**R401 – Architectures sécurisées**

# Accès distants - VPN

*TP 2*

## Consignes

Dans de nombreux cas, des employés ont besoin d'accéder à des ressources de l'entreprise lorsqu'ils sont en déplacement. Cela pose le problème d'accès au réseau interne depuis une zone non fiable qui peut être le réseau internet. Dans ce cas, il est indispensable de mettre en œuvre un accès particulier qui peut garantir la confidentialité des échanges et une sécurité suffisante. C'est l'objet de ce TP : mettre en place un VPN (Virtual Private Network) entre une zone non fiable (internet) et une zone fiable (l'intérieur de votre SI).

## 1 Questions préliminaires

Dans un premier temps, il s'agit de réaliser l'architecture matérielle. Vous câblerez le réseau présenté en figure 1

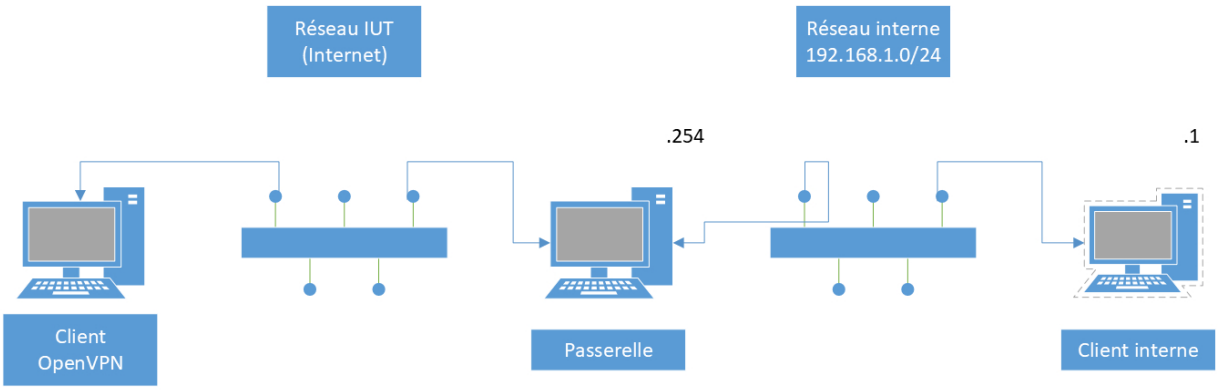


FIGURE 1 – Architecture réseau pour mise en place d'un VPN

**Exercice 1** Configurer la passerelle de sorte que le client interne ait accès à la partie internet. Il s'agira de mettre du NAT en place

**Exercice 2** Donner la configuration (adresses, masques, routes, iptables) de chacun des équipements.

**Exercice 3** Installer OpenVPN et la librairie **lzo** sur la passerelle et sur le client.

## 2 Premiers tests

**Exercice 4** Vérifier dans un premier temps la liste des interfaces réseau sur votre machine. Ensuite, on cherche à vérifier si OpenVPN peut être lancé à la main. Sur la passerelle, exécuter la commande suivante :

```
openvpn --dev tun0 --ifconfig 192.168.10.1 192.168.10.2
```

Ce document est distribué sous licence
Creative Commons Paternité - Partage à l'Identique 2.0 France (http://creativecommons.org/licenses/by-sa/2.0/fr/).
Les autorisations au-delà du champ de cette licence peuvent être demandées à frederic.comby@umontpellier.fr.

Version du document
12 avril 2023

Et sur le client OpenVPN celle indiquée ci-dessous.

```
openvpn --remote ip_passerelle --dev tun0 --ifconfig 192.168.10.2
    ↪ 192.168.10.1
```

**Exercice 5** Vérifiez que la connexion est correctement effectuée en réalisant un ping judicieux.

**Exercice 6** Lister les interfaces présentes sur vos machines. Que constatez-vous ?

**Exercice 7** Pendant que le ping fonctionne, capturez une trame à l'aide de wireshark sur chacune des deux interfaces du client openvpn. Que constatez-vous ? Expliquez et détaillez l'encapsulation du paquet capturé sur l'interface réseau ethernet de votre machine.

**Exercice 8** Démarrer un service non chiffré quelconque sur la passerelle ( telnet, ftp, etc. ). Capturer les paquets échangés sur l'interface ethernet. Sont-ils chiffrés ?

## 3 Ajout d'une clé de chiffrement partagée

Pour que votre VPN soit d'une quelconque utilité, il est impératif de chiffrer les communications qui y transitent. On commence donc simplement, avec une clé secrète partagée qu'il va falloir générer et installer à la fois sur le client et sur le serveur.

