openVPN

Installation

openvpn

Normalement déjà installé avec Ubuntu mais en version 2. Pour installer openvpn3 suivre la procédure suivante :

```
sudo apt purge openvpn
sudo mkdir -p /etc/apt/keyrings && curl -fsSL
https://packages.openvpn.net/packages-repo.gpg | sudo tee
/etc/apt/keyrings/openvpn.asc
DISTRO=$(lsb_release -c -s)
echo "deb [signed-by=/etc/apt/keyrings/openvpn.asc]
https://packages.openvpn.net/openvpn3/debian $DISTRO main" | sudo tee
/etc/apt/sources.list.d/openvpn-packages.list
sudo apt update
sudo apt install openvpn3
```

easy-rsa

```
sudo apt install easy-rsa
```

Création des certificats sur le serveur

Configuration autorité de certification

```
sudo make-cadir /etc/openvpn/easy-rsa
```

- Editer le fichier /etc/openvpn/easy-rsa/vars pour l'adapter à ses besoins.

```
set_var EASYRSA "${0%/*}"
set_var EASYRSA_OPENSSL "openssl"
set_var EASYRSA_PKI             "$PWD/pki"
set_var EASYRSA_KEY_SIZE        2048
set_var EASYRSA_ALGO            rsa
set_var EASYRSA_CA_EXPIRE       3650
set_var EASYRSA_TEMP_FILE       "$EASYRSA_PKI/extensions.temp"
```

- Pour vérifier en listant les lignes non vides ne commençant pas par un commentaire :

```
cat vars | awk 'NF>0' | grep -v "^#"
```

Création de l'infrastructure

```
sudo -s
cd /etc/openvpn/easy-rsa
./easyrsa init-pki
./easyrsa build-ca nopass
```

Certificats et clefs serveur

- Génération certificat

```
./easyrsa gen-req <nomserveur> nopass
```

- Signature du certificat

```
./easyrsa gen-dh
./easyrsa sign-req server <nomserveur>
```

- Copier certificats et clefs

```
cp pki/dh.pem pki/ca.crt pki/issued/<nomserveur>.crt
pki/private/<nomserveur>.key /etc/openvpn
```

Certificats client

Création certificats

```
./easyrsa gen-req <nomclient> nopass
./easyrsa sign-req client <nomclient>
```

Transfert fichiers

Copier les fichiers suivant sur le client dans le répertoire /etc/openvpn

- pki/ca.crt
- pki/issued/<nomclient>.crt
- pki/private/<nomclient>.key

Haut de page

Configuration Serveur

Configuration

Fichier

- Copier le fichier d'exemple

```
sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz
/etc/openvpn/<nomserveur>.conf.gz
sudo gzip -d /etc/openvpn/<nomserveur>.conf.gz
```

- Mettre à jour le fichier /etc/openvpn/<nomserveur>.conf en vérifiant le chemin des 4 fichiers créés précédemment

```
ca ca.crt
cert <nomserveur>.crt
key <nomserveur>.key
dh dh2048.pem
```

- Autres paramètres intéressants :

```
port 1195                                  ; port (par défaut 1194)
proto udp                                  ; possibilité de mettre udp4 pour
IP V4
server 10.8.0.0 255.255.255.0              ; réseau utilisé par le VPN
comp-lzo                                   ; activer la compression
user nobody                                ;
group nogroup                              ; pas d utilisateur et groupe
particulier pour utilisation du VPN
log         /var/log/openvpn/openvpn.log   ; fichier de log (au lieu de
syslog). Utiliser log ou log-append mais pas les 2.
log-append  /var/log/openvpn/openvpn.log   ; idem mais fichier pas effacé à
chaque redémarrage.
verb 5                                     ; niveau de verbosité
```

> Le paramètre **verb** permet de mettre un niveau d'information plus élevé pour le debug.

TLS

- Générer une clef pour le TLS

```
sudo openvpn --genkey --secret ta.key
```

IP forwarding

- Enlever le commentaire dans le fichier /etc/sysctl.conf

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

- Recharger sysctl

```
sudo sysctl -p /etc/sysctl.conf
```

Activation VPN

```
sudo systemctl start openvpn@<nomserveur>
```

Logs

```
journalctl -u openvpn@<nomserveur> -xe
```

Haut de page

Configuration client

Configuration

```
openvpn3 config-import --config /file/to/profile.ovpn --name <nom connexion>
--persistent
openvpn3 config-acl --show --lock-down true --grant root --config <nom
connexion>
```

Lister les configurations

```
openvpn3 configs-list --verbose
```

Suppression d'une configuration

```
openvpn3 config-remove --config <nom connexion>                          #
suppression par nom config
openvpn3 config-remove --path /net/openvpn/v3/configuration/<xxxxxxxx>   #
suppression par chemin (si plusieur config du même nom)
```

Activation VPN

```
sudo systemctl start openvpn3-session@<nom connexion>.service
```

Logs

Possibilité de modifier le niveau de verbosité des logs dans le fichier de conf en mettant verb 5 (de 0 à 11)

```
journalctl -u openvpn@<nomclient> -xe
tail -f /var/log/syslog
```

Haut de page

Vérifications

Côté serveur

Service

```
sudo systemctl status openvpn@<nomserveur>
```

Tunnel

Vérifier la présence de l'interface tun0

```
ip addr
```

Le port 1194 (ou autre) n'apparaîtra pas avec la commande **ss -tlna**

Client

Tunnel

Vérifier la présence de l'interface tun0, vérifier les routes et tenter de pinger la gateway du réseau VPN

```
ip addr
ip route
ping <IP gateway>
```

Haut de page

Sources

- OpenVPN
- OpenVPN3

Haut de page