REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE
Département informatique

MEMOIRE

DE FIN D'ETUDES

EN VUE DE L'OBTENTION DU DIPLOME DE MASTER EN INFORMATIQUE
SPECIALITE : Système Informatique

THEME

Mise en place d'un système de messagerie sécurisé dans une PMI/PME

Réalisé par :
Melle Hammiche melissa
Hesnaoui katia

soutenue le 26/09/2018

Devant le jury :

PRESIDENT: Mr SADOU Samir

PROMOTEUR : Mme BOURKACHE Ghenima

EXAMINATRICE: Mme BELATAF

Résumer :

Il ne fait désormais plus aucun doute que les technologies de l'information et de la Communication représentent la révolution la plus importante et la plus innovante qui a marque la vie de l'humanité en ce siècle passé. En effet, elles viennent nous apporter de multiples conforts _a notre mode de vie en révolutionnant le travail des individus par leur capacité de traitement d'information, d'une part, et de rapprochement des distances d'une autre. Parmi ces technologies, la messagerie électronique qui est assez développée dans les organisations aux cours de ces quinze dernières années, grâce a sa facilite d'utilisation et son utilité perçue. C'est un service gratuit qui constitue un moyen de communication privilégie entre des personnes _a travers un réseau informatique. Utilisé pour des applications très variées personnelles, professionnelles, associatives, politiques, etc., celui-ci occupe une place de plus en plus prépondérante par rapport aux moyens de communication traditionnels. Outre son faible cout, la messagerie électronique a l'avantage d'optimiser la communication et la divulsion d'informations ce qui la rend indispensable au sein d'une entreprise, néanmoins la dépendance du réseau internet touche a la disponibilité de ce service ainsi qu'_a sa sécurité. Ainsi une mise en place d'un serveur de messagerie stable, disponible et sécuriste s'impose. Dans ce contexte, nous allons indiquer comment un système de messagerie interne, de par sa mise en place et sa sécurisation pourrait répondre aux besoins en termes de technologies de l'information et de la communication d'une entreprise. Ce rapport est composte de trois chapitres :

Dans le Chapitre 01 nous présentons un aperçu général sur les réseaux leurs architectures, leurs principales caractéristiques puis nous allons parler sur la sécurité des réseaux, et les mécanismes qui nous permettent de sécuriser un réseau local d'une entreprise.

Le chapitre 02 sera consacre _a la présentation de la messagerie électronique pour une PME/PMI et d'une manière théorique et détaille les bêlements importants d'un serveur de messagerie électronique.

Le chapitre 03 sera consacre _a la réalisation de notre projet, et les différentes étapes suivies pour la réalisation d'un serveur de messagerie sécuriste. Et en nous réalisons le travail par une conclusion générale résumant les grands points qui ont et abordes ainsi que les perspectives que nous souhaitons accomplir prochainement.

Les mots clés :

-la messagerie électronique
-serveur de messagerie
-architecture client/serveur
-la messagerie dans une PME/PMI
-sendmail
-zimbra

Remerciement

Nos remerciements vont droit à Madame BOURKACHE d'avoir accepter de nous encadrer.Nous vous remercions pour la gentillesse et la spontanéité avec lesquelles vous avez bien voulu diriger ce travail. Nous avons eu le grand plaisir de travailler avec vous, et avons trouvé auprès de vous la conseillère et la guide qui nous a reçu avec sympathie et bienveillance.Veuillez trouver dans ce modeste travail l'expression de notre haute considération, de notre sincère reconnaissance et de notre profond respect.

Nos remerciements vont droit aux membres du jury, c'est pour nous un grand honneur de vous voir siéger dans notre jury. Nous vous sommes très reconnaissants, de L'amabilité avec laquelle vous avez accepté de juger notre travail. Veuillez trouver le témoignage de notre grande reconnaissance et de notre profond respect.

Dédicace

Je dedie ce modeste travail

A mes chers parents A ma sœur amel, son

époux Toufik et a mon petit chéri Lounas

A mon frére Amar sa femme et a mon petit neveu adoré Naél

je remercie BELHARRAT HAKIM pour son éternel soutient et la confiance qu'il a en mes capacités

A toute ma famille.

A tous mes ami(e)s surtout a OULDFELLA Nora qui ma vraiment aidé

HESNAOUI Katia

Dédicace

Je dédie ce travail,

A mes chers parents qui n'ont jamais cessé de m'encourager

tout au long de mon parcoure et qui ont toujours tout sacrifié pour faire de moi ce que je suis à présent

que dieux les protège

A ma petite sœur adoré qui ma toujours soutenue

A toute ma famille mes oncles et mes tantes que j'aime beaucoup

A mes voisins en particularité Nina que je remercie beaucoup

A mes amis kamelia , Ahlem , Mounir , Amine

A mes camarades proche avec qui Jai passé de bon moment

Melissa

Table des matières

Introduction générale **6**

1 généralité sur les réseaux **7**

1.1 Introduction 8
1.2 Définition 8
1.3 Intérêt des réseaux 8
1.4 Classification des réseaux 8
1.4.1 Selon leur taille : 9
1.4.1.1 Les LAN : 9
1.4.1.2 Les MAN 9
1.4.1.3 Les WAN 9
1.4.2 Selon leur topologie 9
1.4.2.1 La topologie en bus 9
1.4.2.2 La topologie en Étoile 10
1.4.2.3 La topologie en anneau 10
1.5 Normalisation des réseaux 11
1.5.1 l'architecture en couches 11
1.5.2 le modèle OSI 12
1.5.3 Le modèle TCP/IP 13
1.6 Client/serveur 14
1.6.1 L'architecture client/serveur à deux niveaux : 14
1.6.2 L'architecture client/serveur à trois niveaux : 15
1.7 Serveur DNS (Domain Name Server) : 17
1.7.1 Principaux types d'enregistrement : 17
1.8 Serveur DHCP : 17
1.9 La sécurité dans les réseaux 18
1.9.1 les menaces 19
1.9.2 Les logiciels malveillants 19
1.9.3 Mécanismes de la sécurité 20

1.10 Conclusion 21

2 Messagerie électronique 22

2.1 la messagerie électronique pour une PME/MPI : 23
2.1.1 Introduction 23
2.1.2 Besoin de PME/PMI en termes de TIC : 23
2.1.3 Apport d'un système de messagerie a une PME/PMI 23
2.1.4 Enjeux et objectifs de sécurité sur un tel système 24
2.2 Problématique 24
2.3 Suggestions : 25
2.4 Les systèmes de messageries électroniques et leurs sécurités 25
2.4.1 Introduction 25
2.4.2 Courrier électronique : 25
2.4.2.1 Serveur de messagerie 25
2.4.2.2 L'adresse électronique 26
2.4.3 Structure d'un courrier électronique. 26
2.4.4 L'architecture de la messagerie électronique et son fonctionnement 27
2.4.5 Les serveurs et les clients de la messagerie électronique 28
2.4.5.1 Les serveurs de messagerie 29
2.4.5.2 Les clients de messagerie 30
2.4.6 Les protocoles de courrier électronique 31
2.4.6.1 Protocoles de transfert de courrier électronique 31
2.4.6.2 Protocoles d'accès au courrier 32
2.5 Sécurité de la messagerie 32
2.5.1 Les menaces de serveurs de messagerie 32
2.5.2 Les protocoles de sécurité des serveurs de messagerie. 33
2.5.2.1 Le Protocol SSH 33
2.5.2.2 Le protocole TLS 34
2.5.2.3 Un certificat numérique : 34
2.5.3 Anti-virus et anti-spam des serveurs de messagerie 34
2.6 Conclusion 35

3 Réalisation 36

3.1 Introduction : 37
3.2 Installation et configuration du système d'exploitation : 37
3.3 Création du réseau local du serveur de messagerie : 37
3.3.1 Installation et configuration du serveur DNS : 38
3.3.2 Installation et configuration d'un serveur DHCP : 41

3.3.3 Installation de serveur apache et de language php 42
3.3.4 Installation d'un serveur Mysql-server et de l'interface web Php-

MyAdmin 43
3.3.5 Génération d'un certificat 44
3.3.6 Installation et configuration de Postfix et de l'interface web Post-fixadmin : 45
3.3.7 Installation et configuration de Dovecot imap et Dovecot pop3 51
3.3.8 Installation et configuration d'un antivirus et d'un anti-Spam (clamv, amavis, spamassassin) : 54
3.3.9 Installation d'un webmail (Roundcube) : 56
3.4 conclusion 63

conclusion générale **64**

Table des figures

1.1 La topologie en bus 10
1.2 La topologie en étoile 10
1.3 la topologie en anneau 11
1.4 les couches de modèle OSI 12
1.5 le passage de modéle OSI au modéle TCP/IP 14
1.6 Architecture client/serveur à deux niveaux 15
1.7 Architecture client/serveur à 3 niveaux. 16
1.8 architecture client/serveur à n-tiers 16
1.9 Fonctionnement de serveur DHCP 18

2.1 le fonctionnement de la messagerie électronique. 28

3.1 création d'un réseau local 38
3.2 Installation d'un serveur DNS 38
3.3 Définition des deux zone mail.com et 1.168.192.in-addr.arpa . . 39
3.4 Configuration de fichier mail.zone 39
3.5 Configuration de fichier mail.invzone 40
3.6 Indication de l'adresse du serveur DNS 40
3.7 Test de fonctionnement de serveur DNS 41
3.8 Configuration du fichier dhcpd.conf 42
3.9 Vérification de l'installation d'Apache2 42
3.10 Vérification de l'installation de php7 43
3.11 Interface de Phpmyadmin 43
3.12 Génération de la clé privée et la clé non sécurisée 44
3.13 Génération d'une demande de signature de certificat 44
3.14 Génération d'un certificat auto-signé 45
3.15 Configuration du nom de courrier Postfix 45
3.16 La base de donnée postfixadmin et ses tables 46
3.17 Créer le mot de passe et générer son hash 46
3.18 Insertion de la valeur de hachage de mot de passe generé 47

3.19 Page de connexion 47
3.20 Ajouter le domaine mail.dz 48
3.21 liste des utilisateurs 48
3.22 Création de répertoire des courriers électroniques 48
3.23 Configuration de fichier main.cf 49
3.24 Configuration de fichier main.cf 49
3.25 Le fichier mysql_virtual_domains_maps.cf de postfix 50
3.26 Le fichier mysql_virtual_alias_maps.cf 50
3.27 Configuration de fichier master.cf de postfix 51
3.28 Configuration de fichier master.cf de postfix 51
3.29 Configuration de ficher dovecot.d de Dovecot 52
3.30 Configuration de fichier 10-auth.conf de Dovecot 52
3.31 Configuration de fichier auth-sql.conf.ext de Dovecot 53
3.32 Configuration de fichier dovecot-sql.conf.ext de Dovecot 53
3.33 Configuration de fichier 10-mail.conf de Dovecot 54
3.34 Configuration de fichier 10-lda.conf de Dovecot 54
3.35 Configuration de fichier 15-content_filter_mode de amavisd . . 55
3.36 Configuration de fichier spamassassin de Spamassassin 55
3.37 Résultat de la commande openssl 56
3.38 Création et configuration de fichier webmail.conf dans Apache2 . . 57
3.39 Vérification de l'environnement de serveur 57
3.40 Spécification de port imap sécurisé et le nom de domaine 58
3.41 Spécification de port smtp sécurisé 59
3.42 Le fonctionnement de port 465 de Postfix 60
3.43 Le fonctionnement de port 993 de Dovecot 60
3.44 La page de connexion de Roundcube 61
3.45 Composer et envoyer un mail 61
3.46 La réception de message transmis 62
3.47 Message conservé dans le répertoire créé dans le serveur 62

Introduction générale

Il ne fait désormais plus aucun doute que les technologies de l'information et de la communication représentent la révolution la plus importante et la plus innovante qui a marqué la vie de l'humanité en ce siècle passé. En effet, elles viennent nous apporter de multiples conforts à notre mode de vie en révolutionnant le travail des individus par leur capacité de traitement d'information, d'une part, et de rapprochement des distances d'une autre. Parmi ces technologies, la messagerie électronique qui est assez développée dans les organisations aux cours de ces quinze dernières années, grâce à sa facilité d'utilisation et son utilité perçue. C'est un service gratuit qui constitue un moyen de communication privilégié entre des personnes à travers un réseau informatique. Utilisé pour des applications très variées personnelles, professionnelles, associatives, politiques, etc., celui-ci occupe une place de plus en plus prépondérante par rapport aux moyens de communication traditionnels. Outre son faible coût, la messagerie électronique a l'avantage d'optimiser la communication et la diffusion d'informations ce qui la rend indispensable au sein d'une entreprise, néanmoins la dépendance du réseau internet touche a la disponibilité de ce service ainsi qu'à sa sécurité. Ainsi une mise en place d'un serveur de messagerie stable, disponible et sécurisé s'impose. Dans ce contexte, nous allons indiquer comment un système de messagerie interne, de par sa mise en place et sa sécurisation pourrait répondre aux besoins en termes de technologies de l'information et de la communication d'une entreprise. Ce rapport est composé de trois chapitres :

Dans le Chapitre 01 nous présentons un aperçu général sur les réseaux leurs architectures, leurs principales caractéristiques puis nous allons parler sur la sécurité des réseaux, et les mécanismes qui nous permettent de sécuriser un réseau local d'une entreprise.

Le chapitre 02 sera consacré à la présentation de la messagerie électronique pour une PME/PMI et d'une manière théorique et détaillé les éléments importants d'un serveur de messagerie électronique.

Le chapitre 03 sera consacré à la réalisation de notre projet, et les différentes étapes suivies pour la réalisation d'un serveur de messagerie sécurisé. Et enfin nous finalisons le travail par une conclusion générale résumant les grands points qui ont été abordés ainsi que les perspectives que nous souhaitons accomplir prochainement.

Chapitre 1

généralité sur les réseaux

1.1 Introduction

Les réseaux sont nés du besoin d'échanger des informations de manière simple et rapide entre des machines. En d'autres termes, les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux, et enfin des machines terminales, telles que les stations à leur serveur. Dans un premier temps, ces communications étaient uniquement destinées au transfert des données informatiques, mais aujourd'hui avec l'intégration de la voix et de la vidéo, elle ne se limitent plus aux données mêmes si cela ne va pas sans difficulté. Dans ce chapitre nous allons définir des notions qui sont en relation avec notre thème et qui vont nous aider à bien réaliser notre projet.

1.2 Définition

Un réseau informatique, Est un ensemble d'équipements matériels et logiciels interconnectés les uns avec les autres dans le but de partager des ressources (données). Ces équipements peuvent être éloignés ou rapprochés [1].

1.3 Intérêt des réseaux

La nécessité de communication et du partage des informations en temps réel, impose aujourd'hui aux entreprises la mise en réseau de leurs équipements informatiques en vue d'améliorer leurs rendements. Un réseau permet :

- La communication entre personnes (grâce au courrier électronique, la discussion en direct,).
- La communication entre processus (entre des machines industrielles)
- La garantie de l'unicité de l'information (bases de données)
- Le partage de fichiers, d'applications

1.4 Classification des réseaux

Les réseaux sont classés en deux parties selon leur taille ou topologie

1.4.1 Selon leur taille :

1.4.1.1 Les LAN :

les LAN[1] sont des réseaux ne dépassant pas 5 km (ex : pour un immeuble). Ces réseaux sont privés (on ne peut pas y accéder de l'extérieur). Le taux d'erreur (c'est le nombre de bit erroné principalement à cause des composants matériels tel que les câbles. . .) est faible : de 1 bit erroné sur 10(8) à un bit sur 10(20). Le débit peut aller de quelques Mbits/s à 100 Mbits/s. Le nombre de station ne dépasse généralement pas 1000 mètres.

1.4.1.2 Les MAN

Les MAN[2] ne dépassent pas 200 km (ex : d'une ville à une région). Ces réseaux peuvent être privés ou publics. Le taux d'erreur reste faible : de 1bit erroné sur 10(8) à 1 bits sur 10(15). Le débit est élevé car supérieur à 100 Mbits/s. Ces réseaux fédérateurs permettent de relier plusieurs LAN entre eux.

1.4.1.3 Les WAN

Les WAN[3] sont des réseaux à l'échelle nationale ou internationale. La plupart sont publics. Le taux d'erreur est plus élevé : de 1bit erroné sur 10(6) à un bit erroné sur 10(12). Les débits dépendent du support, des réseaux. . . : de 56Kbits/s pour les modems les plus performant à l'heure actuelle à plus de 512Kbits/s (ex : ADSL quand il fonctionne normalement. . .).

