

Mise en place OPENVPN

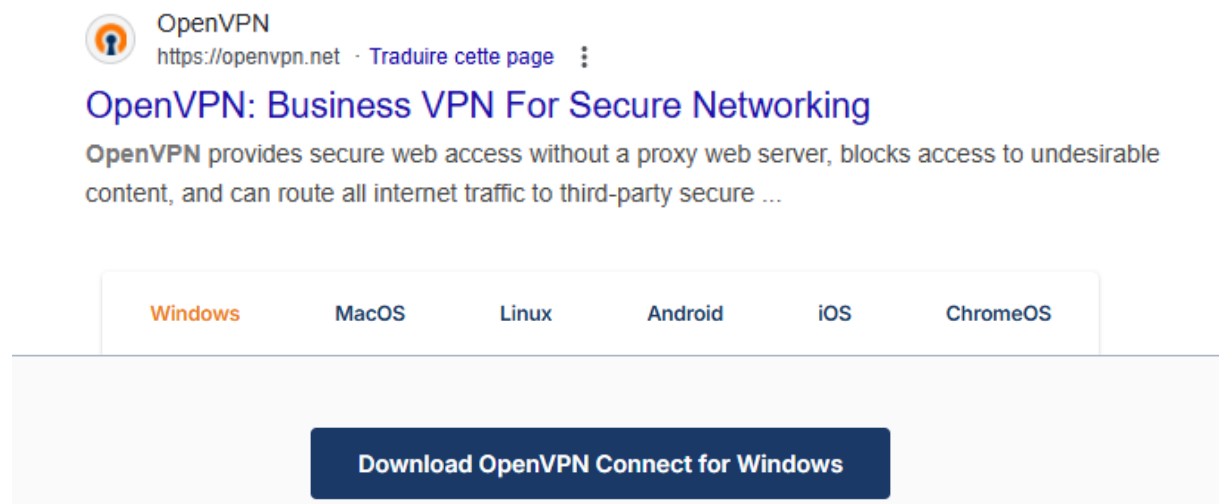
Via Serveur NAS Synology



Mise en place open VPN sur un serveur NAS

Comment permettre un accès distant, sécurisé et centralisé aux ressources internes d'une entreprise en utilisant un serveur NAS comme point de terminaison VPN avec OpenVPN, tout en garantissant la confidentialité des données, la facilité de gestion et la continuité d'activité ?

Etape 1) Installer le logiciel openvpn sur le poste client.

