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 professionnel
en Informatique
Option
Administration et sécurité des réseaux
Thème

La mise en place d'un serveur de messagerie au sein de l'entreprise BMT (Bejaia Mediterranean Terminal).

Présenté par

M^r^ ***CHIKHOUNE*** **Mouloud**
M^r^ ***MOUSSAOUI*** **Walid**

Soutenu devant le jury composé de :

Président	M^me^ ***TAHAKOURT*** **Zineb**
Encadreur	M^me^ ***KHALED*** **Hayette**
Examinatrice	M^me^ ***GHANEM*** **Souhila**
Examinateur	M^r^ ***ELSAKAAN*** **Nadim**

Promotion 2015/2016

Remerciements

Louange A Dieu, le miséricordieux, sans lui rien de tout cela n'aurait pu être.

Nous tenons à remercier vivement M^{me} KHALED Hayette, pour nous avoir honoré par son encadrement, pour sa disponibilité, ses orientations, ses precieux conseils et ses encouragements qui nous ont permis de mener à bien ce travail.

Nous tennons à exprimer notre gratitude aux membres de jury pour avoir accepté de juger ce travail.

Nous remercions chaleureusement M^{r} BOUMERZOUG Moussa et à tous nos ensignants pour leurs conseils, leurs gentillesse, et leurs générosité.

Un merci particulier à nos parents, pour leur amour, leur sacrifices et leurs patiences.

Un énorme merci à nos familles et amis pour leurs éternel soutient et la confiance qu'ils ont en nos capacité.

Dédicaces

Je dédie ce modeste travail :

A mes parents,

A ma grand-mère,

A mon frère,

A toute la famille,

A mes amies et collègues, et tous ceux qui m'ont aidé ;

A mon binôme Walid et sa famille.

CHIKHOUNE Mouloud

Dédicaces

Je dédie ce modeste travail :

A mes parents,

A mon frére et ma soeur,

A toute la famille,

A mes amies et collègues, et tous ceux qui m'ont aidé ;

A mon binôme Mouloud et sa famille.

A Une personne spéciale OURTEMACHE Lynda.

MOUSSAOUI Walid

Résumé

La messagerie électronique est un service très répondu 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 être une menace pour la sécurité, d'où vient l'obligation de maintenir sa sécurité.

Notre travail consiste à mettre en œuvre et administrer un serveur de messagerie pour la BMT de Bejaia pour répondre à leurs besoins.

Nous avons commencé par expliquer quelques notions de base sur les réseaux ainsi que la messagerie électronique, puis nous avons détaillé le fonctionnement de la messagerie électronique, puis nous avons présenté les outils utilisés avant de passer à sa réalisation, et nous avons finis par la sécurisé.

La réalisation est faite en utilisant le serveur de messagerie postfix et squirrelmail comme client pour la gestion des mails.

Mots-clés : Messagerie électronique, SSL, Postfix, Postfixadmin, Squirrelmail.

Abstract

Email is a very needed service and responded in the professional field and in everyday life. This service makes the communications easier and simpler thanks to time gain and response quality. However, it can be a threat to security, so we must maintain its security.

Our memory focuses on the mail server implementation and administration for BMT Bejaia to assure their needs.

We began by explaining some basics of networks and email after that we details emails operation and the tools used before passing to its realization, and we finally assure its security.

The realization is made using the postfix mail server and squirrelmail as client for mail management.

Keywords : Email, SSL, Postfix, Postfixadmin, Squirrelmail.

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES ABRÉVIATIONS

LAN	**L**ocal **A**rea **N**etwork
MAN	**M**etropolitan**A**rea **N**etwork
WAN	**W**ide **A**rea **N**etwork
WIFI	**Wi**reless **FI**delity
OSI	**O**pen **S**ystems **I**nterconnection
TCP/IP	**T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol
DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol
DNS	**D**omain **N**ame **S**ystem
VPN	**V**irtual **P**rivate **N**etwork
NAT	**N**atwork **A**ddress **T**ranslation
SSL	**S**ecure **S**ocket **L**ayer
SSH	**S**ecure **SH**ell
MTA	**M**ail **T**ransfert **A**gent
MUA	**M**ail **U**ser **A**gent
MDA	**M**ail **D**elivery **A**gent
IMAP	**I**nteractive **M**ail **A**ccess **P**rotocol
POP3	**P**ost **O**ffice **P**rotocol 3
SMTP	**S**imple **M**ail **T**ransfer **P**rotocol 3
IP	**I**nternet **P**rotocole
UID	**U**ser **ID**entifier
GID	**G**roup **ID**entifier
CTMS	**C**onference **T**erminal **M**anagement **S**ystem
CA	**C**ertificat **A**utority
URL	**U**niform **R**essource **L**ocator

INTRODUTION GÉNÉRALE

Les technologies de l'information et de la communication représentent une révolution importante, qui a marqué la vie de l'humanité, elle apporte les conforts et le rapprochement des distances.

Parmi ces technologies, la messagerie électronique qui est parmi les services les plus utilisés et les plus répondu pour les entreprises et les individus dans la technologie de l'information et la communication, car, il optimise la communication, facile à utiliser et c'est un service gratuit et assez développé, ce qui le rend indispensable.

Dans le cadre de préparation, de notre projet fin d'études, spécialité Informatique, option, Administration et Sécurité des Réseaux, nous avons opté pour le thème, de mise en place d'un serveur de messagerie, afin de remédier aux problèmes de l'échange d'informations, au sein de notre organisme d'accueil, Bejaia Mediterranean Terminal, où nous avons effectué notre stage. Ces problèmes sont souvent lié par les moyens de communication utilisés. Dans le but de faciliter leurs taches, nous leurs avons suggéré des solutions.

En revanche, ce service est la cible des attaques, à cause du nombres d'informations qui sont échangées et l'importance qu'ils peuvent avoir. C'est la raison pour laquelle, il faut le sécuriser, pour la sécurité, il existe des mécanismes qui nous la garantissent.

Ce mémoire est organisé en quatre chapitres

Dans le ***chapitre 1***, nous présentons dans un premier temps un aperçu général sur les réseaux : leurs architectures, leurs principales caractéristiques. Dans un second temps, nous allons parler sur la sécurité des réseaux, et les mécanismes qui nous permettent de sécuriser un réseau local d'une entreprise.

Le ***chapitre 2*** présente l'organimse d'accueil et le cahier de charge.

Dans le ***chapitre 3***, sera consacré à la présentation d'une maniére théorique et détaillé des éléments importants de la messagerie éléctronique à savoir : protocole SMTP, protocole POP et protocole IMAP

Le ***chapitre 4***, quant à lui, sera consacré à la réalisation de notre projet, et les différentes étapes suivies, pour la mise en oeuvre et l'administration de notre serveur de messagerie .

Enfin, notre travail s'achève par une conclusion générale résumant les grands points qui ont été abordés ainsi que les perspectives que nous souhaitons accomplir prochainement.

CHAPITRE 1

GÉNÉRALITÉS

1.1 Introduction

Dans ce chapitre, nous allons illustrer certains termes en relation avec notre thème. Des notions de bases ainsi que des définitions qui nous aiderons à réaliser notre projet, dans ce chapitre nous aurons à mettre en avant la partie théorique afin d'aboutir à un résultat : la partie pratique. Mettre en place un serveur de messagerie repose sur les deux aspects à savoir une architecture réseau performante et cette performance s'introduit dans sa sécurité. Dans ce qui suit nous traiterons ces deux aspects.

1.2 Généralités sur les réseaux

Un réseau de communication est un ensemble d'équipements (ordinateurs, périphériques, etc) connectés entre eux par des liaisons filaires ou sans fil. L'objectif est de s'échanger des informations et partager des ressources matérielles et logicielles (imprimante, scanner,données, etc) [1].

1.2.1 Les supports de communication

Généralement, il existe deux grandes classes de support de communication :

- **Technologies filaires**

Les technologies filaires utilisées comme support de communication peut être classées en trois classes : câbles coaxiaux, câbles en paires torsadées et fibres optiques [3].

- **Technologies sans fil**

La technologie sans fil transfère les données au moyen d'ondes radio au lieu d'utiliser des câbles (l'Infrarouge, Wifi, Bluetooth) [4].

1.2.2 Les principaux types de réseaux

Nous distinguons différents types de réseaux (Figure 1.1) selon leur taille, leur vitesse de transmission et la nature des informations transmises :

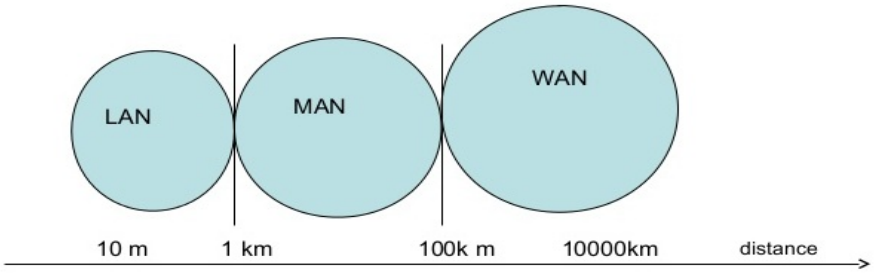

FIGURE 1.1 – Catégories des réseaux informatiques [33].

- **Les réseaux locaux (Local Area Network)**

Un réseau local (LAN) peut s'étendre de quelques mètres à quelques kilomètres et permet d'interconnecter des équipements d'une même entreprise. Il peut se développer sur plusieurs bâtiments et permet de satisfaire tous les besoins internes de cette entreprise.

- **Les réseaux métropolitains (Metropolitan Area Network)**

Un réseau métropolitain (MAN) interconnecte plusieurs lieux situés dans une même ville, par exemple les différents sites d'une entreprise ou d'une administration, chacun possédant son propre réseau local.

- **Les réseaux étendu (Wide Area Network)**

Un réseau étendu (WAN) couvre généralement une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent, voire de la planète entière. Ces réseaux reposent sur une infrastructure très étendue [2].

1.2.3 Les topologies des réseaux

La topologie décrit la manière dont les équipements réseau sont connectés entre eux. Nous distinguerons :

- Les topologies physiques : décrivant la manière dont les équipements sont reliés par des médias.

- Les topologies logiques : décrivant la manière dont les équipements communiquent [4].

1.2.4 Internet

Internet est un système de communication qui permet aux ordinateurs autour du monde de se communiquer et de s'échanger l'information entre eux. Cette communication entre ordinateurs permet plusieurs possibilités et offre une masse d'informations plus importante dans les différents domaines comme la médecine, la science et la technologie [5].

1.2.5 Intranet

Le concept d'Intranet consiste à appliquer le concept d'Internet à l'intérieur de l'entreprise. C'est un réseau Internet propre à l'entreprise, basé sur la technologie d'Internet et qui n'est pas ouvert aux utilisateurs externes [5].

1.2.6 Architecture réseau

Il existe deux types d'architecture réseaux : l'architecture client/serveur et l'architecture peer to peer ou poste à poste.

- **client/serveur**

L'architecture client/serveur désigne un mode de communication entre plusieurs ordinateurs d'un réseau qui distingue un ou plusieurs clients du serveur : chaque logiciel client peut envoyer des requêtes à un serveur. Un serveur peut être spécialisée en serveur d'applications, de fichiers, de terminaux, ou encore de messagerie électronique. Le modèle client/serveur, est un modèle d'architecture applicative où les programmes sont répartis entre processus clients et serveurs communiquants par des requêtes avec réponses. Le client, envoie des requêtes au serveur, ce dernier les traite et renvoie des réponses au client. Il existe de différentes architectures client/serveur, parmi ces architectures [6] :

- **L'architecture client/serveur à deux niveaux :**

Cette architecture (Figure 1.2) caractérise les systèmes clients/serveurs pour lesquels le client demande une ressource et le serveur la lui fournit directement, en utilisant ses propres ressources [6].

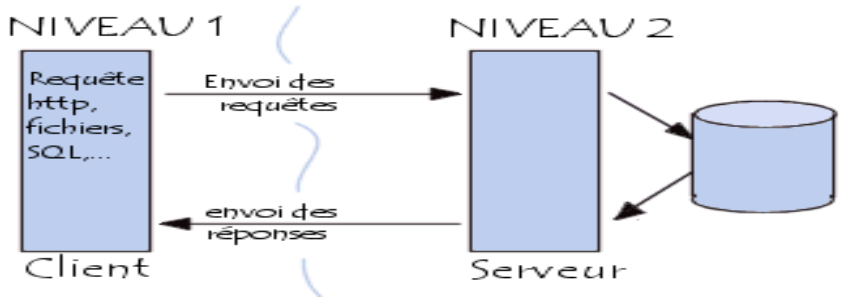

FIGURE 1.2 – Architecture à deux niveaux [34].

- **L'architecture client/serveur à trois niveaux :**

Dans cette architecture (Figure 1.3) un niveau intermédiaire se fait place entre les deux niveaux de l'architecture précédente [6] :

- Le client (niveau un) : demandeur de ressource,
- Le serveur d'application (niveau deux) : est chargé de fournir la ressource mais qui fait appel à un autre serveur pour certaines demandes de ressources. Le niveau deux lui-même est le client d'un serveur de base de données,
- Le serveur de base de données (niveau trois) : fournit les ressources au premier serveur [6].

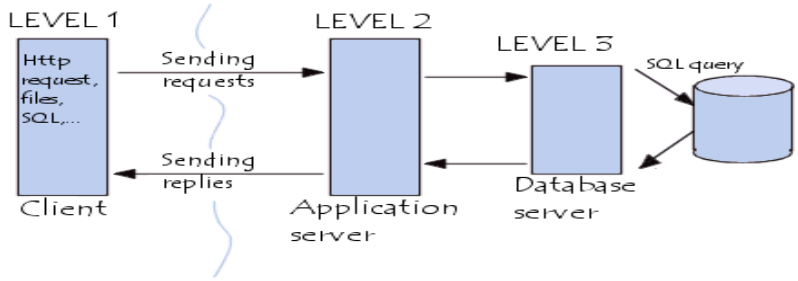

FIGURE 1.3 – Architecture à trois niveaux [34].

- **Architecture Peer to Peer**

Cette architecture (Figure 1.4) est en fait un réseau sans serveur constitué de deux ou plusieurs ordinateurs. Ainsi chaque ordinateur joue à la fois le rôle de serveur et de client, cela signifie que chacun de ces ordinateurs du réseau est libre de partager ses ressources [6].

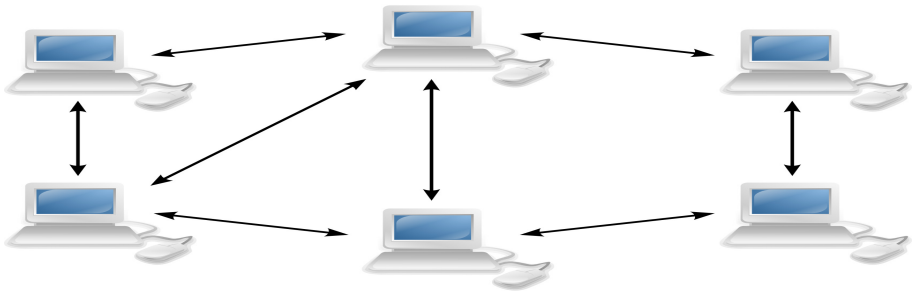

FIGURE 1.4 – Architecture Peer to Peer [34].

1.2.7 Modéles de communication réseau

Le transport des données d'une extrémité à une autre d'un réseau, nécessite une architecture logiciel qui contrôle des paquets dans le réseau. Il existe deux grandes architectures qui sont actuellement dans le marché mondial des réseaux [1] :

- **Le Modéle OSI**

Le modéle OSI(Open Systems Interconnection) (Figure 1.5) est un modéle de communication entre odinateurs qui décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions. Le Modéle consiste en une architecture en sept couches [1] :

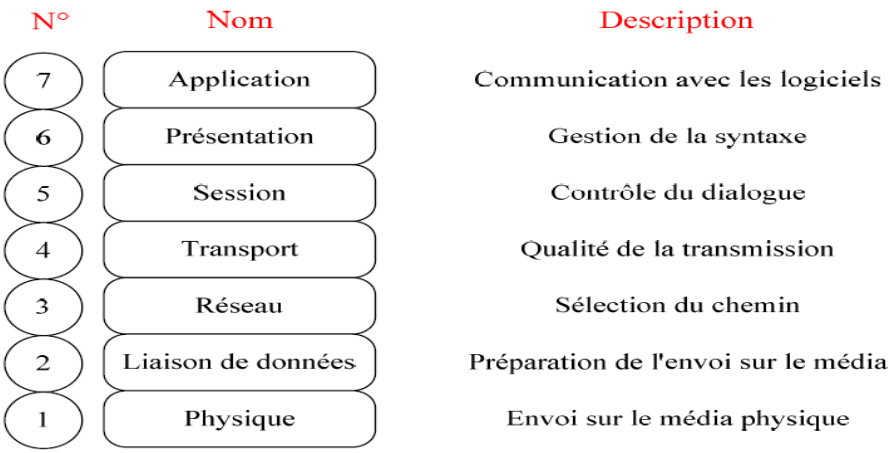

FIGURE 1.5 – Les sept couches du modéle OSI.

- **Le Modéle TCP/IP**

Les modèles (Figure 1.6) de communication entre utilisateurs réseau le plus répandu est le modèle TCP/IP (Transmission Control Protocol / Internet Protocol). TCP/IP est plus qu'un modèle de conception théorique, c'est sur lui que repose le réseau Internet actuel, qui est un modèle en quatre couches [1] :

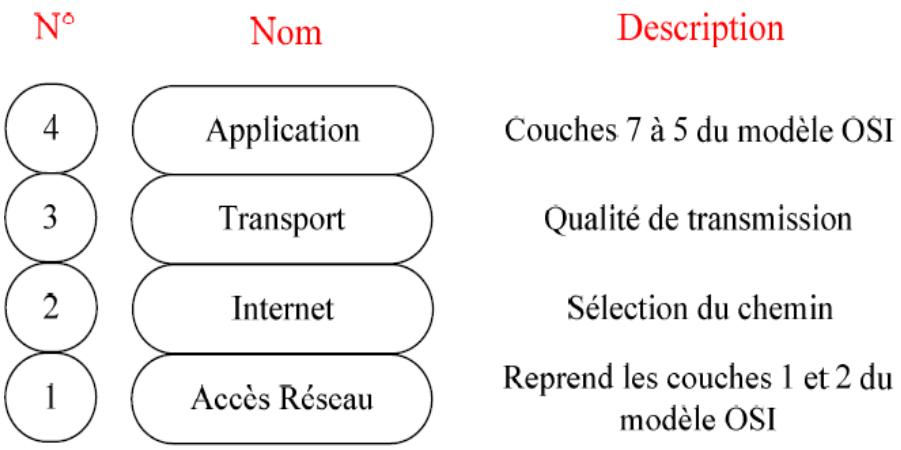

FIGURE 1.6 – Les quatre couches du modéle TCP/IP.

1.2.8 Protocoles de routage

Un protocole de routage est un programme qui définit l'ensemble des chemins que peuvent empreinter les informations transférées dans un réseau depuis la station émettrice jusqu'à destination, et pour cela il existe deux types de protocoles de rourage, statique et dynamique [7].

1.2.9 Les serveurs

Un serveur est un dispositf informatique matériel ou logiciel qui a pour mission répondre au déffirentes requêtes des clients. Il existe d'autres, offrant des services internet, ceux-ci possèdent des numéros de ports propres à eux, citant à titre d'exemple :

- Le port 21 (service ftp),
- Le port 22 (service ssh),
- Le port 23 (le service telnet),
- Le port 25 (service smtp),
- Le port 80 (service http).

Il existe d'autres serveurs qu'on appelle serveurs locaux, ils sauvegardent les informations internes à l'entreprise et offrent des services aux utilisateurs de cette dernière [8].

- **Serveur Messagerie**

Un serveur de messagerie électronique est un logiciel qui est connecté à Internet, permet à ses utilisateurs d'envoyer et de recevoir des courriers électroniques. Pour se connecter au serveur de messagerie, l'utilisateur a recours à un logiciel client, capable de gérer l'adressage (ou envoi) du courriel mais aussi sa réception [9].

Nous allons détailler le serveur de messagerie, son fonctionnement et les protocoles utilisé dans le chapitre trois, qui est le but de notre projet.

- **Serveur DHCP**

Un serveur DHCP (Figure 1.7)est un serveur qui délivre dynamiquement des adresses IP aux ordinateurs qui se connectent sur le réseau. Le processsus d'attribution se déroule en quatre phases : [10].

- Découverte (DISCOVER) : Le client envoie une demande de configuration sur le réseau en diffusion, plusieurs serveurs DHCP peuvent être en écoute et donc recevoir la demande,
- Offre (OFFER) : Tous les serveurs DHCP répondent au client en lui faisant une offre,
- Demande (REQUEST) : Le client répond à un serveur parmi ceux qui ont offert en lui précisant qu'il accepte l'offre proposée,
- Accusé de reception(ACK) : Le serveur DHCP confirme le bail avec sa durée et les options DHCP associées, et met à jour sa table des addresses IP allouées [8].

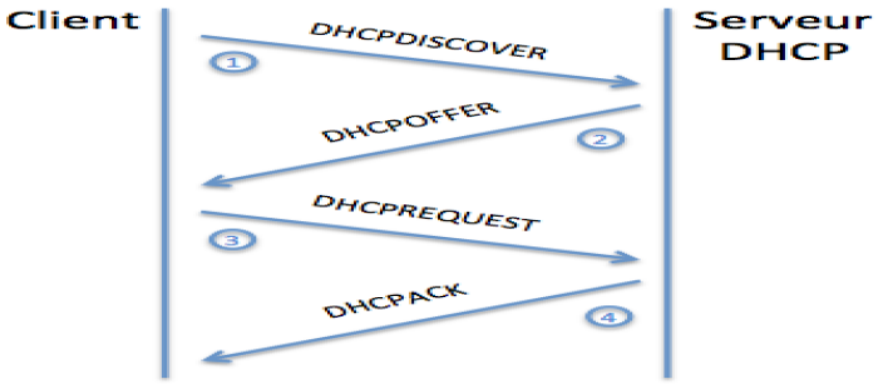

FIGURE 1.7 – Fonctionnement de DHCP [35].

