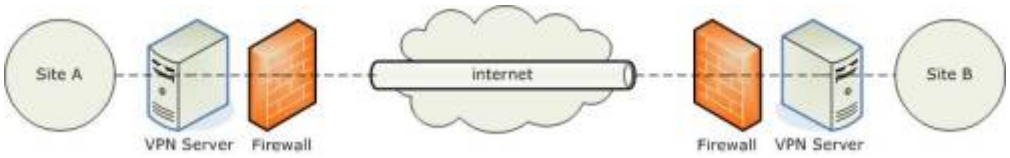
Principe du VPN

Selon Wikipedia : *En informatique, un réseau privé virtuel (Virtual Private Network en anglais, abrégé en VPN) est une abstraction permettant de considérer plusieurs ordinateurs distants comme étant sur le même réseau local.*

En pratique, on utilise un logiciel pour se connecter à un serveur et établir un tunnel chiffré évitant que les informations ne transitent en clair. La configuration réseau mise en place permet de faire croire à la machine distante qu'elle fait partie intégrante du réseau interne du laboratoire.



Afin de passer la plupart des pare-feu sortant, nous avons mis en place un serveur sur le port 443 (qui est le port https classique, donc autorisé par la majorité des sites).

Note

Tout le trafic est redirigé au travers du VPN. Nous vous rappelons que les règles de la charte informatique s'appliquent également lorsque vous êtes connecté en VPN.

Rappel: Il ne faut absolument pas connecter de **machines non mises à jour** sur le réseau du laboratoire. Nous demandons à tout le monde de bien vouloir contrôler que vos ordinateurs soient bien à jour. Il s'agit d'une **question de sécurité majeure**.

Le laboratoire propose un accès VPN délivré par le logiciel OpenVPN.

Fichier de configuration

Téléchargez le fichier de configuration :

vpn-ias.zip

La connexion au VPN nécessite un compte dans l'annuaire du laboratoire

Configuration

Windows

Installation

Depuis un terminal :

```
winget install OpenVPNTechnologies.OpenVPN --source winget
```

Avec l'installateur :

Télécharger depuis le site officiel : https://openvpn.net/community/

Configuration

Il est recommandé de placer les fichiers de configuration directement dans le répertoire d'installation de l'application (par défaut *C:\Program Files\OpenVPN\config*).
Une fois le fichier de configuration **client.ovpn** extrait dans un répertoire dont vous possédez les droits de modification (*Téléchargements* par exemple) déplacez le dans *C:\Program Files\OpenVPN*//config // (directement à ce niveau, pas dans un sous répertoire). Windows vous demandera d'utiliser vos droits administrateur pour effectuer cette copie : Cliquer sur continuer

Redémarrez l'application pour que la nouvelle configuration prenne effet

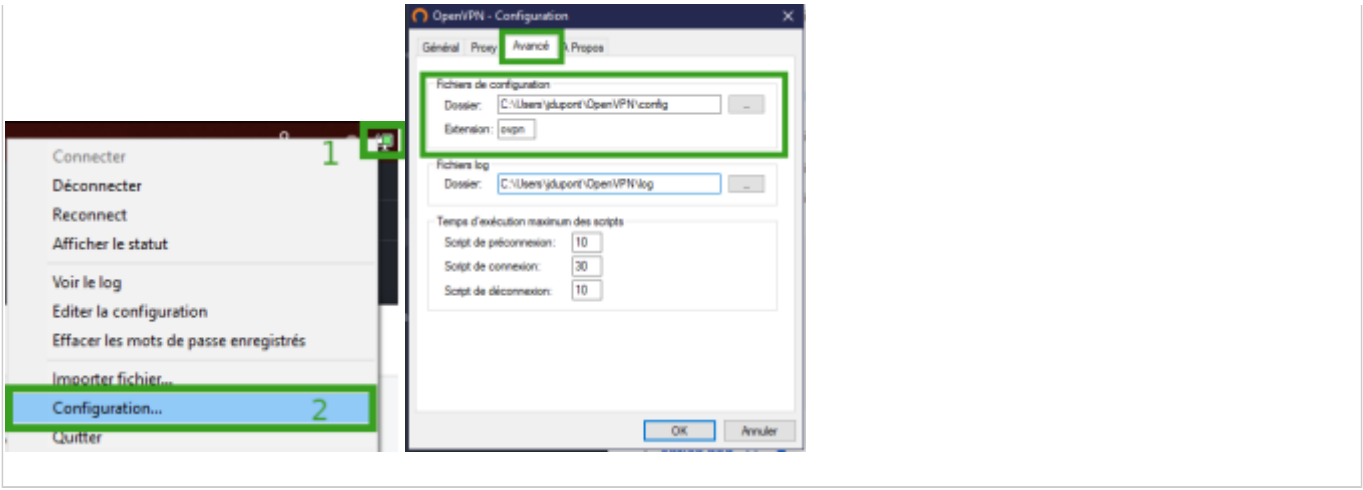
Dans le cas ou vous rencontrez ce problème:

```
Cannot pre-load tls-auth keyfile (ta.key)
Exiting due to fatal error
```