1.4.2 Selon leur topologie

1.4.2.1 La topologie en bus

La topologie en bus est caractérisée par un câble central sur lequel tous les membres du réseau sont connectés. Dans ce type d'architecture, l'information est envoyée dans les deux sens donc le serveur est au centre. L'émission des données sur le bus se fait après écoute et absence du signale sur le bus [2].

1. local area network
2. Metropolitan Area Network
3. Wide Area Network

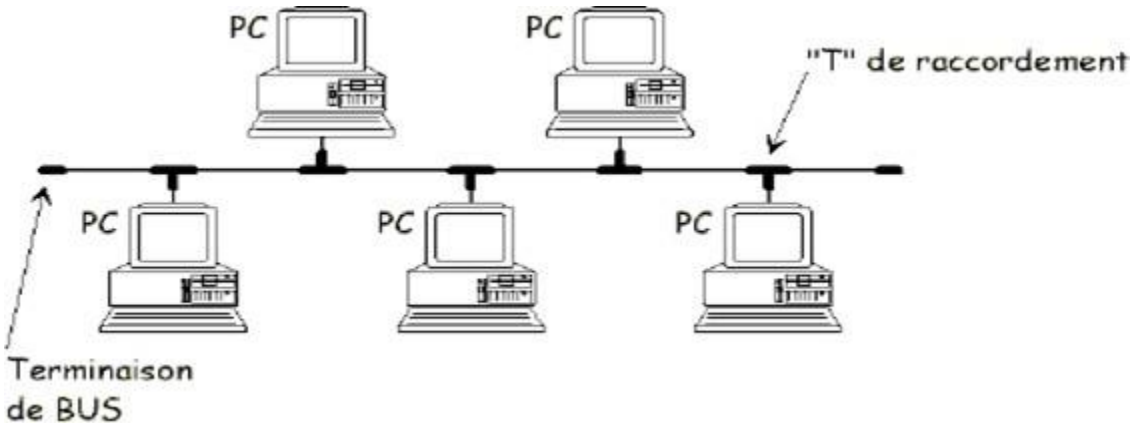

Figure 1.1 – La topologie en bus

1.4.2.2 La topologie en Étoile

La topologie en étoile est caractérisée par un point central (HUB ou SWITH) sur lequel tous les membres du réseau sont connectés. Le HUB permet le transport à 10 Mbps alors que le Switch permet le transport à 100 Mbps, il s'utilise au moins dans un réseau de 50 postes [2].

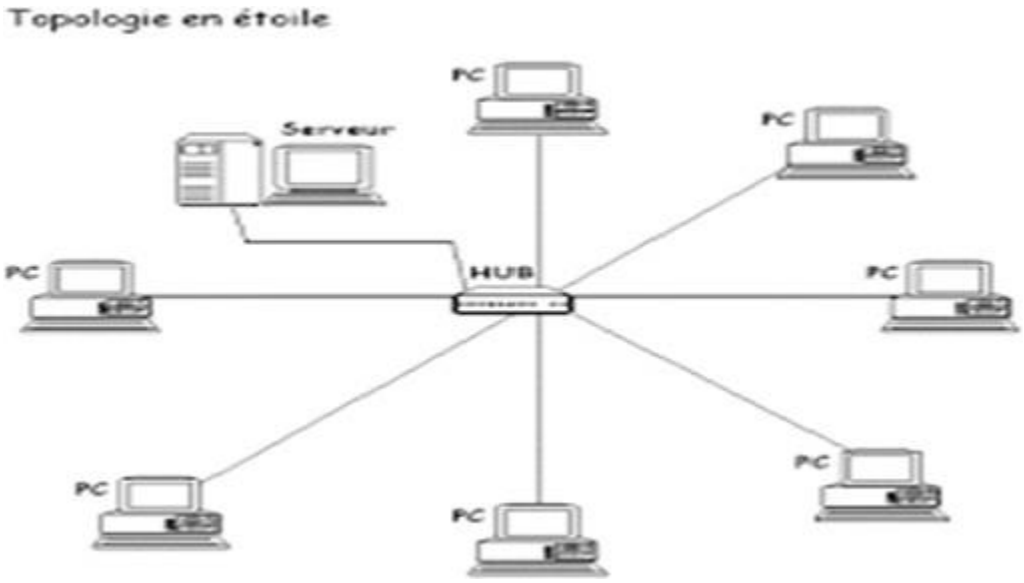

Figure 1.2 – La topologie en étoile

1.4.2.3 La topologie en anneau

La topologie en anneau tout comme en étoile est caractérisé par un point central sur lequel tous les membres du bureau du réseau sont connectés. Ce point central est

communément appelé MAU [4] [2].

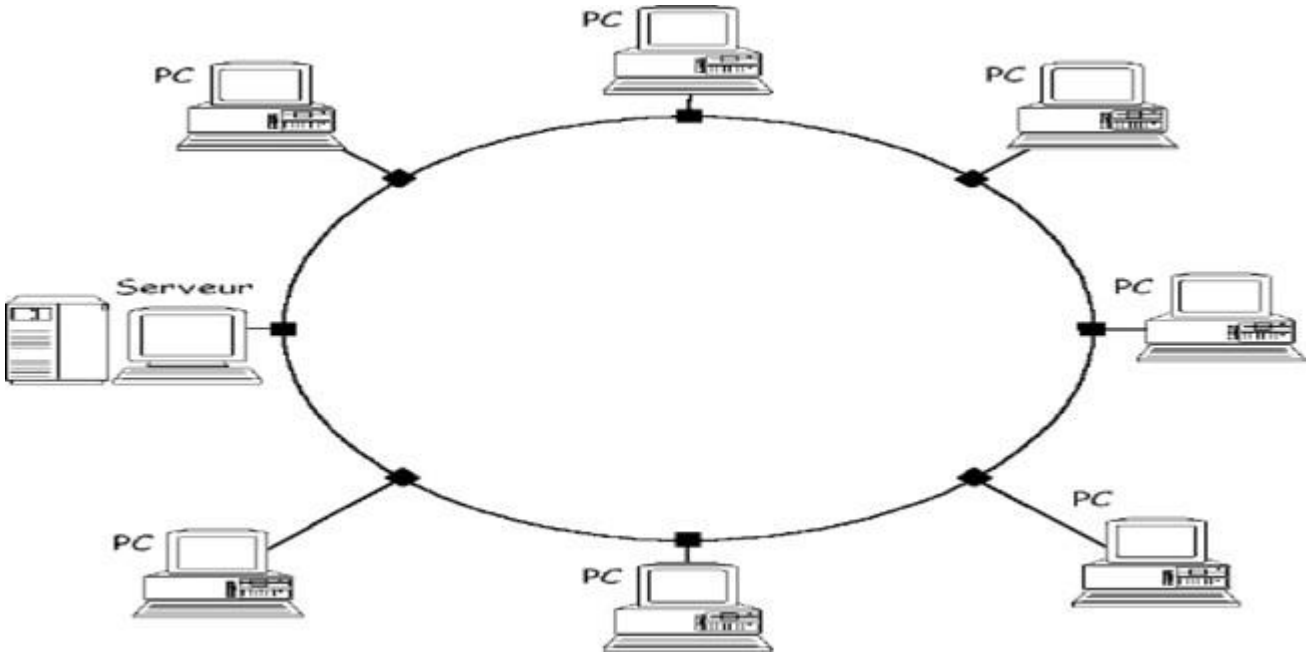

Figure 1.3 – la topologie en anneau

1.5 Normalisation des réseaux

Le transport des données d'une extrémité à une autre d'un réseau nécessite un support physique ou hertzien de communication. Cependant, pour que ces données arrivent correctement à leurs destinations il faut une architecture logicielle. Un protocole est une méthode standard qui permet la communication entre processus (s'exécutant éventuellement dans sur différents machines), c'est-à-dire un ensemble de règles et de procédure à respecter pour émettre et recevoir des données sur un réseau.

1.5.1 l'architecture en couches

Il existe plusieurs façons de représenter les protocoles dans une architecture, celle qu'on utilise depuis longtemps dans les réseaux consiste à les classer par couche, les couches doivent être indépendante les unes des autres, de quelle sorte qu'il soit possible de modifier un protocole dans une couche sans avoir à modifier les protocoles des autres couches. Les éléments actifs de chaque couche s'appellent entité, une entité de la même couche sur des machines différentes sont appeler entités paires, le concept d'architecture en couche consiste à attribuer à chaque couche de niveau N trois objets, qui sont [3] :

4. Multiple Accès Unit

— Service N : désigne le service qui doit être rendu par la couche N à la couche supérieure, ce service correspond à un ensemble d'actions effectuées par cette couche pour rendre au niveau supérieur
— Protocole N : désigne l'ensemble des règles définissent les mécanismes permettant de transporter les informations d'un même service N à une couche N. En particulier, le protocole N propose les règles de contrôle de données.
— Point d'accès au service N : : les points d'accès à un service N sont situés à la frontière entre les couches (N+1) et N, les services N sont fournis par une entité N à une entité (N+1) par le biais de ces points.

1.5.2 le modèle OSI

Le modèle OSI [5] est un standard de communication, en réseau, de tous les systèmes informatiques. C'est un modèle de communications entre ordinateurs proposé par l'ISO [6] qui décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions [3].

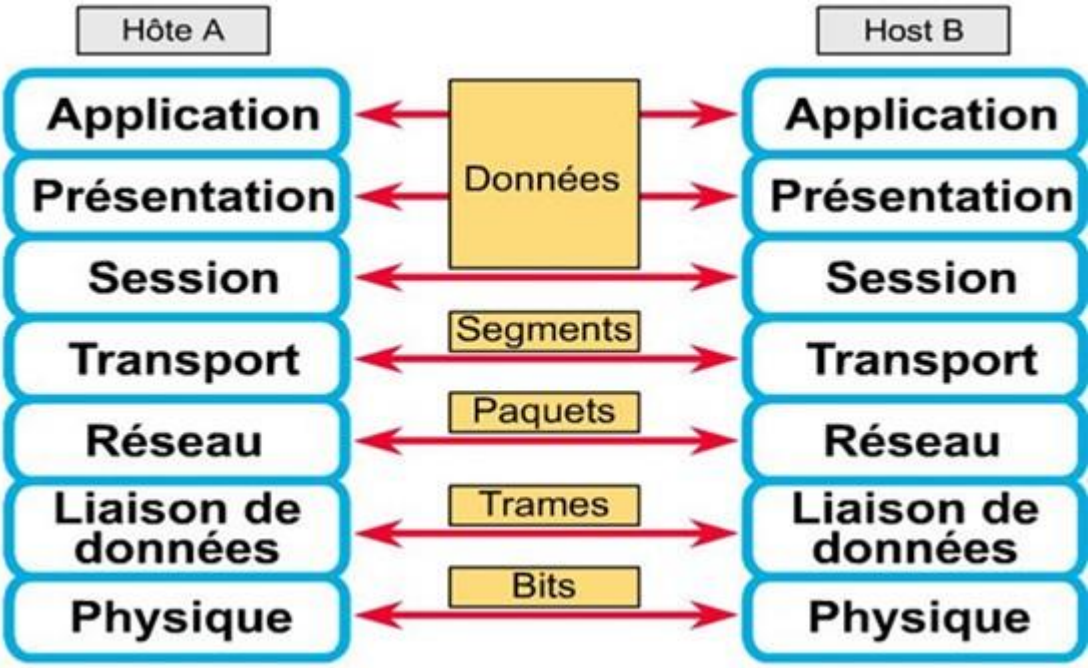

Figure 1.4 – les couches de modèle OSI

— Couche physique : Cette couche gère les connections matérielles, elle définit aussi la manière dont les données sont converties en signaux numériques.
— Couche liaison de données : cette couche fractionne les données d'entrées de l'émetteur en trame, transmet ces trames en séquence et gère les trames d'ac-

5. Open Systems Interconnection
6. Organisation Internationale de Normalisation

quittement renvoyées par le récepteur. Un rôle important de cette couche est la détection et la correction d'erreurs intervenues sur la couche physique.

— Couche réseau : cette couche est responsable des questions d'adressages notamment la traduction d'adresses physiques, c'est ici que l'on détermine la meilleure route entre la source et la destination. C'est également ici que l'on s'occupe de problème de congestion (trop de trafic sur la ligne) et de commutation (switching).

— Couche transport : Responsable de la transmission sans erreur et dans la bonne séquence des données sans perte ni duplication inutile.

— Couche session : Permet à deux applications d'établir, d'exploiter, et de terminer une connexion, cette couche est responsable de la reconnaissance des noms d'ordinateurs, la sécurité, la synchronisation entre taches.

— Couche présentation : détermine le format employé pour échanger une information entre deux ordinateurs. Fournit des services de cryptage et de compression de données (afin de réduire la quantité effective de données transmises).

— Couche application : cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichiers, la messagerie...

1.5.3 Le modèle TCP/IP

La suite TCP/IP est l'ensemble des protocoles utilisés pour le transfert des données sur Internet. Elle est souvent appelée TCP/IP, d'après le nom de ses deux premiers protocoles : TCP[7] et IP[8]. Le modèle OSI, qui décompose les différents protocoles en sept couches, peut être utilisé pour décrire la suite de protocoles Internet, bien que les couches du modèle OSI ne correspondent pas toujours avec les habitudes d'Internet (Internet étant basé sur TCP/IP qui ne comporte que quatre couches). Chaque couche résout un certain nombre de problèmes relatifs à la transmission de données, et fournit des services bien définis aux couches supérieures. Les couches hautes sont plus proches de l'utilisateur et gèrent des données plus abstraites, en utilisant les services des couches basses qui mettent en forme ces données afin qu'elles puissent être émises sur un médium physique. Le modèle Internet a été créé afin de répondre à un problème pratique, alors que le modèle OSI correspond à une approche plus théorique, et a été développé plus tôt dans l'histoire des réseaux. Le modèle OSI est donc plus facile à comprendre, mais le modèle TCP/IP est le plus utilisé en pratique. Il est préférable d'avoir une connaissance du modèle OSI avant d'aborder TCP/IP, car les mêmes principes s'appliquent, mais

7. Transmission Control Protocol
8. Internet Protocol

sont plus simples à comprendre avec le modèle OSI [3].

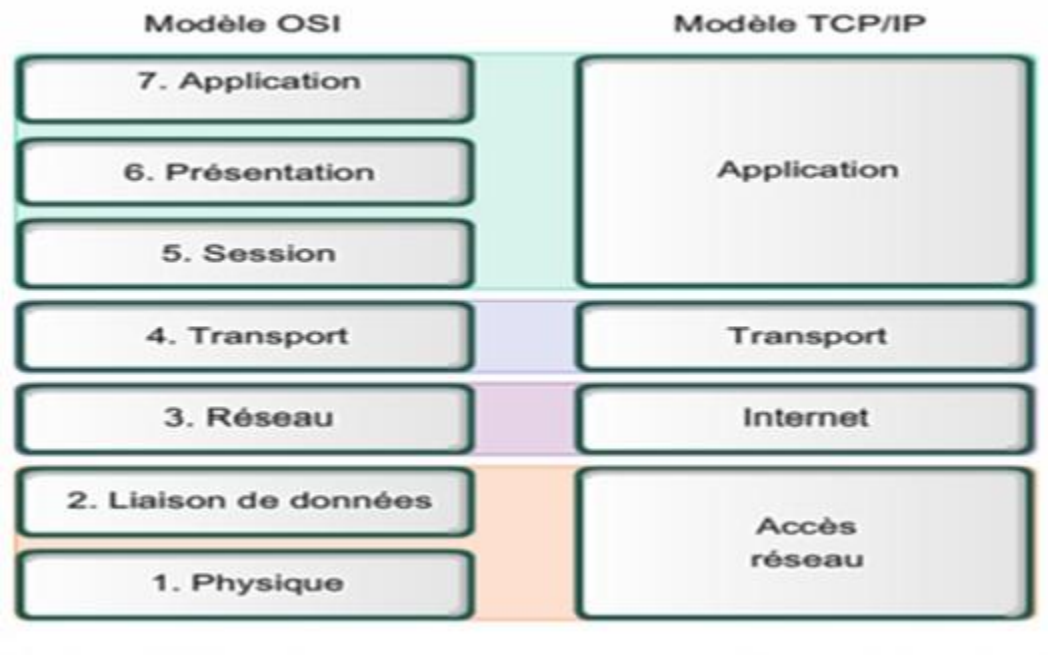

Figure 1.5 – le passage de modéle OSI au modéle TCP/IP

1.6 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 spécialisé en serveur d'applications, de fichier, 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 communiquant 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 [4] :

1.6.1 L'architecture client/serveur à deux niveaux :

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

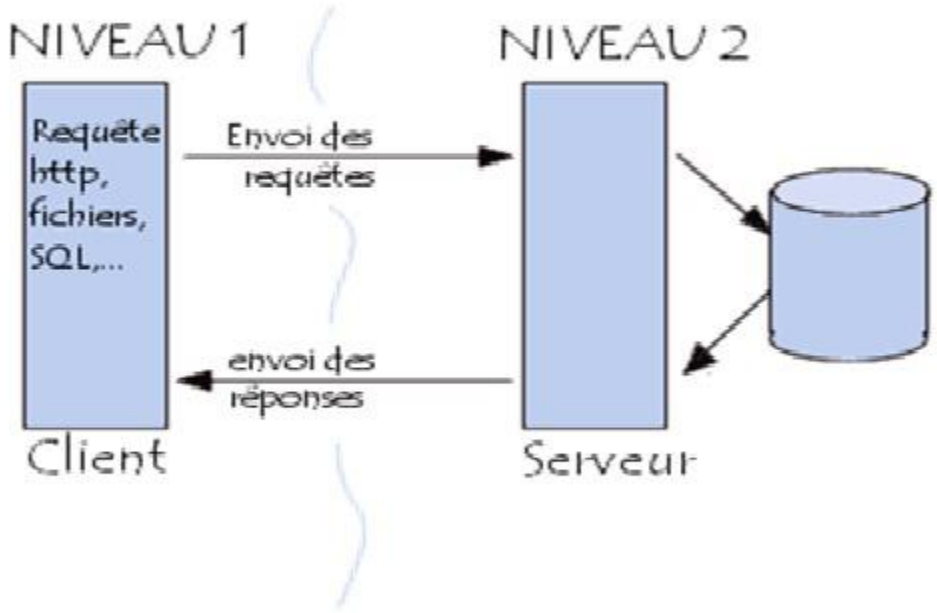

Figure 1.6 – Architecture client/serveur à deux niveaux

1.6.2 L'architecture client/serveur à trois niveaux :

Dans cette architecture un niveau intermédiaire se fait place entre les deux niveaux de l'architecture précédente :

- 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.

