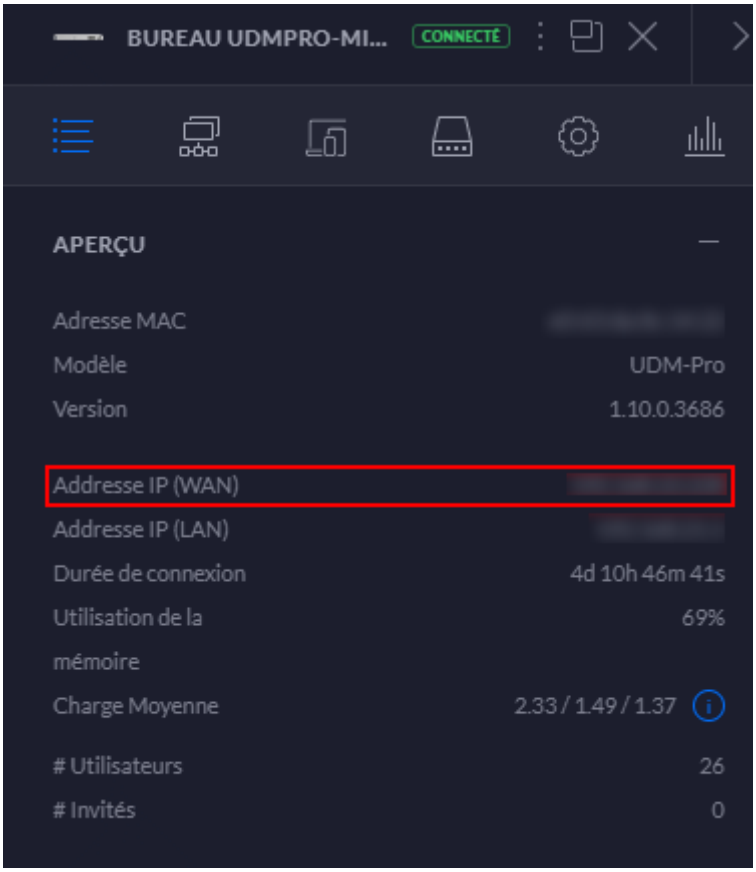
Configuration VPN L2TP Synology ou UDM

Table des matières

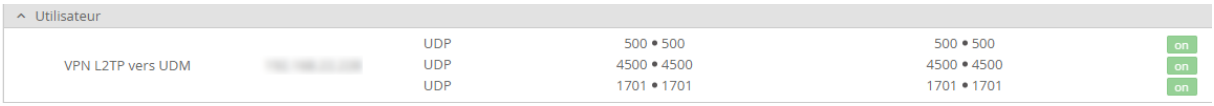
I) Ouvrir les ports correspondant au VPN L2TP

Sur le panneau d'administration du routeur, il faut ouvrir les ports 500, 1701, 4500 avec le protocole UDP redirigé vers l'adresse IP du Synology. Le mieux est d'avoir le NAS avec une IP fixe pour ne pas être embêté par la suite.

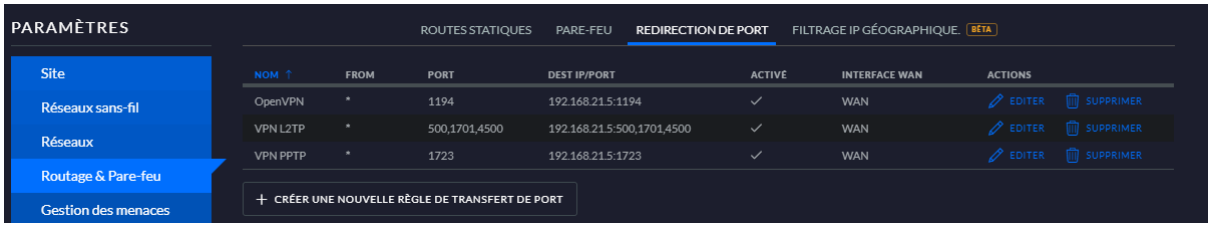
S'il y a un contrôleur Unifi il faudra d'abord rediriger le port vers l'Unifi puis après dans l'Unifi le rediriger vers le NAS.



Il faut utiliser l'adresse du WAN de l'Ufini sur la box on peut la trouver dans Équipement puis en cliquant sur UDM-PRO/Dream Machine Pro.



S'il y a un Unifi rediriger les ports vers l'IP WANN de l'Unifi sinon directement vers l'IP du NAS.



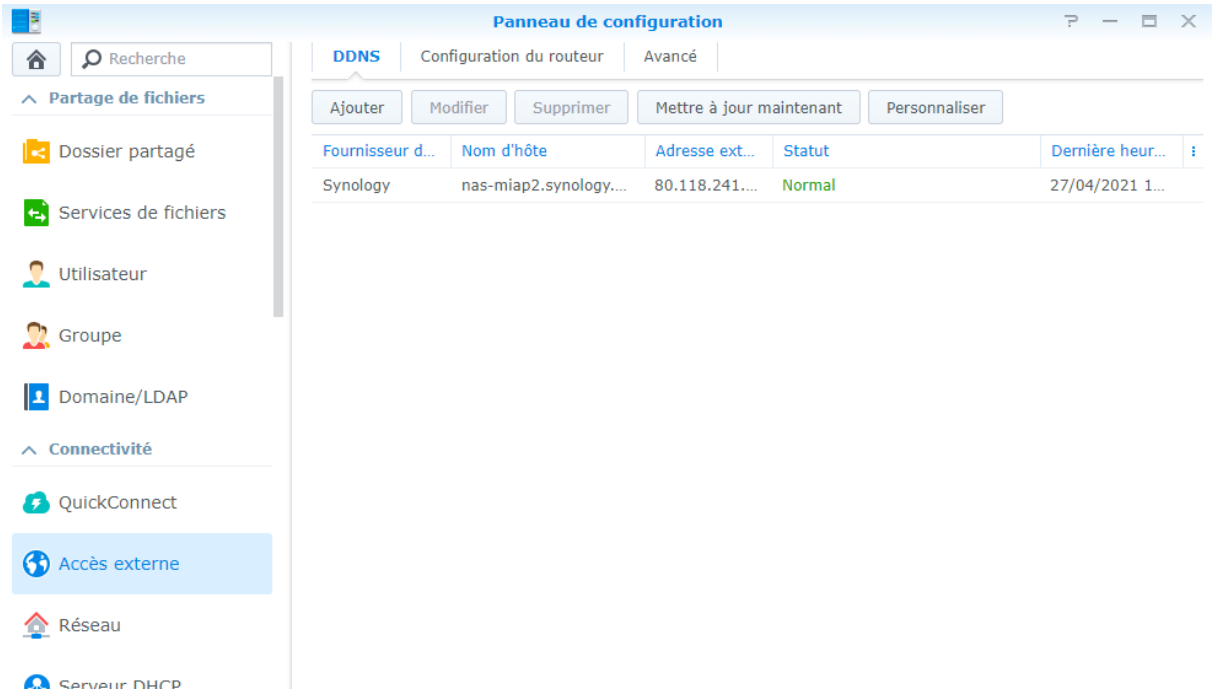
Si le VPN est installé sur l'Unifi il n'y a pas besoin de faire la redirection de port ci-dessus.

!! ATTENTION : le Telnet ne peut pas être utilisé, en revanche il existe des outils pour vérifier que ce port est bien ouvert !!

