République Algérienne Démocratique et PopulaireMinistère de l'Enseignement Supérieur et de la Recherche Scientiftque

Université A/Mira de Béjaïa

Faculté des Sciences Exactes

Département d'Informatique

Mémoire de fin de cycle en vue d'obtention du diplôme de master professionnel en informatique

spécialité : Administration et Sécurité des Réseaux

Thème

La mise en place d'un serveur de messagerie sur un réseau LAN

Cas d'étude : Entreprise Portuaire de Bejaia

Présenté par:

- ***HADID Yamina***
- ***OUAKKOUCHE Chahrazed***

Membres du jury :

-Présidente : BOUTRID Samia	***MAA, U.A.M, Béjaia.***
-Examinateur : AISSANI Sofiane	***MAB, U.A.M, Béjaia.***
-Examinateur : ELSAKAAN Nadim	***Doctorant, U.A.M, Béjaia.***
-Promoteur : BOUKERRAM Abdellah	***Professeur, U.A.M, Béjaia***
-Co-Promoteur : AMROUN Kamel	***MAA, U.A.M, Béjaia***
- Encadreur: BETTACHE Idir	***Assistant PDG/IT Manager, EPB.***

Promotion 2015/2016

Liste des abréviations

AJAX : **A**synchronous **J**avaScript **A**nd **X**ML

BIND : **B**erkley **I**nternet **N**aming **D**aemon.

CNAME : **A** **C**anonical **N**ame record

DMZ : **D**eMilitarized **Z**one

DHCP : **D**ynamic **H**ost **C**onfiguration **P**rotocol

DNS : **D**omain **N**ame **S**erver

EPB : **E**ntreprise **P**ortuaire de **B**ejaia

FQDN : **F**ully **Q**ualified **D**omain **N**ame

GPL : **G**eneral **P**ublic **L**icense

HTML : Hypertext Markup Language

IBM : **I**nternational **B**usiness **M**achines **C**orporation

IHM : **I**ntéraction **H**omme **M**achine

IMAP : **I**nteractive **M**ail **A**ccess **P**rotocol

IP : **I**nternet **P**rotocol

ISO : **O**rganosation **I**nternational de normalisation

LAMP : **L**inux **A**pache2 **M**ysql **P**hp

LAN : **L**ocal **A**rea **N**etwork

LTS : **L**ong **T**erm **S**upport

MAN : **M**etropolitan **A**rea **N**etwork

Mac OS : Macintosh Operating System

MS-DOS : Microsoft Disk Operating System

MDA : **M**ail **D**elivery **A**gent

MTA : **M**ail **T**ransfert **A**gent

MUA : **M**ail **U**ser **A**gent

MX : **M**ail e**X**changer

NS *:* Name Server

OSI : Open Systems Interconnection

PHP : **P**ersonal **H**ome **P**ages

PTR : PoinTeuR.

POP3 : **P**ost **O**ffice **P**rotocol version 3

SASL : **P**imple **A**uthentication and **S**ecurity **L**ayer

SMTP : **S**imple **M**ail **T**ransfer **P**rotocol

SOA : Start Of Authority

SOAP : **S**imple **O**bject **A**ccess **P**rotocol

SSH : **S**ecure **S**hell

TCP : **T**ransmission **C**ontrol **P**rotocol

TLS : **T**ransport **L**ayer **S**ecurity

WAN : **W**ide **A**rea **N**etwork

Sommaire

Table des matières

Chapitre IV : Réalisation & administration

Liste des tableaux

Table des figures

Introduction Générale

Il ne fait désormais plus aucun doute que les technologies de l'information et de la communication représentent la révolution la plus importante et la plus innovante qui a marqué la vie de l'humanité en ce siècle passé. En effet, elles viennent nous apporter de multiples conforts à notre mode de vie en révolutionnant le travail des individus par leur capacité de traitement d'information, d'une part, et de rapprochement des distances d'une autre.

Parmi ces technologies, la messagerie électronique qui est assez développée dans les organisations aux cours de ces quinze dernières années, grâce à sa facilité d'utilisation et son utilité perçue.C'est un service gratuit qui constitue un moyen de communication privilégié entre des personnes à travers un réseau informatique. Utilisé pour des applications très variées personnelles, professionnelles, associatives, politiques, etc., celui-ci occupe une place de plus en plus prépondérante par rapport aux moyens de communication traditionnels.

Outre son faible coût, la messagerie électronique a l'avantage d'optimiser la communication et la diffusion d'informations ce qui la rend indispensable au sein d'une entreprise, néaumoins la dépendance du réseau internet touche a la disponibilité de ce service ainsi qu'à sa sécurité. Ainsi une mise en place d'un serveur de messagerie stable, disponible et sécurisé s'impose.

Dans ce contexte, nous allons indiquer comment un système de messagerie interne, de par sa mise en place et sa sécurisation pourrait répondre aux besoins en termes de technologies de l'information et de la communication d'une entreprise.

Ce rapport est composé de quatres chapitres ;

Le premier porte sur les concepts fondamentaux de la mise en place d'un serveur de messagerie électronique ainsi que ses composants et les différentes manières d'assurer leur sécurité.

Le second concerne la présentation du cadre du stage ainsi qu'un cahier de charge regroupant les besoins de l'entreprise et les suggestions que nous leur avons proposé.

Le troisième chapitre consiste en une étude comparative de tous les moyens existants et ceux que nous avons choisi de mettre en œuvre.

Enfin, nous terminons par la réalisation de serveur de méssagerie électronique de manière explicite et détaillée. Une conclusion générale accompagnée de perspectives viennent terminer ce travail.

- **Introduction :**

Dans ce chapitre nous allons présenter les concepts fondamentaux de la mise en place d'un serveur de messagerie électronique, nous allons d'abord définir certains concepts des réseaux informatiques, ensuite nous allons définir et expliquer le fonctionnement de la messagerie electronique ainsi que ses composants et enfin nous expliquerons les différentes manières de sécuriser un serveur mail.

1. Les réseaux informatiques :

Un réseau informatique est un ensemble de machines reliées entre elles, échangeant des informations sous forme de données numériques [1].

Un réseau informatique peut servir à plusieurs buts :

- Le partage de ressources (fichiers, applications, connexion à internet, etc.)
- La communication entre utilisateurs (courrier électronique, messagerie instantanée).
- La communication entre processus (entre stations industrielles).

Il existe trois types de réseaux à distinguer, selon leur :

-taille :en terme de nombre de machines.

-vitesse de transfert des données.

-étendue : en terme de distance.

1.1. LAN (Local Area Network) :

Un LAN est un ensemble de nœuds appartenant à une même organisation et reliés entre eux ; il se distingue des MAN et des WAN par son aire géographique plus limitée, sa taille qui peut atteindre jusqu'à 100 voire 1000 utilisateurs ainsi que sa vitesse de transfert de données qui varie entre 10Mbits/s et 1Gbits/s [2].

En élargissant le contexte de la définition aux services qu'apportent le réseau local, il est possible de distinguer deux modes de fonctionnement :

- dans un environnement d'**"égal à égal"** (peer to peer), dans lequel il n'y a pas de machine centrale ainsi chacun des noeuds a un rôle similaire qui est à la fois celui de serveur et de client et chacun est libre de partager ses ressources.

- dans un environnement **"client/serveur"**, dans lequel deux types de machines sont interconnectées au réseau. Le serveur assure la gestion des données partagées entre les utilisateurs. Le client gère l'interface graphique de la station de travail personnelle.

1.2. Le réseau internet :

L'internet est l'interconnexion de différents réseaux, il permet le partage d'informations d'une manière facile et fiable en utilisant des protocoles de routage et de contrôle. Il offre plusieurs services dont : le world wide web, le courrier electronique, la messagerie instantanée, la téléphonie sur IP…etc [3].

1.3. Le réseau intranet :

L'intranet est un réseau informatique local c'est-à-dire utilisé uniquement à l'intérieur d'une entreprise ou d'une organisation quelconque. Ce réseau local utilise les mêmes technologies de communication que le réseau internet.Il s'appuie sur l'architecture client-serveur, tout comme lors de l'utilisation d'un navigateur internet , le client envoie la requête au serveur qui, à son tour, va renvoyer une réponse au client [4].

2. Serveur de messagerie :

Un serveur de messagerie a pour vocation de recevoir et d'envoyer le courrier électronique à travers le réseau. Un utilisateur n'est jamais en contact direct avec ce serveur, il utilise soit logiciels de messagerie, soit un webmail, qui se charge de contacter le serveur pour envoyer ou recevoir les messages via l'internet [5].

3. Le courrier électronique :

Le courrier électronique est un service de transmission de messages via un réseau informatique dans la boîte aux lettres électronique d'un ou plusieurs destinataires choisis par l'émetteur [6].

Pour émettre et recevoir des messages par courrier électronique, il faut disposer d'une adresse électronique et d'un client de messagerie ou d'un webmail permettant l'accès aux messages via un navigateur web.

4. Adresse electronique :

Une adresse électronique, adresse e-mail ou adresse courriel est une chaîne de caractères, permet l'acheminement du courrier électronique dans une boîte aux lettres informatique [7].

Elle est composée de :

- une partie locale, identifiant une personne ou un nom de service ;
- le caractère séparateur @ (arobase), signifiant at (« à » ou « chez ») en anglais ;
- l'adresse du serveur, généralement un nom de domaine identifiant l'entreprise hébergeant la boîte électronique.

5. Client de messagerie :

Un client de messagerie est un logiciel qui sert à lire et envoyer des courriers électroniques, La notion de client s'entend dans une architecture client-serveur.

il existe deux types de clients :

- **Client lourd** :est un logiciel qui propose des fonctionnalités complexes avec un traitement autonome. Contrairement au client léger, le client lourd ne dépend du serveur que pour l'échange des données dont il prend généralement en charge l'intégralité du traitement [8].
- **Client léger**: appelé aussi webmail, est un client de messagerie qui s'exécute sur un serveur web. Il sert d'interface entre un serveur de messagerie et un navigateur web. Contrairement au client lourd qui permet les mêmes opérations à partir d'un logiciel installé localement sur un ordinateur personnel [8].

6. Structure d'un message électronique :

La structure explicite d'un courrier électronique, celle que tout un chacun peut observer dans son logiciel de messagerie électronique, se présente selon deux parties distinctes : un en-tête et un corps [9].

6.1. Les champs d'en-tête :

Voici la signification des champs à remplir lorsque vous envoyez un mail :

- **From :** contient l'adresse mail de l'expéditeur.
- **To** : une partie de l'en-tête qui contient les adresses de tous les destinataires.
- **CC (Carbon Copies) :** cela permet d'envoyer un mail à de nombreuses personnes en écrivant leurs adresses respectives séparées par des virgules.
- **Subject :** sujet du message.
- **Date :** date et heure d'envoi du message.
- **Replay-To :** pour spécifier l'adresse à laquelle les réponses doivent être expédiées.
- **Message-ID :** identifiant unique du message.
- **Received :** ce champ permet de retracer le chemin emprunté par le message, car tous les hôtes par lesquels le message transite ajoute ce champ à l'en-tête ; sur ce dernier on trouve les caractères suivants : l'identifiant du site, un identificateur du message, le moment de la réception du message, le site de provenance du message ainsi que le nom du logiciel de transport utilisé.

6.2. Le corps du message :

est le contenu du message proprement dit, séparé de l'en-tête par une ligne vide.

7. Avantages et inconvénients du courrier électronique :

Le courrier électronique possède de nombreux avantages qui sont :

-Rapidité, asynchrone, gestion de listes de messagerie, gestion de boîtes aux lettres et économie.

Sa facilité d'utilisation a engendré son plus grand inconvénient qui est :

- Utilisation à tort et à travers et surcharge des boîtes aux lettres par des messages publicitaires et indésirables.Il est donc impératif de vider régulièrement sa boîte aux lettres car elle utilise des ressources de stockage (disque) sur le serveur et souvent des quotas sont attribués.

8. Protocoles de communication (de transport) :

Il y a lieu de distinguer deux types de protocoles, des protocoles d'envoi et des protocoles de réception.

8.1. Protocoles d'émission des messages :

Le protocole SMTP (Simple Mail Transfer Protocol) est le protocole standard permettant de transférer le courrier d'un serveur à un autre en connexion point à point. Le courriel est remis directement au serveur de courriel du destinataire. Les MTAs communiquent entre eux en utilisant SMTP [6].

8.2. Protocoles de réception des messages :

Dans ce qui suit, nous allons présenter les caractéristiques de chacun des protocoles POP (Post Office Protocol) et IMAP (Internet Message Access Protocol) et nous allons les comparer.

- **POP :**Le protocole POP télécharge le courrier électronique depuis le serveur et le rapatrie chez le client (C'est-à-dire sur l'ordinateur personnel de l'utilisateur).

  De cette manière, après le téléchargement de son courriel, un utilisateur peut le lire hors connexion. Par défaut, POP efface du serveur les courriels téléchargés, sauf en cas d'indication contraire du client [6].

- **IMAP :**C'est un protocole alternatif à POP, et offrant plus de fonctionnalités.

  Sur un serveur IMAP, les messages restent toujours sur le serveur de courrier même après leur téléchargement et ne sont pas enregistrés chez le client. Seuls les en-têtes des courriels sont téléchargés en local, et les messages ne sont téléchargés qu'a à la demande de l'utilisateur [6].

- **POP et IMAP :** Le protocole POP correspond à un utilisateur qui consulte son courriel à partir d'un seul poste. Et ce contrairement à IMAP, où l'utilisateur est mobile et IMAP lui permet de consulter son courriel à partir de n'importe quel poste [6].

9. Architecture logicielle de la messagerie :

Il y a trois types d'intervenant dans le courrier électronique:

9.1. Le Mail User Agent (MUA) :

Le MUA est un programme qui sert à lire, écrire, répondre et recevoir des messages. Il présente une interface graphique riche à la disposition de l'utilisateur, il compose un courriel et l'envoie à un MTA.

Un MUA a des méthodes pour accéder à une boite de réception tels que les protocoles POP et IMAP [13].

9.2. Le Mail Transfer Agent (MTA) :

Un MTA est un programme utilisé pour acheminer un courrier d'un hôte vers un autre hôte, que ce soit en local ou sur des machines distantes.

Un MTA reçoit par le protocole SMTP, les emails envoyés par des clients de messagerie électronique (MUA). Son rôle est de redistribuer ces courriers à des Mail Delivery Agent (MDA) et d'autres MTA [13].

9.3. Le Mail Delivery Agent (MDA) :

Un Mail Delivery Agent marque la fin de l'acheminement du mail vers la destination. C'est le MDA qui reçoit le message du MTA et se charge de le placer dans la boite aux lettres de l'utilisateur, il doit donc gérer les éventuels problèmes tel qu'un disque plein ou une boite aux lettres corrompue et doit impérativement signaler au MTA toute erreur de délivrance.

Un MDA assure également des fonctions utilisateurs telles que la réponse automatique quand la personne est indisponible [13].

10. Fonctionnement de la messagerie électronique :

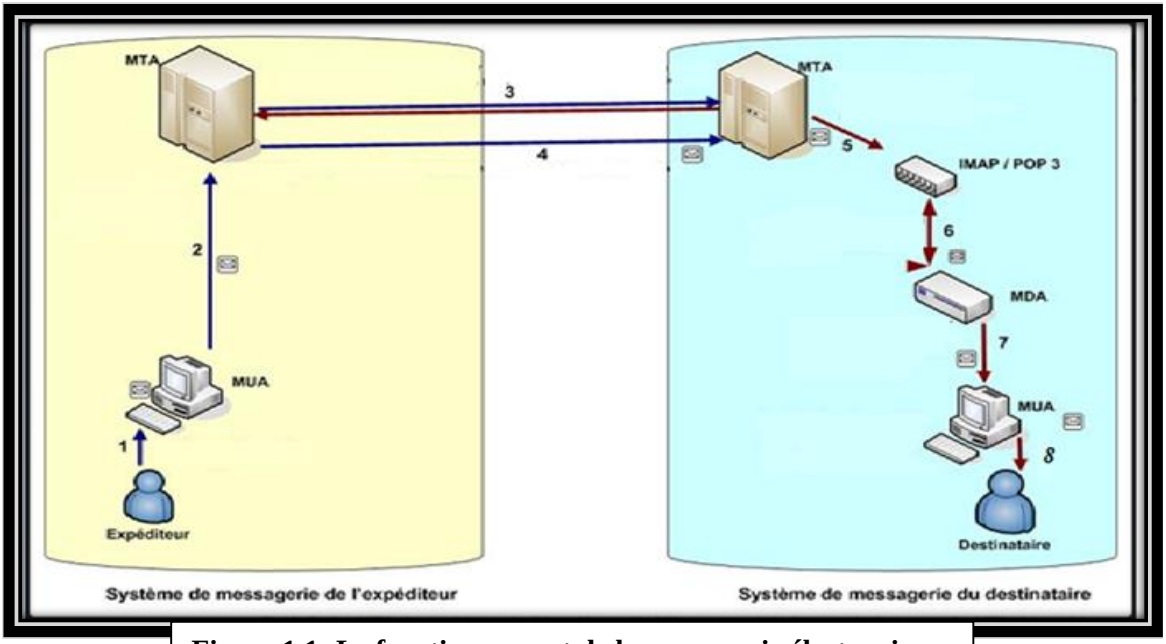

Figure 1.1: Le fonctionnement de la messagerie électronique

Ce schéma présente le transfert d'un courriel d'un expéditeur à un destinataire.

1. L'expéditeur saisit et valide l'envoi de son courrier.
2. Le MUA transmet le courriel au MTA.
3. Le MTA du système de l'émetteur établit un canal de transmission avec le MTA du système du destinataire, par émissions successives de requêtes bidirectionnelles.
4. Une fois le canal établit, le courriel est transmis d'un système à un autre par les MTAs.
5. Dans le système du destinataire, le MTA transmet le courrier reçu au serveur IMAP ou POP.
6. Le MDA récupère le courriel sur le serveur IMAP /POP3, par émissions successives de requêtes.
7. Le MDA récupère le courriel du serveur IMAP/POP3, par émissions successives de requêtes. Et le met à disposition du MUA.
8. Le MUA dépose le courriel dans la boîte aux lettres du destinataire qui pourra le consulter à tout moment.

11. Serveur DNS (Domain Name Server) :

Le système de noms de domaine est un service permettant de traduire un nom de domaine en informations de type adresse IP de la machine portant ce nom.

Le service de résolution de nom d'hôte DNS, permet d'adresser un hôte par un nom, plutôt que de l'adresser par une adresse IP [11].

11.1. Domaine :

Un nom de domaine est un identifiant de domaine internet. C'est est un sous arbre de l'espace de nommage, il peut être organisé en sous domaine, par exemple : .univ.com est un sous domaine du domaine .com .

11.2. Zone:

Une zone est une organisation logique (organisation administrative) des domaines. Son rôle est de simplifier l'administration des domaines. Un domaine peut être découpé en plusieurs zones, Z1.com, Z2.com …etc.

11.3. Délégation :

La délégation consiste à déléguer ou décentraliser l'administration d'une partie de l'espace de nommage d'un domaine.

11.4. Résolution DNS :

- **La résolution directe :** Le principe de la résolution de noms, consiste à affecter un nom d'hôte à une adresse IP. On parle de résolution de noms directe.
- **La résolution inverse :** Le processus inverse doit pouvoir également être mis en œuvre. On parle de résolution de noms inverse ou reverse.

  Le processus doit fournir, pour une adresse IP, le nom correspondant. Pour cela il y a une zone particulière, in-addr.arpa, qui permet la résolution inverse d'adresse IP.

