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

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

Mémoire de Master
en Informatique
Option
Administration et sécurité des réseaux informatiques
Thème

Mise en oeuvre d'une solution de sécurité basée sur les VPN et SNORT.

"Cas d'étude : Entreprise NAFTAL GPL"

Présenté par :

M^elle ***OUATMANI*** **Amina**
M^elle ***ZAOUCHE*** **Rahima**

Soutenu devant le jury composé de :

Président	M^r ***BADACHE*** **Abderahman**
Examinateur	M^r ***SALHI*** **Nadir**
Examinateur	M^r ***KHENOUS*** **Lachemi**
Encadreur	M^r ***HAMOUMA*** **Moumen**

Promotion 2012/2013

Dédicaces

Ce modeste travail est dédié à ma famille ainsi qu'aux personnes qui sont chères à mon coeur.

ZAOUCHE Rahima

Dédicaces

La vie n'est qu'un éclair,
et le jour de réussite est un jour très cher :
A mes parents,
A mon mari,
A mes frères et soeurs,
A toute ma famille et la famille "ZAOUCHE",
A mes amis et collègues, et tous ceux qui m'ont aidé ;

OUATMANI Amina

Résumé

Suite à notre étude sur la sécurité dans les réseaux informatiques, on se rend bien compte que le réseau d'une entreprise est vulnérable à tout type d'attaques, que ça soit au niveau du réseau local ou en dehors de celui-ci. L'intégrité ,la disponibilité et la confidentialité des données qui circulent au sein d'un réseau informatique est une contrainte de taille. Diverses technologies existent dans le but d'assurer les objectifs de la sécurité informatique à savoir : l'authentification, la confidentialité, l'intégrité des données et la non répudiation.
La mise en place d'un réseau privé virtuel est l'une des technologies les plus récentes, qui consiste à assurer un transport fiable des données traversant le réseau.

Afin d'assurer la centralisation des informations associées aux utilisateurs, la mise en place d'un annuaire LDAP a été faite.
Dans le but de renforcer la sécurité de l'entreprise " NAFTAL GPL ", un système de détection d'intrusions nommé " SNORT", qui consiste à pouvoir détecter les violations de sécurité lorsqu'elles se produisent a été mis en place.

Mots-clés : Réseau privé virtuel, couche de sockets sécurisée, SNORT, LDAP.

Abstract

Following our study on security in computer networks, we can realize that the corporate network is vulnerable to all kinds of attacks, in the local network or outside. The integrity and confidentiality of the data that flows in a network is a real constraint.Various technologies exist in order to achieve the objectives of computer security which are : authentication, confidentiality, data integrity and non-repudiation. The establishment of a virtual private network is one of the latest technologies, which is to provide a reliable data transport through the network.

To ensure the centralization of information related to users, setting up an LDAP directory has been made. To enhance the security of " NAFTAL GPL ", an intrusion detection system named "Snort," which is able to detect security violations when they occur has been established.

Keywords : Virtuel Private Network, Secure Sockets Layers, SNORT, Lightweight Directory Access Protocol.

LISTE DES ABRÉVIATIONS

AH	**A**uthentifacation de **H**eader
ACLs	**A**ccess **C**ontrol **L**ist
CRL	**C**ertificate **R**evocation **L**ist
DES	**D**irectory **E**ntry **S**ervice
DN	**D** Distinguished textbfName
DIT	**D**irectory **I**nformation **T**ree
ESP	**E**ncapsulating-**S**ecurity **P**lauload
FCS	**F**rame-**C**heck **S**equence
HIDS	**H**ost **I**ntrusion **D**etection **S**ystem
HDLC	**H**igh **D**ata **L**evel **C**ontrol
IDS	**I**ntrusion **D**etection **S**ystem
IP	**I**nternet **P**rotocol
IPX	**I**nternet **P**acket **X**change
ISO	**I**nternational **S**tandartization **O**rganisation
IPSec	**I**nternet **P**rotocol **Sec**urity
IKE	**I**nternet **K**ey **E**xchange
LDAP	**L**ightweight **D**irectory **A**ccess **P**rotocol
LAC	**L**L2TP **A**ccess **C**oncentrator
LCP	**L**ink **C**ontrol **P**rotocol
L2F	**L**ayer **2**two **F**orwarding
LNS	**L**L2TP **N**etword **S**erver
LDIF	**L**ighit-weight **D**ata **I**nter change **F**ormat
NCP	**N**etwork **C**ontrol**P**rotocol
NIDS	**N**etwork **I**ntrusion **D**etection **S**ystem
OID	**O**bjectif **ID**entifier

PPP	**P**oint to **P**oint **P**rotocol
PPTP	**P**oint to **P**oint **T**unneling **P**rotocol
RFC	**R**equest **F**or **C**omments
RDN	**R**elative **D**istinguished **N**ame
SET	**S**ecure **E**lectronic **T**ransaction
SSH	**S**ecure **SH**ell
S-http	**S**ecure http
SSL	**S**ecure **S**ocket **L**ayer
TCP/IP	**T**ransport **C**ontrol **P**rotocol **I**nternet **P**rotocol
VPN	**V**irtual **P**rivate **N**etwork

TABLE DES MATIÈRES

LISTE DES TABLEAUX

TABLE DES FIGURES

INTRODUTION GÉNÉRALE

Les réseaux informatiques, composés d'équipements interconnectés, ont aujourd'hui beaucoup plus d'importance qu'ils en avaient, il ya quelques années. En effet, les entreprises dès leur création n'hésitent pas à mettre en place un réseau informatique pour faciliter la gestion de leur infrastructure.

Les technologies utilisées pour transmettre des données d'un ordinateur à un autre font appel à un grand nombre de composants. Depuis l'avènement des premiers réseaux IP, les problèmes de sécurité se sont diversifiés et ont conduit au développement de nouvelles techniques de sécurité. Du cryptage à l'implémentation d'une architecture de sécurité et à la mise en place des firewalls, les réseaux IP ont connu une amélioration au niveau de l'aspect sécurité.

Aujourd'hui, de très nombreuses entreprises, quelle que soit leur taille ou leur activité sont connectées à Internet. Mais l'utilisation d'Internet pose un problème de taille, il s'agit de la sécurité des échanges. Pour garantir l'intégrité et l'inviolabilité des données conservées et échangées, le système d'information doit adapter les outils et les technologies appropriés pour assurer les objectifs de la sécurité.

L'une des solutions envisagée est l'implémentation de réseaux privés virtuels " VPN ", qui permet de renforcer l'intégrité et la confidentialité lors de l'échange de données sur un réseau.

Avec le développement des réseaux, les services offerts se sont multipliés. On retrouve couramment sur un même réseau un service de messagerie, un service de fichiers, un service web, etc. Avant d'accéder à un service, il est souvent demandé aux utilisateurs de s'authentifier afin de se faire reconnaitre par un service en question. Le concept d'annuaire prend alors son sens, il permet de centraliser toutes les informations liées aux utilisateurs et aux services dont ils ont accès. C'est dans ce contexte là, que nous avons envisagé d'assurer une authentification

des utilisateurs à partir de l'annuaire LDAP.

Le manuscrit a été organisé en quatre chapitres :

Le premier chapitre s'intitule " Organisme d'accueil et étude du contexte ", dans lequel nous présenterons l'entreprise d'accueil " NAFTAL GPL" ainsi que le réseau requis par celle-ci, suivi de la définition du contexte du projet à réaliser.

Le deuxième chapitre est dédié à "La sécurité des réseaux informatiques". En effet, nous décrierons les concepts associés à la sécurité des réseaux informatiques ainsi que la nécessité de la mise en oeuvre d'une sécurité au sein d'un réseau informatique.

Le troisième chapitre quant à lui concerne " Les réseaux privés virtuels ", nous présenterons dans ce chapitre tous les concepts associés aux réseaux privés virtuels, ainsi que les divers protocoles que comprennent ce type de réseaux.

La réalisation et l'implémentation fera l'objet du quatrième chapitre, dans lequel nous illustrerons les différentes étapes nécessaires à l'accomplissement de notre projet suivi des tests associés.

Enfin, nous conclurons ce travail en résumant les connaissances acquises durant la réalisation du projet.

CHAPITRE 1

ORGANISME D'ACCUEIL ET CONTEXTE DU PROJET

1.1 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 tâches 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 "Division GPL".

1.2 Présentation de l'entreprise NAFTAL

1.2.1 Historique

L'entreprise ERDP (Entreprise de Raffinage des Produits Pétroliers), issue de SONATRACH, a été créé 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, la raison sociale de la société change suite à cette séparation.

NAFTAL est désormais chargée de la commercialisation et de la distribution des produits pétroliers et dérivés. A partir de 1998, elle change de statut et devient société par action filiale à 100NAFTAL est réparti en 19 districts sur le plan national, dont le district de Bejaia.
Elle intervient dans les domaines de :

- Formulation de bitumes ;
- L'enfûtage des GPL *"Gaz de Pétrole Liquéfié"* ;
- Distribution, stockage et commercialisation des carburants, GPL, lubrifiants, bitumes, pneumatiques, GPL/carburant, produits spéciaux ;
- Transport des produits pétroliers.

1.2.2 Les activités principales de l'entreprise

a) La commercialisation de carburants pour la motrice essence et diesel :

- Essence normale ;
- Essence Super ;
- Essence Super Sans plomb ;
- Gas Oïl/CPL/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.

1.3 Présentation du District GPL

1.3.1 Les activités principales du District GPL

- Commercialiser les GPL vrac et conditionnés, leurs emballages et accessoires ;
- Veiller au respect des normes et consignes de sécurité sur toute la chaîne GPL (transport, installation d'enfûtage 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 GPL.

1.3.2 Organisation de la branche GPL

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

- Direction des ressources humaines ;
- Direction administration et moyens ;
- Direction finances et comptabilités ;
- Direction technique et maintenances ;
- Direction hygiène 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 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)Activité commerciale et marketing du district : les taches associées à cette activité sont comme suit :

- 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 de coûts ;
- 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 (BEJAIA ; JIJEL ; BOUIRA et BBA) ;
- Assurer l'approvisionnement et la commercialisation des produits GPL sur l'ensemble des quatre wilayas ;
- Elaborer des plans en liaisons avec d'autres districts visant la couverture du marché national en produits GPL.

1.3.2.1 Organigramme du District GPL

Le schéma suivant illustre, l'organigramme établi par la branche GPL d'Alger depuis 2001 :

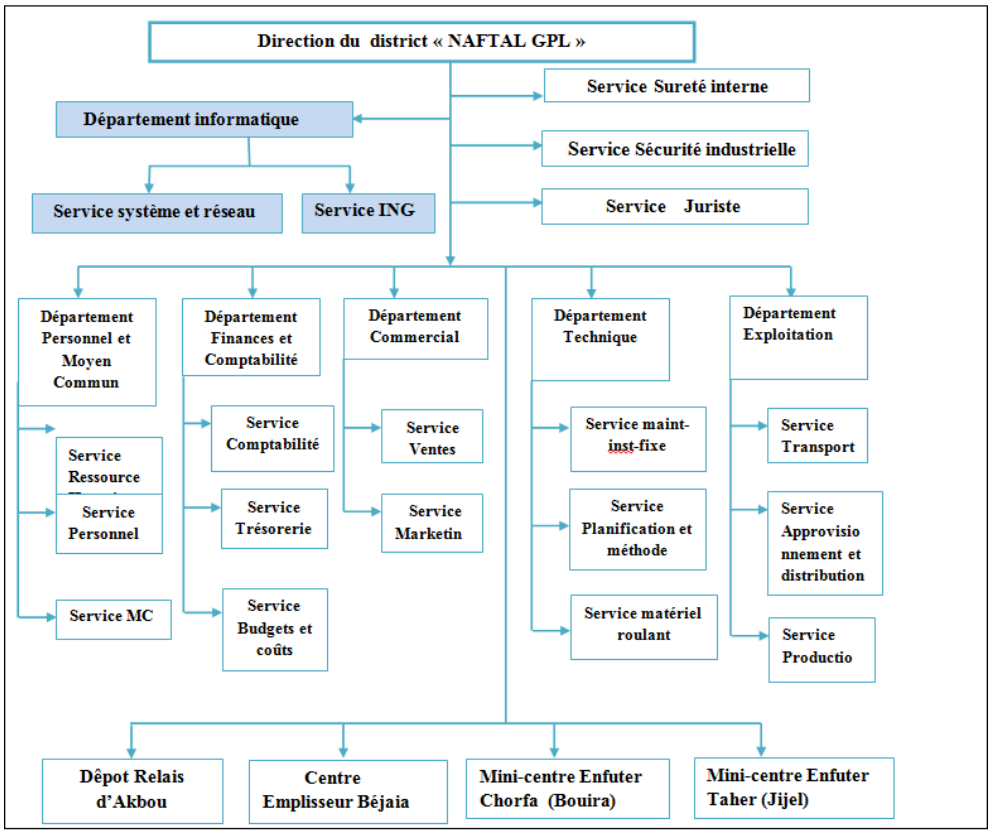


FIGURE 1.1 – Organigramme du District GPL Bejaia.

1.3.2.2 Description et rôle de chaque service au sein de l'entreprise NAFTAL

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

▷ **Service Sécurité Industrielle :** ce service se charge d'assurer les tâches suivantes :

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

▷ **Service Juriste** .

▷**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'assurer les taches suivantes :

- Suivi des performances des moyens de transport ;

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

▷**Département Technique :** ce département quant à lui assure la gestion des projets dans leurs phases d'étude et de la 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 de lui permettre l'écoulement.

▷**Département Finances et Comptabilité** :qui est chargé de procéder aux écritures comptable conformément aux préconisations du système comptable financière ; il a comme mission :

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

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

1.4 Présentation du département informatique

1.4.1 Le rôle du département d'informatique de GPL

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

1.4.2 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.

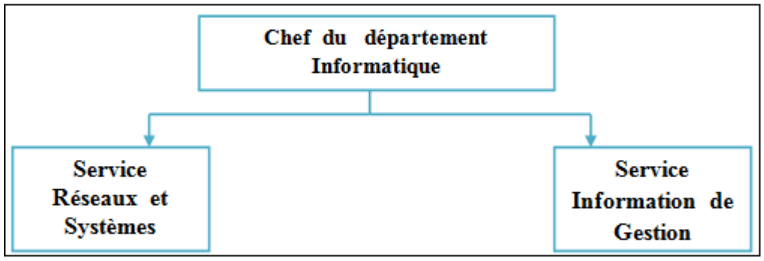


FIGURE 1.2 – Organigramme du département informatique.

1.4.2.1 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 assure :

- Maintenance de matériels informatique ;
- Maintenance des logiciels, système et application ;
- Suivi des différentes activités administrateur réseau.

▷ Service Information de Gestion assure :

Ce service se charge à remplir certaine tâches et responsabilités :

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

1.5 Architecture réseau du district GPL

Une architecture réseau est un ensemble d'équipements matériels et logiciels interconnectés en réseau, afin de régir des activités informatiques collectives, en centralisant ou répartissant les ressources et les tâches 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'architecture de l'entreprise NAFTAL GPL, dispose d'un réseau LAN constitué d'un ensemble d'équipements matériels et logiciels. GPL de Bejaia se compose de quatre armoires séparées, chaque armoire, regroupe un commutateur de niveau 2, un onduleur, un panneau de brassage. L'Armoire située au département informatique est reliée en cascade " câble RJ45 " avec les autres armoires existantes (département ressource humaine, département archive) et celle située au département commerciale est liée en fibre optique, par contrainte de distance entre ces deux départements soit 150m.

Le département informatique comprend un serveur qui offre certains services, on cite parmi eux : FTP, DNS, DHCP et l'annuaire Active Directory. Pour qu'une machine interne puisse accéder à un réseau étendu, il est impératif qu'elle passe en premier lieu par un mécanisme de filtrage, qui représente dans notre cas le " pare-feu " et pour se connecter à Internet, le LAN de NAFTAL est connecté à un fournisseur d'accès, en passant par le routeur qui se trouve dans l'armoire du département.

La figure suivante illustre l'architecture décrite :

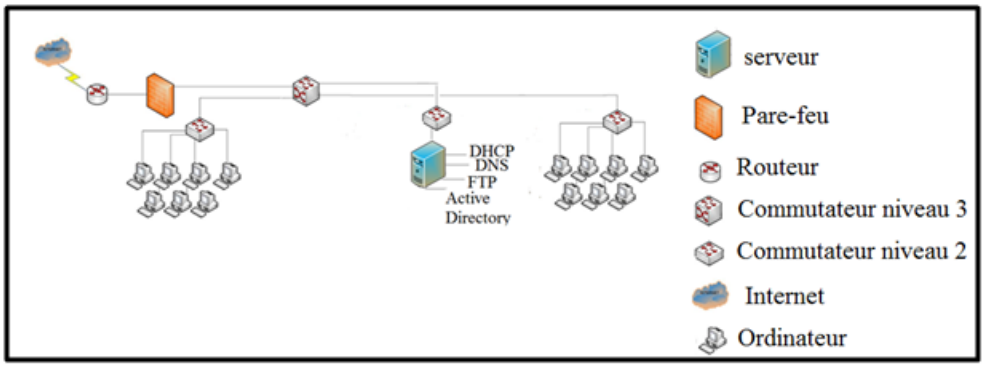


FIGURE 1.3 – Architecture du réseau du district GPL.

1.5.1 Classification des équipements réseaux

A présent, nous allons définir les différents équipements réseaux utilisés au sein de l'entreprise NAFTAL "GPL", les équipements varient selon les fonctions requises et les technologies choisies.

1.5.1.1 Matériel actif

On appelle matériel actif, tout matériel comportant un équipement électronique chargé d'assurer la répartition des signaux, entre les différentes branches d'un réseau informatique[1].

a) Aspect réseau Il s'agit des équipements permettant de faire transiter les données entre les stations de travail, on cite :

- Les commutateurs ;
- Les routeurs ;
- Les concentrateurs.

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

- **Le contrôleur de domaine "Active Directory" :** l'Active Directory est un service d'annuaire, qui fournit un certain nombre de différents services relatifs au stockage des ressources du réseau.

  Nous citons ci-dessous certaines caractéristiques de l'Active Directory[1] :

  - *Approche Organisée :* Active Directory met de l'ordre dans le réseau de l'entreprise, à partir de l'organisation apportée aux ressources du réseau, tels que les comptes d'utilisateurs, dossier partagés, imprimantes .. ;
  - *Facilité d'administration :* le contrôleur de domaine nous permet la simplicité d'administrer le réseau et offre une excellente tolérance aux pannes ;
  - *On retrouve aussi les différents services : DNS, DHCP, FTP.*

1.5.1.2 Matériel passif

a) Support physique de transmission : Les supports physiques utilisés au sein du réseau de NAFTAL "GPL" sont les suivants :

- **Support en cuivre :**

  - Câble à paires torsadées : on distingue deux catégories associées à ce premier[1] :
  - 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 de câbles obtenus en utilisant des conventions de câblage spécifiques sont les suivants :
    - Ethernet direct ;

- Croisement Ethernet ;
- Renversement.

Les catégories de câbles UTP utilisés par le réseau de NAFTAL " GPL " sont de catégorie 3, 4, 5, 5e, 6, 6a et 7.

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

– **Support fibre optique [1] :**

La fibre optique : Le câblage en fibre optique 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 optique 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 maîtrise ;

– **Support sans fil [1] :** le réseau de NAFTAL, dispose de points d'accès de gamme **"Aironet Cisco"**, permettant d'assurer une connexion sans fil ;

b) Les connecteurs réseau Connecteurs RJ45 : utiliser avec des câbles pairs torsadés ;

c) Les panneaux de brassage : le panneau de brassage est le point ou se concentrent tous les câbles de chaque prise murale RJ45 d'un bâtiment. Il sert à relier ces prises à un commutateur grâce à un cordon de brassage.

1.5.1.3 Autre équipement

Armoire de brassage : une armoire de brassage appelée aussi " baie de brassage " est conçue 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.)

1.6 Contexte du projet à réaliser

Dans cette partie, nous allons en premier lieu présenter le projet à réaliser, suivi des objetctifs issus à l'accomplissement de ce dernier, en second lieu nous allons dégager la problématique associée au cahier des charges de l'organisme.

1.6.1 Présentation du projet

Le projet à réaliser, s'intitule "La mise en oeuvre d'une solution de sécurité".La mise en oeuvre de ce projet permettra d'assurer un accès distant sécurisé entre les utilisateurs du district GPL et ceux du centre d'"AKBOU". Afin d'accentuer la sécurité du réseau local du siège "NAFTALGPL" et du centre d'AKBOU , nous avons jugé que la mise en oeuvre d'un système de détection d'intrusions serait intéressante au sein des deux sites.

1.6.2 Objectifs du projet à réaliser

Notre tâche principale consiste, à assurer une communication sûre et confidentielle entre les utilisateurs distants, situés dans le centre d'"AKBOU" et le serveur central situé au niveau de l'organisation GPL.
La division GPL, souhaite exploiter les avantages d'une liaison internet entre ses utilisateurs, en intégrant une connexion site à site pour d'éventuelles tâches d'administration à distance. Afin de renforcer la sécurité du réseau de l'organisme, nous avons songé à introduire un système de détections d'intrusions au sein de chaque site de l'entreprise.

1.6.3 Problématique

Assurer l'intégrité et la confidentialité des données qui traversent le réseau, est une contrainte de taille dans le monde des réseaux informatiques.
Les utilisateurs du centre d'"AKBOU", se retrouvent confronter à plusieurs problèmes tels que le problème de complexité, qui est engendré par le transfert d'information qui se fait dans de grands intervalles de temps à cause de la distance, qui sépare deux ou plusieurs secteurs de traitement de l'information dans l'arborescence de la division GPL, ce qui engendre une exécution lente des taches spécifiques. Pour pallier à ces problèmes nous avons pensé à mettre en place un réseau virtuel entre le siège de "NAFTAL GPL" et le centre d'"AKBOU".

