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

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

Mémoire De Fin de cycle

En vue d'obtention du diplôme de master professionnel en informatique spécialité : Adminstration et Sécurité des Réseaux Informatiques

Thème

Etude et amélioration de l'architecture et sécurité du réseau de l'EPB

Réalisé par :
M^elle^ SAOUD *Siham* et M^elle^ SAOUD *Amina* .

Soutenu le 28/06/2016 devant le jury composé de :

Président	**D^r^ M.AMAD**	**U. A/Mira Béjaïa.**
Examinateur	**M^me^ N.HALFOUNE**	**U. A/Mira Béjaïa.**
Encadreur	**D^r^ A/M. BOUDRIES**	**U. A/Mira Béjaïa.**

Promotion 2015/2016

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES ABRÉVIATIONS

ACL : Access Control List.
AD : Active Directory.
ADCS : Active Directory Certificate Services.
ADDS : Active Directory Domain Services.
ADFS : Active Directory Federation Services.
ADLDS : Active Directory Lightweight Directory Services.
ADRMS : Active Directory Rights Management Services.
ARP : Address Resolution Protocol.
ASLR : Address Space Layout Randomization.
BDD : Base de données.
BS OHSAS : British Standard Occupational Health and Safety Advisory Services.
CAS : Client Access Server.
DAG : Database Availability Group.
DAS : Direct Attached Storage.
DC : Direction Capitainerie.
DC : Domain Controller.
DDD : Direction Domaine et du Développement.
DEP : Data Execution Prevention).
DFC : Direction des Finance et comptabilité.
DGAF : DG Adjointe Fonctionnelle.
DGAO : DG Adjointe Opérationnelle.
DL : Direction de la Logistique.
DLP : Data Loss Prevention.
DMA : Direction Manutention et Acconage.
DMI : Direction du Management Intégré.
DMZ : zone démilitarisé.
DNS : Domain Name System.

DR : Direction Remorquage.
DRH : Direction des Ressources Humaines.
EAC : Exchange Administration Center.
ECC : Erorr Correction Code.
EMET : Enhanced Mitigation Experience Toolkit.
EPB : Entreprise Portuaire de Bejaia.
FAI : Fournisseur d'Accès Internet.
FTP : File Transfer Protocol.
FTP : Foiled Twisted Pairs.
FQDN : Fully Qualified Domain Name.
HTTP : HyperText Transfer Protocol.
HTTPS : HyperText Transfer Protocol Secure.
ICMP : Internet Control Message Protocol.
IDS : Intrusion Detection System.
IEEE : Institute of Electrical and Electronics Engineers.
IIS : Internet Information Services.
IMAP : Internet Message Access Protocol.
IP : Internet Protocol.
IPS : Intrusion Prevention System.
ISA : Internet Security and Acceleration.
ISO : International Organization for Standardization.
LAN : Local Area Network.
LAN : LAN Management Solution.
MAN : Metropolitan Area Network.
MBX : Mailbox Server.
MDA : Mail Delivery Agent.
MTA : Mail Transport Agent.
MUA : Mail User Agent.
MY SQL : Structured Query Language.
OMA : Outlook mobile Access.
OWA : Outlook Web Application.
PDA : Personal Digital Assistant.
PDG : président-directeur général.
PHP : Hypertext Preprocessor.
POP : Post Office Protocol.
PC : Personel Computer.
RAID : Redundation Array of Inexpensive Disks.
RJ45 : Registred Jack 45.
RPC : Remote procedure call.

SLC : Smart Link Communication.

SMTP : Simple Mail Transfer Protocol.

SNMP : Simple Network Management Protocol.

SP : Service Pack.

SSL : Secure Sockets Layer.

STP : Shielde Twisted Paire.

TCP : Transmission Control Protocol.

UTP : Unshielded Twisted Pair.

UO : Unité d'Organisation.

VLAN : Virtual Local Area Network.

VPN : Virtual Private Network.

VTP : VLAN Trunking Protocol.

WAN : Wide Area Network.

WIFI : Wireless Fidelity.

WIMAX : Worldwide Interoperability for Microwave Access.

W3C : World Wide Web Consortium.

UTP : Unshielded Twisted Pair.

