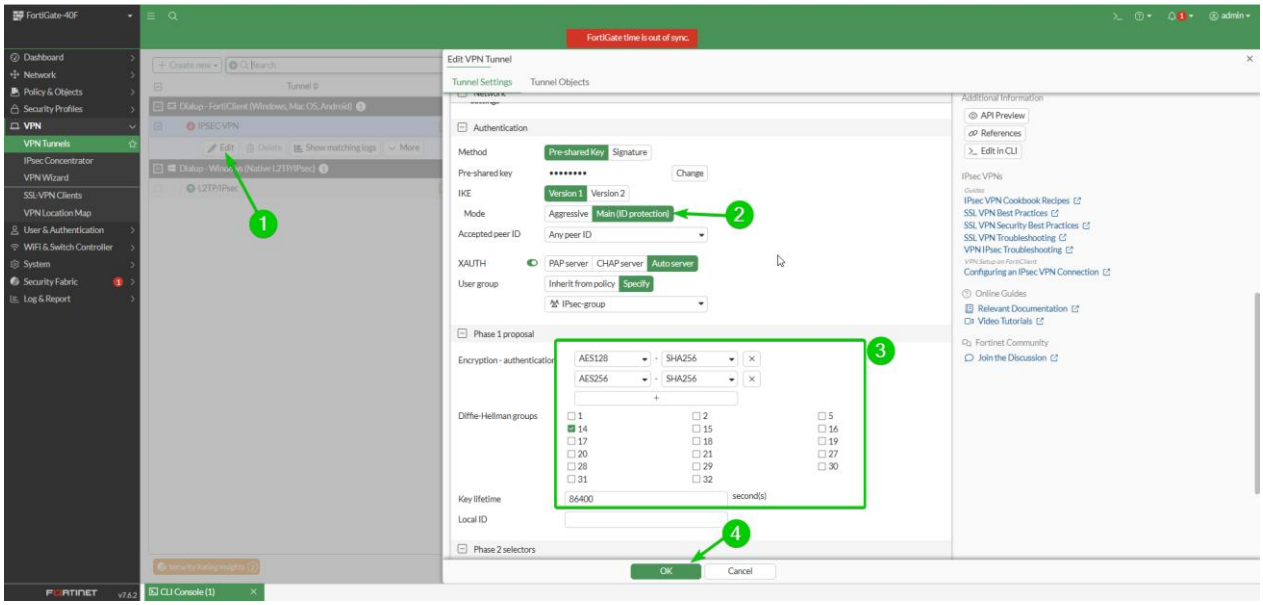

FortiGate-40F
FortiGate time is out of sync.
admin
Dashboard
Network
Policy & Objects
Security Profiles
VPN
VPN Tunnels
VPN Wizard
VPN Location Map
User & Authentication
WiFi & Switch Controller
System
Security Fabric
Log & Report
VPN Wizard
The IPsec VPN tunnel wizard gets you started with templates for common use cases. If the templates below do not fulfill your needs, fully custom tunnels can be set up. For convenience, it is also possible to start with a template and convert it to a fully custom tunnel after.
Select a Template
IPSEC_VPN
Site to Site
Offices in multiple, fixed locations can establish secure connections with each other. Branch offices can also access the main office's intranet.
Supported remote peers:
Remote Site
VPN Tunnel
Local FortiGate
Hub and Spoke with ADVPN
VPN connections radiate from a central FortiGate unit (the hub) to multiple remote peers (the spokes). Traffic can pass between private networks that are each behind a hub or remote peer (spoke). Additionally, spoke to spoke traffic is possible via ADVPN tunnels.
Supported remote peers:
Spokes
VPN Tunnels
Hub
Remote Access
Employees who need to access their company's network from off-site locations or users who want to securely connect to a private network from a public area frequently use this type of VPN.
Supported remote clients:
Remote Endpoints
VPN Tunnels
Local FortiGate
Begin
IPsec VPNs
SSL VPN Best Practices
SSL VPN Security Best Practices
SSL VPN Troubleshooting
VPN IPsec Troubleshooting
Online Guides
Relevant Documentation
Video Tutorials
Fortinet Community
Join the Discussion
1
2
3
4

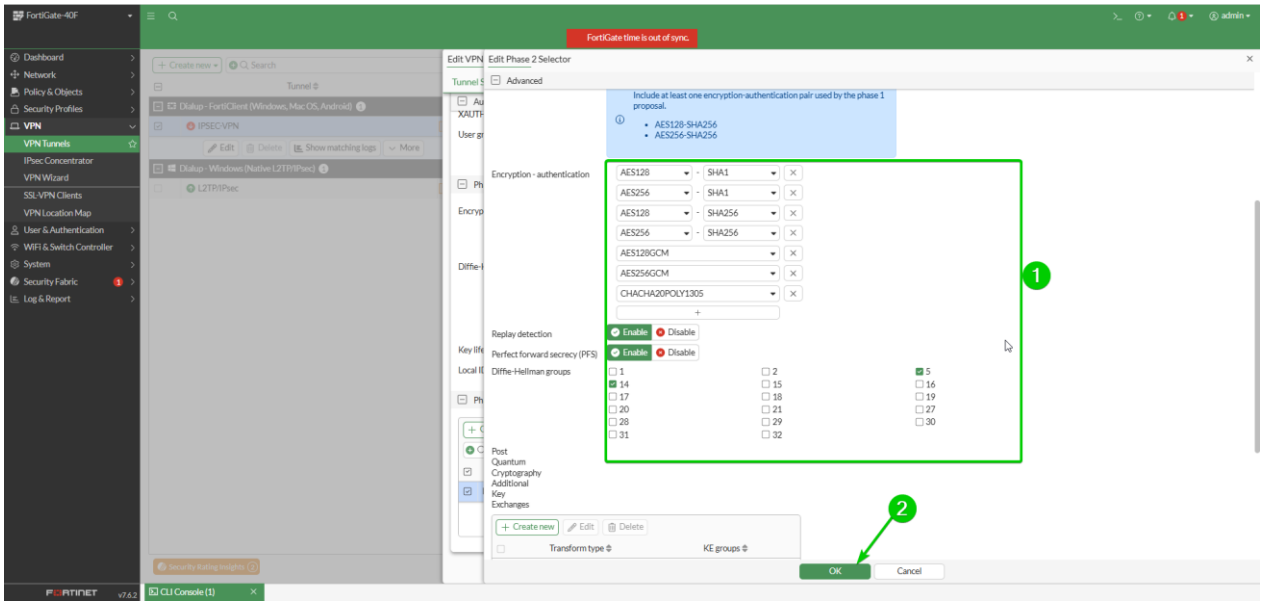

FortiGate-40F
FortiGate time is out of sync.
admin
VPN Wizard - IPSEC_VPN
Remote Endpoint
VPN Tunnel
Local FortiGate
VPN tunnel
VPN client type
Authentication method
Pre-shared key
Signature
Pre-shared key
password
IKE
Version 2
Version 1
NAT traversal
Enable
Disable
Forced
Keepalive frequency
10
User authentication method
Phase 1 interface
Inherit from policy
IPSEC_grp
DNS Server
Use System DNS
Specify
Enable IPv4 Split Tunnel
Next
Cancel
IPsec VPNs
SSL VPN Best Practices
SSL VPN Security Best Practices
SSL VPN Troubleshooting
VPN IPsec Troubleshooting
Online Guides
Relevant Documentation
Video Tutorials
Fortinet Community
Join the Discussion
1
2
3
4





Puis active le **main** mode et laisser les paramètres par défaut des encryptions.

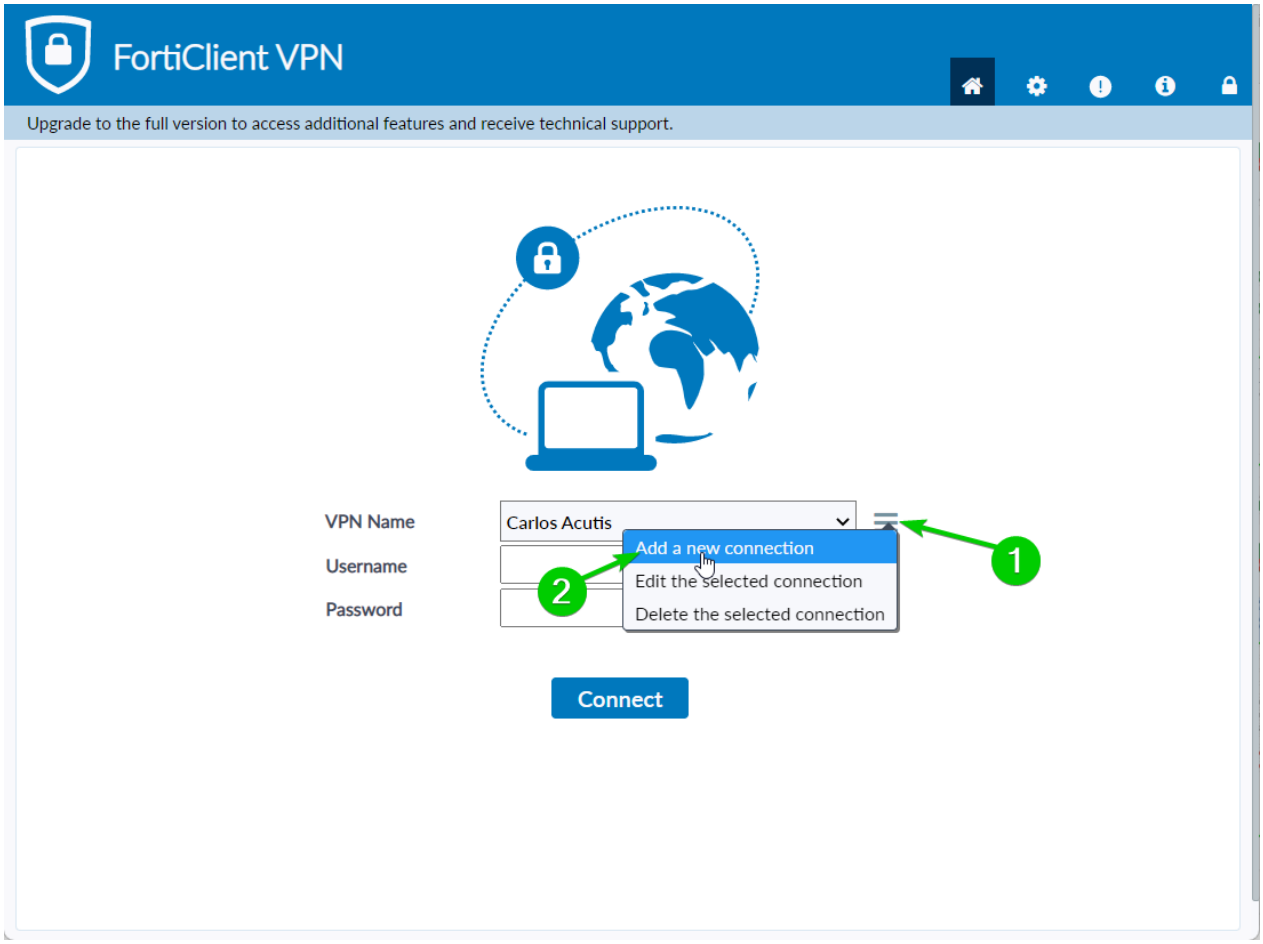




5.4.3.2 Configuration du FortiClient IPsec

Pour configurer le FortiClient il faut :

Se rendre dans **les trois petits points**-> **Add a new connection**



Puis sélectionner -> **IPsec VPN**

Et remplir les informations du VPN :