1.6.4 Cahier des charges

Le projet à réaliser permettra d'assurer la sécurité du réseau de l'entreprise "NAFTAL GPL", en suivant l'enchainement suivant :

1. Installation et configuration d'un réseau privé virtuel entre les deux sites "District GPL" et "AKBOU" ;
2. Assurer le processus d'authentification à l'aide de l'annuaire LDAP ;
3. Installation d'un système de détection d'intrusion au sein des deux sites de l'entreprise ;
4. Les clients externes doivent avoir un accès sur le serveur central du district.

1.7 Conclusion

Les réseaux sont devenus un pilier de l'économie mondiale. Les besoins et les enjeux de ces technologies ne cessant d'augmenter, ont engendrés l'évolution de la sécurité informatique, afin d'apporter une garantie de fiabilité et de sureté.
Après avoir pris connaissance de l'architecture réseau associée à l'entreprise NAFTAL "GPL" et du contexte du projet à réaliser, nous consacrons le prochain chapitre à la présentation des objectifs de la sécurité des réseaux, ainsi que les outils qui interviennent à assurer ces objectifs.

CHAPITRE 2

SÉCURITÉ DES RÉSEAUX INFORMATIQUES

2.1 Introduction

L'interconnexion croissante des réseaux, la dépendance croissante des activités aux systèmes d'informations, induisent une vulnérabilité accrue de ces derniers vis-à-vis des atteintes à leur sécurité. Au cours de ce chapitre, nous abordons principalement les différents aspects liés à la sécurité des réseaux. Nous commençons par présenter les divers risques qu'encourent les entreprises et les menaces auxquelles sont exposés leur réseau. Dans une seconde partie, nous illustrons quelques exemples des solutions retenues actuellement pour faire face aux différents risques et menaces.

2.2 Définition de la sécurité informatique

L'information est un actif qui, comme tout autre actif pour l'entreprise, a une valeur et qui doit donc être convenablement protégée. L'approche de la sécurité de l'information permet de protéger l'information des menaces, qui pourraient corrompre sa qualité tout en garantissant la continuité des activités de l'entreprise. L'information peut prendre différentes formes. Quelle que soit la forme qu'elle revêt, quels que soient les moyens par lesquels elle est partagée, transmise ou stockée, elle doit toujours être correctement protégée[2].
Lorsque l'on parle de sécurité de l'information, il faut avoir à l'esprit certaines notions, que l'on va définir dans ce qui suit :

2.2.1 Objectifs de la sécurité informatique

Le système d'informations représente l'ensemble des données de l'entreprise, ainsi que ses infrastructures matérielles et logicielles. La sécurité informatique d'une manière générale, consiste à assurer que les ressources (matérielles/logicielles) d'une organisation, sont uniquement utilisées dans le cadre prévu [18].
La sécurité informatique vise généralement à assurer les cinq principaux objectifs suivants :

- **La confidentialité :** consiste à rendre l'information déchiffrable uniquement par les entités autorisées.
- **L'authentification :** consiste à assurer l'identité d'un utilisateur, c'est-à-dire garantir à chacun des correspondants, que son partenaire est bien celui qu'il croit être.
- **L'intégrité :** le service d'intégrité assure la conformité de l'information. L'intégrité permet aux utilisateurs d'avoir la certitude, que l'information est correcte et qu'elle n'a pas été modifiée par une entité non autorisée.
- **La non-répudiation :** il s'agit de garantir qu'aucun des correspondants ne pourra nier la transaction.
- **La disponibilité :** c'est le fait de garantir l'accès à un service ou à des ressources par les personnes autorisées.

2.2.2 Terminologie de la sécurité informatique

La sécurité informatique utilise un ensemble de terme bien spécifique, que nous énumérons dans ce qui suit [18] :

- **Vulnérabilité :** il s'agit d'une faille dans un système informatique, permettant à un attaquant de porter atteinte à l'intégrité de ce système.
- **Une attaque :** une attaque est un programme, qui exploite une vulnérabilité dans un logiciel spécifique.
- **Une contre-mesure :** il s'agit d'une procédure ou d'une technique, permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique.
- **Une menace :** il s'agit d'un événement, qui pourrait violer la sécurité d'un système d'information.

2.3 Les attaques sur un système informatique

Tout ordinateur connecté à un réseau informatique, est potentiellement vulnérable à une attaque.
Les motivations des attaques peuvent être pour divers objectifs [18] :

- Obtenir un accès au système ;

- Collectionner des informations personnelles sur un utilisateur ;
- S'informer sur l'organisation ;
- Troubler le bon fonctionnement d'un service ;
- Utiliser le système de l'utilisateur comme " rebond " pour une attaque ;
- Utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

2.3.1 Types d'attaques

Il existe trois types d'attaques [18] :

a) Attaque directe

C'est la plus simple des attaques. Le hacker attaque directement sa victime à partir de son propre ordinateur.

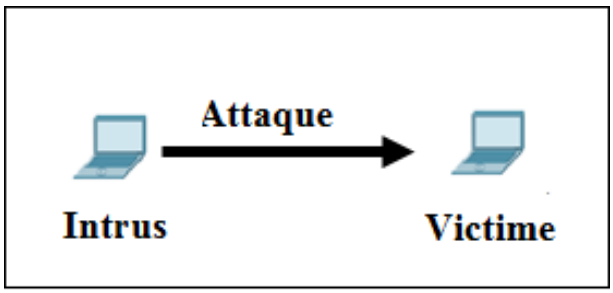


FIGURE 2.1 – Attaque directe.

b) Attaque indirecte par rebond

Cette attaque est très prise des hackers, car le principe est simple, les paquets d'attaques sont envoyés à l'ordinateur intermédiaire, qui récupère l'attaque vers la victime. D'où le terme de rebond qui permet de :

- Masquer l'identité (l'adresse IP) du hacker ;
- Utiliser éventuellement les ressources de l'ordinateur intermédiaire, car il est plus puissant pour l'attaque.

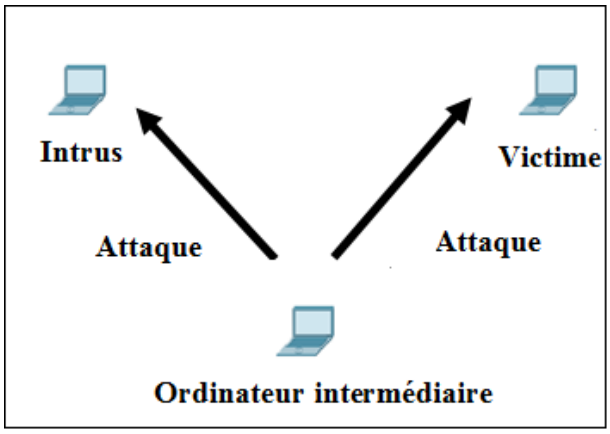


FIGURE 2.2 – Attaque par rebond.

c)Attaque indirecte par réponse

Cette attaque est dérivée de l'attaque par rebond. Cependant au lieu d'envoyer une attaque à la machine intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête, cette dernière va être envoyée à la machine victime.

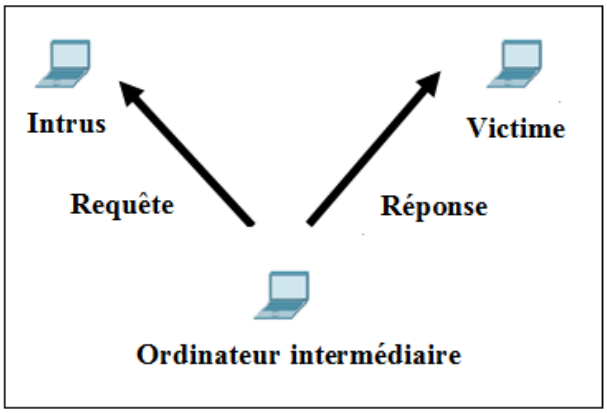


FIGURE 2.3 – Attaque indirecte par réponse.

2.3.2 Quelques attaques courantes

- **a) IP spoofing :** le spoofing consiste en une usurpation, par un utilisateur du réseau, d'une adresse IP, afin de se faire passer pour la machine à laquelle cette adresse correspond réellement.
- **b) Virus :** un virus est un programme informatique, qui s'exécute et se réplique automatiquement. Il modifie le fonctionnement d'un ordinateur sans que l'utilisateur ne s'en aperçoive ni l'autorise. Lorsqu'un virus est actif, il peut endommager des fichiers, engendrer un comportement imprévisible du système ou afficher des messages inopportuns.

- **c) Denis de service :** les attaques par Dénis de service (Dos, Denial of service) sont des attaques, qui rendent impossible l'utilisation des ressources par les utilisateurs légitimes.
- **d) Brute force :** cette méthode consiste à essayer des mots de passe d'origines des systèmes, dont le but consiste à prendre le contrôle d'une machine d'un autre réseau.
- **e) Les scanners (appelé analyseur de réseaux) :** ce sont des utilitaires permettant de réaliser un audit de sécurité d'un réseau en analysant les ports ouverts sur une machine donnée, afin de déterminer les risques en matière de sécurité.
- **f) Le flood :** un flood consiste à envoyer très rapidement de gros paquets d'informations à une personne. Cette dernière visée ne pourra plus répondre aux requêtes et le modem va donc se déconnecter, c'est cette méthode qui a été employée à grande échelle dans l'attaque des grands sites commerciaux[18].

2.3.3 Les éléments à sécuriser dans un réseau

Les réseaux sont constitués de divers équipements d'une part et de liens filaires ou non filaires, qui les relient d'autre part. Toute où partie de ces équipements peuvent être gérés par des programmes adaptés et plusieurs sortes de données y sont stockées. Certaines d'entre elles peuvent être l'objet de transferts selon des protocoles appelés protocoles de réseaux. Dans ce cadre, la sécurité concerne celle du matériel, celle des programmes, celle des données et celle des protocoles [18].

Avant de réaliser un système de sécurité, il faut spécifier d'abord les éléments à protéger. On dénombre trois types essentiels qui sont :

a) Matériel : Mis à part les ordinateurs que les réseaux relient, le matériel inclut aussi, les équipements intermédiaires comme les répéteurs, commutateurs(Switch), routeurs, serveurs, modems, firewalls, etc. La limitation d'accès à chaque matériel participe à la sécurité de l'ensemble.
b) Programme : Les programmes incluent les systèmes d'exploitation y compris les pilotes de périphériques ainsi que les logiciels programmés gérant les différents mécanismes de réseaux. Les services permettant une meilleure gestion à distance et plus d'autonomie, on parle dans ce cas-là de services réseau tels que : DHCP, DNS, FTP, etc.
c) Données : On distingue deux sortes de données ; celles qui servent au fonctionnement du réseau comme les tables de routage, les bases de données des clients, les fichiers relatifs aux droits d'accès, etc. On retrouve aussi des données qui ne sont pas en rapport avec le fonctionnement du réseau tels que : les documents et les archives.

2.4 Mise en oeuvre de la sécurité

La mise en oeuvre de la sécurité consiste à déployer des moyens et des dispositifs visant à sécuriser le système d'information, ainsi qu'à faire appliquer les règles définies dans la politique de sécurité [18].

2.4.1 Les dispositifs de protèction

Les principaux dispositifs permettant de sécuriser un réseau contre les intrusions sont :

2.4.1.1 Un antivirus

Il s'agit d'un logiciel permettant de protéger le système contre les infections informatiques (virus, vers). Ce logiciel surveille et analyse régulièrement l'ensemble des fichiers, puis filtre les contenus suspects. Une fois l'anomalie détectée, il nous en informe et la détruit. La plupart des logiciels antivirus, intègrent également une protection anti spam, qui permet d'analyser l'ensemble des messages entrants avant, qu'ils ne soient délivrés au destinataire.

2.4.1.2 Un pare-feu

un pare-feu est un système permettant de protéger un ordinateur, ou un réseau. Sa fonction principale consiste à filtrer les paquets de données échangées avec le réseau. Pour ce faire, il est placé entre l'accès Internet et le réseau local.
Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, qui constitue un intermédiaire entre le réseau local (ou la machine locale) et les réseaux extérieurs.

2.4.1.3 Un serveur proxy (serveur mandataire)

Un proxy est un ensemble de processus permettant d'éliminer la connexion directe entre les applications des clients et les serveurs. Les organisations utilisent les proxys pour permettre à des machines de leur réseau d'utiliser Internet sans risque que les utilisateurs de l'extérieur ne soient capables d'accéder à ce réseau.

2.4.1.4 Un système de détection d'intrusions

La détection d'intrusions **(IDS :*Intrusion Detection System*)** est définie comme étant un mécanisme écoutant le trafic réseau de manière furtive, afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une stratégie de prévention sur les risques d'attaques. Il existe différents types d'IDS, que l'on classe comme suit [4] :

a) Système de détection d'intrusions de "réseau" **NIDS** (**N**etwork **IDS**) : un NIDS analyse de manière passive les flux transitant sur le réseau et détecte les intrusions en temps réel, en d'autres termes, un NIDS écoute tout le trafic réseau, puis l'analyse et génère des alertes si des paquets semblent dangereux.

- Principe de fonctionnement d'un IDS :

  La détection d'attaques repose sur des techniques de sondage (une sonde permet la capture de paquets), des tentatives de compromissions de systèmes, d'activités suspectes internes, des activités virales ou encore audit des fichiers de journaux(logs). Le fonctionnement d'un IDS repose sur les principes suivants :

  - Le principe de détection.
  - Le comportement de l'IDS après détection.
  - Les sources de données.

- Approches permettant la détection d'une intrusion :
  - Approche par signature : cette technique s'appuie sur la connaissance des techniques utilisées par les attaquants pour déduire des scénarios typiques. Elle tient compte des signatures d'attaques existantes (ensemble de caractéristiques permettant d'identifier une activité intrusive, qui peut représenter une chaine alphanumérique, une taille de paquet inhabituelle, une trame formatée de manière suspecte,...).
  - Approche comportementale : cette technique consiste à détecter une intrusion en fonction du comportement passé de l'utilisateur. Il faut préalablement dresser un profil utilisateur et déclencher une alerte lorsque des événements hors profil se produisent.

b) Système de détection d'intrusions de type "hôte" **HIDS** (**H**ost **IDS**) : un HIDS est généralement placé sur des machines sensibles, susceptibles de subir des attaques et possédant des données sensibles pour l'entreprise.

c) Système de détection d'intrusions "hybride" : il s'agit d'un système capable de réunir des informations provenant d'un système HIDS ainsi que d'un NIDS. Généralement utilisé dans un environnement décentralisé, il permet de réunir les informations de diverses sondes placées sur le réseau [4].

2.4.1.5 Les protocoles de sécurité

Un protocole est un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau. Sur Internet, les protocoles utilisés font partie d'une suite de protocoles TCP/IP, tel que la plupart de ces protocoles ne sont pas sécurisés lors de la transmission

des données sur le réseau. Les protocoles sécurisés ont été mis au point, afin d'encapsuler les messages dans des paquets de données chiffrées. On cite parmi ces protocoles les suivants [18] :

a) Protocole SSH (Secure SHell)

Il permet à des services TCP/IP d'accéder à une machine à travers une communication chiffrée appelée "tunnel".

b) Protocole SSL (Secure Socket Layer)

SSL est un procédé de sécurisation des échanges, développé par Netscape. Il a été conçu pour assurer la sécurité des transactions effectuées via Internet (notamment entre un client et un serveur).

SSL fonctionne de manière indépendante par rapport aux applications qu'ils l'utilisent, il est obligatoirement au-dessus de la couche TCP.

c) Protocole SET(Secure Electronic Transaction)

SET est un protocole de sécurisation des transactions électroniques, s'appuyant sur le standard SSL. Le protocole SET est basé sur l'utilisation d'une signature électronique au niveau de l'acheteur et une transaction mettant en jeu non seulement l'acheteur et le vendeur, mais aussi leurs banques respectives

d) Protocole S-http (Secure HTTP)

S-HHTP est un procédé de sécurisation des transactions HTTP reposant sur une amélioration du protocole http par l'EIT (Entreprise Integration Technologies). Il permet de fournir une sécurisation des échanges lors des transactions de commerce-électronique en cryptant les messages, afin de garantir aux clients la confidentialité de toute information personnelle.

e) Protocole IPsec (Internet Protocole Security)

IPsec est un protocole de couche 3 du modèle OSI, il a été développé par l'IETF et fonctionne sous IPv6. C'est un protocole destiné à fournir différents services de sécurité, il propose ainsi plusieurs choix et options, lui permettant de répondre de façon adaptée aux besoins des entreprises, tel que l'encryptage de la charge utile IP, l'encapsulation dans un autre paquet IP, et l'envoi à travers un réseau.

2.4.2 Les outils cryptographiques

La cryptographie demeure la technique indispensable pour d'une part, protéger la confidentialité des informations transmises sur les réseaux ou stockées dans les serveurs de données et pour, d'autre part, assurer l'intégrité d'un document ou pour prouver l'authenticité d'une opération ou d'une transaction. Elle applique des concepts mathématiques et met en place des paradigmes informatiques afin de résister aux attaques potentielles d'assaillants ou de prouver, de manière quasi sûre, qu'une procédure est incorruptible [19].

2.4.2.1 Algorithme

Il existe deux grandes familles d'algorithmes de chiffrement, ceux à clés symétriques et ceux à clés asymétriques.

- **a) Algorithme de chiffrement symétrique :** Le chiffrement symétrique consiste à utiliser la même clé pour le chiffrement ainsi que pour le déchiffrement. Il est donc nécessaire que les deux interlocuteurs se soient mis d'accord sur une clé privée, où ils doivent utiliser un canal sécurisé pour l'échanger.
- **b) Algorithme de chiffrement asymétrique :** Pour résoudre le problème de l'échange de la clé secrète, un nouveau type de cryptographie a été inventé, il s'agit de la cryptographie asymétrique. Elle désigne une méthode cryptographique faisant intervenir une paire de clés asymétriques (une clé publique et une clé privée). Elle utilise cette paire de clés pour le chiffrement et le déchiffrement. La clé publique est rendue publique et est distribuée librement, la clé privée quant à elle n'est jamais distribuée et doit être garder secrète.

2.4.2.2 La fonction de hachage

Une fonction de hachage, est une fonction à sens unique, qui transforme un message de taille quelconque en un résumé court de taille fixe, appelé le condensé de message, l'empreinte du message, le résumé du message ou encore le message haché.

2.4.2.3 Signature numérique

la signature numérique est un moyen de lier l'information à une entité.

2.5 Principe d'authentification

L'authentification est le premier rempart aux attaques informatique ; c'est un procédé permettant de vérifier l'identité d'une entité (personne, groupe, ordinateur), largement utilisé dans les réseaux informatiques. Le service et l'utilisateur souhaitant y a accéder partagent un secret commun, ce secret peut prendre diverses formes, il peut s'agir d'un couple de login/mot de passe, d'un badge magnétique, d'une clé ou d'une empreinte digitale. On peut classer les techniques d'authentification, en catégories basées sur la nature de la sécurité qu'elles mettent en uvre[19].

De nombreuses problématiques sécuritaires se posent dans les réseaux modernes, de manière à restreindre au maximum les risques pouvant affecter le système d'information. Une

solution globale s'occuperait d'assurer les éléments de base de la sécurité à savoir l'authentification des terminaux ou des utilisateurs, ces derniers peuvent être stockés dans une base de données centralisée comme un annuaire LDAP.

2.6 Présentation d'un annuaire

Un annuaire est un recueil de données, dont le but est de pouvoir retrouver facilement des ressources (généralement des personnes ou des organisations) à l'aide d'un nombre limité de critères.
Un annuaire est un référentiel, il sert avant tout à localiser quelque chose, qu'il s'agisse de personnes ou de n'importe quelles autres ressources. Il doit offrir de plus des services particuliers comme la recherche, le classement ou l'organisation de l'information. Un annuaire est d'autant plus utile qu'il est simple à utiliser, notamment lorsqu'on recherche quelque chose avec très peu d'informations[17].

2.6.1 Les annuaires électroniques

Les annuaires électroniques sont un type de base de données spécialisée, permettant de stocker des informations de manière hiérarchique, dont la fonction première est de retourner un ou plusieurs attributs d'un objet grâce à des fonctions de recherche multicritères.

2.6.1.1 Caractéristiques d'un annuaire électronique

- **a) Dynamique :** la mise à jour d'un annuaire électronique est beaucoup plus simple à réaliser que celle d'un annuaire papier. D'autant plus que les personnes recensées(les administrateurs) dans l'annuaire peuvent, elles-mêmes modifier les informations les concernant.
- **b) Sûr :** un annuaire dispose de mécanismes d'authentification des utilisateurs, grâce à un mot de passe et un nom d'utilisateur ainsi que des règles d'accès permettant de définir les branches de l'annuaire auxquelles l'utilisateur peut accéder.
- **c) Souple :** un annuaire permet de classer l'information selon différents critères, contrairement aux annuaires papiers imprimés, permettant de rechercher une information selon un critère figé.

2.6.1.2 Rôle d'un annuaire

L'utilisation d'un annuaire ne se limite pas à la recherche de personnes ou de ressources. En effet, un annuaire peut servir à :

- Authentifier des utilisateurs ;

- Recenser des informations associées au matériel (ordinateur, serveur, leurs adresses IP et adresses MAC) ;
- Décrire les applications disponibles.

