

BTS SIO

Mise en place d'un VPN



Aleksandar Nikolic

PLAN DE LA SITUATION



Introduction



Matériel et environnement
utilisés



Schéma de l'infrastructure VPN



Objectifs du projet



Processus de réalisation



Tests et vérifications



Conclusion et apports

INTRODUCTION

Dans le cadre de ma formation BTS SIO – spécialité SISR, j'ai mis en œuvre une solution VPN afin de sécuriser l'accès distant aux ressources internes de l'entreprise Nikodex

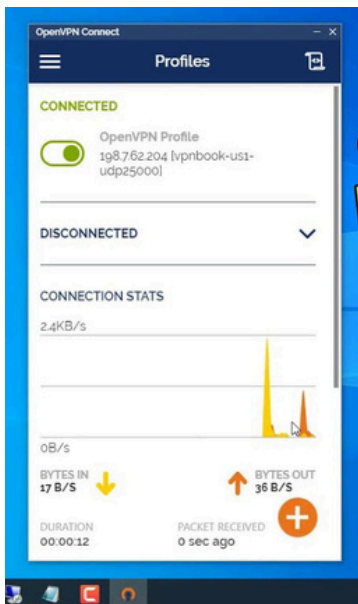
L'objectif était de permettre aux collaborateurs de se connecter depuis l'extérieur tout en garantissant la confidentialité des données échangées.

La solution choisie repose sur le protocole OpenVPN, déployé sur un serveur NAS Synology déjà en place dans l'entreprise.



Matériel et environnement utilisés

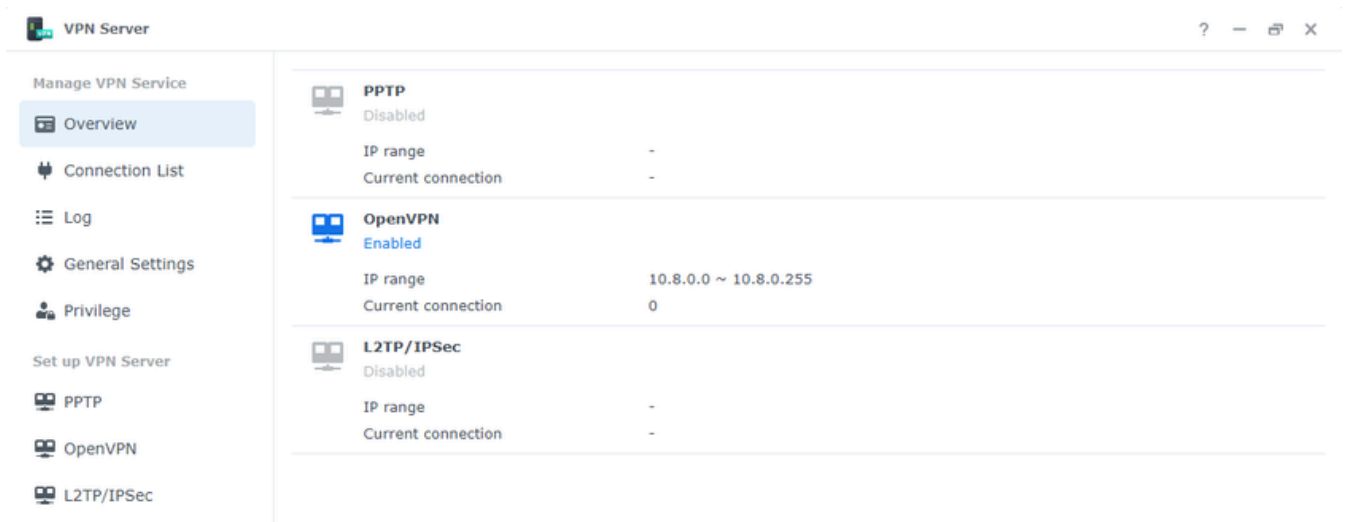
- NAS Synology avec DSM (DiskStation Manager)
- Module VPN Server (installé via le Centre de Paquets)
- Routeur avec redirection de port UDP 1194
- Clients OpenVPN (ordinateur portable, smartphone)
- Certificat SSL pour le chiffrement
- Connexion Internet avec IP publique ou domaine dynamique