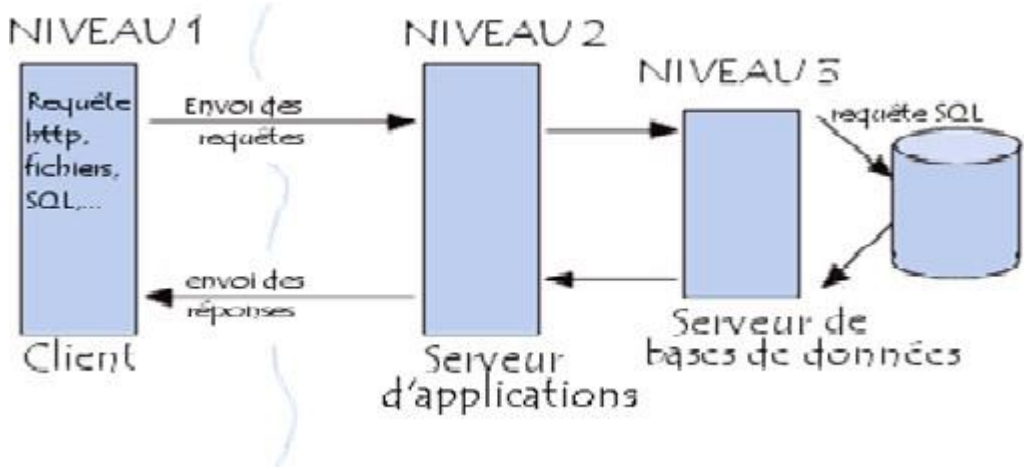

Figure 1.7 – Architecture client/serveur à 3 niveaux.

— l'architecture n-tiers : l'architecture n-tiers a été pensée pour concevoir des applications puissantes et simples a maintenir, ce type d'architecture permet de distribuer plus librement la logique applicative, ce qui facilite la répartition de la charge entre tous les niveaux, elle supprime toutes les limites des architectures précédentes :

1. Elle permet l'utilisation d'une interface utilisateur riche.
2. Elle sépare nettement tous les niveaux de l'application.
3. Elle offre de grande capacité d'extension.

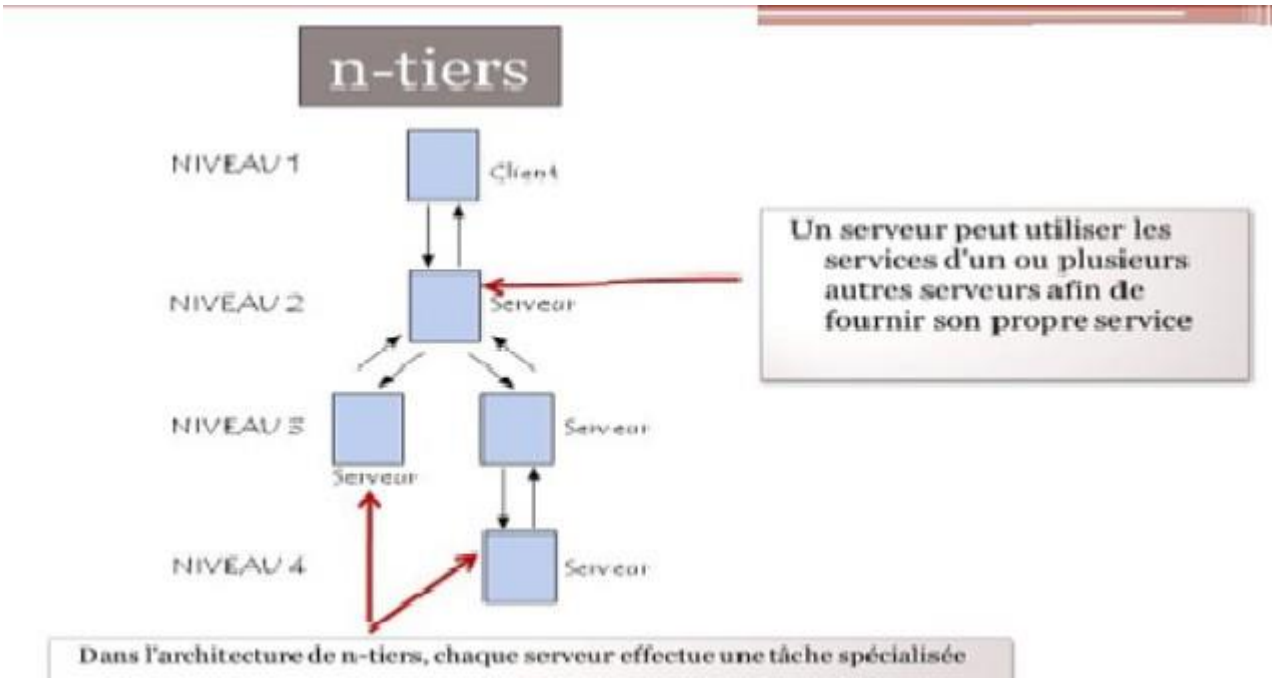

Figure 1.8 – architecture client/serveur à n-tiers

1.7 Serveur DNS (Domain Name Server) :

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 types de résolution :

- La résolution directe : Le principe de la résolution de noms, consiste à affecter un nom d'hôte à une adresse IP. On parle de résolution de noms directe.
- La résolution inverse : Le processus inverse doit pouvoir également être mis en œuvre. On parle de résolution de noms inverse ou reverse [26].

1.7.1 Principaux types d'enregistrement :

Les types d'enregistrements qui enrichissent une base de données DNS sont de plusieurs types, nous citons les principaux enregistrements [27] :

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

1.8 Serveur DHCP :

Un serveur DHCP est un serveur qui délivre dynamiquement des adresses IP aux ordinateurs qui se connectent sur le réseau. Le processus d'attribution se déroule en quatre phases : [28]

- 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 réception(ACK) : Le serveur DHCP confirme le bail avec sa durée et les options DHCP associées, et met à jour sa table des adresses IP allouées.

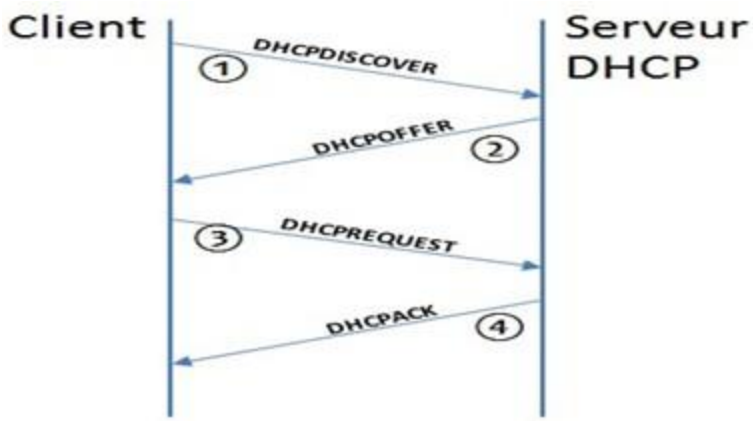

Figure 1.9 – Fonctionnement de serveur DHCP

1.9 La 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 à suivre.

— Les objectifs à assurer : Nous distinguons généralement cinq principaux objectifs de sécurité [5] :

1. Disponibilité : elle consiste à garantir l'accès à un service ou à une ressource
2. Intégrité : elle consiste à s'assurer que les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle)
3. Confidentialité : consiste à assurer que seules les personnes autorisées aient accès aux ressources échangées
4. Authentifiaction : 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
5. Non répudiation : elle consiste à garantir qu'aucun des correspondants ne pourra nier la transaction.

1.9.1 les menaces

Les menaces peuvent également être classées en deux catégories, soit elles ne changent rien (menaces passives) ou elles perturbent le réseau (menaces actives) [6].

1. 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.
2. Menaces actives : Elles sont de nature à modifier l'état du réseau.

1.9.2 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 proposés. Nous citons les plus répandus [6] :

Virus : Un virus est un morceau de programme informatique malicieux, conçu et écrit pour qu'il se reproduise. Cette capacité à se répliquer, peut toucher l'ordinateur, sans la permission de l'utilisateur et sans qu'il le sache. 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.

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.

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 il effectue des actions cachées. Le cheval de Troie contrairement au ver ne se réplique pas.

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

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.

1.9.3 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 [7] :

chiffrement : 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 déchirement. Ce principe est généralement lié au principe d'accès conditionnel.

Par-feu : Le Par-feu 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.

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.

VPN : Dans les réseaux informatiques, 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.

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.

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. 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.

1.10 Conclusion

Dans ce chapitre, nous avons présenté les différents concepts appelés à être utilisés dans notre travail, définition des réseaux, classification des réseaux, le rôle indispensable du serveur DNS, nous avons défini également le serveur DHCP et enfin, nous avons présenté certaines techniques qui permettent de sécuriser un réseau interne. Dans le chapitre suivant nous allons présenter la messagerie électronique son architecture son fonctionnement ainsi que sa sécurisation.

Chapitre 2

Messagerie électronique

2.1 la messagerie électronique pour une PME/MPI :

2.1.1 Introduction

Comme tout être vivant, l'entreprise est guidée dans ses actions par des objectifs qu'elle doit déterminer et réaliser avec efficience pour assurer sa survie et sa croissance. Ces objectifs consistent principalement à maximiser la valeur apportée : aux propriétaires, aux clients, aux salariés et aux sociétés aux seins desquelles elle exerce son activité.

2.1.2 Besoin de PME/PMI en termes de TIC :

La capacité à fixer et à réaliser les objectifs d'une entreprise de la bonne manière est appelée performance qui peut être fortement influencée par les technologies de l'information et de la communication (TIC) utilisées par l'entreprise. En effet, les TIC peuvent améliorer le fonctionnement de l'entreprise de différentes manières.

Premièrement, ces technologies permettent une communication plus efficace, plus facile, et à moindre coût entre les membres éloignés de l'organisation et entre l'organisation et ses différents partenaires. Elles fournissent des informations et des réseaux sociaux ne connaissant aucune frontière.

Deuxièmement, elles permettent de traiter les données internes et externes en temps réel, et d'exposer les informations produites sur des supports convenables.

Troisièmement, elles permettent de développer de nouvelles structures plus souples, plus interactives et plus éclatées. Enfin, ces technologies fournissent un soutient considérable à la décision par le biais des différentes formes d'intelligences artificielles. [8]

2.1.3 Apport d'un système de messagerie a une PME/PMI

Le système de messagerie est aujourd'hui le moyen de communication le plus populaire sur Internet. C'est également l'un des moins chers à mettre en œuvre, parce que simple, rapide et fiable. En raison de sa popularité, le courrier électronique permet de communiquer avec un vaste auditoire. Il tend à prendre une place de plus en plus prépondérante par rapport aux moyens de communication traditionnels. Bien qu'il puisse incorporer des graphiques, des fichiers sonores et visuels, il sert principalement à l'envoi de textes avec ou sans documents annexés. Grâce au courrier électronique, les PME/PMI peuvent communiquer avec leurs clients et fournisseurs dans le but d'échanger des renseignements commerciaux, relatifs à leurs activités quotidiennes, y compris des renseignements sur les ventes, la prise de rendez-vous, le soutien à la clientèle, la diffusion de documents, la prise de commandes, l'envoi des factures et la

vérification des comptes en souffrance. La messagerie électronique permet de réduire le nombre d'appels internes et externes, de rencontres entre direction et personnel. Il est aussi un excellent moyen de coordination d'une équipe ou d'un service. On peut citer d'autres cas que l'utilisation de la messagerie favorise :

— Un texte expédié par un système de messagerie électronique sera non seulement lu par son destinataire mais il pourra également être stocké dans un fichier.
— La grande majorité des systèmes actuels permettent d'envoyer des fichiers attachés à vos messages. Ces fichiers peuvent être, par exemple, des données spécifiques à une application de votre client ou fournisseur. C'est aussi souvent des fichiers de l'un des tableurs ou système de traitement de textes présents sur le marché.
— La transmission est immédiate, et votre interlocuteur pourra avoir accès à son courrier en déplacement ou depuis son domicile.
— Des filtres sélectifs peuvent être programmés pour trier les messages adressés à un destinataire.

2.1.4 Enjeux et objectifs de sécurité sur un tel système

La messagerie électronique est devenue le système critique d'une entreprise puisque c'est le cœur de toutes communications externe vis-à-vis du marché et interne qui permet d'établir un climat social bénéfique et favorable aux bons résultats. Le fonctionnement de ce service impactera directement sur l'activité de l'entreprise. Pour cela il faut avoir un système fiable qui na pas besoin d'une réinitialisation suite a une attaque et aussi les ressource doivent être disponible a tout moment, d'ou la raison pour une PME/PMI d'investir en sécurité de sa messagerie. la question qui nous vient a l'esprit pourquoi disposer administrer et sécuriser son propre serveur de courrier électronique ?

2.2 Problématique

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

— La distance, ainsi en cas de panne de connexion internet toute la correspondance devient indisponible.
— Le risque de perte de confidentialité des messages échangées..
— L'utilisation d'un simple logiciel navigateur web, permet d'accéder à son webmail depuis tout ordinateur connecté à internet, ce qui augmente le risque d'utiliser un ordinateur mal sécurisé et infecté d'un logiciel espion qui relève le mot de passe utilisé.

— l'exposition du réseau interne au réseau internet peut engendrer une surcharge de courrier électronique dus aux spams reçus, par conséquent une perte de données importante. Comment donc assurer la disponibilité continue d'un serveur de messagerie électronique fiable et sécurisé au sein du réseau interne de l'entreprise ?

2.3 Suggestions :

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

— Mise en place d'un serveur de messagerie interne (Postfix, Dovecot) avec l'interface webmail Roundcube, qui sera propre à l'entreprise.
— Faciliter l'administration du serveur de messagerie.
— Sécuriser le serveur à l'aide du protocole TLS.

2.4 Les systèmes de messageries électroniques et leurs sécurités

2.4.1 Introduction

Nous avons vu dans la partie précédent, la nécessité de mettre en place un serveur de messagerie dans une PME/PMI .Dans ce qui suit, nous allons voir plus en détail les protocoles utilisés dans les serveurs de messagerie ainsi leur architecture et quelques protocoles de sécurité de courrier électronique.

