

Configuration VPN L2TP Synology ou UDM

Table des matières

Configuration VPN L2TP Synology ou UDM	1
I) Ouvrir les ports correspondant au VPN L2TP	2
II) Configuration du serveur VPN sur SYNOLOGY.....	3
1) Configurer l'adresse externe du SYNOLOGY pour faire du DDNS.....	3
2) Désactiver les passerelles multiples	3
3) Installer le paquet "VPN Server"	4
4) Sélectionner la bonne carte réseau si plusieurs sont disponibles	4
5) Activer le serveur L2TP/IPSec	5
6) Autoriser l'utilisation des services VPN correspondant aux utilisateurs.....	5
III) Configuration du serveur VPN sur UNIFI	6
1) Activer le service radius avec les paramètres par défaut.....	6
2) Créer les utilisateurs radius, sélectionner L2TP et IPv4 en type de tunnel.....	6
3) Créer un réseau pour le VPN L2TP	7
4) Ajouter un suffixe DNS (facultatif).....	8
IV) Connexion au serveur VPN	9
1) Ajouter une clé de registre dans l'éditeur de registre.....	9
2) Création d'un profil VPN.....	9
3) Activation du MS-CHAP v2	11
V) Mappage de lecteurs réseaux	14
VI) Changer de passerelle pour débit internet (Split tunneling) (facultatif).....	15
1) Changer de passerelle	15
2) Créer la route pour donner l'accès au réseau distant	15
VII) Résolution de problèmes	16

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.

BUREAU UDMPRO-MI...		CONNECTÉ	⋮	⋮	X	⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮
						⋮
APERÇU						⋮
Adresse MAC						
Modèle					UDM-Pro	
Version					1.10.0.3686	
Adresse IP (WAN)						
Adresse IP (LAN)						
Durée de connexion					4d 10h 46m 41s	
Utilisation de la mémoire					69%	
Charge Moyenne					2.33 / 1.49 / 1.37	
# Utilisateurs					26	
# Invités					0	

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.

Utilisateur				
VPN L2TP vers UDM	UDP	500 • 500	500 • 500	on
	UDP	4500 • 4500	4500 • 4500	on
	UDP	1701 • 1701	1701 • 1701	on

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

The screenshot shows the Synology DSM Control Panel with the following details:

- Panneau de configuration** window title.
- DDNS** tab selected.
- Configuration du routeur** and **Avancé** tabs available.
- Ajouter**, **Modifier**, **Supprimer**, **Mettre à jour maintenant**, and **Personnaliser** buttons.
- Fournisseur d...**, **Nom d'hôte**, **Adresse ext...**, and **Statut** columns.
- A single entry listed: **Synology** (Fournisseur), **nas-miap2.synology....** (Nom d'hôte), **80.118.241....** (Adresse ext...), and **Normal** (Statut).
- Dernière heure...** and **27/04/2021 1...** status indicators.
- Partage de fichiers**, **Connectivité**, **Accès externe** (highlighted in blue), and **Réseau** sections in the sidebar.

