

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaia

Faculté des Sciences Exactes

Département D'Informatique



جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Mémoire de fin de cycle

En vue de l'obtention du diplôme master professionnel en informatique

Spécialité : Administration et Sécurité des Réseaux

Thème

**Mise en Place d'un Serveur de Messagerie Électronique
Au Sein de l'Entreprise Portuaire de Béjaia « EPB »**

Membres du jury :

Président : Mr. BAADACHE Abderrahmane

Examineur : Mr. SALHI Nadir

Invité : Mr. BONDIRRA Saïd

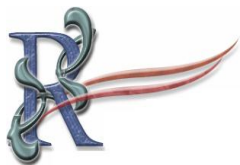
Encadreur : Mr. TOUAZI Djoudi

Présenté par :

MOAD Melkhir

MOULAI Mounira

Promotion 2016/2017



Remerciements

En premier lieu nos plus sincères remerciements vont au **bon Dieu** tout puissant qui nous avoir donné la grande volonté et un savoir adéquat pour mener à bien ce modeste travail.

Nos remerciements sont adressés également à nos **chers parents** pour tous les sacrifices consentis à notre égard et leur énorme soutien.

Nous tenons également, à exprimer notre sincère reconnaissance et notre profonde gratitude à **Pr. KAID TLILANE Nouara** pour son aide et ses précieux conseils.

Nos vifs remerciements, s'adressent à notre Encadreur **Mr. TOUAZI Djoudi** dont les conseils et orientation nous ont été précieusement utiles pour la réalisation de ce projet.

Nous remercions également **Mr. BOUNDERRA Said**, notre Co-promoteur de nous avoir proposé ce projet et aidé et assisté tout au long de sa réalisation.

Nous adressons un grand remerciement aussi à tout le personnel de l'Entreprise Portuaire de Béjaïa « EPB », en particulier, **Mr. BETTACHE Idir** directeur du service informatique qui nous a beaucoup aidé, guidé et conseillé tout au long de ce travail.

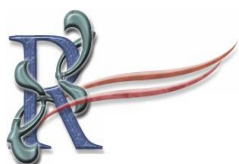
Nous remercions très respectueusement tous les membres de jury :

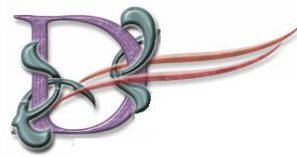
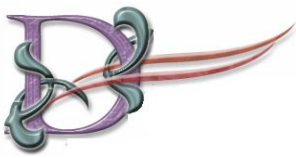
Mr. BAADACHE Abderrahmane qui nous a fait l'honneur de présider ce jury.

Mr. SALHI Nadir et **Mr. BONDIRRA Saïd** qui ont accepté d'examiner notre travail.

Enfin, nos remerciements s'adressent à toutes les personnes ayant contribué de près ou de loin à la réalisation de ce travail.

« **MERCI** »





Dédicaces

En signe de reconnaissance et de respect, je dédie ce modeste travail :

Aux deux êtres les plus chers au monde : **mes parents** qui m'ont aidé durant mes études, que Dieu les protège, les garde, leur prête une longue vie et une bonne santé.

A mes sœur **Chérifa, djawida.**

Mes frères **Nacer, loucif, jugurtha.**

A ma nièce **Maya.**

A mon mari **Belkacem** qui a toujours été présent et soutenu et lequel je ne remercierai jamais assez.

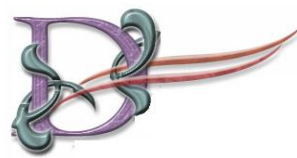
A ma **belle-famille** en particulier **Tarik.**

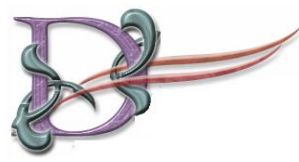
A ma chère binôme **Mounira** et **sa famille.**

A tous mes amis(es) : **Dihia (Ahlia), Sabrina, Chafiaa, Warda, Linda, Kousaila, Farid, Wahib, Sofiane, Lamine...**

Je remercie tous ceux et celles qui m'ont aidé à réaliser ce travail.

Melkhir.





Dédicaces

En signe de reconnaissance et de respect, je dédie ce modeste travail :

Aux deux êtres les plus chers au monde : **mes parents** qui m'ont aidé durant mes études, que Dieu les protège, les garde, leur prête une longue vie et une bonne santé.

A mes sœur **Nedjma, Chérifa, Sabrina, Assia.**

Mon frère **Fares.**

A mon cher **Wahib** qui a toujours été présent et soutenu et lequel je ne remercierai jamais assez ainsi que **sa famille.**

Ma chère binôme **Melkhir** et **sa famille.**

A tous mes amis(es): **Vanissa, Diana, Zina, Kahina, Siham, Samiha, Bilal, Arezki, Boualem, Haroun, Houa, Sofiane, Lamine, Tarik, Hicham, Sonia, Nora ...**

Je remercie tous ceux et celles qui m'ont aidé à réaliser ce travail.

Mounira.



Liste des figures

Figure I.1 :	Classification des réseaux.....	3
Figure I.2 :	Les sept couches du modèle OSI.....	6
Figure I.3 :	Les quatre couches du modèle TCP/IP.....	7
Figure I.4 :	Schéma de fonctionnement d'un système client/serveur.....	10
Figure II.1 :	Organigramme générale de l'Entreprise Portuaire de Béjaia.....	16
Figure II.2 :	Organigramme du département informatique de l'EPB.....	17
Figure II.3 :	L'architecture réseau de l'EPB.....	19
FigureIII.1 :	Réseau maillé de MTA.....	35
FigureIII.2 :	Acheminement de bout en bout.....	36
Figure IV.1 :	Lancement de l'installation de MariaDB.....	46
Figure IV.2 :	Bienvenue sur MariaBD.....	46
Figure IV.3 :	Acceptation du contrat de licence.....	47
Figure IV.4 :	Spécification du dossier d'installation de MariaDB.....	47
Figure IV.5 :	Définition du mot de passe pour L'utilisateur root de la base de données.....	48
Figure IV.6 :	Installation de MariaDB.....	48
Figure IV.7 :	Fin d'installation.....	49
Figure IV.8 :	Création de la base de donnée « mail1epb ».....	49
Figure IV.9 :	Création d'un utilisateur.....	50
Figure IV.10 :	Lancement de l'installation de HMailServer.....	50
Figure IV.11 :	Acceptation de la licence d'agrément.....	51
Figure IV.12 :	Choix du dossier d'installation du programme.....	51
Figure IV.13 :	La sélection des composants.....	52
Figure IV.14 :	Sélection d'un type de base de données.....	52
Figure IV.15 :	Choix du nom de l'icône.....	53
Figure IV.16 :	Insertion d'un mot de passe.....	53
Figure IV.17 :	Vérification des paramètres d'installation.....	54

Figure IV.18 : Installation HmailServer.	54
Figure IV.19 : Fin de l'installation d'HMailServer.	55
Figure IV.20 : La connexion au HmailServer.....	55
Figure IV.21 : Nom du domaine.	56
Figure IV.22 : Ajout des comptes.....	57
Figure IV.23 : Spécification du nom de hot publique.	58
Figure IV.24 : Paramètres IMAP.	58
Figure IV.25 : Détection de l'anti SPAM.	59
Figure IV.26 : Détection de l'Antivirus.	60
Figure IV.27 : Lancement de l'installation de Thunderbird.	61
Figure IV.28 : Choix du dossier d'installation.	61
Figure IV.29 : Installation de Thunderbird.....	62
Figure IV.30 : Fin d'installation.	62
Figure IV.31 : Aperçu de l'interface de Thunderbird.	63
Figure IV.32 : Ajout d'un compte avec Thunderbird.	64
Figure IV.33 : Recherche du fournisseur.....	64
Figure IV.34 : Spécification des protocoles de courrier entrant et sortant.	65
Figure IV.35 : Acceptation des risques.....	65
Figure IV.36 : L'envoi d'un message.	66
Figure IV.37 : La réception d'un message.....	66

Liste des Tableau

Tableau III.1 : Exemple de serveur de messagerie.	40
Tableau III.2 : Exemple de clients lourds de messagerie.....	41
Tableau III.3 : Exemple de clients légers de messagerie.	43

Table des matières

Liste des figures	I
Liste des tableau	III
Table des matières	IV
Liste des abréviations	VIII
Introduction générale.....	1

Chapitre I : Généralités sur les réseaux

Introduction	2
I.1. Les réseaux informatiques	2
I.2. Classification des réseaux	2
I.2.1. Les réseaux personnels (PAN: Personal Area Network).....	3
I.2.2. Les réseaux locaux (LAN : Local Area Network).....	3
I.2.3. Les réseaux métropolitaines (MAN : Metropolitan Area Network)	3
I.2.4. Les réseaux étendus (WAN: Wide Area Network)	3
I.3. Les réseaux internet	4
I.3.1. Les services internet.....	4
I.4. Les modèles de communication réseau	6
I.4.1. Modèle OSI.....	6
I.4.2. Modèle TCP/IP	6
I.5. La sécurité informatique	7
I.5.1. Principe de la sécurité informatique	7
I.5.2. Quelques techniques de protection	8
I.5.2.1. Les pare-feux(Firewall)	8
I.5.2.2. Le NAT (Natwork Address Translation).....	8
I.5.2.3. Les antivirus.....	8
I.5.2.4. La cryptographie	8

I.5.2.5. Serveur proxy.....	8
I.5.2.6. VPN (Virtual Private Network).....	9
I.5.2.7. Le DMZ (Demilitarized Zone)	9
I.6. L'architecture client/serveur	9
I.6.1. Présentation	9
I.6.2. Les avantages de l'architecture client/serveur	9
I.6.3. Les inconvénients du modèle client/serveur.....	10
I.6.4. Fonctionnement de l'architecture client/serveur	10
Conclusion.....	11

Chapitre II: Présentation de l'organisme d'accueil

Introduction	12
II.1. Présentation de l'Entreprise Portuaire de Béjaia (EPB).....	12
II.2. Missions et activité de l'EPB.....	12
II.2.1. Missions	12
II.2.2. Activités	13
II.3. Les différentes structures de l'EPB	13
II.4. Présentation du centre des systèmes et réseaux d'information de l'E.P.B..	17
II.4.1. Section système d'information	17
II.4.2. Section réseau	17
II.5. Les équipements informatiques utilisés à l'EPB	18
II.6. Le réseau informatique de l'EPB.....	19
II.7. Contexte du projet à réaliser	20
II.7.1. Présentation du sujet	20
II.7.2. Problématique	20
II.7.3. Objectifs.....	20
II.7.4. Hypothèses.....	21

II.7.5. Suggestions	21
Conclusion	22

Chapitre III: La messagerie électronique et les protocoles associés

Introduction	34
III.1. Serveur de messagerie électronique	34
III.2. L'adresse électronique.....	34
III.3. Les fonctionnalités de la messagerie électronique	34
III.4. Service de messagerie	35
III.4.1. Stockage et retransmission.....	35
III.4.2. Acheminement de bout en bout.....	36
III.4.3. Architecture modulaire d'un système de messagerie Internet	37
III.5. Les agents de messagerie	37
III.6. Les principaux protocoles de messagerie.....	38
III.7. Les différents outils de la messagerie électronique	39
III.7.1. Les serveurs de messagerie	39
III.7.2. Les clients de messagerie	40
III.7.2.1. Les clients lourds	40
III.7.2.2. Les clients légers ou webmail.....	42
III.8. Les risques d'un serveur de messagerie	43
III.8.1. L'infrastructure de l'entreprise	43
III.8.2. Le spam	43
III.8.3. Attaque par déni de service	43
III.9. Sécuriser le système de messagerie.....	43
Conclusion	44

Chapitre IV: Configuration et la mise en œuvre du système

Introduction	45
IV.1. Choix du serveur de messagerie.....	45
IV.1.1. Fonctionnalités de HMailServer	45
IV.1.2. Installation et configuration de HMailServer au sein de l'EPB :	45
IV.1.2.1. Installation de MariaDB	45
IV.1.2.2. Configuration de MariaDB	49
IV.1.2.3. Installation de HMailServer.....	50
IV.1.2.4. Configuration basique de HMailServer :.....	55
IV.2. Choix du client lourd	61
IV.2.1. Installation du client de messagerie Thunderbird.....	61
IV.2.2. Configuration du Client Thunderbird	63
Conclusion.....	67
Conclusion générale	68

Liste des Abréviations

DMZ	D emilitarized Z one.
EPB	E ntreprise P ortuaire de B éjaia.
EPE	E ntreprise P ublique E conomique.
FAI	F ournisseur d' A ccès I nternet.
FTP	P rotocole de T ransfert de f ichier.
HTML	H yper T ext M arkup L anguage.
HTTP	H ypertext T ransfer P rotocol.
IMAP	I nternet M essage A ccess P rotocol.
IP	I nternet P rotocol.
LAN	L ocal A rea N etwork.
MAN	M etropolitan A rea N etwork.
MDA	M ail D elivery A gent.
MTA	M ail T ransfert A gent.
MUA	M ail U se A gent.
MySQL	M y S tructured Q uery L anguage.
NAT	N etwork A ddress T ranslation.
NNTP	N etwork N ews T elnet P rotocol.
OOF	O ut of O ffice.
OSI	O pen S ystems I nterconnection.
PAN	P ersonal A rea N etwork.

POP Post Office Protocol.

SMTP Simple Mail Transfer Protocol.

SPA Société Par Actions.

TCP Transmission Control Protocol.

VPN Virtual Private Network.

WAN Wide Area Network.

WWW World Wide Web.

Introduction générale

Introduction générale

La technologie est aujourd'hui un élément fondamental pour toute entreprise. L'évolution dans le domaine de l'informatique offre des opportunités pour améliorer les processus de flux des travaux favoriser l'innovation et acquérir un avantage concurrentiel.

La diffusion des réseaux techniques de communication s'effectue dans un contexte de réorganisation des entreprises, on ne saurait le séparer.

Les outils de communication permettent d'organiser des groupes, dont les membres peuvent être géographiquement dispersés. L'internet offre plusieurs services : courrier électronique, forum de discussion, chat, commerce électronique, accès aux bases de données distantes, etc.

La messagerie électronique, le courrier électronique, le mail, sont différentes dénominations pour désigner l'outil de communication le plus connu et le plus coutumier des réseaux. Le courrier électronique permet d'échanger des messages et des documents annexes au message « pièces jointes ». Les correspondants d'une messagerie électronique doivent tout avoir une adresse électronique, une adresse de messagerie qui les identifie sur le réseau.

Le travail présenté dans ce mémoire concerne la mise en place d'un serveur de messagerie interne au sein de l'Entreprise Portuaire de Béjaia « EPB ». Il s'agit d'amélioration du système d'échange de l'information en quantité importante en temps réel ou dans des délais très courts pour :

- Offrir un ensemble d'outils collaboratifs qui permettent une meilleure interaction et transparence d'échange et le partage de ressources.
- Faciliter l'administration du serveur de messagerie.
- Amélioration des conditions de sécurité.

Pour mener bien notre travail, nous avons adopté la structure suivante:

- Le premier chapitre explique les généralités sur les réseaux Internet, les serveurs, l'architecture client/serveur, la sécurité des réseaux et quelques protocoles.
- Le second est consacré à la présentation de l'organisme d'accueil.
- Le troisième présente la messagerie électronique et les protocoles associés.
- Le quatrième chapitre décrit la configuration et la mise en œuvre du système.

Nous terminons par une conclusion et perspectives.

Chapitre I :

Généralités sur les

réseaux

Introduction

Vu l'évolution rapide de l'information et l'intérêt croissant de vouloir gagner en temps, de conserver les données, de limiter le nombre d'employés et pas mal d'autres raisons, ont poussé petites, moyennes et grandes entreprises à chercher des solutions informatiques capables de répondre à leurs besoins. Les réseaux informatiques sont devenus très vaste aujourd'hui, ils sont employés dans toutes les entreprises privés ou étatiques. Les réseaux couvrent complètement la planète grâce à divers équipements et l'apparition de l'Internet et le Web offrent des services énormes.

Dans ce chapitre, nous allons présenter quelques notions de base sur les réseaux informatiques en premier lieu, puis nous donnerons un aperçu sur les réseaux Internet, les modèles de communication réseau, la sécurité des réseaux, et nous terminerons par l'architecture client/serveur.

I.1. Les réseaux informatiques [1]

Ensemble d'ordinateurs (ou périphériques) interconnectés entre eux grâce à des lignes physiques ou sans fils et échangeant des informations sous forme de données numériques (des valeurs binaire, c'est-à-dire codées sous forme de signaux pouvant prendre des valeurs : 0 et 1), et parmi ces objectifs on trouve :

- ✓ Partage de ressources ainsi rendre accessible à chacun les données, les programmes et équipements indépendamment de leurs situation physique par rapport à l'utilisateur.
- ✓ Augmentation de la fiabilité faces aux pannes des machines en permettant de différentes copies d'un même fichier sur plusieurs machines.
- ✓ Faciliter le travail entre des personnes éloignées géographiquement.
- ✓ Gain du temps, d'argent et en infrastructures en partageant les données entre les différents périphériques.
- ✓ Communication entre des personnes éloignées grâce au courrier électronique ou discussion direct (chat).

I.2. Classification des réseaux [2]

La classification des réseaux peut être faite selon plusieurs critères, la plus évidente est celle qui considère le critère distance ou taille, la classification peut être aussi en fonction de la topologie:

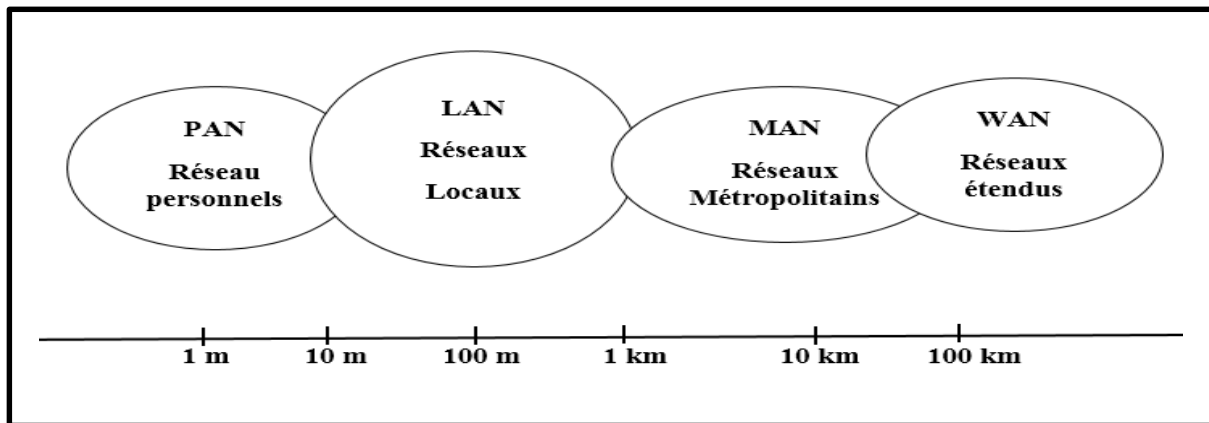


Figure I.1 : Classification des réseaux.

I.2.1. Les réseaux personnels (PAN: Personal Area Network)

Un réseau personnel permet l'interconnexion sur quelque mètre des équipements personnels tels que terminaux GSM, portables, organiseurs ... etc., d'un même utilisateur.

I.2.2. Les réseaux locaux (LAN : Local Area Network)

Un réseau local (LAN) correspond par leur taille aux réseaux intra-entreprises. Ils servent au transport de toutes les informations numériques de l'entreprise. En règle générale, les bâtiments à câbler s'étendent sur plusieurs centaines de mètres. Les débits de ces réseaux vont aujourd'hui de quelques mégabits à plusieurs centaines de mégabits par seconde.

I.2.3. Les réseaux métropolitaines (MAN : Metropolitan Area Network)

Un réseau métropolitain (MAN) permet l'interconnexion des entreprises ou éventuellement des particuliers sur un réseau spécialisé à haut débit qui est géré à l'échelle d'une métropole. Ils doivent être capables d'interconnecter les réseaux locaux des différentes entreprises pour leur donner la possibilité de dialoguer avec l'extérieur.

I.2.4. Les réseaux étendus (WAN: Wide Area Network)

Un réseau étendu (WAN) est destiné à transporter des données numériques sur des distances à l'échelle d'un pays, voire d'un continent ou de plusieurs continents. Le réseau est soit terrestre, et il utilise dans ce cas des infrastructures au niveau du sol, essentiellement de grands réseaux de fibre optique, soit hertzien, comme les réseaux satellite.

I.3. Les réseaux internet [3]

Internet signifie réseaux interconnectés (*interconnected networks*). Constitue un réseau qui relie dans le monde entier des ordinateurs en utilisant un protocole de transmission et de communication constituant un langage commun permettant la connexion de toute les machines (PC, Mac, Unix). Ce langage s'appelle la Transmission Control Protocol / Internet Protocol (**TCP/IP**).

Pour pouvoir se raccorder à l'Internet quatre aspects doivent être pris en compte :

- Posséder un ordinateur suffisamment puissant.
- Un modem suffisamment rapide.
- Un compte ouvert auprès de fournisseur d'accès Internet.
- Des logiciels spécifiques d'accès à l'Internet (navigateur...).

I.3.1. Les services internet [4]

La disponibilité d'une infrastructure de télécommunication comme Internet a permis le déploiement de devers services :

- ✓ **La recherche d'informations sur le WEB :** Le **Web** ou **WWW** (World Wide Web), que l'on pourrait traduire en français par «toile d'araignée mondiale», est aujourd'hui le service le plus connu et le plus utilisé d'Internet. Le Web est un ensemble de serveurs proposant des documents et des données accessibles à l'aide d'un protocole appelé HTTP. Il offre aux utilisateurs la possibilité de consulter en temps réel un vaste étendu d'informations, présentées sous différentes formes.
- ✓ **La messagerie électronique (Email):** est l'un des services les plus couramment utilisé sur internet, permettant à un expéditeur d'envoyé un message à un ou plusieurs destinataires. le principe d'utilisation du Courrier électronique est relativement simple. à la manière du service postal classique, il suffit de connaitre l'adresse de son expéditeur pour lui faire parvenir un message avec un cout réduit et une rapidité de transmission. De plus, le courrier électronique permet d'envoyer instantanément un courrier à plusieurs personnes simultanément.
- ✓ **Transfert de fichier (ftp) :** comme son nom l'indique protocole de transfère de fichier, il permet d'échanger des fichiers entre ordinateur (l'envoi et la réception) sur un réseau **TCP/IP**.

