Raspberry Pi : configurer un serveur VPN

Par Alexandre Laurent

Date de publication : 24 avril 2017

CONFIRMÉ

Cet article a pour but de vous expliquer comment configurer un serveur VPN afin de protéger vos données lors de vos navigations sur Internet, ou encore de vous permettre d'accéder au réseau de votre domicile lorsque vous êtes en déplacement.

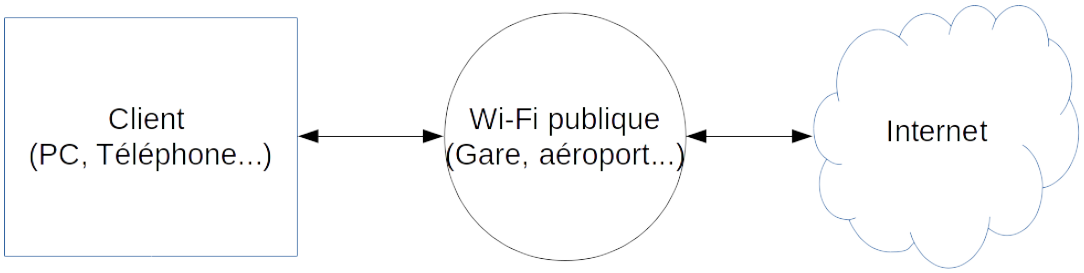
Commentez

I - Introduction....3
I-A - Prérequis....4
II - Configuration simple....4
III - Configuration avancée....5
III-A - Installation d'OpenVPN....5
III-B - Génération des certificats....5
III-C - Configuration du serveur....7
III-C-1 - Topologie réseau de l'exemple....7
III-C-2 - Configuration....7
III-C-3 - Règle du pare-feu....8
III-C-4 - Redémarrage....9
III-D - Configuration du client....9
III-D-1 - Linux....9
III-D-2 - Windows....9
III-D-3 - Mac OS....9
III-D-4 - Android....10
IV - Vérification du fonctionnement....10
V - Sécuriser le serveur....10
V-A - Longueur des clés Diffie-Hellman....10
V-B - Mises à jour....10
V-C - Mots de passe....10
V-D - Configuration du routeur Internet....11
V-E - Fail2ban....11
V-F - Journaux....11
V-G - Note finale....12
VI - Conclusion....12
VII - Remerciements....12

Les sources présentées sur cette page sont libres de droits et vous pouvez les utiliser à votre convenance. Par contre, la page de présentation constitue une œuvre intellectuelle protégée par les droits d'auteur. Copyright ® 2017 Alexandre Laurent. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc. sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à trois ans de prison et jusqu'à 300 000 € de dommages et intérêts.

I - Introduction

Bien que les connexions Wi-Fi publiques soient utiles, elles peuvent être une source de danger pour vos données (1) . En effet, contrairement à la configuration de votre foyer, la machine fournissant le réseau Wi-Fi n'est pas gérée par vous-même.