- **Serveur DNS**

DNS est le service de résolution de nom d'hôte, il permet d'associer un nom d'une machine à une adresse IP. Nous distinguons deux résolutions :

- **Résolution itérative**

Le serveur (Figure 1.8) sollicité fournit en réponse le nom d'un autre serveur DNS à contacter pour avancer dans la résolution [8].

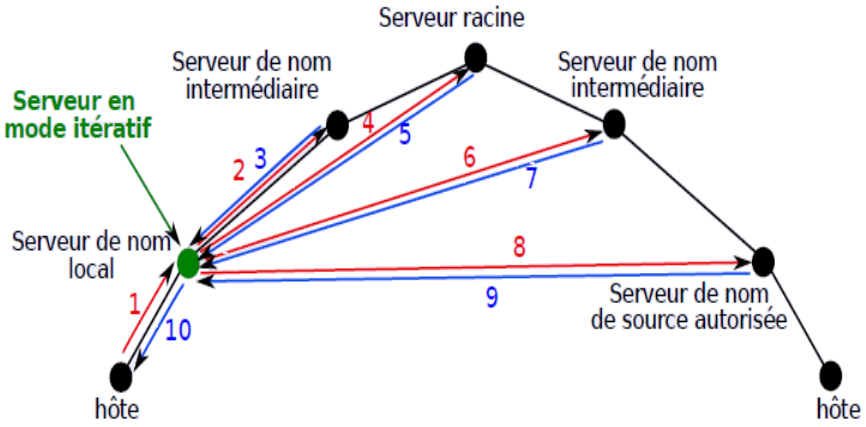

FIGURE 1.8 – Résolution itérative [36].

- **Résolution récursive**

la machine (Figure 1.9) qui demande la résolution contacte un serveur DNS et attend que ce dernier retourne la réponse désirée [8].

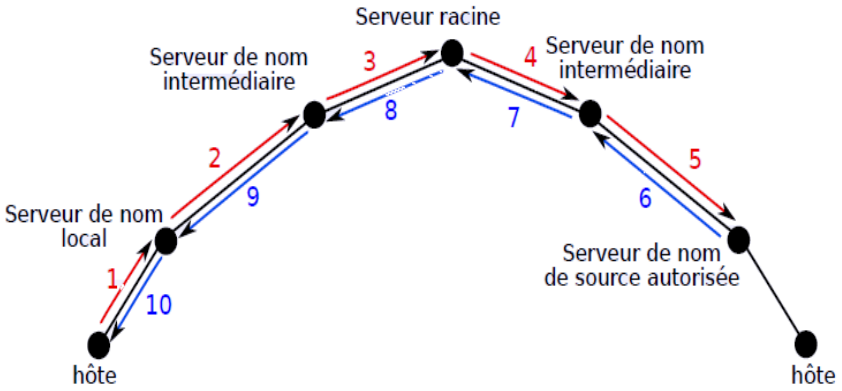

FIGURE 1.9 – Résolution récursive [36].

1.3 Sécurité dans les Réseaux

La sécurité des réseaux devient une problématique essentielle des entreprises, il est important de définir la politique et le mécanisme de sécurité pour garder leurs informations en confidentialité, il y'a donc des objectifs à assurer et des étapes a suivre.

- **Les objectifs à assurer :**

Nous distinguons généralement cinq principaux objectifs de sécurité :

- Disponibilité : elle consiste à garantir l'accès à un service ou à une ressource,
- Intégrité : elle consiste à s'assurer que les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle),
- Confidentialité : consiste à assurer que seules les personnes autorisées aient accès aux ressources échangées [12],
- Authentification : elle consiste à assurer l'identité d'un utilisateur, c'est-à dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être,
- Non répudiation : elle consiste à garantir qu'aucun des correspondants ne pourra nier la transaction [12].

1.3.1 Les menaces

Les menaces peuvent également être classées en deux catégories, soit elles ne changent rien (menaces passives) ou elles perturbent effectivement le réseau (menaces actives).

- **menaces passives :**

Elles consistent essentiellement à copier ou à écouter l'information sur le réseau, elles nuisent à la confidentialité des données. Dans ce cas, celui qui prélève une copie n'altère pas l'information elle même [13].

- **menaces actives :**

Elles sont de nature à modifier l'état du réseau [13].

1.3.2 Les logiciels malveillants

Un logiciel malveillant est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur. Plusieurs types de logiciels malveillants ont été proposées. Nous citons les plus répandus :

- **Virus**

Un virus est un morceau de programme informatique malicieux, conçu et écrit pour qu'il se reproduit. Cette capacité à se répliquer, peut toucher votre ordinateur, sans votre permission et sans que vous le sachiez. En termes plus techniques, le virus classique s'attachera à un de vos programmes exécutables et se copiera systématiquement sur tout autre exécutable que vous lancez [14].

- **Vers**

Un ver est un type de virus particulier qui se propage dans le réseau. Les vers contrairement aux virus, une fois implantés et activés dans un ordinateur, ils sont des programmes capables de se propager d'un ordinateur à un autre via le réseau, sans intervention de l'utilisateur et sans exploiter le partage de fichiers [14].

- **Cheval de Troie**

Un cheval de Troie (Trojan horse) est un programme qui exécute des instructions sans l'autorisation de l'utilisateur. Ces instructions sont généralement nuisibles à l'utilisateur, et qui une fois installé sur un ordinateur y effectue des actions cachées. Le cheval de Troie contrairement au ver ne se réplique pas [14].

- **Spam**

Le spam est une vraie problématique. Il encombre les résultats de recherche ce qui gène l'utilisateur. Un spam peut être définit comme étant un email anonyme, non sollicité, indésirable et envoyé en grand nombre de façon automatique sans l'accord de son destinataire [14].

- **Porte dérobée**

La porte dérobée est un moyen de contourner les mécanismes de contrôle d'accès. Il s'agit d'une faille du système de sécurité due à une faute de conception accidentelle ou intentionnelle [14].

1.3.3 Mécanismes de la sécurité

À cause des menaces provenant des logiciels malveillants, Il faut mettre en place des mécanismes pour assurer la confidentialité, l'intégrité et la disponibilité des services. Parmi ces mécanismes, on peut citer :

- **Cryptage**

Le chiffrement (Figure 1.10) est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de chiffrement et de déchiffrement. Ce principe est généralement lié au principe d'accès conditionnel [15].

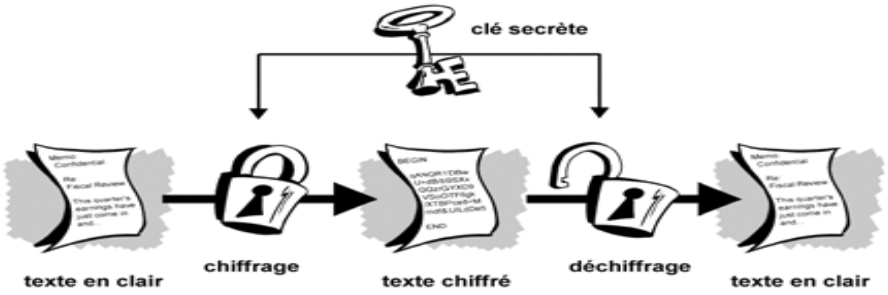

FIGURE 1.10 – Fonctionnement de chiffrement [37].

- **Par-feu**

Par-feu (Figure 1.11) un ensemble de différents composants matériels et logiciels qui contrôlent le trafic intérieur/extérieur selon une politique de sécurité. Il permet d'une part de bloquer des attaques ou connexions suspectes d'accéder au réseau interne. D'un autre côté, un firewall sert dans de nombreux cas également à éviter la fuite non contrôlée d'informations vers l'extérieur. Il propose un véritable contrôle sur le trafic réseau de l'entreprise, il permet donc d'analyser, de sécuriser et de gérer le trafic réseau [15] .

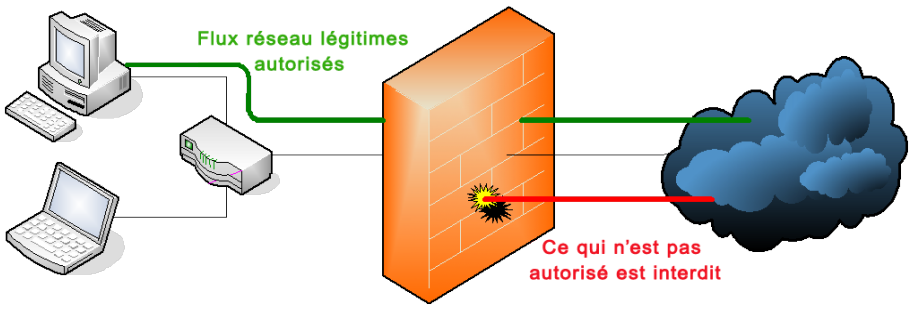

FIGURE 1.11 – par-feu [38].

- **Antivirus**

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants. Ceux-ci peuvent se baser sur l'exploitation de failles de sécurité, mais ils peuvent également s'agir de programmes modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur de l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur [16].

- **VPN**

Dans les réseaux informatiques , le réseau privé virtuel (Figure 1.12)est une technique permettant aux postes distants de communiquer de manière sûre, tout en empruntant des infrastructures publiques (internet). Un VPN repose sur un protocole, appelé protocole de tunnelisation, c'est-à-dire un protocole permettant aux données passant d'une extrémité à l'autre du VPN d'être sécurisées par des algorithmes de cryptographie [17].

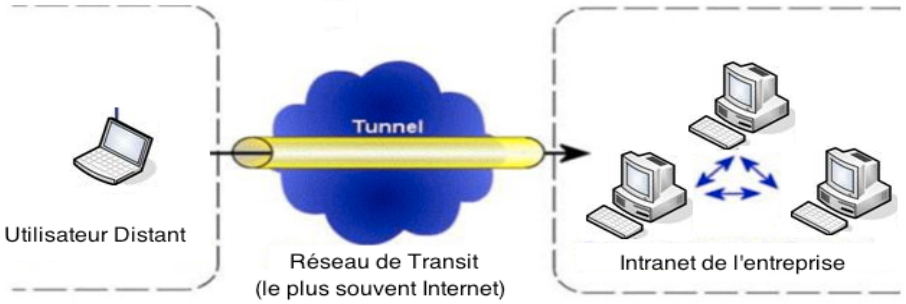

FIGURE 1.12 – Principe de VPN [39].

- **NAT**

Le NAT permet d'utiliser des adresses n'ayant pas de signification globale (par exemple des adresses privées, non routable) pour se connecter à travers l'Internet en traduisant celles-ci en adresses globales routables. On distingue deux types de NAT, le NAT statique et le NAT dynamique [18].

- **Proxy**

Le proxy est un autre moyen de sécurité, utilisé comme une passerelle entre le réseau privé et le réseau publique, il est généralement utilisé dans les systèmes institutionnels ou d'entreprise [18]. Le proxy a trois fonctions principales :

- Caching : stocke les pages demandés par les clients et les redistribuer en cas de demande ;

- Traking : création des journaux de connexion où se trouvent les informations du client ;

- Filtring : filtrage des requêtes et réponses.

1.4 Conclusion

Dans ce chapitre, nous avons cité les différents concepts des réseaux. Une introduction aux réseaux informatique, support de communication, les topologies, les protocoles de routage et le courier éléctronique et nous avons présenté les différents problémes majeurs de sécurité, les objectifs, les logiciels malveillants. Nous avons terminé ce chapitre avec les principaux composants de la sécurité d'un réseau interne de l'entrprise.

Dans le chapitre suivant, nous présenterons, BMT (Bejaia Mediterranean Terminal), notre organisme d'accueil.

CHAPITRE 2

PRÉSENTATION DE L'ORGANISME D'ACCUEIL

2.1 Introduction

Notre projet consiste à mettre en place un serveur de messagerie, pour la gestion des courries au sein de l'entreprise BMT (Bejaia Mediterranean Terminal). Pour cela, il s'avère nécessaire de présenter d'abord cet organisme, ses différentes structures, ses missions ainsi que ses objectifs afin de comprendre ses activités principales.

2.2 Historique de l'entreprise BMT

BMT est une entreprise prestataire de services spécialisés dans le fonctionnement, l'exploitation, et la gestion du terminal à conteneurs. Pour atteindre son objectif, elle s'est dotée d'un personnel compétant particulièrement formé dans les opérations de gestion du terminal. Elle dispose d'équipements d'exploitation des plus perfectionnés pour les opérations de manutention et d'acconage afin d'offrir des prestations de services de qualité, d'efficacité et de fiabilité en des temps records et à des coûts compétitifs. BMT offre ses prestations sur la base de 24h/7j.

Le niveau de la technologie mis en place et la qualité des infrastructures et équipements performants (portiques de quai, portiques gerbeurs) font aujourd'hui du port de Bejaia et de BMT, le premier terminal moderne d'Algérie avec une plate-forme portuaire très performante.

2.3 Structure de l'entreprise

L'entreprise de Bejaïa est divisé en plusieurs directions (Figure 2.1) :

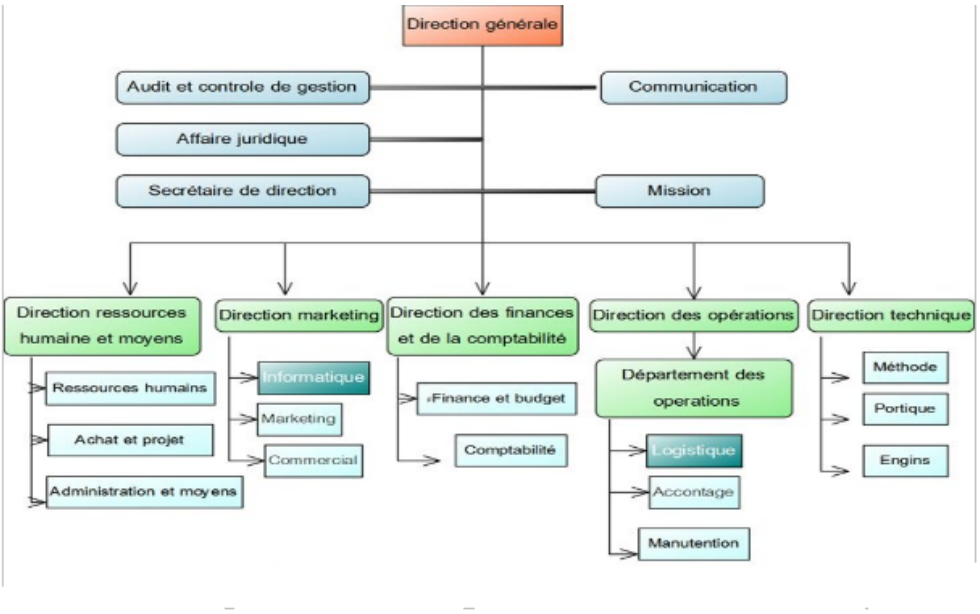

FIGURE 2.1 – Organigramme géneral de BMT.

- **Direction générale (DG)**

A sa tête, le directeur général qui gère l'entreprise. Il a le pouvoir de décision, d'administrer l'entreprise et d'assigner des directives pour les différentes structures.

- **Direction des ressources humaines (DRH)**

La direction des ressources humaines posséde plusieurs services :

- **Service personnel :**

Son rôle est de mettre en oeuvre des systèmes de gestion intégrés à la stratégie de l'entreprise, traduisant une adéquation entre les impératifs économiques et les attentes du personnel. Pour cela, la véritable importance de cette structure réside dans la recherche du meilleur potentiel et le conserver, en lui offrant les meilleurs conditions (salaire, climat de travail et environnement, formation).

- **Service des moyens généraux :**

Chargé des achats et de la gestion des stocks de l'entreprise.

- **Service hygiène et sécurité :**

Assure la sécurité de la marchandise, du parc à conteneurs et la propreté de l'entreprise et de son environnement.

- **Direction des opérations (DO)**

Assure la planification des escales, de parc à conteneurs et la planification des ressources (humaines et matérielles).

Elle prend en charge les opérations de manutentions, comme la réception des navires porte conteneurs et leurs chargements et déchargements. De plus, elle suit les opérations de l'acconage tel que : le suivi des livraisons, dépotages, mise à disposition des conteneurs vides, traitement des conteneurs frigorifiques.

- **Direction marketing (DM)**

Veille à la marque de l'entreprise en se préoccupant en permanence d'entretenir des relations avec les clients. Elle vise à faire connaître ses missions, ses programmes, ses orientations et ses performances auprès de ses clients. En outre, elle amène son environnement externe à prendre conscience de l'importance des démarches qu'elle entreprend, dans le développement et l'amélioration de la qualité de ces services. Elle se compose de deux services :

- **Service commercial :**

Suit la facturation, la gestion de portefeuille client et le recouvrement des créances.

- **Département informatique :**

Assure le bon fonctionnement du CTMS (Conference Terminal Management System), la maintenance du parc informatique de l'entreprise et le développement de nouvelles applications aux différentes structures.

- **Direction des finances et de comptabilité (DFC)**

Procède à l'enregistrement de toutes les opérations effectuées par l'entreprise au cours de l'année. Elle est constituée de deux services :

- **Service de comptabilité :**

Procède au contrôle et l'enregistrement de toutes les factures d'achat, de présentation et d'investissement.

- **Service des finances :**

Procède au règlement de toutes les factures d'un coté, et de l'autre coté à l'encaissement de toutes les créances de l'entreprise émis à la banque de l'autre coté.

- **Direction technique (DT)**

Assure une maintenance préventive et curative des engins du parc à conteneurs.

2.3.1 Missions et objectifs de BMT

L'activité principale de BMT est le suivi, la gestion et l'exploitation du terminal à conteneurs.
Elle a pour mission et objectifs de :

- Traiter dans les meilleures conditions de délais, de coûts et de sécurité, l'ensemble des navires porte conteneurs et des conteneurs.
- La manutention sur navire aussi bien le chargement et le déchargement des conteneurs et leurs entreposages dans les zones de stockage.
- Le service d'acconage sur les aires spécialisées ainsi que leurs livraisons.
- Le déchargement des céréales selon les capacités de BMT. Pour se faire, elle est dotée d'équipements performants et de systèmes informatisés CTMS liés à la logistique pour pouvoir à la fois offrir des services de qualité, avec efficacité et fiabilité, ainsi que de satisfaire les différents besoins des clients.
- Faire du terminal à conteneurs de BMT une infrastructure moderne et même de répondre aux exigences les plus sévères, en matière de qualité, dans le traitement des conteneurs.
- La mise à disposition d'une nouvelle technologie dans le traitement des conteneurs pour :
  - Un gain de productivité.
  - Une réduction des coûts d'escale.
  - Une fiabilité de l'information.
  - Un meilleur service.
  - Sauvegarder la marchandise des clients.
  - Faire face à la concurrence nationale et internationale.
  - Propulser le terminal au stade international.
  - Gagner des parts du marché.
- La création et la gestion d'un centre de formation.

2.4 Cahier des charges

2.4.1 Problématique

Au sein de BMT, de nombreuses informations, fichiers, documents sont échangés entre le personnel de différents services. Certains problémes ont été soulevé :

- Utilisation du fax entre le personnel, pour s'échanger l'information, ce qui engendre une perte de temps,
- Fusion des documents reçus/envoyés au niveau national et local, occasionnée par l'utilisation d'une boite au lettre qui n'est pas propre à l'entreprise,
- Nombres impotatnts d'archives a stocké pour le personnel,
- Difficulté de chercher les documents papiers archivé ce qui cause une perte de temps.

2.4.2 Suggestions

Aprés concertation et discution avec l'ingérieur informatique de BMT, pour remédier aux problémes soulevés ci-dessus, nous avons proposé de :

- Mettre en place un serveur de messagerie, qui sera propre à l'entreprise de BMT de Béjaïa pour une meilleure gestion,
- Sécuriser le serveur,
- Faciliter l'administration du serveur de messagerie.

2.4.3 Objectifs

Nous avons pour but, d'atteindre les objectifs suivants :

- Faciliter la communication entre le personnel,
- Le message électronique peut être archivé et imprimé,
- Le courrier électronique est peu couteux.

2.5 Conclusion

Dans ce chapitre, nous avons présenté l'entreprise BMT pour pouvoir comprendre le fonctionnement de ces déffirentes structures, et nous avons spécifié leur besoins dans le cahier de charge, ce qui engendre la nécessité de mettre en oeuvre un serveur de messagerie électronique. Dans le chapitre prochain, nous allons développer et détailler les caractéristiques d'un serveur de messagerie qui sera utile à la réalisation de notre projet.

CHAPITRE 3

SERVEUR DE MESSAGERIE

3.1 Introduction

Nous avons vu dans le chapitre précedent, la nécessité de mettre en place un serveur de messagerie pour l'entreprise BMT. Dans ce qui suit, nous allons voir plus en dètail les protocoles utilisés dans les serveurs de messagerie ainsi leur architecture et quelques protocoles de sécurité de courrier électronique.

3.2 Courrier électronique

Le courrier électronique est une application très importante et plus utiles dans le réseaux. Elle présente un moyen de communication rapide et moins chér. Le courrier électronique est un outil de plus en plus important dans la communication aussi bien interne qu'externe, il est devenu la solution d'archivage des données dans de nombreuses entreprises [22].

3.2.1 Serveur de messagerie

Un serveur de messagerie est un serveur servant à la réception et à l'envoie de courrier à travers le réseau. Cela permettra à n'importe qui d'aller cherchez son courrier sur le serveur, depuis n'importe quelle station de travail [22].

3.2.2 L'architecture logicielle de la messagerie

L'architecture logicielle de la messagerie (Figure 3.1) est constituée de trois entités distinctes qui coopèrent et communiquent par le bais de protocoles bien défini afin d'assurer un service entre utilisateurs [22].

