

Configuration serveur OpenVPN Synology (UDM incompatible)

Table des matières

Configuration serveur OpenVPN Synology (UDM incompatible)	1
I) Ouvrir les ports correspondant à OpenVPN	1
II) Configuration du serveur VPN sur SYNOLOGY.....	2
1) Configurer DDNS	2
2) Désactiver les passerelles multiples	2
3) Installer le paquet "VPN Server"	3
4) Sélectionner la bonne carte réseau si plusieurs sont disponibles.....	3
5) Activer OpenVPN.....	4
6) Exporter la configuration.....	4
7) Autoriser l'utilisation des services VPN correspondant aux utilisateurs	4
III) Connexion au serveur via le client OpenVPN	5
IV) Ajouter une entrée dans le fichier hosts de Windows résoudre le nom du NAS (facultatif).....	6
V) Résolution de problèmes	7

**Cette procédure concerne la configuration d'un serveur
OpenVPN sur un NAS SYNOLOGY**

I) Ouvrir les ports correspondant à OpenVPN

Sur le panneau d'administration du routeur, il faut ouvrir le port 1194 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.

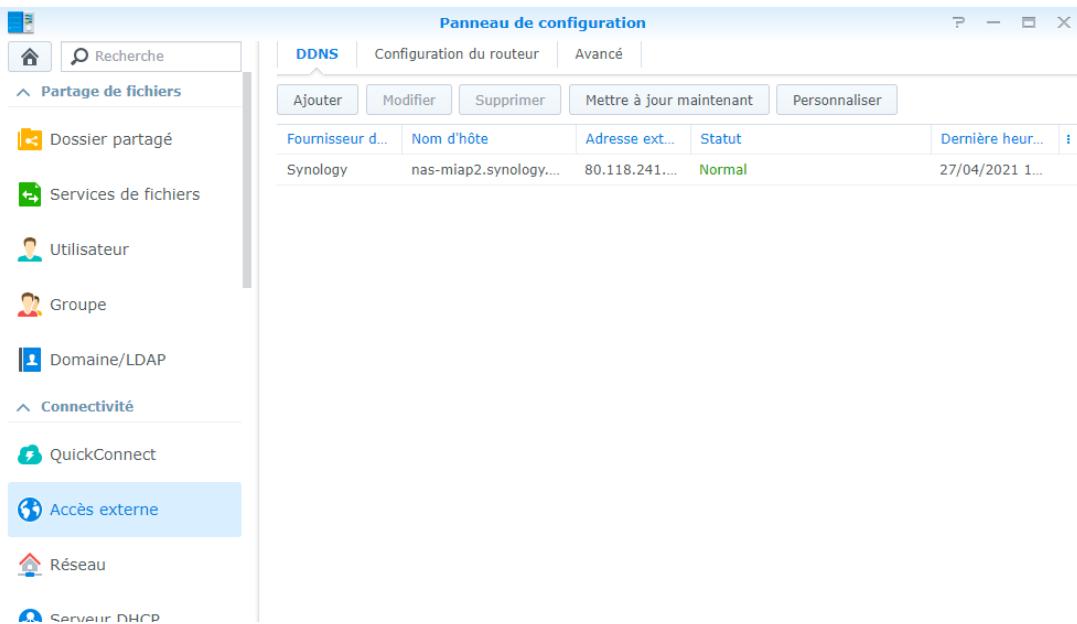
PARAMÈTRES		ROUTES STATIQUES	PARE-FEU	REDIRECTION DE PORT	FILTRAGE IP GÉOGRAPHIQUE	BETA
Site	NOM ↑	FROM	PORT	DEST IP/PORT	ACTIVE	INTERFACE WAN
Réseaux sans fil	OpenVPN	*	1194	192.168.215.1194	✓	WAN
Réseaux	VPN L2TP	*	500,1701,4500	192.168.215.500,1701,4500	✓	WAN
Routage & Pare-feu	VPN PPTP	*	1723	192.168.215.1723	✓	WAN
Gestion des menaces	+ CRÉER UNE NOUVELLE RÈGLE DE TRANSFERT DE PORT					

