PROCÉDURE D'INSTALLATION

OpenVPN sur NAS Synology

Version	1.0
Système	Synology DSM 7.x
Package	VPN Server (Centre de paquets)
Auteur	Documentation Technique
Date	31/05/2026

1. Prérequis

1.1 Matériel et logiciels nécessaires

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Un NAS Synology compatible DSM 7.x (ex. DS220+, DS720+, DS920+, RS1221+…)
- Accès administrateur au DSM (interface web Synology)
- Une connexion Internet avec une adresse IP fixe ou un service DDNS
- Le port UDP 1194 (ou TCP 443) ouvert et redirigé vers le NAS sur votre routeur/box
- Un client OpenVPN installé sur l'appareil distant (PC, Mac, smartphone)

1.2 Vérification de la compatibilité

Vérifiez que votre NAS supporte le package VPN Server :

1. Connectez-vous à l'interface DSM via votre navigateur : http://<IP_NAS>:5000
2. Allez dans Centre de paquets → Tous les paquets
3. Recherchez « VPN Server » dans la barre de recherche
4. Vérifiez que le package est disponible et compatible avec votre modèle

Info : Les NAS à architecture ARM (ex. DS118, DS220j) peuvent avoir des limitations. Consultez le site Synology pour la liste complète des modèles compatibles.

2. Installation du package VPN Server

2.1 Téléchargement et installation

Le package VPN Server est disponible directement depuis le Centre de paquets Synology :

5. Ouvrez le Centre de paquets depuis le bureau DSM
6. Dans la barre de recherche, tapez VPN Server
7. Cliquez sur Installer en regard du package VPN Server
8. Acceptez les conditions d'utilisation si demandé
9. Attendez la fin du téléchargement et de l'installation (environ 1 à 2 minutes)
10. Une fois l'installation terminée, cliquez sur Ouvrir

⚠ **Note :** Si le Centre de paquets ne trouve pas VPN Server, assurez-vous que votre DSM est à jour (Panneau de configuration → Mise à jour DSM).

3. Configuration du serveur OpenVPN

3.1 Activation du serveur OpenVPN

Une fois VPN Server installé et ouvert, procédez à la configuration :

11. Dans VPN Server, cliquez sur OpenVPN dans le panneau de gauche
12. Cochez la case Activer le serveur OpenVPN
13. Configurez les paramètres selon le tableau ci-dessous :

Paramètre	Valeur recommandée	Description
Port	`1194`	Port UDP par défaut d'OpenVPN
Protocole	`UDP`	Plus rapide que TCP pour le VPN
Interface réseau	`eth0`	Interface réseau principale du NAS
Sous-réseau VPN	`10.8.0.0`	Plage IP attribuée aux clients VPN
Masque de sous-réseau	`255.255.255.0`	Standard /24 pour 254 clients max
Chiffrement	`AES-256-CBC`	Chiffrement fort recommandé
Authentification	`SHA256`	Algorithme de hachage sécurisé

3.2 Options avancées

Activez les options suivantes selon vos besoins :

- Autoriser les clients VPN à accéder au LAN du serveur : cochez cette option pour accéder aux ressources réseau locales depuis le VPN
- Compression LZO : activez pour améliorer les performances sur les connexions lentes
- Rediriger la passerelle : cochez si vous souhaitez que tout le trafic Internet du client passe par le VPN (tunnel complet)

14. Cliquez sur Appliquer pour enregistrer la configuration

4. Création des certificats et comptes utilisateurs

4.1 Génération des certificats

Les certificats sont générés automatiquement par DSM lors de l'activation d'OpenVPN. Vous pouvez les exporter pour les distribuer aux clients :

15. Dans VPN Server → OpenVPN, cliquez sur Exporter la configuration
16. Un fichier ZIP est téléchargé contenant les fichiers suivants :
    - VPNConfig.ovpn — fichier de configuration client principal
    - ca.crt — certificat de l'autorité de certification
    - README.txt — instructions d'utilisation
17. Conservez ces fichiers en lieu sûr

4.2 Création d'un compte utilisateur VPN

Chaque utilisateur qui se connectera au VPN doit disposer d'un compte DSM avec les droits VPN :

18. Allez dans Panneau de configuration → Utilisateur et groupe
19. Cliquez sur Créer pour ajouter un nouvel utilisateur
20. Renseignez le nom d'utilisateur et un mot de passe fort
21. Dans l'onglet Applications, trouvez VPN Server et cochez Autoriser
22. Cliquez sur Enregistrer

⚠ **Note :** Pour des raisons de sécurité, créez un compte dédié au VPN (ex. vpnuser) plutôt que d'utiliser le compte administrateur principal.

5. Configuration du routeur / box Internet

5.1 Redirection de port (NAT)

Pour que les clients externes puissent atteindre votre serveur VPN, configurez la redirection de port sur votre routeur :

23. Connectez-vous à l'interface d'administration de votre box/routeur
24. Recherchez la section Redirection de ports / NAT / Virtual Server
25. Créez une nouvelle règle avec les paramètres suivants :

Champ	Valeur	Exemple
Protocole	`UDP`	UDP
Port externe	`1194`	1194
Adresse IP interne	`IP du NAS`	192.168.1.100

Port interne	`1194`	1194

26. Enregistrez les modifications

5.2 Configuration DDNS (IP dynamique)

Si votre FAI vous attribue une adresse IP dynamique, configurez le DDNS Synology :

27. Dans DSM → Panneau de configuration → Accès externe → DDNS
28. Cliquez sur Ajouter
29. Sélectionnez le fournisseur : synology.me (gratuit)
30. Choisissez un nom d'hôte (ex. monnas.synology.me)
31. Cliquez sur Tester la connexion puis sur Enregistrer