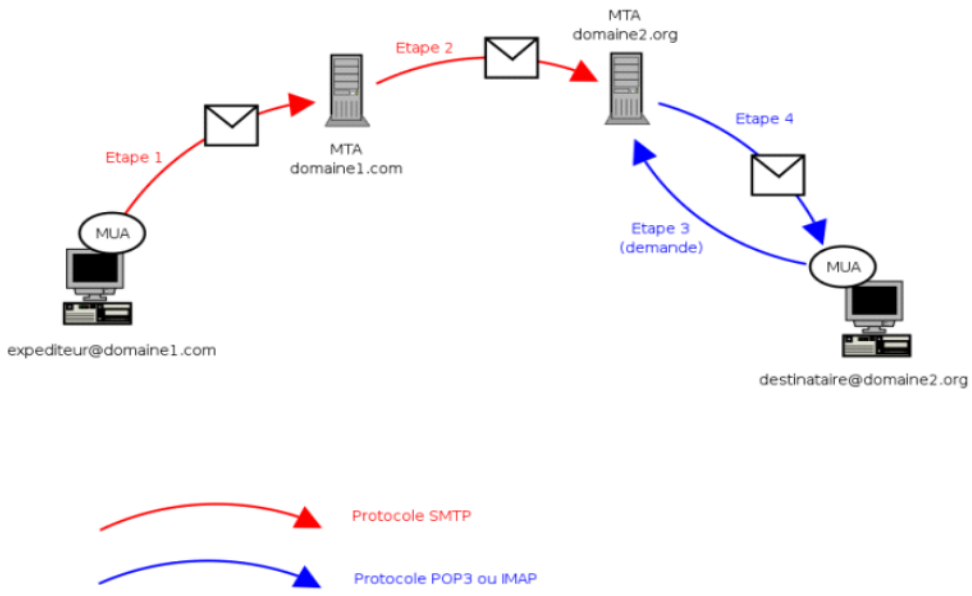

FIGURE 3.1 – Description de l'architecture de fonctionnement de la messagerie.

- **Mail Transfer Agent (MTA)**

Ce logiciel est situé sur chaque serveur de messagerie. C'est lui qui s'occupe de livrer un message envoyé par un utilisateur donné au récepteur. Comme exemple de logiciel assurant ce rôle : Sendmail (l'un des plus utilisées), Postfix (promis à remplacer Sendmail) et Exchange (Microsoft) [8].

- **Mail User Agent (MUA)**

MUA (Mail User Agent), est le programme utilisé par le client pour composer, envoyer et recevoir les messages. MUA est un logiciel client pour le MTA (lors d'un envoi d'un courrier) et un client pour le MDA (lors d'une réception d'un courrier). Comme exemple, nous avons Outlook (MS) et Thunderbird (Mozilla). Avec l'apparition du web, des clients web légers aussi sont utilisées : Roundcube, Squirrelmail ou ceux qu'on trouve sur les hébergeurs gratuits de courrier comme Yahoo, Hotmail et Gmail [8].

- **Mail Delivery Agent (MDA)**

Les MDA servent à récupérer le courrier par un lecteur de courrier en ligne ou hors ligne. Ce serveur est aussi appelé Serveur de courrier entrant. Comme exemple de MDA, nous avons Dovecot, maildrop-Courrier, IMAP, POP3, (etc) [8].

3.2.3 L'adresse électronique

L'adresse électronique est une désignation conventionnelle permettant l'identification d'un utilisateur du courrier électronique et l'acheminement des messages qui lui sont destinés. Cette adresse permet d'idenfier une boite aux lettres de façon unique. L'adresse électronique peut être constituée des éléments suivants :

- Le nom d'utilisateur,
- Le symbole séparateur @, dit ' a commercial' ,
- Le nom de domaine [19].

Ces adresses prennent toujours la forme suivante : nom-utilisateur@nom-de-domaine.

Il existe de différents types d'utilisations d'adresses électroniques :

- Adresse personnelle : adresse personnelle d'un utilisateur associée à une adresse mail nominative qui désigne un individu. Ces adresses sont de la forme prenom.nom@medbejaia.dz ;
- Adresse fonctionnelle : adresse fonctionnelle métier associée à une adresse mail qui désigne une structure matérielle, immatérielle (service, association ...) ou une fonction. Elle n'est pas la propriété d'un utilisateur et par conséquent elle peut être transmise lors d'un changement de personnel ou de responsabilité. Exemple : chef.service@medbejaia.dz ;
- Adresse partagée : adresse partagée utilisable par plusieurs utilisateurs. Exemple : diffuse@medbejaia.dz [20].

3.2.4 Structure d'un courrier électronique

La structure d'un courrier électronique possède fondamentalement deux parties :

- **L'enveloppe**

L'enveloppe est un ensemble de lignes contenant les informations de transport telle que l'adresse de l'expéditeur, l'adresse du destinataire ou encore l'horodatage du traitement du courrier par les serveurs intermédiaires nécessaires aux serveurs de transports (MTA) faisant office de bureaux de tri postal. L'enveloppe commence par une ligne From et elle est modifiée par chaque serveur intermédiaire. Ainsi, grâce à l'enveloppe, il est possible de connaître le chemin parcouru par le courrier et le temps de traitement par chaque serveur.

- **Le message**

Le message est composé de corps du message contenant le message séparé de l'en-tête par une ligne vide [21] et de champs d'en-tête qui est un ensemble de lignes décrivant les paramètres du message, tels que l'expéditeur, le destinataire, la date, etc. Chaque en-tête possède la forme suivante :

- From : adresse électronique de l'expéditeur ;
- To : adresse électronique du destinataire ;
- Date : date de création du courrier.

Il peut contenir les en-têtes facultatifs suivants :

- Received : diverses informations sur les serveurs intermédiaires et la date de traitement du message associée ;
- Reply-To : Une adresse pour la réponse ;
- Subject : Le sujet du message ;
- Message-ID : un identifiant unique du message.

3.2.5 Les serveurs et les clients de la messagerie électronique

Nous distinguons plusieurs seveurs et clients de la messagerie :

- **Les serveurs de messagerie**

Il existe plusieurs serveurs de messagerie életroniques :

* **Sendmail** : est un serveur de messagerie dont le code source est ouvert. Il se charge de la livraison des messages électroniques et possède les atouts suivants :

Les avantages

- Sendmail est très puissant et résiste beaucoup à la grande charge,
- Code source libre,
- Multi plate-forme de type UNIX (MAC OS, GNU/LINUX).

Inconvénients

- Sendmail est difficile à configurer car son architecture est vieille,
- Lent et très complexe avec une maintenance difficile [22].

* **Zimbra** : Zimbra est un logiciel serveur collaboratif qui permet à ses utilisateurs de stocker, organiser et partager leurs documents, contacts, courriels. Citant quelques avantages :

Les avantages

- Accessible de partout : du bureau, de chez soi,
- Toutes les fonctions disponibles au sein de la même interface : emails, agendas, carnets d'adresses, fichiers, tâches, messagerie instantannée [23].

Inconvénients

- Pas de mode "hors ligne",
- Création des scripts [22].

* **Qmail** : Est un serveurs de messagerie les plus performant, les plus surs et les plus stables. Il représente un haut niveau de sécurité grâce à sa structure. Qmail est un outil difficile à installer et à maîtriser [22].

* **Microsoft Exchange Server** : Microsoft Exchange est un logiciel de messagerie qui permet de gérer les Mails, les Calendriers et les Contacts. Microsoft Exchange permet l'accés en mobilité et assure une bonne sécurité d'antispam, parmi ces inconvéniants : un code souce n'est pas libre et uni plate-forme (Microsoft Windows) [22].

* **Postfix** : Postfix est un serveur libre de messagerie électronique développé à l'origine comme une alternative, plus simple et plus sécurisée, à sendmail. Postfix ne posséde pas des inconvénients majeurs [22].

Les avantages

- Il est adapté pour les grandes entreprises et facile à installer et à configurer ,
- Maintenance aisée,
- Sécurisé avec anti Spam et multi plate-forme,
- Codes sources libres et gratuit,
- Accessible en mobilité.

* **Postfixadmin** : est une interface web pour postfix, développé en php permettant la création et la gestion des mots de passes et l'administration de nos domaines et de nos utilisateurs dans le domaine, stockés au sein d'une base de données mysql.

* **Dovecot** : Dovecot est un serveur pop3 et imap pour la récupérations des courriers éléctroniques dans les boîtes aux lettres des utilisateurs. Dovecot est une excellente alternative pour la mise en place de petites ou grandes structures. Dovecot a les caractéristiques suivantes : Rapide, simple à installer, il ne nécessite pas une charge d'administration extraordinaire et utilise très peu de mémoire [31].

* **Cyrus** : Cyrus est un serveur de messagerie électronique (MDA) créé dans un objectif de fiabilité et d'extensibilité optimales, utilisé essentiellement pour gérer de très grandes quantités de comptes de courrier électronique. Cyrus permet de consulter ses emails par POP3 et IMAP [32].

- **Les clients de messagerie**

Un client de messagerie est un logiciel permettant de lire et d'envoyer des courriels. Il existe deux méthodes pour envoyer ou recevoir des courriers électroniques :

- **Le client de messagerie** : logiciel à installer sur son ordinateur et à configurer, prenant quelques exemples : Thunderbird, Outlook, Zimbra Desktop, etc.

- **Le webmail** : site web qui permet de gérer son courrier par intermédiaire d'une interface web. Pour accéder à votre courrier, il suffit de vous authentifier. Exemple de webmail : Squirrelmail, Roundcube, web mail de Zimbra, etc [24].

3.2.6 Protocoles de courrier électronique

Les protocoles de courrier électronique permettent à différents ordinateurs exécutant souvent différents systèmes d'exploitation et utilisant des programmes de messagerie électroniques différents, d'envoyer et de recevoir des emails. Les protocoles présentés ci-dessous plus fréquemment utilisés pour le transfert de courrier électronique entre systèmes.

- **Protocoles de transfert de courrier électronique**

La livraison de courrier d'une application cliente au serveur et d'un serveur d'origine à un serveur de destination est traitée par le protocole nommé Simple Mail Transfert Protocol (SMTP).

- **SMTP** : est basé sur le TCP (port 25). L'objectif primaire de SMTP consiste à transférer le courrier électronique entre les serveurs de messagerie. Toutefois, il a également une importance critique pour les clients de messagerie. Afin d'envoyer un email, le client envoie le message électronique à un serveur de messagerie sortant, qui à son tour contacte le serveur de messagerie de destination pour la livraison du message. Dans de telles circonstances, il est nécessaire de spécifier un serveur SMTP lors de la configuraton d'un client de messagerie [25].

- **Protocoles d'accès au courrier**

Pour récupérer le courrier électronique stocké sur les serveurs de messagerie, les applications client de messagerie utilisent deux protocoles primaires : Post Office Protocol (POP) et Internet Message Access Protocol (IMPA). Contrairement à SMTP, ces deux protocoles exigent des clients qui se connectent de s'authentifier au moyen d'un nom d'utilisateur (aussi appelé identifiant) et d'un mot de passe [25].

- **POP** : Le protocole POP permet comme son nom l'indique d'aller récupérer son courrier sur un serveur distant (le serveur POP, port 110). Il est nécessaire pour les personnes n'étant pas connectées en permanence à Internet afin de pouvoir consulter les mails reçus hors connexion [25].

- **IMAP** : Le protocole IMAP est utile tout particulièrement pour les utilisateurs accédant à leur courrier électronique au moyen d'ordinateurs multiples. Ce protocole est également pratique pour les utilisateurs se connectant au serveur de messagerie par le biais d'une connexion lente, car seule l'information d'en-tête du message est téléchargée jusqu'à ce qu'il soit ouvert, économisant ainsi la largeur de la bande. En outre, l'utilisateur peut également supprimer des messages sans devoir les lire ou les télécharger [25].

3.3 Sécurité de la messagerie

Dans les entreprises, la messagerie électronique est de plus en plus utilisée et elle est devenue une application Internet indispensable. Parce que la messagerie est un moyen de communication sensible, sa sécurité et sa disponibilité sont des préoccupations légitimes des entreprises.

3.3.1 Les menaces des serveurs de messagerie

Un serveur de messagerie peut avoir des risques menaçant sa sécurité, lesquels nous les citons :

- **Perte d'un e-mail** : la perte d'un e-mail au cours de sa transmission ou la disparition d'un message reçu.

- **Perte de confidentialité** : la perte de confidentialité peut être provoquée par différents événements : une divulgation accidentelle de mot de passe, espionnage des messages lors de la transmission sur réseau local.

- **Perte d'intégrité** : la perte d'intégrité peut également parvenir des modifications ou ajouts volontaires effectués au niveau du serveur de messagerie [26].

3.3.2 Les protocoles de sécurité des serveurs de messagerie

Nous présentons deux protocoles de sécurité d'un serveur de messagerie :

- **Le protocole SSH**

Le protocole SSH il s'agit d'un protocole permettant à un client (un utilisateur ou bien même une machine) d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des courriers ou des fichiers de manière sécurisée. Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau.

- **Fonctionnement de SSH**

L'établissement d'une connexion SSH se fait en plusieurs étapes : Dans un premier temps le serveur et le client s'identifient mutuellement afin de mettre en place un canal sécurisé. La mise en place d'une couche de transport sécurisée débute par une phase de négociation entre le client et le serveur afin de s'entendre sur les méthodes de chiffrement à utiliser. Dans un second temps le client s'authentifie auprès du serveur pour obtenir une session. Une fois que la connexion sécurisée est mise en place entre le client et le serveur, le client doit s'identifier sur le serveur afin d'obtenir un droit d'accès, il existe deux méthodes :

* la méthode la plus connue est le traditionnel mot de passe,

* une méthode moins connue mais plus souple est l'utilisation de clés publiques [27].

- **Le protocole SSL**

Il repose sur un procédé de cryptographie par clef publique afin de garantir la sécurité de la transmission de données. Son principe consiste à établir un canal de communication sécurisé (chiffré) entre deux machines (le client et le serveur) après une étape d'authentification.

- **Fonctionnement de SSL**

La sécurisation des transactions par SSL, est basée sur un échange de clés entre client et serveur. Elle se fait selon le modèle suivant :

* Dans un premier temps, le client se connecte au serveur sécurisé par SSL et lui demande de s'authentifier. Le client envoie également la liste des cryptosystèmes qu'il supporte, triée par ordre décroissant selon la longueur des clés,

* Le serveur à la réception de la requête envoie un certificat au client, contenant la clé publique du serveur, signée par une autorité de certification (CA), ainsi que le nom du cryptosystème le plus haut dans la liste avec lequel il est compatible,

* Le client vérifie la validité du certificat, puis crée une clé secrète aléatoire , chiffre cette clé à l'aide de la clé publique du serveur, puis lui envoie le résultat,

* Le serveur est en mesure de déchiffrer la clé de session avec sa clé privée. Ainsi, les deux entités sont en possession d'une clé commune dont ils sont seuls connaisseurs. Le reste des transactions peuvent se faire à l'aide de clé de session, garantissant l'intégrité et la confidentialité des données échangées [28].

3.3.3 Anti-virus et Anti-spam des serveurs de messagerie

Nous distinguons quelques anti-virus et anti-spam :

- **SpamAssasin**

Spamassasin filtre tous les messages reçus sur votre adresse courriel et en fonction de certaines règles décide que le message en question est indésirable. Les emails indésirables peuvent être automatiquement supprimés ou re-tagués pour faciliter le trie.

- **Fonctionnement**

SpamAssassin fonctionne en attribuant des "scores" à chaque message électronique selon différents tests destinés à déterminer s'il s'agit ou non d'un spam. De nombreux tests sont proposés, pour vérifier notamment la validité des adresses de l'expéditeur et du destinataire, la validité de la date des messages, la présence dans le corps du message d'un mot répertorié sur une liste de mots interdits, l'appartenance ou non d'un des serveurs expéditeurs à une liste noire, etc. Outre ces tests, SpamAssassin inclut un algorithme de Bayes qui "apprend" à reconnaître les nouveaux messages non sollicités à partir d'anciens spams [29].

- **Amavis**

Amavis est un open source filtre, le contenu pour le courrier électronique , la mise en oeuvre électronique de transfert de message passe par un certain traitement (le décodage, le contrôle), et l'interfaçage avec des filtres de contenu externe pour fournir une protection contre le spam , les virus et autres logiciels malveillants . Il peut être considéré comme une interface entre agent de transfert de courrier et un ou plusieurs filtres de contenu. Amavis peuvent être utilisés pour :

- détecter les virus, le spam, les types de contenu interdits ou des erreurs de syntaxe dans les messages de courrier,

- transmission des messages en utilisant un désinfectant externe [30].

3.4 Conclusion

Tout au long de ce chapitre, nous avons détaillé l'aspect théorique de notre projet, nous avons pu bien déterminer le fonctionnement de serveur de messagerie et ses différents protocoles, en plus, nous avons présenté quelques protocoles de sécurité.Ce chapitre est de trés grande utilité pour la partie réalisation que nous allons effectuer dans le prochain chapitre.

CHAPITRE 4

RÉALISATION

4.1 Introduction

Ce chapitre sera consacré pour la mise en œvre de toutes les notions vu dans la partie théorique. Nous la considèrons comme étant l'étape la plus cruciale puisqu'elle traite l'onglet pratique du projet. Dans ce qui suit, nous montrons les étapes d'installations et configurations de notre serveur de messagerie.

4.2 Installation et configuration des composants de la messagerie

Les étapes suivantes, montrent les différents éléments à installer pour mettre en place notre serveur de messagerie :

- Installation et configuration d'un serveur DNS (Domain Name System),
- Installation et configuration d'un serveur DHCP(Dynamic Host Configuration Protocol),
- Installation d'un serveur Apache et de langage php,
- Installation d'un serveur Mysql-server et une interface web d'administration PhpMyAdmin,
- Installation et configuration d'un serveur postfix (MTA) et une interface web Postfixadmin qui gére le serveur Postfix,
- Installation et configuration du dovecot POP (Post Office Protocol) et du dovecot IMAP (Interactive Mail Acess Protocol),

- Installation et configuration d'un antivirus et d'un anti-Spam (clamv, amavis, spamassassin),

- Installation d'un webmail : Squirrelmail (MUA).

Pour éviter les éventuelles erreurs de systéme linux liées aux droits d'accés des propriétaires et l'exécution des commandes, nous travaillerons en super utilisateur (en mode root).

4.2.1 Installation et configuration d'un serveur DNS

Avant d'entamer l'installation de serveur DNS, nous allons fixer une addresse IP pour notre machine, en créant un réseau adhoc (Figure 4.1) appelé " RXBMT ".

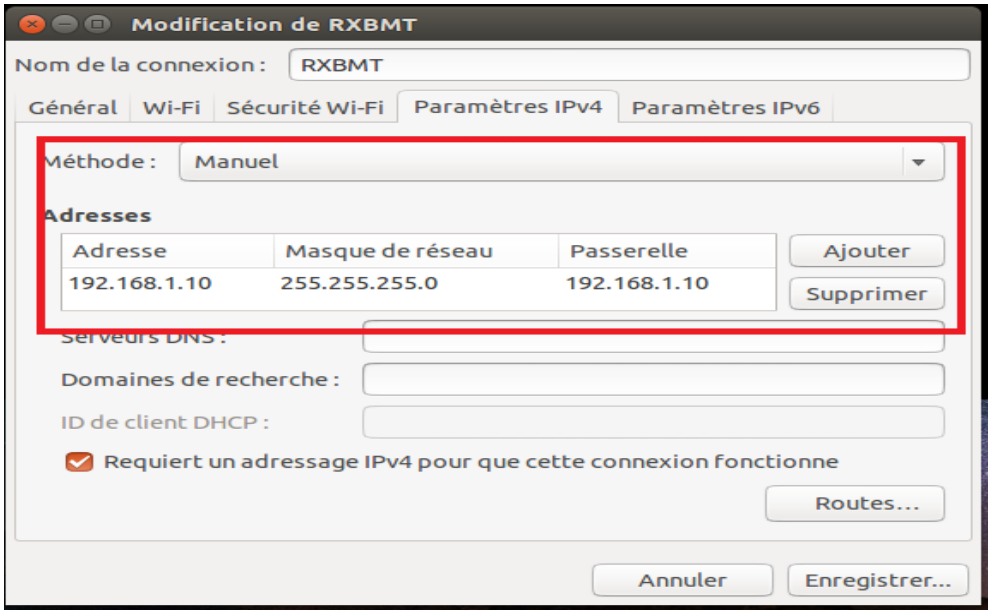

FIGURE 4.1 – Création d'un réseau adhoc.

Une fois l'adresse IP de la machine est fixée, nous installerons et nous configurerons un serveur DNS, et pour cela nous avons choisi d'installer "bind9" (Figure 4.2).

FIGURE 4.2 – Installation de bind9.

Aprés avoir installé bind9. Nous configurerons le premier fichier à l'aide de la commande *"gedit"* :

- ***named.conf.default-zones*** : ce fichier nous permet tout simplement de pouvoir déclarer un nom de domain (zone) et une adresse IP statique avec laquelle elle fera la résolution (medbejaia.dz et 1.168.192.in-addr.arpa) (Figure 4.3).

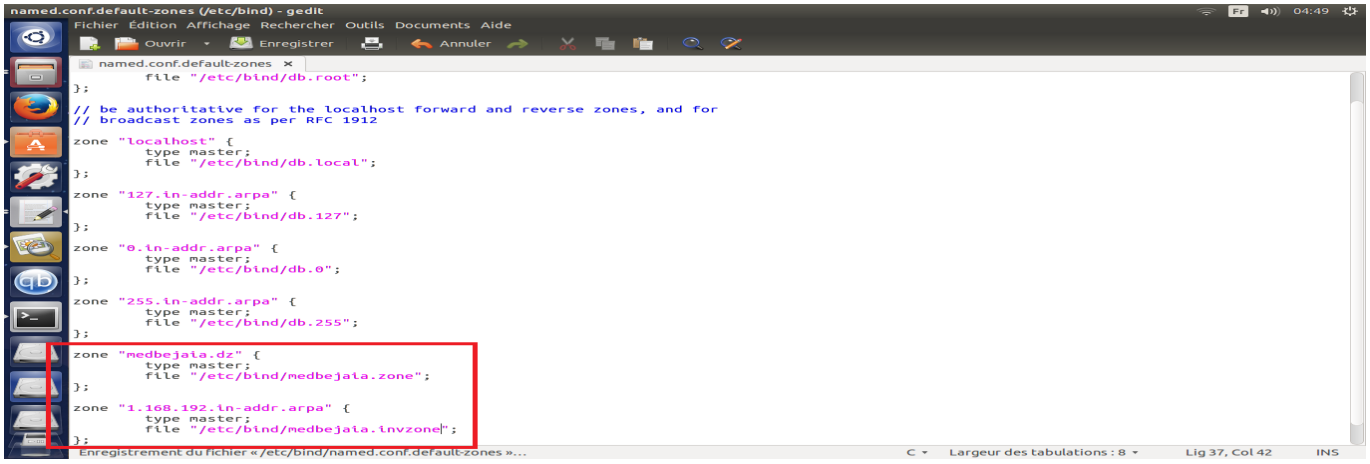

FIGURE 4.3 – Créations des zones.