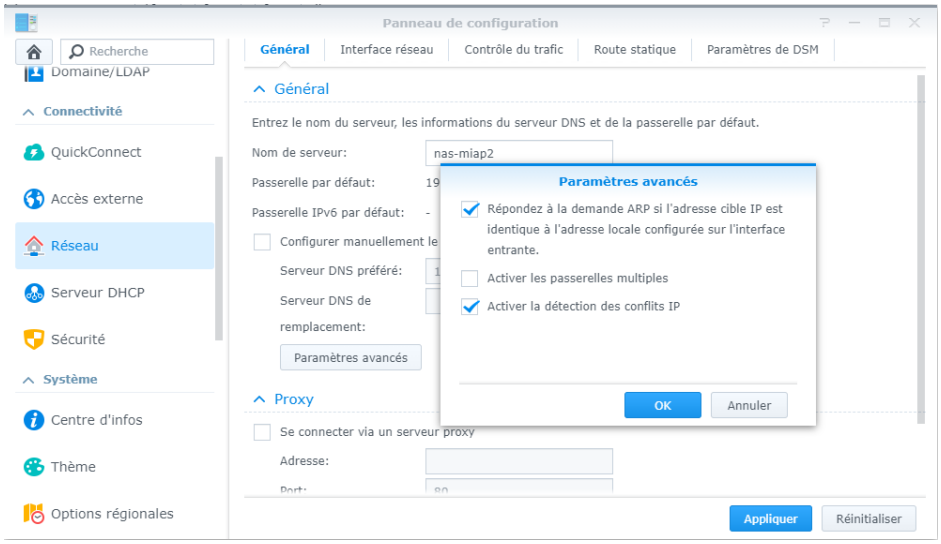
II) Configuration du serveur VPN sur SYNOLOGY

1) Configurer l'adresse externe du SYNOLOGY pour faire du DDNS

Pour cela il faut se rendre dans "Panneau de configuration" puis "Accès externe"
L'adresse externe correspond à l'IP Public de la box

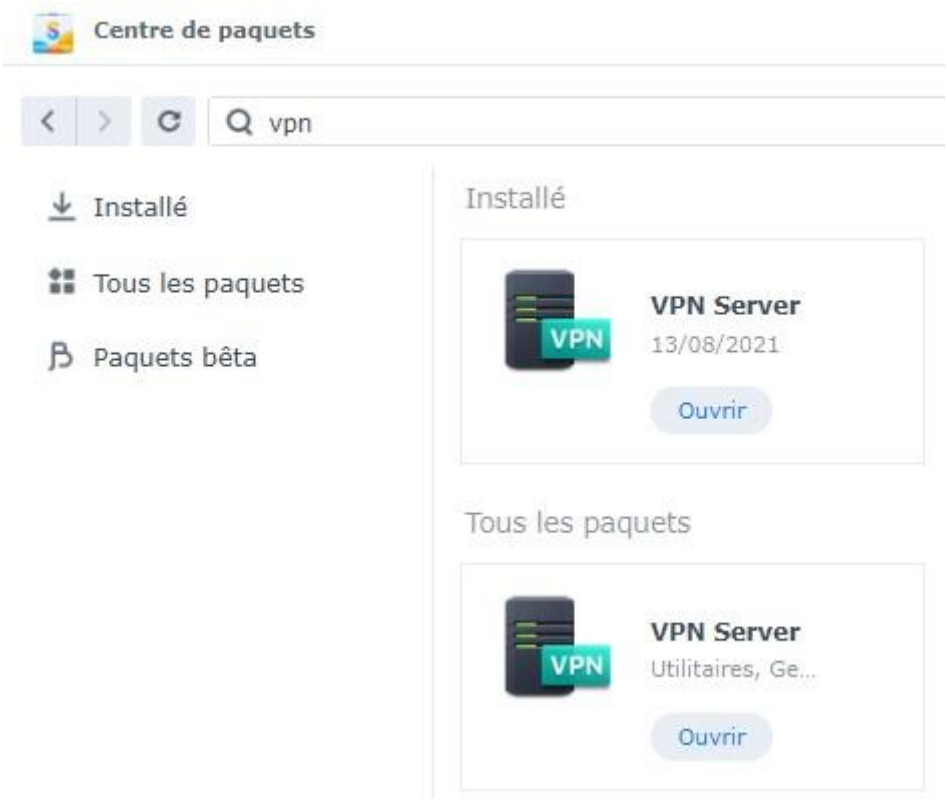


2) Désactiver les passerelles multiples



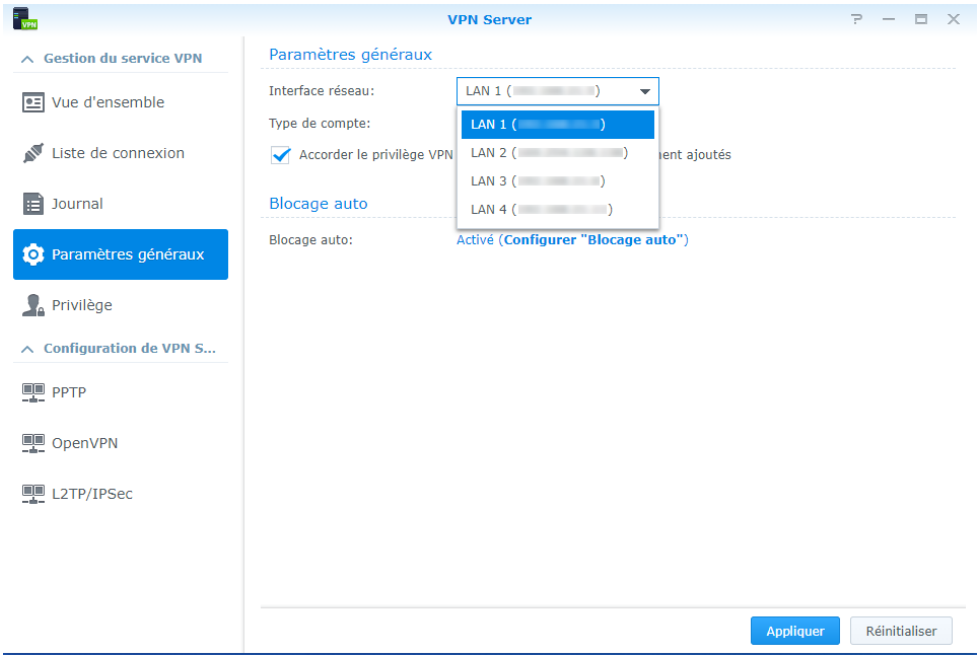
Panneau de configuration -> Réseau -> Général -> Paramètres avancés

3) Installer le paquet "VPN Server"



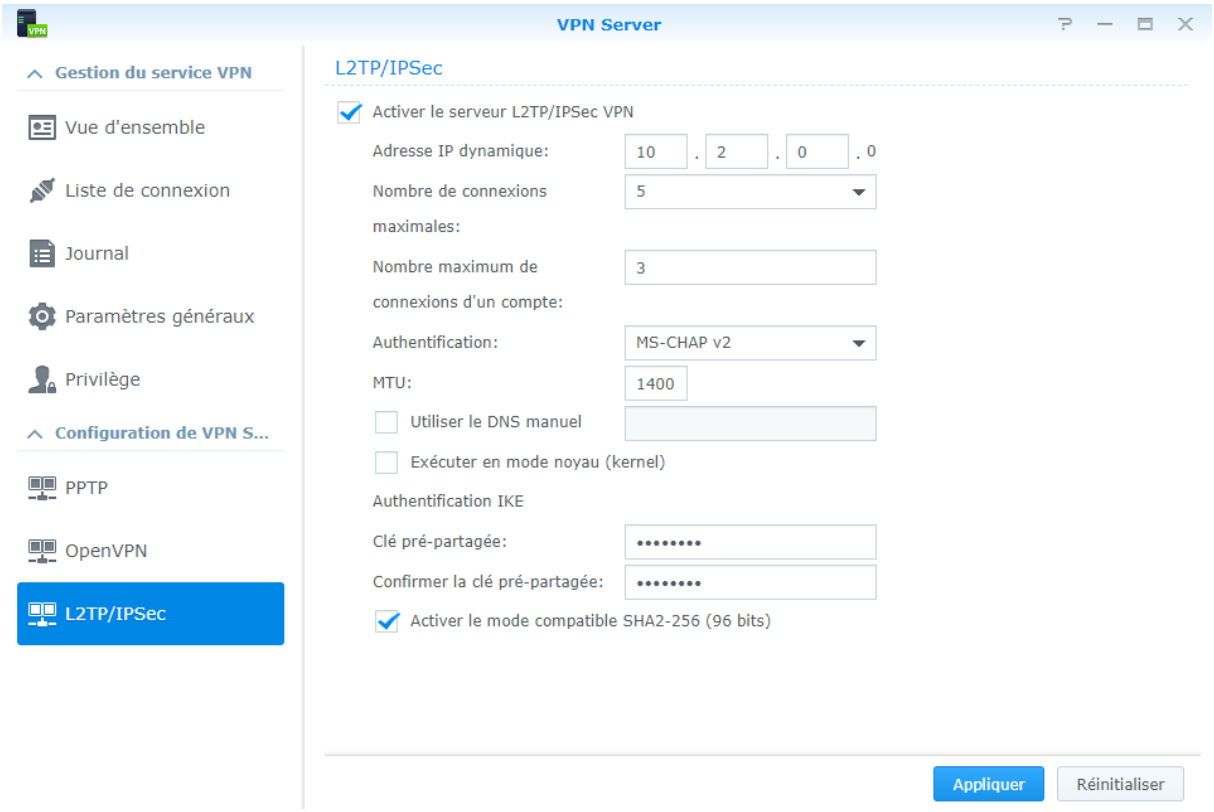
Rechercher « VPN » depuis le centre de paquets