-Nom

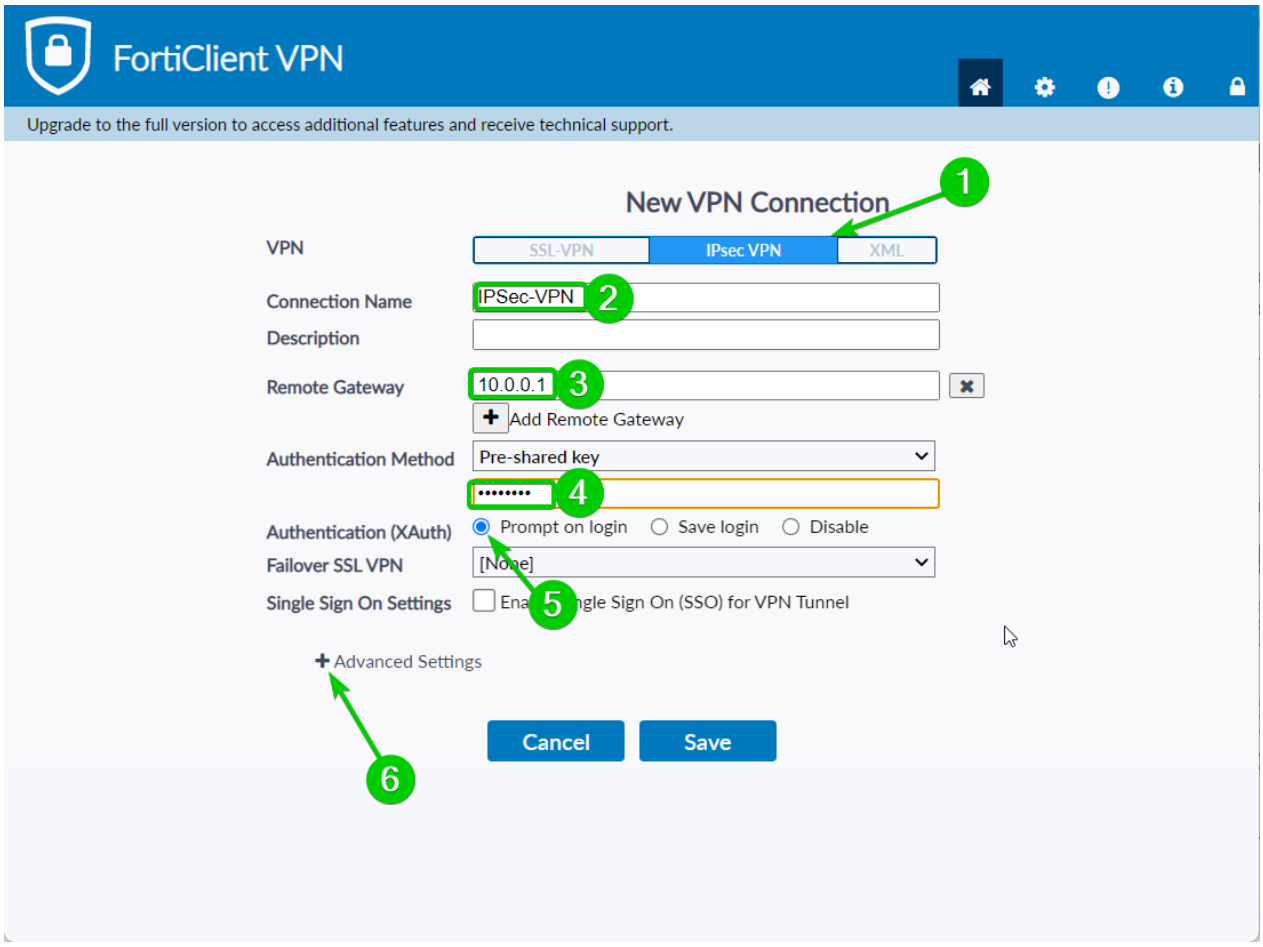
-@IP

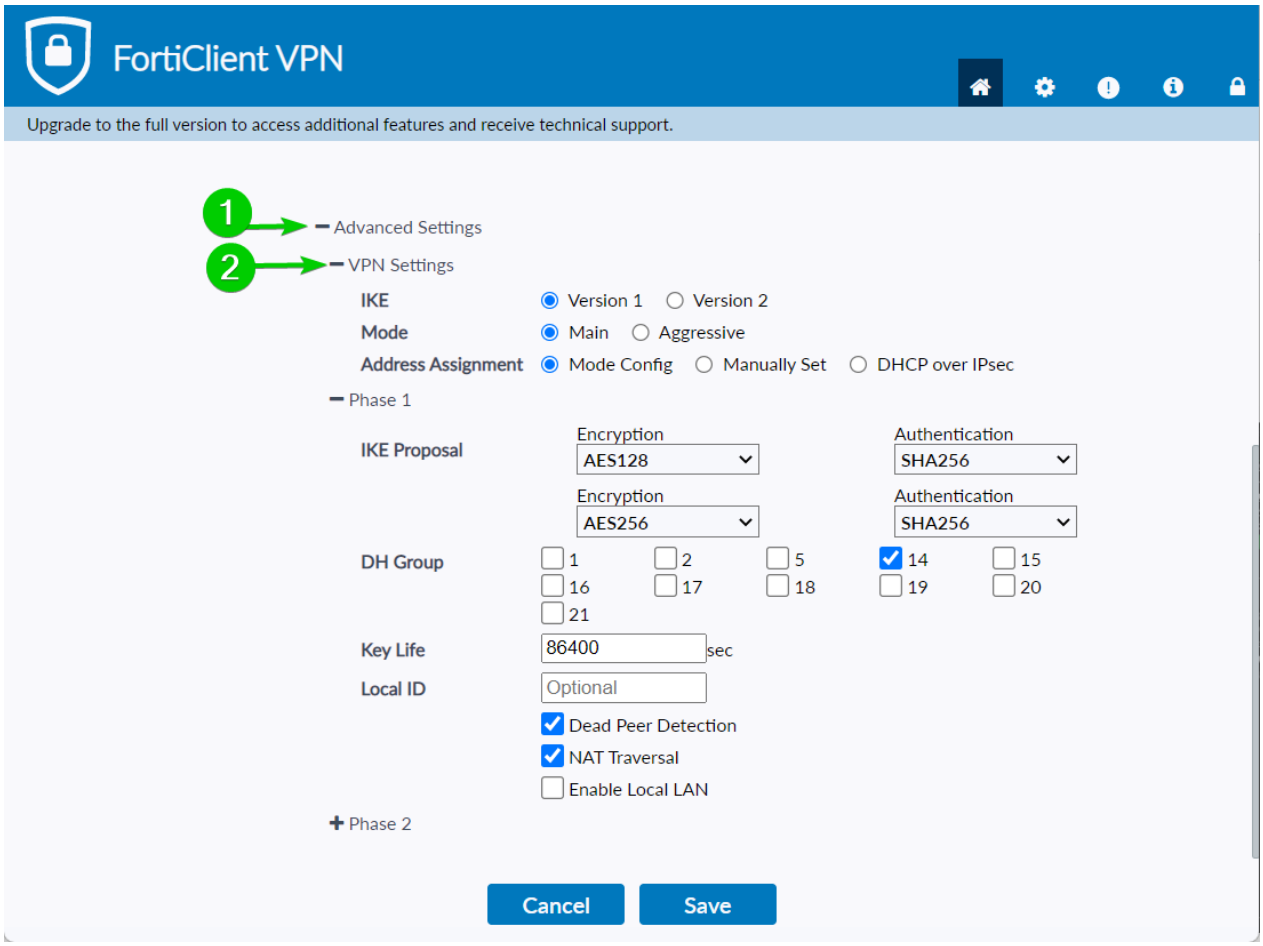
-PSK

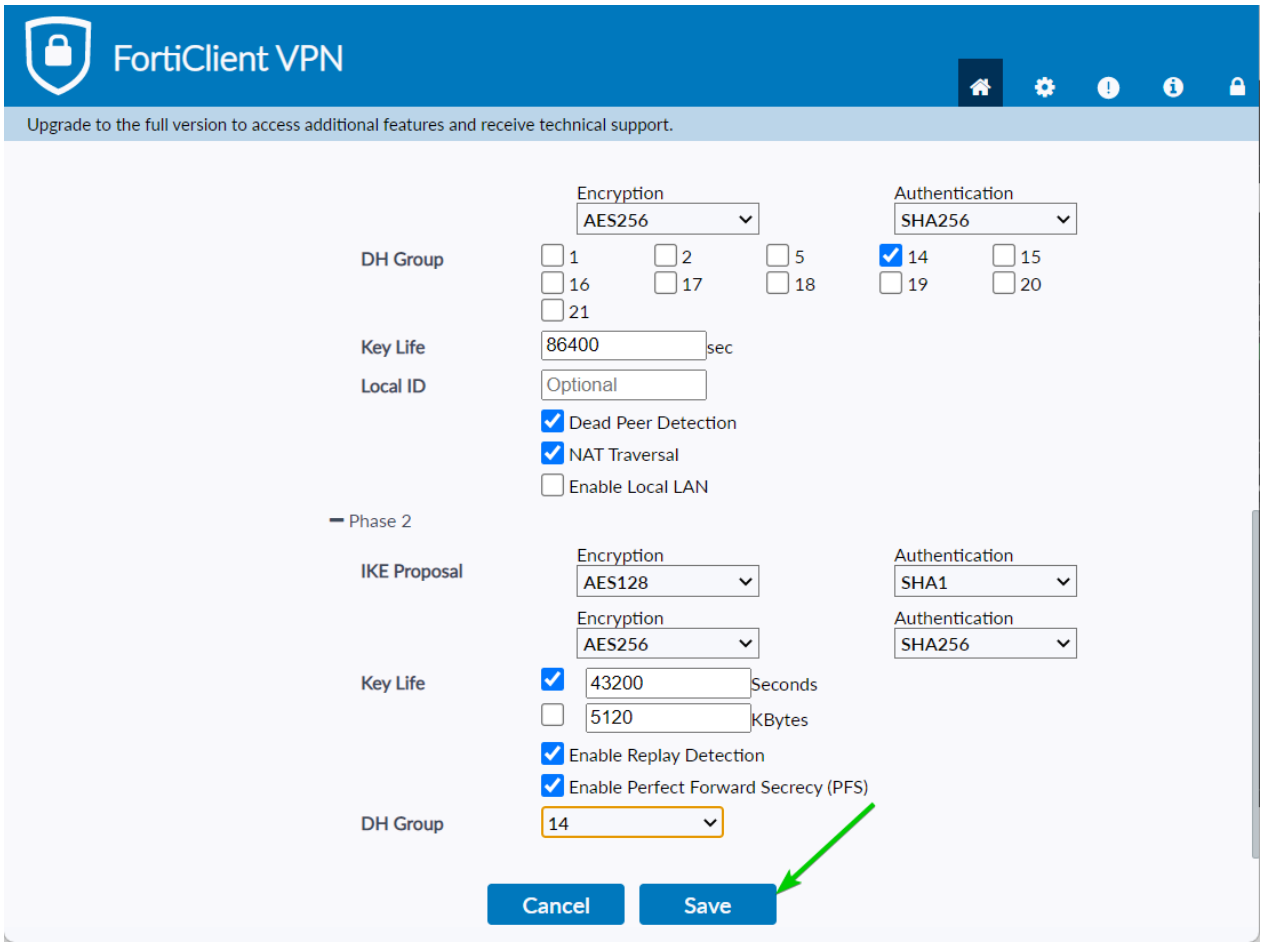
-Information de connexion

Puis sélectionner -> **Advanced Settings -> VPN Settings -> Phase 1**

Et remplir à l'identique les informations du tunnel VPN que nous avons configurer ci-dessus. Faire de même pour la phase 2.


FortiClient VPN
Upgrade to the full version to access additional features and receive technical support.
New VPN Connection
VPN
SSL-VPN
IPsec VPN
XML
Connection Name
IPSec-VPN
Description
Remote Gateway
10.0.0.1
Add Remote Gateway
Authentication Method
Pre-shared key
Authentication (XAuth)
Prompt on login
Save login
Disable
Failover SSL VPN
[None]
Single Sign On Settings
Advanced Settings
Cancel
Save
1
2
3
4
5
6


FortiClient VPN
Upgrade to the full version to access additional features and receive technical support.
1
Advanced Settings
2
VPN Settings
IKE
Version 1
Version 2
Mode
Main
Aggressive
Address Assignment
Mode Config
Manually Set
DHCP over IPsec
Phase 1
IKE Proposal
Encryption
AES128
Authentication
SHA256
Encryption
AES256
Authentication
SHA256
DH Group
1
2
5
14
15
16
17
18
19
20
21
Key Life
86400
sec
Local ID
Optional
Dead Peer Detection
NAT Traversal
Enable Local LAN
Phase 2
Cancel
Save



Une fois cela fait cliquer sur -> **Save**

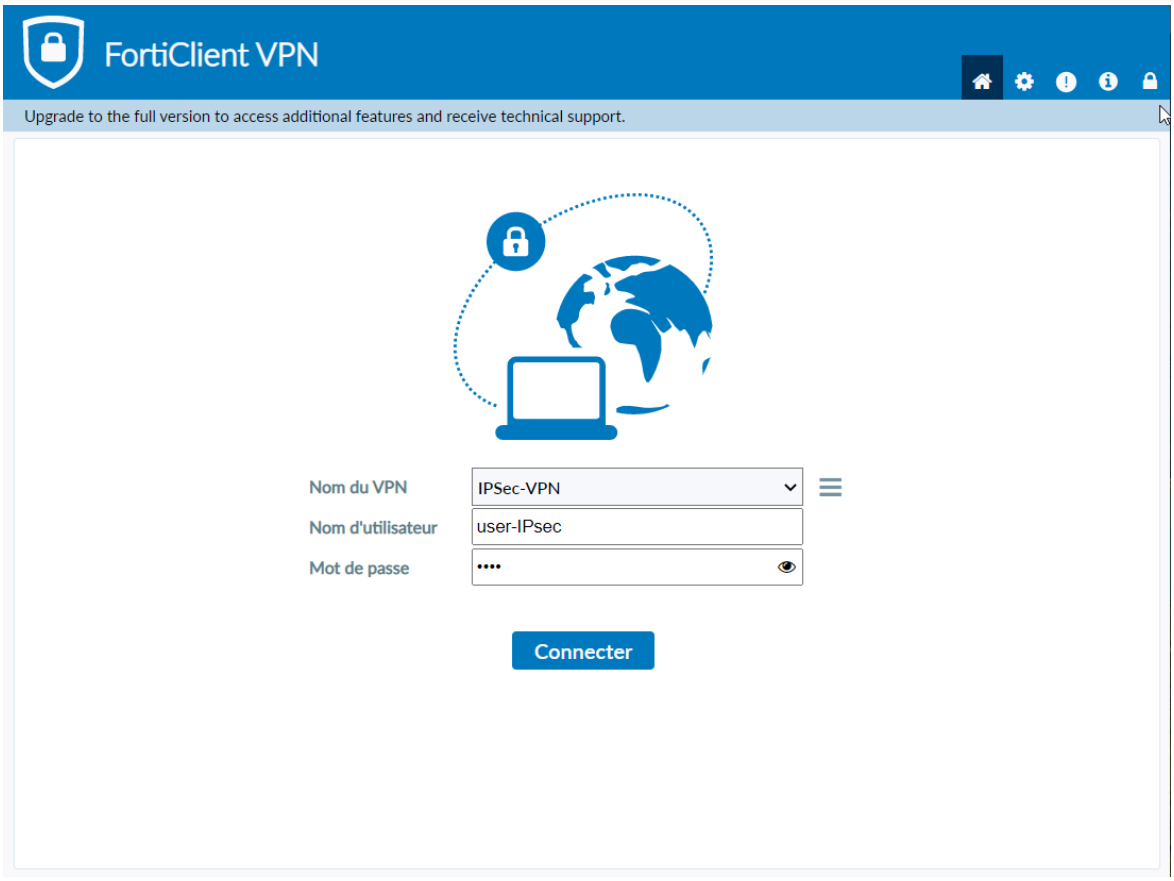
5.4.3.3 Test de connexion Utilisateur IPsec

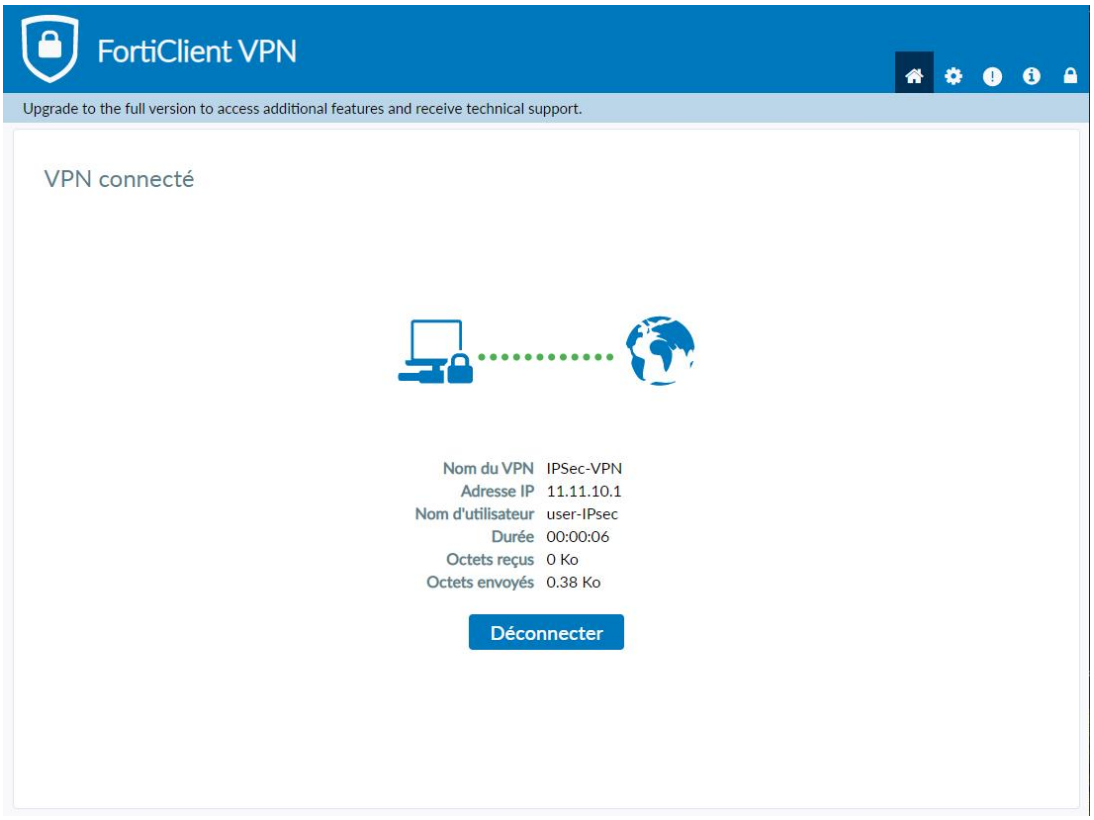
Remplir les informations du compte que nous avons créé précédemment

ID : **user-IPsec**

MDP : **user**

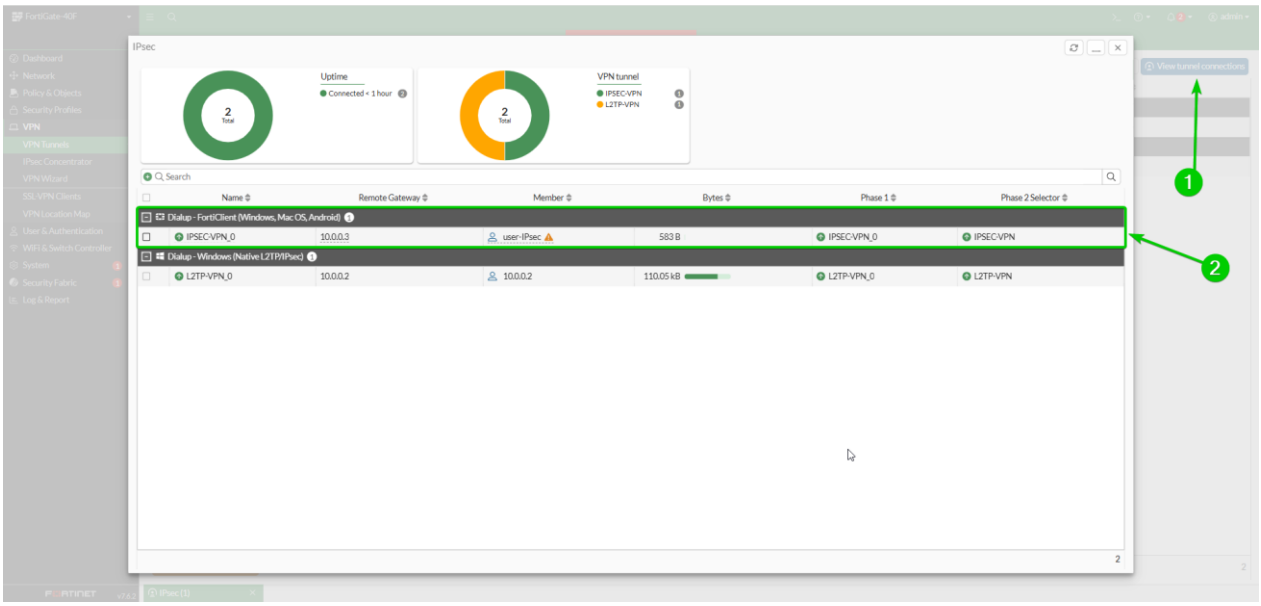
Puis cliquer sur connecter


FortiClient VPN
Upgrade to the full version to access additional features and receive technical support.
Nom du VPN
IPSec-VPN
Nom d'utilisateur
user-IPsec
Mot de passe
Connecter


FortiClient VPN
Upgrade to the full version to access additional features and receive technical support.
VPN connecté
Nom du VPN IPSec-VPN
Adresse IP 11.11.10.1
Nom d'utilisateur user-IPsec
Durée 00:00:06
Octets reçus 0 Ko
Octets envoyés 0.38 Ko
Déconnecter

5.4.3.4 Rapport de Test du VPN IPsec

Sur l'interface de Fortinet, nous pouvons voir que l'hôte est bien connecté, donc la connexion VPN à bien fonctionner.