> **Info :** Notez votre adresse DDNS, elle sera nécessaire pour configurer les clients VPN. Ex. : monnas.synology.me

6. Configuration du fichier client (.ovpn)

6.1 Modification du fichier VPNConfig.ovpn

Le fichier .ovpn exporté doit être modifié avant distribution aux utilisateurs :

32. Ouvrez le fichier VPNConfig.ovpn avec un éditeur de texte (Notepad++, VSCode…)
33. Repérez la ligne commençant par remote et remplacez-la par votre adresse :

```
remote YOUR_SERVER_IP 1194
```

Remplacer par :

```
remote monnas.synology.me 1194
```

34. Vérifiez que les lignes suivantes sont présentes et correctes :

```
client
dev tun
proto udp
resolv-retry infinite
nobind
persist-key
persist-tun
cipher AES-256-CBC
auth SHA256
comp-lzo
```

```
verb 3
```

⚠ **Note :** Si la ligne ca.crt est présente dans le fichier .ovpn, assurez-vous que le fichier ca.crt se trouve dans le même dossier que le fichier .ovpn sur le client.

7. Installation et configuration du client VPN

7.1 Windows

35. Téléchargez OpenVPN GUI depuis https://openvpn.net/community-downloads/
36. Lancez l'installeur et acceptez les options par défaut
37. Copiez le fichier VPNConfig.ovpn (et ca.crt si séparé) dans le dossier :

```
C:\Users\VotreNom\OpenVPN\config\
```

38. Clic droit sur l'icône OpenVPN GUI dans la barre des tâches
39. Cliquez sur Connecter
40. Entrez vos identifiants DSM (login/mot de passe créé à l'étape 4.2)

7.2 macOS

41. Téléchargez et installez Tunnelblick depuis https://tunnelblick.net/
42. Double-cliquez sur le fichier VPNConfig.ovpn pour l'importer dans Tunnelblick
43. Cliquez sur l'icône Tunnelblick dans la barre de menu → Connecter
44. Entrez vos identifiants DSM

7.3 iOS / Android

45. Installez l'application OpenVPN Connect depuis l'App Store ou Google Play
46. Transférez le fichier .ovpn sur votre appareil (par e-mail, AirDrop, etc.)
47. Ouvrez le fichier .ovpn avec l'application OpenVPN Connect
48. Ajoutez votre profil et connectez-vous avec vos identifiants DSM

7.4 Linux

49. Installez le client OpenVPN :

```
sudo apt-get install openvpn   # Debian/Ubuntu
sudo yum install openvpn       # CentOS/RHEL
```

50. Placez le fichier .ovpn dans /etc/openvpn/
51. Lancez la connexion :

```
sudo openvpn --config /etc/openvpn/VPNConfig.ovpn
```

8. Tests et vérification

8.1 Vérification côté serveur

Depuis VPN Server sur le DSM, vérifiez la connexion :

- Allez dans VPN Server → Aperçu : l'état OpenVPN doit indiquer En cours d'exécution
- Allez dans Journaux pour voir les tentatives de connexion et les connexions actives
- La liste des connexions actives affiche l'IP du client, l'utilisateur et la durée

8.2 Vérification côté client

Pour confirmer que la connexion VPN fonctionne correctement :

52. Une fois connecté, ouvrez un navigateur et visitez https://whatismyip.com
53. L'adresse IP affichée doit correspondre à celle de votre NAS (ou de votre connexion Internet)
54. Essayez d'accéder à une ressource de votre réseau local (ex. 192.168.1.x)
55. Vous pouvez aussi utiliser la commande ping depuis un terminal :

```
ping 192.168.1.1
```

Info : Si la connexion échoue, vérifiez la redirection de port sur le routeur, le pare-feu DSM (Panneau de configuration → Sécurité → Pare-feu), et les journaux VPN Server.

9. Sécurité et bonnes pratiques

- Utilisez des mots de passe forts et uniques pour les comptes VPN (12+ caractères, mixte)
- Activez la vérification en deux étapes (2FA) pour les comptes DSM sensibles
- Limitez les tentatives de connexion : Panneau de configuration → Sécurité → Compte (protection anti-brute force)
- Effectuez des sauvegardes régulières de la configuration VPN Server
- Mettez à jour régulièrement DSM et le package VPN Server
- Restreignez l'accès VPN uniquement aux utilisateurs qui en ont besoin
- Consultez régulièrement les journaux VPN pour détecter des connexions suspectes
- Envisagez d'utiliser un port non standard (ex. 1195) pour réduire les scans automatisés

10. Dépannage

Problème	Cause probable	Solution
Connexion refusée (timeout)	Port non redirigé ou pare-feu actif	Vérifier NAT du routeur et pare-feu DSM
Authentification échouée	Mauvais identifiants ou droits VPN non accordés	Vérifier l'utilisateur dans Panneau de configuration
Connexion instable	Qualité réseau ou paramètres de compression	Désactiver comp-lzo, passer en TCP/443
Impossible d'accéder au LAN	Option accès LAN non cochée	VPN Server → OpenVPN → Autoriser accès LAN
Certificat invalide	Fichier ca.crt manquant ou corrompu	Ré-exporter la configuration depuis VPN Server
TLS handshake failed	Décalage d'horloge ou certificat expiré	Synchroniser l'heure du NAS (Panneau de config → Info régionales)

Fin du document — Pour toute assistance, consultez la documentation officielle Synology ou le forum Synology Community.