- ✓ **News** : c'est un ensemble de machines qui communiquent grâce au protocole NNTP (Network News Telnet Protocole), reliées aux différents réseaux mondiaux qui transmettent et relient les articles postés dans les groupes de discussion.
- ✓ **Chat** : il s'agit d'un système qui permet aux utilisateurs connectés à un serveur IRC (Internet Relay Chat) de communiquer à plusieurs en mode texte, dans des forums appelés canaux.
- ✓ **La téléphonie** : la téléphonie via internet et l'échange de communication audio en temps réel entre deux ordinateurs reliés à internet équipé chacun de carte sonore, de baffes et microphone. La plus challenge de l'information est de sortir internet de l'univers de l'ordinateur pour lui permettre de s'attaquer à la radio, la télévision et la téléphonie (fixe et mobile).
- ✓ **la visioconférence** : la visioconférence est la discussion en directe sur internet avec échange de son et d'image. Elle est destinée à ramener l'école et le travail à la maison, à réduire les frais de mission professionnelles en permettant aux hommes d'affaires de suivre des conférences dans le monde sans avoir à trop voyager et apportée l'aide et la connaissance aux gens géographiquement défavorisés (formation à distance, aide humanitaire,...).
- ✓ **Intranet** : est le synonyme de «réseau privé» s'appuie sur de nombreux services de communication et de travail coopératif :(la messagerie, circulation de documents, travail coopératif en temps partagé).
 - Intérêt de l'intranet :
 - permettre l'accès aux bases de données internes de l'entreprise.
 - Améliorer la productivité dans le partage des ressources et la recherche d'informations par la centralisation des données.
 - Intensifier la communication de groupe parmi le personnel connecté.
 - Contribuer à la mise en œuvre de certains services coopératifs.
 - Faciliter le partage des ressources et la communication.
- ✓ **Extranet** : Un extranet est une extension du système d'information de l'entreprise offrant à des partenaires situés au-delà du réseau un accès privilégié à certaines ressources informatiques de l'entreprise via une interface Web.

I.4. Les modèles de communication réseau

Pour assurer la bonne transmission de données d'une extrémité à l'autre d'un réseau avec une qualité de service exigée, il faut un support physique de communication et une architecture logicielle.

I.4.1. Modèle OSI [5]

Ce modèle a été créé par l'organisme ISO. C'est une norme internationale. Elle est implémentée dans presque tous les réseaux et la plupart des protocoles en sont dérivés. Les entreprises se sont rendu comptes que si tout le monde se basait sur les mêmes spécifications, la communication entre réseau serait énormément améliorée. Ce modèle est formé de sept couches ayant chacune des applications bien distinctes :

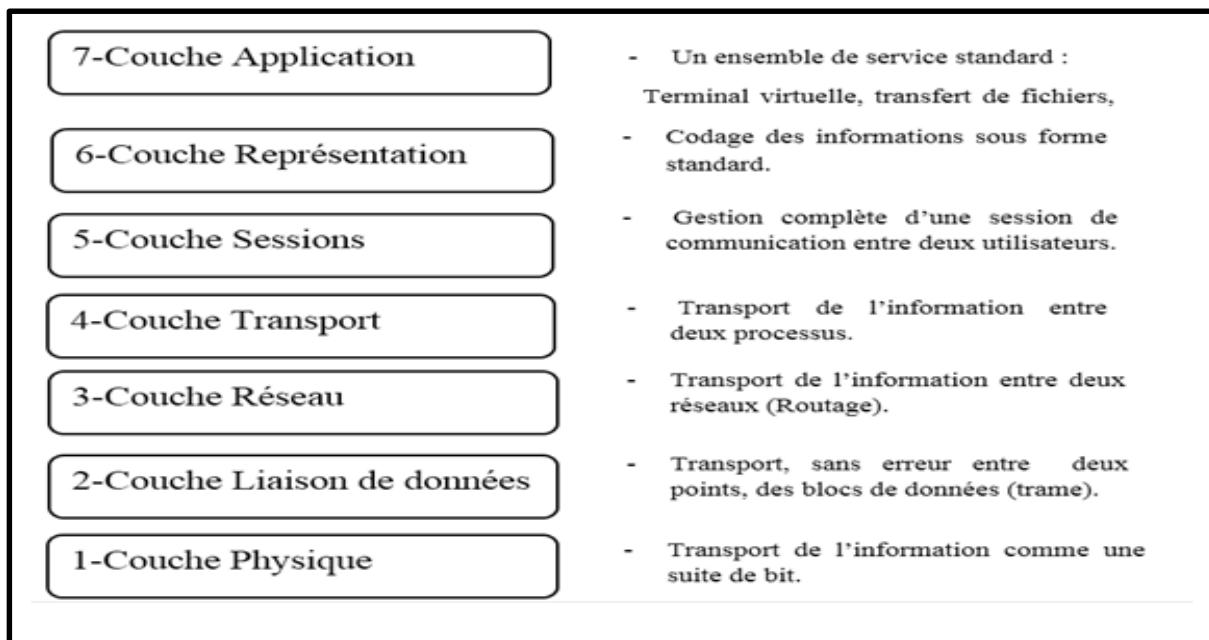


Figure I.2 : Les sept couches du modèle OSI.

I.4.2. Modèle TCP/IP [2]

Le modèle TCP/IP est un ensemble de protocoles, développés au début des années 70 par le département American de la défense afin de permettre l'interconnexion en réseau local des machines hétérogènes. Il contient 4 couches :

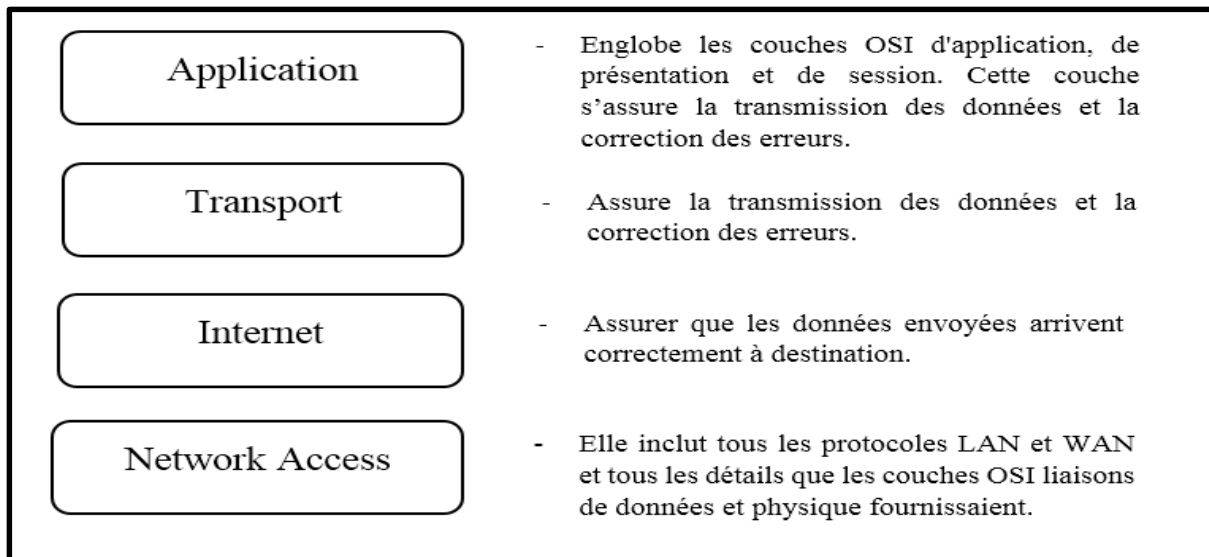


Figure I.3 : Les quatre couches du modèle TCP/IP.

I.5. La sécurité informatique [Web.1]

La sécurité informatique est de nos jours devenue un problème majeur dans la gestion des réseaux d'entreprise ainsi que pour les particuliers toujours plus nombreux à se connecter à internet.

La transmission d'informations sensibles et le désir d'assurer la confidentialité de celles-ci est devenue un point primordial dans la mise en place de réseaux informatiques.

I.5.1. Principe de la sécurité informatique

Les moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles:

- **Disponibilité** : demande que l'information sur le système soit *disponible* aux personnes autorisées.
- **Confidentialité** : demande que l'information sur le système ne puisse être *lue* que par les personnes autorisées.
- **Intégrité** : demande que l'information sur le système ne puisse être *modifiée* que par les personnes autorisées.
- **Non-répudiation** : les acteurs impliqués dans la communication ne peuvent nier y avoir participé.
- **Authenticité** : l'identité des acteurs de la communication est vérifiée.

I.5.2. Quelques techniques de protection

De nombreux moyens techniques sont mise en œuvre pour assurer la sécurité du système d'information :

I.5.2.1. Les pare-feux(Firewall) [5]

La plupart des réseaux privés sont munis d'un pare-feu (*firewall*), ordinateur qui filtre les communications, un peu comme un routeur d'ailleurs il est possible de configurer un routeur pour lui faire jouer le rôle d'un pare-feu simple. Un routeur doit décider au coup par coup du sort de chaque paquet, avec seulement une faible possibilité d'analyse historique, alors qu'un pare-feu efficace contre les attaques subtiles doit pouvoir faire des choses plus compliquées.

I.5.2.2. Le NAT (Network Address Translation) [5]

Le système de traduction d'adresses NAT (*Network Address Translation*) est apparu en 1994, initialement pour permettre la communication entre l'Internet et des réseaux privés contenant des adresses IP non conformes au plan d'adressage de l'Internet, et il a été ensuite très largement utilisé pour pallier le déficit d'adresses IP engendré par l'étranglement de la plage d'adresses de la version 4 du protocole. Il est devenu de ce fait à la fois une solution et un problème de sécurité des réseaux.

I.5.2.3. Les antivirus [5]

L'antivirus est un programme capable de détecter la présence de virus sur un ordinateur, ainsi il servira généralement à inspecter et désinfecter le disque dur (il convient de garder à l'esprit que certains virus s'exécutent en mémoire vive, sans s'enregistrer sur le disque).

I.5.2.4. La cryptographie [6]

La cryptographie permet généralement de se protéger contre de nombreuses faiblesses de sécurité et de contrôler la sécurité des systèmes d'information. Cette science peut cependant être aussi utilisée par les auteurs de virus afin de renforcer leur caractère nocif.

I.5.2.5. Serveur proxy [web.2]

Un serveur proxy est un ordinateur ou un module qui sert d'intermédiaire entre un navigateur web et l'internet. Le proxy participe à la sécurité du réseau.

I.5.2.6. VPN (Virtual Private Network) [web.3]

Un VPN (Virtual Private Network) est un type de réseau informatique qui permet la création de liens directs entre des ordinateurs distants.

Côté fonctionnement, le VPN repose sur la création d'un tunnel (via un protocole d'encapsulation) entre les deux ordinateurs. Bien que distants, ces deux ordinateurs sont alors connectés à un même réseau local, virtuel.

I.5.2.7. Le DMZ (Demilitarized Zone) [web.4]

Une zone démilitarisée (ou DMZ, de l'anglais *demilitarized zone*) est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet.

I.6. L'architecture client/serveur

I.6.1. Présentation [7]

Le client/serveur est une expression décrivant la relation qui existe entre un ordinateur client et un ordinateur serveur au niveau des applications mises en réseau. Le système client est en général l'ordinateur de bureau d'un collaborateur. Le serveur est le plus souvent un ordinateur de plus grande puissance qui peut stocker de gros volumes de données et servir à exécuter des programmes importants.

I.6.2. Les avantages de l'architecture client/serveur [Web.5]

Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité, ses principaux atouts sont :

- **Des ressources centralisées** : étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction.
- **Une meilleure sécurité** : car le nombre de points d'entrée permettant l'accès aux données est moins important.
- **Une administration au niveau serveur** : les clients ayant peu d'importance dans ce modèle, ils ont moins besoin d'être administrés.

- **Un réseau évolutif** : grâce à cette architecture il est possible de supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modification majeure.

I.6.3. Les inconvénients du modèle client/serveur

L'architecture client/serveur a tout de même quelques lacunes parmi lesquelles :

- **un coût élevé** dû à la technicité du serveur.
- **un maillon faible** : le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est architecturé autour de lui ! Heureusement, le serveur a une grande tolérance aux pannes (notamment grâce au système RAID).

I.6.4. Fonctionnement de l'architecture client/serveur

Un système client/serveur fonctionne selon le schéma suivant :

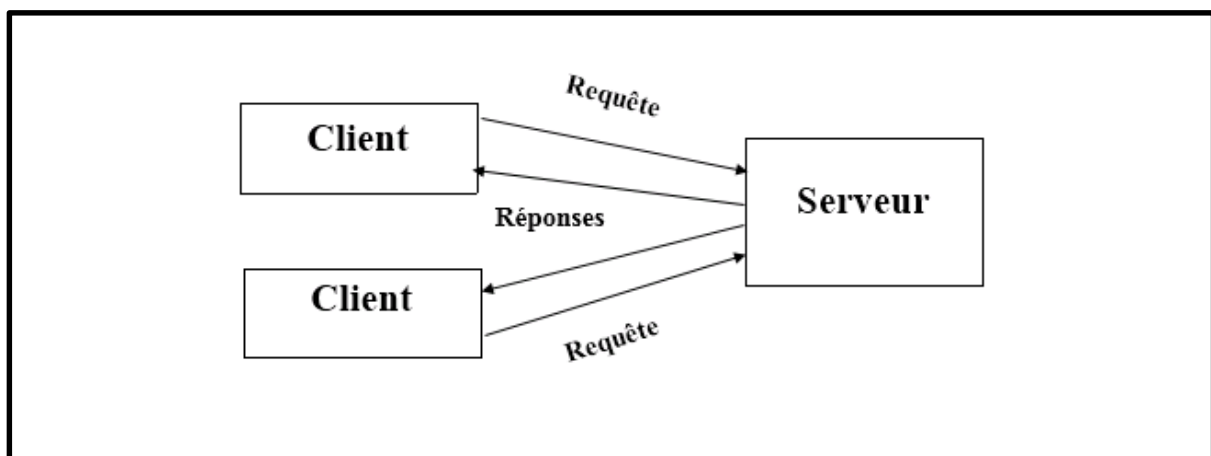


Figure I.4 : Schéma de fonctionnement d'un système client/serveur.

- **Client (client)** : C'est un processus demandant l'exécution d'une opération à un autre processus par envoi d'un message contenant le descriptif de l'opération à exécuter et attendant la réponse à cette opération par un message en retour.

Les caractéristiques d'un client :

- ✓ il est passif.
- ✓ il envoie des requêtes au serveur.
- ✓ il attend et reçoit les réponses du serveur.

- **Serveur (server) :** C'est un processus accomplissant une opération sur demande d'un client et transmettant la réponse à ce client.

Les caractéristiques d'un serveur :

- ✓ il est actif.
 - ✓ il est à l'écoute, prêt à répondre aux requêtes envoyées pas les clients.
 - ✓ dès qu'une requête lui parvient, il a traite et envoie une réponse au client.
- **Requête (request) :** C'est un message transmis par un client à un serveur décrivant l'opération à exécuter pour le compte du client.
 - **Réponse (reply) :** C'est un message transmis par un serveur à un client suite à l'exécution d'une opération contenant les paramètres de retour de l'opération.

Conclusion

Dans ce chapitre nous avons présenté quelques généralités sur les réseaux informatiques, nous avons évoqué les différents équipements qui le compose et aussi les moyens d'interconnexion. Nous avons référence OSI ainsi que le TCP /IP. Enfin nous avons illustré la sécurité informatique, ces principes et quelques techniques de protection.

Dans le chapitre qui suit nous allons aborder une présentation générale de l'organisme d'accueil.

Chapitre II :
Présentation de
l'organisme d'accueil

Introduction

Au cours de ce chapitre nous allons présenter l'organisme d'accueil : EPB (l'Entreprise Portuaire de Béjaia) au sein duquel nous avons effectué le stage relatif au présent projet, ses missions et activité ainsi que son organisation. Nous nous intéresserons plus exactement au centre informatique de l'EPB, à ces différents départements, service ainsi que sa méthode de sécurité.

II.1. Présentation de l'Entreprise Portuaire de Béjaia (EPB)

Vu la place et la position géographique du port de Béjaia, il joue un rôle très important dans les transactions internationales.

L'EPB a été créé le 14 août 1982 suite au décret n°82-285, elle est l'une des entreprises socialiste à caractère économique ; elle est transformée en Entreprise Publique Economique, Société par Actions (EPE-SPA).

Aujourd'hui, il est classé 2^{ème} port d'Algérie en marchandises générales et 3^{ème} port pétrolier. Il est également le 1^{er} port du bassin méditerranéen certifié ISO 9001.2000 pour l'ensemble de ses prestations, et à avoir ainsi installé un système de management de la qualité. Cela constitue une étape dans le processus d'amélioration continue de ses prestations au grand bénéfice de ses clients. L'Entreprise Portuaire a connu d'autres succès depuis, elle est notamment certifiée à la Norme ISO 14001 :2004 et au référentiel OHSAS 18001 :2007, respectivement pour l'environnement et l'hygiène et sécurité au travail.

II.2. Missions et activité de l'EPB

II.2.1. Missions

L'entreprise Portuaire de Béjaia a pour missions :

- La gestion, le développement et l'exploitation du domaine portuaire. dans le but de promouvoir les échanges extérieurs du pays.
- Elle est chargée des travaux d'entretien, d'aménagement, de renouvellement et de création d'infrastructures.
- L'EPB assure également des prestations à caractère commercial, à savoir ; le remorquage, la manutention et l'acconage.

II.2.2. Activités

Activités issues de l'objet statuaire de l'entreprise :

- Exploitation de l'outillage et des installations portuaires.
- Exécution des travaux d'entretien, d'aménagement et de renouvellement de la super structure portuaire.
- Elaboration avec autorités concernées de programmes d'entretien, d'aménagement et de création d'infrastructure portuaires.
- Exercice du monopole des opérations de pilotage, lamanage et remorquage.
- Exercice du monopole des opérations d'aconage et de manutention portuaire.
- L'exercice du monopole des opérations de remorquage, de pilotage et d'amarrage.
- Exercice des activités de police et la sécurité portuaire dans la limite géographique du domaine public portuaire.

II.3. Les différentes structures de l'EPB

L'EPB est organisé selon des directions opérationnelles et fonctionnelles:

➤ **Directions opérationnelles**

Elle s'agit des structures qui prennent en charge les activités sur le terrain et qui ont une relation directe avec les clients.

➤ **Direction Manutention et Aconage (DMA)**

C'est la direction qui est chargée de prévoir, organiser, coordonner et contrôler l'ensemble des actions de manutention et d'aconage liées à l'exploitation du port. La direction de manutention effectue la présentation de services qui se rapportent aux opérations de chargement et de déchargement des navires et aconage qui comprend les opérations tendant à assurer la réception, le pointage et la reconnaissance à terre des marchandises embarquées ou débarquées ainsi que le gardiennage, jusqu'à leur embarquement ou leur délivrance au destinataire.

➤ **Direction Domaine et Développement (DDD)**

A pour tâches :

- Amodiation et location de terre-pleins, hangar, bureaux, immeubles, installations et terrains à usage industriel ou commercial.
- Enlèvement des déchets des navires et assainissement des postes à quai.
- Pesage des marchandises (pont bascule).
- Avitaillement des navires en eau potable.

➤ **Direction Capitainerie (DC)**

Elle est chargée de la sécurité portuaire, ainsi que de la bonne régulation des mouvements des navires, et la garantie de sauvegarde des ouvrages portuaires.

Elle assure également les fonctions suivantes :

- **Pilotage** : La mise à disposition d'un pilote pour assister ou guider le commandant du navire dans les manœuvres d'entrée, de sortie. Cette activité s'accompagne généralement de pilotines, de canots et de remorqueurs.
- **Amarrage** : Cette appellation englobe l'amarrage et le désamarrage d'un navire.
- **Accostage** : Le port met à la disposition de ces clients des quais d'accostage en fonction des caractéristiques techniques du navire à recevoir.

➤ **Direction Remorquage (DR)**

Elle est chargée d'assister le pilote du navire lors de son entrée et de sa sortie du quai. Son activité consiste essentiellement à remorquer les navires entrants et sortants, ainsi que la maintenance des remorqueurs.

➤ **Directions Fonctionnelles**

Il s'agit des structures de soutien aux structures opérationnelles.

➤ **Direction Générale (DG)**

Elle est chargée de concevoir, coordonner et contrôler les actions liées à la gestion et au développement de l'entreprise.

➤ **Direction du Management Intègre (DMI)**

Elle est chargée de :

- La mise en œuvre, le maintien et l'amélioration continue du Système de Management Intégré (plans projets et indicateurs de mesure).
- L'animation et la coordination de toutes les activités des structures dans le domaine QHSE.
- La Contribution active à l'instauration et au développement d'une culture HSE au sein de l'entreprise et de la communauté portuaire.
- La Contribution dans des actions de sensibilisation et de formation à la prévention des risques de pollution, à la protection de l'environnement, la santé des travailleurs et à l'intervention d'urgence.

➤ **Direction Finances et Comptabilités (DFC)**

Elle est chargée de :

- La tenue de la comptabilité.
- La gestion de la trésorerie (dépenses, recettes et placements).
- La tenue des inventaires.
- Le contrôle de gestion (comptabilité analytique et contrôle budgétaire).

➤ **Direction Ressources Humaines (DRH)**

Elle est chargée de prévoir, d'organiser et d'exécuter toutes les actions liées à la gestion des ressources humaines en veillant à l'application rigoureuse des lois et règlements sociaux. Elle assure les tâches suivantes :

- La mise en œuvre de la politique de rémunération, de recrutement et de la formation du personnel.
- La gestion des carrières du personnel (fichier).
- La gestion des moyens généraux (achats courants, parc automobile, assurances, ...etc.).

