



Documentation OpenVPN

INSTALLATION CLIENT

Sommaire

Notions	2
Qu'est-ce qu'un VPN ?	2
Avantage en entreprise :	2
Schéma de l'utilisation d'un VPN	3
Sans Vpn :	3
Avec vpn	3
OpenVPN.....	4
Comment fonctionne OpenVPN ?.....	4
Quels protocoles sont utilisés par OpenVPN ?	4
Quels ports Utilisé par OpenVPN ?	4
Utilisation Routeur Wifi	5
Pour utiliser le routeur wifi.....	5
Installation Windows.....	5
Téléchargement applicatif	5
Installation Logiciel.....	5
Phase de test	14
Annexe 1 : Fichier du client	20
Installation Linux	21
Phase de test	23
Annexe 2 : Transfert du fichier de configuration de votre clé USB à votre client. .	26
Installation Android / IOS	27
Annexe 3 : A quoi peut servir un VPN sur mobile	34

NOTIONS

Qu'est-ce qu'un VPN ?

Un VPN (de Virtual Private Network) est un réseau privé qui est envoyé depuis un serveur sur un client en passant par un tunnel de chiffrement (dans la plupart des cas en SHA-256) ce qui permet de sécuriser le réseau pour qu'il ne soit pas visible par l'extérieur et qu'il ne soit pas possiblement « piratable » (ou du moins écoutable depuis le réseau extérieur sans la clé de chiffrement valide).

On dit virtuel car le réseau n'existe pas vraiment sur la machine (du moins physiquement) car seul le réseau « externe » (internet) passe réellement dans l'interface du client.

On utilise un principe de TUN et TAP, TUN permet de créer une carte réseau (en l'émulant) pour que celle-ci se connecte sur le TAP. Un principe de client/serveur.

Avantage en entreprise :

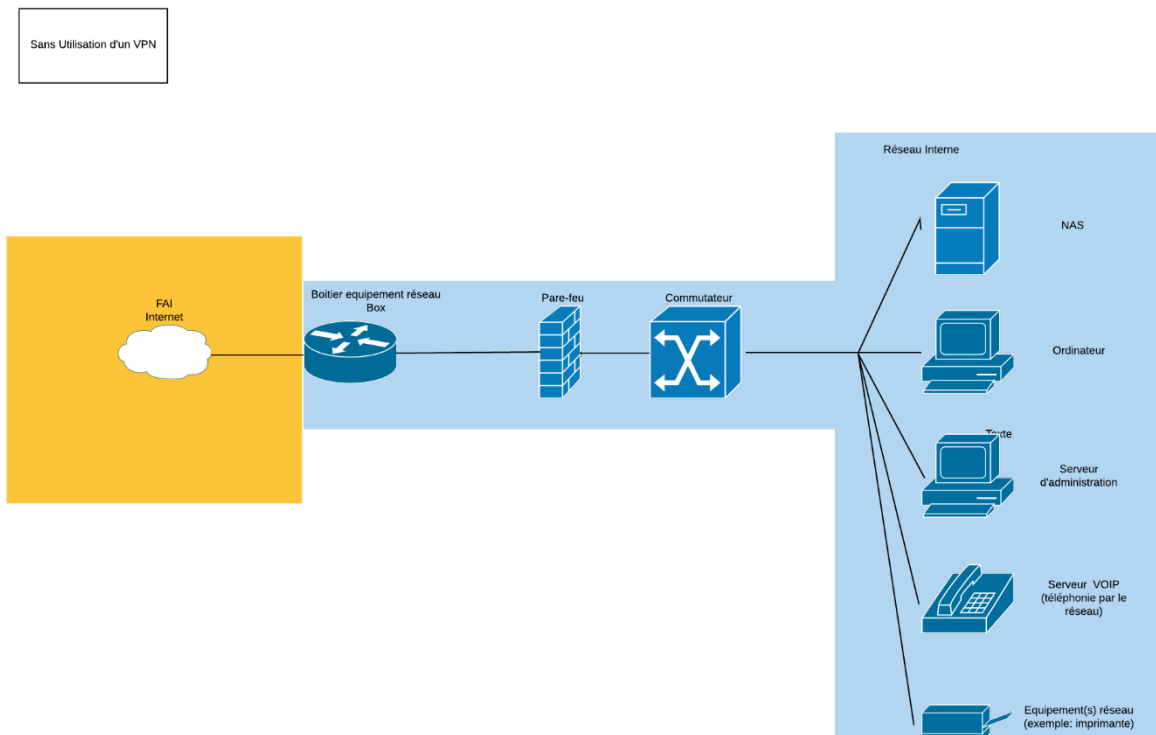
Si une entreprise a des employés qui se déplacent souvent ou alors qu'elle a plusieurs locaux géographiquement séparés (par la distance), elle peut quand même faire bénéficier des ressources de son réseau et donc ne pas faire souffrir les différents services qui peuvent la composer (Les ressources peuvent être multiples, par exemple une imprimante, un NAS, etc...).

Un VPN d'entreprise ne journalise (ce n'est pas son

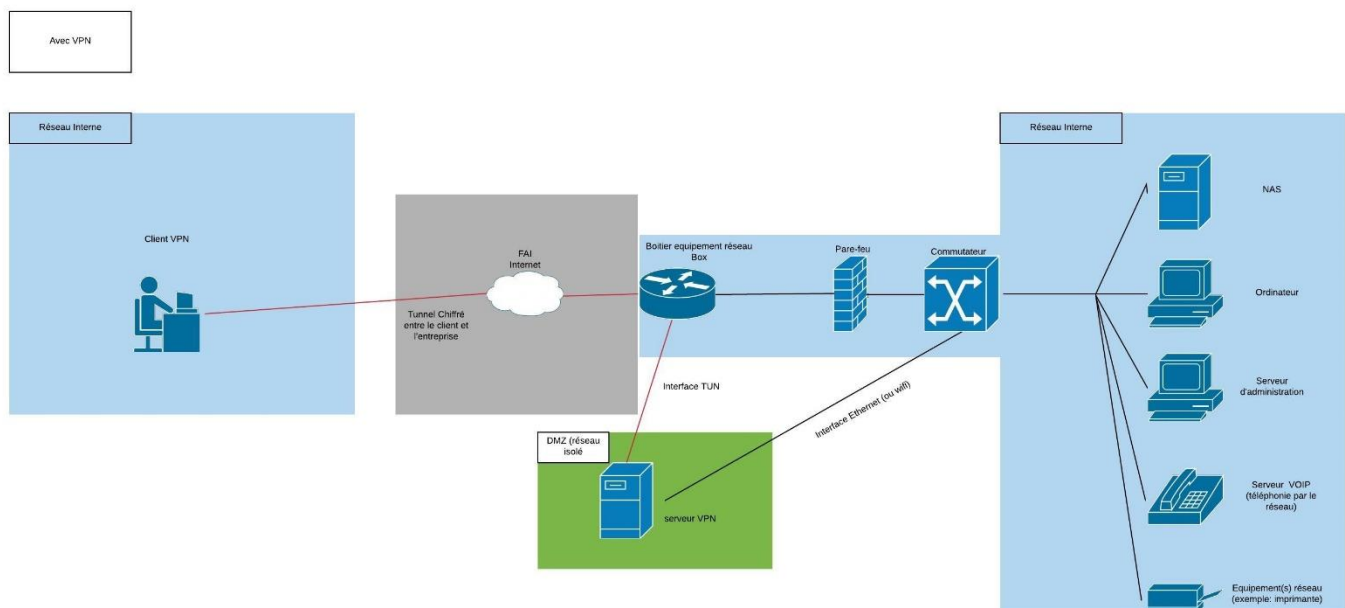
Par contre le VPN ne rend pas anonyme la personne sur internet (bien au contraire).

SCHEMA DE L'UTILISATION D'UN VPN

Sans Vpn :



Avec vpn



OPENVPN

Comment fonctionne OpenVPN ?

Open VPN est une application informatique ouverte pour la mise en place de techniques de réseaux privés virtuels avec des connexions sécurisées point-par-point ou site-par-site, pour des configurations via routage ou pont, ainsi que pour les accès à distance.

Il a été défini par James Yonan et est publié sous licence publique GNU en tant que GPL (en anglais : General Public License).

Il exploite un protocole de sécurité sur mesure qui utilise SSL/TLS pour les échanges de clés. Il est capable de traverser des transpondeurs de réseaux d'adresses (en anglais NAT : Network Address Translators) et des pare-feux.

Quels protocoles sont utilisés par OpenVPN ?

Un protocole Open VPN permet à des homologues de s'authentifier mutuellement en utilisant une clé secrète pré-partagée. Lorsqu'il est utilisé dans une configuration multi client-serveur, il permet au serveur de libérer un certificat d'authentification pour chaque client, en utilisant la signature et l'autorité de certification. Ce système utilise en grande partie la base de cryptage OpenSSL, ainsi que le protocole SSLv3/TLSv1.

Le but de SSL et d'IPSEC est le même : créer des VPNs et ainsi chiffrer le trafic entre deux équipements avec les mêmes algorithmes.

Bien sûr, IPSec et SSL ne sont pas compatibles.

IPSEC	SSL	
RFC:	2401	4346 (TLS 1.1)
Couche OSI:	Couche Réseau	Entre les couches réseau et application
Installation:	Non-propriétaire	Propriétaire
Configuration:	Complexe	Simple
NAT:	Problématique	Pas de problème
Pare-feu:	Moins amical	Amical

Quels ports Utilisé par OpenVPN ?

OpenVPN utilise par défaut le port 1194 mais dans l'entreprise nous utiliserons le port 6542 pour ne pas avoir de problème de sécurité (en cas de scan des ports, le port associé ne sera pas associé directement à une application ou serveur Vpn qui pourrait créer une backdoor dans le réseau de l'entreprise).

UTILISATION ROUTEUR WIFI

Pour utiliser le routeur wifi

Connexion image

Cherchez votre wifi dans votre système d'exploitation,

Cliquez ici pour vous connecter une fois la connexion effectuée, le point d'accès vous demandera un mot de passe, entrez ici ce mot de passe :

I20tRIklyu9iYE9GGISLCKmWCgjE

Attendez un peu et vous serez connecté.