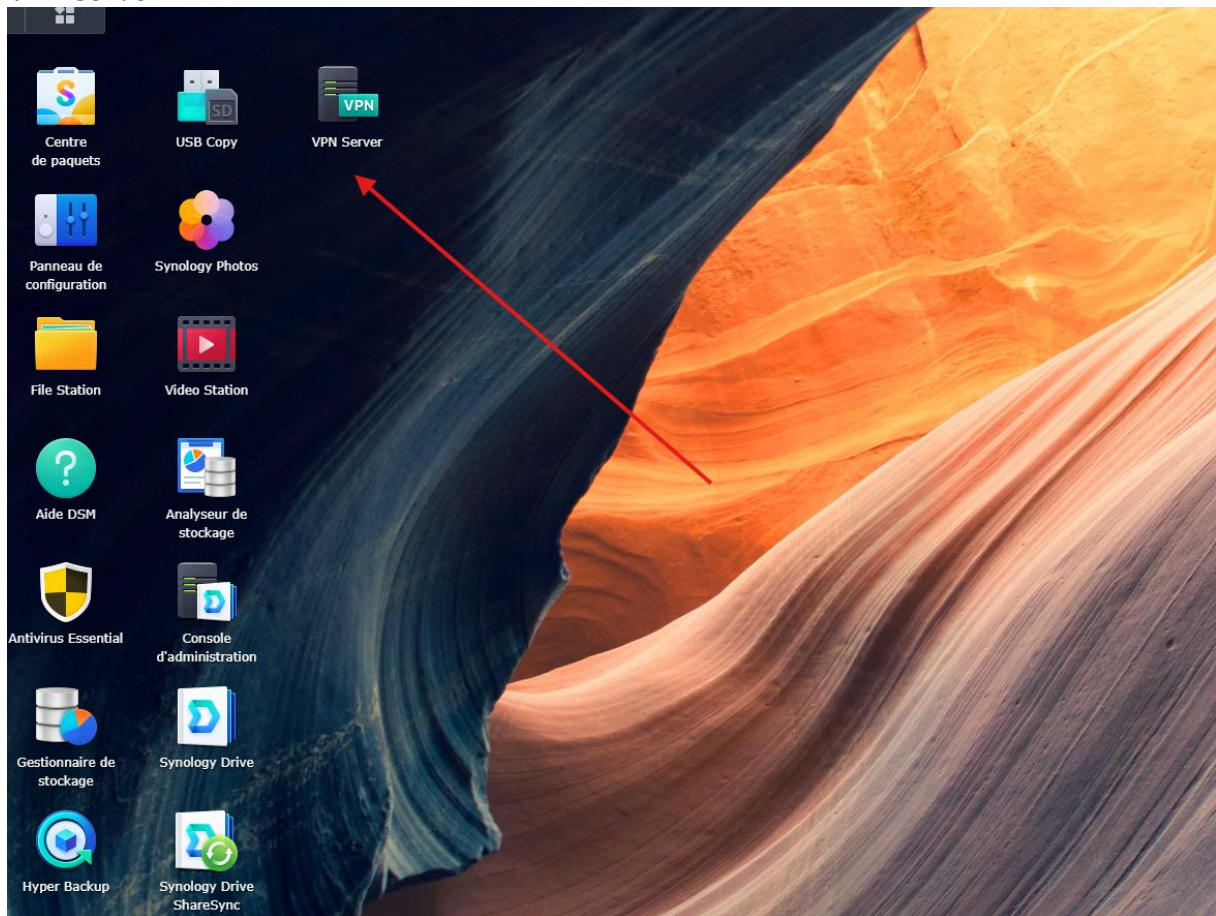


The screenshot shows the OpenVPN website interface. At the top left is the OpenVPN logo and the text "OpenVPN" followed by the URL "https://openvpn.net" and a "Traduire cette page" link. Below this is the main heading "OpenVPN: Business VPN For Secure Networking" and a descriptive paragraph: "OpenVPN provides secure web access without a proxy web server, blocks access to undesirable content, and can route all internet traffic to third-party secure ...". A horizontal navigation bar contains tabs for "Windows", "MacOS", "Linux", "Android", "iOS", and "ChromeOS". The "Windows" tab is selected and highlighted in orange. Below the navigation bar is a large dark blue button with the text "Download OpenVPN Connect for Windows".

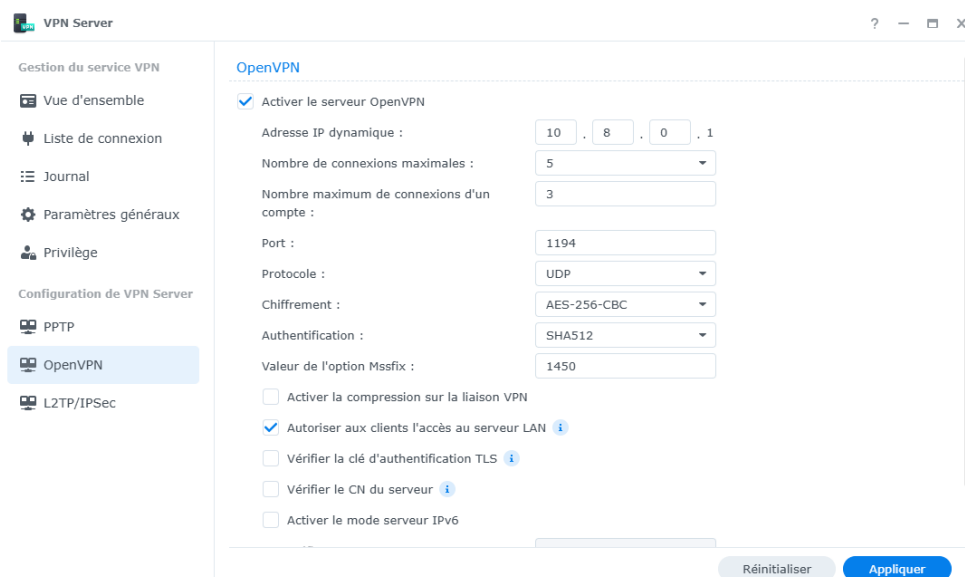
OpenVPN crée un **tunnel chiffré** entre l'utilisateur à distance (employé en télétravail, technicien en déplacement...) et le réseau local.