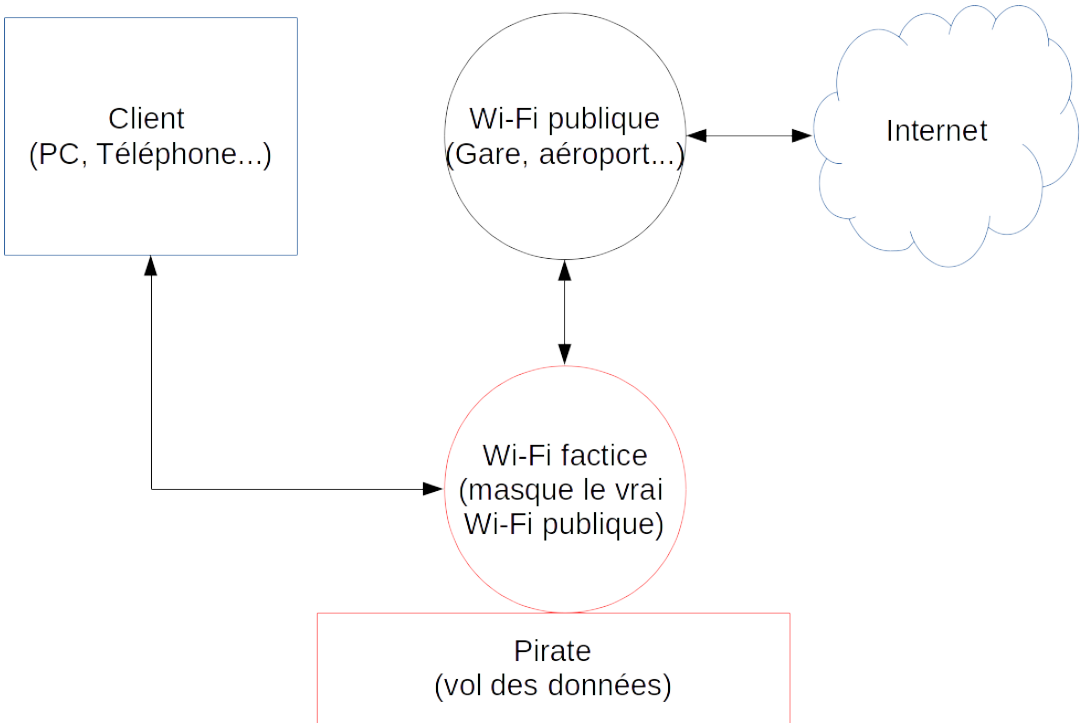


Un réseau Wi-Fi public classique

Il est de votre droit de faire confiance en l'autorité fournissant le réseau Wi-Fi, toutefois, rien ne vous assure que :

- celui-ci ne copie pas les données qui transitent sur son réseau ;
- votre appareil se connecte au réseau fourni par l'autorité publique ;
- personne ne surveille les ondes.

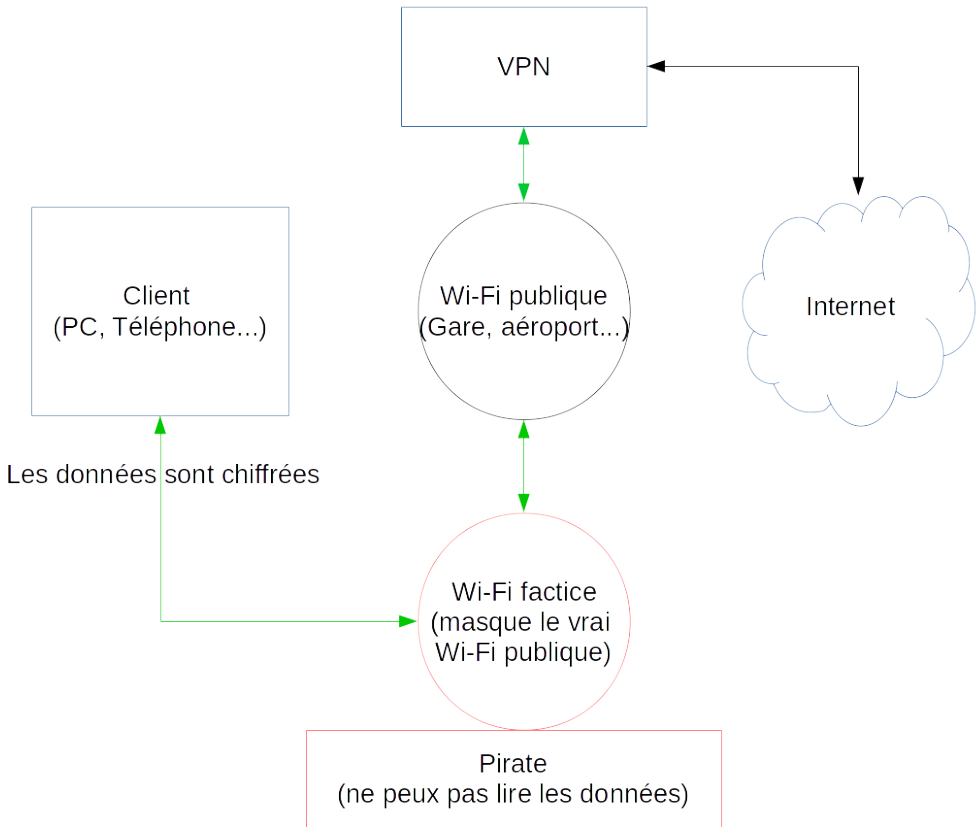
En effet, il est très simple (vraiment trop simple) pour un pirate de créer un point d'accès Wi-Fi portant le même nom que celui de l'autorité publique. Sans vous en rendre compte, vous entrez dans la configuration suivante :