J'effectue un ipconfig pour voir ma configuration :

1 : Carte Ethernet en dehors du réseau

2 : Carte Ethernet FortiClient

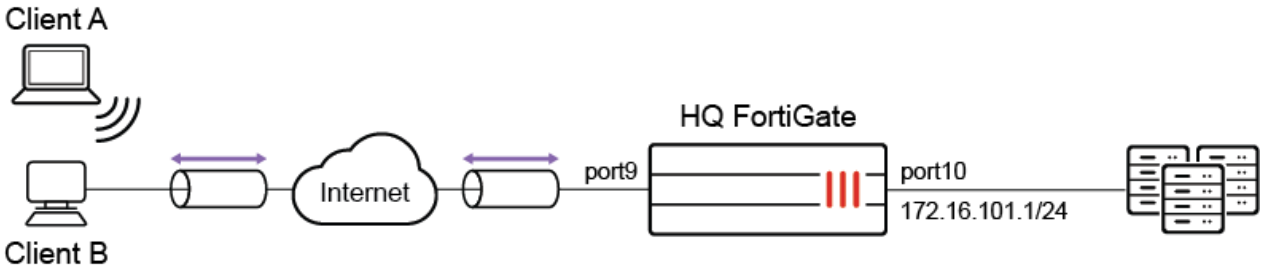
```
Carte Ethernet Ethernet 2 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::6b07:68a0:ec3e:d8c6%4
   Adresse IPv4. . . . . . . . . . . . . .: 11.11.10.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :

Carte Ethernet Ethernet :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte Ethernet Ethernet 3 :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte Ethernet Ethernet 4 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::69fc:d29e:1973:b703%18
   Adresse IPv4. . . . . . . . . . . . . .: 10.0.0.3
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . : 10.0.0.1
```

Puis-je **ping du PC** à la passerelle du **réseau local** pour vérifier son bon fonctionnement. Nous pouvons voir que la passerelle **répond bien aux pings**, donc la configuration VPN fonctionne.

```
C:\Users\c.caron>ping 192.168.1.99

Envoi d'une requête 'Ping'  192.168.1.99 avec 32 octets de données :
Réponse de 192.168.1.99 : octets=32 temps=1 ms TTL=255
Réponse de 192.168.1.99 : octets=32 temps=1 ms TTL=255
Réponse de 192.168.1.99 : octets=32 temps=2 ms TTL=255
Réponse de 192.168.1.99 : octets=32 temps=1 ms TTL=255

Statistiques Ping pour 192.168.1.99:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms

C:\Users\c.caron>
```

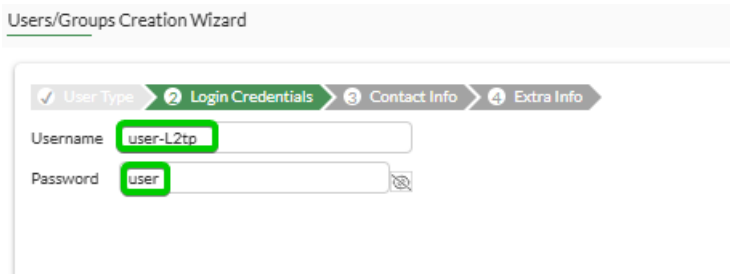
5.4.3.5 Configuration du user et du tunnel L2TP over IPsec

Pour pouvoirs connecter le NAS au VPN il faut rajouter **le L2TP au tunnel IPSEC** existant comme le schéma ci-dessous :

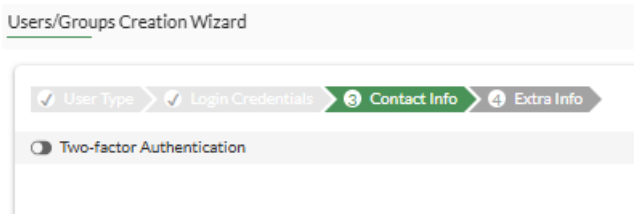


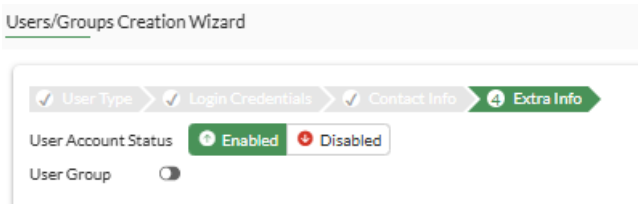
Commençons par crée l'utilisateur :

Se rendre dans **User Definition** -> **Create user** -> **Local user** -> **Next**



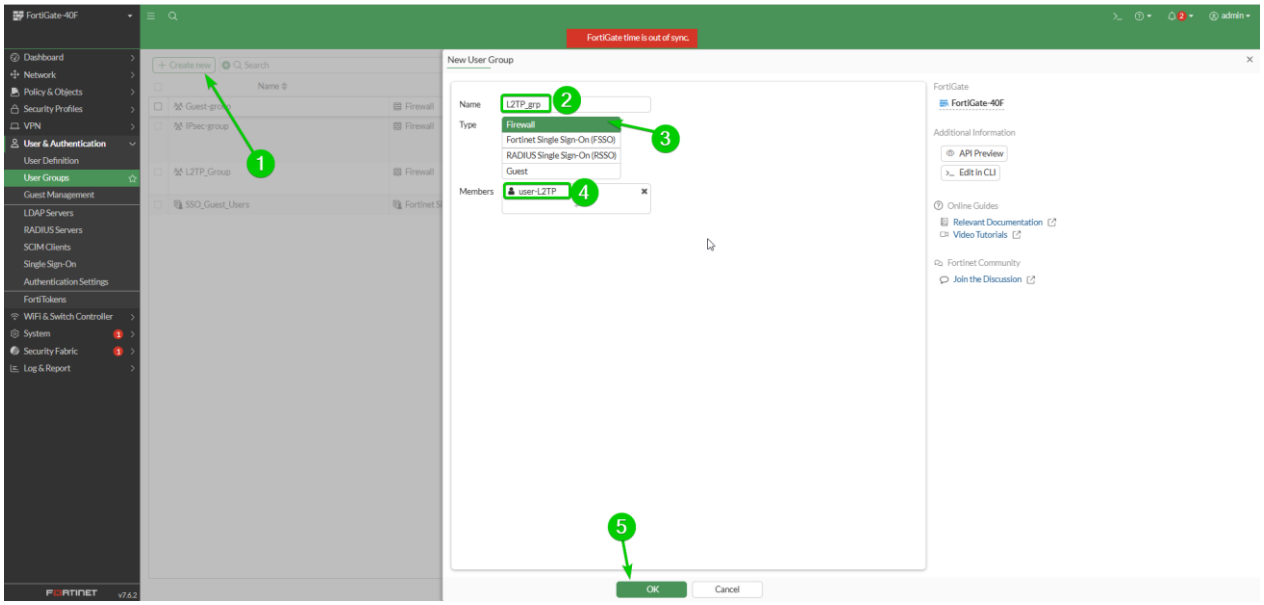
Désactiver l'authentification à double facteur pour la connexion de **l'utilisateur**





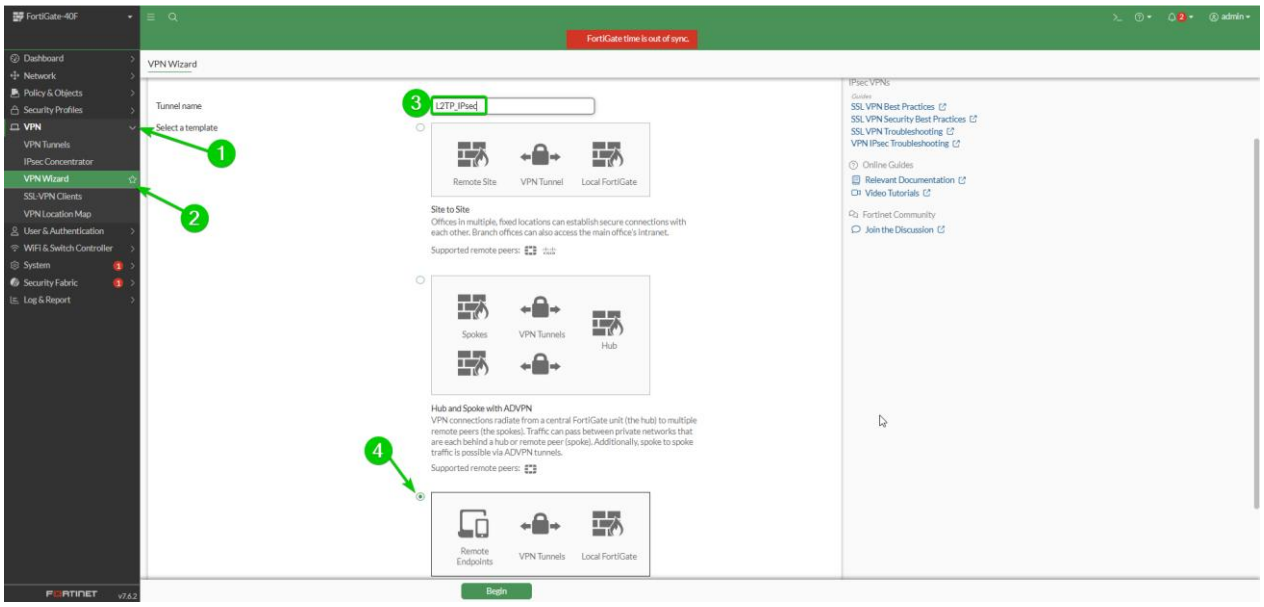
Puis crée un groupe :

User Groups -> **Create New** -> remplir les informations -> **ok**

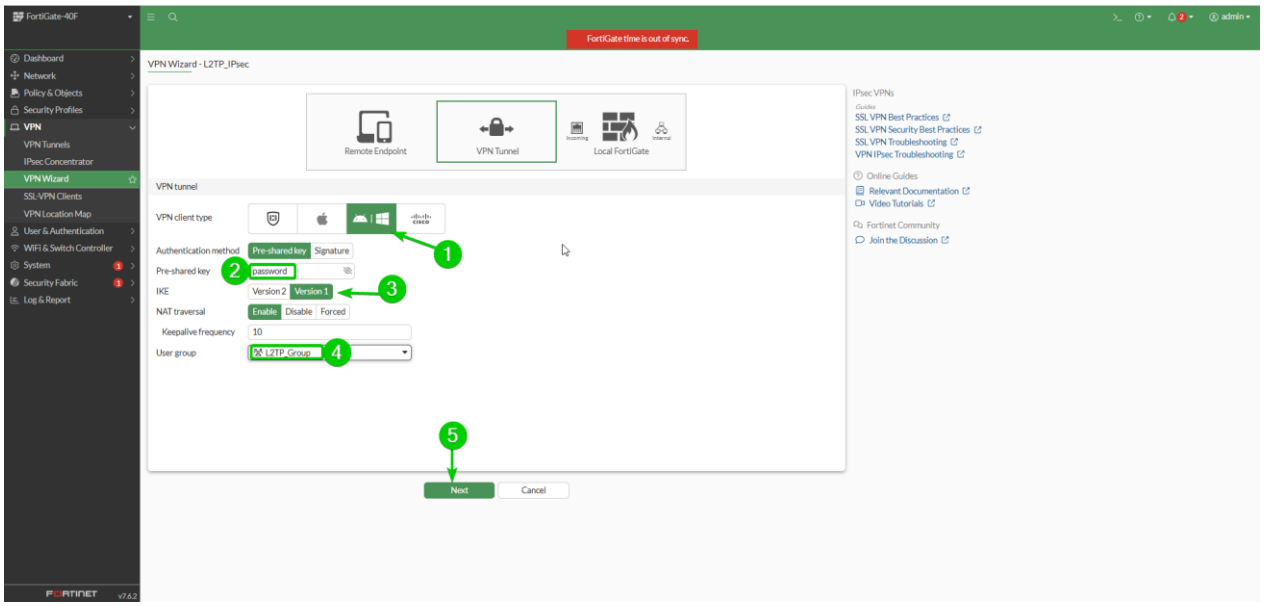


Nous allons maintenant crée le tunnel L2TP :

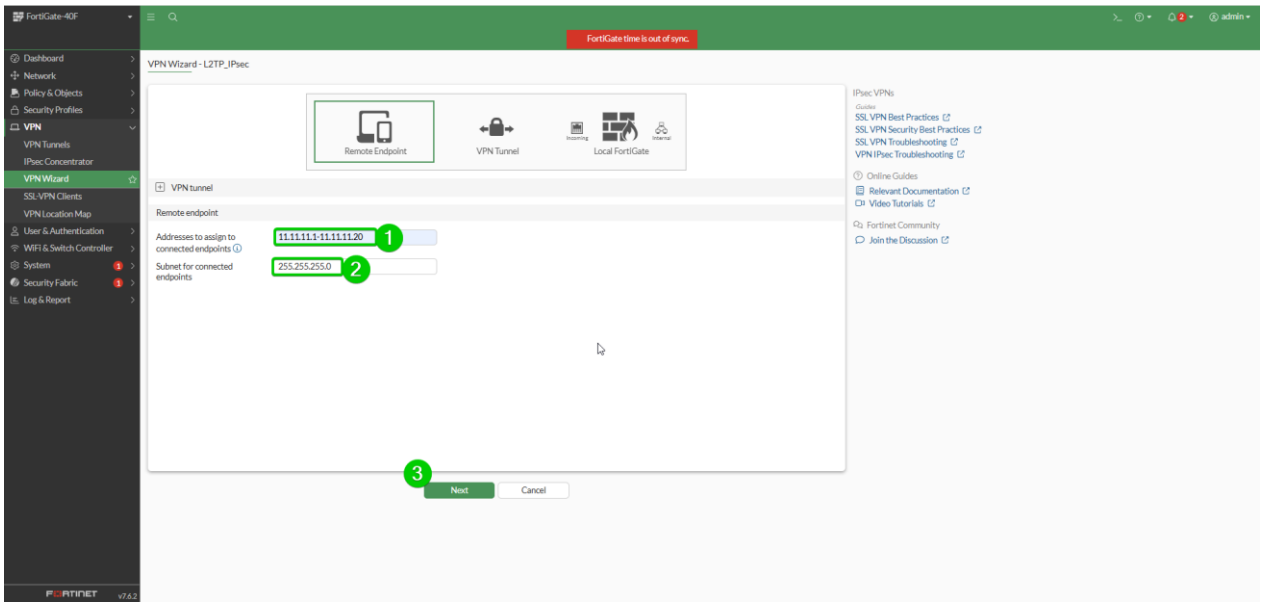
Se rendre dans **VPN** -> **VPN Wizzard** -> **Create New**



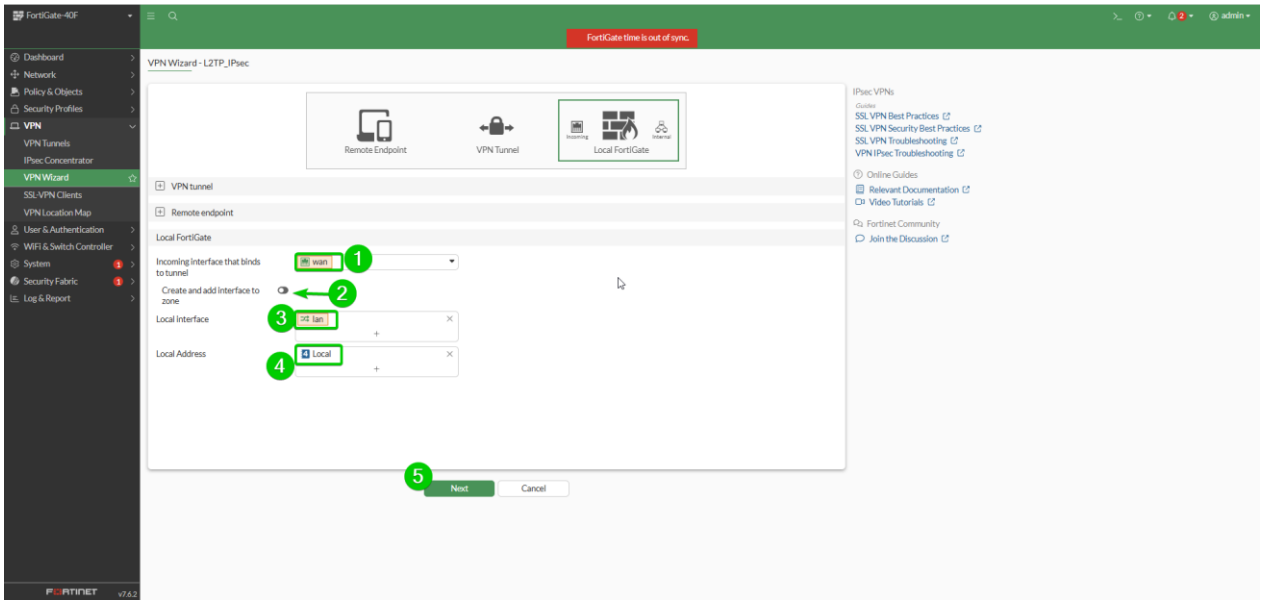
Il est nécessaire de remplir les différentes informations de configuration pour le client VPN, il faut obligatoirement sélectionner le type de client VPN approprié, à savoir **Android & Windows natif (L2TP)**, avant de compléter les autres paramètres requis pour assurer le bon fonctionnement de la connexion avec le NAS.



Pour éviter tout conflit d'adressage, j'ai ensuite configuré une plage d'adresses IP dédiée au VPN. Celle-ci doit être différente de celle utilisée par le réseau local et du VPN IPsec déjà en place. J'ai donc choisi la plage suivante : **11.11.11.1 à 11.11.11.20/24**, ce qui permet d'éviter les conflits.



