Mise en place tunnel VPN (openvpn)

Qu'est-ce qu'un VPN ?

Un VPN, ou Réseau Privé Virtuel (Virtual Private Network en anglais), est une technologie qui crée une connexion sécurisée et chiffrée entre votre appareil (ordinateur, smartphone, tablette) et un serveur distant opéré par le service VPN. Cette connexion sécurisée permet de transmettre des données de manière confidentielle sur des réseaux publics ou partagés comme Internet.

Fonctionnement d'un VPN

Le VPN fonctionne en établissant un "tunnel" sécurisé entre votre appareil et le serveur VPN. Voici les étapes clés du processus :

Connexion à un Serveur VPN : Lorsque vous vous connectez à un VPN, votre appareil se connecte à un serveur VPN choisi (parmi une liste de serveurs disponibles) via une connexion chiffrée.

Chiffrement des Données : Toutes les données envoyées et reçues via cette connexion sont chiffrées, ce qui signifie qu'elles sont converties en un format illisible pour toute personne qui tenterait de les intercepter.

Adresse IP Masquée : Votre adresse IP réelle est remplacée par l'adresse IP du serveur VPN, rendant votre activité en ligne anonyme et protégeant votre identité.

Transmission des Données : Les données chiffrées sont transmises à travers le tunnel sécurisé jusqu'au serveur VPN, qui les déchiffre et les envoie à leur destination finale (par exemple, un site web ou un service en ligne).

Utilités d'un VPN

Un VPN offre plusieurs avantages, notamment :

Sécurité en Ligne : Le chiffrement des données protège vos informations personnelles et sensibles contre les cybercriminels, surtout lorsque vous utilisez des réseaux Wi-Fi publics (dans les cafés, les aéroports, etc.).

Confidentialité et Anonymat : En masquant votre adresse IP, un VPN empêche les sites web, les annonceurs et même votre fournisseur d'accès Internet de suivre vos activités en ligne.

Accès à du Contenu Restreint : Un VPN permet de contourner les restrictions géographiques et de censurer l'accès à des contenus ou services disponibles uniquement dans certaines régions (comme certains catalogues de streaming).

Éviter la Surveillance : Les VPN peuvent aider à protéger contre la surveillance en ligne par des gouvernements ou des entreprises, assurant une navigation plus privée et sécurisée.

Télétravail Sécurisé : De nombreuses entreprises utilisent des VPN pour permettre à leurs employés de se connecter en toute sécurité au réseau interne de l'entreprise lorsqu'ils travaillent à distance.

Types de VPN

Il existe plusieurs types de VPN, adaptés à différents besoins :

VPN Accès à Distance : Utilisé par les particuliers pour se connecter à Internet de manière sécurisée depuis n'importe où.

VPN Site-à-Site : Utilisé par les entreprises pour relier plusieurs réseaux locaux (LAN) situés dans différents endroits.

VPN Mobile : Conçu pour les appareils mobiles afin de sécuriser les connexions sur des réseaux sans fil.

En résumé, un VPN est une solution puissante pour améliorer la sécurité, la confidentialité et l'accès à des contenus en ligne, en chiffrant les connexions et en masquant les adresses IP des utilisateurs.

Prerequis de la procedure

Mise en place Côté Serveur (Linux)

Logiciels :

- OpenSSH-Server : Logiciel nécessaire pour exécuter le serveur SSH.

Configurations :

- Fixer l'adresse IPv4
- Installation d'OpenSSH-Server : Utilisez le gestionnaire de paquets de votre distribution pour installer openssh-server.
- Démarrage du service SSH : Assurez-vous que le service SSH est actif (sudo systemctl start ssh).
- Activation au démarrage : Configurez SSH pour qu'il démarre automatiquement lors du boot (sudo systemctl enable ssh).
- Sécurité : (Optionnel mais recommandé) Configurez les clés SSH pour une authentification sans mot de passe, changez le port par défaut (22) pour réduire les scans automatiques et envisagez d'utiliser Fail2Ban pour protéger contre les tentatives de connexion abusives.

Côté Client

Logiciels :

- Linux/Unix : Client SSH intégré (aucune action requise).
- Windows : PuTTY ou Windows Subsystem for Linux (WSL) pour une expérience similaire à Linux.

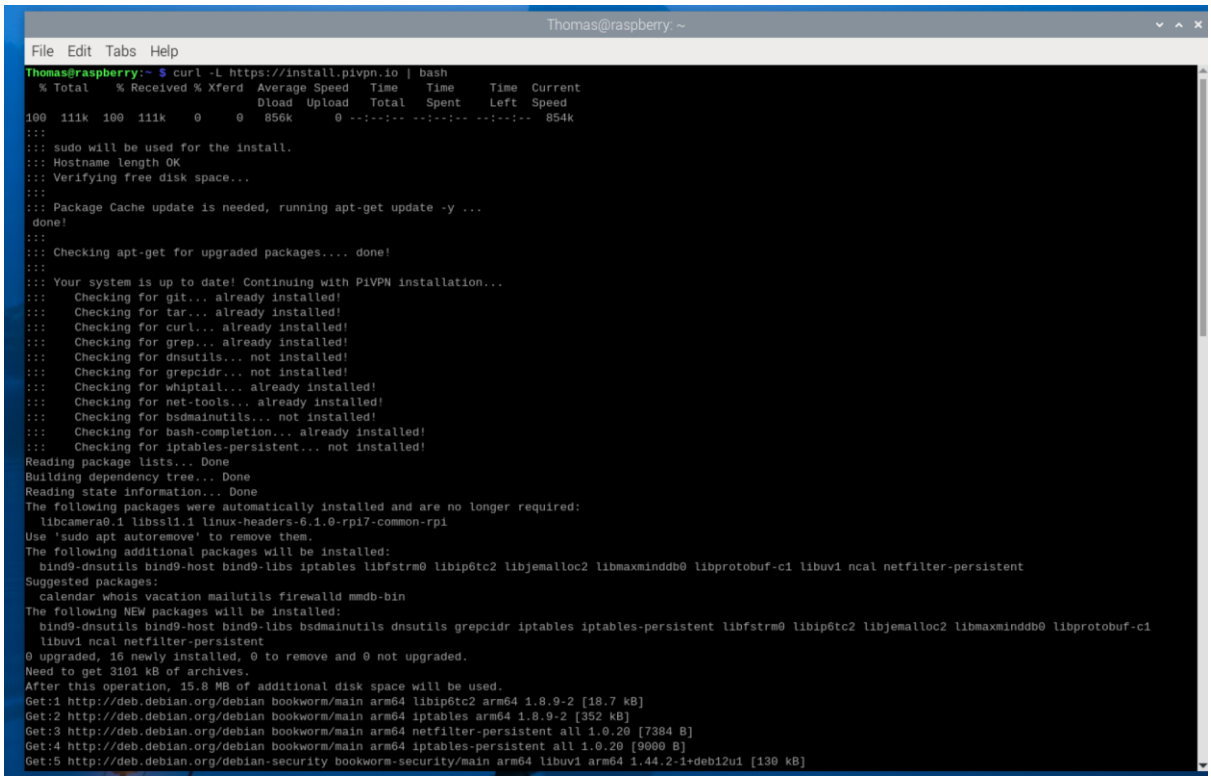
Configurations :

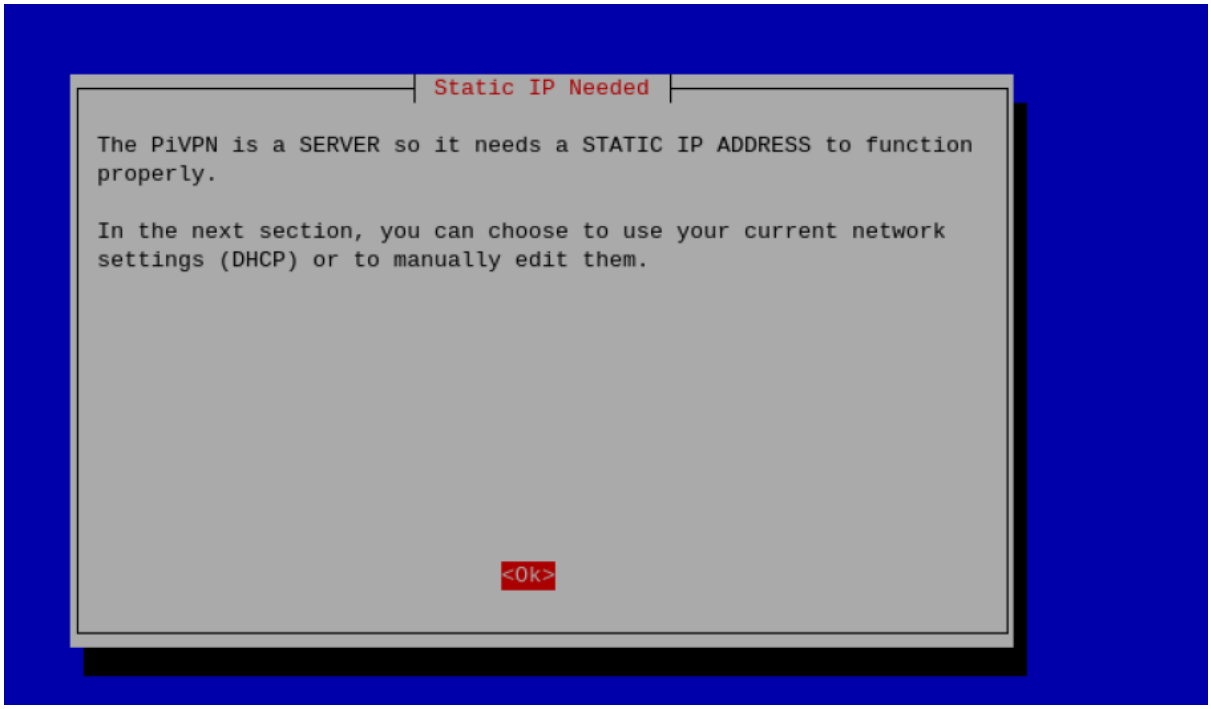
- Connaître l'adresse IP : Déterminez l'adresse IP du serveur (locale pour le réseau interne ou publique pour l'accès à distance).
- Port Forwarding : (Si accès à distance via Internet) Configurez le routeur pour rediriger le port SSH vers le serveur.
- Sécurité : Utilisez des clés SSH pour une connexion sécurisée depuis le client, surtout si vous accédez au serveur via Internet.
- Cette liste constitue le fondement d'une configuration minimale pour la mise en place d'un serveur SSH et l'accès à celui-ci. Pour des environnements spécifiques ou des configurations avancées, des étapes supplémentaires peuvent être nécessaires.

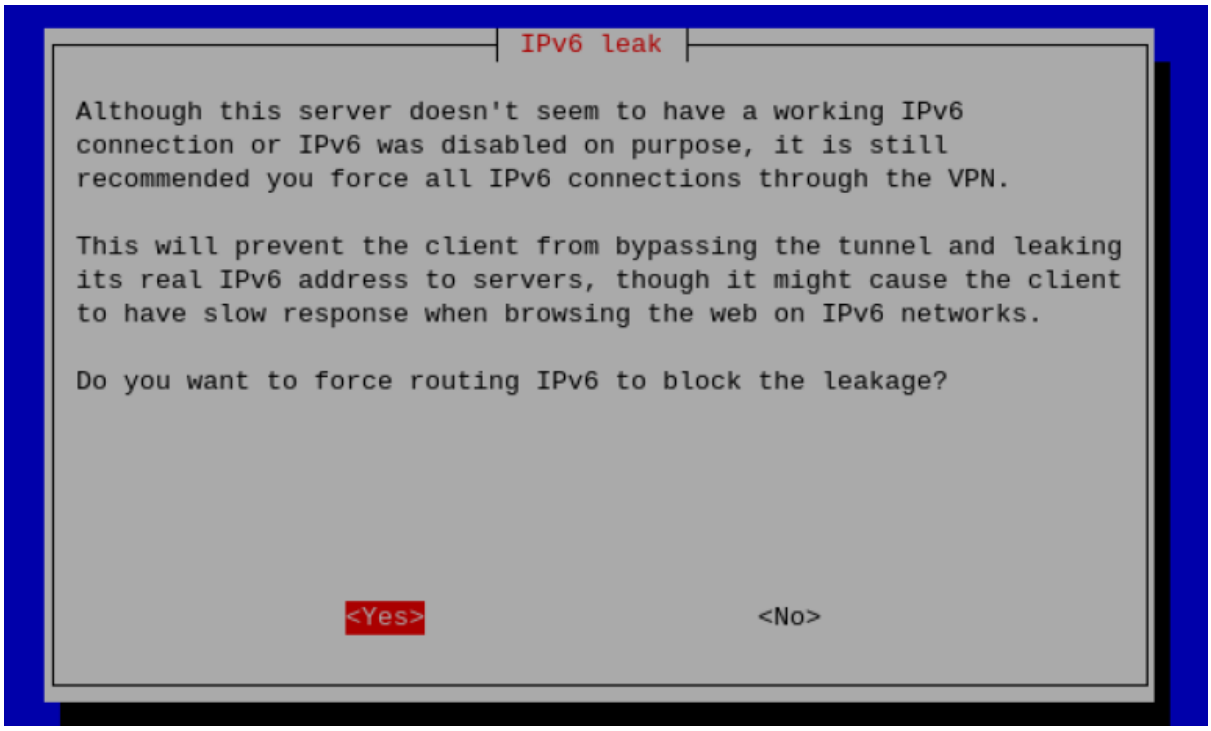
Mise en place d'open VPN serveur sous Raspberry OS