4)Sélectionner la bonne carte réseau si plusieurs sons disponibles



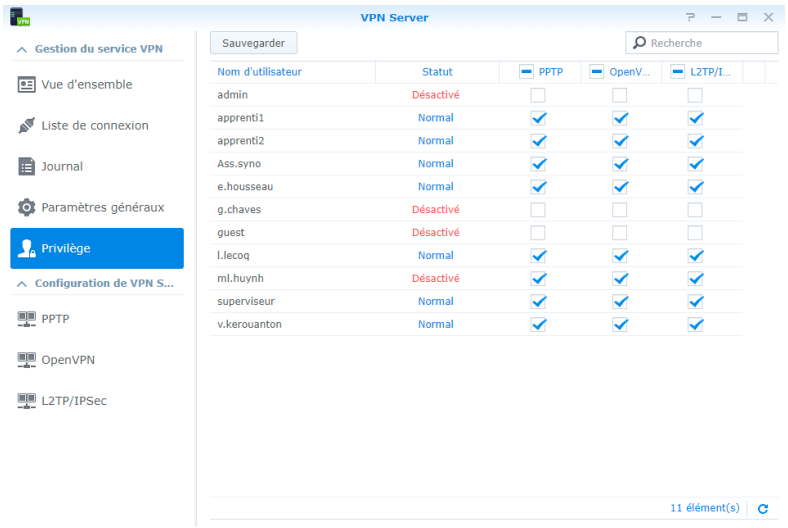
Lancer le "VPN Server" et se rendre dans "Paramètres généraux" pour s'assurer que ce soir la bonne carte réseau qui soit sélectionnée.

5) Activer le serveur L2TP/IPSec



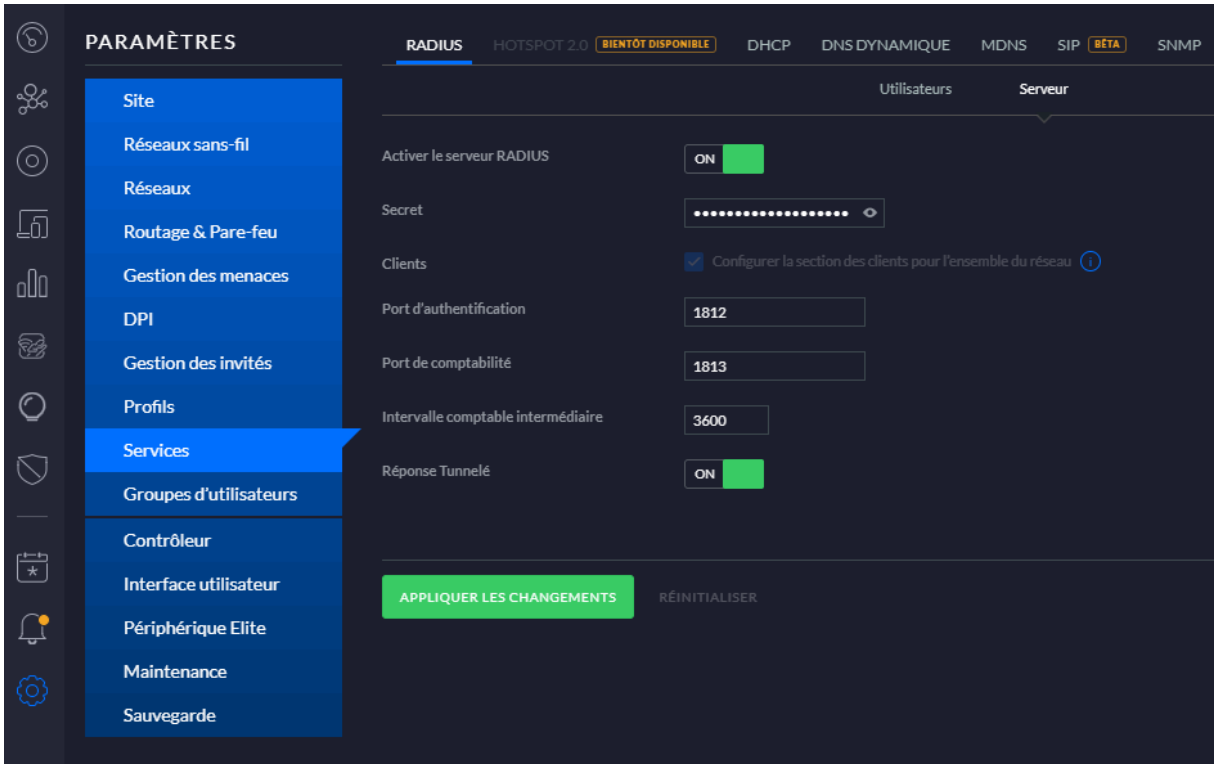
Se rendre dans "L2TP" puis l'activer, pour la clé pré-partagée, les caractères spéciaux ne sont pas pris en charge sur Synology, cliquer sur "Appliquer".

6) Autoriser l'utilisation des services VPN correspondant aux utilisateurs



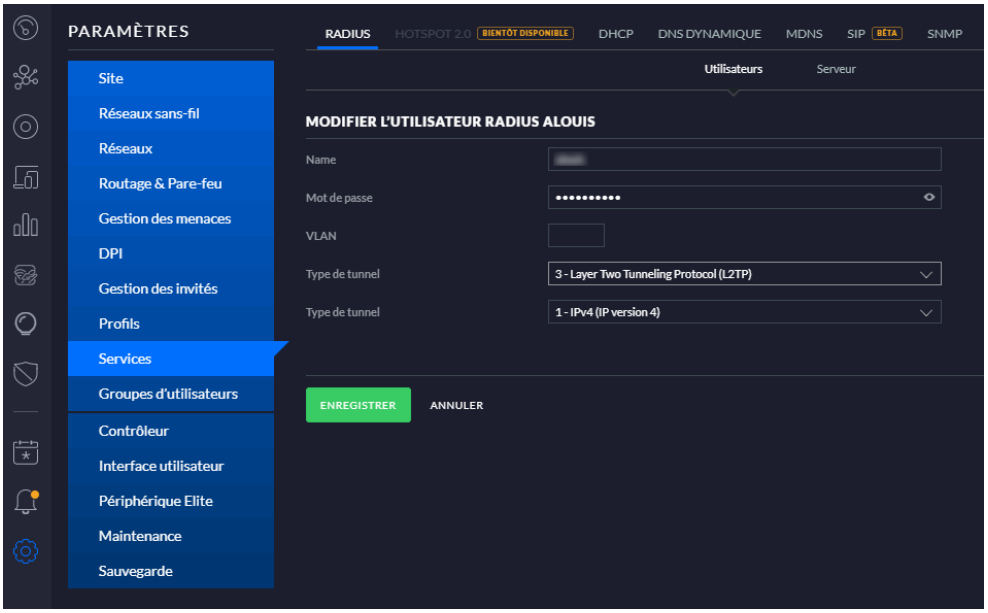
III) Configuration du serveur VPN sur UNIFI