Interface OpenVPN Clients sur Windows



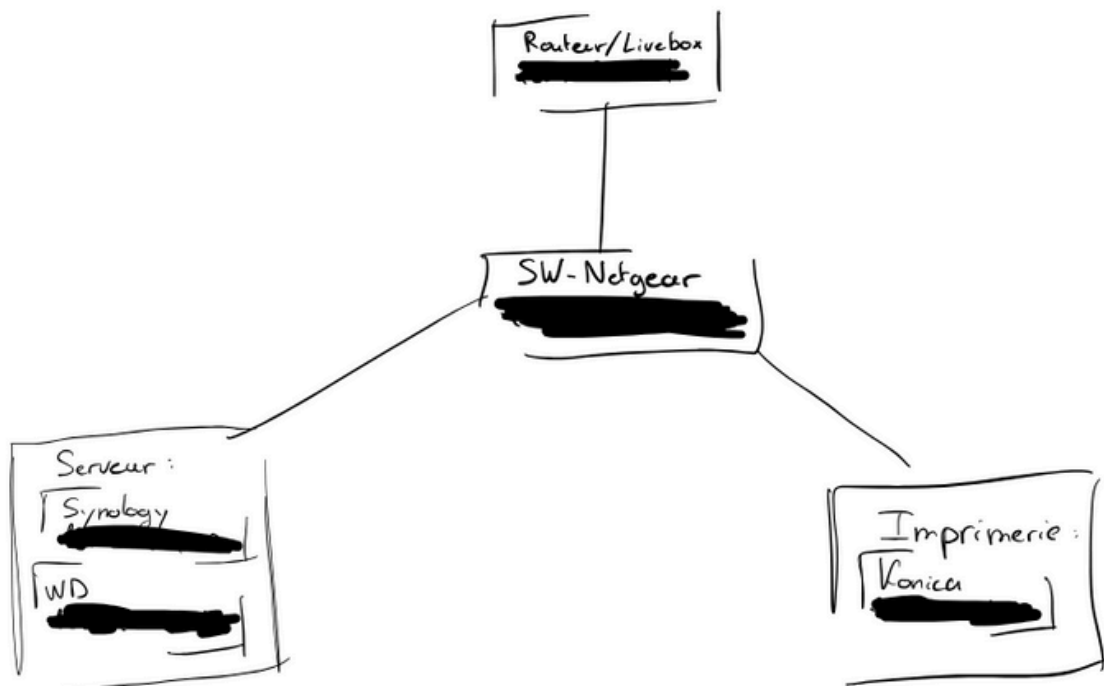
Interface DSM



Interface de l'option VPN sur le NAS Synology

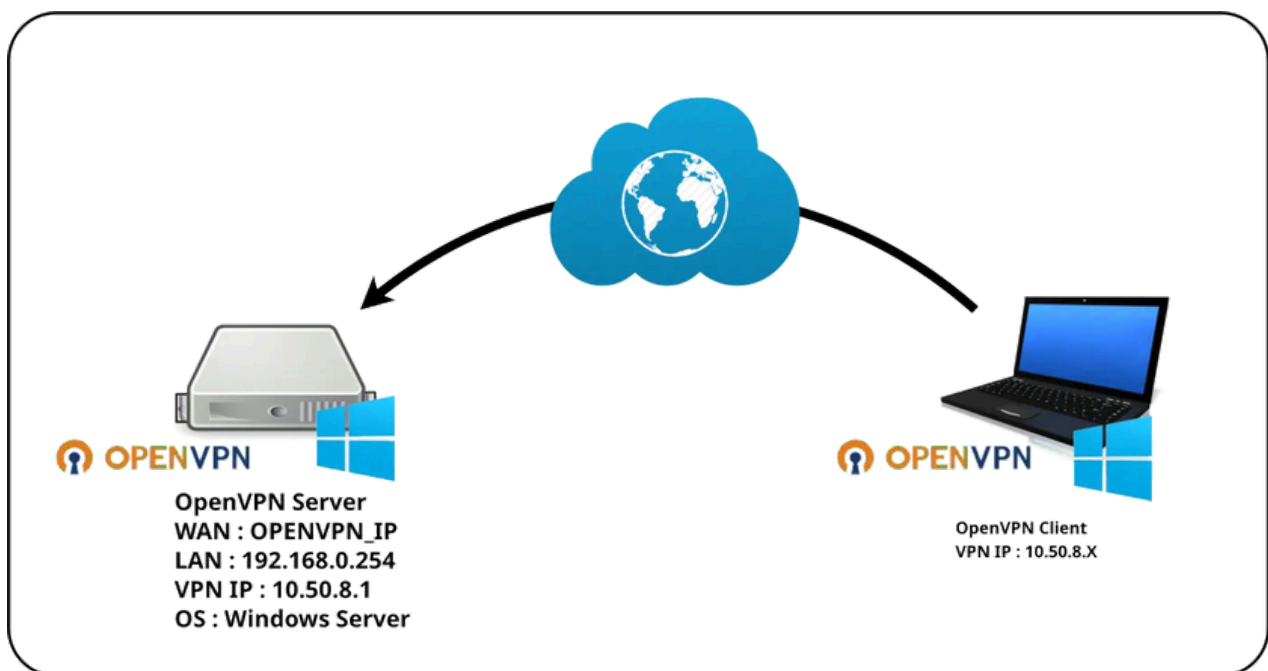
Schéma de l'infrastructure VPN

- Le NAS héberge le serveur OpenVPN.
- Le routeur redirige les connexions sur le port UDP 1194 vers le NAS.
- Les collaborateurs utilisent un fichier .ovpn pour se connecter depuis l'extérieur.
- Une fois connectés, ils ont accès aux ressources internes du réseau local (fichiers partagés, imprimantes, applications internes).



Objectifs du projet

- Mettre en place un accès distant sécurisé aux ressources de l'entreprise.
- Garantir la confidentialité des données échangées via le chiffrement SSL.
- Améliorer la mobilité des collaborateurs sans compromettre la sécurité.
- Permettre une gestion des droits d'accès selon les utilisateurs.
- Offrir une solution simple et évolutive.