Serveur Raspberry OS

- Installation de pivpn (solution de Openvpn pour Raspberry) :
    - curl -L https://install.pivpn.io | bash







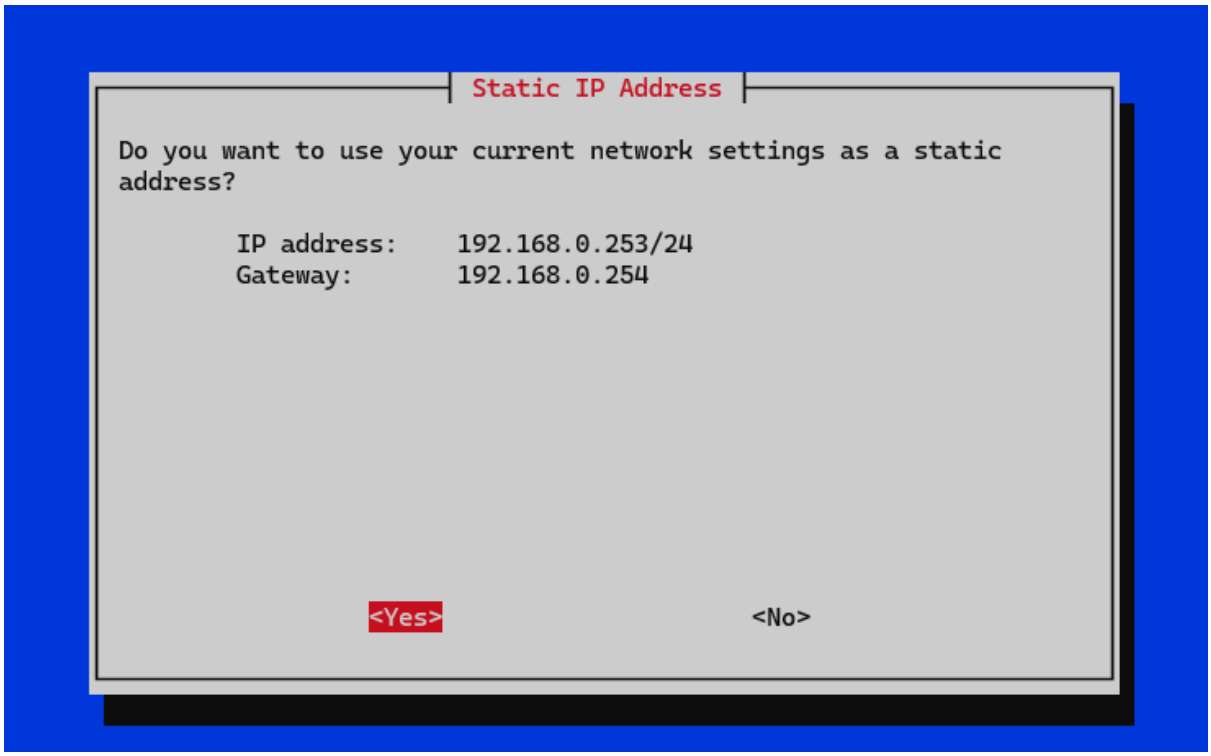
Il semble que vous soyez confronté à une alerte concernant une possible fuite d'IPv6 pendant la configuration de votre VPN. Cette alerte indique que, bien que le serveur VPN ne dispose pas d'une connexion IPv6 active ou que l'IPv6 a été désactivé volontairement, il est recommandé de forcer toutes les connexions IPv6 à passer par le VPN. Cela empêchera votre client VPN de divulguer son adresse IPv6 réelle en dehors du tunnel VPN, ce qui pourrait se produire si votre client essaie d'accéder à des sites ou des services qui utilisent l'IPv6.

Le message vous avertit également que forcer le routage de l'IPv6 peut ralentir la navigation sur les réseaux IPv6, car toutes les données doivent passer par le tunnel VPN, qui peut ne pas avoir une latence aussi faible que votre connexion directe habituelle.

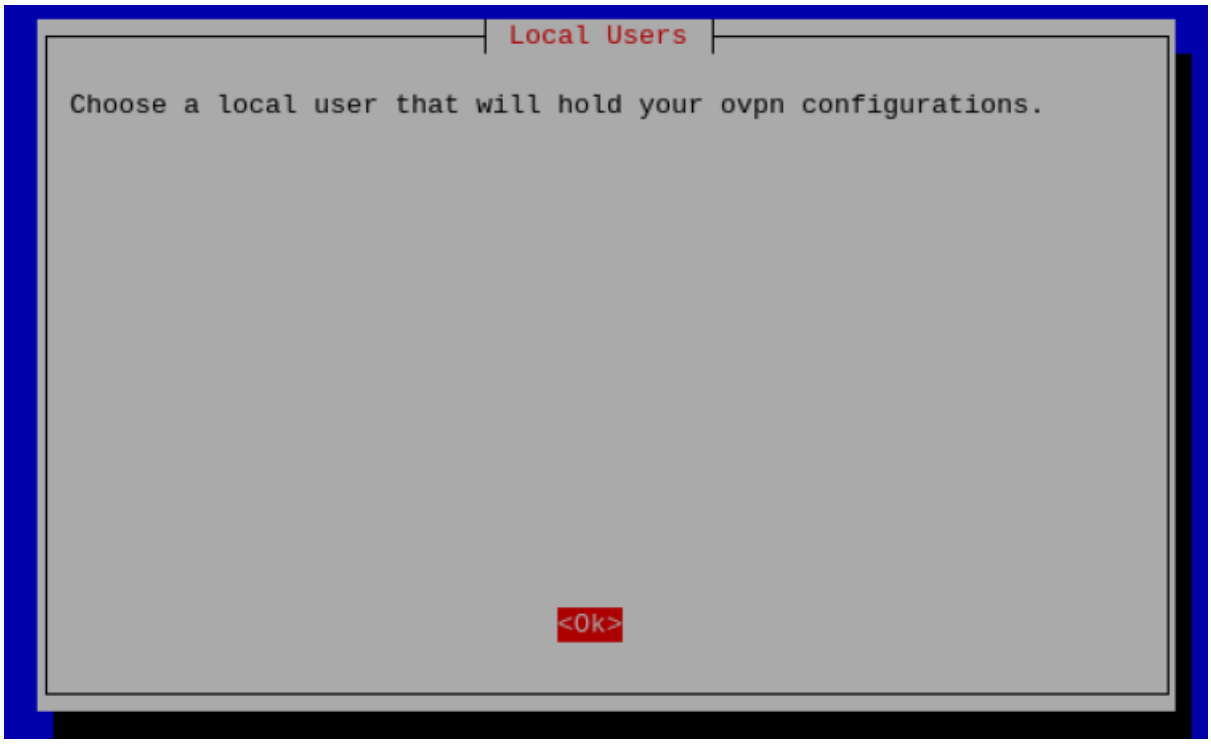
Sélectionnez « Yes » si vous souhaitez maximiser la confidentialité et la sécurité pour éviter toute fuite d'IPv6. Cela garantira que tout le trafic passe par le VPN, y compris l'IPv6, ce qui est crucial si vous avez des préoccupations en matière de sécurité ou de confidentialité.

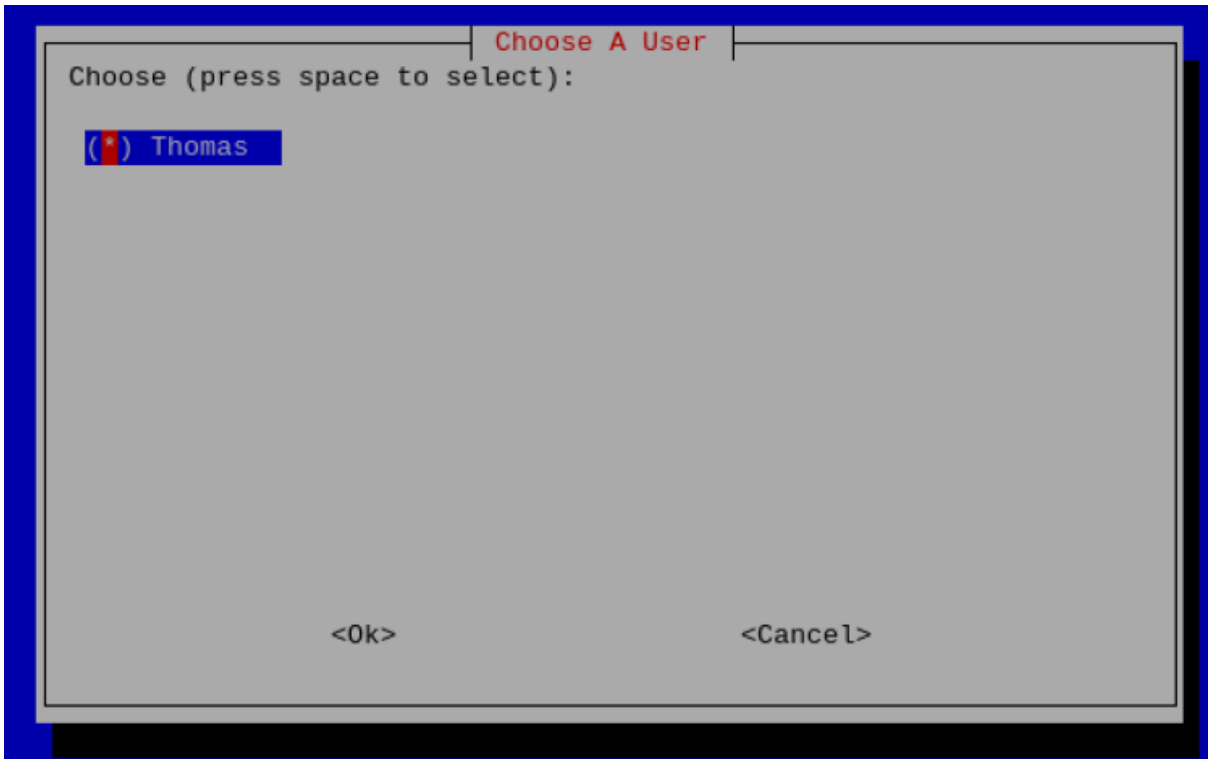
Sélectionnez « No » si la performance de navigation sur IPv6 est une priorité pour vous et que vous êtes prêt à accepter les risques de fuite d'IPv6. Cela pourrait être le cas si vous utilisez des services qui requièrent une réponse rapide en IPv6 et que le serveur VPN ne supporte pas bien l'IPv6 ou est significativement plus lent pour le trafic IPv6.