Pour se connecter avec Windows Openvpn a créer deux logiciel (qui ont la même utilisation) : OpenVPN GUI et OpenVPN connect

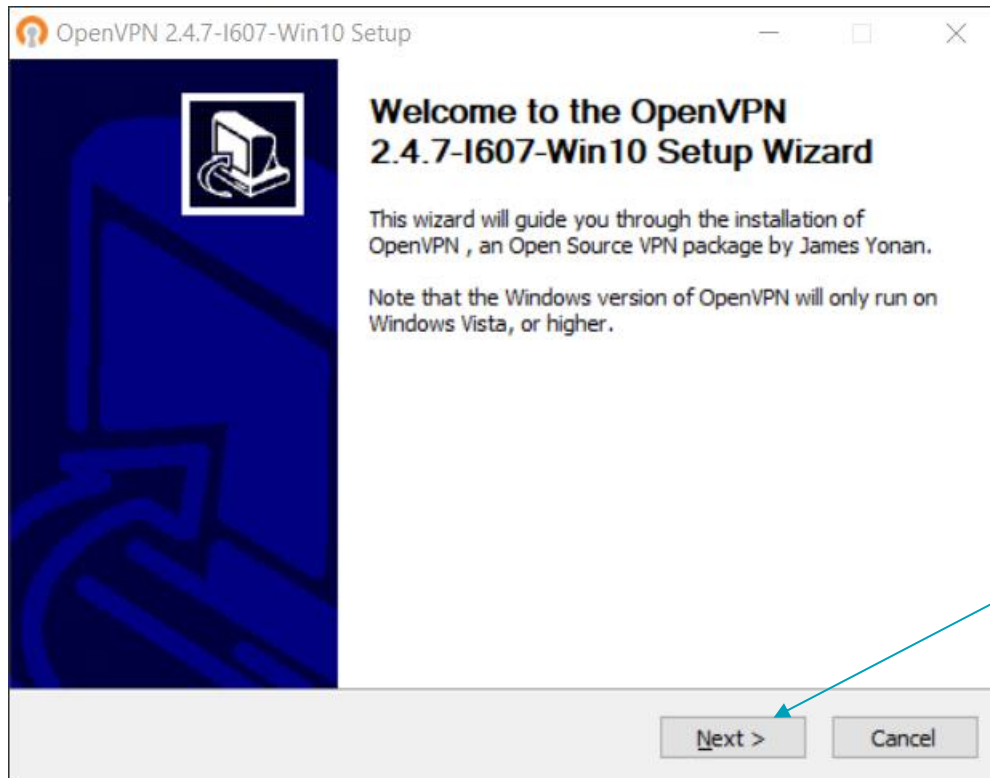
Les deux logiciels ont les mêmes propriétés au niveau applicatif (dans une utilisation sur un seul serveur sinon pour la connexion à plusieurs serveurs VPN en même temps choisissez OpenVPN GUI) donc choisissez celui que vous souhaitez :

- OpenVPN GUI (lien de téléchargement direct : [Windows 10](#), [Windows 7 et moins](#))
- OpenVPN connect (lien de téléchargement direct : [Tout types](#))

[Lien de la page en cas de problème sur les liens](#)

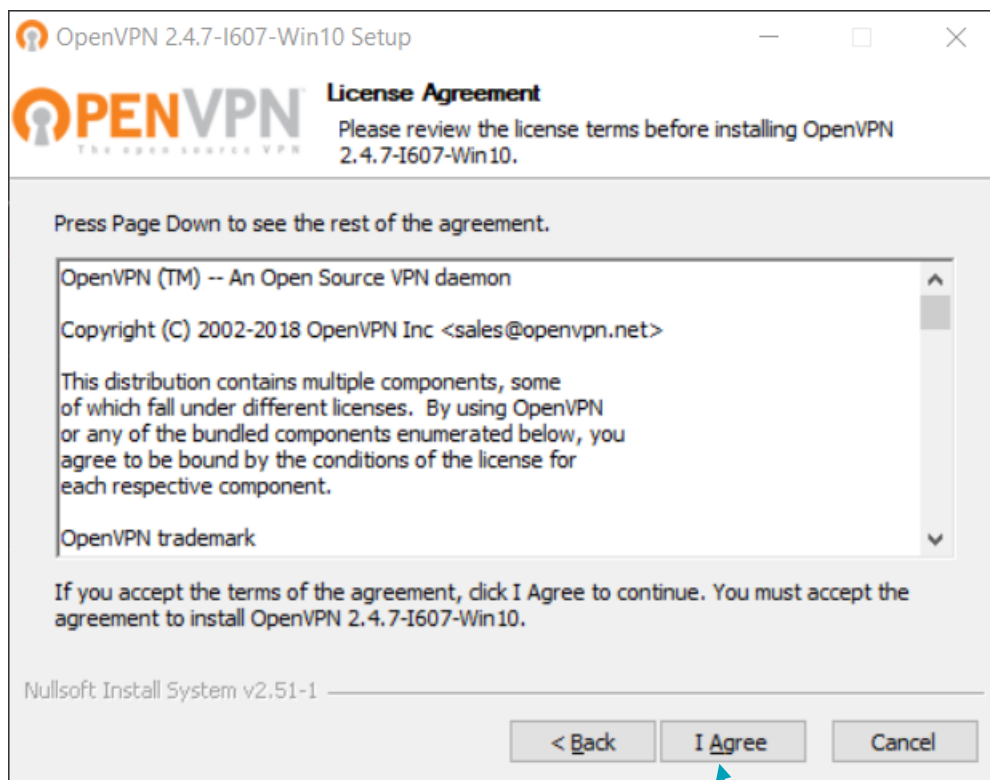
Installation Logiciel

L'installation commencera comme ceci après avoir exécuter l'application que vous aurez téléchargé.



Cliquez sur « Next »
(Suivant)

Comme toute application, Openvpn a des licences et **vous devez les lire** avant l'utilisation du logiciel.



Après lecture de la License.

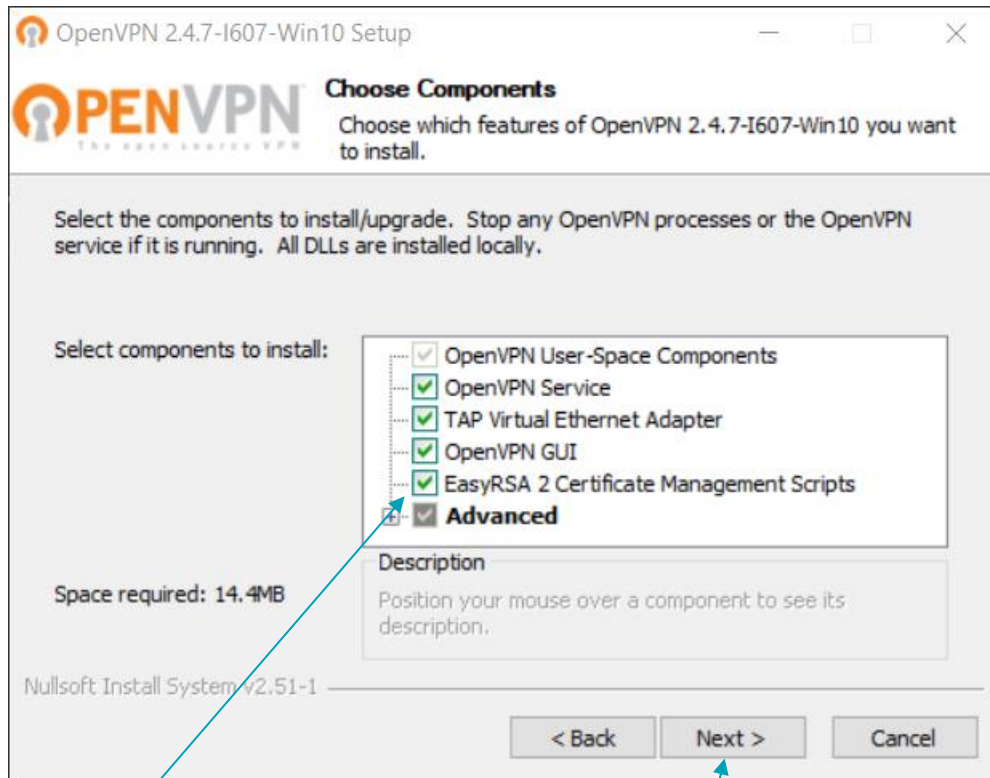
Cliquez sur « I Agree »

(Qui signifie que vous acceptez les conditions d'utilisations)

Une fois cela fait, vous devez choisir les composants qu'installera l'exécutable :

- **OpenVPN Service** : permet le démarrage de openVPN comme un service.
- **Tape Virtual Ethernet adapter** : permet la création d'une création réseau (émulé).
- **OpenVPN GUI** : la commande visuelle qui vous permettra de le configurer par interface graphique.
- **EasyRSA 2 certificate Management Scripts** : Permet la gestion des certificats créer par notre serveur OpenVPN.

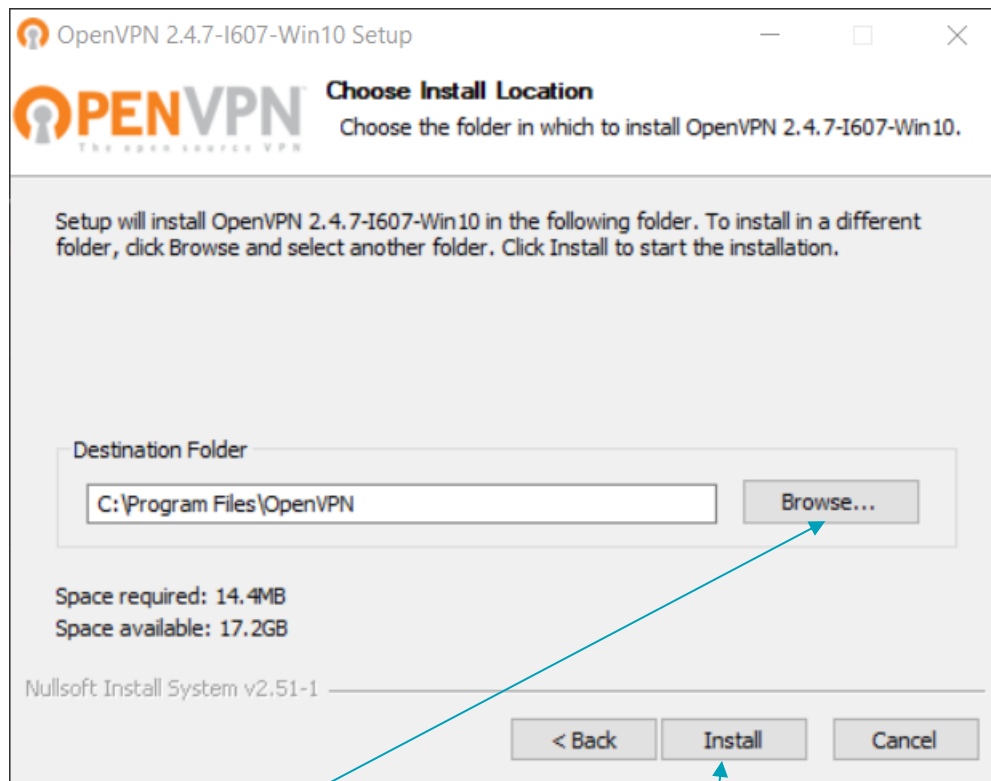
Tous ces composants sont importants à l'installation



Cliquez ici pour que les certificats soit pris en compte plus facilement par le fichier de configuration (.ovpn)

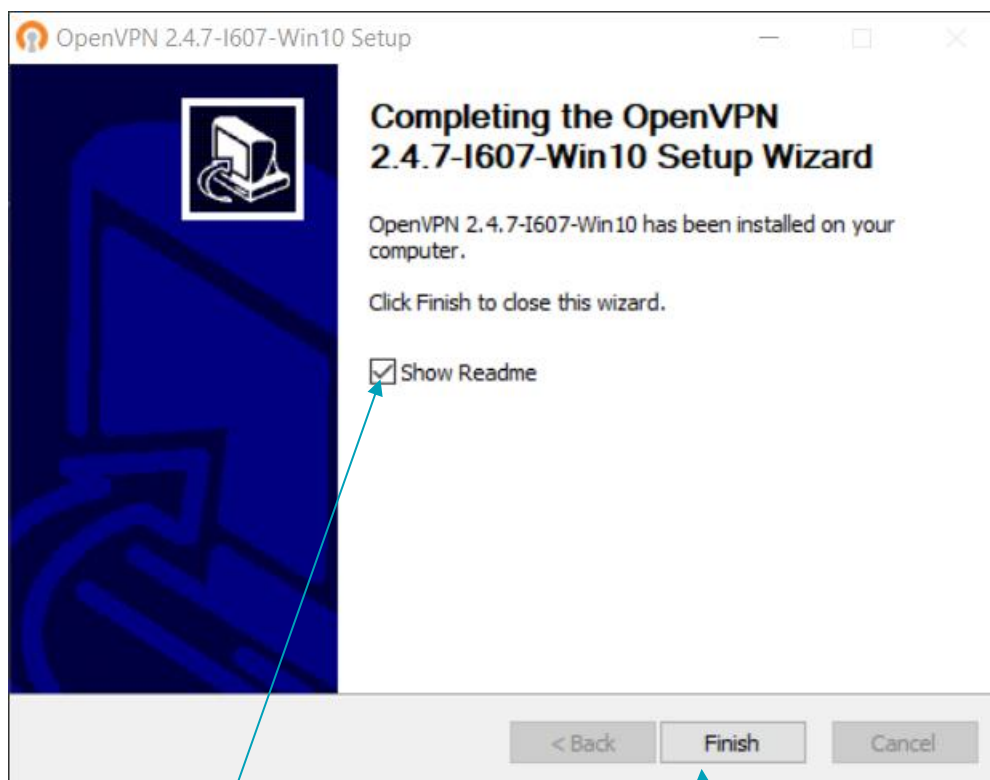
Cliquez sur « Next »
(Suivant)

L'exécutable va maintenant demander votre chemin.



