

OpenVPN

Informations



OpenVPN est un logiciel libre permettant de créer, ou de se connecter à un VPN.

Ce logiciel permet à d'établir des connexions VPN, que ce soit de site-en-site ou bien en tant qu'accès nomade, de manière chiffré grâce à TLS.

Disponible sur Linux / Windows / Mac OS X / iOS / Android, c'est l'une des solutions les plus sécurisées aujourd'hui.

Installation et pré-configuration

Toute la manipulation côté serveur est réalisé sur le paquet OpenVPN 2.4 (sous debian 9)

```
# apt install openvpn easy-rsa
```

Ensuite on va créer tous les dossiers nécessaires

```
# mkdir -p /etc/openvpn/jail/tmp && cp -r /usr/share/easy-rsa /etc/openvpn/
```

Il faut ensuite autoriser le noyaux linux à faire du 'FORWARD', il faut juste lancer les deux commandes suivante :

```
# sed -i 's/#net.ipv4.ip_forward=1/net.ipv4.ip_forward=1/g' /etc/sysctl.conf
&& echo 1 > /proc/sys/net/ipv4/ip_forward
```

On va passer aux différentes configurations possibles. Il faudra obligatoirement faire des modifications dans certains fichiers, certaines seront expliquées, à vous de faire vos recherches pour vous adapter à vos besoins.

Configuration Nomade

Objectif

L'objectif est simple, permettre à un usagé d'accéder à des services internes où alors que chiffrer leurs communications

Configuration du serveur

Il va falloir créer les certificats :

Modifier le fichiers de variables `/etc/openvpn/easy-rsa/vars` afin de faire correspondre à la réalité les valeurs suivantes :

```
export KEY_COUNTRY="FR"
export KEY_PROVINCE="75"
export KEY_CITY="Ville"
export KEY_ORG="Nom de la société"
export KEY_EMAIL="email@domaine.fr"
export KEY_OU="IT"
```

On va ensuite générer les clés et les certificats pour le serveur en lançant le script suivant

`setup.sh`

```
#!/bin/bash

source /etc/openvpn/easy-rsa/vars
/etc/openvpn/easy-rsa/clean-all
openssl dhparam -out keys/dh4096.pem 4096
/etc/openvpn/easy-rsa//pkitool --initca
/etc/openvpn/easy-rsa//pkitool --server server
openvpn --genkey --secret keys/ta.key
```

Le script va vous poser plein de question et va être un peu long sur certaines étape.

Téléchargé le fichier [suivant](#).

Il est fait pour fonctionner, cependant vous pouvez modifier certains paramètres mais il faudra les reporter dans la configuration du client.

Attention au règles de NAT qui peuvent être nécessaire.¹⁾

Il ne restera plus qu'a lancer le service :

```
# systemctl start openvpn@nomade
```

Configuration du client

Téléchargé le fichier [suivant](#).

Et modifier le pour qu'il correspond à votre configuration notamment à la ligne 'remote' où il faudra y mettre l' IP/FQDN du serveur.

Si vous voulez que tout le trafic du client soit rediriger dans le tunnel il faut ajouter à la fin de ce fichier :

```
redirect-gateway def1
```

sinon, il faut ajouter toutes les routes que vous voulez router à la fin de ce même fichier

```
route 10.0.0.0 255.255.255.0
```

Ajouter un client

Pour créer un client il faut lancer les commandes suivantes :

```
# /etc/openvpn/easy-rsa/vars && /etc/openvpn/easy-rsa/build-key-pass  
$NOMDUCLIENT
```

La première 'passphrase' demandé est celle qui sera demander a chaque fois que le client veux se connecter.

Pour le reste, laissez vous guider.

Il faudra modifier le fichier de configuration du client afin de remplir le champs <**nom**> afin qu'il soit identique à celui fournit plus tôt.

Il ne vous restera qu'a fournir au client son fichier de configuration, ainsi que les fichiers :

- /etc/openvpn/easy-rsa/keys/ta.key
- /etc/openvpn/easy-rsa/keys/ca.crt
- /etc/openvpn/easy-rsa/keys/\$NOMDUCLIENT.crt
- /etc/openvpn/easy-rsa/keys/\$NOMDUCLIENT.key

qu'il devra mettre dans un même dossier.

Configuration Site-à-Site



Configuration d'Accès Public



Note :

Règle iptables pour rediriger les requêtes vers une autre une ip (NAT 1.1) sans modification de l'adresse qui émet

```
iptables -t nat -A PREROUTING -p tcp -d 188.165.42.128 -j DNAT --to-  
destination 10.8.0.6
```

Note 2 :

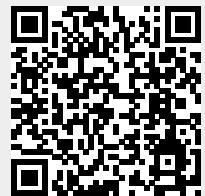
Le packet Resolvconf installer nativement sur Debian bloque les modifications DNS invoqué par Openvpn. Pour outrepasser cela, il suffit de rajouter les lignes suivante dans le fichier de configuration du client :

```
script-security 2
up /etc/openvpn/update-resolv-conf
down /etc/openvpn/update-resolv-conf
```

¹⁾

Voir [ceci](#)

From:
<https://wiki.virtit.fr/> - **VirtIT**



Permanent link:
<https://wiki.virtit.fr/doku.php/kb:linux:generalites:openvpn>

Last update: **2018/07/25 20:44**