4.1 Notion de VPN

4.1.1 Introduction au VPN

Les applications et les systèmes distribués font de plus en plus partie intégrante du paysage d'un grand nombre d'entreprises. Ces technologies ont pu se développer grâce aux performances toujours plus importantes des réseaux locaux. Mais le succès de ces applications a fait aussi apparaître un de leur écueil. En effet si les applications distribuées deviennent le principal outil du système d'information de l'entreprise, comment assurer leur accès sécurisé au sein de structures parfois réparties sur de grandes distances géographiques ? Concrètement comment une succursale d'une entreprise peut-elle accéder de façon sécurisé aux données situées sur un serveur de la maison mère distant de plusieurs milliers de kilomètres comme si elles étaient locales ? Les VPN, Virtual Private Network ou RPV, Réseau Privé Virtuel en français, ont commencé à être mis en place pour répondre à ce type de problématique. Mais d'autres problématiques sont apparues et les VPN ont aujourd'hui pris une place importante dans les réseaux informatique et l'informatique distribuées.

4.1.2 Principe de fonctionnement

Un réseau VPN repose sur un protocole appelé "protocole de tunneling". Ce protocole permet de faire circuler les informations de l'entreprise généralement de façon cryptée, d'un bout à l'autre du tunnel; ainsi les utilisateurs ont l'impression de se connecter directement sur le réseau de l'entreprise. Le principe du tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données au moyen d'algorithmes de cryptographie négociés entre le client et le serveur et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets et extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé alors qu'ils utilisent en réalité une infrastructure d'accès partagée telle que l'Internet. Les données à transmettre peuvent être prise en charge par un protocole différent d'IP, mais dans ce cas le protocole de tunneling encapsule les données en ajoutant un en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

4.1.3 Utilisation d'un VPN

Il existe trois types standard d'utilisation des VPNs:

- **Le VPN d'accès** qui est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé.
- **L'intranet VPN** qui permet de relier deux intranets distants d'une même entreprise.
- **L'extranet VPN** qui permet d'ouvrir une partie ou la totalité du réseau privé à un client ou un partenaire de l'entreprise afin de communiquer avec lui.

Un système de VPN doit pouvoir mettre en oeuvre les fonctionnalités suivantes :

- **Authentification d'utilisateur:** Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel. De plus, un historique des connexions et des actions effectuées sur le réseau doit être conservé.

- **Gestion d'adresses:** Chaque client sur le réseau doit avoir une adresse propre. Cette adresse doit rester confidentielle. Un nouveau client doit pourvoir se connecter facilement au réseau et recevoir une adresse.

- **Cryptage des données:** Lors de leurs transports sur le réseau public les données doivent être protégées par un cryptage efficace.

- **Gestion de clés:** Les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.

- **Prise en charge multiprotocole:** La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

4.1.4 Protocole utilisé pour réaliser une connexion VPN

Il existe plusieurs classes de protocoles permettant de réaliser une connexion VPN:

- **Protocole de niveau 2** comme PPTP (Point to Point Tunneling Protocol) développé et soutenu de nos jours par Microsoft (notamment utilisé dans les systèmes d'exploitations Windows), L2F (Layer Two Forwarding) développé par Cisco et presque disparu aujourd'hui, L2TP (Layer Two TUnneling Protocol) qui est une évolution des deux précédents.

4.2 Openvpn

4.2.1 Présentation

Comme expliqué plus haut, Openvpn est un logiciel libre de droit et il est donc une très bonne alternative en ce qui concerne la création de tunnels protégés utilisant Internet comme support physique. Openvpn se base sur le protocole de sécurisation SSL/TLS pour assurer la confidentialité des échanges, ce protocole a été élaboré dans le but de protéger les données via des navigateurs web (ex: https [16]). L'authentification se fait la plupart du temps à l'aide de certificats accompagnés de clés.

Il existe deux modes d'utilisations principales concernant Openvpvn:

- **Mode de niveau 2 :** utilisation d'une interface TAP (mode bridgé)
- **Mode de niveau 3 :** utilisation d'une interface TUN (mode routé)

Dans ce TP, nous allons voir 2 cas (scénarios) :
1. VPN sans chiffrement : On établit un réseau privé virtuel, mais les données qui transitent par le tunnel ne sont pas chiffrées.

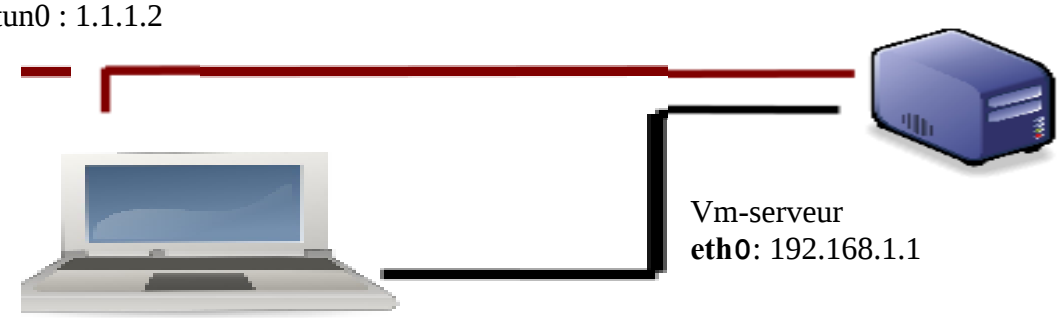
2.VPN par clé de chiffrement symétrique : On établit un réseau privé virtuel. Les données qui transitent par le tunnel sont chiffrées. Le chiffrement et le déchiffrement se fait par une même clé présente sur les 2 extrémités du tunnel.

Maquette à réaliser sous Vmware ou Virtualbox
Prérequis : Les interfaces eth0 client et serveur doivent être configurées comme c'est indiqué sur le schéma.

Client VPN : **Serveur VPN :**

tun0 : 1.1.1.1

tun0 : 1.1.1.2



Vm-serveur
eth0: 192.168.1.1

Vm-client **eth0**: 192.168.1.2

1. VPN sans chiffrement :

Coté serveur
Exécuter les 2 commandes root suivantes :

```
apt-get install openvpn wireshark
openvpn --port 1234 --dev tun0 --ifconfig 1.1.1.1  1.1.1.2 --comp-lzo --verb 5
```

Coté client
Exécuter les commandes root suivantes :

```
apt-get install openvpn
openvpn --remote 192.168.1.1 --port 1234 --dev tun0 --ifconfig\ 1.1.1.2  1.1.1.1 --comp-lzo --verb 5
```

Lancer une capture de trame wireshark sur l'interface eth0 puis un `ping 1.1.1.2` vers le client et vérifier que le canal UDP 1234 n'est pas chiffré .

2.VPN par clé de chiffrement symétrique :

On va créer une clé de chiffrement symétrique qui sera partagée par le client et le serveur VPN .

Coté serveur
Exécuter les 2 commandes root suivantes :

```
openvpn --genkey --secret sec.key

openvpn --port 1234 --dev tun1 --ifconfig 1.1.1.1 1.1.1.2 --comp-lzo --verb 5 --secret sec.key
```

Coté client
Je vous laisse le soin de copier la clé `sec.key` sur le client.
Exécuter la commande root suivante :

```
openvpn --remote 192.168.1.1  --port 1234 --dev tun1 --ifconfig 1.1.1.2 1.1.1.1 --comp-lzo --verb 5 --secret sec.key
```

Lancer une nouvelle fois une capture de trame wireshark sur l'interface eth0 puis un ping vers le client 1.1.1.2 et vérifier que le canal UDP 1234 est crypté.