République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Superieur
et de la Recherche Scientifique

Université Abderrahmane Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle

En vue de l'obtention du diplôme de
Master Professionnel en Informatique

Option
Administration et Sécurité des Réseaux

Solution de sécurité pour le LAN étendu de NAFTAL GPL

Réalisé par :

KADI Farid
DJOULANE Athmane

Soutenue publiquement devant un jury composé de :

Président	M^r BAADACHE Abderrahmane	Université de Béjaïa
Examinateurs	M^r SAADI Mustapha	Université de Béjaïa
	M^{lle} BOUCHETOUT Lilya	Université de Béjaïa
Encadreur	M^r TOUAZI Djoudi	Université de Béjaïa
Co-Encadreur	M^r REDOUANE Salim	Université de Béjaïa

2013-2014

Résumé

Le travail réalisé dans ce mémoire de fin d'étude fait état des résultats obtenus lors de la proposition d'une solution de sécurité pour le LAN étendu de NAFTAL. Il s'agit d'une architecture VPN IPSec site-to-site, reliant le district GPL de Béjaia avec la direction générale de NAFTAL à Alger. Il en ressort que la technologie VPN basée sur le protocole IPSec est l'un des facteurs clés de succès qui évolue et ne doit pas passer en marge des infrastructures réseaux et des systèmes d'information qui progressent de façon exponentielle. En effet, grâce à cette nouvelle technologie, nous avons offert aux employés une solution pour partager de façon sécurisée leurs données via le protocole IPSec qui est le principal outil permettant d'implémenter les VPNs.

Mots clés : VPN, RPV, IPSec, Tunneling, Site-to-site.

Security solution for the extended LAN of NAFTAL GPL

Abstract

The work done in this memory of end of study reported the results achieved at the proposal of asecurity solution for the extended LAN of NAFTAL. It is an architecture site-to-site of IPSec VPN, linking the GPL district of Bejaia with NAFTAL branch in Algiers. It appears that based on IPSec VPN technology is one of the key factors of success that evolves and should not go outside the network infrastructure and information system progressing exponentially. Indeed, with this new technology, we have offered employees a solutionto securely share their data via the IPSec protocol, which is the primary tool to implement VPN.

Keywords: VPN, RPV, IPSec, Tunneling, Site-to-site.

Remerciements

Avant d'entamer ce projet de fin d'étude, nous tenons à exprimer notre sincère gratitude envers tous ceux qui nous ont aidés ou ont participé au bon déroulement de ce projet.

Nous sommes particulièrement reconnaissants à notre encadreur : M^r TOUAZI DJOUDI *d'avoir accepté de nous encadrer et diriger notre travail, et notre co-encadreur* M^r REDOUAN SALIM *qui nous a beaucoup aider, nous les remercions pour leurs qualités humaines et professionnelles, pour leurs patiences, leurs directives, leurs remarques constructives et leurs aides inestimables.*

Nous tenons à exprimer toute notre grande gratitude aux membres de jury : M^r BAADACHE ABDERRAHMANE, M^r SAADI MUSTAPHA *et* M^{lle} BOUCHETOUT LILYA *d'avoir accepté de juger ce travail.*

Nos remerciements vont également à l'ensemble du personnel du district GPL de NAFTAL, pour l'aide et tous les moyens qu'ils nous ont offert.

Nos vifs remerciements s'adressent à tous nos enseignants de département Informatique de l'université ABDERRAHMAN MIRA *de* BÉJAÏA *pour la formation qu'ils ont eu le soin de nous apporter le long de notre cursus universitaire.*

Nous rendons grâce à Dieu, le tout puissant et miséricordieux, de nous avoir donné le savoir, le courage et la force pour mener à bien et à terme ce modeste travail.

Dédicaces

À mes très chers parents

Pour tout l'amour dont vous m'avez entouré, pour tout ce que vous avez fait pour moi.

Je ferai de mon mieux pour rester un sujet de fierté à vos yeux .

Que ce modeste travail, soit l'exaucement de vos veux tant formulés et de vos prières quotidiennes.

Que dieu, le tout puissant, vous préserve et vous procure santé et longue vie afin que je puisse à mon tour vous combler.

À toute ma famille ...

Vous occupez une place particulière dans mon coeur. Je vous dédie ce travail en vous souhaitant un avenir radieux, plein de bonheur et de succès.

À mon binôme et toute sa famille.

À mes très chers amis

Salim, Walid, Dadi, Aida, Dehia, Moumouh, Lamin, Bohou, Ahcen, ...

KADI Farid.

Dédicaces

Je dédie ce modeste travail de fin d'étude

À mes très chers parents et à toute ma famille,

Avec tous mes sentiments de respect, d'amour, de gratitude et de reconnaissance pour tous les sacrifices déployés

pour m' élever dignement et assurer mon éducation dans les meilleurs conditions

À mes très chers frères et sœurs.

À mon binôme et toute sa famille.

À mes très chers amis,

Mourad, Djidjih, Bizak, Hanine, Sofiane, Nawal *et surtout* **Loubna.**

DJOULANE Athmane.

Table des matières

Résumé i

Abstract iii

Remerciements iv

Dédicaces v

Dédicaces vi

Table des matières vii

Table des figures xii

Liste des tableaux xiv

Liste des abréviations xv

Introduction 1

État de l'art 3

1 La sécurité informatique 4

1.1 Quelques définitions 5

1.1.1 La sécurité informatique 5

1.1.2 Menace 5

1.1.3 Vulnérabilité 6

1.1.4 Attaque 6
1.1.5 Intrusion 6
1.1.6 Contre-mesure 6
1.1.7 Risque 6
1.2 Propriétés de la sécurité informatique 7
1.3 Politique de sécurité 7
1.4 Domaines d'application de la sécurité informatique 8
1.4.1 Sécurité physiques 8
1.4.2 Sécurité de l'exploitation 9
1.4.3 Sécurité logique 9
1.4.4 Sécurité applicative 10
1.4.5 Sécurité des télécommunications 10
1.5 Attaques portantes atteinte à la sécurité informatique 11
1.5.1 Classification des attaques 11
1.5.2 Description d'attaques 12
1.6 Les mécanismes de défense et de sécurité 15
1.6.1 Les défenses logicielles 15
1.6.1.1 Le cryptage 15
1.6.1.2 La signature numérique 15
1.6.1.3 Les certificats 16
1.6.1.4 Les antivirus 16
1.6.2 Les défenses Matérielles 17
1.6.2.1 Les pare-feu 17
1.6.2.2 Les systèmes de détection d'intrusion 19
1.6.2.3 Segmentation 23

2 Les réseaux privés virtuels 27
2.1 Introduction 27
2.2 Présentation d'un réseau privé virtuel 28
2.2.1 Définition 28
2.2.2 Rôle d'un VPN 28
2.2.3 Les fonctionnalités d'un réseau privé virtuel 28
2.2.4 Principe de fonctionnement d'un VPN 29

2.2.5 Types des VPNs 29
2.2.5.1 VPN d'accès (*host to LAN*) 30
2.2.5.2 Intranet VPN (*LAN to LAN*) 30
2.2.5.3 Extranet VPN (*host to host*) 31
2.3 Protocoles utilisés pur réaliser une connexion VPN 31
2.3.1 Le protocole PPP 32
2.3.2 Le protocole PPTP 32
2.3.3 Le protocole L2F 33
2.3.4 Le protocole L2TP 33
2.3.5 Le protocole IPSec 34
2.3.5.1 Architecture du protocole IPSec 35
2.3.5.2 Association de Sécurité 35
2.3.5.3 Base de données des associations de sécurité 36
2.3.5.4 Base de données des politiques de sécurité 37
2.3.5.5 Principe de fonctionnement 37
2.3.5.6 Les deux modes de fonctionnement d'IPSec 38
2.3.6 Le protocole SSL 39
2.3.6.1 Fonctionnement du protocole SSL 39
2.4 Conclusion 40

Étude des charges et mise en œuvre de la solution 41

3 Organisme d'accueil 42
3.1 Introduction 42
3.2 Présentation de l'entreprise NAFTAL 42
3.2.1 Historique 42
3.2.2 Les activités principales de l'entreprise 43
3.3 Présentation du district GPL 43
3.3.1 Les activités principales du district GPL 43
3.3.2 Organisation de la branche GPL 44
3.3.2.1 Organigramme du district GPL 45
3.3.2.2 Description et rôle de chaque service au sein de l'entreprise 47

3.4 Présentation du département informatique 48
3.4.1 Rôle du département informatique de la GPL 48
3.4.2 Organigramme du département informatique 48
3.4.2.1 Description et rôle de chaque service au sein du département informatique 49
3.5 Architecture réseau du district GPL 50
3.5.1 Classification des équipements réseau 53
3.5.1.1 Matériel actif 53
3.5.1.2 Matériel passif 53
3.5.1.3 Autre équipement 54
3.6 Critique 55
3.7 Besoins de l'entreprise 56
3.8 Solution retenue 56
3.9 Présentation du projet 56
3.10 Conclusion 57

4 Mise en œuvre de la solution 58
4.1 Présentation du simulateur Cisco GNS3 58
4.1.1 Définition 58
4.1.2 Les composants du logiciel 59
4.1.3 L'objectif de GNS3 60
4.1.4 Configuration de GNS3 60
4.2 Présentation générale et principe de la solution proposée 65
4.2.1 Description de la maquette à configurer 65
4.2.2 Schéma idéalisé 65
4.2.3 Schéma réel – Principe de mise en place 66
4.3 Configuration (En ligne de commandes) 67
4.3.1 Configuration des routeurs 67
4.3.2 Configuration du protocole IPSec 70
4.3.3 Configuration d'IKE 71
4.3.3.1 Activation du protocole IKE 71
4.3.3.2 Configuration des paramètres de la SA ISAKMP (IKE phase 1) 71

4.3.3.3 Configuration de l'authentification par clé pré-partagée . . 73
4.3.4 Configuration des paramètres IPSec (transform-set) 74
4.3.5 Configuration des listes d'accès 75
4.3.6 Configuration de la carte de cryptage (crypto map) 75
4.3.7 Application des crypto map aux interfaces 76
4.4 tests de fonctionnement 77
4.5 Conclusion 82

Conclusion générale **83**

Annexes 84

A Audit de sécurité **85**
A.1 Présentation d'un audit 85
A.1.1 Délimitation du besoin et des objectifs de l'audit 85
A.1.2 Types d'audit existants 86
A.1.3 Présentation de l'audit de la sécurité informatique 86
A.1.4 Cycle de vie d'un audit de sécurité 86

B Installation de VirtualBox **88**

C Attestation **92**

Bibliographie **94**

Table des figures

1.6.1 Emplacement d'un pare-feu. 19
1.6.2 Un pare-feu au centre d'un réseau. 19
1.6.3 Emplacement d'un HIDS. 22
1.6.4 Emplacement d'un NIDS. 23
1.6.5 Exemple de réseau segmenté avec un DMZ. 25

2.2.1 Tunnel interconnectant A et B à travers Internet. 29
2.2.2 VPN poste à site. 30
2.2.3 VPN site à site. 30
2.2.4 VPN poste à poste. 31
2.3.1 Structure d'un paquet PPTP contenant un datagramme IP. 33
2.3.2 Structure d'un paquet L2TP contenant un datagramme IP. 34
2.3.3 Principe de fonctionnement d'IPSec. 37
2.3.4 IPSec, mode transport et mode tunnel. 39

3.3.1 Organigramme du district GPL Béjaïa. 46
3.4.1 Organigramme du département informatique. 49
3.5.1 Architecture du réseau étendu des districts GPL de NAFTAL. 50
3.5.2 Architecture réseau du district GPL de Béjaïa. 52
3.5.3 Quelques équipements du réseau de GPL Béjaïa. 55

4.1.1 L'espace de travail GNS3. 61
4.1.2 Création d'un nouveau projet sous GNS3. 62
4.1.3 L'ajout des IOS. 63
4.1.4 L'ajout d'une machine virtuelle à la topologie GNS3. 64

4.2.1 Schéma idéalisé. 66
4.2.2 Schéma réel. 67
4.3.1 Capture d'un échange de données non sécurisé entre SITE1 et SITE2. . . 70
4.4.1 Affichage des connexions cryptées actives. 77
4.4.2 Affichage des types d'encodage actifs. 78
4.4.3 Affichage en détails de la SA IPSec. 79
4.4.4 Affichage des routes crées. 80
4.4.5 Affichage de la SA ISAKMP. 80
4.4.6 Affichage des `crypto map`. 81
4.4.7 Capture d'un échange de données sécurisé entre SITE1 et SITE2. 81

A.1 Cycle de vie d'audit de sécurité. 87

B.1 Lancement de VirtualBox. 89
B.2 Guide de création d'une machine virtuelle. 90
B.3 Guide de création d'une machine virtuelle-Paramètres. 91

Liste des tableaux

4.1 Caractéristiques des deux routeurs. 65
4.2 Liste des paramètres de sécurité pour IKE. 72
4.3 Description des étapes de configuration de la SA ISKAMP. 73
4.4 Liste des transformations disponibles. 74
4.5 Description des étapes de configuration de la crypto map. 76

Liste des abréviations

ACK (ACKnowledgement)

ACL (Access Control List)

AH (Authentication Header)

ATM (Asynchronous Transfer Mode)

CLI (Command-Line Interpreter)

DHCP (Dynamic Host Configuration Protocol)

DMZ (DeMilitarized Zone)

ESP (Encapsulating Security Payload)

FAI (Fournisseurs d'Accès à Internet)

GRE (Generic Routing Encapsulation)

HIDS (Host Intrusion Detection System)

HTTP (Hypertext Transfer Protocol)

ICMP (Internet Control Message Protocol)

IETF (Internet Egineering Task Force)

IKE (Internet Key Exchange)

IOS (Internetwork Operating Systems)

IP (Intenet Protocol)

IPSec (Internet Protocol Security)

ISAKMP (Internet Security Association and Key Management Protocol)

L2F (Layer Two Forwarding)

L2TP (Layer Two Tunneling Protocol)

LAN (Local Area Network)

MPPE (Microsoft Point-to-Point Encryption)

Ms-Chap2 (Microsoft Challenge Handshake Authentification Protocol v.2)

NIDS (Network Intrusion Detection System)

NVRAM (No Volatil Random Access Memory)

OS (Operating Systems)

OSI (Open System Interconnection)

Ping (Packet InterNet Groper)

PPP (Point to Point Protocol)

PPTP (Point to Point Tunneling Protocol)

RAM (Random Access Memory)

RFC (Request for Comments)

SA (Security Association)

SAD (Security Association Database)

SMTP (Simple Network Management Protocol)

SPD (Security Policy Database)

SPI (Security Parameter Index)

SSL (Secure Socket Layers)

SSL (Secure Socket Layers)

SYN (SYNcronize)

TCP (Transmission Control Protocol)

UDP (Transmission Control Protocol)

VLAN (Virtual Local Area Network ou Réseau Local Virtuel)

VPN (Virtual Private Network)

WAN (Wide Area Network)

WIFI (WIreless Fidelity Internet)

Introduction

Cadre général

Les systèmes informatiques et les réseaux sont devenus des outils indispensables pour la société actuelle. Ils sont aujourd'hui déployés dans tous les secteurs professionnels. Initialement, isolés les uns des autres, ces systèmes informatiques sont devenus interconnectés et le nombre de points d'accès ne cesse de croître.

Ce développement phénoménal a permis la construction d'une infrastructure mondiale de communication, l'Internet. De nos jours, Internet assure la communication entre les différents sites d'une même entreprise ou entre différentes entreprises. Pourtant, l'utilisation de ce réseau public pour échanger des données sensibles et confidentielles pose problème.

À l'heure actuelle les entreprises doivent désormais faire face à un nombre croissant d'utilisateurs. Que ce soit des concessionnaires, télétravailleurs ou autres. Mais aussi à des sites distants tels les filiales qui ont besoin d'accéder à leurs informations. Où que résident celle ci et quelle que soit la méthode pour les récupérer, les entreprises ont besoin d'un accès sécurisé, fiable et à un prix faible.

De plus, Internet est de plus en plus utilisé par les entreprises et véhicule donc des données sensibles. Contrôler strictement l'accès au site ne suffit plus, il est nécessaire de sécuriser les données en transit sur Internet à destination d'autres sites de l'intranet, afin d'empêcher qu'elles ne soient interceptées ou corrompues sur le réseau. Justement, le district NAFTAL GPL de Béjaia a souhaité faire évoluer son architecture WAN afin de mieux servir sa filiale, et ses utilisateurs en termes d'accès aux ressources de l'entreprise situées sur le siège de la direction générale à Alger.

Objectifs

‹Même si la sécurité informatique ne se limite pas à celle du réseau, il est indéniable que la plupart des incidents de sécurité surviennent par les réseaux, et vise les réseaux›[1]. Il est donc important d'implémenter des mécanismes et des solutions sûres permettant de configurer automatiquement un réseau informatique de sorte que son comportement soit conforme à une politique de sécurité donnée. C'est dans cet axe d'étude que se situe notre travail.

En effet, à travers ce présent mémoire notre travail vise à proposer une solution de sécurité pour permettre l'interconnexion de deux réseaux locaux de NAFTAL d'une manière fiable et à moindre coût.

Organisation du mémoire

Après l'introduction générale, le premier chapitre sera une synthèse de l'état de l'art sur la sécurité informatiques et les différents outils et techniques de sécurisation d'un réseau informatique.

Dans le second chapitre nous allons présenter les réseaux privés virtuels (VPNs) ainsi que les protocoles utilisés pour leur mise en œuvre.

Dans le troisième chapitre nous allons présenter l'organisme d'accueil et l'étude effectuée durant notre stage au sein de ce dernier.

Le quatrième chapitre décrit la partie pratique de notre travail, dans lequel nous allons présenter l'environnement de travail ainsi que le cas d'étude qui consiste à faire une simulation d'une transmission sécurisée de données entre de site distant, et définir les différentes configurations réalisées.

Enfin, nous terminerons ce mémoire par le chapitre présentant nos conclusions ainsi que les perspectives de ce travail.

État de l'art

« La vie n'est qu'un éclair, et un jour de réussite est un jour très chèr. »"

(Proverbe français)

Chapitre 1

La sécurité informatique

Introduction

Les réseaux informatiques deviennent de plus en plus complexes, dynamiques et hétérogènes. Cette situation a d'énormes conséquences sur leur sécurité. En effet, comme tout système informatique, un réseau doit assurer la confidentialité, l'intégrité et la disponibilité de ses données. Cet objectif justifie à lui seul la nécessité d'accorder une attention particulière à la sécurisation des réseaux informatiques. Il faut notamment protéger l'accès et la manipulation des données et autres ressources du réseau par des mécanismes d'authentification, d'autorisation et de contrôle d'accès. Toutefois, il est estimé que la plupart des malveillances informatiques ont une origine ou complicité interne aux organismes. Devant une telle spécificité il est donc essentiel d'élaborer une politique de sécurité et la mettre en œuvre dès la conception même des infrastructures.

La sécurisation d'un réseau nécessite un long processus qui remonte jusqu'à la conception de son architecture. Comme tout système complexe, la conception d'un réseau d'ordinateurs nécessite une attention particulière afin de mettre en œuvre une politique globale de sécurité. Il faudra notamment choisir les dispositifs appropriés et les placer aux bons endroits. Parmi ces dispositifs, on peut citer les pare-feu et les systèmes de détection et de prévention d'intrusions (IDS/IPS).

Dans ce chapitre, nous étudions quelques notions de la sécurité informatique. Nous commençons par décrire les différents aspects de la sécurité d'un réseau et définir la notion de politique de sécurité avant d'explorer plusieurs stratégies permettant de la

mettre en œuvre. Nous verrons notamment les dispositifs cités ci-haut ainsi que différents mécanismes de segmentation.

1.1 Quelques définitions

D'une manière générale le système d'information concerne l'ensemble des moyens (organisation, acteurs, procédures et systèmes informatiques) nécessaires à l'élaboration, au traitement, au stockage, à l'acheminement et à l'exploitation des informations. L'essentiel du système d'information est porté par le système informatique et donc assurer la sécurité de l'information implique d'assurer la sécurité des systèmes informatiques.

1.1.1 La sécurité informatique

La sécurité informatique est le domaine de l'informatique qui analyse les propriétés de sécurité des systèmes informatiques. Elle a pour but la protection des ressources matérielles et logicielles (incluant les données et les programmes) d'un système informatique contre la révélation, la modification, ou la destruction accidentelle ou malintentionnée.

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles portant sur celui-ci, et donc de connaître et de prévoir la façon de procéder de ces menaces et ensuite la mise en œuvre des mécanismes de sécurité qui permettent de minimiser la vulnérabilité d'un système informatique contre ces menaces[2].

1.1.2 Menace

La menace (en anglais « *threat* ») représente le type d'action susceptible de nuire dans l'absolu. Les menaces sont caractérisées par les possibilités et les probabilités d'attaque contre la sécurité. Elles engendrent des risques et des coûts humains et financiers : perte de confidentialité de données sensibles, indisponibilité des infrastructures et des données, etc. Les risques peuvent se réaliser si les systèmes menacés présentent des vulnérabilités[3, 4].

1.1.3 Vulnérabilité

La vulnérabilité (en anglais « *vulnerability* », appelée parfois faille ou brèche) est une faute de conception ou de configuration du système informatique, intentionnelle ou accidentelle, qui favorise la réalisation d'une menace ou la réussite d'une attaque[5].

1.1.4 Attaque

Une attaque est une action visant à violer une ou plusieurs propriétés de sécurité des systèmes informatiques. C'est l'exploitation d'une faille d'un système informatique (système d'exploitation, réseau, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables[5].

1.1.5 Intrusion

Une intrusion est définie comme une faute malveillante interne d'origine externe, résultant d'une attaque qui a réussi à exploiter une vulnérabilité. Elle est susceptible de produire des erreurs pouvant provoquer une défaillance vis-à-vis de la sécurité, c'est-à-dire une violation de la politique de sécurité du système.

Le terme d'intrusion sera employé dans le cas où l'attaque est menée avec succès et où l'attaquant a réussi à introduire et/ou compromettre le système[6].

1.1.6 Contre-mesure

La contre-mesure est l'ensemble des actions mises en œuvre en prévention de la menace[6].

1.1.7 Risque

Les risques sont le résultat de la combinaison des menaces et des vulnérabilités. Ils doivent être évalués, soit pour obtenir le meilleur compromis possible entre sécurité et coût pour un système donné, soit simplement pour calculer le montant des primes d'assurance pour couvrir ces risques.

Le risque en termes de sécurité est généralement caractérisé par l'équation suivante [3, 7] :

$$Risque = (Menace * Vulnérabilité)/Contre - mesure.$$

1.2 Propriétés de la sécurité informatique

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources d'un système d'information sont uniquement utilisées dans le cadre prévu. L'objectif est d'assurer que ces ressources aient les 5 propriétés suivantes [8] : la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation.

- **La confidentialité :** Les données ne doivent être visibles que par les personnes autorisées. C'est le fait de ne pas divulguer des informations sensibles propres à l'entreprise.
- **L'intégrité :** Il faut pouvoir garantir que les données protégées n'ont pas été modifiées par une personne non autorisée. Le but étant de ne pas altérer les informations sensibles de l'entreprise.
- **La disponibilité :** Les données doivent rester accessibles aux utilisateurs. C'est la capacité à délivrer un service permanent à l'entreprise.
- **L'authentification :** S'assurer qu'une entité ou un processus est bien celui qu'il prétend être.
- **La non répudiation :** On doit pouvoir certifier avec certitude quand un fichier a subi des modifications par la personne qui l'a modifié.

1.3 Politique de sécurité

La sécurité des systèmes informatiques se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leur ont été octroyés.

Les mécanismes de sécurité mis en place peuvent néanmoins provoquer une gêne au niveau des utilisateurs et les consignes et règles deviennent de plus en plus compliquées au fur et à mesure que le réseau s'étend. Ainsi, la sécurité informatique doit être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute

confiance.

C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité, dont la mise en œuvre se fait selon les quatre étapes suivantes [9] :

- Identifier les besoins en terme de sécurité, les risques informatiques pesant sur le système d'information et leurs éventuelles conséquences.
- Élaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés.
- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés.
- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace.