2.6.2 La différence entre un annuaire et une base de données

Un annuaire est un type de base de données spécifique, c'est-à-dire qu'il s'agit d'une sorte de base de données ayant des caractéristiques particulières :

- Un annuaire est prévu pour être plus sollicité en lecture qu'en écriture. Les données sont stockées de manière hiérarchique dans l'annuaire, tandis que les bases de données dites " relationnelles " stockent les enregistrements de façon tabulaire.
- Les annuaires doivent être compacts et repose sur un protocole réseau léger.
- Les annuaires doivent pouvoir être répartis. Cela signifie qu'un serveur d'annuaire doit comporter des mécanismes permettant de coopérer, c'est-à-dire d'étendre la recherche sur des serveurs tiers si jamais aucun enregistrement n'est trouvé.
- Un annuaire doit être capable de gérer l'authentification des utilisateurs ainsi que des droits qui leur sont attribués, pour la consultation ou la modification de données, comme il fournit un ensemble de services, permettant de retourner facilement les enregistrements à l'aide de requêtes simples [17].

2.6.3 Nécessité d'une normalisation

Un annuaire est un serveur remplissant les conditions décrites, mais l'implémentation peut être totalement différente d'un serveur à un autre, c'est pourquoi il a été nécessaire de définir une interface normalisée permettant d'accéder de façon standard aux différents services de l'annuaire. C'est le rôle du protocole LDAP, qui consiste à fournir un moyen unique (standard ouvert) d'effectuer des requêtes sur annuaire (compatible LDAP) [17].

2.7 Présentation de l'annuaire LDAP

Le protocole LDAP (Lightweight Directory Access Protocol), développé en 1993 par l'université du Michigan, avait pour but de supplanter le protocole DAP. LDAP est un protocole basé sur TCP/IP qui permet de partager des bases de données d'informations sur un réseau interne ou externe.
Ces bases de données sont appelées annuaires électroniques (Directory) et peuvent contenir tout type d'informations, il est possible de faire des modifications et des recherches dans l'annuaire,

qui est très rapide en lecture mais l'est beaucoup moins en écriture ; un serveur LDAP agit en tant qu'intermédiaire entre une source de données et un client [17].

2.7.1 Les différentes taches associées à l'annuaire LDAP

- Le protocole LDAP définit la méthode d'accès aux données sur le serveur au niveau du client ;
- Le protocole LDAP est uniquement prévu pour gérer l'interfaçage pour les annuaires. Plus exactement il s'agit d'une norme définissant la façon dans laquelle les informations sont échangées entre le client et le serveur LDAP, ainsi que la manière dans laquelle les données sont représentées ;
- Il permet la communication serveur-serveur pour échanger et synchroniser leur contenu (service de réplication) et créer des liens permettant de relier des annuaires les uns aux autres.

2.7.2 LDAP et son architecture Client-serveur

Le dialogue entre un client et un serveur LDAP est basé sur un protocole client/serveur. Sa particularité est de reposer sur un mécanisme de question et de réponse sous forme de messages, traités par le serveur de façon synchrone ou asynchrone, réduisant au maximum la charge de travail du client.

Un client transmet une requête au serveur. Le serveur exécute la requête et renvoie une réponse contenant le résultat de la requête ou les erreurs éventuelles. Un client doit s'identifier aux prés du serveur par (login, password et une fonction qui vas spécifier l'utilisateur comme le numéro de téléphone). Chaque requête émise peut être exécutée en mode synchrone ou en mode asynchrone[17].

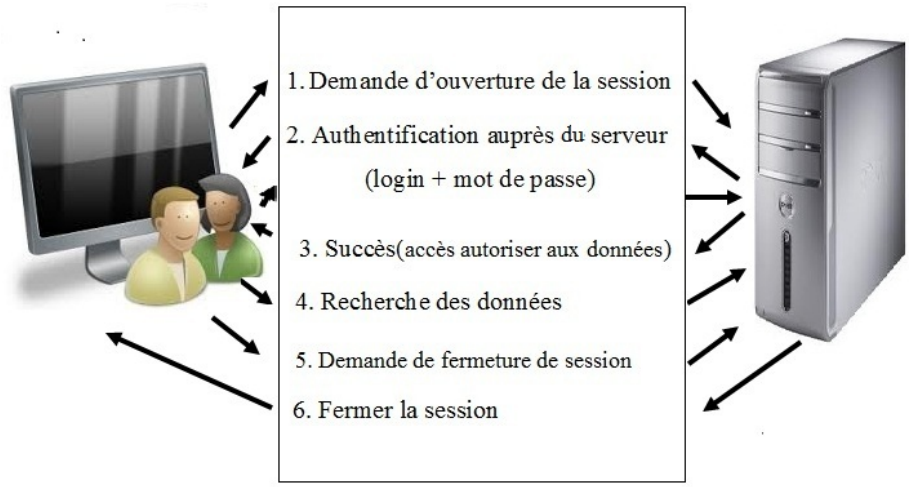


FIGURE 2.4 – LDAP et l'architecture client-serveur.

D'autre part, LDAP fournit un format d'échange (LDIF, Light-weight Data Inter change Format) permettant d'importer et d'exporter les données d'un annuaire avec simple fichier texte.

2.7.3 Les modèles LDAP

Le standard LDAP s'appuie sur différents concepts issus d'une approche objet, il définit [17] :

- Un modèle d'information : définissant le type d'information stockée dans l'annuaire.
- Un modèle de nommage : définissant la manière dans laquelle les informations sont organisées dans l'annuaire et leur désignation, suivant une structure logique qui est le Directory Information Tree (DIT).
- Un modèle de service : définissant la manière d'accéder aux informations et éventuellement de les modifier, c'est-à-dire les services offerts par l'annuaire.
- Un modèle de sécurité : définissant les mécanismes d'authentification et de droits d'accès des utilisateurs à l'annuaire.

2.7.3.1 Le modèle d'information

Le standard LDAP s'appuie sur différents concepts issus d'une approche objet. Il correspond à un objet abstrait ou réel (une personne, un objet matériel, des paramètres,). Une entrée est constituée de plusieurs objets.
Un objet est constitué d'un ensemble de paires clé/valeur appelé " attribut ". On parle ainsi de classe d'objet pour désigner la structure d'un objet, c'est-à-dire l'ensemble des attributs qu'il doit comporter.
Les attributs et les classes d'objet sont identifiés à l'aide d'un numéro unique, dénommé "OID"

(**O**bjet **ID**entifier). Ce numéro permet de partager un même ensemble d'attributs et de classes, ayant une sémantique commune, entre différents éditeurs de solutions LDAP [17].

- **a) Schéma de l'annuaire :** On appelle schéma l'ensemble des définitions d'objets et d'attributs qu'un serveur LDAP peut gérer ainsi que leur syntaxe. Le schéma est en effet lui-même stocké dans l'annuaire à un emplacement spécifique (il s'agit d'une instance de la classe subschéma). Lorsqu'une entrée est créée dans l'annuaire, celui-ci vérifie sa conformité à la classe d'objet, on parle alors de schéma cheking.
- **b) Les attributs :** chaque entrée est constituée d'un ensemble d'attributs (attributs /valeurs d'attributs) permettant de caractériser l'objet que l'entrée définit. On distingue deux types d'attributs :
  - Les attributs utilisateurs : ce sont des attributs qui peuvent être modifiés par les utilisateurs, en fonction de leurs permissions (âge, mail,..).
  - Les attributs opérationnels : ce sont des attributs auxquelles seul l'administrateur peut accéder. Par exemple, l'attribut " modifytimestamp " qui donne la date de la dernière mise à jour de l'objet.
- **c) Les classes d'objets :** un objet est une " instanciation " d'une classe d'objet, c'est-à-dire un ensemble d'attributs avec des valeurs particulières. Une classe d'objet est ainsi composée d'un ensemble d'attributs obligatoires et éventuellement des attributs facultatifs. Le type d'une classe est lié à la nature des attributs qu'elle utilise :
  - Une classe structurelle : correspond à la description d'objets basiques de l'annuaire (les personnes, les groupes, les unités organisationnelles).
  - Une classe auxiliaire : désigne des objets qui permettent de rajouter des informations complémentaires à des objets structurels. (mailRecipient rajoute les attributs concernant la messagerie électronique d'une personne).
  - Une classe abstraite : désigne des objets basiques de LDAP comme les objets alias.
- **d)Les OID "Objet Identifier" :** un OID est un identifiant unique associé à chaque classe d'objet et à chaque type d'attribut. Un OID est une séquence de nombres entiers séparés par des points. Les OID sont alloués de manière hiérarchique de telle manière que seule l'autorité qui a délégation sur la hiérarchie "1, 2, 3" peut définir la signification de l'objet "1, 2, 3, 4".

2.7.3.2 Le modèle de nommage (modèle de désignation)

Le modèle de nommage, est la manière dont sont organisées les données dans l'annuaire. LDAP organise les données de manière hiérarchique dans l'annuaire. Ceci signifie que toutes les informations découlent d'une seule et même "racine" [17].

- **a) Directory Information Tree (DIT) :** LDAP présente les informations sous forme d'une arborescence d'information hiérarchique appelée DIT (**D**irectory **I**nformation **T**ree), dans laquelle les informations sont appelées entrés (DES : **D**irectory **S**ervice **E**ntry).
- **b) Le nom des objets (DN, RDN) :** Le standard LDAP définit deux concepts pour nommer un objet, un nom relatif désigné par le RDN (**R**elative **D**istinguished **N**ame) et un nom absolu désigné par le DN (**D**istinguished **N**ame). Le DN constitue le nom absolu d'un objet. Il permet de le référencer sans ambiguïté, car il est unique dans la totalité de l'annuaire.

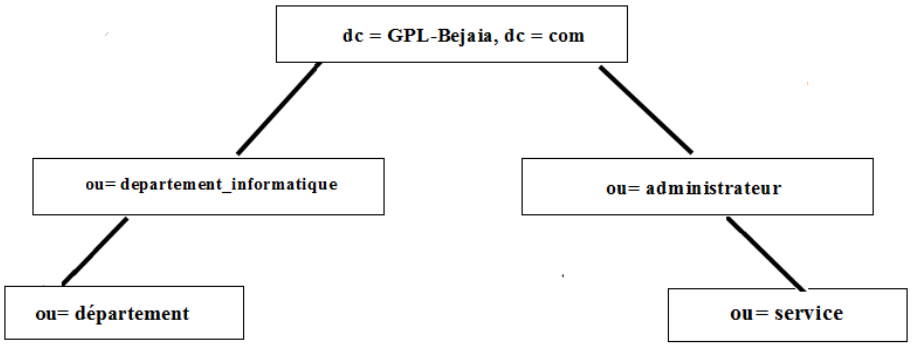


FIGURE 2.5 – Schéma illustrant le DN du département informatique.

2.7.3.3 Le modèle de service (fonctionnel)

Le standard LDAP définit une liste de services ou d'opérations, on peut les classer dans les catégories suivantes [17] :

- Les services de connexion et de déconnexion : ce sont les services qui permettent au client de s'identifier au près d'un serveur d'annuaire afin de démarrer une session, puis le déconnecter en fin de la session.
- Les services de recherches : ce sont les services de recherches dans l'annuaire qui utilisent différents critères.
- Les services de mise à jour : ce sont les services de mise à jour dans l'annuaire (créer, supprimer, modifier, renommer).
- Les opérations de base : elles jouent un rôle analogue aux commandes de manipulation de fichiers d'Unix (cp, mv).

Opération LDAP	Service	Description
Search	Recherche	Recherche à partir de critères
Compart	Comparer	Comparaison de contenu de deux objets
Add	Ajout	Ajout d'une entrée
Delete	Supprimer	Supression d'un objet
Bind	Connexion	Connexion
Unbind	Déconnexion	Déconnexio

TABLE 2.1 – Opérations et services offerts par LDAP.

2.7.3.4 Le modèle de sécurité

La sécurité se fait à plusieurs niveaux [17] :

- Par l'authentification pour se connecter à un service ;
- Par un modèle de contrôle d'accès aux données ;
- Par le chiffrement des transactions entre clients et serveurs ou entre serveurs.

a)L'authentification : LDAP est un protocole avec connexion, il faut s'authentifier pour ouvrir la connexion (Bind) en fournissant une identité. LDAP propose plusieurs choix d'authentification :

- Anonymous authentification : un accès au serveur sans authentification, qui permet uniquement de consulter les données accessibles en lecture.
- Root DN Authentifcation : c'est l'utilisateur privilégié. Il a accès en modification à toutes les données.
- Mot de passe en clair : c'est la méthode classique ou le mot de passe transite en clair sur le réseau.
- Mot de passe + SSL : la session entre le serveur et le client est chiffrée et le mot de passe ne transite plus en clair.

b)Le contrôle d'accès : le serveur attribue à l'utilisateur identifié, des droits d'accès aux données (lecture, écriture, recherche et comparaison), qui lui ont été définis par l'administrateur sous la forme d'ACLs (Acces Control Lists). OpenLDAP : sous la forme de directives de contrôle d'accès dans sldap.conf.

c)Le chiffrement : LDAPv3 supporte le chiffrement des transactions (entre clients et serveurs ou entre serveurs) via l'utilisation de SSL (ldaps). SSL sert également pour l'authentification par certificats, il permet au client de prouver son identité au serveur et en retour à celui-ci d'en faire de même vis-à-vis du client.

2.8 Conclusion

Au cours de ce chapitre, nous avons pris connaissance des différents aspects liés à la sécurité des réseaux informatiques, ensuite nous avons mit l'accent sur l'avantage de la fonction d'un annuaire électronique de manière générale, puis détailler l'utilisation de l'annuaire LDAP de manière particulière et présenter ainsi les différents modèles qu'il comprend.

Dans le chapitre qui suit, nous présenterons les divers concepts associés à l'utilisation des réseaux privés virtuels "VPN".

CHAPITRE 3

LES RÉSEAUX PRIVÉS VIRTUELS

3.1 Introduction

La confidentialité et la vie privée sur Internet sont régulièrement remises en question, car les données transmises sur Internet sont beaucoup plus vulnérables que lorsqu'elles circulent sur un réseau interne à une organisation et cela est dû au chemin emprunté, qui n'est pas défini à l'avance. Ainsi, il n'est pas impossible que sur le chemin parcouru, le réseau soit écouté par un utilisateur malveillant.
Il n'est donc pas concevable de transmettre dans de telles conditions des informations sensibles pour l'organisation de l'entreprise. La solution d'interconnexion que fournit Internet pour répondre à ce besoin de communication sécurisé, consiste à utiliser les réseaux privés virtuels(VPN), qui sont idéals pour pouvoir exploiter au mieux les capacités du réseau Internet et de relier des sites à l'échelle de la planète en toute sécurité.
Dans ce chapitre, nous allons aborder les principales caractéristiques des VPN, à travers certaines définitions et principes de fonctionnement.

3.2 Présentation d'un réseau privé virtuel

3.2.1 Définition

VPN (**V**irtual **P**rivate **N**etwork) ou RPV (**R**éseau **P**rivé **V**irtuel) 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 [2].

Un VPN assure divers objectifs et se caractérise par [3] :

- Étanchéité du trafic entre les différents réseaux privés virtuels ;
- La sécurité des communications qui est assurée à travers l'authentification des utilisateurs ou des DATA, ainsi que la confidentialité à travers le chiffrement effectué sur 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 ;

3.2.2 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 traffic 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[6].

3.2.3 Les fonctionnalités d'un réseau privé virtuel

Un réseau privé virtuel, repose sur les principes fondamentaux de la sécurité, en assurant la mise en oeuvre de diverses fonctionnalités [7] :

3.2.3.1 Authentification d'utilisateurs

Elle désigne le processus visant à confirmer qu'un commettant est bien celui qu'il prétend être, donc seuls les utilisateurs autorisés doivent avoir accès au canal VPN. Les réseaux privés virtuels peuvent utiliser des mots de passes, des certificats numériques, des cartes à puce, pour vérifier l'identité des parties à l'autre extrémité du réseau.

3.2.3.2 Confidentialité de données

La confidentialité est une fonction conceptuelle qui vise, à protéger les messages contre toute divulgation par des sources non authentifiées ou non autorisées. La confidentialité est garantie grâce à l'encapsulation et au chiffrement effectués sur les données, traversant les réseaux privés virtuels.

3.2.3.3 Prise en charge multi-protocole

Tous les protocoles utilisés sur les réseaux publics doivent être supportés par la solution VPN.

3.2.3.4 Gestion des clés

La génération, la distribution, le stockage et la suppression des clés sont assurées dans les VPN que ce soit, pour le client ou pour le serveur.

3.2.3.5 Intégrité des données

L'intégrité des données garantit qu'aucune altération ou modification n'a été apportée aux données lors de leurs parcours entre la source et la destination. En général, les réseaux privés virtuels utilisent des fonctions de hachages, qui ressemblent à une somme de contrôle garantissant que personne n'a lu le contenu, tout en étant plus robuste.

3.2.4 Principe de fonctionnement d'un VPN

Un réseau 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.
Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprises, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagé.
Les données à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans ce cas, le protocole de tunneling encapsule les données en ajoutant un en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de dés encapsulation[6].

3.2.5 Types de VPN

On distingue trois catégories principales de VPNs selon leur mode d'utilisation [6] :

3.2.5.1 VPN d'accès (Host to LAN)

Un VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau de leur entreprise. L'utilisateur se sert d'une connexion Internet afin d'établir une liaison sécurisée.
L'utilisateur distant, sera connecté logiquement au réseau LAN de l'entreprise comme s'il l'était physiquement.
La figure suivante montre un utilisateur VPN connecté à un réseau d'entreprise à travers Internet.

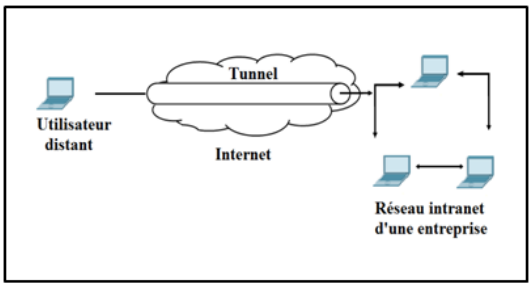


FIGURE 3.1 – VPN poste à site

3.2.5.2 Intranet VPN (LAN to LAN)

Il est utilisé pour relier deux ou plusieurs intranets, d'une même entreprise. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants.

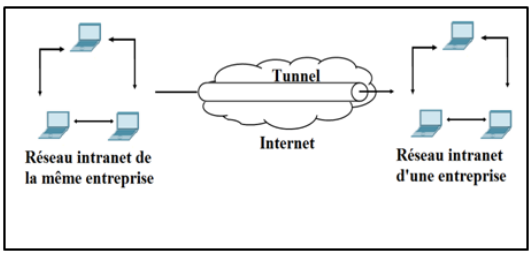


FIGURE 3.2 – VPN site à site.

3.2.5.3 Extranet VPN (Host to Host)

Une entreprise peut utiliser un 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.

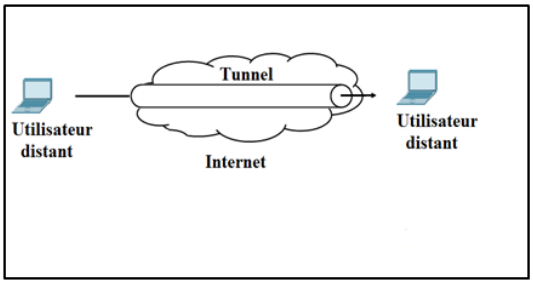


FIGURE 3.3 – VPN poste à poste.

3.3 Protocoles utilisés pour réaliser une connexion VPN

3.3.1 Le protocole PPP (point-to-point Protocol)

C'est un protocole qui permet de transférer des données sur un lien synchrone ou asynchrone, il est full duplex, garantie l'ordre d'arrivé des paquets et encapsule les paquets IP, IPX dans des trames PPP, puis transmet ces paquets encapsulés au travers de la liaison point à point.

3.3.2 Les phases d'une connexion PPP

Une connexion PPP se déroule en trois phases comme suit [6] :

- Une méthode d'encapsulation des paquets IP (datagrammes) sur la liaison série. PPP utilise le format de trame HDLC (Hight Data Level Control).
- Un protocole de contrôle de liaison LCP (Link Control Protocol) permet d'établir, de configurer et de tester la connexion de la liaison de données.
- Plusieurs protocoles de contrôles de réseaux NCP (Network Control Protocol) permettant d'établir et de configurer les différents protocoles de la couche réseau.
  Le format d'une trame "PPP" est le suivant :

Fanion	Adresse	Contrôle	Protocole	Données	FCS	Fanion
0111110	11111111	00000011	16 bits		16 bits	01111110

FIGURE 3.4 – Format d'une trame "PPP".

Nous expliquons la signification et le rôle de chaque champ de la trame " PPP ", comme suit :

- **Fanion :** il s'agit du champ séparateur de trame, un seul drapeau est nécessaire entre deux trames ;
- **Adresse :** le champ adresse correspond à une adresse HDLC, or PPP ne permet pas un adressage individuel des stations, donc ce champ doit être à << 0xFF >> (pour toutes les stations), toute adresse non reconnue fera que la trame sera détruite.
- **Contrôle :** le champ contrôle doit être à "0x03", ce qui correspond à une trame HDCL non numérotée. Toute autre valeur fera que la trame sera détruite.
- **Protocole :** la valeur contenue dans ce champ doit être impaire, l'octet de poids fort étant pair, ce champ identifie le protocole encapsulé dans le champ informations de la trame. Les différentes valeurs utilisables sont définies dans la RFC et représentent les différents protocoles supportés par PPP (IP, IPx).

- **Données :** les données sont de longueur comprise entre 0 et 1500 octets, ce champ contient le datagramme du protocole supérieur indiqué dans le champ "protocole". Sa longueur est détectée par le drapeau de fin de trame, qui comprend au moins deux octets de contrôle.
- **FCS (Frame Check Sequence) :** ce champ contient la valeur du checksum de la trame "PPP", vérifie le contenu du FCS lorsqu'il reçoit un paquet.