INTRODUCTION GÉNÉRALE

Le besoin d'échanger des données se faisait sentir juste après l'apparition des ordinateurs, puis l'homme eut l'idée de les relier entre eux, c'est là qu'apparait le concept des réseaux informatiques.

Dans toute entreprise la notion de réseaux sonne comme une évidence, chaque entreprise existante d'une certaine taille dispose en générale d'un réseau informatique LAN ou WAN, qui lui permet d'effectuer le partage de ressources et de données. Vu l'importance des informations qui sont souvent véhiculées dans les réseaux, ceux-ci requièrent une bonne gestion du réseau, une souplesse d'utilisation et un certain degré de sécurité. Ces derniers sont devenus des éléments clés de la continuité des systèmes d'information de l'entreprise quels que soient son activité, sa taille et sa répartition géographique.

De ce fait, la gestion des réseaux informatiques se réfère aux activités, méthodes, procédures comme la surveillance du fonctionnement du réseau, et aux outils de mise en oeuvre par l'administrateur réseau ayant trait à l'exploitation, l'administration, la maintenance et la fourniture des réseaux informatiques.

Aussi bien que, pour avoir une bonne souplesse d'utilisation, il faut assurer la continuité du réseau, dû aux changements apportés à ce réseau en fonction de l'évolution rapide du secteur informatique et la qualité de service des informations selon le matériel et le logiciel utilisés.

Sachant de plus que la sécurité informatique au sens large devient une problématique planétaire. Avec l'avènement de l'Internet, la maitrise et la mesure de la sécurité logique des réseaux basés sur les installations et les configurations des équipements réseaux devient une priorité majeure pour les administrateurs réseaux.

Ainsi l'entreprise portuaire de Bejaïa ne fait pas exception à cette règle car la nécessité de protéger les données stratégiques, les services disponibles et la fragilité du réseau actuel aux différentes attaques internes et externes est primordiale. Pour cela il nous a été demandé d'améliorer et de mettre

en oeuvre une architecture réseau au sein de celle-ci.

Tout d'abord nous donnerons un aperçu sur les réseaux et la sécurité, ensuite dans le deuxième chapitre l'objet de notre étude va se porté sur la présentation de l'entreprise portuaire de Bejaïa et nous concentrerons aussi notre attention sur les critiques des parties réseau et sécurité de l'architecture existante et nous proposerons d'une éventuelles solution. Puis le troisième chapitre sera consacré à la mise en oeuvre de quelques améliorations, et enfin nous terminerons notre mémoire par une conclusion générale.

CHAPITRE 1

GÉNÉRALITÉS SUR LES RÉSEAUX ET LA SÉCURITÉ

1.1 Introduction

A l'origine, un réseau était un rassemblement de personnes ou d'objets. De nos jours on entend par réseau, les réseaux d'entreprises, qui connectent différentes machines afin de pouvoir les faire communiquer entre elles. Que ce soit pour le partage de fichiers ou l'envoi de messages, la plupart des entreprises sont aujourd'hui dotées d'un réseau afin d'être plus efficientes.

Une autre préoccupation est apparue, celle de la sécurité du transport des données, ainsi que l'accès aux informations sur les différents postes de travail. L'apparition d'Internet a posé beaucoup de problèmes, en terme de sécurité des informations, lors des échanges au travers les réseaux privés ou publiques, ce qui a nécessité la mise en oeuvre des mécanismes et des stratégies de sécurité.

Ce chapitre examine deux sections essentielles, la première décrit d'une manière générale les réseaux informatiques, la deuxième énumère les différentes attaques réseau ainsi que les moyens et technologies qui permettent de faire face à ces attaques.

1.2 Les réseaux informatiques des entreprises

1.2.1 Définition d'un Réseau

Le Réseau informatique est un ensemble d'ordinateurs et de périphériques reliés entre eux par des canaux électroniques de communications (filaire ou sans fil), qui leur permettent d'échanger des informations.

1.2.2 Les différents types de réseaux d'entreprise

On peut distinguer différent types de réseaux selon plusieurs critère tel que la taille de réseau, sa vitesse de transfert des données et aussi son etendu.