Cliquez sur « *browse* » pour changer le fichier où se situera l'application et ses fichiers.

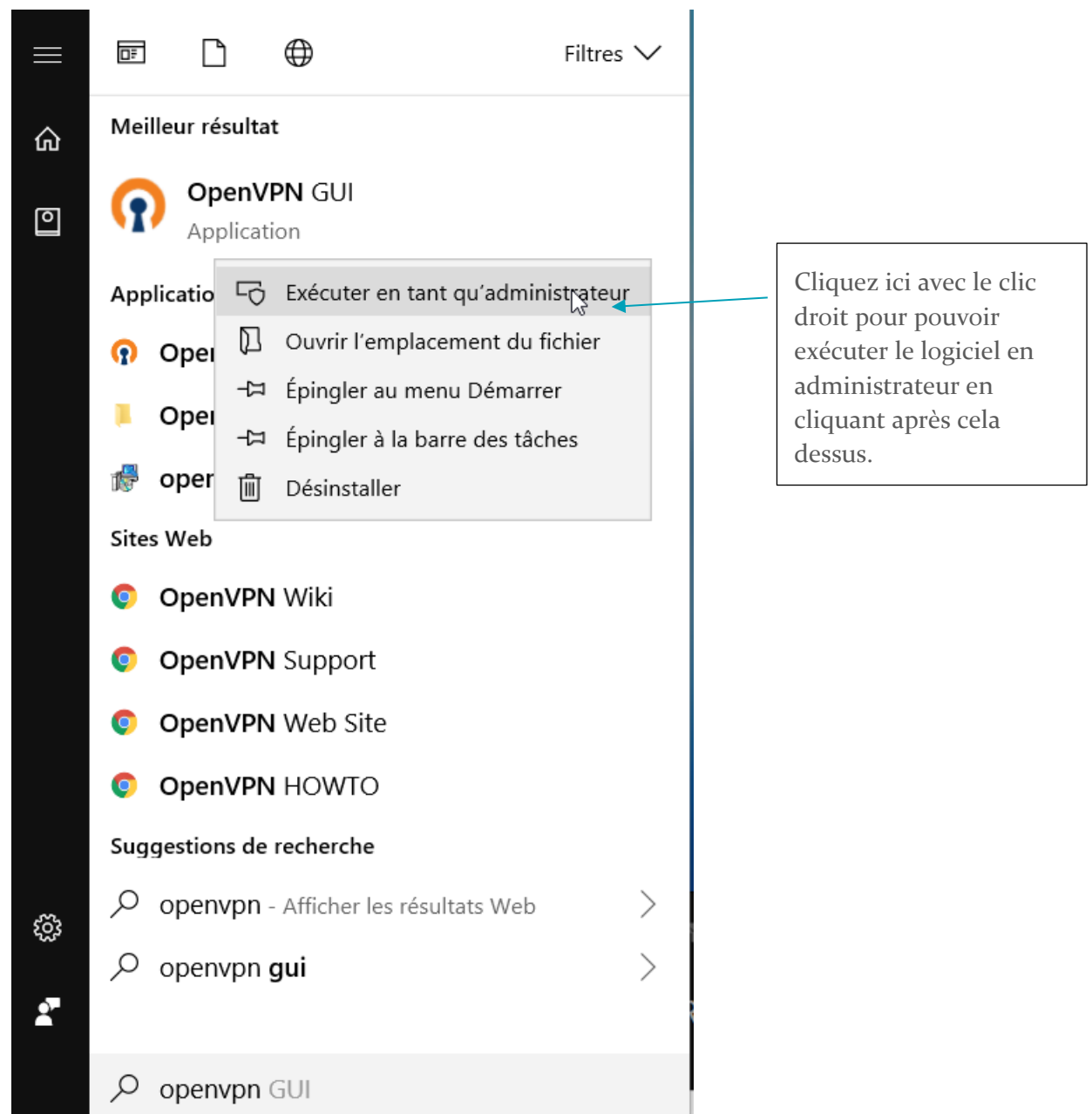
Cliquez sur « *install* » pour que l'installation commence



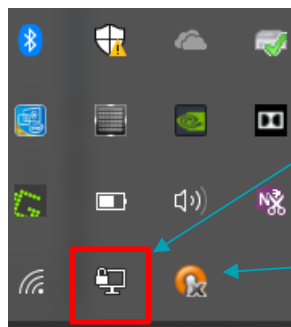
Cliquez ici pour ne pas avoir à lire le fichier contenant les informations de OpenVPN

Cliquez sur « *Finish* » pour finir l'installation

Il faut maintenant ouvrir le logiciel pour l'utiliser.



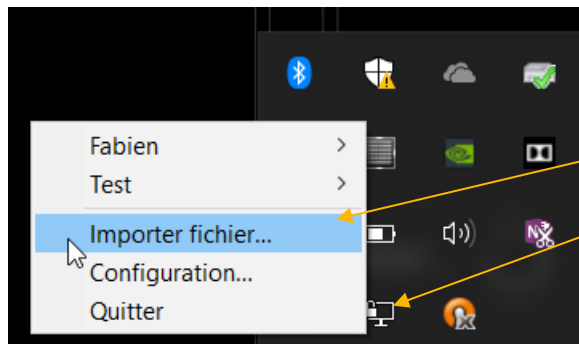
Le logiciel est lancé et on peut le voir depuis la barre des icones cachées.



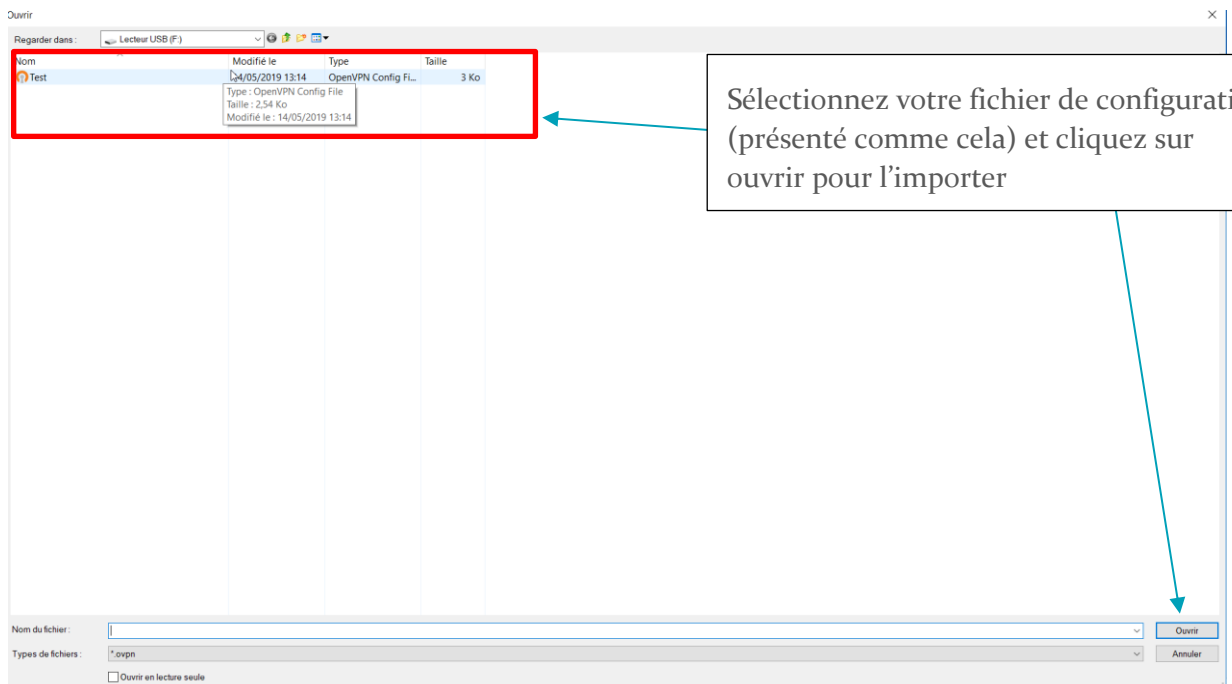
OpenVPN GUI est affiché (si c'est celui que vous avez

OpenVPN connect est affiché (si c'est celui que vous avez téléchargé)

Il faut maintenant importer le fichier de configuration ovpn.



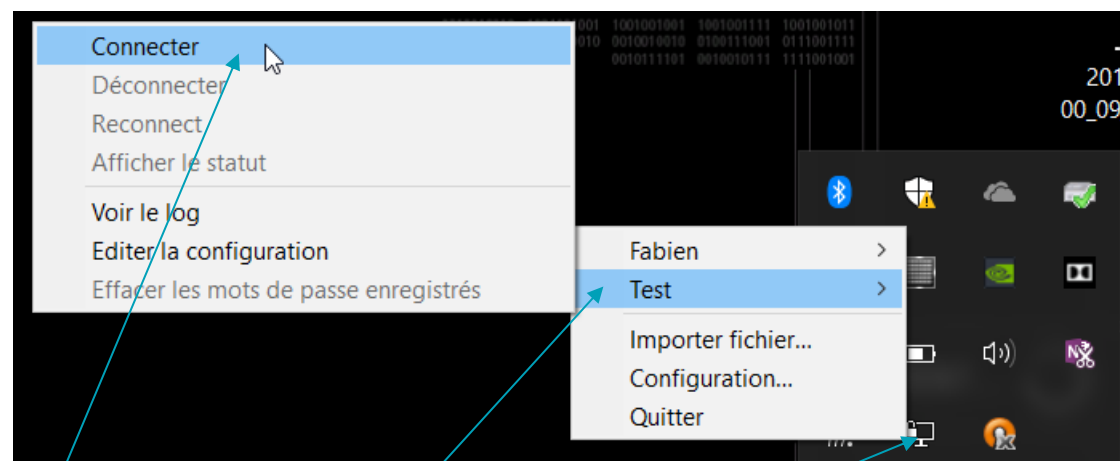
Cliquez avec le clic droit sur l'icône de l'application et cliquez avec le clic gauche sur « importer fichier »



Sélectionnez votre fichier de configuration (présenté comme cela) et cliquez sur ouvrir pour l'importer

Une fois l'importation faite, nous allons pouvoir nous connecter via le fichier de configuration que nous avons transmis au logiciel

Ce fichier de configuration contient les logins du client, le mot de passe du client, le certificat donné par le serveur ainsi que la clé de chiffrement pour pouvoir déchiffrer les informations du serveur.



