

BTS Services informatiques aux organisations - SISR**Session 2022****E4 – Support et mise à disposition de services informatiques****Coefficient 4****DESCRIPTION DE LA REALISATION PROFESSIONNELLE****NOM et prénom du candidat : LEDUC Quentin**

N° candidat : 02145639104

Contexte de la réalisation professionnelle

Scani travail avec la Mairie de Joigny pour créer des backup de leur machines virtuelles directement sur notre infrastructure. Pour accéder a leur Backup, le service informatique de la Mairie à besoin d'un VPN afin d'accéder a leur Synology.

Intitulé de la réalisation professionnelle

Création d'un VPN - OpenVPN avec Synology

Période de réalisation : DU 15/08/21 AU 17/08/21**Lieu : Joigny****Modalité : Individuelle****Principale(s) activité(s) concernée(s) :**

- Mettre en œuvre des outils et stratégies de veille informationnelle
- Déployer un service
- Accompagner les utilisateurs dans la mise en place d'un service

Conditions de réalisation

- **Ressources présentes** VPN PPTP
- **Résultats attendus** Un nouveau type de VPN qui est plus sécurisé pour accéder au réseau local
- **Durée de réalisation** 1H

Modalités d'accès à cette réalisation professionnelle.Site internet : www.netwaze.fr

Aller dans « Réalisations Professionnelles » Mot de passe : Mr.Robot

Partie 1 – Procédure de mise en œuvre.**PRÉREQUIS MATÉRIEL**

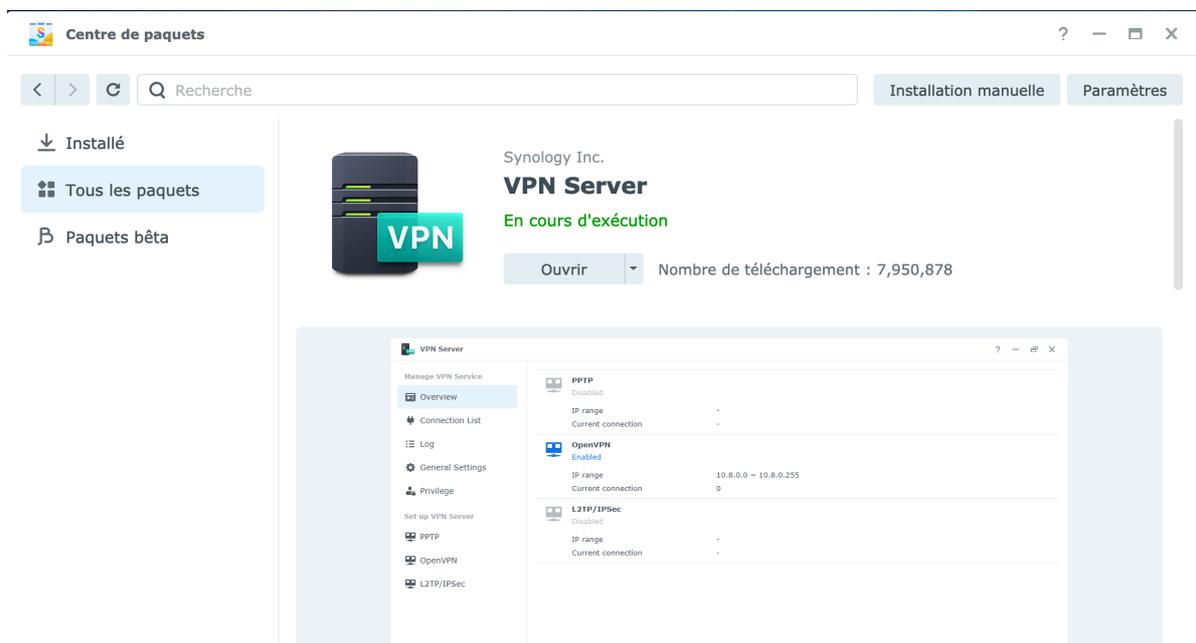
- Un Synology
- Un routeur (Asus avec Merlin dessus)
- L'application OpenVPN Connect

PRÉREQUIS

Avant de commencer il faut savoir que mon NAS n'est pas disponible de l'extérieur. Il fonctionne sur le port par défaut 5000 et 5001 pour le HTTP et le HTTPS. Mais il est connecté à internet pour effectuer des backups distant.