Le but d'une politique de sécurité est de définir les droits d'accès des utilisateurs, les actions autorisées et celles qui ne le sont pas au niveau d'un système d'information. Elle est constituée par l'ensemble des lois, règles et pratiques qui régissent le traitement des informations sensibles et l'utilisation des ressources par le matériel et le logiciel d'un système.

1.4 Domaines d'application de la sécurité informatique

La sécurité d'un système informatique est comparée régulièrement à une chaîne en expliquant que le niveau de sécurité d'un système est caractérisé par le niveau de sécurité du maillon le plus faible. Ainsi, une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue.

Cela signifie que la sécurité doit être abordée dans un contexte global. En effet tous les domaines de l'informatique sont concernés par la sécurité d'un système d'information. En fonction de son domaine d'application, la sécurité informatique se décline en : sécurité physique, sécurité de l'exploitation, sécurité logique, sécurité applicative et sécurité des télécommunications[10].

1.4.1 Sécurité physiques

Elle concerne tous les aspects liés à l'environnement dans lequel les systèmes se trouvent. C'est la sécurité au niveau des infrastructures matérielles : salles sécurisées, lieux

ouverts au public, postes de travail des personnels, alimentation électrique, climatisation, etc.

Mesures pour la sécurité physique :

- Respect de normes de sécurité.
- Protection de l'environnement contre les accidents (incendie, température, humidité, ...).
- Protection des accès physiques.
- Application de la redondance physique.
- Mise en œuvre d'un plan de maintenance préventive (ex. test) et corrective (ex. pièce de rechange), etc.

1.4.2 Sécurité de l'exploitation

Elle concerne la sensibilisation des utilisateurs aux problèmes de sécurité. Elle vise le bon fonctionnement des systèmes. Cela comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic et de mise à jour.

Mesures pour la sécurité d'exploitation :

- Mise en œuvre d'un plan de sauvegarde, de secours, de continuité et de tests.
- Application des inventaires réguliers et si possible dynamiques.
- Gestion du parc informatique, des configurations et des mises à jour.
- Contrôle et suivie de l'exploitation, etc.

1.4.3 Sécurité logique

Elle concerne la sécurité au niveau des données, notamment les données du système d'information, les applications ou encore les systèmes d'exploitation. Elle fait référence à la réalisation de mécanismes de sécurité par logiciel.

Mesures pour la sécurité logique :

- Mise en œuvre d'un système de contrôle d'accès logique s'appuyant sur un service d'authentification, d'identification et d'autorisation.
- Mise en place des dispositifs pour garantir la confidentialité dont la cryptographie.
- Gestion efficace des mots de passe et des procédures d'authentification.
- Mise en place des mesures antivirus et de sauvegarde d'informations sensibles, etc.

1.4.4 Sécurité applicative

L'objectif est d'éviter les ‹bugs› dans les applications.

Mesures pour la sécurité applicative :

- Application d'une méthodologie de développement des applications.
- Assurance de la robustesse des applications.
- Réalisation de contrôles programmés et des jeux de test.
- Mise en œuvre d'un plan de migration d'applications critiques.
- Mise en œuvre d'un plan d'assurance de sécurité, etc.

1.4.5 Sécurité des télécommunications

Elle concerne les technologies réseau, les serveurs de l'infrastructure, les réseaux d'accès, etc. Elle permet d'offrir à l'utilisateur final une connectivité fiable et de qualité de « bout en bout ».

Mesures pour la sécurité applicative :

- La mise en œuvre d'un canal de communication fiable entre les correspondants, quels que soit le nombre et la nature des éléments intermédiaires. Cela implique la réalisation d'une infrastructure réseau sécurisée au niveau des accès, des protocoles de communication, des systèmes d'exploitation et des équipements.

1.5 Attaques portantes atteinte à la sécurité informatique

Une attaque peut être définie comme toute action ou ensemble d'actions qui peut porter atteinte à la sécurité des informations d'un système ou réseau informatique. Étant donné le nombre important d'attaques possibles, nous allons d'abord commencer par les classer puis nous en présenterons quelques-unes[11].

1.5.1 Classification des attaques

Malgré la diversité des attaques de sécurité, nous retiendrons quatre classifications possibles.

Première classification

Un système informatique peut être attaqué :

- Soit par des utilisateurs internes, dans le but d'abuser de leurs droits et privilèges, on parlera alors d'attaques internes .
- Soit par des utilisateurs externes qui essayent d'accéder à des informations ou ressources de manière illégitime et non autorisée et dans ce cas on parlera d'attaques externes.

Deuxième classification

C'est la classification la plus classique, elle regroupe quatre types d'attaques. Ainsi une attaque peut porter atteinte à :

- La confidentialité des informations en brisant des règles privées.
- L'intégrité, en altérant les données.
- L'authenticité des données.
- La disponibilité, en rendant un système ou réseau informatique indisponible. On parle alors d'attaque de déni de service.

Troisième classification

Elle identifie deux types d'attaques :

– Les attaques passives.
– Les attaques actives.

Les attaques passives regroupent les attaques portant atteinte à la confidentialité. Elles ne sont pas facilement détectables car elles n'impliquent aucune altération des informations. Il en existe deux types :

– La lecture de contenus de messages confidentiels : courrier électronique, fichier transféré.
– L'analyse de trafic pour déterminer la nature d'une communication : identité des "*hosts*" communiquants, fréquence et longueur des messages échangés.

Les attaques actives concernent celles qui entraînent une modification des données ou création de données incorrectes. Autrement dit, celles qui portent atteinte à l'intégrité, l'authenticité et la disponibilité. On retrouve alors quatre types d'attaques actives :

– L'usurpation : c'est lorsqu'une entité se fait passer pour une autre.
– Le rejeu : retransmission de messages capturés lors d'une communications, et cela à des fins illégitimes.
– La modification de messages.
– Le déni de service.

Quatrième classification

Les attaques de sécurité peuvent également être classées en termes :

– D'attaques réseaux : leur but principal est d'empêcher les utilisateurs d'utiliser une connexion réseau, de rendre indisponible une machine ou un service et de surveiller le trafic réseau dans le but de l'analyser et d'en récupérer des informations pertinentes.
– D'attaques systèmes : ce sont des attaques qui portent atteinte au système, comme par exemple effacer des fichiers critiques (tel que le fichier "*password*") ou modifier la page web d'un site dans le but de le discréditer ou tout simplement le ridiculiser.

1.5.2 Description d'attaques

Dans la littérature, nous retrouvons un très grand nombre d'attaques, dans le cadre de ce mémoire nous nous limiterons à une brève description de quelques-unes d'entre elles[11].

Attaques réseaux

- ***IP spoofing*** **:** l'*IP spoofing* est l'action d'envoyer des paquets avec une autre adresse source que celle de l'expéditeur réel afin de laisser le serveur croire que les paquets proviennent d'une autre machine, de préférence une machine à qui il est permis d'établir une connexion. En d'autres termes, l'agresseur change l'adresse de sa machine pour faire croire qu'il est un client certifié par le serveur. Le but de cette attaque est de se faire passer pour un client certifié afin d'obtenir des droits d'accès et surtout un accès *root*.
- ***ICMP flooding*** **:** connue aussi sous le nom de "*Smurf attack*", est une attaque récente et très dangereuse. Son principe est d'envoyer un grand nombre de paquets ICMP "*echo request*" (qui sont essentiellement des requêtes "*ping*") dont l'adresse IP de destination est une adresse "*broadcast*" du réseau cible. Son but est de noyer ainsi le réseau et de le rendre indisponible. En effet, lorsque le routeur reçoit les paquets ICMP, il les diffuse sur toutes les machines du réseau en congestionnant ainsi le réseau, vu l'importance du trafic. De plus, l'adresse source est souvent modifiée et remplacée par l'adresse d'une autre machine, qui sera à son tour victime car elle recevra toutes les réponses "*ICMP reply*" engendrées par les paquets ICMP "*echo request*". Il existe un cousin de cette attaque, appelé "*fraggle attack*", qui utilise le même principe que l'*ICMP flooding*, sauf qu'au lieu que cela soit des paquets "*ICMP echo*", se sont des paquets "*UDP echo*".
- ***TCP SYN flooding*** **:** elle est également connue sous le nom de "*SYN attack*". Son objectif est de rendre indisponible un service TCP offert sur une machine. Le principe de cette attaque est de créer des connexions TCP semi-ouvertes sur la machine cible afin de remplir la file d'attente où sont stockées les demandes d'ouverture de connexions. L'attaquant envoie un grand nombre de requêtes SYN à la machine cible et remplace son adresse source avec l'adresse d'une machine indisponible ou inexistante afin que les réponses SYN/ACK ne soient jamais reçues et que donc les messages ACK ne soient jamais générés, ce qui signifie que la file d'attente restera pleine. Les conséquences de cette attaque est que toutes les requêtes arrivant sur le port TCP cible seront ignorées et de ce fait le service fourni sur ce port sera indisponible. Dans certains cas, la machine peut aussi devenir indisponible.

- ***Doorknob Rattling* :** elle se traduit par des essais répétés de "*login*" (*login / password*) sur plusieurs machines différentes dans le but d'obtenir un accès à un compte.
- ***Ping of Death* :** cette attaque se traduit par l'envoie de paquets IP dont la taille excède la longueur maximale (*65507 octets*) autorisée par le protocole IP. Ce qui rendra indisponible la machine cible.
- ***Sniffing* :** elle se traduit par l'observation et l'analyse du trafic réseau. Son but est d'obtenir des informations pertinentes afin de préparer d'autres attaques.

Attaques systèmes

- **Virus et bombe logique :** un virus est un programme écrit dans le but de détruire un système (exemple effacer des disques, des fichiers pertinents, etc.), alors qu'une bombe logique est un programme conçu uniquement dans le but de détruire des activités lorsqu'elles sont lancées.
- **Vers :** c'est un agent autonome capable de se propager sans une action extérieure (programme ou personne) mais uniquement en utilisant les ressources d'une machine pour attaquer d'autres machines. L'exemple le plus célèbre est celui qui s'est produite en novembre 1988, lorsqu'un étudiant lança un programme sur Internet qui était capable de se développer par lui-même à travers le réseau de serveur. Huit heures après, 2000 à 3000 machines avaient été infestées et commençaient à tomber en panne.
- **Cheval de Troie :** c'est un programme qui se cache lui-même dans un autre programme apparemment au-dessus de tout soupçon. Quand la victime lance ce programme, elle lance par la même occasion le cheval de Troie caché. Un cheval de Troie peut par exemple, lorsqu'il est exécuté, ouvrir l'accès au système à des personnes particulières ou même à tout le monde.
- **Trappe :** c'est un point d'entrée dans un système informatique qui passe au-dessus des mesures de sécurité normales. La plupart du temps, c'est un programme caché qui est souvent activé par un évènement ou une action normale et dont le but est de fragiliser un système de protection ou même le rendre inefficace.
- **"Craquage" de mots de passe :** le moyen le plus classique, de "craquer" des mots de passe est d'utiliser un programme appelé "*cracker*". Ce programme utilise un

dictionnaire de mots et de noms propres et opère sur les mots de passe encryptés, qui se trouvent dans un fichier (par exemple le fichier *UNIX /etc/passwd*).

1.6 Les mécanismes de défense et de sécurité

Un mécanisme est un moyen pour la mise en œuvre de la politique. La sécurité ne doit jamais reposer sur un seul mécanisme de sécurité. Une imbrication de mécanismes offre une garantie de sécurité bien supérieure.

1.6.1 Les défenses logicielles

Tous les systèmes de défense utilisent des programmes ou des algorithmes pour gérer essentiellement l'authentification, le cryptage des données et la détection de malwares. Ces défenses logicielles sont mises en place sur des architectures matérielles.

1.6.1.1 Le cryptage

Cryptographie est une science mathématique dans laquelle on fait les études des méthodes permettant de transmettre des données de manière confidentielle. Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible, c'est ce qu'on appelle le chiffrement, qui, à partir d'un texte clair, donne un texte chiffré ou cryptogramme. Inversement, le déchiffrement est l'action qui permet de reconstruire le texte en clair à partir du texte chiffré. Dans la cryptographie moderne, les transformations en question sont des fonctions mathématiques, appelées algorithmes cryptographiques, qui dépendent d'un paramètre appelé clé[12].

1.6.1.2 La signature numérique

La signature électronique permet d'identifier et d'authentifier l'expéditeur des données. Elle permet en outre de vérifier que les données transmises sur le réseau n'ont pas subi de modification.

Différentes techniques permettent de signer un message à envoyer. L'une d'elles fait appel aux algorithmes à clé publique, mais les plus utilisées sont les fonctions de hachage

– **Le hash :** Un algorithme de hachage est une fonction mathématique qui converti une chaine de caractères d'une longueur quelconque en une chaine de caractères de taille fixe appelée empreinte ou hash ou encore digest. Cette fonction possède deux propriétés essentielles :

1. Elle est irréversible : il est impossible de retrouver le message lorsqu'on connait le hash.
2. Elle est résistante aux collisions : deux messages différents ne produiront jamais le même hash.

Ce type de fonction cryptographique est conçu de façon qu'une modification même infime du message initial entraîne une modification du hash. Si un message est transmis avec son hash, le destinataire peut vérifier son intégrité en recalculant son hash et en le comparant avec le hash reçu[12].

1.6.1.3 Les certificats

Une difficulté qui s'impose à la station d'un réseau qui communique avec beaucoup d'interlocuteurs consiste à se rappeler de toutes les clés publiques dont elle a besoin pour récupérer les clés secrètes de session. Pour cela, il faut utiliser un service sécurisé et fiable, qui délivre des certificats. Un organisme offrant un service de gestion de clés publiques est une autorité de certification, appelée tiers de confiance. Cet organisme émet des certificats au sujet de clés permettant à une entreprise de les utiliser avec confiance.

Un certificat est constitué d'une suite de symboles et d'une signature[12].

1.6.1.4 Les antivirus

Sont des programmes qui permettent de détecter la présence de virus, vers ou chevaux de Troie sur un ordinateur et les supprimer. Éradiquer un virus est le terme utilisé pour nettoyer un ordinateur. Il existe plusieurs méthodes d'éradication : Nettoyer le fichier infecté en supprimant le code malveillant, la suppression du fichier infecté entièrement, et la mise en quarantaine du fichier infecté, qui consiste à le déplacer vers un endroit où il ne peut pas être exécuté. Les outils antivirus appliquent souvent des techniques de détection à base de signatures et présentent de nombreuses similitudes avec les systèmes de détection d'intrusions.

Les antivirus peuvent s'installer principalement en deux sortes d'endroits :

– Soit à l'entrée d'un réseau local, là où arrivent les flux en provenance de l'Internet, certains de ces flux seront filtrés pour y détecter des virus, essentiellement les flux relatifs aux protocoles SMTP (*Simple Network Management Protocol*) [1] et HTTP (*Hypertext Transfer Protocol*).
– Soit sur le poste de travail de l'utilisateur, et l'a l'antivirus servira généralement à inspecter et désinfecter le disque dur[10].

1.6.2 Les défenses Matérielles

Les défenses Matérielles interviennent au niveau de l'architecture du réseau, directement sur le support sur lequel est stockée l'information à protéger (protection d'une base de donnée centralisée sur le disque dur d'un serveur par exemple), sur les médias servant à transporter cette information (sécurisation du réseau WIFI) et sur les équipements intermédiaires traversées lors du transport (utilisation d'un firewall installer sur le retour d'accès).

1.6.2.1 Les pare-feu

Un pare-feu (*firewall*) est un dispositif utilisé pour empêcher les accès non autorisés à un réseau. Sa fonction est double : renforcer une politique de sécurité et journalier un trafic réseau. Le renforcement d'une politique de sécurité consiste à décider s'il faut accepter ou rejeter une connexion selon des règles spécifiques de filtrage permettant de forcer un réseau à se conformer à une politique donnée. La journalisation quant à elle, consiste à enregistrer tous les aspects du trafic afin de pouvoir mieux l'analyser. Un pare-feu est donc un composant clé pour la conception d'un réseau sécurisé. Cependant, étant un point de passage pour tout le trafic réseau, un pare-feu peut aussi être un unique point de défaillance. Par conséquent, son choix ainsi que son emplacement sont d'importantes tâches pour la sécurité des infrastructures réseau[13].

1. SMTP : *Simple Mail Transport Protocol* est le protocole d'échange de messages électroniques entre serveurs de messagerie, il est également utilisé par les logiciels de courrier électronique sur les postes de travail pour l'envoi des messages.

Types des pare-feu

1. **Filtrage de paquets** (*packet-filtering firewall*) : Un pare-feu de filtrage de paquets opère au niveau de la couche réseau. Il examine le contenu des paquets IP et filtre le trafic en fonction des adresses, ports et autres options des paquets. Le fait d'opérer au niveau réseau lui procure une performance assez élevée car le trafic réseau passe sans délai notable. Ce type de pare-feu est alors une excellente solution lorsque la performance est une exigence importante. Par exemple, la conception d'un réseau qui doit accueillir une application web telle qu'un site de *e-commerce*.
2. **Circuit de passerelles** (*circuit gateway firewall*) : Un pare-feu à circuit de passerelle opère au niveau de la couche transport. Il filtre également le trafic en fonction des adresses. Son principal objectif est de créer un circuit virtuel entre les hôtes source et destination afin d'avoir une connexion plus transparente. Cependant, sa mise en œuvre requiert des "*sockets*" pour garder une trace des connexions séparées.
3. **Application proxy** (*application-proxy firewall*) : Un pare-feu d'application de proxy œuvre au niveau application et contrôle toutes les connexions entrantes et sortantes du réseau. Si une connexion est autorisée, l'application-proxy l'initie vers l'hôte destination au nom de l'hôte source. Ce type de pare-feu est capable de s'assurer que le trafic qui le traverse est conforme à la politique de sécurité et que les fonctions au sein d'un protocole ou d'une application sont conformes aux politiques spécifiées.

Emplacement d'un pare-feu

Après le choix du pare-feu approprié, son emplacement nécessite également une attention particulière. Un pare-feu n'est pas une solution magique qui résoudra tous les problèmes de sécurité. Son emplacement doit être choisi selon les fonctions et objectifs envisagés.

Emplacement périphérique : Étant un dispositif qui doit empêcher tout accès non autorisé, un pare-feu est le plus souvent placé comme intermédiaire entre le réseau qu'il protège et l'extérieur. Cette disposition simple lui permet d'inspecter tout le trafic en provenance ou vers le réseau protégé.

Emplacement interne : Un pare-feu peut aussi être placé à l'intérieur d'un réseau pour le diviser en plusieurs sous-réseaux et contrôler les différents accès entre eux. Ainsi le

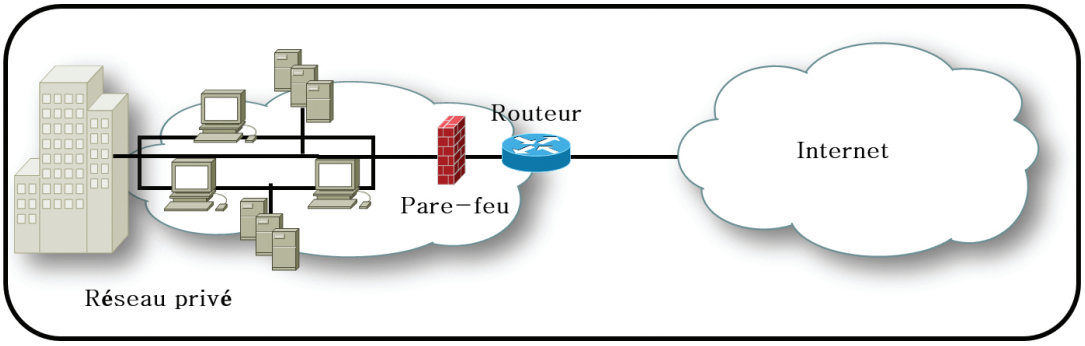


Figure 1.6.1 : Emplacement d'un pare-feu.

pare-feu fournit une protection interne entre les différents segments du réseau. Il peut être configuré pour octroyer des accès privilégiés ou restreintes. Une telle disposition nécessite une puissance de traitement élevée ainsi qu'un dispositif avec plusieurs interfaces. Ce qui est plus coûteux qu'un commutateur normal.

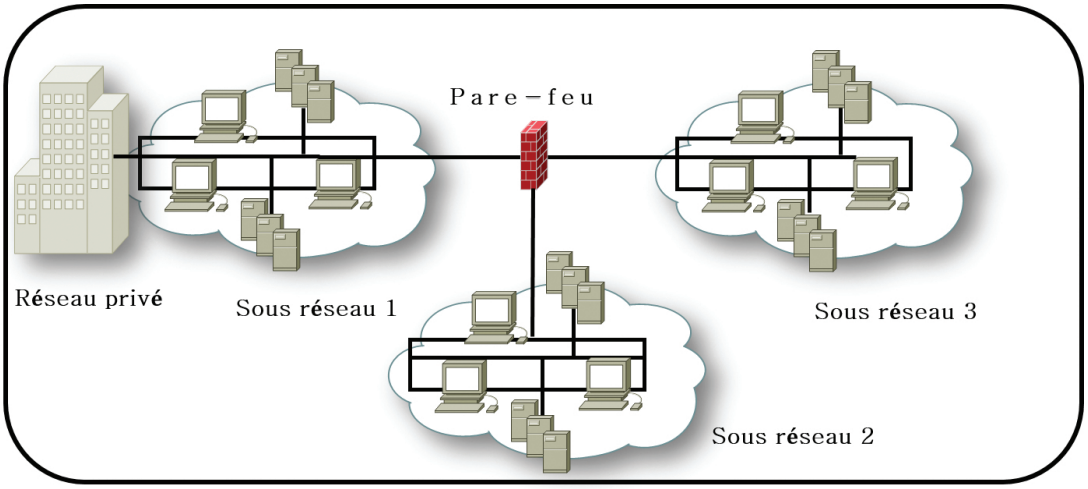


Figure 1.6.2 : Un pare-feu au centre d'un réseau.

1.6.2.2 Les systèmes de détection d'intrusion

Malgré la mise en place des pare-feu, les utilisateurs malveillants tentent de contourner les politiques de sécurité. Il est donc du ressort de l'administrateur d'analyser régulièrement l'état du système et de vérifier qu'il n'a pas été compromis. Cette tâche d'audit (Annexe A) suppose un mécanisme d'enregistrement des évènements du système au sein

de «journaux» et une phase d'analyse de ces journaux afin d'identifier d'éventuelles violations. La détection d'intrusion est née de la nécessité d'automatiser cette tâche d'audit des systèmes informatiques. Ainsi, les premiers systèmes de détection d'intrusions (IDS pour *Intrusion Detection Systems*) avaient pour objectif d'analyser le trafic réseau contre des modèles d'attaques connues et de déclencher une alarme lorsqu'un modèle est rencontré. L'administrateur peut ensuite élaborer un plan de défense contre l'éventuelle attaque. Mais la relative naïveté des algorithmes de détection conduit à un nombre élevé d'alertes, dont une bonne partie n'est constituée que de fausses alertes (faux positifs) alors que certaines intrusions ne sont pas détectées (faux négatifs) [2].

D'énormes améliorations ont été introduites et les nouveaux dispositifs produisent moins de fausses alertes. Dans certains cas, ils ont même la possibilité de stopper les intrusions. D'autres IDS vont plus loin dans la prévention en reconfigurant les listes de contrôle d'accès ACL [3] des routeurs et en implémentant dynamiquement la politique du pare-feu afin d'exclure les paquets suspects. Cette nouvelle génération d'équipements combine les fonctionnalités des IDS et des pare-feu, ce qui leur procure le nom de «Système de prévention d'intrusions» (IPS pour *Intrusion Prevention Systems*)[14].

Approches de détection d'intrusion

Les IDS/IPS utilisent principalement deux approches pour détecter une intrusion :

1. **Approche basée sur la connaissance :** Cette approche se base sur la connaissance des techniques employées par les attaquants. On en tire des scénarios d'attaque et on cherche leur éventuelles causes dans les traces d'audits. Cette technique fournit des informations précises sur la signature des intrusions. Cependant, la base de connaissance du système est à mettre à jour continuellement selon les dernières signatures. Elle est également source de faux négatifs car une attaque n'est détectée que lorsque sa signature est dans la base de connaissance.
2. **Approche basée sur le comportement :** Cette approche est fondée sur l'hypothèse qui consiste à définir le comportement normal de l'utilisateur et du système. Toute déviation ou action inhabituelle par rapport à ce comportement sera consi-

2. Un IDS est parfaitement fiable en absence de faux négatif, il est parfaitement pertinent en l'absence de faux positif.