Exemple schéma représentatif d'une connexion via OpenVPN

Processus de réalisation

➤ Étape 1 : Préparation

Analyse des besoins : utilisateurs, services à rendre accessibles

- Vérification des prérequis techniques :
 - Accès admin NAS
 - Connexion Internet stable
 - Nom de domaine ou IP fixe

➤ Étape 2 : Installation du serveur VPN

- Installation du paquet VPN Server via DSM
- Activation d'OpenVPN dans l'interface VPN Server
- Génération du fichier .ovpn par DSM

➤ Étape 3 : Configuration OpenVPN

- Modification du fichier .ovpn : adresse IP publique ou domaine personnalisé
- Activation du chiffrement SSL
- Définition de la plage IP attribuée aux clients VPN

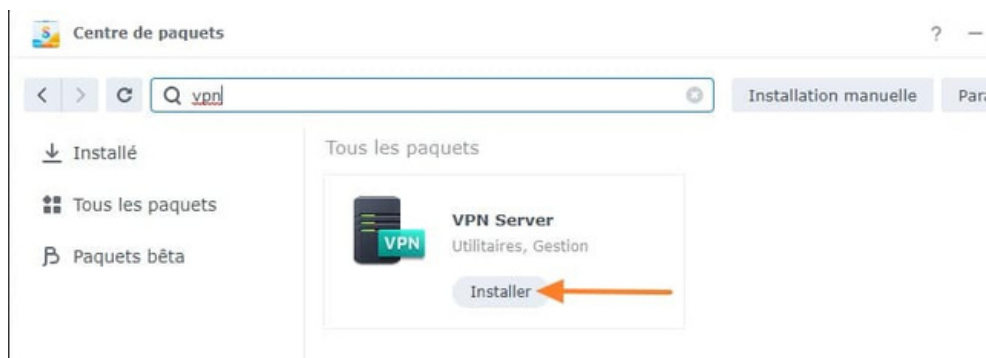
➤ Étape 4 : Configuration réseau

- Ouverture du port UDP 1194 sur le NAS
- Redirection NAT/PAT sur le routeur vers l'IP du NAS
- Activation des permissions VPN dans le pare-feu DSM