La figure suivante illustre la hiérarchie des différentes directions de l'EPB :

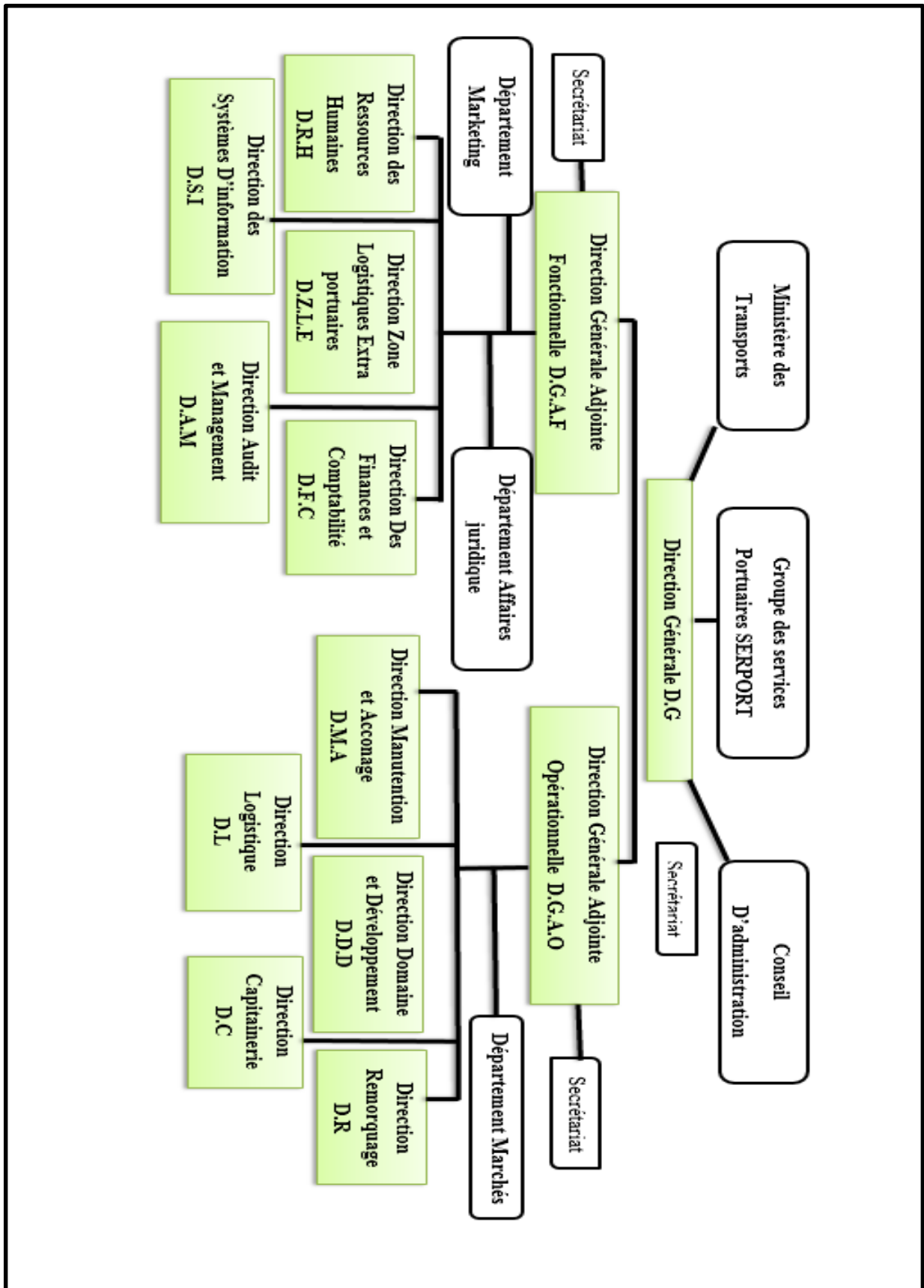


Figure II.1 : Organigramme générale de l'Entreprise Portuaire de Béjaia.

II.4. Présentation du centre des systèmes et réseaux d'information de l'E.P.B

L'EPB se constitue de deux sections : la section système d'information et la section réseau.

II.4.1. Section système d'information

La section système d'information a pour mission de mettre en œuvre la politique des systèmes d'information et des technologies de l'information et de la communication, la gestion d'une manière plus générale à tout ce qui touche au traitement automatique de l'information.

II.4.2. Section réseau

La section réseau a pour mission de maintenir le fonctionnement normal du réseau intranet de l'entreprise, d'assurer la sécurité des équipements réseaux et des services offerts par le réseau au système d'information et aux applications et enfin de fournir des services de connexion internet, de messagerie électronique, de support utilisateur.

La structure de système et réseau d'information de l'EPB est basée sur un plan d'urbanisation composé de :

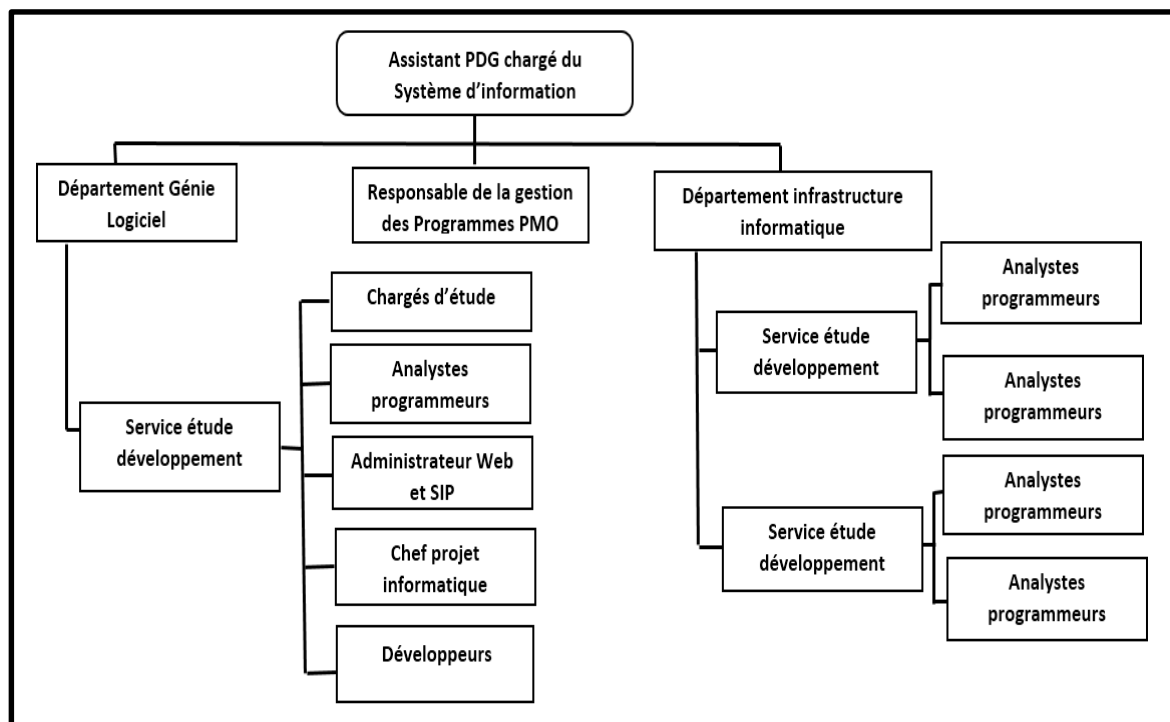


Figure II.2 : Organigramme du département informatique de l'EPB.

II.5. Les équipements informatiques utilisés à l'EPB

L'EPB dispose de 220 PC HP et ACER répartis à travers les différentes directions de l'entreprise et interconnecté à un réseau informatique constitué de fibre optique et de câbles à paires torsadés.

- Les systèmes d'exploitation utilisés sur les postes de travail sont Windows et Linux sous différentes distributions.
- La majorité des PC est reliée à des imprimantes de plusieurs types (matricielle, laser et à jet d'encre couleur).
- Chaque ordinateur est branché à un onduleur APC de 400 à 1000 VA.
- Tous les PC sont dotés d'un anti-virus ESET END point.
- Tous les PC sont connectés à l'internet.
- Deux contrôleurs de domaines DC1 et DC2 sous Windows Serveur 2012 et également serveur DNS en plus L'infrastructure de clés publiques PKI hébergées dans DC1, DC2 hébergera un serveur DHCP et aussi un serveur WDS (Windows Deployment Services).
- Deux serveurs de base de données en redondance sous Windows Server 2008.
- Un serveur de sauvegarde en réseau NAS intégrant le système RAID.
- Un serveur d'Application
- Un serveur de messagerie externe Microsoft Outlook.
- Un réseau Wimax composé de deux connexions internet (Algérie Télécom, Icosnet), elles sont reliées directement à un pare-feu PFSense configuré afin de garantir la haute disponibilité des dispositifs de sécurité et un contrôle total du flux entrant et flux sortant.

II.6. Le réseau informatique de l'EPB

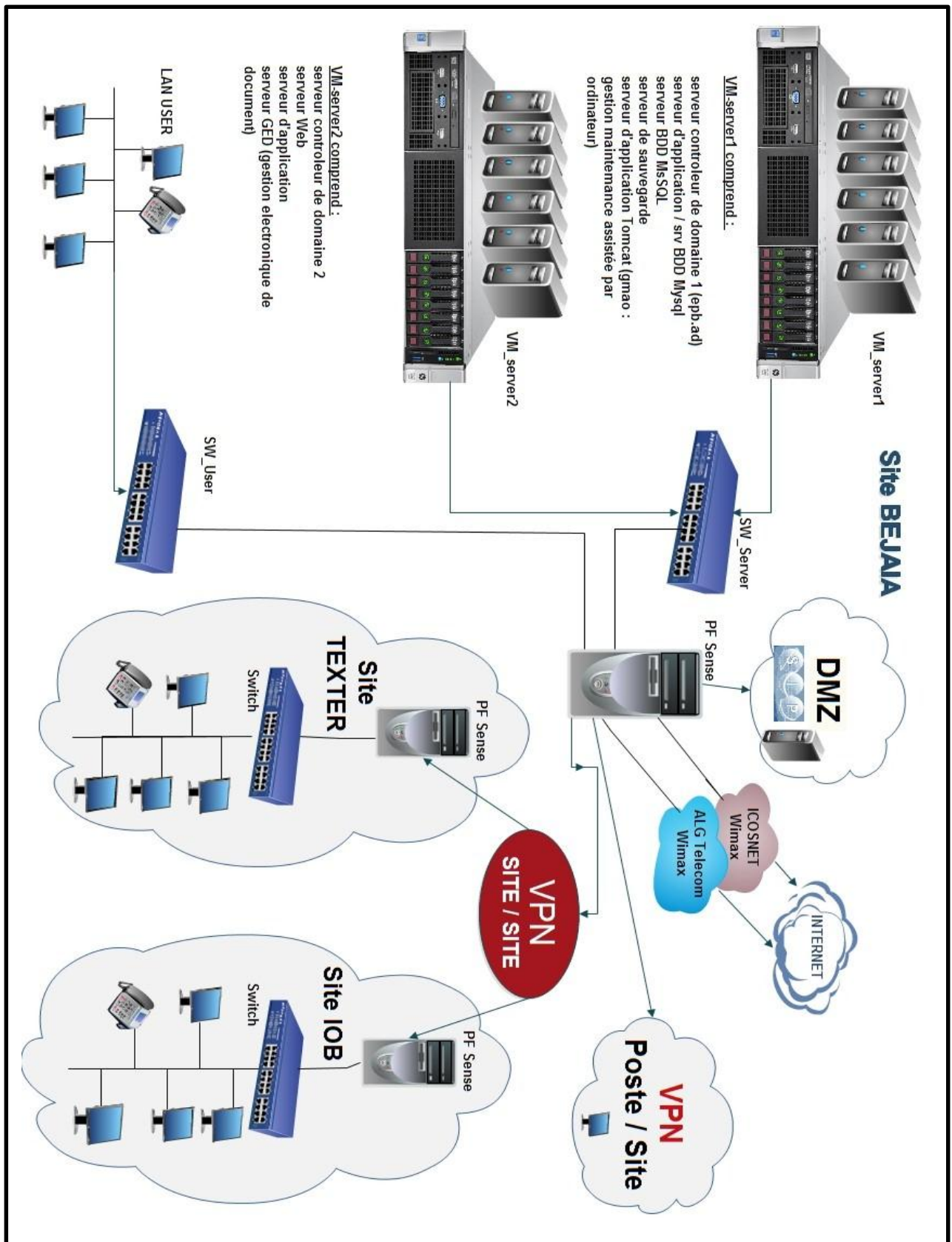


Figure II.3 : L'architecture réseau de l'EPB.

II.7. Contexte du projet à réaliser

Cette partie focalise sur la présentation du projet à réaliser, suivi de sa méthodologie.

II.7.1. Présentation du sujet

Au sein de l'EPB, de nombreuses informations, fichiers, documents sont échangés entre le personnel et ses services extérieurs, cette dernière souhaite faciliter cet échange. Les infrastructures et les normes qui permettant d'échanger aussi facilement et rapidement des messages à travers le monde sont nombreuses. On distingue le Web, les serveurs de messagerie électronique et protocoles de communication.

C'est dans ce cadre de projet de fin d'étude, que nous apportons des améliorations à leur système d'échange, en leur installant un serveur de messagerie électronique qui s'adapte aux besoins de l'entreprise.

II.7.2. Problématique

L'utilisation d'un serveur de messagerie électronique externe au niveau de l'EPB, engendre un certain nombre de problèmes tels que :

- Fusion des messages reçus/envoyer au niveau national et local.
- Le risque de perte de confidentialité des messages échangées, du fait d'un des membres du réseau internet par lequel transit le trafic entre le navigateur web et le serveur web mail.
- La distance, en cas de panne de connexion internet toute la correspondance devient indisponible.

On peut dire que la gestion des E-mails demeure donc une problématique très importante et un défi pour les années à venir alors que les échanges électroniques vont continuer à augmenter, sous forme ou sous la forme nouvelle des messageries instantanées.

II.7.3. Objectifs

Notre objectif est :

- Rédaction et envoi d'un mail très rapide à un ou plusieurs destinataires à la fois.
- Le message électronique peut être archivé et imprimé.

- Permettre à l'administrateur de :
 - Créer, détruire des comptes utilisateurs (boîtes aux lettres).
 - Créer, modifier des listes de diffusion (ensemble de destinataires réunis sous une même dénomination).
- Permettre à l'utilisateur de :
 - Rédiger, expédier et consulter les messages.
 - Classer les messages dans des dossiers
 - Répondre à un message sans avoir à retaper l'entête.
 - Utilisation de fonctions de recherches répondant à des critères : date, nom, sujet.
 - Création d'un annuaire personnel.

II.7.4. Hypothèses

- La mise en place d'un système de messagerie électronique pourrait améliorer considérablement les applications du système informatique dans notre entreprise.
- Du point de vue technique la messagerie présenterait les caractéristiques les mieux adaptées à la bonne utilisation des services de l'internet.

II.7.5. Suggestions

Pour résoudre à ces problèmes, on a décidé d'élaborer un système d'information permettant d'atteindre les objectifs suivants :

- Mise en place d'un serveur de messagerie (HmailServer) avec l'interface webmail Rundcube, qui sera propre à l'EPB pour une meilleure gestion.
- Faciliter l'administration du serveur de messagerie.
- Sécuriser le serveur à l'aide SSL.
- Pour plus de sécurité, le déploiement de notre serveur dans la DMZ existante dans l'entreprise.

Conclusion

Ce chapitre nous a permis de décrire l'organisme d'accueil de l'EPB, pour pouvoir comprendre le fonctionnement de ces différentes structures pour répondre mieux à ses besoin qui son spécifié dans le contexte, Ce qui engendre la nécessité de mettre en œuvre un serveur de messagerie dont les caractéristiques seront développées dans le chapitre qui suit.

Chapitre III :
La messagerie
électronique et les
protocoles associés

Introduction

Ce chapitre constitue une introduction sur le système de messagerie électronique, l'architecture et le principe de fonctionnement, les protocoles associés, la sécurité de la messagerie et les protocoles de sécurité.

III.1. Serveur de messagerie électronique [Web.6]

Un serveur de messagerie électronique est un logiciel serveur de courrier électronique. Il a pour vocation de transférer les messages électroniques d'un serveur à un autre. Un utilisateur n'est jamais en contact direct avec ce serveur mais utilise soit un client de messagerie, soit une messagerie web, qui se charge de contacter le serveur pour envoyer ou recevoir les messages.

La plupart des serveurs de messagerie actuels disposent des fonctions d'envoi et de réception, mais elles sont indépendantes, et peuvent être dissociées physiquement en utilisant plusieurs serveurs.

III.2. L'adresse électronique [Web.7]

L'adresse électronique est un service permettant à des utilisateurs d'échanger des messages via un réseau informatique. Pour pouvoir émettre et recevoir des courriers électroniques, la première condition est de connaître l'adresse électronique du correspondant et de posséder sa propre adresse. Une adresse électronique, aussi appelée « e-mail address », se présente sous forme suivante : nom@domaine.

Elle est composée de deux parties distinctes par le signe @. La partie nom précédant ce désigne le nom de la boîte aux lettres, qui correspond au nom de la machine jouant le rôle de serveur de messagerie.

III.3. Les fonctionnalités de la messagerie électronique [Web.8]

Les fonctionnalités de la messagerie électronique ou du courrier électronique sont nombreuses et s'apparentent aux différents services que propose la poste :

- **La boîte aux lettres** pour chaque utilisateur.
- **La notification personnalisée** interpelle en temps réel le destinataire qu'un courrier vient de lui parvenir.

- **L'accusé de réception** informe l'expéditeur que son message est bien arrivé.
- **La réponse** à un courrier peut inclure le message d'origine.
- **Les pièces jointes** annexés au message peuvent être de toutes les formes possibles (textes, photos, sons, vidéos, graphique, table d'une base de données, ...).
- **L'envoi en copie** du même message à un autre destinataire (avec le champ Carbon Copy).
- **L'expédition groupée** d'un même message à plusieurs destinataires.
- **L'annuaire** (Directory en anglais) répertorie tous les abonnés aux services de messagerie.
- **La récupération** des messages effacés par erreur.
- **L'absence de bureau** (OOO pour Out of Office en anglais) permet d'indiquer au correspondant que le destinataire de leur courrier n'est pas là et qu'il reviendra bientôt...

III.4. Service de messagerie

Le service de messagerie est constitué de deux entités distinctes qui coopèrent et communiquent par le biais de protocoles bien définis afin d'assurer un service entre utilisateurs :

III.4.1. Stockage et retransmission

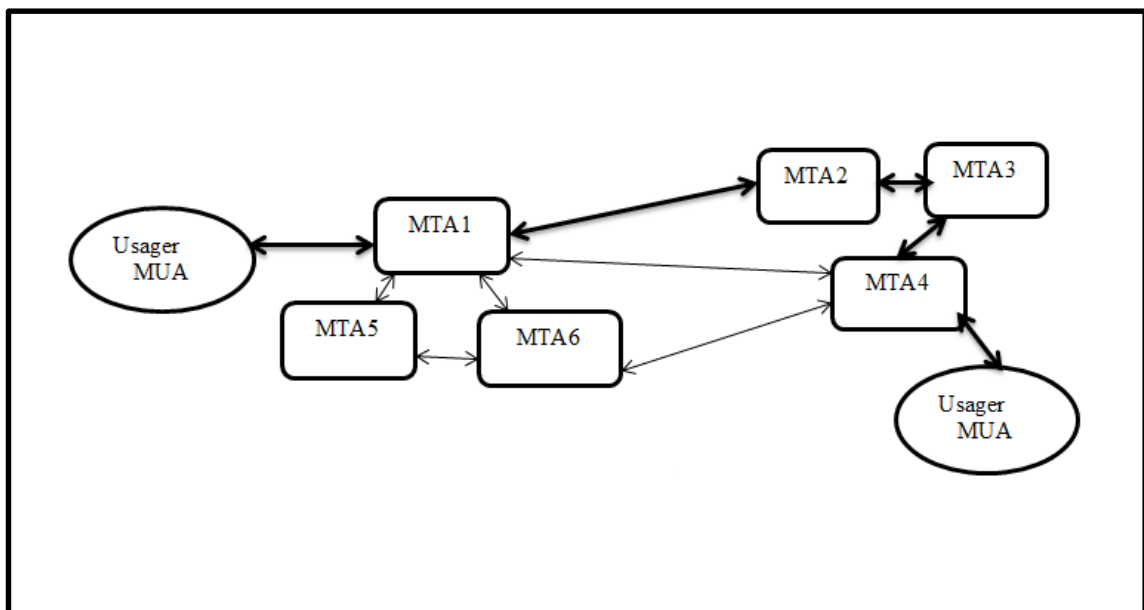
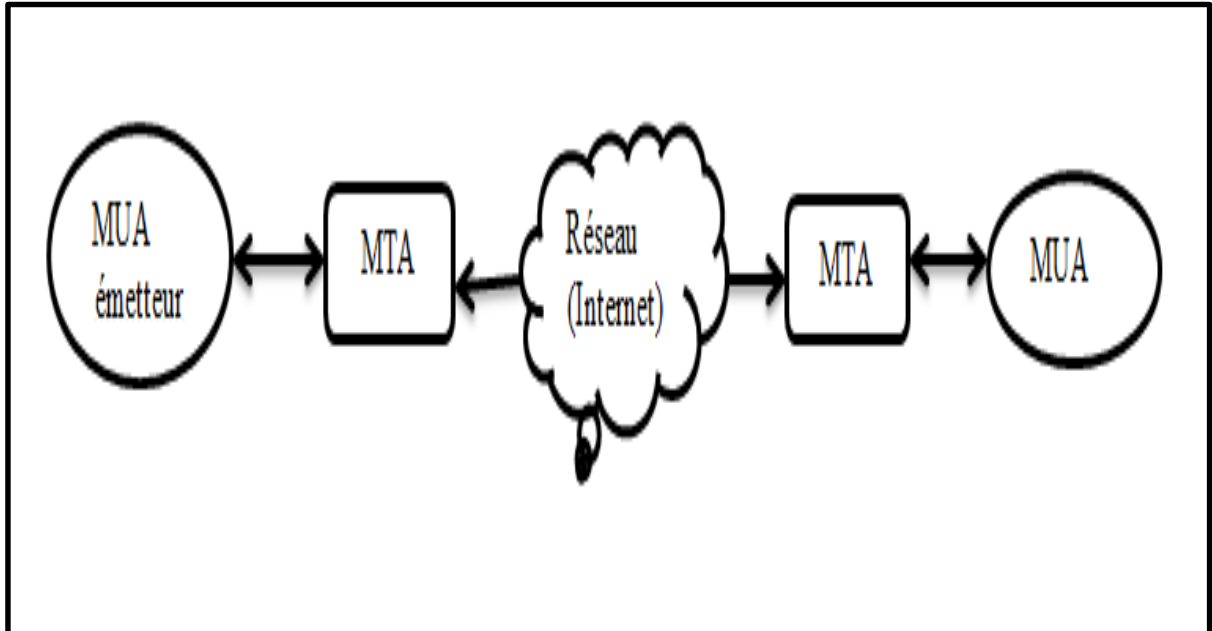


Figure III.1. Réseau maillé de MTA.

- La messagerie réalise l'acheminement des courriers comme le fait un réseau à **commutation de paquets**.

III.4.2. Acheminement de bout en bout



FigureIII.2. Acheminement de bout en bout.

- Un serveur de courrier utilise une connexion de bout en bout (transport) pour remettre ses messages => fiable et simple (si l'on dispose d'une couche transport fiable comme TCP).