3. ACL : *Access Control List*, elles permettent de filtrer le trafic qui entre ou sort par les interfaces d'un routeur, selon les adresse IP, les ports, ou bien les protocoles utilisés IP, TCP, UDP, ICMP.

dérée comme suspecte. Ainsi, une alerte est déclenchée lors qu'un nouveau comportement est détecté. Une telle approche peut détecter beaucoup d'intrusions mais n'est pas aussi précise que la base de connaissance et peut engendrer beaucoup de fausses alertes car elle ne supporte aucune déviation par rapport au comportement préalablement décrit. Ce qui peut résulter d'une simple évolution du système.

Emplacement des IDS/IPS

La position optimale pour un IDS/IPS dépend de ses fonctions et caractéristiques. Un IDS de surveillance passive a besoin d'une position lui permettant d'analyser le trafic réseau et de déclencher une alerte à travers un canal prédéfini tel qu'une console, un courriel, etc. La meilleure position d'un tel IDS est derrière le pare-feu et près des données protégées. Par contre, un IDS/IPS capable de stopper les attaques devrait être déployé entre le routeur et le pare-feu.

Les IDS sont classés selon le type de protection qu'ils fournissent. Ainsi, on peut distinguer un HIDS (*Host Intrusion Detection System*) qui surveille un seul poste d'un NIDS (*Network Intrusion Detection System*) qui contrôle le trafic de tout un réseau.

HIDS : Un HIDS est généralement un programme installé sur un hôte nécessitant une protection particulière. Il examine toutes les activités de l'hôte qu'il surveille et relève tout ce qui compromet sa sécurité pour le stopper ou pour déclencher une alerte.

Un HIDS s'exécute généralement sur un serveur. En effet, les données d'un serveur change constamment mais sa configuration et ses fonctions restent statiques tandis qu'un poste de travail peut changer à tout moment. Un tel poste n'est pas moins exposé qu'un serveur situé derrière un pare-feu, mais y installer un HIDS demeure un véritable challenge.

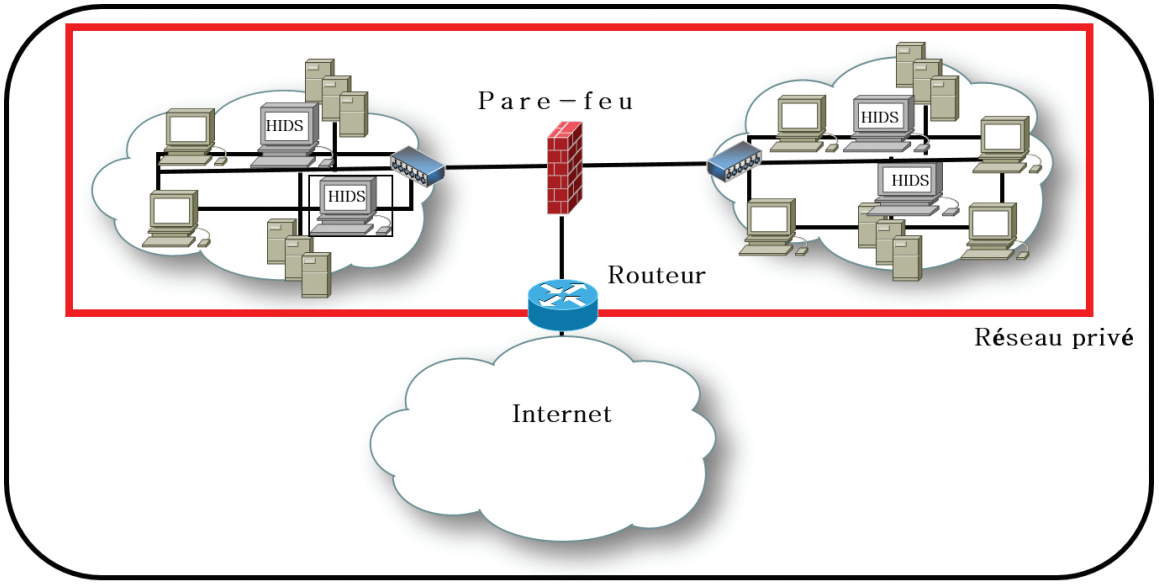


Figure 1.6.3 : Emplacement d'un HIDS.

NIDS : Un NIDS est habituellement un équipement connecté à un réseau pour surveiller le trafic. Il a besoin de voir ce trafic afin de pouvoir l'analyser. On peut donc le placer avant ou après le pare-feu périphérique.

1. **Avant le pare-feu :** Un NIDS placé avant le pare-feu peut voir toutes les attaques possibles survenant contre le réseau à partir du moment où elles commencent. Ce qui donne à l'administrateur un temps maximal pour réagir et empêcher tout dommage. En effet, un NIDS n'a pas besoin de console. L'administrateur réseau le configure directement à travers une interface de lignes-de-commande ou un navigateur web pour recevoir les alertes. Cependant, un NIDS placé avant le pare-feu signale des attaques que ce dernier peut facilement stopper. Ce qui entraîne beaucoup de fausses alertes.
2. **Après le pare-feu :** Pour signaler uniquement les attaques entrants dans le réseau protégé, un NIDS doit être placer après le pare-feu. Un tel emplacement permet également de détecter des attaques que le précédent manquerait. En effet, de nombreux réseaux ont des VPNs (*Virtual Private Networks*, réseaux privés virtuels) qui s'étendent jusque derrière leurs pare-feu. Ainsi, toute attaque acheminée par un client VPN compromis pourra contourner l'ensemble des pare-feu ainsi que le NIDS qui les devance. Limiter le VPN avant le pare-feu peut atténuer ce problème, mais

cela ouvre d'énormes trous sur la connexion VPN et le pare-feu aura de la difficulté à stopper les attaques. La meilleure solution serait alors de placer le NIDS entre le pare-feu et le réseau à protéger.

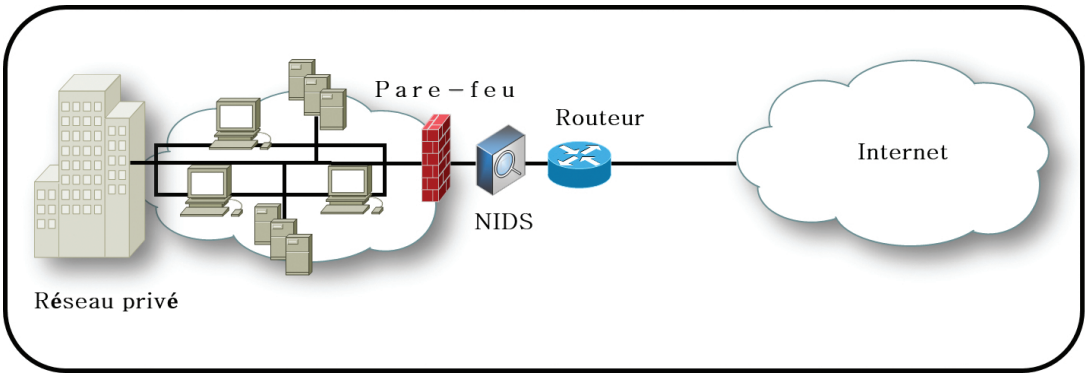


Figure 1.6.4 : Emplacement d'un NIDS.

Notons enfin qu'on n'a pas besoin de faire le choix entre un HIDS et un NIDS pour sécuriser un réseau. On devrait plutôt acquérir les deux à la fois.

1.6.2.3 Segmentation

La segmentation est une technique couramment utilisée pour atténuer la congestion d'un réseau. Cette technique consiste à diviser l'architecture du réseau en sections afin de réduire la taille des domaines de diffusion (*broadcast*) et ainsi augmenter l'efficacité du réseau. Cette technique peut aussi être utilisée pour augmenter la sécurité d'un réseau. En effet, elle permet d'implémenter des dispositifs de sécurité entre les frontières des différents segments. Ce qui permet de mieux contrôler le trafic en destination des ressources critiques.

La segmentation peut s'effectuer de plusieurs façons [13] :

1. **Segmentation par séparation physique :** La séparation physique des sous-réseaux est probablement la méthode de segmentation la plus sécurisée, mais elle est également la plus coûteuse en termes de cartes réseau, d'infrastructures de commutations additionnelles et intensifie l'administration.
2. **Segmentation avec des VLANs :** Un VLAN (*Virtual Local Area Network* ou Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de

façon logique et non physique. Il s'agit d'un dispositif de la couche 2 (liaison de données) qui fait ce que les VPNs font au niveau de la couche 3 (réseau). Le trafic au sein d'un VLAN ne peut traverser un autre sans passer par un routeur. Ce qui permet de segmenter un réseau sans infrastructures additionnelles. Cependant, la configuration des commutateurs reliant les différents segments est d'une importance capitale car la sécurité d'un VLAN dépend en partie de l'assignation des ports de ces commutateurs.

3. **Segmentation en fonction des services :** Une autre technique de segmentation est de considérer les services fournis par les différentes ressources et segmenter le réseau en conséquence. Chaque segment est alors définie selon le service fourni par ses ressources. Cette approche permet un contrôle très rigoureux entre les différents segments du réseau, mais elle peut mener à un grand nombre de segments dépendamment des services disponibles. Ce qui nécessite également des dispositifs de sécurités additionnels.
4. **Segmentation utilisant un DMZ :** Les administrateurs réseau se considèrent en guerre contre les attaquants et les utilisateurs même de leurs systèmes. Il n'est pas surprenant qu'ils empruntent alors des termes militaires comme DMZ (*DeMilitarized Zone*). Un DMZ désigne une zone tampon d'un réseau, située entre ce dernier et l'Internet (l'extérieur en général). Il s'agit d'un réseau intermédiaire protégé aussi bien contre l'extérieur que le réseau interne. Le but est de pouvoir y regrouper les ressources du réseau offrant des services accessibles de l'interne comme à l'externe afin d'éviter toute connexion directe au réseau. Ces ressources sont souvent des serveurs publics tels que serveur HTTP, serveur DHCP, etc. Tel que décrit ci-haut, un DMZ divise le réseau en deux. Ce principe est utilisé pour segmenter un réseau en mettant en place un ou plusieurs DMZ. La Figure qui suit montre un exemple de réseau segmenté avec un DMZ. Toutes les connexions passent par cette zone. Le pare-feu envoie tous les courriels entrants au proxy du serveur SMTP qui se fait passer pour le serveur réel de messageries pour des fins de filtrage ou d'autres fonctions. Si le proxy du serveur SMTP n'est plus fonctionnel, le réseau interne reste sous la protection du pare-feu.

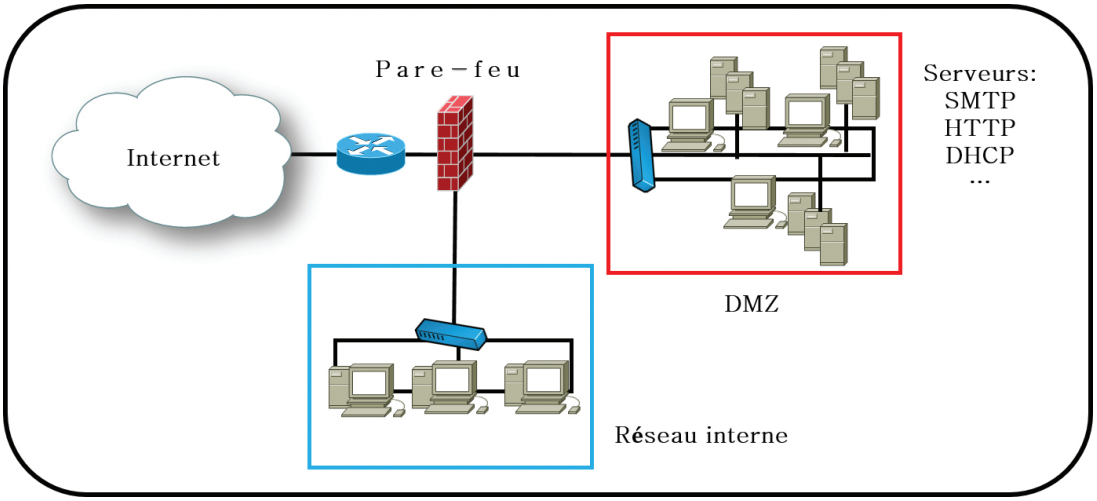


Figure 1.6.5 : Exemple de réseau segmenté avec un DMZ.

Conclusion

Dans ce chapitre, nous avons très rapidement évoqué les enjeux de la sécurité des réseaux afin de mettre en évidence la nécessité d'élaborer des politiques de sécurité complètes et cohérentes. La mise en place de telles politiques nécessite de penser à prévoir une architecture sécurisée dès la conception avec des redondances aux points stratégiques. Nous avons ainsi exploré plusieurs techniques de conception sécuritaire d'un réseau telles que les pare-feu, les systèmes de détection et de prévention d'intrusions et la segmentation. Le pare-feu est l'outil le plus utilisé pour sécuriser un réseau grâce à ses capacités de renforcer une politique de sécurité et d'enregistrer tous les aspects du trafic réseau. Il existe plusieurs types de pare-feu qui pouvant être placés à l'intérieur comme à la périphérique d'un réseau.

Bien qu'étant un puissant outil pour sécuriser un réseau, un pare-feu tout seul ne peut fournir la protection complète souhaitée. La sécurité d'un réseau ne doit pas se reposer sur un seul mécanisme. Une imbrication de mécanismes offre une garantie de sécurité bien supérieur, d'où la nécessité d'inclure des systèmes de détection et de prévention d'intrusion (IDS/IPS) afin de s'assurer d'une meilleur aptitude à détecter toute éventuelle intrusion. Ces IDS/IPS peuvent fonctionner selon une approche basée sur la connaissance ou une approche comportementale. Le déploiement des IDS/IPS devient de

plus en plus vaste grâce à leur capacité d'examiner les trafics réseau.

Enfin, pour éviter de concentrer la sécurité en un seul point et optimiser les performances du réseau en réduisant la taille des zones de diffusion (*broadcast*) et augmenter son efficacité, un réseau peut être segmenté en plusieurs sections en effectuant une séparation physique ou logique de ses composantes. Ainsi, on obtient un équilibre entre la sécurité, la vivacité, le coût et la commodité du réseau.

Chapitre 2

Les réseaux privés virtuels

2.1 Introduction

La présence grandissante d'Internet a considérablement modifié les modes de travail et de fonctionnement d'un grand nombre d'organisations. Pour garder une longueur d'avance face à la concurrence, un nombre accru d'organisations demandent à leurs employés de se connecter à des réseaux d'entreprise depuis des sites distants, qu'il s'agisse de leur domicile, de filiales, d'hôtels, de cybercafés ou des locaux d'un client. Ces connexions distantes sont généralement établies à l'aide des technologies de réseau privé virtuel.

Grâce aux connexions VPN, des employés ou des partenaires peuvent en toute sécurité se connecter au réseau local d'une entreprise sur un réseau public. Tout accès distant reposant sur des technologies VPN ouvre ainsi la voie à une large palette de nouvelles opportunités commerciales, notamment l'administration à distance et les applications haute sécurité. Un nombre considérable de groupes commerciaux et d'utilisateurs fait appel à des applications de productivité et d'administration qui exige un accès à distance régulier et fiable à des réseaux locaux d'entreprise.

2.2 Présentation d'un réseau privé virtuel

2.2.1 Définition

VPN (*Virtual Private Network*, RFC 4381 [1]) est une technique permettant à un ou plusieurs postes distants de communiquer de manière sure. C'est un environnement de communication dans lequel l'accès est contrôlé, afin de permettre des connexions entre une communauté d'intérêts seulement. Il est construit avec un partitionnement d'un média de communication commun, qui offre des services de façon non exclusive[15].

Un VPN assure divers objectives, et se caractérise par :

- Étanchéité du trafic entre les différents réseaux privés virtuels.
- La sécurité des communications qui est assurée à travers l'authentification des utilisateurs ou des données, ainsi que la confidentialité à travers le chiffrement effectué entre les données échangées.
- La mise en place d'une liaison VPN réduit les coûts liés à l'infrastructure réseau des entreprises.
- La mise en place d'une liaison VPN assure la qualité de service.

2.2.2 Rôle d'un VPN

Le rôle d'un réseau privé virtuel est de fournir un tunnel sécurisé de bout en bout entre un client et un serveur. Un VPN permet, entre autre, d'identifier et d'autoriser l'accès ainsi que de chiffrer tout trafic circulant dans le réseau.

L'utilisation d'un VPN est la manière la plus fiable de sécuriser un réseau. C'est aussi la méthode la plus utilisée[16].

2.2.3 Les fonctionnalités d'un réseau privé virtuel

Un VPN repose sur les principes fondamentaux de la sécurité informatique, en assurant la mise en œuvre de diverses fonctionnalités [16] :

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

1. RFC pour *Request for Comments*, Ce sont des documents indiquent les normes à respecter pour les communications sur Internet. Ils sont produits par l'IS (*Internet Society*) et sont gratuits.

actions effectuées sur le réseau doit être conservé.

- **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.

2.2.4 Principe de fonctionnement d'un VPN

Un VPN repose sur un protocole appelé protocole de *tunneling*. Ce protocole permet de faire circuler les informations de l'entreprise 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 leur entreprise[16].

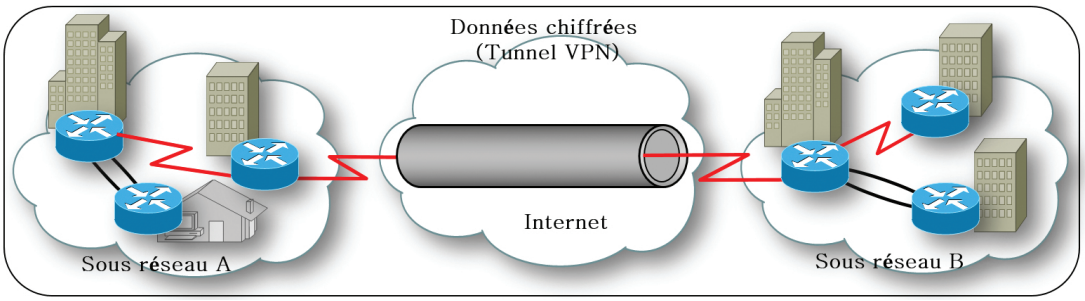


Figure 2.2.1 : Tunnel interconnectant les sous réseaux A et B, à travers Internet.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet.

2.2.5 Types des VPNs

Selon le mode d'utilisation, on distingue trois types d'architecture VPN [16] :

- Le VPN d'accès.
- L'intranet VPN.

– L'extranet VPN.

2.2.5.1 VPN d'accès (*host to LAN*)

Le VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur distant se sert d'une connexion Internet pour établir la connexion VPN, il sera connecté logiquement au réseau LAN de l'entreprise comme s'il l'était physiquement.

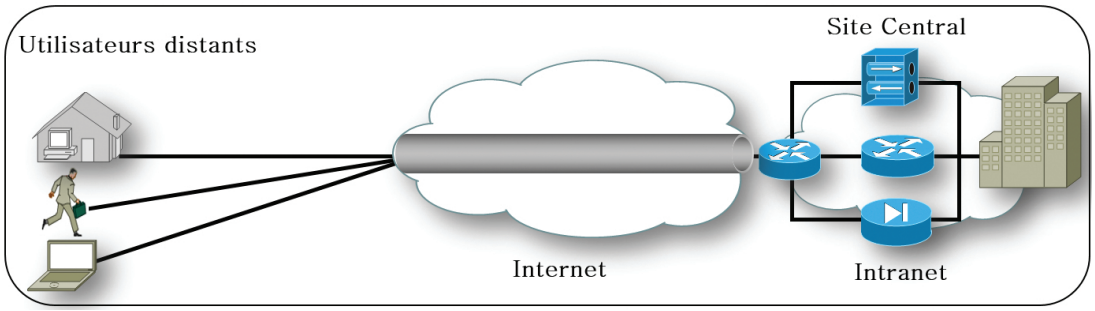


Figure 2.2.2 : VPN poste à site.

2.2.5.2 Intranet VPN (*LAN to LAN*)

L'intranet VPN est utilisé pour relier deux ou plusieurs intranets d'une même Entreprise entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Cette technique est également utilisée pour relier des réseaux d'entreprise, sans qu'il soit question d'intranet (partage de données, de ressources, exploitation de serveurs distants...).

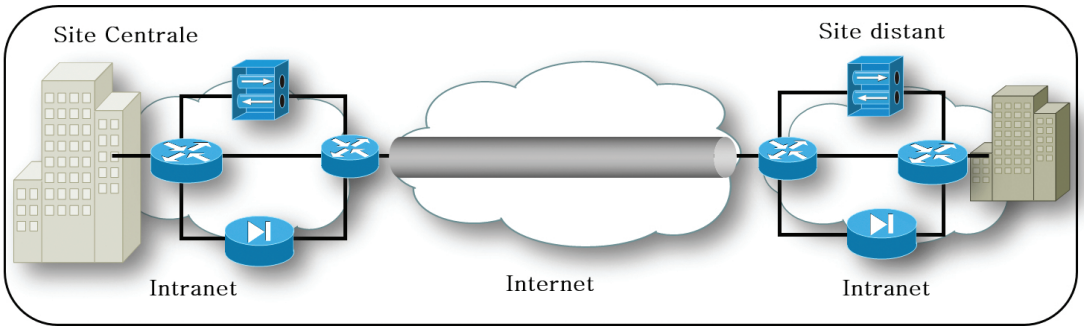


Figure 2.2.3 : VPN site à site.

2.2.5.3 Extranet VPN (*host to host*)

C'est le cas d'utilisation le plus simple. Il s'agit de mettre en relation deux serveurs. Le cas d'utilisation peut être le besoin de synchronisation de bases de données entre deux serveurs d'une entreprise disposant de chaque coté d'un accès Internet. L'accès réseau complet n'est pas indispensable dans ce genre de situation.

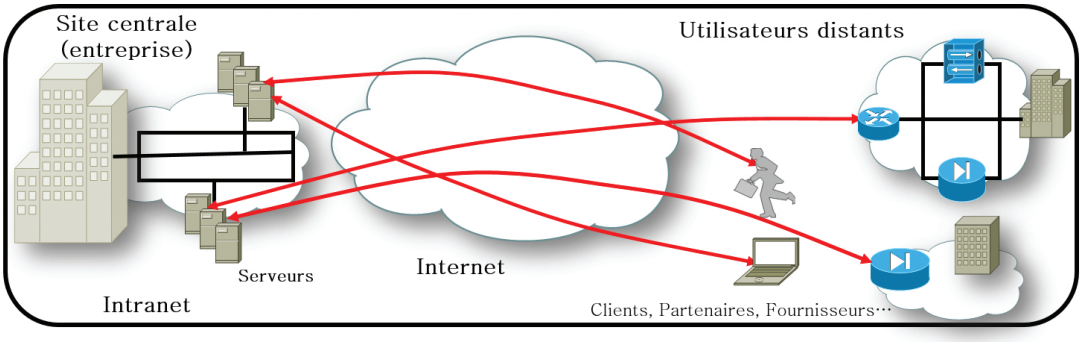


Figure 2.2.4 : VPN poste à poste.

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans ce cas, il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès. De plus, seul une partie des ressources sera partagée, ce qui nécessite une gestion rigoureuse des espaces d'échange.

2.3 Protocoles utilisés pour réaliser une connexion VPN

Les protocoles permettant un *tunneling* sécurisé se classent en deux catégories [17] :

- Les protocoles de niveau 2 comme PPTP (soutenu par Microsoft), L2F (développé par Cisco) et L2TP (évolution reprenant les avantages des 2 précédents), tous étant dépendants de PPP.
- Les protocoles de niveau 3 comme IPSec.
- À ces deux catégories peut s'ajouter le protocole SSL, de niveau 4, dans le cadre de VPN-SSL.

2.3.1 Le protocole PPP

PPP (*Point to Point Protocol*) est un protocole qui permet de transférer des données sur un lien synchrone ou asynchrone. Il est full duplex et garantit l'ordre d'arrivée des paquets. Il encapsule les paquets IP dans des trames PPP, puis transmet ces paquets encapsulés au travers de la liaison point à point. PPP est employé généralement entre un client d'accès à distance et un serveur d'accès réseau. Le protocole PPP est défini dans la RFC 2153.