11.5. Principaux types d'enregistrements :

Les types d'enregistrements qui enrichissent une base de données DNS sont de plusieurs types [12].

Donc voici les principaux :

- **Enregistrement de type SOA (*Start Of Authority*) :** indique l'autorité sur la zone. Ces enregistrements contiennent toutes les informations sur le domaine. Par exemple le délai de mise à jour des bases de données entre serveurs de noms primaires et secondaires, le nom du responsable du site.
- **Enregistrements de type NS (*Name Server*) :** ces enregistrements donnent les adresses des serveurs de noms pour le domaine.
- **Enregistrement de type A (*Adresse*) :** ces enregistrements permettent de définir les nœuds fixes du réseau (ceux qui ont des adresses IP statiques). Serveurs, routeurs, switchs ...
- **Enregistrements de type MX (*Mail eXchanger*) :** ils servent pour déclarer les serveurs de messagerie.
- **Enregistrements de type CNAME (*Canonical Name*) :** ils permettent de définir des alias sur des noeuds existants et de différencier le nommage des machines des standards de nommages des services (www, ftp, news, smtp, mail, pop...).
- **Enregistrement de type PTR (Pointeur) :** ils permettent la résolution de noms inverse dans le domaine in-addr.arpa.

11.6. Serveur primaire et serveur secondaire:

Le serveur maître ou primaire dispose d'un fichier d'information sur la zone. Le ou les serveurs esclaves (secondaires) obtiennent des informations à partir d'un serveur primaire ou d'un autre serveur esclave. Les serveurs maîtres et esclaves ont autorité sur la zone.

12.Le serveur DHCP :

Dynamic Host Configuration Protocol (DHCP) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut, des serveurs de noms DNS [13].

Pour qu'un serveur DHCP puisse servir des adresses IP, il est nécessaire de lui donner un « réservoir » d'adresses dans lequel il pourra puiser : c'est la plage d'adresses (address range). Il est possible de définir plusieurs plages, disjointes ou contiguës.

Les adresses du segment qui ne figurent dans aucune plage mise à la disposition du serveur DHCP ne seront en aucun cas distribuées, et peuvent faire l'objet d'affectations statiques (couramment : pour les serveurs nécessitant une adresse IP fixe, les routeurs, les imprimantes réseau…). Il est également possible d'exclure pour un usage en adressage statique par exemple, des adresses ou blocs d'adresses compris dans une plage [14].

13. La sécurité informatique:

13.1. Les protocoles de sécurité :

13.1.1. Définition du protocole TLS :

Un usage courant de la cryptographie par clé publique est le chiffrement du trafic réseau d'une application en utilisant TLS (Transport Layer Security). TLS est un protocole de cryptage qui garantit pleinement la sécurité des communications pour tous les mails échangés. Ce système est utilisé pour garantir la sécurité des communications sur un réseau internet ou intranet. Il est positionné entre les couches application et transport du modèle TCP/IP et dans la couche session du modèle OSI. TLS se comporte en effet comme une couche intermediaire supplémentaire car il est indépendant du protocole utilisé au niveau application donc TLS est transparent pour l'utilisateur [15].

13.1.2. Objectifs et moyens mis en œuvre :

TLS propose les fonctionnalités suivantes :

- **Authentification**

  Le client doit pouvoir s'assurer de l'identité du serveur et le serveur peut aussi demander au client de s'authentifier. Cette fonctionnalité est assurée par l'emploi de certificats.

- **Confidentialité**

  Le client et le serveur doivent avoir l'assurance que leur conversation ne puisse pas être écoutée par un tiers. Cette fonctionnalité est assurée par un algorithme de chiffrement.

- **Identification et intégrité**

  Le client et le serveur doivent pouvoir s'assurer que les messages transmis ne sont ni tronqués ni modifiés (intégrité), qu'ils proviennent bien de l'expéditeur attendu. Ces fonctionnalités sont assurées par la signature des données.

TLS repose donc sur la combinaison de plusieurs concepts cryptographiques, exploitant à la fois le chiffrement asymétrique et le chiffrement symétrique.

13.1.3. Fonctionnement :

Le protocole est composé de deux niveaux: TLS Handshake Protocol et TLS Record Protocol [16].

- **TLS Handshake Protocol *:*** Ce protocole a pour objectif de réaliser l'authentification par l'échange de certificats et permet la négociation entre le client et le serveur d'un niveau de sécurité au travers du choix d'un algorithme de cryptage. C'est le protocole de configuration de la transaction.

- **TLS Record Protocol :** Encapsule les données. C'est le protocole de transmission des données.

- **Un certificat numérique**: Un certificat permet de distribuer une clé publique et d'autres informations à propos d'un serveur et de l'organisation responsable de ce serveur**.** Les certificats peuvent être signés numériquement par une autorité de certification (Certification Authority) ou créer son propre certificat auto-signé.

- **Certificats X.509** : Le modéle de certificats X.509 permet d'ajouter l'identité à la clé. Le modéle X.509 est en fait un ensemble de champs, qu'ils soient obligatoires ou optionnels.

13.2. La Zone démilitarisée (DMZ):

Une DMZ c'est une zone démilitarisée située derrière un parefeu où l'on place des serveurs devant être accessible de plusieurs réseaux. Cette zone cloisonnée, isolée sert de tampon entre le réseau à protéger (interne) et le réseau hostile (internet) [17].

-**DMZ publique :** C'est une zone accessible depuis l'extérieur (internet) et l'intérieur (réseau interne entreprise).

-**DMZ privée :** Uniquement accessible par le réseau interne.

- **Conclusion**

Dans ce chapitre, nous avons présenté les différents concepts appelés à être utilisés dans notre travail ; définition des réseaux, le courrier electronique, son fonctionnement ainsi que ses composants. Nous avons mis l'accent sur le rôle indispensable du serveur DNS, où nous avons mentionné ses différentes fonctions, ses types d'enregistrement et la résolution DNS. Nous avons défini également le serveur DHCP. Enfin, nous avons présenté certaines techniques qui permettent de sécuriser un réseau interne.
Dans le chapitre suivant,nous présenterons l'organisme d'accueil ainsi qu'une analyse de ses besoins.

- **Introduction**

Dans ce chapitre nous allons présenter notre organisme d'accueil: l'Entreprise Portuaire de Béjaia,ses missions ainsi que son organisation. Nous nous intéresserons plus précisément au centre informatique de l'EPB,à ses services, applications, sa gestion du système d'information ainsi que sa méthode de sécurité. Nous allons également présenter un cahier de chargeoù nous expliquons de façon détaillée notre projet.

1. Présentation générale de l'organisme d'accueil:

Le port de Bejaia joue un role très important dans les transactions internationals vu sa place et sa position géographique. Aujourd'hui, il est classé premier port d'Algérie en marchandises générales et troisième port pétrolier. Il est également le premier port du basin méditerranéen certifié ISO 9001 /2000 pour l'ensemble de ses prestations et à avoir ainsi installé un système de management de qualité. Cela constitue une étape dans le processus d'amélioration continue de ses prestations au grand benefice de ses clients, l'EPB a connu d'autres succès depuis, elle est notamment certifiée à la norme 14001 /2004 et au réféentiel OHSAS 18001 /2007, respectivement pour l'environnement et l'hygiène et sécurité au travail.

L'entreprise portuaire de Béjaia se charge éssentiellement de la gestion, l'exploitation et le développement du domaine portuaire, dans le but de promouvoir les échanges éxtérieurs du pays ceci en garantissant :

- Un traitement de l'ensemble des passagers, machandises et navires dans les meilleures conditions de délais, de coût et de sécurité. La gestion et l'exploitation des infrastructures et des superstructures portuaires.

- La manutention et l'acconage des marchandises en transit par le port de Béjaia.

- Mise à disposition d'infrastructures nécessaires aux activités relatives aux hydrocarbures (exportation pétrole et de cabotage national des profuits raffinés et gaz de pétrole liquéfié).

- Le pilotage, le remorquage et lamanage des navires dans les limites de la zone de pilotage dans le port de Béjaia.

Les différentes structures de l'EPB sont présentées dans l'organigramme ci-dessous :

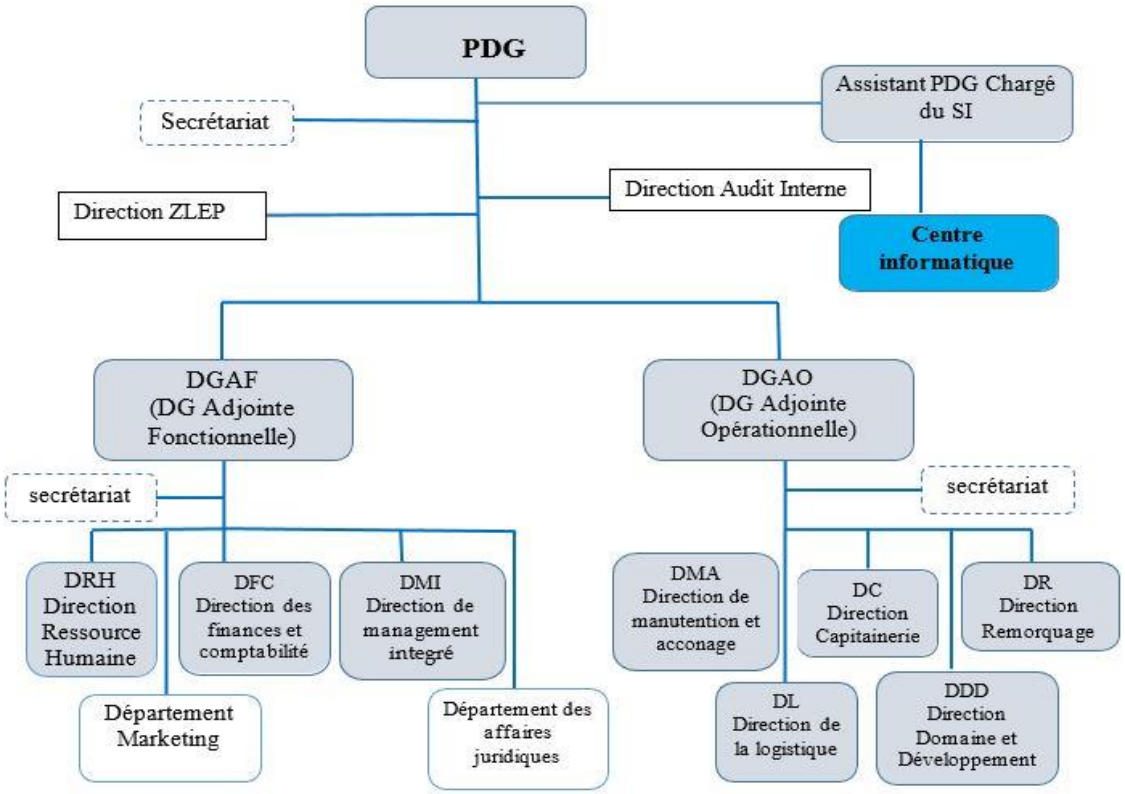

Figure 2.1: Organigramme général de l'EPB

2. Présentation du centre système d'information de l'EPB:

Le centre système d'informations est une structure de l'EPB rattachée directement à la direction générale, elle a pour mission l'automatisation des métiers de l'entreprise , cela en mettant en place les logiciels et l'infrastructure nécessaires pour la gestion du système d'information.

L'EPB déploie des systèmes d'informations pour:

- accroitre la productivité.
- automatiser les processus métiers.
- fournir un meilleur service aux clients.

Ces systèmes intègrent de plus en plus de fonctionnalités réseau pour relier tous les utilistaeurs à l'entreprise ou établir des liens avec la clientèle et les fournisseurs. Le réseau local de l'entreprise apporte aujourd'hui une réelle valeur ajoutée en permettant d'intégrer de nouveaux partenaires, fournisseurs et clients.

Le centre système d'information de l'EPB se compose de trois départements sous la coupe de l'assistant du PDG chargé du SI, chaque département est structuréen services comme le montre l'organigramme suivant:

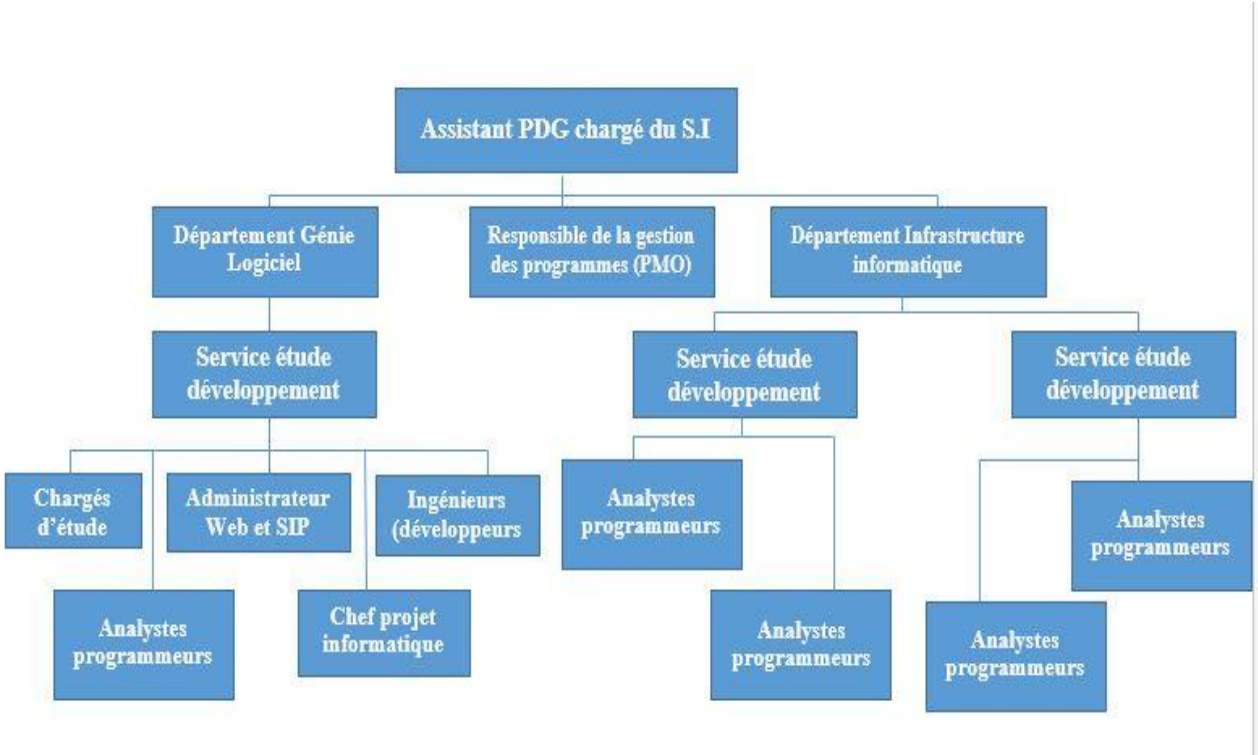

Figure 2.2 : Organigramme du centre sysème d'information de l'EPB

3. Le réseau local actuel de l'EPB :

Le réseau local de l'EPB permet aux différents postes de travail de s'échanger des informations, de se connecter vers l'extérieur et d'utiliser les applications hébergées en interne, nécéssaires à l'exécution des tâches quotidiennes des employés.

L'architecture du réseau local de l'entreprise est représentée dans la figure suivante:

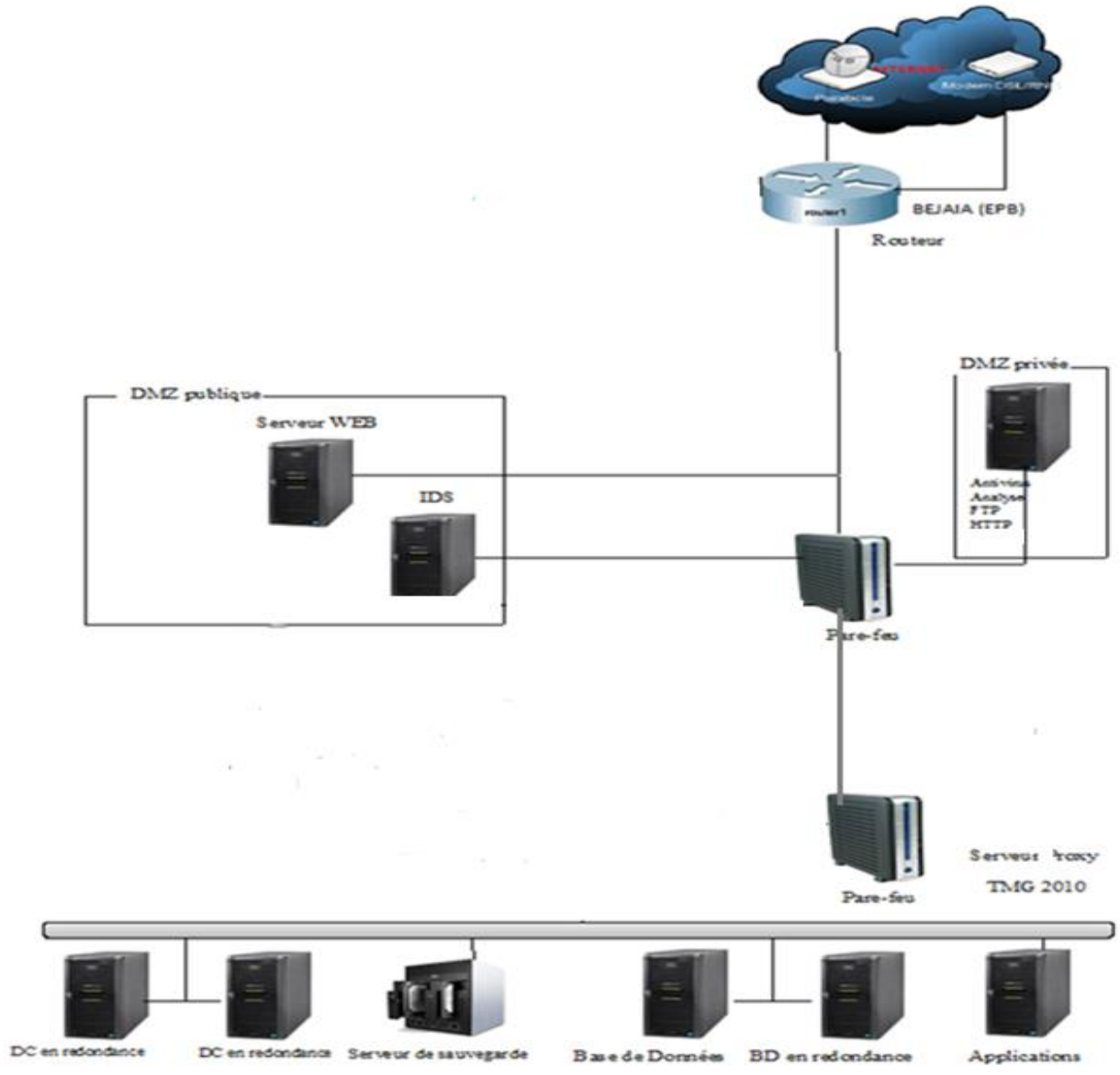

Figure 2.3 : Architecture actuelle du réseau local de l'EPB

4. Les applications et les matériaux utilisés à l'EPB :

L'EPB dispose de 180 PC répartis à travers les différentes directions de l'entreprise et interconnecté à un réseau informatique constitué de fibre optiques et de câbles à paires torsadés.