III.4.3. Architecture modulaire d'un système de messagerie Internet

La figure suivante illustre l'architecture du système de messagerie électronique :

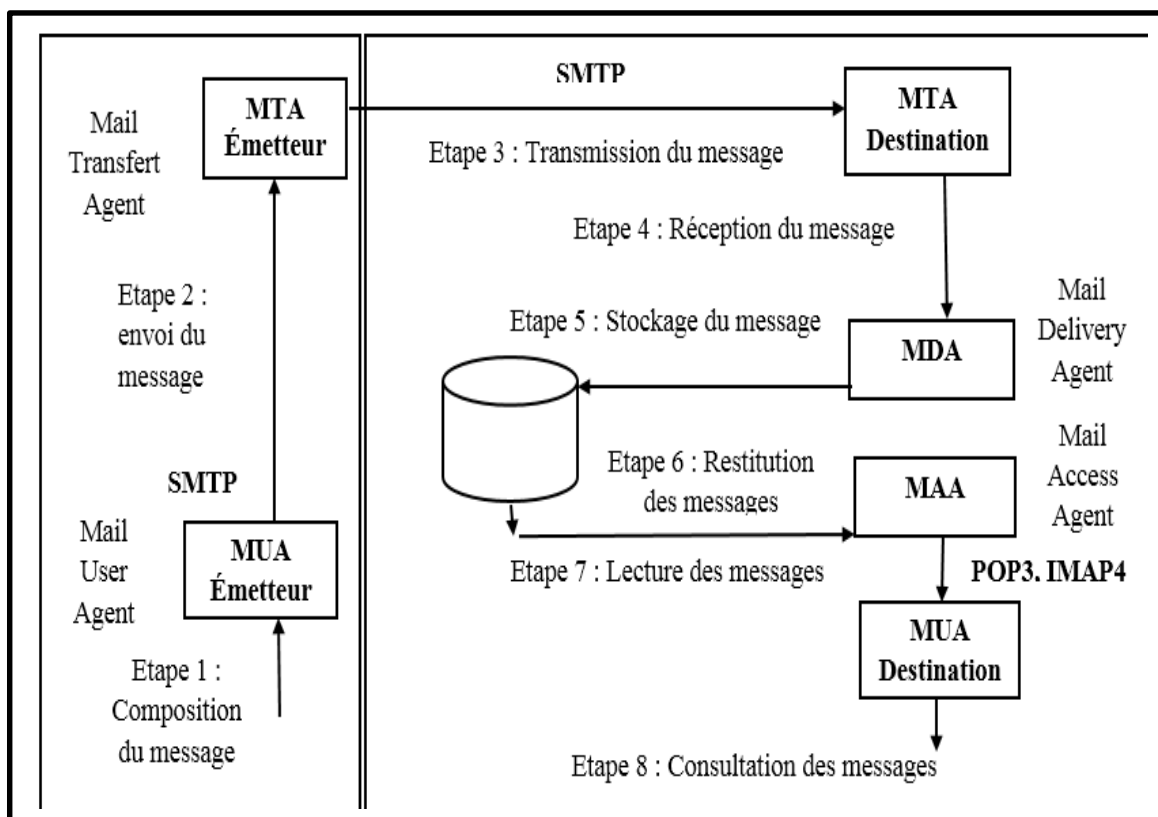


Figure III.3 Architecture du système de messagerie électronique.

III.5. Les agents de messagerie [Web.9] [Web.10]

- **LE MTA (Mail Transfert Agent ou Agent de transfert de courrier) :** Un agent de transport (MTA, Mail Transport Agent), aussi appelé serveur de messagerie, pour revêtir des formes très diverses. Toutefois, sendmail reste le plus utilisé sur Internet. Il existe depuis de nombreuses années, et les versions actuelles sont remarquablement stables et puissantes. Son seul défaut vient de sa popularité : il est la cible fréquente d'attaques ou tentatives de détournement de la sécurité.
- **Le MUA (Mail Use Agent ou Agent utilisateur de messagerie) :** L'agent utilisateur (MUA) est le programme dont vous vous servez pour communiquer avec le système de courrier électronique. Sous Linux l'agent utilisateur le plus simple se nomme mail. Il s'agit d'un client très limité; incapable d'utiliser le protocole POP3, il ne peut lire que les messages d'une boîte aux lettres locale. Toutefois, il suffit pour tester votre système de courrier électronique.

- **LE MDA (Mail Delivery Agent ou Agent de distribution locale) :** est le service de remise du courrier dans les boîtes aux lettres des destinataires. Le MTA transmet au MDA les messages destinés aux clients du domaine.

III.6. Les principaux protocoles de messagerie [Web.11][Web.12][Web.13]

Les trois principaux protocoles utilisés par un serveur de messagerie sont le SMTP (Simple Mail Transfer Protocol), le POP (Post Office Protocol) et l'IMAP (Internet Message Access Protocol).

- **Le protocole SMTP (Simple Mail Transfer Protocol) :** c'est le protocole standard permettant de transférer le courrier entre deux serveurs de messagerie - celui de l'expéditeur et celui du destinataire.
- **Le protocole POP3 (Post Office Protocole version 3) :** Il s'agit du protocole standard qui permet la récupération des mails situés sur un serveur distant (serveur POP). L'objectif de ce protocole est de relever le courrier électronique depuis un hôte qui ne contient pas sa boîte aux lettres. Il vient tout simplement télécharger les messages à partir du serveur et les stocke sur le poste de travail.
- **Le protocole IMAP4 (Internet Mail Access Protocole version 4) :** c'est un protocole utilisé par les serveurs de messagerie électronique. Ce protocole permet de laisser les e-mails sur le serveur dans le but de pouvoir les consulter de différents clients e-mails ou webmail. Il comporte des fonctionnalités avancées, comme les boîtes aux lettres multiples, la possibilité de créer des dossiers pour trier ses e-mails... Le fait que les messages soient archivés sur le serveur fait que l'utilisateur peut accéder à tous ses messages depuis n'importe où sur le réseau et que l'administrateur peut facilement faire des copies de sauvegarde.

III.7. Les différents outils de la messagerie électronique

III.7.1. Les serveurs de messagerie

Serveur de messagerie	Description	Avantages	Inconvénients
HmailServer	hMailServer est un serveur de courrier électronique open source supportant les protocoles POP3, IMAP et SMTP.	HmailServer est facile à installer et à paramétrer, il s'intègre sans difficultés dans un réseau intranet.	HmailServer lui manque quelques outils de messagerie comme : le forum et les news.
Postfix	Postfix est un serveur de messagerie et un logiciel libre, il se charge de la livraison des courriels.	Postfix est bénéficié de l'expérience de sendmail, facile à administrer, rapide et évolutif, compatibilité sendmail maximale.	L'inconvénient de postfix est son mode de configuration, manque de sécurité.
Exim	Exim est un serveur de messagerie très complet, il est utilisable dans de nombreux contextes.	Exim est facile et rapide à utiliser, simple à configurer.	L'inconvénient d'Exim la configuration plutôt difficile
QMail	Qmail est un serveur de messagerie, il permet de mettre en place un service SMTP permettant l'envoi de courriels.	Rapide, un fichier de configuration par module. Il est performant.	L'inconvénient de Qmail réside au niveau utilisation de la bande passante,...
Microsoft Exchange	Microsoft Exchange est un Logiciel de groupware (travail collaboratif) de Microsoft pour serveurs de	-Plus rapide et plus efficace que tout autre type de messagerie. -Microsoft Exchange est vital pour les entreprises.	-Microsoft exchange occupe beaucoup d'espace.

	messagerie	-Les utilisateurs de l'e-mail seront en mesure d'accéder à leur compte plus rapidement. -Portabilité du système de messagerie.	
--	------------	---	--

Tableau III.1. Exemple de serveur de messagerie.

III.7.2. Les clients de messagerie [Web.14]

Un client de messagerie est logiciel de lecture des emails qui est installé sur le poste de l'utilisateur et qui permet rapatrier et stoker les emails reçus sur le disque de l'utilisateur.

Il existe deux types de catégories de client de messagerie : Les clients mails mail installés sur poste informatique appelés « lourds » et les clients web, accessible à partir d'une connexion sur navigateur, appelés « webmail ».

III.7.2.1. Les clients lourds [Web.15]

Un client de messagerie lourd englobe toutes les applications que l'on peut installer sur chaque poste de travail des différents collaborateurs. Ces applications peuvent être liées à un serveur qui sauvegardera les données.

Parmi ces clients lourds on peut citer :

Le client	Description	Avantage	Inconvénient
-----------	-------------	----------	--------------

Thunderbird	Thunderbird est l'un des meilleurs logiciels de messagerie. c'est un client mail libre, distribué gratuitement par la fondation Mozilla qui possède toutes les fonctionnalités que l'on attend d'un tel outil.	<ul style="list-style-type: none"> -Il est facile à utiliser, personnalisable, complet et performant. -Il intègre un filtre anti-spam très performant. -Il comporte un filtre anti-phishing pour lutter contre une forme dangereuse de spam. -Il permet de créer des dossiers virtuels et dynamiques. 	<ul style="list-style-type: none"> - Problèmes d'incompatibilité de licences. - La création et l'ajout d'une signature ne sont pas conviviaux. -Dans Thunderbird, la date est absente pour les messages du jour, seul l'heure s'affiche.
Microsoft Outlook	Microsoft Outlook est un gestionnaire d'informations personnelles et un client de courrier électronique propriétaire édité par Microsoft.	<ul style="list-style-type: none"> -Gérer facilement de grandes quantités de courrier électroniques. -Condenser, catégoriser ou même ignorer des conversations entières en quelques clics. -Gagner du temps lors de l'affichage, de la création et de la gestion de courriers électroniques. -Accédez aux informations vitales n'importe où et n'importe quand. 	<ul style="list-style-type: none"> -Outlook ne dispose pas de l'accès IMAP. -Il n'inclut pas les recherches sauvegardées. - Pas de module d'accès (lecture) aux newsgroups.

Tableau III.2. Exemple de clients lourds de messagerie.**III.7.2.2. Les clients légers ou webmail**

Un client léger est entièrement géré par un serveur, de la gestion au stockage des données. Les utilisateurs de l'application auront accès aux données par un portail sécurisé depuis leur navigateur (Internet Explorer, Firefox...).

On peut distinguer quelques types de clients légers :

Le client	Description	Avantage	Inconvénient
RoundCube	RoundCube est un webmail open source d'ores et déjà accessible à tous les détenteurs d'une adresse e-Mail Free.	-La liberté d'accéder aux mails depuis n'importe quel FAI	-Manque de confidentialité
Zimbra	Zimbra est serveur de messagerie avec des fonctionnalités de travail collaboratif.	-Compatible avec tous les clients ou plateforme (Windows, linux, macOS ...). -il est très facile d'adapter les produits Zimbra aux besoins.	-il est possible de l'installer en dur sur la machine dans ce cas ça en revient au même qu'un client mail classique.
Squirrelmail	Squirrelmail est un webmail. Il supporte les protocoles IMAP et SMTP, et toutes les pages créées en HTML ceci afin d'être compatible avec le maximum de navigateurs	-Fournir une compatibilité optimale pour se rendre aussi accessible que possible. -il dispose d'une interface agréable (gestion de dossiers,	-Risque d'espionnage.

		de forwards,...).	
--	--	-------------------	--

Tableau III.3. Exemple de clients légers de messagerie.

III.8. Les risques d'un serveur de messagerie [Web.15]

La messagerie électronique est la base de la communication dans une entreprise. Et pourtant les risques et les menaces liés à son usage sont nombreux. Si certains problèmes sont tolérables, d'autres sont vitaux.

III.8.1. L'infrastructure de l'entreprise

La messagerie électronique est le principal vecteur de malwares dans les infrastructures de l'entreprise. Les virus et les codes malicieux sont souvent insérés dans les pièces jointes des e-mails ou dans le cœur même des messages. L'ouverture de ces fichiers déclenche instantanément l'installation de ces malwares sur le pc.

III.8.2. Le spam

Le spam est un courrier électronique indésirable utilisé par les pirates comme support pour l'envoi de pièces jointes infectées. Il peut également être un simple courriel envoyé en grand nombre dans le but de saturer la messagerie électronique de l'entreprise.

III.8.3. Attaque par déni de service

Une attaque par déni de service est dommageable pour l'entreprise car elle peut rendre indisponible sa messagerie. Si son adresse électronique est blacklistée, le service peut également être interrompu. Les pirates utilisent le phishing ou hameçonnage pour collecter les coordonnées bancaires de la société.

III.9. Sécuriser le système de messagerie

Plusieurs solutions s'offrent aux entreprises qui souhaitent renforcer la sécurité de leur messagerie électronique. Parmi elles, on peut citer :

- **Sécurisation des communications entre le client et le serveur :** Généralement les communications sont sécurisées en utilisant un chiffrement avec openSSL.
- **Sécurisation de l'environnement de messagerie.**

- **Mise à jour du logiciel serveur.**
- **Sécuriser l'authentification.**
- **Sécuriser les données :** utiliser un anti-spam pourra analyser les courriers puis les affecter un score.

Conclusion

Au cours de ce chapitre, nous nous sommes rapprochés de l'environnement technique de notre projet et cela nous a fait comprendre le fonctionnement du système de messagerie électronique et d'expliquer et comparer les différents outils de messagerie pour répondre au mieux aux besoins de l'entreprise et à ceux de ses personnels.

Dans le chapitre suivant, nous utilisons les informations récolté en se présent chapitre afin d'aborder la configuration et l'administration de notre système de messagerie.

Chapitre IV :
Configuration et la
mise en œuvre du
système

Introduction

Après avoir terminé la partie de conception définie au préalable, nous allons passer à la mise en œuvre du système, où nous citons d'une manière explicite les étapes d'installation et configuration de notre serveur de messagerie.

IV.1. Choix du serveur de messagerie

Parmi les serveurs de messagerie les plus utilisés dans le milieu professionnel, **HMailServer**, faisant parti de la gamme Windows Server System, est le choix qui a retenu notre attention. Nous opterons la version standard.

IV.1.1. Fonctionnalités de HMailServer

➤ Appui de base de données

Le HMailServer soutient MySQL et serveur de Microsoft SQL. MySQL est logiciel ouvert de source et est le choix recommandé. L'installation de HMailServer inclut une installation minimale et intégrée du serveur de base de données de MySQL. Elle est offerte comme option. Si vous la choisissez, le serveur intégré sera installé et configuré automatiquement pendant l'installation de HMailServer. Le serveur intégré vous sauve la dispute de devoir installer et configurer un serveur séparé de base de données pour le HMailServer.

➤ Sécurité

Le hMailServer est préconfiguré pour avoir la sécurité élevée quand il vient au relais et à l'authentification de sorte que personne ne puisse utiliser votre serveur pour envoyer des messages de Spam. Il soutient également le module de balayage ouvert très populaire ClamAV de virus de source. HMailServer de configuration pour employer des prises de ClamAV seulement un clic simple ! Le serveur soutient également les gestionnaires Listserv noirs et d'autres mécanismes d'Spam-arrêt tels que des consultations de SPF et de MX.

IV.1.2. Installation et configuration de HMailServer au sein de l'EPB :

Avant de lancer l'installation de HMailServer il faut tout d'abord installer un système de gestion de base de données. Nous avons choisi MariaDB car il est un fork de MySQL.

IV.1.2.1. Installation de MariaDB

C'est la manière habituelle de procéder à installer. Pour démarrer le programme d'installation, on clique sur MariaDB :

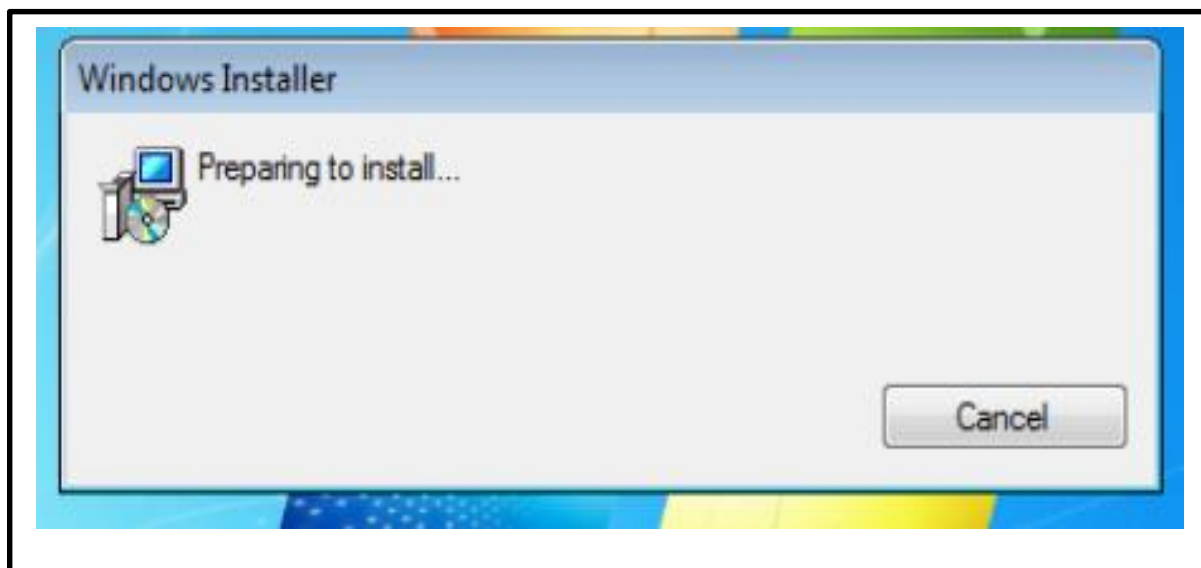


Figure IV.1. Lancement de l'installation de MariaDB.

- Bienvenue sur MariaDB en cliquant sur suivant :

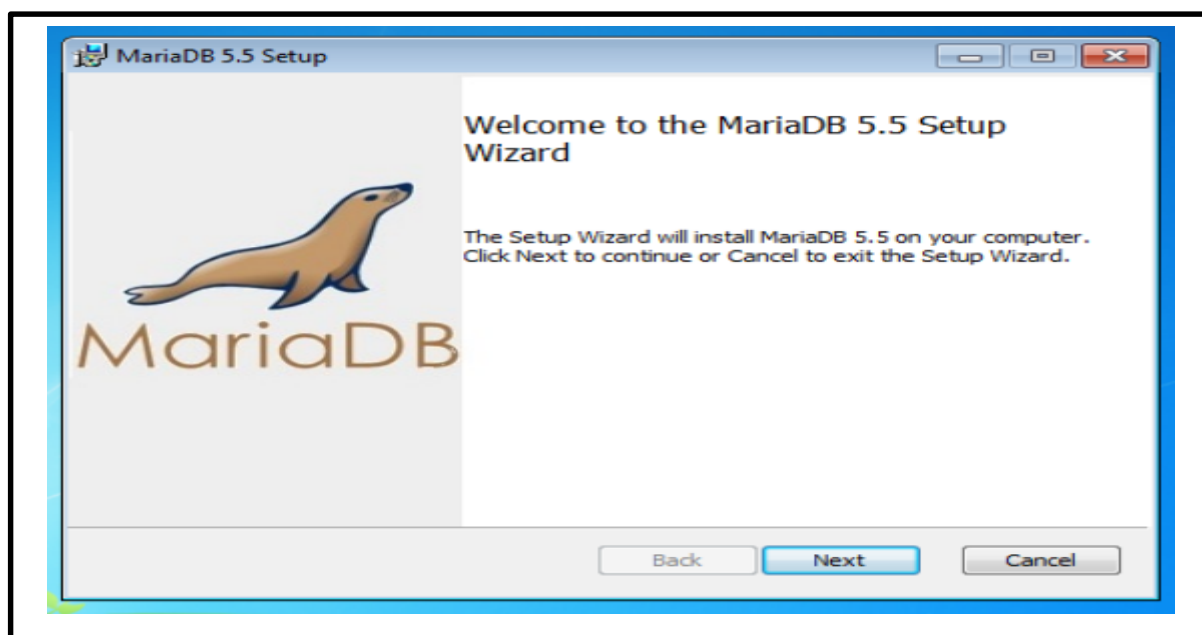


Figure IV.2. Bienvenue sur MariaBD.

-Acceptation du contrat de licence :



Figure IV.3. Acceptation du contrat de licence.

- Programme d'installation personnalisé :

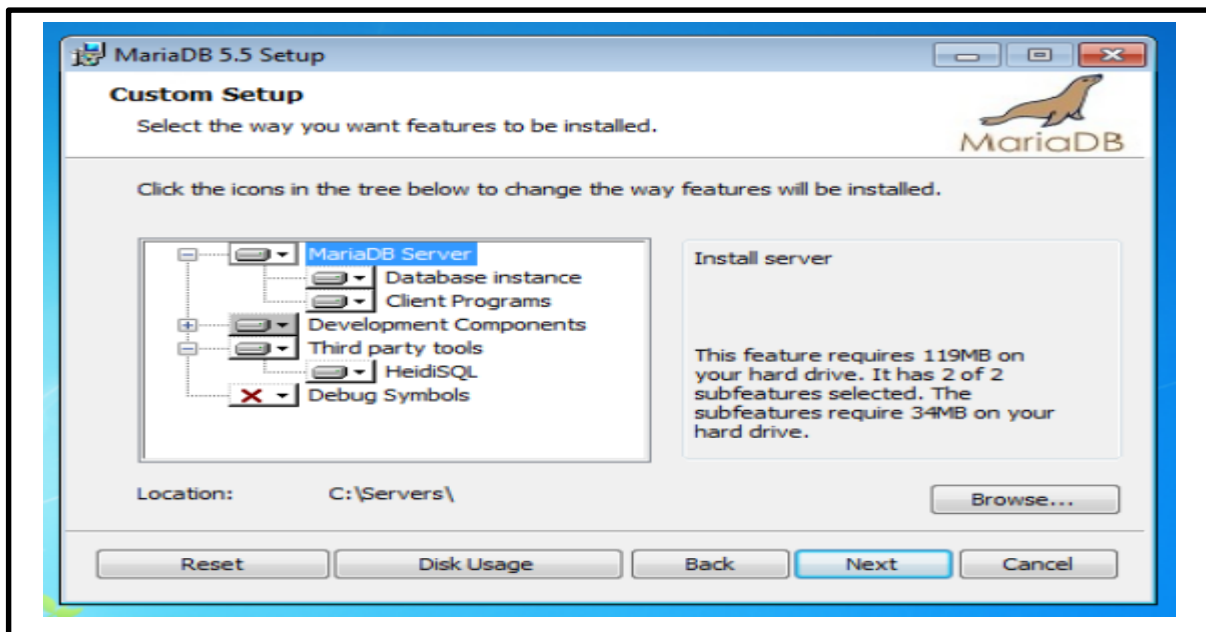


Figure IV.4. Spécification du dossier d'installation de MariaDB.