3.3.3 Le protocole PPTP (Point-to-Point Tunneling Protocol)

PPTP (Point-to-Point Tunnelling Protocol) est un protocole réseau permettant le transfert sécurisé des données entre un client distant et un serveur privé. Ceci est possible par la création d'un VPN utilisant TCP/IP. PPTP supporte les VPNs à la demande multi-protocole sur des réseaux publics comme Internet. La technologie utilisée par PPTP est une extension du protocole permettant l'accès à distance PPP (Point to Point Protocol)[6].

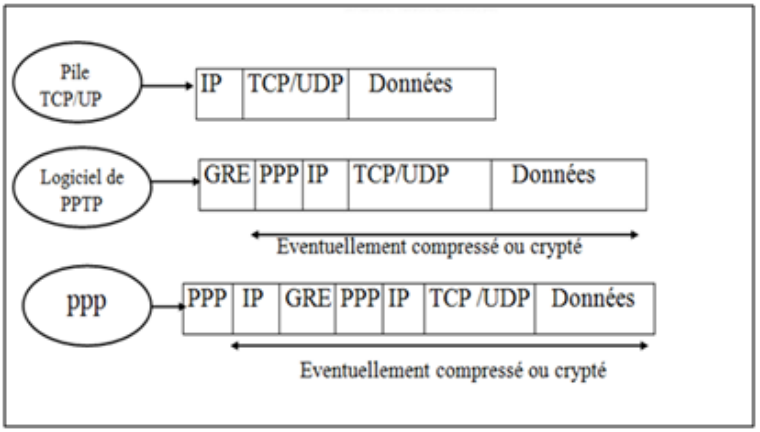


FIGURE 3.5 – Encapsulation d'une trame PPTP.

- **Principe de fonctionnement**

  Le principe du protocole PPTP est de créer des paquets, sous le protocole PPP et de les encapsuler dans des datagrammes IP. Le tunnel PPTP se caractérise par une initialisation de connexion à partir du client, une connexion de contrôle entre le client et le serveur ainsi que par la clôture du tunnel par le serveur. Lors de l'établissement de la connexion, le client effectue d'abord une connexion avec son fournisseur d'accès à Internet. Cette première connexion de type PPP permet de faire circuler des données sur Internet. Par la suite, une deuxième connexion est établie. Elle permet d'encapsuler les paquets PPP dans des datagrammes IP. C'est cette deuxième connexion qui forme le tunnel PPTP [6].

3.3.4 L2F (Layer Two Forwarding)

L2F est un protocole de niveau 2, qui permet à un serveur d'accès distant de véhiculer le trafic sur PPP et de transférer ces données jusqu'au serveur L2F (routeur). Ce serveur L2F dés-encapsule les paquets et les envoie sur le réseau. Il faut noter que contrairement à PPTP et L2TP, L2F n'a pas besoin de client, ce protocole est progressivement remplacé par L2TP qui est plus souple [5].

3.3.5 L2TP(Layer Two Tunneling Protocol)

Microsoft et Cisco, reconnaissant les mérites des deux protocoles L2F et PPTP, se sont associés pour créer le protocole L2TP, qui réunit les avantages de ces deux premiers.
L2TP est un protocole réseau qui encapsule des trames PPP pour les envoyer sur des réseaux IP. On utilise souvent ce protocole pour créer des VPN sur Internet. Dans ce cas, il transporte des trames PPP dans des paquets IP. Il se sert d'une série de messages L2TP afin d'assurer la maintenance du tunnel et UDP pour envoyer les trames PPP [5].

a)Concentrateurs d'accès L2TP (LAC :L2TP Access Concentrator)

Les périphériques LAC fournissent un support physique aux connexions L2TP. Le trafic étant alors transféré sur les serveurs réseau L2TP.Ces derniers peuvent s'intégrer à la structure d'un réseau commuté RTC ou alors à un système d'extrémité PPP prenant en charge le protocole L2TP. Ils assurent le fractionnement en canaux de tous les protocoles basés sur PPP. Le LAC est l'émetteur des appels entrants et le destinataire des appels sortants.

b) Serveurs réseau L2TP (LNS :L2TP Network Server)

Les serveurs réseau L2TP ou LNS, peuvent fonctionner sur toute plate-forme prenant en charge la terminaison PPP. Le protocole L2TP n'utilise qu'un seul support, sur lequel arrivent les canaux L2TP. C'est pourquoi, les serveurs réseau LNS, ne peuvent avoir qu'une seule interface de réseau local(LAN) ou étendu (WAN). Ils sont cependant capables de terminer les appels en provenance de n'importe quelle interface PPP du concentrateur d'accès LAC. LNS est l'émetteur des appels sortants et le destinataire des appels entrants. C'est le LNS qui sera responsable de l'authentification du tunnel.

3.3.6 IP Security Protocol

IPsec, définit par la RFC 2401, est un ensemble de protocoles pour sécuriser les communications IP et garantir le chiffrement, l'intégrité et l'authentification. Il est conceptuellement unique, car il permet de sécuriser le réseau même. Ce protocole spécifie les messages nécessaires

pour sécuriser les communications du réseau privé tout en se basant sur les algorithmes existants.
La force fondamentale de cette approche est son fonctionnement à des couches de bas niveau. Comme IP est transparent aux utilisateurs, IPSec l'est aussi en rajoutant une couche qui permet d'assurer la sécurité et l'intégrité des communications[6].

3.3.6.1 Architecture du protocole IPSec

L'architecture des réseaux basés sur IPsec, permet d'assurer les besoins de la sécurité (Authentification, Confidentialité, Intégrité). IPSec offre trois technologies, qui combinées entre elles permettent de se protéger des différentes attaques à la sécurité[6] :

- **Authentication Header (AH) :** il assure l'authentification et l'intégrité des données pour les paquets IP circulant entre deux systèmes. AH correspond à un entête, qui attache les données de chaque paquet à une signature, qui permet de vérifier l'identité de la personne en envoyant les données et que ces derniers n'ont pas été modifiées. Si le protocole AH est utilisé seul, sa protection est faible car il ne garantit pas le chiffrement des données (confidentialité) dans les paquets. C'est pourquoi, il est utilisé avec ESP pour permettre aux données d'être chiffrées et pour sécuriser contre toute altération.
- **Encapsulating Security Payload (ESP) :** il assure la confidentialité et l'authentification grâce au chiffrement de paquets IP tel que cette fonction masque les données et l'identité de leurs sources et leurs destinations. Ce protocole authentifie le paquet IP interne et l'en-tête ESP. L'authentification permet d'identifier la source des données et garantir leur intégrité.
- **Internet Key Exchange (IKE) :** IKE est un système développé spécifiquement pour IPsec, qui vise à fournir des mécanismes d'authentification et d'échange de clés adaptés à l'ensemble des situations qui peuvent se présenter sur Internet. Il est composé de plusieurs éléments : le cadre générique ISAKMP (Internet Security Association and Key Management Protocol) et une partie des protocoles Oakley et Skeme.

3.3.6.2 Fonctionnement d'IPsec

IPSec implémente deux protocoles **AH** et **ESP**, qui permettent au protocole IPsec de fonctionner suivant deux modes distincts [6] :

- **Mode transport :** dans le cas où le but, est de sécuriser seulement les données. Il sert donc pour des configurations *poste à poste*. Dans ce mode, les protocoles AH et ESP protègent la couche transport en interceptant les paquets provenant de la couche transport dans la couche réseau.

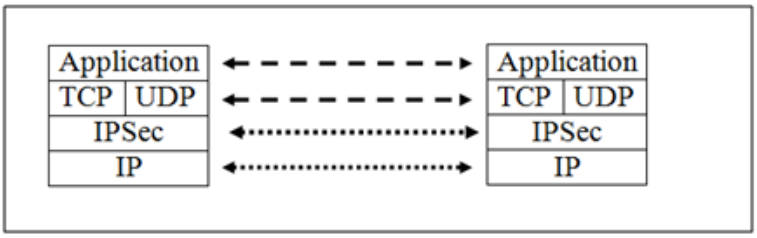


FIGURE 3.6 – Poste à poste dans le mode de transport.

- **Mode tunnel :** en général, ce mode est utilisé pour des configurations LAN-to-LAN, le trafic non protégé est envoyé vers une passerelle implémentant IPSec.
  Comme le montre la figure ci-dessous, le Gateway encapsule tout le paquet IP, entête comprise, avec l'encryptage d'IPSec. Il rajoute ensuite un nouvel entête IP et envoie ce nouveau paquet à travers le réseau public vers le Gateway destinataire. Là, les paquets sont ensuite déchiffrés et envoyés sous forme originale à sa propre destination.

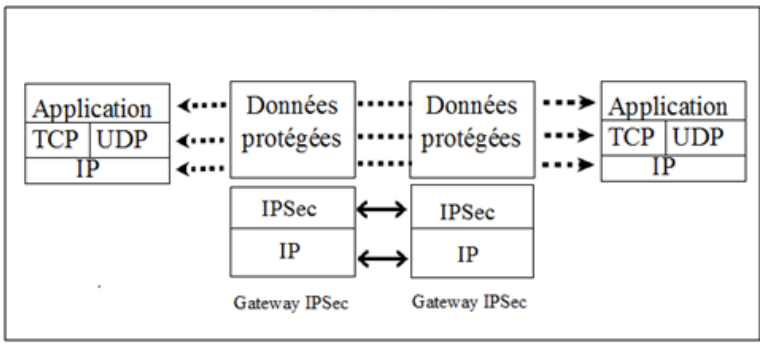


FIGURE 3.7 – LAN-to-LAN dans le mode tunnel.

3.3.7 Protocole SSL

SSL **(Secure Sockets Layers)** est un procédé de sécurisation des transactions effectuées via Internet. Il repose sur un procédé de cryptographie par clé publique afin de garantir la sécurité de la transmission de données sur Internet. Son principe consiste à établir un canal de communication 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 [10].
SSL est un protocole de couche 4 " niveau transport ", utilisé par une application pour établir un canal de communication sécurisé avec une autre application.

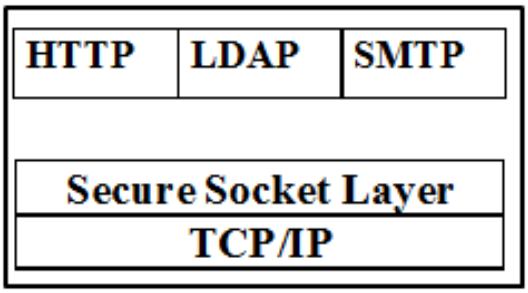


FIGURE 3.8 – La couche SSL.

3.3.7.1 Fonctionnement du protocole SSL

Le protocole **SSL Handshake** débute une communication SSL. Suite à la requête du client, le serveur envoie son certificat ainsi que la liste des algorithmes qu'il souhaite utiliser. Le client commence par vérifier la validité du certificat du serveur. 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 les vérifications sont passées, le client génère une clé symétrique et l'envoie au serveur. Ce dernier peut alors envoyer un test 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 clé, valeur de la clé, algorithme de chiffrement.

La phase suivante consiste en l'échange de données cryptées (protocole SSL Records). Les clés générées avec le protocole Handshake sont utilisées pour garantir l'intégrité et la confidentialité des données échangées. Les différentes phases du protocole sont [10] :

- 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 messages et des données ;
- Chiffrement des paquets et du résultat du hachage à l'aide de la clé symétrique générée lors du Handshake ;
- Ajout d'un en-tête SSL au paquet.

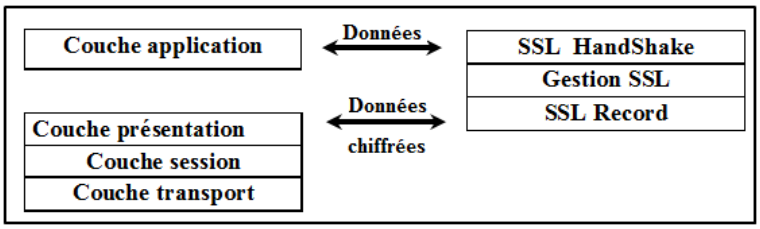


FIGURE 3.9 – Fonctionnement du protocole SSL.

3.4 Conclusion

Ce chapitre nous a permi de prendre connaissance des différents concepts et généralités, associés aux VPNs et de comprendre l'intérêt qu'ils y apportent dans le domaine des réseaux. On a évidemment pris connaissance de la multitude de protocoles, de techniques et d'architectures qui existent pour le déploiement des VPNs.

Dans le chapitre qui suit, nous allons entamer la mise en place d'un réseau privé virtuel avec authentification LDAP, en illustrant les différentes étapes suivies pour aboutir à la réalisation de ce projet.

CHAPITRE 4

MISE EN OEUVRE D'UNE SOLUTION DE SÉCURITÉ

4.1 Introduction

Le chapitre présent comprend deux parties essentielles, la première partie comprend la phase de réalisation du projet. En premier lieu nous allons définir l'architecture à implémenter, ainsi que l'environnement de travail choisi, en second lieu nous présenterons les pré-requis nécessaires à la mise en oeuvre d'un réseau privé virtuel, ainsi que les étapes à suivre pour aboutir à cet objectif, suivi de l'implémentation de l'annuaire LDAP et enfin nous passerons à la mise en oeuvre d'un système de détection d'intrusions " SNORT ". La seconde partie quant à elle, comprend la phase de "tests", cette partie sera consacrée à l'illustration des différents tests d'évaluation permettant de garantir le succès de l'implémentation réalisée.

4.2 Architecture à implémenter

Avant d'entamer la mise en oeuvre de la solution de sécurité, il est essentiel de définir l'architecture de l'implémentation à réaliser, pour ce faire nous avons illustré la figure ci-dessous suivi de la description qui lui est associée.

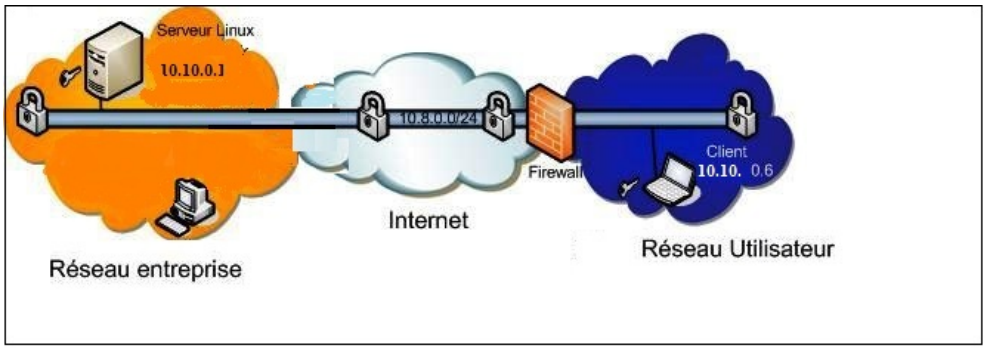


FIGURE 4.1 – Architecture implémentée.

Comme la figure le montre, il s'agit de deux réseaux distincts "le réseau du siège NAFTAL GPL ", ainsi que "le réseau du centre d'AKBOU ", en tenant compte de la distance qui sépare les deux sites et de l'ampleur que prennent les données pour se transférer d'un site à l'autre, nous avons jugé que la solution appropriée pour assurer une fiabilité et une flexibilité de transfert de données entre les deux sites est la mise en oeuvre d'un réseau privé virtuel. On note aussi qu'à l'issue de l'étude de l'architecture du réseau associée au siège de " NAFTAL GPL ", un annuaire d'authentification est indispensable et nécessaire dans le but de gérer les différents utilisateurs, c'est dans ce contexte-là, que nous avons choisi d'implémenter l'annuaire LDAP. Enfin en termes d'efficacité et de protection au niveau du réseau local de chaque site, la mise en place d'un système de détection d'intrusions est nécessaire, pour ce faire nous avons choisi la mise en place de l'IDS "SNORT".

4.3 Description de l'environnement de travail

Pour une sécurité optimale, nous avons choisi de travailler dans un environnement "Linux", plus précisément : Ubuntu 10.04LTS, car il nous fournit un espace de travail unique et nous assure une fiabilité de résultats incomparables.
Ubuntu est une distribution Gnu/Linux récente, développée par la société "Canonical LTD, fondée par Mark Shuttleworth", constitué de logiciels libres et est disponible gratuitement y compris pour les entreprises[8].

4.4 Installation et configuration VPN

Nous allons voir dans ce qui suit les étapes à suivre afin de configurer et de mettre en place un serveur/client VPN via OpenVPN.

4.4.1 Présentation d'OpenVPN

Openvpn est un démon VPN robuste et très flexible tel qu'il supporte SSL/TLS, transport UDP, tunnel à travers les proxys ou NAT et la portabilité à la plupart des principales plates-formes. Openvpn est étroitement lié à la bibliothèque OpenSSL, et tire une grande partie de ses capacités de chiffrement de ce dernier. Il prend également en charge les tunnels TCP/UDP et il est conçu pour fonctionner avec le TUN/TAP interface réseau virtuelle, qui existe sur la plupart des plates-formes [10].

4.4.2 Présentation d'OpenSSL

OpenSSL est un utilitaire cryptographique, implémentant le protocole "SSL" (Secure Sockets Layer), qui représente une couche de sockets sécurisées, ainsi que le protocole "TLS" (Transport Layer Security), qui assure la sécurité au niveau de la couche transport, sans omettre les standards cryptographiques liés dont ils ont besoin[9].

4.4.3 Critères de choix d'utilisation d'Openssl/Openvpn

Notre choix s'est porté sur l'utilisation d'OpenSSL/OpenVPN, par rapport à ces caractéristiques suivantes [10] :

- Solution libre ;
- Multi-platformes (Windows, Linux, BSD, MacOS X, Solaris) ;
- Implémentation sécurisée (réduction des privilèges, chroot, ...) ;
- Compression optionnelle avec la bibliothèque LZO ;
- Fonctionnement en mode TUN (routage) ou TAP (pont) ;
- Développement dynamique ;
- Adaptation au mode client/serveur avec plusieurs clients (version 2.0) ;
- Simplicité de mise en oeuvre.

4.5 Mise en place du réseau virtuel

4.5.1 Installation d'OpenVPN

L'installation d'openVPN repose essentiellement sur l'installation de la bibliothèque "OpenSSL", pour ce faire, on introduit la commande suivante à partir du shell :

```
root@ubuntu:/home/rahima# apt-get install openssl openvpn
```

FIGURE 4.2 – Installation d'openssl et d'openvpn.

4.5.2 Génération des clés et des certificats

"OpenVPN" peut fonctionner avec plusieurs types d'authentification. Nous utiliserons l'authentification par clés et certificats, plus sure que le classique "login/motdepasse". Pour générer les clés et les certificats nécessaires, des scripts figurent dans le répertoire /usr/share/doc/openvpn/examples/easy-rsa/2.0, nous allons copier ces scripts dans le répertoire /etc/openvpn/easy-rsa/ que nous avons créé nous même et lui attribuer les droits d'accès adéquats, comme indiqué ci-dessous :

```
root@ubuntu:/etc/openvpn/easy-rsa# ls
build-ca           build-key-server  Makefile              sign-req
build-dh           build-req         openssl-0.9.6.cnf.gz  vars
build-inter        build-req-pass    openssl.cnf           whichopensslcnf
build-key          clean-all         pkitool
build-key-pass     inherit-inter     README.gz
build-key-pkcs12   list-crl          revoke-full
root@ubuntu:/etc/openvpn/easy-rsa# sudo chown -R $USER /etc/openvpn/easy-rsa/
root@ubuntu:/etc/openvpn/easy-rsa#
```

FIGURE 4.3 – Copie des scripts.

Maintenant, nous allons passer à l'édition du fichier "vars" situé dans le répertoire "/etc/openvpn/easy − rsa/", à l'aide de la commande "vim", qui nous donne l'accès à la modification du contenu de ce fichier comme suit :

```
♯cd /etc/openvpn/easy-rsa
♯vim vars
```

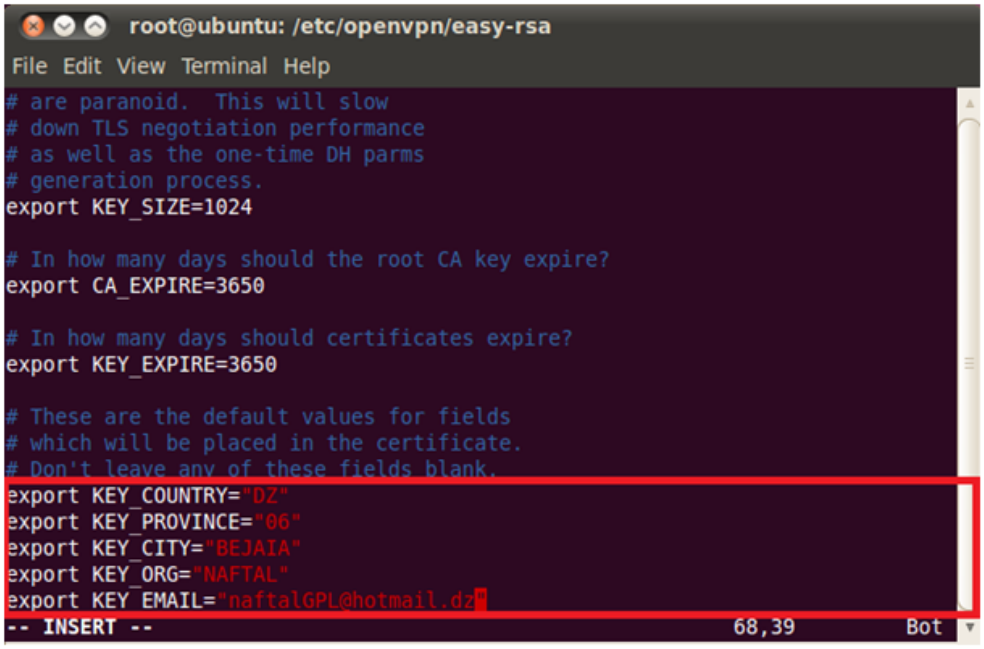


FIGURE 4.4 – Edition du fichier vars.

