Un serveur VPN sur Raspberry Pi avec OpenVPN

OpenVPN est un logiciel libre permettant de créer facilement une liaison VPN site à site.

Il fonctionne sur un mode client/serveur, et doit donc être installé sur les 2 sites distants, l'un en client, l'autre en serveur.

Mise en place du serveur OpenVPN sur le RasPi

Tout se passe en ligne de commande, éventuellement par SSH.

Installation

Installation d'OpenVPN :

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

Installation d'OpenSSL pour la sécurisation des données :

```
sudo apt-get install openssl
```

L'installation d'OpenVPN crée un dossier /usr/share/doc/openvpn/easy-rsa/ contenant les scripts permettant de générer facilement les certificats et clés d'authentification nécessaires au fonctionnement d'OpenVPN.

Créer dans le répertoire d'OpenVPN un dossier `easy-rsa` et y copier les fichiers et scripts originaux

```
sudo mkdir /etc/openvpn/easy-rsa/
sudo mkdir /etc/openvpn/easy-rsa/keys
sudo cp -r /usr/share/doc/openvpn/examples/easy-rsa/2.0/* /etc/openvpn/easy-
rsa/
sudo chown -R $USER /etc/openvpn/easy-rsa/
```

Génération des certificats et clés d'authentification

Initialisation des variables de génération

Toujours en ligne de commande sur le Raspi, Se placer dans le répertoire /etc/openvpn/easy-rsa/ et éditer le fichier `vars` :

```
cd /etc/openvpn/easy-rsa/
```

```
sudo nano /etc/openvpn/easy-rsa/vars
```

Renseigner au moins les lignes suivantes (vers la fin du fichier) :

Informations à renseigner dans le fichier vars

```
...
export KEY_COUNTRY=FR
export KEY_PROVINCE=IdF
export KEY_CITY=Paris
export KEY_ORG=MaCompagnie
export KEY_EMAIL="your@email.com"
```

Pays :

- KEY_COUNTRY="code pays" (ex : "FR")

Région :

- KEY_PROVINCE="nom de la région" (ex : "IdF")

Ville :

- KEY_CITY="ville" (ex : "Paris")

Compagnie :

- KEY_ORG="compagnie" (ex : "MaCompagnie")

e-mail

- KEY_EMAIL="email" (ex : "mon@email.com")

Sauvegarder (Ctrl+O), ↵ Entrée pour accepter le nom de fichier, enfin Ctrl+X pour sortir de nano.

Génération du certificat (.crt) et de la clé d'autorité de certification (.key)

OpenVPN fonctionne en mode PKI (Public Key Infrastructure) : le serveur et chaque client possèdent une clé publique (certificat) et une clé privée qui leur sont propres.

Pour générer le certificat et la clé correspondante, il faut exécuter les commandes suivantes :

```
source vars
./clean-all
./build-dh
./pkitool --initca
./pkitool --server server
sudo openvpn --genkey --secret keys/ta.key
```

Une fois ce long processus terminé, copier les clés et certificats utiles pour le serveur dans le répertoire /etc/openvpn/ :

```
sudo cp keys/ca.crt keys/ta.key keys/server.crt keys/server.key
keys/dh1024.pem /etc/openvpn/
```

Configuration du serveur

Créer un répertoire /etc/openvpn/jail dans lequel le processus OpenVPN sera chrooté (afin de limiter les dégâts en cas de faille dans OpenVPN) et un autre répertoire /etc/openvpn/clientconf qui contiendra la configuration des clients :

```
sudo mkdir /etc/openvpn/jail
sudo mkdir /etc/openvpn/clientconf
```

Editer le fichier de configuration server.conf :

```
sudo nano server.conf
```

et lui donner le contenu suivant :

server.conf

```
# Serveur TCP/443
mode server
proto tcp
port 443
dev tun
# Cles et certificats
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
tls-auth ta.key 0
cipher AES-256-CBC
# Reseau
server 10.8.0.0 255.255.255.0
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.4.4"
push "dhcp-option DNS 8.8.8.8"
keepalive 10 120
# Securite
user nobody
group nogroup
chroot /etc/openvpn/jail
persist-key
persist-tun
comp-lzo
# Log
```

```
verb 3
mute 20
status openvpn-status.log
log-append /var/log/openvpn.log
```

Ce fichier permet de créer un serveur VPN SSL routé basé sur le protocole TCP et utilisant le port HTTPS (443) qui est le port sécurisé, pour une accessibilité depuis des réseaux sécurisés par des Firewalls.

Les clients obtiendront une nouvelle adresse IP dans la palette 10.8.0.0/24.

On peut maintenant lancer le service OpenVpn avec la commande suivante :

```
sudo service openvpn start
```

A ce stade les machines clientes peuvent se connecter au serveur VPN qui est à présent fonctionnel.