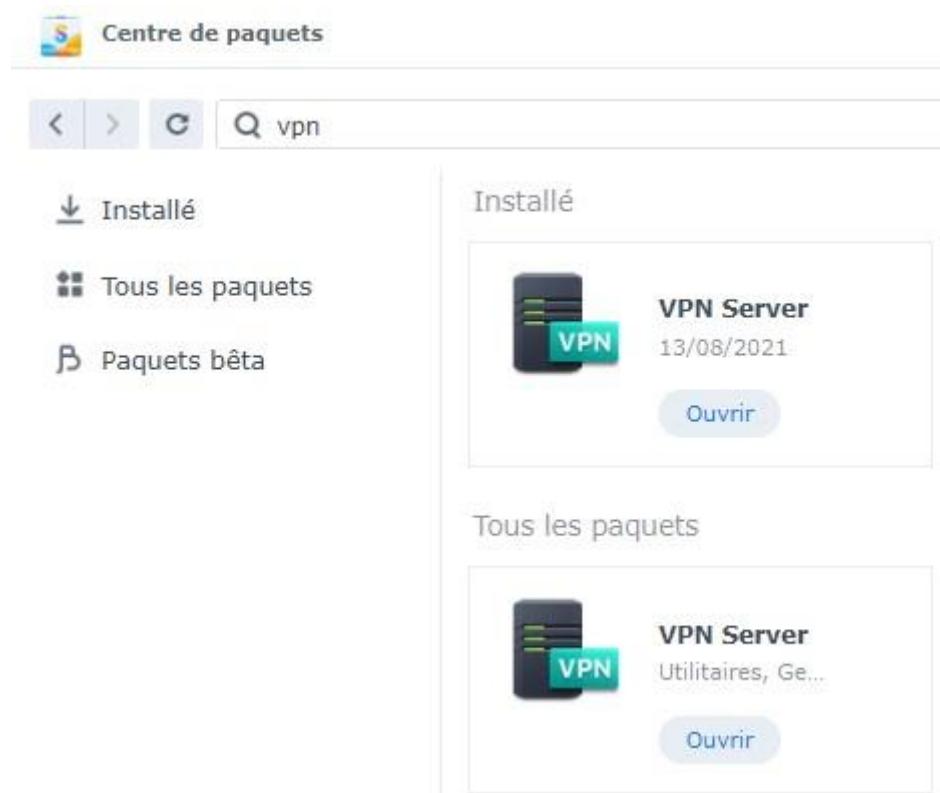
2) Désactiver les passerelles multiples

The screenshot shows the Synology DSM Control Panel with the following details:

- Panneau de configuration** window title.
- Général** tab selected.
- Interface réseau**, **Contrôle du trafic**, **Route statique**, and **Paramètres de DSM** tabs available.
- General** section:
 - Entrez le nom du serveur, les informations du serveur DNS et de la passerelle par défaut.
 - Nom de serveur:** nas-miap2
 - Passerelle par défaut:** 192.168.1.1
 - Passerelle IPv6 par défaut:** -
 - Configurer manuellement le routeur:**
 - Servere DNS préféré:** 1
 - Servere DNS de remplacement:** -
 - Paramètres avancés** button.
- Paramètres avancés** panel:
 - Répondez à la demande ARP si l'adresse cible IP est identique à l'adresse locale configurée sur l'interface entrante.
 - Activer les passerelles multiples
 - Activer la détection des conflits IP
- Proxy** section:
 - Se connecter via un serveur proxy
 - Adresse: -
 - Port: -
- OK** and **Annuler** buttons.
- Réinitialiser** button at the bottom right.
- Connexion**, **Accès externe** (highlighted in blue), **Réseau**, **Servere DHCP**, **Sécurité**, **Système**, **Centre d'infos**, **Thème**, and **Options régionales** sections in the sidebar.

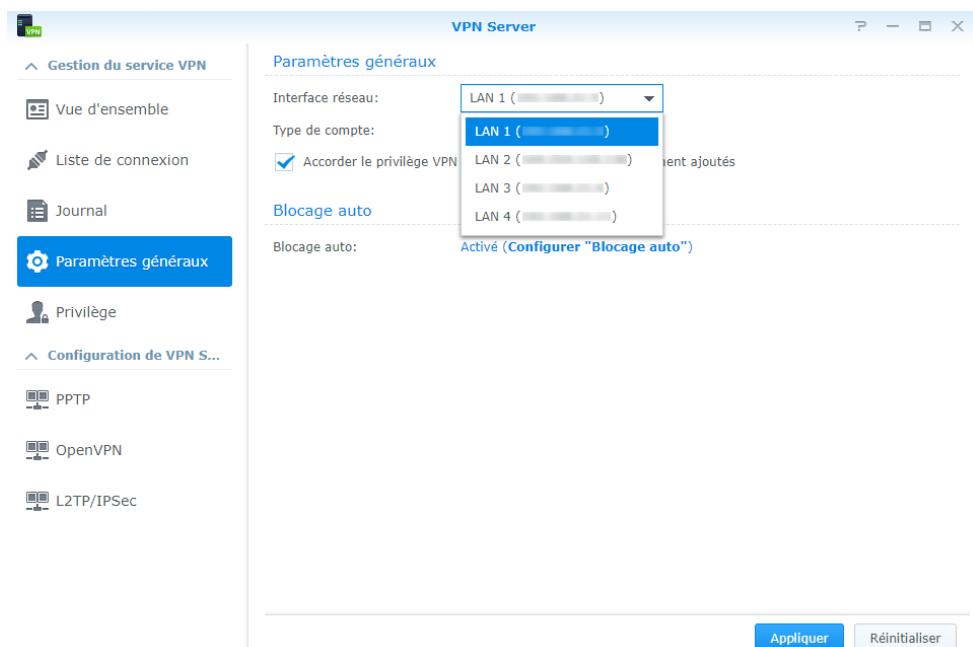
Panneau de configuration -> Réseau -> Général -> Paramètres avancés

3) Installer le paquet "VPN Server"



Rechercher « VPN » depuis le centre de paquets

4) Sélectionner la bonne carte réseau si plusieurs sont 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

The screenshot shows the "L2TP/IPSec" configuration page within the "VPN Server" application. On the left, a sidebar lists various VPN services: "Vue d'ensemble", "Liste de connexion", "Journal", "Paramètres généraux", "Privilège", "PPTP", "OpenVPN", and "L2TP/IPSec", which is highlighted with a blue box. The main panel is titled "L2TP/IPSec" and contains the following settings:

- Activer le serveur L2TP/IPSec VPN**: Checked.
- Adresse IP dynamique:** 10 . 2 . 0 . 0
- Nombre de connexions maximales:** 5
- Nombre maximum de connexions d'un compte:** 3
- Authentification:** MS-CHAP v2
- MTU:** 1400
- Utiliser le DNS manuel**: Unchecked.
- Exécuter en mode noyau (kernel)**: Unchecked.
- Authentification IKE**: Fields for "Clé pré-partagée" and "Confirmer la clé pré-partagée" both contain "*****".
- Activer le mode compatible SHA2-256 (96 bits)**: Checked.

At the bottom right are "Appliquer" and "Réinitialiser" buttons.

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

The screenshot shows the "Privilège" configuration page within the "VPN Server" application. On the left, a sidebar lists "Vue d'ensemble", "Liste de connexion", "Journal", "Paramètres généraux", and "Privilège", which is highlighted with a blue box. The main panel displays a table of users and their privileges for PPTP, OpenVPN, and L2TP/IPSec:

Nom d'utilisateur	Statut	PPTP	OpenV...	L2TP/I...
admin	Désactivé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
apprenti1	Normal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
apprenti2	Normal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ass.syno	Normal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
e.housseau	Normal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
g.chaves	Désactivé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
guest	Désactivé	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I.lecoq	Normal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ml.huynh	Désactivé	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
superviseur	Normal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
v.kerouanton	Normal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

At the bottom right, it says "11 élément(s)" and has a refresh icon.

III) Configuration du serveur VPN sur UNIFI

1) Activer le service radius avec les paramètres par défaut

The screenshot shows the 'PARAMÈTRES' (Parameters) section of the Unifi Controller interface. The left sidebar has a blue highlight over the 'Services' category. The main panel is titled 'RADIUS' with tabs for 'HOTSPOT 2.0' (disabled), 'DHCP', 'DNS DYNAMIQUE', 'MDNS', 'SIP' (Beta), and 'SNMP'. Under the 'Utilisateurs' tab, there's a checkbox for 'Activer le serveur RADIUS' (Enable RADIUS server) which is checked and set to 'ON'. Below it, 'Secret' is listed as a masked password. Under 'Clients', 'Port d'authentification' is set to 1812 and 'Port de comptabilité' is set to 1813. 'Intervalle comptable intermédiaire' is set to 3600. 'Réponse Tunnelé' is also checked and set to 'ON'. At the bottom are green 'APPLIQUER LES CHANGEMENTS' (Apply Changes) and grey 'RÉINITIALISER' (Reset) buttons.

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

The screenshot shows the 'MODIFIER L'UTILISATEUR RADIUS ALOUIS' (Modify RADIUS User ALouis) configuration page. The left sidebar has a blue highlight over the 'Services' category. The main panel shows fields for 'Name' (ALouis), 'Mot de passe' (password), 'VLAN' (VLAN), 'Type de tunnel' (Tunnel Type) set to '3 - Layer Two Tunneling Protocol (L2TP)', and 'Type de tunnel' (Tunnel Type) set to '1 - IPv4 (IP version 4)'. At the bottom are green 'ENREGISTRER' (Register) and grey 'ANNULER' (Cancel) buttons.

3) Créer un réseau pour le VPN L2TP

The screenshot shows the 'PARAMÈTRES' sidebar with 'Réseaux' selected. The main panel is titled 'MODIFIER LE RÉSEAU - VPN L2TP'. The configuration fields include:

- Nom:** VPN L2TP
- Usage:** Utilisateur VPN distants (selected)
- VPN Type:** Serveur L2TP
- Pre-Shared Key:** *****
- Interface:** WAN (selected)
- IP passerelle / Sous-réseau:** 192.168.24.0 (with a help icon)
- Network IP Count:** 14
- Network IP Range:** 192.168.24.1 - 192.168.24.14
- IP Pool:** (empty)
- Serveur de Nom:** Auto (selected)
- RADIUS:**
 - Profil RADIUS: Default
 - Créer un nouveau profil RADIUS
 - MS-CHAP v2: checked

At the bottom are 'ENREGISTRER' and 'ANNULER' buttons.