Une fois le fichier *named.conf.default-zones* édité, nous avons besoin de créer deux fichiers vides mentionnés dans le fichier précedent à savoir : medbejaia.zone et medbejaia.invzone (Figure 4.4).

FIGURE 4.4 – Créations des fichiers medbejaia.zone et medbejaia.invzone.

- ***medbejaia.zone*** : une fois le fichier medbejaia.zone est crée, nous initialisons son contenu avec le contenu du fichier *" db.local"* (Figure 4.5).

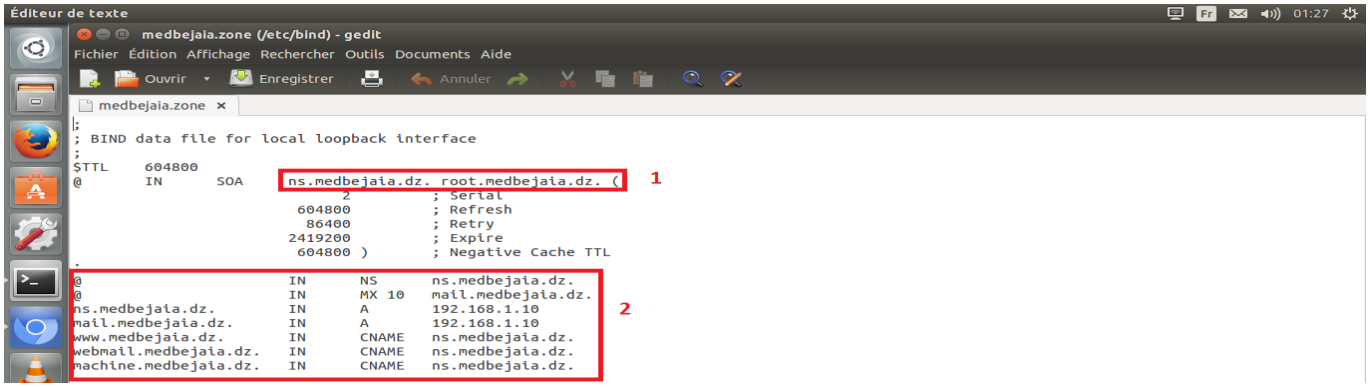

FIGURE 4.5 – Configuration le medbejaia.zone.

Concernant le code, qui se trouve dans le fichier medbejaia.zone, la première partie consiste à synchroniser notre serveur DNS. La deuxième partie, indique : le nom du serveur par l'enregistrement NS et les adresses, qui correspondent aux machines.

- ***medbejaia.invzone*** : le fichier (Figure 4.6), suit la même modification que le fichier medbejaia.zone avec quelques changements. La partie deux indique la résolution inverse, en introduisant le dernier chiffre de notre adresse IP.

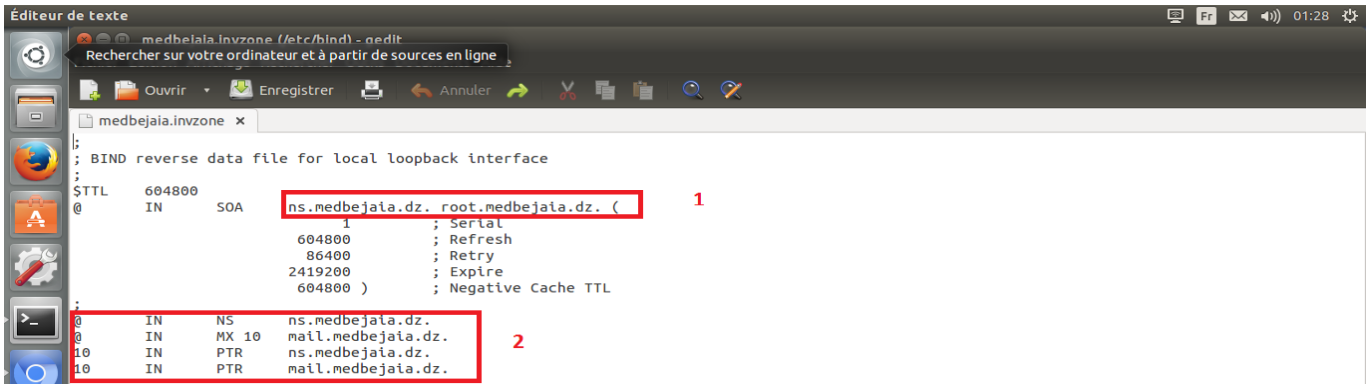

FIGURE 4.6 – Configuration de medbejaia.invzone.

Nous entamons ensuite la configuration du fichier, " resolv.conf ", qui permet d'indiquer le domaine de recherche ainsi que l'adresse du serveur DNS. En tapant la commande suivante : *"gedit /etc/resolv.conf"*. Nous rajoutons les trois instructions montrées dans le rectangle rouge (Figure 4.7).

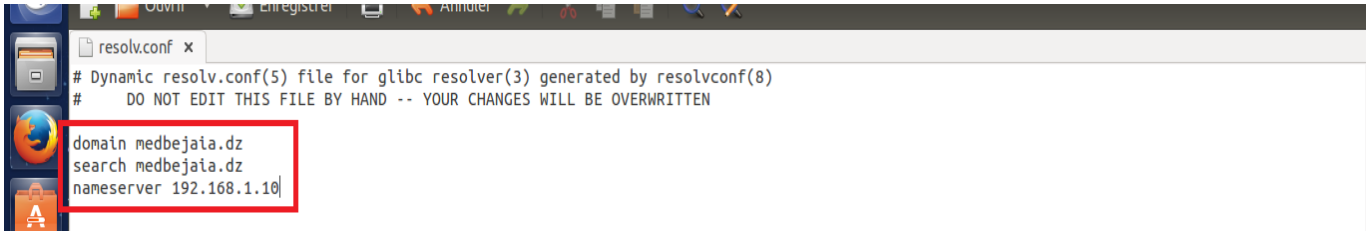

FIGURE 4.7 – Configuration de fichier resolv.conf .

Pour tester le bon fonctionnement de notre serveur DNS, nous tapons la commande suivante : *nslookup* , lorsqu'il nous rend la main, nous pouvons effectuer plusieurs testes, en entrant le nom de notre domaine et l'adresse IP de notre machine. Les testes effectués sont soulignés en lignes rouge (Figure 4.8).

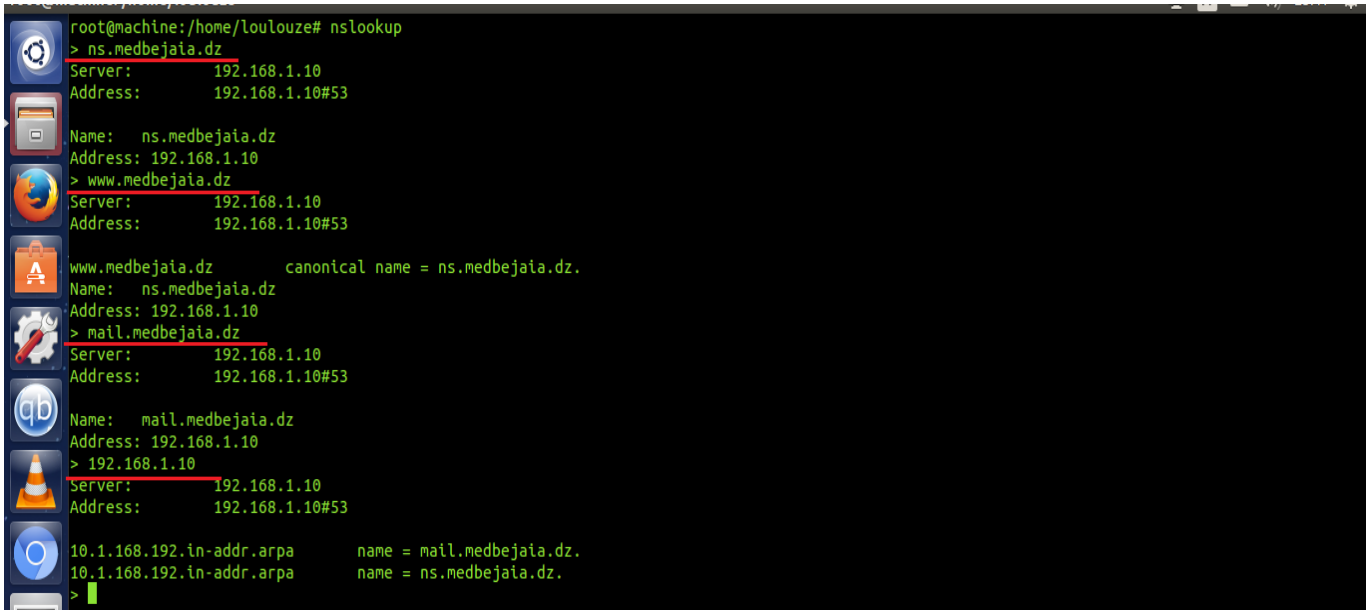

FIGURE 4.8 – Teste de fonctionnement de serveur DNS.

Nous remarquons que notre serveur DNS, fait correctement la résolution en retournant le nom de serveur DNS *"ns.medbejaia.dz"* et l'adresse IP de la machine *"192.168.1.10"*.

4.2.2 Installation et configuration d'un serveur DHCP

Cette étape permet de configurer le serveur DHCP. Nous avons choisi d'installer "isc-dhcp-server", en tapant la commande : *" apt-get install isc-dhcp-server "*. Par la suite nous allons modifier le fichier qui se situe dans *" /etc/dhcp/dhcpd.conf "*.

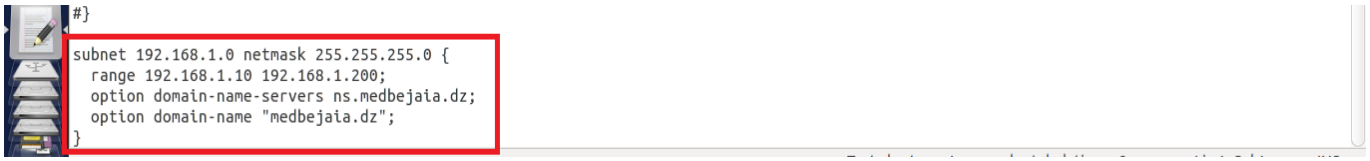

FIGURE 4.9 – Configuration de dhcpd.conf.

Dans ce fichier (Figure 4.9) nous allons introduire l'adresse de réseau, le masque de sous réseau, la plage d'adresses IP et le nom de serveur DNS. Une fois la configuration est terminée , nous redémarrons le service : *" service isc-dhcp-server restart"*.

4.2.3 Installation de serveur apache et de language php

cette étape représente l'installation d'un serveur apache (Figure 4.10), en tapant la commande : *" apt-get install apache2 "*.

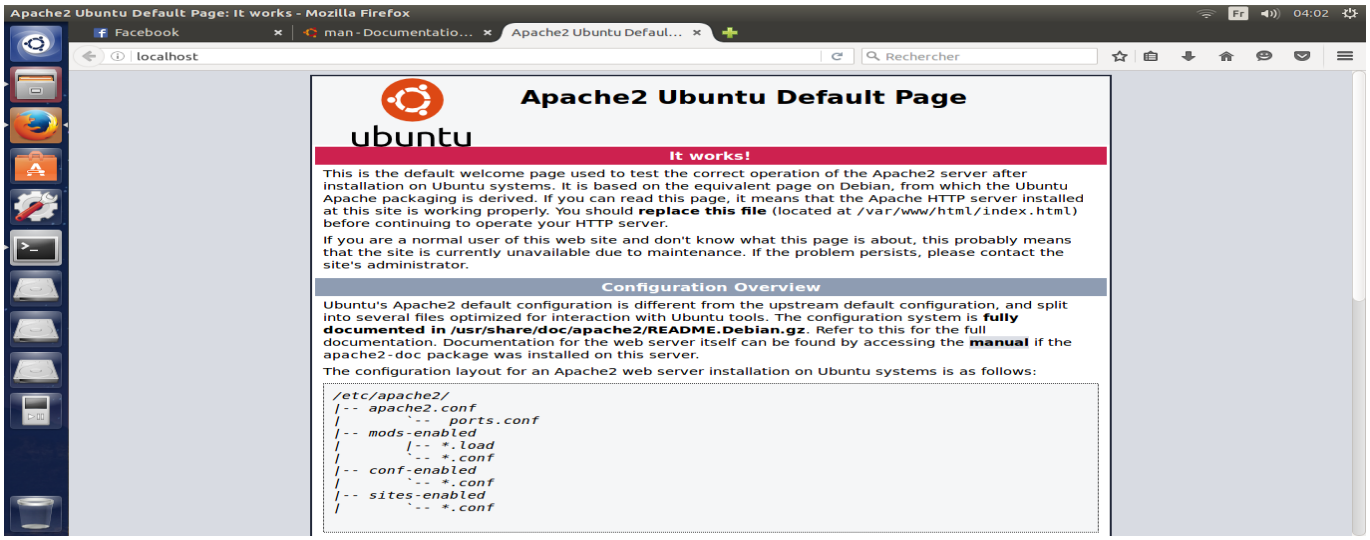

FIGURE 4.10 – Installation de serveur Apache.

Passant maintenant à l'installaion de langage php, en tapant la commande : *" apt-get install php5 "*. Pour tester le fonctionnement de php, nous éditons le fichier *"teste.php"* et écrivons une fonction prédifinie de php : *"< ?php phpinfo() ; ?>"* et plaçons le fichier dans : *" /var/www/html/"*.

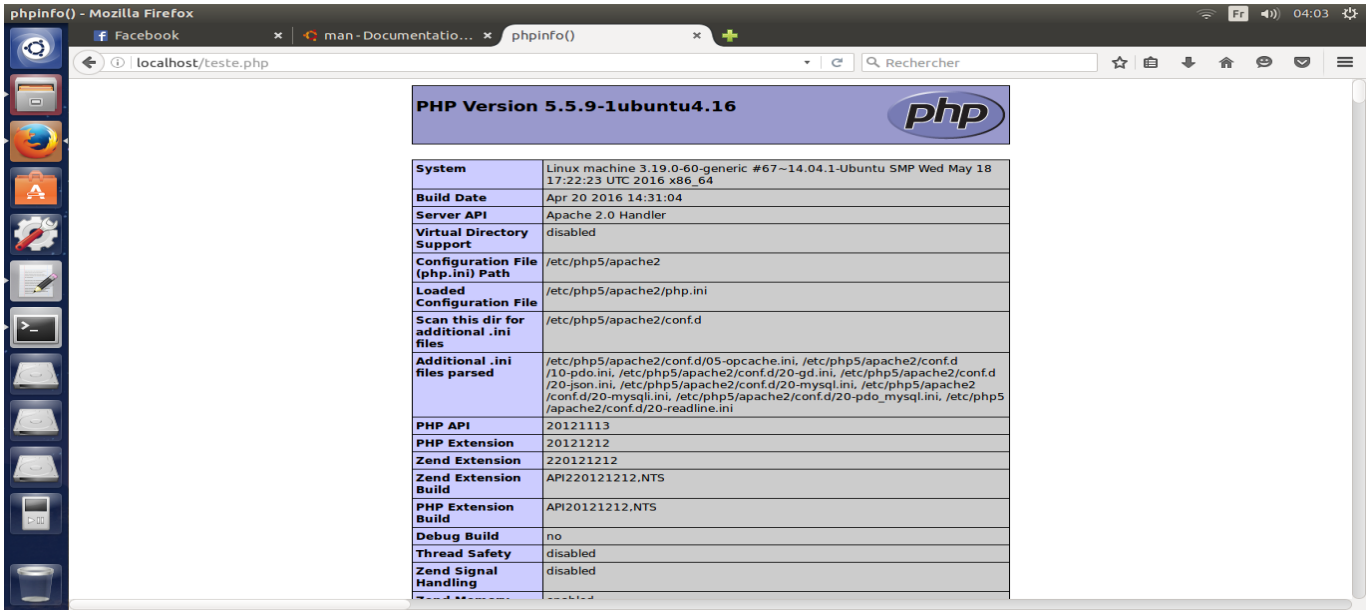

FIGURE 4.11 – Vérification de l'installation de php5.

La figure nous montre les différentes informations de langage php (Figure 4.11).

4.2.4 Installation d'un serveur Mysql-server et l'interface web PhpMyAdmin

Dans cette étape, nous nous intéresserons à l'installation et la configuration de la base de données, en tapant la commande : *" apt-get install mysql-server "*. Durant l'instalation, un mot de passe sera demandé (Figure 4.12).

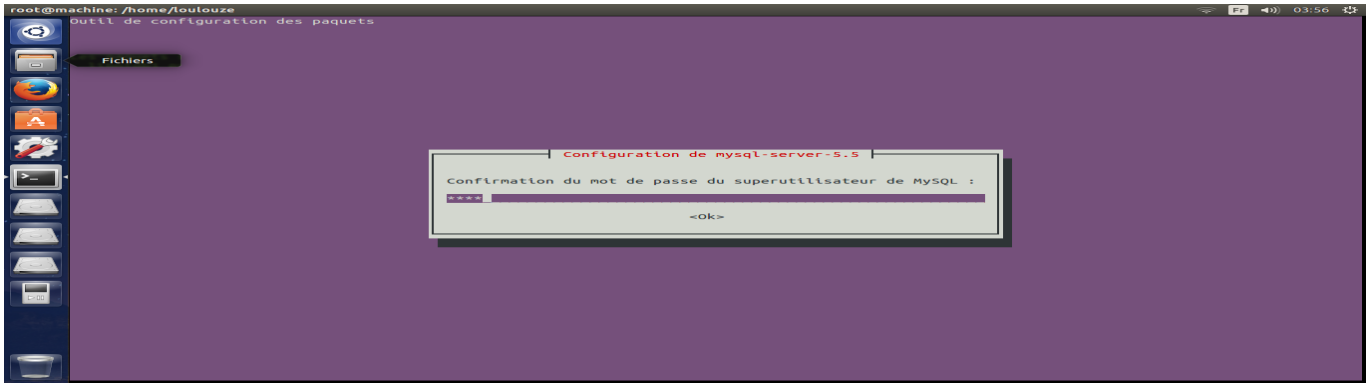

FIGURE 4.12 – Installation d'un serveur Mysql-server.

Une fois mysql-serveur est installé, nous passons à l'installation d'une interface web Phpmyadmin (Figure 4.13), qui gére notre base de données, en tapant la commande : *" apt-get install phpmyadmin "*.

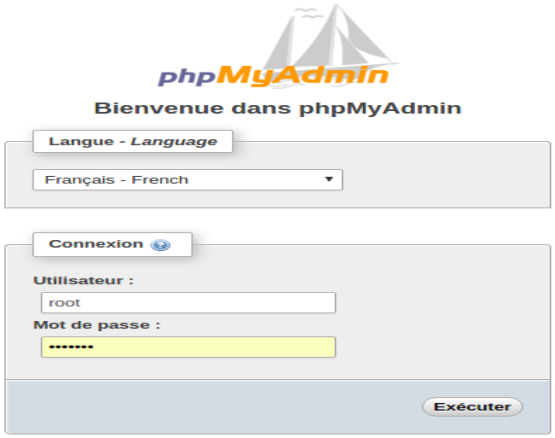

FIGURE 4.13 – L'interface de Phpmyadmin.

4.2.5 Installation et configuration d'un serveur postfix (MTA) et l'interface web postfixadmin

Cette étape consiste à installer le serveur Postfix (serveur smtp) avec une extension mysql, et pour cela, nous tapons la commande suivante : *" apt-get install postfix-mysql "*. Lors de l'installation, le serveur postfix nous demande d'introduire le nom de courrier (Figure 4.14).

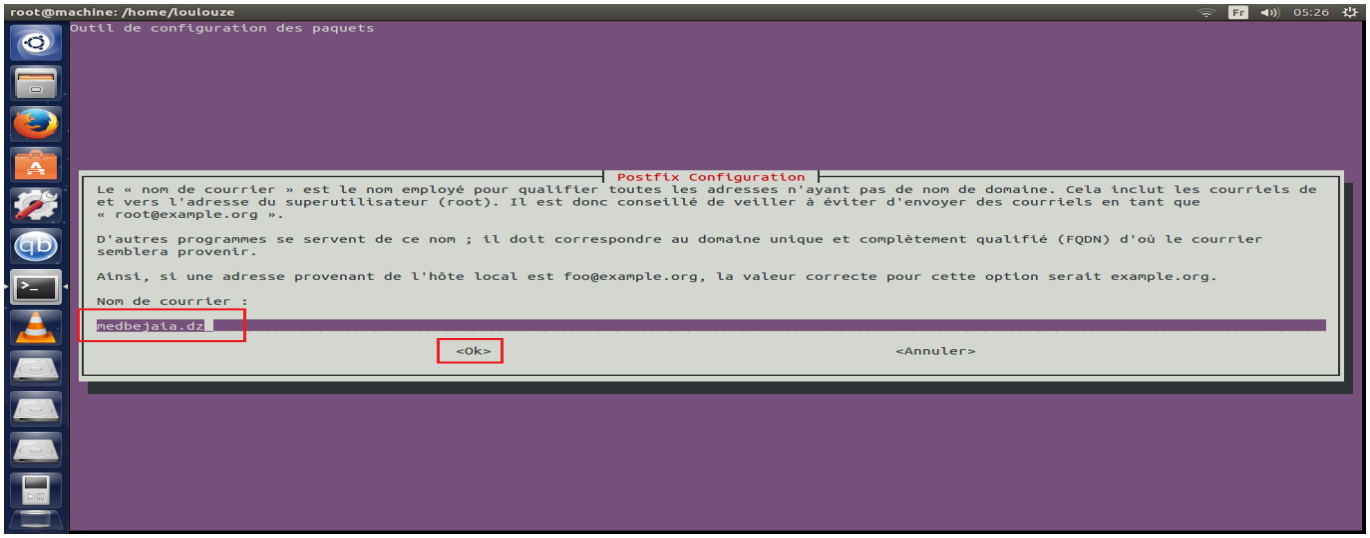

FIGURE 4.14 – Installation de postfix.