Cliquez avec le clic droit sur l'icône de l'application. Après cela passez votre souris sur l'utilisateur et cliquez sur « connecter » pour vous connectez.



Et voilà vous êtes connecté au VPN (sinon contacter l'administrateur pour voir le problème que vous pouvez avoir).

Phase de test

On peut voir que l'interface que l'interface est connectée avec l'adresse IP du VPN (10.8.0.0/24 est l'adresse réseau par défaut de OpenVPN).



```
Carte Ethernet Ethernet 3 :
  Suffixe DNS propre à la connexion. . . :
  Description. . . . . : TAP-Windows Adapter V9
  Adresse physique . . . . . : 00-FF-CD-61-24-91
  DHCP activé. . . . . : Oui
  Configuration automatique activée. . . : Oui
  Adresse IPv6 de liaison locale. . . . : fe80::28c2:c0b5:9ffc:a2d2%18(préféré)
  Adresse IPv4. . . . . : 10.8.0.2(préféré)
  Masque de sous-réseau. . . . . : 255.255.255.0
  Bail obtenu. . . . . : jeudi 16 mai 2019 11:42:31
  Bail expirant. . . . . : vendredi 15 mai 2020 11:42:30
  Passerelle par défaut. . . . . :
  Serveur DHCP . . . . . : 10.8.0.254
  IAID DHCPv6 . . . . . : 83951565
  DUID de client DHCPv6. . . . . : 00-01-00-01-23-FC-93-34-98-28-A6-0A-F5-B9
  Serveurs DNS. . . . . : 8.8.8.8
                        8.8.4.4
  NetBIOS sur Tcpip. . . . . : Activé
```

Via cette capture on effectue le test d'avant le VPN et après, à ce moment on cherche à contacter la passerelle de notre point d'accès wifi.

```
C:\Users\Ark>ping 192.168.10.254

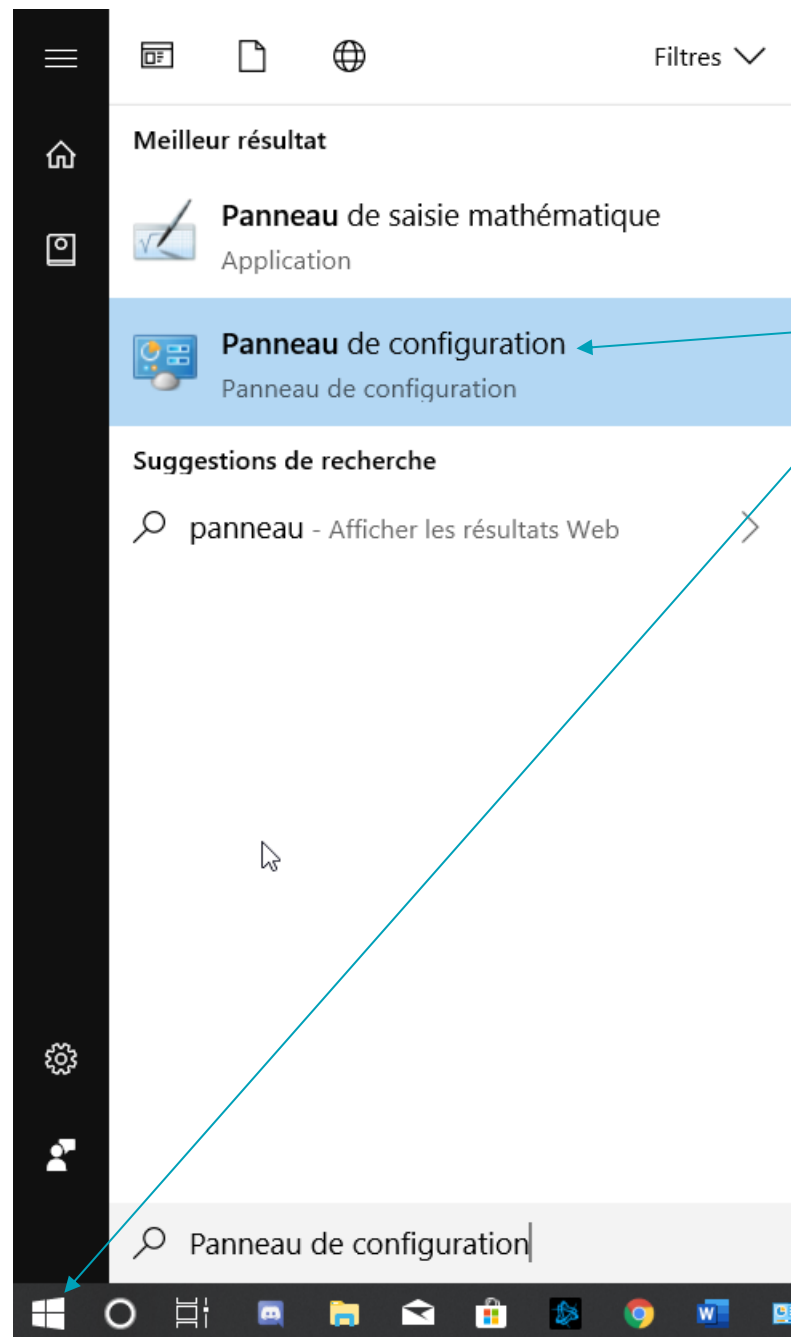
Envoi d'une requête 'Ping' 192.168.10.254 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.10.254:
    Paquets : envoyés = 2, reçus = 0, perdus = 2 (perte 100%),
Ctrl+C
^C
C:\Users\Ark>ping 192.168.10.254

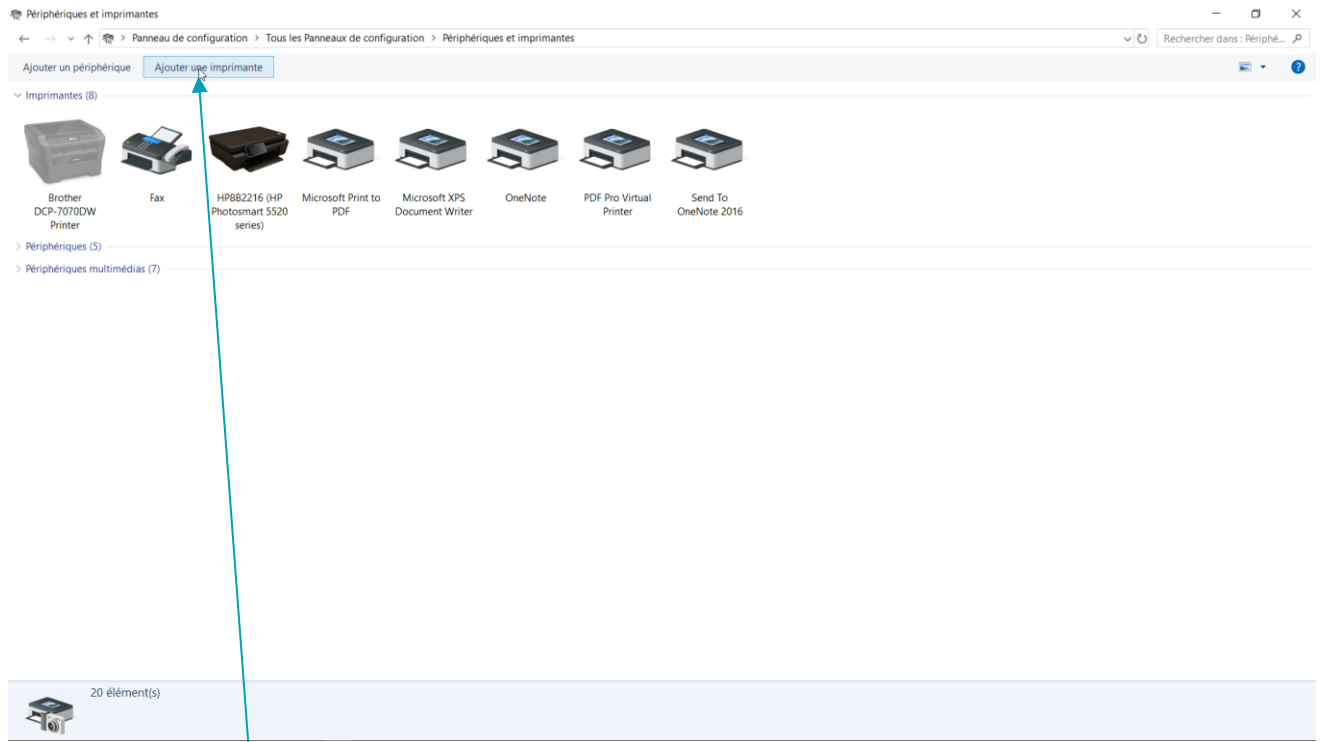
Envoi d'une requête 'Ping' 192.168.10.254 avec 32 octets de données :
Réponse de 192.168.10.254 : octets=32 temps=97 ms TTL=63
Réponse de 192.168.10.254 : octets=32 temps=91 ms TTL=63
Réponse de 192.168.10.254 : octets=32 temps=72 ms TTL=63

Statistiques Ping pour 192.168.10.254:
    Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 72ms, Maximum = 97ms, Moyenne = 86ms
Ctrl+C
^C
C:\Users\Ark>
```

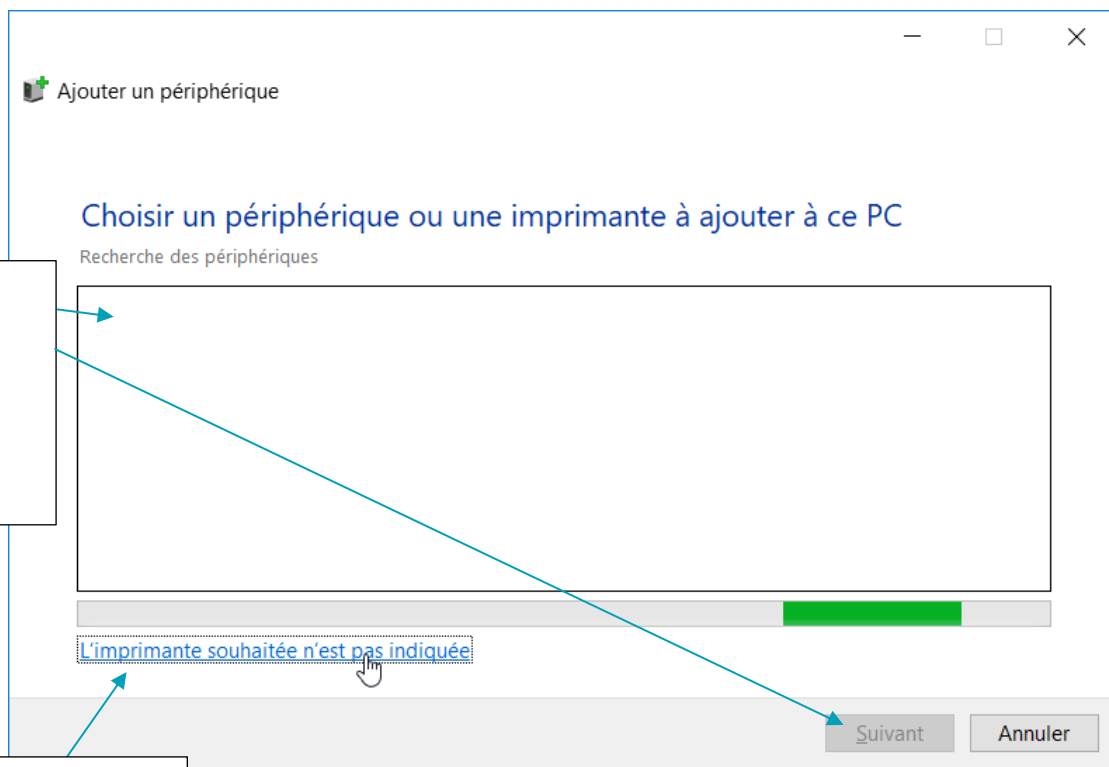
On va donc maintenant essayer de rajouter un équipement telle qu'une imprimante, pour cela il faudra se rendre dans le panneau de configuration.