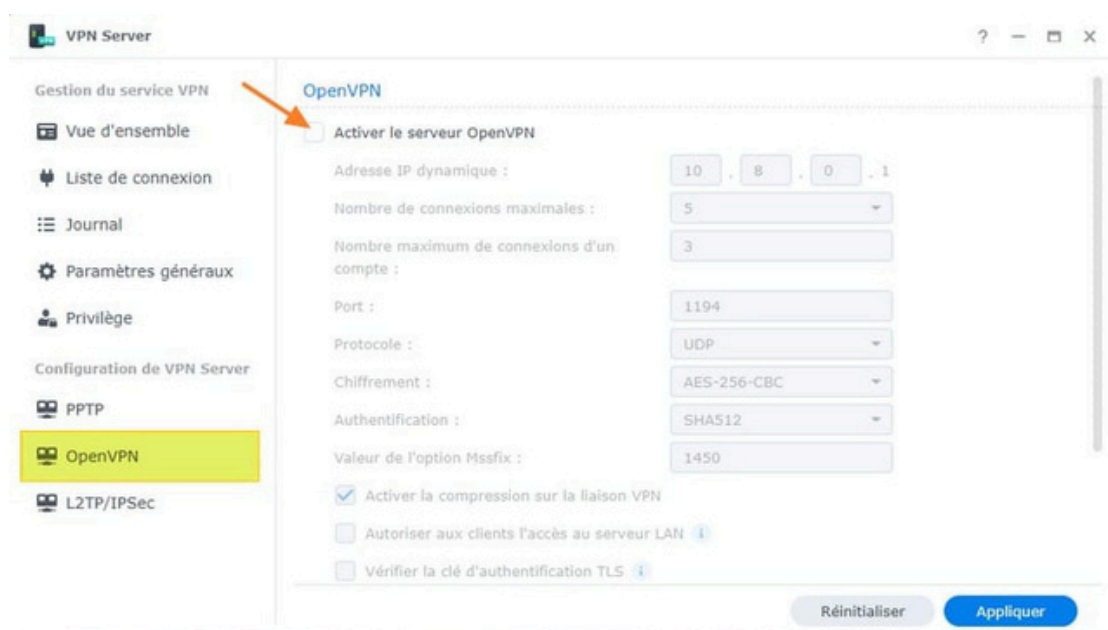
➤ Étape 5 : Gestion des utilisateurs

- Création des utilisateurs VPN dans DSM
- Attribution des droits d'accès aux ressources internes (dossiers partagés, services)

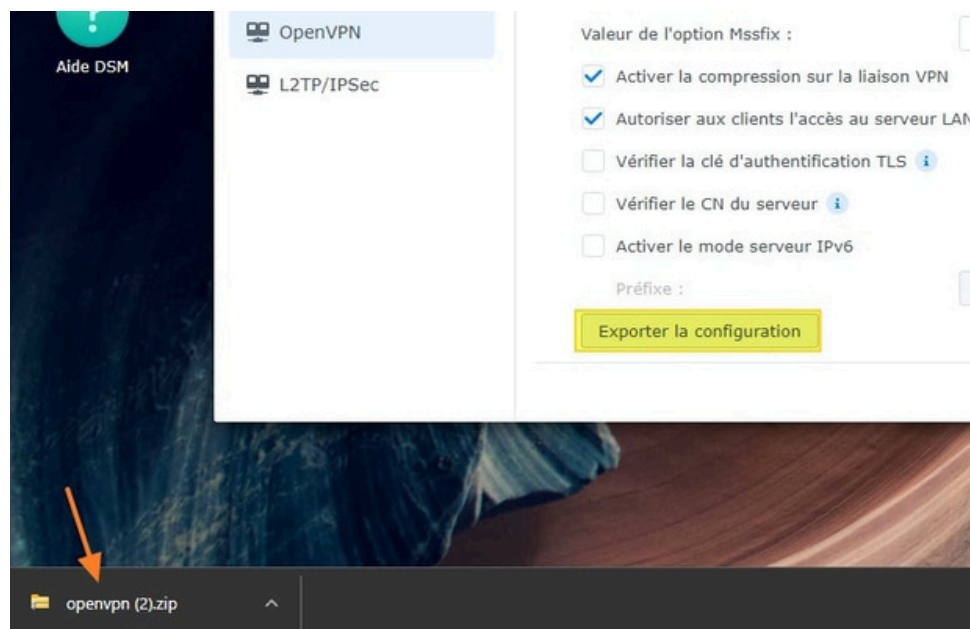
Image pour illustrer les étapes



Installation du paquet VPN Server via DSM



Activation d'OpenVPN dans l'interface VPN Server



Exportation de la configuration
.ovpn

VPNConfig.ovpn - Bloc-notes

Fichier Modifier Affichage

```
dev tun
tls-client
remote YOUR_SERVER_IP 14911


# The "float" tells OpenVPN to accept authenticated packets from any address,
# not only the address which was specified in the --remote option.
# This is useful when you are connecting to a peer which holds a dynamic address
# such as a dial-in user or DHCP client.
# (Please refer to the manual of OpenVPN for more information.)

#float

# If redirect-gateway is enabled, the client will redirect it's
# default network gateway through the VPN.
# It means the VPN connection will firstly connect to the VPN Server
# and then to the internet.
# (Please refer to the manual of OpenVPN for more information.)

#redirect-gateway def1
```