INSTALLATION DE NAS-SERVER

Pour installer Nas-Server il n'y a rien de compliquer. Il suffit d'aller dans la « logitech » et de cliquer sur installer.



Une fois installer nous pouvons ouvrir l'application et passer à la configuration.

CONFIGURATION DE OPENVPN

VPN Server

Gestion du service VPN

- Vue d'ensemble
- Liste de connexion
- Journal
- Paramètres généraux
- Privilège

Configuration de VPN Server

- PPTP
- OpenVPN**
- L2TP/IPSec

OpenVPN

Activer le serveur OpenVPN

Adresse IP dynamique : 192 . 168 . 5 . 1

Nombre de connexions maximales : 10

Nombre maximum de connexions d'un compte : 10

Port : 1194

Protocole : UDP

Chiffrement : AES-256-CBC

Authentification : SHA512

Valeur de l'option Mssfix : 1450

Activer la compression sur la liaison VPN

Autoriser aux clients l'accès au serveur LAN [i](#)

Activer le mode serveur IPv6

Réinitialiser Appliquer

Dans « configuration de VPN Server » Il faut cliquer sur « Activer le serveur OpenVPN » pour débloquer la partie configuration. On lui donne une adresse dynamique qui est celle du Synology. Pour des raisons plus pratique je lui donne l'adresse IP 192.168.5.1. J'augmente le nombre de connexion à 10 et pareil pour le maximum de connexion d'un compte. En port on peut le laisser par défaut mais pour plus de sécurité on peut le changer. On laisse le protocole UDP et le type de chiffrement on peut laisser par défaut.

On désactive la compression sur la liaison VPN car il est possible qu'il y est des failles de sécurités avec cette option. Pour ma part je veux pouvoir prendre en SSH tout mes serveurs et VM par conséquent j'active l'accès au serveur LAN puis nous pouvons cliquer sur appliquer. On peut ensuite exporter la configuration.

VPN Server

Gestion du service VPN

- Vue d'ensemble
- Liste de connexion
- Journal
- Paramètres généraux
- Privilège

Configuration de VPN Server

- PPTP
- OpenVPN**
- L2TP/IPSec

Nombre de connexions maximales : 10

Nombre maximum de connexions d'un compte : 10

Port : 1194

Protocole : UDP

Chiffrement : AES-256-CBC

Authentification : SHA512

Valeur de l'option Mssfix : 1450

Activer la compression sur la liaison VPN

Autoriser aux clients l'accès au serveur LAN [i](#)

Activer le mode serveur IPv6

Préfixe :

Exporter la configuration

Nom	Date de modification	Taille	Type
ca_bundle.crt	aujourd'hui à 10:56	4 Ko	certificat
ca.crt	aujourd'hui à 10:56	2 Ko	certificat
README.txt	5 juillet 2021 à 11:38	2 Ko	Format texte
VPNConfig.ovpn	aujourd'hui à 12:15	5 Ko	OVPN Profile

The screenshot shows the 'VPN Server' configuration window. On the left is a sidebar with navigation options: 'Gestion du service VPN' (containing 'Vue d'ensemble', 'Liste de connexion', 'Journal', 'Paramètres généraux', and 'Privilège'), and 'Configuration de VPN Server' (containing 'PPTP', 'OpenVPN', and 'L2TP/IPSec'). The main area is titled 'Paramètres généraux' and contains the following settings: 'Interface réseau' set to 'LAN 1 (192.168.3.245)', 'Type de compte' set to 'Utilisateurs locaux', and an unchecked checkbox for 'Accorder le privilège VPN aux utilisateurs locaux nouvellement ajoutés'. Below this is the 'Blocage auto' section, where 'Blocage auto' is set to 'Activé (Configurer "Blocage auto")'. At the bottom right are 'Réinitialiser' and 'Appliquer' buttons.