Cela protège les données contre les interceptions (ex. : Wi-Fi publics non sécurisés).

Etape 2) Installer dans le centre de paquets sur l'interface web de synology le paquet VPN server.



Etape 3) Activer le service → désactiver la compression et Autoriser aux client l'accès au lan. On clique sur Appliquer.



Etape 4) On se connecte sur l'interface ip de la box du FAI.



Par la suite on va créer une règle NAT pour faire une redirection de port pour faire simple dans l'exemple ci-dessous le port interne et externe sont les mêmes néanmoins je recommande de changer cela car c'est beaucoup moins sécurisé car c'est le port par défaut.

Navigation tabs: DHCP | NAT/PAT | DNS | UPnP | DynDNS | DMZ | NTP | IPv6 | CGN

Les règles NAT/PAT sont nécessaires pour autoriser une communication initiée depuis Internet avec un équipement particulier de votre réseau. Utiles pour certaines applications comme des jeux en lignes ou des serveurs de type FTP ... Assurez-vous que cet équipement a une adresse IP statique (paramétrable dans l'onglet DHCP).
Uniquement pour des équipements IPv4.

Vos règles personnalisées

Choisissez des ports qui ne sont pas bloqués par le pare-feu.
Nous vous déconseillons la création d'une règle sur le port 53 (service DNS).
Les équipements doivent être configurés avec une adresse IP statique pour être disponibles.

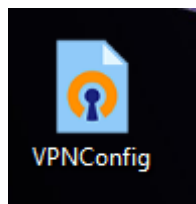
Form fields: FTP Server (dropdown), 21 (input, ex.: 1000), 21 (input, ex.: 1000-2000), TCP (dropdown), RE705X (dropdown), Toutes (dropdown), Créer (button), IP externes autorisées

Activer	Application/Service	Port interne	Port externe	Protocole	Équipement	IP externe	
<input checked="" type="checkbox"/>	OPENVPN	1194	1194	UDP	victor25	Toutes	

Etape 5) Exporter la configuration pour l'implanter dans le logiciel openvpn.

Adresse IP dynamique :	10 . 8 . 0 . 1
Nombre de connexions maximales :	5
Nombre maximum de connexions d'un compte :	3
Port :	1194
Protocole :	UDP
Chiffrement :	AES-256-CBC
Authentification :	SHA512
Valeur de l'option Mssfix :	1450
<input type="checkbox"/> Activer la compression sur la liaison VPN	
<input checked="" type="checkbox"/> Autoriser aux clients l'accès au serveur LAN i	
<input type="checkbox"/> Vérifier la clé d'authentification TLS i	
<input type="checkbox"/> Vérifier le CN du serveur i	
<input type="checkbox"/> Activer le mode serveur IPv6	
Préfixe :	
<input type="button" value="Exporter la configuration"/>	