Faite une recherche du « *panneau de configuration* » dans votre démarrage et après cela cliquer sur l'icone du panneau de configuration.



Cliquez sur « *ajouter une imprimante* »




Si votre imprimante s'affiche cliquez dessus et après cliquez sur « *suivant* »

Sinon cliquez sur « *l'imprimante souhaitée n'est pas indiquée* »

Dans mon exemple l'imprimante ne s'affiche pas donc il faut aller la chercher via son adresse IP.



←  Ajouter une imprimante

Rechercher une imprimante par d'autres options

☐ M'aider à trouver mon imprimante un peu plus ancienne

☐ Sélectionner une imprimante partagée par nom

Parcourir...

Exemple : \\ordinateur\imprimante ou
http://ordinateur/printers/imprimante/.printer

☒ Ajouter une imprimante à l'aide d'une adresse TCP/IP ou d'un nom d'hôte


☐ Ajouter une imprimante Bluetooth, sans fil ou réseau détectable

☐ Ajouter une imprimante locale ou réseau avec des paramètres manuels

Suivant

Annuler

Cliquez sur « ajouter une imprimante à l'aide d'une adresse TCP/IP ou d'un nom d'hôte ».

←  Ajouter une imprimante

Entrer un nom d'hôte ou une adresse IP d'imprimante

Type de périphérique : Détection automatique ▾

Nom d'hôte ou adresse IP :

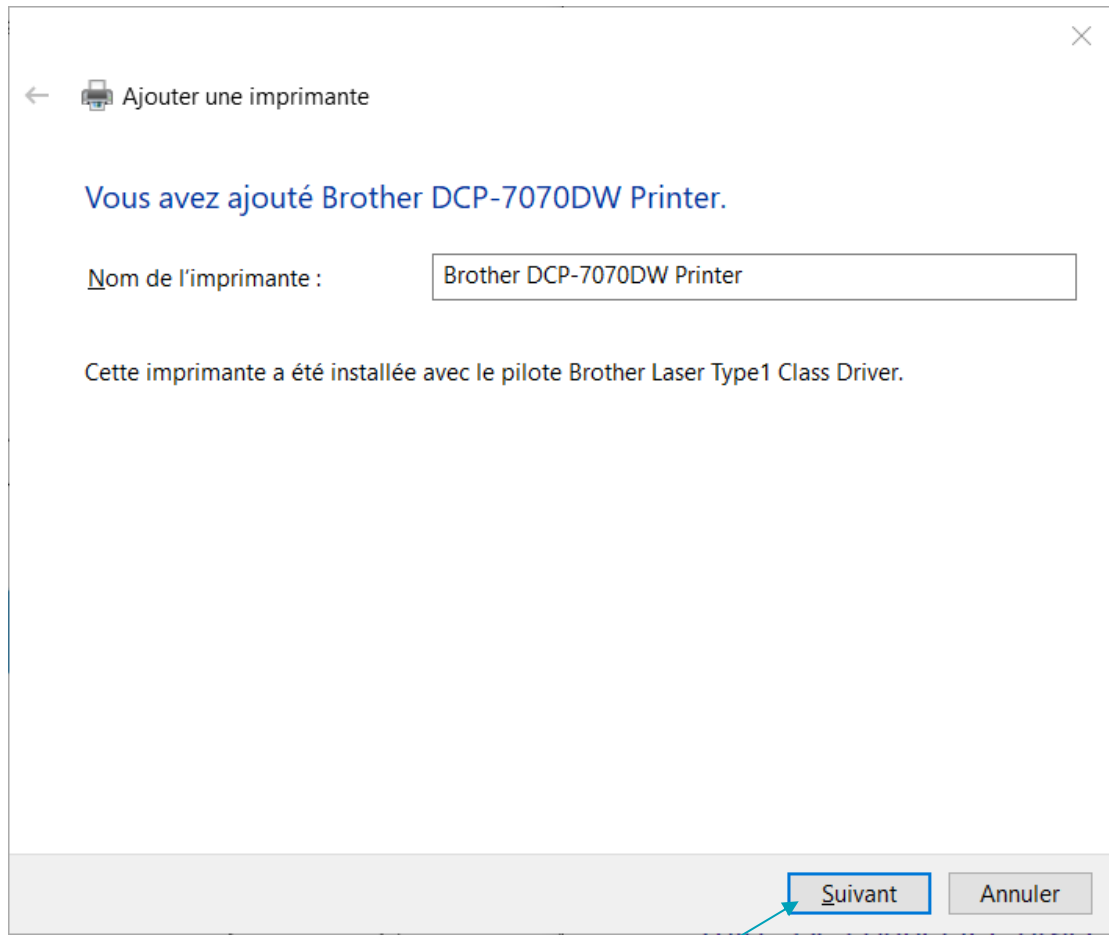
Nom du port :

☒ Interroger l'imprimante et sélectionner automatiquement le pilote à utiliser

Suivant Annuler

Entrez l'IP de l'imprimante (dans mon cas 192.168.1.13) et cliquez sur suivant pour la rajouter.

Cela peut prendre un peu de temps, mais vous aurez quoi qu'il arrive une réponse soit positive soit négative (si l'équipement n'est pas détecté).



Cliquez sur « *suivant* » pour valider et votre imprimante sera disponible dans la gestion des imprimantes.

On a donc l'imprimante qui est pris en compte et on peut donc maintenant l'utiliser à travers le VPN.

Annexe 1 : Fichier du client

Une fois que vous avez importé le fichier de configuration donné par le serveur il se situera ici (mais pas en la forme du fichier de configuration avec l'extension en. ovpn).

Ce PC > Disque local (C:) > Program Files (x86) > OpenVPN Technologies > OpenVPN Client > etc >

Nom	Modifié le	Type	Taille
log	15/05/2019 20:41	Dossier de fichiers	
profile	15/05/2019 20:41	Dossier de fichiers	
scripts	15/05/2019 20:41	Dossier de fichiers	
tmp	15/05/2019 20:41	Dossier de fichiers	
update	15/05/2019 20:41	Dossier de fichiers	
users	15/05/2019 20:41	Dossier de fichiers	
as.conf	26/02/2019 06:46	Fichier CONF	2 Ko
ca	15/05/2019 20:41	Certificat de sécuri...	1 Ko
local-sites.json	15/05/2019 20:41	Fichier JSON	4 Ko
openvpn	26/02/2019 06:46	Certificat de sécuri...	3 Ko
settings.json	15/05/2019 20:41	Fichier JSON	1 Ko
update-ca	26/02/2019 06:46	Certificat de sécuri...	1 Ko

INSTALLATION LINUX

Sur une machine avec un système d'exploitation qui est sur le noyau de linux, on devra télécharger le package de OpenVPN pour pouvoir se connecter au VPN.

On utilisera donc la commande :

Cette commande permet de se connecter en administrateur (mode « root »)

```
sudo su
```

Cette commande permet de faire toutes les mises à jour avant de prendre un package qui pourrait ne pas comprendre le logiciel (n'étant pas à jour).

```
apt-get update
```

Cette commande va chercher le package openvpn et l'installe après cela.

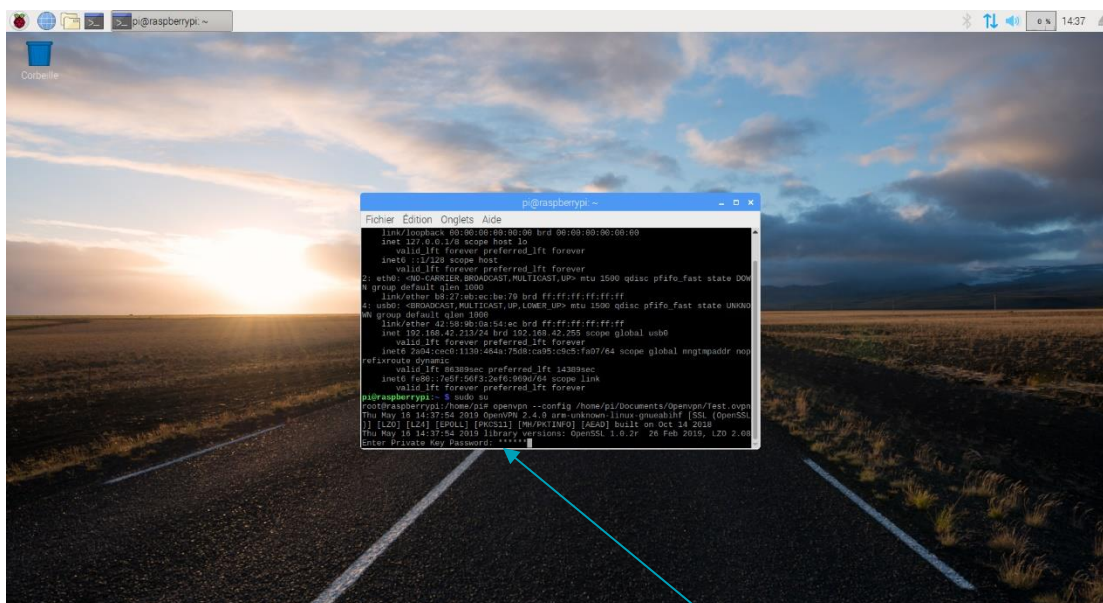
```
apt-get install openvpn
```

```
root@NUL:~# apt-get install openvpn
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
The following additional packages will be installed:
  easy-rsa libccid liblzo2-2 libpkcs11-helper1 opensc opensc-pkcs11 openssl pcscd
Paquets suggérés :
  pcmciautils ca-certificates resolvconf
Les NOUVEAUX paquets suivants seront installés :
  easy-rsa libccid liblzo2-2 libpkcs11-helper1 opensc opensc-pkcs11 openssl openvpn pcscd
0 mis à jour, 9 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 2 774 ko dans les archives.
Après cette opération, 7 069 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [0/n] _
```