Dans les « paramètres généraux » on vérifie son interface réseau. Personnellement je prends l'interface LAN1 (très important pour la suite). On décoche aussi d'accorder les privilèges aux utilisateurs ajoutés récemment. Je préfère faire ceci à la main.

CRÉATION D'UTILISATEUR ET PRIVILÈGE

Nous allons créer un utilisateur Scani et lui donner des privilèges pour se connecter à notre VPN.

Pour ce faire nous allons dans le panneau de configuration puis créer dans utilisateur et groupe.

The screenshot shows the 'Assistant de création d'utilisateur' dialog box, specifically the 'Saisir les informations utilisateur' step. It contains the following fields and options: 'Nom *' with the value 'Scani'; 'Description'; 'Courrier électronique'; 'Mot de passe *' with a strength indicator of 'Forte' and a 'Générer un mot de passe aléatoire' button; 'Confirmez le mot de passe *'; and three checkboxes: 'Envoyer un courrier de notification au nouvel utilisateur créé', 'Afficher le mot de passe utilisateur dans le courrier de notification', and 'Ne pas autoriser l'utilisateur à changer le mot de passe du compte'. A note at the bottom states '* Ce champ est requis.' A 'Suivant' button is located at the bottom right.

Assistant de création d'utilisateur

Rejoindre les groupes

Nom	Description	<input type="checkbox"/> Ajouter
administrators	System default admin group	<input type="checkbox"/>
http	System default group for Web services	<input type="checkbox"/>
users	System default group	<input checked="" type="checkbox"/>

3 éléments

Retour Suivant

Assistant de création d'utilisateur

Attribuer les permissions sur les dossiers partagés

Nom	Aperçu	Autorisations de g...	Permissions utilisateur		
			<input type="checkbox"/> Aucun acc...	<input type="checkbox"/> Lecture/é...	<input type="checkbox"/> Lecture ...
[redacted]	Aucun accès	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[redacted]	Aucun accès	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Music	Aucun accès	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[redacted]	Aucun accès	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[redacted]	Aucun accès	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
usbshare1	Aucun accès	-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

6 éléments

Remarque : L'autorisation dépend des autorisations d'utilisateur et de groupe. Priorité des autorisations : **NA > RW > RO**

Retour Suivant

Assistant de création d'utilisateur

Attribuer un quota utilisateur

Volume/dossier pa...	Quota effectif	Quota de groupe	Quota utilisateur
Volume 1 (btrfs)	Sans limite	Sans limite	Illimité
Music	Sans limite	Sans limite	Illimité
Volume 2 (btrfs)	Sans limite	Sans limite	Illimité
Volume 4 (btrfs)	Sans limite	Sans limite	Illimité
Volume 5 (btrfs)	Sans limite	Sans limite	Illimité

5 éléments

Remarque : Vous pouvez spécifier un quota utilisateur pour un volume ou un dossier spécifique ; sinon, le quota de groupe sera appliqué.

Retour Suivant

Assistant de création d'utilisateur

Attribuer les permissions sur l'application

Nom	Aperçu	Autorisations de groupe	Permissions utilisateur	
			<input type="checkbox"/> Autoriser	<input type="checkbox"/> Refuser
AFP	Autoriser	Autoriser	<input type="checkbox"/>	<input type="checkbox"/>
Audio Station	Autoriser	Autoriser	<input type="checkbox"/>	<input type="checkbox"/>
DSM	Autoriser	Autoriser	<input type="checkbox"/>	<input type="checkbox"/>
FTP	Autoriser	Autoriser	<input type="checkbox"/>	<input type="checkbox"/>
File Station	Autoriser	Autoriser	<input type="checkbox"/>	<input type="checkbox"/>
Note Station	Autoriser	Autoriser	<input type="checkbox"/>	<input type="checkbox"/>
SFTP	Autoriser	Autoriser	<input type="checkbox"/>	<input type="checkbox"/>
Synology Mail Server	Autoriser	Autoriser	<input type="checkbox"/>	<input type="checkbox"/>
Synology Drive	Autoriser	Autoriser	<input type="checkbox"/>	<input type="checkbox"/>