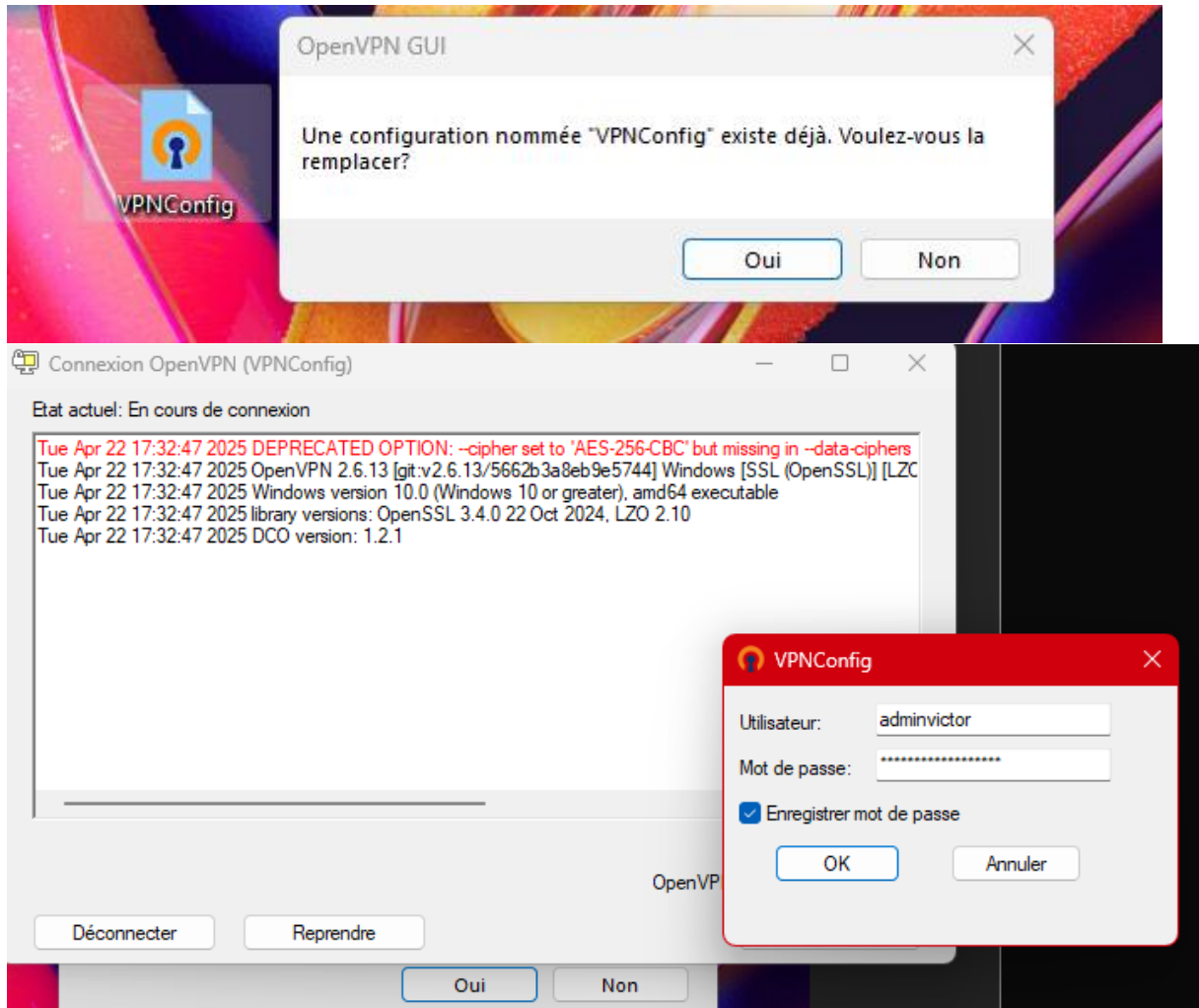
Ouvrir le fichier VPNConfig avec un bloc note → ajouter l'ip ou dans le cas ici présent le lien Quickconnect de serveur synology avec le port à la suite qui correspond à l'ouverture dans le pare-feu.



```
dev tun
tls-client
remote [redacted].synology.me 1194

# 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.)
```

Etape 6) Implanter la configuration en double-cliquant sur le fichier config VPN



A la fin le tunnel VPN s'active



www