1) Activer le service radius avec les paramètres par défaut

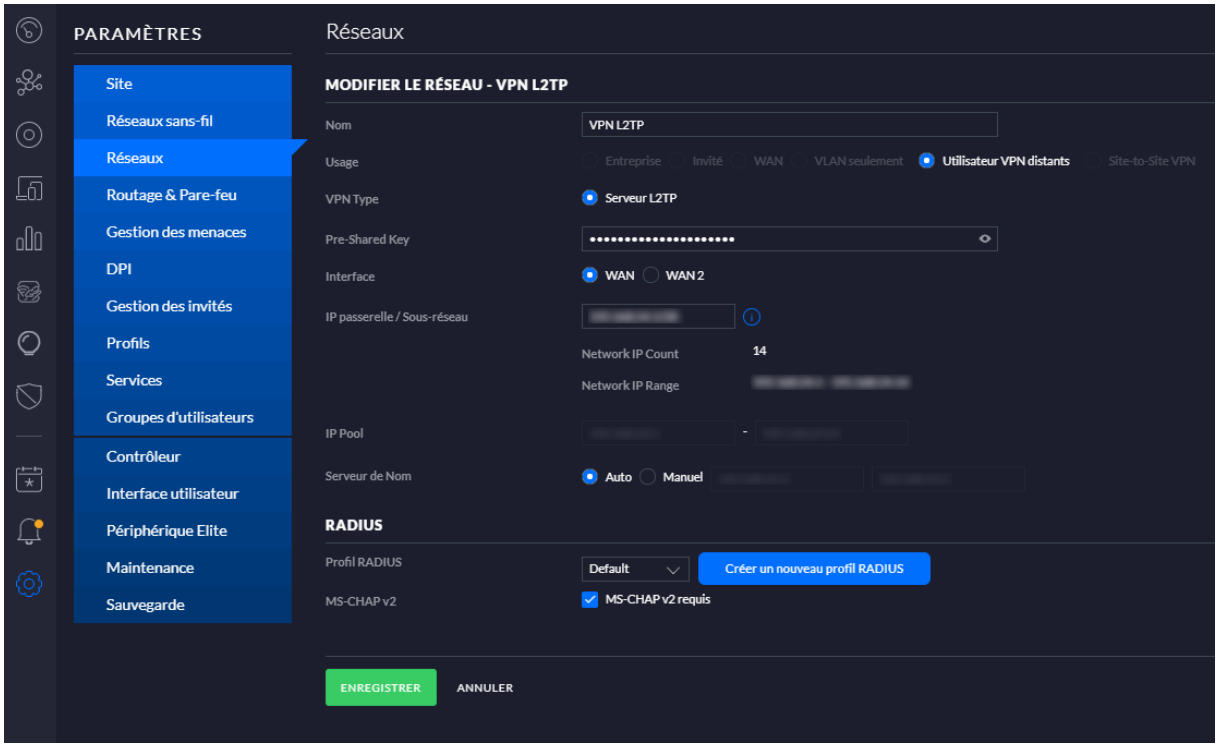


Secret doit être identique à la clé pré-partagée, Unifi prend en charge les caractères spéciaux.

2) Créer les utilisateurs radius, sélectionner L2TP et IPv4 en type de tunnel



3) Créer un réseau pour le VPN L2TP



Sélectionner Utilisateur VPN distants,

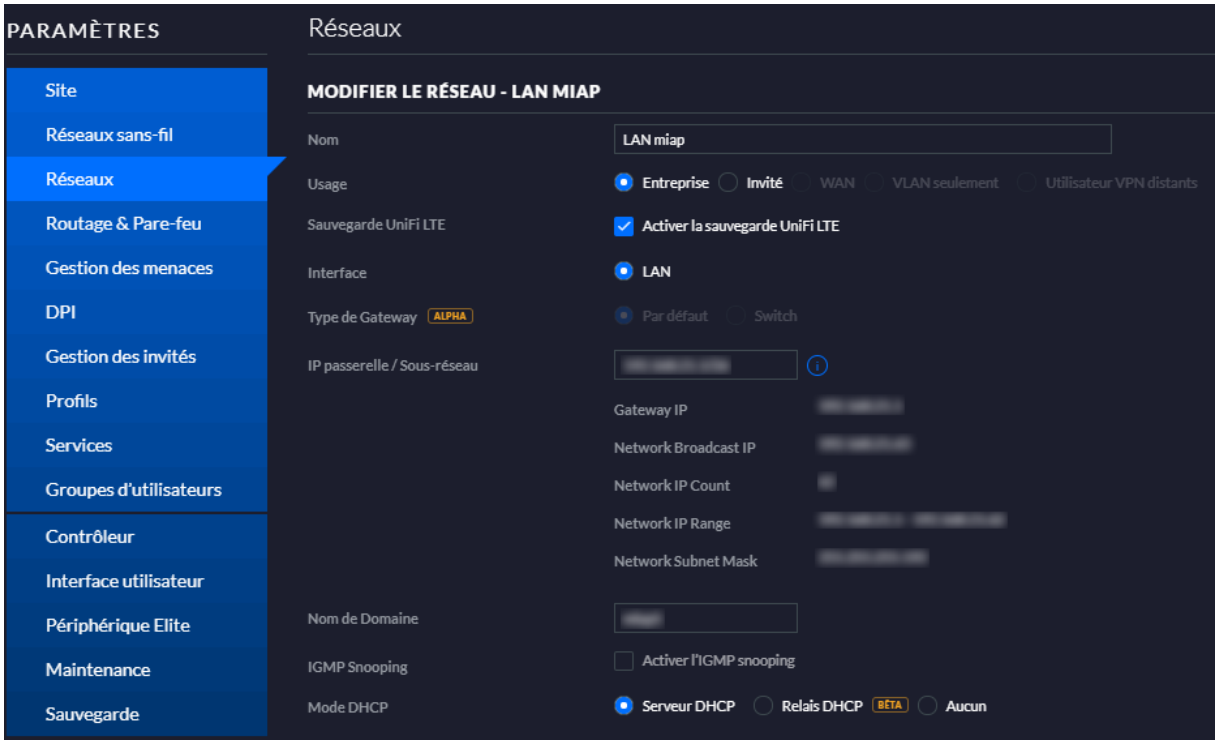
Serveur L2TP,

Clé pré-partagée *********

IP passerelle / sous réseau : Choisir un réseau disponible, ici le réseau 192.168.24.0 est disponible mais on peut en utiliser un autre, le masque de sous-réseau /28 a été choisi pour limiter le nombre de connections simultanées, cette valeur changera en fonction de la taille de l'entreprise.