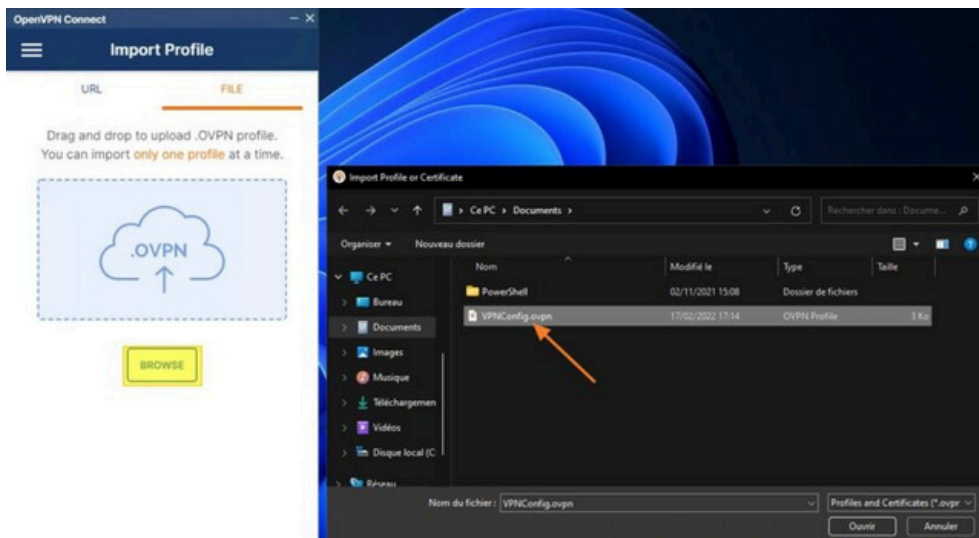
Modification de la configuration .ovpn pour mettre l'adresse publique

	#	Nom de service	Type de service	Port de début externe	Port de fin externe	Port de début interne	Port de fin interne	Adresse IP interne
	1	NAS Synology - VPN	UDP	14911	14911	14911	14911	192.168.1.20

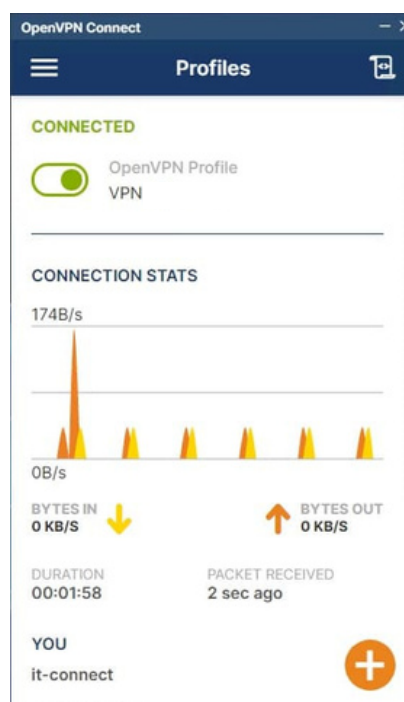
Regle de redirection de ports pour l'accès externe

Tests et vérifications

- Téléchargement du fichier .ovpn sur les terminaux client (PC, smartphone)
- Connexion au VPN via OpenVPN GUI / app mobile
- Test d'accès aux fichiers partagés, imprimantes réseau et autres services internes
- Vérification de l'adresse IP locale attribuée, du routage, et de la stabilité



Importation de la configuration sur le openvpn client gui



Test et succès de la connexion

Conclusion

Ce projet m'a permis de :

- Mettre en œuvre une solution VPN concrète dans un contexte professionnel.
- Apprendre à configurer OpenVPN sur un NAS Synology.
- Gérer la sécurité réseau (ports, certificats, droits d'accès).
- Comprendre les enjeux liés à la mobilité et à la protection des données.

Cette solution apporte à l'entreprise une connexion distante sécurisée, tout en restant facile à maintenir et à faire évoluer selon les besoins.