Piratage par attaque d'homme du milieu

Il est évident que vous voulez éviter cette situation. C'est pourquoi vous devez utiliser un réseau privé virtuel (« Virtual Private Network », ou plus couramment appelé VPN). En effet, le VPN vous permettra d'établir une passerelle entre vous et Internet : votre machine se connectant à Internet chiffrera les données avec une clé secrète et celles-ci ne seront déchiffrées que par le VPN. Seul ce dernier enverra les données sur Internet. Dans le cas présenté ci-dessus, le pirate ne pourra plus lire les données car elles sont chiffrées.

Les sources présentées sur cette page sont libres de droits et vous pouvez les utiliser à votre convenance. Par contre, la page de présentation constitue une œuvre intellectuelle protégée par les droits d'auteur. Copyright ® 2017 Alexandre Laurent. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc. sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à trois ans de prison et jusqu'à 300 000 € de dommages et intérêts.



Beaucoup de sociétés proposent des VPN auxquels vous pouvez vous connecter et qui assurent cette même protection. Toutefois, il faut accorder sa confiance à ces sociétés, alors que vous avez la possibilité d'héberger vous-même votre serveur VPN et ce, à bas coût grâce au Raspberry Pï.

En plus de la protection par le chiffrement, le VPN vous permettra de vous connecter au réseau de votre domicile et d'accéder à vos machines qui y sont connectées. Ainsi, même en déplacement, vous pourrez accéder à vos fichiers comme si vous étiez dans un réseau local. Toutefois, le débit sera limité par votre fournisseur d'accès Internet et correspondra au débit montant de votre connexion à la maison.

I-A - Prérequis

Votre Raspberry Pi doit être accessible depuis Internet. Pour cela, votre fournisseur d'accès Internet doit vous permettre d'avoir une adresse IP fixe ou de disposer d'un DNS dynamique vous permettant de vous connecter chez vous, depuis l'extérieur. Aussi, le port utilisé par le serveur VPN doit être redirigé par votre box Internet.

Les explications de ce tutoriel seront données pour le cas d'une adresse IP fixe.

Le Raspberry Pi sera donc le serveur, et Raspbian sera le système d'exploitation utilisé tout au long de cet article.

II - Configuration simple

Vous pouvez aisément configurer un serveur VPN sur le Raspberry Pi grâce au script **PiVPN**. Ce dernier fonctionne sur Raspbian. Pour lancer l'installation, vous n'avez qu'à insérer cette commande dans un terminal :

```
curl -L https://install.pivpn.io | bash
```


Les sources présentées sur cette page sont libres de droits et vous pouvez les utiliser à votre convenance. Par contre, la page de présentation constitue une œuvre intellectuelle protégée par les droits d'auteur. Copyright ® 2017 Alexandre Laurent. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc. sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à trois ans de prison et jusqu'à 300 000 € de dommages et intérêts.