- Vous avez probablement mal déplacé le fichier de configurations
- Un dossier OpenVPN existe dans votre dossier utilisateur → ex: C:\Users\jdupont\OpenVPN.

Dans ce cas, quitter l'application OpenVPN puis supprimer le dossier OpenVPN présent dans votre dossier utilisateur. Assurez-vous que les fichiers de configurations soient bien situés dans le dossier C:\Program Files\OpenVPN\config\

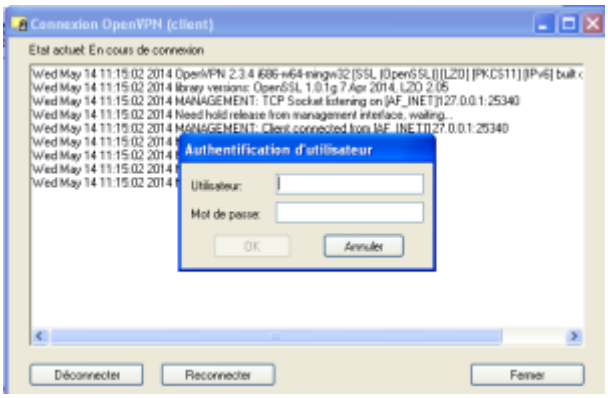
Vous pouvez également voir où sont situés vos fichiers de configurations en cliquant droit sur l'icône OpenVPN en bas à droite de votre écran.



Vous pouvez ensuite lancer OpenVPN, puis choisir de vous connecter.

Note : Il faut démarrer le logiciel avec des droits d'administrateur pour pouvoir modifier la configuration réseau (*clic droit, exécuter en tant qu'administrateur*). Note : il est possible de conserver la mémoire de cette exigence en utilisant le clic droit puis *résoudre les problèmes de compatibilité*, puis *Dépanner le programme*, puis *Le programme requiert des autorisations supplémentaires*.

Une fois le programme démarré, une icône grisée avec un cadenas ouvert apparait dans la zone d'icônes, il faut maintenant faire un clic droit sur cette icône puis "Connecter".
Une fenêtre apparaît vous demandant vos identifiants du laboratoire.