-Authentification de la base de données/sécurité des attributs :

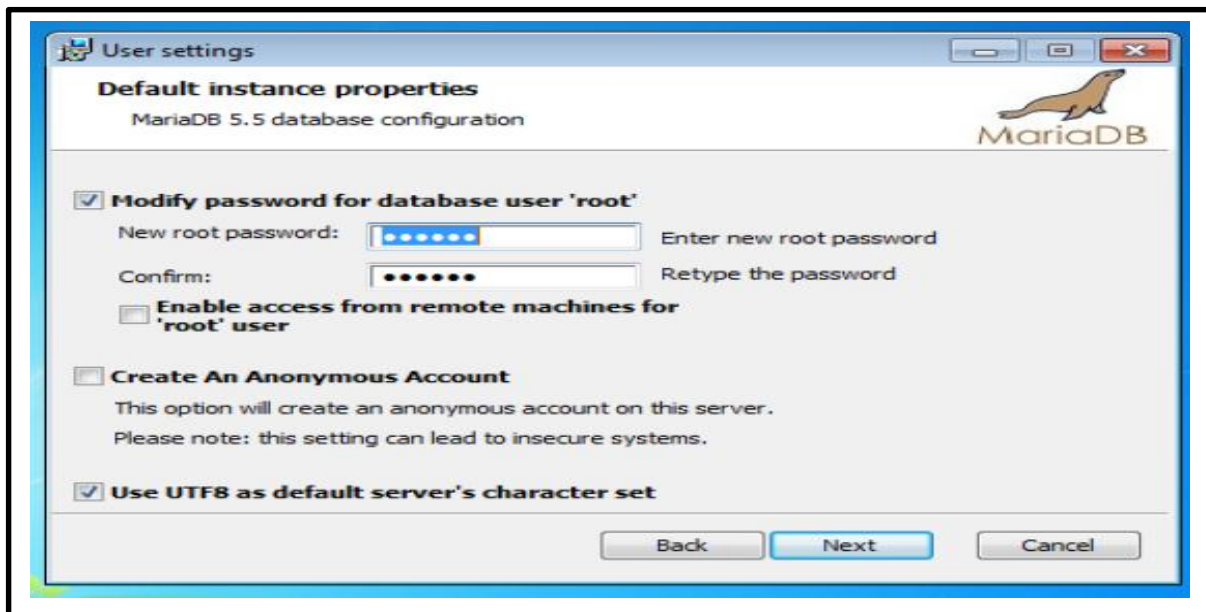


Figure IV.5. Définition du mot de passe pour L'utilisateur root de la base de données.

- Prêt à installer, tous les paramètres d'installation sont recueillis. Cliquez sur le bouton Install :

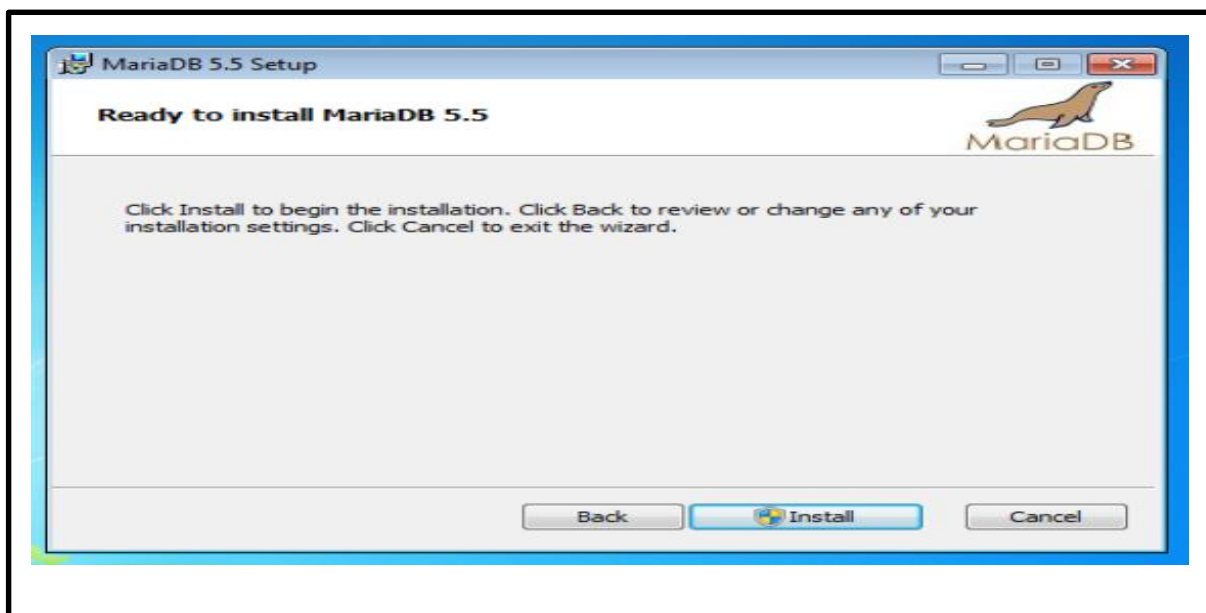


Figure IV.6. Installation de MariaDB.

-Fin d'installation

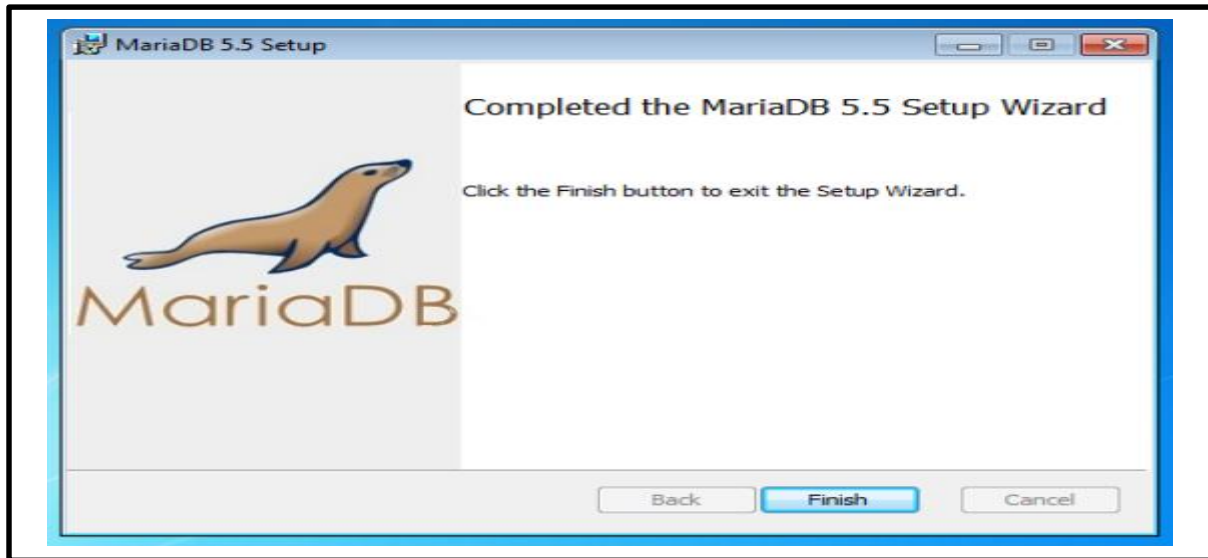


Figure IV.7. Fin d'installation.

IV.1.2.2. Configuration de MariaDB

- Création d'une base de donnée sous le nom 'maillep'

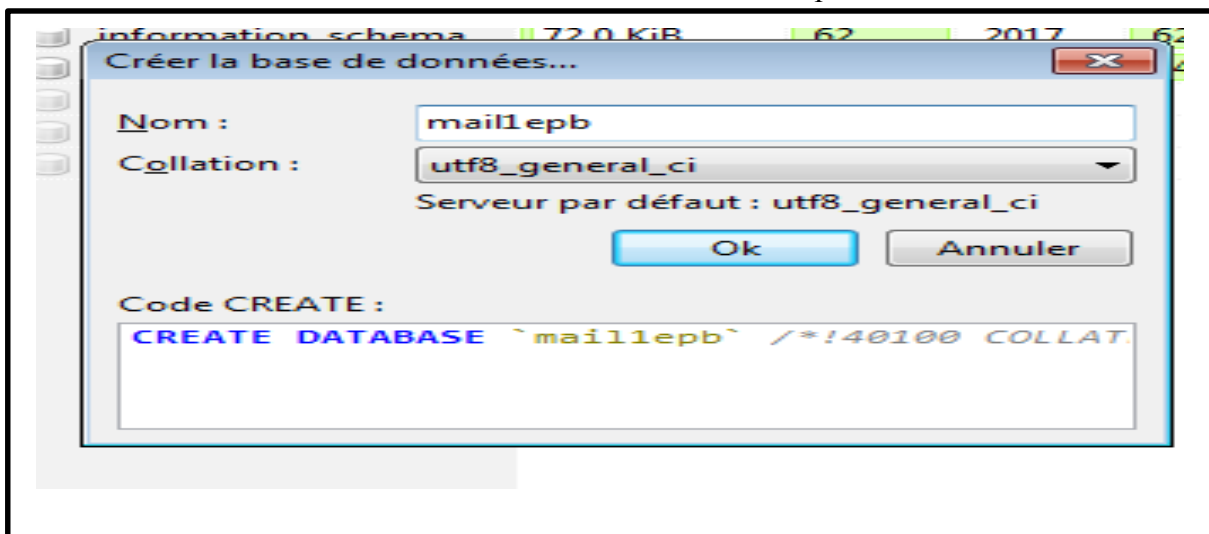


Figure IV.8. Création de la base de donnée « maillep ».

- Création d'utilisateur « mail » avec tous les privilèges :

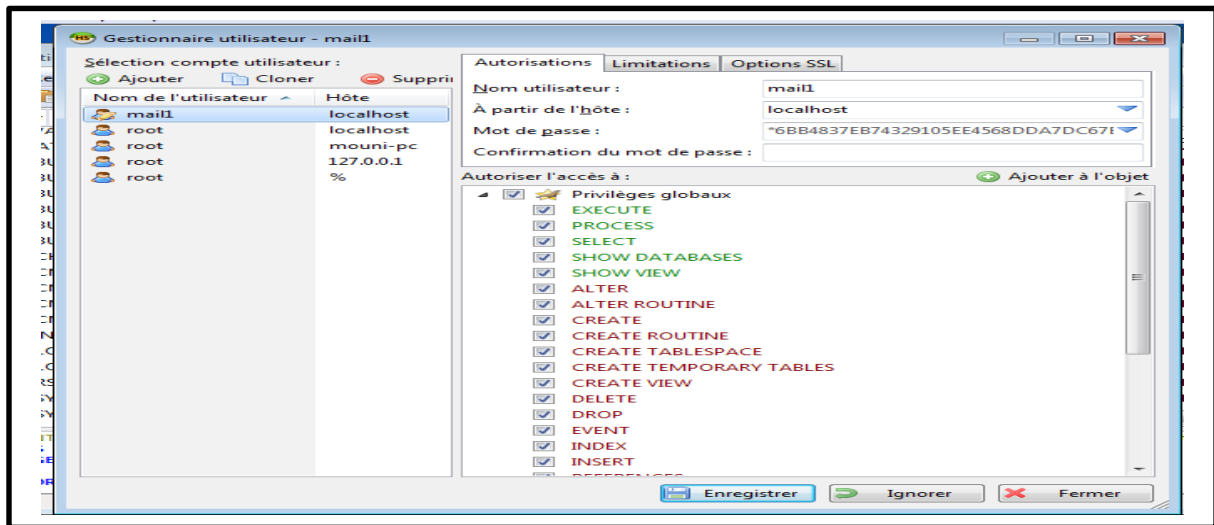


Figure IV.9. Création d'un utilisateur.

IV.1.2.3. Installation de HMailServer

Cette partie décrit les étapes requises pour installer hMailServer-5.6.6.

1. Double-cliquez sur le fichier téléchargé pour lancer le programme d'installation. La première boîte de dialogue qui apparaît est la boîte de dialogue de bienvenue, dans celui-ci, il suffit de cliquer sur Suivant :

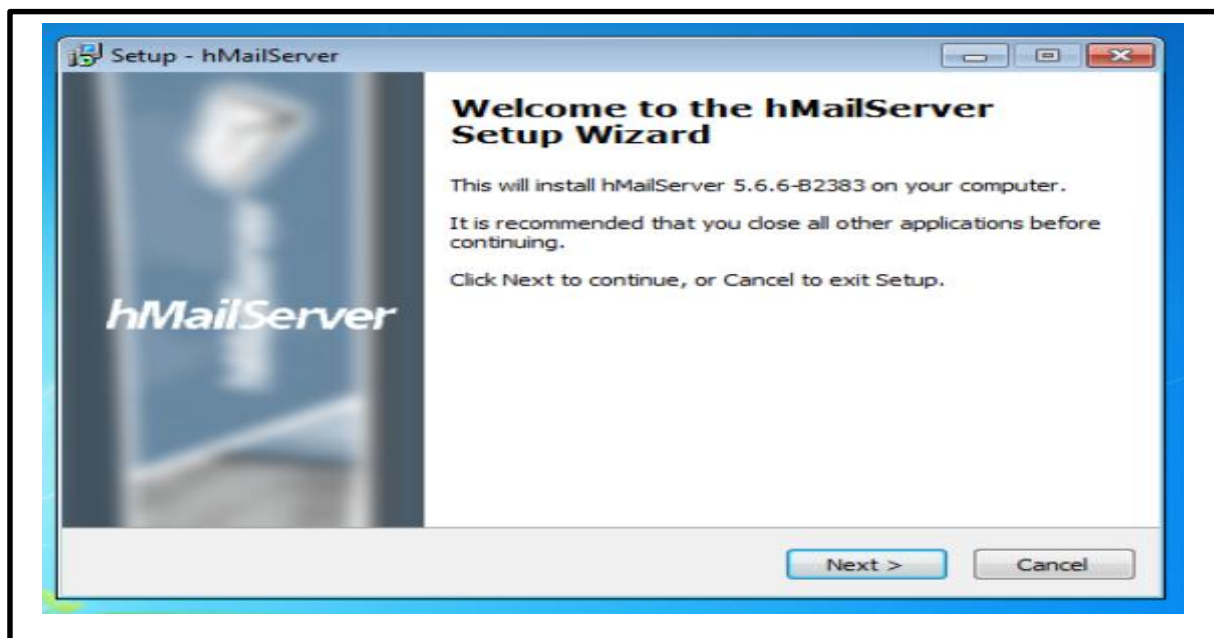


Figure IV.10. Lancement de l'installation de HMailServer.

2. L'étape suivante consiste à lire le contrat de licence. Si vous ne les acceptez pas l'accord de licence, s'il vous plaît annuler l'installation. Si vous êtes d'accord, sélectionnez «J'accepte l'accord » et cliquez sur Suivant.

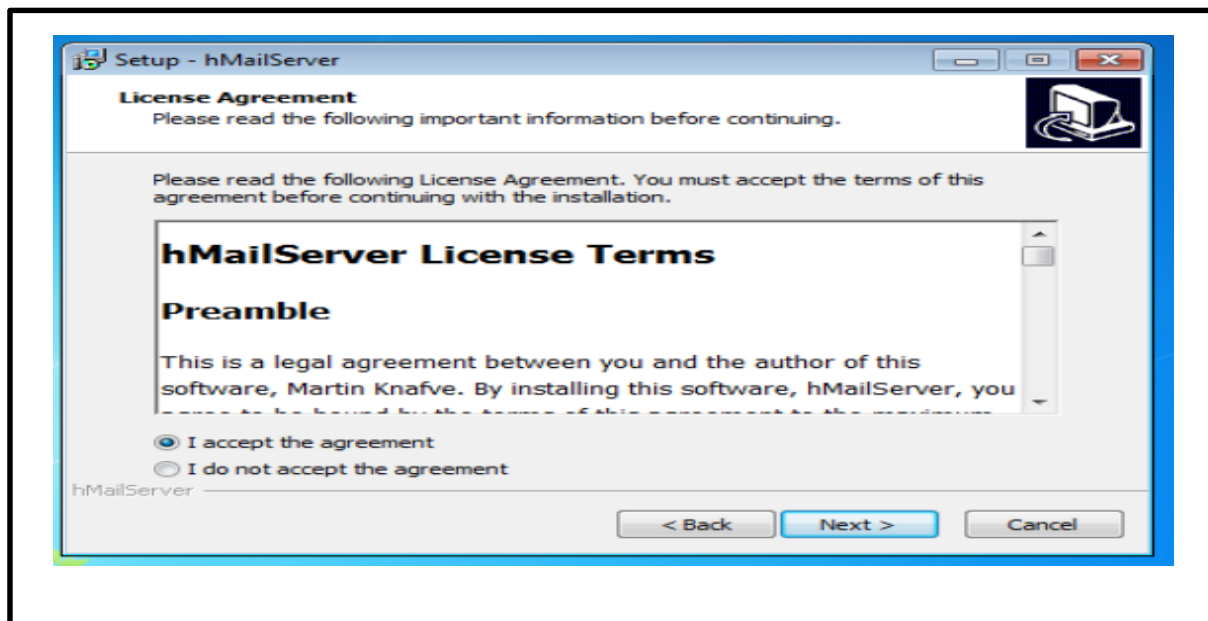


Figure IV.11. Acceptation de la licence d'agrément.

3. Sélectionnez le dossier de destination et cliquez sur Suivant. Vous devez sélectionner un lecteur local et non un dossier réseau. Il est possible d'installer sur HMailServer périphériques amovibles, mais vous ne serez pas en mesure d'exécuter HMailServer de l'appareil sur un autre ordinateur.

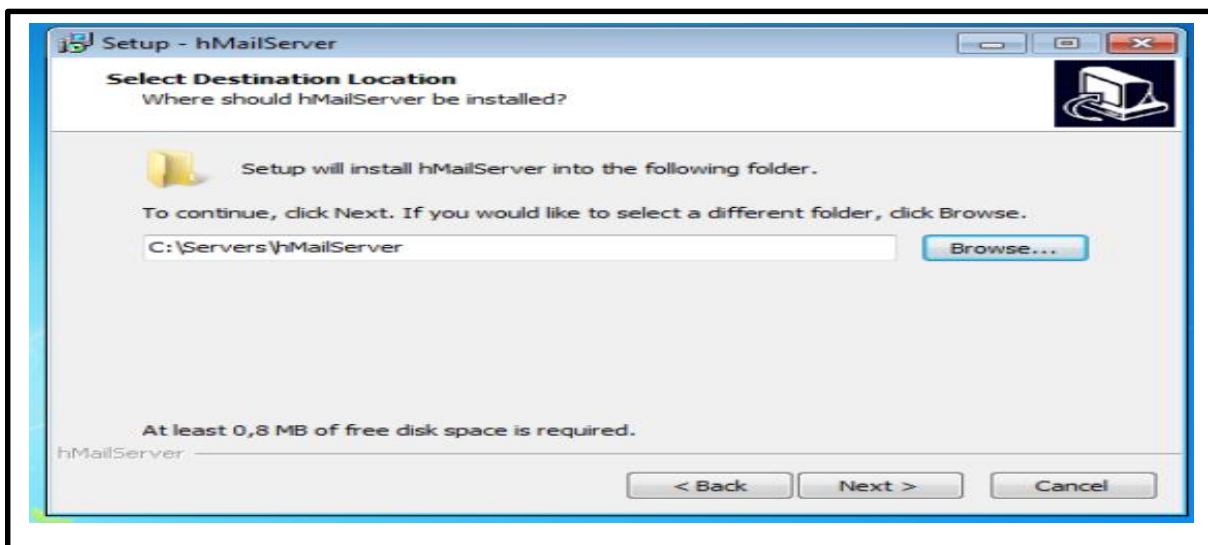


Figure IV.12. Choix du dossier d'installation du programme.

4. Sélectionnez les composants que vous souhaitez installer et cliquez sur Suivant. Sur le serveur, vous devez installer tous les composants disponibles. Si vous avez déjà installé le serveur HMailServer sur un autre ordinateur et que vous voulez gérer cette distance, il vous suffit d'installer les outils d'administration.

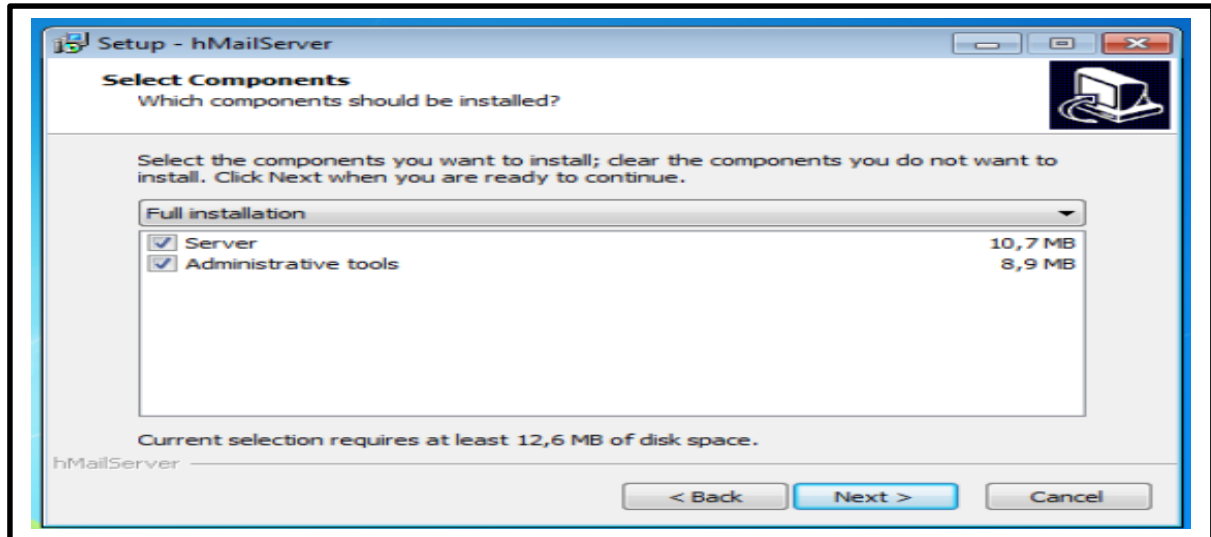


Figure IV.13. : La sélection des composants.

5. Sélectionner la base de donnée que HMailServer va utiliser. Il est recommandé de laisser le premier choix comme propose par le setup. Cela permet d'utiliser la base de données incluse dans le serveur et qui la rend indépendante de toute autre base. Pouvant être associée à un autre service (Apache, MySQL ou Microsoft SQL etc...).

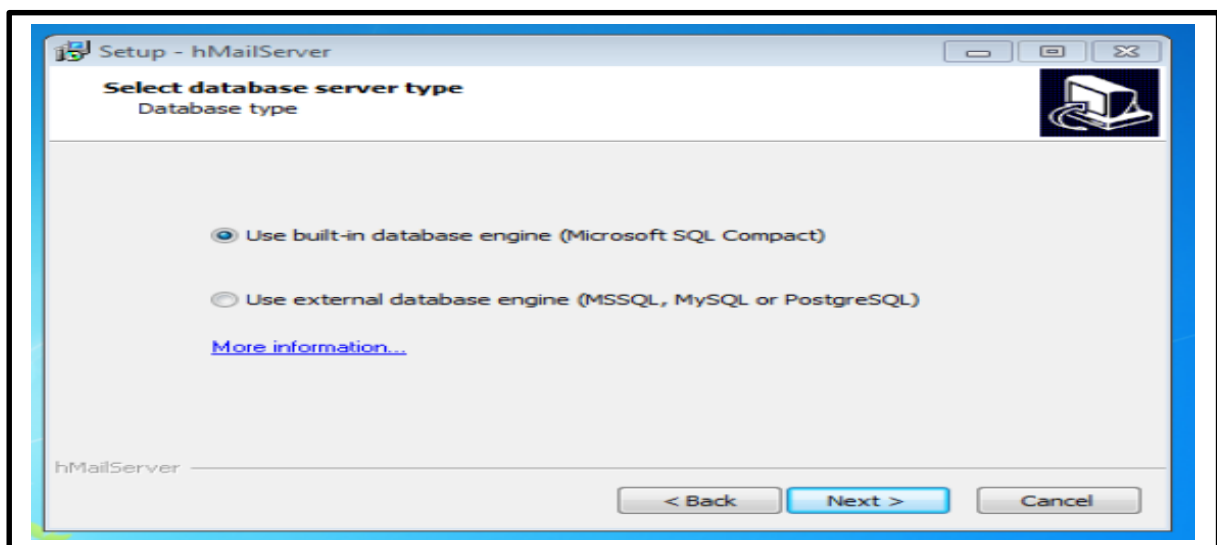


Figure IV.14. Sélection d'un type de base de données.