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

Réseaux

MODIFIER LE RÉSEAU - LAN MIAP

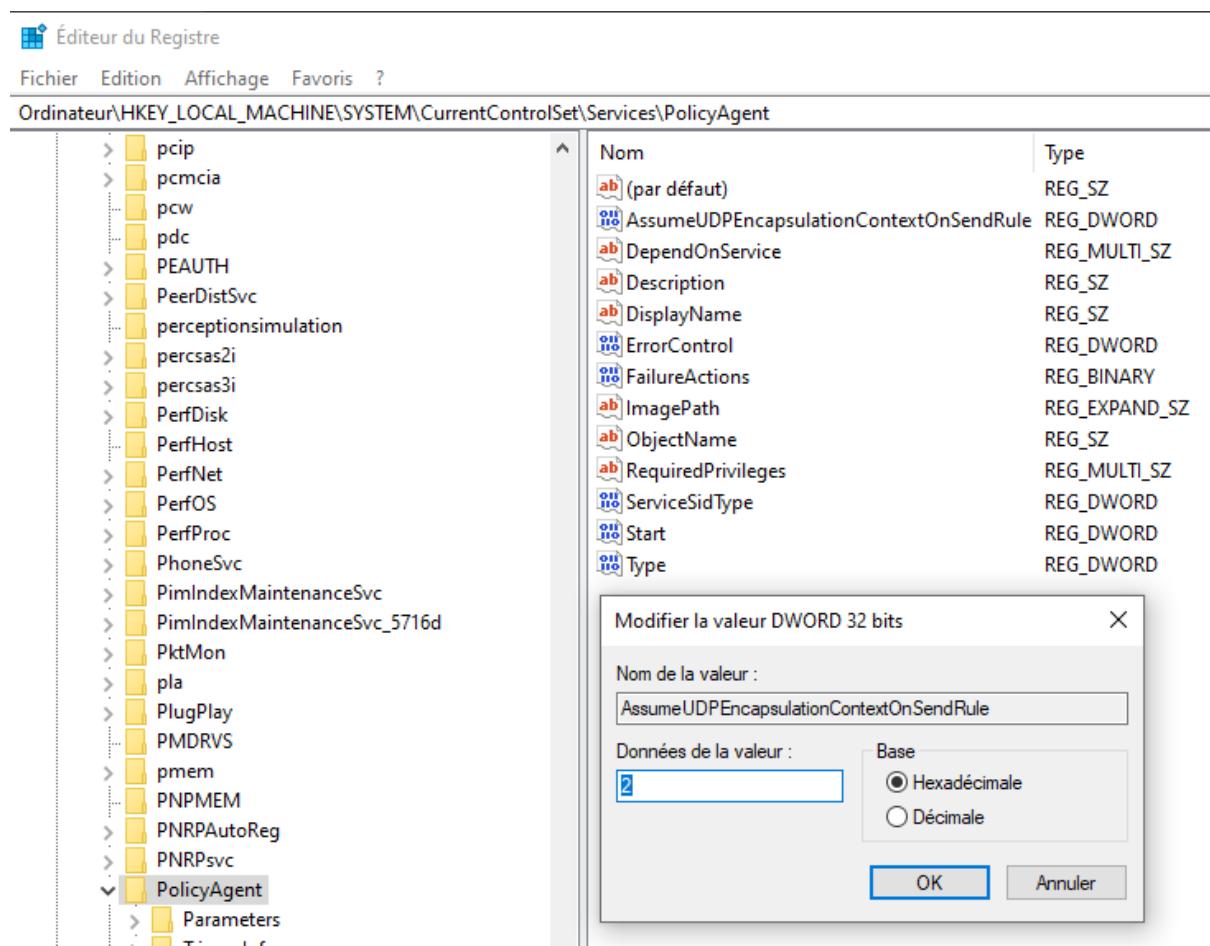
Paramètre	Valeur
Nom	LAN miap
Usage	<input checked="" type="radio"/> Entreprise <input type="radio"/> Invité <input type="radio"/> WAN <input type="radio"/> VLAN seulement <input type="radio"/> Utilisateur VPN distants
Sauvegarde UniFi LTE	<input checked="" type="checkbox"/> Activer la sauvegarde UniFi LTE
Interface	<input checked="" type="radio"/> LAN <input type="radio"/> Par défaut <input type="radio"/> Switch
Type de Gateway	ALPHA
IP passerelle / Sous-réseau	Gateway IP Network Broadcast IP Network IP Count Network IP Range Network Subnet Mask
Nom de Domaine	[redacted]
IGMP Snooping	<input type="checkbox"/> Activer l'IGMP snooping
Mode DHCP	<input checked="" type="radio"/> Serveur DHCP <input type="radio"/> Relais DHCP <small>BETA</small> <input type="radio"/> Aucun

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

Ajouter une connexion VPN

Fournisseur VPN

Windows (intégré) ▾

Nom de la connexion

VPN

Nom ou adresse du serveur

IP public OU Quickconnect

Type de réseau privé virtuel

L2TP/IPsec avec clé pré-partagée ▾

Clé pré-partagée

••••••••••••••••

Type d'informations de connexion

Nom d'utilisateur et mot de passe ▾

Nom d'utilisateur (facultatif)