Linux (Debian / Ubuntu) GUI

Installation

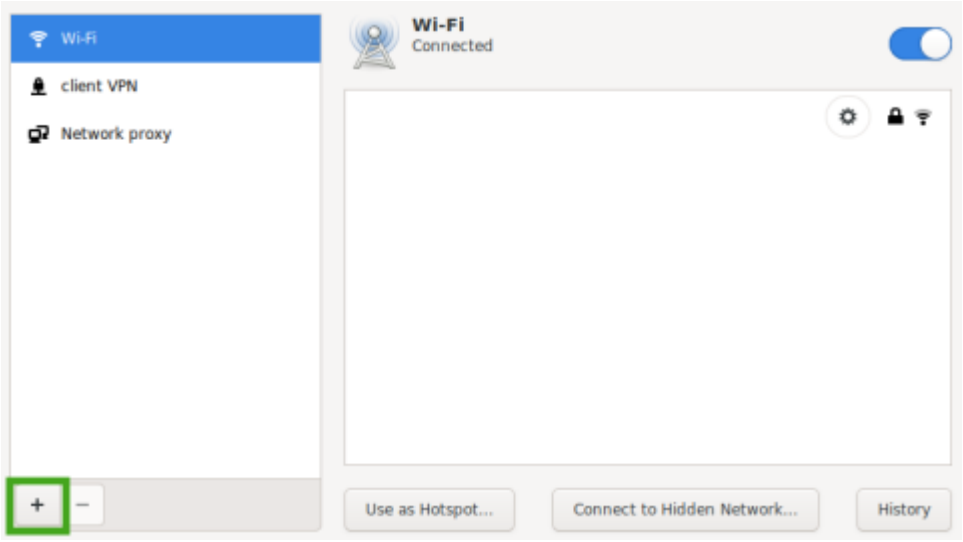
Installer l'intégration d'OpenVPN pour le network-manager (elle devrait être installée par défaut)

```
sudo apt install network-manager-openvpn network-manager-openvpn-gnome
```

