OpenVPN et Shorewall : ajout d'un client

De Docs du CCRI

Sommaire

1) Créer un client

- Les commandes ci-dessous sont tapées en tant que **root**
- Cette partie ne concerne que le serveur OpenVPN

A - Création en ligne de commande

Il faut se déplacer dans le répertoire :

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

On charge la configuration :

```
source vars
```

On créé le client en utilisant la nomenclature Adonis (prenom.nom) :

```
./build-key prenom.nom
```

Les informations suivantes seront demandées avant de signer le certificat :

- Country Name : **FR**
- State or Province Name : **ESSONNE**
- Locality Name : **Orsay**
- Organizational Unit Name : **CCRI** (vous pouvez mettre le nom du département ou du service)
- Common Name : **prenom.nom**
- Name : **prenom.nom**
- Email Address : **prenom.nom@u-psud.fr**
- Challenge password : Ne rien mettre
- An optional Company name : **IUT Orsay**

B - Stocker les fichiers pour les fournir aux utilisateurs

Important : Fichiers nécessaires au client

- Le certificat de l'autorité de certification (le serveur lui même) : **ca.crt**
- La clef secrète qui renforce la sécurité : **ta.key**
- Le certificat client : **prenom.nom.crt**
- La clef privée du certificat client : **prenom.nom.key**
- Le fichier de configuration du VPN : **client.conf**

Tous ces fichiers sont disponibles dans le répertoire : **/etc/openvpn/easy-rsa/keys**.
Pour faciliter les choses, il convient de créer un répertoire au nom de l'utilisateur (sous la forme prenom.nom) dans le répertoire : **/etc/openvpn/clients-config**.
Vous trouverez également dans ce répertoire, deux sous répertoires :

- windows : Il contient le fichier de configuration du client pour Windows
- linux : Il contient le fichier de configuration du client pour Linux

2) La configuration IP des clients

Important : Le serveur lira automatiquement le fichier **/etc/openvpn/clients-routes/prenom.nom**.
Dans ce fichier, il y a deux informations primordiales :

- L'adresse IP fixe du client.

- Les différentes routes que l'on souhaite donner au client.

Exemple : /etc/openvpn/clients-routes/benoit.tonnerre

```
ifconfig-push 10.42.0.10 255.255.255.0                    # Adresse IP fixe du client "benoit.tonnerre
push "route 130.79.200.181 255.255.255.255 10.42.0.1"     # Route permettant l'accès au KMS de Strasbo
push "route 129.175.248.34 255.255.255.255 10.42.0.1"     # Route permettant l'accès au serveur webapp
push "route 192.70.36.6 255.255.255.255 10.42.0.1"        # Route permettant l'accès au serveur vader-
push "route 192.70.36.27 255.255.255.255 10.42.0.1"       # Route permettant l'accès au serveur tohno
push "route 192.70.36.33 255.255.255.255 10.42.0.1"       # Route permettant l'accès au serveur ldap (
push "route 192.70.36.55 255.255.255.255 10.42.0.1"       # Route permettant l'accès au serveur webapp
```

3) Les ACL

- Cette partie ne concerne que Shorewall

Voici un exemple du fichier **/etc/shorewall/rules** qui illustre les règles énoncées ci-dessus:

```
# Client : Benoît Tonnerre - benoit.tonnerre :          10.42.0.10
KMS(ACCEPT):NFLOG       vpn:10.42.0.10  net                                                 # Autori
HTTPS(ACCEPT):NFLOG     vpn:10.42.0.10  srv:192.70.36.55                                    # Autori
LDAP(ACCEPT):NFLOG      vpn:10.42.0.10  srv:192.70.36.33                                    # Autori
LDAP(ACCEPT):NFLOG      vpn:10.42.0.10  srv:192.70.36.27                                    # Autori
LDAPS(ACCEPT):NFLOG     vpn:10.42.0.10  srv:192.70.36.27                                    # Autori
SSH-IUT(ACCEPT):NFLOG   vpn:10.42.0.10  srv:192.70.36.33                                    # Autori
SMB(ACCEPT):NFLOG       vpn:10.42.0.10  srv:192.70.36.6                                     # Autori
HTTPS(ACCEPT):NFLOG     vpn:10.42.0.10  net:129.175.248.34                                  # Autori
MYSQL(ACCEPT):NFLOG     vpn:10.42.0.10  net:129.175.248.34                                  # Autori
```

Très important : Dès lors ou vous donnez accès à une IP, via une route, il faut bien penser à autoriser **tous** les flux nécessaires.
Exemple : En autorisant la connexion à anakin (loadbalancer LDAP), il faut aussi autoriser la connexion SSH.