Cocher le MS-CHAP v2 requis

4) Ajouter un suffixe DNS (facultatif)
Uniquement pour la résolution de nom

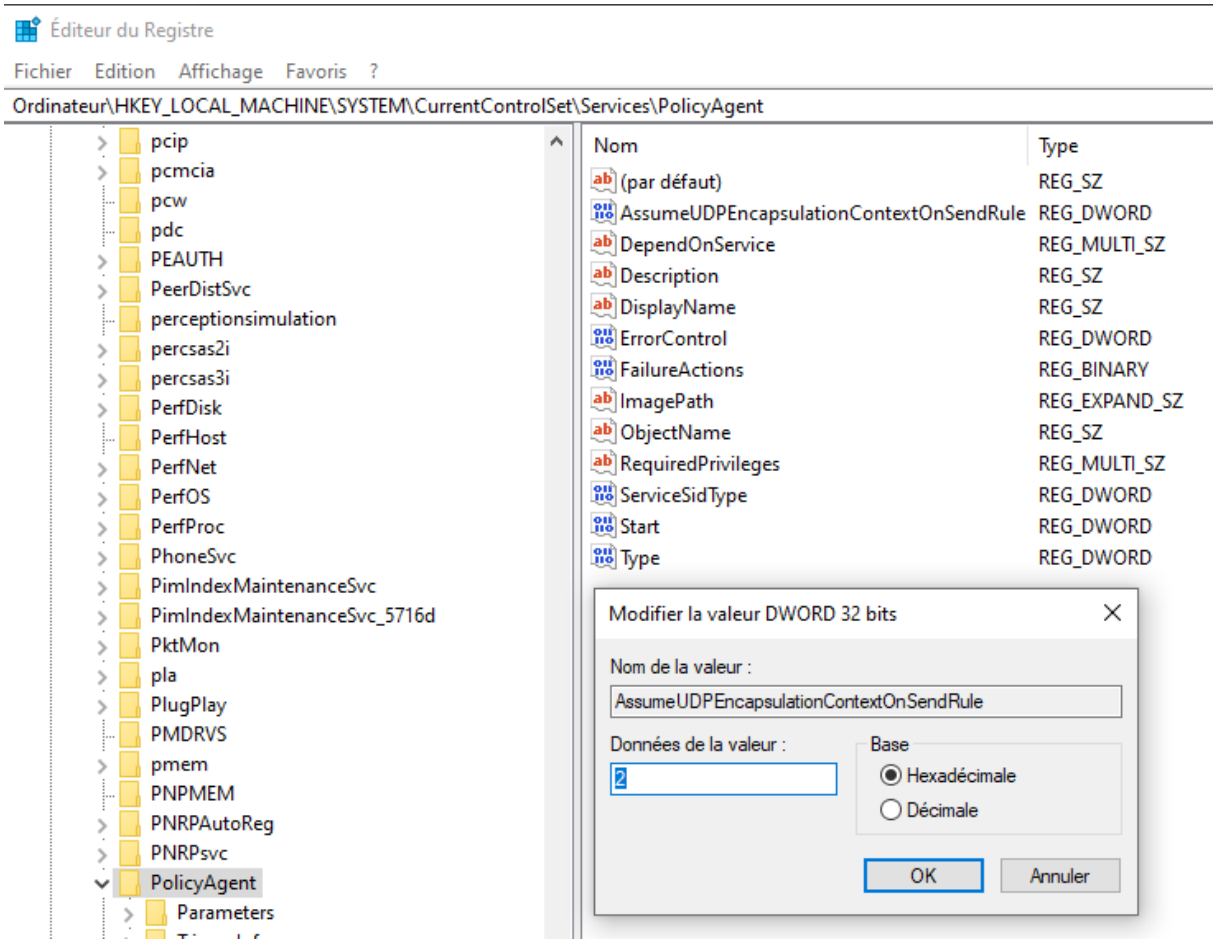


Dans le réseau LAN ajouter un suffixe DNS dans la zone "Nom de Domaine" pour avoir une résolution de nom en VPN.

IV) Connexion au serveur VPN

1) Ajouter une clé de registre dans l'éditeur de registre

Dans le Regedit ajouter la clé de registre : AssumeUDPEncapsulationContextOnSendRule avec la valeur "2" en Hexadécimal à cet emplacement
: Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent



Cette clé est nécessaire pour établir une connexion VPN L2TP situé derrière un NAT
: https://docs.microsoft.com/en-US/troubleshoot/windows-server/networking/configure-l2tp-ipsec-server-behind-nat-t-device

2) Création d'un profil VPN

Dans les paramètres Windows aller dans Réseau et internet puis dans VPN.

Ajouter une nouvelle connexion VPN,

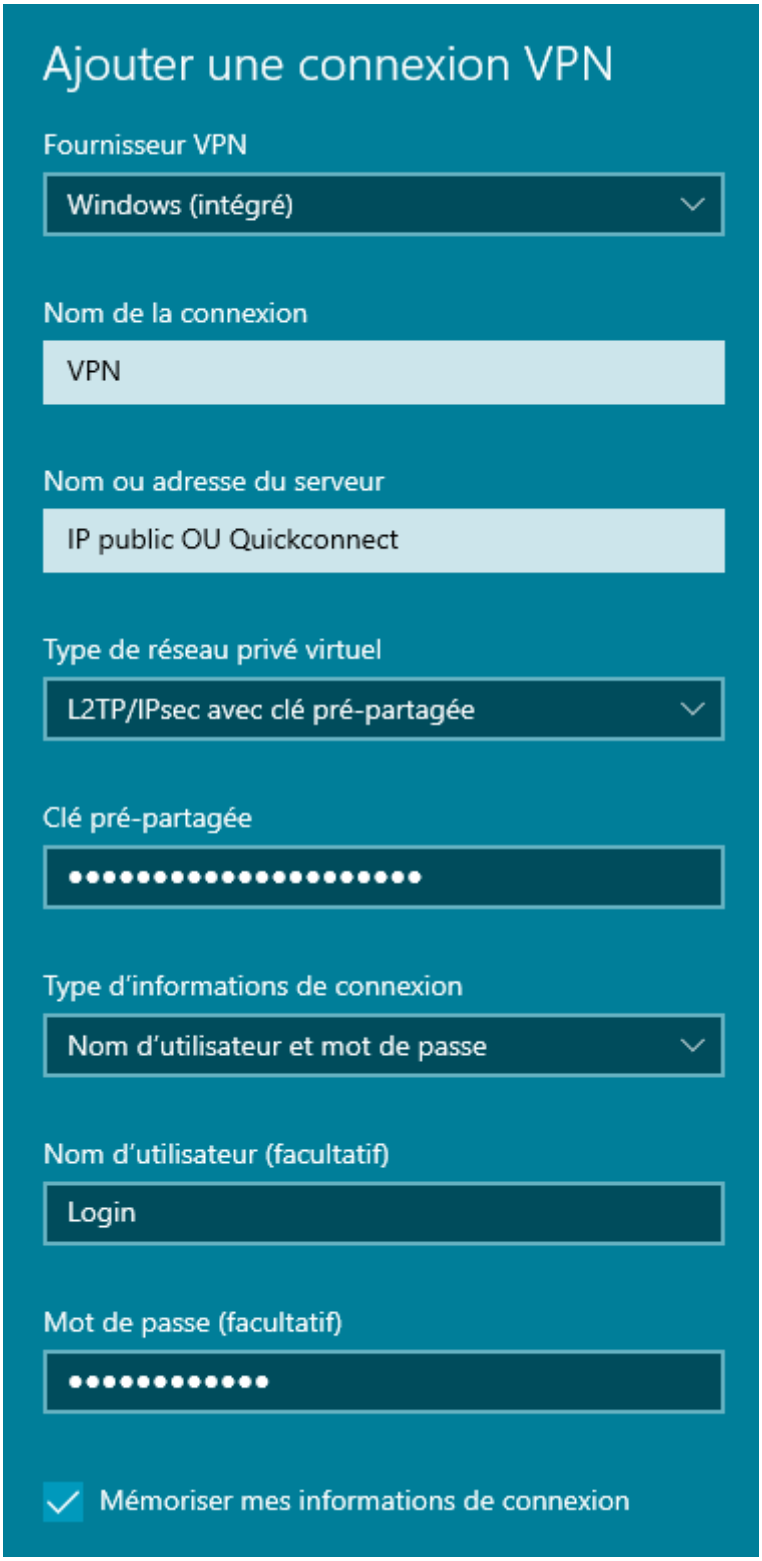
Fournisseur : Windows

Nom ou adresse du serveur : IP Public de la box ou Quickconnect (seulement avec Synology)