Login

Mot de passe (facultatif)

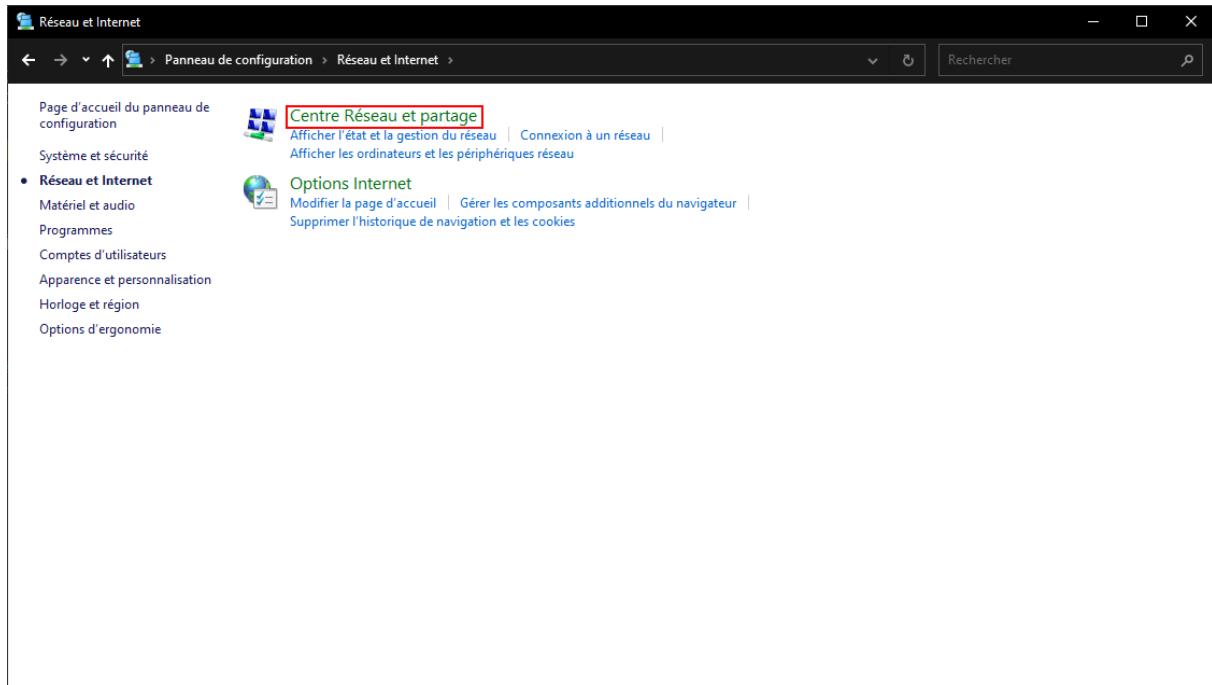
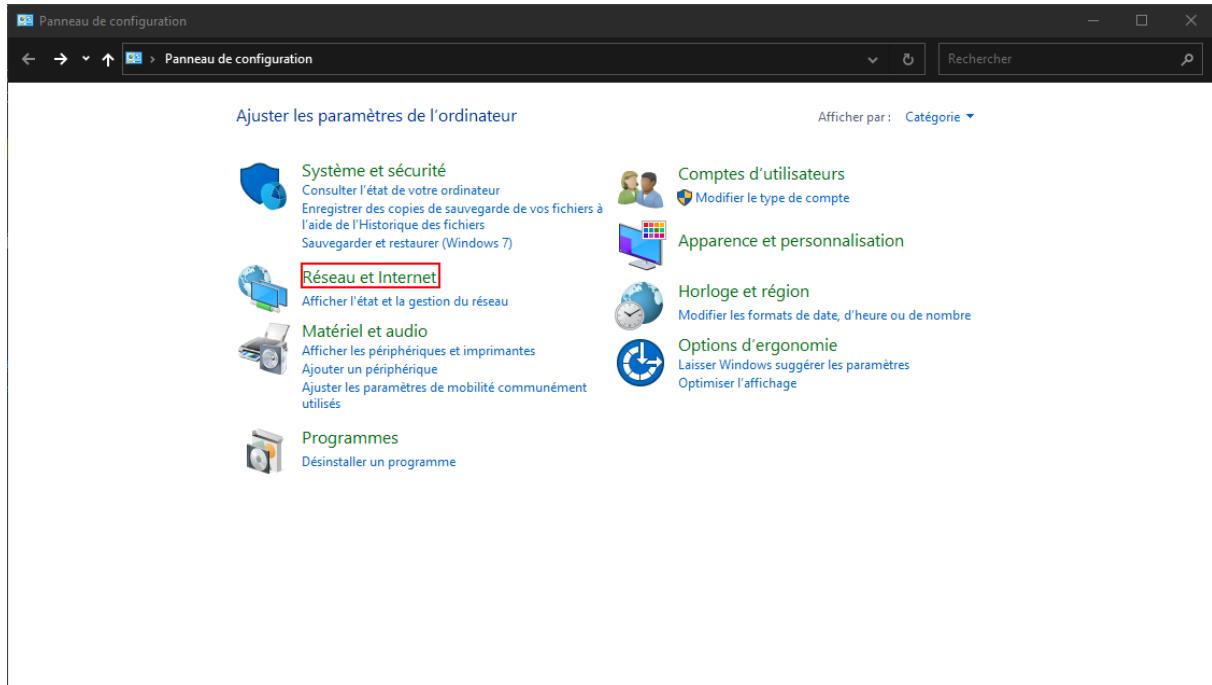
••••••••••