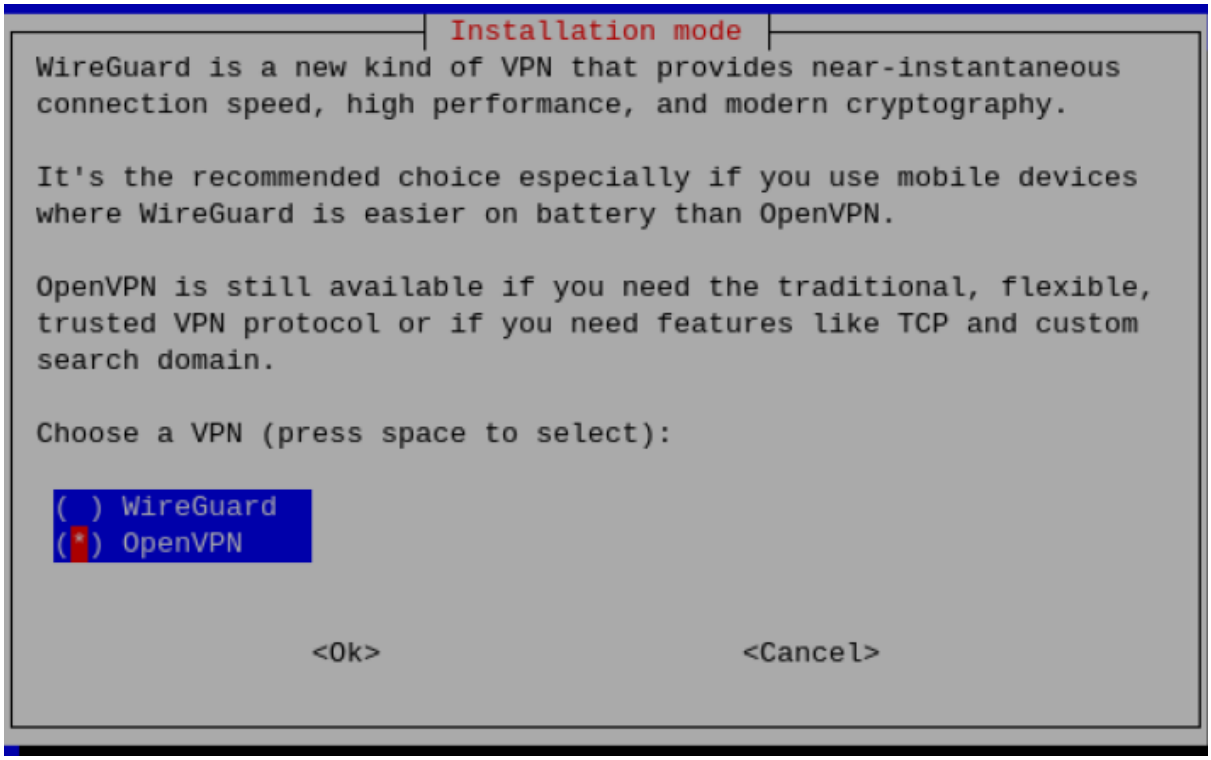
Prenez en compte que même si votre serveur VPN n'est pas configuré pour l'IPv6, cela ne signifie pas nécessairement que votre client n'essaiera pas d'utiliser l'IPv6. Si la sécurité est votre priorité absolue, il est généralement conseillé de bloquer toute possibilité de fuite d'IPv6.

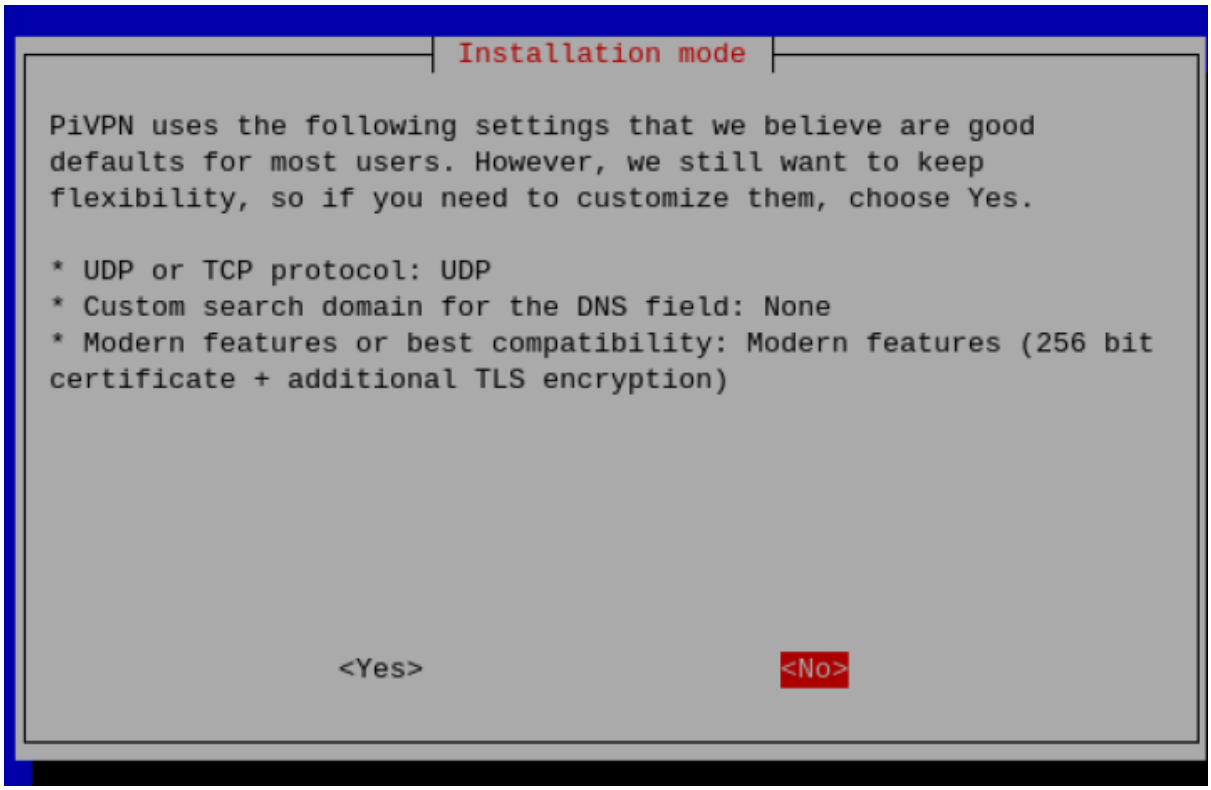


- Sur mon routeur j'ai procédé à la réservation de l'adresse ip pour le serveur


Local Users
Choose a local user that will hold your ovpn configurations.
<Ok>


Choose A User
Choose (press space to select):
(*) Thomas
<Ok>
<Cancel>





UDP ou TCP protocol: UDP est sélectionné par défaut. UDP est généralement préféré pour les VPN car il offre des vitesses de connexion plus rapides que TCP.

Domaine de recherche personnalisé pour le champ DNS: Aucun domaine de recherche personnalisé n'est configuré par défaut.

Fonctionnalités modernes ou meilleure compatibilité : Les fonctionnalités modernes sont sélectionnées par défaut, ce qui inclut un certificat de 256 bits et un chiffrement TLS additionnel.

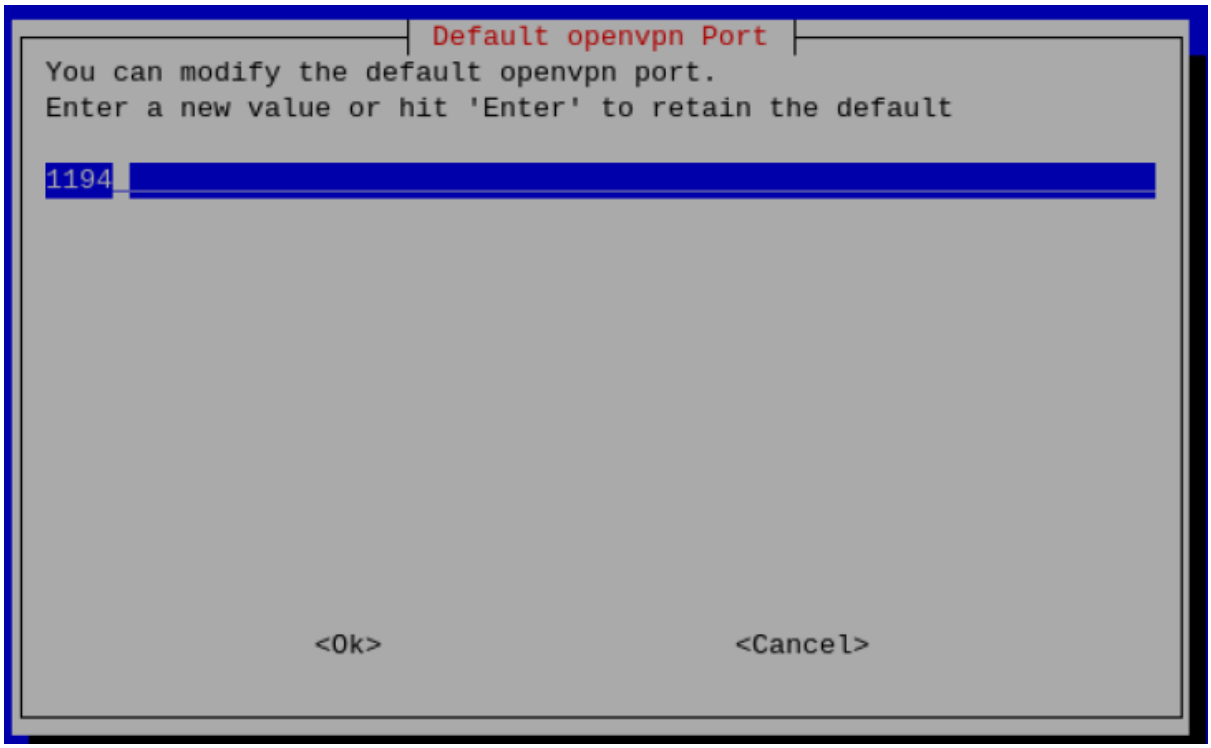
La question est de savoir si vous souhaitez personnaliser ces paramètres. La plupart des utilisateurs trouveront que les paramètres par défaut conviennent à leurs besoins. Cependant, si vous avez des exigences spécifiques qui nécessitent de s'éloigner des paramètres par défaut, vous devriez sélectionner « Yes ».

Pour la plupart des installations de serveurs VPN domestiques, en l'absence de besoins spécifiques :

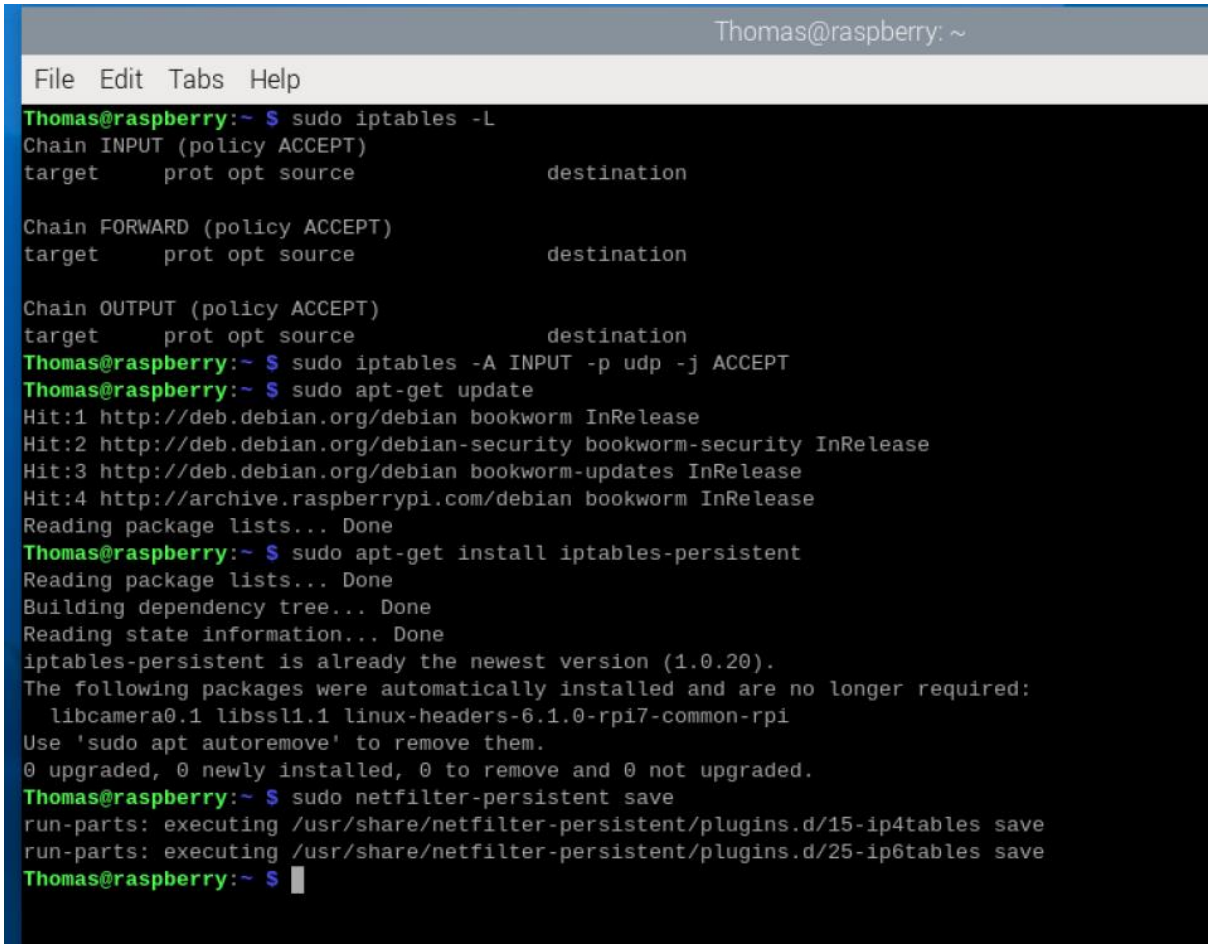
Sélectionnez « No » si vous êtes satisfait des paramètres par défaut, ce qui est recommandé pour la simplicité et la facilité d'utilisation.

