

DOCUMENTATION

Configuration & Installation Serveur VPN



02 février 2024

projet uf infra

Aix Ynov Campus

# Configuration de VPN Server

Grâce au paquet **VPN Server**, vous pouvez facilement transformer votre Synology NAS en un serveur VPN afin de permettre aux utilisateurs d'accéder en toute sécurité aux ressources partagées à distance dans le cadre du réseau local de votre Synology NAS. En intégrant les protocoles VPN communs (PPTP, OpenVPN et L2TP/IPSec), VPN Server fournit des options pour établir et gérer des services VPN adaptés à vos besoins personnels.

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Remarque :

* L'activation du service VPN affecte la performance réseau du système.
* Seul le groupe **administrators** peut installer et configurer VPN Server.

# PPTP

Le protocole PPTP (Point-to-Point Tunneling Protocol) est une solution VPN couramment utilisée et prise en charge par la plupart des clients (tels que Windows, Mac, Linux et les périphériques mobiles).

## Pour activer le serveur VPN PPTP :

Ouvrez **VPN Server**, puis accédez à **PPTP** dans le panneau de gauche.



Cochez Activer le serveur VPN PPTP.

Spécifiez une adresse IP virtuelle de serveur VPN dans les champs Adresse IP dynamique.

Définissez le Nombre maximal de connexions pour limiter le nombre de connexions VPN simultanées.

Définissez le Nombre maximal de connexions avec le même compte pour limiter le nombre de connexions VPN avec le même compte.

Choisissez l'une des options suivantes dans le menu déroulant **Authentification** pour authentifier les clients VPN :

**PAP** : le mot de passe des clients VPN n'est pas chiffré lors de l'authentification.

**MS-CHAP v2** : le mot de passe des clients VPN est chiffré lors de l'authentification à l'aide de Microsoft CHAP version 2.

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

Nous avons sélectionné **MS-CHAP v2** pour l'authentification précédente, choisissez l'une des options suivantes dans le menu déroulant **Chiffrement** pour chiffrer la connexion VPN :

**Pas de MPPE** : la connexion VPN n'est pas protégée par un mécanisme de chiffrement.

**MPPE facultatif** : la connexion VPN est protégée ou non par un mécanisme de chiffrement 40 bits ou 128 bits, selon les paramètres du client.

**Exiger MPPE** : la connexion VPN est protégée par un mécanisme de chiffrement 40 bits ou 128 bits, selon les paramètres du client.

Dans notre cas nous avons choisi **MPPE facultatif** :

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Définissez la **MTU** (unité de transmission maximale) pour limiter la taille de paquet de données transitant via le VPN.

Dans notre cas nous avons choisi 1400



Cochez **Utiliser un DNS manuel** et spécifiez l'adresse IP d'un serveur DNS pour pousser le DNS vers les clients PPTP. Si cette option est désactivée, le serveur DNS utilisé par le Synology NAS sera poussé vers les clients.



Cliquez sur **Appliquer** pour que la modification prenne effet.

Remarque :

Lorsque vous vous connectez au VPN, les paramètres d'authentification et de chiffrement des clients VPN doivent être identiques aux paramètres spécifiés sur VPN Server, sinon les clients ne parviendront pas à se connecter.

Afin d'être compatible avec la plupart des clients PPTP dotés des systèmes d'exploitation Windows, Mac OS, iOS et Android, le MTU par défaut est réglé sur 1400. Pour un environnement réseau plus complexe, un MTU inférieur sera peut-être nécessaire. Essayez de réduire la taille du MTU si vous continuez à recevoir des erreurs d'expiration ou que vous disposez d'une connexion instable.

Veuillez vérifier les paramètres de transmission des ports et de pare-feu sur votre Synology NAS et sur votre routeur afin de vous assurer que le port TCP 1723 est ouvert.

Le service VPN PPTP est intégré sur certains routeurs, il est donc possible que le port 1723 soit occupé. Afin de vous assurer que VPN Server fonctionne correctement, vous devrez peut-être désactiver le service VPN PPTP via l'interface d'administration du routeur pour que le PPTP de VPN Server fonctionne. Par ailleurs, certains anciens routeurs bloquent le protocole GRE (protocole IP 47) et entraînent par conséquent un échec de la connexion VPN. Il est donc recommandé d'utiliser un routeur capable de prendre en charge les connexions pass-through VPN.

# L2TP/IPSec

L2TP (Layer 2 Tunneling Protocol) sur IPSec fournit des réseaux virtuels privés avec une sécurité accrue et est pris en charge par la plupart des clients (tels que Windows, Mac, Linux et les périphériques mobiles).

Remarque :

Pour utiliser L2TP/IPSec, assurez-vous que votre Synology NAS est équipé de DSM 4.3 ou version ultérieure.

## Pour activer le serveur L2TP/IPSec VPN :

Ouvrez **VPN Server**, puis accédez à **L2TP/IPSec** dans le panneau de gauche.



Cochez Activer le serveur L2TP/IPSec VPN.

Spécifiez une adresse IP virtuelle de serveur VPN dans les champs Adresse IP dynamique

Définissez le Nombre maximal de connexions pour limiter le nombre de connexions VPN simultanées.

Définissez le Nombre maximal de connexions avec le même compte pour limiter le nombre de connexions VPN avec le même compte.

Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement

Choisissez l'une des options suivantes dans le menu déroulant **Authentification** pour authentifier les clients VPN :

**PAP** : le mot de passe des clients VPN n'est pas chiffré lors de l'authentification.

**MS-CHAP v2** : le mot de passe des clients VPN est chiffré lors de l'authentification à l'aide de Microsoft CHAP version 2.

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

Nous avons sélectionné **MS-CHAP v2** pour l'authentification précédente, choisissez l'une des options suivantes dans le menu déroulant **Chiffrement** pour chiffrer la connexion VPN :

**Pas de MPPE** : la connexion VPN n'est pas protégée par un mécanisme de chiffrement.

**MPPE facultatif** : la connexion VPN est protégée ou non par un mécanisme de chiffrement 40 bits ou 128 bits, selon les paramètres du client.

**Exiger MPPE** : la connexion VPN est protégée par un mécanisme de chiffrement 40 bits ou 128 bits, selon les paramètres du client.

Dans notre cas nous avons choisi **MPPE facultatif** :

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Définissez la **MTU** (unité de transmission maximale) pour limiter la taille de paquet de données transitant via le VPN.

Dans notre cas nous avons choisi 1400



Cochez **Utiliser un DNS manuel** et spécifiez l'adresse IP d'un serveur DNS pour pousser le DNS vers les clients PPTP. Si cette option est désactivée, le serveur DNS utilisé par le Synology NAS sera poussé vers les clients.



Pour des performances maximales du VPN, sélectionnez **Exécuter en mode noyau** (kernel).



Saisissez et confirmez une **clé prépartagée**. Cette clé secrète peut être donnée à votre utilisateur VPN L2TP/IPSec pour authentifier la connexion.

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

Cochez **Activer le mode compatible SHA2-256 (96 bits)** pour autoriser certains clients (qui ne sont pas à la norme RFC) à utiliser une connexion L2TP/IPSec.



Dans notre cas nos clients ayant tous cette norme il est préférable de ne pas cocher cette case pour des raison de sécurité.

Cliquez sur **Appliquer** pour que la modification prenne effet.