2.4.2 Courrier électronique :

La messagerie électronique est une application très importante et plus utiles dans les réseaux qui permet la transmission de messages et de documents, à partir d'un ordinateur. Elle fonctionne grâce à un serveur de messagerie. Pour émettre et recevoir des messages par courrier électronique, il faut disposer d'une adresse électronique et d'un client de messagerie ou d'un webmail permettant l'accès aux messages via un navigateur web [9].

2.4.2.1 Serveur de messagerie

Un serveur de messagerie est un ordinateur-serveur qui offre des espaces disques pour le stockage des comptes de messagerie personnels et assure la transmission et la réception des messages a travers le réseau, cela permettra à n'importe qui d'aller

cherchez son courrier sur le serveur, depuis n'importe quelle station de travail grâce a un logiciels de messagerie ou un webmail, qui se charge de contacter le serveur. [10]

2.4.2.2 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'identifier 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.

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

2.4.3 Structure d'un courrier électronique.

La structure explicite d'un courrier électronique, celle que chaque personne peut observer dans son logiciel de messagerie électronique, se présente selon deux parties distinctes : une enveloppe l'entête et le corps :

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.

L'entête du courrier Une partie de l'entête du courrier électronique est générée de manière automatique par le logiciel de messagerie MUA (Mail User Agent, client de messagerie électronique), d'autres sont ajoutées directement par le serveur de messagerie ou les relais de messagerie intermédiaire (pour le champ Received notamment). Les champs d'entête sont donc composés de plusieurs paramètres d'entête, certains essentiels pour le courrier électronique :

- From : adresse électronique de l'expéditeur
- To : adresse électronique du destinataire
- Date : c'est la date d'envoi du courrier. Dans le cas où vous n'indiquez aucune date, le serveur de messagerie se chargera de l'ajouter
- Received il s'agit des informations sur tous les serveurs de messagerie traversés par le mail, serveur expéditeur, serveurs intermédiaires et serveur destinataire.

Ce champ comprend les noms, adresses IP et date du courrier électronique traité par tous les serveurs

— CC[1] : cela permet d'envoyer un mail à de nombreuses personnes en écrivant leurs adresses respectives séparées par des virgules
— Reply-To : Une adresse pour la réponse
— Subject : Le sujet du message
— Message-ID : référence qui permet d'identifier de manière unique votre message.

Message : est le contenu du message proprement dit, séparé de l'en-tête par une ligne vide [11].

2.4.4 L'architecture de la messagerie électronique et son fonctionnement

La messagerie réalise l'acheminement des courriers électroniques comme le fait un réseau à commutation de paquets, on présentera les différents agents qui interviennent dans le courrier électronique et par la suite une image qui illustre le fonctionnement de la messagerie.

— Mail Transfert Agent (MTA) : Ce logiciel est situé sur chaque serveur de messagerie, son premier rôle est de transmettre les messages à une autre machine du réseau et son second rôle est d'accepter les messages à destination de ses utilisateurs. Exemple de MTA : Sendmail, Postfix et Exchange [12].
— Mail User Agent (MUA) : C'est le client de messagerie, 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) [12].
— Mail Delivery Agent (MDA) : Un Mail Delivery Agent marque la fin de l'acheminement du mail vers la destination. C'est le MDA qui reçoit le message du MTA et se charge de le placer dans la boite aux lettres de l'utilisateur, il doit donc gérer les éventuels problèmes tel qu'un disque plein ou une boite aux lettres corrompue et doit impérativement signaler au MTA toute erreur de délivrance. Un MDA assure également des fonctions utilisateurs telles que la réponse automatique quand la personne est indisponible. Comme exemple, nous avons Dovecot, maildrop-Courrier [12].

1. carbon copies

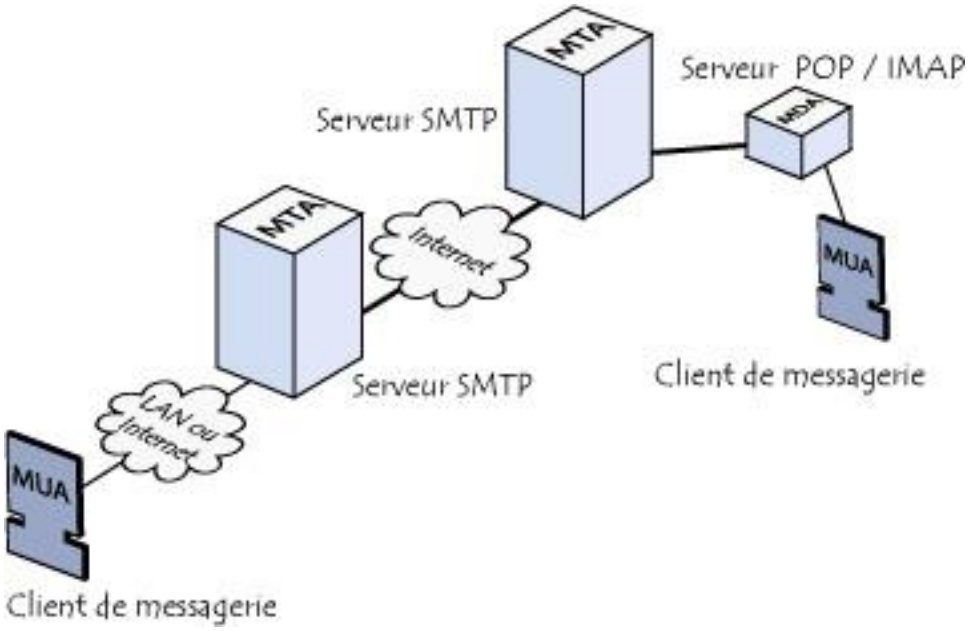

Figure 2.1 – le fonctionnement de la messagerie électronique.

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

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

2.4.5 Les serveurs et les clients de la messagerie électronique

Une messagerie électronique a besoin essentiellement d'un serveur de messagerie pour livrer un courrier et pour la récupération ainsi qu'un client de messagerie pour consulter rédiger et supprimer un courrier, nous distinguons plusieurs serveurs et clients de la messagerie :

2.4.5.1 Les serveurs de messagerie

Un serveur de messagerie électronique est un logiciel serveur de courrier électronique, il a pour vocation de transférer les messages électroniques d'un serveur a un autre. La plupart des serveurs de messagerie possèdent ces deux fonctions (envoi/réception), mais elles sont indépendantes et peuvent être dissociées physiquement en utilisant plusieurs serveurs. Nous citons quelques serveurs de messagerie :

1. Sendmail : est un serveur de messagerie dont le code source est ouvert. Il se charge de la livraison des messages électroniques, il est très puissant et résiste beaucoup à la grande charge, code source libre, multi plate-forme de type UNIX (MAC OS, GNU/LINUX). En revanche Sendmail et difficile à configurer car son architecture est vieille, lent et très complexe avec une maintenance difficile.
2. Zimbra : Zimbra est un logiciel serveur collaboratif qui permet à ses utilisateurs de stocker, organiser et partager leurs documents, contacts, courriels, accessible de partout : du bureau, de chez soi et toutes les fonctions disponibles au sein de la même interface : emails, agendas, carnets d'adresses, fichiers, tâches, messagerie instantanée, par contre pas de mode "hors ligne" [13].
3. Qmail : Qmail est un serveur de messagerie électronique pour LINUX. Il permet de mettre en place un service SMTP (Simple Mail Transfert Protocol) permettant l'envoi de courriels. Qmail a la même utilité que Sendmail ou encore Postfix mais il possède une architecture modulaire, comportant un ensemble de commandes [14].
4. 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'accès en mobilité et assure une bonne sécurité d'anti-spam, parmi ces inconvénients : un code source n'est pas libre et uni plate-forme (Microsoft Windows).
5. Postfix : Postfix est un serveur de messagerie et un logiciel libre, il se charge de la livraison de courriers électroniques et a été conçu comme une alternative plus rapide, plus facile à administrer et plus sécurisée que l'historique Sendmail [15].
6. Dovecot : Dovecot est un serveur pop3 et imap pour les récupérations des courriers électroniques 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 [16].
7. Cyrus : Cyrus est un serveur de messagerie électronique (MDA) créé dans un

objectif de fiabilité et d'extensibilité optimale, utilisé essentiellement pour gérer de très grandes quantités de comptes de courrier électronique. Cyrus permet de consulter ses emails par POP3 et IMAP [17].

2.4.5.2 Les clients de messagerie

Des logiciels permettant de rédiger, consulter et envoyer des courriers électroniques, la notion de client s'entend dans une architecture client-serveur. Il existe deux types de client de messagerie qui nous permettent d'accéder à la messagerie électronique :

Les clients lourds : Un client de messagerie de type lourd désigne une application cliente graphique exécutée sur le système d'exploitation de l'utilisateur. Un client lourd possède généralement des capacités de traitement évoluées et peut posséder une interface graphique sophistiquée. Néanmoins, ceci demande un effort de développement et tend à mêler la logique de présentation (l'interface graphique) avec la logique applicative (les traitements). La mise en place d'un système de type client lourd nécessitera une installation de l'application sur chaque poste. Il faudra donc prévoir des ressources à l'arrivée de chaque nouveau collaborateur pour l'installation du logiciel sur le nouveau poste de travail. Les applications du type client lourd sont généralement plus sécurisées si elles ne concernent que quelques utilisateurs. Il faut cependant que tous les postes qui utilisent l'application soient sécurisés car une partie des données est stockée sur les postes des différents collaborateurs. Cela peut donc multiplier les risques. Parmi ces clients lourds on peut citer :

Thunderbird : C'est un client de messagerie et de messagerie instantanée, libre, distribué gratuitement par la fondation Mozilla. Il fonctionne sur diverses plates-formes. Il est également extensible, c'est-à-dire qu'il peut facilement recevoir de nouvelles fonctionnalités par l'ajout d'extensions [18].

Outlook : est un programme de Microsoft corporation et fait partie de la suite Microsoft office. Le logiciel agit comme un client de messagerie. Plus précisément il comprend un calendrier, un calendrier des activités, notes, journal, contacts.

Les clients légers ou webmail : Un client de messagerie de type léger est un logiciel qui est installé sur un poste client. Les utilisateurs de l'application auront accès aux données par un portail sécurisé depuis leur navigateur (Internet Explorer, Firefox...). Pour les systèmes en client léger, l'installation est beaucoup plus simple. On a tendance à penser que les applications Web sont moins sécurisées, pourtant elles permettent de réduire les risques à un seul serveur. Bien entendu, la sécurisation de

celui-ci est primordiale, surtout lors d'un partage de l'application sur Internet. On peut distinguer quelques types de clients légers :

— RoundCube : est un client web mail pour le protocole IMAP écrit en PHP et JavaScript. Cette application libre est publiée sous licence GPL. Il peut être installé sur plateforme LAMP. Il est compatible avec les serveurs web Apache, Nginx, Lighttpd ou encore Cherokee, et les bases de données MySql, PostgreSQL et SQLite sont supportées. La gestion des thèmes se base sur les standards du web [19].

— Squirrelmail : Squirrelmail est une application qui permet de consulter son courrier électronique, stocké sur un serveur, grâce à un simple navigateur, développé par Luke et Nathan Ehresman, écrit en php4. Il supporte les protocoles IMAP et SMTP, et toutes les pages créées le sont en pur HTML (sans aucun JavaScript), ceci afin d'être compatible avec le maximum de navigateurs. Son objectif est de fournir une compatibilité optimale pour se rendre aussi accessible que possible web mail de Zimbra, etc [20].

2.4.6 Les protocoles de courrier électronique

Afin de rendre le processus de l'envoi et de la récupération des courriers électronique possible, un ensemble de protocoles permettent aux 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.

2.4.6.1 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 Transfer Protocol (ou SMTP).

— SMTP Son objectif primaire 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 configuration d'un client de messagerie. Il utilise le protocole de contrôle de transmissions TCP pour le transfert des données et par défaut le port 25 [21].

2.4.6.2 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 (IMAP). 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 nous allons présenter dans ce qui suit les deux protocole ainsi une comparaison entre les deux.

POP Le protocole POP est aujourd'hui disponible dans sa version 3, POP3. Il s'agit du protocole standard qui permet la récupération des mails situés sur un serveur distant (serveur POP port 110) les courriels sont supprimés du serveur et sont téléchargés sur votre ordinateur, Il est nécessaire pour les personnes n'étant pas connectées en permanence à Internet afin de pouvoir consulter les mails reçus hors connexion [21].

IMAP Le protocole IMAP permet de récupérer des messages tel que le protocole POP, il a l'avantage de synchroniser la messagerie avec le serveur sur lequel sont stockés les messages, donc les utilisateurs accèdent à leur courrier électronique au moyen d'ordinateurs multiples [21].

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

2.5 Sécurité de la messagerie

La messagerie électronique est un outil de communication très sollicitée en entreprise. Elle peut véhiculer des données sensibles et importantes, son niveau de protection est peu élevé, parfois négligé. Les menaces qui planent en dessous de la messagerie électronique sont très nombreuses. Le renforcement de la protection de cet outil est donc plus que nécessaire.

2.5.1 Les menaces de serveurs de messagerie

La messagerie électronique est un outil extrêmement puissant dont les bénéfices sont importants, mais une mauvaise utilisation et son infection par différents types de menaces peut provoquer des effets dévastateurs sur différents plans. Nous citons quelques risques menaçant la sécurité d'un serveur de messagerie :

— 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 effectué au niveau du serveur de messagerie

2.5.2 Les protocoles de sécurité des serveurs de messagerie.

La sécurité des serveurs de messagerie doit être une priorité car ils centralisent un grand nombre de données, il existe plusieurs protocoles de sécurité, nous nous concentrerons sur les plus utilisés .

2.5.2.1 Le Protocol SSH

Le protocole SSH[2] 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 [22].

2. Secure Shell

2.5.2.2 Le protocole TLS

TLS [3] Un usage courant de la cryptographie par clé publique est le chiffrement du trafic réseau d'une application en utilisant TLS . TLS est un protocole de cryptage qui garantit pleinement la sécurité des communications pour tous les mails échangés. Ce système est utilisé pour garantir la sécurité des communications sur un réseau internet ou intranet. Il est positionné entre les couches application et transport du modèle TCP/IP et dans la couche session du modèle OSI. TLS se comporte en effet comme une couche intermédiaire supplémentaire car il est indépendant du protocole utilisé au niveau application donc TLS est transparent pour l'utilisateur [23].

Fonctionnement de TLS Le protocole est composé de deux niveaux TLS Handshake Protocol et TLS Record Protocol [23].

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

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

2.5.2.3 Un certificat numérique :

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

2.5.3 Anti-virus et anti-spam des serveurs de messagerie

Ce service anti-virus et anti-spam est une passerelle de filtrage des emails et qui protège le serveur de messagerie de toute intrusion, virus, logiciel malveillant, spam qui inondent les boites aux lettres et qui peuvent réduire la productivité ou diffuser du contenu inapproprié sur un espace de travail. Nous citons quelques anti-virus et anti-spam :

3. Transport Layer Security

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 différentes 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 [24].

Amavis Amavis est un open source filtre le contenu pour le courrier électronique, la mise en œuvre 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 [25].

2.6 Conclusion

Nous avons parlé et détaillé l'aspect théorique de notre projet, nous avons aussi déterminé le fonctionnement de serveur de messagerie et ses différents protocole ainsi quelque protocoles de sécurité. Cette partie est de très grande utilité et importance pour le chapitre de réalisation que nous allons effectuer par la suite.

Chapitre 3

Réalisation

3.1 Introduction :

Ce chapitre sera consacré pour la mise en œuvre de toutes les notions vu dans les chapitres précédents dont on a parlé de notre projet d'une façon théorique. Nous la considérons 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 électronique sécurisé.

3.2 Installation et configuration du système d'exploitation :

Tout d'abord, en ce qui concerne notre système d'exploitation nous avons choisi Linux, il existe plusieurs distributions linux basées sur Debian ou Ubuntu. En effet, l'installation de programmes fonctionne différemment d'une distribution à une autre, c'est justement l'une des différences majeures qui existent entre elles. Dans notre cas, nous avons choisi d'installer la distribution Ubuntu version 17.10 de Linux. Une fois l'épuisement de l'installation qui est assez rapide, nous passons en mode : root sur le terminal afin d'obtenir tous les droits de super utilisateur pour pouvoir mettre à jour, modifier et configurer le système.

3.3 Création du réseau local du serveur de messagerie :

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

Figure 3.1 – création d'un réseau local

3.3.1 Installation et configuration du serveur DNS :

Maintenant que l'adresse du serveur a été définie nous allons passer à l'installation de serveur DNS grâce a la commande apt-get install bind9 puis a sa configuration.