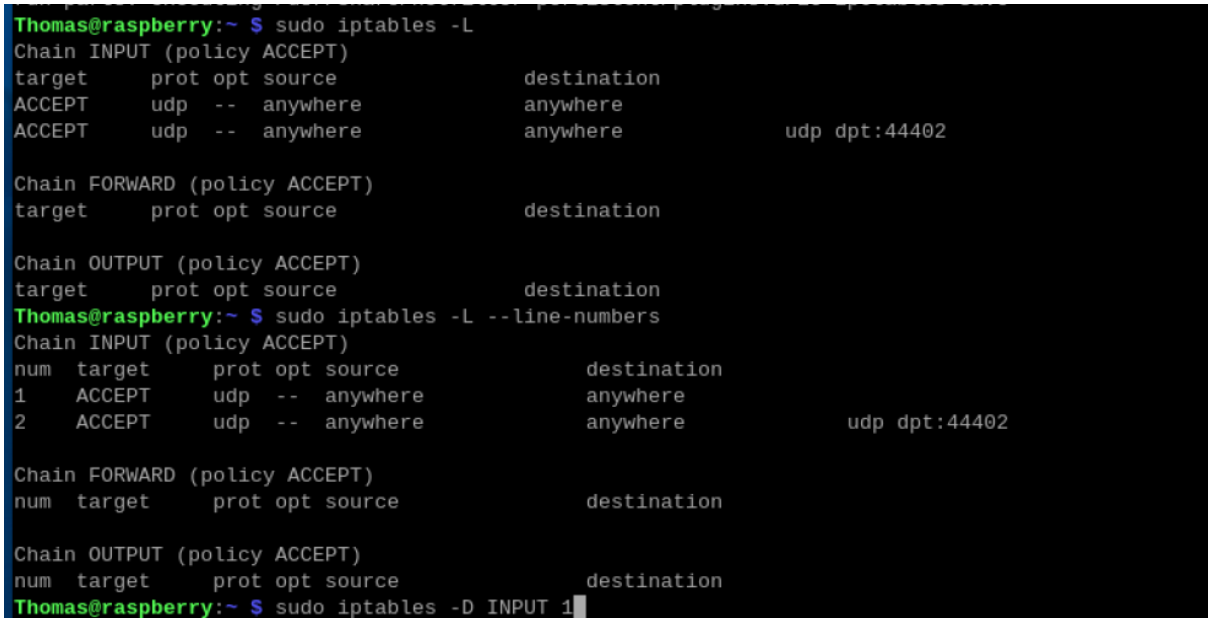
Sélectionnez « Yes » seulement si vous avez besoin de personnaliser les paramètres, par exemple, si vous avez un réseau qui nécessite un domaine de recherche DNS spécifique, ou si vous devez utiliser le protocole TCP pour une meilleure fiabilité dans un environnement de réseau instable.

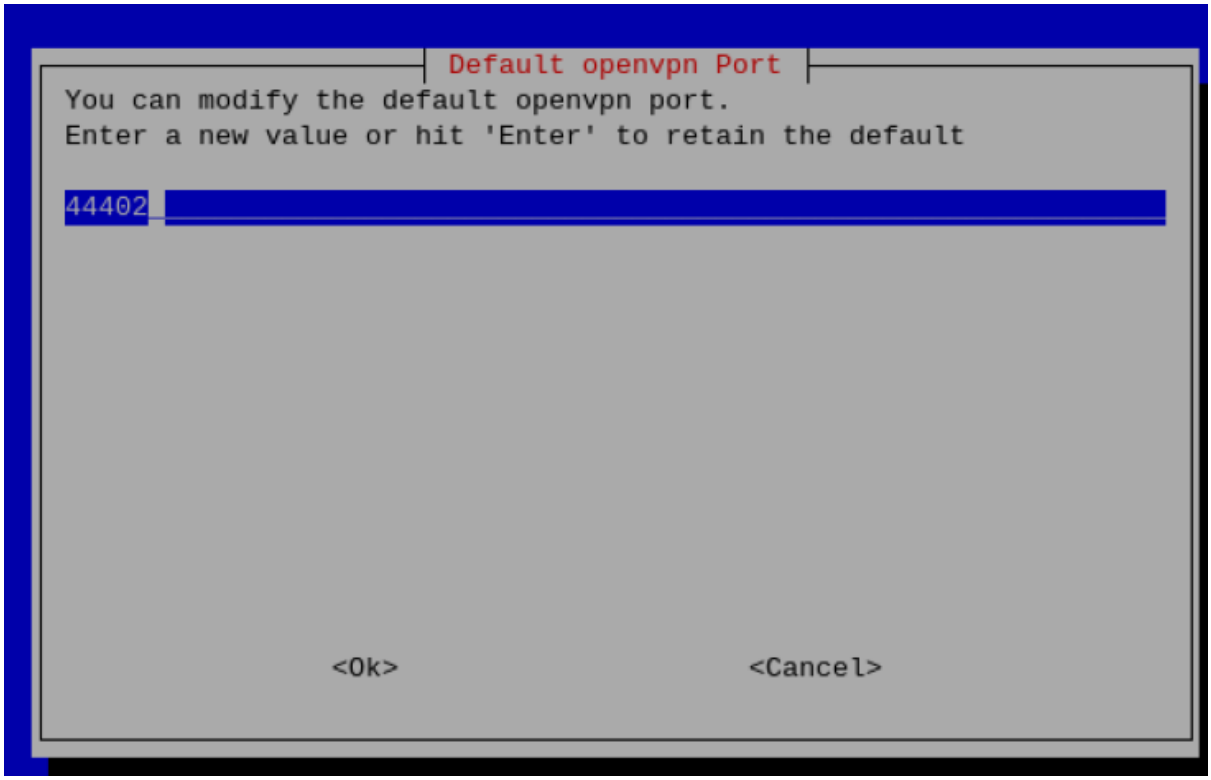
En général, il est conseillé de commencer avec les paramètres par défaut et de ne personnaliser que si vous rencontrez des problèmes ou avez des exigences qui ne sont pas remplies par ces paramètres.



Creation d’un port atypique

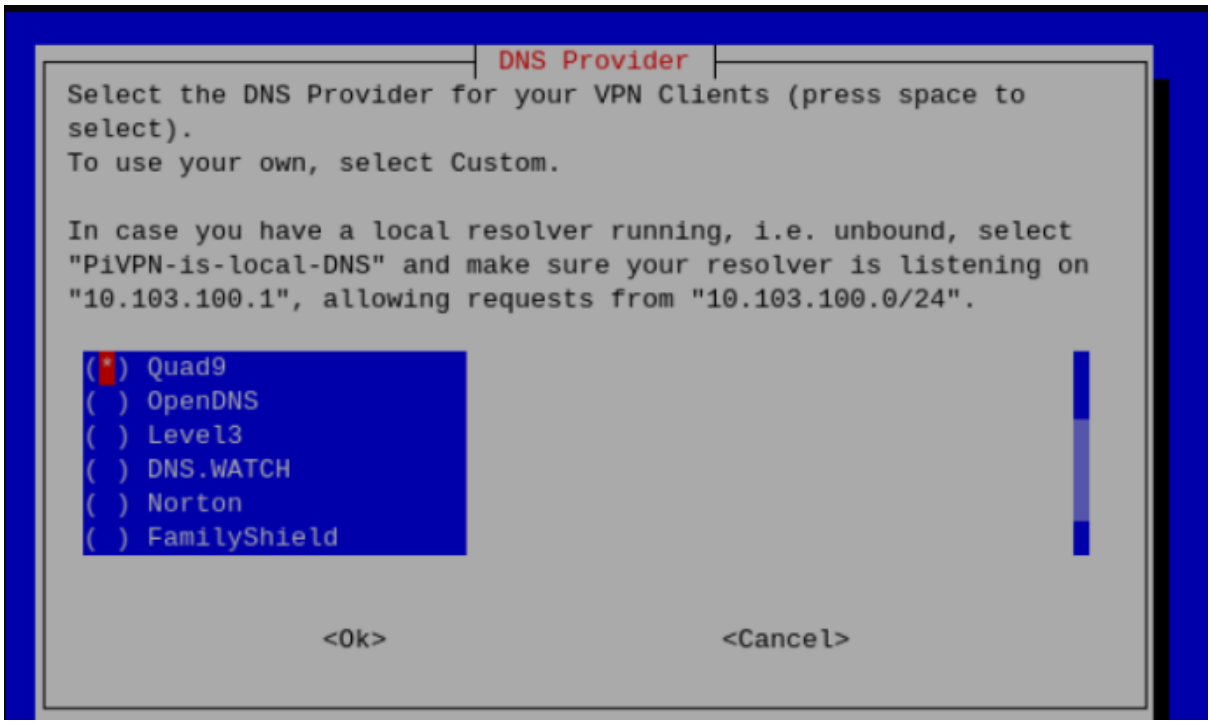

Thomas@raspberry: ~
File Edit Tabs Help
Thomas@raspberry:~ $ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Thomas@raspberry:~ $ sudo iptables -A INPUT -p udp -j ACCEPT
Thomas@raspberry:~ $ sudo apt-get update
Hit:1 http://deb.debian.org/debian bookworm InRelease
Hit:2 http://deb.debian.org/debian-security bookworm-security InRelease
Hit:3 http://deb.debian.org/debian bookworm-updates InRelease
Hit:4 http://archive.raspberrypi.com/debian bookworm InRelease
Reading package lists... Done
Thomas@raspberry:~ $ sudo apt-get install iptables-persistent
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables-persistent is already the newest version (1.0.20).
The following packages were automatically installed and are no longer required:
libcamera0.1 libssl1.1 linux-headers-6.1.0-rpi7-common-rpi
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Thomas@raspberry:~ $ sudo netfilter-persistent save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
Thomas@raspberry:~ $


Thomas@raspberry:~ $ sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT udp -- anywhere anywhere
ACCEPT udp -- anywhere anywhere udp dpt:44402
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Thomas@raspberry:~ $ sudo iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num target prot opt source destination
1 ACCEPT udp -- anywhere anywhere
2 ACCEPT udp -- anywhere anywhere udp dpt:44402
Chain FORWARD (policy ACCEPT)
num target prot opt source destination
Chain OUTPUT (policy ACCEPT)
num target prot opt source destination
Thomas@raspberry:~ $ sudo iptables -D INPUT 1

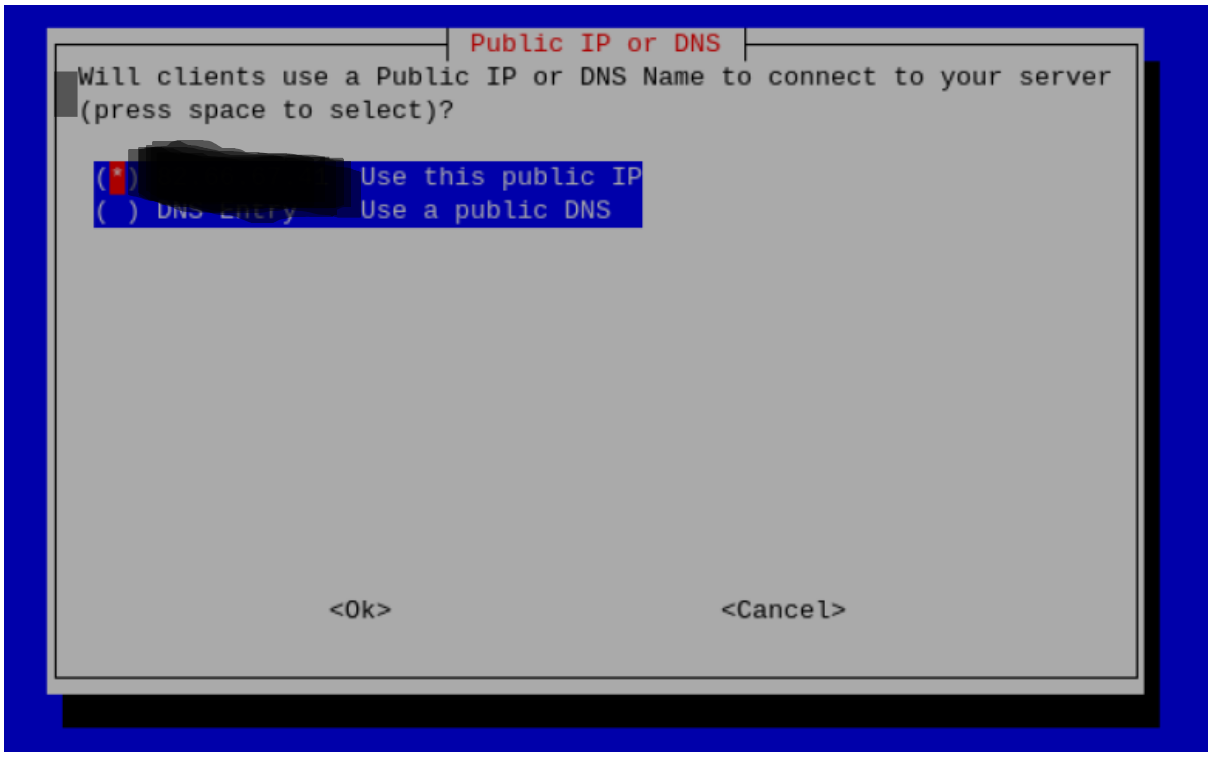

Default openvpn Port
You can modify the default openvpn port.
Enter a new value or hit 'Enter' to retain the default
44402
<Ok>
<Cancel>