Le script va vous demander plusieurs détails tels que :

- l'utilisateur sur la machine gérant les configurations du serveur ;
- le port à utiliser ;
- le protocole ;
- le client DNS ;
- des informations pour le certificat ;
- la longueur des clés de chiffrement (la taille conseillée est de 2048 bits).

Sachant que le script est prévu pour des utilisateurs de tous niveaux, il est possible de faire une configuration complète et fonctionnelle rien qu'en validant les choix par défaut.

Ensuite, le serveur va redémarrer. À partir de là, vous pouvez ajouter des utilisateurs à votre serveur VPN grâce à la commande :

```
pivpn add
```

Cela va générer un fichier `.ovpn` (dans le dossier *~/ovpns*) qu'il faudra installer sur la machine cliente afin qu'elle puisse se connecter au VPN.

Le script offre aussi les commandes suivantes :

- `pivpn clients` : pour obtenir la liste des utilisateurs actuellement connectés ;
- `pivpn list` : pour obtenir la liste des certificats valides ou révoqués ;
- `pivpn revoke` : pour révoquer un certificat ;
- `pivpn uninstall` : pour désinstaller le serveur VPN.

III - Configuration avancée

Si l'utilisation d'un script tel que PiVPN ne correspond pas à vos besoins, il est toujours possible de configurer un serveur VPN « à la main ». Pour obtenir votre serveur, vous avez besoin d'installer OpenVPN, de générer des certificats et de configurer votre machine afin qu'elle puisse rediriger le trafic Internet de vos clients VPN.

III-A - Installation d'OpenVPN

Il est toujours conseillé de faire les mises à jour et cela est d'autant plus vrai pour un serveur :

```
sudo apt-get update
sudo apt-get upgrade
```

Ensuite, vous pouvez installer OpenVPN :

```
sudo apt-get install openvpn
```

Une fois cela fait, il faut déplacer le répertoire *easy-rsa* à un nouvel emplacement afin que les modifications à faire ne soient pas écrasées lors d'une mise à jour du logiciel :

```
sudo cp -r /usr/share/easy-rsa /etc/openvpn/
```

III-B - Génération des certificats

Les certificats permettent d'authentifier les machines. Pour obtenir un nouveau certificat, il faut une autorité gérant les certificats. Les certificats ont aussi une date d'expiration, permettant ainsi de donner un accès à votre serveur

Les sources présentées sur cette page sont libres de droits et vous pouvez les utiliser à votre convenance. Par contre, la page de présentation constitue une œuvre intellectuelle protégée par les droits d'auteur. Copyright ® 2017 Alexandre Laurent. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc. sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à trois ans de prison et jusqu'à 300 000 € de dommages et intérêts.

pendant un temps défini. Toutefois, vous pouvez aussi rejeter un certificat si vous souhaitez supprimer l'accès à une machine, et cela même si la date d'expiration n'est pas dépassée.

La configuration des certificats se fait à travers le fichier */etc/openvpn/easy-rsa/vars*. Dans celui-ci vous trouverez la configuration du dossier de travail, de la taille de la clé à générer, des valeurs par défaut, de la durée de validité du certificat et ainsi de suite.

Il est aussi d'usage de modifier la variable KEY_SIZE. Cette dernière permet de définir la longueur de la clé de chiffrement.

```
export KEY_SIZE=4096
```

Vous pouvez maintenant procéder à la création de l'autorité gérant les certificats :

```
su
cd /etc/openvpn/easy-rsa
. ./vars
./clean-all
./build-ca
```

Le script vous demandera un nom, ainsi que d'autres informations générales sur les certificats. Pour le nom commun (« Common Name »), vous pouvez simplement mettre « ServeurVPN ». Pour le reste, vous pouvez passer en appuyant sur Entrée.