13 éléments

Remarque : L'autorisation est déterminée par les autorisations des utilisateurs et des groupes. Priorité des autorisations : **Refuser > Autoriser**.

Retour Suivant

Assistant de création d'utilisateur

Définir la limite de vitesse utilisateur

Paramètres avancés

Service	Résultat	Limite de vitesse	Limites de ch...	Limite de télé...
File Station	Illimité / Illimité	Appliquez les paramètres d...	-	-
FTP	Illimité / Illimité	Appliquez les paramètres d...	-	-
Rsync	Illimité / Illimité	Appliquez les paramètres d...	-	-
Synology Dr...	Illimité / Illimité	Appliquez les paramètres d...	-	-

4 éléments

Retour Suivant

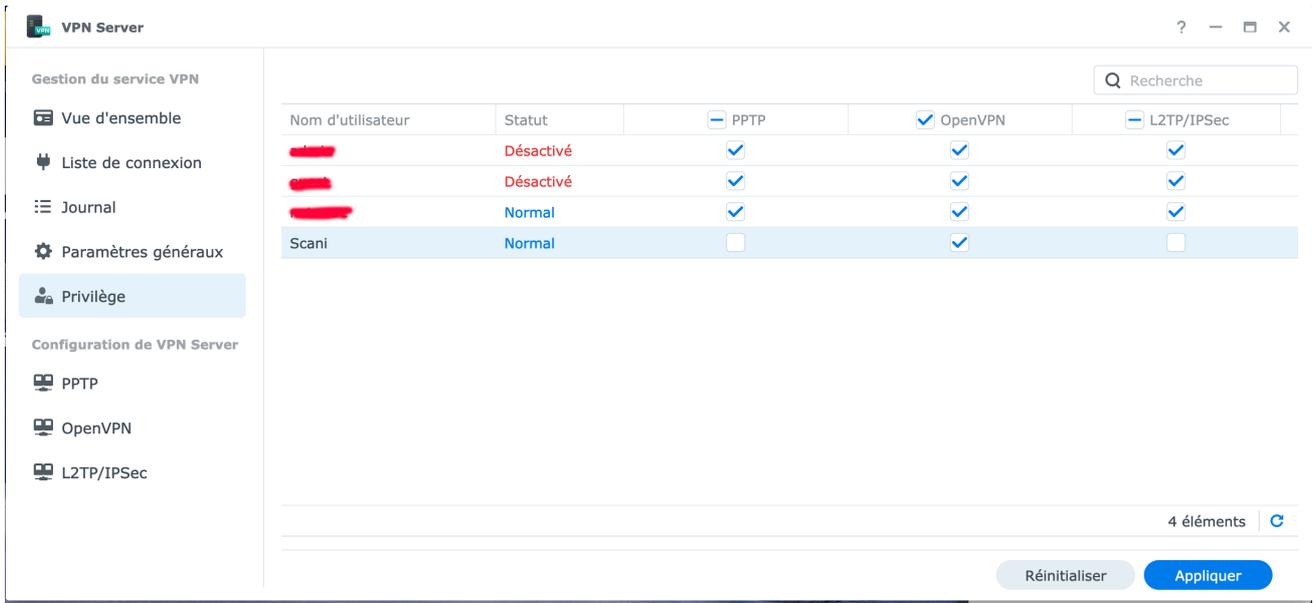
Assistant de création d'utilisateur

Confirmer les paramètres

Élément	Valeur
Nom	Scani
Description	VPN
Courrier électronique	
Liste de groupes	users
Inscriptible	
Lecture seule	
Pas d'accès	Backup, BackupPI, Music, Netwaze, Perso, usbshare1
Le privilège inclut	
Le privilège exclut	
Paramètres de limite de vi...	