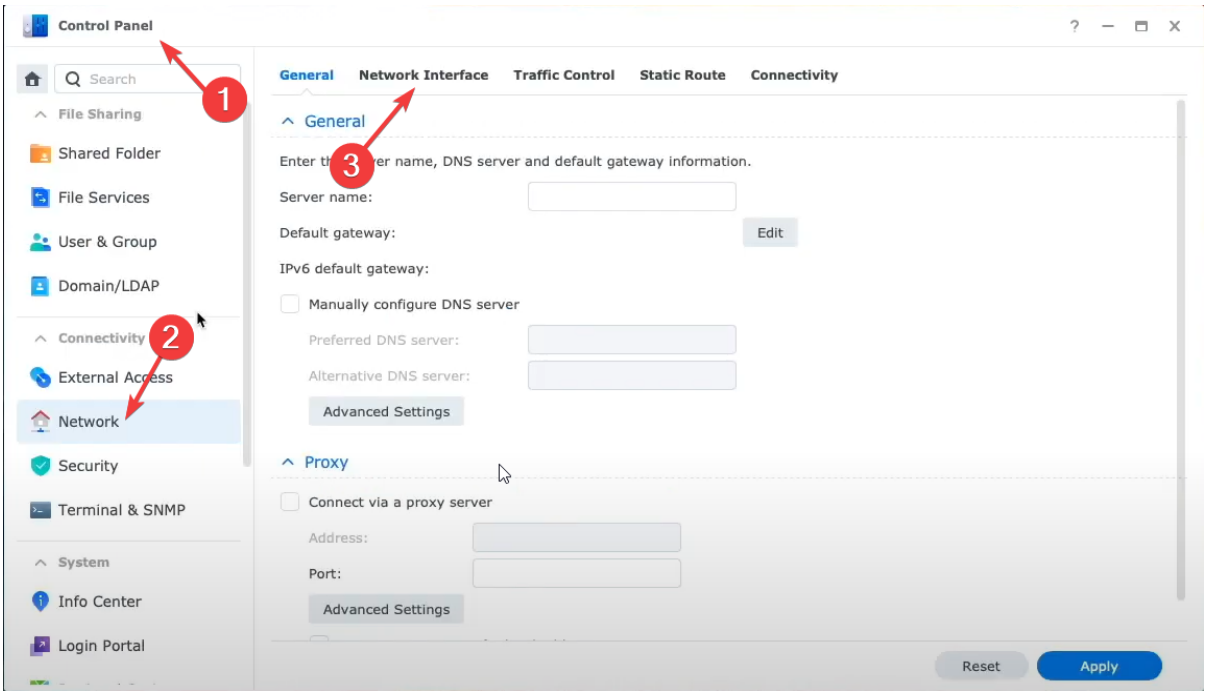
Les connexions VPN vont arriver de l'interface **WAN** vers le réseau local. Il est donc nécessaire de renseigner les paramètres de configuration en conséquence, comme montré sur la capture d'écran.



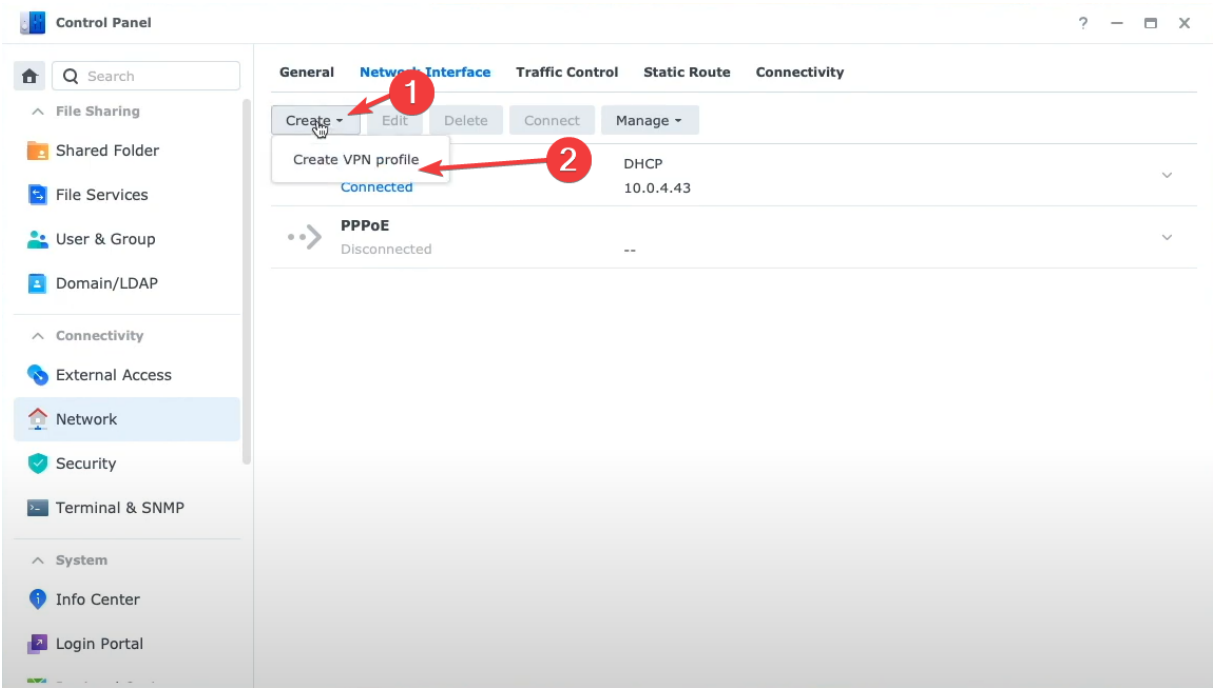
5.4.3.6 Configuration du NAS en L2TP

Une fois cela fait, il faut configurer le NAS.

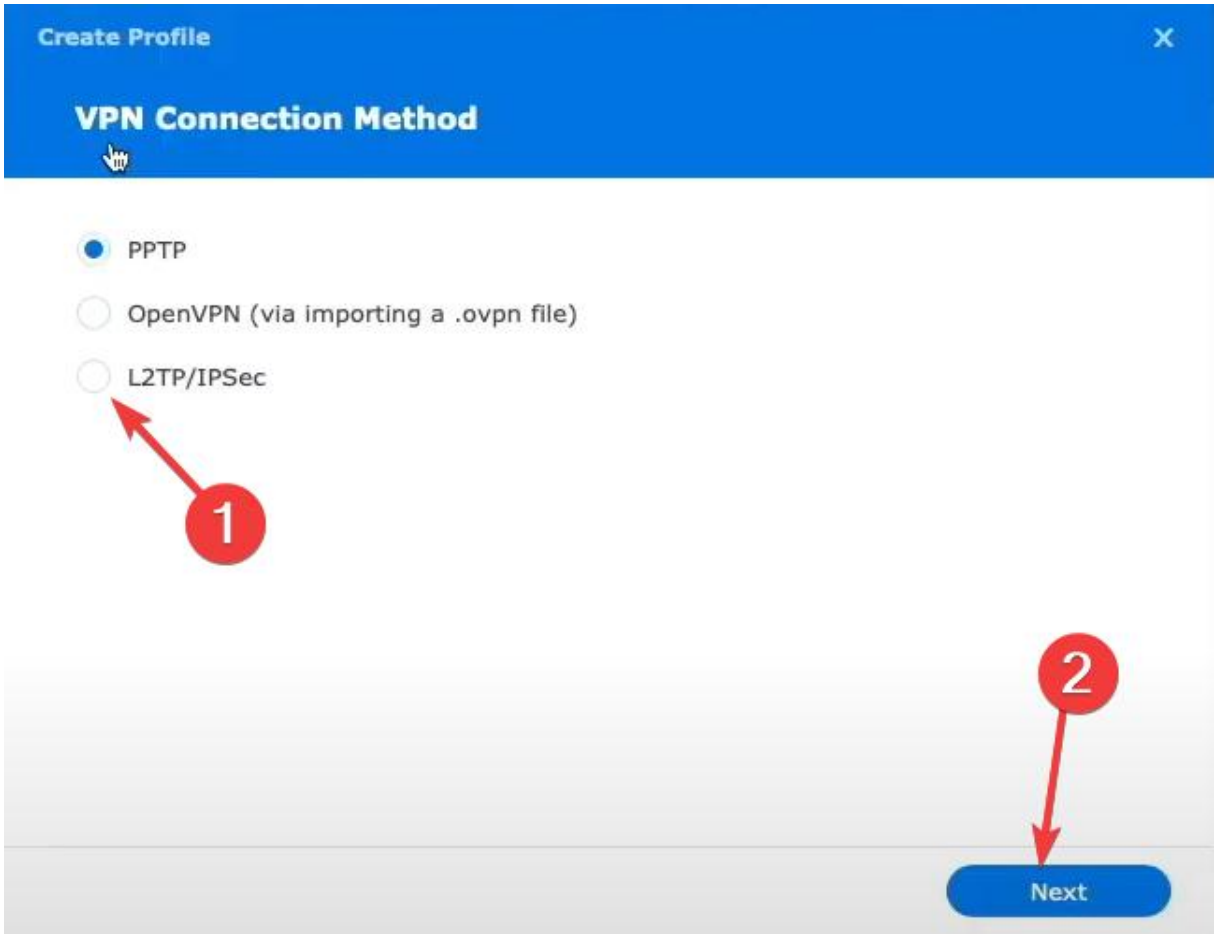
Aller dans **Control Panel**-> **Network** -> **Network Interface**

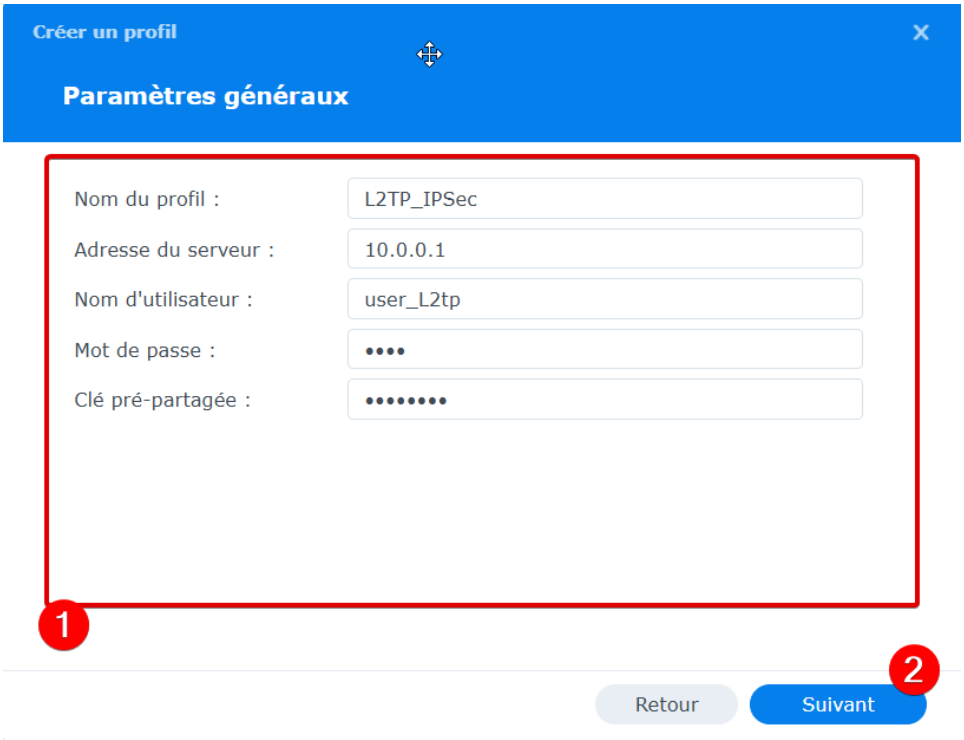


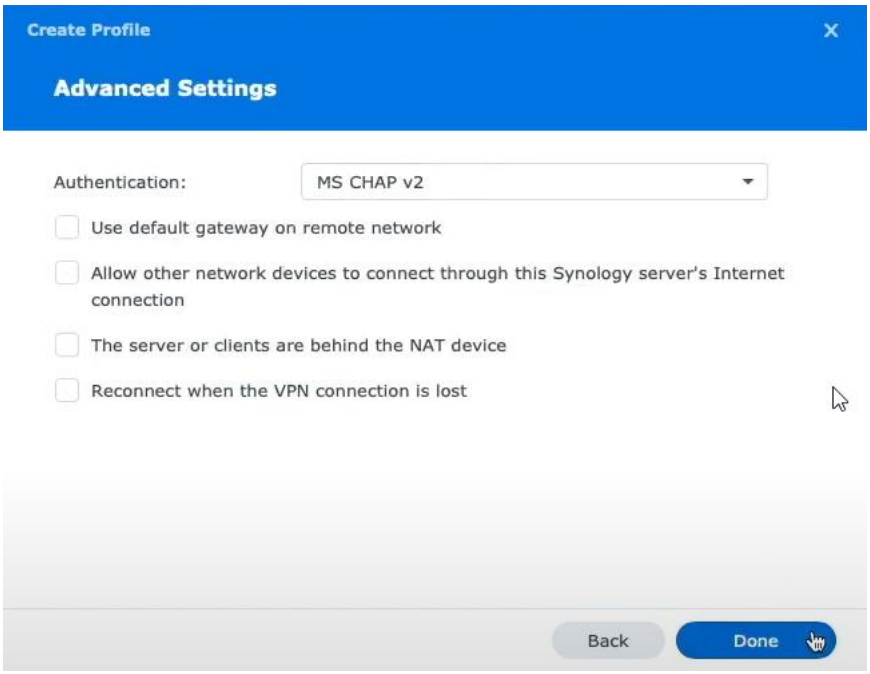
Puis aller dans : **Create**-> **Create VPN Profile**



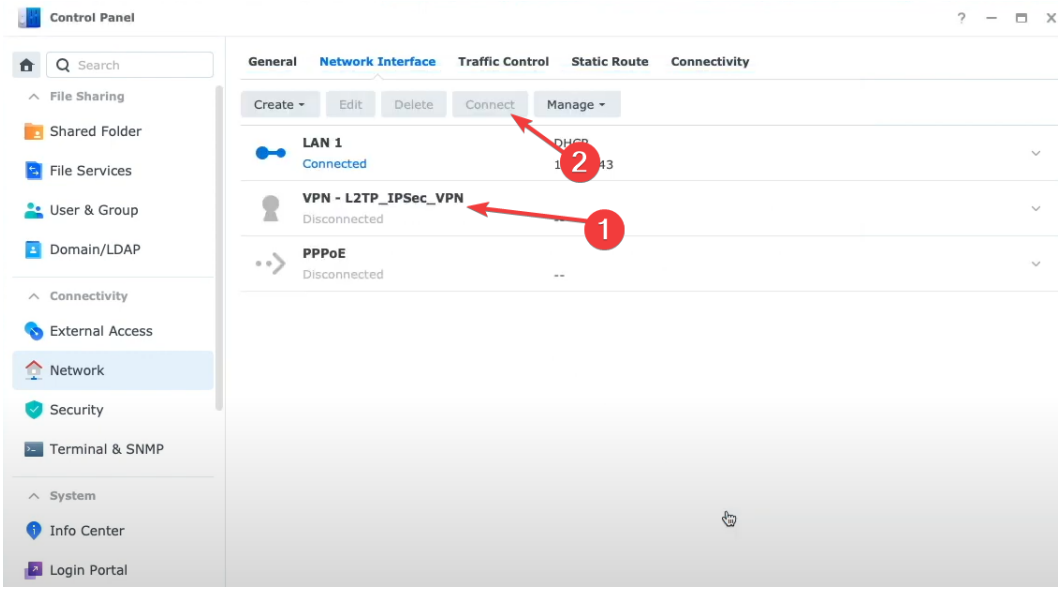
Puis appuyer sur l'option : **L2TP/IPSec**







5.4.3.7 Test de connexion Utilisateur L2TP



La négociation IPSec a échoué. Veuillez vérifier ce qui suit : la clé pré-partagée est correcte. Le port utilisé pour le service VPN est configuré sur des périphériques de réseau (tels que le pare-feu, NAT ou des routeurs) entre le DiskStation et le serveur VPN, ou activer l'option "Le serveur est derrière un appareil NAT".

Temps de connexion : --
Passerelle : --
Envoyé : --
Reçu : --

5.4.3.8 Résolution du problème connexion L2TP

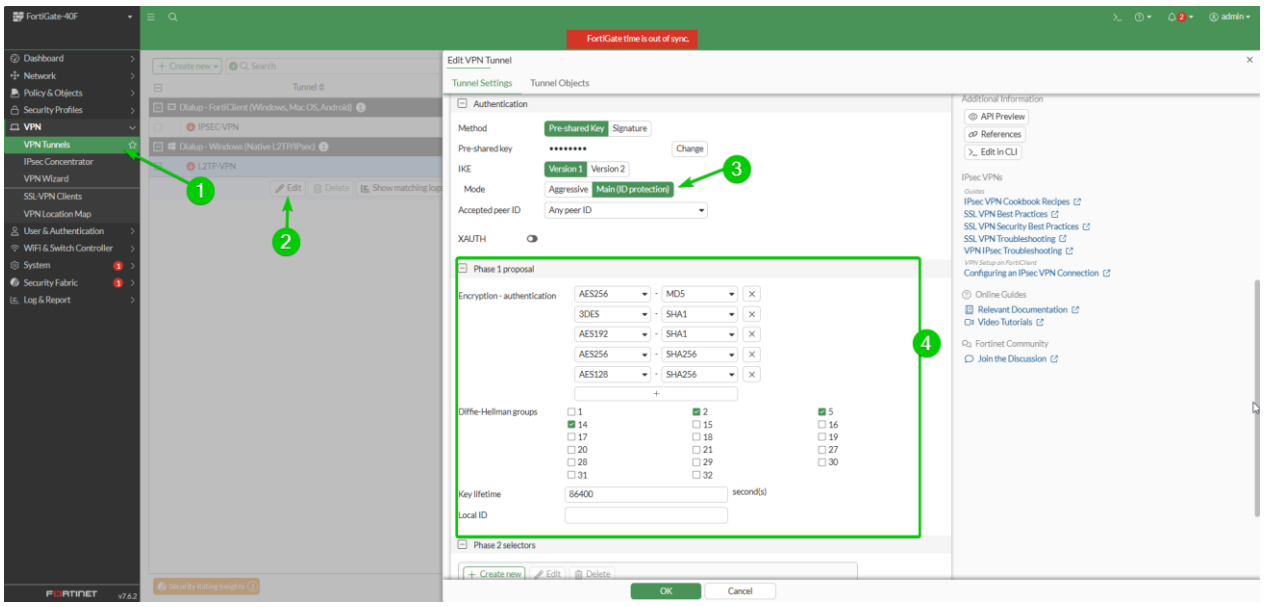
Apres l'erreur rencontré lors de la création VPN j'ai regardé toutes les documentations de Synology, Fortinet ...

