ÉCOLE PRATIQUE DES HAUTES ETUDES COMMERCIALES

Avenue du Ciseau, 15

1348 Louvain-la-Neuve

# Title

---

Travail de fin d'études présenté en vue de l'obtention du diplôme de bachelier en Informatique et Systèmes : finalité Technologie de l'informatique

*Author :*
Christian JUCKLER 3TL1

*Rapporteur :*
Virginie Van den Schriek

Année Académique 2014-2015

**Résumé**

Test

# Table des matières

# Liste des tableaux

# Table des figures

# Introduction

Première partie

# La problématique des accès distants en entreprise

# Chapitre 1

# Les besoins habituels

# Chapitre 2

# Les besoins spécifiques

# Chapitre 3

# La situation actuelle





FIGURE I – Test figure

# Chapitre 4

# Méthodologie et objectifs

Deuxième partie

# Technologies d'accès distant

# Chapitre 5

# Description des technologies

Dans ce chapitre, je présente les technologies d'accès distants. Dans un premier temps, je présente les tunnels VPN, y compris les protocoles de tunneling et de chiffrement. Ensuite, je présente d'autres technologies d'accès à distance, comme le https, le RDS. Finalement, je passe en revue les solutions des fournisseurs d'accès pour les accès distants.

## 5.1 VPN

Le terme VPN est un acronyme pour « Virtual Private Network ». Un VPN est par définition un réseau virtuel qui transfère des données privées en créant un tunnel à travers un réseau public.

Historiquement, les VPN étaient construits sur des lignes louées, mais le coût de ces infrastructures était trop important. Maintenant, les VPN sont construits sur l'Internet. L'avantage principal est son faible coût. Mais en utilisant l'Internet, les données sont accessibles à tout le monde. Il a donc été nécessaire de fournir des protocoles permettant d'assurer la confidentialité et l'intégrité des données à travers le réseau public.

Un tunnel VPN est monté entre deux passerelles VPN, ces passerelles sont d'un point de vue logique connectées directement l'une à l'autre comme illustré sur la figure. Le tunnel permet d'envoyer des données du réseau privé à travers le réseau public. Le tunnel encapsule les données dans un protocole compris par les deux passerelles. La passerelle émettrice encapsule les données et la passerelle destinataire récupère les données. En plus de l'encapsulation des données, les tunnels VPN peuvent réaliser du chiffrement. Le chiffrement permet de rendre les données inutilisables en cas de vol.

### 5.1.1 Les types de VPN

Il existe deux grands types de VPN : les VPN site-à-site et les VPN client-à-site.

#### Les VPN site-à-site

Ils sont utilisés pour connecter des sites entre eux. Le tunnel est monté entre deux passerelles VPN dont les configurations sont connues. Le réseau Internet opère comme une liaison WAN entre les sites. Les employées peuvent échanger des informations entre les différents sites comme s'ils sont connectés sur le site distant. Dans ce cas-ci, nous utilisons des tunnels VPN IPsec. Je discute d'IPsec plus loin dans ce chapitre.

#### Les VPN client-à-site

Ils sont généralement utilisés par des travailleurs pour accéder aux ressources de l'entreprise depuis des emplacements non fiables. L'utilisateur se connecte via son ordinateur ou son smartphone à la passerelle VPN de son entreprise. Dans ce cas, la configuration n'est pas connue, car selon la localisation de l'utilisateur, les paramètres de connexion changent. Il est souvent nécessaire d'installer sur l'appareil

mobile un client VPN. Nous utilisons des tunnels VPN SSL pour la simplicité de configuration. Je discute de SSL plus loin dans ce chapitre.

### 5.1.2 Les protocoles de tunneling

Ces protocoles permettent de transférer les paquets d'un protocole à l'intérieur d'un autre protocole. On parle d'encapsulation. Il est nécessaire que les deux extrémités du tunnel comprennent le protocole encapsulé. Il existe plusieurs protocoles, je ne discuterai que de ceux utilisés actuellement.

#### Point-to-Point Tunneling Protocol (PPTP)

PPTP est un protocole de tunneling. Il permet de router n'importe qu'elle protocole à travers le réseau IP. Il fonctionne en quatre phases dont une est optionnelle : Link Establishment Phase, Authentication Phase, Callback Control Phase, Network Control Phase.

1. La phase une sert à établir, maintenir et terminer la connexion physique entre les deux hôtes. C'est aussi à ce moment que les protocoles d'authentification sont choisis.
2. La phase une sert à établir, maintenir et terminer la connexion physique entre les deux hôtes. C'est aussi à ce moment que les protocoles d'authentification sont choisis.
3. La phase trois est optionnel et elle permet une sécurité accrue. Elle déconnecte le client et le serveur. Ensuite, le serveur rappelle le client.
4. La dernière phase sert à négocier et implémenter les protocoles de compression et de chiffrement.