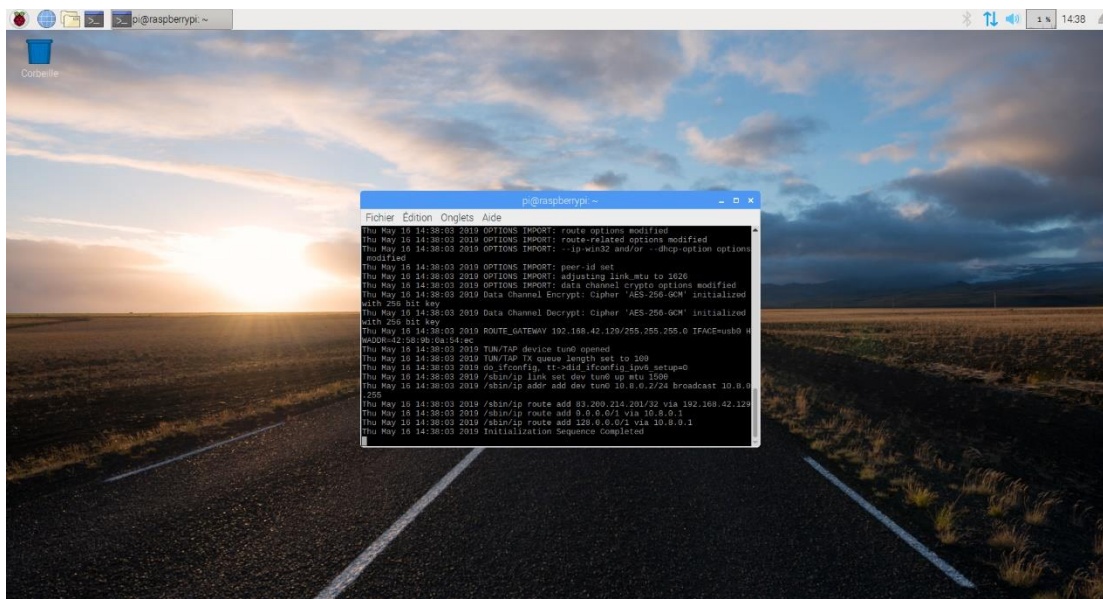
Avant d'utiliser la commande suivante, vous devez avoir le fichier de configuration sur votre machine. (Si vous souhaitez plus d'information voir annexe 2)

`openvpn --config /DOSSIERSOURCE/NOMDEFICHIER.ovpn`



A ce moment-là, il faudra rentrer votre mot de passe

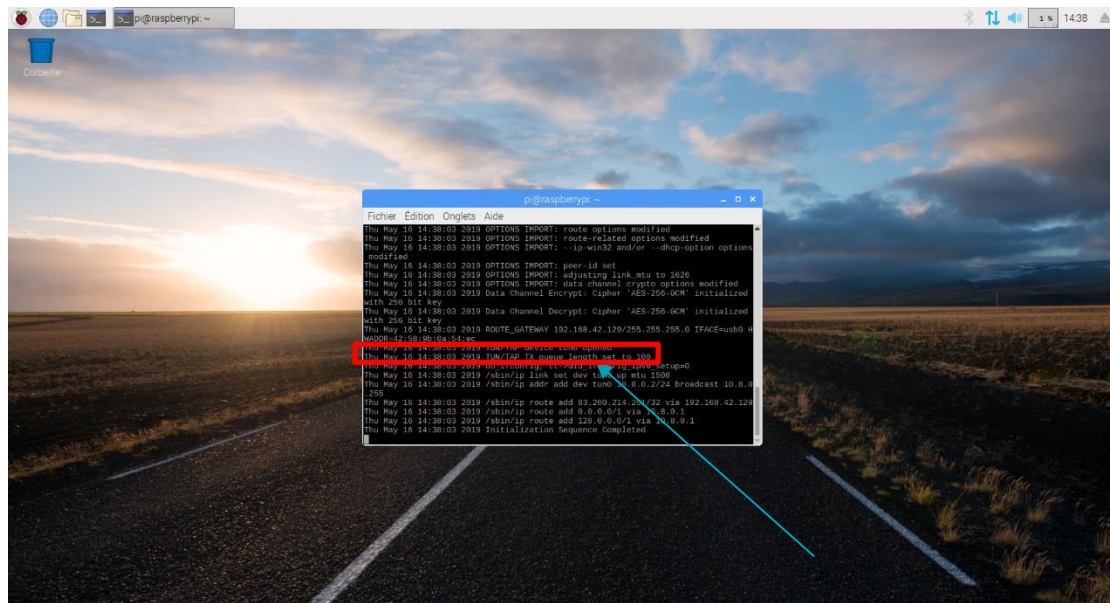
On pourra donc après cela se connecter au Vpn via le fichier de configuration que le serveur nous aura donné (affiché avec une extension .ovpn, exemple : test.ovpn)



A savoir qu'il faudra garder ce terminal ouvert pour garder la connexion active avec le VPN.

Phase de test

Pour tester que le client fonctionne après s'être connecter il faut regarder dans l'interface que certains paramètres se soient bien déroulés.



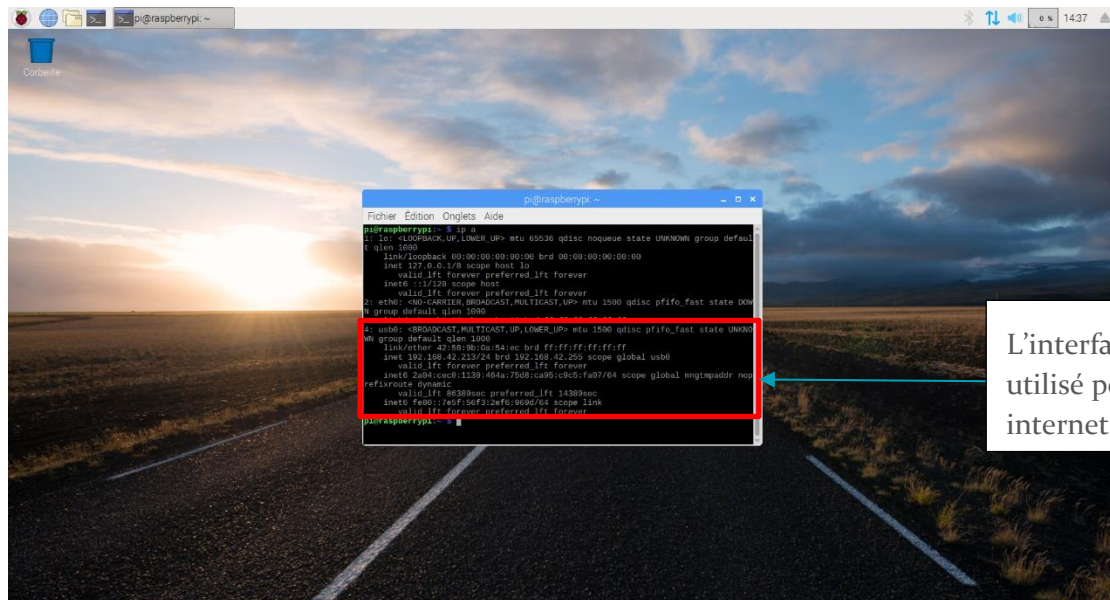
Si après avoir entrez le mode de configuration, vous obtenez cette ligne, c'est que vous avez réussi à vous connecter.

On va pouvoir après cela tester le réseau en lui-même et les changements sur le client.

Après notre connexion, on peut voir qu'une nouvelle interface est présente dans notre configuration via la commande

ip a

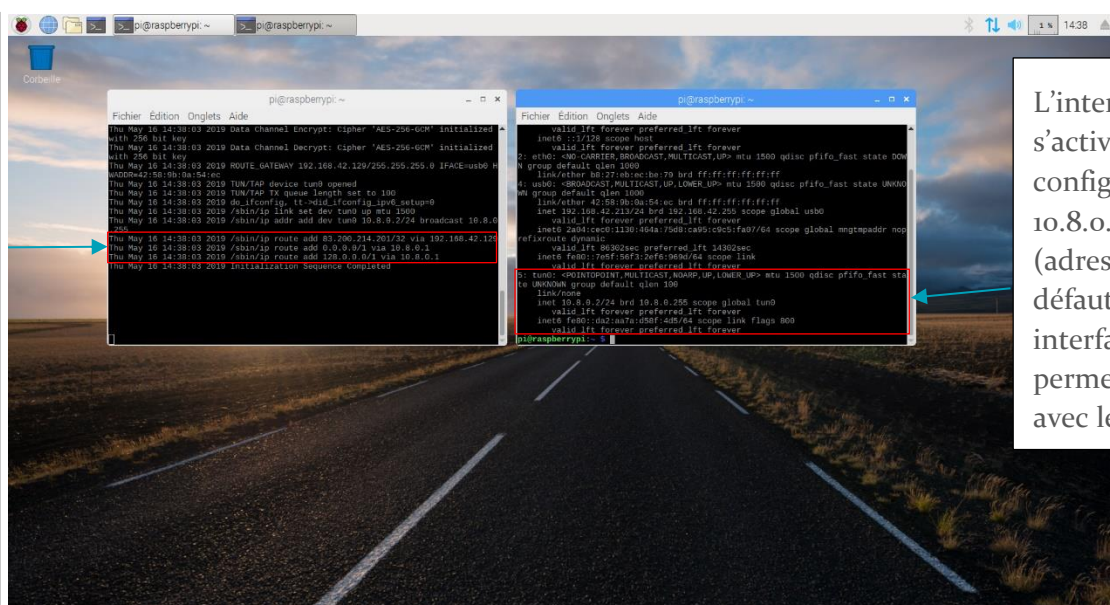
Avant connexion :



L'interface réseau utilisée pour sortir vers internet.

Après connexion :

La connexion à générer les routes qui sont sur le serveur permettant le contact avec le réseau local (ainsi que le réseau extérieur comme dans l'exemple avec l'adresse 83.200.214.201/32 qui passe par l'interface 192.168.42.129.)



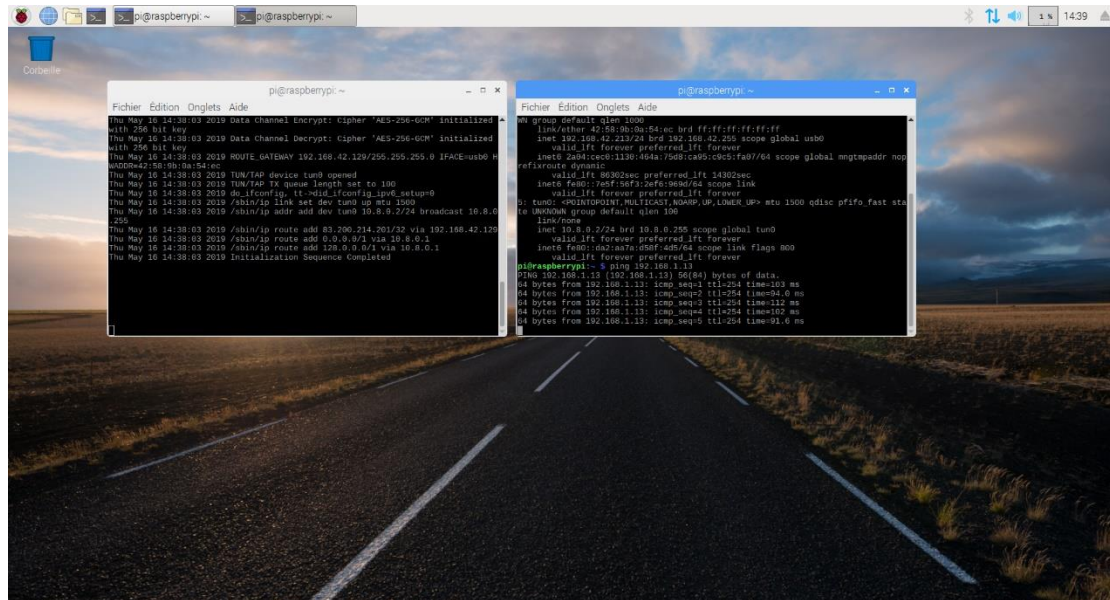
L'interface TUN s'active pour se configurer en 10.8.0.2/24 (adresse par défaut), c'est cette interface qui permet la liaison avec le VPN.