Ensuite, vous générez la clé et le certificat du serveur :

```
./build-key-server server
```

Encore une fois, vous serez amené à donner des informations. De même que précédemment, vous pouvez simplement appuyer sur Entrée. Pour le nom commun, mettez « serveur ». La commande vous demandera aussi un mot de passe, que vous devez laisser vide. De plus, il faut répondre 'y' aux deux questions liées au certificat.

Finalement, il faut générer la clé et le certificat authentifiant le client :

```
./build-key-pass client1
```

Un mot de passe « PEM pass phrase » vous sera demandé. Ce mot de passe sera exigé lors de la connexion du client au serveur. Pour le reste des informations, mot de passe et certificats, la procédure à suivre par le client est exactement la même que pour le certificat du serveur. Bien sûr, mettez un nom commun particulier au client.

Cette étape est à faire pour chacune des machines différentes que vous souhaitez pouvoir connecter au serveur VPN.

Ensuite, vous devez générer les clés pour **l'échange des clés Diffie-Hellman** :

```
./build-dh
```

Le temps de génération est long, proportionnel à la longueur des clés : il faut compter plus de trente minutes pour une clé de 2048 bits.

La dernière étape est de générer une clé *Hash-based message authentication code* (HMAC) prépartagée pour contrer les attaques reposant sur les injections de paquets et les interceptions (homme du milieu). En effet, si la clé est

Les sources présentées sur cette page sont libres de droits et vous pouvez les utiliser à votre convenance. Par contre, la page de présentation constitue une œuvre intellectuelle protégée par les droits d'auteur. Copyright ® 2017 Alexandre Laurent. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc. sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à trois ans de prison et jusqu'à 300 000 € de dommages et intérêts.

partagée avant toute connexion, il n'y aura pas besoin que le serveur et le client fassent des échanges de messages pour valider leur authenticité :

```
openvpn --genkey --secret /etc/openvpn/easy-rsa/keys/ta.key
```

Comme la sécurité repose sur le prépartage des clés, nous devons envoyer les fichiers suivants à la machine cliente :

```
/etc/openvpn/easy-rsa/keys/client1.key
/etc/openvpn/easy-rsa/keys/client1.crt
/etc/openvpn/easy-rsa/keys/ca.crt
/etc/openvpn/easy-rsa/keys/ta.key
```

III-C - Configuration du serveur

III-C-1 - Topologie réseau de l'exemple

Pour la réalisation de ce tutoriel, le Raspberry Pi se trouve à l'adresse IP 192.168.0.102.

La box Internet se trouve à l'adresse 192.168.0.254.

L'adresse IP publique est : 42.43.44.45

Port utilisé : 2000

III-C-2 - Configuration

Premièrement, il est nécessaire de configurer OpenVPN grâce au fichier */etc/openvpn/server.conf*.

Un fichier par défaut a été fourni lors de l'installation du paquet OpenVPN. Vous pouvez le récupérer ainsi :

```
gunzip -c /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz >/etc/openvpn/
server.conf
```

À l'intérieur, vous devez vous assurer des valeurs de :

Les sources présentées sur cette page sont libres de droits et vous pouvez les utiliser à votre convenance. Par contre, la page de présentation constitue une œuvre intellectuelle protégée par les droits d'auteur. Copyright ® 2017 Alexandre Laurent. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc. sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à trois ans de prison et jusqu'à 300 000 € de dommages et intérêts.