Une fois le serveur postfix est installé, nous procédons à l'instalation de Postfixadmin qui permet de gérer et administrer à partir d'une interface web le serveur postfix. Durant l'installations de postfixadmin une base de données est créée " *postfixadmin* " ainsi que les tables nécessaires pour le serveur postfix (Figure 4.15).

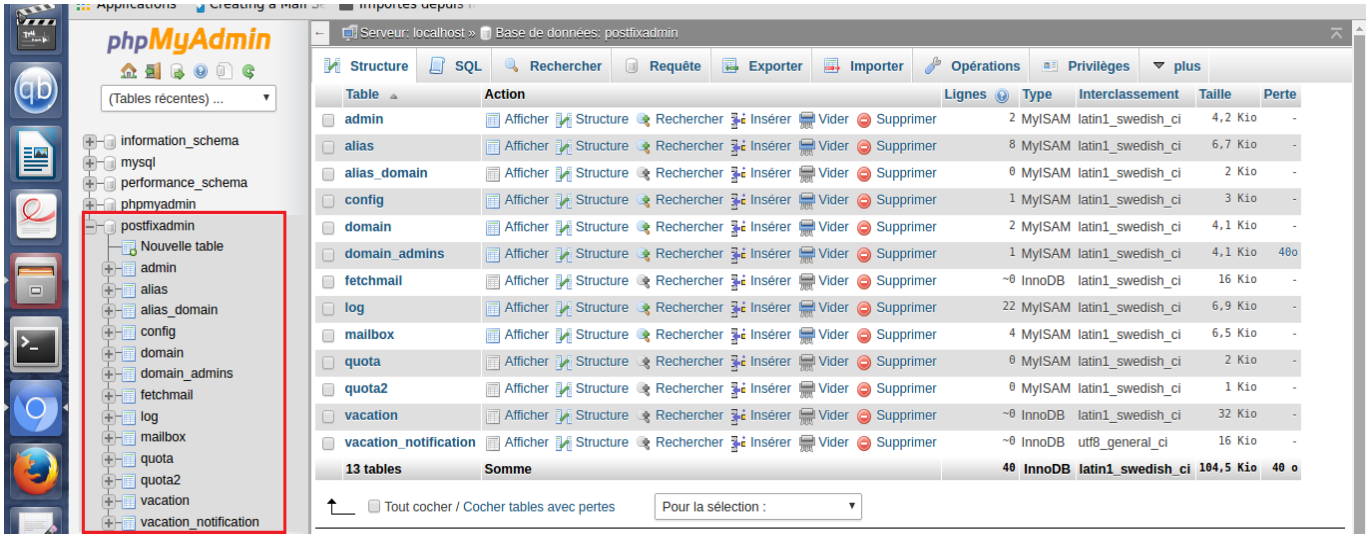

FIGURE 4.15 – Base et les tables de données postfixadmin.

Pour ajouter un administrateur, nous écrivons ce lien dans la barre d'URL *" localhost/postfixadmin/setup.php "* (Figure 4.16). Postfixadmin nous demande de valider la génération d'un code haché.

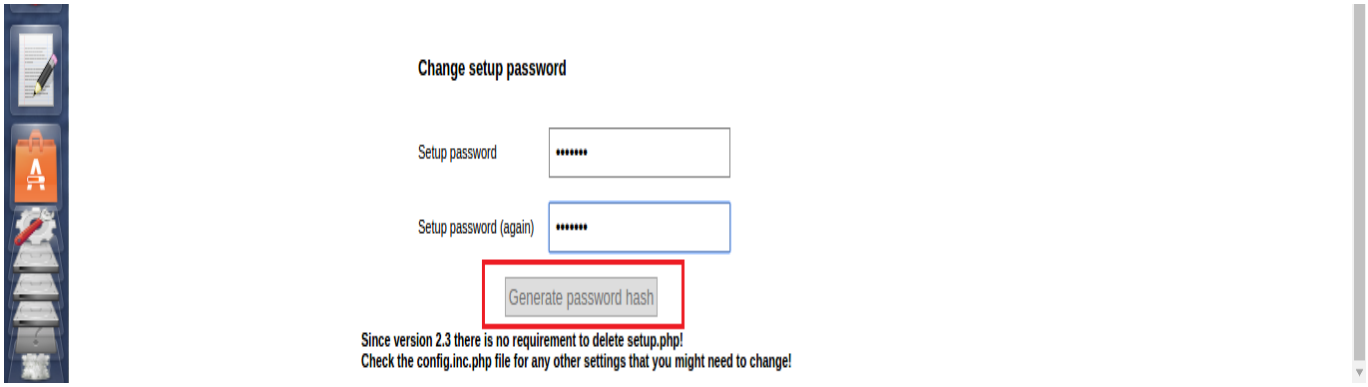

FIGURE 4.16 – Génération de mot de passe pour un administrateur.

La figure (Figure 4.17) montre le code haché généré :

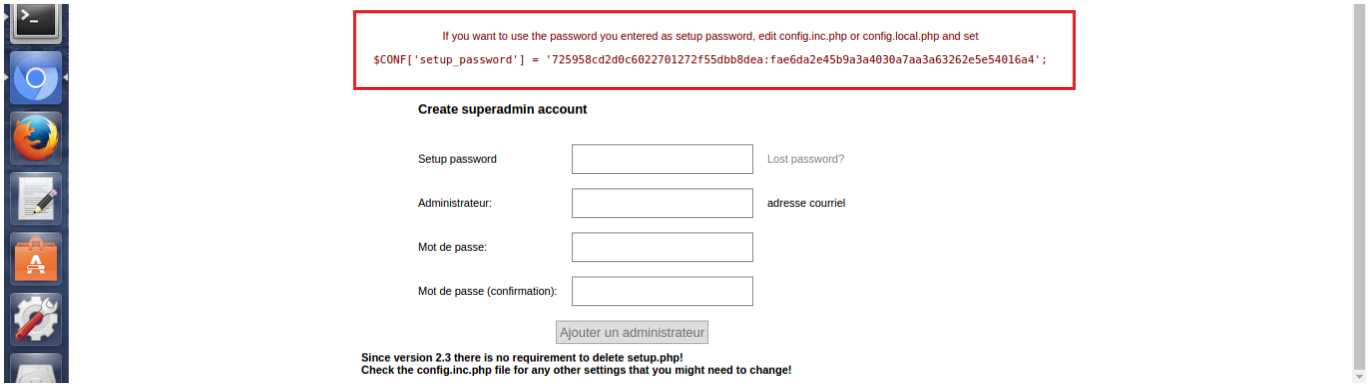

FIGURE 4.17 – Mot de passe généré.

Par la suite nous allons copier le code générer et le coller dans le fichier de configuration de postfixadmin et remplir les champs restants *" /etc/postfixadmin/config.inc.php"* (Figure 4.18) :

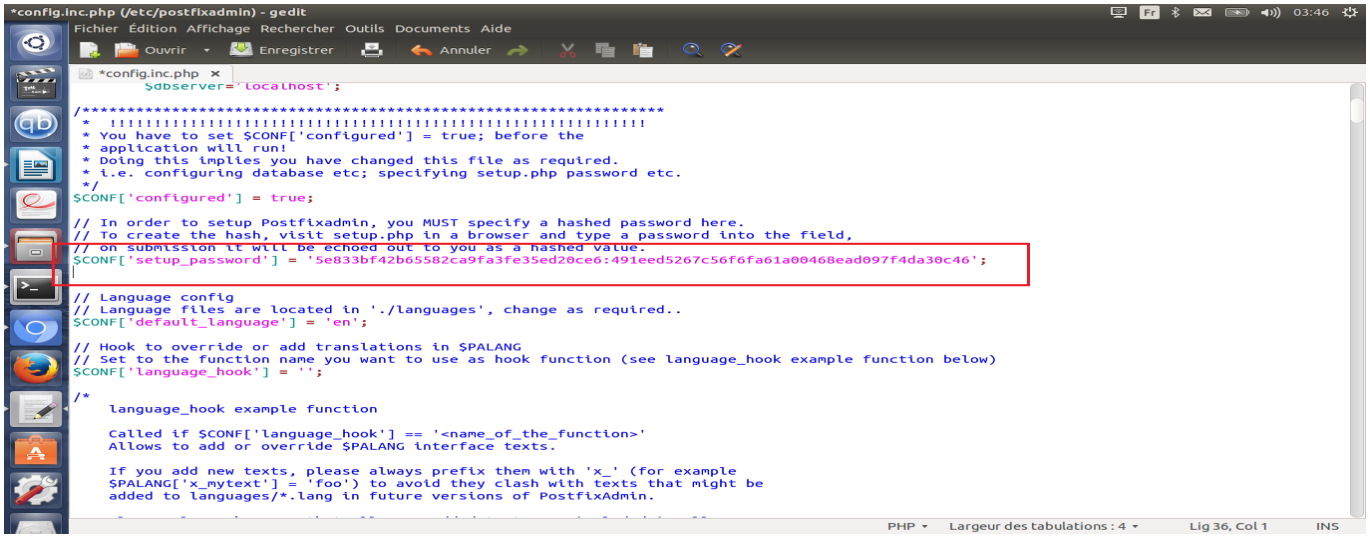

FIGURE 4.18 – Insertion de mot de passe.

Aprés l'ajout de l'administrateur, désormais nous pouvons y accéder, en entrant le liens suivant *" localhost/postfixadmin/login.php "* (Figure 4.19) :

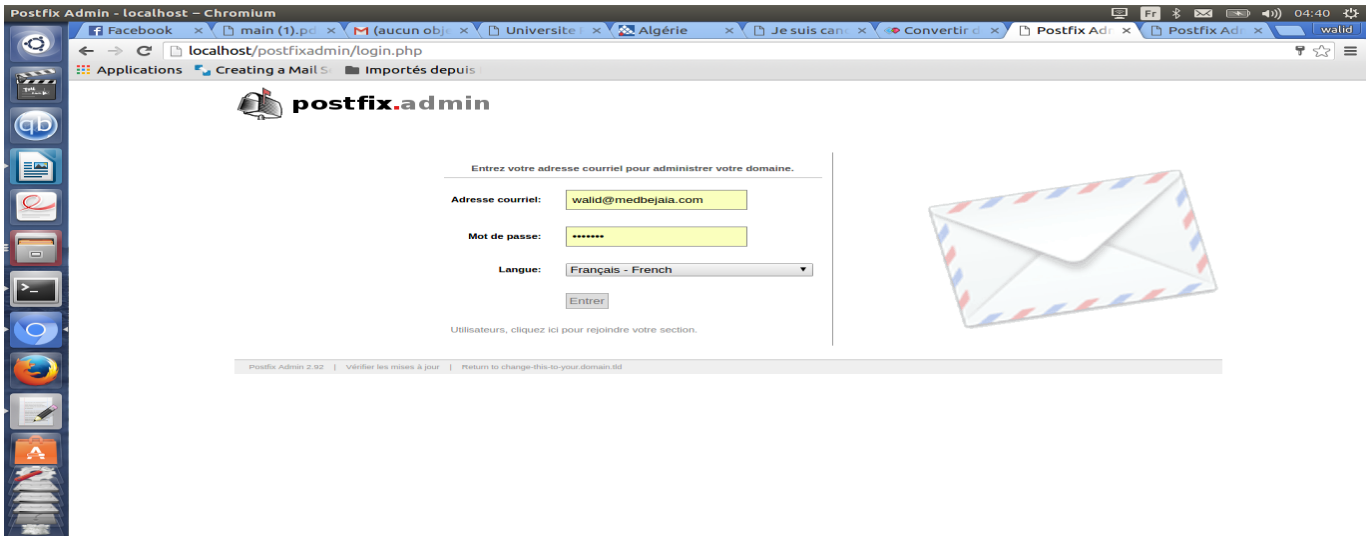

FIGURE 4.19 – La page de l'administrateur.

L'étape suivante consiste à configurer les deux fichiers principaux (main.cf et master.cf), qui se trouvent dans le répértoire : *" /etc/postfix/"*.

Avant d'entamer la configuration des fichiers de postfix, nous allons créer un compte spécifique qui aura son répertoire dans *"/home"*, c'est ici que se trouve tous les répertoires personnels, dans lesquels on configure postfix pour déposer les mails et aussi dovecot se servira de ces répertoires pour récupérer les mails en IMAP et POP3. Voila donc la commande qui nous permettera de créer ce répertoire : *" useradd -r -g mail -m -d /etc/sbin/nologin -c 'email virtuel' vmail "*.

- r : pour dire que c'est un compte système,
- g : pour dire qu'il appartient à un groupe,
- m : pour créer un répetoire personnel,
- s : pour dire son equivalent dans le shell,
- /user/sbin/nologin : comme ce n'est pas des personnes réels qui ouvrent de sessions interactives donc on va le mettre sur un shell qui va l'empecher de se loguer,
- c : pour mettre une description.

A présent nous allons chercher l'UID et GID de répertoire crée vmail, qui nous aideront par la suite dans la configuration. Nous tapons la commande suivante : *" grep vmail /etc/passwd "*, qui permet de récupérer les informations du compte *"vmail"*, en nous retournant comme résultats ce qui est montré dans (Figure 4.20). Le rectangle rouge représente réspectivement l'UID et le GID.

FIGURE 4.20 – Résultat de la commande grep.

A ce niveau, nous nous ntéresserons à la configuration de fichier main.cf (Figure 4.21).

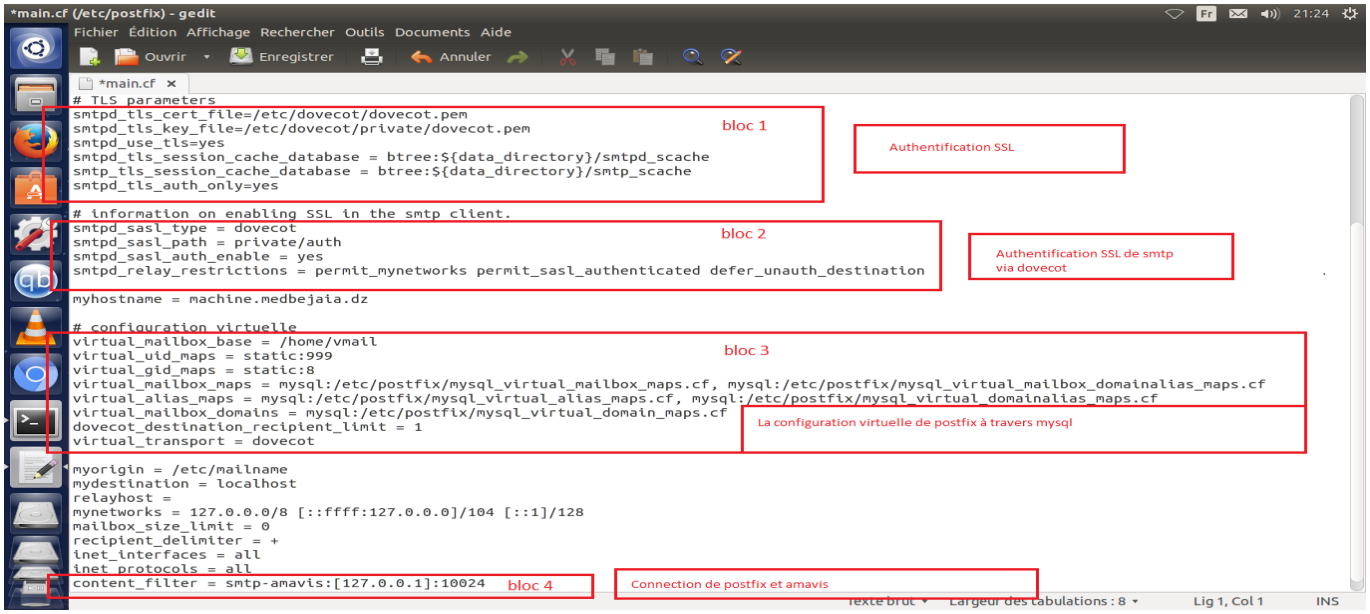

FIGURE 4.21 – Configuration de fichier main.cf .

Dans le premier bloc, nous avons établi une connexion SSL. Lors de l'installation de dovecot un certificat auto-signé et une clé privée sont installés automatiquement (Figure 4.22), alors nous allons réutiliser ce certificat, en indiquant le chemin : *" /etc/dovecot/dovecot.pem et /etc/dovecot/private/dovecot.pem "*.

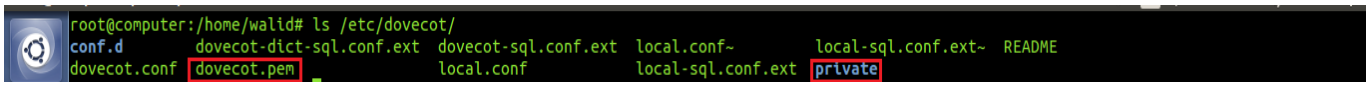

FIGURE 4.22 – Certificat SSL.

Dans le deuxiéme bloc, nous avons configuré l'authentification de protocole SMTP à partir de decovecot en SSL.

Dans le troisiéme bloc, nous avons indiqué à postfix où va aller chercher les informations stockées dans mysql et facilité à postfixadmin la recherche de différents éléments. Nous avons besoin de créés les cinq fichiers montrés en (Figure 4.23) :

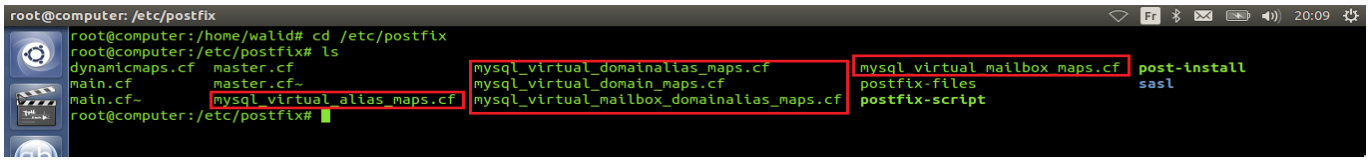

FIGURE 4.23 – Les cinq fichiers crées.

Ces fichiers indiqueront au serveur postfix, la base de données *" postfixadmin"*, les utilisateurs, les tables ainsi que les noms de domaines.

- Création de fichier : mysql_virtual_domain_maps.cf (Figure 4.24)

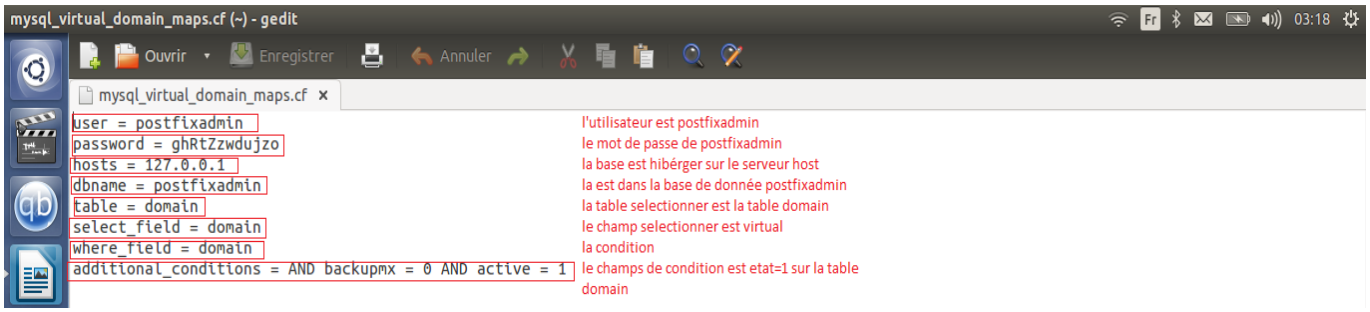

FIGURE 4.24 – Le fichier mysql_virtual_domaines.cf .

Comme le montre la figure (Figure 4.24), le fichier mysql_virtual_domaines.cf contient huit lignes, les quatres premiéres lignes sont les mêmes pour tous les autres fichiers, il n'y aura que les quatres derniéres qui seront changées.

- Création de fichier : mysql_virtual_mailbox_maps.cf.

Pour ne pas perdre le temps à réecrire les lignes une dexiéme fois, il suffit de copier le contenu du fichier mysql_virtual_domaines.cf dans le fichier mysql_virtual_mailbox-maps.cf en utilisant la commande "cp" (Figure 4.25)

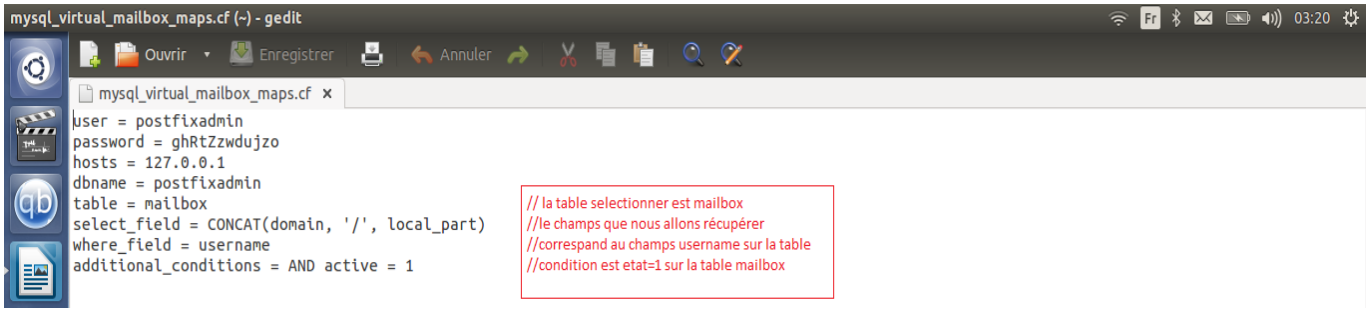

FIGURE 4.25 – Le fichier mysql_virtual_mailbox_maps.cf .