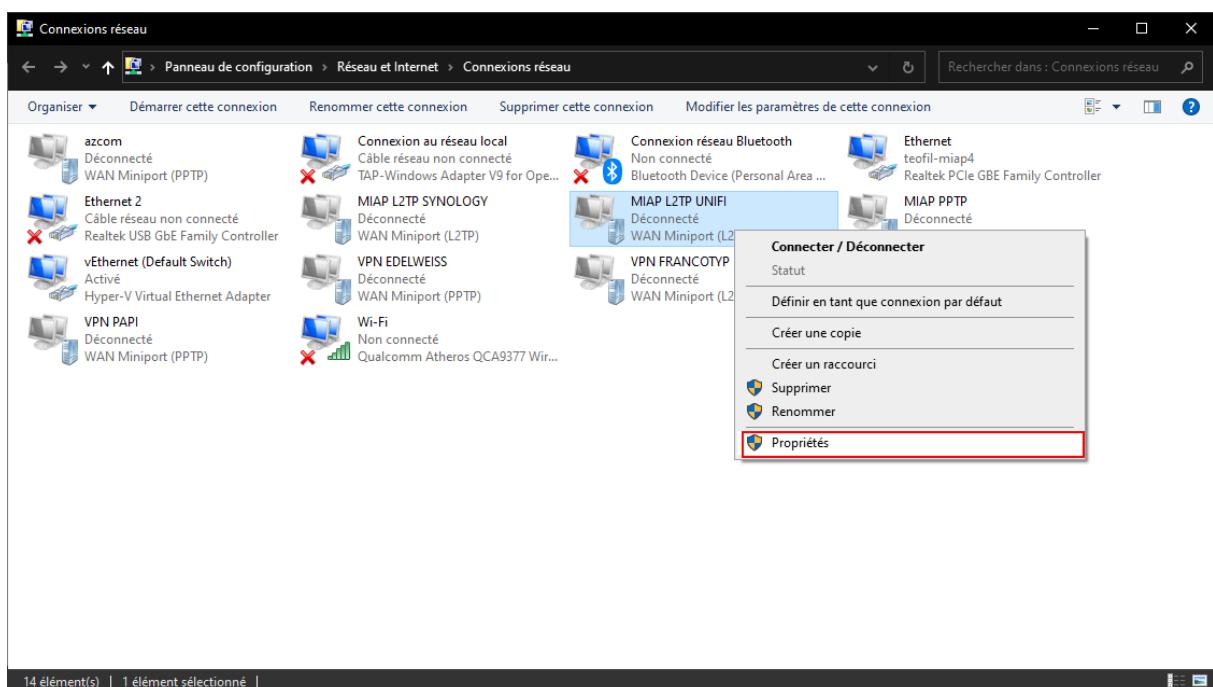
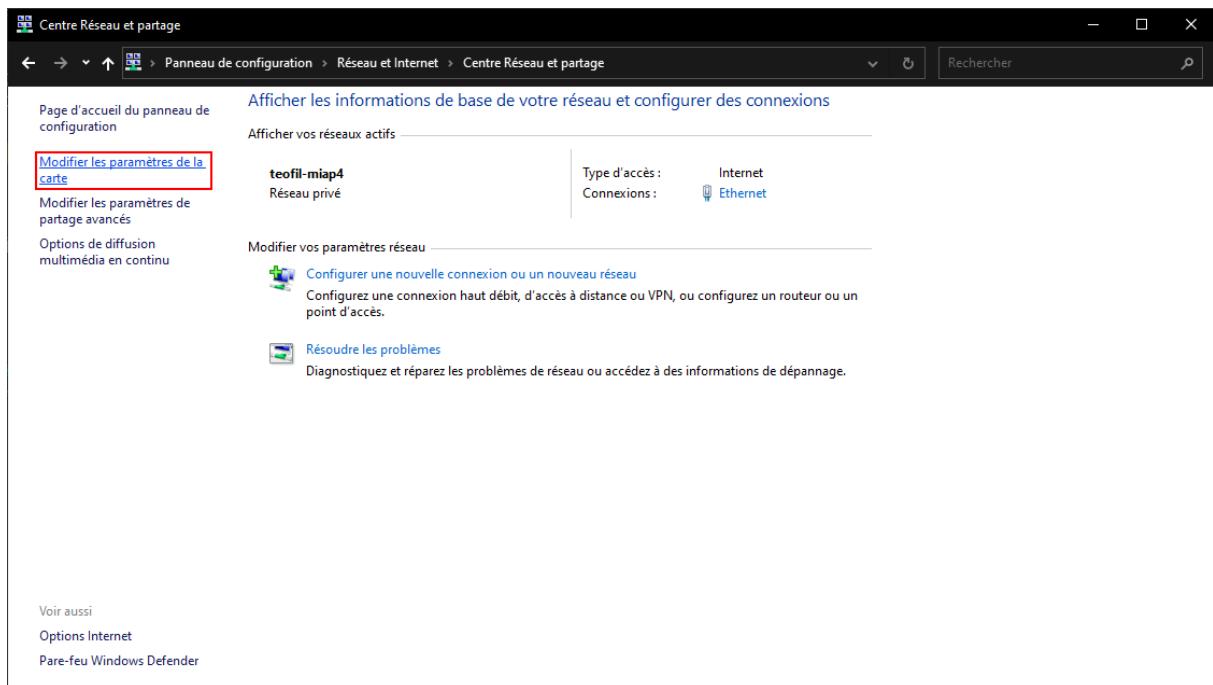
Mémoriser mes informations de connexion