Le port	port 2000
L'autorité de certification	ca /etc/openvpn/easy-rsa/keys/ca.crt
Le certificat du serveur	cert /etc/openvpn/easy-rsa/keys/server.crt
La clé privée du serveur	key /etc/openvpn/easy-rsa/keys/server.key
Les clés Diffie-Hellman	dh /etc/openvpn/easy-rsa/keys/dh2048.pem
L'adresse du sous-réseau VPN	server 10.8.0.0 255.255.255.0
Les routes pour que le client puisse accéder à d'autre sous-réseaux ou aux machines du réseau de votre domicile	push "route 10.8.0.1 255.255.255.255" push "route 192.168.0.0 255.255.255.0"
L'activation de la redirection de tout le trafic du client pour que celui passe par le VPN	push "redirect-gateway def1"
La définition d'adresse de DNS (ici opendns.com)	push "dhcp-option DNS 208.67.222.222" push "dhcp-option DNS 208.67.220.220"
La possibilité pour les clients de se parler entre eux	client-to-client
L'authentification par les clés prépartagées	tls-auth /etc/openvpn/easy-rsa/keys/ta.key 0
Les options du démon OpenVPN	user nobody group nogroup

Ensuite, vous devez activer la redirection des paquets. Cela se fait en insérant la ligne :

```
net.ipv4.ip_forward=1
```

dans le fichier */etc/sysctl.conf*.

Par défaut, la ligne est déjà présente dans le fichier. Il suffit de la décommenter.

Pour prendre en compte la modification, vous pouvez utiliser la commande suivante :

```
sysctl -p
```

III-C-3 - Règle du pare-feu

Le pare-feu permet de créer les règles de gestion des paquets entrants et sortants. Ici, nous souhaitons rediriger les paquets provenant des clients VPN (et réciproquement) afin qu'ils puissent accéder à Internet.

Voici la règle pour ce faire :

```
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
```

Si vous utilisez le Wi-Fi et non pas la connexion filaire de votre Raspberry Pi, vous devez changer eth0 pour wlan0.

Si vous redémarrez le serveur, le pare-feu se réinitialisera. Pour pallier ce souci, vous pouvez installer le paquet iptables-persistent. Lors de son installation, il vous sera demandé si vous souhaitez sauvegarder la configuration actuelle. Ainsi, au prochain redémarrage, votre règle sera restaurée et vos clients VPN auront accès à Internet.

Les sources présentées sur cette page sont libres de droits et vous pouvez les utiliser à votre convenance. Par contre, la page de présentation constitue une œuvre intellectuelle protégée par les droits d'auteur. Copyright ® 2017 Alexandre Laurent. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc. sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à trois ans de prison et jusqu'à 300 000 € de dommages et intérêts.

III-C-4 - Redémarrage

Redémarrez le serveur.

III-D - Configuration du client

La configuration se fait à travers un fichier, similaire à celui vu pour le serveur. Il vous suffit d'éditer les règles suivantes, afin de correspondre à votre configuration :

L'adresse et le port du serveur	remote 42.43.44.45 2000
Option pour désactiver des avertissements qui arrivent souvent avec les connexions Wi-Fi	mute-replay-warnings
L'emplacement des clés et certificats	ca /etc/openvpn/keys/ca.crt cert /etc/openvpn/keys/client.crt key /etc/openvpn/keys/client.key tls-auth /etc/openvpn/keys/ta.key 1

Il est aussi possible de placer le contenu des fichiers `.crt`/`.key` dans le fichier de configuration. Au lieu de spécifier une simple ligne `ca chemin_menant_vers_le_certificat`, il faut placer le certificat entre des balises `<ca>` et `</ca>`.

III-D-1 - Linux

Après avoir installé OpenVPN, vous pouvez configurer le client pour le connecter au serveur. Copiez le fichier client.conf servant d'exemple :

```
cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf /etc/openvpn/client.conf
```

Une fois réalisées les modifications afin de correspondre à votre configuration , il ne reste plus qu'à démarrer OpenVPN :

```
sudo openvpn client.conf
```

III-D-2 - Windows

Vous pouvez télécharger le client sur **cette page**.

Sous Windows, le fichier *client.conf* doit avoir l'extension `.ovpn`. À part cela, le contenu du fichier est le même que sous Linux. Toutefois, les chemins indiqués pour les certificats et les clés doivent être modifiés pour convenir aux conventions de Microsoft.