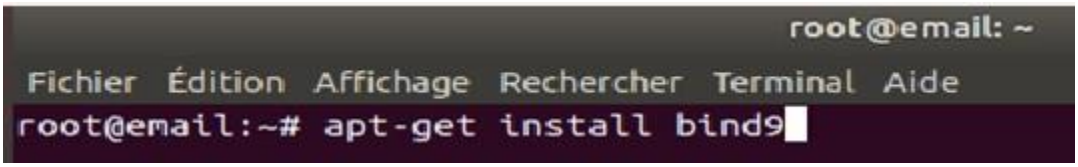

Figure 3.2 – Installation d'un serveur DNS

Nous passons maintenant à la configuration de serveur DNS nous allons éditer le fichier named.conf.default-zones pour définir notre zone directe mail.dz et inverse 1.168.192.in-addr.arpa .

```
 GNU nano 2.8.6          Fichier : named.conf.default-zones

        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};

zone "mail.dz" {
        type master;
        file "/etc/bind/mail.zone";
};


zone "1.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/mail.invzone";
};
```

Figure 3.3 – Définition des deux zone mail.com et 1.168.192.in-addr.arpa

Une fois le fichier named.conf.default-zones modifié, nous avons besoin de créer deux fichiers mail.zone et mail.invzone et les configurer comme illustré dans les deux figures qui suivent.

```
 GNU nano 2.8.6                  Fichier : mail.zone

;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns.mail.dz. root.mail.dz. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;

@               IN      NS      ns.mail.dz.
@               IN      MX 10   email.mail.dz.
ns.mail.dz.     IN      A       192.168.1.5
email.mail.dz.  IN      A       192.168.1.5
www.mail.dz.    IN      CNAME   ns.mail.dz.
```

Figure 3.4 – Configuration de fichier mail.zone

Concernant le code, qui se trouve dans le fichier mail.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.

```
 GNU nano 2.8.6                Fichier : mail.invzone

;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns.mail.dz. root.mail.dz. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS          ns.mail.dz.
@       IN      MX 10       email.mail.dz.
5       IN      PTR         ns.mail.dz.
5       IN      PTR         email.mail.dz.
```

Figure 3.5 – Configuration de fichier mail.invzone

le fichier mail.invzone suit la même modification que le fichier mail.zone avec quelques changements dans La partie deux qui indique la résolution inverse, en introduisant le dernier chiffre de notre adresse IP.

Maintenant nous allons éditer le fichier /etc/resolv.conf pour introduire l'adresse de notre serveur DNS.

```
 GNU nano 2.8.6              Fichier : /etc/resolv.conf

# This file is managed by man:systemd-resolved(8). Do not edit.
#
# 127.0.0.53 is the systemd-resolved stub resolver.
# run "systemd-resolve --status" to see details about the actual nameservers.
nameserver 192.168.1.5
```

Figure 3.6 – Indication de l'adresse du serveur DNS

Pour tester le bon fonctionnement de notre serveur DNS, nous tapons la commande 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 comme illustré dans la figure ci-dessous.

```
root@email:~# nslookup
> 192.168.1.5
Server:         192.168.1.5
Address:        192.168.1.5#53

5.1.168.192.in-addr.arpa        name = email.mail.dz.
5.1.168.192.in-addr.arpa        name = ns.mail.dz.
> email.mail.dz
Server:         192.168.1.5
Address:        192.168.1.5#53

Name:   email.mail.dz
Address: 192.168.1.5
> www.mail.dz
Server:         192.168.1.5
Address:        192.168.1.5#53

www.mail.dz     canonical name = ns.mail.dz.
Name:   ns.mail.dz
Address: 192.168.1.5
> ns.mail.dz
Server:         192.168.1.5
Address:        192.168.1.5#53
```

Figure 3.7 – Test de fonctionnement de serveur DNS

3.3.2 Installation et configuration d'un serveur DHCP :

Nous procédons à l'installation du serveur DHCP qui permet de configurer automatiquement les paramètres IP des machines qui se connectent au réseau créé auparavant en tapant la commande apt-get install isc-dhcp-server ,puis nous passons à la configuration de ce dernier en éditant /etc/dhcp/dhcpd.conf , afin de préciser la plage d'attribution d'adresses ainsi que l'adresse IP et le nom de domaine de notre serveur mail.

```
  GNU nano 2.8.6                Fichier : dhcpd.conf
#}
subnet 192.168.1.0 netmask 255.255.255.0 {

    option domain-name "mail.dz";

    option domain-name-servers ns.mail.dz;

    range  192.168.1.5 192.168.1.200;
}
```

Figure 3.8 – Configuration du fichier dhcpd.conf

3.3.3 Installation de serveur apache et de language php

Cette étape représente l'installation d'un serveur apache, en tapant la commande apt-get install apache2 . Une fois installé, nous vérifions en tapant l'adresse IP du serveur sur le navigateur web et cette page s'affiche :

Figure 3.9 – Vérification de l'installation d'Apache2

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

Figure 3.10 – Vérification de l'installation de php7

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

Dans cette étape, nous nous intéresserons à l'installation de mysql-server qui est un serveur de bases de données, en tapant la commande apt-get install mysql-server . Une fois mysql-serveur est installé, nous passons à l'installation d'une interface web Phpmyadmin qui gère les bases de données, en tapant la commande apt-get install phpmyadmin

Figure 3.11 – Interface de Phpmyadmin

3.3.5 Génération d'un certificat :

Nous procédons à la sécurisation de l'échange du courrier entre le serveur et des utilisateurs, pour cela nous générerons un certificat numérique pour TLS. Génération de la clé privée et de la clé non sécurisée en introduisant notre mot de passe tel qu'il est montré dans cette figure :

Figure 3.12 – Génération de la clé privée et la clé non sécurisée Génération

d'une demande de signature de certificat en introduisant le mot de passe
et il nous sera demandé d'introduire quelque informations :

Figure 3.13 – Génération d'une demande de signature de certificat

Génération d'un certificat auto-signé en introduisant le mot de passe et l'installation le fichier de clé server.key et le fichier de certificat server.crt :

```
root@email:~# openssl x509 -req -days 365 -in server.csr -signkey server.key -
out server.crt
Signature ok
subject=/C=TO/ST=DZ/L=TO/O=DZ/OU=DZ/CN=email.mail.dz/emailAddress=katia02@mail
.dz
Getting Private key
root@email:~# sudo cp server.crt /etc/ssl/certs
root@email:~# sudo cp server.key /etc/ssl/private
```

Figure 3.14 – Génération d'un certificat auto-signé

3.3.6 Installation et configuration de Postfix et de l'interface web Postfixadmin :

Comme nous l'avons expliqué dans le chapitre précédent, le MTA constitue l'un des plus important composant à mettre en place dans un serveur de messagerie car il permet l'envoi du courrier électronique. Avant d'entamer l'installation, on met à jour le système comme suit apt-get update et puis nous installons notre MTA qui est Postfix avec une extension mysql par la commande apt-get install postfix postfix-mysql . Une fois le paquet installé, un menu de configuration s'affiche Parmi les choix proposés nous sélectionnons site internet pour utiliser le protocole SMTP et il nous demande d'introduire le nom de courrier.

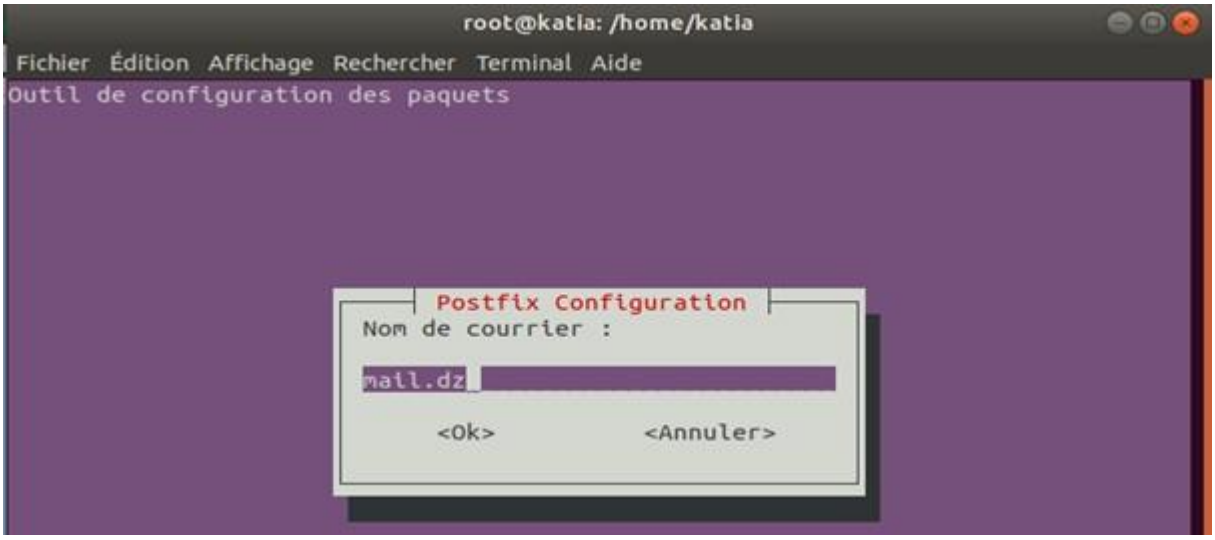

Figure 3.15 – Configuration du nom de courrier Postfix

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'installation de Postfixadmin une base de données est créée " postfixadmin " ainsi que les tables nécessaires pour le serveur Postfix tel qu'il est montré dans la figure :

Figure 3.16 – La base de donnée postfixadmin et ses tables

On passe à la création de l'administrateur qui s'occupera de l'ajout des domaines, des utilisateurs et des alias, pour cela nous devrions d'abord créer un mot de passe pour la configuration et générer son hash :

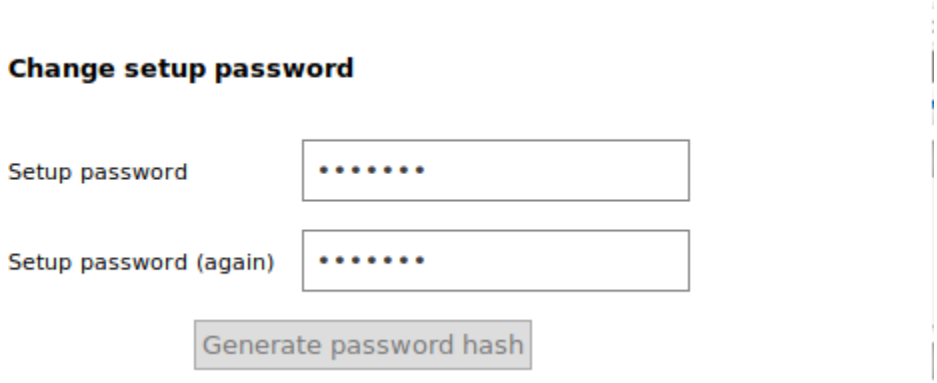

Figure 3.17 – Créer le mot de passe et générer son hash

Nous ajoutons la valeur de hachage de mot de passe généré dans le fichier /etc/postfixadmin/config.i pour pouvoir créer l'administrateur en utilisant le mot de passe de configuration :

Figure 3.18 – Insertion de la valeur de hachage de mot de passe generé

Nous allons se connecter a Postfixadmin avec le compte de l'administrateur déjà créé :

Figure 3.19 – Page de connexion

Nous allons créer notre domaine en accédant a Liste des domaines -> Nouveau domaine en introduisant les informations de notre domaine, on peut limiter le nombre de boite au lettre et les alias

Figure 3.20 – Ajouter le domaine mail.dz

Nous allons maintenant créer nos utilisateurs en accédant à Liste virtuelle -> Ajouter une boîte aux lettres :

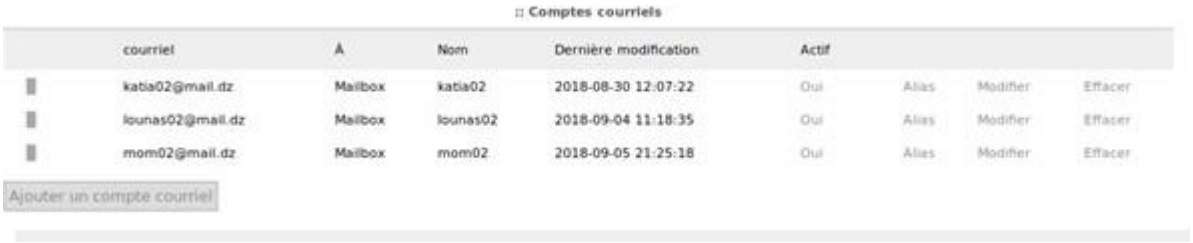

Figure 3.21 – liste des utilisateurs

Avant d'entamer la configuration des fichiers de postfix, nous allons créer un compte spécifique dans lequel on configure postfix pour déposer les mails et aussi dovecot pour récupérer les mails en IMAP et POP3. Les étapes de la création de répertoire est illustré dans la figure ci-dessous :

```
root@katia:/home/katia# groupadd -g 5000 vmail && mkdir -p /var/mail/vmail
root@katia:/home/katia# useradd -u 5000 vmail -g vmail -s /usr/sbin/nologin -d /
var/mail/vmail
root@katia:/home/katia# chown -R vmail:vmail /var/mail/vmail
root@katia:/home/katia#
```

Figure 3.22 – Création de répertoire des courriers électroniques

Cette étape consiste à configurer les deux fichiers principaux main.cf et master.cf qui se trouvent dans le répertoire /etc/postfix/ . Maintenant, nous nous intéresserons à la configuration de fichier main.cf tel qu'il est illustré dans les deux figures qui suivent :

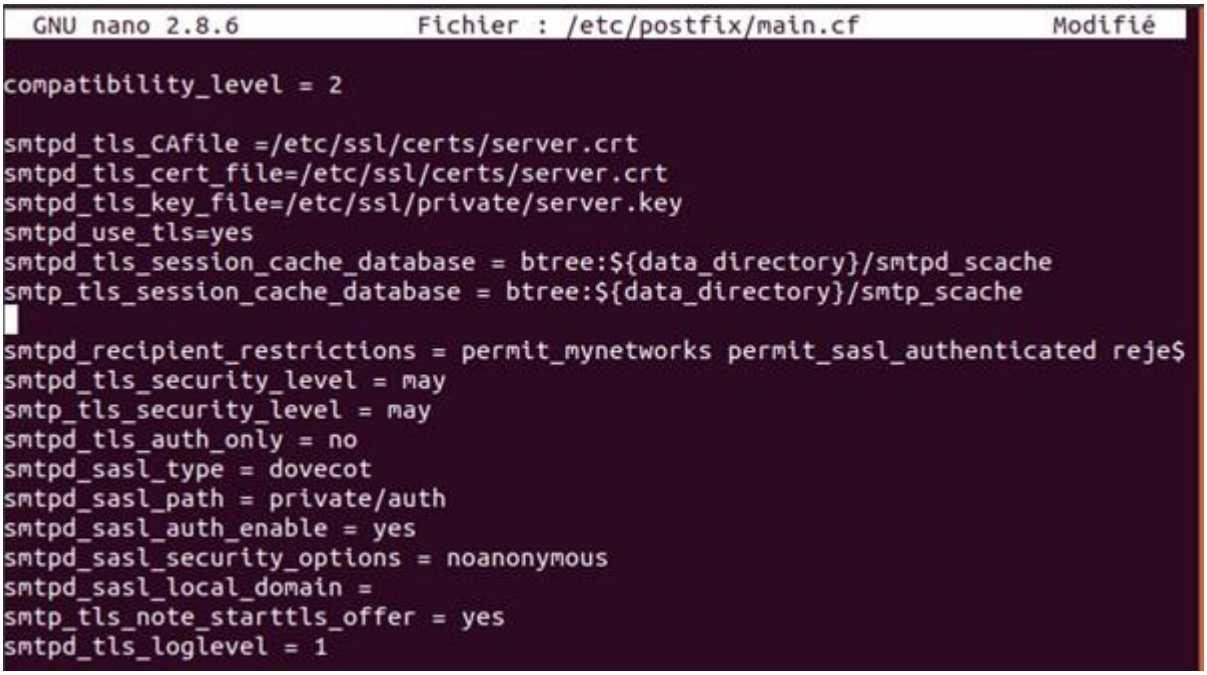

Figure 3.23 – Configuration de fichier main.cf

Dans cette premiére partie nous avons établi une connexion SSL, spécifié le certificat SSL utilisé pour sécuriser la connexion, activer SASL pour forcer l'authentification pour l'envoi d'e-mails et l'authentification de dovecot