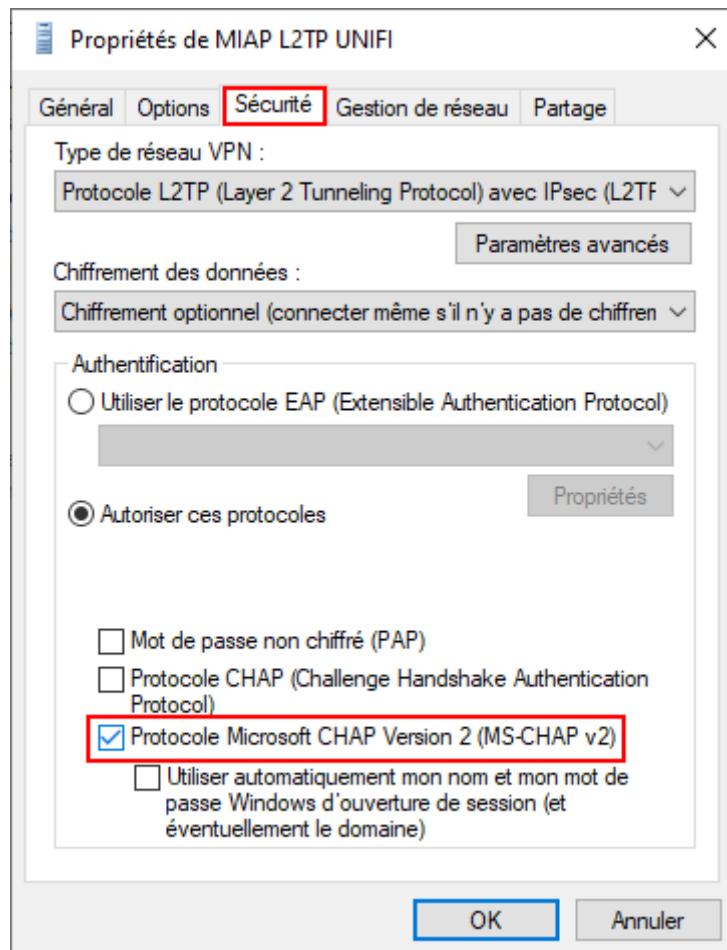
3) Activation du MS-CHAP v2

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



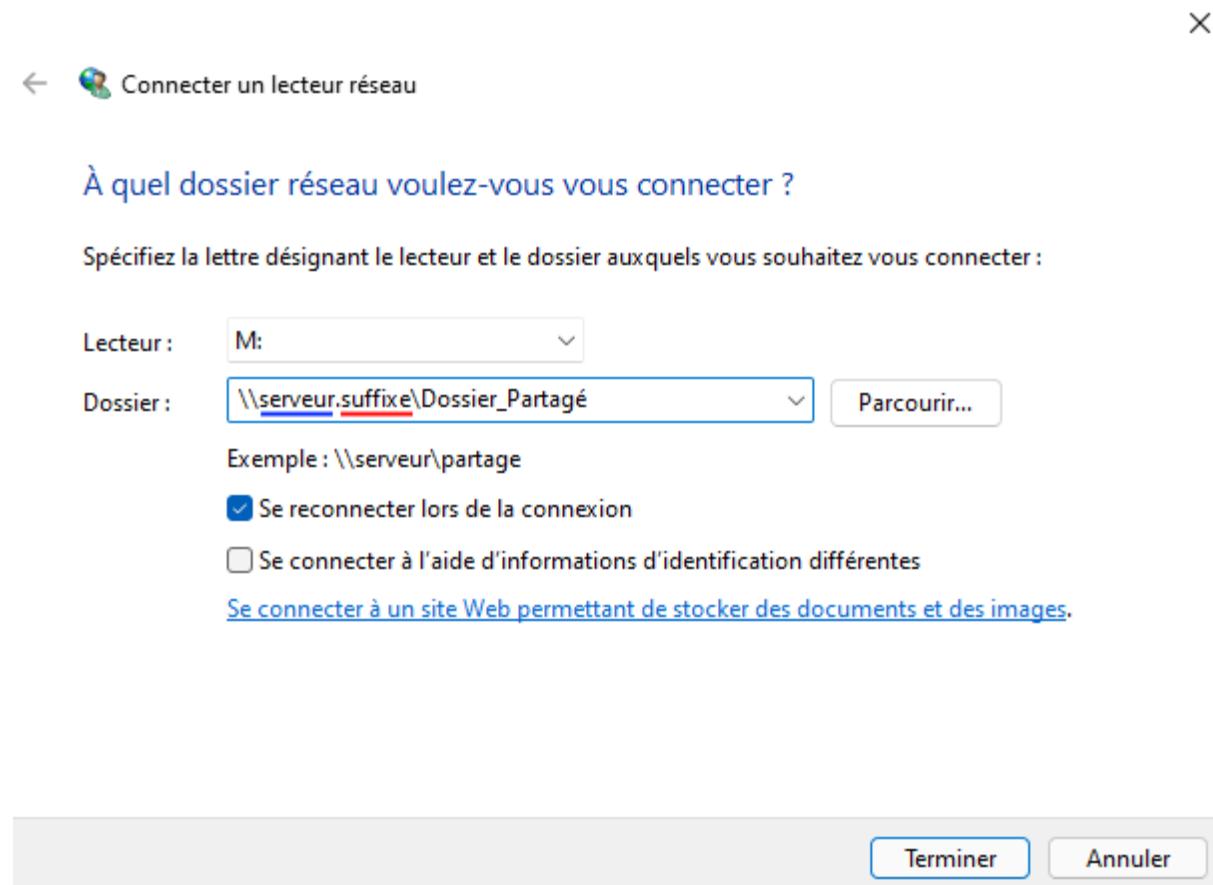




V) Mappage de lecteurs réseaux

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.