Créer une clé partagée sur le serveur à l'aide de la commande suivante

```
openvpn --genkey --secret static.key
```

**Exercice 9** Que contient le fichier static.key ?

**Exercice 10** De quel type de clé s'agit-il ?

**Exercice 11** Quelle est sa longueur ?

**Exercice 12** Il faut maintenant transférer cette clé de façon sécurisée sur le client. Comment procéder ?

Relancez le VPN entre les deux machines en concaténant aux commandes précédentes la directive suivante :

```
--secret /chemin/vers/votre/clef
```

**Exercice 13** Vérifier le bon fonctionnement du réseau.

**Exercice 14** Montrez que vos communications au travers du vpn sont maintenant chiffrées.

Pour gagner de la bande passante, vous pouvez également ajouter la directive suivante aux commandes précédentes.

```
--comp-lzo --keepalive 10 60 --float
```

**Exercice 15** Tester et expliquer.

## 4 Finalisation

Pour se simplifier la vie, il est préférable de mettre au point un fichier de configuration. Le démarrage d'openvpn se fera alors de la façon suivante :

```
openvpn /path/to/pc.conf
```

Avec le fichier de configuration suivant (pour le client) :

```
dev tun
remote ip_de_la_passerelle
ifconfig 192.168.10.2 192.168.10.1
secret /etc/openvpn/static.key
comp-lzo
keepalive 10 60
float
```

**Exercice 16** Créer le fichier de configuration du serveur, et tester le bon fonctionnement du tout.

## 5 Utilisation de TLS et PKI

**Exercice 17** À l'aide de votre moteur de recherche préféré, expliquez en quelques phrases ce qu'est TLS.

La première étape pour obtenir une véritable configuration est de construire une PKI (public key infrastructure), qui consiste en :

- ▷ Un certificat séparé (clef publique) et une clé privée pour le serveur et pour chaque client.
- ▷ Une autorité de certification qui signe les certificats précédents.

On construit d'abord l'autorité de certification (CA) au moyen des scripts fournis et distribués dans le paquet : **easy-rsa**.

**Exercice 18** Que signifie X509 ? Suivre la procédure pour générer les clefs, les certificats et les procédures d'échange de clefs indiquée à l'adresse suivante https://community.openvpn.net/openvpn/wiki/EasyRSA3-OpenVPN-Howto.

**Exercice 19** Vous pouvez copier le fichier "vars.exemple" dans un fichier nommé "vars". Ensuite, mettez à jour les informations du certificat X509 (fichier vars).

Réaliser l'initialisation de la PKI sur le CA : générer les paires de clefs ainsi que le certificat à l'aide les commandes suivantes :

```
/usr/share/easy-rsa/ ./easyrsa init-pki
/usr/share/easy-rsa/ ./easyrsa build-ca
```

**Exercice 20** Où sont stockées les clefs ? À quoi correspondent les différents fichiers ?

**Exercice 21** Sur le client et le serveur, générer une paire de clef ainsi que la requête pour l'échange à l'aide des commandes suivantes :

```
./easyrsa init-pki
./easyrsa gen-req PASSERELLE nopass
```

```
./easyrsa init-pki
./easyrsa gen-req CLIENTEXTERNE
```

**Exercice 22** Envoyer les requêtes du serveur et du client sur le CA, puis importez-les à l'aide de la commande

```
./easyrsa import-req Chemin/vers/les/fichiers/req PASSERELLE
./easyrsa import-req Chemin/vers/les/fichiers/req CLIENT
```

**Exercice 23** Signer les clefs publiques pour la passerelle et le client avec les commandes

```
./easyrsa sign-req client CLIENT
./easyrsa sign-req server PASSERELLE
```

**Exercice 24** Qu'est-ce qu'un échange de Diffie-Hellman ?

**Exercice 25** Construire ensuite les paramètres de l'échange de clés par Diffie-Helmann avec la commande suivante :

```
./easyrsa gen-dh
```

**Exercice 26** Tester votre configuration, et faire valider par l'enseignant que cela fonctionne.

## 6 Pontage ( bridge )

Maintenant que votre VPN est en place, il reste à configurer votre serveur afin que :

- ▷ Les deux clients puissent communiquer sans problème.
- ▷ Les deux clients accèdent à internet par la passerelle

Montrez comment, avec l'utilitaire bridge-utils, vous pouvez procéder.

**Exercice 27** Faites valider par l'enseignant que cela fonctionne.