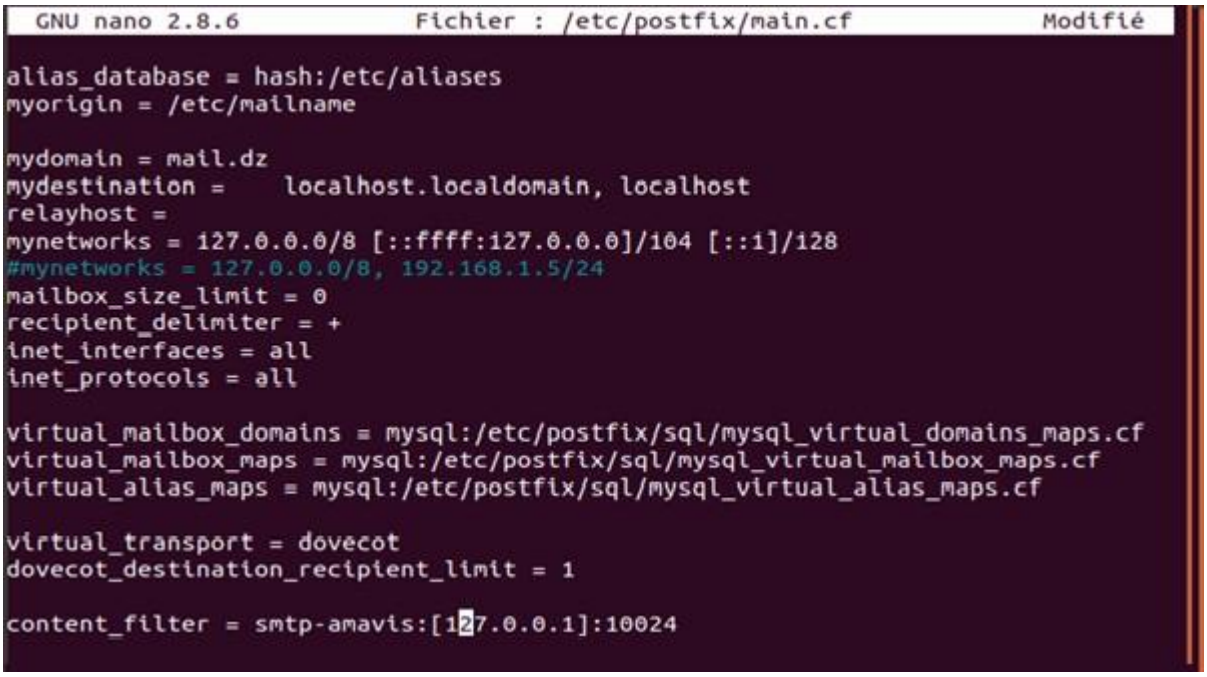

Figure 3.24 – Configuration de fichier main.cf

Dans cette seconde partie nous avons spécifié le nom de domaine et l'anti-spam utilisé ainsi les fichiers de configuration de la base de données qui seront configurés par

la suite. Postfix à besoin de 03 fichiers de base de données lui permettant d'accéder a la base de données qui a été créée automatiquement lors de l'installation de postfix, Le fichier mysql_virtual_domains_maps.cf contenant la liste des noms de domaine hébergés sur le serveur. Cela permettra à postfix de déterminer si notre serveur est en charge d'un domaine (mail.dz) lorsqu'il reçoit un email. Si c'est le cas, cela signifie que le domaine est dans notre base de données :

```
  GNU nano 2.8.6        Fichier : mysql_virtual_domains_maps.cf

user = postfixadmin
password = katia
hosts = 127.0.0.1
dbname = postfixadmin
query = SELECT domain FROM domain WHERE domain='%s' AND active = '1'
```

Figure 3.25 – Le fichier mysql_virtual_domains_maps.cf de postfix

Le fichier mysql_virtual_mailbox_maps.cf pour stocker toutes les adresses électroniques. Il sera utilisé pour vérifier également si les boîtes aux lettres existent :

```
  GNU nano 2.8.6        Fichier : mysql_virtual_mailbox_maps.cf

user = postfixadmin
password = katia
hosts = 127.0.0.1
dbname = postfixadmin
query = SELECT maildir FROM mailbox WHERE username='%s' AND active = '1'
```

Figure 3.26 – Le fichier mysql virtual alias maps.cf

Nous passons à la configuration de fichier master.cf de postfix pour déterminer les services à ouvrir de postfix. On ouvre le port SMTP sécurisé vu que nous avons établi une connexion SSL dans le fichier main.cf de postfix tel qu'il est montré dans cette figure :

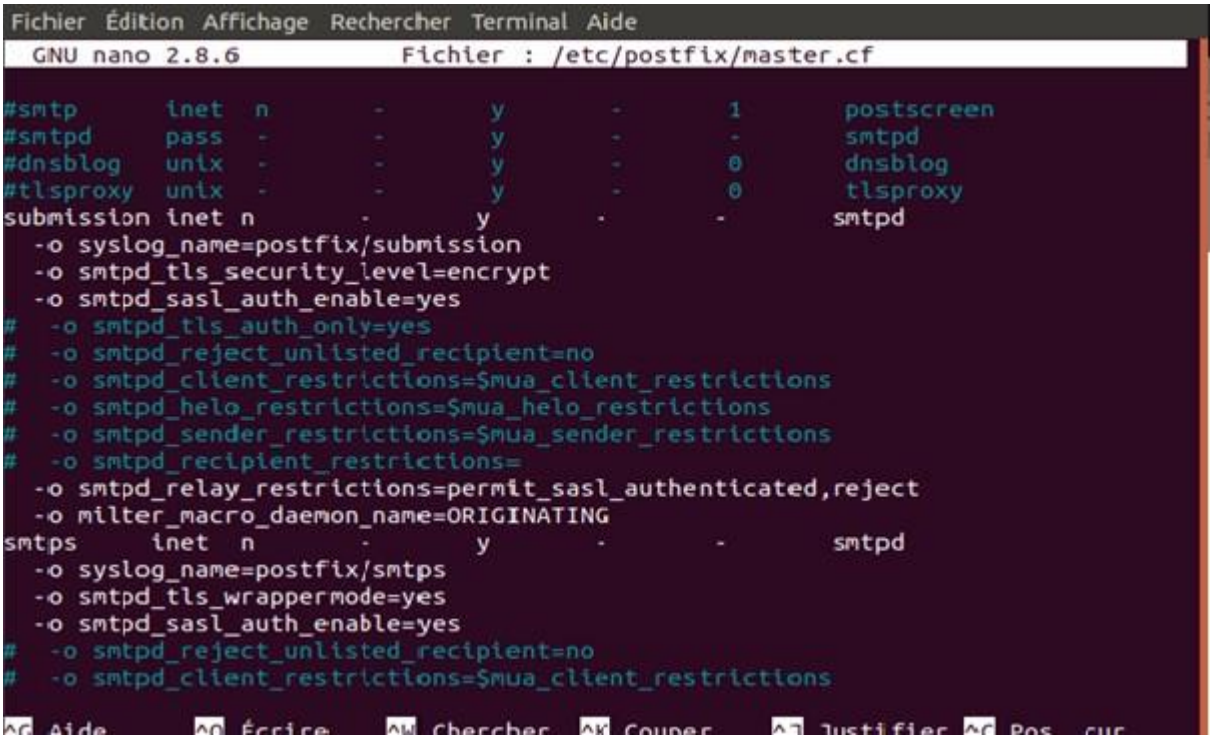

Figure 3.27 – Configuration de fichier master.cf de postfix

Ensuite on indique a postfix dovecot pour travailler ensemble et ouvrir le service de amavis :

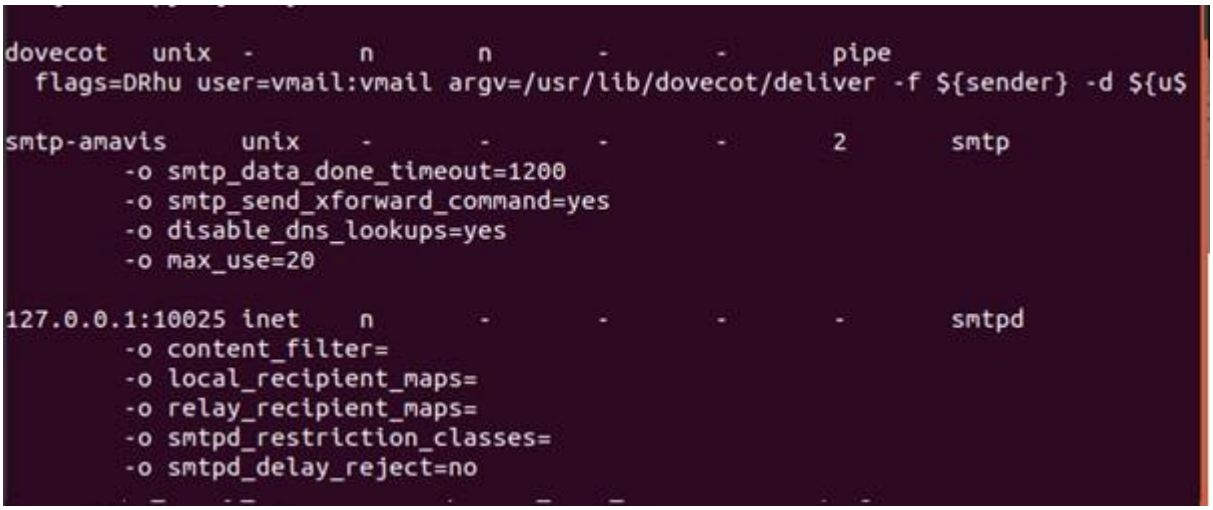

Figure 3.28 – Configuration de fichier master.cf de postfix

3.3.7 Installation et configuration de Dovecot imap et Dovecot pop3

Cette étape, consiste à installer et configurer Dovecot POP Dovecot IMAP et Dovecot manageived, pour le faire on tape dans le terminal la commande suivante : apt-get

install dovecot-imapd dovecot-pop3d dovecot-mysql dovecot-manageived une fois l'installation terminée on passe a la configuration des fichiers de Dovecot. La configuration de Dovecot est contenue dans de multiples fichiers dans /etc/dovecot/conf.d pour cela on doit vérifier que le dossier conf.d est bien inclus dans etc/dovecot/dovecot.conf :

Figure 3.29 – Configuration de ficher dovecot.d de Dovecot

Maintenant, nous allons dans le dossier contenant les fichiers de configuration en tapant la commande cd /etc/dovecot/conf.d et éditons : Le fichier 10-auth.conf pour modifier les mécanismes de connexion pour l'authentification auprès de Dovecot et inclure le fichier auth-sql.conf.ext pour la configuration de sql :

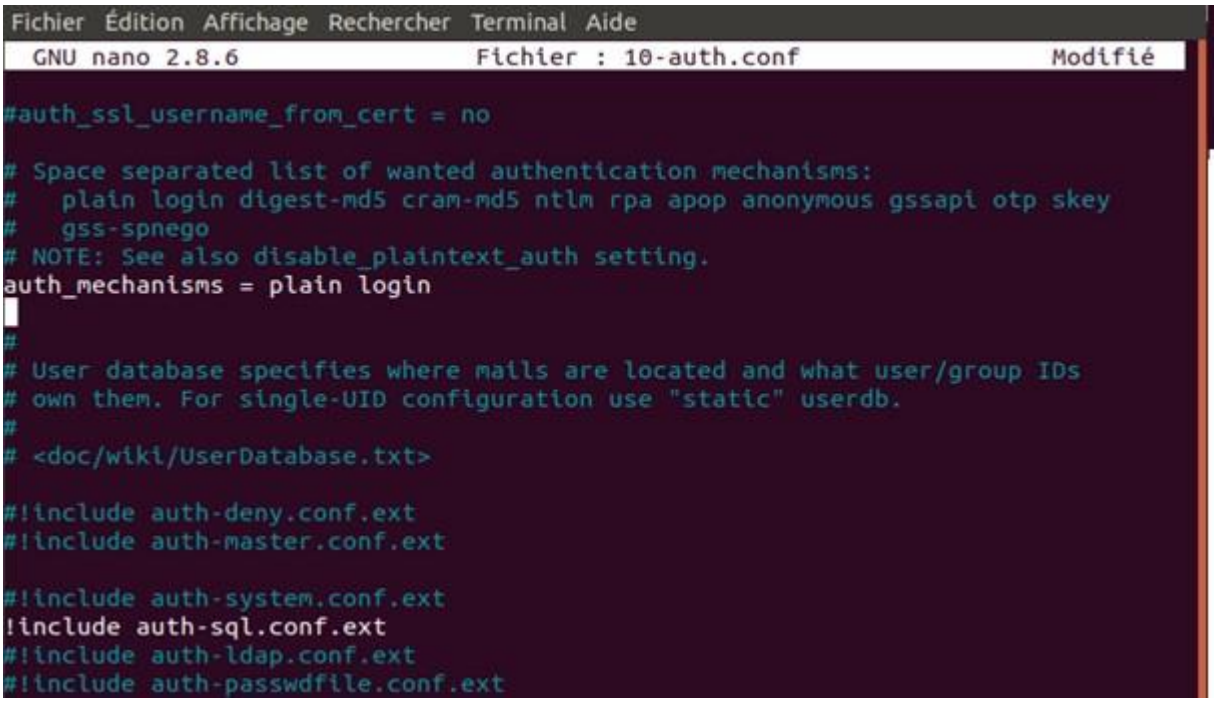

Figure 3.30 – Configuration de fichier 10-auth.conf de Dovecot

Le fichier auth-sql.conf.ext pour spécifier le chemin du fichier de configuration SQL et le répertoire pour la récupération des courriers électroniques et les variables " %d et %n" sont des variables préfini de Dovecot qui désignent respectivement (domaine, utilisateur) :

Figure 3.31 – Configuration de fichier auth-sql.conf.ext de Dovecot

Le fichier /etc/dovecot/dovecot-sql.conf.ext pour indiquer à Dovecot comment se connecter a la base de données SQL :

Figure 3.32 – Configuration de fichier dovecot-sql.conf.ext de Dovecot

Le fichier 10-mail.conf pour configurer le répertoire de l'emplacement des courriers électroniques :

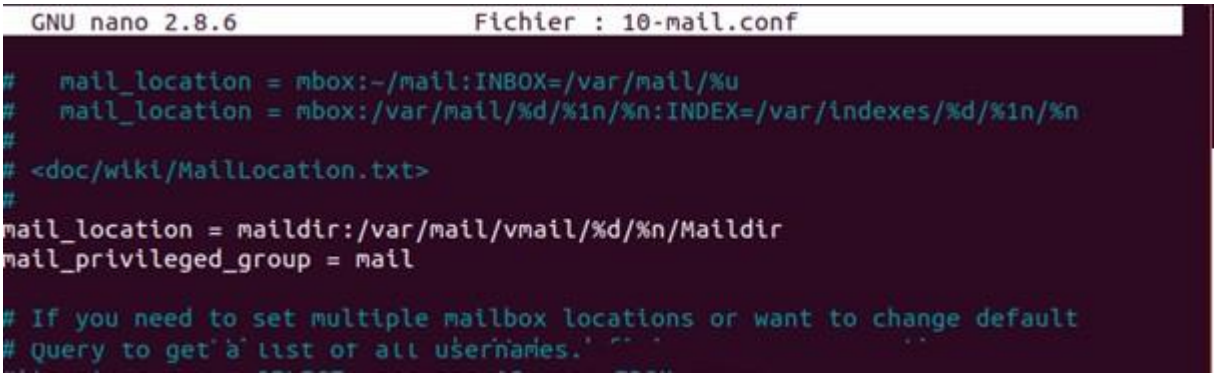

Figure 3.33 – Configuration de fichier 10-mail.conf de Dovecot

Et enfin nous configurons le fichier LDA 15-lda.conf pour indiquer le filtre afin d'organiser automatiquement le courrier dans le dossier correspondant :

Figure 3.34 – Configuration de fichier 10-lda.conf de Dovecot

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

Dans cette section, nous nous intéresserons au filtrage de contenu pour la détection de spam et les virus pour cela nous avons installé un antivirus et un anti-spam en tapant la commande suivante apt-get install amavisd-new clamv-daemon spamassassin

D'abord, nous activons la détection de spam et de virus dans amavisd-new en éditant le fichier /etc/amavis/conf.d/15-content_filter_mode :

```
 GNU nano 2.8.6          Fichier : 15-content_filter_mode

@bypass_virus_checks_maps = (
   \%bypass_virus_checks, \@bypass_virus_checks_acl, \$bypass_virus_checks_re);


#
# Default SPAM checking mode
# Please note, that anti-spam checking is DISABLED by
# default.
# If You wish to enable it, please uncomment the following lines:


@bypass_spam_checks_maps = (
   \%bypass_spam_checks, \@bypass_spam_checks_acl, \$bypass_spam_checks_re);
```