- Les systèmes d'exploitation utilisés sur les postes de travail sont Windows et Linux sous différentes distributions.
- La majorité des PC est reliée à des imprimantes de plusieurs types (matricielle, laser et à jet d'encre couleur).
- Chaque ordinateur est branché à un onduleur APC ou MGE de 400 à 1000 VA.
- Tous les PC sont dotés d'un anti-virus KASPERSKY 10 end point .
- Tous les PC sont connectés à Internet.

-Deux contrôleurs de domaines DC1 et DC2 sous Windows Server 2012 et également serveur DNS en plus de l'infrastructure de clés publiques PKI hébergées dans DC1, DC2 hébergera un serveur DHCP et aussi un serveur WDS (Windows Deployment Services).
-Deux serveurs de bases de données en redondance sous Windows Server 2008.
-Un serveur de sauvegarde en réseau NAS intégrant le système RAID.
-Un serveur d'Application
-Un serveur de méssagerie externe Microsoft Outlook.
-un réseau Wimax composé de deux connexion internet (Algerie Télécom, Icosnet), elles sont reliées directement à un pare-feu OPNsense configuré afin de garantir la haute disponibilité des dispositifs de sécurité et un contrôle total du flux entrant et flux sortant, à partir de là trois connexions sont établies:

- la première vers la zone tampon DMZ privée
- la seconde vers la zone tampon DMZ publique (serveur web, serveur IDS).

5. Cahier de charge:

5.1. Présentation du sujet:

L'entreprise portuaire de Béjaia inclue un grand réseau, ce qui se traduit par un nombre assez important de flux de données: informations, fichiers, documents…etc échangés au niveau interne entre le personnel.

5.2. Problématique :

L'utilisation d'un serveur de messagerie externe au niveau de l'entreprise, engendre les problèmes suivants :

- La distance, ainsi en cas de panne de connexion internet toute la correspondance devient indisponible.
- Le risque de perte de confidentialité des messages échangées, du fait d'un des membres du réseau internet par lequel transite le trafic entre le navigateur web et le serveur webmail.
- L'utilisation d'un simple logiciel navigateur web, permet d'accéder à son webmail depuis tout ordinateur connecté à internet, ce qui augmente le risque d'utiliser un ordinateur mal sécurisé et infecté d'un logiciel espion qui relève le mot de passe utilisé.
- l'exposition du réseau interne au réseau internet peut engendrer une surcharge de courrier électronique dus aux spams reçus, par conséquent une perte de données importante.

Comment donc assurer la disponibilité continue d'un serveur de méssagerie électronique fiable et sécurisé au sein du réseau interne de l'entreprise?

5.3. Objectifs :

- ✓ Rédaction et envoi très rapide à un ou plusieurs destinataires à la fois.
- ✓ Le message electronique peut etre archivé et imprimé.
- ✓ Permettre à l'administrateur de :
  - Créer, détruire des comptes utilisateurs (boites aux lettres).
  - Créer, modifier des listes de diffusion (ensemble de destinataires réunis sous une même dénomination).

- ✓ Permettre à l'utilisateur de :
  - Rédiger, expédier et consulter les messages.
  - Classer les messages dans des dossiers.
  - Répondre à un message sans avoir à retaper l'entête.
  - Utilisation de fonctions de recherches répondant à des critères : date, nom , sujet.
  - Création d'un annuaire personnel.

5.4. Suggestions:

Afin de palier aux différents problèmes cités ci-dessus, nous proposons les solutions suivantes :

- ➢ Mise en place d'un serveur de messagerie interne (Postfix, Dovecot) avec l'interface webmail Squirrelmail, qui sera propre à l'EPB.
- ➢ Faciliter l'administration du serveur de messagerie.
- ➢ Sécuriser le serveur à l'aide du protocole TLS.
- ➢ Pour plus de sécurité, le déploiement de notre serveur dans la DMZ existente dans l'entreprise.

5.5. Architecture proposée :

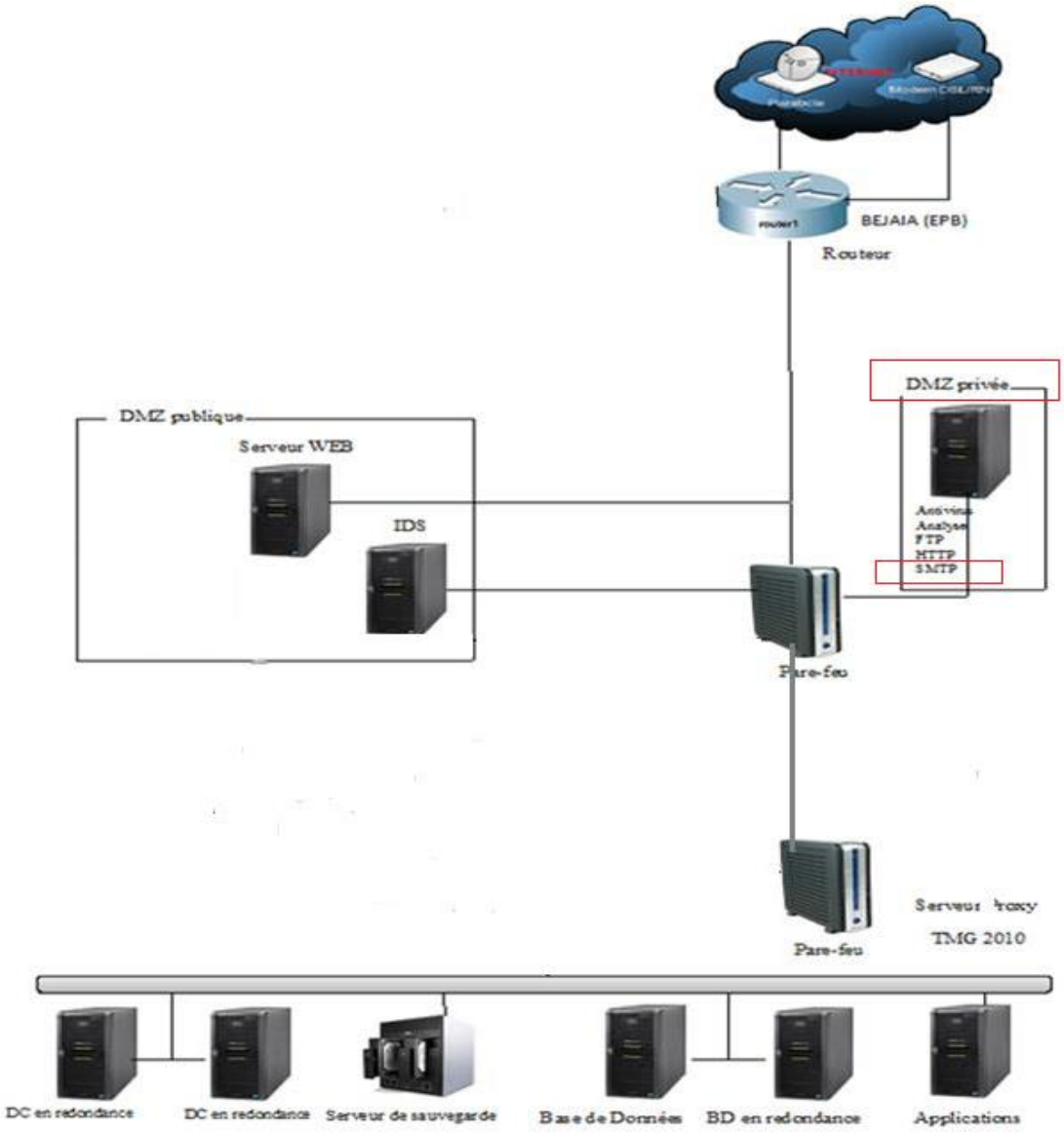

Figure 2.4 : Architecture proposée du réseau local de l'EPB

- **Conclusion**

Dans ce chapitre nous avons présenté l'organisme d'accueil, où nous avons élaboré ses différents services et spécifié leur besoins dans le cahier de charge ; ce qui engendre la nécessité de mettre en oeuvre un serveur de messagerie électronique dont les caractéristiques seront développées dans les chapitres qui suivent.

- **Introduction :**

Dans ce troisième chapitre nous allons présenter les différents outils existants de la messagerie électronique, ensuite nous ferons une étude comparative de ces outils afin de justifier les choix de notre solution.

1 .Les différents outils de la messagerie électronique :

1.1 Les serveurs de messagerie :

1.1.1 Sendmail :

Sendmail est un serveur de messagerie dont le code source est ouvert. Il se charge de la livraison des messages électroniques. C'est un programme très flexible supportant un large éventail de moyens de transfert et de livraison de courriers électroniques [17].

1.1.2 Postfix :

Postfix est un serveur de messagerie et un logiciel libre, il se charge de la livraison de courriers électroniques et a été conçu comme une alternative plus rapide, plus facile à administrer et plus sécurisée que l'historique Sendmail [17].

1.1.3 Qmail :

Qmail est un serveur de messagerie électronique pour LINUX. Il permet de mettre en place un service SMTP (Simple Mail Transfert Protocol) permettant l'envoi de courriels .

Qmail a la même utilité que Sendmail ou encore Postfix mais il possède une architecture modulaire, comportant un ensemble de commandes [17].

1.2 . Les clients de messagerie :

1.2.1 Les clients lourds :

Un client de messagerie de type lourd désigne une application cliente graphique exécutée sur le système d'exploitation de l'utilisateur. Un client lourd possède généralement des capacités de traitement évoluées et peut posséder une interface graphique sophistiquée. Néanmoins, ceci demande un effort de développement et tend à mêler la logique de présentation (l'interface graphique) avec la logique applicative (les traitements).

La mise en place d'un système de type client lourd nécessitera une installation de l'application sur chaque poste. Il faudra donc prévoir des ressources à l'arrivée de chaque nouveau collaborateur pour l'installation du logiciel sur le nouveau poste de travail.

Les applications du type client lourd sont généralement plus sécurisées si elles ne concernent que quelques utilisateurs. Il faut cependant que tous les postes qui utilisent l'application soient sécurisés car une partie des données est stockée sur les postes des différents collaborateurs. Cela peut donc multiplier les risques. Parmi ces clients lourds on peut citer :

- **Thunderbird:** C'est un client de messagerie et de messagerie instantanée, libre, distribué gratuitement par la fondation Mozilla. Le projet uniquement consacré au courrier électronique, au groupe de discussion et aux flux RSS et Atom, se veut plus léger et plus rapide que la suite Mozilla.

  Tout comme Firefox, Thunderbird est basé sur le moteur Geko et dispose d'une interface en XUL, ce qui lui permet de fonctionner sur diverses plates-formes. Il est également extensible, c'est-à-dire qu'il peut facilement recevoir de nouvelles fonctionnalités par l'ajout d'extensions [18].

- **Outlook:** est un programme de Microsoft corporation et fait partie de la suite Microsoft office. Le logiciel agit comme un client de messagerie [18].

  Plus précisément il comprend :

  -Un calendrier.

  -Un calendrier des activités.

  - Notes.

  -Journal.

  -Contacts.

1.2.2 Les clients légers ou webmail :

Un client de messagerie de type léger est un logiciel qui est installé sur un poste client. Les utilisateurs de l'application auront accès aux données par un portail sécurisé depuis leur navigateur (Internet Explorer, Firefox...).

Pour les systèmes en client léger, l'installation est beaucoup plus simple. On a tendance à penser que les applications Web sont moins sécurisées, pourtant elles permettent de réduire les risques à un seul serveur. Bien entendu, la sécurisation de celui-ci est primordiale, surtout lors d'un partage de l'application sur Internet.

On peut distinguer quelques types de clients légers :

- **MS Outlook Web Access :** est un logiciel de messagerie web créé par Microsoft. Il permet aux usagers d'accéder à leur courrier électronique à l'aide d'un navigateur web.

- **RoundCube :** est un client web mail pour le protocole IMAP écrit en PHP et JavaScript. Cette application libre est publiée sous licence GPL. Il peut être installé sur plateforme LAMP. Il est compatible avec les serveurs web Apache, Nginx, Lighttpd ou encore Cherokee, et les bases de données MySql, PostgreSQL et SQLite sont supportées. La gestion des thèmes se base sur les standards du web [15].

- **Zimbra :** est un logiciel serveur collaboratif qui permet à ses utilisateurs de stocker, organiser et partager rendez-vous, contacts, courriels, liens, documents et plus. Zimbra est un logiciel développé sur un mode "Web service" : Son interface entièrement en AJAX est chargée à la première connexion, puis les interactions et ajouts/modifications d'informations sont envoyés au serveur par le protocole SOAP. Zimbra propose aussi un logiciel client utilisable en mode déconnecté : le Yahoo! Zimbra Desktop [16].
- **Squirrelmail :** Squirrelmail est une application qui permet de consulter son courrier électronique, stocké sur un serveur, grâce à un simple navigateur, développé par Luke et Nathan Ehresman, écrit en php4. Il supporte les protocoles IMAP et SMTP, et toutes les pages créées le sont en pur HTML (sans aucun JavaScript), ceci afin d'être compatible avec le maximum de navigateurs. Son objectif est de fournir une compatibilité optimale pour se rendre aussi accessible que possible [16]

2 Etude comparative des serveurs messagerie existants :

Serveurs mail	Système d'exploitation			Fonctionnalités						
/	Linux/Unix	Windows	Mac OS X	Smtp	Pop3	Imap	Smtp sur TLs	Pop sur TLs	SSL	Webmail
Sendmail	✓	✗	✓	✓	✗	✗	✓	✗		✗
Postfix	✓	✗	✓	✓	✗	✗	✓	✗	✓	✗
Qmail	✓	✗	✓	✓	✓	✗	✓	✗	✓	✗

Tableau 1 : Tableau comparatif des serveurs de messagerie électronique [16].

3 Etude comparative des clients de messagerie existants :

Clients mail	Système d'exploitation			Fonctionnalités						
/	Linux/ Unix	Windows	Mac OS X	Smtp	Pop3	Imap	Smtp sur TLs	Pop sur TLs	SSL	Webmail
Zimbra	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓
Roundcube	✓	✗	✓	✓	✓	✗	✓	✗	✓	✗

Tableau 2 : Tableau comparatif des clients de messagerie électronique [16].

4 Système d'exploitation :

4.1 Définition :

Le système d'exploitation est l'application la plus importante d'un ordinateur. Il permet le démarrage de l'ordinateur et est indispensable au fonctionnement de toute application présente sur l'ordinateur. Il assure donc le fonctionnement général de l'ordinateur, regroupe l'ensemble des fonctions de base permettant l'utilisation de l'ordinateur et de ses périphériques et sans lequel rien n'est possible.

Tout système d'exploitation est composé d'au moins trois éléments distincts:

- Un noyau qui gère et coordonne les différents périphériques et assure la sécurité.
- Un système de fichier qui organise le stockage des données.
- Une interface graphique pour l'utilisateur.

L'interface graphique représente la partie visible du système d'exploitation permettant l'interaction entre l'homme et la machine via par exemple le pointeur de souris, les fenêtres, le bureau, les icônes. Des contrôles graphiques sont également utilisés pour interagir avec l'utilisateur : les boutons, les menus, les barres de défilement. Cet environnement rend accessible et convivial un ordinateur.

4.2 Les différents systèmes d'exploitation :

Il existe de nombreux systèmes d'exploitation mais les principaux sont Windows et Ubuntu.

4.2.1. Windows :

C'est une gamme de systèmes d'exploitation produite par Microsoft. Depuis les années 1990, et notamment avec la sortie de Windows 95, son succès commercial pour équiper les ordinateurs personnels est tel qu'il possède un statut de quasi-monopole.

Les premières versions de Windows étaient lancées depuis dos et utilisaient le système de fichiers de DOS, ce qui a donné à Windows la réputation de n'être qu'un environnement graphique sur un noyau DOS. Cependant, Windows a immédiatement eu les fonctions d'un système d'exploitation, notamment un format d'exécutables propres, la gestion des processus en multitâches coopératifs, la gestion de mémoire virtuelle, et des pilotes pour gérer l'affichage, l'impression, le clavier, le son, etc.

On pouvait utiliser Windows avec d'autre dos que le MS-DOS de Microsoft, comme pc dos d'IBM ou DR Dos, sous réserve de passer outre les messages de dissuasion émis lors de l'installation. À partir de Windows 95, l'interface graphique est devenue commercialement associée à MS-DOS.

À partir de Windows xp, on peut considérer que le DOS a bel et bien disparu des systèmes d'exploitation grand public de Microsoft, bien qu'une émulation reste disponible.

Parallèlement au développement de Windows NT, Microsoft décida d'éditer un système d'exploitation à destination du grand public, qui reprendrait certains avantages de Windows NT tout en restant compatible avec les versions antérieures de Windows et MS-DOS.

4.2.2. Linux :

Linux est un système d'exploitation intuitif et sécurisé, idéal pour les ordinateurs de bureau, les serveurs, les netbooks et les ordinateurs portables. Dans Ubuntu le noyau s'appelle Linux. Il y a de nombreux systèmes d'exploitation libres basés sur ce noyau Linux. Ces différents systèmes s'appellent des distributions Linux car ils sont tous basés sur le noyau Linux. Ubuntu est donc une distribution GNU/Linux qui réunit stabilité et convivialité. Elle s'adresse aussi bien aux particuliers qu'aux professionnels, débutants ou confirmés qui souhaitent disposer d'un système d'exploitation libre et sécurisé. « Ubuntu » est un ancien mot africain qui signifie « Humanité » et également « Je suis ce que je suis grâce à ce que nous sommes tous ».

Il réunit :

- Le monde de l'audio et de la vidéo numérique.
- L'exploitation complète d'Internet.
- Tous les outils de graphiques pour les photos et les images.
- Une suite (un ensemble de logiciels) bureautique reconnue et compatible (open office).

En résumé nous avons choisi d'utiliser ubuntu car c'est un système libre, gratuit, fiable et simple.

Cependant il est très important de comprendre que c'est un système d'exploitation différent de Windows dans sa conception.

5. TLS par rapport aux autres solutions :

D'autres protocoles permettent d'assurer la sécurité sur le réseau. Bien qu'ils proposent des fonctionnalités concurrentes à TLS, ils sont plutôt considérés comme complémentaires.

- **SSH** : SSH est un protocole de niveau application qui propose une alternative sécurisée aux utilitaires classiques (rlogin, rsh, telnet) qui n'offrent pas de confidentialité. La possibilité d'exploiter un mécanisme de tunneling rend SSH, comme TLS compatible avec les autres protocoles de niveau application déjà existants. Tout comme TLS, SSH assure l'authentification des machines, la confidentialité et l'intégrité des données. Il assure aussi l'authentification des utilisateurs par mot de passe.

  SSH souffre de faiblesses par rapport à TLS : il n'intègre pas la notion de certificats X509 v3 et nécessite l'installation d'une application cliente spécifique (donc pas de transparence).

- **IPSec** : IPSec fournit un mécanisme de sécurisation au niveau de la couche réseau . Il est utilisé notamment pour la mise en oeuvre de réseaux privés virtuels (VPN). Les fonctionnalités d'IPSec sont l'authentification des machines, la confidentialité et l'intégrité des transactions.

  Son implémentation indissociable de la prochaine version du protocole IP, IPv6, entre en concurrence avec les fonctionnalités de confidentialité et d'intégrité de TLS.

  Elle offre en outre une sécurisation du réseau dans sa globalité et non des applications au cas par cas.Cependant, IPSec ne peut assurer l'authentification des utilisateurs, ce qui pose le problème de la fiabilité des postes individuels.

  A ce jour, donc, les fonctionnalités de sécurité d'IPSec et IPv6 sont vues comme un important complément la sécurité offerte par TLS.