6. Sélectionnez le dossier de démarrage menu que vous souhaitez placer les icônes HMailServer et cliquez sur Suivant :

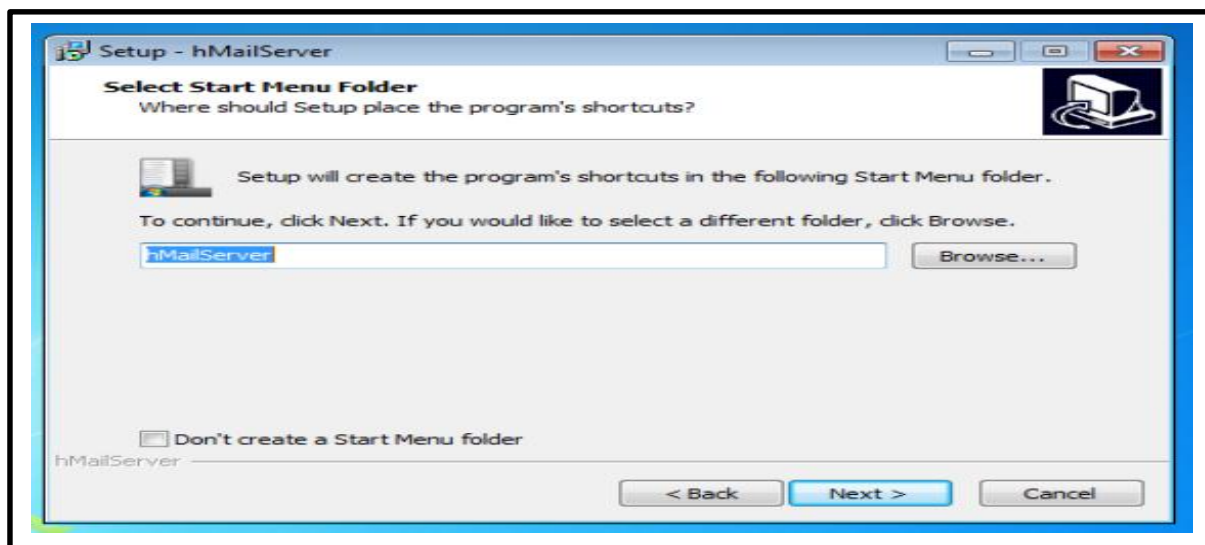


Figure IV.15. Choix du nom de l'icône.

7. Une fois les fichiers installés, vous devez fournir le programme d'installation avec un mot de passe principal de HMailServer. Le mot de passe peut être tout ce que vous voulez tant que c'est plus de 5 caractères. Vous aurez besoin du mot de passe plus tard lors de l'exécution de l'administration serveur, ne l'oubliez pas. Il vous suffit de spécifier le mot de passe la première fois que vous installez HMailServer.

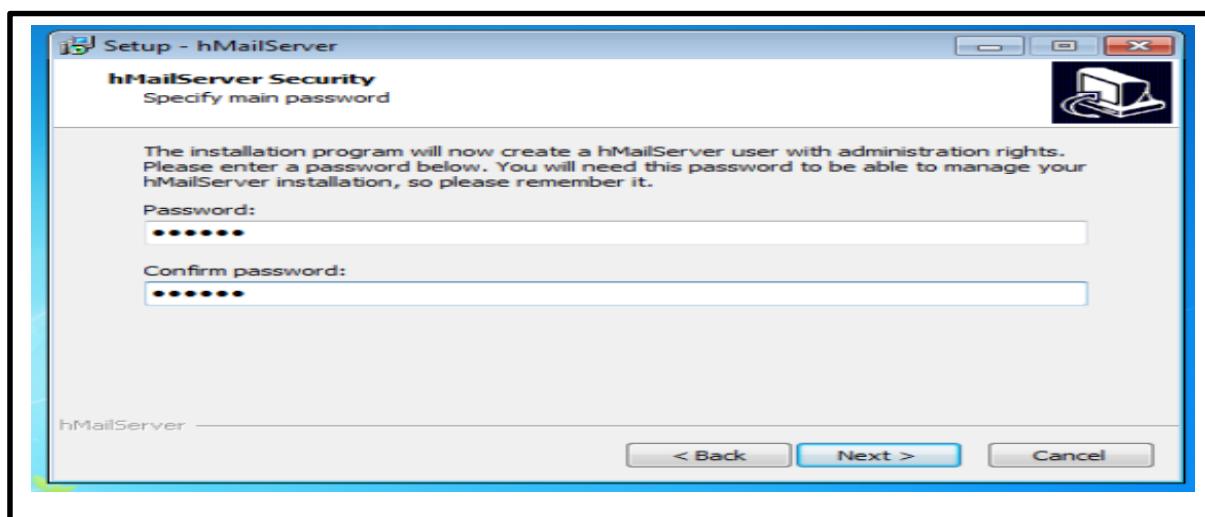


Figure IV.16. Insertion d'un mot de passe.

8. Assurez-vous que les paramètres sont corrects, puis cliquez sur Installer pour procéder à l'installation.

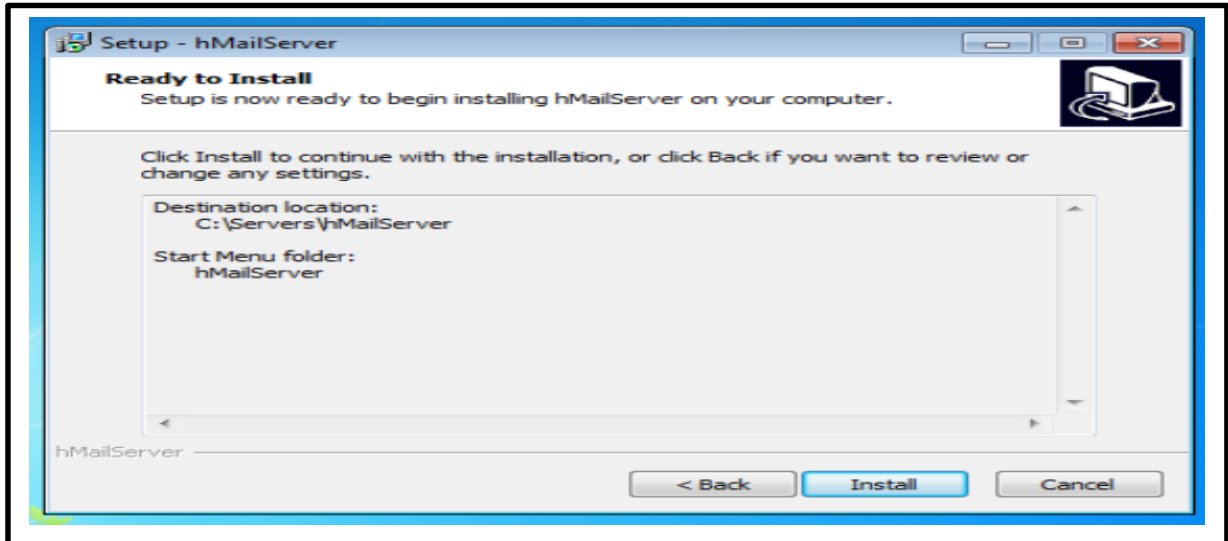


Figure IV.17. Vérification des paramètres d'installation.

9. Attendez ... L'installation devrait prendre environ 10-20 secondes.

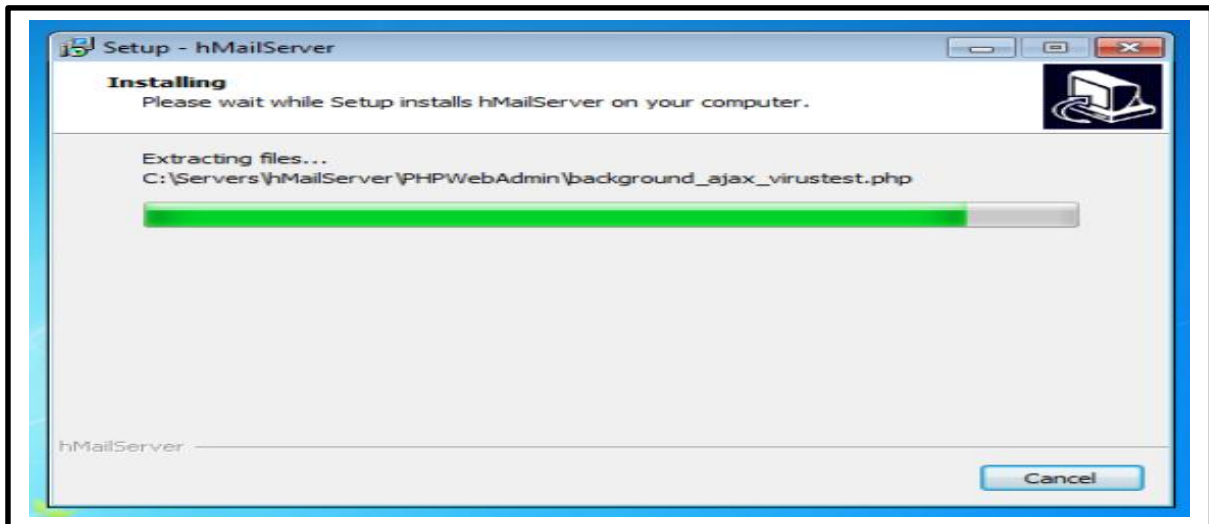
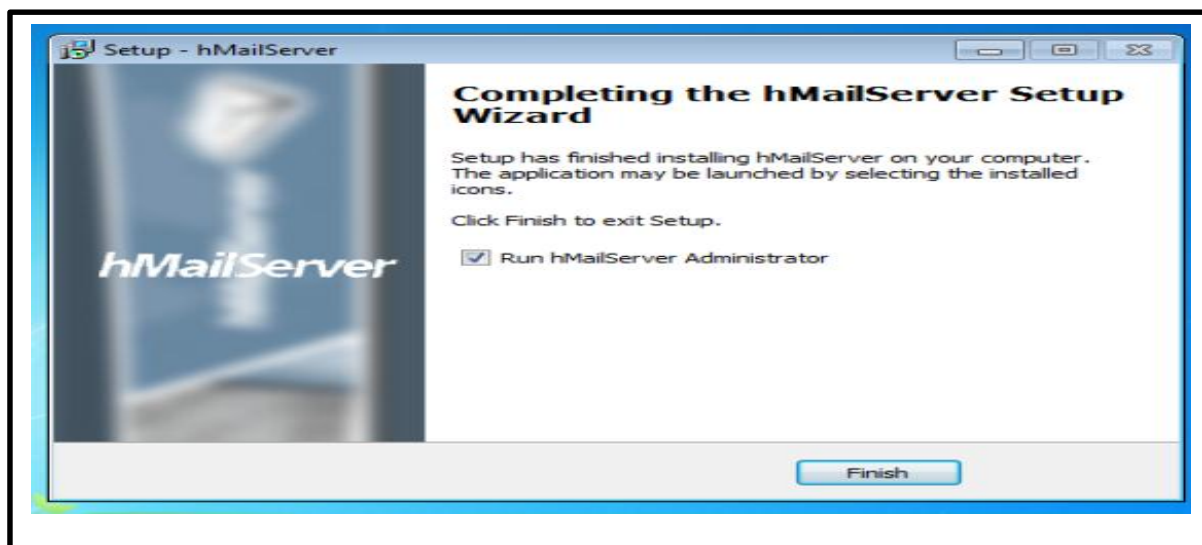
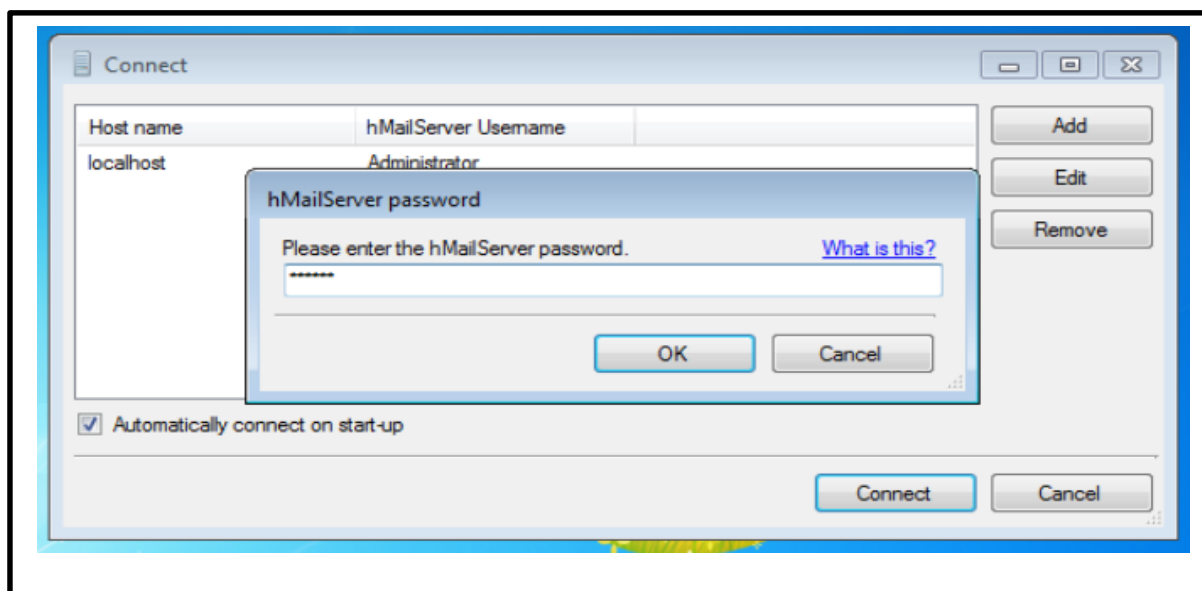


Figure IV.18. Installation HmailServer.

10. Fin de l'installation.**Figure IV.19** Fin de l'installation d'HMailServer.**IV.1.2.4. Configuration basique de HMailServer :****1. Connexion à HMailServer :**

A l'apparition de la boîte de dialogue « connect », connectez-vous à localhost en renseignant le mot de passe que nous avons spécifiée lors de l'installation de HMailServer.

**Figure IV.20.** La connexion au HmailServer.

2. Domaines et comptes

Chaque domaine HMailServer doit être connecté à un domaine Internet. Dites que vous êtes le propriétaire du domaine portdebejaia.dz, alors vous devez ajouter portdebejaia.dz un domaine dans HMailAdmin:

1. Démarrez HMailAdmin.
2. Cliquez sur *Ajouter un domaine*.
3. Entrez portdebejaia.dz le nom de domaine.
4. Cliquez sur *Enregistre*.

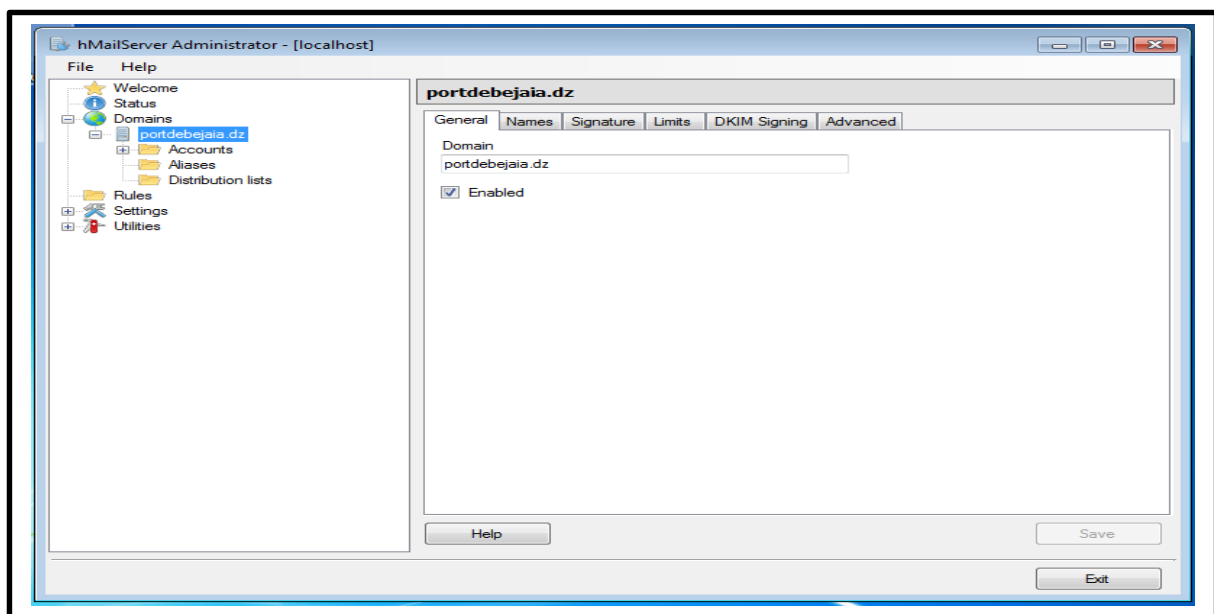


Figure IV.21. Nom du domaine.

L'étape suivante consiste à ajouter des comptes à votre serveur. La configuration normale est d'avoir un compte par adresse e - mail que vous voulez être en mesure d'envoyer et de recevoir des e- mails. On va ajouter les adresses mounira@portdebejaia.dz et melkhir@portdebejaia.dz, simplement ajouter à HMailAdmin:

1. Démarrer HMailAdmin.
2. Développez le *Domains* nœud dans l'arborescence à gauche.
3. Cliquez sur le domaine *portdebejaia.dz*.
4. Cliquez sur *Ajouter un compte*.
5. Entrez mounira l'adresse du compte, définissez le mot de passe et cliquez sur *Enregistrer*.

6. Cliquez sur le domaine epb.net dans l'arborescence à gauche.
7. Cliquez sur *Ajouter un compte*.
8. Entrez melkhir l'adresse du compte, définissez le mot de passe et cliquez sur *Enregistrer*.

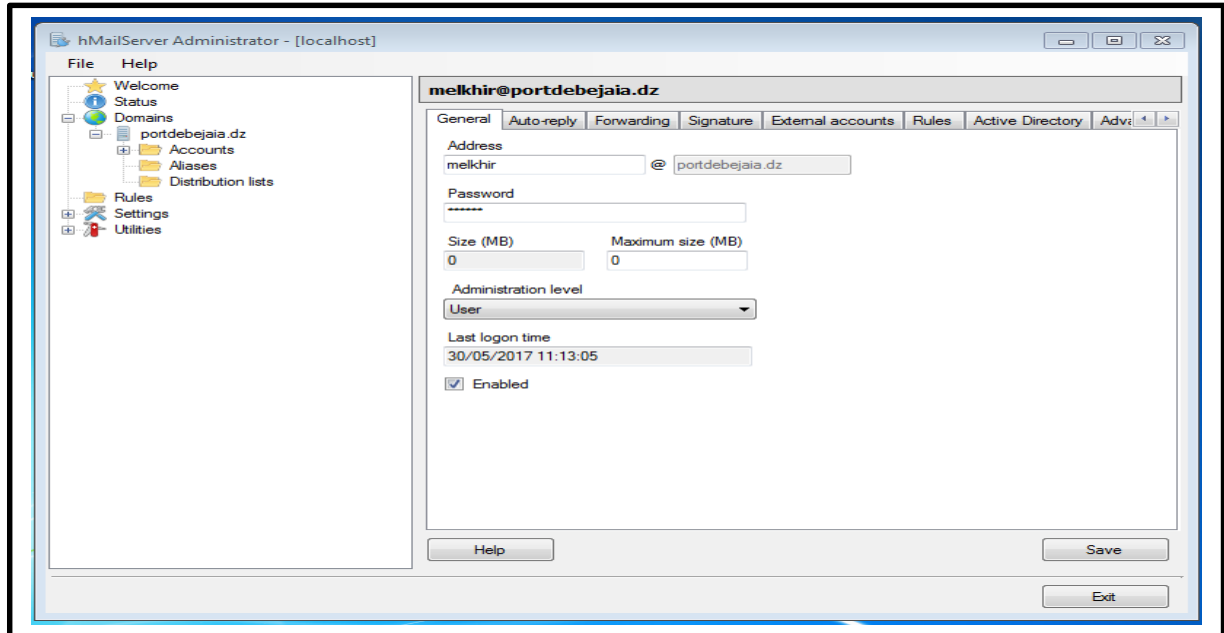


Figure IV.22. Ajout des comptes.

3. Spécification nom d'hôte public

Pour un serveur de messagerie fonctionne correctement, il a besoin de connaître son nom public sur Internet. Ceci est normalement quelque chose comme mail.portdebejaia.dz. Comme il n'y a pas de bonne façon pour le logiciel pour détecter automatiquement le nom d'hôte du public de l'ordinateur où il est en cours d'exécution, nous devons indiquer à HMailServer quel nom d'hôte public à utiliser. Bien qu'il soit possible d'exécuter HMailServer sans dire son nom d'hôte.

1. Démarrer HMailAdmin.
2. Dans l'arborescence à gauche, allez à *Paramètres -> Protocoles -> SMTP*.
3. A droite, les paramètres SMTP sont maintenant affichés. Cliquez sur la *livraison du courrier électronique(ou delivery of e-mail)* onglet.
4. Sous le *nom d'hôte*, entrez le nom d'hôte public de l'ordinateur sur lequel HMailServer est en cours d'exécution.
5. Enregistrez le changement.