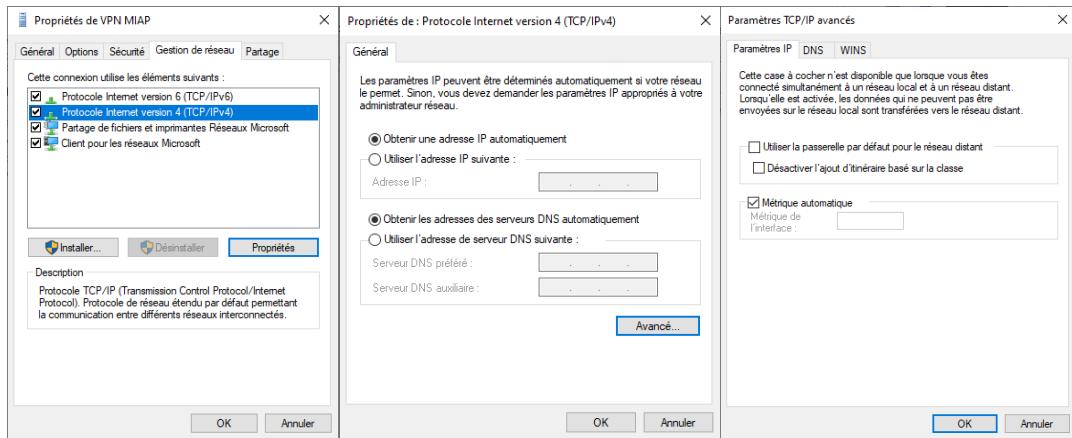


Nom du NAS, **suffixe DNS**.

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 -> Découcher 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

!! ATTENTION : 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