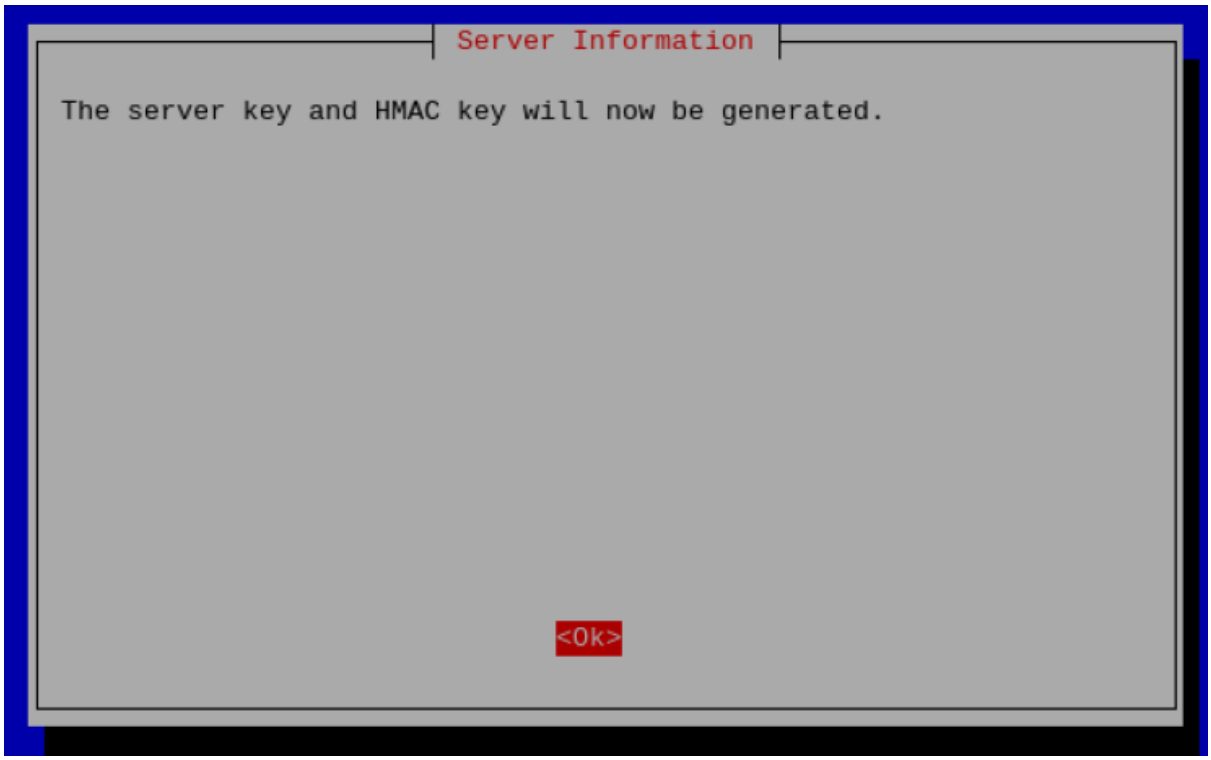

Confirm Custom Port Number
Are these settings correct?
PORT: 44402
<Yes>
<No>

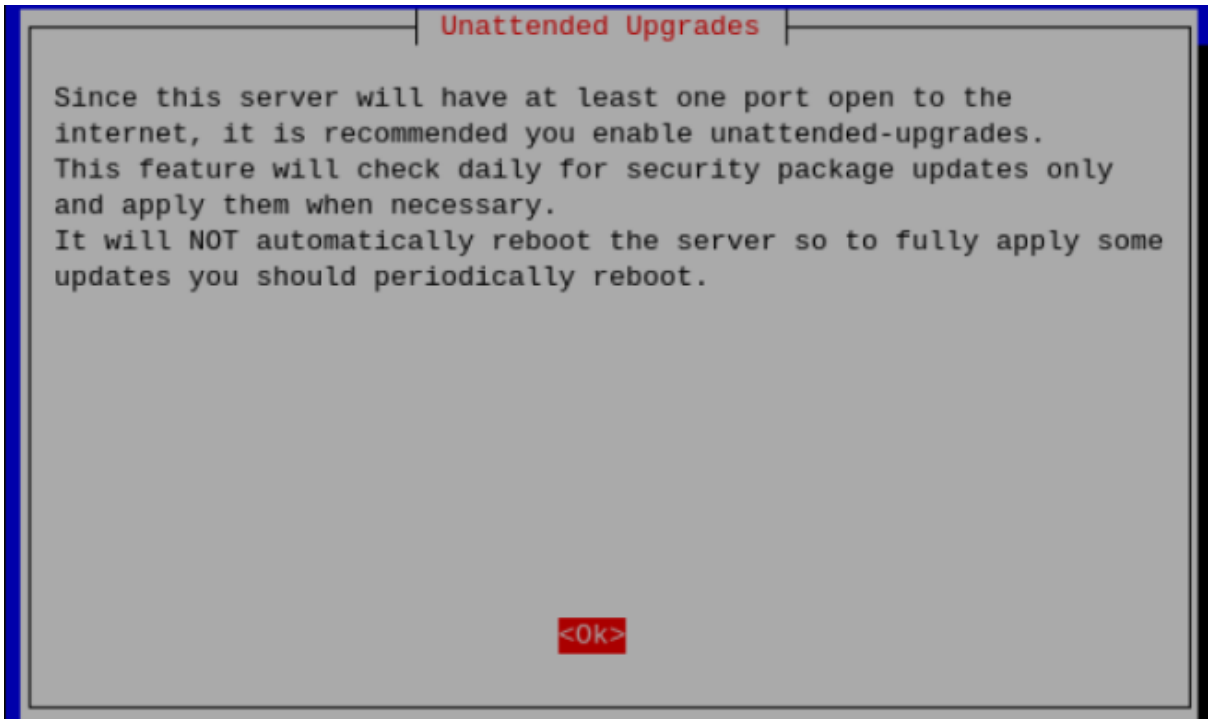
Choix du dns

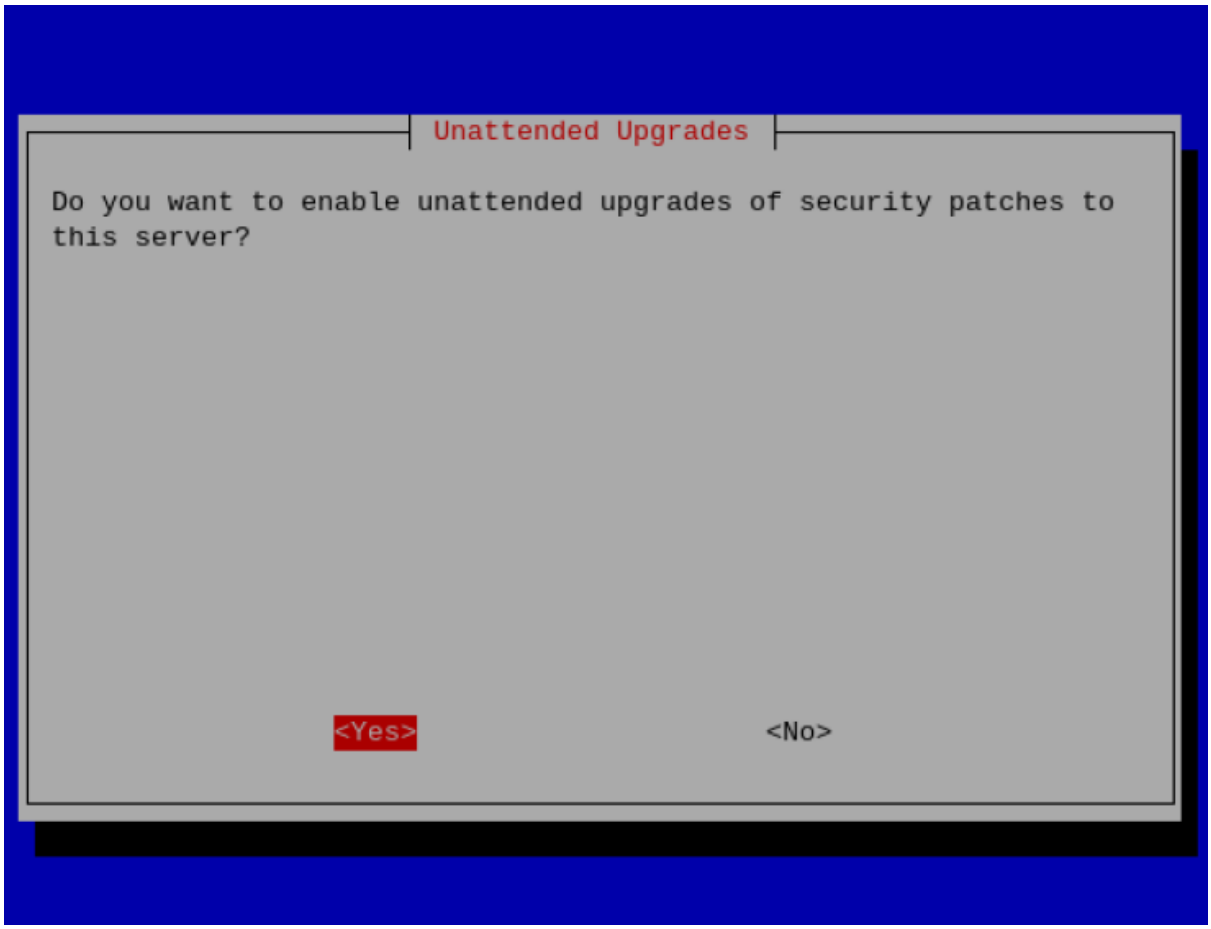


On chosi le DNS google




Server Information
The server key and HMAC key will now be generated.
<Ok>


Unattended Upgrades
Since this server will have at least one port open to the
internet, it is recommended you enable unattended-upgrades.
This feature will check daily for security package updates only
and apply them when necessary.
It will NOT automatically reboot the server so to fully apply some
updates you should periodically reboot.
<Ok>


Unattended Upgrades
Do you want to enable unattended upgrades of security patches to this server?
<Yes>
<No>


Installation Complete!
Now run 'pivpn add' to create the client profiles.
Run 'pivpn help' to see what else you can do!
If you run into any issue, please read all our documentation carefully.
All incomplete posts or bug reports will be ignored or deleted.
Thank you for using PiVPN.
<Ok>

sudo systemctl start openvpn@server

sudo systemctl enable openvpn@server

Étape 2: Génération d'un Profil Client VPN

Après l'installation de PiVPN, créez un profil client VPN :

Dans le terminal du Raspberry Pi, exécutez :

pivpn add

Nommez le profil client et définissez un mot de passe pour ce profil. Ce fichier. ovpn sera utilisé sur votre client Windows pour se connecter au VPN.