Par contre impossible d'aller plus loin que le serveur car l'adresse 10.8.0.x n'est par routée en dehors du serveur.

Il faut donc configurer le serveur pour qu'il joue le rôle de routeur entre l'interface VPN (tun0) et l'interface physique (eth0) et rediriger les adresses 10.8.0.x sur son adresse IP réelle.

Autrement dit, il faut interfacer le serveur et internet, pour que le client connecté au serveur ait plein accès à internet.

Pour configurer le routage, taper la ligne de commande suivante :

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

Pour rendre ce paramétrage de routage permanent (même après un reboot), éditer le fichier /etc/sysctl.conf :

```
sudo nano /etc/sysctl.conf
```

et faut donc modifier la ligne suivante :

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

en la dé-commentant (enlever le #) :

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

Pour configurer la translation d'adresse (NAT), taper en ligne de commande:

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

Pour rendre cette règle de NAT persistante après un reboot du serveur, il faut :

- créer un script de chargement de règles de Firewall (ou utiliser un script existant) :

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

- puis modifier le fichier /etc/network/interfaces :

  ```
  sudo nano /etc/network/interfaces
  ```

  en y ajoutant la ligne suivante après la définition de l' interface réseau principale (“iface eth0 inet...”) :

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

Le serveur est maintenant prêt à accueillir les clients. Nous allons donc voir à présent comment déclarer un client sur le serveur.

Création d'un compte client OpenVPN sur le serveur

Pour créer une clé pour le client pcDistant (à remplacer par le vrai nom du compte voulu), saisir les commandes suivantes sur le RasPi (remplacer pcDistant par le nom du client) :

```
source vars
./build-key PCDISTANT
```

<note tip>pour protéger l'accès aux clés par un mot de passe (c'est à dire qu'un mot de passe sera demandé à la mise en place du tunnel VPN), il faut utiliser la commande ./build-key-pass au lieu de ./buil-key</note>

Le script ./build-key génère 3 fichiers dans le répertoire /etc/openvpn/easy-rsa/keys:

- PCDISTANT.crt: Certificat pour le client
- PCDISTANT.csr: Certificat à garder sur le serveur
- PCDISTANT.key: Clés pour le client

Copier les fichiers nécessaires un sous répertoire du répertoire /etc/openvpn/clientconf/ préalablement créé:

```
sudo mkdir /etc/openvpn/clientconf/PCDISTANT/
sudo cp /etc/openvpn/ca.crt /etc/openvpn/ta.key keys/PCDISTANT.crt
keys/PCDISTANT.key /etc/openvpn/clientconf/PCDISTANT/
```

Créer le fichier client.conf dans le répertoire /etc/openvpn/clientconf/PCDISTANT/

```
sudo nano /etc/openvpn/clientconf/PCDISTANT/client.conf
```

Copier l'exemple ci-dessous (remplacer A.B.C.D par l'adresse publique du serveur VPN que l'on peut obtenir par la commande :

```
wget -qO- ifconfig.me/ip):
```

```
# Client
client
dev tun
proto tcp-client
remote A.B.C.D 443
resolv-retry infinite
cipher AES-256-CBC
# Cles
ca ca.crt
cert pcDistant.crt
key pcDistant.key
tls-auth ta.key 1
# Securite
nobind
persist-key
persist-tun
comp-lzo
verb 3
```

Pour assurer la compatibilité avec le client Windows OpenVPN, on fait une copie du fichier client.conf vers client.ovpn

```
sudo cp client.conf client.ovpn
```

On doit avoir les fichiers suivants dans le répertoire /etc/openvpn/clientconf/pcDistant/ :

- ca.crt : Certificat du serveur
- client.conf : Fichier de configuration du client OpenVPN (Linux, BSD, MacOS X)
- client.ovpn : Fichier de configuration du client OpenVPN (Windows)
- PCDISTANT.crt : Certificat du client
- PCDISTANT.key : Clés du client
- ta.key : Clés pour l'authentification

Il ne reste plus qu'à mettre ces fichiers dans une archive ZIP (installer zip si besoin) et de la transmettre sur le PC client:

```
cd /etc/openvpn/clientconf/PCDISTANT/
sudo apt-get install zip
sudo zip pcDistant.zip *.*
```

Utilisation du VPN à partir d'un poste Windows

Utiliser la solution libre “OpenVPN Windows” à télécharger sur leur site officiel http://openvpn.net.

Une fois installé, il suffit de décompresser l'archive pcDistant.zip dans le répertoire C:\Program Files\OpenVPN\config et de se connecter en utilisant OpenVPN GUI, (dans le menu Démarrer). Une fois OpenVPN GUI lancé, il apparaîtra en bas à droite de la barre de tâche. Un clic droit dessus, puis sur connect, et la connexion est établie.