PPP n'est pas un protocole permettant l'établissement d'un VPN mais il est principalement utilisé pour transférer les informations au travers d'un VPN, et sert comme support aux protocoles PPTP ou L2TP [17].

2.3.2 Le protocole PPTP

Point to Point Tunneling Protocol est défini par la RFC 2637. Microsoft a implémenté ses propres algorithmes afin de l'intégrer dans ses versions de Windows. PPTP est ainsi une solution très employée dans les produits VPN commerciaux à cause de son intégration au sein des systèmes d'exploitation Windows. PPTP est un protocole de niveau 2 qui permet l'encapsulation des données ainsi que leur compression. L'authentification se fait grâce au protocole Ms-Chap2 (*Challenge Handshake Authentification Protocol v.2*, RFC 2759) de Microsoft. Le cryptage s'effectue grâce au protocole MPPE (*Microsoft Point-to-Point Encryption*). Le protocole PPTP encapsule les trames PPP dans des datagrammes IP pour leur transmission sur le réseau. Il utilise une connexion TCP pour la gestion de tunnel et une version modifiée de GRE (*Generic Routing Encapsulation*, RFC 2784) pour encapsuler les trames PPP pour les données tunnelées. Les charges utiles des trames PPP encapsulées peuvent être chiffrées, compressées ou les deux en même temps. La figure suivante illustre la structure d'un paquet PPTP contenant un datagramme IP[17].

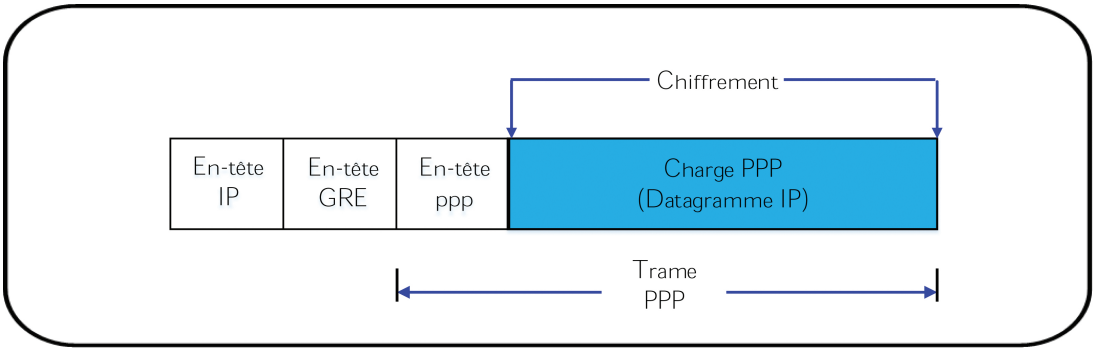


Figure 2.3.1 : Structure d'un paquet PPTP contenant un datagramme IP.

2.3.3 Le protocole L2F

Layer Two Forwarding est un protocole de niveau 2 qui permet à un serveur d'accès distant de véhiculer le trafic sur PPP et transférer ces données jusqu'à un serveur L2F (routeur). Ce serveur L2F désencapsule les paquets et les envoie sur le réseau. Il faut noter que contrairement à PPTP et L2PT, L2F n'a pas besoin de client. Ce protocole est progressivement remplacé par L2TP qui est plus souple[17].

2.3.4 Le protocole L2TP

L2TP (*Layer Two Tunneling Protocol*) est un protocole combinant les avantages du PPTP de Microsoft et du L2F de Cisco, ce protocole est décrit dans la RFC 2661 et a été créé par l'IETF (*Internet Egineering Task Force*) [2]. L2TP est aujourd'hui principalement utilisé par les FAI (Fournisseurs d'Accès à Internet).

Sur la base des spécifications des protocoles L2F et PPTP, Nous pouvons utiliser le protocole L2TP pour configurer des tunnels entre les réseaux concernés. À l'instar de PPTP, L2TP encapsule les trames PPP qui encapsulent ensuite les protocoles IP et permettent aux utilisateurs d'exécuter à distance des programmes qui sont tributaires de protocoles réseau déterminés[17].

2. Organisme de normalisation responsable de la conception de protocoles pour Internet. Les publications émises par l'IETF s'intitulent des RFC (*Request for Comments*).

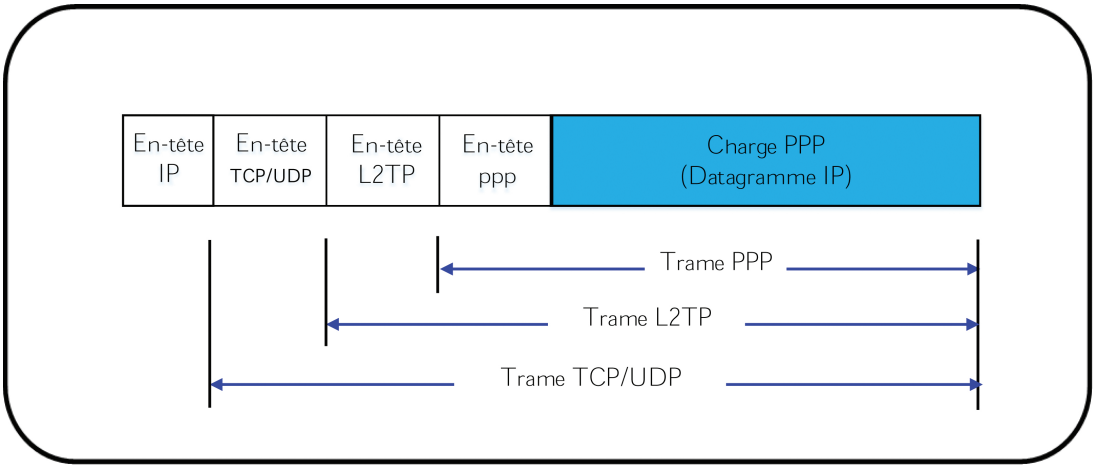


Figure 2.3.2 : Structure d'un paquet L2TP contenant un datagramme IP.

2.3.5 Le protocole IPSec

IPSec (*Internet Protocol Security*), définit par la RFC 2411, est un ensemble de protocoles pour sécuriser les communications IP et garantir le chiffrement, l'intégrité et l'authentification. Ce protocole spécifie les messages nécessaires pour sécuriser les communications du réseau privé tout en se basant sur les algorithmes existants[16].

Aujourd'hui, le protocole le plus utilisé pour la mise en place des VPNs est IPSec. Il est l'un des standards [3] les plus diffusé et le plus ouvert. Effectivement IPSec vise à sécuriser les échanges au niveau de la couche réseau.

Le réseau IPv4 étant largement déployé et la migration complète vers IPv6 nécessitent encore beaucoup de temps, il est vite apparu intéressant de définir des mécanismes de sécurité qui soient communs à la fois à IPv4 et IPv6. Ces mécanismes sont couramment désignés par le terme IPSec. Le protocole IPSec fournit ainsi [17] :

- Des mécanismes de confidentialité et de protection contre l'analyse du trafic.
- Des mécanismes d'authentification des données.
- Des mécanismes garantissants l'intégrité des données.
- Des mécanismes de protection contre le rejeu [4].

3. Organisme de normalisation responsable de la conception de protocoles pour Internet. Les publications émises par l'IETF s'intitulent des RFC (*Request for Comments*).

4. IPSec permet de se prémunir contre les attaques consistant à capturer un ou plusieurs paquets dans le but de les envoyer à nouveau (sans pour autant les avoir déchiffrés) pour bénéficier des même

– Des mécanismes de contrôle d'accès.

2.3.5.1 Architecture du protocole IPSec

IPSec repose en fait sur plusieurs protocoles différents dont certains existent à part entière hors d'IPSec qui lui offrent en retour une grande souplesse d'utilisation[18, 19] :

Le protocole initial et principal est le protocole IKE (*Internet Key Exchange*, RFC 2409). Appliqué à IPSec, ce protocole a pour objectif dans un premier temps d'établir un premier tunnel entre les deux machines (le tunnel IKE), que l'on pourra qualifier de tunnel administratif. C'est la phase 1 du protocole IKE. Ce protocole est dit administratif car il ne sert pas à la transmission des données utilisateur ; il est utilisé pour gérer les tunnels secondaires, leur création, le rafraîchissement des clés, etc... La phase 2 du protocole IKE consiste en effet à établir autant de tunnels secondaires que nécessaire pour la transmission des données utilisateur entre les deux machines. IKE est un protocole hybride qui implémente les échanges de clés dans le cadre ISAKMP (*Internet Security Association and Key Management Protocol*, RFC 2408).

Les tunnels destinés aux échanges de données vont s'appuyer sur deux protocoles différents suivant les besoins en sécurité des utilisateurs.

– Le premier est le protocole AH (*Authentication Header*, RFC 2402) qui vise à établir l'identité des extrémités de façon certaine. Il inclut un hachage du paquet IP et garantit l'intégrité. Bien que le contenu du datagramme ne soit pas chiffré, le destinataire est sûr que le contenu du paquet n'a subi aucune modification et que l'expéditeur a envoyé les paquets.
– Le deuxième protocole est le protocole ESP (*Encapsulating Security Payload*, RFC 2406) qui chiffre les données IP et obscurcit, par conséquent, le contenu des paquets lors de leur transmission (confidentialité). ESP garantit également l'intégrité des données par le biais d'une option d'algorithme d'authentification.

2.3.5.2 Association de Sécurité

Les mécanismes mentionnés ci-dessus font appel à la cryptographie et utilisent un certain nombre de paramètres (algorithmes de chiffrement utilisés, clefs, mécanismes sélectionnés...) sur lesquels les tiers communicants doivent se mettre d'accord. Afin de gérer

avantages que l'envoyeur initial.

ces paramètres, IPSec a recours à la notion d'association de sécurité (SA pour *Security Association*).

Une association de sécurité Ipsec est une connexion qui fournit des services de sécurité au trafic qu'elle transporte. On peut aussi la considérer comme une structure de données servant à stocker l'ensemble des paramètres associés à une communication donnée.

Une SA est unidirectionnelle, en conséquence, protéger les deux sens d'une communication classique requiert deux associations, une dans chaque sens. Les services de sécurité sont fournis par l'utilisation soit de AH soit de ESP. Si AH et ESP sont tout les deux appliqués au trafic en question, deux SA sont créées.

Chaque association est identifiée de manière unique à l'aide d'un triplet composé de :

- L'adresse de destination des paquets.
- L'identifiant du protocole de sécurité utilisé (AH ou ESP).
- Un index des paramètres de sécurité (SPI pour *Security Parameter Index*). Un SPI est un bloc de 32 bits inscrit en clair dans l'en-tête de chaque paquet échangé.

Tous ces éléments sont appelés sélecteurs et permettent d'identifier quelle SA s'applique à tel ou tel trafic. Néanmoins, la fonction primaire de la SA est d'indiquer quels traitements doivent être appliqués au trafic identifié précédemment. On distingue les éléments suivants [20] :

- Données et paramètres d'authentification : pour AH ou ESP, algorithmes, clés...
- Données et paramètres de confidentialité : pour AH ou ESP, algorithmes, clés...
- Données et paramètres d'anti-rejeu : nombres de séquence, compteurs divers, fenêtres d'anti-rejeu...
- Type d'en-tête IPSec : modes Transport, Tunnel ou les deux.
- Durée de vie de la SA : temps ou quantité maximale de données à protéger.

2.3.5.3 Base de données des associations de sécurité

Pour gérer les associations de sécurités actives, on utilise une base de données des associations de sécurité (SAD pour *Security Association Database*), qui contient tous les paramètres relatifs à chaque SA et sera consultée pour savoir comment traiter chaque paquet reçu ou à émettre[19].

2.3.5.4 Base de données des politiques de sécurité

Les protections offertes par IPSec sont basées sur des choix définis dans une base de données de politique de sécurité (SPD pour *Security Policy Database*). Cette base de données est établie et maintenue par un utilisateur, un administrateur système ou une application mise en place par ceux-ci. Elle permet de décider, pour chaque paquet, s'il se verra apporter des services de sécurité, s'il sera autorisé à passer ou rejeté[19].

2.3.5.5 Principe de fonctionnement

Le schéma ci-dessous représente tous les éléments présentés ci-dessus (en bleu), leurs positions et leurs interactions[19].

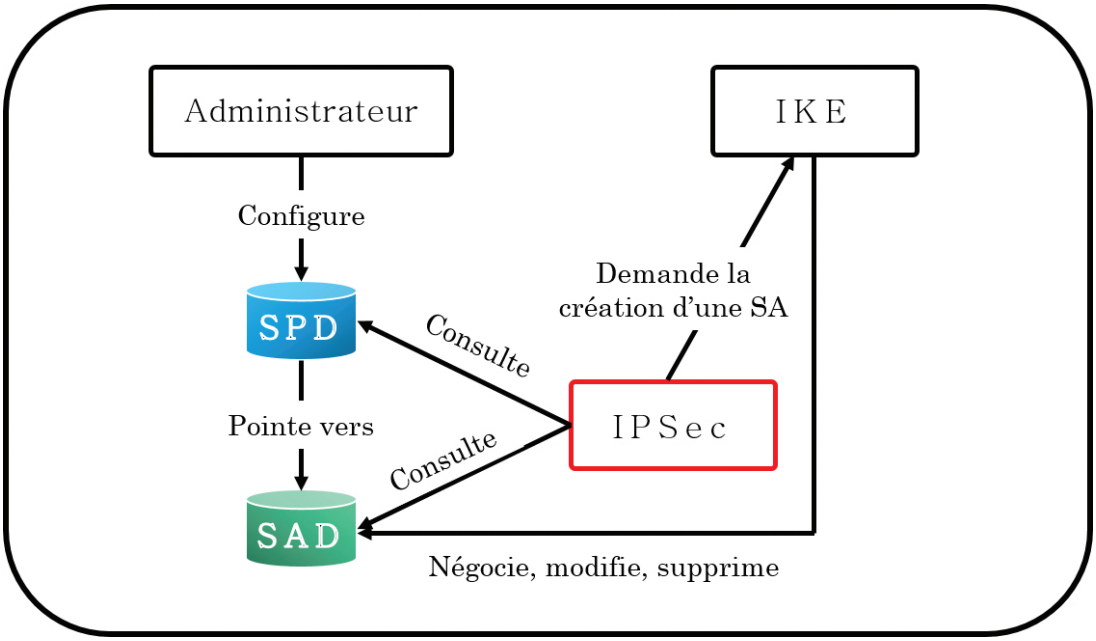


Figure 2.3.3 : Principe de fonctionnement d'IPSec.

On distingue deux scénarios :

1. **Scénario d'un trafic sortant :** Lorsque la couche IPSec reçoit des données à envoyer, elle commence par consulter la base de données des politiques de sécurité (SPD) pour savoir comment traiter ces données. Si cette base lui indique que le trafic doit se voir appliquer des mécanismes de sécurité, elle récupère les caractéristiques requises pour la SA correspondante et va consulter la base des SA (SAD).

Si la SA nécessaire existe déjà, elle est utilisée pour traiter le trafic en question. Dans le cas contraire, IPSec fait appel à IKE pour établir une nouvelle SA avec les caractéristiques requises.

2. **Scénario d'un trafic entrant :** Lorsque la couche IPSec reçoit un paquet en provenance du réseau, elle examine l'en-tête pour savoir si ce paquet s'est vu appliquer un ou plusieurs services IPSec et si oui, quelles sont les références de la SA. Elle consulte alors la SAD pour connaître les paramètres à utiliser pour la vérification et/ou le déchiffrement du paquet. Une fois le paquet vérifié et/ou déchiffré, la SPD est consultée pour savoir si l'association de sécurité appliquée au paquet correspondait bien à celle requise par les politiques de sécurité. Dans le cas où le paquet reçu est un paquet IP classique, la SPD permet de savoir s'il a néanmoins le droit de passer.

2.3.5.6 Les deux modes de fonctionnement d'IPSec

Pour chacun des mécanismes de sécurité d'IPSec, il existe deux modes de fonctionnement :

Le mode transport prend un flux de niveau transport (couche de niveau 4 du modèle OSI) et réalise les mécanismes de signature et de chiffrement puis transmet les données à la couche IP. Dans Ce mode, l'insertion de la couche IPSec est transparente entre TCP et IP. TCP envoie ses données vers IPSec comme il les enverrait vers IP. L'inconvénient de ce mode réside dans le fait que l'en-tête extérieur est produit par la couche IP c'est-à-dire sans masquage d'adresse. De plus, le fait de terminer les traitements par la couche IP ne permet pas de garantir la non-utilisation des options IP. L'intérêt de ce mode réside dans une relative facilité de mise en œuvre.

Dans le mode tunnel, les données envoyées par l'application traversent la pile de protocole jusqu'à la couche IP incluse, puis sont envoyées vers le module IPSec. L'encapsulation IPSec en mode tunnel permet le masquage d'adresses. Le mode tunnel est utilisé entre deux passerelles de sécurité (routeur, firewall, ...) alors que le mode transport se situe entre deux hôtes.

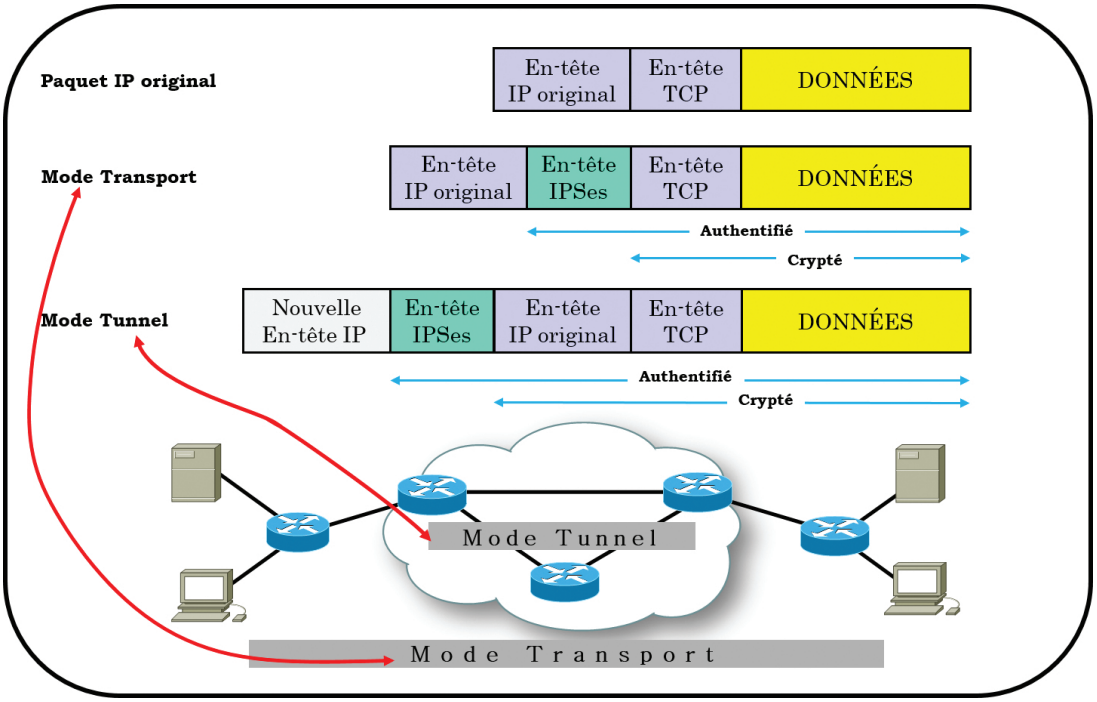


Figure 2.3.4 : IPSec, mode transport et mode tunnel.

2.3.6 Le protocole SSL

SSL (*Secure Socket Layers*, RFC 2246) est un procédé de sécurisation des transactions effectuées via Internet. Il repose sur un procédé de cryptographie à clés publique afin de garantir la sécurité de la transmission des données sur Internet. Son principe consiste à établir un canal de transmission sécurisé (chiffré) entre un client et un serveur après une étape d'authentification.

SSL a deux grandes fonctionnalités : l'authentification du serveur et du client à l'établissement de la connexion et le chiffrement des données durant la connexion.

SSL est un protocole de niveau transport, utilisé par une application pour établir un canal de communication sécurisé avec une autre application.

2.3.6.1 Fonctionnement du protocole SSL

Le protocole SSL Handshake débute une communication SSL. Suite à la requête du client, le serveur envoi son certificat ainsi que la liste des algorithmes qu'il souhaite

utiliser. Le client commence par vérifier la validité du certificat. Cela se fait à l'aide de la clé publique de l'autorité de certification contenue dans le navigateur du client. Le client vérifie aussi la date de validité du certificat. Si toutes vérifications sont passées, le client génère une clé symétrique et l'envoi au serveur. Ce dernier peut alors envoyer un teste au client, que le client doit signer avec sa clé privée correspondant à son propre certificat. Ceci est fait de façon à ce que le serveur puisse authentifier le client.

De nombreux paramètres sont échangés durant cette phase : type de clés, valeur de la clé, algorithmes de chiffrement.

La phase suivant consiste en l'échange de données cryptées avec le protocole SSL Record. Les clés générées avec le protocole Handshake sont utilisées pour garantir l'intégrité et la confidentialité des données échangées. Les différentes phases de protocole sont [5] :

- Segmentation des paquets en paquets de taille fixe.
- Compression (mais peu implémenté dans la réalité).
- Ajout du résultat de la fonction de hachage composé de la clé de cryptage, du numéro de message, de la longueur du message et des données.
- Chiffrement des paquets et du résultat du hachage à l'aide de la clé symétrique générée lors du Handshak.
- Ajout d'un en-tête SSL au paquet.

2.4 Conclusion

Ce chapitre nous a permis de prendre connaissance des différents concepts liés aux VPNs et de comprendre l'intérêt qu'ils y apportent dans le domaine de la sécurité des réseaux.

On a évidemment pris connaissance de la multitude de protocoles, de techniques et d'architectures qui existent pour le déploiement d'un VPN.

Dans le chapitre qui suit, nous présenterons l'entreprise d'accueil NAFTAL GPL, ainsi que l'architecture réseau requise par celle-ci, et nous définirons le contexte du projet à réaliser.

5. Consultez les RFC 5878, 3943 pour plus d'informations sur SSL Handshake et SSL Record.

Étude des charges et mise en œuvre de la solution

Chapitre 3

Organisme d'accueil

3.1 Introduction

Afin de nous familiariser avec l'environnement de l'entreprise NAFTAL «division Gaz de Pétrole Liquéfié», nous avons en premier lieu pris connaissance de celle-ci, des différents services qui la constituent, ainsi que les taches associées à chaque service. En second lieu, nous nous sommes intéressées au département informatique afin de comprendre l'architecture réseau requise par l'entreprise et illustrer par la suite les différents équipements qui la constituent sous trois aspects : réseau, système et sécurité.

Ce chapitre est donc, une introduction au réseau et à l'environnement de l'entreprise NAFTAL GPL.

3.2 Présentation de l'entreprise NAFTAL

3.2.1 Historique

L'entreprise ERDP (Entreprise de raffinage des produits pétroliers), issue de SONATRACH, a été crée par le décret n° 80/101 du 06/04/1982, elle est chargée de l'industrie du raffinage et la distribution des produits pétroliers. En 1987, l'activité de raffinage est séparée de l'activité de distribution, le raisin social de la société change suite à cette séparation.

NAFTAL est désormais chargée de la commercialisation et de la distribution des

produits pétroliers et dérivés. À partir de 1998, elle change de statut et devient SPA (société par actions) 100% de SONATRACH avec un capital de 15 650 000 000 DA.

La structure centrale de NAFTAL est située à Cherraga, elle est subdivisée en 19 districts sur le plan national, dont le district de Béjaïa. Elle intervient dans les domaines de :

- Formation de bitumes.
- L'enfutage des GPL (Gaz de pétrole liquéfia).
- Distribution, stockage et commercialisation des carburants : GPL, lubrifiants, bitumes, pneumatique, GPL/carburant, produit spéciaux.
- Transport des produits pétroliers.

3.2.2 Les activités principales de l'entreprise

a) La commercialisation des carburants pour la motrice essence et diésel :

- Essence normal.
- Essence super.
- Essence super sans plomb.
- Gaz oïl/GPL/C.

b) Commercialisation des pneumatiques de grandes marques.

c) Commercialisation d'une gamme de lubrifiants, ce dernier couvre toutes les applications d'un secteur automobile et industriel.

d) Le traitement du gaz naturel où gaz associés.

e) Le raffinage du pétrole.

f) La liquéfaction du gaz naturel.