Conclusion :

Dans ce chapitre nous avons cité, expliqué et comparé les différents outils de la messagerie électronique , les principaux systèmes d'exploitation ainsi que les différentes solutions de sécurisation afin du justifier nos choix pour la mise en œuvre du serveur de messagerie . Le chapitre final qui suit est consacré au coté pratique de la réalisation de notre travail .

- **Introduction**

Dans les chapitres précédents, nous avons parlé de notre projet d'une façon théorique, ce chapitre est la partie pratique de la réalisation de notre objectif. Dans ce qui suit nous citons, d'une manière explicite les étapes d'installation et configuration de notre serveur de messagerie électronique.

1. Pré-requis pour passer à la configuration des composants de notre serveur mail:

1.1. Installation et configuration du système d'exploitation:

Tout d'abord, en ce qui concerne notre système d'exploitation nous avons choisi Linux, il existe plusieurs distributions linux basées sur Debian ou Ubuntu. En effet, l'installation de programmes fonctionne différemment d'une distribution à une autre, c'est justement l'une des différences majeures qui existent entre elles.

Dans notre cas, nous avons choisi d'installer la distribution Ubuntu version 14.04. LTS de Linux.

Une fois l'épuisement de l'installation qui est assez rapide, nous passons en mode *:root* sur le terminal afin d'obtenir tous les droits de super utilisateur pour pouvoir mettre à jour, modifier et configurer le système.

1.2. Création du réseau local du serveur de messagerie « EPB » :

En premier lieu, nous créons le réseau ad-hoc car il constitue la toile qui reliera toutes les machines des utilisateurs du serveur de messagerie ainsi que le serveur lui-même afin qu'ils puissent être connectés. Nous avons choisi **l'adresse IP : 192.168.1.5** comme adresse fixe du serveur mail.

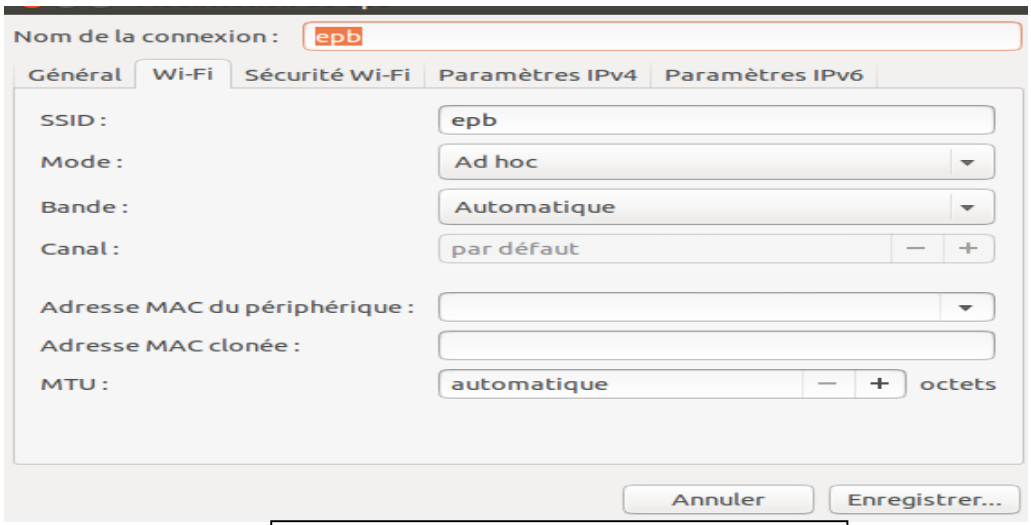

Figure 4.1 : Création du réseau « EPB »

1.3. Installation et configuration du serveur DHCP :

Nous procédons à l'installation du serveur DHCP, ce service constitue la seconde étape tout de suite après la création du réseau local car il permet de configurer automatiquement les paramètres IP des machines qui se connectent au réseau créé « EPB ».

Le principe est qu'une machine se connecte sur le réseau local et envoie une requête DHCP pour demander au serveur DHCP une adresse IP.

Installation du paquet : ***isc-dhcp-server.***

```
root@mina-LIFEBOOK-AH512: /home/mina
root@mina-LIFEBOOK-AH512:/home/mina# apt-get install isc-dhcp-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
```

Figure 4.2 : Installation du serveur DHCP

Nous passons à la configuration du serveur DHCP, afin de préciser la plage d'attribution d'adresses ainsi que l'adresse IP et le nom de domaine de notre serveur mail.

Pour accéder au fichier de configuration DHCP , on tappe la commande suivante : ***#cd /etc/dhcp*** puis ***gedit dhcpd.conf*** .

```
dhcpd.conf
#host fantasia {
#  hardware ethernet 08:00:07:26:c0:a5;
#  fixed-address fantasia.fugue.com;
#}

# You can declare a class of clients and then do address allocation
# based on that.   The example below shows a case where all clients
# in a certain class get addresses on the 10.17.224/24 subnet, and all
# other clients get addresses on the 10.0.29/24 subnet.

#class "foo" {
#  match if substring (option vendor-class-identifier, 0, 4) = "SUNW";
#}

#shared-network 224-29 {
#  subnet 10.17.224.0 netmask 255.255.255.0 {
#    option routers rtr-224.example.org;
#  }
#  subnet 10.0.29.0 netmask 255.255.255.0 {
#    option routers rtr-29.example.org;
#  }
#  pool {
#    allow members of "foo";
#    range 10.17.224.10 10.17.224.250;
#  }
#  pool {
#    deny members of "foo";
#    range 10.0.29.10 10.0.29.230;
#  }
#}
subnet 192.168.1.0 netmask 255.255.255.0{
  range 192.168.1.5  192.168.1.200;
  option domain-name-servers ns.epb.dz;
  option domain-name "epb.dz";
}
```

Figure 4.3 : Configuration du fichier *dhcpd.conf*

Chaque fois que DHCP attribue une adresse IP, il enregistre un message dans le fichier ***/var/log/syslog*** .

Nous allons maintenant le réinitialiser afin qu'il soit à jour, après les modifications apportées.

On tappe la commande suivante : ***#service isc-dhcp-server restart*** ou

 # /etc/init.d/isc-dhcp-server restart (Dans les deux cas nous obtenons le même résultat).

1.4. Installation et configuration du serveur DNS :

Maintenant que l'adresse du serveur et la plage d'adresses à attribuer aux machines ont été définies par le serveur DHCP nous devons identifier notre FQDN relatif a l'adresse du serveur et attribuer des noms automatiquement aux adresses appartenant à la plage définie précédemment, ceci grâce au serveur DNS.

Sur un serveur Unix, la liste des serveurs DNS est définie dans le fichier ***/etc/resolv.conf*** . Nous tappons la commande ***#gedit /etc/resolv.conf***.

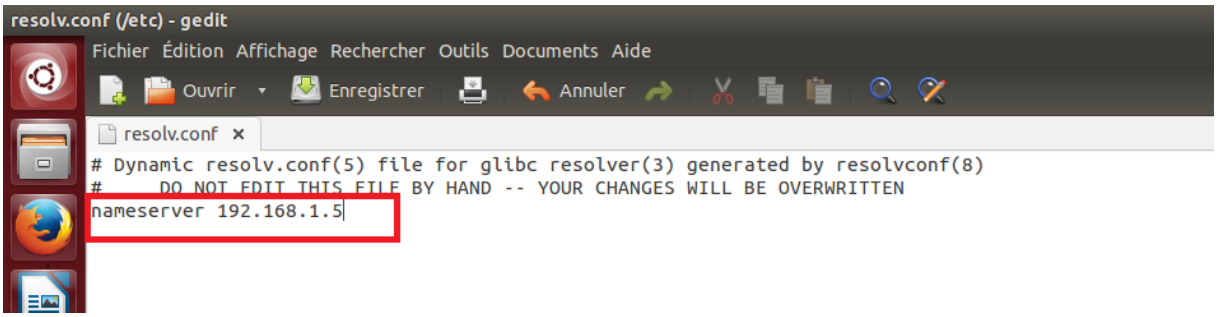

Figure 4.4 : Indication de l'adresse du serveur DNS

Nous allons maintenant identifier et configurer notre *FQDN* dans le fichier ***/etc/hostname .***
Nous tappons la commande : ***#gedit /etc/hostname*** et nous introduisons le nom de domaine : ***mail.epb.dz***.
Nous éditons également le fichier ***/etc/hosts*** avec la commande :
 # gedit /etc/hosts et nous rajoutons l'adresse IP : ***192.168.1.5***
ainsi que le nom de domaine : ***mail.epb.dz*** .

- **Installation et configuration de BIND :**

  BIND9 est un serveur qui héberge le service DNS, appelé "serveur de noms". Ubuntu est livré par défaut avec BIND (Berkley Internet Naming Daemon). BIND9 peut être utilisé de différentes manières, dans notre cas nous l'utilisons comme « Serveur Maitre » c'est-à-dire ;utilisé pour contenir les enregistrements DNS du domaine epb.dz .

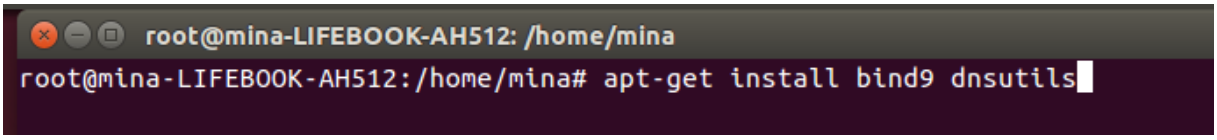

Figure 4.5 : installation de Bind9 dnsutils

Nous passons maintenant à sa configuration, nous allons définir notre zone directe ***« epb.dz »*** et inverse ***« 1.168.192.in-addr.arpa »*** dans le fichier ***named.conf.default-zones,*** après avoir copié son contenu dans un nouveau fichier nommé ***epb.zone*** avec la commande : ***#cp named.conf.default-zones epb.zone***.

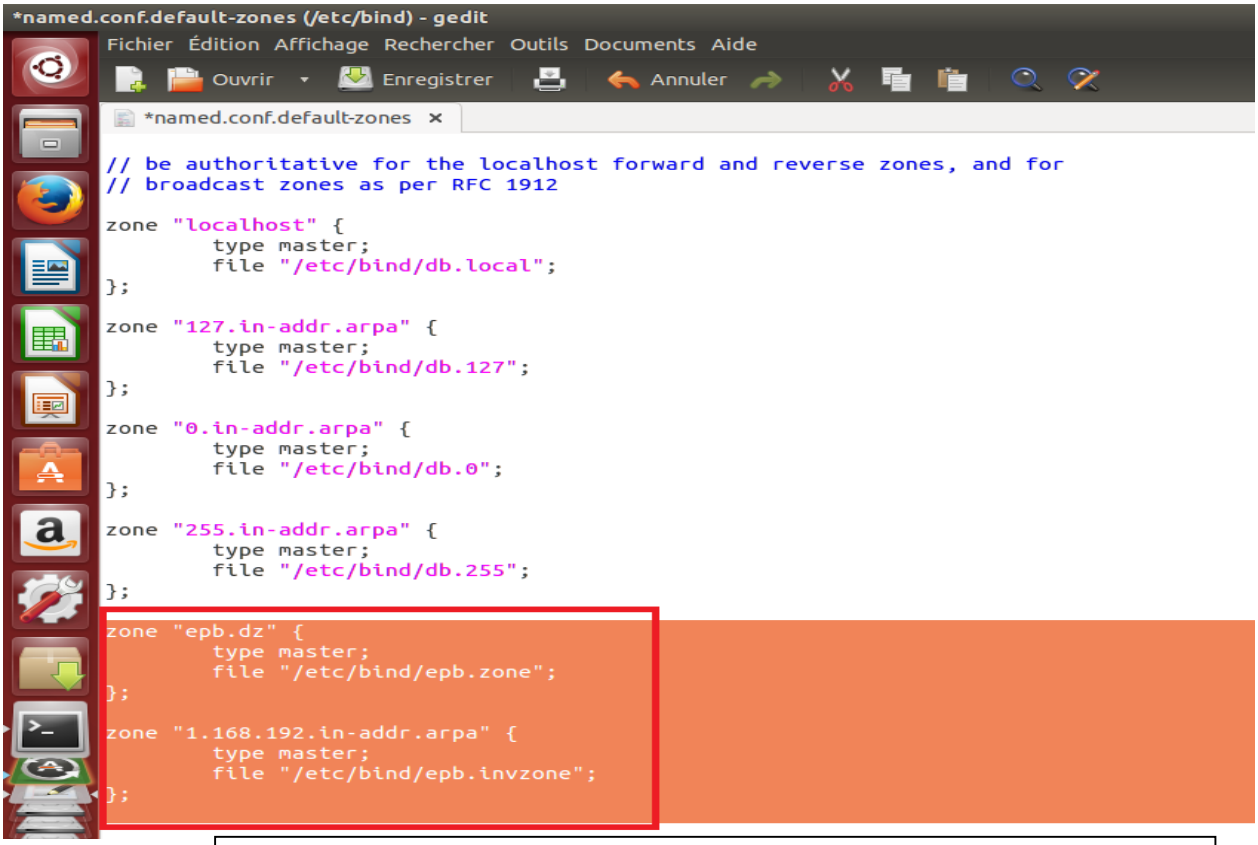

Figure 4.6 : Définition des zones *« epb.zone »* et *« 1.168.192.in-addr.arpa »*

Nous procédons maintenant à la configuration des fichiers ***epb.zone*** et ***epb.invzone*** .

epb.zone

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     epb.dz. root.epb.dz. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@             IN      NS            ns.epb.dz.
@             IN      MX 10         mail.epb.dz.
ns.epb.dz.    IN      A             192.168.1.5
mail          IN      A             192.168.1.5
www.epb.dz.   IN      CNAME         ns.epb.dz.
```

Figure 4.7 : Configuration du fichier *epb.zone*

epb.invzone

```
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     epb.dz. root.epb.dz. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.epb.dz.
6       IN      PTR     ns.epb.dz.
```

Figure 4.8 : Configuration du fichier *epb.invzone*

A présent, nous allons vérifier notre configuration des fichiers du serveur DNS à l'aide de la commande suivante : ***#named–checkconf –z named.conf.default-zones*** , si la configuration est valide nous obtenons le résultat suivant :

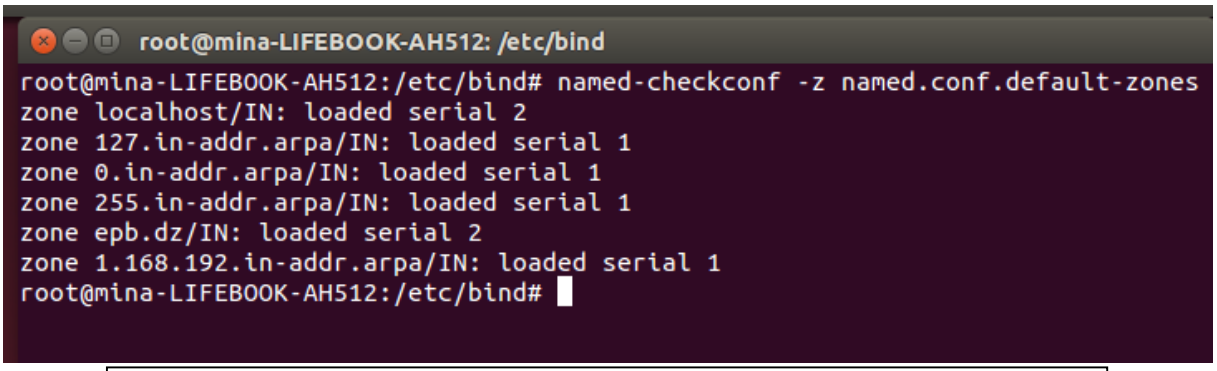

Figure 4.9 : Vérification de la configuration des fichiers du serveur DNS

Enfin, nous réinitialisons le serveur DNS en tappant la commande : ***#/etc/init.d/bind9 restart*** ou ***#service bind9 restart*** et nous testons le fonctionnement de notre serveur DNS avec la commande : ***#nslookup*** , en introduisant l'adresse IP ou notre *FQDN*.

Nous obtenons ceci :

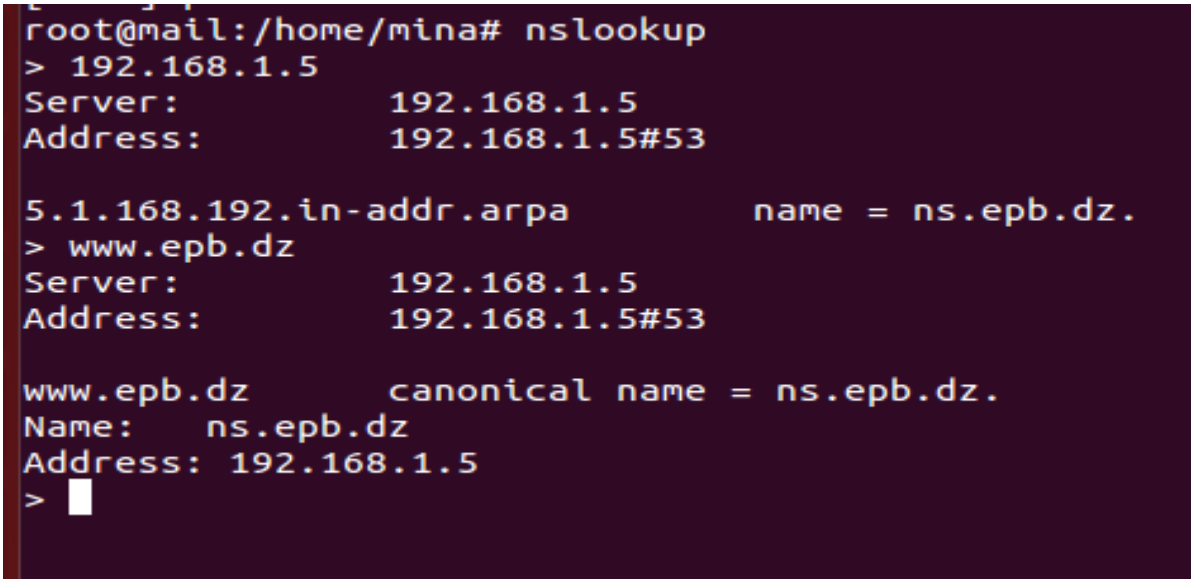

Figure 4.10 : Test du fonctionnement du serveur DNS

2. Installation et configuration des composants de notre serveur de méssagerie électronique :

2.1. Installation et configuration du MTA :

Comme nous l'avons expliqué dans le premier chapitre, le MTA constitue le premier composant à mettre en place car il permet l'envoi du courrier électronique.

Avant d'entamer l'installation, on met à jour le système comme suit : ***#apt-get update*** et puis nous installons notre MTA qui est POSTFIX par la commande : ***# apt-get install postfix*** .

Une fois le paquet installé, un menu de configuration s'affiche Parmi les choix proposés nous sélectionnons « site internet » comme illustré sur la figure ci-dessus pour utiliser le protocole SMTP.

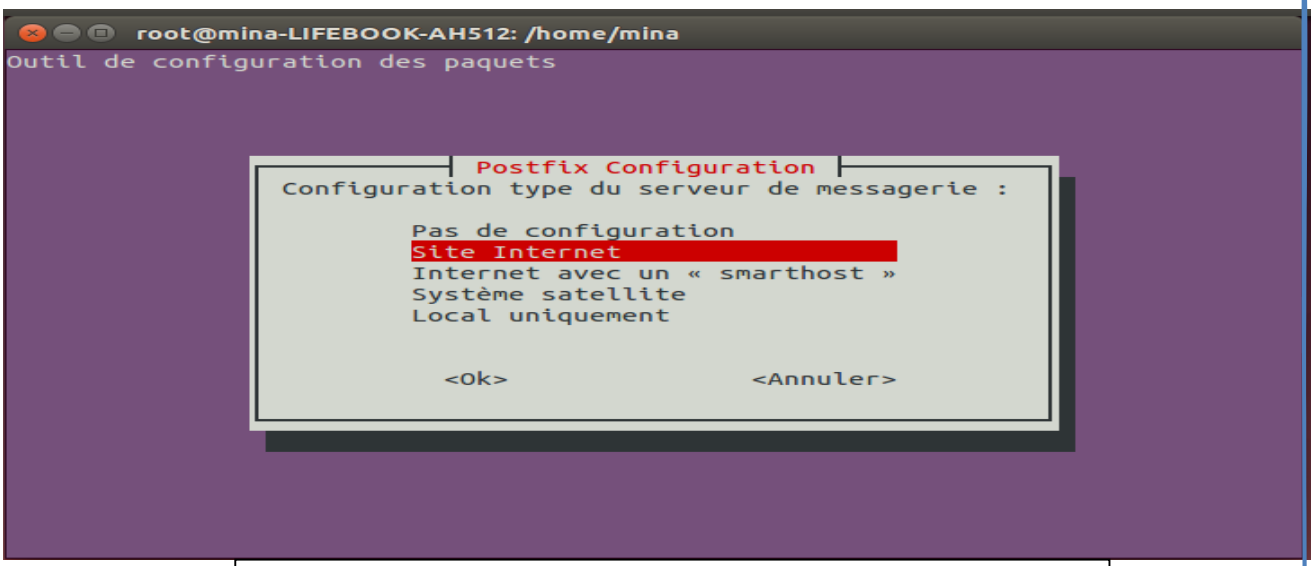

Figure 4.11 : Configuration du type de serveur de messagerie

Ensuite , nous introduisons le nom de courrier qui est notre *FQDN* comme illustré dans cette figure :

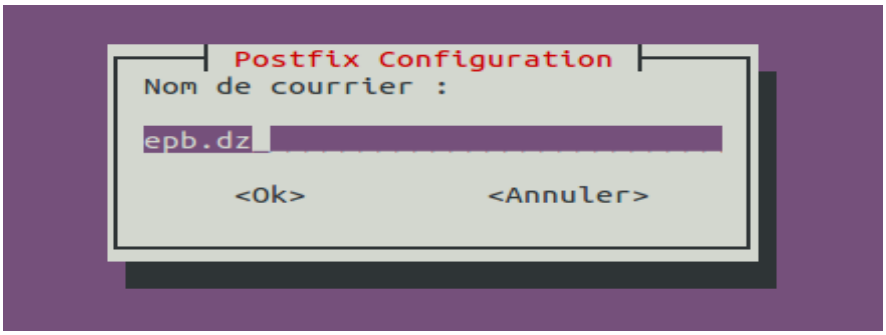

Figure 4.12 : Configuration du nom de courrier Postfix

Nous allons à présent paramétrer le fichier de configuration principal de postfix ***main.cf*** qui est sous le répertoire ***/etc/postfix/main.cf*** .

Nous ajoutons dans le fichier :

- La partie 01 qui définit les paramètres de postfix.
- La partie 02 pour configurer *SMTP -AUTH* en utilisant *Dovecot SASL*.

main.cf