#### Layer 2 Tunneling Protocol (L2TP)

Ce protocole a été créé en utilisant les avantages des protocoles PPTP et L2F. Mais il ne permet toujours pas la confidentialité du trafic. Il est possible de faire de l'authentification et du chiffrement avec les paquets PPP, mais la connexion reste vulnérable au niveau de la couche transport. Il est donc intéressant d'associer L2TP avec un autre protocole de sécurité comme IPSec.

## 5.2 IPSec

IPsec est un ensemble de protocole visant à sécuriser les données au niveau de la couche réseau. Il est composé de trois protocoles : AH (*Authentication Header*), ESP (*Encapsulating Security Payload*) et IKE (*Internet Key Exchange*). IKE est utilisé lors de la négociation des paramètres du tunnel VPN. Les deux autres protocoles fournissent la sécurité des données en les encapsulant au sein du tunnel VPN.

Le protocole AH fournit une authentification sur la source du paquet, l'intégrité des données et une protection contre les attaques par rejeu. Le protocole ESP fournit les mêmes sécurités que AH, sauf qu'il n'authentifie l'en-tête IP des paquets. Il fournit en plus la confidentialité des données en chiffrant une partie du paquet. AH et ESP peuvent travailler en mode tunnel ou en mode transport.

Le mode transport est utilisé lorsque les terminaisons du tunnel VPN sont les destinataires finaux de la communication. Ce mode offre une sécurité de bout en bout. Au niveau des paquets, les en-têtes AH et ESP sont placés après l'en-tête IP, il n'y a donc qu'un seul en-tête IP.

Le mode tunnel est plus souple, mais il consomme plus de bande passante. Les destinataires finaux sont connectés via des passerelles VPN. Il n'y a pas de différence entre les VPN site-à-site et les VPN client-à-site. Les passerelles VPN ont pour objectif d'encapsuler les paquets pour les faire passer dans le tunnel VPN. Nous trouvons donc dans le paquet encapsulé l'en-tête IP du paquet d'origine. Comme le paquet est passé à travers la passerelle, il possède un deuxième en-tête IP qui sert au routage entre les deux passerelles (voir figure).

Quand nous parlons de monter un tunnel, en réalité, nous synchronisons un état partagé entre les terminaisons du tunnel. Cet état partagé se nomme une SA (*security association*) en IPSec. Une SA contient l'algorithme de chiffrement utilisé et les clés utilisées, l'algorithme d'authentification, un numéro

d'identifiant, le *security parameter index* (SPI), ... Plus d'autres paramètres qui servent à maintenir les tunnels VPN. Les SA peuvent être créées manuellement ou gérées par l'IKE. Chaque terminaison possède deux SA, une pour le trafic entrant et une pour le trafic sortant. De plus, chaque pair est lié à un protocole. Les SA se caractérisent par un triplet formé du SPI, de l'adresse de destination et du protocole. Les SA sont stockées dans une SAD (*security association database*). Cette SAD est utilisée pour déterminer quel protocole est utilisé pour les paquets sortants et pour fournir les paramètres pour déchiffrer et/ou authentifier les paquets entrants. Il est possible de combiner les SA pour créer des tunnels VPN complexe.

Les SA sont des éléments simples, c'est-à-dire qu'elles traitent tous les paquets de la même manière. Pour un réglage plus fin, IPSec utilise des policies. Ces policies se basent sur les champs suivants des en-têtes du paquet.

— L'adresse de destination
— L'adresse source
— Le protocole de la couche transport
— Le port source
— Le port de destination

Elles servent à déterminer quels paquets à émettre sur quel tunnel, à dropper les paquets ne correspondant à aucune des règles décrites dans les policies. De la même manière que les SA, les policies sont stockées dans une SPD (*security policy database*). Le fonctionnement est similaire, pour chaque paquet entrant ou sortant, le système consulte la SPD pour déterminer les règles à appliquer au paquet. Si une règle est trouvé, le système cherche après la SA correspondante.

IKE a un seul objectif : procéder à des échanges de clé Diffie-Hellman pour sécuriser un tunnel VPN. Il négocie le chiffrement, l'authentification nécessaire au tunnel, qui satisfont les policies. IKE dérive du *Internet Security Association and Key Management* Protocol (ISAKMP). ISAKMP est un framework qui fournit des outils pour la sécurisation des échanges et l'échange de clé. De plus, IKE utilise différents mode du protocole OAKLEY. IKE établit une SA en deux phases. Dans la première phase, le protocole s'occupe de l'authentification des intervenants et de créer un canal sécurisé. Lors de la deuxième phase, il négocie les SA.

### 5.2.1 Les protocoles de chiffrements

## 5.3 Web

## 5.4 Propriétaires

## 5.5 Fournisseurs d'accès

# Chapitre 6

# Comparaison théorique

# Chapitre 7

# Architecture

# Troisième partie

# Comparaison des solutions commerciales

# Chapitre 8

# Choix des solutions

# Chapitre 9

# Installation des solutions

# Chapitre 10

# Scénario de test

# Chapitre 11

# Critères de comparaison

| Test | de | tableau |
|---|---|---|

Table 11.1 – Test de tableau

# Conclusion