Transférez le fichier .ovpn généré vers votre PC Windows. Vous pouvez le faire via une clé USB, un service de stockage cloud sécurisé, ou par SCP si vous avez un client SSH installé sur votre PC Windows.

```
Thomas@raspberry:~ $ pivpn add
::: Create a client ovpn profile, optional nopass
:::
::: Usage: pivpn <-a|add> [-n|--name <arg>] [-p|--password <arg>]|[nopass] [-d|--days <number>] [-b|--bitwarden] [-i|--iOS] [-o|--ovpn] [-h|--help]
:::
::: Commands:
:::  [none]              Interactive mode
:::  nopass              Create a client without a password
:::  -n,--name           Name for the Client (default: "raspberry")
:::  -p,--password       Password for the Client (no default)
:::  -d,--days           Expire the certificate after specified number of days (default: 1080)
:::  -b,--bitwarden      Create and save a client through Bitwarden
:::  -i,--iOS            Generate a certificate that leverages iOS keychain
:::  -o,--ovpn           Regenerate a .ovpn config file for an existing client
:::  -h,--help           Show this help dialog

Enter a Name for the Client:  Thomas
How many days should the certificate last?  1080
Enter the password for the client:
Enter the password again to verify:
* Notice:
Using Easy-RSA configuration from: /etc/openvpn/easy-rsa/pki/vars

* Notice:
Using SSL: openssl OpenSSL 3.0.11 19 Sep 2023 (Library: OpenSSL 3.0.11 19 Sep 2023)

-----
* Notice:

Keypair and certificate request completed. Your files are:
req: /etc/openvpn/easy-rsa/pki/reqs/Thomas.req
key: /etc/openvpn/easy-rsa/pki/private/Thomas.key

Using configuration from /etc/openvpn/easy-rsa/pki/ebbaf9d8/temp.805c1746
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'Thomas'
Certificate is to be certified until Mar  1 15:00:57 2027 GMT (1080 days)

Write out database with 1 new entries
Database updated

* Notice:
Certificate created at: /etc/openvpn/easy-rsa/pki/issued/Thomas.crt

Client's cert found: Thomas.crt
Client's Private Key found: Thomas.key
CA public Key found: ca.crt
tls Private Key found: ta.key
```

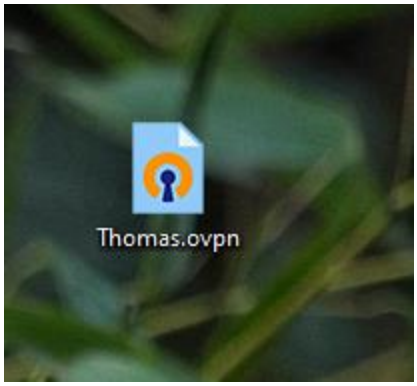
```
================================================================
Done! Thomas.ovpn successfully created!
Thomas.ovpn was copied to:
  /home/Thomas/ovpns
for easy transfer. Please use this profile only on one
device and create additional profiles for other devices.
================================================================
```

- J'ai importé le fichier sur la machine cliente
    - Pour se faire j'ai utilisé un server python sur mon réseaux local (natif de la distribution raspberry OS):

```
thomas@raspberrypi:~ $ cd ovpns/
thomas@raspberrypi:~/ovpns $ ls
PosteFixeThomas.ovpn  tphone.ovpn
```

- cd ovpns/
    - python -m http.server 8000

```
thomas@raspberrypi:~/ovpns $ python -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/)
```



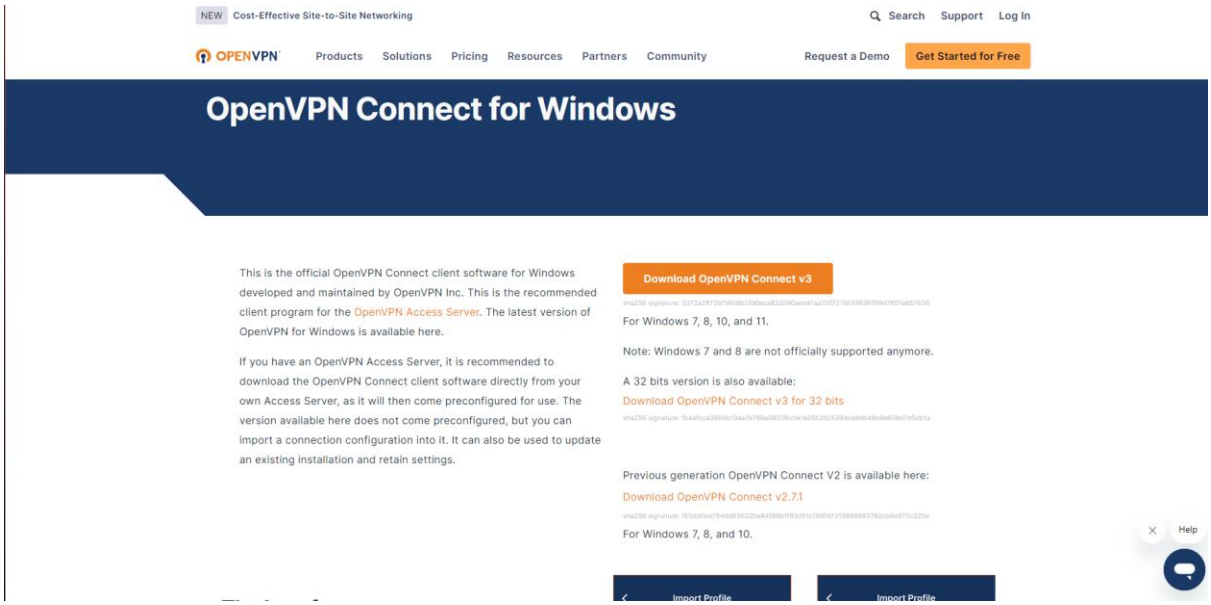
Mise en place d'open VPN sous Windows

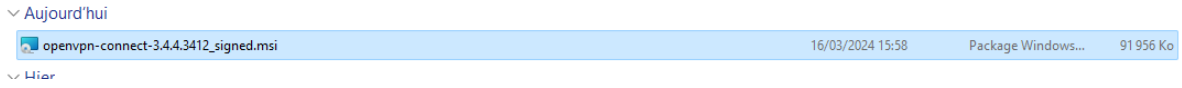
Installation de Open vpn connect

- Aller sur le site officiel

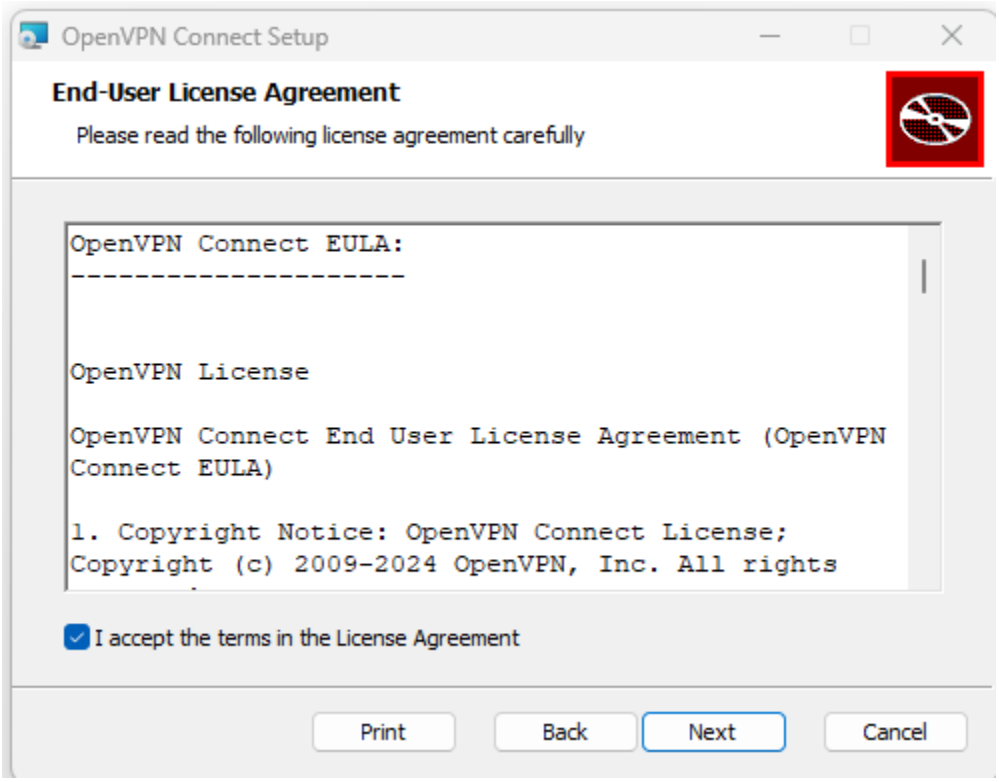
https://openvpn.net/client/client-connect-vpn-for-windows/

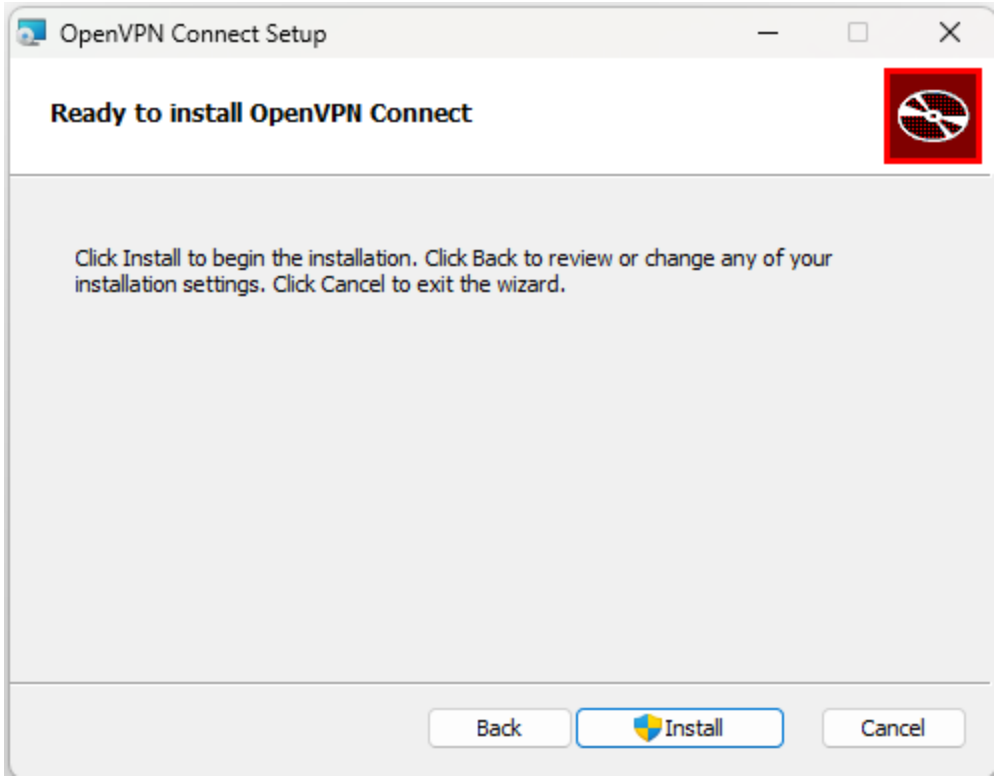
https://openvpn.net/downloads/openvpn-connect-v3-windows.msi