3.3 Présentation du district GPL

3.3.1 Les activités principales du district GPL

- Commercialiser les GPL vrac et conditionnés, leur emballages et accessoires.

- Veiller au respect des normes et consignes de sécurité sur toute la chaine GPL (transport, installation d'enfutage et de stockage, bouteilles, citernes, accessoires, ... etc.).
- Organiser et développer le réseau commercial et de distribution.
- Développer et valoriser les GPL sous toutes ses formes particulièrement vrac et gaz carburant.
- Distribuer les GPL aux utilisateurs dans les meilleures conditions de coût, qualité, délais et sécurité.
- Moderniser les infrastructures pour améliorer la productivité, la sécurité et la gestion.
- Développer le partenariat et la coopération dans domaine des GPLs.

3.3.2 Organisation de la branche GPL

a) Au niveau centrale, la branche GPL comprend les activités suivantes :

- Direction des ressources humaines.
- Direction administration et moyen.
- Direction finances et comptabilités.
- Direction techniques et maintenance.
- Direction hygiènes sécurité et environnement.
- Direction marketing et exploitation .
- Groupe juridique et informatiques plus audit.

b) Au niveau opérationnel, à travers le territoire national l'activité est organisée en 19 districts (régionaux), couvrant les centres opérationnels que sont les centres emplisseurs (CE et MCE), centre vrac (CV) et dépôt relais (DR). Les districts fonctionnent dans l'optique de décentralisation, responsabilisation. Ils sont entièrement autonomes, sur le plan opérationnel de la distribution, sur le plan comptable et personnel. Ils exécutent et animent toutes les fonctions de stockages, livraison, vente, assistance technique, entretien, gestion financière et gestion des ressources humaines.

Une direction de maintenance et réalisation (DMR) assiste les districts pour les nouvelles installations et les gros travaux de maintenance des véhicules, chariots élévateurs, pompes et autres équipements.

c) Activités commerciales et marketing du district, les taches associées à cette activité sont comme suite :

- Organiser et développer la commercialisation et la distribution des produits GPL.
- Connaître les différents marchés du GPL et les besoins actuels.
- Satisfaire sa clientèle dans les meilleures conditions d'efficacité et des couts.
- Organiser et coordonner les activités de programmation des approvisionnements, de ravitaillement et de distribution des différents centres de stockage répartis à travers les quatre wilayas (Béjaïa, Jijel, Bouira et Alger).
- Assurer l'approvisionnement et la commercialisation des produits GPL sur l'ensemble des quatre wilayas.
- Élaborer des plans en liaison avec d'autres districts visant la couverture du marché national en produits GPL.

3.3.2.1 Organigramme du district GPL

Le schéma suivant illustre l'organigramme établit par la branche GPL d'Alger :

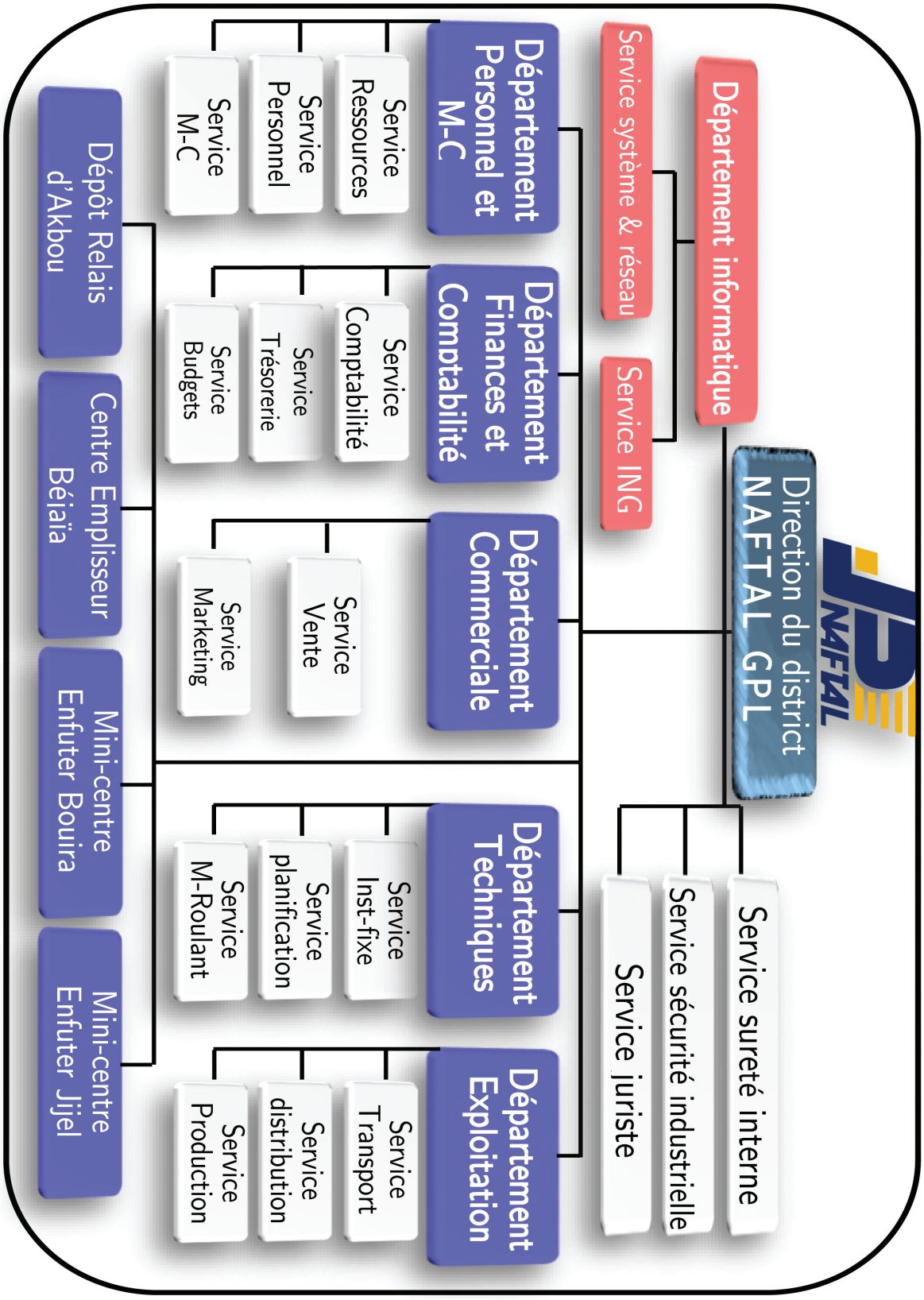


Figure 3.3.1 : Organigramme du district GPL Béjaïa.

3.3.2.2 Description et rôle de chaque service au sein de l'entreprise

▷ **Service sureté :** Ce service assure la sécurité au sein de l'entreprise NAFTAL.

▷ **Service sécurité industrielle :** Ce service se charge d'assurer les taches suivantes :

- La protection et la préservation du personnel.
- La préservation et la protection du patrimoine industriel.
- La protection de l'environnement.

▷ **Département informatique :** Ce département se charge d'assurer la coordination de l'activité informatique au niveau de l'entreprise « NAFTAL GPL ».

▷ **Département exploitation :** Ce département se charge d'assure les taches suivante :

- Suivie des performances des moyens de transports.
- De diriger et de programmer les moyens de transports (transport ravitaillement vrac, transport ravitaillement conditionné).
- D'établir un plan adéquat des distributions et de provisionnement. répond aux exigences des marchés.
- Il s'occupe du conditionnement du gaz butane vrac en bouteille de 13 kg et 3 kg.
- De la veille de la disponibilité du produit pour la clientèle qu'ils soient conditionnés en GPL ou ne vrac.

▷ **Département technique :** Le rôle de ce département est d'assurer la gestion des projets dans leurs phases d'étude et de supervision des travaux.

▷ **Département commercial :** Assure ce qui suit :

- L'accueil de la clientèle par identification en constituant un dossier comportant toutes les informations nécessaires pour sa distribution.
- La satisfaction de la demande de la clientèle.
- L'évaluation des besoins en GPL de la zone d'influence.
- Il s'occupe de l'étude du marché et de l'environnement où le produit sera destiné à la commercialisation.

▷ **Département finances et comptabilité :** Il se charge de procréer aux écritures comptable conformément aux préconisations du système de comptabilité financière, il a comme mission :

- Coordonner les activités des services.

- Assurer les travaux d'analyse financière et comptable.
- Coordonner la préparation périodique et annuelle des situations comptable.
- Assure le suivie, la coordination et la bonne gestion des systèmes.
- Assurer la saisie et la production informatique des états de synthèse de la zone.
- Assurer tous les problèmes fiscaux de la zone, notamment le bilan fiscal.

▷ **Département personnel et moyen humains :** Il est chargé principalement du recyclage et de la mise à niveau du personnel des différentes structures de l'entreprise.

3.4 Présentation du département informatique

Le département informatique à sa dimension a un impact lié au destin de la société, car son apport est tellement présent et visible dans l'interchangeabilité des données et de l'information au sein du district GPL de NAFTAL, dans l'administration et la maintenance du réseau informatique, etc.

3.4.1 Rôle du département informatique de la GPL

La département informatique rassemble une quinzaine de personnes qui exercent différentes taches, dans le but d'assurer le bon fonctionnement du réseau de l'entreprise NAFTAL GPL.

3.4.2 Organigramme du département informatique

Nous allons à présent illustrer l'organigramme associé à la section informatique, afin d'étudier de plus près les deux services qui y contribuent.

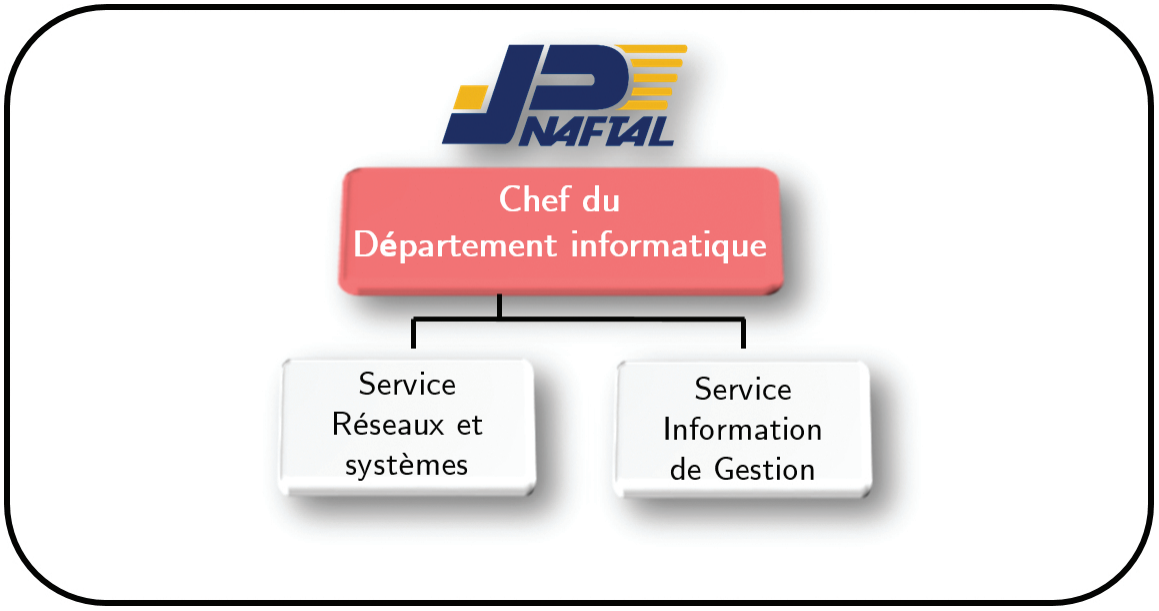


Figure 3.4.1 : Organigramme du département informatique.

3.4.2.1 Description et rôle de chaque service au sein du département informatique

Les deux services associés au département informatique jouent les taches cités ci-dessous :

▷ **Service réseaux et systèmes :** Ce service assure :

- La maintenance de matériel informatique.
- La maintenance des logiciels, systèmes et applications.
- Le suivi des différentes activités d'administration du réseau.

▷ **Service informatique de gestion :** Ce service se charge d'accomplir certaines taches et responsabilités :

- Consolide sur la base des rapports des unités, les rapports périodiques des activités relevant des structures de la zone.
- Veuille au recueil de l'information à partir des CDs (Centre de Stock).
- Analyse les états.
- Participe à l'élaboration des plans de production de la zone, consolidé les plans élaborés par les structures de la zone.
- Exécute toute autre tâche, relevant de ses compétences, pouvant lui être confiée par la hiérarchie.

3.5 Architecture réseau du district GPL

Une architecture réseau est un ensemble d'équipement matériel et logiciels interconnectés en réseau, afin de régir des activités informatiques collectives, en centralisant ou répartissant les ressources et les taches à travers le système. C'est donc une façon d'interconnecter physiquement les différents éléments d'un réseau et de combiner son organisation logicielle, dans le but de communiquer et d'effectuer des opérations informatiques.

L'entreprise NAFTAL, dispose d'un grand réseau informatique réparti sur plusieurs wilayas. En effet le réseau de NAFTAL s'étend actuellement sur quatre principaux pôles à savoir : Béjaïa, Cherraga (Alger), Chourfa (Bouira), et Tahir (Jijel), en plus des connexions à Internet via des FAI (Fournisseur d'accès à Internet). Comme le montre figure suivante :

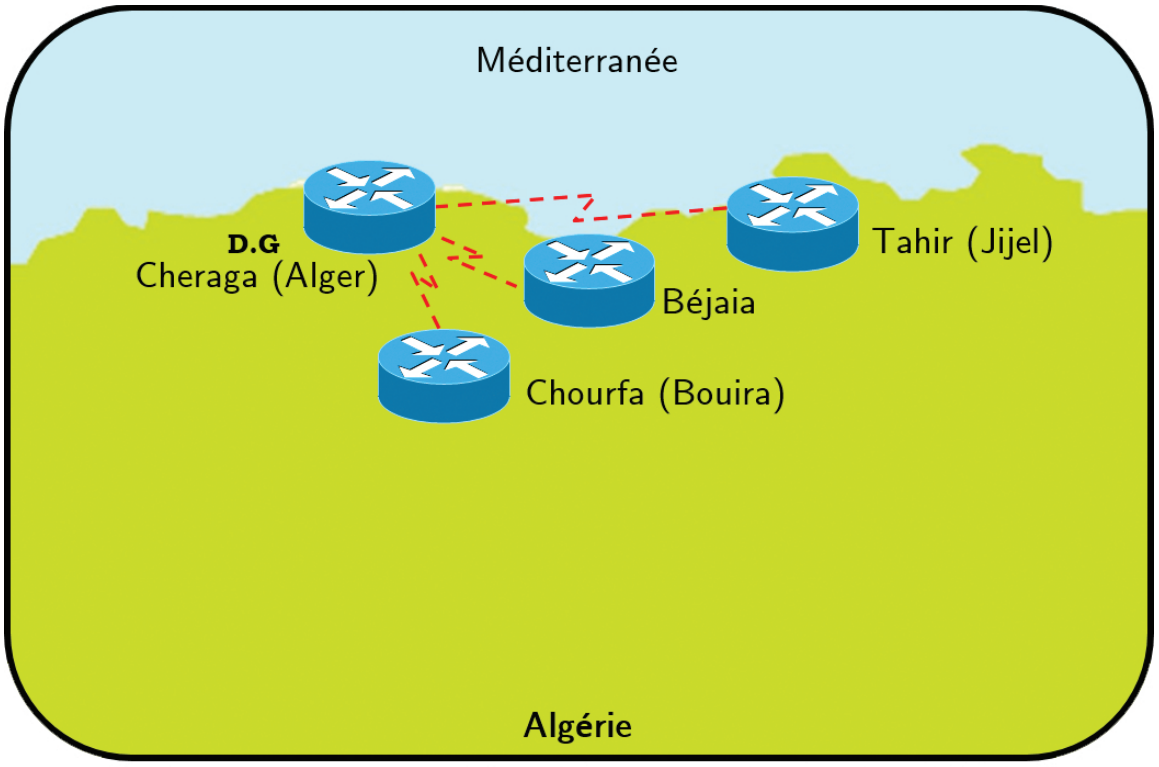


Figure 3.5.1 : Architecture du réseau étendu des districts GPL de NAFTAL.

L'architecture du réseau du district GPL de Béjaïa se compose de quatre armoires séparées, chaque armoire regroupe un commutateur de niveau 2, un onduleur, panneau

de brassage. L'armoire située au département informatique est relié en escale «câble RG 45» avec les autres armoires existantes (département personnels et moyens communs, département archives) et celle situé au département commerciale, qui est liée en fibre optique par contrainte de distance entre les deux départements soit 150 m.

Le département informatique comprend des serveurs en DMZ qui offrent certaines services. Pour qu'une machine interne puisse communiquer avec une autre machine externe, il est impératif qu'elle passe en premier lieu par un mécanisme de filtrage de pare-feu placé à la périphérie du réseau local. Le LAN de NAFTAL est connecté à Internet, en passant par le routeur qui se trouve dans l'armoire du département.

La figure suivante illustre l'architecture décrite :

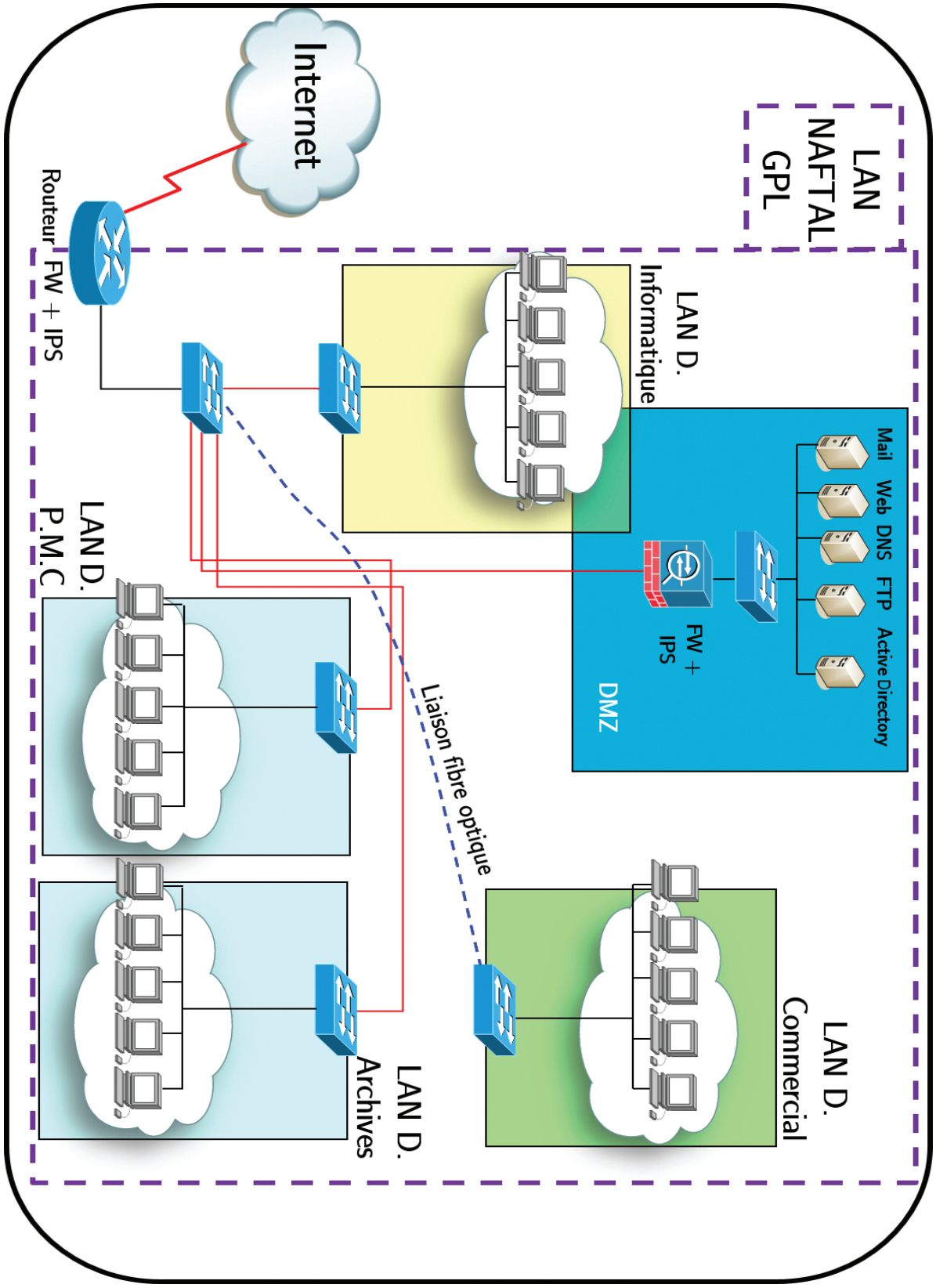


Figure 3.5.2 : Architecture réseau du district GPL de Béjaïa.

3.5.1 Classification des équipements réseau

À présent, nous allons définir les différents équipements réseau utilisés au sein du district NAFTAL GPL de Béjaïa, les équipements varient selon les fonctions requises et les technologies choisies.

3.5.1.1 Matériel actif

On appelle matériel actif, tout matériels comportant un équipement électronique chargé d'assurer la répartition des signaux, entre les différentes branches d'un réseau informatique.

a) Aspect réseau : Il s'agit d'équipements permettant de faire transiter les données entre les stations de travail, parmi ces équipements on trouve : les commutateurs, les routeurs, et les concentrateurs.

b) Aspect système : il s'agit des services existant au sein de l'entreprise dans le but de faciliter la gestion du système d'information, parmi ces services, on cite :

Le contrôleur du domaine «Active Directory» : Active Directory met de l'ordre dans le réseau de l'entreprise, à partir de l'organisation apportée aux ressources du réseau tel que les comptes d'utilisateurs, les dossiers partagés, les imprimantes ...

3.5.1.2 Matériel passif

Support physique de transmission :

Les support physiques utilisées au sein du réseau de NAFTAL GPL sont les suivants :

1. Les supports en cuivre :

Câble à paires torsadées : on distingue deux catégories associées à ce premier[21] :

– Câble ‹UTP› : Le câblage UTP, terminé par des connecteurs RJ-45, est un support en cuivre courant pour l'interconnexion de périphériques réseau. Les principaux types des câbles obtenus en utilisant des conventions de câblage spécifiques sont : Ethernet directe, croisement Ethernet et renversement. Les catégories de câbles UTP utilisés par le réseau de NAFTAL GPL sont de catégorie 3, 4, 5,5^{e}, 6, 6a et 7.

– Câble a paire torsadées blindées ‹STP› : La norme STP utilise deux paires de fils enveloppées dans revêtement tressé, afin d'offrir une meilleure protection parasitaire que le câblage UTP, mais a un prix relativement plus élevé.

2. Supports en fibre optique : Le câblage en fibre utilise des fibres de verre ou de plastique pour guider des impulsions lumineuses de la source à la destination. Les bits sont codés sur la fibre comme impulsions lumineuses. Le câblage en fibre prend en charge des débits de bande passante de données brutes très élevés, l'inconvénient réside seulement dans le coût élevé de la fibre optique ainsi que sa manipulation qui est délicate et qui demande plus de compétences et de maitrise.

3. Support sans fil : le réseau NAFTAL, dispose de points d'accès de gamme ‹Aironet Cisco›, permettant d'assurer une connexion sans fil.

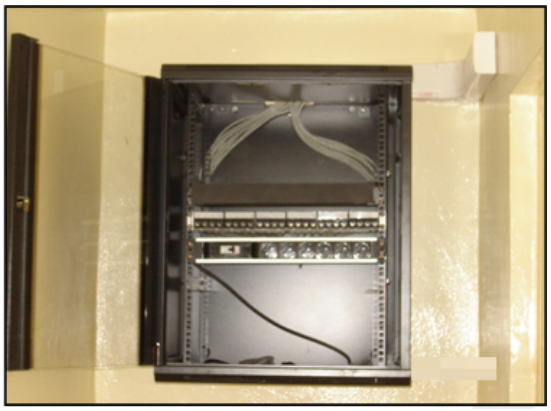
4. Les connecteurs réseau : Des connecteurs RJ-45 utilisés avec des câbles pairs torsadés.