!! 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

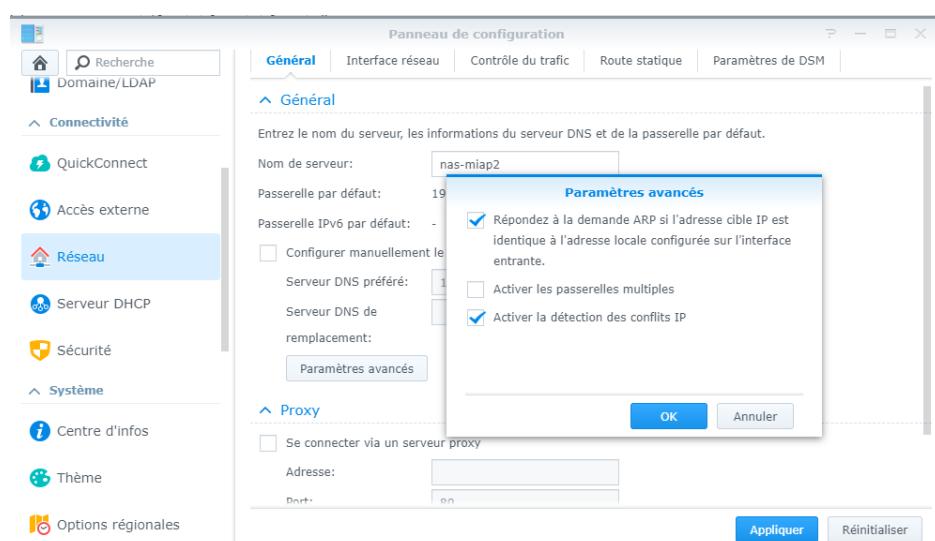
1) Configurer DDNS

Pour cela il faut se rendre dans "Panneau de configuration" puis "Accès externe" puis "Ajouter", sélectionner le service Synology puis entrée un nom d'hôte