```
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = mina-LIFEBOOK-AH512
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = epb.dz,localhost.localdomain, localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.1.5/24
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
```

01

```
home_mailbox = Maildir/
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_local_domain =
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_auth_enable = yes
smtpd_recipient_restrictions = permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination
smtp_tls_security_level = may
smtpd_tls_security_level = may
smtp_tls_note_starttls_offer = yes
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
```

02

Figure 4.13 : Configuration du fichier *main.cf*

- **Sécurité du serveur et ses utilisateurs:**

Avant de finaliser la configuration de notre MTA, nous procédons à la sécurisation de l'échange du courrier ainsi que celle du serveur et des utilisateurs. Nous allons générer un certificat numérique pour TLS .

➢ **Génération de la clé privée** :

```
mina@mina-LIFEBOOK-AH512:~$ openssl genrsa -des3 -out server.key 2048
Generating RSA private key, 2048 bit long modulus
.....................................................+++
.....+++
e is 65537 (0x10001)
Enter pass phrase for server.key:
3073730236:error:28069065:lib(40):UI_set_result:result too small:ui_lib.c:869:You must type in 4 to 8191 characters
Enter pass phrase for server.key:
3073730236:error:28069065:lib(40):UI_set_result:result too small:ui_lib.c:869:You must type in 4 to 8191 characters
Enter pass phrase for server.key:
3073730236:error:28069065:lib(40):UI_set_result:result too small:ui_lib.c:869:You must type in 4 to 8191 characters
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
mina@mina-LIFEBOOK-AH512:~$ openssl rsa -in server.key -out server.key.insecure
Enter pass phrase for server.key:
writing RSA key
mina@mina-LIFEBOOK-AH512:~$ mv server.key server.key.secure
mina@mina-LIFEBOOK-AH512:~$ mv server.key.insecure server.key
```

1 2 3

Figure 4.14 : Génération de la clé privée

➢ **Génération d'une demande de signature de certificat**:

```
mina@mina-LIFEBOOK-AH512:~$ openssl req -new -key server.key -out server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DZ
State or Province Name (full name) [Some-State]:Algeria
Locality Name (eg, city) []:BEJAIA
Organization Name (eg, company) [Internet Widgits Pty Ltd]:dz
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:epb.dz
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:
```

4

Figure 4.15 : génération de la demande de certificat

- **Création du certificat auto-signé :**

```
mina@mina-LIFEBOOK-AH512:~$ openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
Signature ok
subject=/C=DZ/ST=Algeria/L=BEJAIA/O=dz/CN=epb.dz
Getting Private key
mina@mina-LIFEBOOK-AH512:~$
```

5

Figure 4.16 : Création du certificat auto-signé

- **Installation du certificat :**

```
Signature ok
subject=/C=DZ/ST=Algeria/L=BEJAIA/O=dz/CN=epb.dz
Getting Private key
mina@mina-LIFEBOOK-AH512 ~$ sudo cp server.crt /etc/ssl/certs
[sudo] password for mina:
mina@mina-LIFEBOOK-AH512:~$ sudo cp server.key /etc/ssl/private
mina@mina-LIFEBOOK-AH512:~$
```

6

Figure 4.17 : Installation du certificat

- **Configuration du chemin du certificat :**

```
mina@mina-LIFEBOOK-AH512:~$ sudo postconf -e 'smtpd_tls_key_file = /etc/ssl/priv
ate/server.key'
mina@mina-LIFEBOOK-AH512:~$ sudo postconf -e 'smtpd_tls_cert_file = /etc/ssl/cer
ts/server.crt'
mina@mina-LIFEBOOK-AH512:~$
```

7

Figure 4.18 : Configuration du chemin du certificat

Nous reprenons la configuration de Postfix, cette fois nous éditons le fichier de configuration *master.cf* , les modifications apportées au fichier sont encadrées dans la figure qui suit :

*main.cf × *master.cf ×

```
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================
smtp      inet  n       -       -       -       -       smtpd
#smtp      inet  n       -       -       -       1       postscreen
#smtpd     pass  -       -       -       -       -       smtpd
#dnsblog   unix  -       -       -       -       0       dnsblog
#tlsproxy  unix  -       -       -       -       0       tlsproxy
#submission inet n       -       -       -       -       smtpd
  -o syslog_name=postfix/submission
  -o smtpd_tls_security_level=encrypt
  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_reject_unlisted_recipient=no
#  -o smtpd_client_restrictions=$mua_client_restrictions
#  -o smtpd_helo_restrictions=$mua_helo_restrictions
#  -o smtpd_sender_restrictions=$mua_sender_restrictions
#  -o smtpd_recipient_restrictions=
  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
  -o milter_macro_daemon_name=ORIGINATING
#smtps     inet  n       -       -       -       -       smtpd
  -o syslog_name=postfix/smtps
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_reject_unlisted_recipient=no
#  -o smtpd_client_restrictions=$mua_client_restrictions
#  -o smtpd_helo_restrictions=$mua_helo_restrictions
#  -o smtpd_sender_restrictions=$mua_sender_restrictions
#  -o smtpd_recipient_restrictions=
  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
  -o milter_macro_daemon_name=ORIGINATING
#628       inet  n       -       -       -       -       qmqpd
pickup    unix  n       -       -       60      1       pickup
cleanup   unix  n       -       -       -       0       cleanup
qmgr      unix  n       -       n       300     1       qmgr
#qmgr      unix  n       -       n       300     1       oqmgr
```

Figure 4.19 : Configuration du fichier *master.cf* de Postfix

Nous allons maintenant installer Dovecot SASL, par la commande illustrée dans la figure suivante :

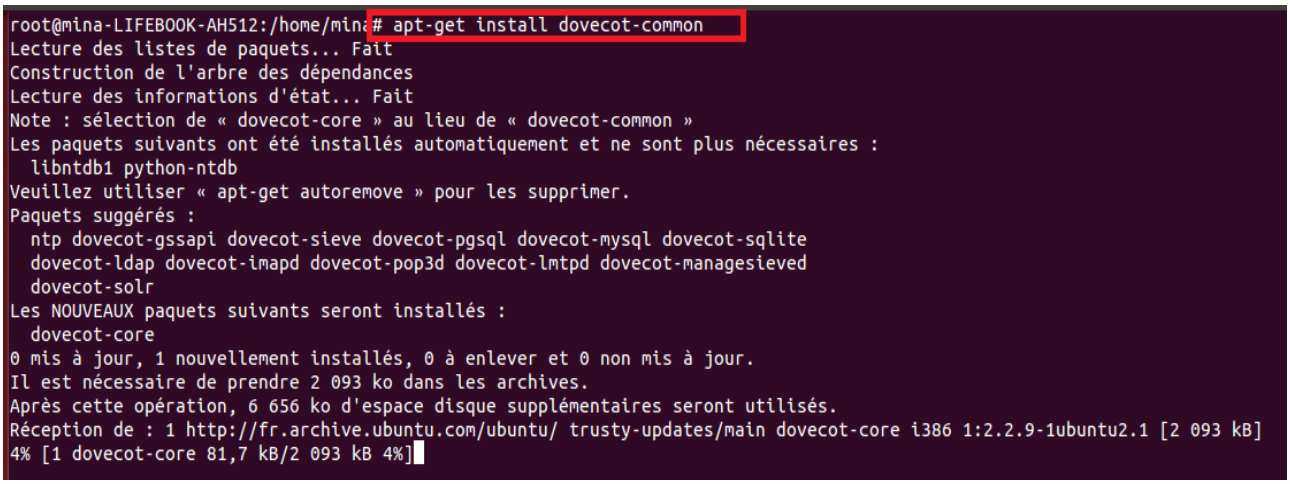

Figure 4.20 : Installation de Dovecot SASL

Nous introduisons par la suite le nom d'hôte demandé, comme le montre la figure ci-dessous :

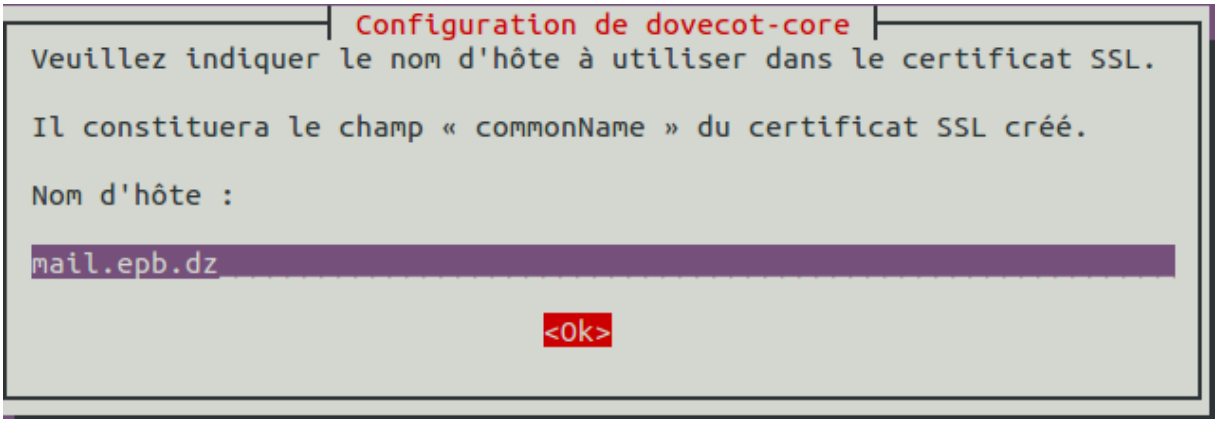

Figure 4.21 : Configuration du nom d'hôte à utiliser dans le certificat SSL

Nous allons configurer les fichiers ajoutés précédemment dans le fichier *main.cf* , ceci en apportant des modifications aux fichiers ***10-master.conf*** et ***10-auth.conf*** sous le répertoire ***/etc/dovecot/conf.d***. comme illustré dans les figures suivantes:

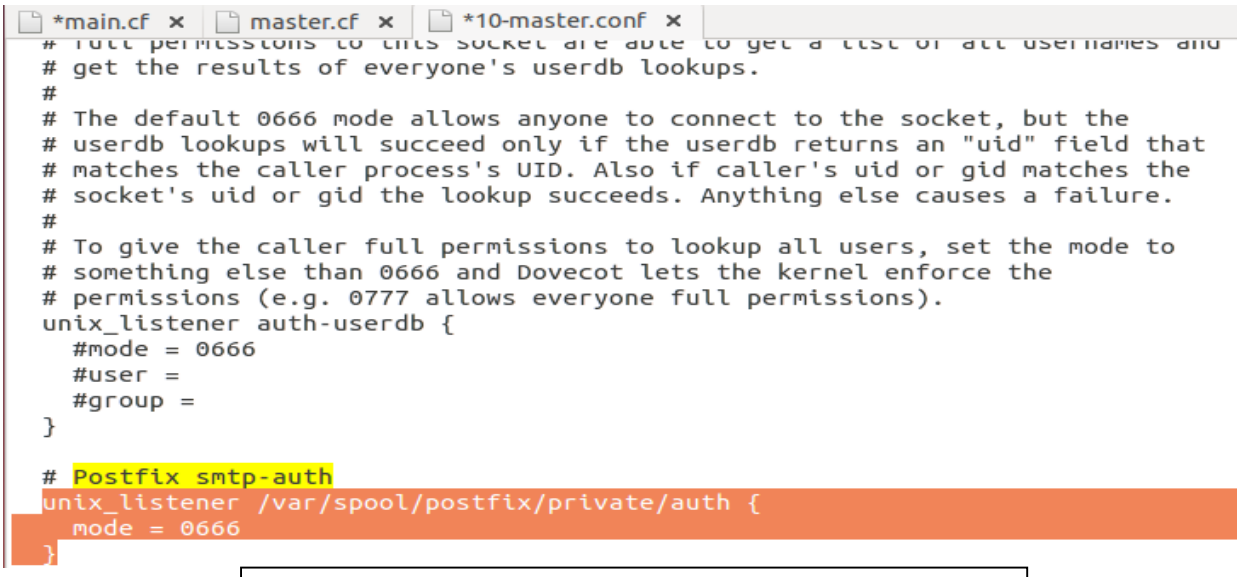

Figure 4.22 : Configuration du fichier *10-master.conf*

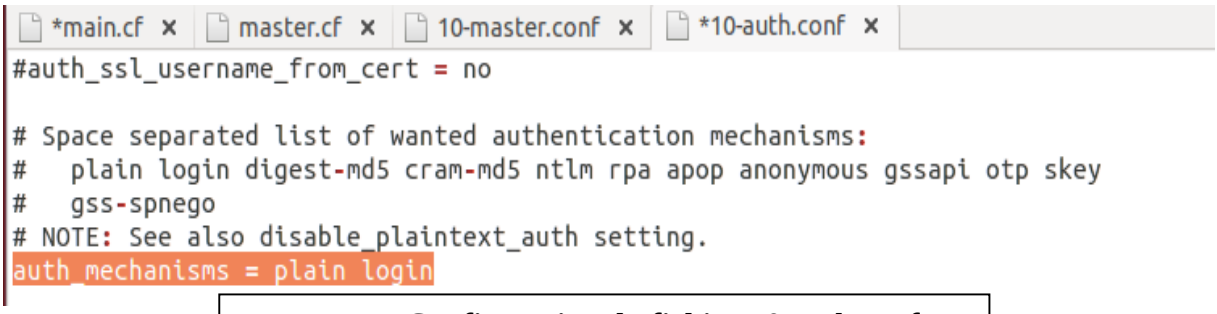

Figure 4.23 : Configuration du fichier *10-auth.conf*

Enfin, nous réinitialisons Postfix et Dovecot en tappant les commandes : ***#service postfix restart*** et ***#service dovecot restart*** .

Nous allons tester le fonctionnement de notre MTA en testant SMTP-AUTH avec l'accès aux ports 25 , 465 et 587.

Sachant que les ports cités ci-dessus définissent :

- 25 : l'envoi du courrier via notre serveur mail smtp.
- 465 : l'envoi du courrier via notre serveur mail en utilisant SSL.
- 587 : l'envoi du courrier via notre serveur mail avec encryption.

Voici les figures qui illustrent les tests :

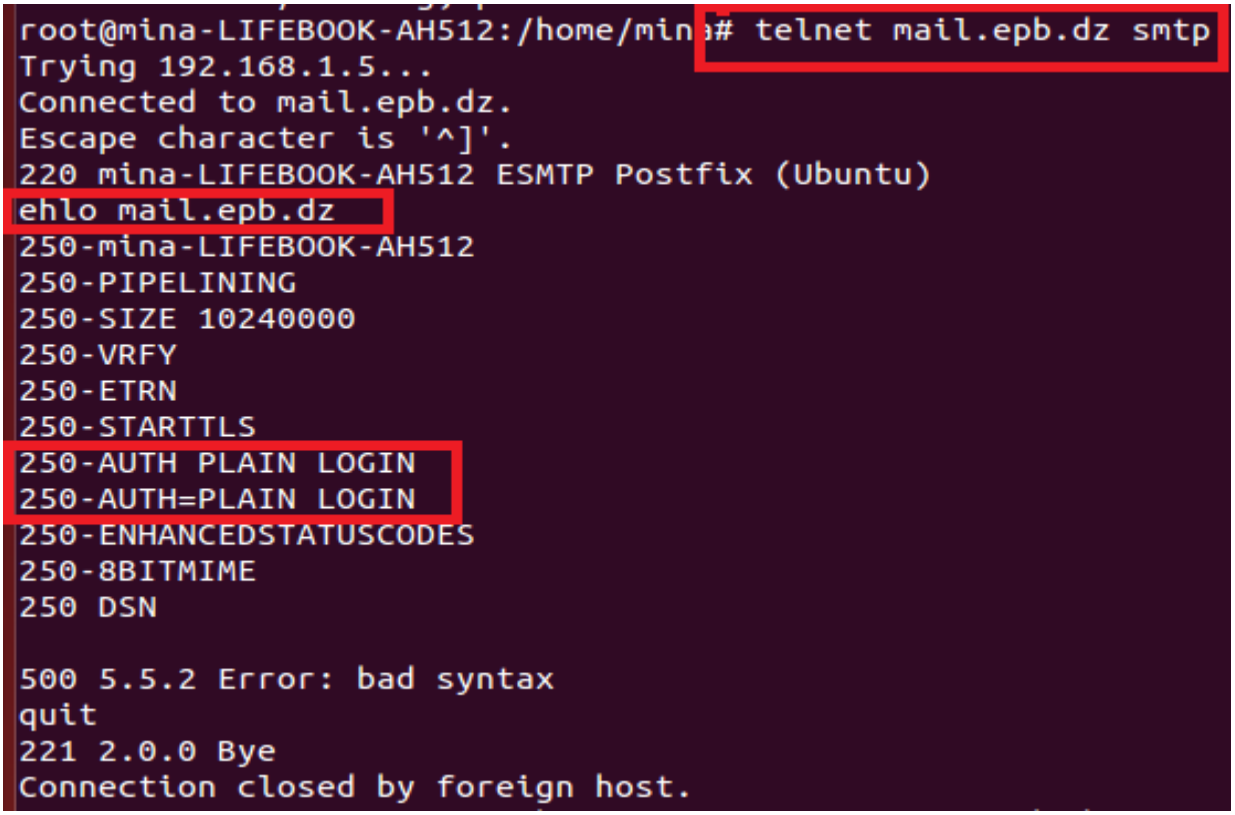

Figure 4.24 : Test du serveur SMTP (port 25)

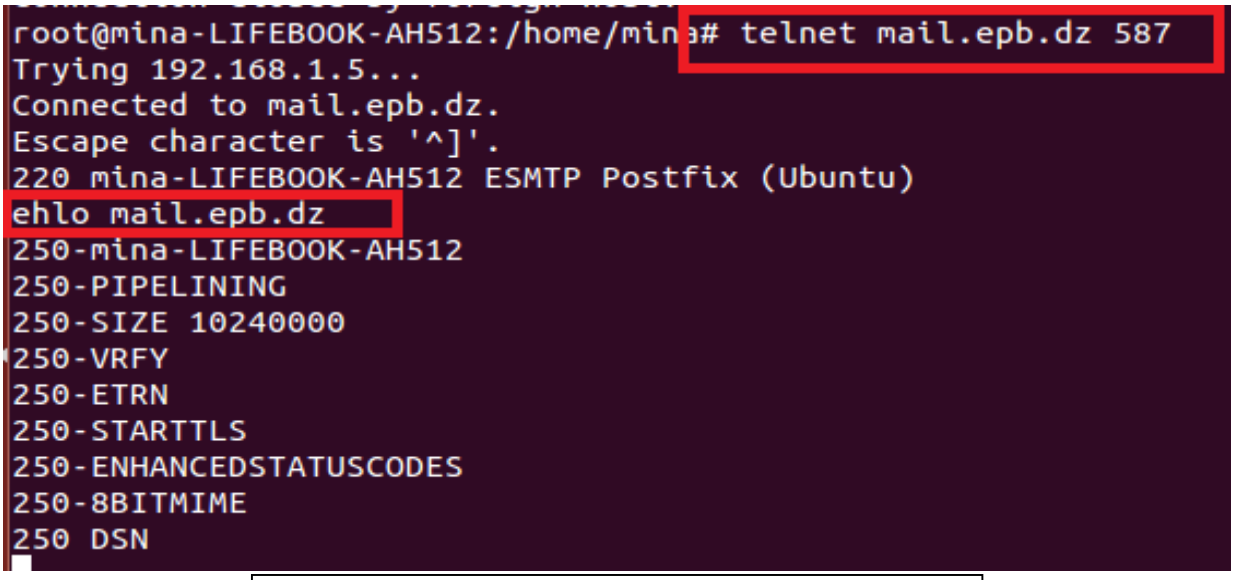

Figure 4.25 : Test du serveur SMTP (port 587)

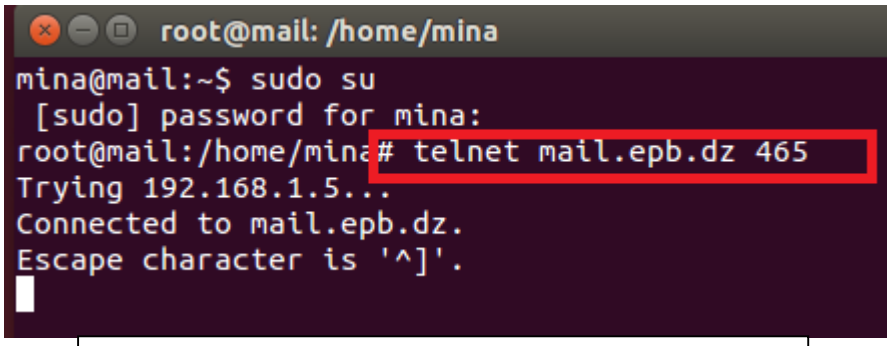

Figure 4.26 : Test du serveur SMTPs (port 465)

2.2. Installation et configuration du MDA :

Nous passons maintenant à l'installation de notre MDA : Dovecot IMAP et Dovecot POP.

