Présentation

Prérequis

Tunnel non chiffré

Serveur

Client

Tunnel avec chiffrement symétrique

Serveur

Client

Tunnel avec chiffrement asymétrique

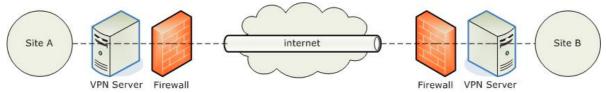
Prérequis

Client

Serveur

Présentation

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



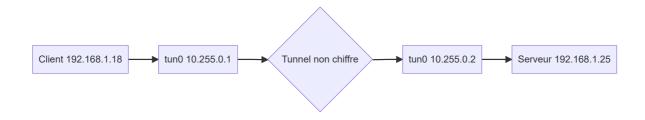
Prérequis

Dans un premier temp on install 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 trés basique sans chiffrement, le but étant de tester l'outils et d'analyser les trames qui transite sur l'interface tun0 avec whireshark. (l'interface tun0 est la carte réseau utiliser par openVPN pour faire le tunnel.)



Serveur

Sur le serveur il vous faudra initialiser le tunnel avec cette commande

```
sudo apt install openvpn easy-rsa -y && sudo openvpn --dev tun0 --verb 5 -- ifconfig 10.255.0.1 10.255.0.2
```

i C'est une commande qui est s'execute en permanance, il ne faut pas la couper au risque de couper aussi le lien VPN!

Client

La client quant a lui a besoin de l'option --remote suivie de l'adress ip du serveur a savoir dans notre exemple 192.168.1.25.

```
sudo apt install openvpn easy-rsa -y && sudo openvpn --dev tun0 --verb 5 -- ifconfig 10.255.0.2 10.255.0.1 --remote 192.168.1.25
```

Quand le message Initialization Sequence Completed apparait c'est bon la connexion entre le 2 machines est effectuer, l'on peut alors vérifier celle si avec un ping du **client** vers le serveur.

```
ping -p70696E67 10.255.0.1
```

i ce ping est un peut spécial le -p70696E67 est du texte au format hexadecimal qui va étre ajouter au ping.

Dans le terminal de connexion ou la commande open a était exécuter une suite de Rwr apparait cela signifie que la connexion s'effectuer bien dans les 2 sens.

```
RWrRWrRWrRWrRWrRWrRWrWRw
```

Pour voir plus en détail les trames qui sont envoyer avec la commande ping rien de mieu q'une analyse wireshark.

```
No. Time Source Destination Protocol Length Info

1 0.00000000 10.255.0.2 10.255.0.1 ICMP 84 Echo (ping) request 1d=0xf83d, seq=18/4608, ttl=64 (reply in 2)

2 0.00109006 10.255.0.1 10.255.0.1 ICMP 84 Echo (ping) reply 1d=0xf83d, seq=18/4608, ttl=64 (request in 1)

3 1.001366618 10.255.0.1 10.255.0.1 ICMP 84 Echo (ping) reply 1d=0xf83d, seq=19/4864, ttl=64 (reply in 4)

4 1.002390906 10.255.0.1 10.255.0.1 ICMP 84 Echo (ping) reply 1d=0xf83d, seq=19/4864, ttl=64 (reply in 4)

5 Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface tun0, id 0

8 Raw packet data

1 Internet Protocol Version 4, Src: 10.255.0.2, Dst: 10.255.0.1

1 Internet Protocol Version 4, Src: 10.255.0.2, Dst: 10.255.0.1

1 Internet Protocol Version 4, Src: 10.255.0.2, Dst: 10.255.0.1

1 Internet Protocol Version 4, Src: 10.255.0.2, Dst: 10.255.0.1

2 0000 45 00 05 54 7a fe 40 00 40 1a9 aa 0a ff 60 00 2

2 0000 00 00 06 ff a0 00 00 00 00 76 06 66 7

2 0001 00 00 00 06 ff a0 00 00 00 00 07 60 96 66 7

2 0002 00 00 00 06 ff a0 00 00 00 00 00 07 60 96 66 7

2 0004 07 69 66 67 70 69 66 67 70 69 66 67 70 69 66 67

2 0004 07 69 66 67 70 69 66 67 70 69 66 67 70 69 66 67

2 0005 07 69 66 67 70 69 66 67 70 69 66 67 70 69 66 67

3 0050 70 69 66 67 70 69 66 67 70 69 66 67 70 69 66 67

3 0050 70 69 66 67 70 69 66 67 70 69 66 67 70 69 66 67

3 0050 70 69 66 67 70 69 66 67 70 69 66 67 70 69 66 67

3 0050 70 69 66 67 70 69 66 67 70 69 66 67 70 69 66 67
```

Avec cette image extrai de wireshark l'on constate que :

- 1. La machine 10.255.0.1 effectue un ping request vers 10.255.0.2
- 2. La machine 10.255.0.2 éffectue un ping reply vers 10.255.0.1
 - il y a bien évidement d'autre informations a retirer comme le port, le protocole, etc...

Tunnel avec chiffrement symétrique

Maintenant je vais crée un tunnel avec une clef pour chiffrer la connexion, ce type de chiffrement est loin être parfait mais il va permettre de constater avec une analyse de tram si les trame du vpn sont bien chiffrer.

1 Veiller bien a arrête 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 qui faut utilier 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 récupère la clef de chiffrement par exemple en SCP

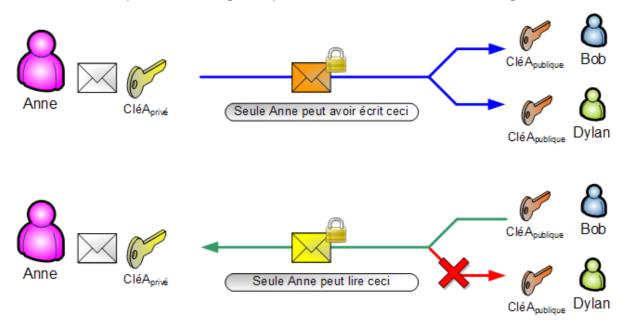
```
cd /tmp && scp toor@192.168.1.25:/tmp/ClefSymetriqueSecrete .
```

Et enfin crée du 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 chiffrement asymétrique est le plus complet ce type de chiffrement est à utiliser. Pour le mettre en place il va falloir généré plusieurs certificat de chiffrement les signée.



Prérequis

Dans un premier temp je vais crée sur le 2 machine une arborescence de dossiers histoire d'organiser les fichier qui vont être générer.

```
sudo mkdir -p /apps/openvpn/keys /apps/openvpn/log /apps/openvpn/conffiles
/apps/pki
```

Puis je recupére le contenue du répetoir /usr/share/easy-rsa --- > /apps/pki

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

Client

Vérifier les validiter 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