5. Les panneaux de brassage : Un panneau de brassage est le point ou se concentrent tous les câbles de chaque prise murale RJ-45 d'un bâtiment. Il sert à relier ces prises à un commutateur grâce à un cordon de brassage.

3.5.1.3 Autre équipement

Armoire de brassage : une armoire de brassage appelée aussi «baie de brassage» est conçu pour héberger et protéger les différents équipements et composants du système de câblage du réseau informatique. Le choix d'une baie de brassage informatique s'effectue après avoir déterminé les équipements à intégrer (nombre de panneaux de brassage, commutateur Ethernet,. . . , etc.).

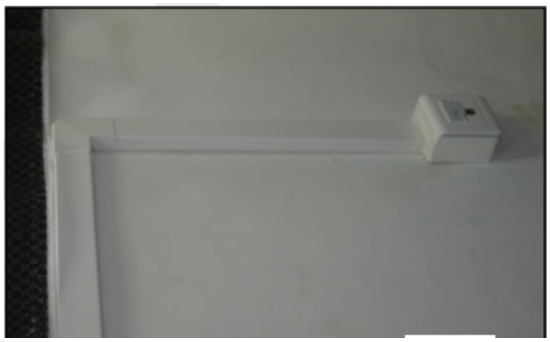
Voici quelques photos prises au sein du district GPL de Béjaïa :



(a) Armoire.

(b) Armoire.

(c) Câblage.



(d) Prise RJ 45.

Figure 3.5.3 : Quelques équipements du réseau de GPL Béjaïa.

3.6 Critique

La critique est un jugement objectif portant sur l'organisation actuelle de l'entreprise qui vient d'être présenté.

L'étude du réseau de NAFTAL GPL de Béjaïa, nous a permis de définir un nombre d'insuffisances qui représentent une pénurie qui touche le bon fonctionnement du réseau, et le rend vulnérable.

En effet, dés notre arrivée au sein du district GPL de Béjaïa, nous avons constaté que le trafic inter-réseau était non sécurisé, toutes les informations du réseau de l'entreprise circulaient en claire sur internet, et ont certainement peut être interceptées à un moment ou à un autre par des personnes non connues.

3.7 Besoins de l'entreprise

L'information est à la base de toutes prises de décisions que ce soit pour mesurer le taux de satisfaction de la clientèle et surtout d'accroitre la vente afin d'atteindre l'objectif. C'est la raison pour laquelle NAFTAL ne peut que tirer d'avantages de se doter d'un réseau VPN site-à-site, moyen efficace et fiable dans le traitement de l'information.

3.8 Solution retenue

La solution retenue pour répondre à ce besoin de communication sécurisée consiste à relier les réseaux distants à l'aide d'une liaison spécialisée. Toutefois la plupart des entreprises ne peuvent pas se permettre de relier deux réseaux locaux distants par une ligne spécialisée, il est parfois nécessaire d'utiliser Internet comme support de transmission. Un bon compromis consiste à utiliser Internet comme support de transmission à l'aide d'un protocole.

Nous avons opté pour la solution VPN IPSec site-à-site, qui consiste à mettre en place une liaison permanente, distante et sécurisée entre les deux sites de NAFTAL, afin de résoudre au mieux aux différentes préoccupations manifestées par les responsables informatiques du district GPL de Béjaïa et aussi pour pallier aux différents problèmes relevés au niveau de la critique.

Il est néanmoins important de préciser que la solution retenue garantie la confidentialité, la sécurité et l'intégrité des données. Elle permet d'obtenir une liaison sécurisée à moindre coût, si ce n'est la mise en œuvre des équipements terminaux.

La mise en place d'un VPN permettra de distribuer un accès à Internet et des applications Web depuis leurs emplacements. Les VPN site-à-site étendent le WAN à moindre coût et en toute sécurité vers des entités non desservies, telles que des administrateurs et des partenaires commerciaux (extranet).

3.9 Présentation du projet

Intitulé du projet : Solution de sécurité pour le LAN étendu de NAFTAL GPL.
Définition : Il est question ici de proposer un moyen sécurisé et sûr pour les échanges

de données entre deux LANs (sites) d'une entreprise.

Caractéristiques : Un routeur « CISCO » sur lequel nous implémenterons le protocole IPSec.

Motif : L'architecture VPN se fait de plus en plus présente dans les entreprises, surtout chez celles qui ont ce besoin naturel d'interconnecter des LANs étendus en garantie d'un service toujours disponible et de meilleure qualité.

Il est nécessaire de noter ici que la solution VPN ou plus précisément le protocole IPSec sera implémenter aux extrémités de chaque réseau sur le routeur servant de passerelle entre l'intranet et internet.

3.10 Conclusion

Dans ce chapitre, nous avons présenté le cadre de travail dans lequel nous avons effectué le stage, ce qui nous a permis de mieux comprendre et apprécier le travail abattu par l'ensemble du personnel du district GPL de NAFTAL, de comprendre la place qu'occupe cette structure dans le domaine, ainsi, l'étude de son réseau nous a permis de bien comprendre son architecture et ses faiblesses, et a conduis à proposer la solution pour palier à ces dernières.

Chapitre 4

Mise en œuvre de la solution

Chaque projet ou travail, commence généralement par une étude théorique, et se termine par une étude pratique qui est la mise en œuvre de la solution ou bien la réalisation du projet.

Ce présent chapitre, consistera à mettre en œuvre la solution proposée pour la réalisation de notre projet, avec l'ensemble des configurations nécessaires à implémenter sur les LANs de NAFTAL. Ces configurations entourent entre la configuration de routage et des différents protocoles de sécurité pour le VPN.

Pour visualiser l'efficacité de notre travail et mettre en évidence l'efficacité de notre solution, nous avons utilisé le simulateur GNS3 version 0.8.6 qui est un logiciel très pratique *open source* pour maquetter un réseau. Il pourra nous servir à reproduire une architecture physique ou logique complète avant la mise en production.

4.1 Présentation du simulateur Cisco GNS3

4.1.1 Définition

GNS3 (*Graphical Network Simulator*) est un simulateur graphique de réseaux qui permet de créer des topologies du réseau complexes et d'en établir des simulations. Ce logiciel est un excellent outil pour l'administration des réseaux Cisco. Il est possible de s'en servir pour tester les fonctionnalités des IOS Cisco ou pour tester les configurations devant être déployées dans le futur sur des routeurs réels. Ce projet est évidemment *Open*

Source et multi-plates-formes[22].

4.1.2 Les composants du logiciel

Afin de fournir une simulation précise et complète, GNS3 est fortement lié à :

▷ **Dynamips :** Dynamips est un émulateur de routeurs Cisco capable de faire fonctionner des images Cisco IOS non modifiées comme si elles s'exécutaient sur de véritables équipements. Le rôle de Dynamips n'est pas de remplacer de véritables routeurs, mais de permettre la réalisation de maquettes complexes avec de vraies versions d'IOS[23]. Écrit en langage C par Christophe Fillot. Il émule 1700, 2600, 3600, 3700, et 7200 plates-formes de matériel [22].

Pour permettre l'exécution d'une image IOS, Dynamips doit émuler le processeur ainsi que tous les périphériques de la plateforme cible : mémoire RAM (*Random Access Memory)*, NVRAM (*No Volatil RAM*), mémoire Flash, interfaces réseaux ... [23].

▷ **Dynagen :** Dynagen est un produit complémentaire écrit en Python s'interfaçant avec Dynamips grâce au mode hyperviseur. Dynagen facilite la création et la gestion de maquettes grâce à un fichier de configuration simple décrivant la topologie du réseau à simuler et une interface texte interactive. GNS3 reprend ces mêmes fonctionnalités sous forme d'interface graphique. Il s'appuie sur des modules de Dynagen.

Dynagen fournit aussi une CLI (*Command-line Interpreter*) de gestion pour les périphériques d'inscription, démarrage, arrêt, recharge, la suspension, la reprise et la connexion aux consoles de routeurs virtuels[23].

▷ **Qemu :** Qemu est un émulateur et une machine de virtualisation qui permet de courir à un système d'exploitation complet juste en tant que autre tâche sur l'ordinateur de bureau. Il peut être très utile pour essayer différents logiciels d'exploitation, logiciels d'essai, et le fonctionnement des applications qui ne fonctionneront pas sur la plate-forme indigène de notre ordinateur de bureau. Qemu fonctionne sur plusieurs plates-formes, et peut accueillir des systèmes de cible d'une gamme de différents microprocesseurs[24].

▷ **VirtualBox :** VirtualBox est un logiciel de virtualisation de systèmes d'exploitation. En utilisant les ressources matérielles de l'ordinateur (système hôte), VirtualBox permet la création d'un ou de plusieurs ordinateurs virtuels dans lesquels s'installent d'autres systèmes d'exploitation (systèmes invités).

Les systèmes invités fonctionnent en même temps que le système hôte, mais seul

ce dernier a accès directement au véritable matériel de l'ordinateur. Les systèmes invités exploitent du matériel générique, simulé par un faux ordinateur (machine virtuelle) créé par VirtualBox.

VirtualBox permet de faire fonctionner plus d'un système d'exploitation en même temps en toute sécurité. En effet, les systèmes invités n'interagissent pas directement avec le système hôte, et n'interagissent pas entre eux. Le champ d'action des systèmes invités est confiné, limité à leur propre machine virtuelle [25].

▷ **Wireshark :** Wireshark, anciennement ETHEREAL, est un logiciel libre d'analyse de protocole, ou *packet sniffer*, utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie, mais aussi le piratage. Wireshark est multiplateformes, il fonctionne sous Windows, Mac OS, Linux, Solaris, ainsi que sous FreeBSD. Wireshark reconnait 759 protocoles[26].

Grâce à ces composants, GNS3 nous permet[22] :

- Le design de topologies réseaux complexes en haute qualité.
- Émulation de plusieurs plates-formes de routeurs Cisco IOS, ou encore IPS, PIX et Firewalls ASA...
- Simulation de switches Ethernet, ATM et Frame Relay.
- Connexion de réseaux simulés au monde réel.
- Capture de paquets grâce à Wireshark.

4.1.3 L'objectif de GNS3

L'objectif de GNS3 est d'apporter aux étudiants et aux professionnels travaillant dans le domaine d'administration des systèmes et réseaux des nouvelles technologies de communication. C'est un outil pour virtualiser et modéliser fidèlement des réseaux informatiques.

Grâce à GNS3, les utilisateurs peuvent tester et estimer, dans des conditions quasi réelles et sans avoir à financer le matériel, leurs configurations avant de les mettre en place physiquement [22].

4.1.4 Configuration de GNS3

1. Lors du lancement du logiciel une fenêtre similaire à celle-ci apparait, c'est l'espace de travail de GNS3.

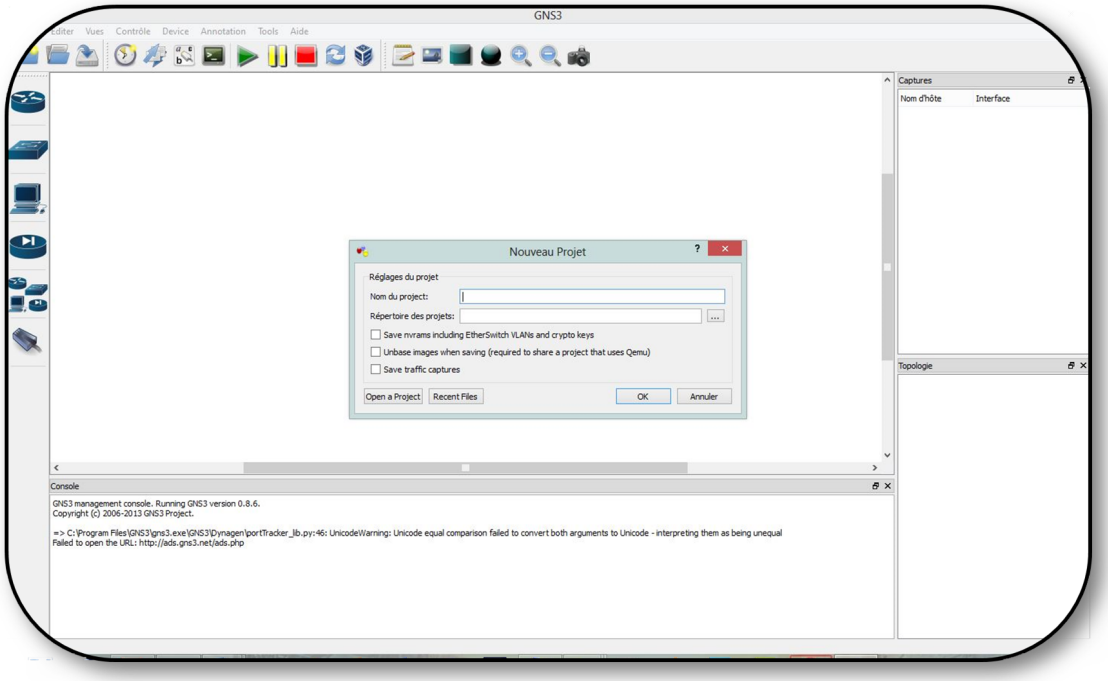


Figure 4.1.1 : L'espace de travail GNS3.

L'interface de GNS3 est divisée en trois parties, la partie gauche affiche la liste des équipements matériels disponibles que nous pouvons ajouter dans notre topologie, la partie droite affiche la liste des éléments actifs et au milieu c'est l'espace de travail.

La petite fenêtre qui apparait au milieu, au lancement de GNS3, à pour objectif la création d'un nouveau projet. Pour cela il faut spécifier dans nom du projet et le chemin où sauvegarder le projet, ensuit cocher les trois cases dessous.

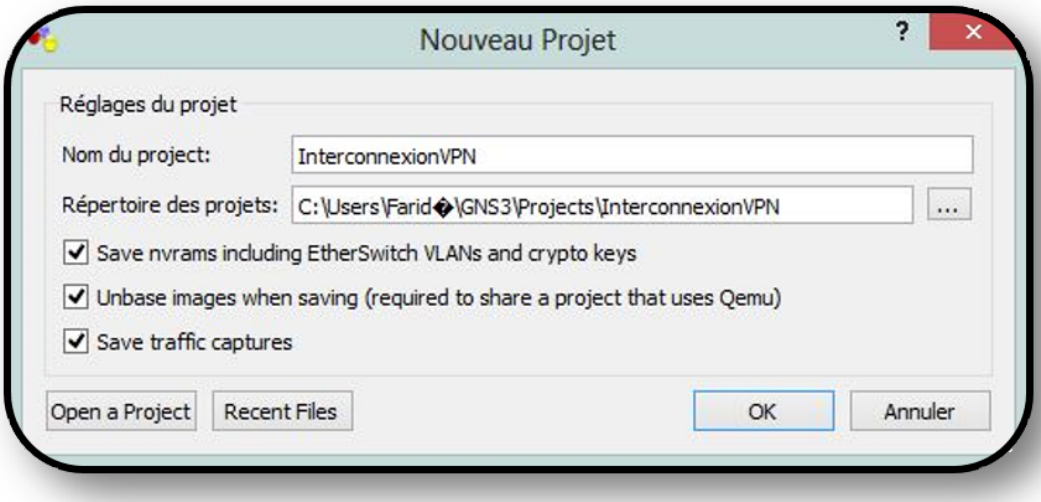


Figure 4.1.2 : Création d'un nouveau projet sous GNS3.

La manipulation d'interface de GNS3 est très simple, généralement son fonctionnement se base sur le principe du glisser-déposer. Il suffit de prendre un élément à placer sur l'espace du travail dans la liste des équipements à gauche.

2. Pour commencer à travailler avec GNS3, nous devons avoir les différentes images (IOS) des équipements Cisco. Une fois téléchargées, Nous devons donner pour chaque modèle d'équipement que nous voulons utiliser, le chemin vers l'image IOS [1].

3. Pour ajouter l'IOS à la plate-forme adéquate aller sur le "Menu Éditer -> Images IOS et hyperviseurs". Cliquer sur "Image binaire", et sélectionner l'une des IOS précédemment téléchargée, puis choisir la plateforme et le modèle d'équipement adéquat puis cliquer sur "Sauvegarder". La figure ci-dessous montre deux modèles d'IOS que nous avons ajoutés.

1. Document officiel de l'IDWG : `http://www.ietf.org/html.charters/idwg-charter.html`

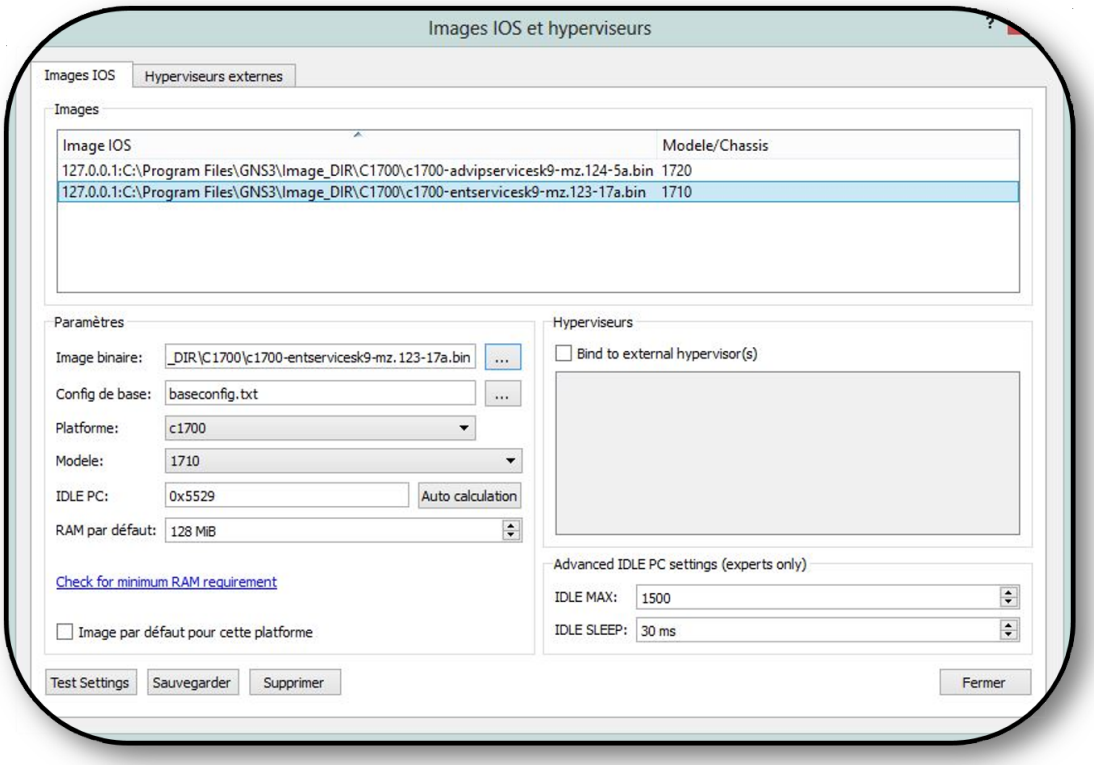


Figure 4.1.3 : L'ajout des IOS.

4. Maintenant pour ajouter un équipement il suffit de faire un glisser-déposer à partir de la liste gauche et de le déposer dans la partie centrale de GNS3. Un clic droit sur le l'équipement pour le démarrer.

5. Pour ajouter une machine virtuelle dans notre architecture GNS3, il nous faut d'abords préalablement installer VirtualBox et avoir déjà configuré au moins une machine virtuelle (Annexe B).

6. Pour intégrer la machine virtuelle dans GNS3 Il faut d'abord l'importer comme suit : aller dans "Éditer -> Préférences -> VirtualBox -> VirtualBoxGuest -> RefreshVM List", puis donner un nom à la machine et dans le menu "VM list", sélectionner la machine à importer en suit sélectionner le numéro de la carte réseau laquelle elle va utiliser dans "Number of NICs" pour se connecter, en fin "Sauvegarder -> Appliquer -> OK".

Figure 4.1.4 : L'ajout d'une machine virtuelle à la topologie GNS3.

Maintenant un glisser-déposer de la machine sur l'interface de travail nous permet de l'utiliser, et pour la configurer un clic droit sur la machine permet d'afficher le menu contextuel de configuration.

4.2 Présentation générale et principe de la solution proposée

4.2.1 Description de la maquette à configurer

Avant d'entamer la mise en œuvre de la solution proposée, il est essentiel de définir l'architecture réseaux utilisée. Pour cela, nous utiliserons la maquette du réseau WAN ci-dessous, constitué de 2 sites distants (LAN du district NAFTAL GPL de Béjaïa et le LAN de la direction générale située à Alger), possédant chacun :

- Un routeur Cisco, avec un IOS supportant les fonctions de cryptage (modules d'accélération de cryptage matériel).
- Une connexion Internet avec des adresses IP fixes.

-	**Interface/IP locale**	**Interface/IP Internet**
Site 1	FastEthernet 0/1 192.168.1.1	Serial 0/1 192.168.10.1
Site 2	FastEthernet 0/1 192.168.2.1	Serial 0/1 192.168.20.1

TABLE 4.1 : Caractéristiques des deux routeurs.

4.2.2 Schéma idéalisé

Le but du VPN est de faire en sorte que les 2 sites communiquent exactement comme s'ils étaient directement reliés entre eux, de manière à ce que les 2 réseaux puissent êtres directement routés.

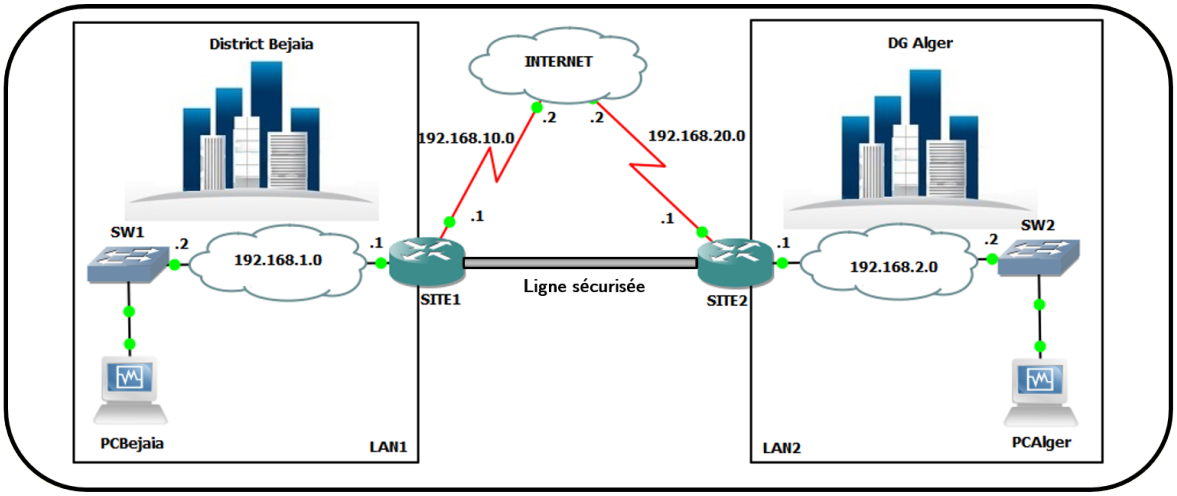


Figure 4.2.1 : Schéma idéalisé.

La liaison directe entre les 2 routeurs que nous avons ajouté symbolise dans le cas idéalisé une ligne sécurisée et fiable.

4.2.3 Schéma réel – Principe de mise en place

Dans la réalité il est évidement hors de question de connecter directement les 2 routeurs, puisque le but premier du VPN est justement de se passer d'une ligne spécialisée.

Ce lien sera donc créé grâce à un tunnel crypté, qui permettra aux 2 sites de communiquer entre eux de manière sécurisée. Pour cela, nous allons réaliser la configuration d'IPSec sur les deux routeurs : en mode automatique avec un secret pré-partagé via le protocole ISAKMP.