```
root@mina-LIFEBOOK-AH512:/home/mina# apt-get install dovecot-imapd dovecot-pop3d
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  libntdb1 python-ntdb
Veuillez utiliser « apt-get autoremove » pour les supprimer.
Les NOUVEAUX paquets suivants seront installés :
  dovecot-imapd dovecot-pop3d
0 mis à jour, 2 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 149 ko dans les archives.
Après cette opération, 1 551 ko d'espace disque supplémentaires seront utilisés.
Réception de : 1 http://fr.archive.ubuntu.com/ubuntu/ trusty-updates/main dovecot-imapd i386 1:2.2.9-1ubuntu2.1 [121 kB]
1% [1 dovecot-imapd 1 151 B/121 kB 1%]
```

Figure 4.27 : Installation de Dovecot IMAP et Dovecot POP

Nous passons à la configuration des fichiers : ***10-mail.conf*** **,** ***20-pop3.conf*** et ***10-ssl.conf*** sous le repertoire ***/etc/dovecot/conf.d*** **,** leurs configurations sont illustrées dans les figures ci-dessous:

main.cf × | master.cf × | 10-master.conf × | 10-auth.conf × | resolv.conf × | epb.zone × | epb.invzone × | dhcpd.conf × | *10-mail.conf ×

```
##
## Mailbox locations and namespaces
##

# Location for users' mailboxes. The default is empty, which means that Dovecot
# tries to find the mailboxes automatically. This won't work if the user
# doesn't yet have any mail, so you should explicitly tell Dovecot the full
# location.
#
# If you're using mbox, giving a path to the INBOX file (eg. /var/mail/%u)
# isn't enough. You'll also need to tell Dovecot where the other mailboxes are
# kept. This is called the "root mail directory", and it must be the first
# path given in the mail_location setting.
#
# There are a few special variables you can use, eg.:
#
#   %u - username
#   %n - user part in user@domain, same as %u if there's no domain
#   %d - domain part in user@domain, empty if there's no domain
#   %h - home directory
#
# See doc/wiki/Variables.txt for full list. Some examples:
#
#   mail_location = maildir:~/Maildir
#   mail_location = mbox:~/mail:INBOX=/var/mail/%u
#   mail_location = mbox:/var/mail/%d/%1n/%n:INDEX=/var/indexes/%d/%1n/%n
#
# <doc/wiki/MailLocation.txt>
#
mail_location = maildir:~/Maildir
```

Figure 4.28 : Configuration du fichier *10-mail.conf*

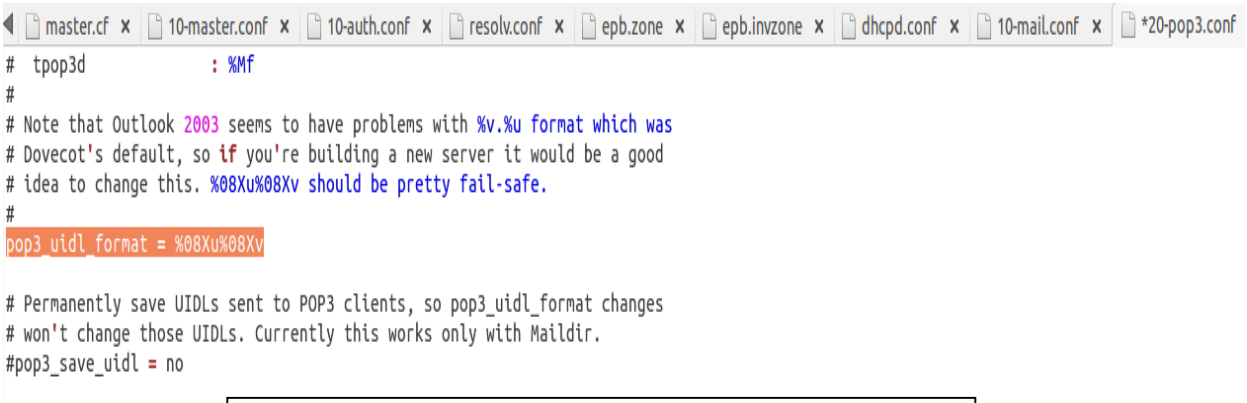

Figure 4.29 : Configuration du fichier *20-pop3.conf*

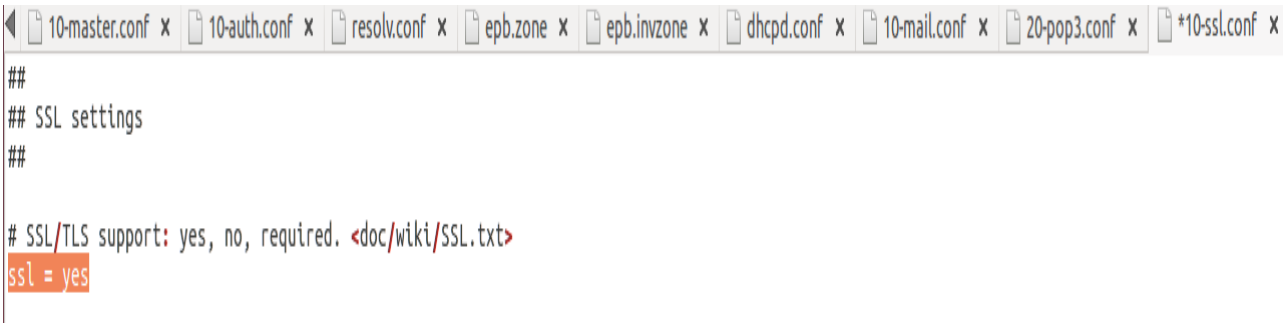

Figure 4.30 : *Configuration du fichier 10-ssl.conf*

Enfin, nous réinitialisons Dovecot en tappant la commande : ***#service dovecot restart***.

Nous allons tester le fonctionnement de notre MDA en testant les ports 143 et 993 d'IMAP et les ports 110 et 995 de POP3.

Sachant que les ports cités ci-dessus définissent :

- 143: La récupération du courrier via IMAP.
- 993 : La récupération du courrier via IMAP en utilisant SSL.
- 110: La récupération du courrier via POP3.
- 995 : La récupération du courrier via POP3 en utilisant SSL.

Voici les figures qui illustrent les tests :

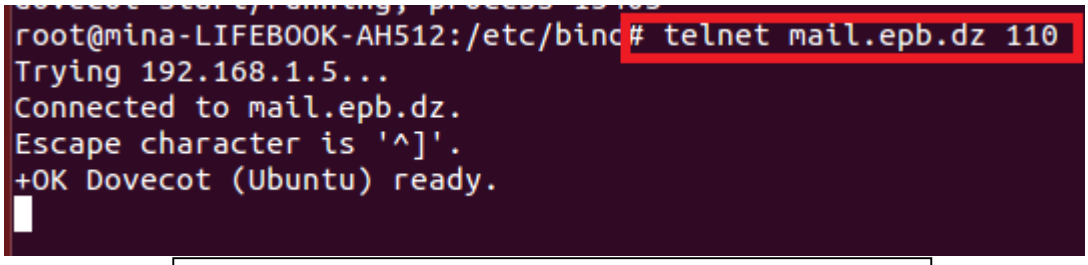

Figure 4.31 : Test du MDA avec POP3 (port 110)

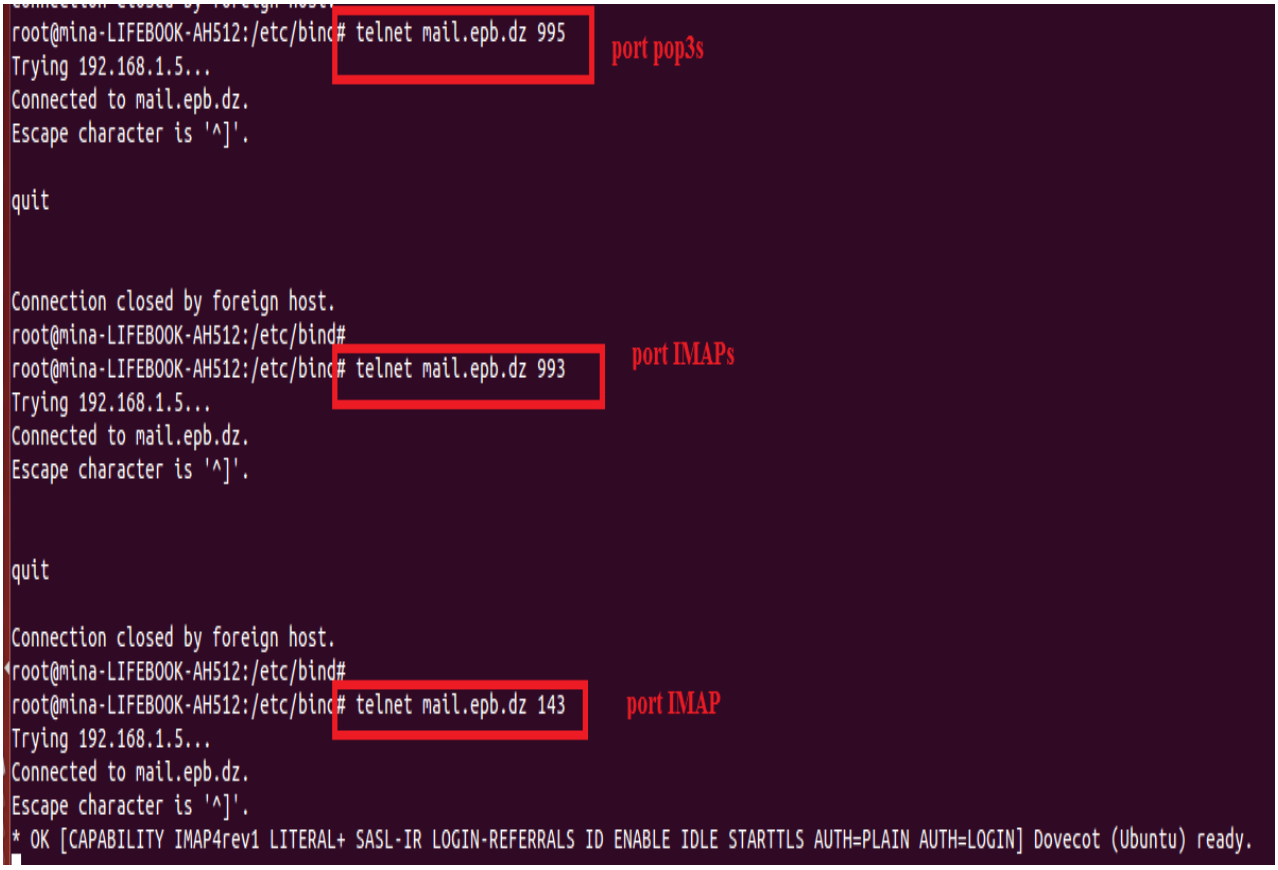

Figure 4.32 : Test du MDA (ports: 995, 993 et 143)

Nous confirmons que l'accès à tous les ports cités ci-dessus sont activés avec la commande : ***#netstat –nl4.***

```
mina@mina-LIFEBOOK-AH512:~$ netstat -nl4
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale          Adresse distante        Etat
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:587             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:465             0.0.0.0:*               LISTEN
tcp        0      0 192.168.1.5:53          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:995             0.0.0.0:*               LISTEN
```

Figure 4.33 : Test de tous les ports (SMTP,SMTPs, DNS, IMAP, IMAPs, POP3 et POP3s)

2.3. Installation et configuration de notre MUA :

Avant d'entammer l'installation de note MUA Squirrelmail, nous allons d'abord installer Apache avec la commande : ***#apt-get install apache2.***

Une fois installé, nous vérifions en tappant l'adresse IP du serveur sur le navigateur web et cette page s'affiche :

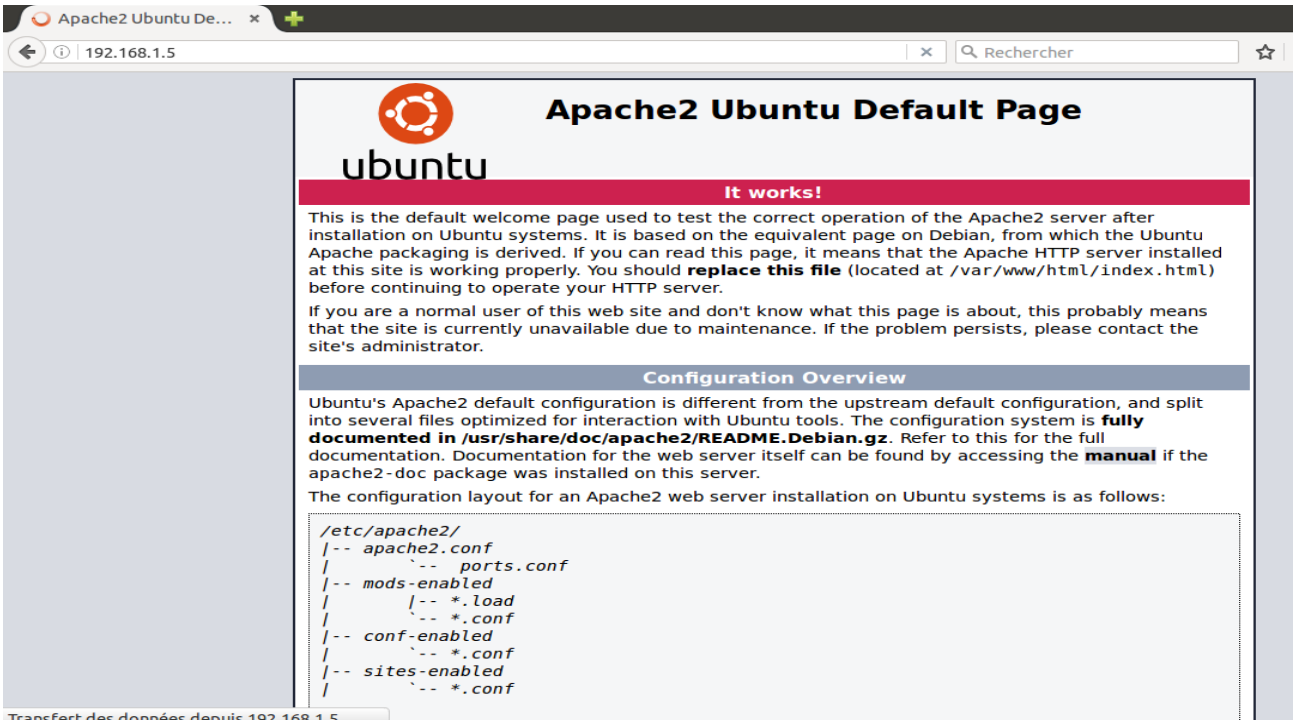

Figure 4.34 : Vérification de l'installation d'Apache2

Nous installons Squirrelmail avec la commande : ***#apt-get install squirrelmail***

Et nous commençons sa configuration comme suit :

