

Présentation

Prérequis

Tunnel non chiffré

Serveur

Client

Tunnel avec chiffrement symétrique

Serveur

Client

Tunnel avec chiffrement asymétrique

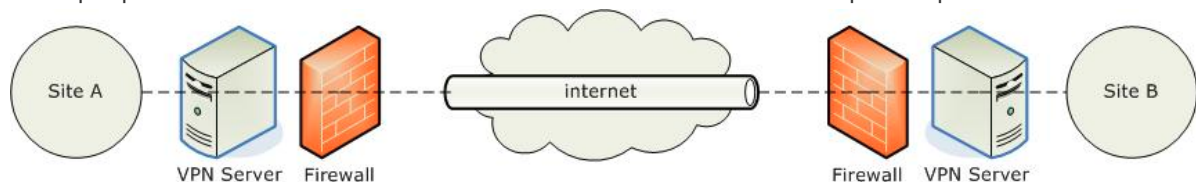
Prérequis

Client

Serveur

Présentation

Openvpn est un logiciel open source qui permet de mettre en place un Tunnel Privée Virtuel entre 2 machines, cet outil est très pratique pour permettre un accès au réseau depuis l'extérieur, par exemple pour effectuer du télétravail avoir accès au réseau de l'entreprise à partir de chez soi.



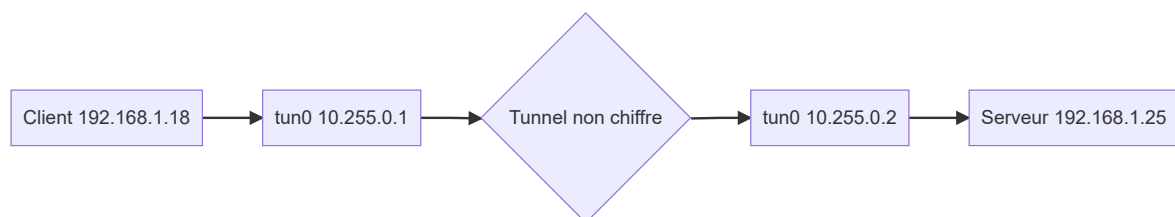
Prérequis

Dans un premier temps on installe openvpn puis easy-rsa pour gérer les certificats.

```
sudo apt install openvpn easy-rsa -y
```

Tunnel non chiffré

Dans ce premier exemple je vais mettre en place un tunnel vpn très basique sans chiffrement, le but étant de tester l'outil et d'analyser les trames qui transitent sur l'interface tun0 avec Wireshark. (l'interface tun0 est la carte réseau utilisée par openVPN pour faire le tunnel.)



⚠ Veiller bien à arrêter la commande du tunnel non chiffré vu précédemment avec un CTRL+C

Serveur

Sur le serveur je génère la clef de chiffrement qui va être utilisée par les 2 machines et je donne accès en lecture à tout le monde sur le fichier clef pour pouvoir le transférer facilement via SCP. (un transfert avec FileZilla est également possible)

```
sudo openvpn --genkey secret /tmp/ClefSymetriqueSecrete && chmod o+r /tmp/ClefSymetriqueSecrete
```

⚠ En chiffrement symétrique tout personne qui peut lire la clef peut déchiffrer le tunnel vpn.

La commande pour initialiser le tunnel est sensiblement identique au tunnel non chiffrer mais avec l'option `--secret` pour indiquer qu'il faut utiliser la clef de chiffrement.

```
sudo openvpn --dev tun0 --verb 5 --ifconfig 10.255.0.1 10.255.0.2 --secret /tmp/ClefSymetriqueSecrete
```

Client

Il faut d'abord récupérer la clef de chiffement par exemple en SCP

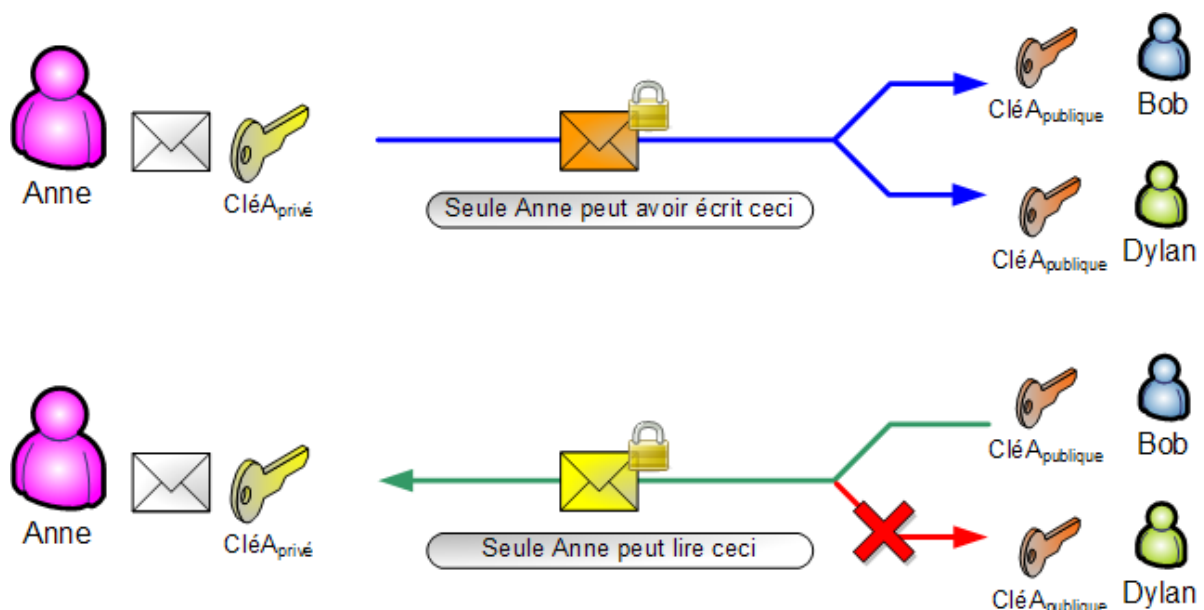
```
cd /tmp && scp toor@192.168.1.25:/tmp/ClefSymetriqueSecrete .
```

Et enfin créer le tunnel côté client.

```
sudo openvpn --dev tun0 --verb 5 --ifconfig 10.255.0.2 10.255.0.1 --remote 192.168.1.25 --secret /tmp/ClefSymetriqueSecrete
```

Tunnel avec chiffrement asymétrique

Le tunnel par chiffement asymétrique est le plus complet ce type de chiffement est à utiliser. Pour le mettre en place il va falloir générer plusieurs certificats de chiffement les signer.



Prérequis

Dans un premier temps je vais créer sur la 2 machine une arborescence de dossiers histoire d'organiser les fichiers qui vont être générés.

```
sudo mkdir -p /apps/openvpn/keys /apps/openvpn/log /apps/openvpn/conf/files  
/apps/pki
```

Puis je récupère le contenu du répertoire `/usr/share/easy-rsa` ---> `/apps/pki`

```
cd /usr/share/easy-rsa/ && sudo cp -rf * /apps/pki
```

Client

Vérifier la validité du fichier de configuration

```
openvpn --config /path/to/server.conf
```

Serveur

<https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/>

<http://csricted.univ-setif.dz/Documents/cours-informatique/Cryptographie-et-OpenVPN.pdf>

https://openmaniak.com/fr/openvpn_tutorial.php