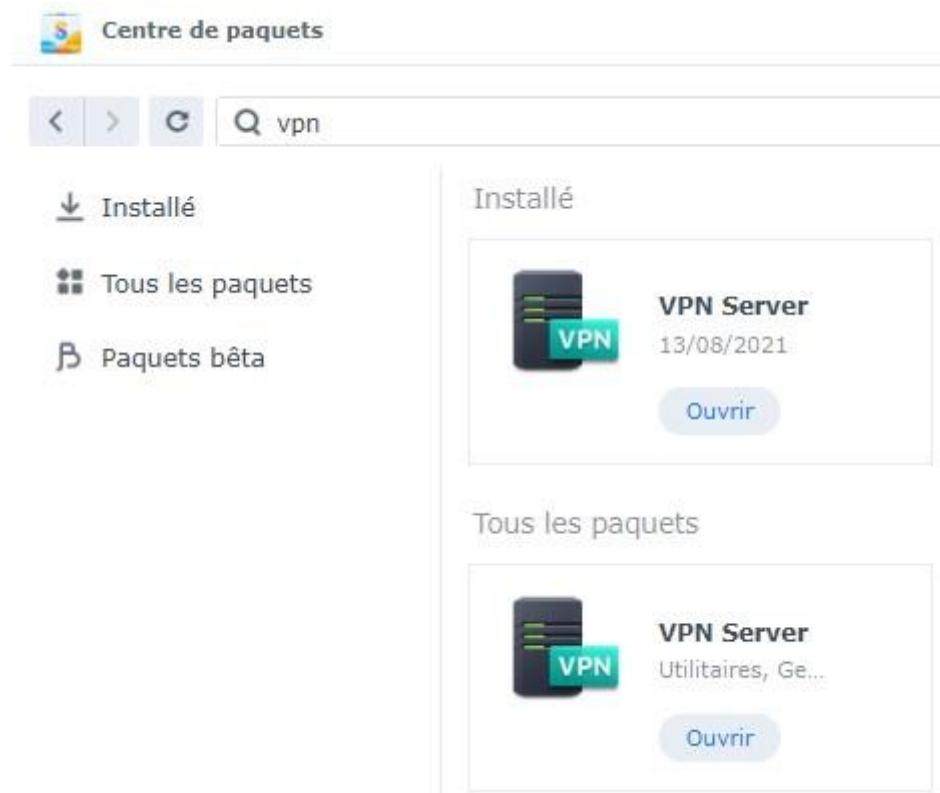


2) Désactiver les passerelles multiples

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

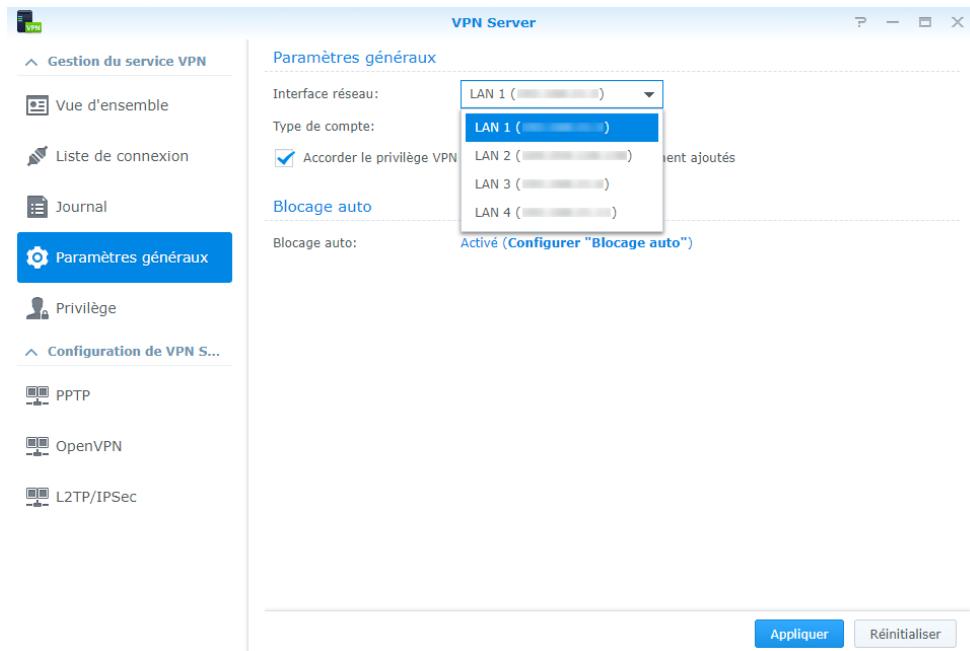


3) Installer le paquet "VPN Server"