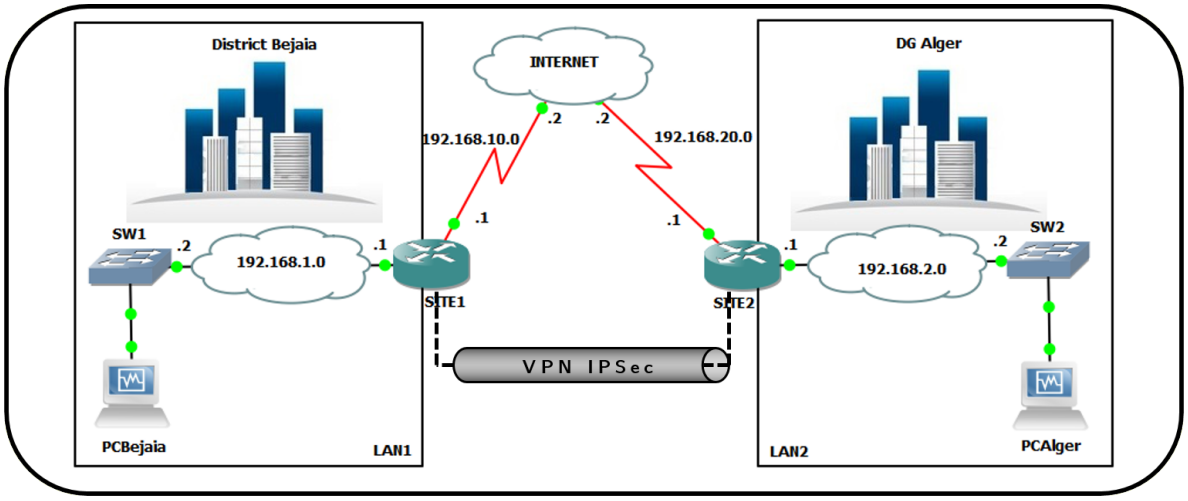


Figure 4.2.2 : Schéma réel.

Les critères de configuration d'IPSec à mettre en place seront :

- Chiffrement et authentification avec le protocole ESP.
- Mode tunnel.
- Les algorithmes de chiffrement et d'authentification sont AES et SHA.

Une fois le tunnel IPSec mis en place, nous lancerons un *Ping* entre les deux machines (PCBejaia et PCAlger), et visualiser les SA établies ainsi que certaines informations sur le trafic échangé.

4.3 Configuration (En ligne de commandes)

4.3.1 Configuration des routeurs

Pour commencer, nous allons configurer les deux routeurs (SITE1 de Béjaïa et SITE2 d'Alger), en indiquant les adresses IP des interfaces associés à chacun d'entre eux, ainsi que le protocole de routage utilisé par chaque routeur.

```
Router1>enable
Router1#configure terminal
Router1(config)#hostname SITE2
SITE1(config)#interface fa0/0
SITE1(config-if)#ip address 192.168.1.1 255.255.255.0
SITE1(config-if)#no shutdown
SITE1(config-if)#exit
SITE1(config)#interface s0/1
SITE1(config-if)#ip address 192.168.10.1 255.255.255.0
SITE1(config-if)#no shutdown
SITE1(config-if)#exit
SITE1(config)#router rip
SITE1(config-if)#version 2
SITE1(config-if)#network 192.168.1.0
SITE1(config-if)#network 192.168.10.0
SITE1(config-if)#no auto-summary
SITE1(config-if)#exit
SITE1(config)#exit
SITE1#writ
```

De même, nous allons effectuer la même configuration pour le routeur 2 :

```
Router2>enable
Router2#configure terminal
Router2(config)#hostname SITE2
SITE2(config)#interface fa0/0
SITE2(config-if)#ip address 192.168.2.1 255.255.255.0
SITE2(config-if)#no shutdown
SITE2(config-if)#exit
SITE2(config)#interface s0/1
SITE2(config-if)#ip address 192.168.20.1 255.255.255.0
SITE2(config-if)#no shutdown
SITE2(config-if)#exit
SITE2(config)#router rip
SITE2(config-if)#version 2
SITE2(config-if)#network 192.168.2.0
SITE2(config-if)#network 192.168.20.0
SITE2(config-if)#no auto-summary
SITE2(config-if)#exit
SITE2(config)#exit
SITE2#writ
```

Pour vérifier le bon fonctionnement du réseau créé, nous allons envoyer un *Ping* depuis la machine PCBejaia vers la machine PCAlger. Une analyse du trafic à l'aide de Wireshark au niveau de l'interface Internet de routeur SITE2 nous a donnée le résultat suivant :

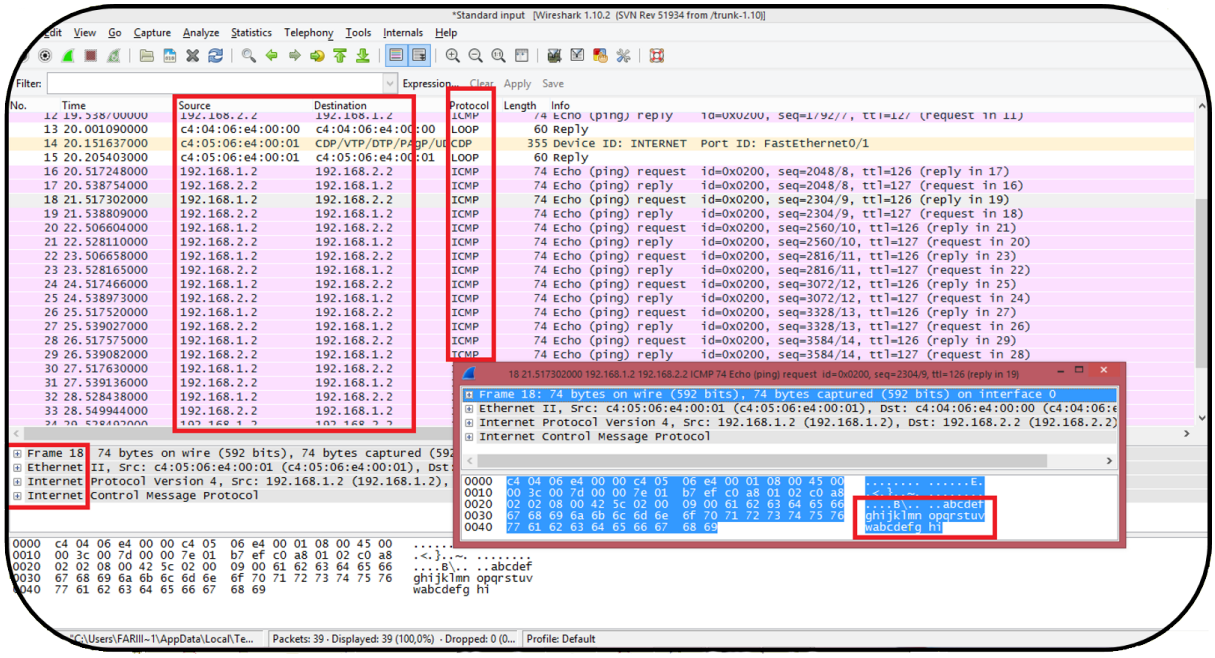


Figure 4.3.1 : Capture d'un échange de données non sécurisé entre SITE1 et SITE2.

Nous remarquons que des informations importantes et détaillées ainsi que des adresses du réseau locale, sont transportées en claire, cela présente une vulnérabilités, car un utilisateur malveillant, en possession de ces informations peut anticiper plusieurs types d'attaques.

4.3.2 Configuration du protocole IPSec

La configuration d'IPSec s'effectue généralement en suivant les étapes ci-dessous :

1. Configuration de la politique d'ISAKMP de la phase 1 du protocole IKE : algorithmes, clés, durée de vie du tunnel ISAKMP qui se trouveront à la suite de la ligne de configuration commençant par `crypto isakmp`.
2. Configuration de la SA IPSec de la phase 2 du protocole IKE (protocoles AH/ESP, algorithmes, durée de vie du tunnel IPSec) se trouveront à la suite de la ligne de configuration commençant par `crypto ipsec`.
3. Description d'une carte de cryptage (crypto map) rassemblant les paramètres des deux phases, l'extrémité du tunnel et la définition du trafic à sécuriser se trouvera à la suite de la ligne de configuration commençant par `crypto map`.

Il est très important de faire attention à ce que les configurations des deux routeurs soient cohérentes et symétriques, l'une par rapport à l'autre.

4.3.3 Configuration d'IKE

Pour configurer le protocole IKE, nous allons réaliser les taches suivantes :
- Activation du protocole IKE.
- Configuration de la politique d'IKE (phase 1).
- Configuration de l'authentification mutuelle par clé pré-partagée.

4.3.3.1 Activation du protocole IKE

Le mécanisme IKE est activé par défaut sur la plupart des IOS Cisco. Il est validé globalement pour toutes les interfaces sur un routeur Cisco. Pour s'assurer, nous allons exécuter les commandes suivantes sur les deux routeurs :

```
SITE1(config)#no crypto isakmp enable
SITE1(config)#crypto isakmp enable
```

De même pour le routeur SITE2 :

```
SITE2(config)#no crypto isakmp enable
SITE2(config)#crypto isakmp enable
```

4.3.3.2 Configuration des paramètres de la SA ISAKMP (IKE phase 1)

Dans cette étape nous allons créer une politique pour le mécanisme IKE sur chaque routeur, cette politique se définit par une combinaison des paramètres de sécurité à employer, le tableau ci-dessous indique la liste de ces paramètres.

Paramètre	**Valeurs acceptées**	**Mot-clé**	**Par défaut**
algorithme d'encryption	DES 56-bit	`Des`	DES 56-bit
	DES 168-bit	`3des`	DES 168-bit
	AES 128-bit	`aes-128`	AES 128-bit
	AES 256-bit	`aes-256`	
algorithme de hachage	SHA1 (HMAC variant)	`Sha`	SHA1
	MD5 (HMAC variant)	`md5`	
méthode d'authentification	Signatures RSA	`rsa-sig`	RSA signatures
	Chiffrement RSA	`rsa-encr`	
	Clés pré-partagées	`pre-share`	
groupe Diffie-Hellman	D-H 768-bit	`1`	D-H 768-bit
	D-H 1024-bit	`2`	
durée de vie de la SA	Spécifier une valeur	-	86400 seconds

TABLE 4.2 : Liste des paramètres de sécurité pour IKE.

Une politique définie indique quels paramètres de sécurité seront employés pour protéger les négociations suivantes et précise également comment les deux routeurs seront mutuellement authentifiés.

Pour la configuration des paramètres relatifs à la SA ISAKMP, nous allons procéder comme suit :

```
étape 1   SITE1(config)#crypto isakmp policy 7
étape 2   SITE1(config-isakmp)#encryption aes
étape 3   SITE1(config-isakmp)#hash sha
étape 4   SITE1(config-isakmp)#authentication pre-share
étape 5   SITE1(config-isakmp)#group 2
étape 6   SITE1(config-isakmp)#lifetime 86400
étape 7   SITE1(config-isakmp)#exit
étape 8   SITE1(config)#exit
```

La même SA, avec les mêmes commandes seront implémentées sur le routeur SITE2.

```
étape 1    SITE2(config)#crypto isakmp policy 7
étape 2    SITE2(config-isakmp)#encryption aes
étape 3    SITE2(config-isakmp)#hash sha
étape 4    SITE2(config-isakmp)#authentication pre-share
étape 5    SITE2(config-isakmp)#group 2
étape 6    SITE2(config-isakmp)#lifetime 86400
étape 7    SITE2(config-isakmp)#exit
étape 8    SITE2(config)#exit
```

Le tableau ci-dessous décrit les différentes commandes utilisées :

Paramètre	Description
étape 1	Création d'une politique ISAKMP avec priorité 7/65535.
étape 2	Spécification d'un algorithme de cryptage.
étape 3	Spécification d'algorithme de hachage.
étape 4	Spécification d'une méthode d'authentification.
étape 5	Spécification de groupe Diffie Hellman.
étape 6	Spécification de la durée de vie de la SA.
étape 7	Quitter le mode de configuration isakmp.
étape 8	Quitter le mode de configuration terminal.

TABLE 4.3 : Description des étapes de configuration de la SA ISKAMP.

À l'issue de cette négociation, un tunnel sécurisé (phase 1 du protocole IKE) est établi entre les deux routeurs SITE1 et SITE2. Désormais, la politique de sécurité de phase 2 (SA IPSec) sera négocié à travers ce tunnel ISAKMP pour ces deux derniers.

4.3.3.3 Configuration de l'authentification par clé pré-partagée

Dans cette étape nous allons configurer les clés pré-partagées que doit utiliser chaque hôte IPSec dans sa politique d'IKE en mode de configuration globale.

Pour le routeur SITE1 nous indiquons "kdfrd" comme clé pré-partagée :

```
SITE1(config)#crypto isakmp key 0 kdfrd address 192.168.20.1
SITE1(config)#exit
```

La même commande doit être saisie pour le routeur SITE2 :

```
SITE2(config)#crypto isakmp key 0 kdfrd address 192.168.10.1
SITE2(config)#exit
```

4.3.4 Configuration des paramètres IPSec (transform-set)

Une fois la négociation de la phase 1 faite, nous devons configurer les paramètres de négociation pour la phase 2. Il s'agit de définir une transformation qui explicite les algorithmes IPSec (AH et/ou ESP) nécessaires pour la mise en œuvre du tunnel IPSec. Le tableau ci-dessous définit la liste des transformations disponibles. Le nom de la transformation est suivi de la commande `crypto ipsec transform-set`. Les `transform-sets` doivent être identiques aux deux paires.

Paramètre	Transform	Description
AH Transform	`ah-md5-hmac`	AH avec authentification MD5
	`ah-sha-hmac`	AH avec authentification SHA
ESP Encryption-Transform	`esp-des`	ESP avec cryptage DES
	`esp-3des`	ESP avec cryptage 3DES
	`esp-aes`	ESP avec cryptage AES
	`esp-null`	ESP sans cryptage
ESP Authentification -Transform	`esp-md5-hmac`	ESP avec authentification MD5
	`esp-sha-hmac`	ESP avec authentification SHA

TABLE 4.4 : Liste des transformations disponibles..

Pour la mise en place de notre transformation, nous allons taper la commande suivante sur le routeur SITE1 :

```
SITE1(config)#crypto ipsec transform-set TRANS esp-sha-hmac esp-aes
SITE1(config)#exit
```

La même commande sur le routeur SITE2 :

```
SITE2(config)#crypto ipsec transform-set TRANS esp-sha-hmac esp-aes
SITE2(config)#exit
```

4.3.5 Configuration des listes d'accès

Il faut configurer une liste d'accès qui définit le trafic à sécuriser. Ces listes d'accès sont différentes des ACLs qui déterminent quel trafic à expédier ou bloquer sur une interface. C'est l'entrée de la `crypto map` référençant la liste d'accès qui décide si le traitement d'IPSec est appliqué au trafic en fonction de l'action (`permit` et/ou `deny`) définie dans la liste d'accès.

Pour le routeur SITE1 nous allons procéder comme suit :

```
SITE1(config)#ip access-list extended VPN-ACL
SITE1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0
0.0.0.255
SITE1(config-ext-nacl)#exit
```

De même, nous allons définir l'ACL associée au SITE2 :

```
SITE2(config)#ip access-list extended VPNACL
SITE2(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 192.168.1.0
0.0.0.255
SITE2(config-ext-nacl)#exit
```

4.3.6 Configuration de la carte de cryptage (`crypto map`)

La carte de cryptage (ou `crypto map`) permet de lier les SA négociées et la politique de sécurité (SP : *Security Policy*). En d'autres termes, elle permet de renseigner :

1. Quel trafic devrait être protégé par IPSec.
2. L'autre extrémité du tunnel vers lequel le trafic IPSec devrait être envoyé.
3. L'adresse locale à employer pour le trafic d'IPSec.
4. Quelle sécurité d'IPSec devrait être appliquée à ce trafic (`transform-set`).

Pour créer les différentes entrées de la carte de cryptage, qui emploieront IKE pour établir les associations de sécurité, nous allons procéder comme suit en suivant les étapes ci-dessous.

étape 1	`SITE1(config)#crypto map VPN-MAP 10 ipsec-isakmp`
étape 2	`SITE1(config-crypto-map)#set peer 192.168.20.1`
étape 3	`SITE1(config-crypto-map)#match address VPN-ACL`
étape 4	`SITE1(config-crypto-map)#set transform-set TRANS`
étape 5	`SITE1(config-crypto-map)#exit`
étape 8	`SITE1(config)#exit`

Les mêmes commandes seront implémentées sur le routeur SITE2 :

étape 1	`SITE2(config)#crypto map VPNMAP 10 ipsec-isakmp`
étape 2	`SITE2(config-crypto-map)#match address VPNACL`
étape 3	`SITE2(config-crypto-map)#set peer 192.168.10.1`
étape 4	`SITE2(config-crypto-map)#set transform-set TRANS`
étape 5	`SITE2(config-crypto-map)#exit`
étape 6	`SITE2(config)#exit`

Le tableau ci-dessous décrit les différentes commandes utilisées :

Paramètre	Description
étape 1	Création d'une carte de cryptage avec priorité 1/65535.
étape 2	Spécification du trafic à sécuriser..
étape 3	Spécification de l'autre extrémité du tunnel IPSec.
étape 4	Application du modèle de transformation à la carte de cryptage.
étape 5	Quitter le mode de configuration de la carte de cryptage.
étape 6	Quitter le mode de configuration terminal.

TABLE 4.5 : Description des étapes de configuration de la crypto map.

4.3.7 Application des `crypto map` aux interfaces

Il faut lier la `crypto map` ainsi définie à une interface du routeur par laquelle le trafic d'IPSec passera. Tout trafic arrivant ou sortant de cette interface est comparé avec le trafic à sécuriser défini dans une liste d'accès : s'il y a correspondance ce dernier est chiffré.

Pour appliquer la `crypto map` VPN-MAP à l'interface Internet sur SITE1, nous allons procéder comme suit :

```
SITE1(config)#int s1/0
SITE1(config-if)#crypto map VPN-MAP
SITE1(config-if)#exit
```

La même chose pour le routeur SITE2 :

```
SITE2(config)#int s1/0
SITE2(config-if)#crypto map VPNMAP
SITE2(config-if)#exit
```

4.4 tests de fonctionnement

Afin de vérifier le bon fonctionnement du VPN, plusieurs commandes sont à notre disposition en mode privilégié.

▷ La commande "`show crypto engine connections active`" nous permet de voir les connexions cryptées actives :

```
SITE1#show crypto engine connections active

  ID Interface            IP-Address      State  Algorithm           Encrypt  Decrypt
   1 FastEthernet0/1      192.168.10.1    set    HMAC_SHA+AES_CBC          0        0
2001 FastEthernet0/1      192.168.10.1    set    AES+SHA                   0       73
2002 FastEthernet0/1      192.168.10.1    set    AES+SHA                  74        0

SITE1#
```

Figure 4.4.1 : Affichage des connexions cryptées actives.

▷ La commande "`show crypto ipsec transform-set`" nous permet de voir les différents types d'encodage actifs.

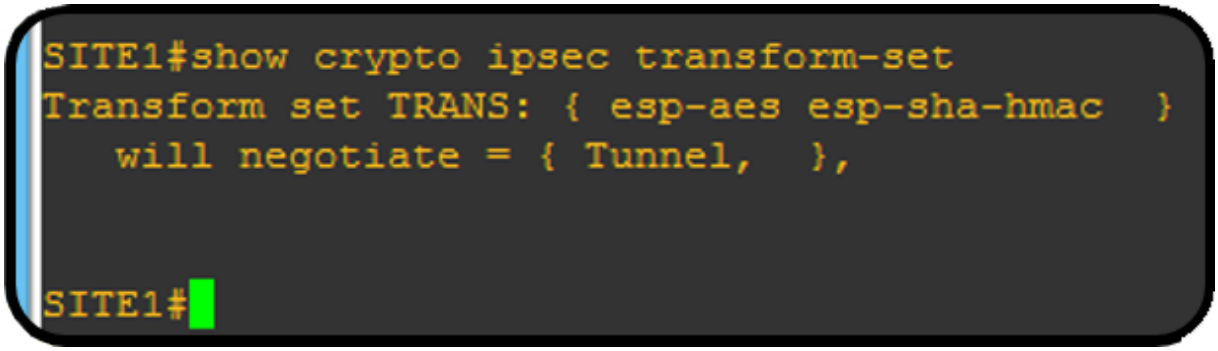


Figure 4.4.2 : Affichage des types d'encodage actifs.

▷ La commande "`show crypto ipsec sa`" fourni une version plus détaillé que les deux commandes citées plus haut.

Figure 4.4.3 : Affichage en détails de la SA IPSec.

▷ La commande "`show ip route`" nous permet de vérifier les routes crées.

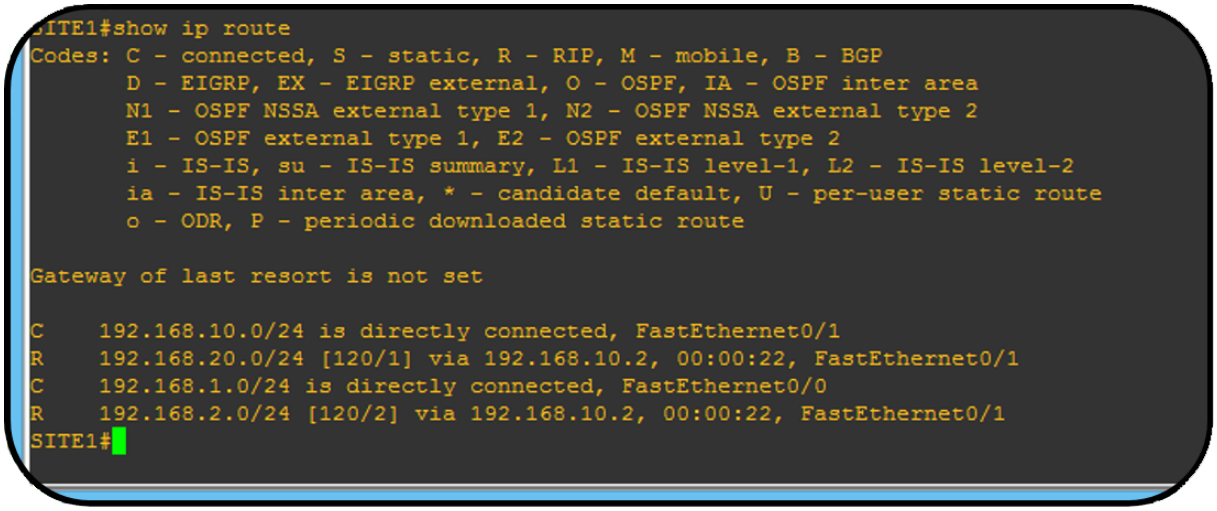


Figure 4.4.4 : Affichage des routes crées.

▷ La commande "`show crypto isakmp sa`" fourni des informations sur l'association de sécurité d'ISAKMP.

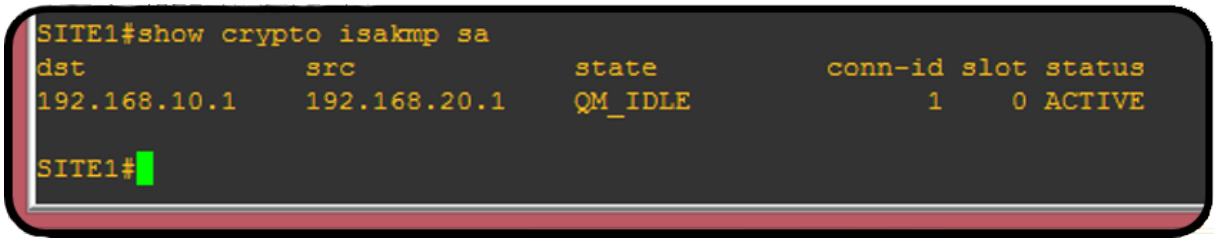


Figure 4.4.5 : Affichage de la SA ISAKMP.

▷ La commande "`show crypto map sa`" nous permet de visionner des informations relatives aux cartes de cryptage crées.

```
SITE1#show crypto map
Crypto Map "VPN-MAP" 10 ipsec-isakmp
        Peer = 192.168.20.1
        Extended IP access list VPN-ACL
            access-list VPN-ACL permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
        Current peer: 192.168.20.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                TRANS,
        }
        Interfaces using crypto map VPN-MAP:
                FastEthernet0/1

SITE1#
SITE1#
```

Figure 4.4.6 : Affichage des `crypto map`.