- Création de fichier : mysql_virtual_alias_maps.cf (Figure 4.26).

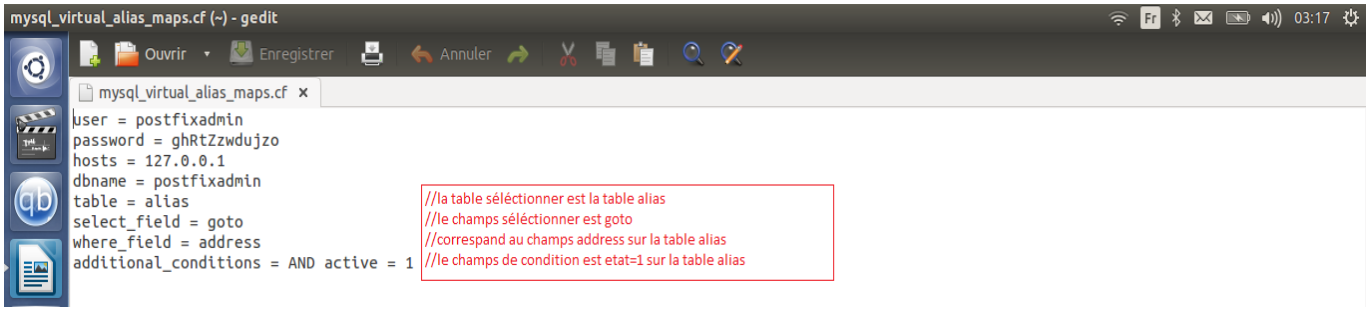

FIGURE 4.26 – Le fichier mysql_virtual_alias_maps.cf

- Création de fichier : mysql_virtual_mailbox_domainalias_maps.cf (Figure 4.27).

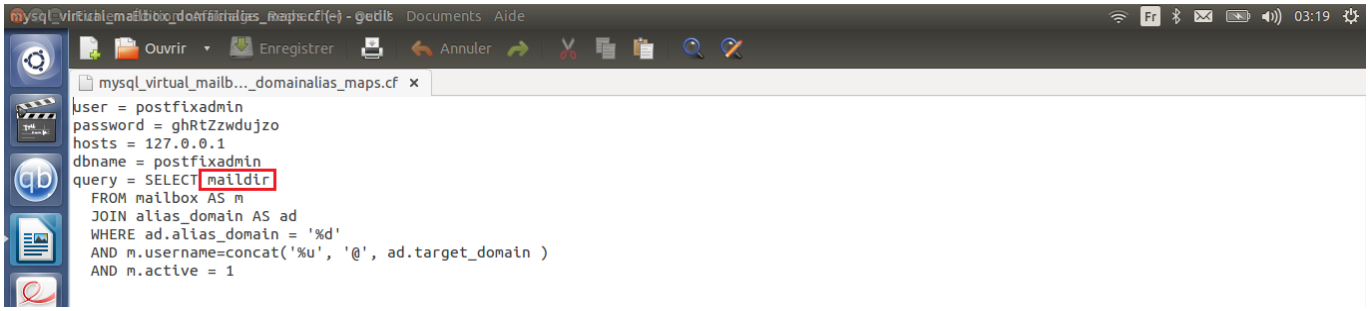

FIGURE 4.27 – Le fichier mysql_virtual_mailbox_domainalias_maps.cf

C'est une requête avec une joiture entre mailbox et alias_domaine pour récupérer le dossier maildir qui provient de l'alias.

- Création de fichier : mysql_virtual_domainalias_maps.cf (Figure 4.28).

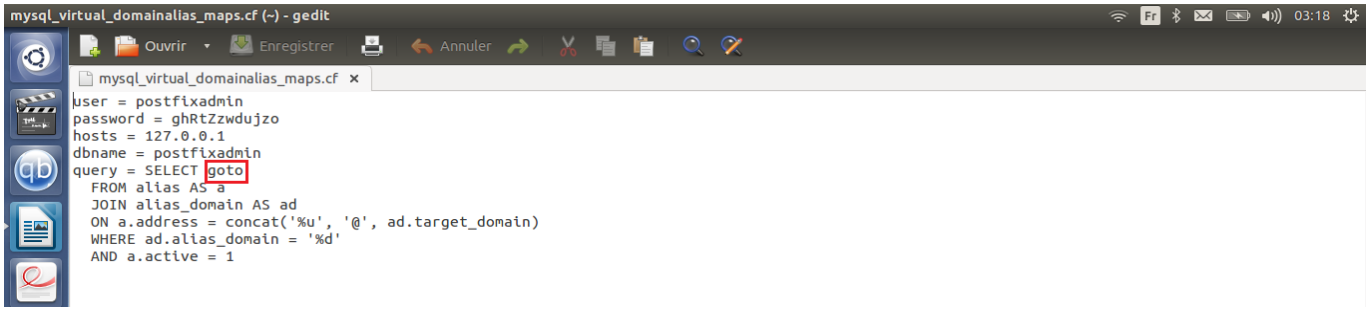

FIGURE 4.28 – Le fichier mysql_virtual_domainalias_maps.cf .

C'est une requête avec une joiture entre alias et alias_domaine pour récupérer le domaine qui provient de l'alias.

Dans le quatrième bloc, nous avons intégré l'anti-spam (amavis) dans postfix. Cette ligne nous permet de filtrer le contenu des mails à l'aide de amavis.

Nous passons à la configurtion de fichier master.cf de postfix qui détermine quels sont les services ouverts de postfix, pour cela nous tapons la commande suivante :" *gedit /etc/postfix/master.cf* ". Dans un premier temps nous allons vérifier la ligne " *smtp* " qui correspond à la colonne " *chroot*", si elle contient un tiret et non pas autre chose (Figure 4.29).

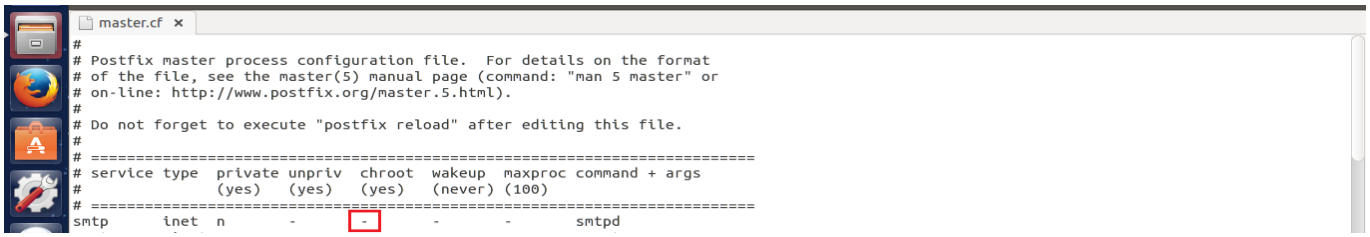

FIGURE 4.29 – Le service smtp.

Ensuite, nous allons décommenter toutes les lignes de smtps, vu que nous avons établi une connexion SSL dans le fichier " *main.cf*" (Figure 4.30).

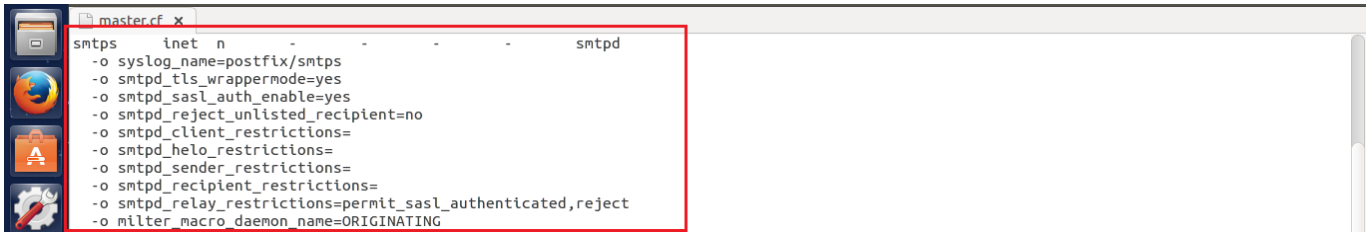

FIGURE 4.30 – Le service smtps.

Nous rajoutons une ligne pour dire quelle est la méthode propre à dovecot (Figure 4.31).

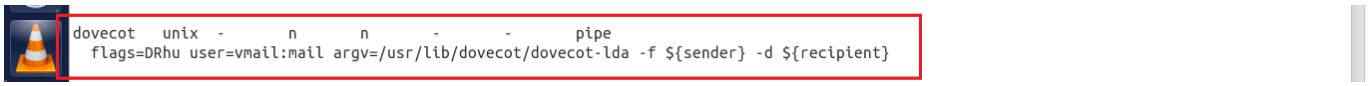

FIGURE 4.31 – Le service dovecot.

Comme nous avons utilisé *"amavis"* dans le *"main.cf"*, nous allons ouvrir le service de amvis, en rajoutant les lignes montrées en (Figure 4.32).

FIGURE 4.32 – Le service amavis.

4.2.6 Installation et configuration du dovecot POP et du dovecot IMAP (MDA)

Cette étape, consiste à installer et configurer dovecot POP et dovecot IMAP, pour cela nous avons choisi d'installer dovecot en tapant la commande suivante : *"apt-get install dovecot-core dovecot-imapd dovecot-pop3d dovecot-mysql "* . A la fin d'installation, nous remarquons qu'un certificat SSL auto-signé a été crée et qui sera valide pendant dix ans (Figure 4.33).

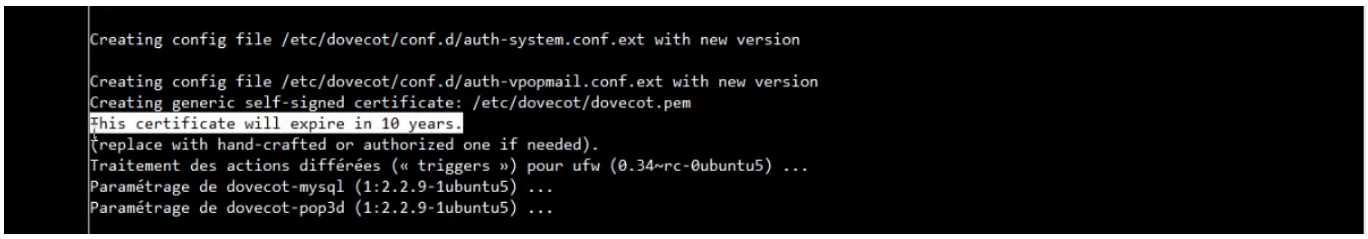

FIGURE 4.33 – Création de certificat.

Nous allons consulter les fichiers de configuration de dovecot (Figure 4.34), notamment le fichier *"dovecot.conf"*, nous remarquons une séries d'includes de tous les fichiers qui sont dans le dossier *"conf.d"* et le fichier *"local.conf"*. Nous allons créer le fichier *"local.conf"* dans le dossier *"/etc/dovecot/"*, où nous sauvegardons notre configuration, pour eviter d'écraser ces configurations pendant les différentes mise a jour de dovecot.

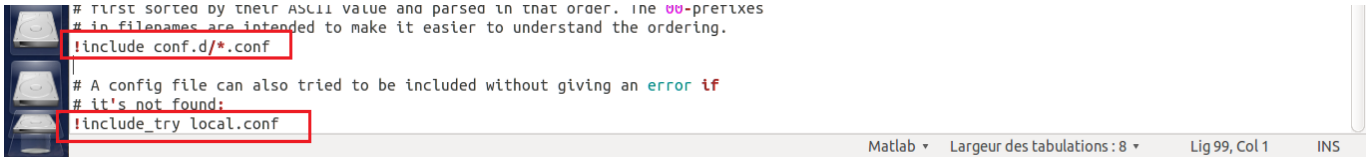

FIGURE 4.34 – Le fichier dovecot.conf.

Maintenant, nous allons copier le code indiquant le lieu par défaut des boîtes mails des utilisateur, les identifiants des utilisateurs valides pour se connecter, les utlisateurs et les groupes qui vont accéder aux mails, qui se trouvent dans le fichier : *"/etc/dovecot/conf.d/10-mail.conf"*, et le coller ensuite dans le ficher : *"/etc/dovecot/local.conf"*(Figure 4.35) .

.

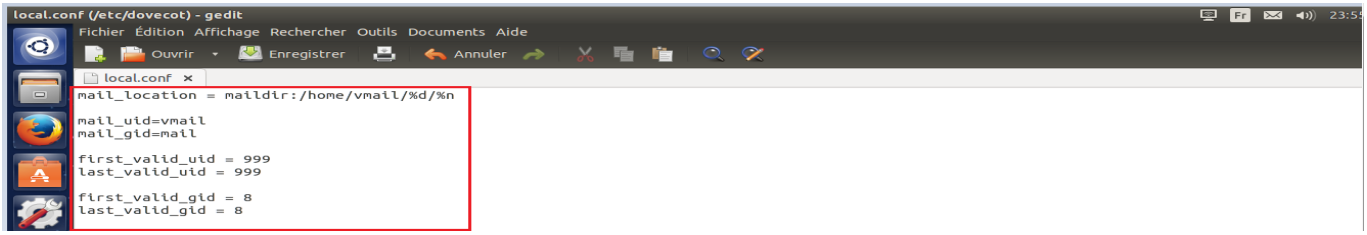

FIGURE 4.35 – Configuration du chemin et de l'autorisation d'accés aux mails dans le fichier local.conf.

Une fois la copie est effectuée, nous passons à la configuration d'authentification des utilisateurs dans dovecot (Figure 4.36), nous allons copier le code qui se trouve : *"/etc/dovecot/conf.d/auth-sql.conf.ext"* et le coller dans le fichier : *"/etc/dovecot/conf.d/local.conf"*.

.

FIGURE 4.36 – Configuration de l'anthentification dans dovecot.

Les deux sections, présente la base de donnée des mots de passes et la base de données des utilisateurs. Comme nous avons un seul utilisateur virtuel qui accéde à la récupérations des couriers éléctroniques, nous avons utilisé un driver static et les informations de l'utilisateur virtuel. Les variables *" %d et %n"* sont des variables prédifini de dovecot qui désignent respectivement(domaine, utilisateur).

Nous avons configuré l'authentification SSL de postfix via dovecot dans le fichier *"main.cf"* (Figure 4.21), et ici nous effectuons la connexion de dovecot à postfix en SSL. Nous allons copier une partie du code du fichier *"/etc/dovecot/conf.d/10-master.conf"* et les coller dans *"/etc/dovecot/local.conf"* (Figure 4.37).

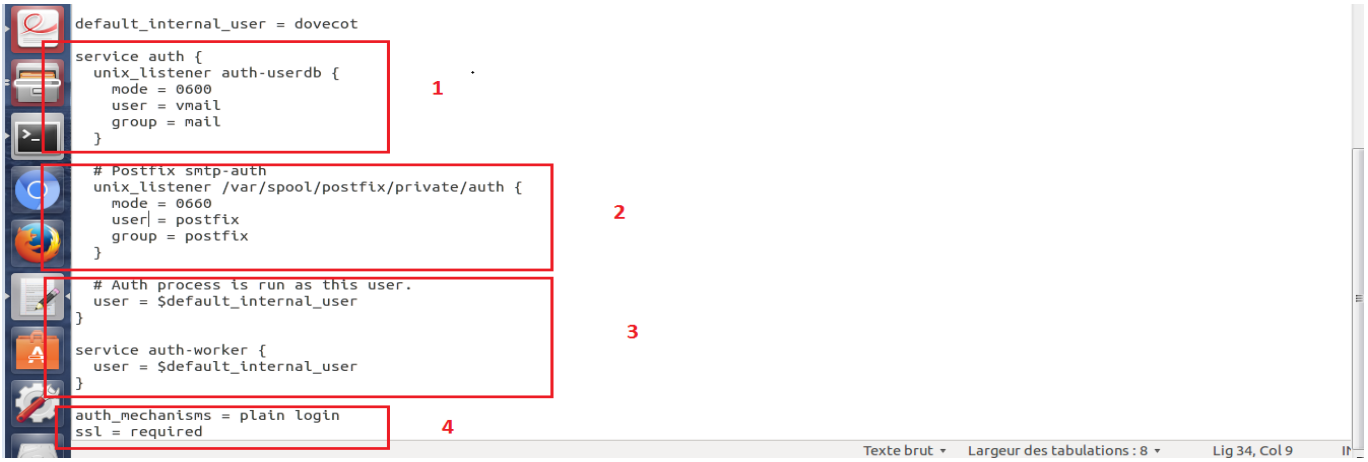

FIGURE 4.37 – Configuration ssl dans dovecot.

Ce code nous permet de définir les services d'authentifications utilisants ssl dans dovecot. Dans la premiére partie, le service *"auth-userdb"* consiste à faire la recherche des utilisateurs et comme nous avons un seul utilisateur virtuel (vmail) qui fait la connexion de tous les autres utilisateurs et pour des raisons de sécurité nous avons donné la permission seulement à l'utilisateur virtuel, les droits d'accés sont exprimés en décimale (0600).

Dans la deuxiéme partie nous avons configuré l'athentification de SMTP via le service *"smtp-auth"* qui est postfix (serveur smtp) et donné les permissions nécessaires pour fonctionner.

Pour sécuriser le prcessus de l'authentification *"service auth"* nous rajoutons la variable *"default_internal_user = dovecot"* dans la troisième partie, forçant le processus de tourner sur le compte de dovecot. Dans le quatrième rectangle nous rajoutons le mécanisme d'authentification utilisé par des clients de la messagerie et activons le protocole ssl.

Une fois la configuration dans le fichier *"local.conf"* est terminée, nous configurons l'accés à la base de données pour dovecot. Nous nous intéresserons au fichier *"/etc/dovecot/dovecot-sql.conf.ext"*, pour s'assurer que le fichier ne soit pas ecrasé lors de différentes mises à jour, nous allons copier le contenu de ficher précédent et le coller dans le fichier *"/etc/dovecot/local-sql.conf.ext"* (Figure 4.38).

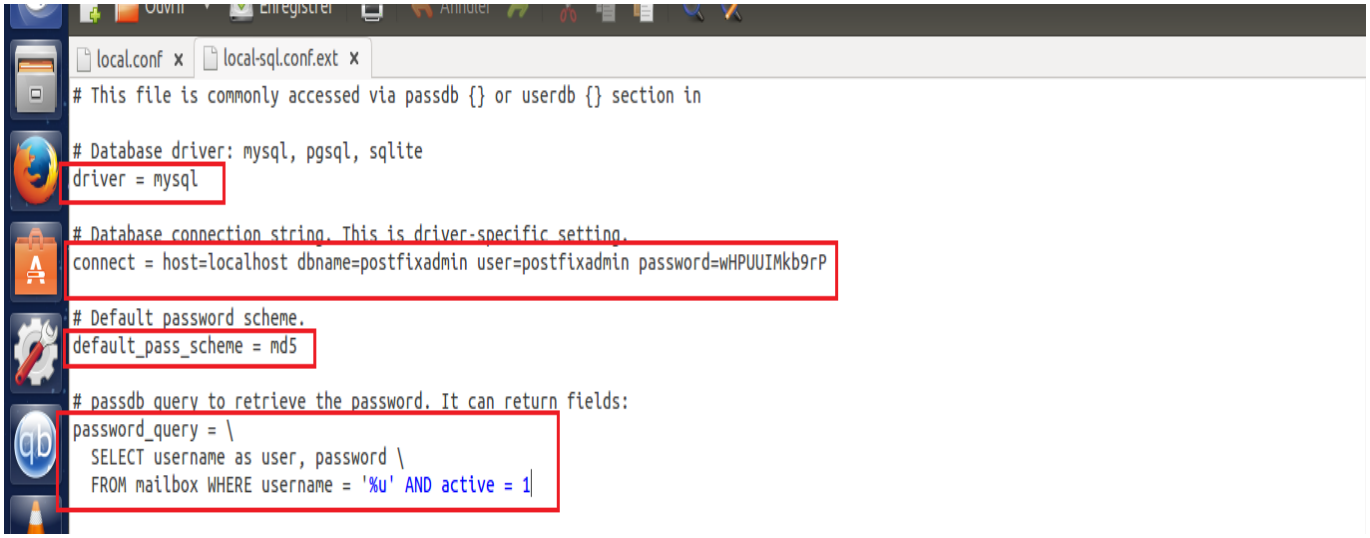

FIGURE 4.38 – Configuration de fichier local-sql.conf.ext.

Dans ce fichier, nous avons précisé le driver de la base de données, la chaine de connexion à la base de données, l'algorithme de chiffrement des mots de passe dans la base de données et enfin une requête pour récupérer les mots de passe.

4.2.7 Installation et configuration d'un antivirus et d'un anti-Spam (clamv, amavis, spamassassin)

Dans cette section, nous intérésserons à sécuriser le contenu de nos mails et pour cela nous avons installé un antivirus et un anti-spam. Il suffit de taper la commande suivante : *" apt-get install amavisd-new clamv clamv-daemon spamassassin "*. Commençons par clamav, il faut mettre à jour régulièrement ces fichiers de définition de virus avec la commande suivante : *" freshclam "*.

Ensuite nous configurerons *" amvis "* (Figure 4.39), en décommentant les lignes qui se trouvent dans le fichier *" /etc/amavis/conf.d/15-content-filter-mode"*.