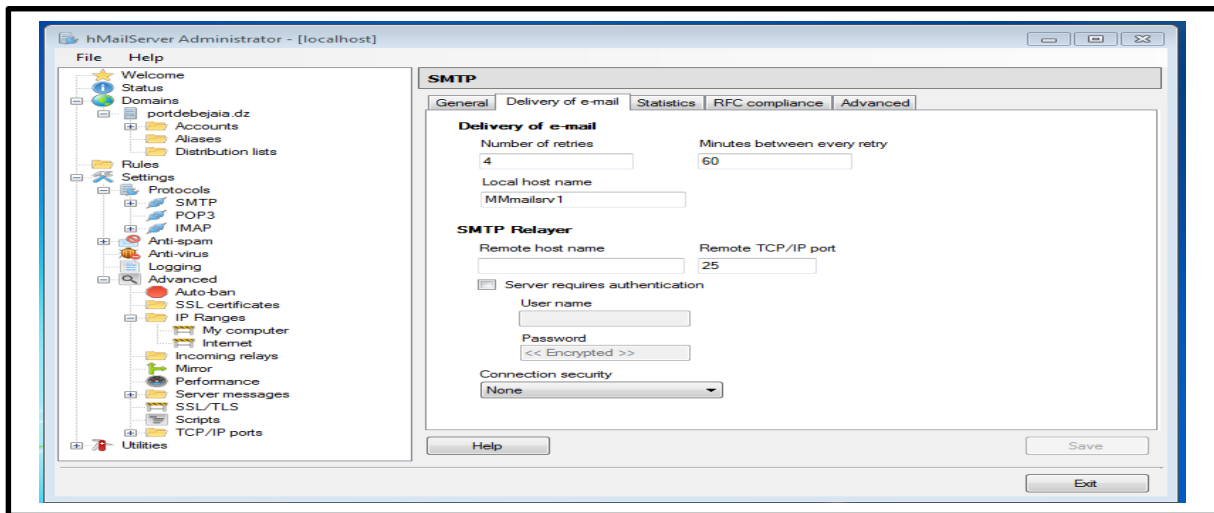


Figure IV.23. Spécification du nom de hot publique.

4. Paramètres IMAP

Utilisez ces paramètres pour activer et désactiver les extensions IMAP sur le serveur.

- L'extension SORT IMAP permet des messages électroniques à trier sur le serveur plutôt que dans le client de messagerie. Cela augmente les performances dans les clients de messagerie Web.
- IMAP quota - L'extension du quota IMAP permet aux clients IMAP pour vérifier l'utilisation des quotas pour le compte.
- IMAP Idle - En utilisant cette extension, le client IMAP peut recevoir des notifications du serveur chaque fois qu'un nouvel email existe. De cette façon, le client de messagerie ne doit pas vérifier manuellement les nouveaux messages chaque minute X.
- IMAP ACL - Lorsque cette extension est activée, vous pouvez configurer les dossiers publics et les autorisations pour ces derniers.

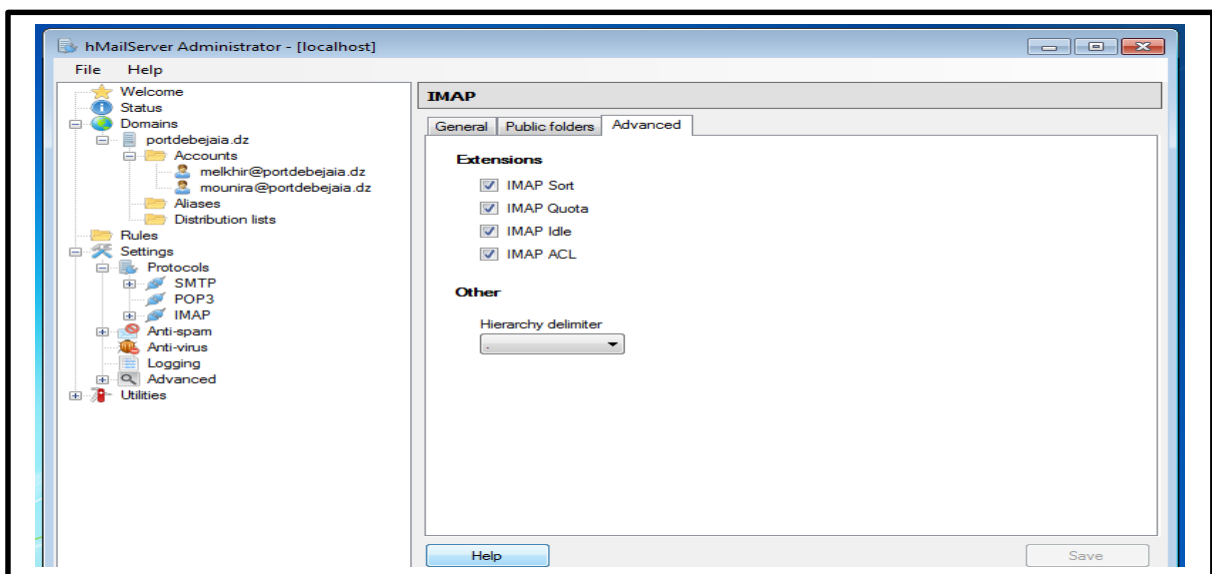


Figure IV.24. Paramètres IMAP.

5. Anti-Spam

hMailServer a un certain nombre de méthodes intégrées de protection anti-spam. Ces travaux en vérifiant l'expéditeur des messages électroniques, le contenu du message et la façon dont le message est remis à hMailServer. Par exemple, si le message contient des liens vers des pages Web spammeur ou est envoyé à partir d'une adresse qui est connu pour envoyer du spam, le message peut être classé comme spam. Une liste complète des méthodes de protection anti - spam intégrés :

✓ **Nom d'hôte**

Ceci est le nom d'hôte du serveur SpamAssassin hMailServer doit se connecter. Si SpamAssassin est en cours d'exécution sur le même ordinateur que hMailServer, la valeur devrait être « localhost » (sans les guillemets).

✓ **port TCP / IP**

Spécifiez le port TCP / IP du serveur SpamAssassin écoute. Par défaut, SpamAssassin écoute sur le port 783.

✓ **Utilisez Score SpamAssassin**

Si cette option est sélectionnée, hMailServer utilisera le score de spam donnée par SpamAssassin et l'ajouter à la note de spam hMailServer. Si l'option est désélectionnée, hMailServer utilisera le score spécifié dans la zone de texte de la partition. Le score de SpamAssassin ne sera utilisé que lorsque le seuil « marque » SpamAssassin est atteinte.

✓ **Tester**

Cliquez sur ce bouton si vous voulez tester hMailServer de se connecter à SpamAssassin. Après hMailServer a fait cela, le résultat du test sera montré à vous.

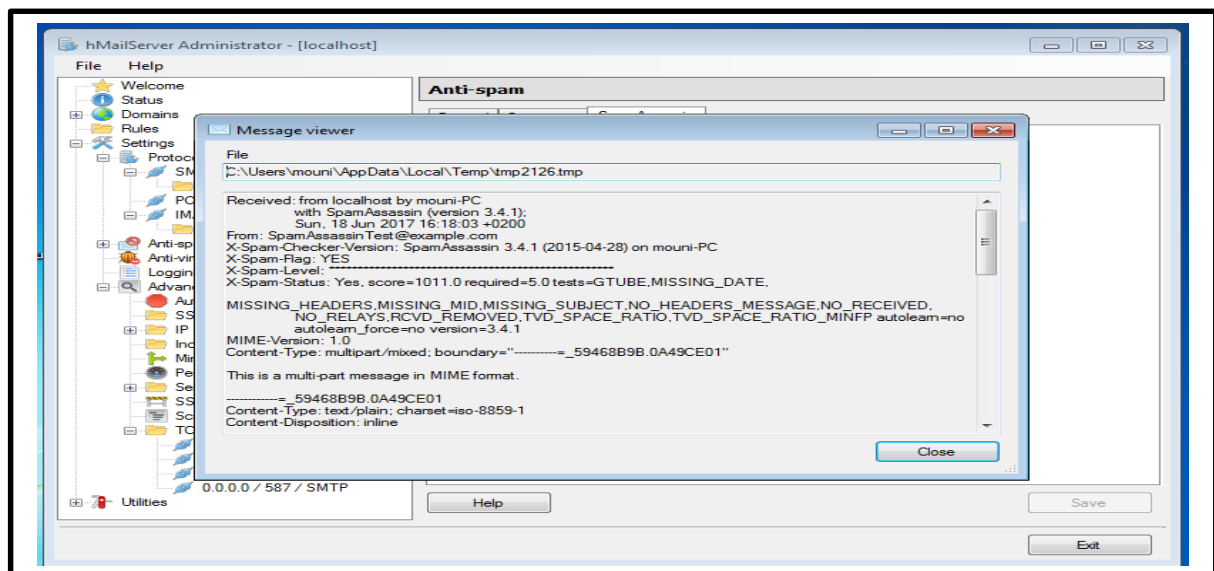


Figure IV.25. Détection de l'anti SPAM.

5. Anti-virus

hMailServer a un support intégré pour le logiciel anti-virus, nous avons utilisé ClamWin car il comprend un système d'installation simple et le code open source. Il a comme fonctionnalités :

- ✓ Analyses Anti-Virus Programmable.
 - ✓ Mis à jour automatique de la base de définition de Virus.
 - ✓ Détecteur de virus autonome.
- Configuration hMailServer pour la détection automatique de l'antivirus ClamWin :
1. Démarrez HMailServer Administrator.
 2. Accédez à *Paramètres -> Protocoles -> SMTP -> Anti - virus.*
 3. Cliquez sur ClamWin.
 4. Couchez Use Clam Win -> Auto-detect.

HMailServer va lire les paramètres ClamWin à partir du Registre de Windows. Une fois les paramètres ont été détectés automatiquement, vous devez vous assurer qu'ils sont corrects.

5. Cliquez sur test...

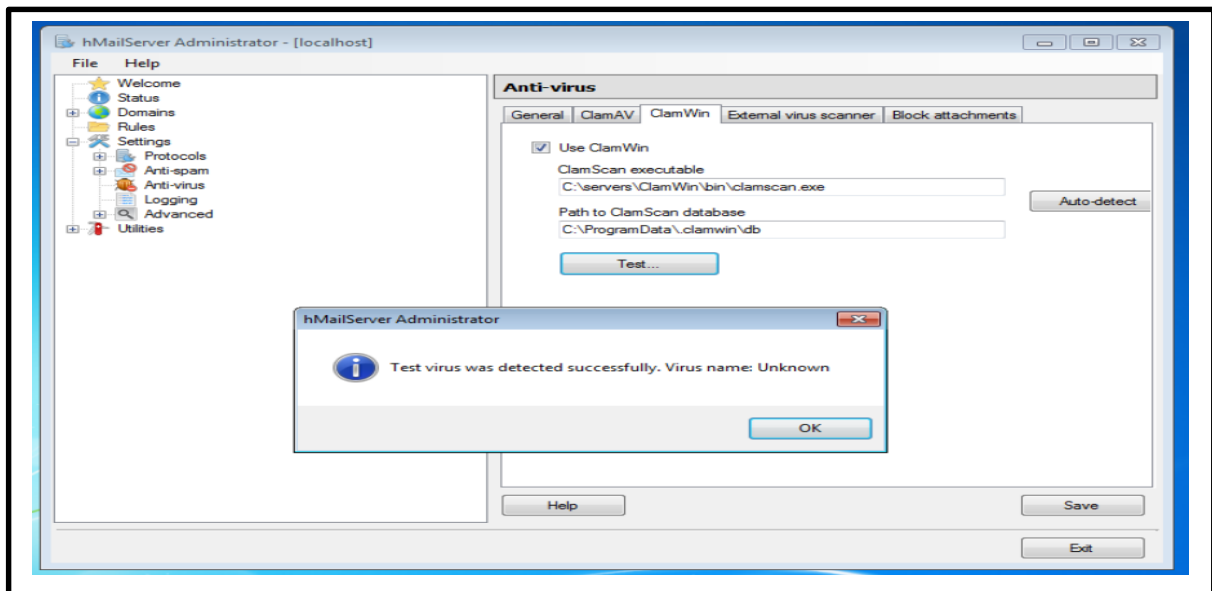


Figure IV.26. Détection de l'Antivirus.

IV.2. Choix du client lourd

Dans notre cas on a choisi Thunderbird comme client lourd.

IV.2.1. Installation du client de messagerie Thunderbird

L'installation de ce client de messagerie est très simple :

1. Lancez l'installation du logiciel, cliquez sur suivant :

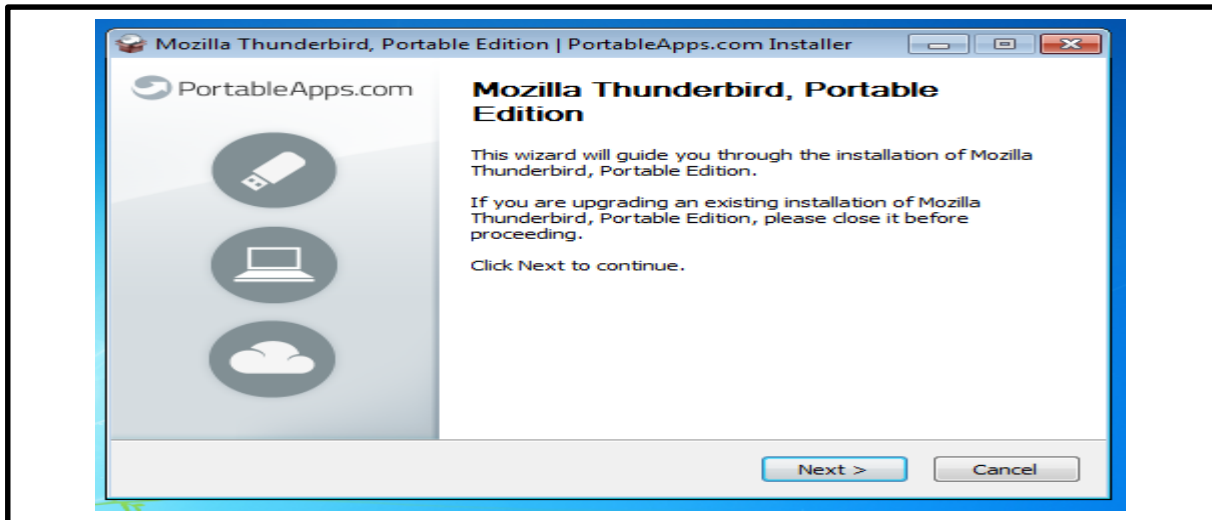


Figure IV.27. Lancement de l'installation de Thunderbird.

2. Installer de Thunderbird dans un dossier personnalisé et cliquer installer:

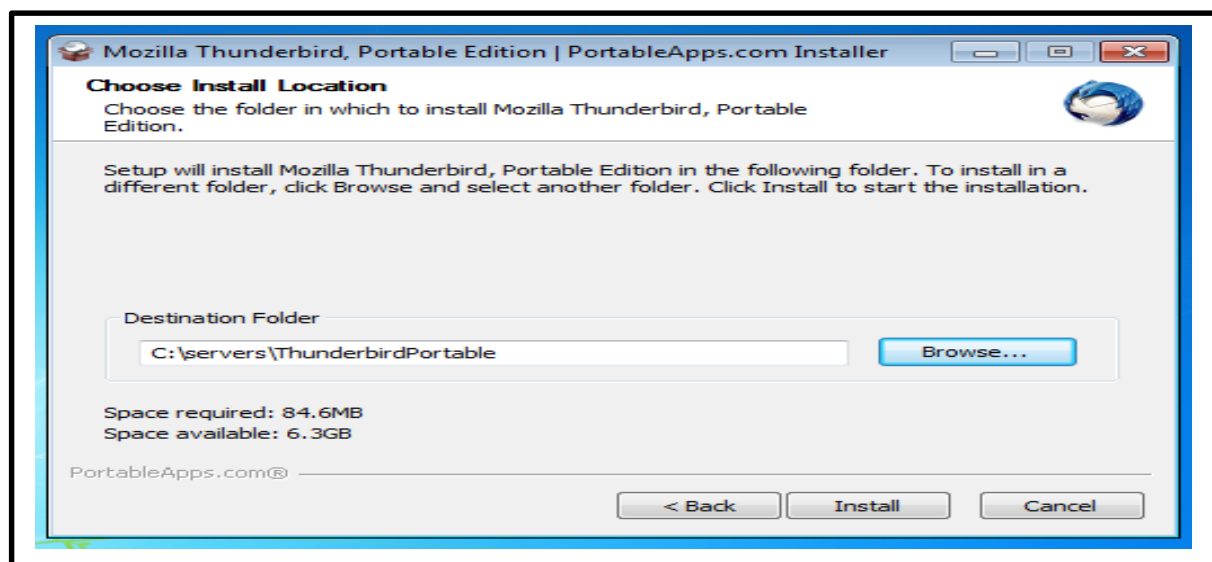


Figure IV.28. Choix du dossier d'installation.

3. Attendez... L'installation doit prendre environ 10-20 Second :

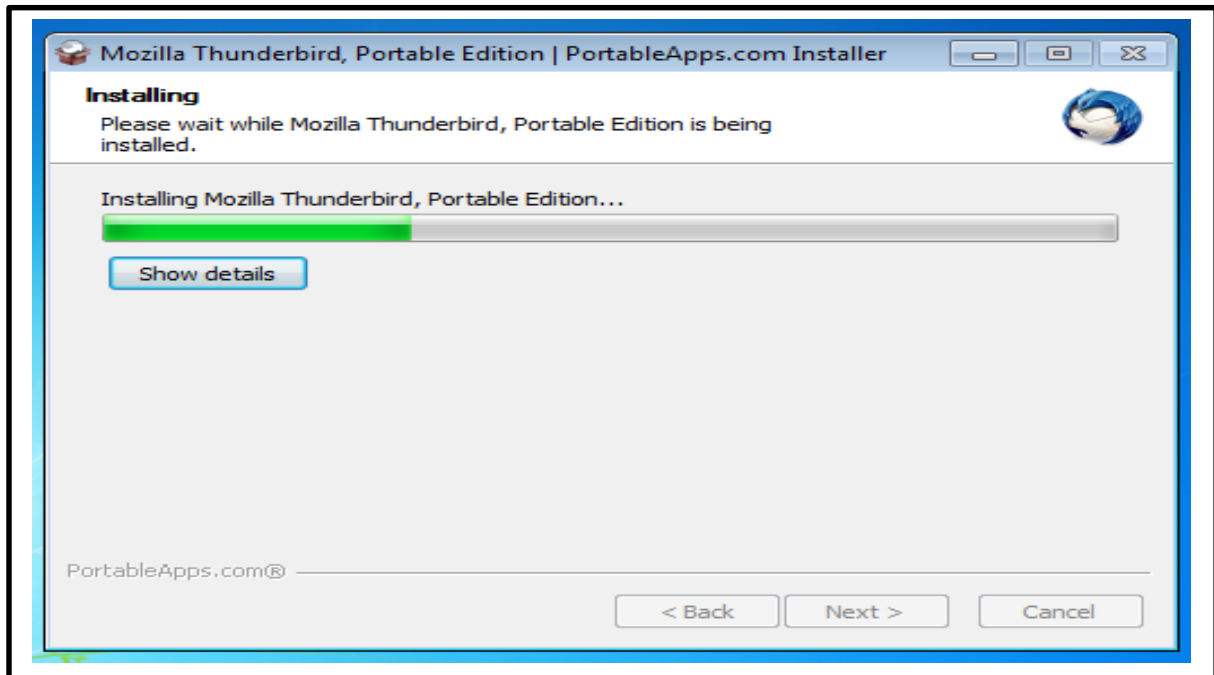


Figure IV.29. Installation de Thunderbird.

4. Cliquez sur Terminer pour compléter la procédure d'installation :

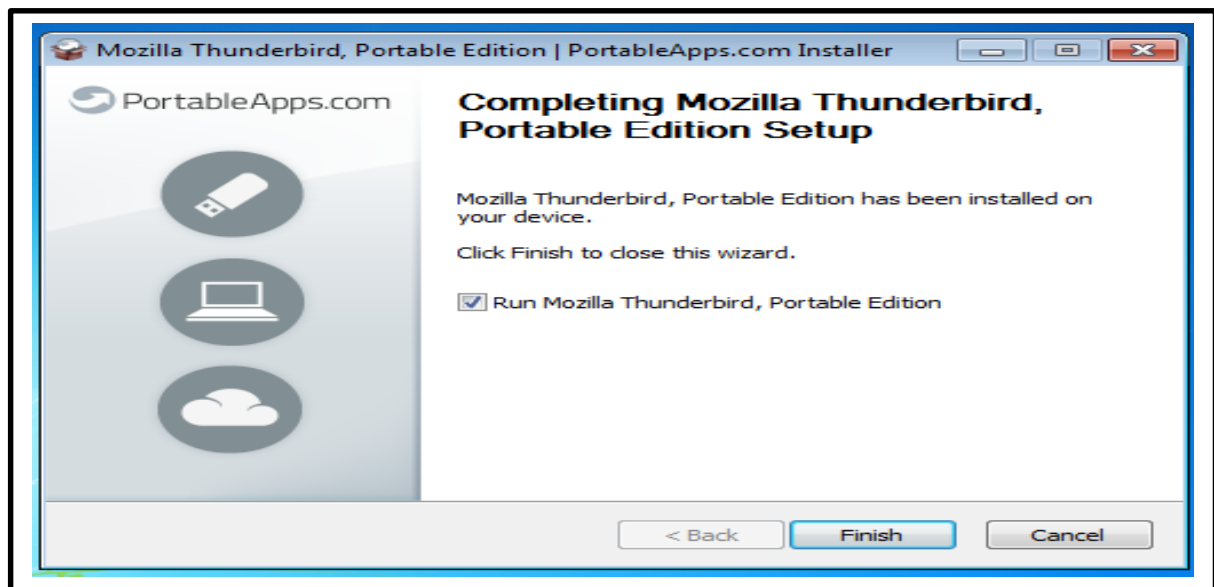


Figure IV.30. Fin d'installation.

5. L'interface d'accueil de Thunderbird se présente de la façon suivante :

- Une barre de menu donnant accès à l'intégralité des fonctions de Thunderbird.

- Une barre d'outils donnant accès aux fonctions les plus utiles (recevoir le courrier, envoyer, transférer, imprimer, etc.).
- Une Barre latérale contenant la liste des dossiers.
- Une fenêtre contenant les entêtes des Emails.
- Une fenêtre de prévisualisation des Emails.