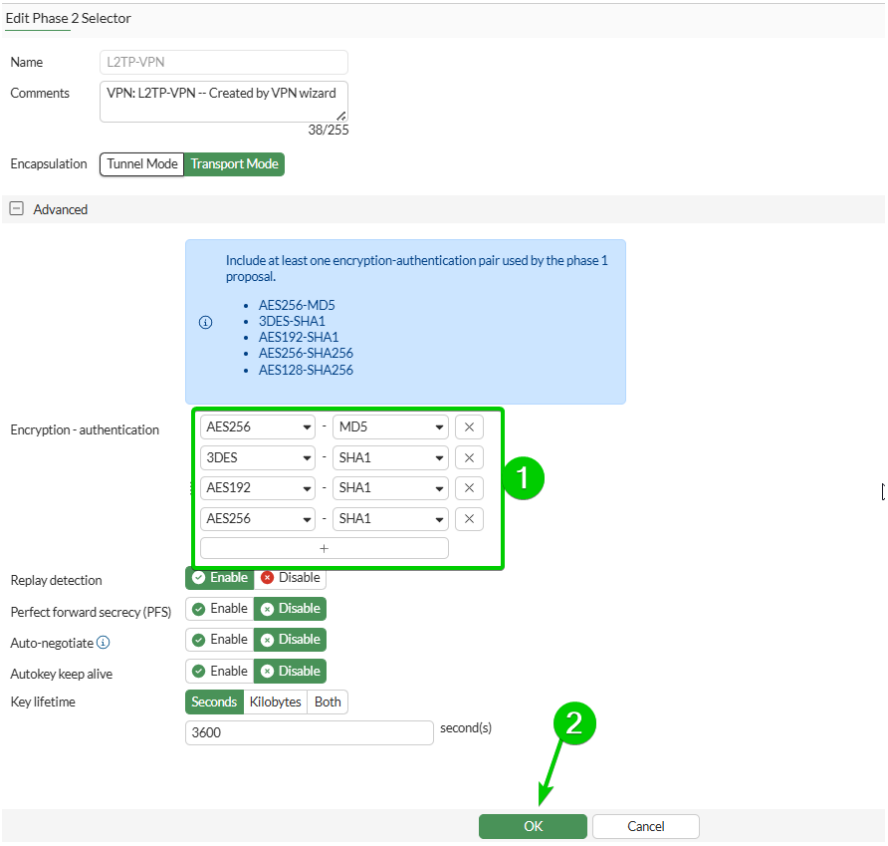
Puis j'ai regardé les logs du Fortinet lors de la connexion et une ligne d'erreur est ressorti « **No SA chose** » en me renseignant, j'ai lu qu'il s'agissait d'une erreur de configuration du VPN

```
ike V=root:0:1b6f9033764a1e5f/0000000000000000:8:        type=OAKLEY_HASH_ALG,
val=MD5.
ike V=root:0:1b6f9033764a1e5f/0000000000000000:8:        type=AUTH_METHOD,
val=PRESHARED_KEY.
ike V=root:0:1b6f9033764a1e5f/0000000000000000:8:        type=OAKLEY_GROUP,
val=MODP1024.
ike V=root:0:1b6f9033764a1e5f/0000000000000000:8: ISAKMP SA lifetime=3600
ike V=root:0:1b6f9033764a1e5f/0000000000000000:8: negotiation failure
ike V=root:Negotiate ISAKMP SA Error:
ike V=root:0:1b6f9033764a1e5f/0000000000000000:8: no SA proposal chosen
```

Je suis donc retournée configurer le tunnel VPN avec les bons paramètres car si les paramètres de configuration ne sont pas identiques entre le NAS et le Fortinet, ils ne pourront pas établir une communication sécurisée, car chacun chiffrera les échanges selon ses propres réglages.

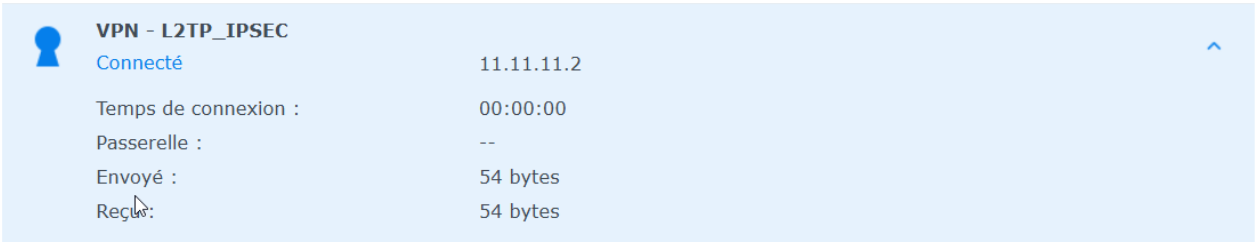
En l'absence de correspondance, les données ne seront pas déchiffrables correctement, ce qui rendra toute communication impossible.





5.4.3.8 Test de connexion après résolution du problème de connexion

Puis j'ai retenté une connexion et elle a réussi.



5.4.3.8 Test de communication après résolution du problème de connexion

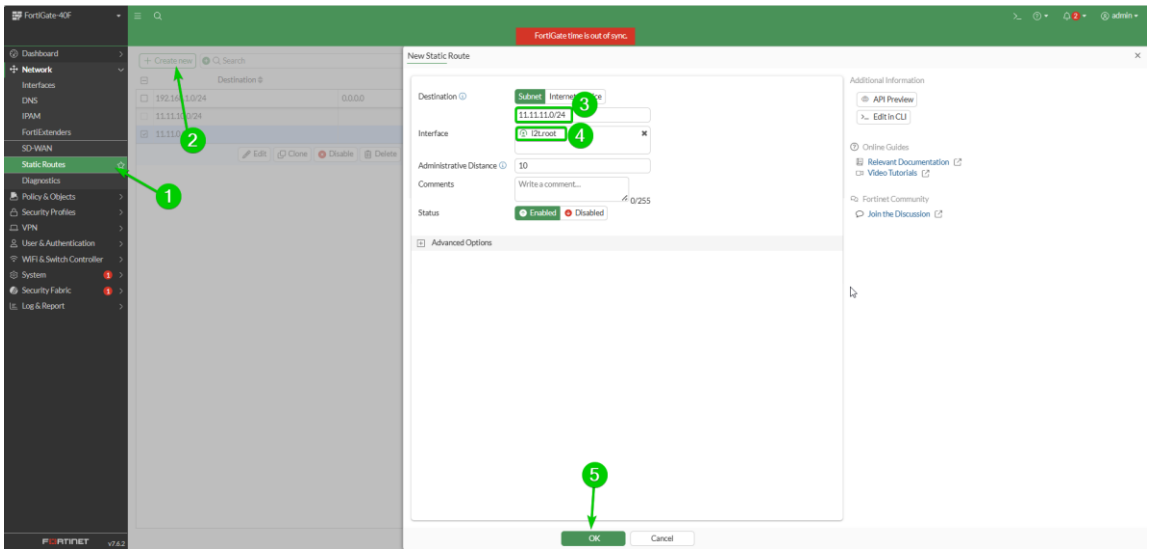
Pour vérifier que je pouvais bien joindre le NAS, j'ai tenté un ping entre mon Laptop et le NAS, malheureusement il n'a pas abouti.

```
C:\Users\caron>ping 11.11.11.2 -S 192.168.1.5

Pinging 11.11.11.2 from 192.168.1.5 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 11.11.11.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Donc j'ai essayé un ping directement depuis le Fortinet mais là encore il n'a pas abouti.

```
FortiGate-40F # execute ping 11.11.11.2
PING 11.11.11.2 (11.11.11.2): 56 data bytes
sendmsg failed: 101(Network is unreachable)
sendmsg failed: 101(Network is unreachable)
sendmsg failed: 101(Network is unreachable)
sendmsg failed: 101(Network is unreachable)
sendmsg failed: 101(Network is unreachable)

--- 11.11.11.2 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

Je suis donc allé voir dans les routes statiques du routeur mais elle n'existait pas, j'ai donc dû créer une route statique : aller dans -> **Network** -> **Static Routes** -> **Create New** -> rentrer le Subnet de Destination -> et l'interface pour joindre ce Subnet



Puis j'ai re tenter de ping depuis le Fortinet et j'ai eu des retours du NAS

```
FortiGate-40F # execute ping 11.11.11.2
PING 11.11.11.2 (11.11.11.2): 56 data bytes
64 bytes from 11.11.11.2: icmp_seq=0 ttl=64 time=0.4 ms
64 bytes from 11.11.11.2: icmp_seq=1 ttl=64 time=0.3 ms
64 bytes from 11.11.11.2: icmp_seq=2 ttl=64 time=0.3 ms
64 bytes from 11.11.11.2: icmp_seq=3 ttl=64 time=0.2 ms
64 bytes from 11.11.11.2: icmp_seq=4 ttl=64 time=0.3 ms

--- 11.11.11.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.3/0.4 ms
```

J'ai donc réessayé le ping de mon PC vers le NAS, mais là encore le ping n'aboutissait pas.

```
C:\Users\caron>ping 11.11.11.2 -S 192.168.1.5

Pinging 11.11.11.2 from 192.168.1.5 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 11.11.11.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Je me suis donc replongé dans les logs du Fortinet pour comprendre les causes de ce dysfonctionnement.

Pour ce faire j'ai rentré des commandes pour filtrer les trames réseau, pour écouter tous le trafic ICMP (proto 1) de l'@ip 192.168.1.5 (mon poste) et j'ai mis une limite de 50 trames.

Cette capture avait pour but de comprendre l'erreur en regardant les logs lors d'un ping infini.

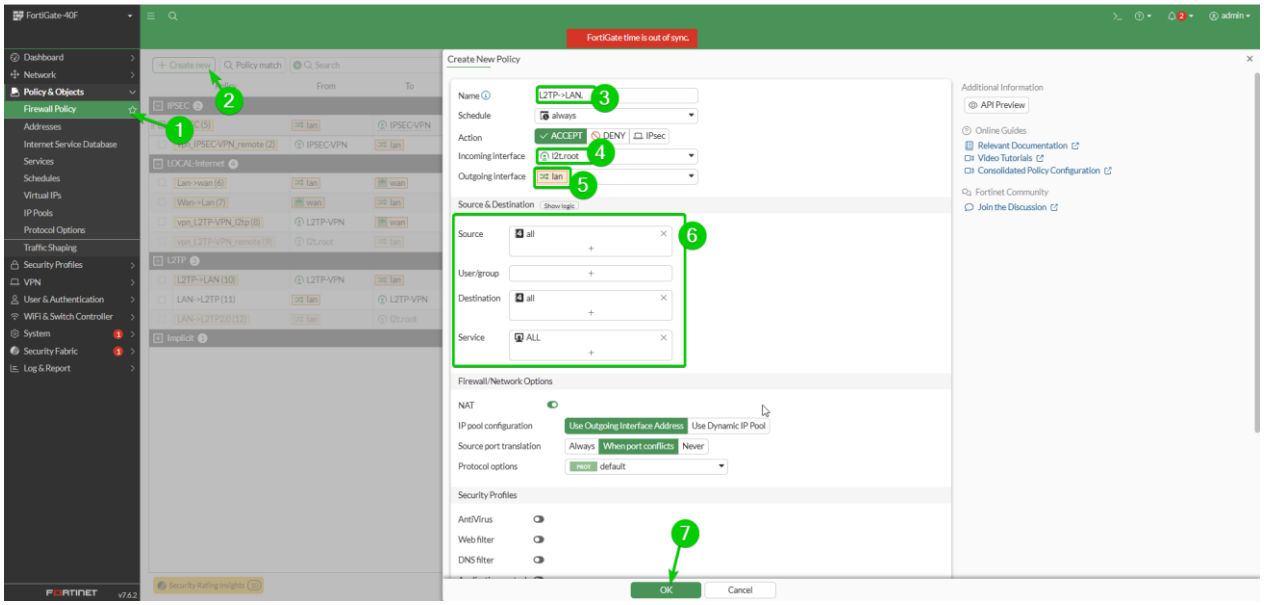
L'erreur **"Denied by forward policy check"** m'a permis d'identifier un oubli dans la configuration de la politique du pare-feu. En effet, la règle par défaut étant **« deny any any »**, toute connexion non explicitement autorisée est automatiquement bloquée.

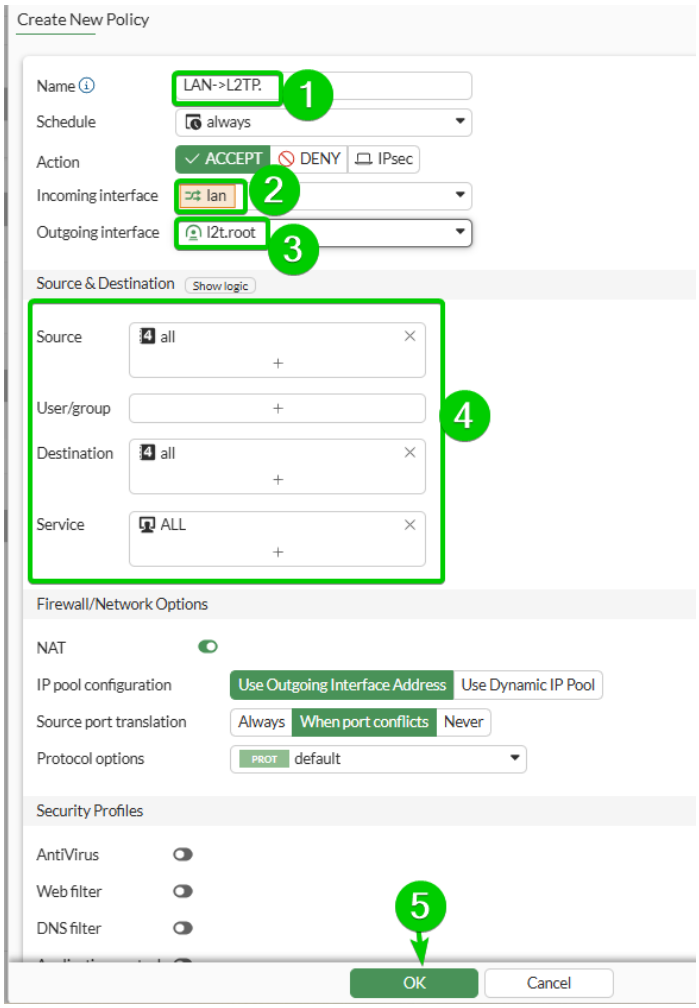
Si aucune politique n'est définie, elle est considérée comme inexistante, et donc rejetée par la règle par défaut.

```
FortiGate-40F # diagnose debug reset

FortiGate-40F # diagnose debug enable

FortiGate-40F # diagnose debug flow filter addr 192.168.1.5

FortiGate-40F # diagnose debug flow filter proto 1

FortiGate-40F # diagnose debug flow trace start 50

FortiGate-40F # id=65308 trace_id=1 func=print_pkt_detail line=6007 msg="vd-root:0 received a
 packet(proto=1, 192.168.1.5:1->11.11.11.2:2048) tun_id=0.0.0.0 from lan. type=8, code=0, id=
1, seq=160."
id=65308 trace_id=1 func=init_ip_session_common line=6206 msg="allocate a new session-0000106
4"
id=65308 trace_id=1 func=vf_ip_route_input_common line=2615 msg="find a route: flag=04000000
gw-11.11.11.2 via l2t.root"
id=65308 trace_id=1 func=__iprope_tree_check line=528 msg="gnum-100004, use int hash, slot=31
, len=1"
id=65308 trace_id=1 func=fw_forward_handler line=835 msg="Denied by forward policy check (pol
icy 0)"
id=65308 trace_id=2 func=print_pkt_detail line=6007 msg="vd-root:0 received a packet(proto=1,
 192.168.1.5:1->11.11.11.2:2048) tun_id=0.0.0.0 from lan. type=8, code=0, id=1, seq=161."
id=65308 trace_id=2 func=init_ip_session_common line=6206 msg="allocate a new session-0000107
c"
id=65308 trace_id=2 func=vf_ip_route_input_common line=2615 msg="find a route: flag=04000000
gw-11.11.11.2 via l2t.root"
id=65308 trace_id=2 func=__iprope_tree_check line=528 msg="gnum-100004, use int hash, slot=31
, len=1"
id=65308 trace_id=2 func=fw_forward_handler line=835 msg="Denied by forward policy check (pol
icy 0)"
```

Deux règles firewall doivent être mises en place, une pour le trajet aller et l'autre pour le trajet retour.

Donc je suis retourné dans le Fortinet dans : **Policy & Object** -> **Firewall Policy** -> **Create New**





Après l'ajout des règles, j'ai retenté un ping.