Retour Effectué

Nous ne lui accordons aucun privilège ni même des applications ou des dossiers partagés. Puis nous pouvons sauvegarder notre utilisateur. Cette utilisateurs sera par conséquent le client VPN.



On lui accorde à présent l'accès au VPN dans les Privilèges de VPN Server puis on applique.

ATTRIBUTION D'IP STATIQUE

Il faut savoir que notre serveur OpenVPN va donner des adresses IP dynamique, hors ce que je souhaiterais c'est que la plupart des clients connus est une IP statique pour avoir un plan de réseau précis.

Pour ce faire nous devons nous connecter à notre Synology en SSH et mettre des bouts de configuration dans les scripts de l'application.

Une fois connecter à notre Synology nous allons créer un répertoire UsersIP dans VPNCenter et nous lui donnons des droits d'écriture et de lecture.

```
[netwaze@Synology-Backup:/$ cd /usr/syno/etc/packages/VPNCenter/
[netwaze@Synology-Backup:/usr/syno/etc/packages/VPNCenter$ sudo mkdir UserIP
[Password:
[netwaze@Synology-Backup:/usr/syno/etc/packages/VPNCenter$ ls
12tp      pptp      syno_conf  synovpn_local_port  synovpn_port
openvpn  privilege  synovpn.conf  synovpnlog.db      UserIP
[netwaze@Synology-Backup:/usr/syno/etc/packages/VPNCenter$ sudo chmod 0755 UserIP
[netwaze@Synology-Backup:/usr/syno/etc/packages/VPNCenter$ █
```

Maintenant nous devons déclarer notre dossier dans le fichier openvpn.conf dans /usr/syno/etc/packages/VPNCenter/openvpn/ puis nous rajoutons en dessous de server cette ligne qui déclare notre dossier : client-config-dir /usr/syno/etc/packages/VPNCenter/UserIP/

```
push "route 192.168.3.0 255.255.255.0"
push "route 192.168.5.0 255.255.255.0"
dev tun

management /var/run/openvpn.sock unix

server 192.168.5.0 255.255.255.0

client-config-dir /usr/syno/etc/packages/VPNCenter/UserIP/

dh /var/packages/VPNCenter/target/etc/openvpn/keys/dh3072.pem
ca /var/packages/VPNCenter/target/etc/openvpn/keys/ca.crt
cert /var/packages/VPNCenter/target/etc/openvpn/keys/server.crt
key /var/packages/VPNCenter/target/etc/openvpn/keys/server.key

max-clients 10

persist-tun
persist-key

verb 3

-- INSERT --
```

1,1 Top

Maintenant nous devons aller modifier le fichier radiusplugin.cnf dans /volume1/@appstore/VPNCenter/etc/openvpn/ qui empêchera d'écraser notre configuration cliente (changement d'ip). A la ligne overwriteccfiles= mettre false.

```
NAS-Identifiant=OpenVpn
Service-Type=5
Framed-Protocol=1
NAS-Port-Type=5
NAS-IP-Address=127.0.0.1
OpenVPNConfig=/usr/syno/etc/packages/VPNCenter/openvpn/openvpn.conf
subnet=255.255.255.0
overwriteccfiles=false
server
{
    acctport=31068
    authport=31067
    name=127.0.0.1
    retry=1
    wait=5
    sharedsecret=4synovpn
}

~
~
~
~

-- INSERT --
```

8,23 All

Maintenant nous devons dire quels utilisateurs a l'adresse ip. Pour ce faire nous retournons dans notre dossier UserIP /usr/syno/etc/packages/VPNCenter/UserIP et nous allons créer un fichier qui correspond à notre utilisateur.

```
[netwaze@Synology-Backup:/volume1/@appstore/VPNCenter/etc/openvpn$ cd /usr/syno/etc/packages/VPNCenter/UserIP
netwaze@Synology-Backup:/usr/syno/etc/packages/VPNCenter/UserIP$ vi Scani
```

Nous rentrons la ligne : ifconfig-push 192.168.5.10 192.168.5.9

Nous devons mettre l'ip souhaitez .10 et retirer 1 à chaque ip bloquer. Le mieux est d'incrémenter de 4 a chaque fois.