En plaçant votre fichier `.ovpn` dans le dossier config de OpenVPN, la configuration sera automatiquement lue par le client. Il suffira de lui dire de se connecter.

III-D-3 - Mac OS

Vous pouvez télécharger le client **Tunnelblick**.

Une fois lancé, il suffit de charger votre fichier client (`.ovpn`/`.conf`).

Les sources présentées sur cette page sont libres de droits et vous pouvez les utiliser à votre convenance. Par contre, la page de présentation constitue une œuvre intellectuelle protégée par les droits d'auteur. Copyright ® 2017 Alexandre Laurent. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc. sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à trois ans de prison et jusqu'à 300 000 € de dommages et intérêts.

III-D-4 - Android

Vous pouvez télécharger « **OpenVPN for Android** » directement sur Google Play.

Ensuite, il suffit d'importer le fichier de configuration pour le client, en intégrant directement les clés et le certificat dans le fichier, pour plus de facilité.

IV - Vérification du fonctionnement

Pour vérifier le fonctionnement de votre nouvelle configuration, effectuez un traceroute à partir du client une fois celui-ci connecté.

```
traceroute www.google.com
```

Vous devriez retrouver dans les premières lignes l'adresse IP de votre serveur VPN (10.8.0.1), indiquant que la connexion se fait bien à travers celui-ci.

V - Sécuriser le serveur

V-A - Longueur des clés Diffie-Hellman

Au cours du tutoriel, vous avez eu besoin de générer des clés Diffie-Hellman. Plus la clé est longue, plus il sera difficile de la pirater. Actuellement 1024 bits n'est plus considéré comme assez robuste. Il est donc conseillé de générer des clés de 2048 bits, voir 4096 bits si vous souhaitez être prudent. Toutefois, la longueur impacte radicalement le temps de génération des clés. Il faut compter une heure pour les clés de 2048 bits et donc plusieurs heures pour la taille supérieure.

V-B - Mises à jour

Il est absolument nécessaire d'être prudent lors de la configuration d'un serveur. En effet, personne n'est à l'abri d'un piratage, d'autant plus que des scripts automatiques scannent régulièrement toutes les plages d'adresse IP disponibles (et ce pour y trouver de très nombreuses failles).

La première chose est d'avoir un système à jour :

```
sudo apt-get update
sudo apt-get upgrade
```

Vous pouvez aussi activer les **mises à jour inattendues** (« unattended upgrades ») pour obtenir les derniers correctifs de sécurité au plus tôt.

V-C - Mots de passe

Ensuite, il est **obligatoire** de changer les mots de passe. Il ne faut **jamais** garder les mots de passe par défaut :

```
passwd
```

À faire pour le compte utilisateur et pour le compte root.

Les sources présentées sur cette page sont libres de droits et vous pouvez les utiliser à votre convenance. Par contre, la page de présentation constitue une œuvre intellectuelle protégée par les droits d'auteur. Copyright ® 2017 Alexandre Laurent. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc. sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à trois ans de prison et jusqu'à 300 000 € de dommages et intérêts.

V-D - Configuration du routeur Internet

Dans la configuration de votre box Internet, ne redirigez que les ports utiles : ici, seulement le port utilisé par votre serveur VPN.

V-E - Fail2ban

fail2ban permet de se protéger contre les attaques par force brute. Celui-ci va ajouter des règles de rejet pour les adresses IP qui tenteront de se connecter (sans réussir) trop de fois sur votre connexion. Malheureusement, pour contourner cela, les pirates utilisent de multiples adresses IP.