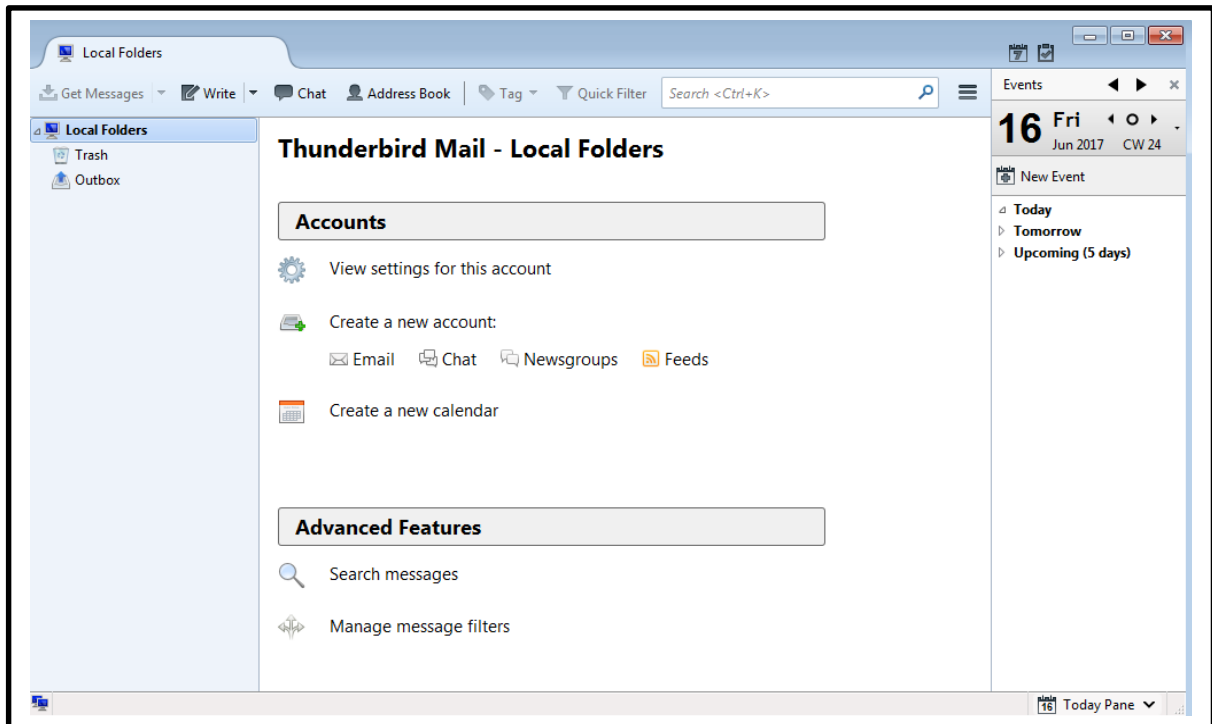


Figure IV.31. Aperçu de l'interface de Thunderbird.

IV.2.2. Configuration du Client Thunderbird

1. Configuration d'un compte de messagerie avec Thunderbird est facile. Tout ce qu'on doit faire est de fournir le nom d'utilisateur et le mot de passe associés à l'adresse courriel dans la boîte de dialogue ci-dessous :

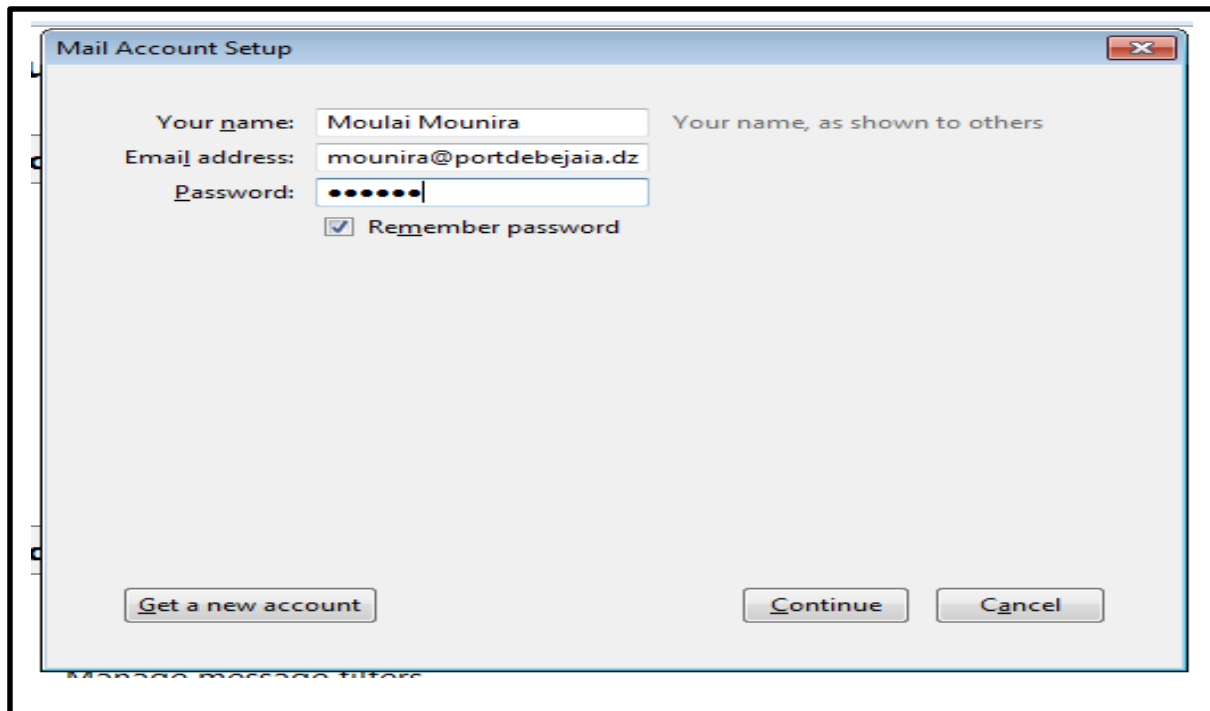


Figure IV.32. Ajout d'un compte avec Thunderbird.

2. Lorsqu'on clique sur le bouton continu, Thunderbird va chercher le fournisseur d'accès et tenter de terminer les paramètres du serveur.

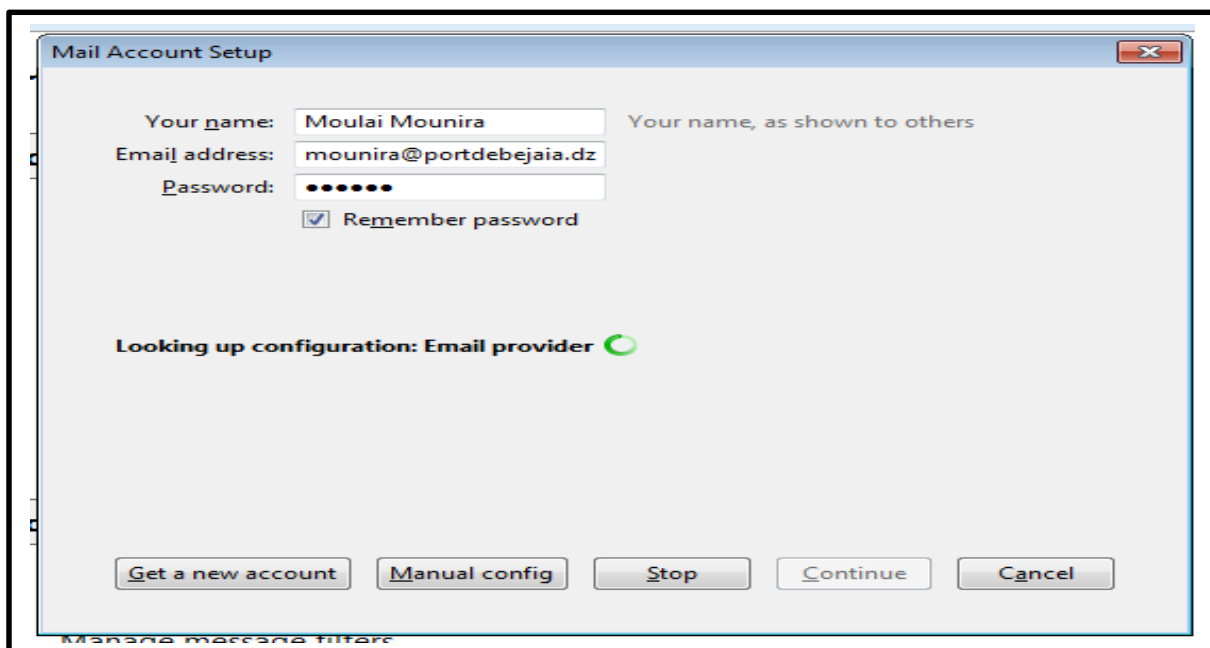


Figure IV.33. Recherche du fournisseur.

3. La configuration manuelle du compte, on spécifiant les protocoles de courrier entrant et sortant après on cliquant sur Re-test et puis Terminer :

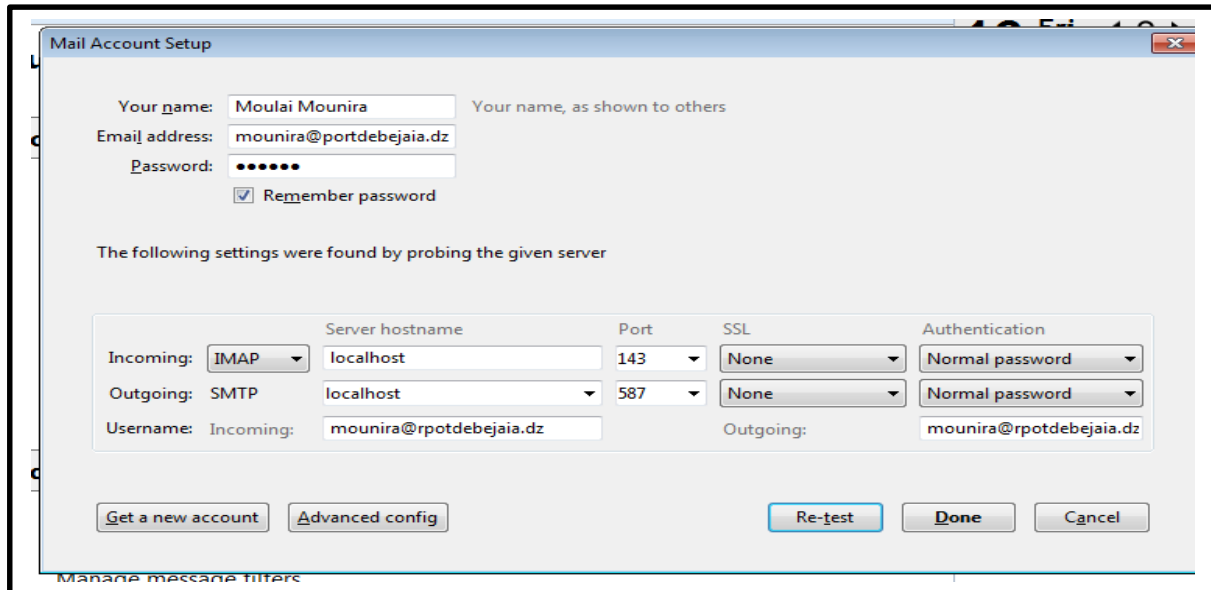


Figure IV.34. Spécification des protocoles de courrier entrant et sortant.

4. Dans la case qui va s'ouvrir on clique sur j'accepte les risques, après cliquer Terminer :

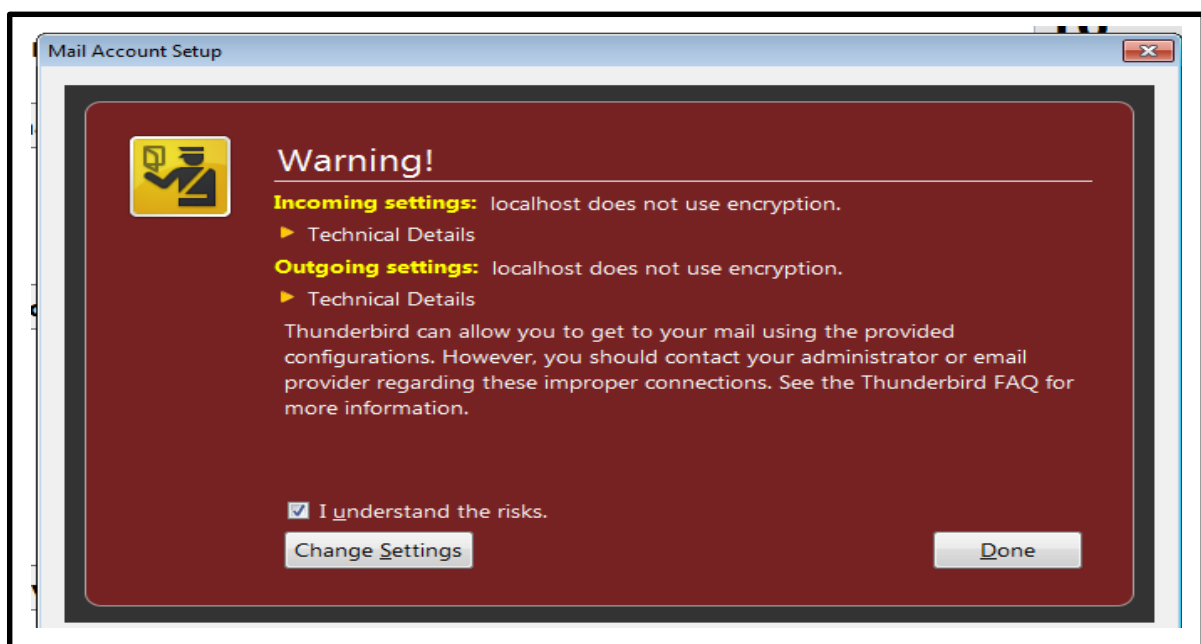


Figure IV.35. Acceptation des risques.

5. Une fois un compte de messagerie est configuré, on est prêt à envoyer et recevoir des messages avec Thunderbird.
 - Pour envoyer un nouveau message il faut cliquer sur **écrire** dans la barre d'outils.
 - Puis la fenêtre pour rédiger le message apparaît.
 - Dans le champ **Pour**, on écrit l'adresse électronique à laquelle on souhaite envoyer le message.
 - Dans le champ **Sujet**, on écrit l'objet du message.
 - Saisir le contenu du message dans la zone blanche.
 - En fin cliquer sur **Envoyer**.

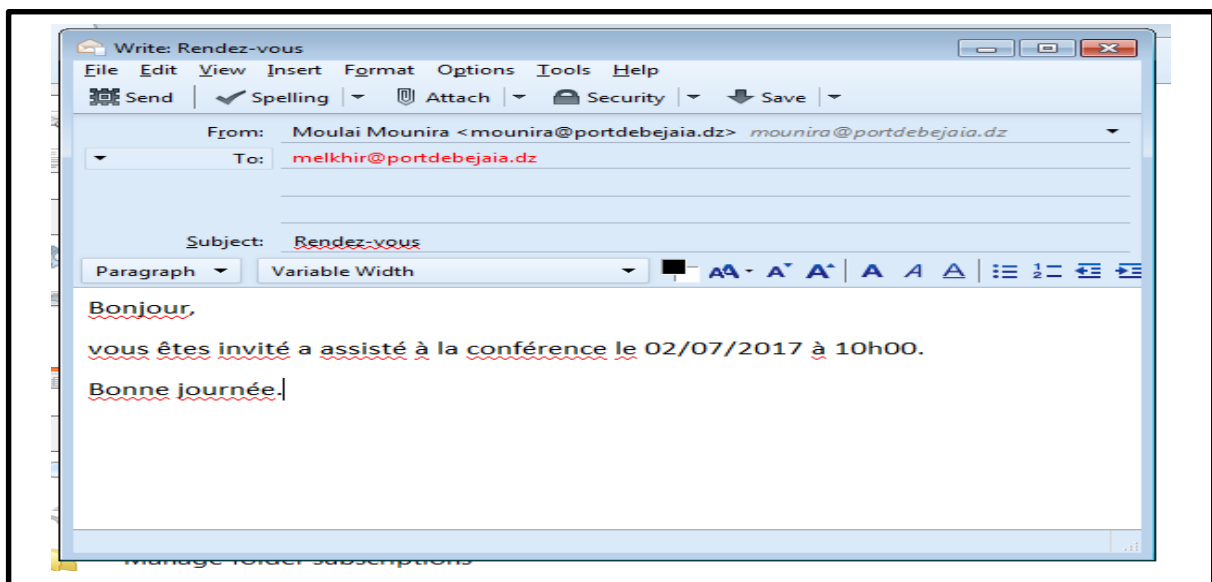


Figure IV.36. L'envoi d'un message.

6. La réception d'un message.

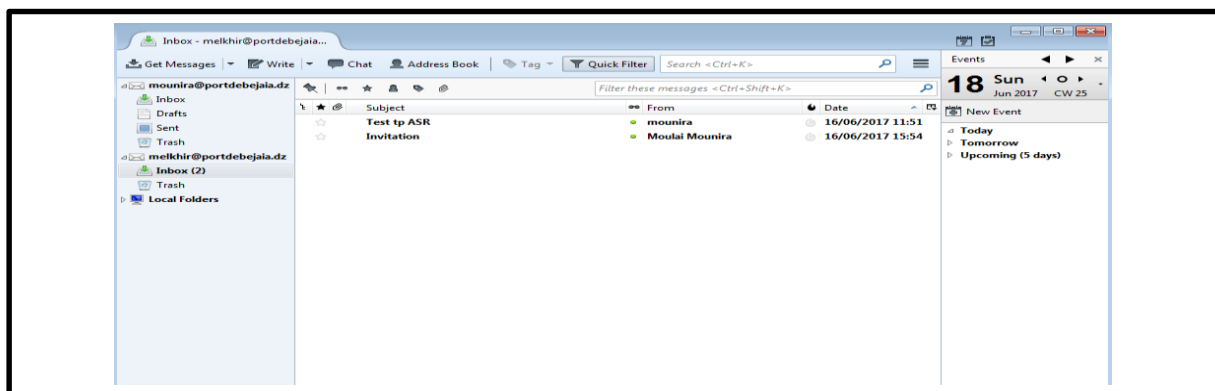


Figure IV.37. La réception d'un message.

Conclusion

Dans ce chapitre, nous avons détaillé les outils qui permettent d'effectuer des opérations d'administration, nous avons choisi le serveur de messagerie et les clients qui nous permettent d'envoyer et de recevoir des messages.

Pour la configuration du serveur on a choisi le IMAP et SMTP comme protocole d'échanger de courrier.

Conclusion générale

Conclusion générale

Le courrier électronique est une application internet très importante, elle est la base du travail collaboratif : le courrier électronique facilite en effet la communication et l'échange de documents de travail (pièce jointe), dans des délais pouvant être très courts.

Notre objectif à travers ce travail est de pallier aux différentes faiblesses de l'organisme d'accueil ; en termes de disponibilité du service de la messagerie électronique et de sa sécurité.

En effet après notre passage à l'Entreprise Portuaire de Béjaïa, nous avons pris le temps d'analyser leurs besoins et de leur suggérer une solution qui consiste à mettre en place un serveur de messagerie électronique dont la disponibilité est continue et qui assure sa sécurité.

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

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

- ✓ HMailServer comme serveur.
- ✓ MariaDB comme Base de données.
- ✓ POP3 et IMAP comme protocoles de la réception des messages.
- ✓ SMTP comme protocole d'envoi des messages.
- ✓ ClamWin comme anti-virus.
- ✓ SpamAssassin comme Anti-SPAM.
- ✓ TLS comme protocole de sécurité.
- ✓ Thunderbird comme client de messagerie.

Nous avons tout au long de ce travail voulu offrir au lecteur la possibilité de mettre en place son propre serveur mail grâce aux différentes directives que nous avons présentées de manière explicite et détaillée. Nous avons commencé dans le premier chapitre à définir quelle que soit la généralité sur les réseaux informatiques, le deuxième chapitre nous a consacré à la présentation de l'organisme d'accueil, le troisième chapitre nous a fait une étude sur la messagerie électronique et les protocoles associés. Enfin, le quatrième chapitre nous a permis de finaliser le tout par la configuration et la mise en œuvre de la messagerie.

Nous souhaitons que ce modeste travail puisse servir comme outil d'aide et de documentation au profit des futures promotions.

Références bibliographiques

Référence bibliographique

- [1] : Tout sur les réseaux et Internet, Jean_François, Dillon, édition DUNOD.2001.
- [2] : GUY Pujolle, Les réseaux, Avec la collaboration de Olivier salvatori et la contribution de Jacques Nozick, Eyrolle, 5^e édition.2010.
- [3] : Internet et commerce électronique 2^eme édition, Lionel Bocherberg, édition Dalloz, Paris 2001.
- [4] : Internet Services et Réseaux, Dominique présent, Stéphane lohier, édition DUNOD. 2003.
- [5] : Sécurité Informatique-principes et méthodes, Laurent bloch, Christophe wolfhugel, édition Eyrolles, 2007.
- [6] : Tableaux de bord de la sécurité réseau, Cédéric Liorens, Lauent Levier, DenisValois, 2^eme édition, Eyrolles, 2006.
- [7] : Internet et commerce électronique, Lionel Bocherberg, 2eme édition, 2007.

Références webographie

- [web.1]: https://fr.m.wikipedia.org/wiki/S%C3%A9curit%C3%A9_des_syst%C3%A8mes_d%27_informations. **Consulter Mai 2017.**
- [web.2] : <http://www.comentcamarche.net/faq/17453-qu-est-ce-qu-un-proxy> **Consulter Mai 2017.**
- [web.3] :<http://www.journaldunet.com/solutions/pratique/dictionnaireduwebmastering/reseau/19567/vpn-virtual-private-network-definition-traduction-et-acteurs.html> **Consulter Février 2017.**
- [Web.4]:[http://fr.m.wikipidia.org/wiki/zone_d%C3%A9militaris%C3%A9e_\(informatique\)](http://fr.m.wikipidia.org/wiki/zone_d%C3%A9militaris%C3%A9e_(informatique)). **Consulter Février 2017.**
- [Web.5]: <https://ead-iseag.univ-st-etienne.fr/claroline/backends>. **Consulter Mars 2017.**
- [Web.6] : https://fr.wikipedia.org/wiki/Serveur_de_messagerie_%C3%A9lectronique **Consulter Février 2017.**
- [Web.7] : <http://www.lea-nantes.com/informatique/CoursInternetRemanie.pdf> **Consulter Février 2017.**
- [Web.8] : [réseaux/architectures/messagerie-electronique.html](#) **Consulter Février 2017.**

[Web.9]: http://clubinforocatin.free.fr/Tutoriels_2013/Messagerie/Protocoles

Messagerie.pdf **Consulter Février 2017.**

[Web.10] : <http://www.provectio.fr/guide/messagerie/serveur/protocole/> **Consulter Mars 2017.**

[Web.11] : http://sgill.profweb.ca/spip/IMG/pdf/Postfix_v2.pdf **Consulter Juin 2017.**

[Web.12] : <http://csricted.univ-setif.dz/files/cours%20informatique/SMTP.pdf> **Consulter Juin 2017.**

[Web.13] : <http://heureuxoli.developpez.com/office/outlook/protocoles/> **Consulter Mai 2017.**

[Web.14] : <http://www.definitions-marketing.com/definition/client-de-messagerie> **Consulter Juin 2017.**

[Web.15] : <https://fqqdn.fr/2014/10/09/les-menaces-liees-a-la-messagerie-electronique-et-les-solutions-appropriees> **Consulter Mai 2017.**

Résumé

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

Notre travail consiste à mettre en place un serveur de messagerie au sein de l'Entreprise Portuaire de Béjaia.

Mots-clés: MUA, MTA, MDA, IMAP, POP3, SMTP, HMAISERVER, THUNDERBIRD.

Abstract

E-mail is a highly answered and indispensable service in the professional field and in everyday life; even it is one of the most important services of the Internet network. It makes communication easier and simpler thanks to the saving of time and quality of response. It may be unavailable because it depends on the Internet and can also pose a security threat, which is why it has to be secured, to maintain its security and to ensure its availability. Our job is to set up a mail server in the Port Enterprise of Béjaia.

Keywords: MUA, MTA, MDA, IMAP, POP3, SMTP, HMAISERVER, THUNDERBIRD.