Rechercher « VPN » depuis le centre de paquets

4) Sélectionner la bonne carte réseau si plusieurs sont disponibles

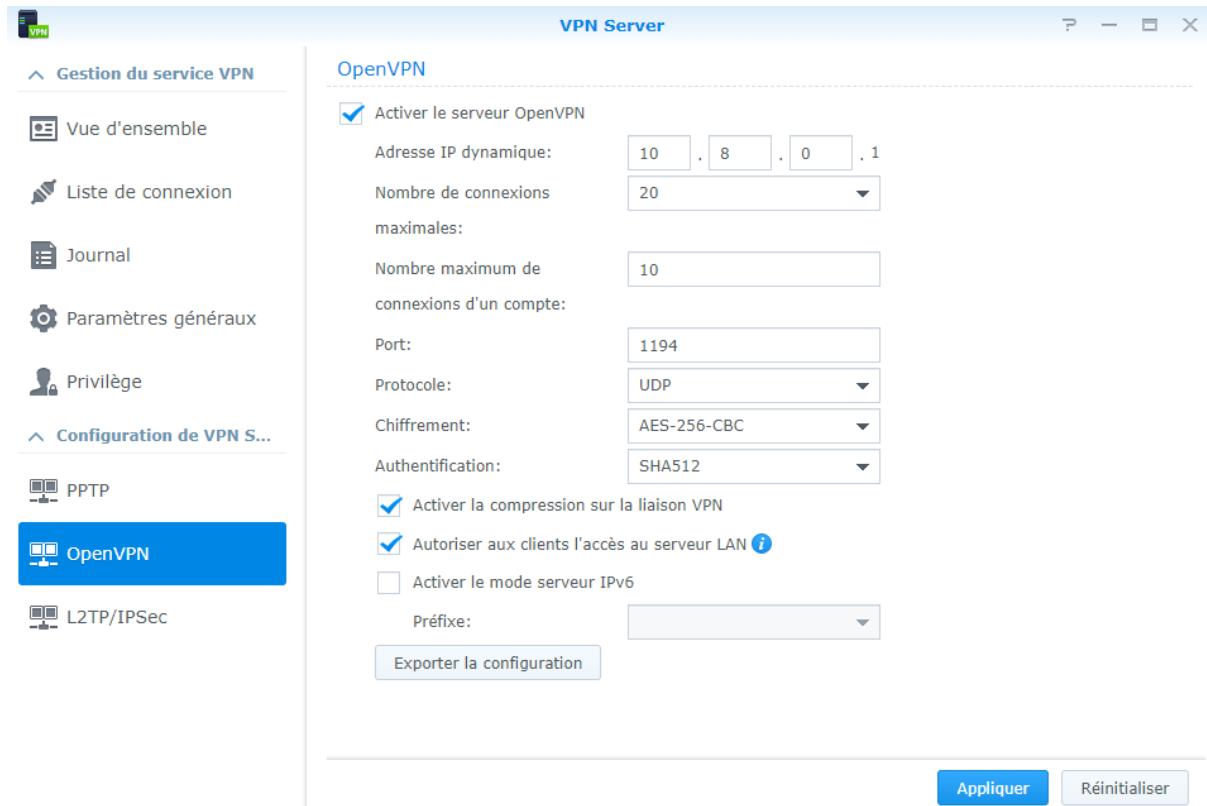


Lancer le "VPN Server" et se rendre dans "Paramètres généraux" pour s'assurer que ce soir la bonne carte réseau qui soit sélectionnée.

5) Activer OpenVPN

6) Exporter la configuration

Permet de télécharger la configuration du serveur avec la clé de chiffrement, le certificat correspondant...



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

The screenshot shows the 'VPN Server' user management interface. On the left, a sidebar lists options: Gestion du service VPN (Vue d'ensemble, Liste de connexion, Journal, Paramètres généraux, Privilège), Configuration de VPN S... (PPTP, OpenVPN, L2TP/IPSec). The 'Privilège' option is selected and highlighted in blue. The main panel displays a table of users and their privileges for PPTP, OpenVPN, and L2TP/IPSec services:

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"/>
l.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) Connexion au serveur via le client OpenVPN