```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Organization Preferences
1.  Organization Name       : s
2.  Organization Logo       : ../images/sm_logo.png
3.  Org. Logo Width/Height  : (308/111)
4.  Organization Title      : SquirrelMail $version
5.  Signout Page            :
6.  Top Frame               : _top
7.  Provider link           : http://squirrelmail.org/
8.  Provider name           : SquirrelMail

R   Return to Main Menu
C   Turn color on
S   Save data
Q   Quit

Command >> q

You have not saved your data.
Save?  [Y/n]: y
Data saved in config.php

Exiting conf.pl.
You might want to test your configuration by browsing to
http://your-squirrelmail-location/src/configtest.php
Happy SquirrelMailing!

root@mina-LIFEBOOK-AH512:/home/mina#
```

Figure 4.35 : Configuration de Squirrelmail

Nous créons un lien symbolique pour la compatibilié de squirrelmail avec Apache2 avec les commandes:

```
$ sudo cp /etc/squirrelmail/apache.conf /etc/apache2/sitesavailable/squirrelmail.conf
```

```
$ sudo a2ensite squirrelmail
```

Enfin, nous procédons à la réinitialisation de Squirrelmail: ***# service apache2 restart.***

Nous vérifions son installation en tappant l'adresse IP de notre serveur / Squirrelmail:

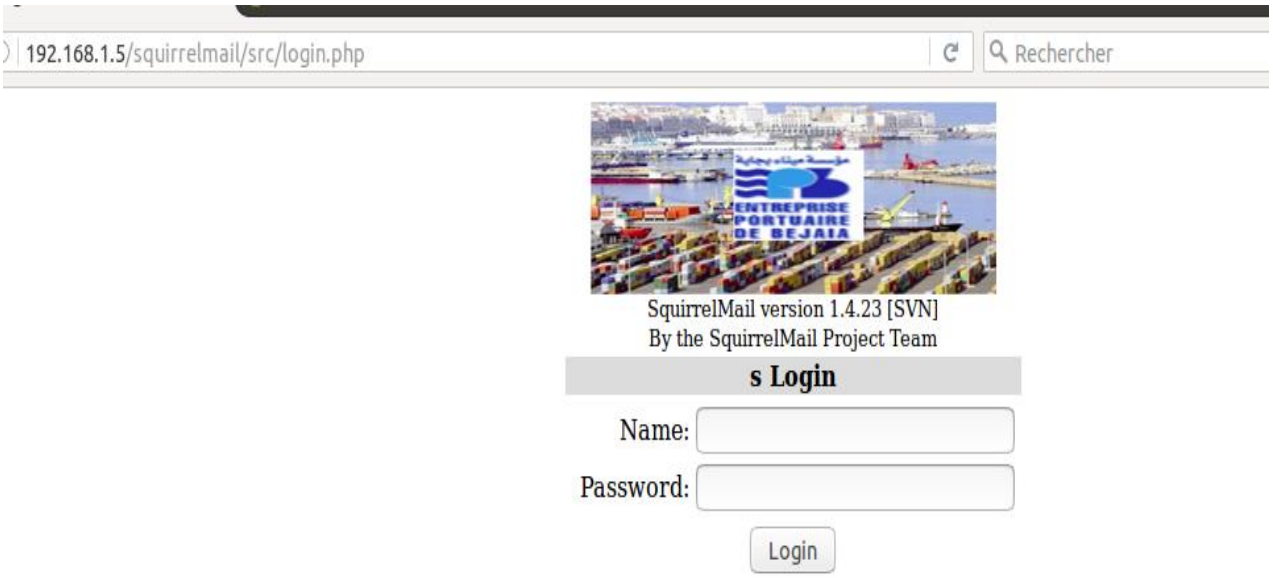

Figure 4.36 : page de connexion Squirrelmail

- **Gestion des utilisateurs :**
  Nous procédons à présent à la gestion des utilisateurs du serveur de messagerie électronique, voici l'interface qui va nous permettre de les gérer :

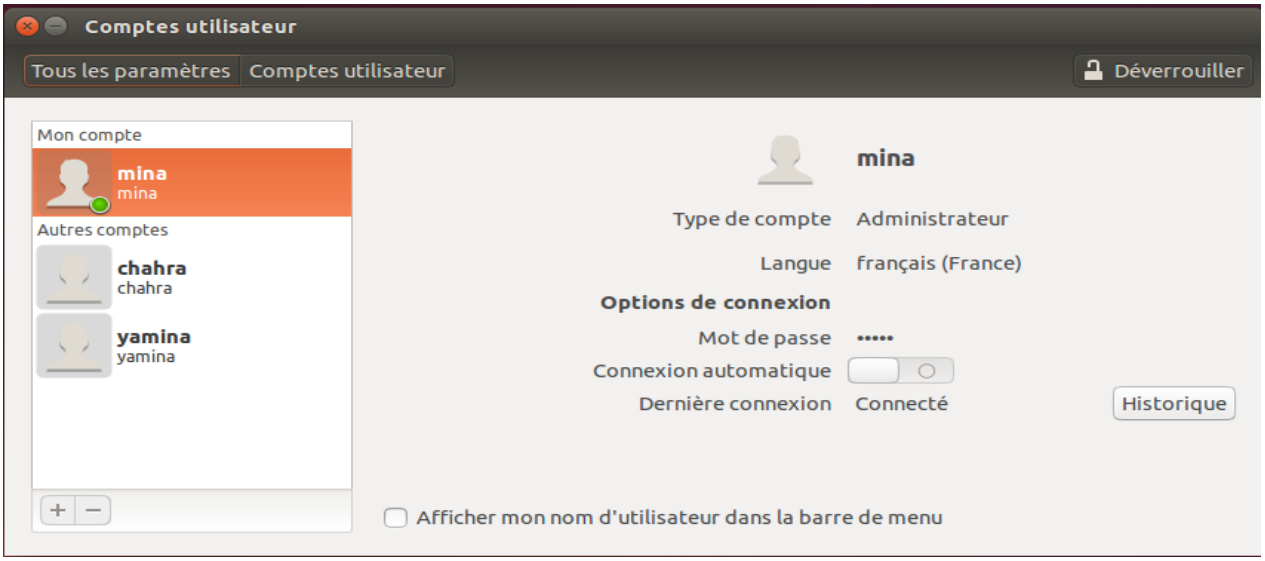

Figure 4.37 : Interface de gestion des utilisateurs

Pour l'ajout , la modification et la suppression, il faudra d'abord s'authentifier :

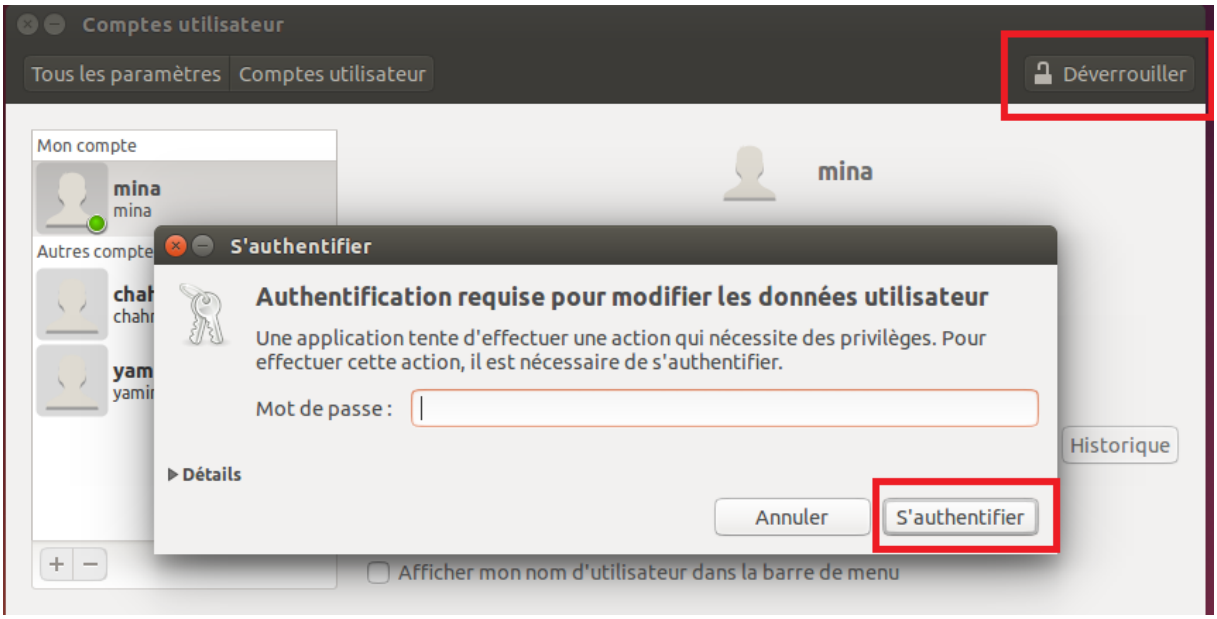

Figure 4.38 : Authentification pour la gestion des utilisateurs

Voici un exemple de l'interface d'ajout d'un compte utilisateur :

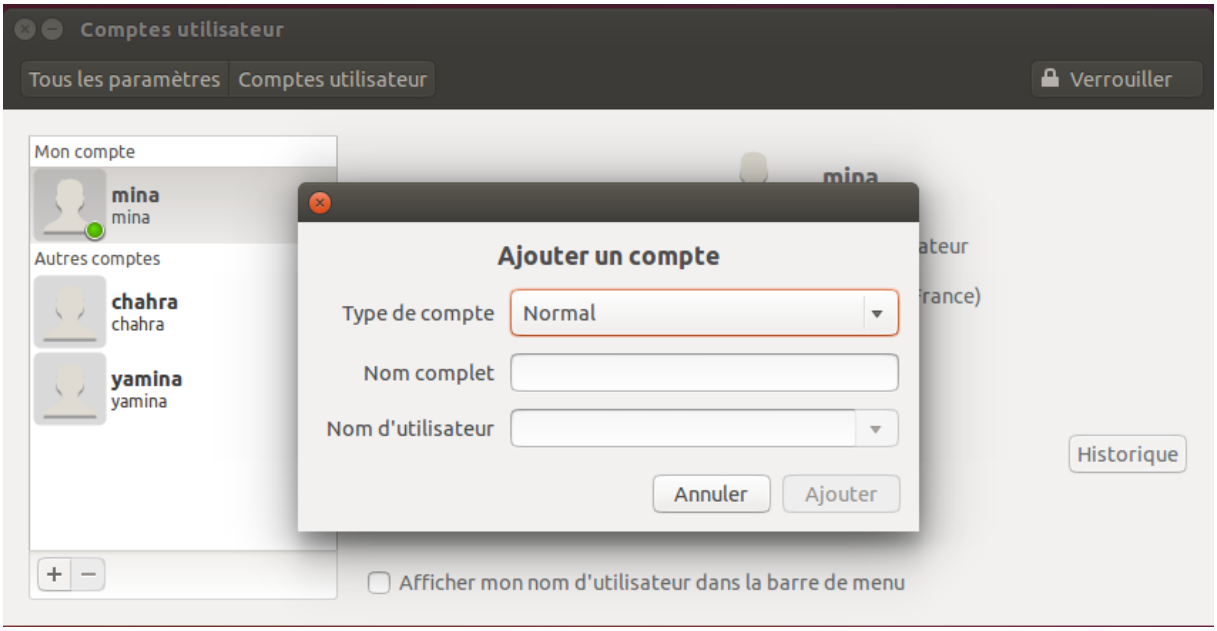

Figure 4.39 : Ajout d'un compte utilisateur

- **Test des fonctionnalités sur serveur de messagerie électronique :**

  - **Authentification :**
    Voici un exemple de login : **mina@epb.dz** et mot de passe , précédemment ajoutés .

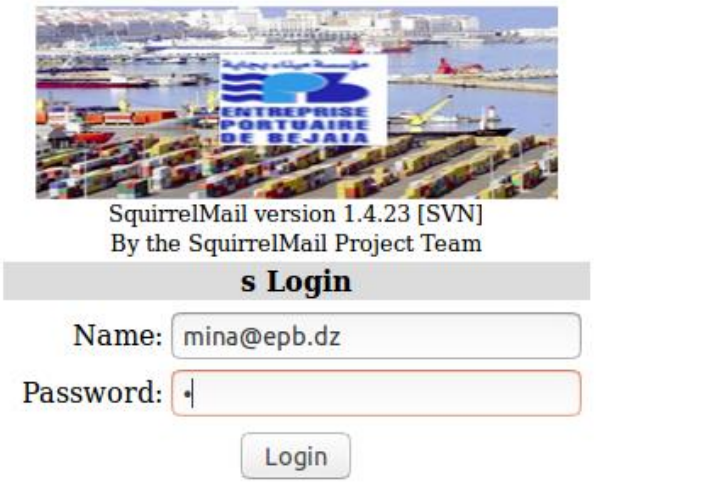

Figure 4.40 : Saisie du login et mot de passe

- **Liste des messages :**
  - **Composer un message :**

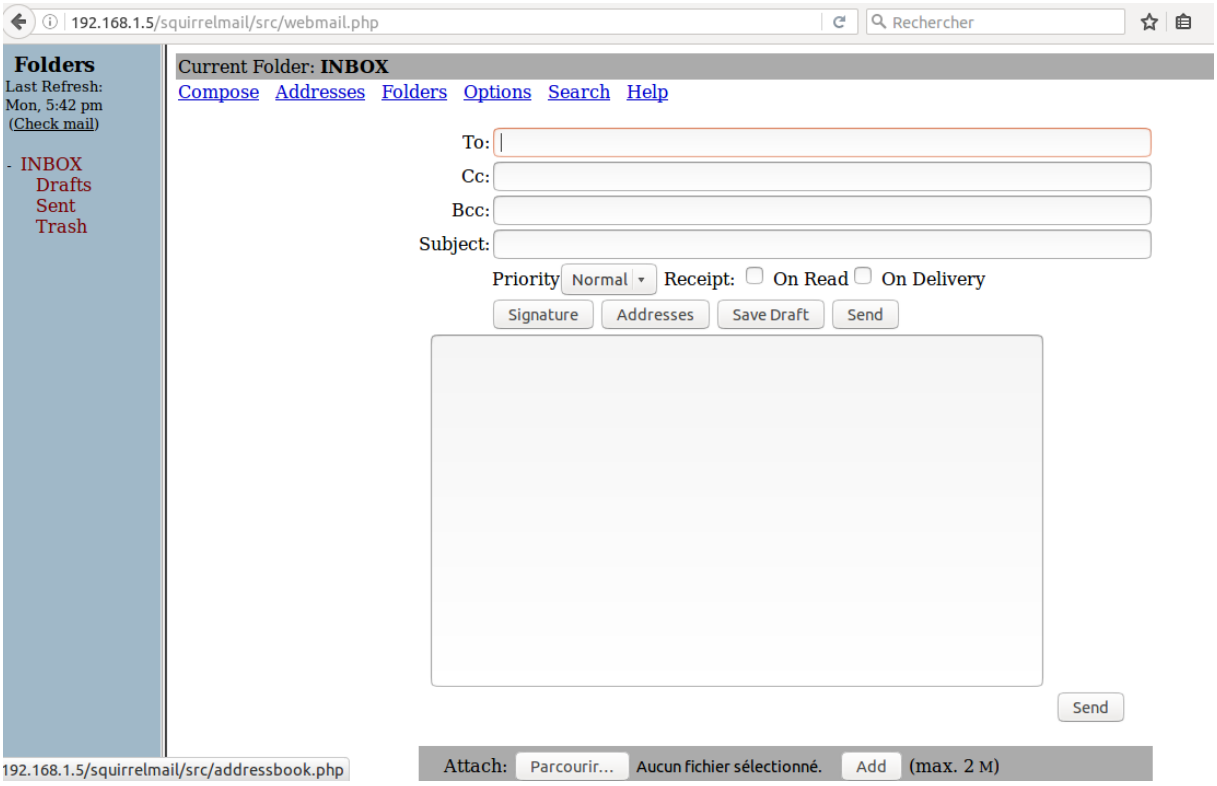

Figure 4.40 : Composer un message

- **Messages envoyés :**

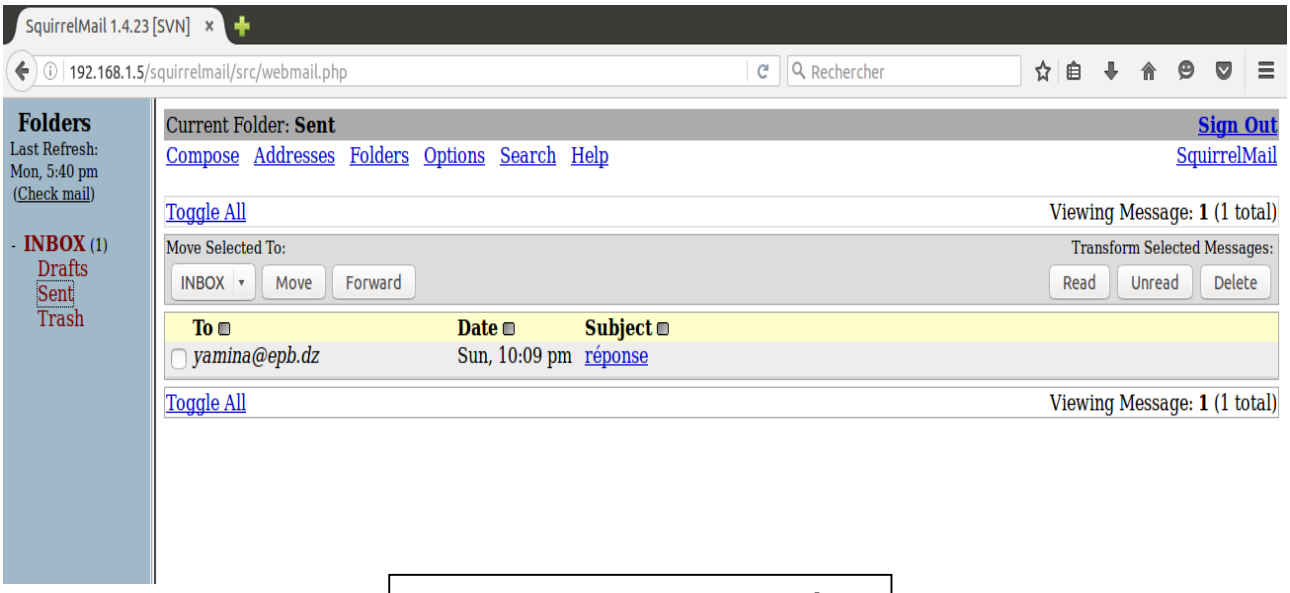

Figure 4.41 : Messages envoyés

- **Messages reçus :**

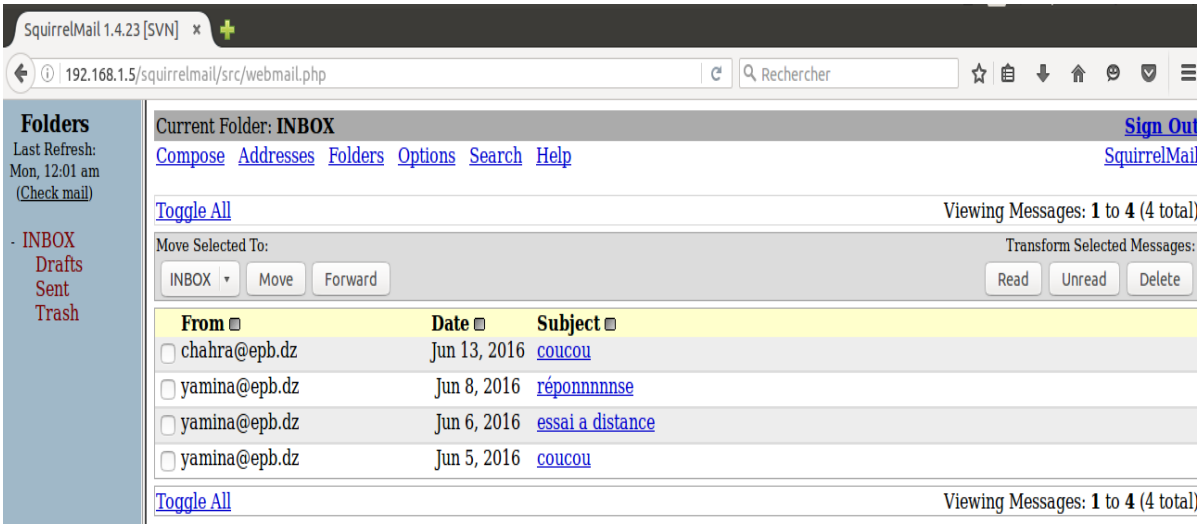

Figure 4.42 : Messages reçus

- **Annuaire personnel d'adresses électroniques:**

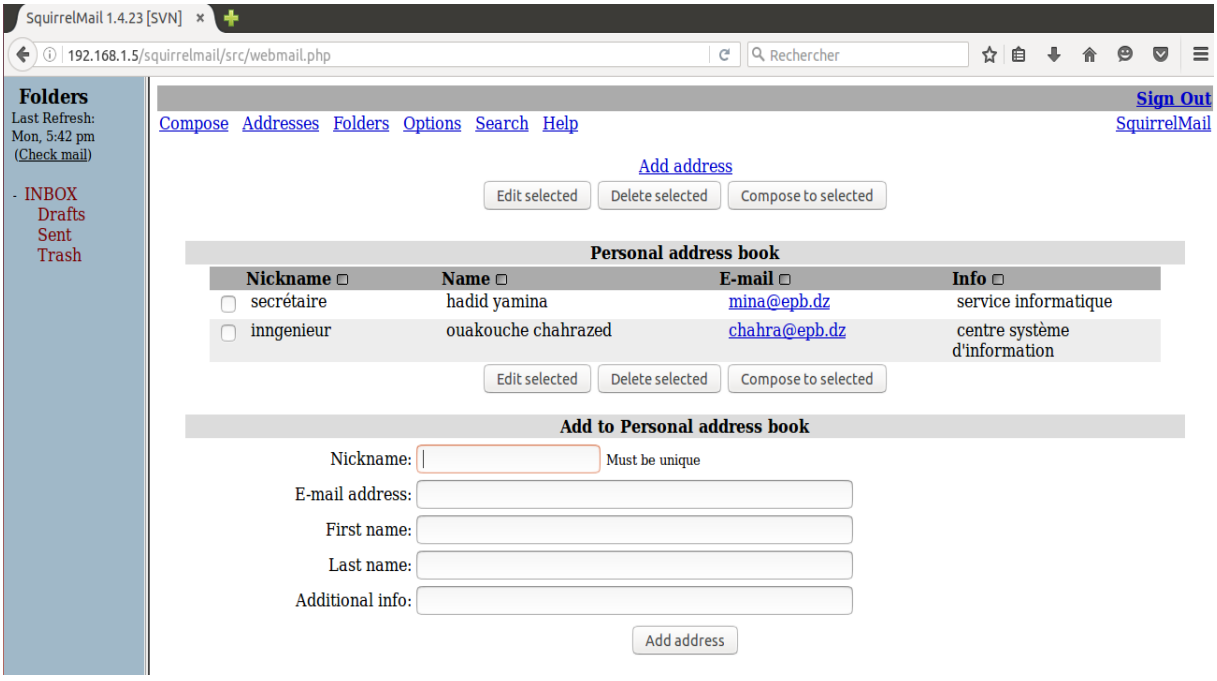

Figure 4.43 : Annuaire personnel d'adresses électroniques

L'annuaire personnel d'adresses électronique, permet la manipulation simple et rapide des contacts, une fois que l'expéditeur clique sur le nom du destinataire, il botient ceci :

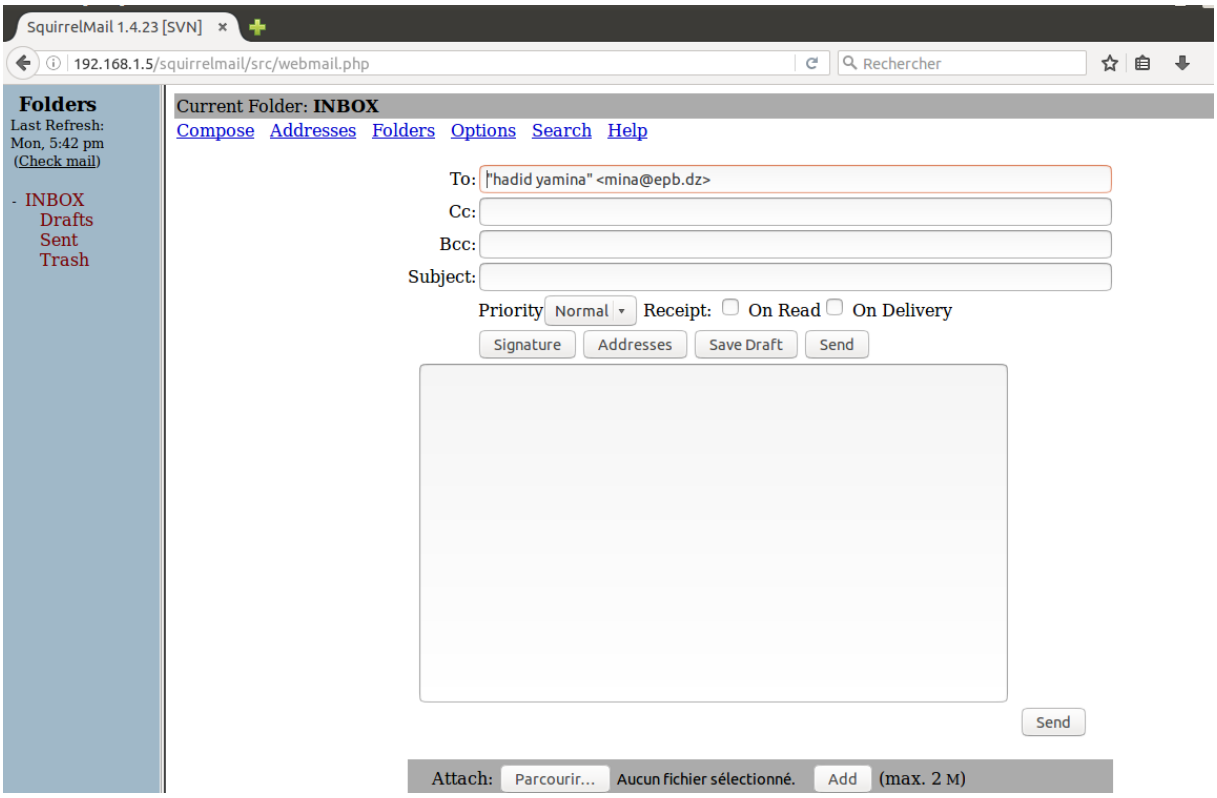

Figure 4.44 : Manipulation rapide des adresses électroniques

- ## Conclusion

Ce chapitre a été consacré à l'explication détaillée de toutes les étapes nécéssaires à la mise en place d'un serveur de messagerie électronique sur un réseau LAN. Nous avons illustré l'installation et la configuration et le test de chaque composant de la messagerie électronique ainsi que la sécurité de l'échange d'informations circulant au sein du réseau. Enfin, Nous avons cloturé le tout par des exemples illustrant le fonctionnement de notre serveur.

Conclusion Générale

Notre objectif à travers ce travail est de palier aux différentes faiblesses de l'organisme d'accueil ; en terme de disponibilité du service de la messagerie électronique et de sa sécurité. En effet après notre passage à l'E.P.Béjaia , nous avons pris le temps d'analyser leurs besoins et de leur suggérer une solution qui consiste à mettre en place un serveur de méssagerie électronique interne dont la disponibilité est continue et qui assure sa sécurité.

A travers ce mémoire, nous avons indiqué comment un système de messagerie interne, de par sa mise en place et sa sécurisation pourrai répondre aux besoins en termes de technologies de l'information et de la communication d'une entreprise.

Pour cela nous avons choisi de mettre en œuvre les composants suivants :

-Postfix comme MTA.

-Dovecot IMAP et POP comme MDA.

-Squirrelmail comme MUA.

-TLS comme protocole de sécurité.

Nous avons tout au long de ce travail voulu offrir au lecteur la possibilité de mettre en place son propre serveur mail grâce aux différentes directives que nous avons présenté de manière explicite et détaillée. Nous avons commencé dans le premier chapitre par donner des définitions sur les concepts fondamentaux de la mise en place d'un serveur de messagerie électronique et ses composants ainsi que les différentes manières possibles d'assurer leur sécurité. Ensuite, nous avons présenté le cadre de notre stage ainsi qu'un cahier de charge regroupant les besoins de l'entreprise et les suggestions que nous leur avons proposé. Dans le troisième chapitre, nous avons fait une étude comparative de tous les moyens existants et de ceux que nous avons choisi de mettre en œuvre. Enfin, nous avons finalisé le tout par la réalisation pratique du serveur de méssagerie électronique .

Ce travail a été pour nous l'occasion d'une émulation intellectuelle dans le domaine de la messagerie électronique, il nous a permis d'acquérir une expérience personnelle et professionnelle très bénéfique et de nous familiariser avec l'environnement du travail ainsi d'élargir et d'approfondir nos connaissances.

En perspective, nous allons déployer notre système au niveau de l'entreprise et améliorer l'interface IHM du webmail de notre serveur.

Annexes

Chapitre 01 :

- **Chiffrement symetrique et asymetrique :**

- **Le chiffrement symétrique** : utilise une clé unique partagée entre les 2 interlocuteurs. On encode et on décode le message avec la même clé.

  Le problème de ce chiffrement est qu'il faut trouver un moyen de transmettre la clé unique entre les 2 interlocuteurs.

- **Chiffrement asymétrique (*à clé publique*) :** les clés existent par paires (le terme de *bi-clés* est généralement employé) :Une clé publique pour le chiffrement ;Une clé secrète pour le déchiffrement.

  Ainsi, dans un système de chiffrement à clé publique, les utilisateurs choisissent une clé aléatoire qu'ils sont seuls à connaître (il s'agit de la clé privée). A partir de cette clé, ils déduisent chacun automatiquement un algorithme (il s'agit de la clé publique). Les utilisateurs s'échangent cette clé publique au travers d'un canal non sécurisé.

  Lorsqu'un utilisateur désire envoyer un message à un autre utilisateur, il lui suffit de chiffrer le message à envoyer au moyen de la clé publique du destinataire. Ce dernier sera en mesure de déchiffrer le message à l'aide de sa clé privée (qu'il est seul à connaître).

- **Le modèle OSI :**
  Le modèle OSI (*Open Systems Interconnection*) est un standard de communication, en réseau, de tous les systèmes informatiques. C'est un modèle de communications entre ordinateurs proposé par l'ISO qui décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions.