On accède à présent au répertoire " /etc/openvpn/easy-rsa " et on saisit un ensemble de commandes, avant de générer les différentes clés et certificats nécessaires pour le cryptage des données comme suit :

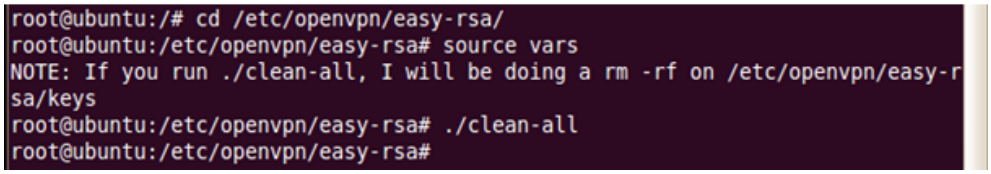


FIGURE 4.5 – Suppression des clés et certificats existants.

- La commande ♯ `sourcevars` : cette commande est nécessaire, pour tenir compte des modifications que nous voulons apporter au fichier de configuration " vars ".
- La commande ♯ `./clean − all` : permet de détruire toutes les clés et certificats existants précédemment.

A présent, nous passons à la création du certificat et de la clé de l'Autorité de Certification Maitre (Master Certificate Authority (CA), à partir de la commande :

♯./build-ca

Les fichiers `ca.crt` et `ca.key` sont alors créés dans le dossier "`keys`" et les variables précédentes devront être confirmées. La clé servira à signer les clés du serveur ainsi que des différents clients, et le certificat servira de "carte d'identité" à laquelle le serveur et les clients

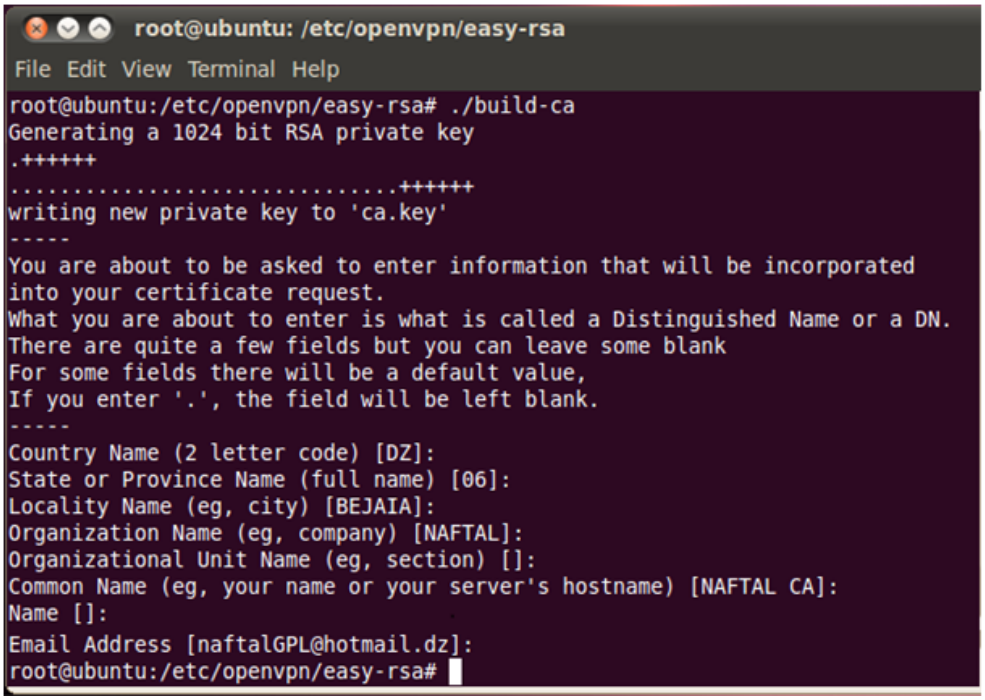


FIGURE 4.6 – Génération du certificat et de la clé d'autorité de certification " CA ".

se réfèreront.

Maintenant, nous allons passer à la génération d'un certificat et d'une clé pour le serveur, pour ce faire nous saisissons la commande suivante :

```
♯ ./build-key-server serveur
```

Tel que " serveur " est le nom que l'on a attribué au serveur. Une fois la commande saisie, il nous sera demandé d'insérer le "Common Name", qui représente le nom associé au serveur, c'est-à-dire " serveur " dans notre cas, ainsi que la saisie d'un mot de passe et d'un nom d'entreprise, bien que ces deux paramètres sont facultatifs, nous avons insérer ce qui suit :

- A challenge password [] : **naftal**.
- An optional company name [] : **naftalGPL**.

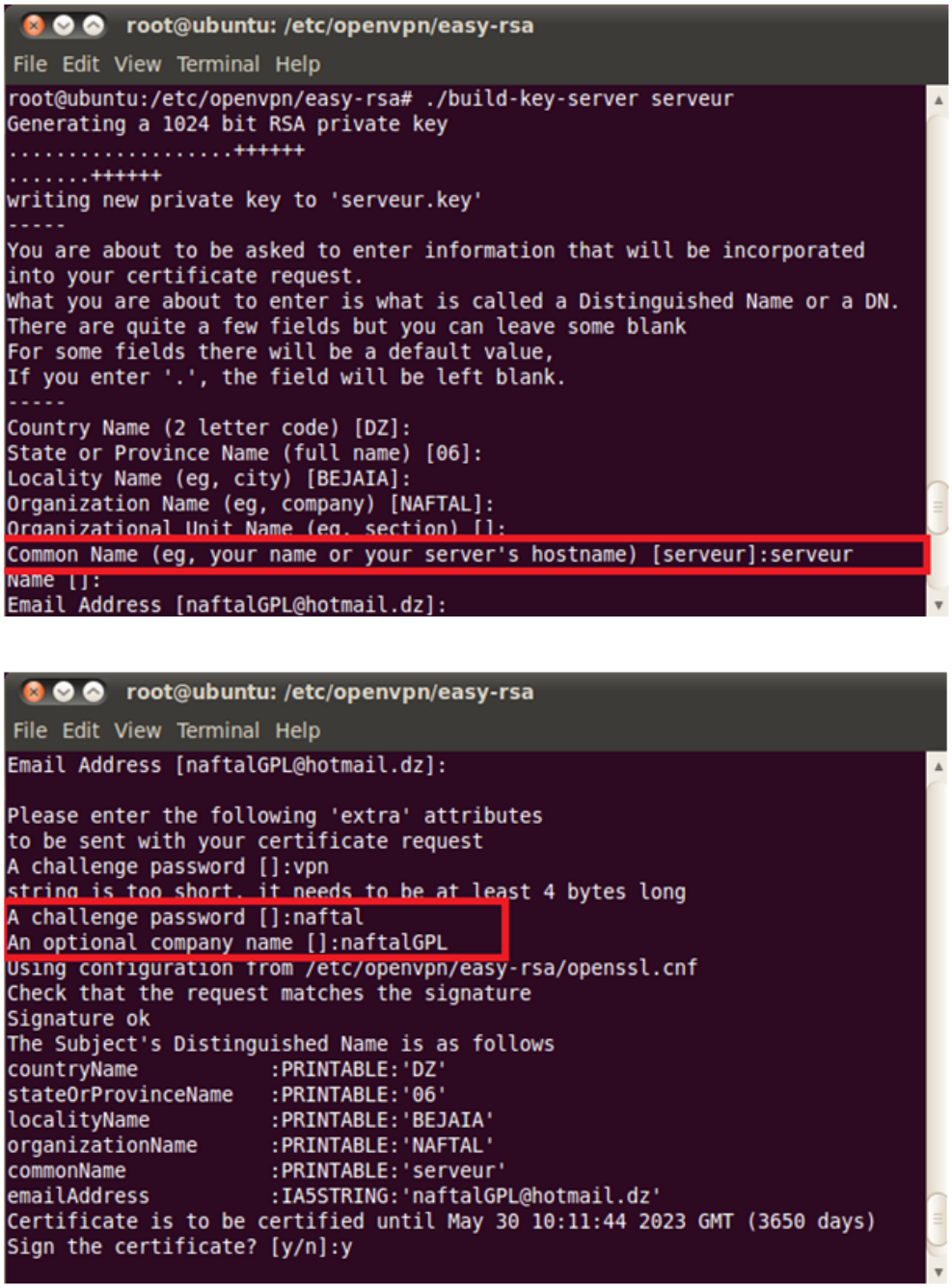


FIGURE 4.7 – Création du certificat et de la clé associés au serveur.

Le certificat et la clé du serveur sont à présent créés : "serveur.crt" et "serveur.key".

Nous allons maintenant générer les certificats et les clés associés aux clients, dont nous avons besoin ; dans notre cas il s'agit de la création de deux clients :

- Un client sous la plate forme " Ubuntu ".
- Un client sous la plate forme " Windows ".

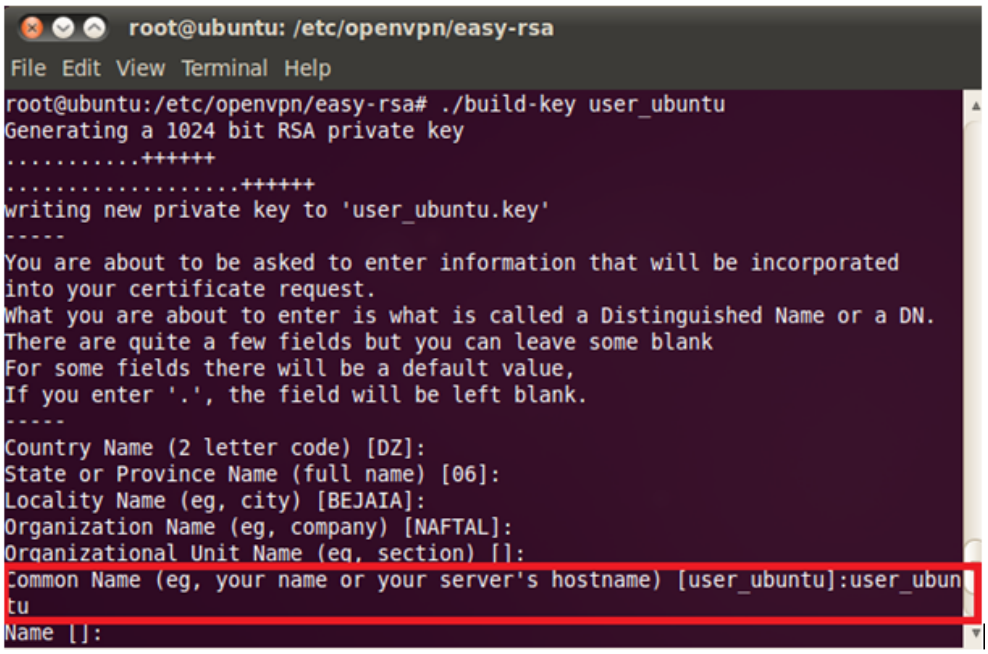


FIGURE 4.8 – Création du certificat et de la clé associés au client.

A présent, nous allons génerer les paramètres " Diffie-Hellman " essentiels pour le fonctionnement du serveur.
La commande ♯./build-dh permet la création du fichier "dh1024.pem", tel que "1024" indique la taille de la clé.

FIGURE 4.9 – Génération des paramètres "Diffie-Hellman".

Au terme de la génération de ces diverses clés et certificats, nous obtenons les fichiers suivants dans le répertoire " /etc/openvpn/easy-rsa/keys " :

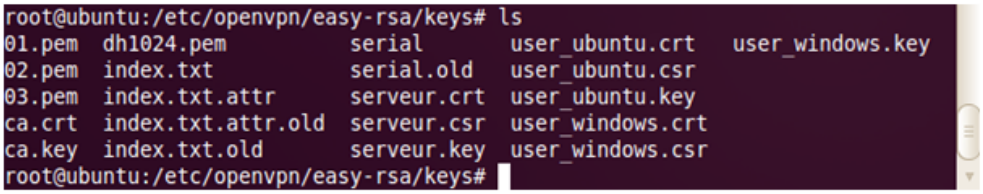


FIGURE 4.10 – Affichage des fichiers créés.

4.5.3 Configuration du fichier " Serveur.conf "

Maintenant que les clés et les certificats générés pour le serveur et les différents clients, nous passons à l'édition des fichiers de configuration, nous commençons par le fichier de configuration du serveur " serveur.conf ", en spécifiant certains paramètres, résumés ci-dessous comme suit :

```
♯ Port d'écoute sur le réseau.
port 1194
management localhost 1195
♯ Protocole de communication utilisé entre le client et le serveur.
proto udp
;proto tcp
♯ Type d'interface utilisée
dev tun
;dev tap
♯ Emplacement de la clé de l'autorité de certification.
ca /etc/openvpn/easy-rsa/keys/ca.crt
♯ Emplacement du certificat associé au serveur
cert /etc/openvpn/easy-rsa/keys/serveur.crt
♯ Emplacement de la clé du serveur.
key /etc/openvpn/easy-rsa/keys/serveur.key
♯ Emplacement du fichier Diffie-Helleman
dh /etc/openvpn/easy-rsa/keys/dh1024.pem
♯ Adresse du réseau VPN
server 10.10.0.0 255.255.255.0
♯Activation de la compression
comp-lzo
♯Pour rendre la connexion persistante
persist-key
persist-tun
♯Fichier de log
status openvpn-status.log
♯Niveau de verbosité
verb 3 push "redirect-gateway def1 bypass-dhcp"
topology subnet
♯configuration LDAP username-as-common-name
plugin /usr/lib/openvpn/openvpn-auth-pam.so openvpn
```

Afin de s'assurer, que la configuration à été faite correctement, nous allons saisir à partir du shell la commande suivante :

```
♯ /etc/init.d/openvpn start
```

```
root@ubuntu:/# /etc/init.d/openvpn start
 * Starting virtual private network daemon(s)...
 *   Autostarting VPN 'serveur'                                    [ OK ]
root@ubuntu:/#
```

FIGURE 4.11 – Lancement du serveur Openvpn.

Et pour vérifier la création et la bonne configuration de l'interface " tun0 ", on saisit la commande suivante à partir du shell :

♯ ifconfig tun0

```
root@ubuntu:/# ifconfig tun0
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
-00-00
          inet addr:10.10.0.1  P-t-P:10.10.0.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@ubuntu:/#
```

FIGURE 4.12 – Configuration de l'interface " tun0 ".

4.5.4 Configuration du fichier " Client.conf "

Maintenant que la configuration du serveur est complète, nous passons à la configuration du fichier "client.conf" associé aux deux clients "user_ubuntu" et "user_windows" crées précédemment en suivant les étapes suivantes :

- Création du dossier "config" dans le répertoire "/etc/openvpn/", qui va contenir le fichier "client.conf".
- Création du dossier "easy − rsa" dans le répertoire "/etc/openvpn/", de sorte à respecter la même hiérarchie de dossiers sur le client que sur le serveur afin de garder une certaine cohérence entre les deux.
- Copie des fichiers "ca.crt", "user_ubuntu.crt" et "user_ubuntu.key", provenant du serveur dans le répertoire "/etc/openvpn/easy − rsa/keys".

La configuration des paramètres associés au fichier "client.conf", est résumée dans la figure suivante :

```
♯Pour signaler qu'il s'agit d'un client
client
♯Type d'interface
dev tun
;dev tap
♯ Le protocole de communication utilisé entre le client et le serveur
proto udp
;proto tcp
♯Adresse ip publique du réseau dans lequel le serveur est installé ainsi que le port utilisé
remote 192.168.119.146 1194
;remote vpnserver.example.com 1194
;remote my-server-2 1194
nobind
♯Pour rendre la connexion persistante
persist-key
persist-tun
♯Emplacement du master CA
ca ca.crt
♯Emplacement du certificat client
cert user_ubuntu.crt
♯Emplacement de la clé privée du client
key user_ubuntu.key
♯/etc/openvpn/easy − rsa/keys/
♯Tentative de connexion infinie
resolv-retry infinite
ns-cert-type server
♯Activation de la compression
comp-lzo
♯niveau de verbosité
verb 3
;configuration de ldap
;user UserUbuntu
;group NaftalGPLGroupe
auth-user-pass
```

Afin de vérifier que la configuration du fichier "Client.conf" associé à l'utilisateur "user_ubuntu" est correcte, nous saisissons les commandes suivantes respectivement :

```
♯ service openvpn start
♯ ifconfig
```

La figure ci-dessous confirme, que les étapes suivies précédemment sont correctes :

```
rahima@ubuntu:~$ sudo su
[sudo] password for rahima:
root@ubuntu:/home/rahima# cd
root@ubuntu:~# ifconfig
eth2      Link encap:Ethernet  HWaddr 00:0c:29:ad:6d:1a
          inet addr:192.168.119.147  Bcast:192.168.119.255  Mask:255.255.255.
0
          inet6 addr: fe80::20c:29ff:fead:6d1a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:54803 errors:0 dropped:0 overruns:0 frame:0
          TX packets:35335 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5876345 (5.8 MB)  TX bytes:3613519 (3.6 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:172 errors:0 dropped:0 overruns:0 frame:0
          TX packets:172 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:12899 (12.8 KB)  TX bytes:12899 (12.8 KB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-
-00-00
          inet addr:10.10.0.4  P-t-P:10.10.0.4  Mask:255.255.255.0
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:1468 (1.4 KB)
```

FIGURE 4.13 – Lancement et configuration de l'interface "tun0" du client.

Concernant la configuration associée à l'utilisateur "windows", nous devons spécifier certaines étapes supplémentaires comme suit :

- Convertion de l'extension ".conf" du fichier "client.conf" en "client.opvn" ;
- Téléchargement du logiciel "OpenVPNClient" ;
- Copie des certificats "ca.crt, ca.key, user_windows.crt" sur C :/ Programmefiles/ Openvpn Technologie/ Openvpn Client/etc/update/.

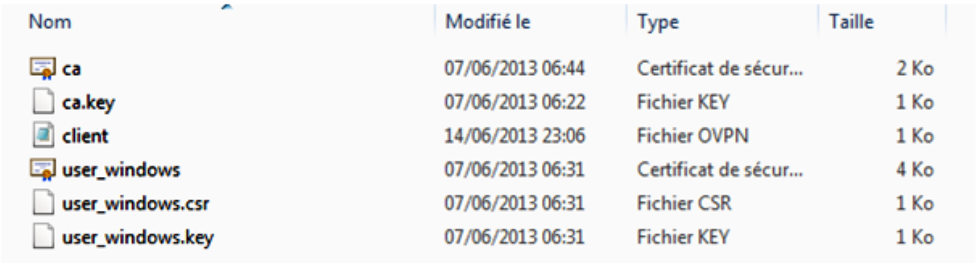


FIGURE 4.14 – Fichiers de configuration associés au client "user_windows".

4.6 Installation LDAP

Dans cette partie, nous allons installé et paramétré le serveur "LDAP" sous Ubuntu. Les étapes suivies sont cité ci-dessus :

4.6.1 Installation d' Openldap

Installation du serveur slapd d'OpenLDAP et du paquet $ldap - utils$, qui contient des utilitaires de gestion de LDAP :

```
♯apt-get install slapd ldap-utils
```

a) Après l'étape d'installation du paquet correspondant, nous avons ajouté les fichiers des schémas suivants :

ldapadd -Y EXTERNAL -H ldapi :/// -f /etc/ldap/schema/core.ldif.
ldapadd -Y EXTERNAL -H ldapi :/// -f /etc/ldap/schema/cosine.ldif.
ldapadd -Y EXTERNAL -H ldapi :/// -f /etc/ldap/schema/nis.ldif.
ldapadd -Y EXTERNAL -H ldapi :/// -f /etc/ldap/schema/inetorgperson.ldif.

b) Cryptage du mot de passe super user : nous choisissons de crypter le mot de passe, afin de renforcer la sécurité, pour ce fait on utilise la commande suivante :

```
♯ slappasswd -h MD5
New password : MON_MOT_DE_PASSE
Re-enter new password :MON_MOT_DE_PASSE
MD5bfg7yGR2fQy1dtsPU1hWow ==
```

c) Création du fichier de configuration $ldiff$: ♯ vim /etc/ldap/config.ldiff.

♯ Load dynamic backend modules
dn : cn=module,cn=config
objectClass : olcModuleList
cn : module
olcModulepath : /usr/lib/ldap
olcModulepath : /usr/lib/ldap
♯ Database settings
dn : olcDatabase=hdb,cn=config
objectClass : olcDatabaseConfig
objectClass : olcHdbConfig
olcDatabase : 1hdb
olcSuffix : dc=naftalgpl,dc=dz
olcDbDirectory : /var/lib/ldap
olcRootDN : cn=Admin,dc=naftalgpl,dc=dz
olcRootPW : MD5bfg7yGR2fQy1dtsPU1HWow==
olcDbConfig : set$_{c}$achesize020971520
olcDbConfig : set$_{l}$k$_{m}$ax$_{o}$bjects1500
olcDbConfig : set$_{l}$k$_{m}$ax$_{l}$ocks1500
olcDbConfig : set$_{l}$k$_{m}$ax$_{l}$ockers1500
olcDbIndex : objectClass eq
olcLastMod : TRUE
olcDbCheckpoint : 512 30
♯ACL
olcAccess : to attrs=userPassword by dn="cn=Admin,dc=naftalgpl,
dc=dz" write by anonymous auth by self write by * none
olcAccess : to attrs=shadowLastChange by self write by * read
olcAccess : to dn.base="" by * none
olcAccess : to * by dn="cn=Admin,dc=naftalgpl,dc=dz" write by * read
Les informations importantes, qui figurent dans ce fichier sont :
La racine de notre arborescence, il s'agit dans notre cas de "naftalgpl.dz" :
olcSuffix : dc=naftalgpl,dc=dz
Le compte administrateur de notre arborescence et son mot de passe :
olcRootDN : cn=Admin,dc=naftalgpl,dc=dz
olcRootPW : MD5bfg7yGR2fQy1dtsPU1HWow==
ldapadd -D cn=Admin,dc=naftalgpl,dc=dz -W -H ldapi :/// -f /etc/ldap/populate$_{i}$nitial.ldiff

4.6.2 Gestion de l'annuaire LDAP GUI

Pour visualiser notre arborescence, nous avons fait recours à l'installation du logiciel LDAP Account Manager, qui est une suite applicative prenant la forme d'une interface web. Elle permet de gérer un annuaire LDAP (type OpenLDAP) à distance, autour d'une interface conviviale, que ce soit pour gérer les comptes ou les groupes.

a) **Sécurisation**

LDAP Account Manager est une interface web, la sécurisation de celle-ci peut se faire sous deux angles distincts :

- L'accès direct à cette interface
- La connexion au serveur LDAP

Dans la première méthode, le contrôle d'accès à l'interface se fait avec une page de login, qui se base sur un user/mot de passe.