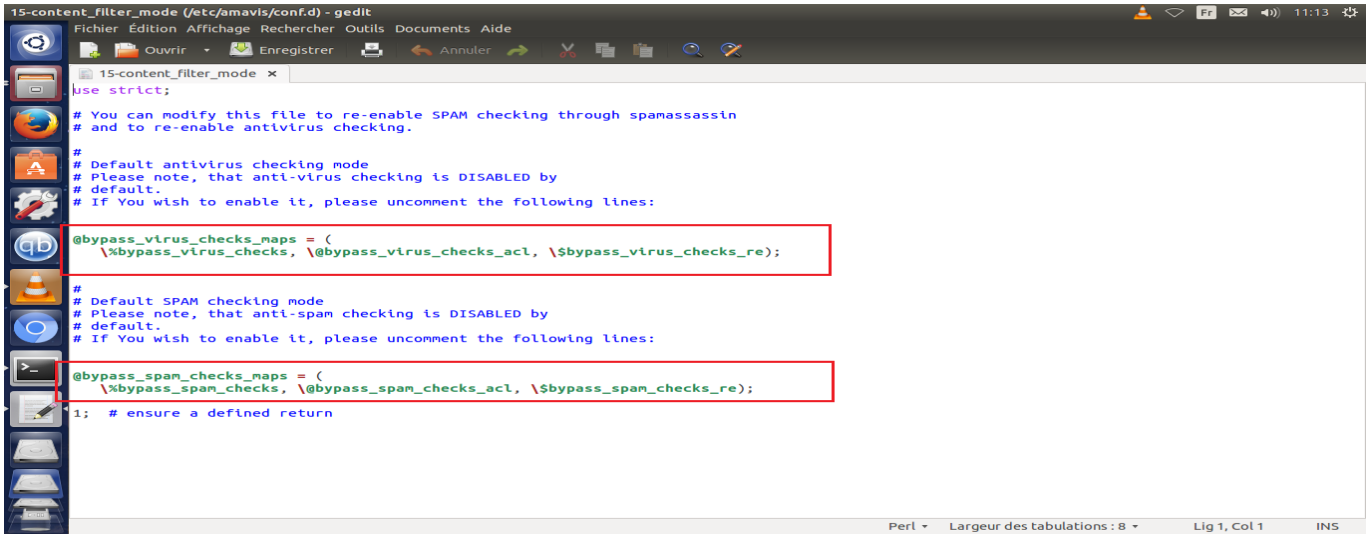

FIGURE 4.39 – Configuration de fichier 15-content-filter-mode.

Dans le premier bloc permet d'activer l'anti-virus et le second permet d'activer l'anti-spam.

Aprés la configuration, nous intégrons *" amavis "* et ces services pour qu'ils soient supportés par le serveur *"postfix"* (Figure 4.21) et (Figure 4.32).

Enfin, nous finalisons notre configurations avec *" Spamassassin "* , nous éditons le fichier *"/etc/default/spamassassin"* (Figure 4.40).

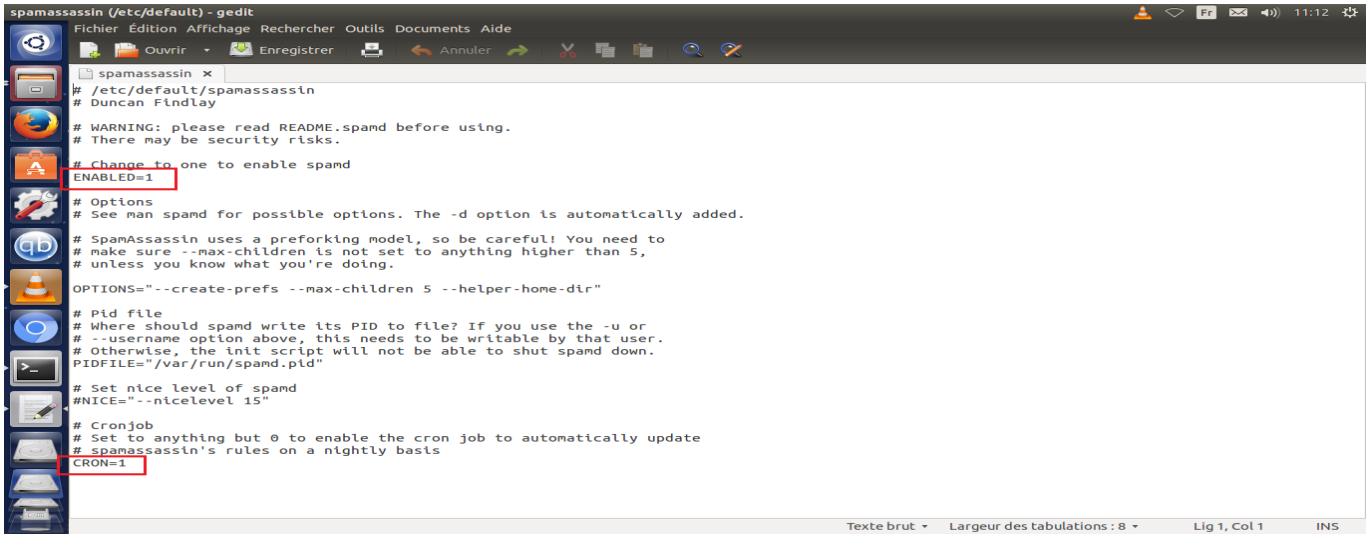

FIGURE 4.40 – Configuration de fichier Spamassasin.

Nous modifions la valeur de *" Enable "* à 1 pour activer l'anti-spam et la valeur de *" CRON "* pour lancer les mises à jour automatiquement.

Aprés avoir fini la configuration de notre serveur de messagerie, nous allons effectuer quelques testes de vérifications :

- Nous allons vérifier la connexion du serveur postfix au base de données, en tapant la commande suivante : " *postmap -q medbejaia.dz mysql :/etc/postfix/mysql_ virtual_ domain_ maps.cf* " (Figure 4.41).

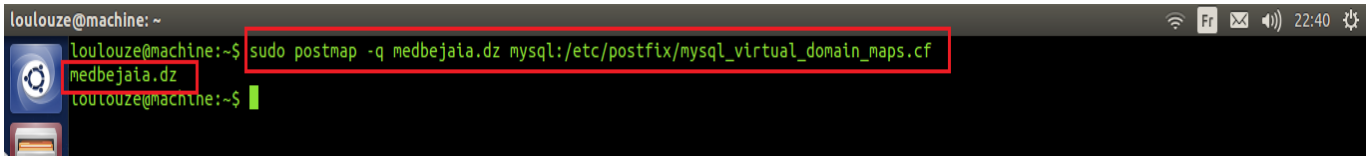

FIGURE 4.41 – Résultat de la commande Postmap.

La commande nous permet de passer en paramétre notre nom de domaine, pour vérifier son existance dans la base de données. Si la requête est bien exécutée, elle nous retourne le nom de domaine introduit.

- Nous allons essayer de se connecter en pop3 sécurisé en ssl (pop3s), en utilisant la commande suivante : " *openssl s_ client -connect mail.medbejaia.dz :pop3s* " (Figure 4.42).

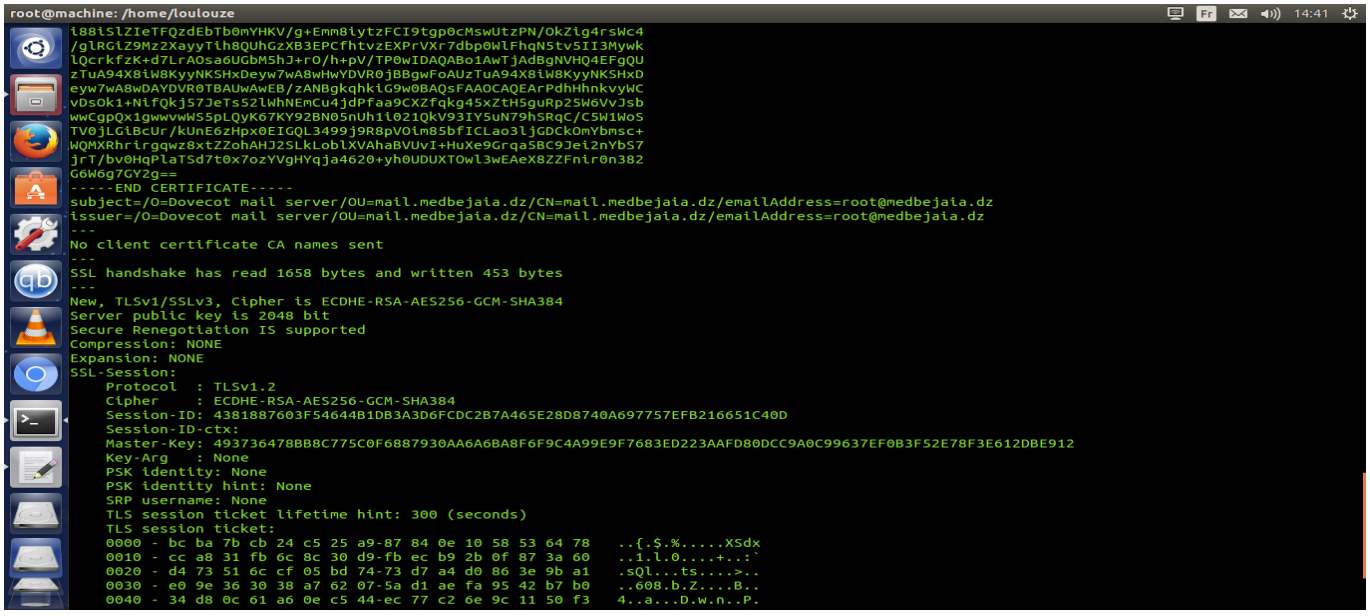

FIGURE 4.42 – Résultat de la commande Openssl.

La figure nous montre les différentes inforamtions du certificat SSL pour chiffrer la session.

4.2.8 Installation d'un webmail : Squirrelmail

Une fois, les vérifications sont faites. Nous Passons à l'installation d'un webmail, nous avons choisi " *Squirrelmail* " (Figure 4.43). Pour l'installer, nous tapons la commande sui-

vante *"apt-get install squirrelmail"*. Une fois l'installation terminée, il suffit de taper *"webmail.medbejaia.dz"* dans la barre d'URL pour y accéder.

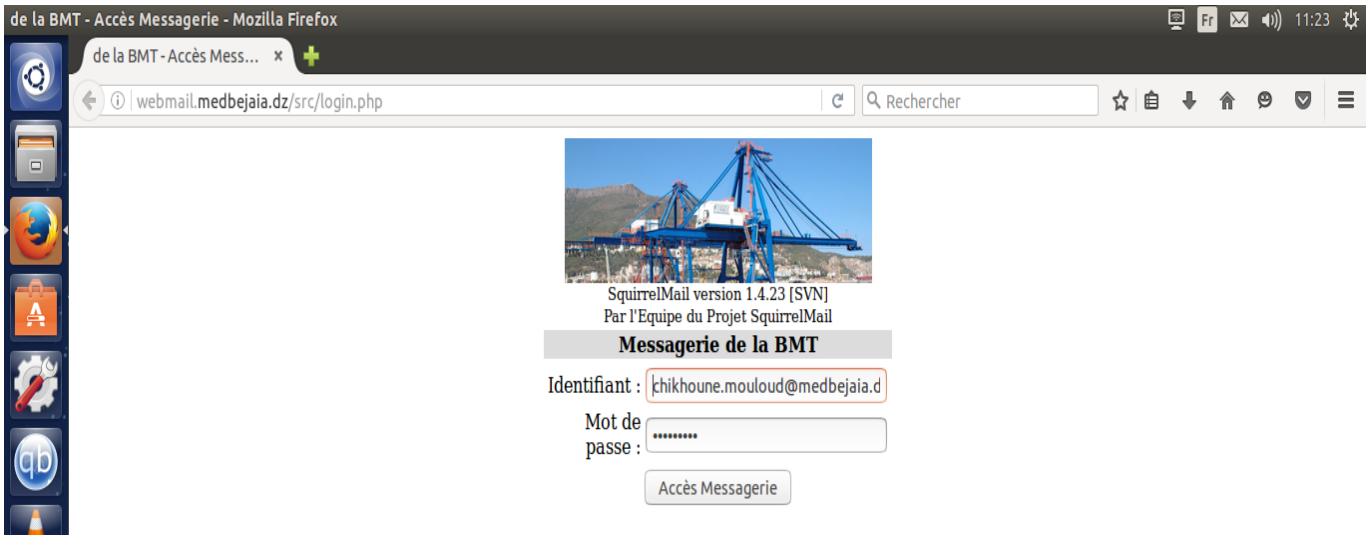

FIGURE 4.43 – Squirrelmail.

4.3 Administration de serveur de messagerie

Dans cette section, nous nous focalisons sur l'administration de notre serveur de messagerie. Nous avons mentionné bien avant que l'interface web *" postfixadmin "* nous permet d'administrer le serveur de messagerie (Figure 4.19).

- **Gérer la liste des administrateurs**

Nous pourrons ajouter d'autres administrateurs, pour administrer le serveur de messagerie et voir la liste des administrateurs actuels (Figure 4.44).

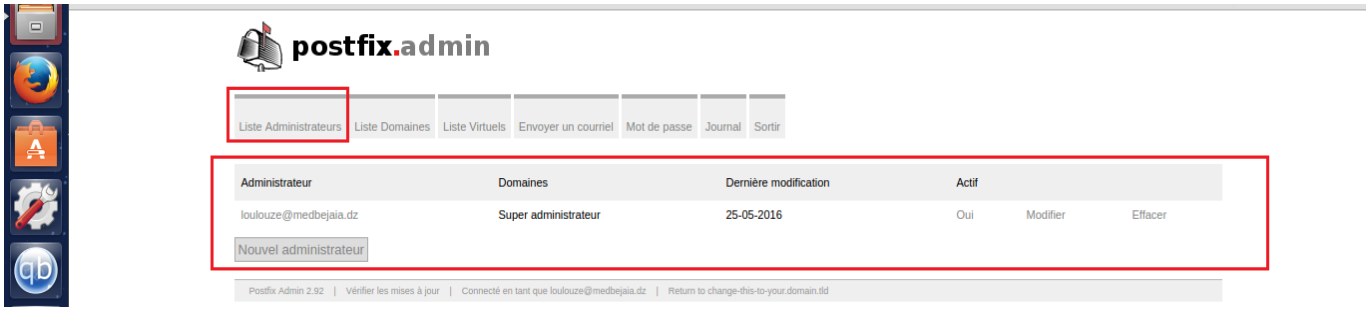

FIGURE 4.44 – Ajouter un administrateur.

- **Gérer la liste des domaines**

Nous ajoutons un domaine, qui permet d'envoyer des mails entres le personnel d'entrprise (Figure 4.45).

FIGURE 4.45 – Ajouter un domaine.

- **Gérer la liste des utilisateurs**

Postfixadmin nous donne la possibilité d'ajouter les utilisateurs virtuels via une interface web (Figure 4.46) .

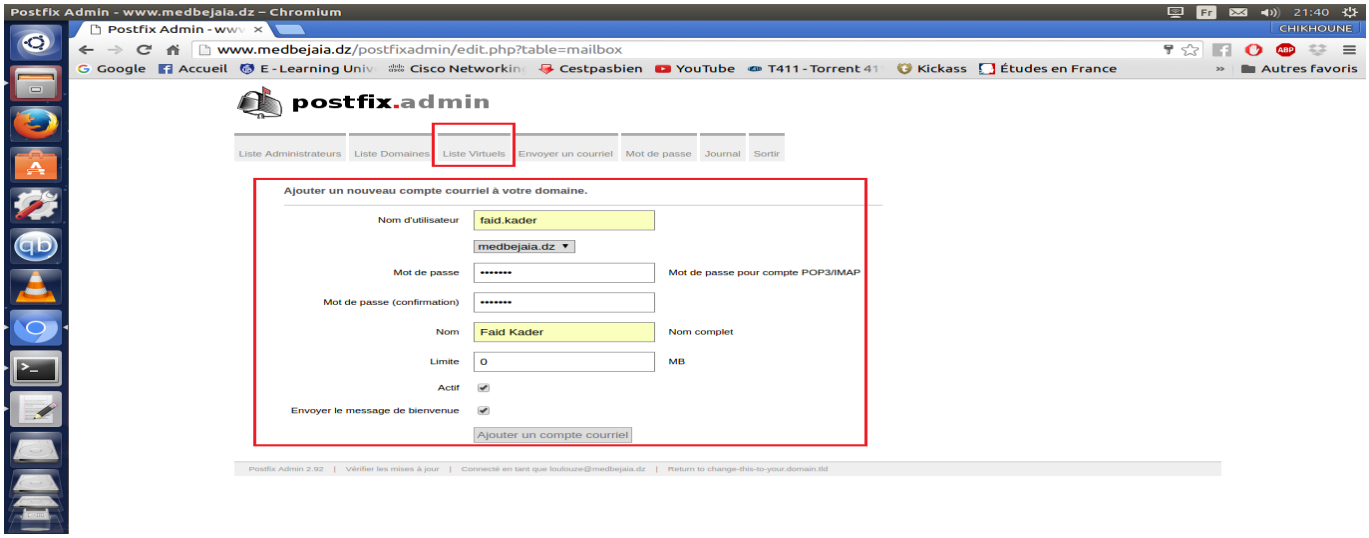

FIGURE 4.46 – Ajouter un utilisateur.

Nous pouvons gérer (modification, supression, activation) les utilisateurs virtuels (Figure 4.47).

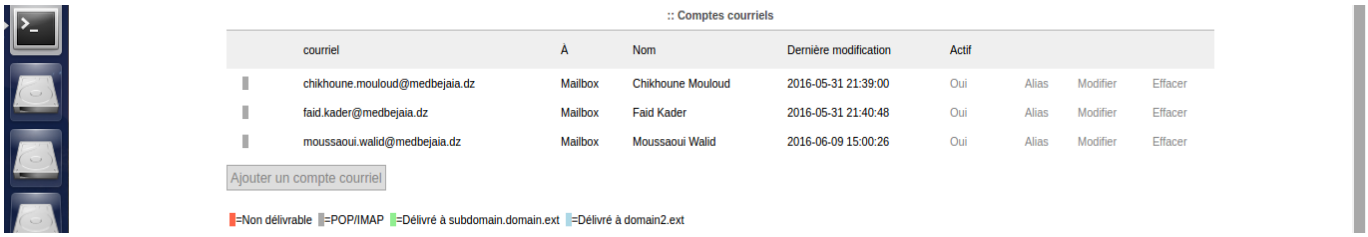

FIGURE 4.47 – La liste des utilisateurs.

4.4 Application

Dans cette phase, nous allons mettre en pratique toutes les configurations faites précédement. Pour accéder au webmail de l'entreprise de BMT, il suffit de taper dans la barre l'URL : *" webmail.medbejaia.dz "*, une interface de *" squirrelmail "* sera affichée (Figure 4.43). En entrant le nom d'utilisateur, avec le mot de passe, nous aurons la page principale montrée dans (Figure 4.48).

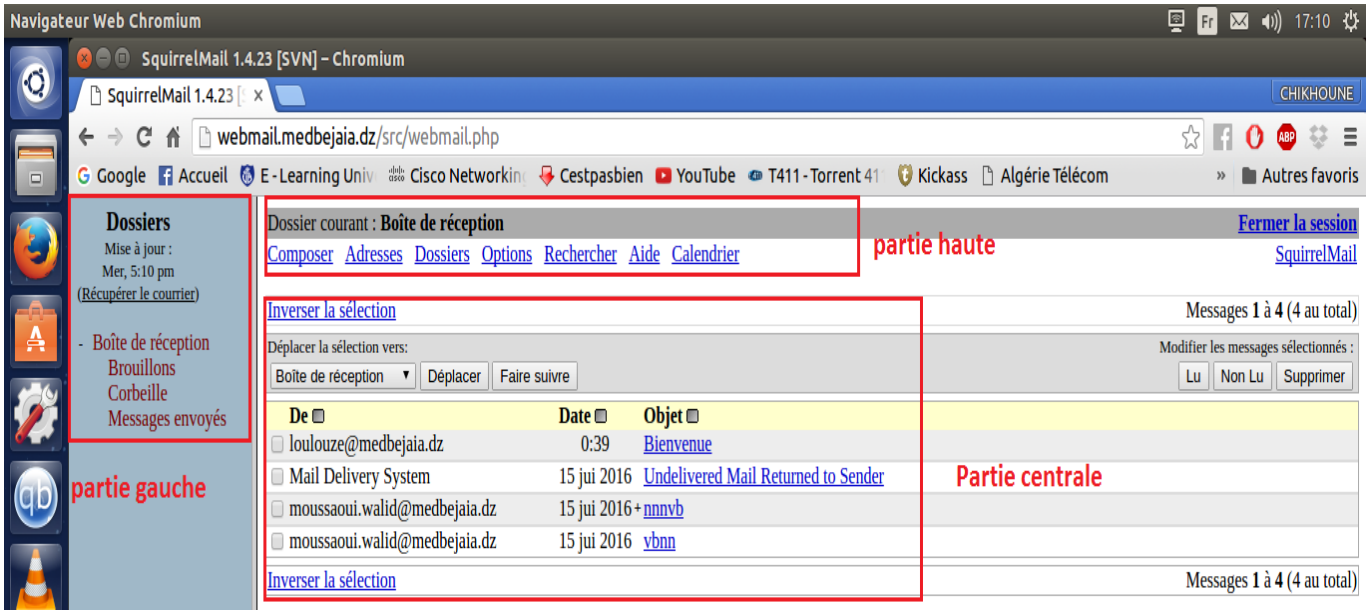

FIGURE 4.48 – la page principale de squirrelmail.

Une fois l'utilisateur est accédé dans sa boîte de couriel, un message et un lien sont adressés par l'administrateur de serveur de messagerie pour changer son mot de passe (Figure 4.49).