Pour le configurer pour OpenVPN, vous devez créer un fichier */etc/fail2ban/filter.d/openvpn.local* contenant :

```
# Fail2Ban filter for selected OpenVPN rejections
#
#

[Definition]

# Example messages (other matched messages not seen in the testing server's logs):
# Fri Sep 23 11:55:36 2016 TLS Error: incoming packet authentication failed from
 [AF_INET]59.90.146.160:51223
# Thu Aug 25 09:36:02 2016 117.207.115.143:58922 TLS Error: TLS handshake failed

failregex = ^ TLS Error: incoming packet authentication failed from \[AF_INET\]<HOST>:\d+$
            ^ <HOST>:\d+ Connection reset, restarting
            ^ <HOST>:\d+ TLS Auth Error
            ^ <HOST>:\d+ TLS Error: TLS handshake failed$
            ^ <HOST>:\d+ VERIFY ERROR

ignoreregex =
```

Et vous devez créer le fichier */etc/fail2ban/jail.d/openvpn* contenant :

```
# Fail2Ban configuration fragment for OpenVPN

[openvpn]
enabled  = true
port     = 2000
protocol = udp
filter   = openvpn
logpath  = /var/log/openvpn.log
maxretry = 3
```

Afin que les changements soient effectifs, vous devez redémarrer le service :

```
service fail2ban restart
```

L'utilisation de fail2ban peut être superflue. En effet, nous protégeons notre serveur VPN avec l'utilisation de certificats. Grâce à ces derniers, seuls les clients en possession des bons certificats peuvent se connecter.

V-F - Journaux

Maintenant que vous avez un serveur, il est conseillé de surveiller les journaux générés par OpenVPN et les autres journaux du système. Ce sont eux qui vous indiqueront si des attaques se produisent et si votre serveur est compromis.

Les sources présentées sur cette page sont libres de droits et vous pouvez les utiliser à votre convenance. Par contre, la page de présentation constitue une œuvre intellectuelle protégée par les droits d'auteur. Copyright ® 2017 Alexandre Laurent. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc. sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à trois ans de prison et jusqu'à 300 000 € de dommages et intérêts.

V-G - Note finale

Toutes ces précautions sont inutiles si vous rendez publics vos certificats et vos clés (que ce soit à travers une clé USB, ou un site Internet). Il faut comprendre que ces certificats et clés sont comme les clés de votre maison. Vous n'allez sûrement pas les poser à la vue de tous.

VI - Conclusion

À travers ce tutoriel, vous avez appris à mettre en place un serveur VPN afin de sécuriser votre connexion à Internet même si vous êtes dans un lieu public. De plus, grâce à votre Raspberry Pi, vous vous offrez la possibilité d'accéder au réseau de votre domicile.

VII - Remerciements

	Cet article n'aurait pas pu voir le jour sans le support de la **Raspberry Pi Foundation**. En effet, la fondation m'a envoyé un exemplaire du **Raspberry Pi 3 : modèle B** afin de permettre l'écriture de ce document. Developpez.com et moi-même tenons à remercier la **Raspberry Pi Foundation**.

Merci aussi à **Philippe Dpt35** et Franck Talbart pour leurs suggestions ainsi qu'au relecteur orthographique : **Maxy35**

Les sources présentées sur cette page sont libres de droits et vous pouvez les utiliser à votre convenance. Par contre, la page de présentation constitue une œuvre intellectuelle protégée par les droits d'auteur. Copyright ® 2017 Alexandre Laurent. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc. sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à trois ans de prison et jusqu'à 300 000 € de dommages et intérêts.

1 : Toute donnée récoltée peut être revendue sur des marchés noirs ou être utilisée contre vous dans des campagnes de manipulation ou de chantage. Les données, quelles qu'elles soient, doivent être protégées, et ce qui est privé doit rester privé !

Les sources présentées sur cette page sont libres de droits et vous pouvez les utiliser à votre convenance. Par contre, la page de présentation constitue une œuvre intellectuelle protégée par les droits d'auteur. Copyright ® 2017 Alexandre Laurent. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents, images, etc. sans l'autorisation expresse de l'auteur. Sinon vous encourez selon la loi jusqu'à trois ans de prison et jusqu'à 300 000 € de dommages et intérêts.