Dans la seconde méthode, il faut sécuriser la ligne entre le serveur web, et le serveur d'annuaire LDAP. Par l'intermédiaire d'une liaison SSL/TLS.

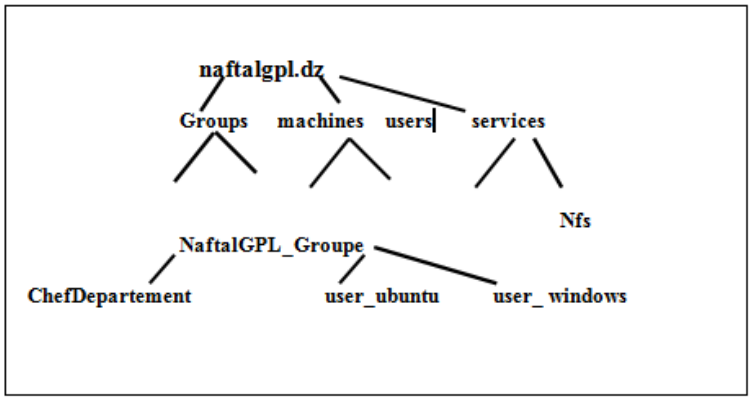


FIGURE 4.15 – : Arborescence appliquée.

4.6.3 Configuration coté serveur

a) Insérer les lignes suivantes pour l'authentification LDAP :
♯username-as-common-name
♯plugin /usr/lib/openvpn/openvpn-auth-pam.so openvpn

b) Redémarrer le service : afin de s'assurer que la configuration a été faire correctement :
♯/etc/init.d/openvpn restart
♯openvpn /etc/openvpn/serveur.conf

4.6.4 Configuration du client ubuntu

a) Installer les librairies pour l'authentification sur le poste client :
Installer le module LDAP pour NSS (Name Service Switch)

```
♯libnss-ldap
♯sudo apt-get install libnss-ldap
```

b) Installer le module PAM (Pluggable Authentication Module) pour LDAP :

```
♯libpam-ldap
```

Cette ligne indique que le client devra s'authentifier : ♯auth-user-pass

Afin de redémarrer le service et se connecter, on utilise les commandes suivantes :

```
♯/etc/init.d/openvpn restart
♯openvpn /etc/openvpn/Client.conf
♯/etc/init.d/slapd restart
```

A présent, nous allons passer à la mise en place du système de détection d'intrusions, il s'agit dans notre cas de "Snort ", nous allons présenter les différentes étapes nécessaires pour ce faire.

4.7 Installation de Snort

4.7.1 Présentation de Snort

Snort est un NIDS écrit par Martin Roesch en 1998 et développé par Sourcefilen, disponible sous licence GNU. Snort a la capacité d'effectuer l'analyse du trafic en temps réel et la journalisatin de paquets sur le protocole Internet IP.
Snort effectue l'analyse de protocole et la recherche de contenu, pour ce faire il utilise une sonde pour détecter les attaques, les scans de ports, etc[11].

4.7.2 Architecture de Snort

L'architecture de Snort est modulaire et est composée de[12] :

- Un noyau de base : au démarrage, ce noyau charge un ensemble de règles, compile, optimise et classe celle-ci. Durant l'exécution, le rôle principal du noyau est la capture de paquets.
- Une série de pré-processeurs : ceux-ci améliorent les possibilités de SNORT en matière d'analyse et de recomposition du trafic capturé. ils reçoivent les paquets directement capturés, éventuellement les retravaillent puis les fournissent au moteur de recherche de signatures.
- Une série d'analyses appliquées aux paquets : ces analyses se composent principalement de comparaisons de différents champs des headers des protocoles(IP, ICMP, TCP et UDP) par rapport à des valeurs précises.
- Une série d'output plugins : aprés la détection d'intrusion, une série de "output plugins" permet de traiter cette intrusion de plusieurs manières : envoie vers un fichier log, envoie d'une message d'alerte vers un serveur syslog...

4.7.3 Dépendances de Snort

4.7.3.1 Mise en place de Barnyard

Barnyard est une couche applicative, qui exploite les événements générés par Snort. Ainsi, Snort inscrira les événements dans les logs au format unifié et ces derniers seront exploités par Barnyard pour une inscription en base de données [13].

4.7.3.2 La console BASE

Par défaut, les alertes de Snort sont enregistrées dans un simple fichier texte. L'analyse de ce fichier n'est pas aisée, même en utilisant des outils de filtre et de tri. C'est pour cette raison qu'il est vivement conseillé d'utiliser des outils de monitoring. Parmi ceux-ci, le plus en vogue actuellement est BASE (Basic Analysis and Security Engine), un projet open-source basé

sur ACID (Analysis Console for Intrusion Databases). La console BASE est une application Webécrite en PHP qui interface la base de données dans laquelle Snort stocke ses alertes [14]. Nous avons choisi d'installer la version " snort 2.8.5.2 ", pour aboutir à une installation complète et correcte de Snort et des composants nécessaires à son fonctionnement, il est impératif d'installer un ensemble de pré-requis qui sont les suivants :

– ♯ sudo apt-get install libpcap0.8-dev libmysqlclient15-dev mysql-client-5.1 mysql-server-5.1 bison flex apache2 php5 libapache2-mod-php5 php5-gd php5-mysql libtool libpcre3-dev php-pear vim ssh openssh-server.

A présent, on tape la commande suivante :
♯ Apt-get install snort

4.7.3.3 Lancement de Snort

Afin de s'assurer que " Snort " s'est correctement installé, nous introduisons la commande qui suit :
♯Snort -V, qui lance snort et affiche la version de snort installée.

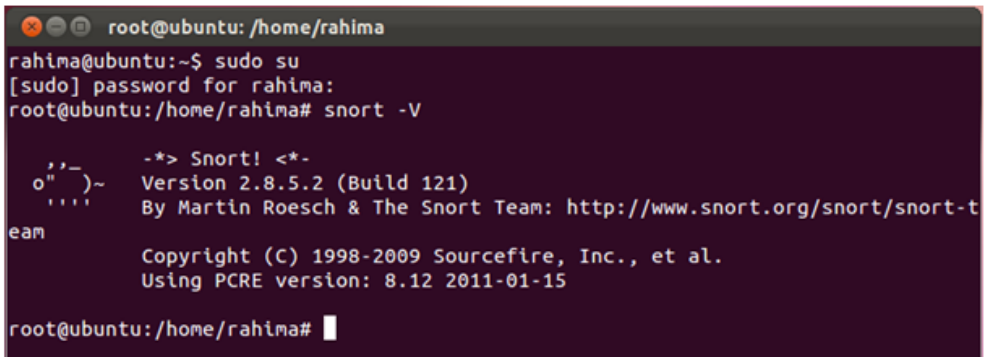


FIGURE 4.16 – Lancement de Snort avec succès "user_windows".

4.7.4 Mode de fonctionnement de Snort

Snort constitue trois modes de fonctionnement : le mode écoute, le mode log de paquets et le mode détection d'intrusions

4.7.4.1 Mode écoute " sniffer "

Ce mode consiste à écouter le réseau, à travers un ensemble de commandes qui indiqueront à Snort le type de résultat à afficher :

- La commande : ♯ snort -v ; cette commande affiche les en têtes TCP/IP
- La commande : ♯snort -vde ; cette commande quant à elle affiche les IP et les en têtes TCP/UDP/ICMP

4.7.4.2 Mode packet logger

Ce mode est en tout point similaire au précédent, à ceci prés que les logs ne s'affiche plus à l'écran, mais s'inscrivent directement dans un fichier log. Le répertoire de log de snort étant /var/log/snort.
La commande à saisir est la suivante :

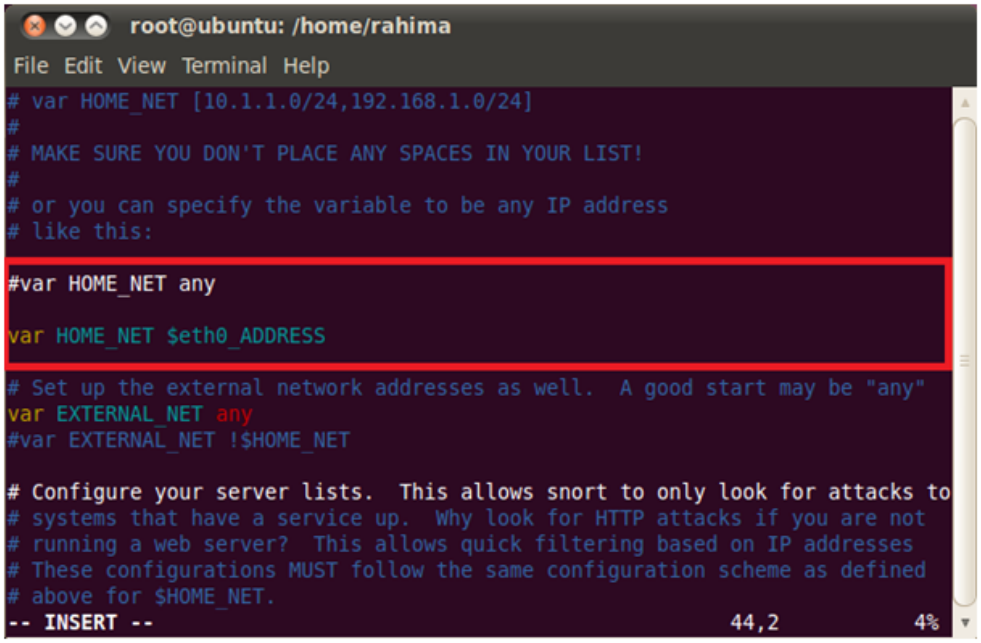
♯ snort -de -l /var/log/snort

4.7.4.3 Mode de détection d'intrusion " NIDS "

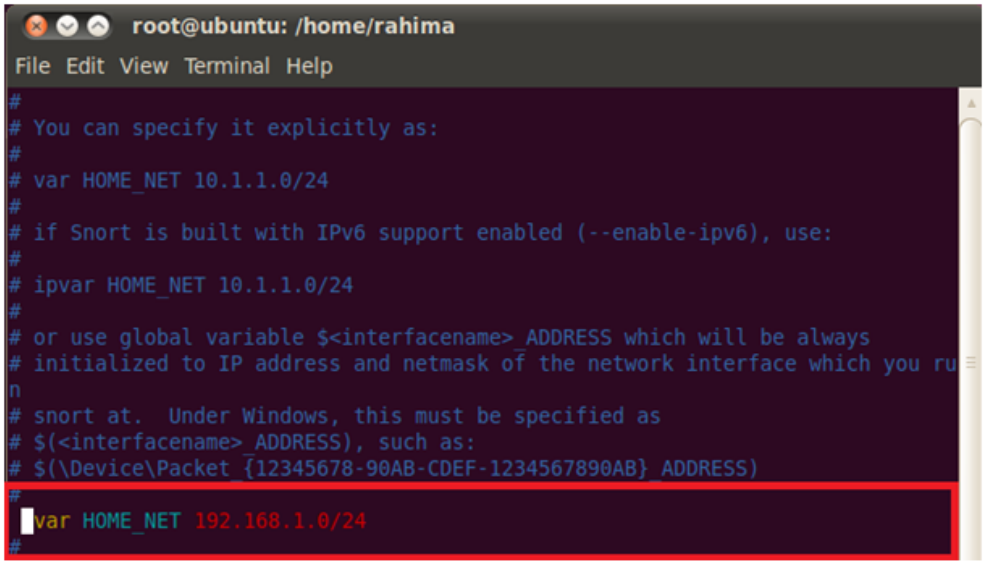
La mise en place de Snort repose sur le mode détection d'intrusion, pour ce faire, nous devons éditer le fichier de configuration associé à SNORT : " snort.conf " à partir de la commande suivante :

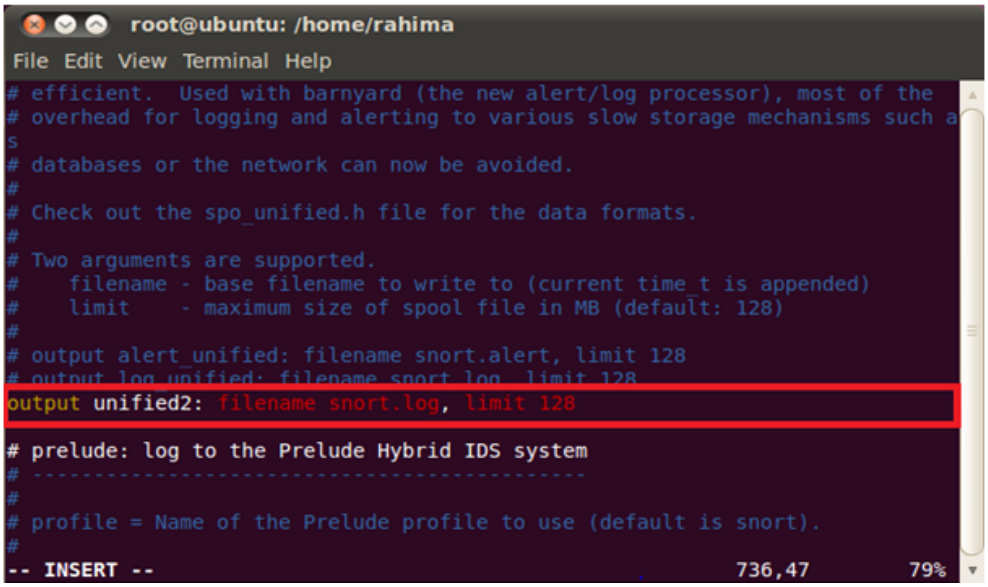
♯vim /etc/snort/snort.conf

Une fois le fichier lancé, on commente la ligne "varHOME_NETany" en ajoutant le symbole "♯", et on rajoute la ligne "varHOME_NETeth0_ADDRESS" afin d'indiquer qu'il s'agit d'une interface Ethernet, ensuite nous spécifions la classe d'adresses associée au réseau en ajoutant la ligne suivante : "varHOME_NET192.168.1.0/24"



Maintenant, nous allons spécifier le format du fichier de sortie, dans notre cas nous avons choisi le format "unified2" pour ce faire, nous allons en premier lieu mettre en commentaire la ligne : "Outputlog_tcpdump : tcpdump.log" contenue dans le fichier "snort.conf", puis insérer la ligne " Output unified2 : filename snort.log, limit 128 " en second lieu.





4.7.5 Mise en oeuvre de la base de données Mysql

4.7.5.1 Installation

Après l'installation des pré-requis associés au serveur et au client Mysql précédemment, nous saisissons à partir du shell la commande qui suit :

♯ sudo apt-get install mysql-server mysql-client

Maintenant que l'installation est faite, nous pouvons accéder à la base de données MYSQL, pour ce faire, nous saisissons la commande suivante :

♯ mysql -u root -p

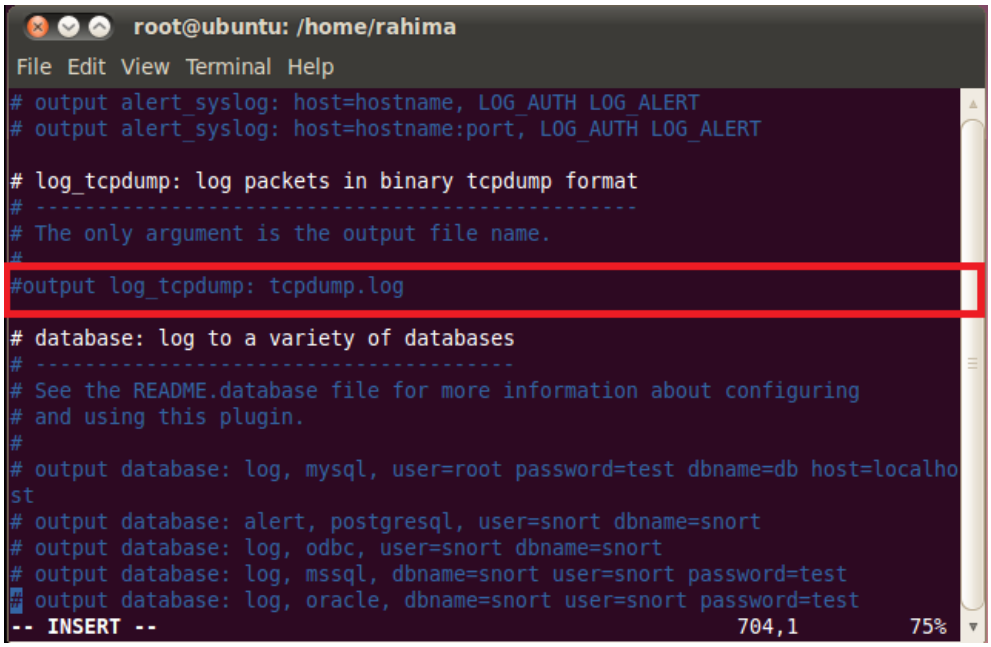


FIGURE 4.17 – Edition du fichier "Snort.conf".

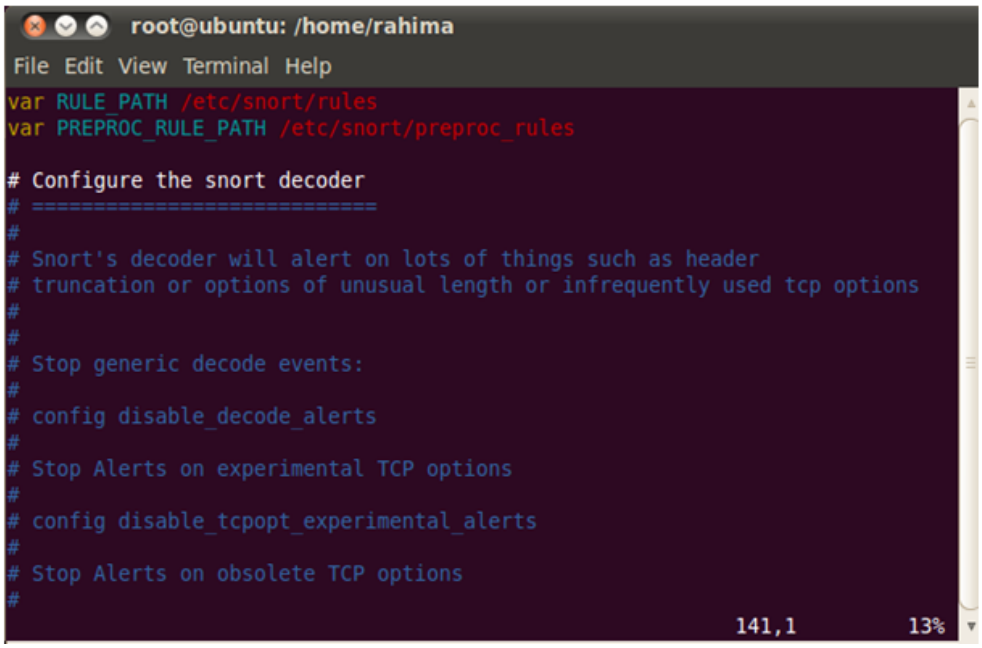


FIGURE 4.18 – Spécification des régles du fichier "Snort.conf"

Puis, nous saisissons le mot de passe associé à la base de données définit durant l'installation de "snort – mysql" précédemment.

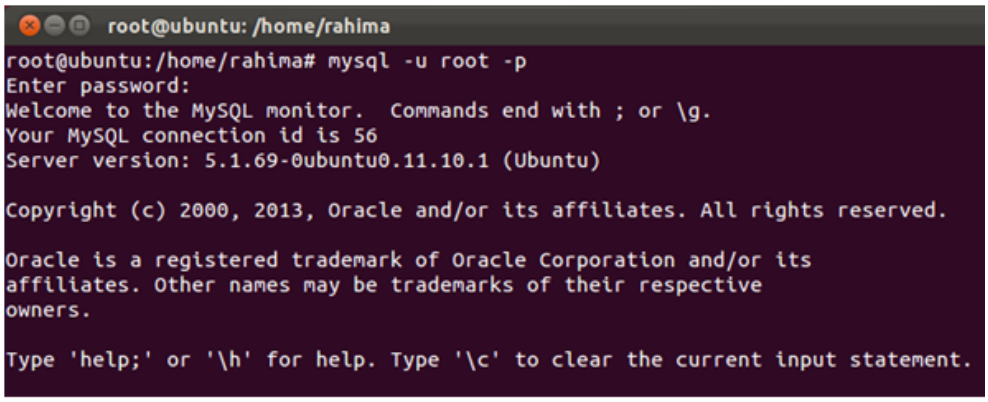


FIGURE 4.19 – Lancement de la base de données "mysql."