On remarque donc que notre TUN est actif

On va pouvoir tester la connexion dans notre réseau local accessible par le VPN

On va utiliser pour cela la commande ping qui nous permettra de voir si le réseau distant communique bien avec notre machine.

Ping x.x.x.x (remplacer les x par votre adresse ip).



Si tous ces tests ont fonctionné le réseau local est accessible à 100%.

Annexe 2 : Transfert du fichier de configuration de votre clé USB à votre client.

CP

INSTALLATION ANDROID / IOS

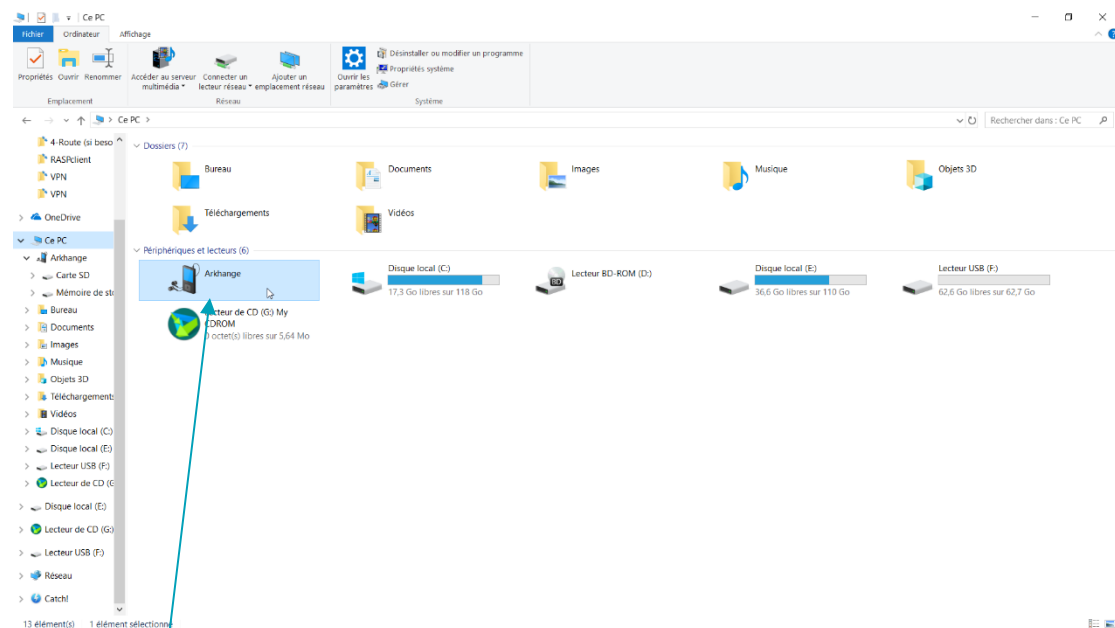
Pour utiliser OpenVPN sur téléphone (ou tablette, il faut télécharger l'application proposé par OpenVPN sur les stores Correspondant au système d'exploitation de votre téléphone.

- Pour Android :
<https://play.google.com/store/apps/details?id=de.blinkt.openvpn&hl=fr>
- Pour IOS :
<https://itunes.apple.com/fr/app/openvpn-connect/id590379981?mt=8>

Vous devez après cela mettre le fichier de configuration dans votre téléphone pour l'utiliser via l'application.

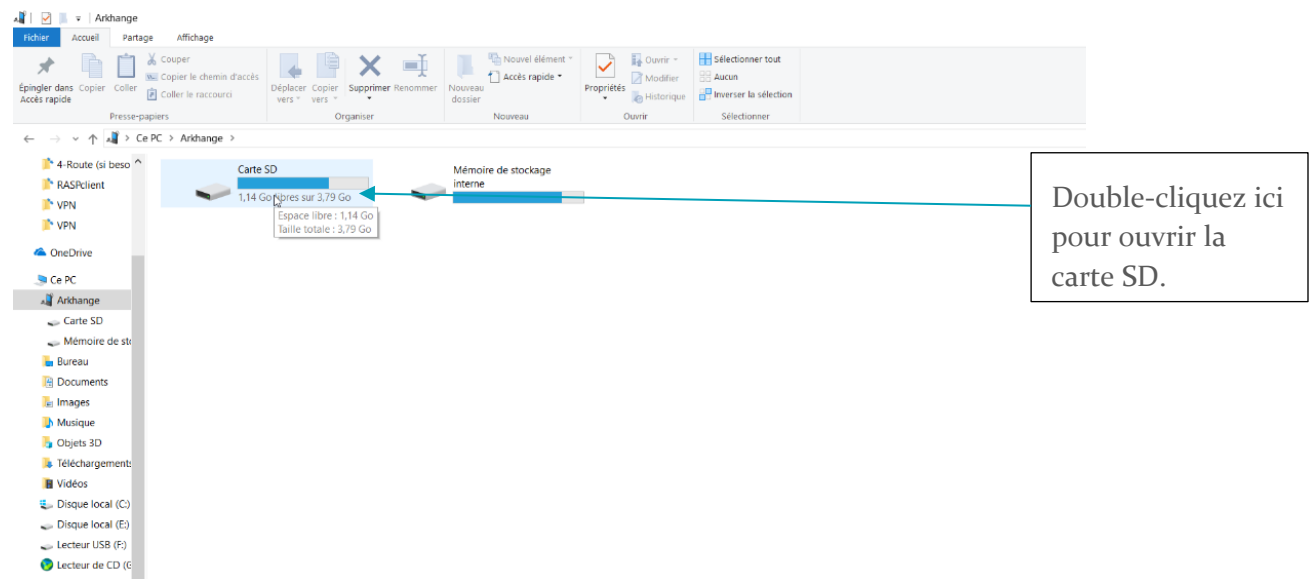
On utilisera pour cela le transfert par stockage du téléphone, pour cela brancher votre téléphone à l'ordinateur (ou une carte de stockage qui convient à votre téléphone).

Vous devez avant cela copier le fichier pour le mettre sur le téléphone (ou sur son stockage).

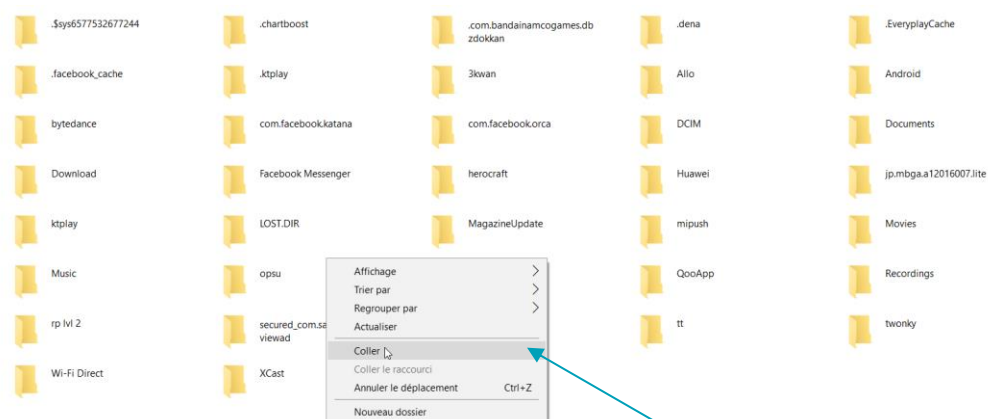


Double-cliquez sur
l'icône du téléphone.

Nous allons maintenant ouvrir la carte pour pouvoir enregistrer le fichier.



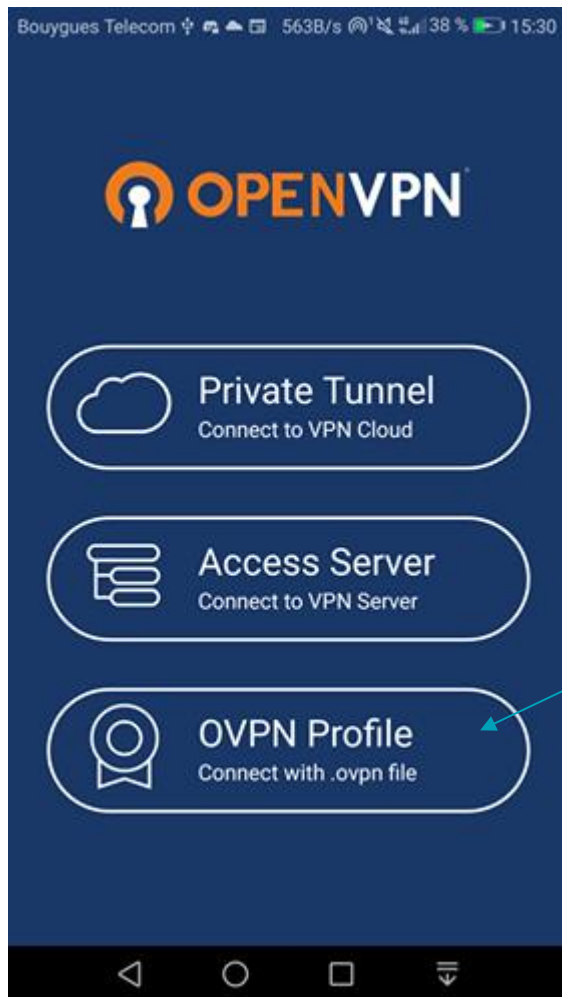
Pour continuer, nous allons coller le fichier pour le réutiliser avec l'application après.



Après cela allez sur votre téléphone (ou remettez votre carte de stockage dans votre téléphone).

Pour l'exemple j'utilise l'application Android de Openvpn (n'ayant pas un appareil Apple). L'application reste très simple d'utilisation et est très explicite pour les paramètres qui concerne les données consommées par le client (en interne donc les données cellulaires et les données utilisés par le réseau interne donc le réseau où se situe le serveur).