Télécharger le client OpenVPN Connect sur le site officiel puis l'installer

<https://openvpn.net/client-connect-vpn-for-windows/>

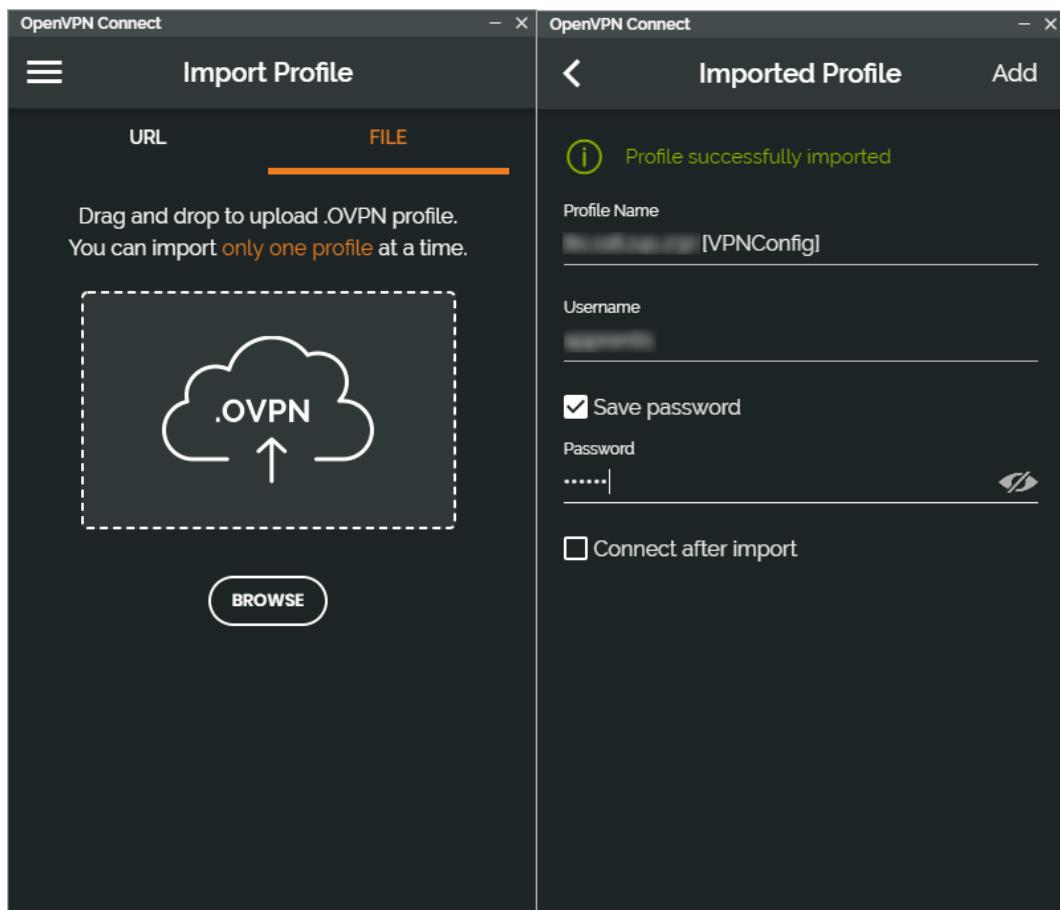
Décompresser le dossier OpenVPN téléchargé plus haut

Modifier via NotePadd++ le fichier VPNConfig.ovpn :

- ligne 4 "remote YOUR_SERVER_IP 1194" changer YOUR_SERVER_IP par l'adresse IP du routeur du FAI

Ajouter la ligne "**client-cert-not-required**" pour ne plus être embêté par le message d'erreur de certificat

Ouvrir OpenVPN et importer le fichier que nous venons de modifier puis sauvegarder



IV) Ajouter une entrée dans le fichier hosts de Windows résoudre le nom du NAS (facultatif)