Type de réseau privé virtuel : L2TP/IPsec avec clé pré-partagée

Type d'information de connexion : Nom d'utilisateur et mot de passe

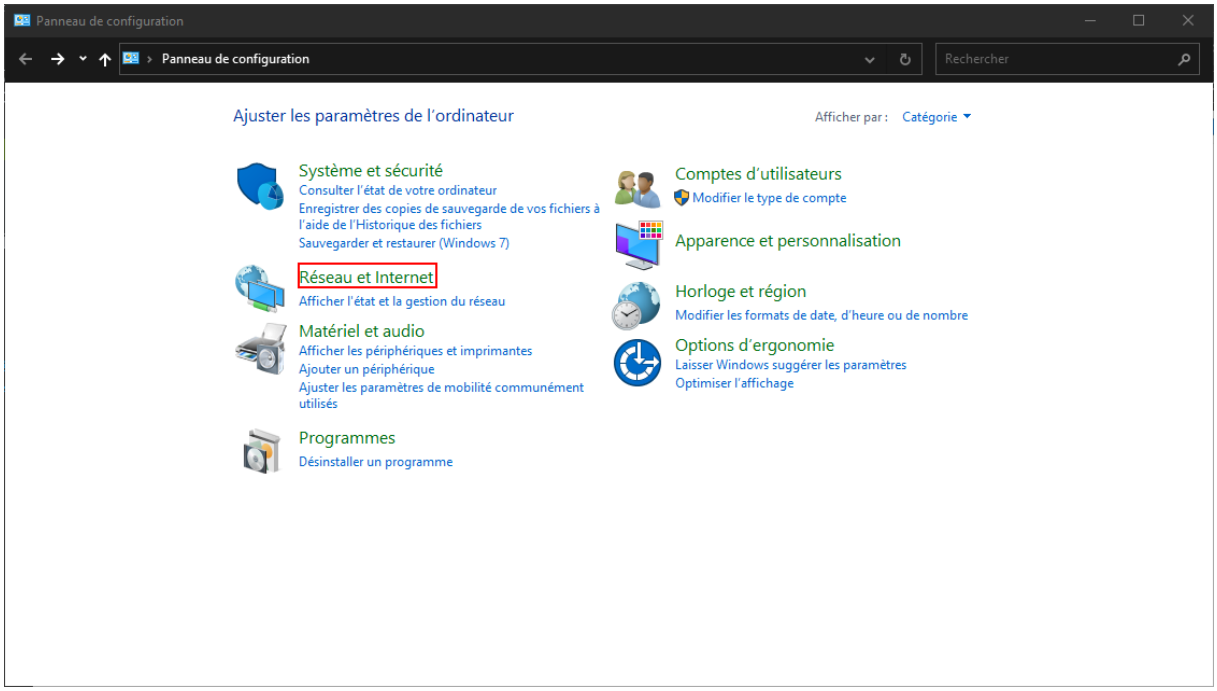
Nom d'utilisateur et mot de passe : utiliser ceux des utilisateurs du NAS/Radius