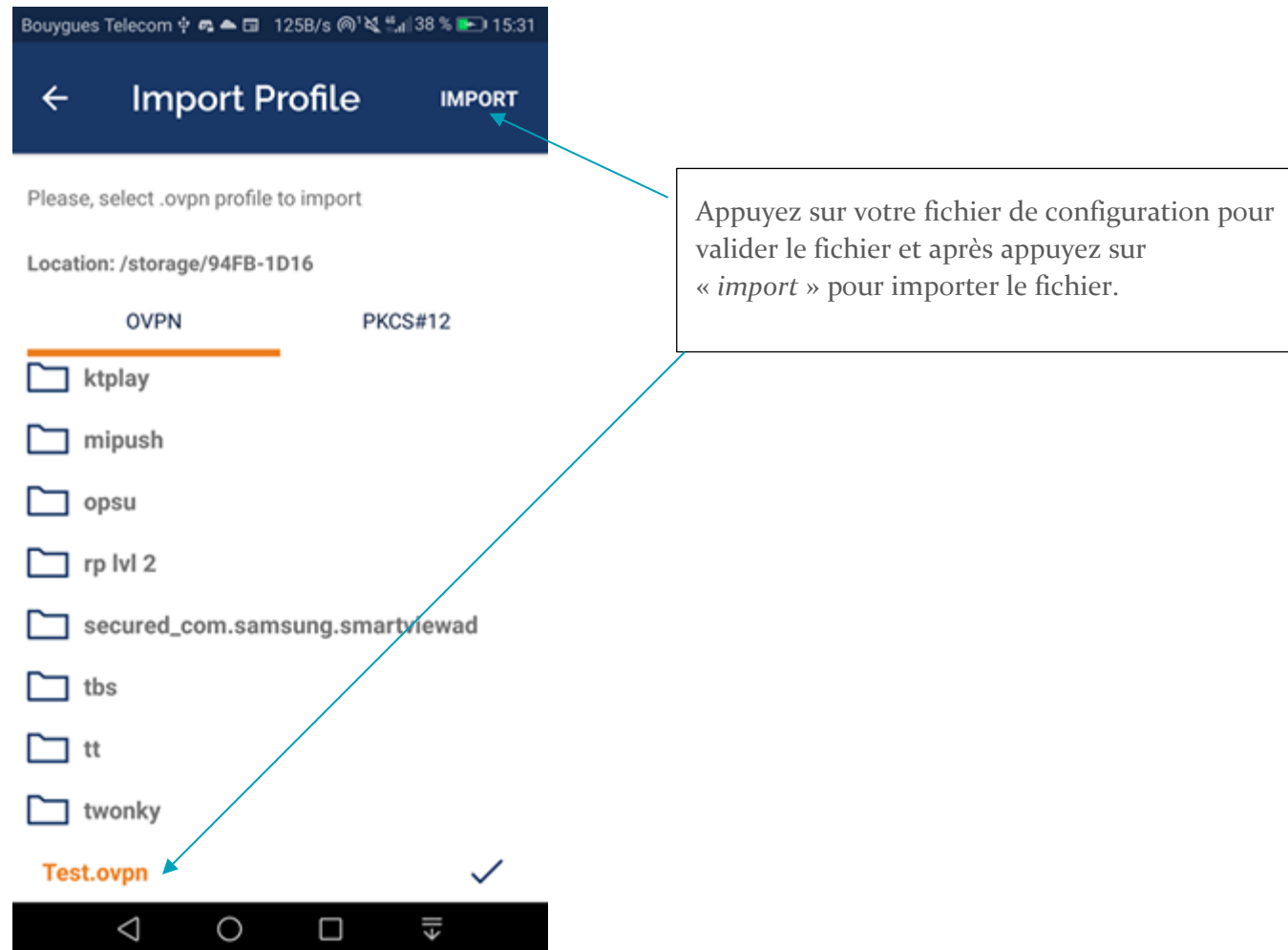
Sur votre téléphone ouvrez l'application OpenVPN



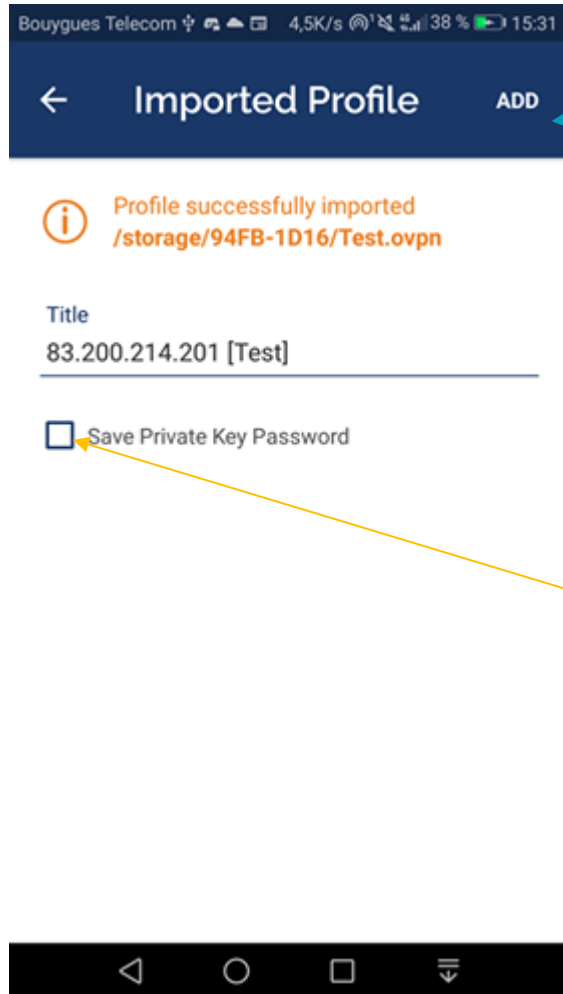
Appuyez sur « OVPN Profile »

Cela vous ouvrira un explorateur de fichiers, il faudra alors chercher le fichier de configuration (.ovpn, exemple : Test.ovpn).

Une fois trouvé, nous allons l'importer pour qu'il soit utilisé par l'application.



Le fichier de configuration exporté, il vous affichera le serveur utilisé (dans le titre, dans notre exemple le serveur n'ayant pas de nom de domaine, il correspond via son adresse IP et aussi le port qui lui est attribué) et aussi l'utilisateur (Test dans notre cas).



Si les données sont valides (Attention au fichier qui pourrait être créé pour pirater votre téléphone via un autre vpn).

Appuyez sur « add » ce qui rajoutera le fichier validé à votre téléphone.

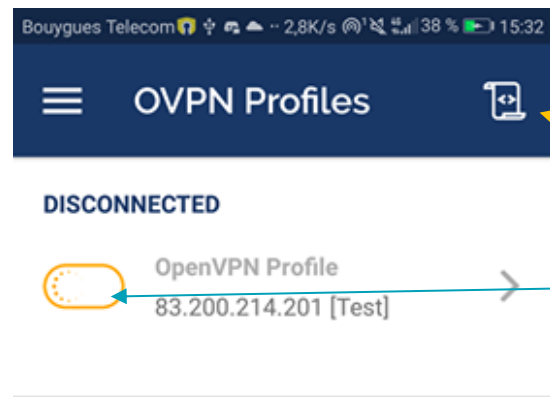
Facultatif et non conseillé :

Vous avez la possibilité de conserver le mot de passe de votre utilisateur grâce à cette case

Appuyez pour cela sur la case à côté de « Save Private Key Password », Cela vous demandera votre Mot de passe. Une fois celui-ci rentré, vous pourrez appuyer sur « add. »

Je ne le conseille pas car cela peut poser un risque de sécurité si le téléphone est perdu ou piraté.

Le fichier de configuration rentré, on peut dès lors se connecter au Vpn.



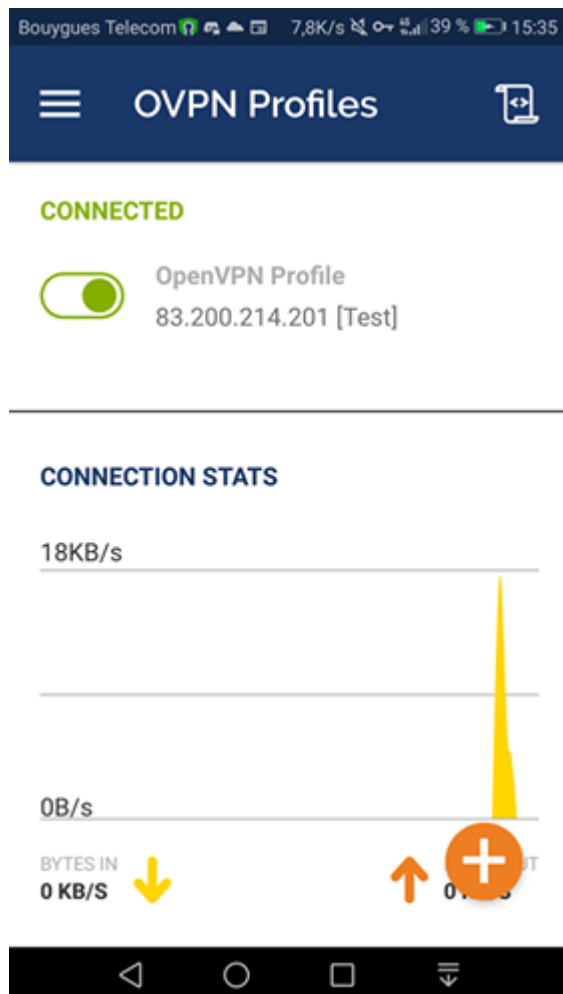
Appuyez ici (flèche bleu) et attendez que le VPN vous demande votre mot de passe, rentrez celui-ci après cela.

L'application peut prendre un peu de temps avant de se connecter (si elle est trop longue pour pouvez regarder au niveau de la flèche orange si le programme n'a pas une erreur).



⚠ Attention en données cellulaires (3G/4G), le débit de votre connexion peut être vite utilisé car il requiert énormément de débit pour rester et utiliser le tunnel chiffré vers le serveur et pouvoir faire les opérations en réseau.
(Statistique réel=)

Une fois la connexion effectuée, si cela a fonctionné, vous aurez cette page qui montre que vous êtes bien sur le réseau local via le VPN (vous pouvez via cette interface voir le débit que vous utilisez sur le réseau local et sur le réseau cellulaire).



Annexe 3 : A quoi peut servir un VPN sur mobile

Le Vpn sur mobile peut vous permettre d'effectuer toute sorte de tâches comme :

- Gérer un appareil du réseau local depuis l'interface du réseau local.
- Gérer un serveur ou utiliser un serveur d'impression (pour imprimer à distance).
- Gérer l'administration : pour gérer la gestion de tous les services du réseau. (Exemples : ouverture de port sur la box internet, bloquer des utilisateurs etc...).



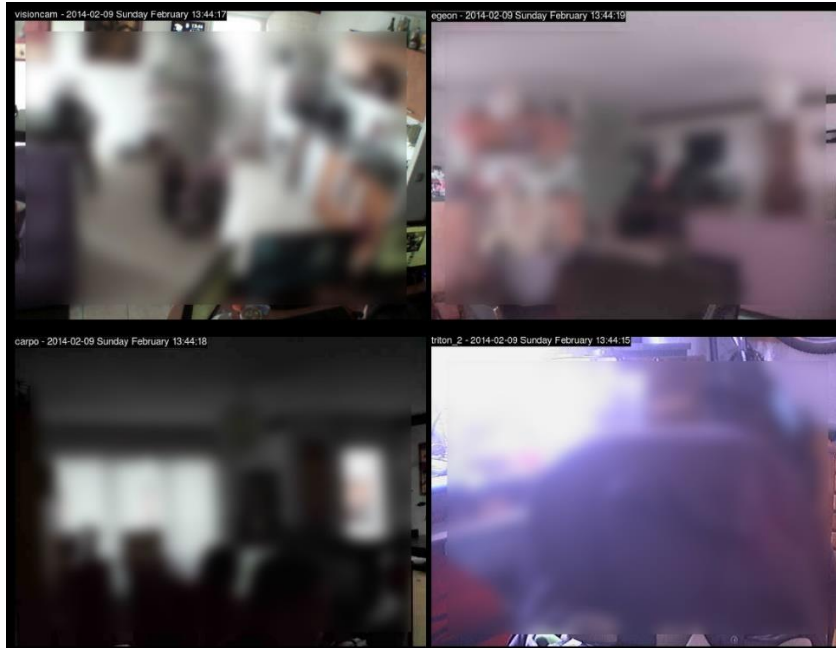
[Source](#)

- Utiliser un serveur de clients légers pour du déploiements de clients légers par le réseau (ceci requiert une connexion locale très bien optimisé ainsi que du côté client) si le mobile renvoi via un point d'accès wifi.



[Source](#)

- Pour la gestion de flux vidéo de caméra (le flux vidéo est plus important sur l'importation, le chiffrement de la vidéo dans le bon format et la rediffusion sur l'appareil que sur du contrôle à distance par une page d'administration qui renvoi les images).



[Source](#)