Uniquement pour faire de la résolution de nom

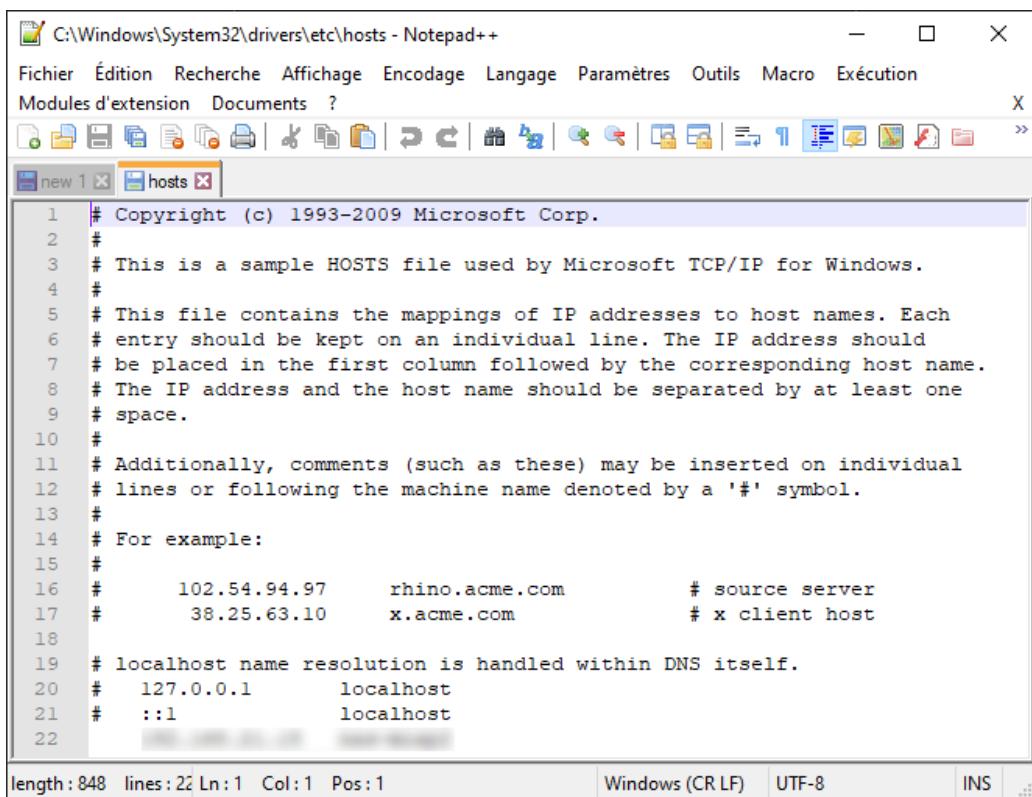
Ajouter dans le fichier OpenVPN cette option :

```
# dhcp-option DNS: To set primary domain name server address.  
dhcp-option DNS 192.168.3.1
```

ou par le fichier ci dessous (moins bien car intervention sur tous les postes) :

Le fichier se trouve à l'emplacement : C:\Windows\System32\drivers\etc\hosts

Avec un clic droit sur hosts faire Edit with Notepad++ puis ajouter une entrée avec l'adresse IP en premier puis le nom à résoudre en second espacé d'un TAB



The screenshot shows the Notepad++ application window with the file 'hosts' open. The content of the file is as follows:

```
1 # Copyright (c) 1993-2009 Microsoft Corp.  
2 #  
3 # This is a sample HOSTS file used by Microsoft TCP/IP for Windows.  
4 #  
5 # This file contains the mappings of IP addresses to host names. Each  
6 # entry should be kept on an individual line. The IP address should  
7 # be placed in the first column followed by the corresponding host name.  
8 # The IP address and the host name should be separated by at least one  
9 # space.  
10 #  
11 # Additionally, comments (such as these) may be inserted on individual  
12 # lines or following the machine name denoted by a '#' symbol.  
13 #  
14 # For example:  
15 #  
16 #       102.54.94.97      rhino.acme.com      # source server  
17 #       38.25.63.10      x.acme.com          # x client host  
18 #  
19 # localhost name resolution is handled within DNS itself.  
20 #       127.0.0.1      localhost  
21 #       ::1            localhost  
22
```

At the bottom of the window, status bars show 'length: 848 lines: 22 Ln: 1 Col: 1 Pos: 1' and encoding information 'Windows (CR LF) UTF-8 INS ...'.

Ne pas mettre de # sinon la ligne ne sera pas prise en compte par le fichier.

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

V) 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