4.7.5.2 Création de la base de données snort

A présent, nous allons procéder à la création de la base de données nommée "snort". Pour cela, nous saisissons l'ensemble des commandes suivantes, afin d'attribuer les paramètres associés à la base de données "snort".

```
Mysql > create database snort ;
Mysql > grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhost ;
Mysql > SET PASSWORD FOR snort@llocalhost=PASSWORD('snort') ;
Mysql > exit
```

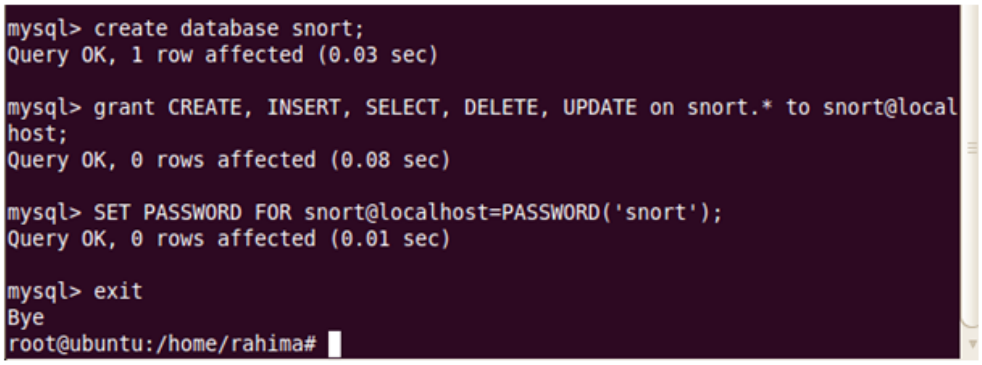


FIGURE 4.20 – Création de la base de données " snort ".

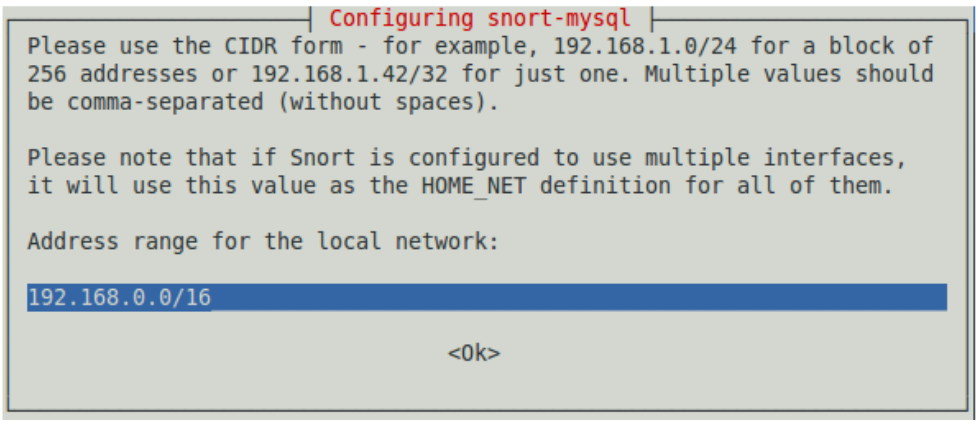
Maintenant que la base de données Snort crée, nous procédons à l'installation de snort-mysql, pour en faire le lien.

a) Installation de Snort-Mysql

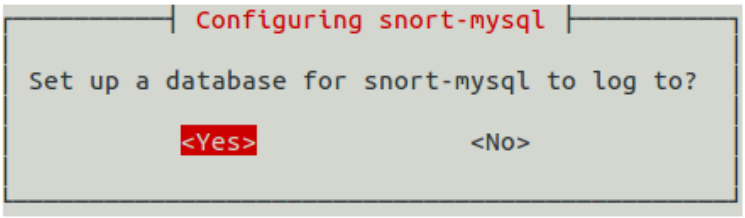
Nous saisissons à partir du shell, la commande suivante :

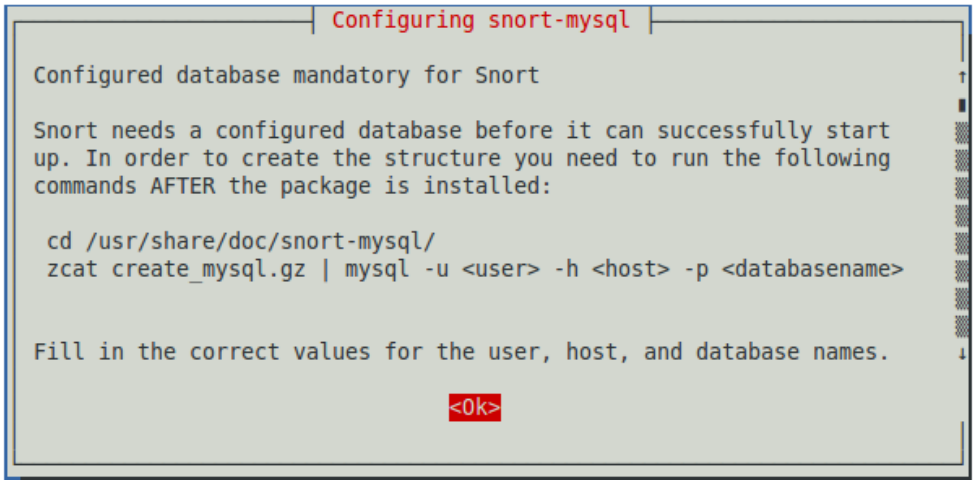
♯ apt-get install snort-mysql

La figure suivante sera affichée :



En appuyant sur <OK>, la fenêtre s'affichera :





b) Import des schémas de données

Maintenant, nous allons procéder à la création du schéma des données pour la base de données Snort, en accédant d'abord dans le répertoire contenant snort-mysql ensuite, nous allons extraire et rapporter le schéma de données, à l'aide de la commande " zcat "

```
♯ cd /usr/share/doc/snort-mysql/
♯ zcat create_mysql.gz|mysql − uroot − p
```

```
root@ubuntu:/home/rahima# cd /usr/share/doc/snort-mysql/
root@ubuntu:/usr/share/doc/snort-mysql# zcat create_mysql.gz | mysql -u root -p
snort
Enter password:
```

FIGURE 4.21 – Import des schémas de données pour la base de données "snort".

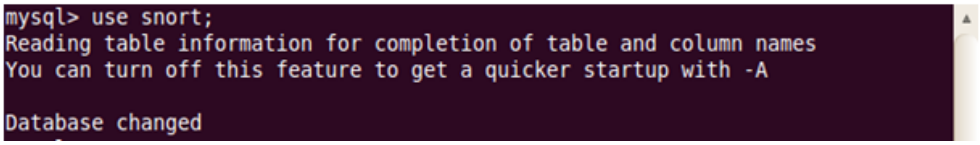
Afin de vérifier que la création de la base de données a été faite correctement ainsi que l'importation du schéma de données, nous utilisons les commandes suivantes :

Mysql> SHOW DATABASES ;

Puis, on saisit la commande :

FIGURE 4.22 – Création de la base de données snort.

Mysql> use snot ; cette commande nous permet de se placer au niveau de la base où l'on veut créer les tables associés à "SNORT"



Mysql> SHOW TABLES ;

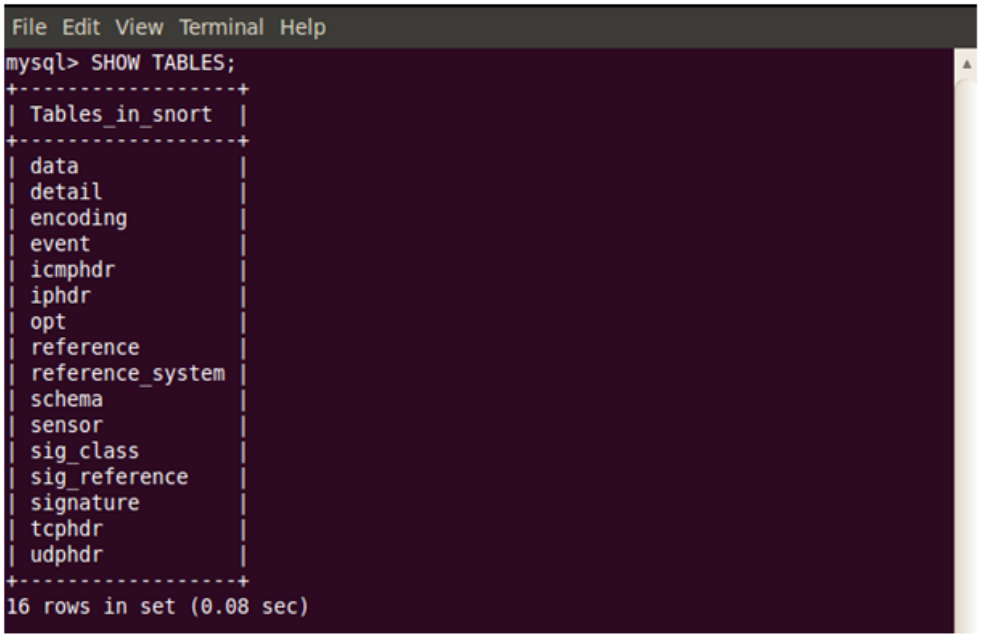


FIGURE 4.23 – Création des tables associées à snort.

4.7.6 Mise en place de la console BASE

Les prés requis associés à l'installation de BASE ont été installé précédemment. A présent nous accédons au fichier "php.ini" pour apporter des modifications nécessaires à ce fichier :

♯vim /etc/php5/apache2/php.ini

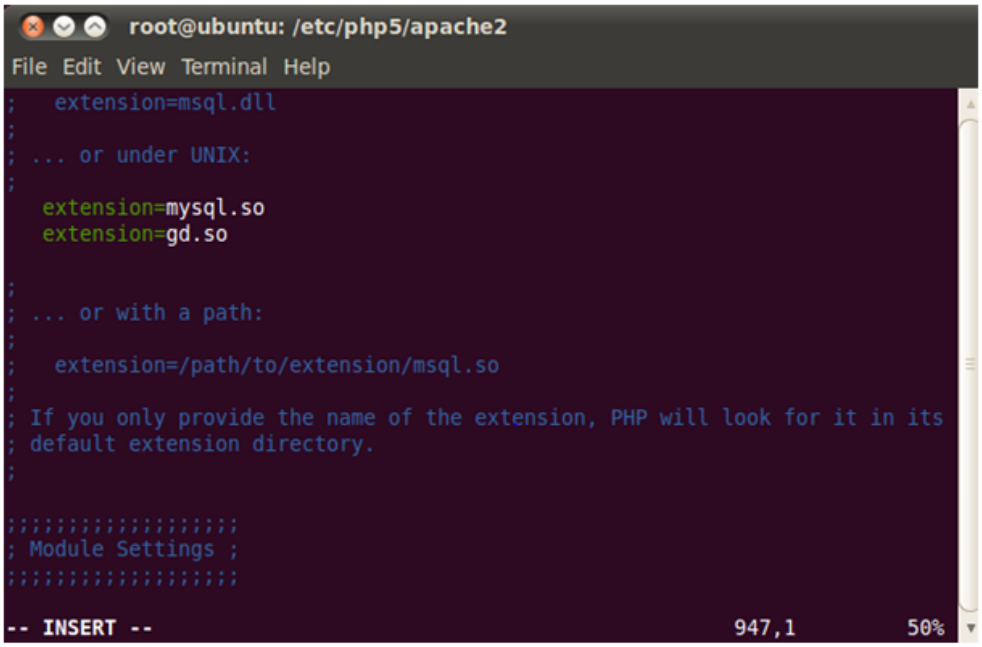


FIGURE 4.24 – Edition du fichier php.ini.

Nous passons maintenant à la configuration du fichier "apache2.conf", dans le but d'ajouter le nom du serveur associé, dans notre cas il s'agit de "localhost."

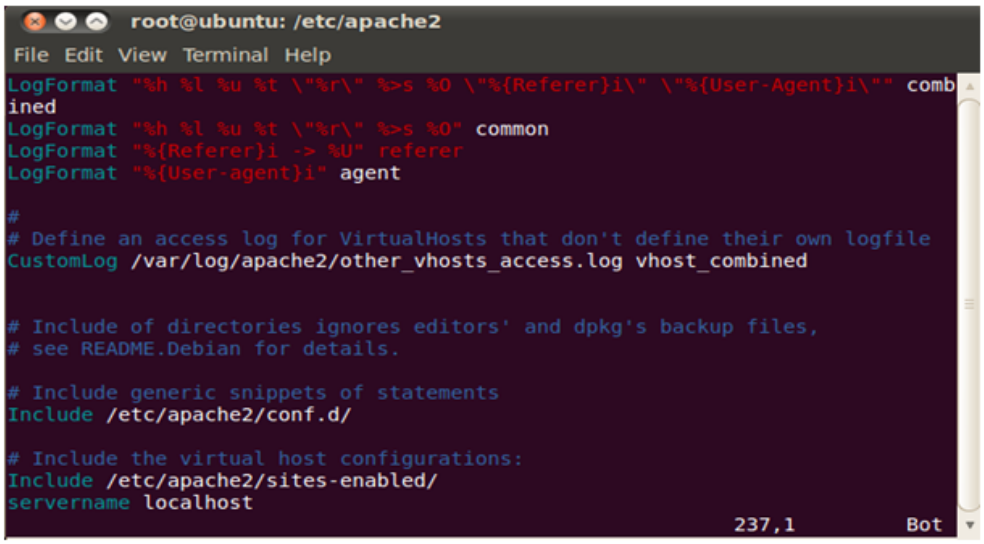


FIGURE 4.25 – Edition du fichier " apache2 ".

♯/etc/init.d/apache2 restrat

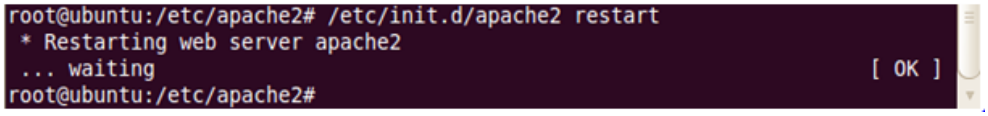


FIGURE 4.26 – Démarrage du serveur apache2 avec succès.

Pour s'assurer que le serveur "apache2" est en marche, on introduit sur le navigateur web l'adresse localhost "127.0.0.1", le résultat figure ci-dessous :

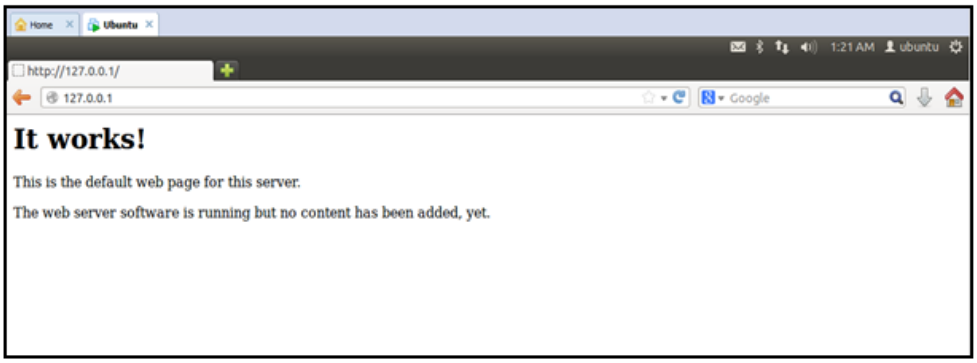


FIGURE 4.27 – Lancement d'apache2 sur le navigateur web.

Maintenant, on installe la version " base-1.4.5.tar.gz ", que l'on décompresse à l'aide de la commande suivante :

♯Tar -xzvf base-1.4.5.tar.gz.

Afin de vérifier que Base à été installer correctement, on accède au répertoire spécifique et on saisit la commande " ls " pour afficher le contenu du répertoire Base :

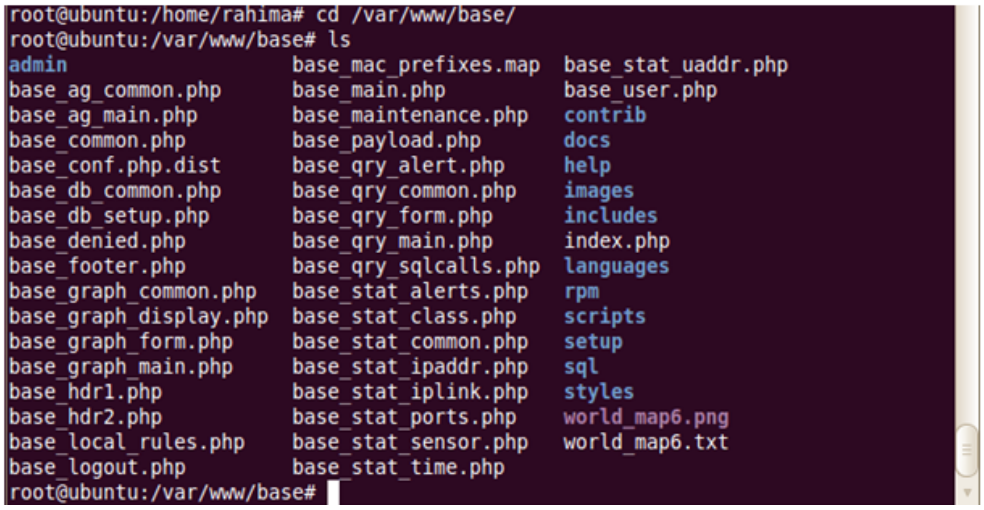


FIGURE 4.28 – Contenu du répertoire base.

Puis, on déplace le répertoire Base dans le répertoire " var/www/base " à l'aide de la commande " mv " comme suit :

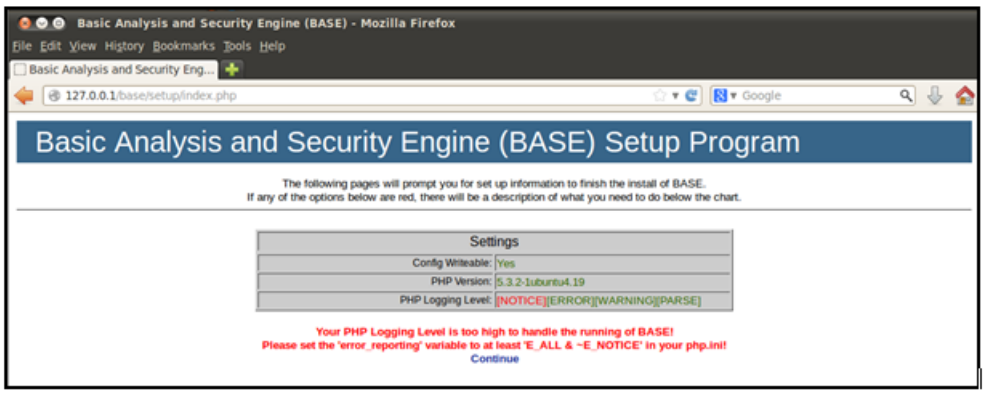
♯mv base-1.4.5 /var/www/base

a) Installation d'adodb5

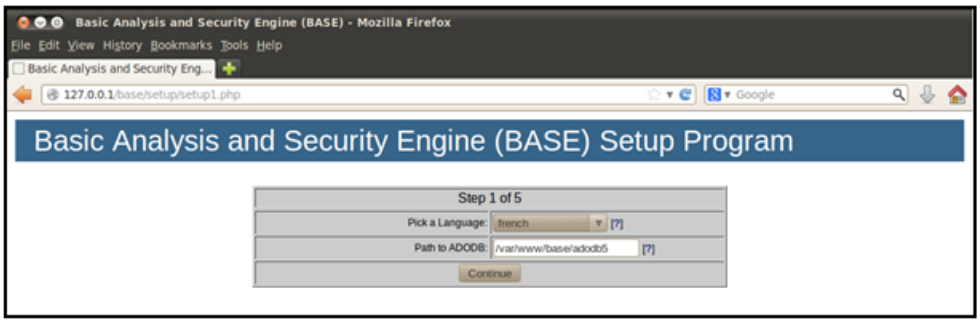
Une fois, le fichier décompressé nous allons déplacer celui-ci vers le répertoire var/www/base et lui attribuer les droits d'accès spécifiques :

```
♯mv adodb5 /var/www/base/
♯-R www-data : /var/www/base/
```

Maintenant que l'installation de base est achevée, nous passons à la vérification de celle-ci, en lançant sur le navigateur web l'adresse suivante : 127.0.0.1/base/, une fois fait la figure suivante est affichée sur le navigateur web :



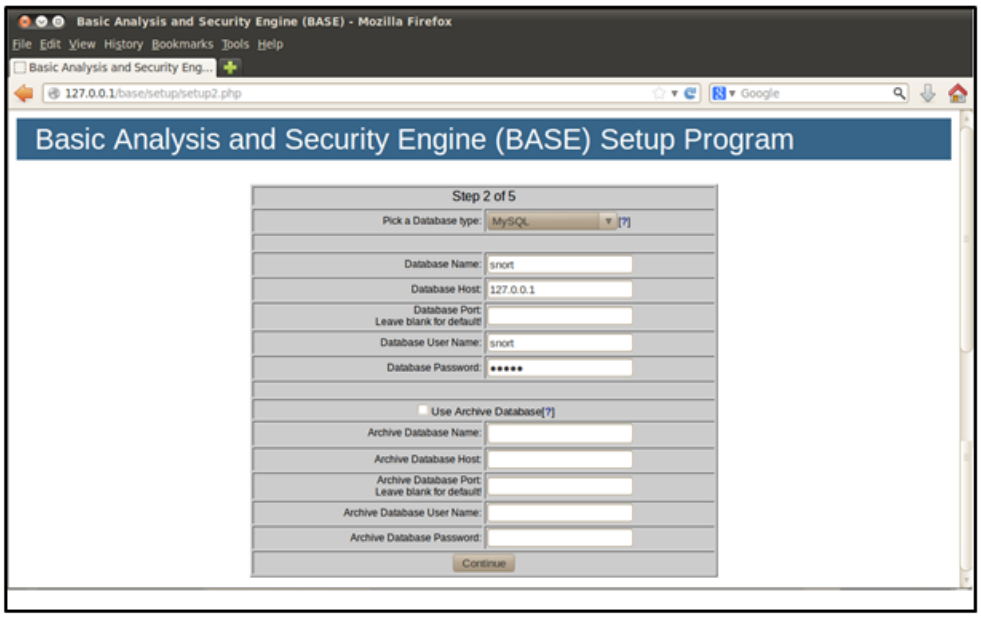
En appuyant sur le bouton " continue ", la figure suivante s'affiche :



