OpenVPN

Informations



OpenVPN est un logiciel libre permettant de créer, ou de se connecter a 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 sécurisés aujourd'hui.

Installation et pré-configuration

Toute la manipulation coté serveur est réalisé sur le packet OpenVPN 2.4 (sous debian 9)

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

Ensuite on va créer tous les dossiers nécessaire

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

ensuite 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 societé"
export KEY_EMAIL="email@domaine.fr"
export KEY_OU="IT"
```

On va ensuite générer les clés et les certificats pour le serveur

```
# cd /etc/openvpn/easy-rsa/
# source vars
# ./clean-all
# openssl dhparam -out keys/dh4096.pem 4096
```

```
# ./pkitool --initca
# ./pkitool --server server
# openvpn --genkey --secret keys/ta.key
```

la commande 'openssl' peut prendre beaucoup de temps (environ 30 min sur un VPS d'OVH).

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 expliqué, à vous de faire vos recherches pour vous adapter à vos besoins.

VPN Nomade

Téléchargé le ficher suivant.
Il est fait pour fonctionner

ANCIENNE VERSION

Mise en place d'une solution d'OpenVPN

1 - Préparation du serveur

L'installation du serveur ce fait sur Debian 8.5
Cette page peux se retrouver obsolète d'ici quelques mois, mais la procédure se retrouvera sensiblement identique.

2 - Installation de l'OpenVPN

OpenVPN étant certifié par la communauté Debian, le paquet est donc disponible librement sur leur dépôts officiel. Il suffi de rentrer :

```
apt-get update
apt-get install openvpn
```

Le paquet emporte avec lui de base des fichiers pour configurer le chiffrement par clé. la configuration de base y etant aussi importé, nous allons la copier au sein du répertoire OpenVPN.

```
mkdir /etc/openvpn/easy-rsa/
```

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

Nous allons simplifier la création des clé chiffré avec l'ajout de paramètres de base, cela sera les information de l'entreprise par exemple:

```
pico /etc/openvpn/easy-rsa/vars
```

Il faut modifier les valeurs suivantes:

```
export KEY_COUNTRY="FR"
export KEY_PROVINCE="06"
export KEY_CITY="Nissa"
export KEY_ORG="nicolargo.com"
export KEY_EMAIL="dtc@hadopi.fr"
```

On va créer la clé privé et publique du serveur:

```
cd /etc/openvpn/easy-rsa/
source vars
./clean-all
./build-dh
./pkitool --initca
./pkitool --server server
openvpn --genkey --secret keys/ta.key
```

On va déplacer la clé du serveurs ainsi que celle de chaques clients dans un dossier spécifiques

```
mkdir /etc/openvpn/clés
cp keys/ca.crt keys/ta.key keys/server.crt keys/server.key keys/dh2048.pem
/etc/openvpn/clés
```

VOIR FICHIER server.conf

Pour activer le FORWARD temporairement (effacer au redémarrage)

```
sh -c 'echo 1 > /proc/sys/net/ipv4/ip_forward'
```

Pour activer définitivement le FORWARD (s'applique au redémarrage)
Dans */etc/sysctl.conf* dé-commenter la ligne :

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

Puis les règles de NAT pour iptables

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

Pour activer la règle au reboot :

```
sh -c "iptables-save > /etc/iptables.rules"
```

Il faut rajouter cette ligne dans /etc/network/interfaces sous “iface eth0 inet ...”

```
pre-up iptables-restore < /etc/iptables.rules
```

Création clé utilisateur: Modifier l'ip dans clés/exemple.ovpn (ligne remote) le 1194 correspond au port

Il suffira de lancer le script newclient.sh pour obtenir une clé client (ca.crt et ta.key sont publique et commune a tous les utilisateurs)

le fichier “nom du clients”.ovpn peut etre lancer par le clients.
ATTENTION le client doit l'ouvrir avec C:\ProgramFiles\OpenVPN\bin\openvpn.exe (En administrateur)

Sources : Blog de Nicolargo (Obselete)

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
```

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

Permanent link:
https://wiki.virtit.fr/doku.php/kb:linux:generalites:openvpn?rev=1503869187

Last update: **2017/12/09 00:19**