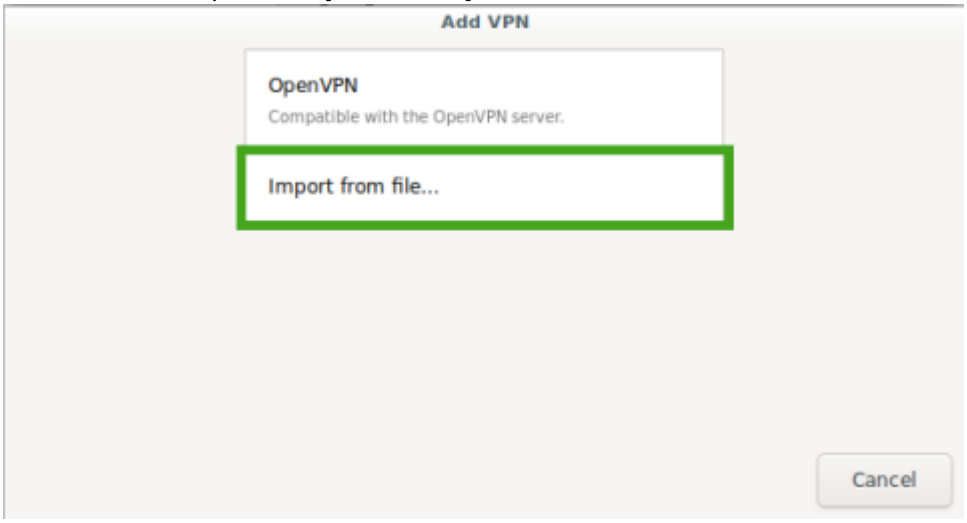
Configuration

Téléchargez et décompressez les fichiers de configuration

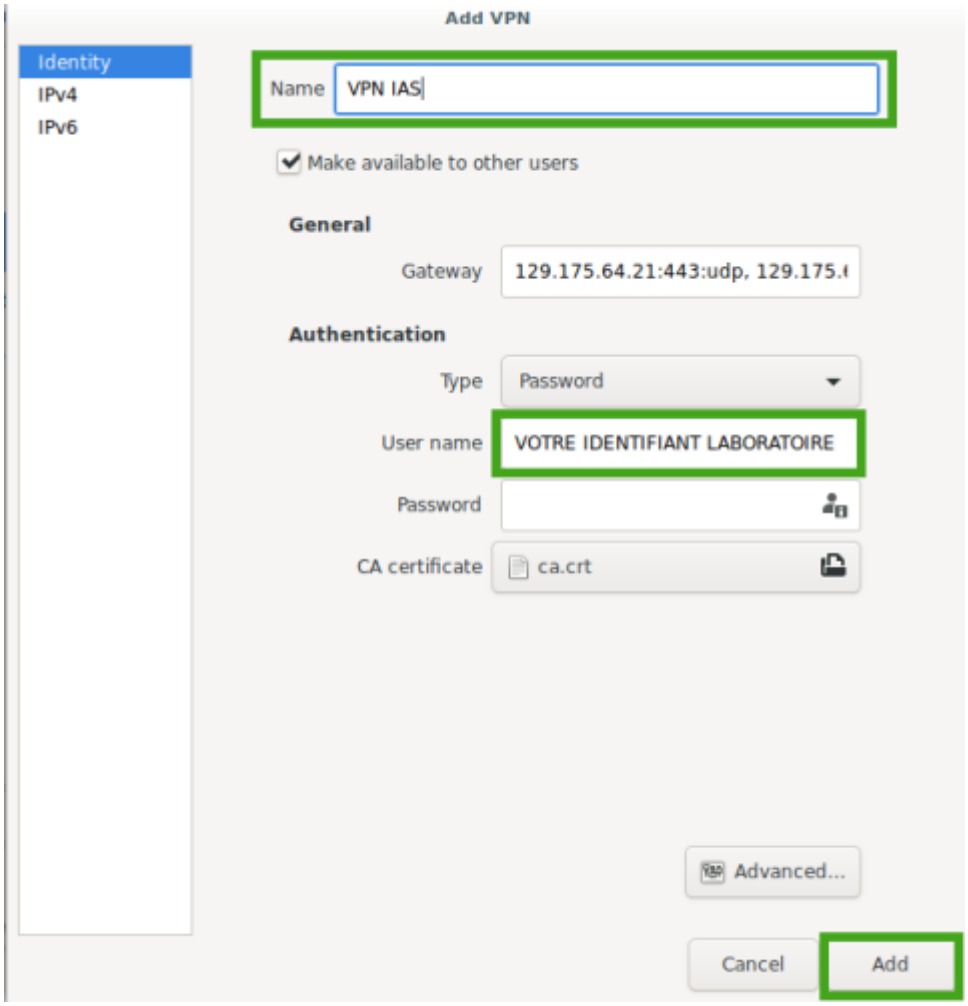
Cliquez maintenant sur votre icône réseau et ajoutez une nouvelle connexion.



Sélectionnez l'option **Importer depuis un fichier...**



Entrer les identifiants laboratoire



Vous pouvez désormais activer la connexion depuis votre gestionnaire réseau



Mac

Installation

Il est recommandé d'utiliser Homebrew pour l'installation sur Mac:

```
brew install --cask tunnelblick
```

Lorsque vous avez cette fenêtre :



Cliquez sur “J'ai déjà une configuration” ou “I have configuration files”

Configuration

Extraire le fichier *client.ovpn* des fichiers de configuration et double-cliquez dessus pour l'importer.

Vous pouvez activer la connexion VPN depuis l’icône Tunnelblick présente dans votre barre des taches.

---

iOS

Installer l'application OpenVPN Connect

Extraire le fichier client.ovpn de l'archive et le partager dans l'application OpenVPN Connect.

Attention

Sous certaines versions de Linux (par exemple Ubuntu), lors de l'installation du package, le daemon openvpn est activé automatiquement au démarrage du système. Sous Ubuntu/Debian, vous pouvez le désactiver avec la commande suivante (en sudo, ou en root directement) :

```
systemctl disable openvpn
```

Attention 2

Sous Ubuntu 16.04 (et peut-être d'autres versions), le service NetworkManager empêche la mise à jour de la configuration DNS à l'activation de OpenVPN. Pour remédier à cela, il faut procéder comme suit :

```
sudo service network-manager stop
sudo vi /etc/NetworkManager/NetworkManager.conf
```

Commenter la ligne :

```
#dns=dnsmasq
```

Sauvegarder le fichier, puis relancer le service :

```
sudo service network-manager start
```

From:
https://docinfo.ias.u-psud.fr/ - **Informations, recommandations et conseils du service informatique de l'IAS**

Permanent link:
https://docinfo.ias.u-psud.fr/doku.php/services_reseau:vpn?rev=1779953741

Last update: **2026/05/28 07:35**