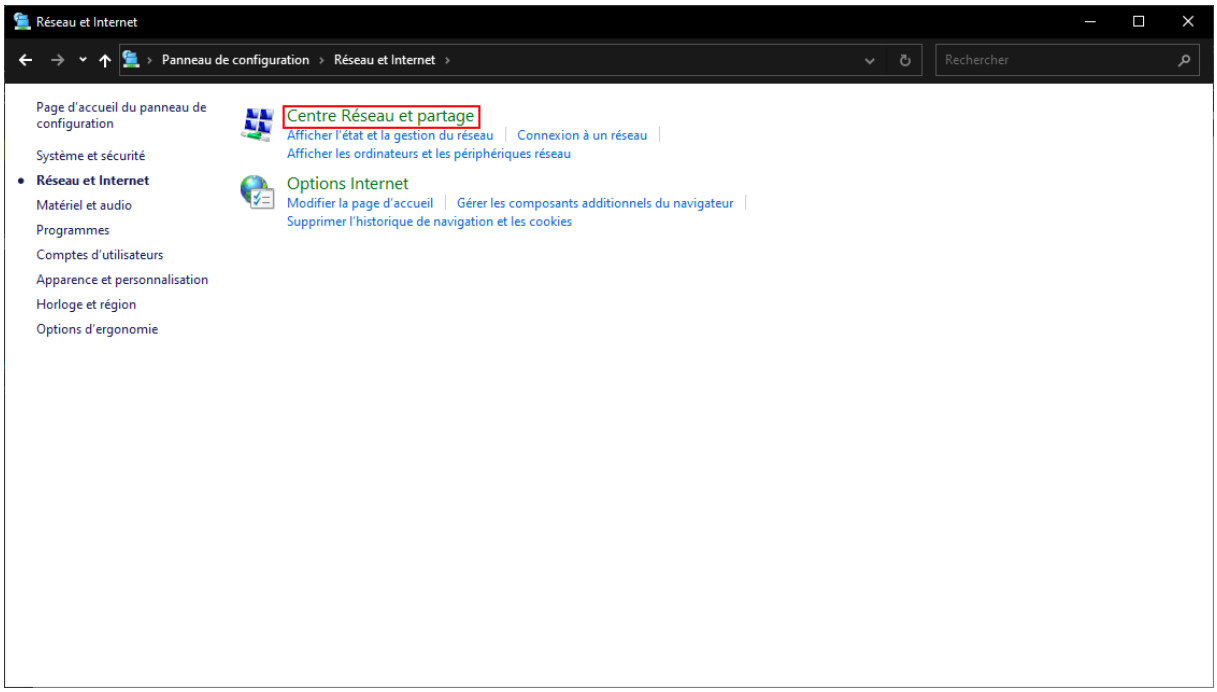


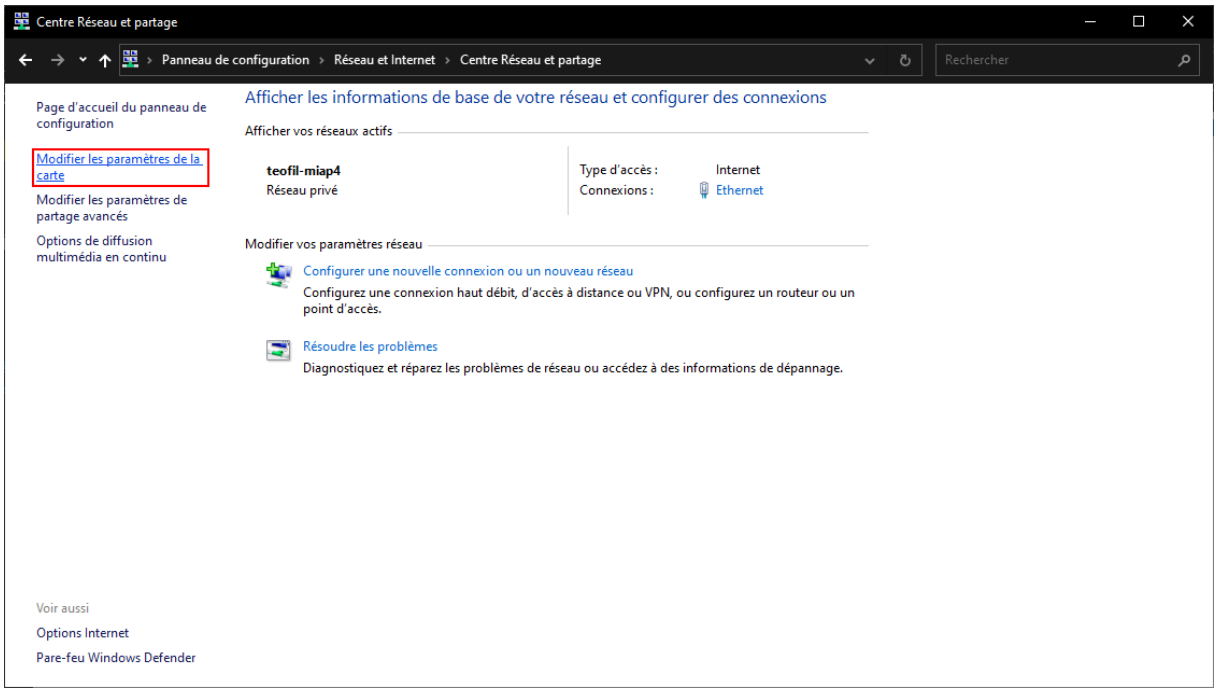
3) Activation du MS-CHAP v2

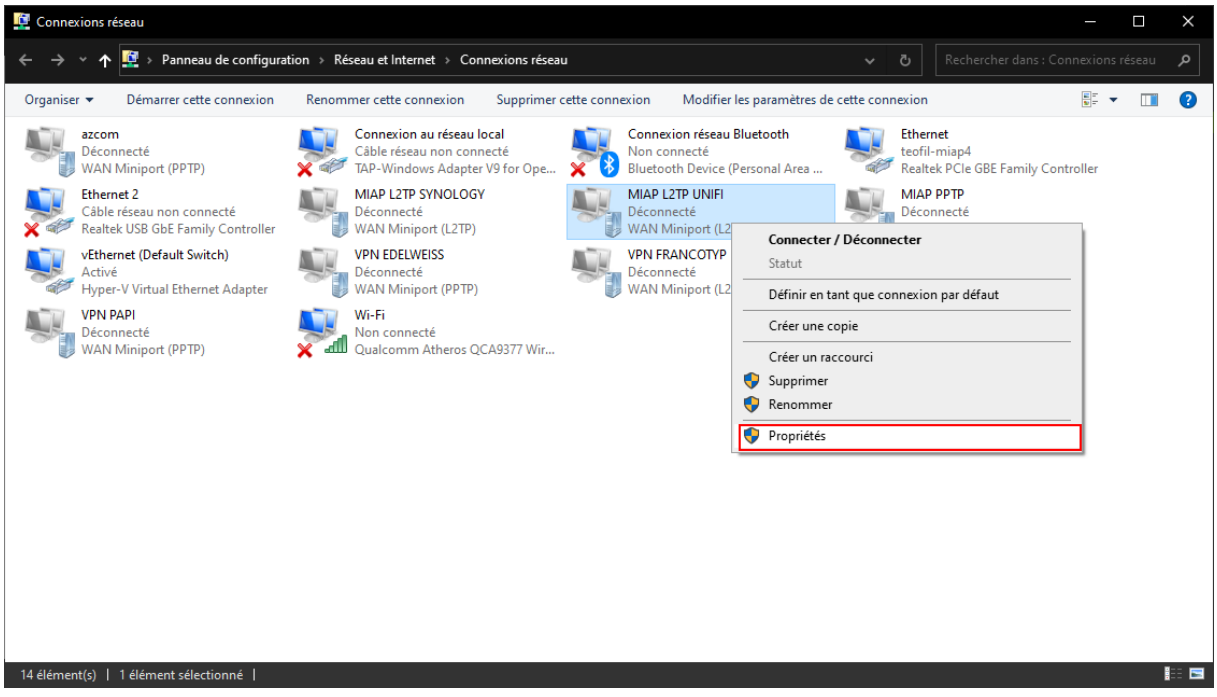
Vérifier que le MS-CHAP v2 est activé sur le profil VPN pour cela aller dans :

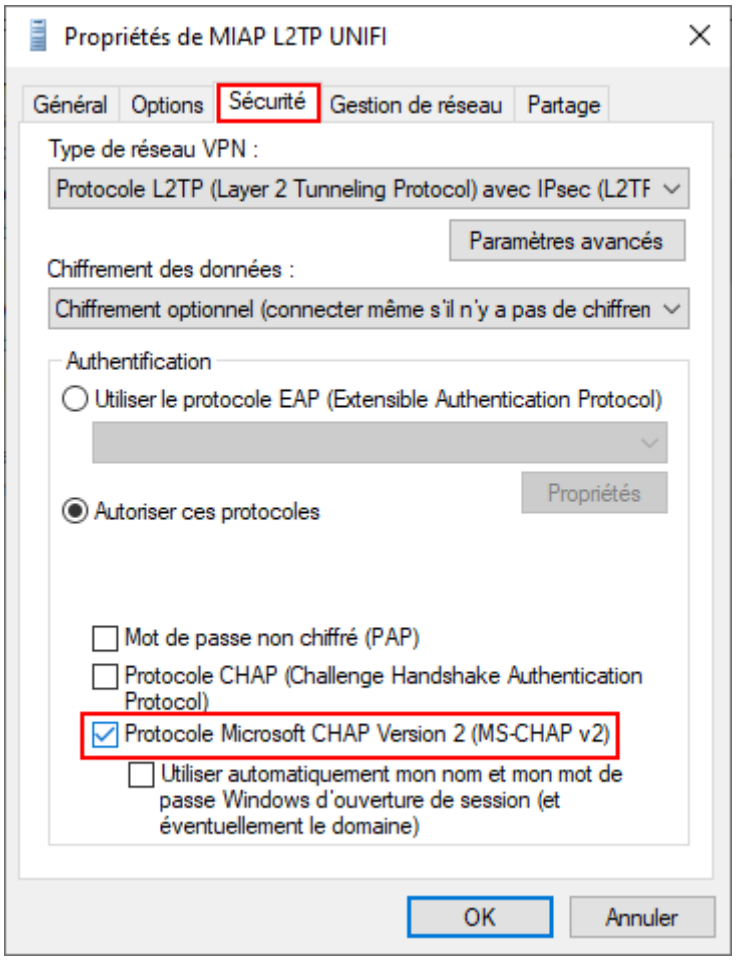
Panneau de Configuration -> Réseau et internet -Centre de Réseau et partage -> Modifier les paramètres de la carte -> Propriétés du profil VPN que l'on vient de créer -> sécurité puis vérifier si la case protocole CHAP Version 2






Centre Réseau et partage
Panneau de configuration › Réseau et Internet › Centre Réseau et partage
Rechercher
Page d'accueil du panneau de configuration
Modifier les paramètres de la carte
Modifier les paramètres de partage avancés
Options de diffusion multimédia en continu
Afficher les informations de base de votre réseau et configurer des connexions
Afficher vos réseaux actifs
teofil-miap4
Réseau privé
Type d'accès : Internet
Connexions : Ethernet
Modifier vos paramètres réseau
Configurer une nouvelle connexion ou un nouveau réseau
Configurez une connexion haut débit, d'accès à distance ou VPN, ou configurez un routeur ou un point d'accès.
Résoudre les problèmes
Diagnostiquez et réparez les problèmes de réseau ou accédez à des informations de dépannage.
Voir aussi
Options Internet
Pare-feu Windows Defender