Nous devons remplir les champs suivants, comme suit :

- Pick a language : French ;
- Path to ADODB : /var/www/base/adodb5 ;

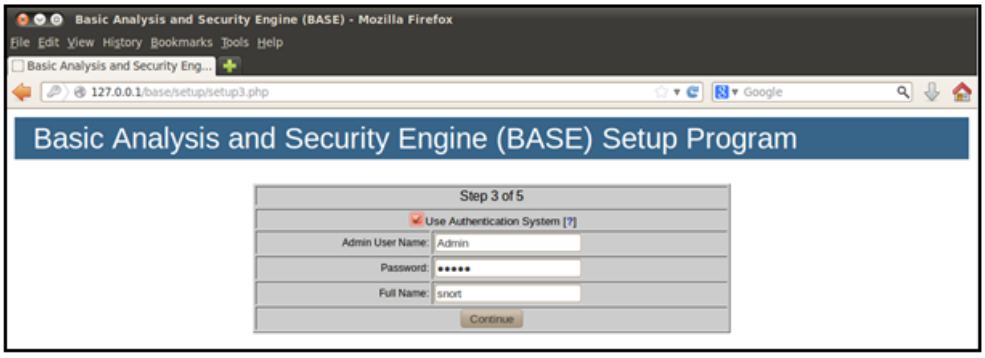
En appuyant sur le bouton " continue ", la figure suivante s'affiche :



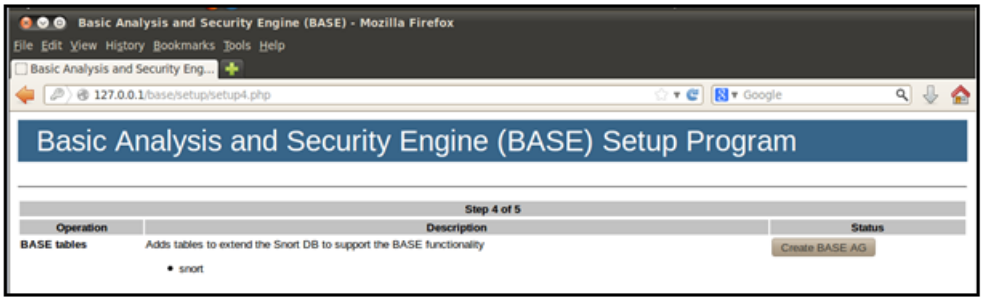
Nous insérons les champs suivants :

- Pick a Database type
- Database Name : snort
- Database Host : 127.0.0.1
- Database User Name : snort
- Database Password : snort

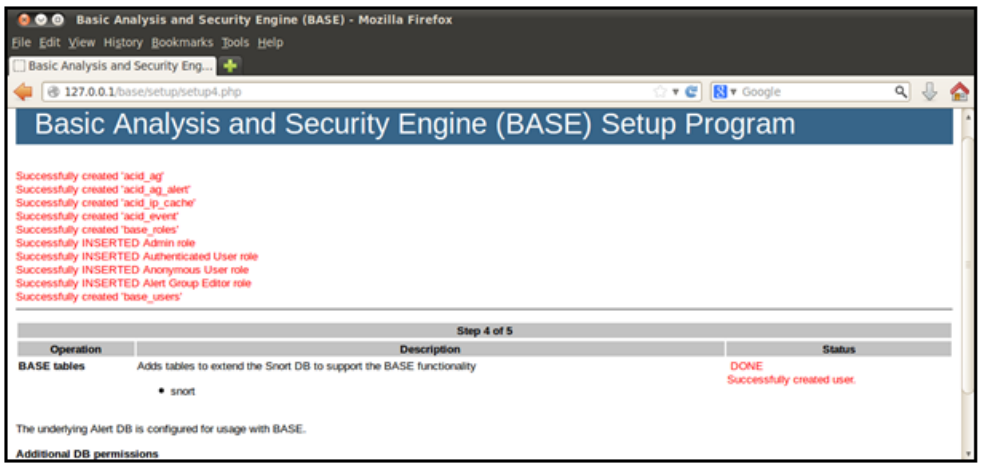
En appuyant sur le bouton " continue ", la figure suivante s'affiche afin que l'administrateur de base s'authentifie :



En appuyant sur le bouton " continue ", la figure suivante s'affiche :



A présent, on clique sur le bouton " create BASE AG ", à ce moment là c'est la figure suivante qui s'affiche :



4.8 Tests et évaluation

La partie présente, consiste à illustrer les différents tests associés à la mise en place du réseau privé virtuel, de l'authentification à partir de l'annuaire LDAP et enfin de l'éfficacité de fonctionnement du système de détection d'intrusions "Snort" réspectivement.

4.8.1 Réseau privé virtuel

Nous avons suivi l'organigramme présenté ci-dessous, afin d'établir un test sur le bon fonctionnement de la configuration implémentée précédemment :

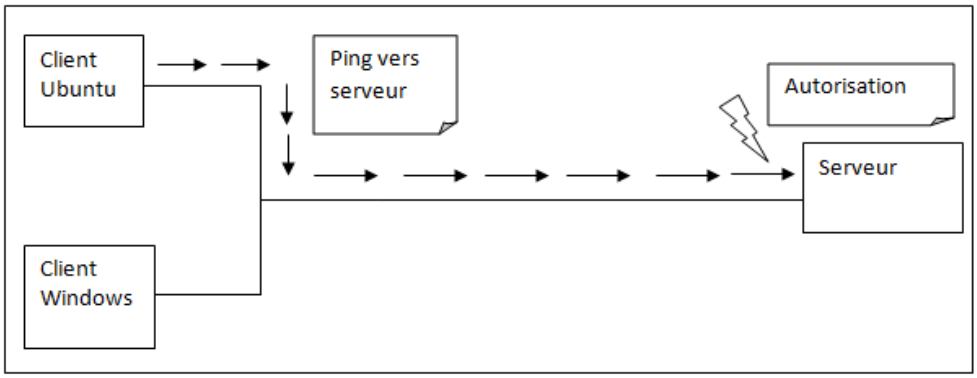


FIGURE 4.29 – Organigramme de solution.

4.8.1.1 Connexion du client Ubuntu vers le serveur

Une fois le serveur lancé, on récupère l'adresse IP du serveur à partir de la commande " ifconfig ", ensuite on lance le client ubuntu situé sur une autre machine virtuelle afin d'effectuer le ping avec l'adresse IP du serveur, le résultat obtenu est le suivant :

```
root@ubuntu:~# ping 10.10.0.1
PING 10.10.0.1 (10.10.0.1) 56(84) bytes of data.
64 bytes from 10.10.0.1: icmp_seq=1 ttl=64 time=0.921 ms
64 bytes from 10.10.0.1: icmp_seq=2 ttl=64 time=0.995 ms
64 bytes from 10.10.0.1: icmp_seq=3 ttl=64 time=0.972 ms
64 bytes from 10.10.0.1: icmp_seq=4 ttl=64 time=0.840 ms
64 bytes from 10.10.0.1: icmp_seq=5 ttl=64 time=0.881 ms
64 bytes from 10.10.0.1: icmp_seq=6 ttl=64 time=1.10 ms
^C
--- 10.10.0.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5021ms
rtt min/avg/max/mdev = 0.840/0.952/1.107/0.093 ms
```

FIGURE 4.30 – Succès du ping à partir du client ubuntu vers le serveur.

D'après les résultats obtenus en lançant le ping, on déduit que la connexion s'est réellement établie entre le client et le serveur par l'échange de paquets udp.

4.8.1.2 Connexion du client windows vers le serveur

Afin de s'assurer que la connexion du client windows vers le serveur ubuntu s'est éffectuée, nous avons installer un client openvpn windows.
Les étapes de connexion se résument à ce qui suit :

a) Lancement du client openvpn

Une fois le client windows openvpn lancé, on saisie l'adresse IP du serveur ubuntu, qui est : 10.10.0.1.

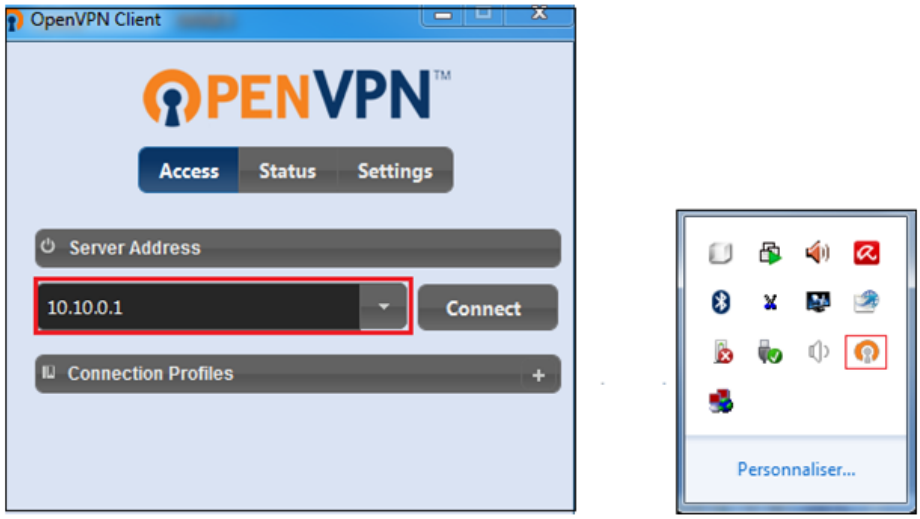


FIGURE 4.31 – Etablissement de connexion vers le serveur Openvpn.

Maintenant, nous importons le fichier " client.opvn ", le client windows apparait sur l'interface comme suit :

FIGURE 4.32 – Ajout du client windows au serveur.

La figure suivante illustre la connexion du client au sein du serveur ubuntu, qui va lui attribuer une adresse IP :

FIGURE 4.33 – Client connecté.

4.8.2 Scan du réseau " nmap "

Afin de confirmer que le système de détection d'intrusions " SNORT " effectue réellement sa fonction, nous avons choisi de déclencher une alerte par scan de ports du réseau à partir de l'outil " nmap ".

On doit en parallèle lancé snort et barnyard comme suit :

♯snort -c /etc/snort/snort.conf -i eth0

♯ barnyard2 -c /etc/snort/barnyard2.conf

-G /etc/snort/gen-msg.map -S /etc/snort/sid-msg.map

- d /var/log/snort -f snort.log -w /var/log/snort/barnyard.waldo

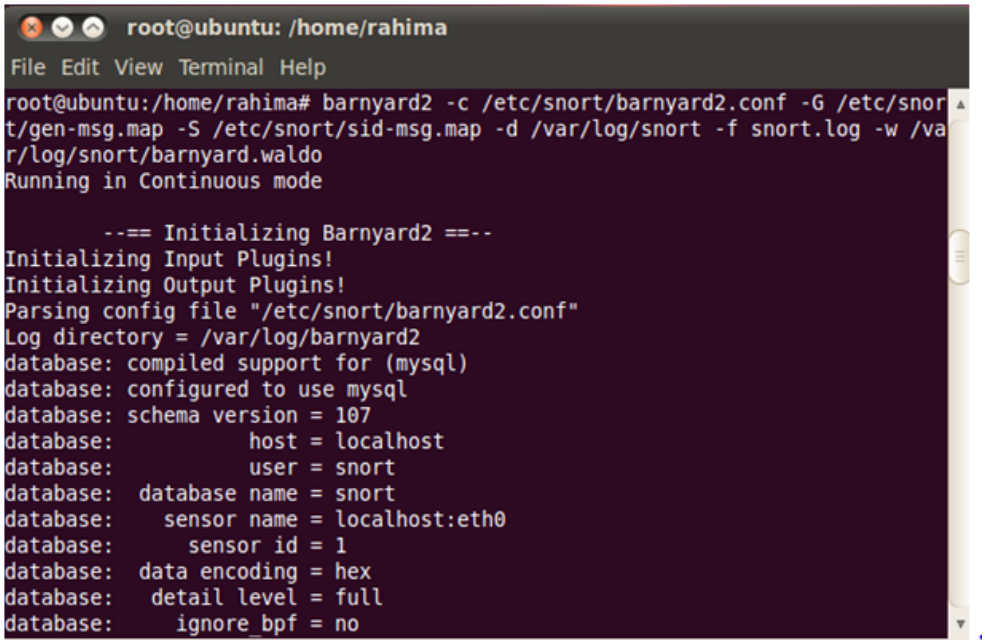


FIGURE 4.34 – Lancement de Barnyard

On aperçoit ensuite, la fenêtre ci-dessous en lançant la commande suivante à partir d'un autre shell : ♯sudo nmap -PN -V -0 192.168.1.0/24

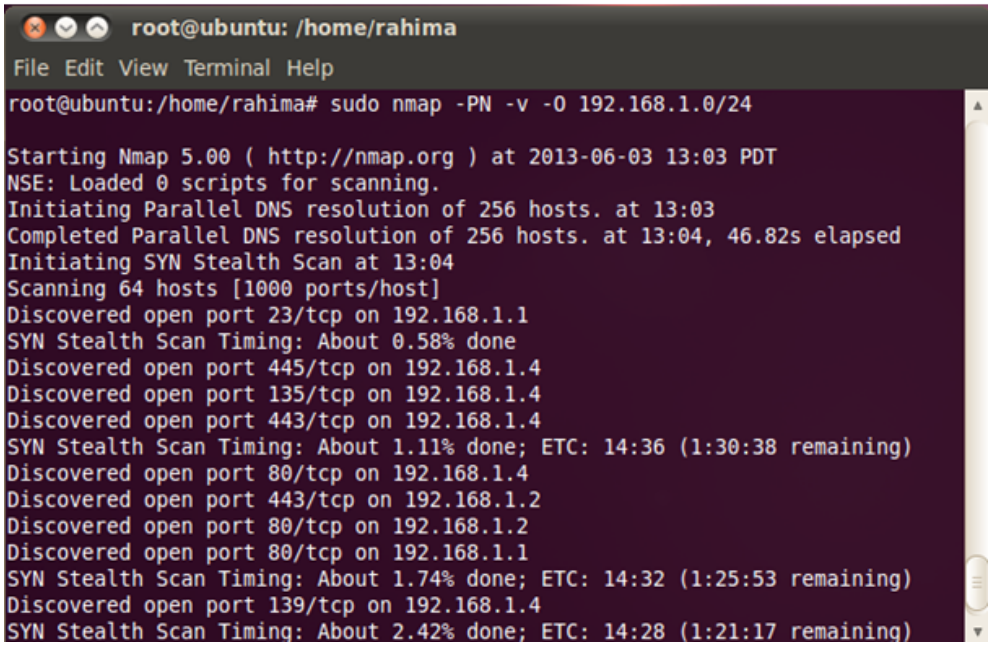


FIGURE 4.35 – Scan nmap.

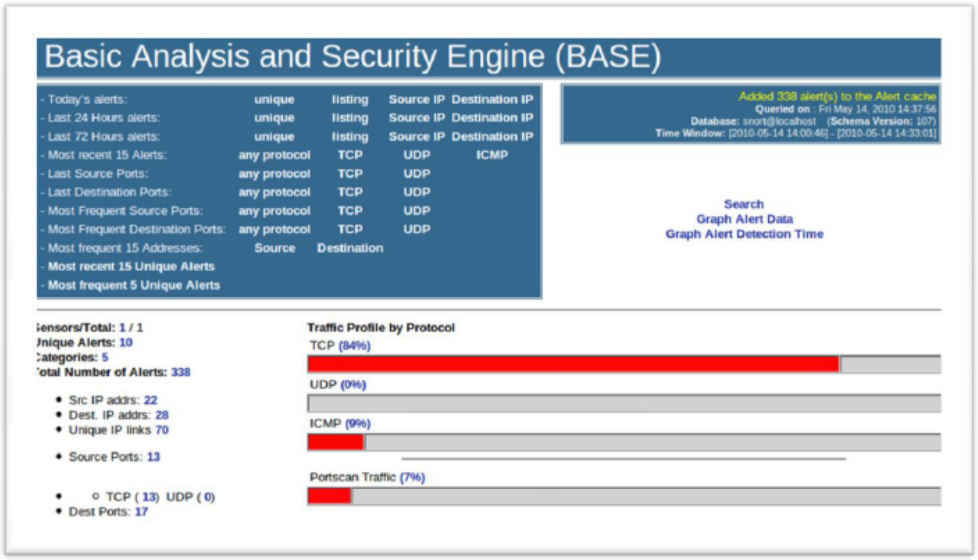


FIGURE 4.36 – Visualisation d'alerte à partir de BASE.

4.9 Conclusion

Nous avons pu aboutir aux objectifs visés pour l'accomplissement de ce projet, en effet nous avons mis en place un réseau privé virtuel constitué d'un serveur et de deux clients de plateforme différentes et nous avons assuré l'authentification des clients à partir de l'annuaire LDAP enfin, nous avons mis en place un système de détection d'intrusions.

Afin de renforcer la sécurité au niveau du réseau local.

CONCLUSION GÉNÉRALE

Les réseaux d'entreprises ont évolué au fil du temps à une vitesse vertigineuse. L'interconnexion de ces réseaux à Internet les a directement exposés aux menaces informatiques.

L'étude que nous avons menée nous a conduit à découvrir l'une des mesures de sécurité à déployer, pour assurer la sécurité du réseau au sein du district "NAFTAL GPL ".
Il s'agit de la mise en place d'un réseau privé virtuel "VPN", ainsi que d'un annuaire d'authentification nécessaire pour centraliser les informations de tous les utilisateurs, notre choix s'est porté sur l'annuaire " LDAP ". Dans le but de renforcer la sécurité au sein du réseau LAN de l'entreprise, nous avons eu l'initiative de mettre en place un système de détection d'intrusions, il s'agit de l'IDS "Snort".

En effet, nous avons présenté un travail divisé en quatre chapitres, à savoir l'aspect théorique qui comprend les trois premiers chapitres, dont le premier a porté sur la présentation de l'entreprise d'accueil et du réseau requis par celle-ci, ensuite nous avons défini la problématique pour en proposer une solution VPN, qui consiste à mettre en place une liaison distante et sécurisée entre le district " NAFTAL GPL " et le centre d'AKBOU, le second chapitre a porté sur la sécurité des réseaux informatiques et toutes les notions qui s y rapportent, le troisième chapitre quant à lui a porté sur les aspects associés aux réseaux privés virtuels.
L'aspect pratique a fait l'objet du quatrième chapitre qui a consisté à l'implémentation de la solution proposée préalablement, suivi des différents tests d'évaluation réalisés, permettant de garantir le succès de la démarche de configuration.

Ce projet a eu énormément d'apport sur nos connaissances, notamment en termes de configuration dans un environnement "Linux". De plus nous avons aussi enrichi nos connaissances dans le domaine de la sécurité d'un réseau d'entreprise que ça soit au niveau

du réseau locale, grâce à la mise en place d'un système de détection d'intrusions ou bien à partir de l'extérieur du réseau de l'entreprise, grâce à l'implémentation d'un réseau privé virtuel .

En terme de perspectives, nous envisageons la mise en place d'un système de prévention d'intrusions " IPS ", pour renforcer d'avantage le réseau de l'entreprise, nous prévoyons aussi l'implémentation de l'annuaire Active Directory sous linux .

BIBLIOGRAPHIE

[1] http ://www.cyberlycee.fr/reseau_barthou/res_ini.html. 28/06/2013.

[2] http ://www.ssi-conseil.com/downloads/ISO 27002FrWP.pdf. 28/06/2013.

[3] http ://www.cedric bailllet.fr/IMG/pdf. *La sécurité de la téléphonie sur IP en entreprise.* 28/06/2013.

[4] http ://litis.univ-lehavre. fr/ duvallet/enseignements/cours/M2MATIS/SIRES-IDS-4p.pdf : Les systèmes de détection d'instructions réseaux. 28/06/2013.

[5] https ://saquet.users.greyc.fr/docradis/VPN Tunneling.pdfLes Réseaux Privés Virtuels (VPN). 28/06/2013.

[6] Tomas Klein et Sebf 2004.2007. http ://www.frameip.com/vpn/ :Document web site consacré à les Réseaux privés Virtuels-VPN., suivi Xavier Lasserre. 28/06/2013.

[7] Cisco networking Academy. 2007/2008.

[8] http ://openvpn.net/index.php/open-source/documentation/manuals/65-openvpn-20x manpage.html. 28/06/2013.

[9] http ://irt.enseeiht.fr/anas/cours/tp igc.pdf. 28/06/2013.

[10] http ://openvpn.ne. 28/06/2013.

[11] http ://repo.zenk security.com/Protocoles_reseaux_securisation/Miseonde28/06/2013.

[12] http : //www.securinets.com/sites/default/files/tuto_pdf/tuto_snort.pdf. 28/06/2013.

[13] http ://www.aldeid.com/wiki/Snort :Detection_analyse :Barnyard. 28/06/2013.

[14] http ://www.inetdoc.net/pdf/Session2k9.analyse.rapport.pdf. 28/06/2013.

[15] Jean-Philippe BAY Jean-François PILLOU. *Tout sur la sécurité informatique, DUNOD.* 2009.

[16] Marcel Rizcallah. *Annuaires LDAP, EYROLLES.* 2004.

[17] Sebastien ROHAUT. Gilles CHAMILLARD. *EDITION, 3 eme edition.* 2010.

[18] Laurent Bloch-Christophe Wolfhugel. *EYROLLES, 2eme edition.* 2005.