Puis nous lui donnons les droits nécessaires à l'exécution et la lecture. 644

```
[netwaze@Synology-Backup:/usr/syno/etc/packages/VPNCenter/UserIP$ sudo chmod 0644 Scani
netwaze@Synology-Backup:/usr/syno/etc/packages/VPNCenter/UserIP$
```

On peut maintenant reboot notre Synology pour que la configuration soit prise en compte.

MODIFICATION DE FICHER VPNCONFIG

Plus haut nous avons télécharger notre configuration VPN. Nous pouvons l'ouvrir (.ovpn) et modifier les informations Serveur. Dans Your_Server_IP nous devons mettre notre nom de domaine. J'ai créer un nouveau sous domaine chez mon registrar pour être vpn.netwaze.fr qui redirige sur l'adresse ip du B38. On rajoute ensuite une ligne : setenv CLIENT_CERT 0 qui empêche une notification que l'on à pas de certificat pour notre connexion.

```
dev tun
tls-client

remote vpn.netwaze.fr 1194
setenv CLIENT_CERT 0

# 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

# dhcp-option DNS: To set primary domain name server address.
# Repeat this option to set secondary DNS server addresses.

#dhcp-option DNS DNS_IP_ADDRESS

pull

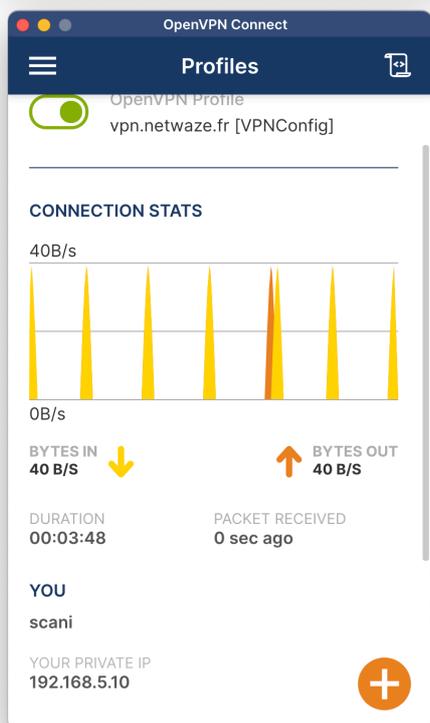
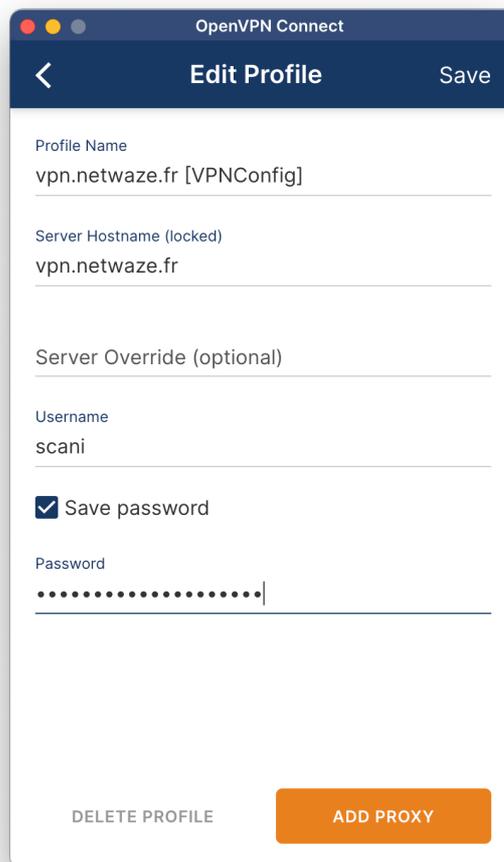
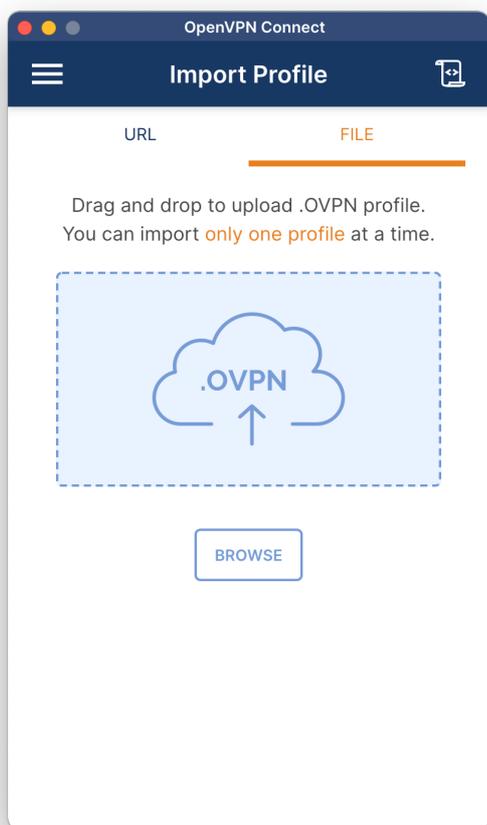
# If you want to connect by Server's IPv6 address, you should use
# "proto udp6" in UDP mode or "proto tcp6-client" in TCP mode
proto udp

script-security 2
```