▷ En fin, nous allons effectuer un *sniffing* à l'aide de Wireshark pour visionner le trafic échangés entre les deux sites. Un "`Ping 192.168.2.2 -t`" de PCBejaia vers PCAlger nous donne le résultat suivant :

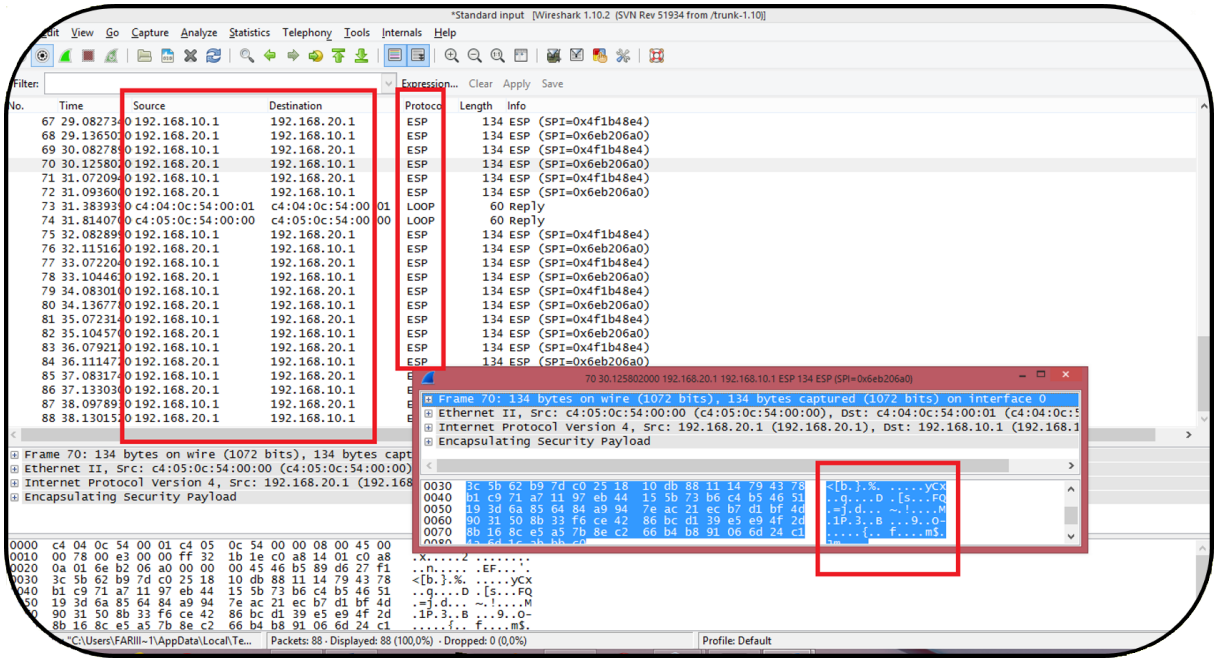


Figure 4.4.7 : Capture d'un échange de données sécurisé entre SITE1 et SITE2.

Nous remarquons très bien que le flux d'informations circulant entre les deux LANs est crypté, et que les adresses machine (sources et/ou destinations) n'apparaissent pas, cela confirme que le VPN fonctionne parfaitement.

4.5 Conclusion

Au cours de ce chapitre, nous avons implémenté une solution de sécurité pour le réseau de NAFTAL qui permet de remédier aux différents problèmes et failles de sécurité constatées lors de stage effectué au sein du district GPL de Béjaïa.

Le simulateur GNS3 nous a permis à partir de son interface graphique de concevoir et tester notre topologie comprenant des commutateurs, des routeurs et des stations de travail ainsi que leurs configurations qui nous a permis de bien concrétiser notre travail. Après la configuration nous avons exposé quelques tests afin de vérifier le bon fonctionnement et la fiabilité de VPN créé.

Conclusion générale

Les réseaux d'entreprises ont évolués au fil du temps à une vitesse exponentielle. L'interconnexion de ces réseaux à Internet les a directement exposés à des menaces informatique.

L'étude que nous avons menée nous a conduits à découvrir l'une des mesures de sécurité à déployer, pour assurer des services de la sécurité au sein du district GPL de NAFTAL. Il s'agit de la mise en œuvre d'un réseau privé virtuel qui demande de la rigueur, car il s'agit en fait de la combinaison de trois technologies (cryptage, routage, firewalling). Ce VPN interconnecte à l'aide d'un tunnel IPSec deux LANs de NAFTAL à savoir, le district GPL de Béjaïa et la direction générale à Alger.

En effet, nous avons présenté un travail divisé en deux parties, la première est une synthèse de l'état de l'art et comprend les deux premiers chapitres, dont le premier a porté sur la sécurité informatiques et les différents outils et techniques de sécurisation d'un réseau, dans le second chapitre nous avons présenté l'une des ces techniques de sécurisation qui est les VPNs.

L'aspect pratique a fait l'objet de la deuxième partie, qui comporte à son tour deux chapitre, dont le premier a porté sur la présentation de l'entreprise d'accueil et l'étude du réseaux requis par celle-ci, le second chapitre de cette partie a porté sur la mise en place de la solution proposée pour le réseau de NAFTAL, dans lequel nous avons expliqué les différente étapes de configuration et de la simulation de la solution.

Ce travail nous a permis d'avoir une visibilité concrète sur un domaine très important, qui est la sécurité informatique. Il est clair que le stage effectué au sein du district NAFTAL GPL de Béjaïa a été très bénéfique quant à l'application de nos connaissances scientifiques et le jumelage de la théorie à la pratique.

Annexes

Annexe A

Audit de sécurité

A.1 Présentation d'un audit

L'audit est l'examen professionnel qui consiste en une expertise par un agent compétent et impartial et un jugement sur l'organisation, la procédure ou une opération quelconque d'une entité. L'audit est une amélioration continue, car il permet de faire le point sur l'existant (état des lieux) afin d'en dégager les points faibles et/ou non conformes (suivant les référentiels d'audit). Cela, afin de mener par la suite les actions adéquates qui permettront de corriger les écarts et disfonctionnements constatés[27].

A.1.1 Délimitation du besoin et des objectifs de l'audit

Selon l'Association Française de l'Audit et du conseil Informatique, les entreprises font appel à une procédure d'audit pour majoritairement s'assurer que les enjeux stratégiques de la direction sont correctement pris en considération à l'intérieur du système d'information de l'entreprise. En effet, l'audit permet avant tout de savoir si le système est perfectible, et dans quelles mesures, dans le but d'assurer l'adéquation du système informatique aux besoins de l'entreprise.

Dans une période où la technologie va plus vite que l'innovation, et où la concurrence est féroce, il faut sans cesse prendre garde à ne pas être dépassé dans les moyens fonctionnels et technologiques mis en place. Cependant, chaque organisation a ses raisons qui la poussent à engager une procédure d'audit, l'important est de bien les cerner pour connaître ses objectifs[28].

A.1.2 Types d'audit existants

Du point de vu général, il existe deux types d'audit[29] :

- **Interne :** L'audit interne se base sur la tâche d'évaluation, de contrôle, de conformité et de vérification. Il est exercé d'une façon permanente par une entreprise. Cet audit a pour mission de déceler les problèmes et de donner des solutions.
- **Externe :** L'audit externe est une opération volontaire décidée par la direction d'une entreprise pour faire apprécier la conformité de son système avec un référentiel, et ce par une firme d'audit tiers reconnu pour ses compétences et sa notoriété dans les secteurs d'activités concernés.

A.1.3 Présentation de l'audit de la sécurité informatique

Un audit informatique a pour objectif principal l'évaluation des risques associés aux activités informatiques, il permet également de s'assurer de l'adéquation du système informatique aux besoins de l'entreprise et de valider que le niveau de services est adapté aux activités de celles-ci. Un audit informatique est un diagnostic et un état des lieux extrêmement fin du système informatique de l'entreprise. Il est réalisé afin de définir des axes d'amélioration et d'obtenir des recommandations pour palier aux faiblesses constatées[30].

A.1.4 Cycle de vie d'un audit de sécurité

Le processus d'audit de sécurité est un processus répétitif et perpétuel. Il se présente essentiellement suivant deux parties comme le présente le schéma illustré dans la figure ci-dessus :

- L'audit organisationnel et physique
- L'audit technique Une troisième partie optionnelle peut être également considérée, il s'agit de l'audit intrusif (test d'intrusions).

Enfin un rapport d'audit est établi à l'issue de ces étapes. Ce rapport présente une synthèse de l'audit, il présente également les recommandations à mettre en place pour corriger les défaillances organisationnelles ou techniques constatées[30].

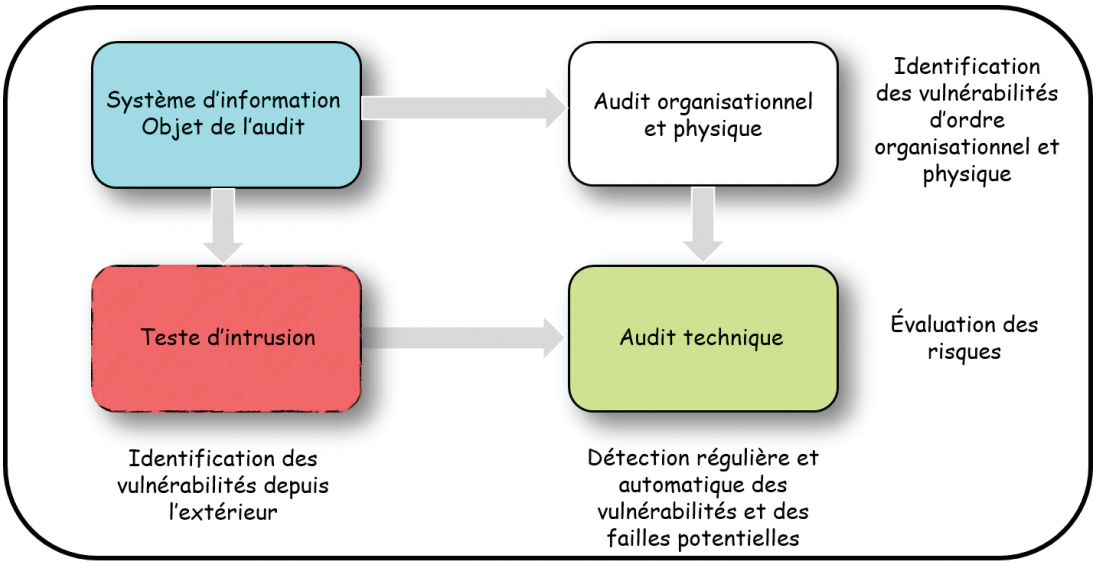


Figure A.1 : Cycle de vie d'audit de sécurité.

Annexe B

Installation de VirtualBox

– Pour télécharger VirtualBox allez sur le site : `https://www.virtualbox.org/wiki/Downloads`.
– Choisir la version adéquate au système que vous souhaitez utiliser, lancez l'installation.
– Cliquer sur l'icône dans le bureau et une fenêtre apparait comme suit :

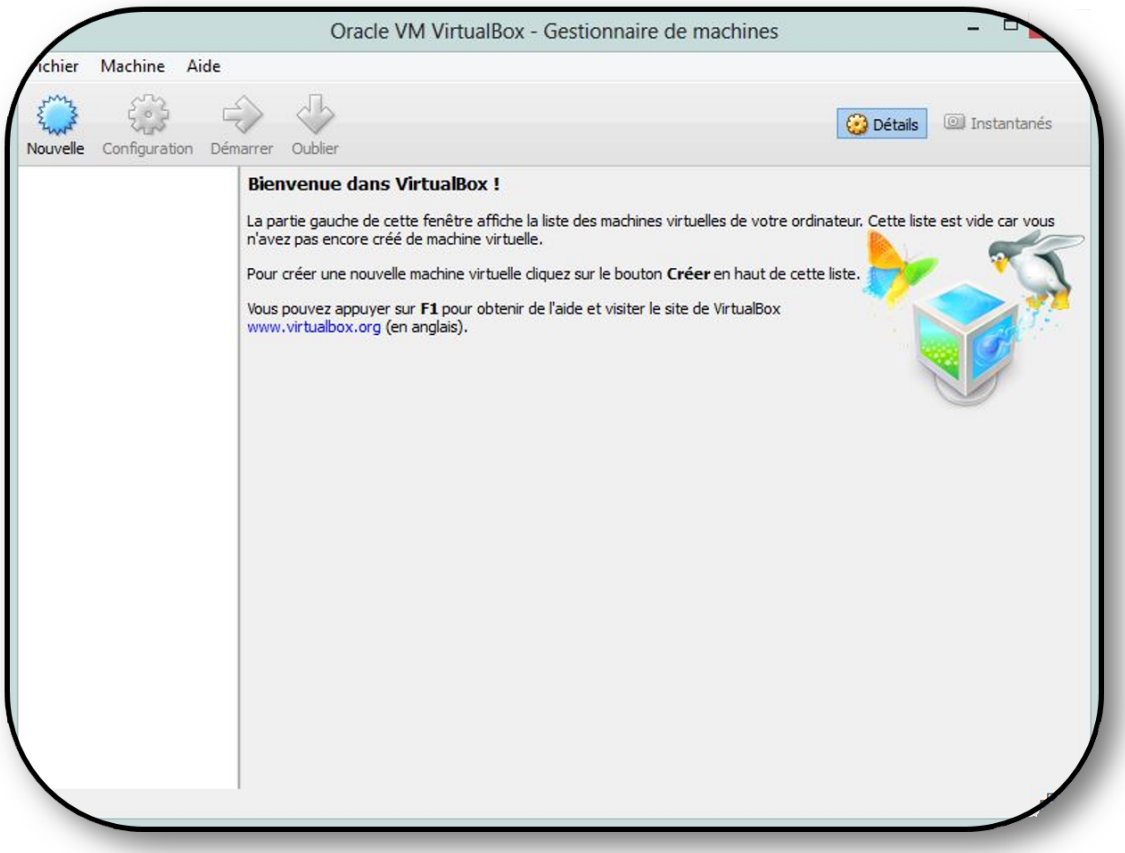


Figure B.1 : Lancement de VirtualBox.

– Pour configurer une nouvelle machine, cliquer sur l'icône sur "Nouvelle", et suivez l'assistant de création de machines virtuelles.

Figure B.2 : Guide de création d'une machine virtuelle.

– Une fois crée, la machine apparaitra sur le menue gauche. Pour lui choisir un système d'exploitation sélectionnez-la et cliquez sur "Configuration" puis "stockage".

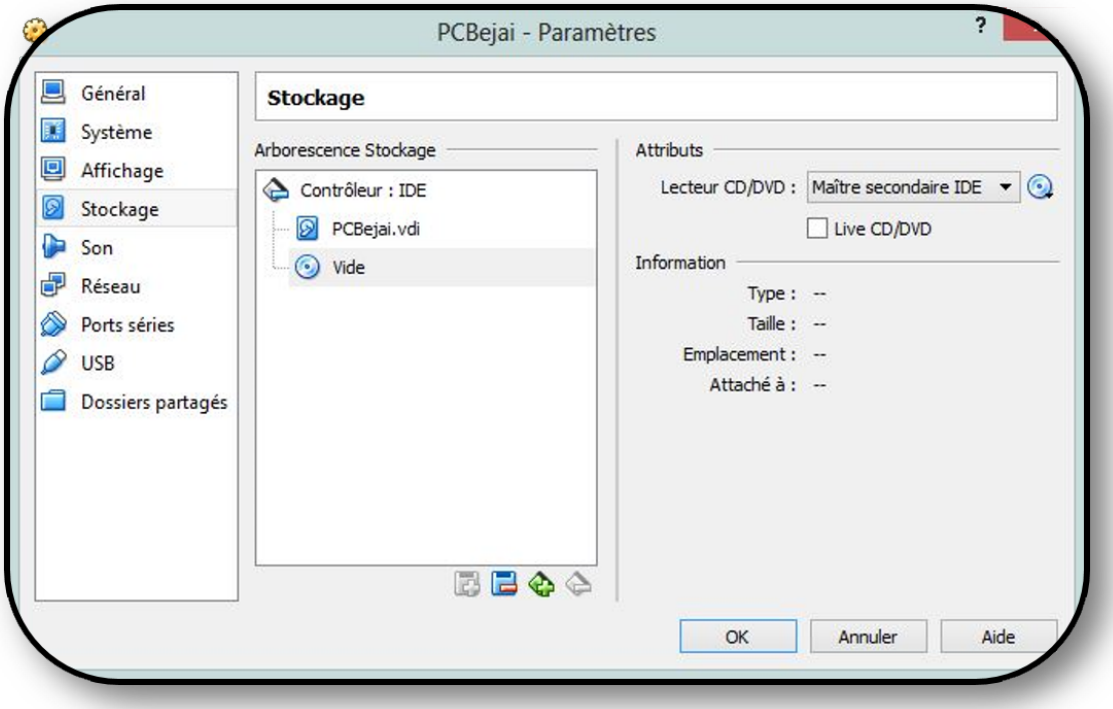


Figure B.3 : Guide de création d'une machine virtuelle-Paramètres.

– Cliquez sur la petite icône de CD la plus à droite. Puis cliquez sur "Choisissez un fichier de CD/DVD virtuel".
– Démarrez la machine virtuelle, et suivez le guide d'installation jusqu'à la fin.

Annexe C

Attestation

Etablissement/Structure NAFTAL GPL BEJAIA / Dept Informatique

Nom, prénom et fonction du responsable Albani Mourad chef dept.

ATTESTATION

Je soussigné, Monsieur/~~Madame~~ Albani Mourad .., responsable du departement informatique .., atteste que le produit fourni par les étudiants

1. DJOULANE ATHMANE
2. KADI FARID ..
3. ..
4. ..
5. ..
6. ..
7. ..
8.
9. ..
10.

dans le cadre de leur stage de fin de cycle de Master. a été testé à notre niveau et a satisfait dans sa globalité les besoins cadrés par leur thème.

Fait à Bejaia .., le 16-06-2014

Signature et Cachet

BRANCHE GPL NAFTAL Département Informatique DISTRICT BEJAIA

Le Chef de Dpt Informatique

M. ALBANI

NB. A joindre en annexe du mémoire et fourni aux membres de jury avant la soutenance.

Bibliographie

[1] D. Valois, C. Lorens et L. Levier : *Tableaux de bord de la sécurité réseau, 2e édition*. Eyrolles, 2006.

[2] A Richard : An introduction to computer security. Rapport technique, Computer Science Department, University of California, Santa Barbara, California, USA, 2010.

[3] DESWARTE Yves : Comment mesurer la sécurité informatique. Rapport technique, Laboratoire d'Analyse et d'Architecture des Systèmes, CNRS, 2000.

[4] BLOCH Laurent et WOLFHUGEL Christophe : *Sécurité Informatique : Principes et méthodes*. Editions Eyrolles, 2009.

[5] ELUARD Marc : *Analyse de sécurité pour la certification d'applications Java Card*. Thèse de doctorat, Ecole doctorale MATISSE de l'université de Rennes 1, 2001.

[6] Malicious and accidental fault tolerance in internet applications : Towards taxonomy of intrusion detection systems and attacks. Rapport technique, Laboratoire MAFTIA Project Delivrable, 2001.

[7] Introduction a la sécurite informatique, 2014. `http://www.commentcamarche.net/contents/secu/secuintro.php3`.

[8] AUBEUF-HACQUIN Yoann : Mise en place d'un système de détection d'intrusion sur le réseau d'une entreprise. Rapport technique, Université Fran cois-Rabelais Tours, 2009.

[9] CARPENTIER Jean-F : *La sécurité informatique dans la petite entreprise, Etat de l'art et bonnes pratiques*. Edition ENI, 2009.

[10] BOUMASSATA Meriem : Vérification de code pour plates-formes embarqués. Mémoire de D.E.A., Université El-Hadj Lakhdar de Batna, 2011.

[11] BOUDAOUD KARIMA : Analyse des attaques de sécurité par rapport aux propriétés des agents intelligents. Rapport technique, 1998.

[12] KHAC PHUNG : La sécurité dans les réseaux hauts débit. Rapport technique, Institut de la francophonie pour l'informatique (IFI), 2005.

[13] B. KENYON, S. ANDRES et E. P. BIRKHOLZ : *Security Sage's Guide to Hardening the Network Infrastructure*. Syngress Publishing, 2004.

[14] L.MÉ, Z.MARRAKCHI, C.MICHEL, H.DEBAR et F.CUPPENS : *La détection d'intrusions : les outils doivent coopérer*. evue de l'électricité et de l'électronique, 2001.

[15] MUNYICK GABY : Mise en place d'un vpn sstp avec ad cs sous 2008 serveur pour les clients mobiles : cas de la banque centrale du congo. Mémoire de D.E.A., IUMM, ingenieur inforamticien, 2011. `http://www.memoireonline.com/`.

[16] LASSERRE XAVIER et KLEIN THOMAS : Réseaux Privés Virtuels - Vpn, 2014. `http://www.frameip.com/vpn/`.

[17] LANDRY WILLIAM : Mise en place d'une architecture vpn mpls avec gestion du temps de connexion et de la bande passante utilisateur. Mémoire de D.E.A., Institut d'ingenierie d'informatique de Limoge, ISTDI - Master Europeen en Informatique OPTION : Administration systèmes résaux, 2009.

[18] ORACLE. *Sécurisation du réseau dans Oracle Solaris 11.1*, 2013. `http://docs.oracle.com/cd/E38898_01/html/E38852/ipsectm-1.html#scrolltoc`.

[19] ROUDEL PHILIPPE et MAROC ALAIN : Les vpns et les protocoles slip, ppp, pptp, l2f, l2tp, lcp, ipsec, mpls, nat, 2002. `shttp://wapiti.telecom-lille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2001ttv02/Roudel_Maroc/main.PDF`.

[20] Ipsec : Internet protocol security, 2014. `https://www.securiteinfo.com/services/formations.shtml`.

[21] Réseau informatique, 2014. `https://www.cyberlycee.fr/reseau_barthou/res_ini.html`.

[22] Présentation de gns3, 2014. `http://www.gns3.net`.

[23] Christophe FILLIOT et BERENGUIER JEAN-MARC : Dynamips : Un émulateur de routeur cisco sur pc. Rapport technique, Université de Technologie de Compiègne, Service Informatique.

[24] Qemu, 2014. http://wiki.qemu.org/Main/Page.

[25] Créer un serveur virtuel avec virtualbox, 2014. http://colibri-libre.org.

[26] 2014. http://www.wireshark.org/docs/.

[27] 2014. http://www.rapibus.sto.ca/index.php?id=53.

[28] 2014. http://www.developpement-durable.gouv.fr/Systemes-de-transportintelligents,12596.html.

[29] Plan stratégique 2008-2018 du nouveau-brunswick sur les systèmes de transport intelligents (sti). Rapport technique, Province du Nouveau-Brunswick Case postale 6000 Fredericton (N.-B.) E3B 5H1, 2008.

[30] 2014. http://road-network-operations.piarc.org/index.php?option=com_content&task=view&id=42&Itemid=71&lang=fr.

Résumé

Le travail réalisé dans ce mémoire de fin d'étude fait état des résultats obtenus lors de la proposition d'une solution de sécurité pour le LAN étendu de NAFTAL. Il s'agit d'une architecture VPN IPSec site-to-site, reliant le district GPL de Béjaia avec la direction générale de NAFTAL à Alger. Il en ressort que la technologie VPN basée sur le protocole IPSec est l'un des facteurs clés de succès qui évolue et ne doit pas passer en marge des infrastructures réseaux et des systèmes d'information qui progressent de façon exponentielle. En effet, grâce à cette nouvelle technologie, nous avons offert aux employés une solution pour partager de façon sécurisée leurs données via le protocole IPSec qui est le principal outil permettant d'implémenter les VPNs.

Mots clés : VPN, RPV, IPSec, Tunneling, Site-to-site.

Abstract

The work done in this memory of end of study reported the results achieved at the proposal of asecurity solution for the extended LAN of NAFTAL. It is an architecture site-to-site of IPSec VPN, linking the GPL district of Bejaia with NAFTAL branch in Algiers. It appears that based on IPSec VPN technology is one of the key factors of success that evolves and should not go outside the network infrastructure and information system progressing exponentially. Indeed, with this new technology, we have offered employees a solutionto securely share their data via the IPSec protocol, which is the primary tool to implement VPN.

Keywords: VPN, RPV, IPSec, Tunneling, Site-to-site.