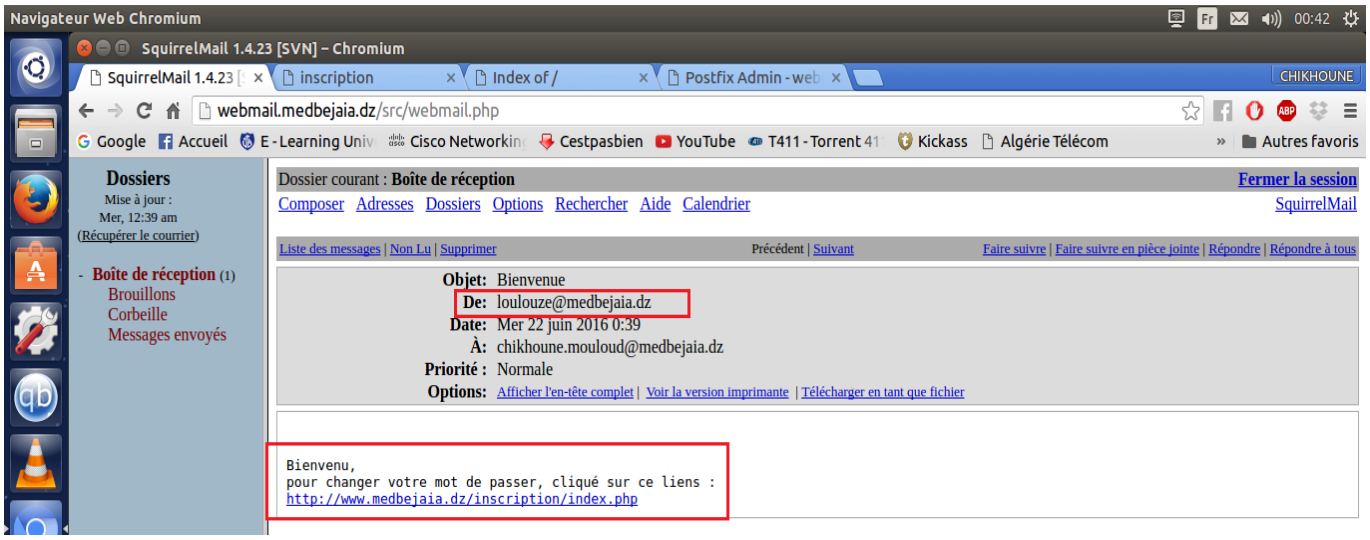

FIGURE 4.49 – Le message de l'administrateur.

En cliquant sur le lien, une page d'athentifiaction est affichée (Figure 4.50).

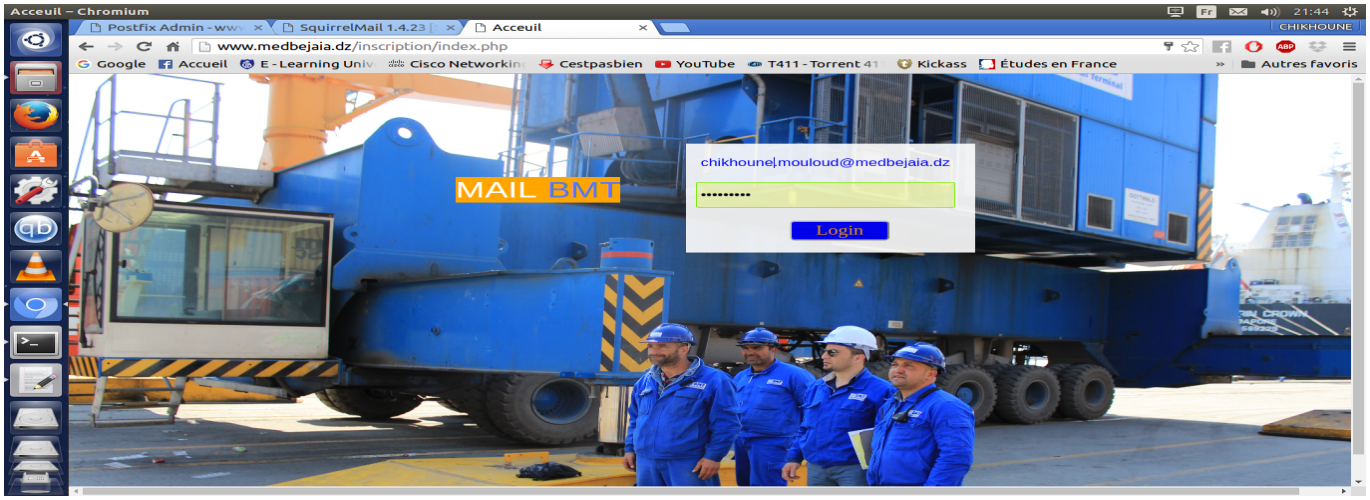

FIGURE 4.50 – La page d'authentification.

Aprés l'athentification, l'utilisateur accéde à une page dant laquelle il va introduire les informations demandées dans le formulaire (Figure 4.51).

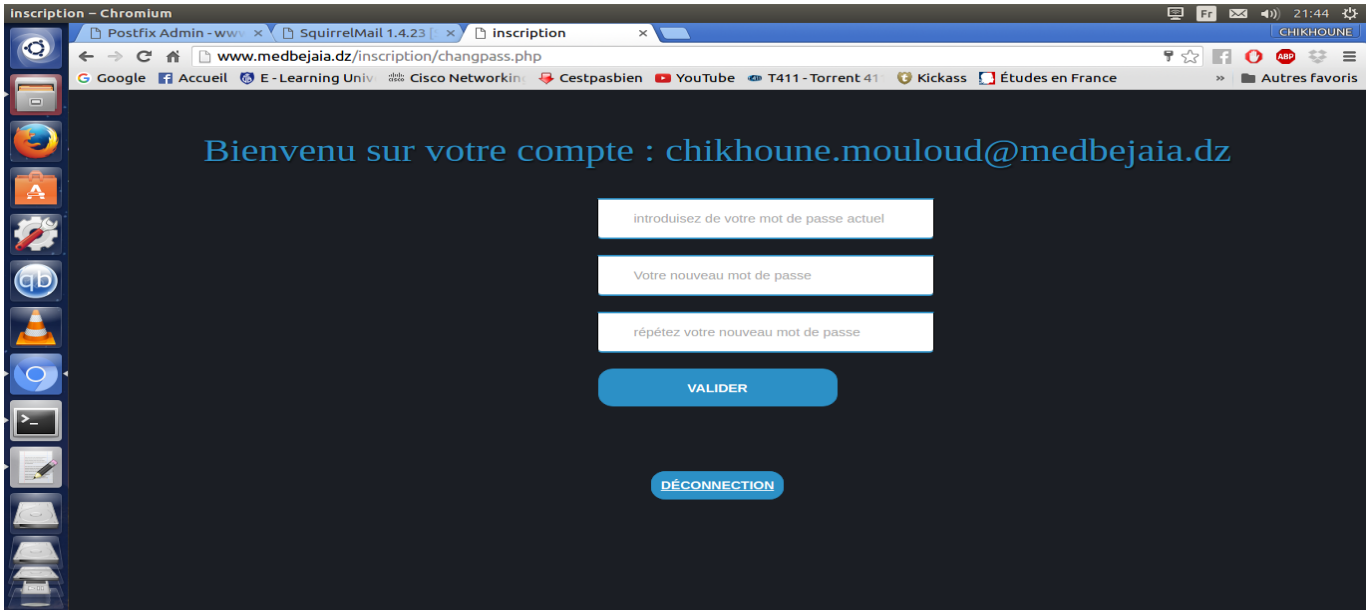

FIGURE 4.51 – La page de changement de mot de passe.

Une fois l'utilisateur a changé son mot de passe, il pourra ensuite utiliser les fonctionnalités de la page principale (Figure 4.48) , qui comporte trois parties :

- La liste des dossiers (partie gauche)
  - "Boite de réception" : dans laquelle les messages reçus sont stockés par défaut,
  - "Brouillons" : permet de stocker temporairement des messages en cours de rédaction pour un envoi ultérieur,
  - "Messages envoyés" : contient une copie de chaque message que nous envoyons,
  - "Corbeille" : contient les messages supprimés.
- Menus (partie haute)

  Se trouve au sommet de la page permettant plusieurs actions :
  - "Composer", pour rédiger un message,
  - "Adresses", pour créer et utiliser le carnet d'adresses,
  - "Dossier", pour gérer les dossiers par défaut ou de créer des nouveaux dossiers ,
  - "Options", permet la personnalisation de l'environnement (modifier les informations personnelles),
  - "Rechercher", nous aide à rechercher un ou plusieurs messages dans nos dossiers,

- "Fermer la session",permet de se déconnecter du webmail et de retourner à la page d'accueil.

- Liste des messages d'un dossier (partie centrale)

  La partie où sont affichés les messages du dossier sélectionné dans la partie gauche de la fenêtre. Organiser selon Une barre de menu avec trois champs (De, Date et Objet) est située juste en dessous. Les messages non lus apparaissent en gras. Pour lire un message il suffit simplement de cliquer sur le sujet (objet) du message. Une ligne se trouve sous le menu, nous informe, le nombre de mail contenu dans ce dossier. Juste en dessous est placé une barre contenant des boutons :

  - Déplacer, qui va déplacer les messages sélectionnés vers le dossier choisi à gauche de ce bouton,
  - Supprimer et Purger, pour effacer les messages sélectionnés,
  - D'autres pour marquer le message comme lu ou non lu et l'autre pour faire suivre.

Nous allons donner un aperçu de quelques actions du menu :

- **Composer**

La fenêtre suivante (Figure 4.52) permet de composer un message :

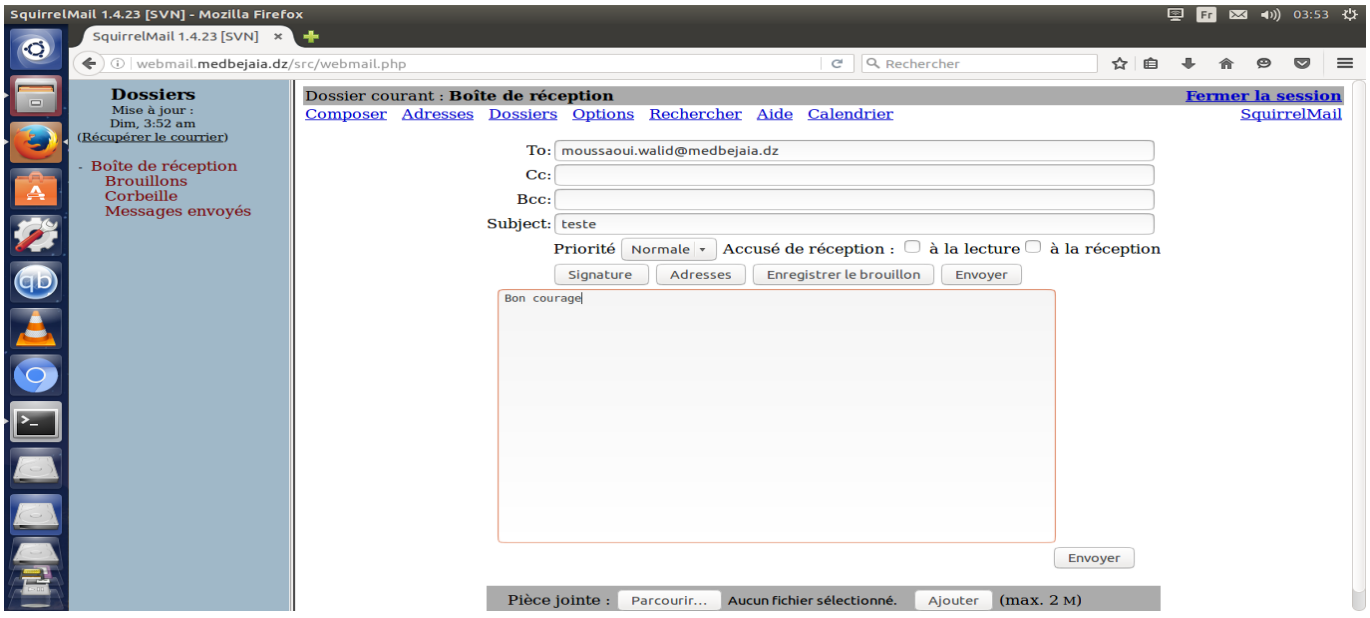

FIGURE 4.52 – Composer un message.

- **Rechercher**

Cette action (Figure 4.53) permet au personnel de faire une recherche sur les messages reçus et envoyés :

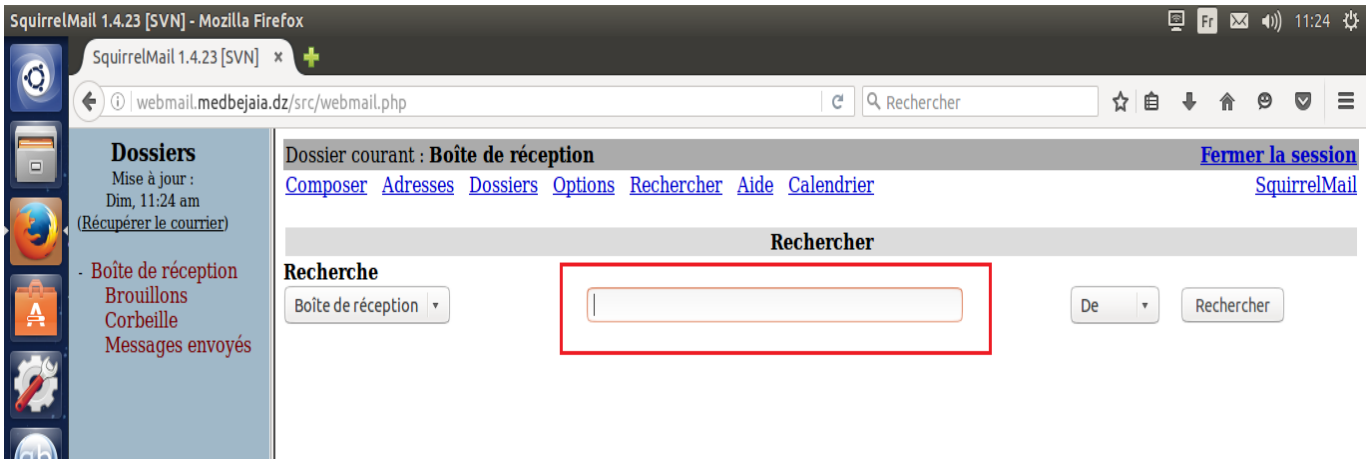

FIGURE 4.53 – Fenêtre de recherche.

- **Adresse**

Le répertoire (Figure 4.54) nous permet un gain de temps appréciable. Il permet d'enregistrer les adresses électroniques des utilisateurs courants.

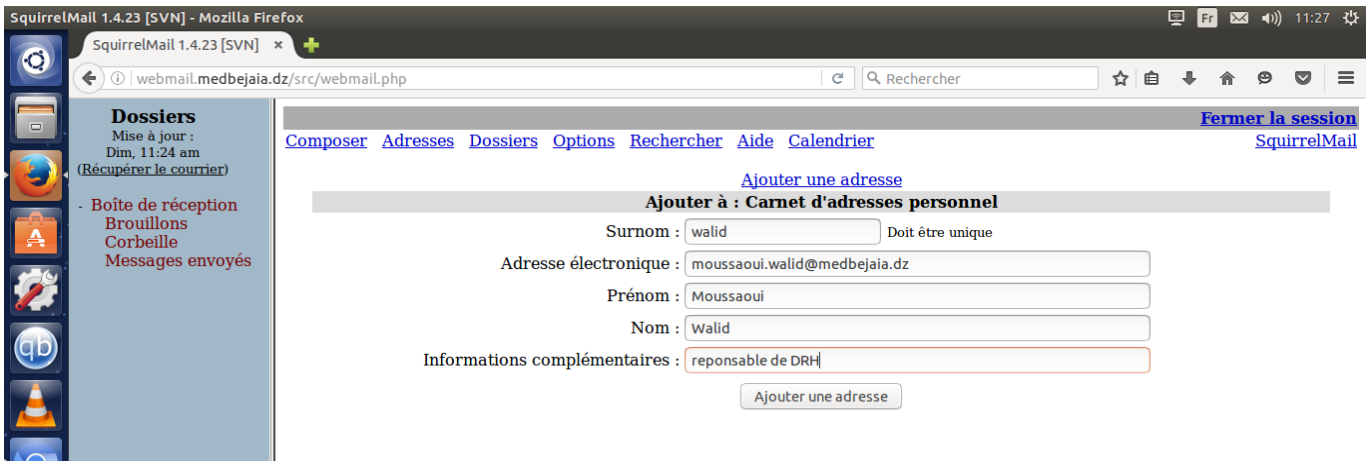

FIGURE 4.54 – Carnet d'adresses.

4.5 Conclusion

Ce chapitre a été consacré à la phase de réalisation de notre projet. Nous avons montré les différentes étapes d'installation et de configuration, ainsi que quelques contextes de sécurité de serveur de messagerie. Et en fin nous avons présenté l'utilisation de quelques fonctionnalitées de notre serveur de messagerie.

CONCLUSION GÉNÉRALE ET PERSPECTIVES

C'est dans le but de mettre en œuvre notre proposition et suggestion, à la BMT de Bejaia, qui est l'administration et la mise œuvre d'un serveur de messagerie, que nous avons réalisé ce projet, qui est le thème de notre projet fin d'études. Après avoir étudié les différents facteurs d'un système de messagerie, nous avons opté pour :

- Postfix, comme MTA.
- Squirrelmail, comme MUA.
- Dovecot IMAP et Dovecot POP, comme MDA.
- SSL, pour la sécurité du serveur.
- Anti-spam, antivirus.

Ces composants, nous les avons installés et configurés. Les étapes que nous avons suivies, sont citées explicitement dans le chapitre quatre. Ce projet a été une expérience, pour exploiter nos connaissances, nos capacités et d'affronter le domaine professionnel. En revanche, la sécurité d'un système de messagerie reste un problème majeur ; ce qui nous oblige à être à jour afin de maintenir sa sécurité. Enfin, nous espérons que notre travail saurait satisfaire Bejaia Mediterranean Terminal (BMT de Bejaia) et qu'il leur serait d'un bénéfice.

- **Perspectives**

- Mettre notre serveur de messagerie comme un relais SMTP,
- Sécuriser l'accés au serveur de messagerie avec le protocole ssh,
- Installation le serveur de massagerie au niveau des autres infrastructures du port de Bejaia.

BIBLIOGRAPHIE

[1] G.Pujolle. *Cours réseaux et télécoms.* Eyrolles, 2008.

[2] N.Pascla. *Cours de réseau mîtrise d'informatique.* Université d'angers, 2000.

[3] A.Baadache. *Réseaux étendus et réseaux d'opérations.* Université de Bejaïa, 2014.

[4] P.junior. *Les réseaux de zéro.* Livre de site de zéro, 2012.

[5] J.Pillou. *Tout sur les réseaux et internet.* 2éme édition, DUNOD, 2009.

[6] G.Gardrin et O.Gardrin. *Le Client-Serveur.* Paris, 2000.

[7] *Comprendre les mécanismes de routage et de commutation.* Ecole Supérieure d'Informatique de Paris, 2008.

[8] A.Sider. *Cours Technologie d'internet master 2.* Université de Bejaïa, 2016.

[9] www.mosaique-info.fr/489-serveur-de-messagerie definition.html. Accés, 2016.

[10] www.culture informatique.net/cest_quoi_un_serveur_dhcp_niv1/. Accés, 2016.

[11] www.linux france.org. Accés, 2016.

[12] E. Mabo. *La sécurité des systèmes informatiques (Théorie).* 2010.

[13] support de cours. *La sécurité des réseaux.* Université de Bejaïa, 2013.

[14] L.Bloch et C.Wolfhugel. *Sécurité Informatique-principes et méthodes.* 2007.

[15] R. Sidi Mohamed El Amine. *Mise en place d'un serveur radius sous linux pour la sécurisation d'un réseau 802.11.* Université Abou Bakr Belkaid, Tlemcen-Algérie, 20011.

[16] V.Erceau et R.Colombier. *GMSI Informatique.* 2011.

[17] R.Nait Bekou et Y.Moussahil. *Etude de fiabilité et conception d'une solution VPN*. Université Mohammed V SOUSSI, 2014.

[18] A.Boukeram. *Cours réseaux informatiques*. Université de Bejaïa, 2016.

[19] www.marche public.fr/Terminologie/Entrees/adresse_de_courrier_electronique.html. Accés, 2016.

[20] www.cri.u-bordeaux2.fr/index.php/messagerie/75 faq/313_boites_aux_lettres_fonctionnelles. Accés, 2016.

[21] www.commentcamarche.net/contents/structure-d-un-courrier-lectronique-enveloppe-entes-et cor.html. Accés, 2016.

[22] www.memoireonline.com/Mise-en-place-dun-systeme-de-messagerie-electronique-Cas-du-fonds-de-prevoyance militaire4.html. Accés, 2016.

[23] www.starxpert.fr/zimbra/les-atouts-de zimbra/. Accés, 2016.

[24] www.c2i.univ-littoral.fr/ressources2010/co/D11-7-logiciels 4.html. Accés, 2016.

[25] www.commentcamarche.net/contents/536-pop3-smtp-imap-protocoles-de-messagerie-le-protocole pop3. Accés, 2016.

[26] Club de la sécurité des systémes d'information Français. *Sécurité de la messagerie*. Paris, 2005.

[27] www.commentcamarche.net/contents/214-ssh-protocole-secure shell3. Accés, 2016.

[28] www.commentcamarche.net/contents/215-ssl-secure-sockets-layers-q_ssl-cur_1 url_ Accés, 2016.

[29] www.zdnet.fr/actualites/spamassassin-mode-d-emploi 39171310.html. Accés, 2016.

[30] https ://help.ubuntu.com/community/PostfixAmavisNew. Accés, 2016.

[31] www.doc.ubuntu fr.org/dovecot. Accés, 2016.

[32] www.doc.ubuntu fr.org/cyrus. Accés, 2016.

[33] www.google.com/Lan. Accés, 2016.

[34] www.google.com/architecture-client server. Accés, 2016.

[35] www.google.com/dhcp. Accés, 2016.

[36] www.google.com/DNS. Accés, 2016.

[37] www.google.com/Cryptage. Accés, 2016.

[38] www.google.com/par feu. Accés, 2016.

[39] www.google.com/vpn. Accés, 2016.