CONNEXION CLIENT

Pour pouvoir se connecter avec notre utilisateur nous utiliseront l'application OpenVPN Connect. Lien : <https://openvpn.net/client-connect-vpn-for-windows/> Attention il faut ouvrir le port sur notre routeur défini dans notre Synology pour que la connexion fonctionne.

Une fois sur notre application on insère notre fichier .ovpn. On vérifie bien nos informations et on y rentre notre utilisateur et notre mot de passe.



Une fois fait on remarque que l'on est connecter avec notre adresse IP définit dans la configuration de OpenVPN.

CONFIGURATION DU ROUTEUR

Maintenant pour que tout nos appareils peuvent discuter ensemble on va créer une route sur notre routeur.

Personnellement mon routeur est un Asus avec Merlin.

Pour créer une route dans mon routeur il faut aller dans « réseau local -> Routage » puis d'ajouter notre route qui est : 192.168.5.0 : 255.255.255.0 : 192.168.3.245

Liste de routage statique (Limite maximum : 64)					
Réseau / adresse IP de l'hôte	Masque réseau	Passerelle	Mesure Web	Interface	Ajouter / Supprimer
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	LAN <input type="text"/>	<input type="button" value="+"/>
192.168.5.0	255.255.255.0	192.168.3.245		LAN	<input type="button" value="-"/>

Maintenant notre route fonctionnelle, nous pouvons désormais pinguer nos hôtes sur notre réseau local et nos autres hôtes avec notre VPN.

The screenshot shows the OpenVPN Connect application interface on the left and two terminal windows on the right. The OpenVPN Connect interface displays the 'Profiles' section with 'OpenVPN Profile' for 'vpn.netwaze.fr [VPNConfig]' and a 'CONNECTION STATS' section showing a connection speed of 2.6KB/s. The terminal windows show the results of ping tests from a MacBook Pro to a web server (192.168.3.16 and 192.168.5.10) and an SSH connection to the web server (192.168.3.183) where further ping tests are performed.

Partie 3 – Veille technologique.

De la même façon nous aurions pu créer une nouvelle machine virtuelle et créer un VPN Wireguard, PPTP, L2TP ou d'installer un équipement Mikrotik pour faire du point à point.