Figure 3.35 – Configuration de fichier 15-content filter mode de amavisd

Nous finalisons notre configurations avec Spamassassin en éditant le fichier /etc/default/spamassassin en activant la détection des spams et la mise à jour automatique :

```
# Change to "1" to enable spamd on systems using sysvinit:
ENABLE = 1

OPTIONS="--create-prefs --max-children 5 --helper-home-dir"
# Where should spamd write its PID to file? If you use the -u or
# --username option above, this needs to be writable by that user.
# Otherwise, the init script will not be able to shut spamd down.
PIDFILE="/var/run/spamd.pid"

# Set nice level of spamd
#NICE="--nicelevel 15"

# Cronjob
# Set to anything but 0 to enable the cron job to automatically update
# spamassassin's rules on a nightly basis
CRON=1
```

Figure 3.36 – Configuration de fichier spamassassin de Spamassassin

Après avoir fini la configuration de notre serveur de messagerie, nous redémarrons Postfix, Dovecot, Spamassassin et Amavis, et tester la connectivité des ports imaps(993) et smtps(465) avec la commande openssl s_client –connect email.mail.dz :993 qui donnera le même résultat avec le port 465 :

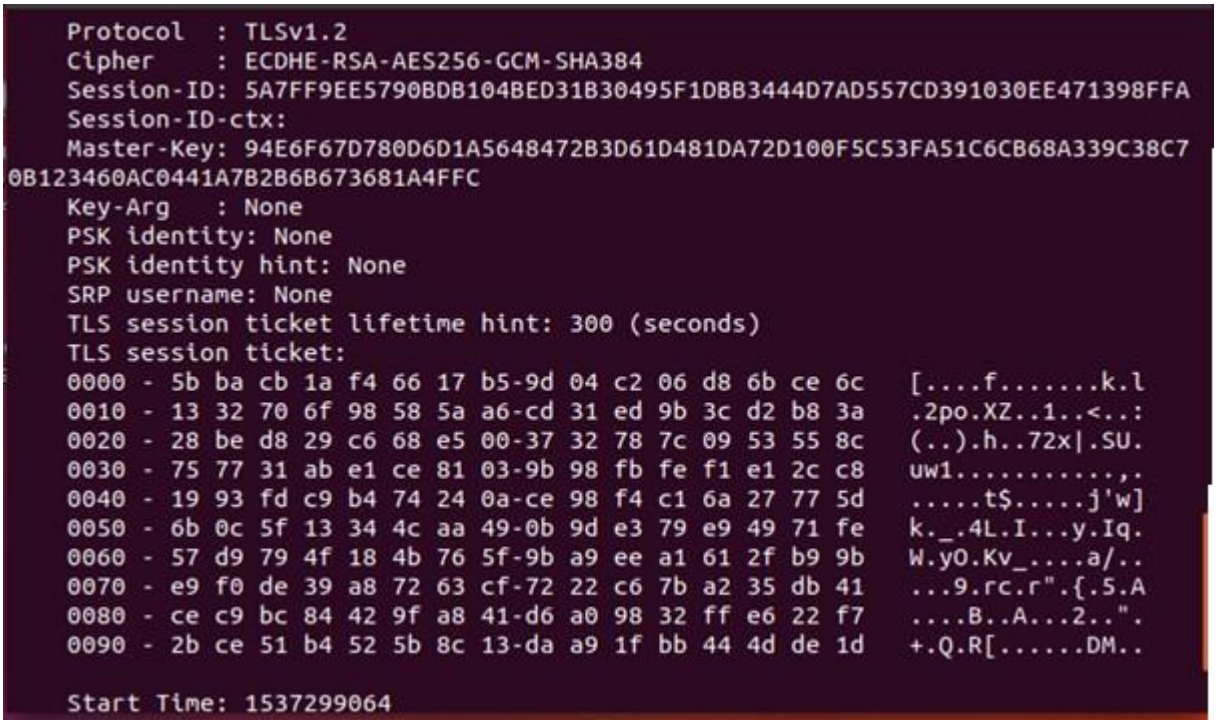

Figure 3.37 – Résultat de la commande openssl

3.3.9 Installation d'un webmail (Roundcube) :

Nous passons maintenant à l'installation d'un webmail qui est Roundcube pour ce faire nous devons le télécharger de la source a l'aide de cette commande wget https ://github.com/roundcube/roundcubemail/releases/download/1.3.6/roundcubemail-1.3.6-complete.tar.gz et le décompresser en tapant cette commande tar xvf roundcubemail-1.3.6-complete.tar.gz .

Une fois l'installation est faite nous devons configurer Apache2 pour héberger Roundcoube en créant et configurant le fichier webmail.conf dans /etc/apache2/sites-available tel qu'il est montré dans cette figure :

```
 GNU nano 2.8.6  Fichier : /etc/apache2/sites-available/webmail.conf  Modifié

<VirtualHost *:80>


        ServerName 192.168.1.5
        ServerAdmin katia02@mail.dz
        DocumentRoot /var/www/html/webmail

        ErrorLog ${APACHE_LOG_DIR}/webmailerror.log
        CustomLog ${APACHE_LOG_DIR}/webmailaccess.log combined

        <Directory /var/www/html/webmail>
                Options -Indexes
                AllowOverride All
                Order allow,deny
                allow from all
        </Directory>
```

Figure 3.38 – Création et configuration de fichier webmail.conf dans Apache2

Enfin, nous allons configurer Roundcube en accédant au programme d'installation tel qu'il est montré dans ces trois figures :

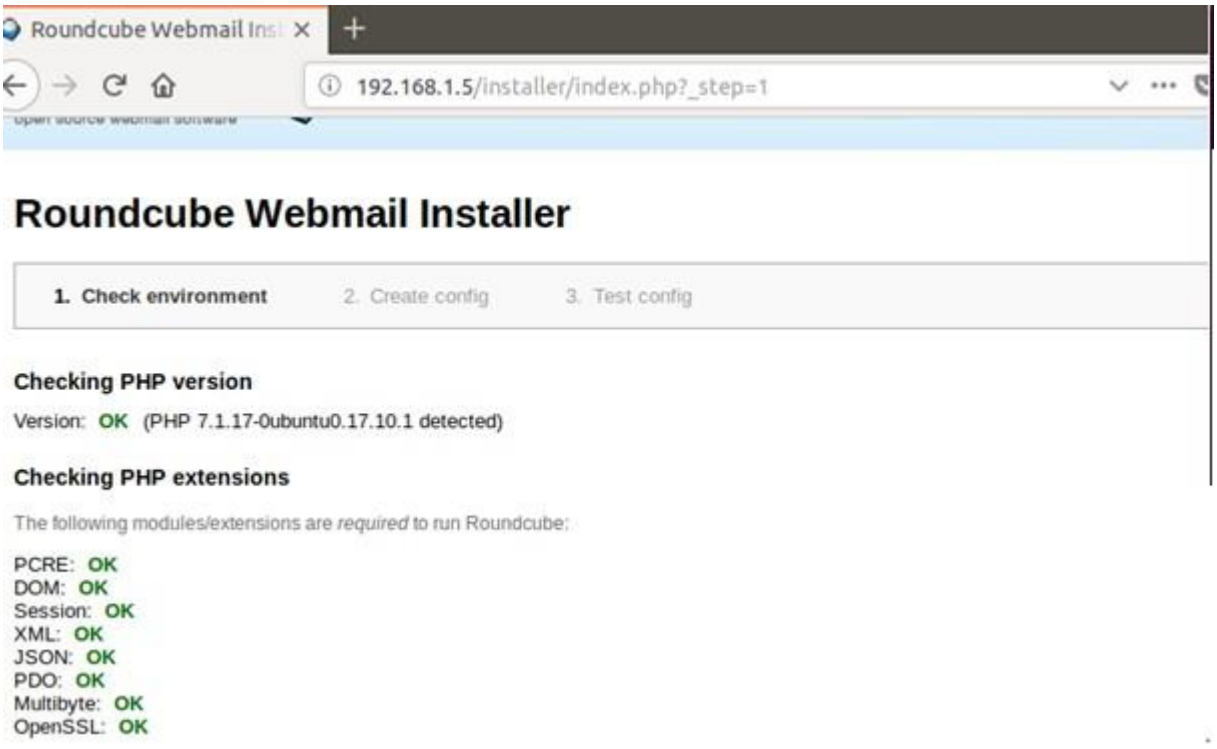

Figure 3.39 – Vérification de l'environnement de serveur

Nous allons à la page suivante pour ajouter certains paramètres pour créer le fichier de configuration par défaut de notre webmail tel qu'il est illustré dans ses deux figures qui suivent :

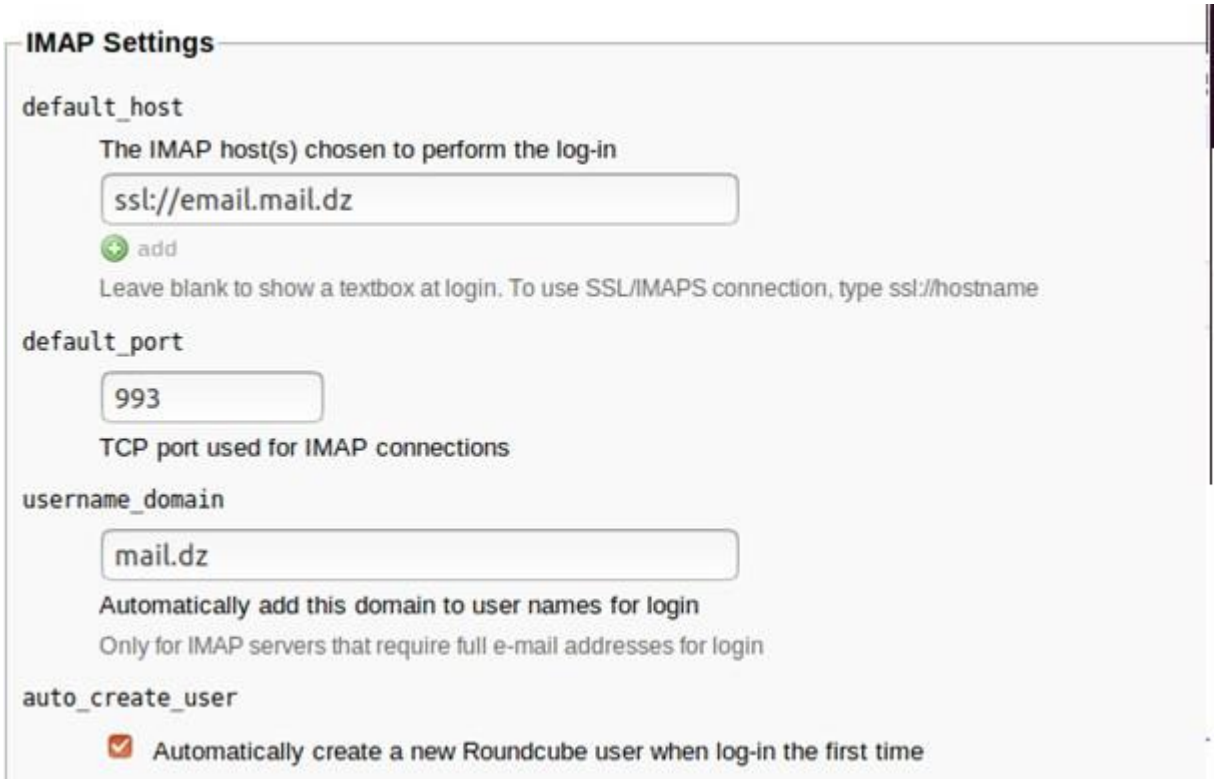

Figure 3.40 – Spécification de port imap sécurisé et le nom de domaine

Dans la figure ci-dessus nous avons spécifié le port 993 (imaps) de Dovecot qui est utilisé par Roundcube et le nom de domaine pour que les utilisateurs puisent se connecter qu'avec le nom d'utilisateur.

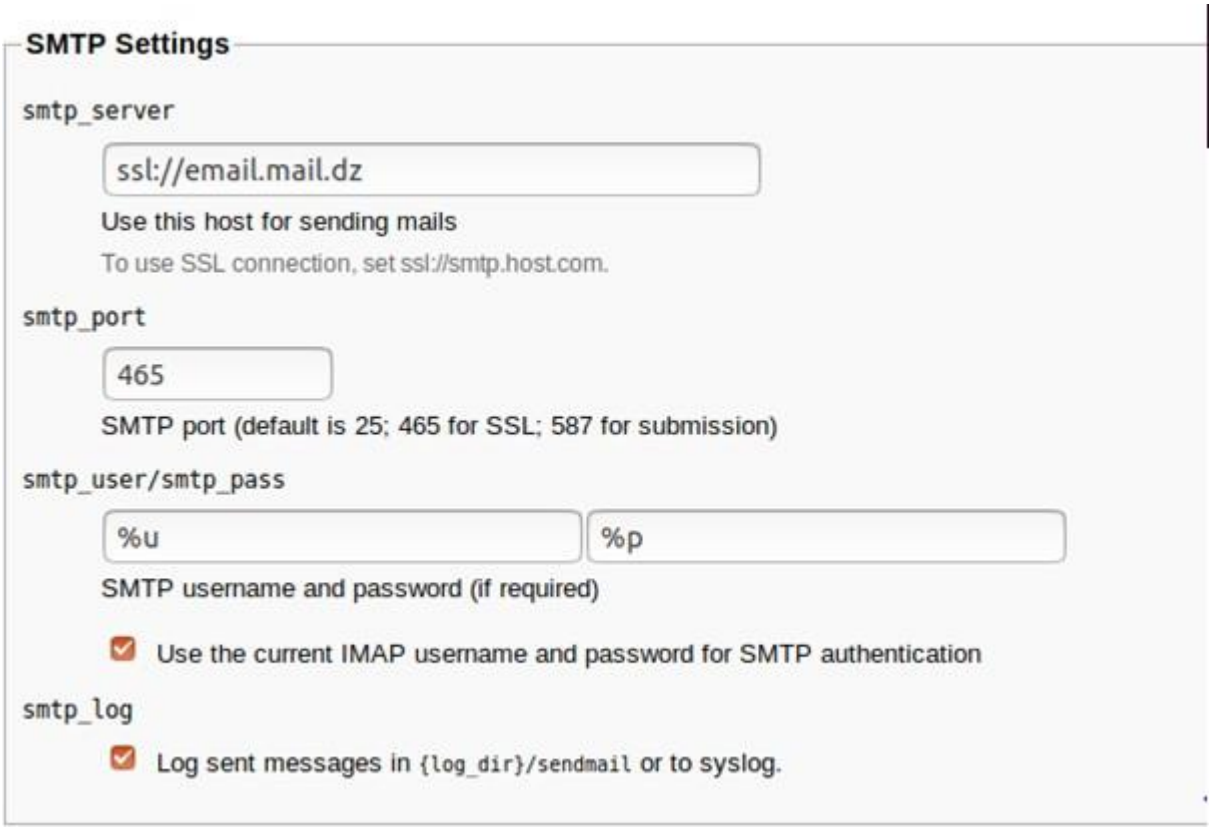

Figure 3.41 – Spécification de port smtp sécurisé

Dans la figure ci-dessus nous avons spécifié le port 465 (smtps) de Postfix et cocher la case Utiliser le nom d'utilisateur et le mot de passe IMAP actuels pour l'authentification SMTP afin que les utilisateurs puissent envoyer des messages sans ressaisir leurs informations d'identification.