```
Ping statistics for 11.11.11.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\caron>ping 11.11.11.2 -S 192.168.1.5

Pinging 11.11.11.2 from 192.168.1.5 with 32 bytes of data:
Reply from 11.11.11.2: bytes=32 time<1ms TTL=63
Reply from 11.11.11.2: bytes=32 time<1ms TTL=63
Reply from 11.11.11.2: bytes=32 time<1ms TTL=63
Reply from 11.11.11.2: bytes=32 time<1ms TTL=63

Ping statistics for 11.11.11.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Le NAS communique correctement avec le Laptop configuré en 192.168.1.5/24, ce qui confirme le bon fonctionnement du routage entre les deux équipements. Les règles de pare-feu ont été configurées de manière adéquate pour autoriser uniquement le trafic nécessaire, renforçant ainsi la sécurité du réseau. Les objectifs de connectivité, de routage et de sécurité ont donc été atteints avec succès, ce qui valide pleinement la mission.

5.4.3.8 Exploitation /Maintenance

Après avoir terminé la maquette, j'ai rédigé une procédure visant à implémenter le protocole L2TP sur un tunnel IPsec existant (voir annexe 2). Cette étape était cruciale pour permettre au NAS Synology de s'intégrer au réseau via un VPN sécurisé.

Une fois la procédure finalisée, nous avons lancé sa mise en œuvre. Très vite, j'ai dû faire quelques ajustements : comme l'authentification passait par Active Directory, il n'était finalement pas nécessaire de créer de groupe ni d'utilisateur local sur le Fortinet, contrairement à ce que j'avais initialement prévu.

Une complication est survenue dès que j'ai ouvert l'interface du pare-feu Fortinet en production : la version du firmware était différente de celle utilisée pour la maquette. La procédure restait globalement correcte, mais certaines options avaient changé de place, voire disparu. Par exemple, sur la version de test, la configuration VPN pour Windows et Android était regroupée, alors que sur la version en production, les deux étaient séparées. Nous avons donc choisi de configurer la version dédiée aux clients Windows.

Lorsque nous avons testé la connexion VPN depuis le NAS, les premiers problèmes sont apparus. Les logs Fortinet (via CLI) montraient que les phases 1 et 2 du tunnel IPsec se passaient bien, mais que la connexion se coupait après environ cinq secondes.

J'ai donc testé la connexion depuis un poste Windows, et celle-ci a fonctionné sans problème. Mais depuis le NAS Synology, toujours aucun résultat.

Je me suis alors demandé sur quel système tournait le NAS. En vérifiant, j'ai découvert qu'il s'agissait d'un noyau Linux (le système DSM de Synology). J'ai donc tenté une configuration VPN similaire à celle utilisée pour Android (également basé sur Linux), mais là encore, la connexion échouait.

En analysant les logs Fortinet et ceux du NAS (via SSH) — car l'interface web de Synology ne permettait pas un suivi assez précis — j'ai repéré un message récurrent :
"No IPv4 pool declared",
alors que la plage d'adresses IP était bien définie. D'autres messages, notamment via SNMP, indiquaient que le tunnel était bien créé… avant d'être immédiatement fermé.

J’ai consulté plusieurs documentations, forums et guides techniques, sans trouver de réponse claire. Puis, en observant plus attentivement les échanges, j’ai remarqué que le NAS envoyait quelques paquets, mais qu’ensuite, aucune réponse ne parvenait, entraînant la fermeture automatique du tunnel.

Pour éviter de perturber davantage le réseau de production, mon maître de stage m’a proposé de rétrograder mon Fortinet 40F à la version 7.4.8, identique à celle du Fortinet 60F en production. J’ai pris soin de faire une sauvegarde complète avant cette opération, et nous avons également restauré une sauvegarde du Fortinet 60F pour repartir sur une base propre.

J’ai ensuite relancé les tests sur mon environnement de lab… et, à ma grande surprise, la connexion VPN a fonctionné parfaitement.

Ne comprenant pas pourquoi cela fonctionnait désormais, nous avons décidé de faire une sauvegarde complète des deux Fortinet et de comparer leurs configurations ligne par ligne. Une ligne différait, que j’ai retirée de mon 40F pour voir si cela changeait quelque chose — mais non, la connexion fonctionnait toujours.

Cela m’a fortement étonné, car nous avions désormais exactement la même configuration sur les deux équipements, sans résultat concluant sur le 60F.

En dernier recours, nous avons tenté de créer un utilisateur et un groupe local sur le Fortinet, sans passer par Active Directory, comme c’était le cas dans le lab. Et là, la connexion VPN a enfin fonctionné sur le NAS connecter au réseau de production. Pendant la matinée du dernier jour, nous avons réussi à trouver la solution à mon sujet de stage.

6. Conclusion

6.1 Sujet de stage

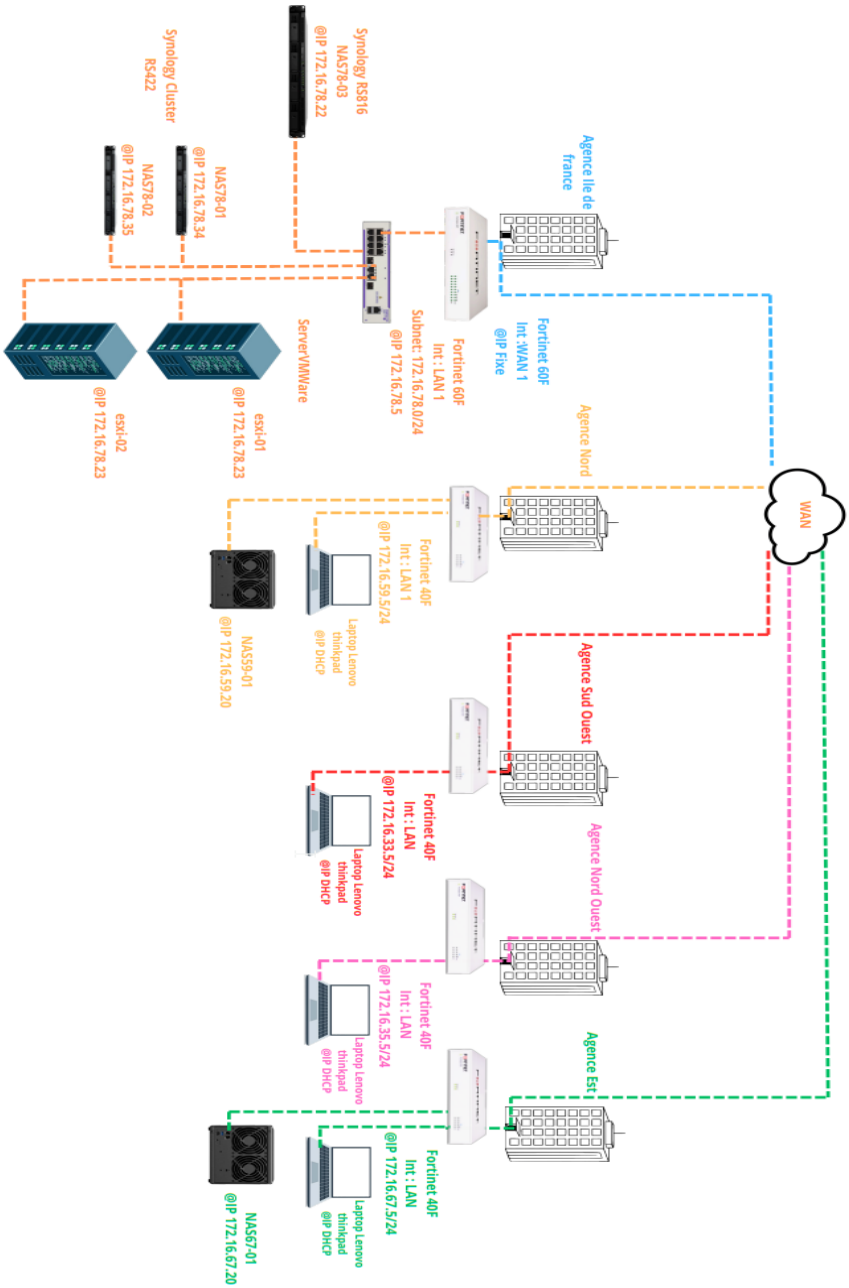
J’ai beaucoup aimé mon sujet de stage, car il m’a permis d’approfondir mes connaissances sur les VPN (IPSEC, SSL, L2TP), ainsi que de découvrir le fonctionnement d’un pare-feu Fortinet et des NAS Synology. Ce que j’ai particulièrement apprécié, c’est de pouvoir consacrer mes journées à travailler sur ces sujets, à chercher, tester et apprendre par moi-même. J’ai aimé devoir réfléchir pour trouver des solutions et me creuser la tête pour y parvenir. Cette expérience a été à la fois enrichissante et motivante, et elle m’a donné envie de continuer à explorer ce domaine.

6.2 Période de stage

J’ai beaucoup aimé mon stage, car j’ai eu l’opportunité de faire des choses variées et d’apprendre sur plusieurs aspects du métier. J’ai découvert le fonctionnement d’une flotte de

terminaux mobiles, l'interface d'un MDM (Mobile Device Management) et comment le paramétrer, ainsi que l'implémentation d'un VLAN sur le réseau de production de l'entreprise. J'ai aussi participé au support à distance, et bien d'autres tâches enrichissantes. L'équipe a été accueillante et chaleureuse tout au long de ma période de stage, ce qui a rendu l'expérience encore plus agréable. J'ai vraiment apprécié ce stage au sein de l'entreprise Talice.

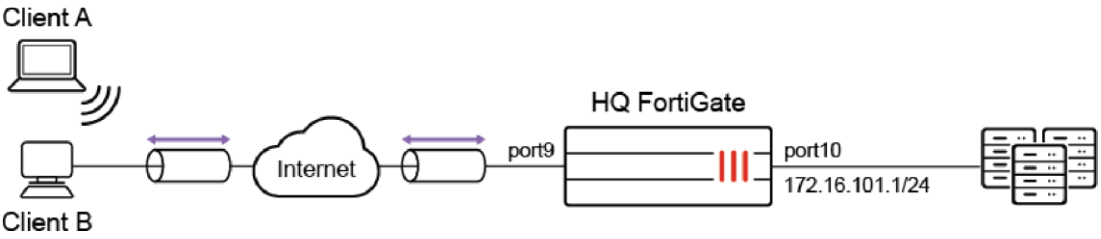
7. Annexes



Annexe 2 :

TALICE

Implémentation L2TP over IPsec

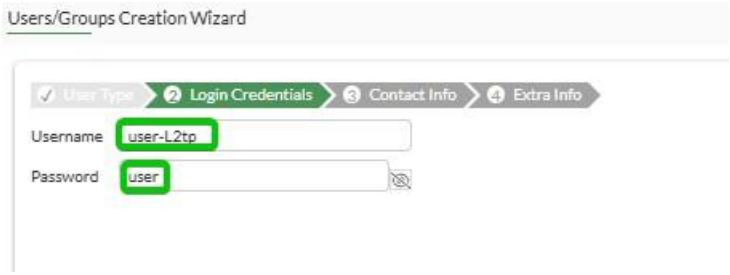


CARON Cyprien
01/07/2025

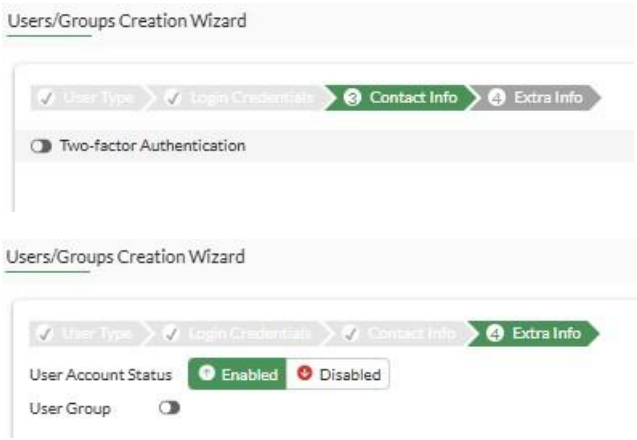
Table des matières

Création de l'utilisateur

Se rendre dans **User Définition** -> **Create user** -> **Local user** -> **Next**

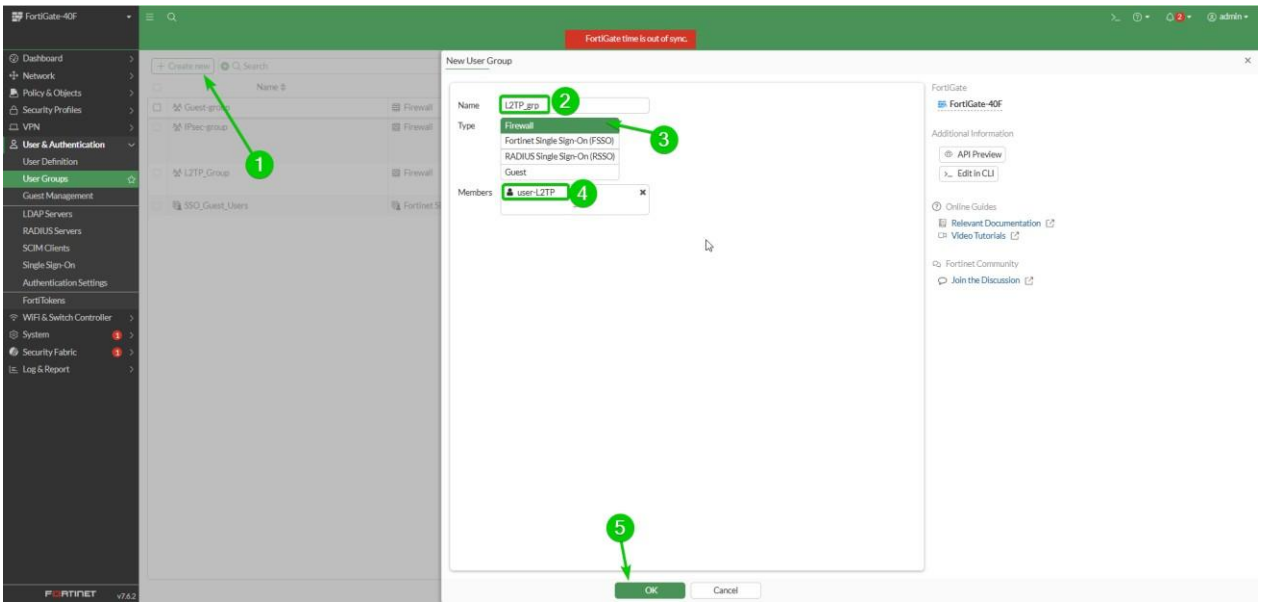


Désactiver l'authentification à double facteur pour la connexion de **l'utilisateur**



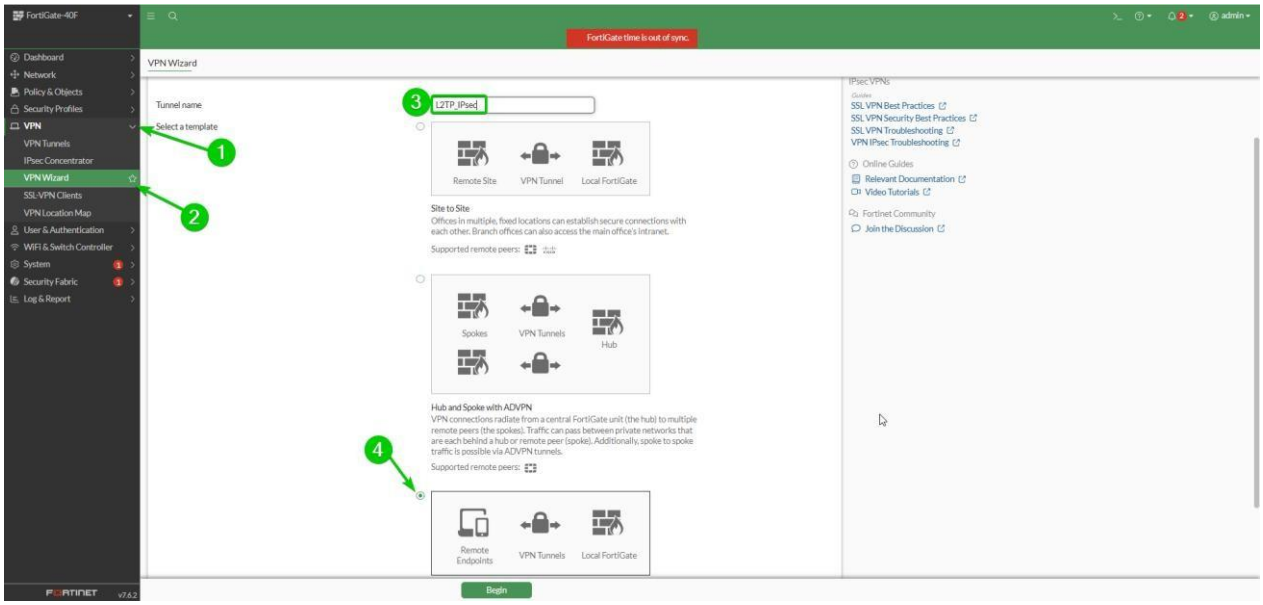
Création du groupe

User Groups -> **Create New** -> remplir les informations -> **ok**



Création du tunnel VPN

Aller dans **VPN Wizard** -> entrer le nom du tunnel -> **Remote Endpoints** -> **Begin**