- **Le modèle TCP/IP :**
  C'est une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante.

Annexes

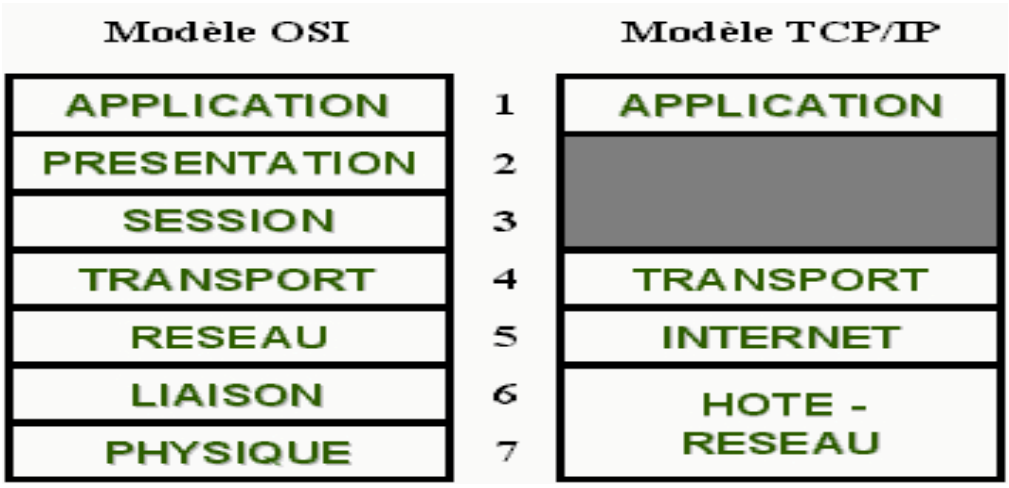

Figure 1 : le modèle OSI et le modèle TCP/IP

- **Encapsulation de données :** Le paquet est l'unité d'information de base transférée via le réseau. Le paquet de base consiste en un en-tête avec les adresses des systèmes émetteur et récepteur, ainsi qu'un corps, ou champ de données, avec les données à transférer.

  Lorsque le paquet parcourt la pile de protocoles TCP/IP, les protocoles de chaque couche ajoutent ou suppriment des champs de l'en-tête de base. Lorsqu'un protocole sur le système émetteur ajoute des données à l'en-tête du paquet, le processus s'appelle encapsulation de données.

Annexes

Chapitre 02 :

- **La norme ISO 9001 (Organisation internationale de normalisation) :**

  Cette norme définit des exigences pour la mise en place d'un système de management de la qualité pour les organismes souhaitant améliorer en permanence la satisfaction de leur client et fournir des produits et services conformes. La norme ISO 9001 s'adresse à tout organisme, quels que soient sa taille et son secteur d'activité. Elle fait partie de la série des normes ISO 9000 (ISO 9000, ISO 9001 et ISO 9004).

  La norme ISO 9001 a été publiée pour la première fois en 1987 et est régulièrement révisée depuis. Sa première révision date de 1994, la suivante de 2000, qui a intégré la notion de processus, puis 2008, et la dernière de 2015.

- **La norme ISO 14001** : définit une série d'exigences spécifiques à la mise en place d'un système de management environnemental au sein d'une organisation, quelle que soit sa taille et son domaine d'activité.

  La norme ISO 14001 a été réalisée par l'Organisation internationale de normalisation et fait partie de la famille des normes ISO 14000 qui regroupe des normes complémentaires relatives au management environnemental. La norme ISO 14001 est aussi un élément de la triple certification qualité-sécurité-environnement ISO 9001, ISO 14001 et OHSAS 18001 qui permet aux entreprises d'avoir une politique globale de management des risques. Ces trois normes reposent sur un modèle similaire qui facilite leur intégration. Elle est également une des normes sur lesquelles s'appuie l'ISO 26000 dans laquelle elle s'imbrique et s'articule.

Chapitre 03 :

- **Licence GPL :** La licence publique générale GNU, ou GNU General Public License , est une licence qui fixe les conditions légales de distribution des logiciels libres du projet GNU.

  Richard Stallman, président et fondateur de la Free Software Foundation en est l'auteur. Sa dernière version est la « GNU GPL version 3 » publiée le 29 juin 2007 avec le concours juridique d'Eben Moglen.

  Cette licence a depuis été adoptée, en tant que document définissant le mode d'utilisation, donc d'usage et de diffusion, par de nombreux auteurs de logiciels libres, en dehors des projets GNU.

Annexes

- **LAMP :** est un acronyme désignant un ensemble de logiciels libres permettant de construire des serveurs de sites web. L'acronyme original se réfère aux logiciels suivants : « Linux », le système d'exploitation (GNU/Linux) ; « Apache », le serveur Web ; « MySQL ou MariaDB », le serveur de base de données .
- **Nginx [engine x]** : est un logiciel libre de serveur Web (ou HTTP) ainsi qu'un proxy inverse écrit par Igor Sysoev, dont le développement a débuté en 2002 pour les besoins d'un site russe à très fort trafic (Rambler). Une partie de la documentation a été traduite du russe vers l'anglais.
- **Lighttpd (ou « lighty »)** : est un logiciel de serveur Web (ou HTTP) sécurisé, rapide et flexible. C'est un logiciel libre écrit en C et distribué selon les termes de la licence BSD.
- **AJAX :** L'architecture informatique Ajax (acronyme d'Asynchronous JavaScript and XML) permet de construire des applications Web et des sites web dynamiques interactifs sur le poste client en se servant de différentes technologies ajoutées aux navigateurs web entre 1995 et 2005.
- **SOAP (Simple Object Access Protocol)** :est un protocole de RPC orienté objet bâti sur XML. Il permet la transmission de messages entre objets distants, ce qui veut dire qu'il autorise un objet à invoquer des méthodes d'objets physiquement situés sur un autre serveur. Le transfert se fait le plus souvent à l'aide du protocole HTTP, mais peut également se faire par un autre protocole, comme SMTP.

  Le protocole SOAP est composé de deux parties :

  - une enveloppe, contenant des informations sur le message lui-même afin de permettre son acheminement et son traitement,
  - un modèle de données, définissant le format du message, c'est-à-dire les informations à transmettre.
- **IBM (International Business Machines Corporation)** :
  est une société multinationale américaine présente dans les domaines du matériel informatique, du logiciel et des services informatiques.

Annexes

Chapitre 04 :

- **SMTP-AUTH :** est une extension du protocole SMTP. Les serveurs qui supportent le protocole SMTP-AUTH peuvent être paramétrés pour n'accepter que des clients capables de s'authentifier (clients possédant cette extension) et ainsi certifier d'une autorisation d'accès pour ces derniers.

  SMTP-AUTH fournit un mécanisme de contrôle d'accès , permet à un serveur de courriers d'indiquer que l'expéditeur a été authentifié lors du relayage de courriers.

- **Dovecot SASL :** Les mécanismes d'authentification SASL peuvent fournir une couche d'intégrité des données laquelle permet d'offrir des services de sécurité des données et de confidentialité des données. Les protocoles d'application qui proposent SASL prennent très souvent en charge le protocole de sécurisation des échanges TLS en complément des services offerts par SASL.

Résumé

La messagerie électronique est un service très répandu et indispensable dans le domaine professionnel et dans la vie quotidienne. Ce service rend la communication plus facile et plus simple grâce au gain du temps et de qualité de réponse. En revanche, il peut manquer de disponibilité puisqu'il dépend du réseau internet et peut également représenter une menace pour la sécurité, d'où vient l'obligation de le sécuriser, de maintenir sa sécurité et de garantir sa disponibilité.

Notre travail consiste à mettre en place un serveur de messagerie électronique dans le réseau LAN de l'Entreprise Portuaire de Bejaia afin de répondre à leurs besoins.

Mots-clés : MUA, MTA, MDA, IMAP, POP3, POSTFIX, SQUIRRELMAIL, TLS.

Abstract

The electronic mail is a very wide-spread and essential server in the professional field and in the daily life. This server makes the communication easier and simpler because it reduces the time it has a better quality of the answer. However, since it depends on the internet network, a lack of availability can happen or even worse, it can represent a threat to security (security threat), and there comes the obligation to secure and maintain this security and guarantee its availability.

our job consists in setting up a mail server in LAN network of the harbour company in Bejaia to meet their needs

Keywords : MUA, MTA, MDA, IMAP, POP3, POSTFIX, SQUIRRELMAIL, TLS.