Nous allons maintenant tester tous les paramètres en remplissant les bons champs smtp et imap pour les tests tel qu'il est illustré dans ces deux figures :

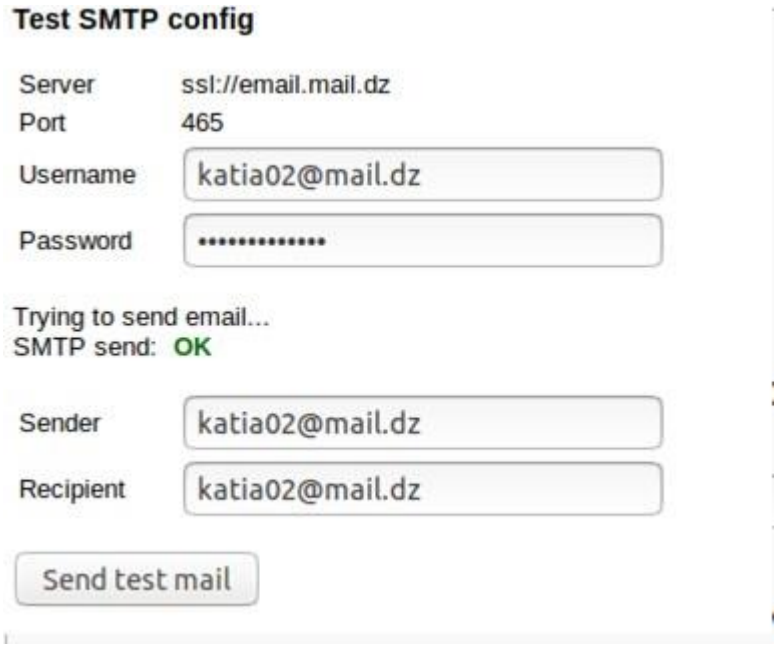

Figure 3.42 – Le fonctionnement de port 465 de Postfix

La figure ci-dessus nous montre que le message de test de Roundcube a était bien envoyé a la boite mail spécifié.

Figure 3.43 – Le fonctionnement de port 993 de Dovecot

La figure ci-dessus nous montre que le message de test de Roundcube a était bien reçu dans la boite mail spécifié.

Dans une machine qui est dans le même sous réseau que notre serveur nous accédons a notre webmail pour se connecter avec l'un des utilisateurs créer auparavant :

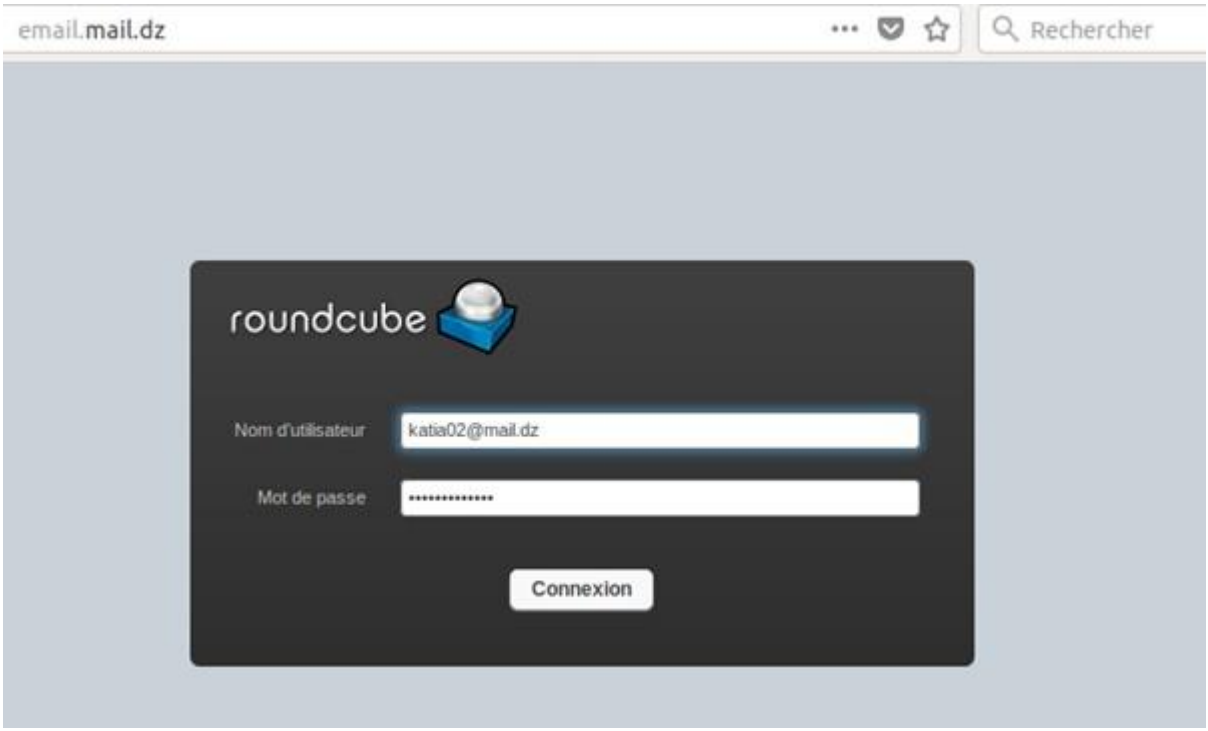

Figure 3.44 – La page de connexion de Roundcube

Maintenant nous pouvons composer un message et l'envoyer en introduisant l'adresse mail de destinataire, objet et le message lui même tel qu'il est montré dans cette figure :

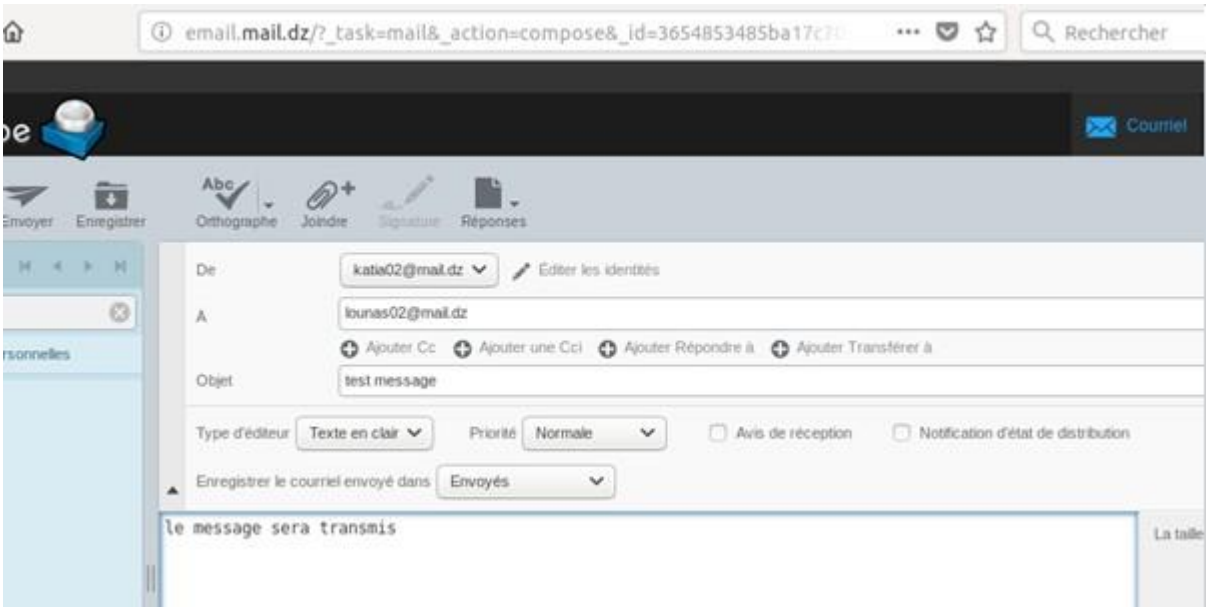

Figure 3.45 – Composer et envoyer un mail

Une fois le message envoyé nous accédons a la boite mail de destinataire pour voir le message s'il est bien reçu :

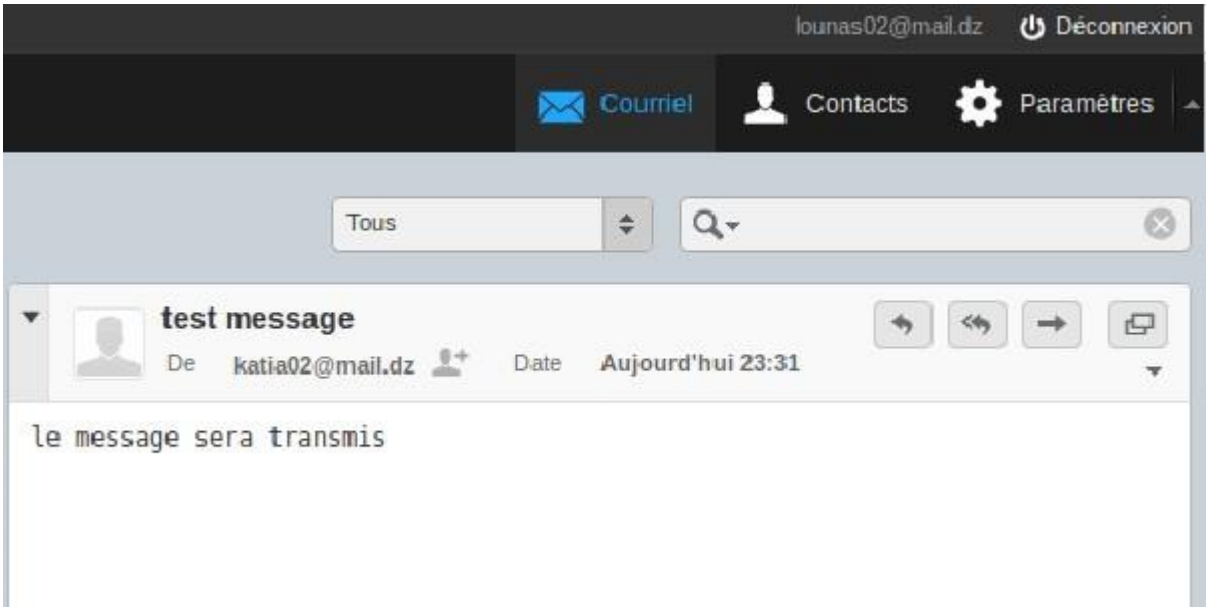

Figure 3.46 – La réception de message transmis

Et dans notre serveur mail nous pouvons voir le message envoyé et un ensemble d'informations concernant le protocole utilisé pour sécuriser la transmission de courrier électronique, algorithmes de chiffrement utilisés ainsi que le filtre de l'anti-virus :

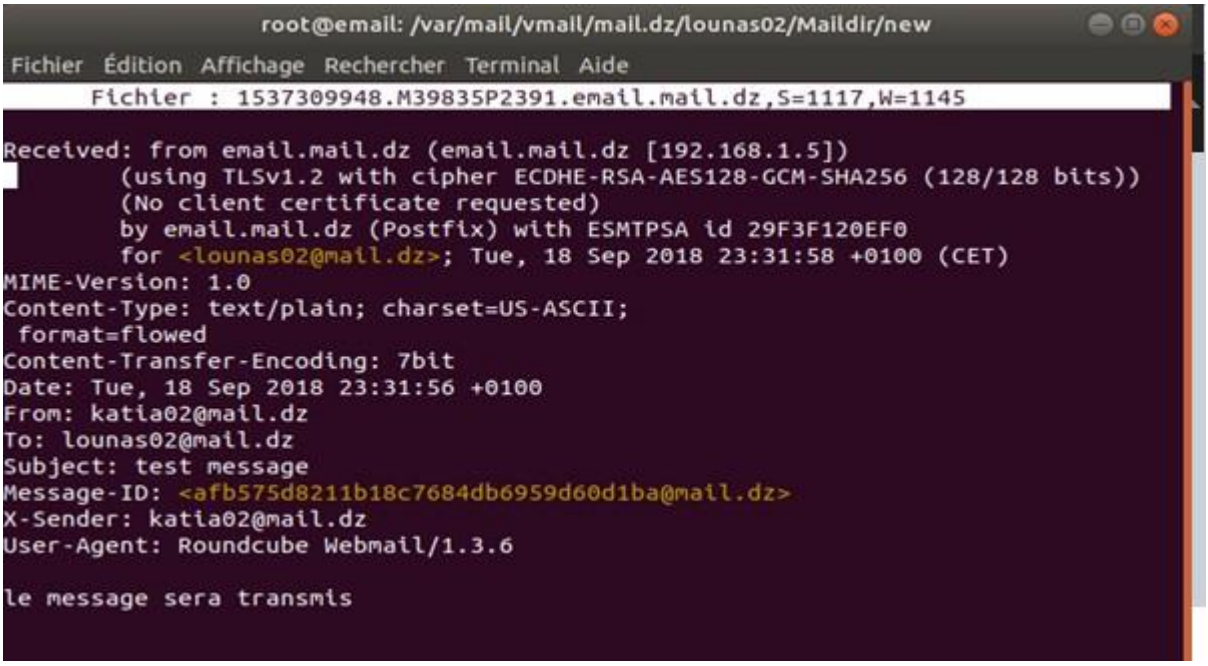

Figure 3.47 – Message conservé dans le répertoire créé dans le serveur

3.4 conclusion

Ce chapitre a été consacré à la phase de réalisation de notre projet d'une façon détaillée, nous avons illustré l'installation et la configuration de notre serveur de messagerie ainsi que la sécurité de l'échange d'informations circulant au sein du réseau et nous avons clôturé quelques fonctionnalités de notre serveur de messagerie

Conclusion générale

Notre objectif à travers ce travail est de mettre en place un serveur de messagerie électronique sécurisé, dans ce mémoire, nous avons indiqué comment un système de messagerie interne, de par sa mise en place et sa sécurisation pourrai répondre aux besoins en termes de technologies de l'information et de la communication d'une entreprise. Pour cela nous avons choisi de mettre en œuvre les composants suivants :

— Postfix comme MTA.
— Dovecot IMAP et POP comme MDA.
— Roundcube comme MUA.
— TLS comme protocole de sécurité.
— Anti-spam, antivirus.

Ces composants, nous les avons installés et configurés. Les étapes que nous avons suivies, sont citées explicitement dans le chapitre trois. Ce travail a été pour nous l'occasion d'une émulation intellectuelle dans le domaine de la messagerie électronique qui nous a permis d'exploiter nos connaissances et nos capacités et de les élargir et les approfondir.

En perspective nous souhaitons déployer notre système au sein d'une PME/PMI, et de créer une page php qui permettra au nouveau utilisateur de créer leur propre boite mail sans l'intermédiaire de l'administrateur.

Bibliographie

[1] Guy Pojolle, ‘les réseaux ‘, édition EYROLLES 3eme édition.

[2] G. PUJOLLE, Initiation aux r eseaux, Edition eyrolles, 27 f evrier 2014.

[3] Littlejohn shider, thomas w.shinder, tonehinkle, ”Administrer les services r eseaux sous Windows 2000” edition EYROLLES 2003.

[4] Alain lefebve ‘l’architecture client/serveur’ edition EYROLLES COLIN.

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

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

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

webographie

[8] http ://www.divona.dz/communication-efficace-entreprise-tic/, Accès, 2018.

[9] https ://www.supinfo.com/articles/single/176-messagerie-electronique, Accès, 2018.

[10] https ://www.supinfo.com/articles/single/176-messagerie-electronique, Accès, 2018.

[11]https ://www.commentcamarche.com/contents/173-structure-d-un-courrier-electronique-enveloppe-en-tetes-et-cor, Accès, 2018.

[12]https ://openclassrooms.com/fr/courses/1358631-gerer-votre-mail-a-la-unix/1358683-le-fonctionnement-de-la-messagerie-electronique. Accès, 2018.

[13] http ://www.siat.com.tn/wp-content/Presentation%20%20zimbra.pdf. Accès, 2018.

[14] https ://www.ossdirectory.com/fr/produits-oss/single/ossproduct/qmail/. Accès, 2018.

[15] https ://guide.ubuntu-fr.org/server/postfix.html. Accès, 2018.

[16] https ://doc.ubuntu-fr.org/dovecot. Accès, 2018.

[17] https ://doc.ubuntu-fr.org/cyrus, Accès, 2018.

[18]https ://toutgratuitpartage.be/thunderbird-60-0-windows-macos-et-linux/, Accès, 2018.

[19]https ://framalibre.org/content/roundcube. Accès, 2018.

[20]https ://blog.microlinux.fr/squirrelmail/, Accès, 2018.

[21].http ://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-fr-4/ch-email.html, Accès, 2018.

[22] https ://www.commentcamarche.com/contents/214-ssh-protocole-secure-shell, Accès, 2018.

[23] https ://www.frameip.com/ssl-tls, Accès, 2018.

[24] https ://guide.ubuntu-fr.org/server/mail-filtering.html. Accès, 2018.

[25] https ://inetdoc.developpez.com/tutoriels/securite-service-courrier-electronique-amavisd-new/. Accès, 2018.

[26] https ://doc.ubuntu-fr.org/dns, Accès, 2018.

[27] https ://openclassrooms.com/fr/courses/857447-apprenez-le-fonctionnement-des-reseaux-tcp-ip/857163-le-service-dns, Accès, 2018.

[28] http ://www.linux-france.org/prj/edu/archinet/systeme/ch27s03.html, Accès, 2018.