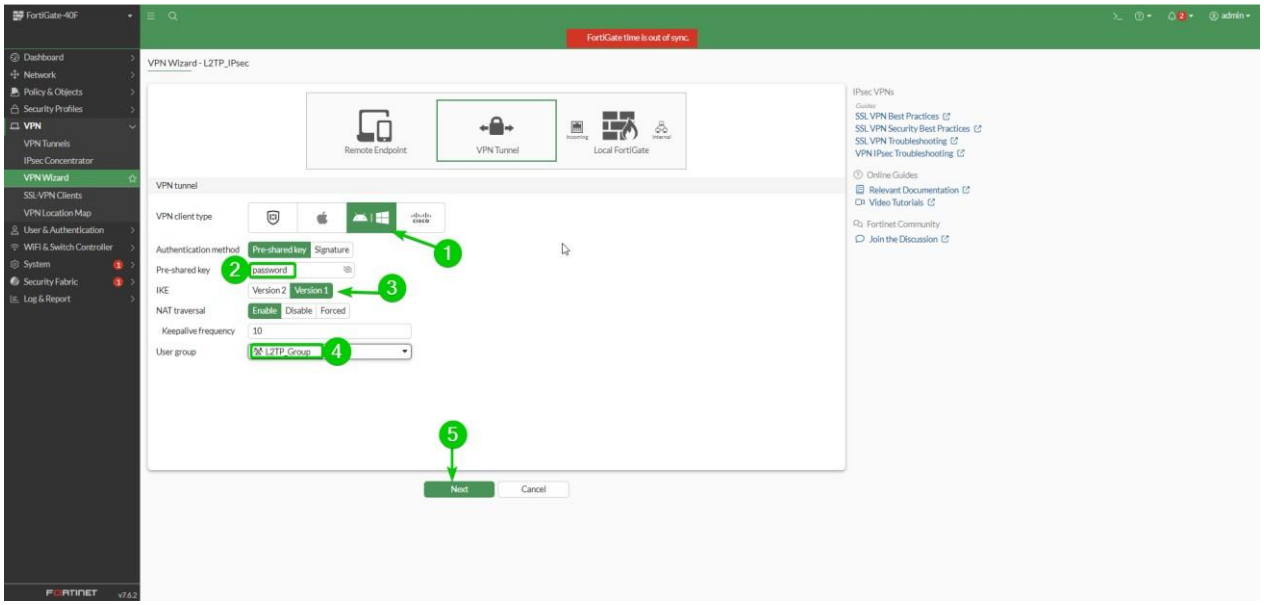
VPN Client Type : **Android & Windows natif (L2TP)**

Entrée une PSK

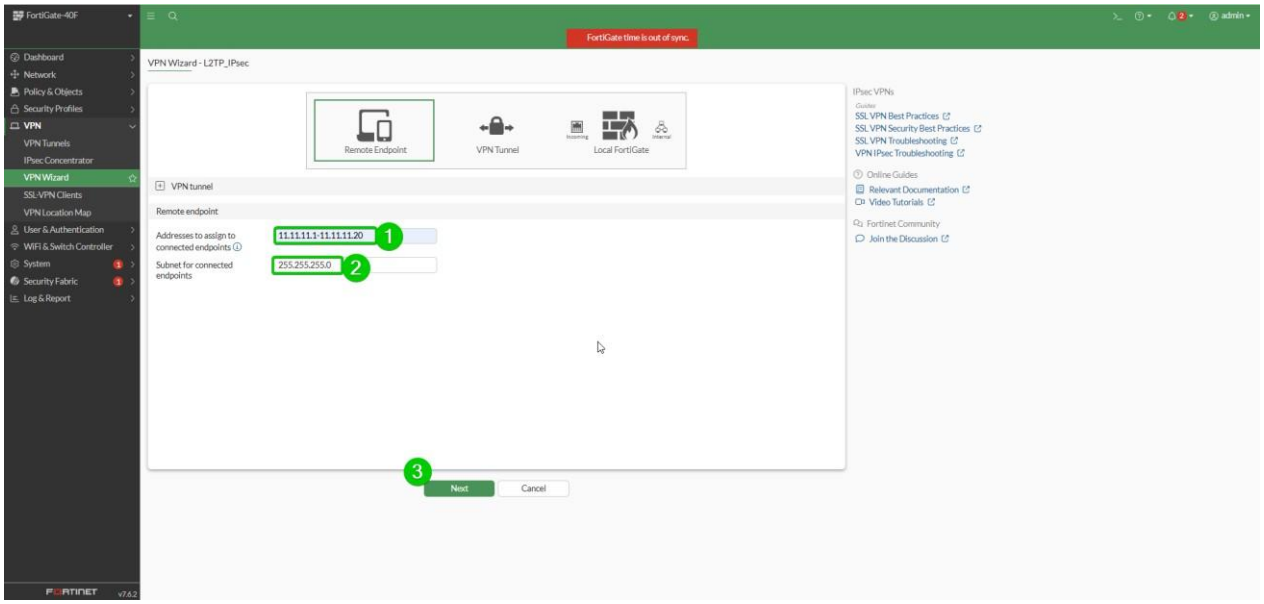
IKE : **Version 1**

NAT Transversal : **Enable**

User group : groupe précédemment créé



Puis sélectionner une **plage d'adresse non utilisée avec le masque approprier** -> **Next**



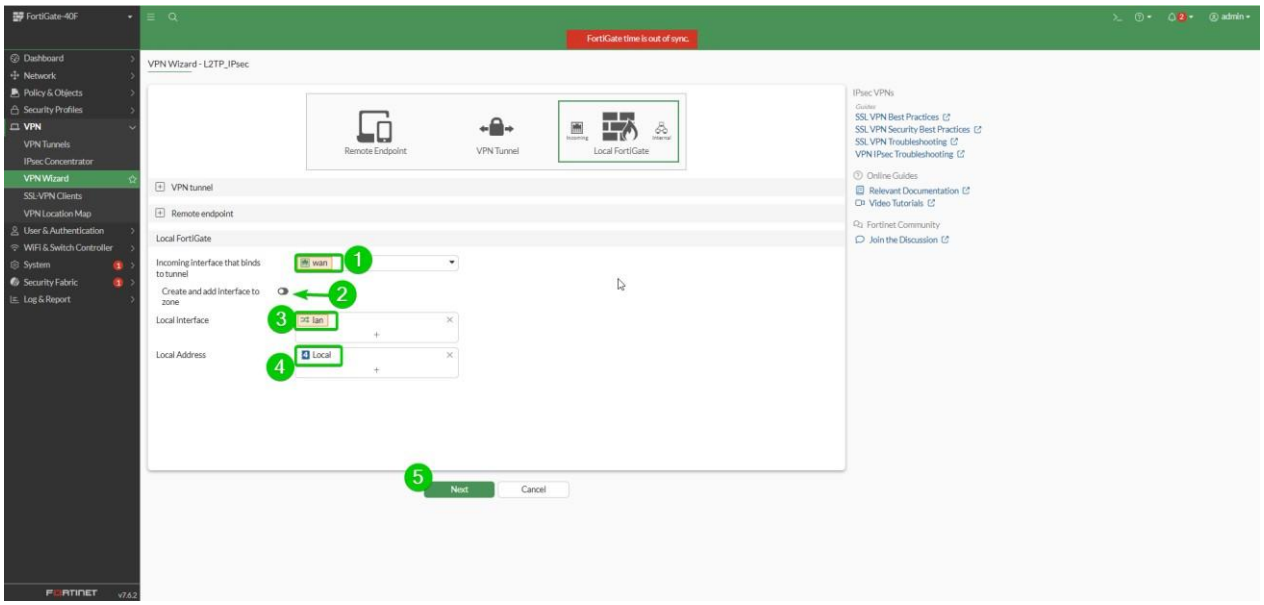
Sélectionner l'interface entrante et sortante

Incoming interface : **WAN**

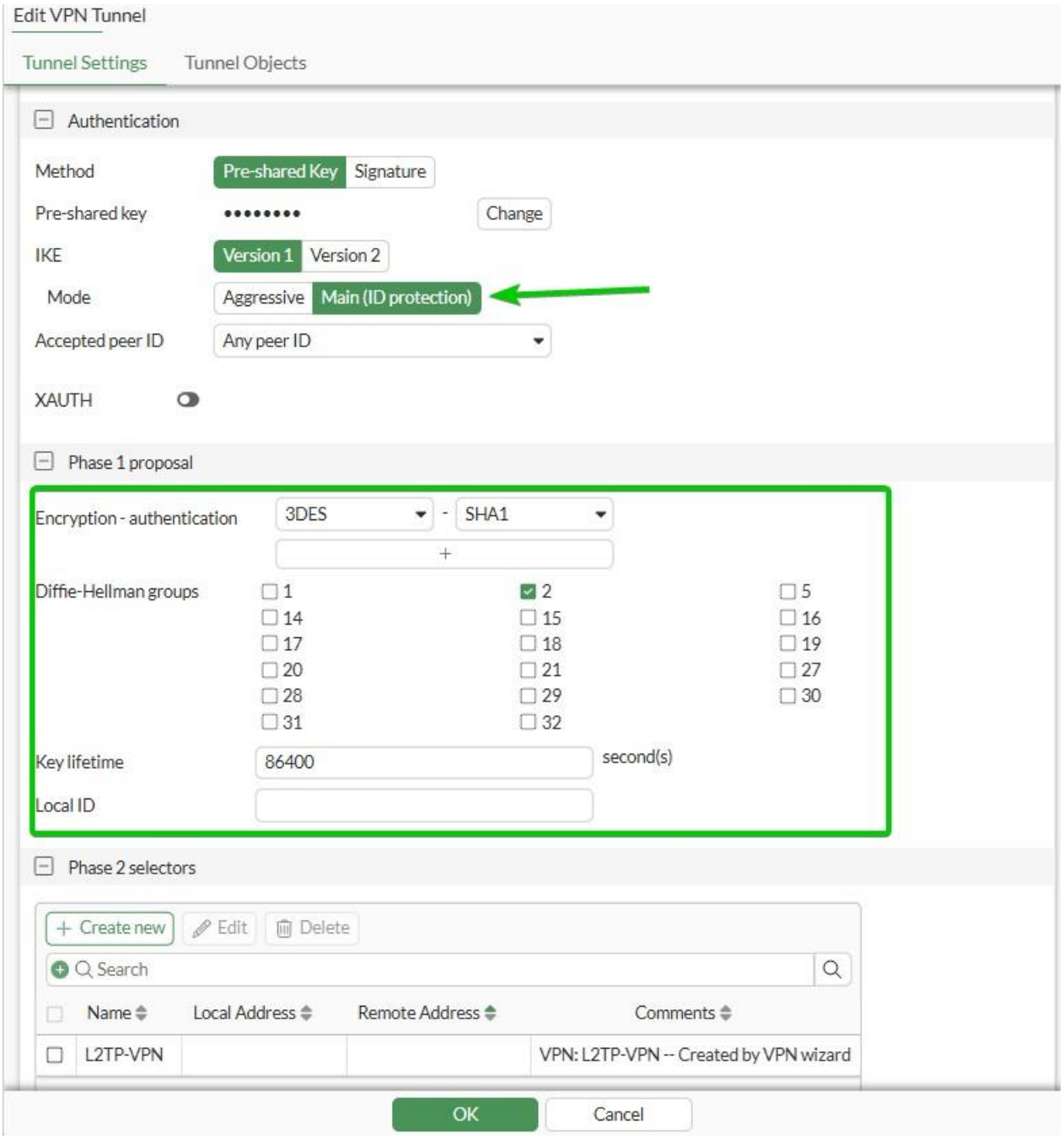
Create and add interface to zone : **Disable**

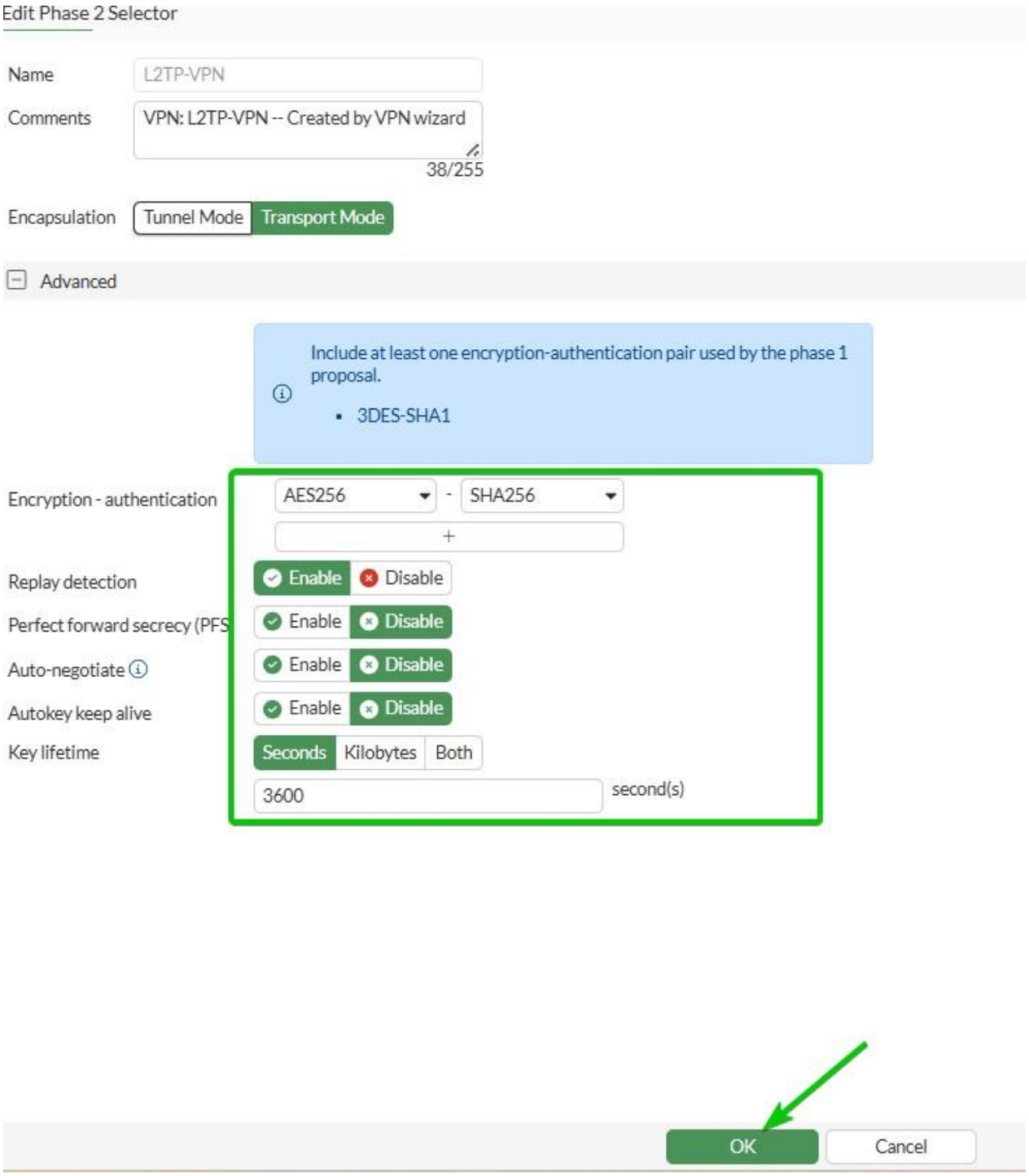
Local interface : Sélectionner l'interface réseau où se situe les NAS

Local Address : Sélectionner le réseau où se situe les NAS à joindre (Subnet 192.168.78.0/24).



Après avoir créé le tunnel cliquer sur édit -> mode : **Main (ID protected)** -> encryptions – authentication : **3DES- SHA1** -> **DH groups : 2** -> **phase 2** -> encryptions – authentication : **AES256-SHA256** -> **ok**


Edit VPN Tunnel
Tunnel Settings
Tunnel Objects
Authentication
Method
Pre-shared Key
Signature
Pre-shared key
Change
IKE
Version 1
Version 2
Mode
Aggressive
Main (ID protection)
Accepted peer ID
Any peer ID
XAUTH
Phase 1 proposal
Encryption - authentication
3DES
SHA1
Diffie-Hellman groups
1
2
5
14
15
16
17
18
19
20
21
27
28
29
30
31
32
Key lifetime
86400
second(s)
Local ID
Phase 2 selectors
Create new
Edit
Delete
Search
Name
Local Address
Remote Address
Comments
L2TP-VPN
VPN: L2TP-VPN -- Created by VPN wizard
OK
Cancel


Edit Phase 2 Selector
Name
L2TP-VPN
Comments
VPN: L2TP-VPN -- Created by VPN wizard
38/255
Encapsulation
Tunnel Mode
Transport Mode
Advanced
Include at least one encryption-authentication pair used by the phase 1 proposal.
3DES-SHA1
Encryption - authentication
AES256
SHA256
Replay detection
Enable
Disable
Perfect forward secrecy (PFS
Auto-negotiate
Autokey keep alive
Key lifetime
Seconds
Kilobytes
Both
3600
second(s)
OK
Cancel

Création de la route statique

Apres avoir créé le tunnel il faut vérifier qu'il y ait bien la route statique pour pouvoir accéder au Subnet du NAS. Pour ce faire aller dans -> **Network** -> **Static routes** -> regarder si la route existe sinon il faut la créé -> **Create New** -> sélectionner le Subnet qui vous intéresse pour ma part « 11.11.11.0/24 » et sélectionner l'interface « **L2T/root** ».

