Projet UF Infra :

Sujet réseau VPN

Thomas DUMONT

Théo DELAS

Promotion 2018/2019

B1

Sommaire

I- Prérequis

Avoir un Raspberry Pi sous Raspbian qui doit être accessible depuis Internet. Pour cela, le fournisseur d'accès Internet doit permettre d'avoir une adresse IP fixe permettant de se connecter depuis l'extérieur. Aussi, le port utilisé par le serveur VPN doit être redirigé par votre box Internet.

Le client, qui se connectera donc au Raspberry Pi, devra être sous une distribution Linux supportant le logiciel libre OpenVPN.

II- Installation d'OpenVPN

Mettre à jour son OS :

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

Installer les logiciels OpenVPN et openssl permettant de créer un VPN :

- `sudo apt-get install openvpn openssl`

Coper le répertoire easy-rsa dans le répertoire openvpn :

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

III- Génération des certificats

Se placer dans le répertoire easy-rsa :

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

Effectuer les commandes suivantes pour la création de l'autorité gérant les certificats :

- `source vars`
- `./clean-all`
- `./build-ca`

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

Générer la clé et le certificat du serveur :

- `./build-key-server server`

Générer la clé et le certificat authentifiant le client :

- `./build-key-pass client1`

Générer les clés pour l'échange des clés Diffie-Hellman :

- `./build-dh`

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) :

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

IV- Configuration du serveur

Dans le fichier de configuration du serveur qui sera nommé « server.conf » dans le répertoire « /etc/openvpn/ » écrire les lignes suivantes :

```
dev tun
proto udp
port 2000
ca /etc/openvpn/easy-rsa/keys/ca.crt
cert /etc/openvpn/easy-rsa/keys/server.crt
key /etc/openvpn/easy-rsa/keys/server.key
dh /etc/openvpn/easy-rsa/keys/dh2048.pem
server 10.8.0.0 255.255.255.0
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 217.237.150.188"
push "dhcp-option DNS 8.8.8.8"
log-append /var/log/openvpn
persist-key
persist-tun
user nobody
group nogroup
status /var/log/openvpn-status.log
verb 3
client-to-client
comp-lzo
```

V- Accès à internet depuis un client

Créer un script nommé « rpivpn » dans le répertoire « /etc/init.d/ » pour accéder au réseau local grâce au tunnel VPN depuis le client et y écrire :

```
#! /bin/sh

echo 'echo "1" > /proc/sys/net/ipv4/ip_forward' |
sudo -s
iptables -A INPUT -i tun+ -j ACCEPT
iptables -A FORWARD -i tun+ -j ACCEPT
iptables -A FORWARD -m state --state
ESTABLISHED,RELATED -j ACCEPT
iptables -t nat -F POSTROUTING
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o
eth0 -j MASQUERADE
```

Pour que la redirection soit effective, il faut ensuite assigner les droits adaptés au script, et l'installer en tant que script Init :

- `sudo chmod +x /etc/init.d/rpivpn`
- `sudo update-rc.d rpivpn defaults`

Exécuter le script et redémarrer le serveur VPN :

- `sudo /etc/init.d/rpivpn`
- `sudo systemctl restart openvpn`

VI- Configuration du client

Après avoir installé OpenVPN sur le client, récupérer les clés et certificats suivants créés plus tôt sur le serveur :

```
/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
```

Et les placer dans le même dossier mais cette fois-ci sur le client.

Toujours sur le client, créer un fichier « client.config » dans le répertoire « /etc/openvpn/ »

```
dev tun
client
proto udp
remote x.x.x.x 2000
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert laptop.crt
key laptop.key
comp-lzo
verb 3
```

x.x.x.x est l'adresse IP publique du réseau sur lequel est connecté le VPN.

VII- Révoquer un utilisateur

Se placer dans le dossier « easy-rsa » :

- `Source vars`
- `./revoke-full client1`

Où “client1” est le nom donné au certificat lors de l’exécution de la commande « build-key-pass ».