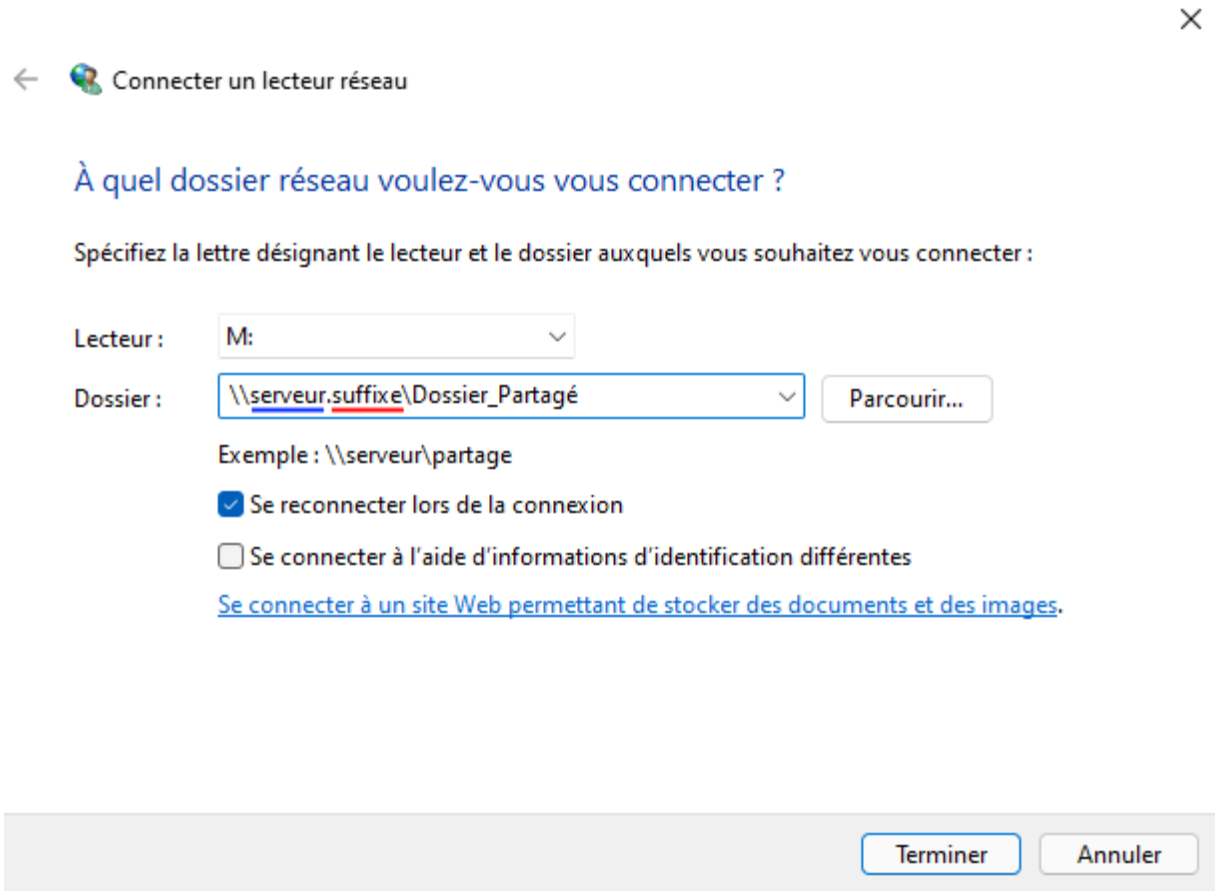

Connexions réseau
Panneau de configuration › Réseau et Internet › Connexions réseau
Rechercher dans : Connexions réseau
Organiser
Démarrer cette connexion
Renommer cette connexion
Supprimer cette connexion
Modifier les paramètres de cette connexion
azcom
Déconnecté
WAN Miniport (PPTP)
Connexion au réseau local
Câble réseau non connecté
TAP-Windows Adapter V9 for Ope...
Connexion réseau Bluetooth
Non connecté
Bluetooth Device (Personal Area ...
Ethernet
teofil-miap4
Realtek PCIe GBE Family Controller
Ethernet 2
Câble réseau non connecté
Realtek USB GbE Family Controller
MIAP L2TP SYNOLOGY
Déconnecté
WAN Miniport (L2TP)
MIAP L2TP UNIFI
Déconnecté
MIAP PPTP
Déconnecté
vEthernet (Default Switch)
Activé
Hyper-V Virtual Ethernet Adapter
VPN EDELWEISS
Déconnecté
WAN Miniport (PPTP)
VPN FRANCOTYP
Déconnecté
VPN PAPI
Déconnecté
WAN Miniport (PPTP)
Wi-Fi
Non connecté
Qualcomm Atheros QCA9377 Wir...
Connecter / Déconnecter
Statut
Définir en tant que connexion par défaut
Créer une copie
Créer un raccourci
Supprimer
Renommer
Propriétés
14 élément(s) | 1 élément sélectionné |


Propriétés de MIAP L2TP UNIFI
Général
Options
Sécurité
Gestion de réseau
Partage
Type de réseau VPN :
Protocole L2TP (Layer 2 Tunneling Protocol) avec IPsec (L2TF
Paramètres avancés
Chiffrement des données :
Chiffrement optionnel (connecter même s'il n'y a pas de chiffren
Authentification
Utiliser le protocole EAP (Extensible Authentication Protocol)
Propriétés
Autoriser ces protocoles
Mot de passe non chiffré (PAP)
Protocole CHAP (Challenge Handshake Authentication Protocol)
Protocole Microsoft CHAP Version 2 (MS-CHAP v2)
Utiliser automatiquement mon nom et mon mot de passe Windows d'ouverture de session (et éventuellement le domaine)
OK
Annuler

V) Mappage de lecteurs réseaux

Pour créer un lecteur réseau accessible depuis une connexion VPN il faut qu'une interface LAN sur le NAS soit en DHCP pour qu'il puisse récupérer le suffixe DNS puis lors du mappage du lecteur le nom et le suffixe DNS soit précisé.

Ou alors utiliser son adresse IP à la place de son nom et du suffixe DNS.

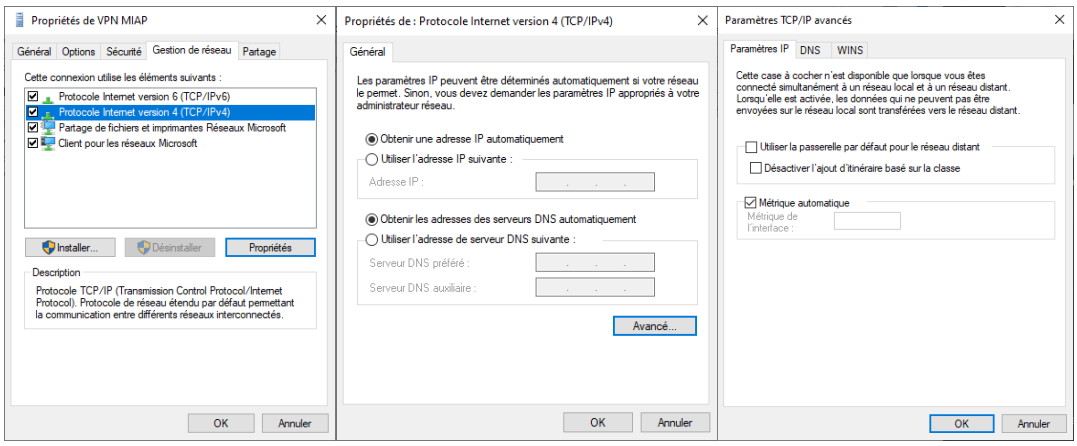


Nom du NAS, suffixe DNS.

VI) Changer de passerelle pour débit internet (Split tunneling) (facultatif)

1) Changer de passerelle

Aller dans Gestion de réseau -> Protocole Internet version 4 (TCP/IPv4) -> Propriétés -> Avancé -> Décocher la case "Utiliser la passerelle par défaut pour le réseau distant"



2) Créer la route pour donner l'accès au réseau distant

Ouvrir l'invite de commande pour créer une route de la manière suivante :

route -p add 192.168.0.0 mask 255.255.255.0 10.2.0.1

Réseau distant auquel on veut accéder, masque du réseau distant, réseau du VPN trouvable dans le VPN Server de Synology ou qui a été créé sur Unifi.

Vérifier que vous ayez accès au NAS par IP et par FQDN en ajoutant un lecteur réseau

!! ATTENION : la réponse au ping peut être longue donc faire un ping avec "ping -t ADRESSE_IP" pour faire un ping en continu

Se connecter au VPN puis vérifier que vous avez accès au LAN en ping le routeur ou l'@IP du NAS

VII) Résolution de problèmes

Tests à faire en cas de blocage :

- Désactiver ce qui peut bloquer (pare feu divers)
- Vérifier le double NAT et les IP
- Reboot ordi
- Reboot box
- Reboot UDM
- Restart serveur VPN
- Essayer d'un autre ordinateur
- Regarder le journal de VPN serveur
- Copier le message d'erreur sur google