Création des règles pare-feu

Après avoir ajouté la route par défaut il faut maintenant configurer les politiques de pare-feu : Aller dans **Policy & Object** -> **Firewall Policy** -> **Create New** -> nommer la comme bon vous semble -> sélectionner : **ACCEPT** -> Incoming interface : **L2T.root** -> Outgoing Interface : **LAN** -> **Source**
« nom_de_votre_VPN_range » ->**Destination : « Local Subnet »** -> Service : ICMP, SMB, NFS, FTP/SFTP-> enable NAT Transversal (puis laisser les paramètres par défaut)

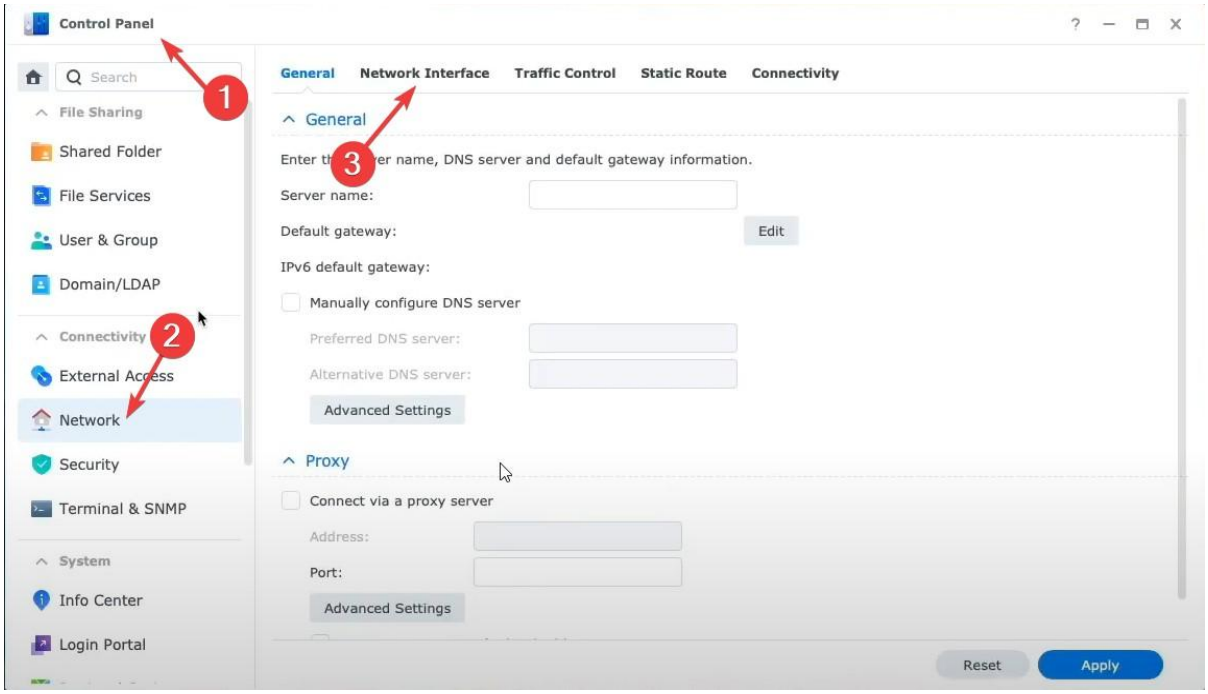
Et faites la même règle pour gérer le retour

Aller dans **Policy & Object** -> **Firewall Policy** -> **Create New** -> nommer la comme bon vous semble -> sélectionner : **ACCEPT** -> Incoming interface : **LAN** -> Outgoing Interface : **L2T.root** -> **Source « Local Subnet »** ->**Destination :**
nom_de_votre_VPN_range » -> Service : ICMP, SMB, NFS, FTP/SFTP-> enable NAT Transversal (puis laisser les paramètres par défaut)

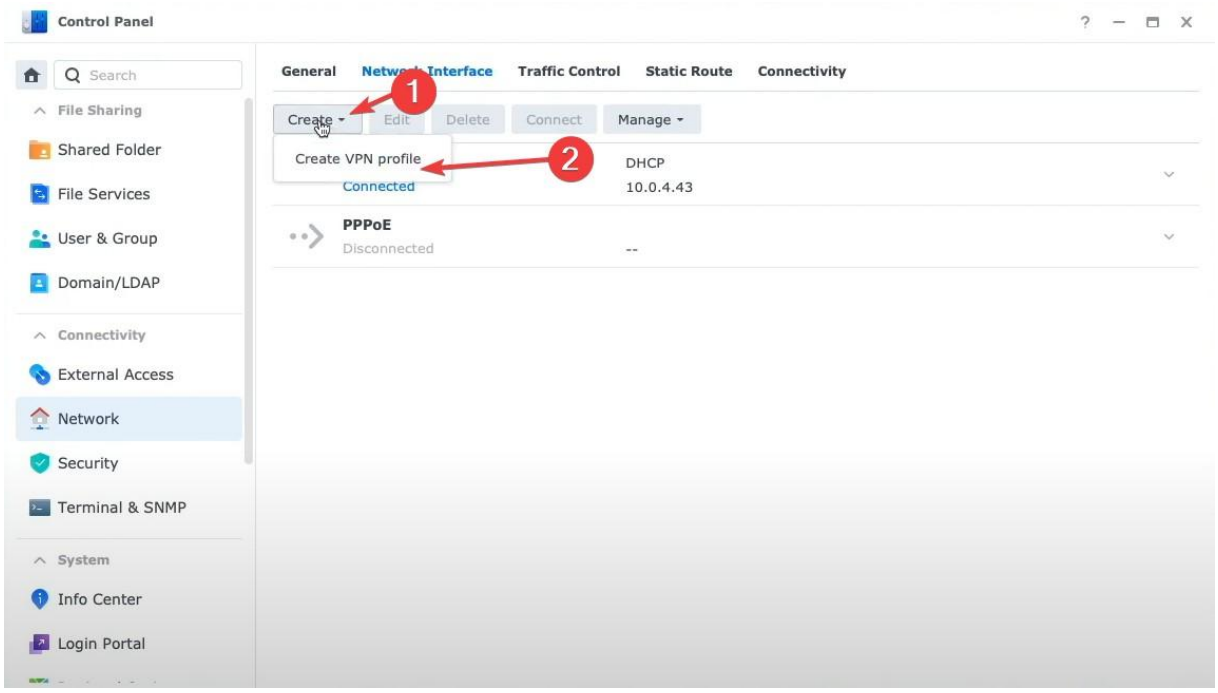
Une fois cela fait, il faut configurer le NAS.

Aller dans **Control Panel**-> **Network** -> **Network Interface**

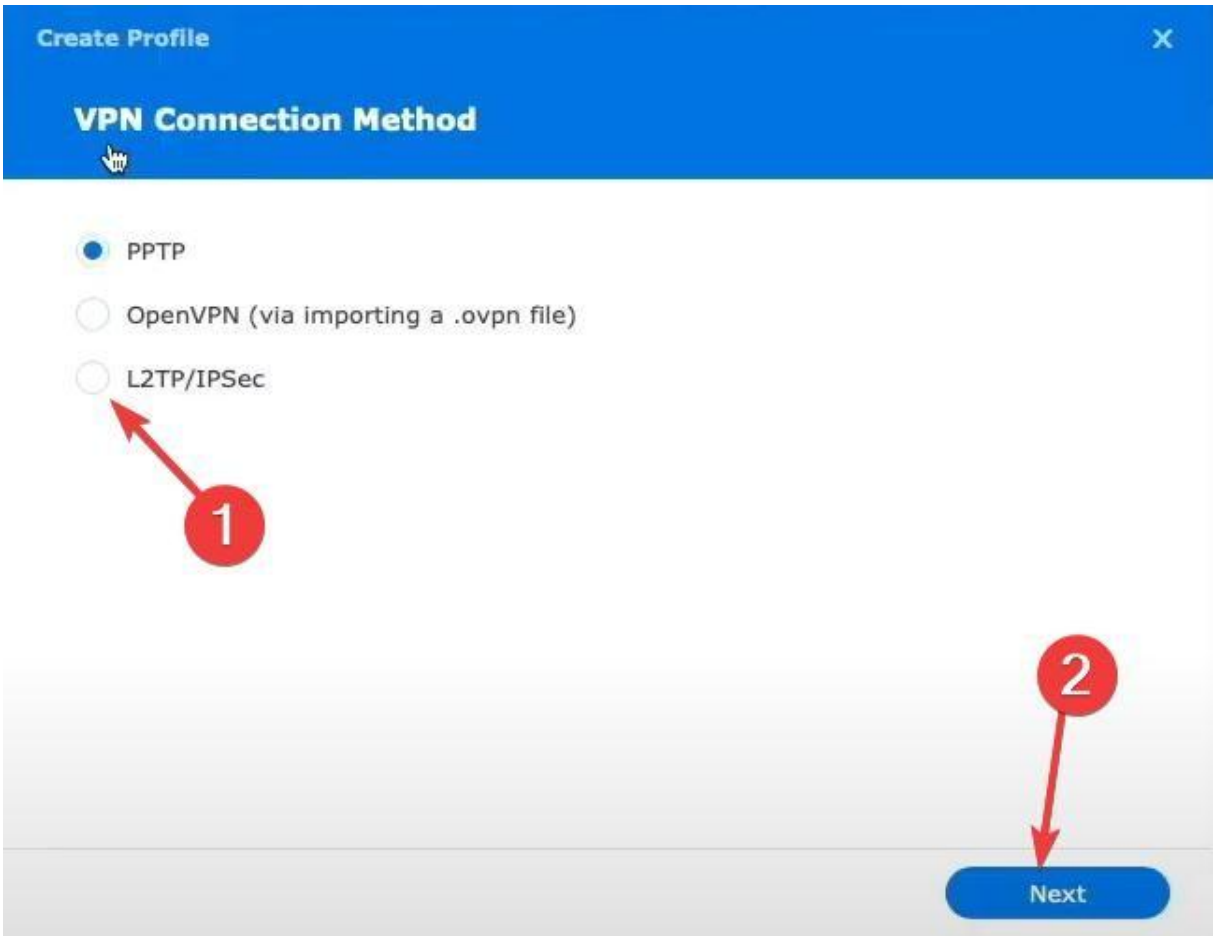
Configuration client VPN

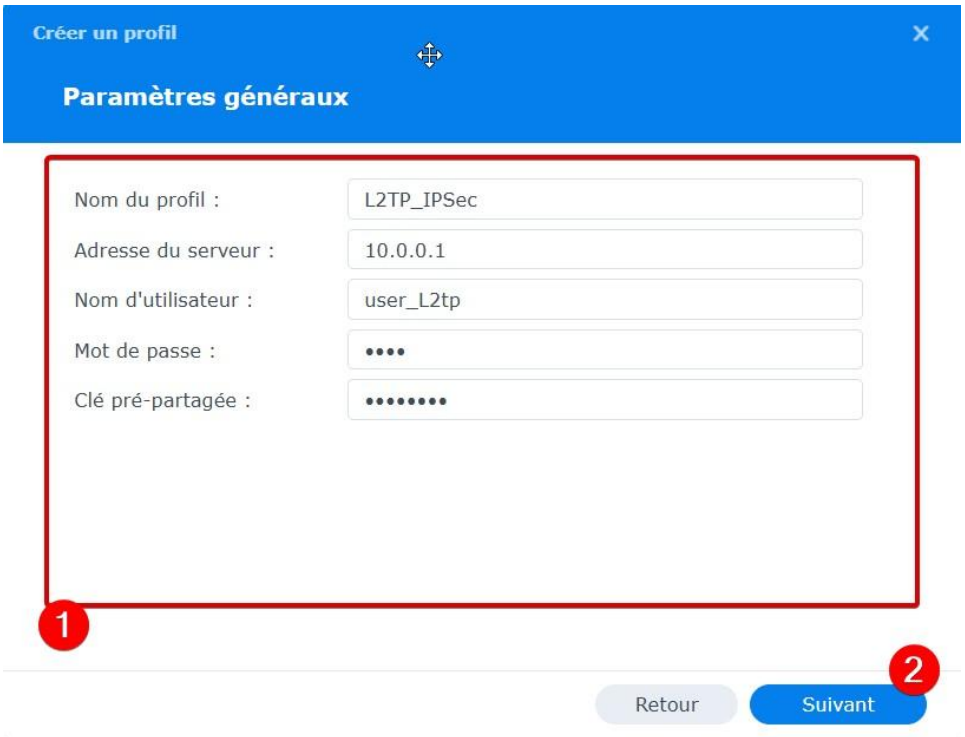


Puis aller dans : **Create**-> **Create VPN Profile**



Puis appuyer sur l'option : **L2TP/IPSec**





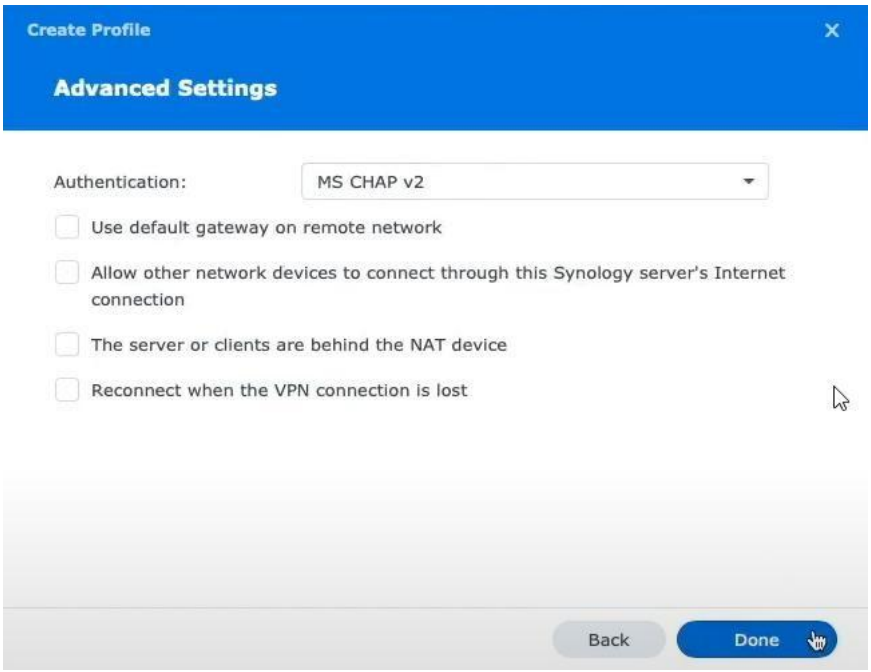
Cochez les cases suivantes :

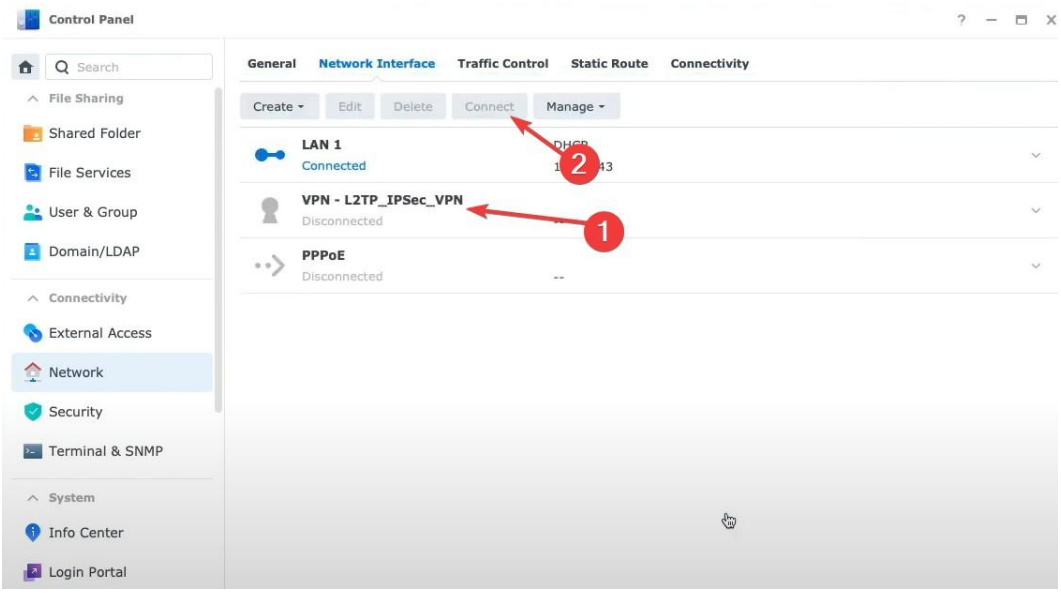
(Si vous voulez accéder au site web du NAS Synology depuis le réseau local cochez -> Allow other network device to connect though this Synology server's Internet)

-Use default gateway on remote network

-The server or client are behind a NAT device

- Reconnect when the connection is lost





Si tout c’est bien passer votre NAS devrait afficher cela :