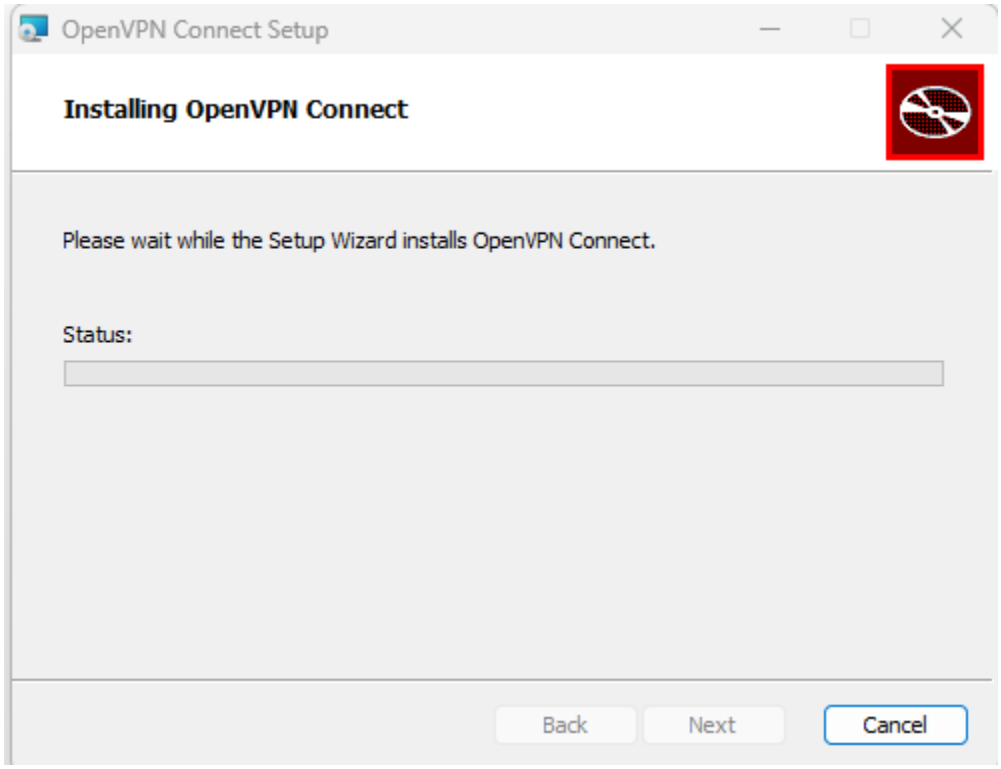


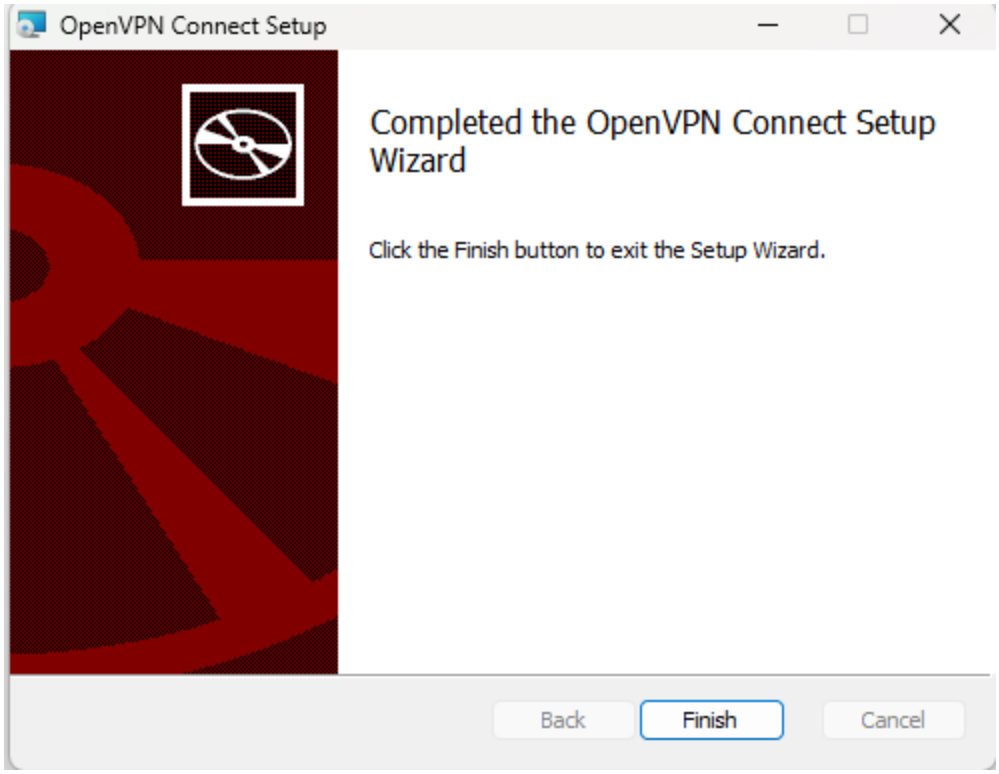

Aujourd'hui
openvpn-connect-3.4.4.3412_signed.msi
16/03/2024 15:58
Package Windows...
91 956 Ko
Hier

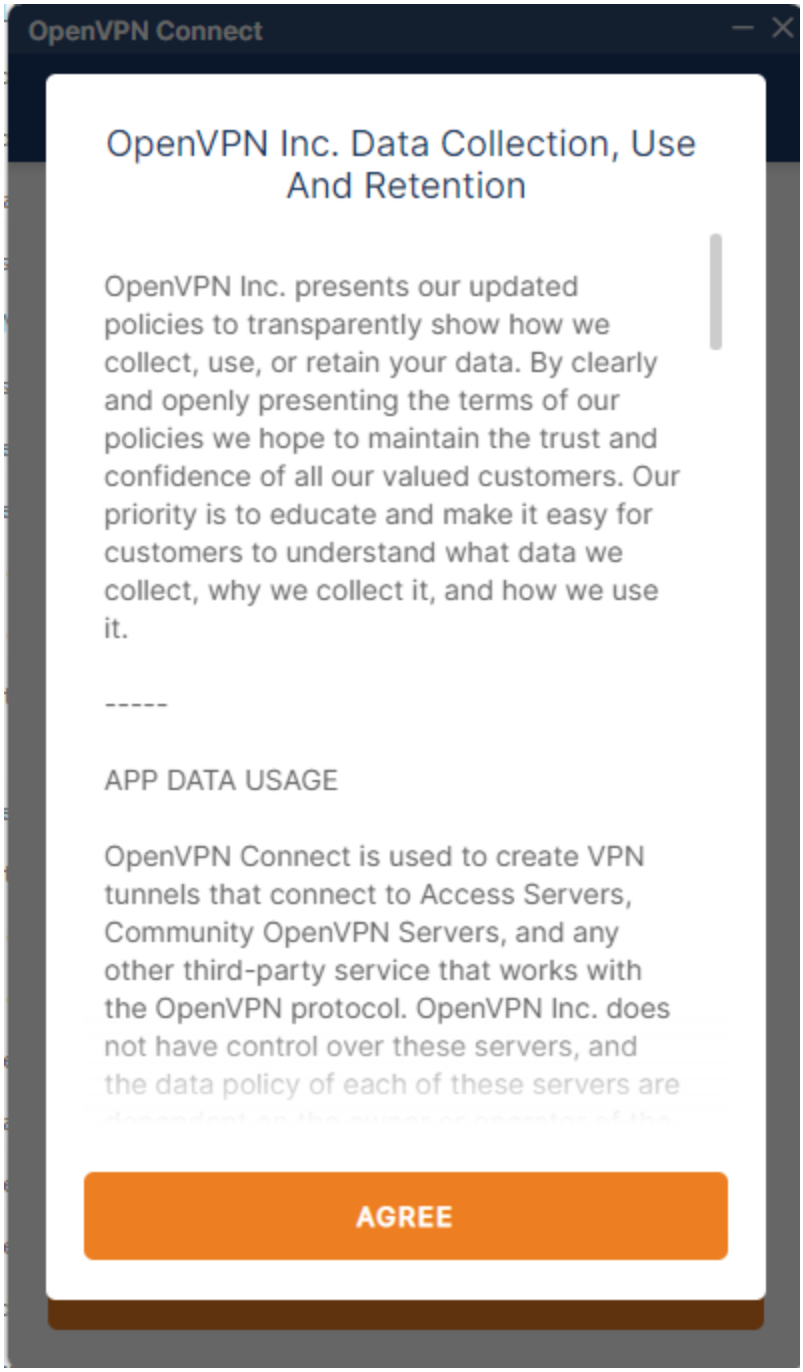

OpenVPN Connect Setup
Welcome to the OpenVPN Connect Setup Wizard
The Setup Wizard will install OpenVPN Connect on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Back
Next
Cancel


OpenVPN Connect Setup
End-User License Agreement
Please read the following license agreement carefully
OpenVPN Connect EULA:
OpenVPN License
OpenVPN Connect End User License Agreement (OpenVPN Connect EULA)
1. Copyright Notice: OpenVPN Connect License; Copyright (c) 2009-2024 OpenVPN, Inc. All rights
I accept the terms in the License Agreement
Print
Back
Next
Cancel

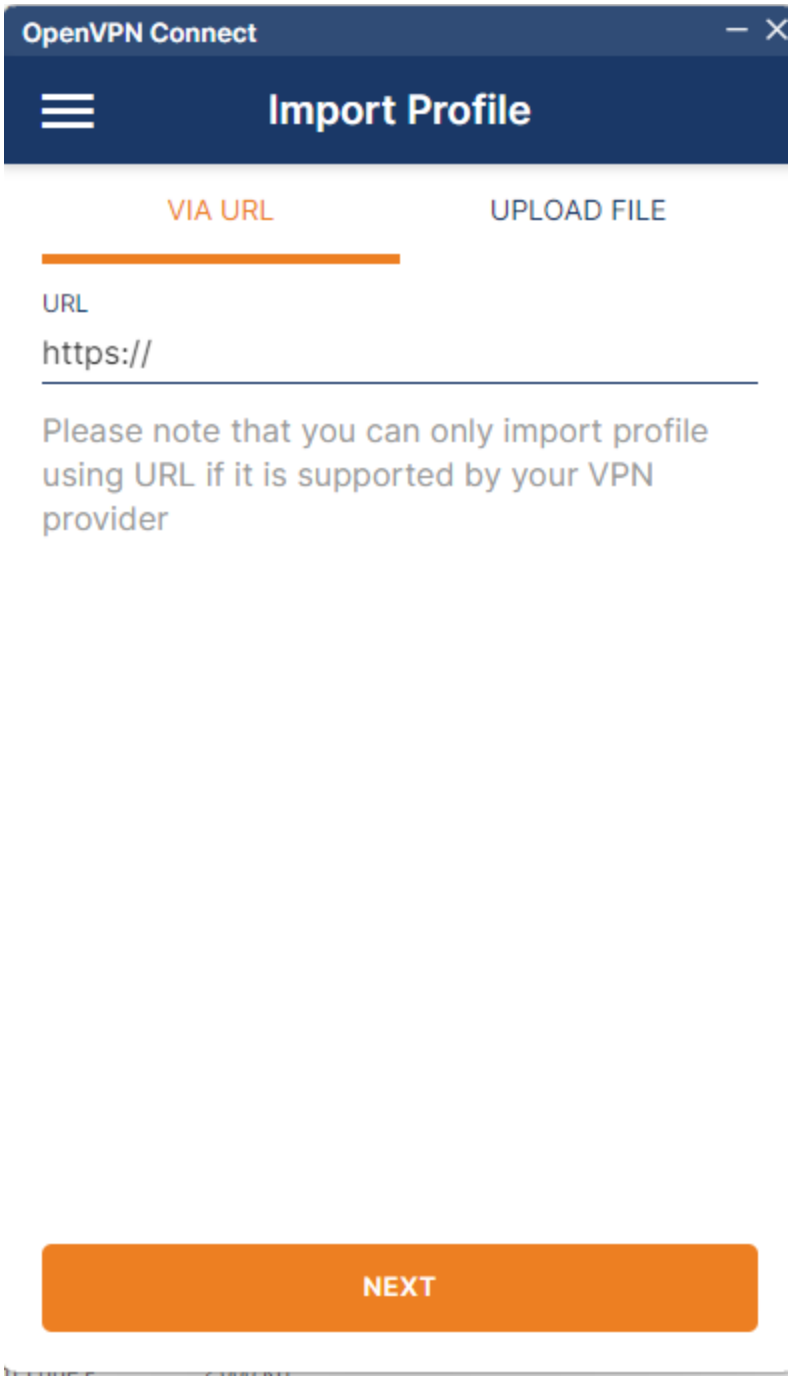

OpenVPN Connect Setup
Ready to install OpenVPN Connect
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

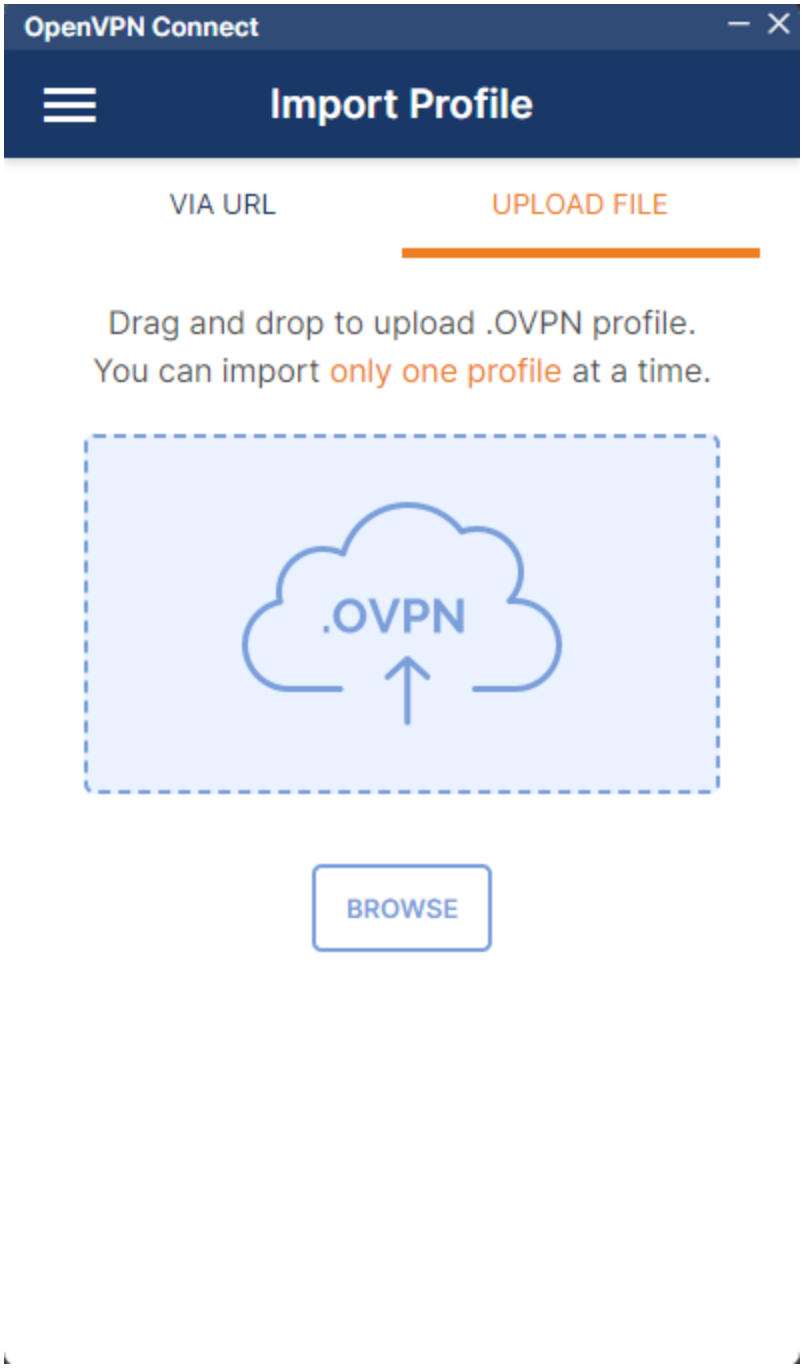

OpenVPN Connect Setup
Installing OpenVPN Connect
Please wait while the Setup Wizard installs OpenVPN Connect.
Status:
Back
Next
Cancel

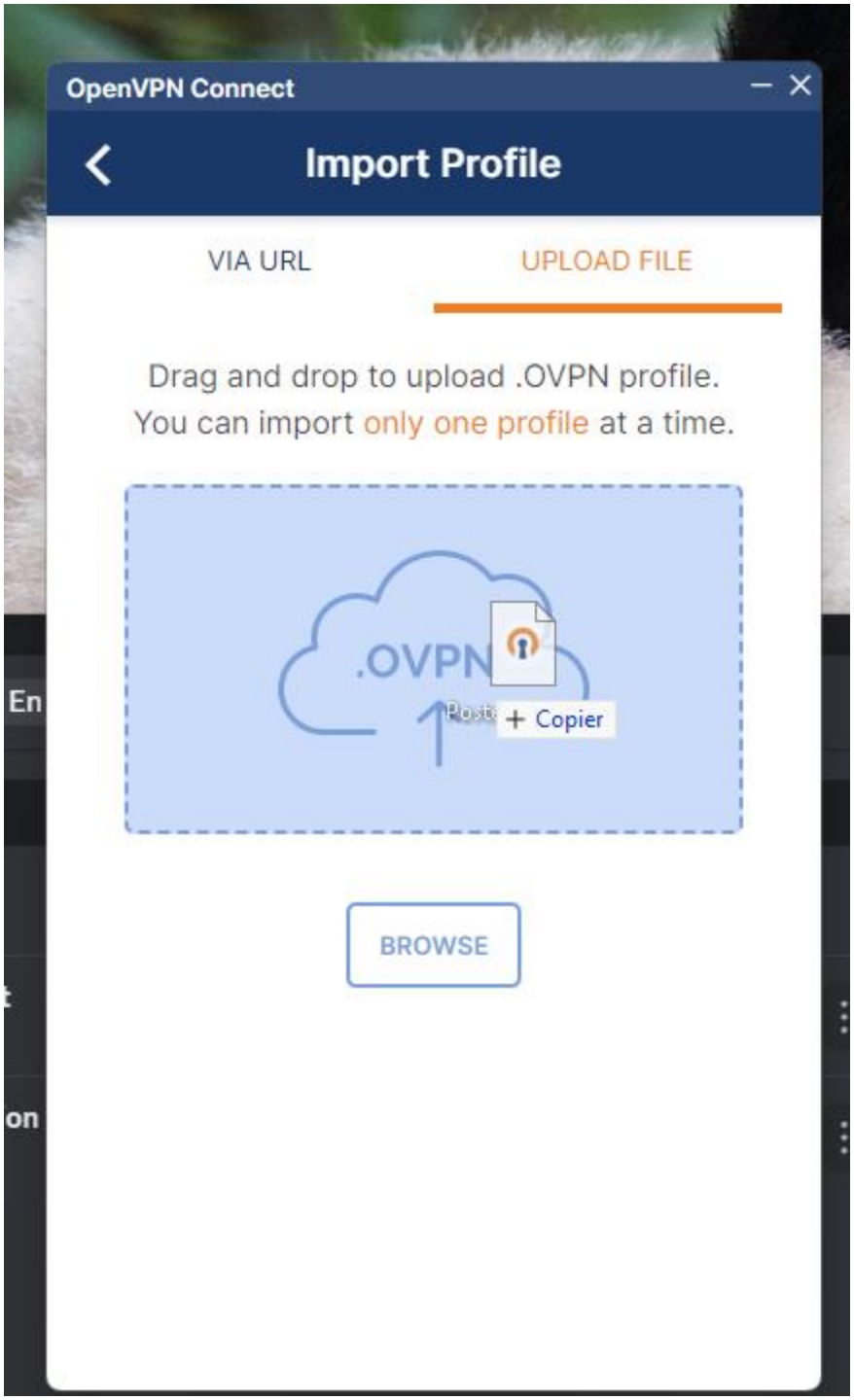

OpenVPN Connect Setup
Completed the OpenVPN Connect Setup Wizard
Click the Finish button to exit the Setup Wizard.
Back
Finish
Cancel

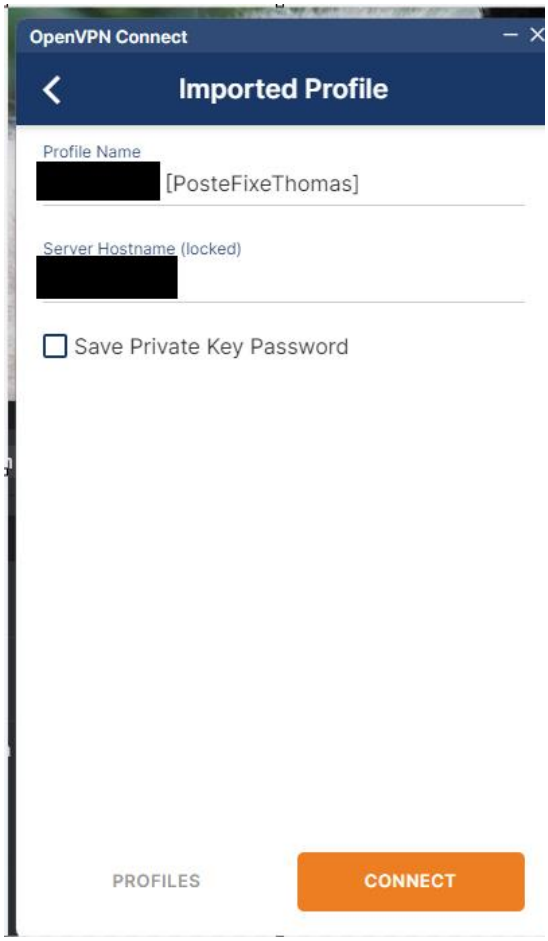

OpenVPN Connect
OpenVPN Inc. Data Collection, Use And Retention
OpenVPN Inc. presents our updated policies to transparently show how we collect, use, or retain your data. By clearly and openly presenting the terms of our policies we hope to maintain the trust and confidence of all our valued customers. Our priority is to educate and make it easy for customers to understand what data we collect, why we collect it, and how we use it.

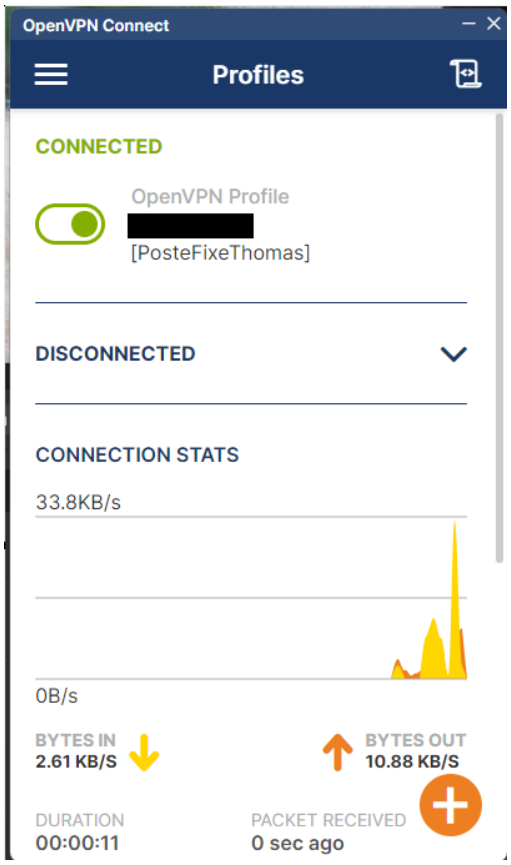
APP DATA USAGE
OpenVPN Connect is used to create VPN tunnels that connect to Access Servers, Community OpenVPN Servers, and any other third-party service that works with the OpenVPN protocol. OpenVPN Inc. does not have control over these servers, and the data policy of each of these servers are
AGREE


OpenVPN Connect
Import Profile
VIA URL
UPLOAD FILE
URL
https://
Please note that you can only import profile using URL if it is supported by your VPN provider
NEXT


OpenVPN Connect
Import Profile
VIA URL
UPLOAD FILE
Drag and drop to upload .OVPN profile.
You can import only one profile at a time.
.OVPN
BROWSE


OpenVPN Connect
Import Profile
VIA URL
UPLOAD FILE
Drag and drop to upload .OVPN profile.
You can import only one profile at a time.
.OVPN
+ Copier
BROWSE


OpenVPN Connect
Imported Profile
Profile Name
[PosteFixeThomas]
Server Hostname (locked)
Save Private Key Password
PROFILES
CONNECT



Installation Open connect sous linux (Raspberry OS)

Commande pour installer :

- Sudo apt install openvpn

```
DMZTM@raspberrypi:~ $ sudo apt install openvpn
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
```

Pour récupérer le fichier sur le serveur python

```
DMZTM@raspberrypi:~ $ wget http://192.168.0.17:8000/DMZTM.ovpn
```

wget http://192.168.0.17:8000/DMZTM.ovpn

```
DMZTM@raspberrypi:~ $ wget wget http://192.168.0.17:8000/DMZTM.ovpn
--2024-03-18 21:27:09--  http://wget/
Resolving wget (wget)... failed: Name or service not known.
wget: unable to resolve host address ‘wget’
--2024-03-18 21:27:09--  http://192.168.0.17:8000/DMZTM.ovpn
Connecting to 192.168.0.17:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2675 (2.6K) [application/octet-stream]
Saving to: ‘DMZTM.ovpn’

DMZTM.ovpn                   100%[=============================================>]   2.61K  --.-KB/s    in 0s

2024-03-18 21:27:09 (60.1 MB/s) - ‘DMZTM.ovpn’ saved [2675/2675]

FINISHED --2024-03-18 21:27:09--
Total wall clock time: 0.07s
Downloaded: 1 files, 2.6K in 0s (60.1 MB/s)
```

```
DMZTM@raspberrypi:~ $ sudo openvpn --config DMZTM.ovpn
2024-03-18 21:29:21 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing in --data-ciphers (AES-256-GCM:AES-128-
GCM:CHACHA20-POLY1305). OpenVPN ignores --cipher for cipher negotiations.
2024-03-18 21:29:21 Note: Kernel support for ovpn-dco missing, disabling data channel offload.
2024-03-18 21:29:21 OpenVPN 2.6.3 aarch64-unknown-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [A
EAD] [DCO]
2024-03-18 21:29:21 library versions: OpenSSL 3.0.11 19 Sep 2023, LZO 2.10
2024-03-18 21:29:21 DCO version: N/A
Enter Private Key Password: **************
```