- **LAN (Local Area Network) ou réseau local**
  Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répondue étant Ethernet) [1].
  La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbit/s et 1Gbit/s [2].
  La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs [2].
- **MAN (Metropolitan Area Network) ou réseau métropolitain**
  Interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants, supérieur à 100 Mbits/s. Ainsi Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique) [1].
- **WAN (Wide Area Network) ou réseau étendu**
  Interconnecte plusieurs LAN à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles. Les WAN fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un noeud du réseau. Le plus connu des WAN est Internet [1].

1.2.3 L'architecture des réseaux d'entreprise

On distingue également deux catégories de réseaux :

- **Les réseaux Post à post (peer to peer= P2P)**
  Sur un réseau post à post, les ordinateurs sont connectés directement l'un à l'autre et il n'existe pas d'ordinateur central, comme présenté dans la figure 1.1. L'avantage majeur d'une telle installation est son faible coût en matériel (les postes de travail et une carte réseau par poste). En revanche, si le réseau commence à comporter plusieurs machines il devient impossible à gérer [3].
- **Les réseaux client-serveur :**
  Sur un réseau à architecture client/serveur, tous les ordinateurs (client) sont connectés à un ordinateur central (le serveur du réseau), une machine généralement très puissante en terme de capacité ; Elle est utilisée surtout pour le partage de connexion Internet et de logiciels centralisés, ce type d'architecture est plus facile a administrer lorsque le réseau et important car l'administration est centralisé mais elle nécessite un logiciel couteux spécialisé pour l'exploitation du réseau.[3], Voir la figure 1 .

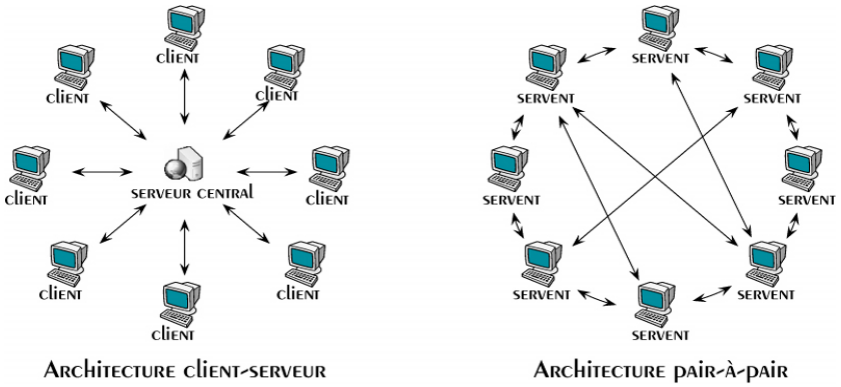

FIGURE 1.1 – Architecture des réseaux

1.2.4 Les topologies des réseaux

1.2.4.1 Topologie en bus

Dans cette topologie, les ordinateurs sont disposés et reliés de part et d'autre d'un câble principal appelé bus (voir figure 2). Le support de transmission utilisé dans ce cas est le câble coaxial. Dans cette topologie, lorsqu'un ordinateur envoi une information, tous les autres ordinateur du réseau reçoivent l'information mais seul la machine à qui l'information est destinée va utiliser [30].

1.2.4.2 Topologie en anneau

Dans cette topologie, les ordinateurs sont connectés à une boucle et communiquent chacun à leur tour (voir figure 2). Les informations circulent dans une direction unique, d'un ordinateur à un autre [30].

1.2.4.3 Topologie en étoile

Dans cette topologie, les ordinateurs du réseau sont reliés à un équipement central appelé concentrateur (hub) ou un commutateur (Switch)[30]. Celui-ci a pour rôle d'assurer la communication entre les différents ordinateurs connectés à lui (voir figure 2).

1.2.4.4 Topologie en Maille

Dans cette topologie, chaque ordinateur est directement relié à tous les autres (voir figure 2). Ainsi lorsqu'un ordinateur veut envoyer une information à un autre celui-ci le fait de façon directe sans passer par un équipement spécifique [30].

1.2.4.5 Topologie en Arbre

Une topologie arborescente est une combinaison des différentes autres topologies ; elle peut reposer à la fois sur des topologies en bus, en étoile et en anneau [30]. (voir figure 2).

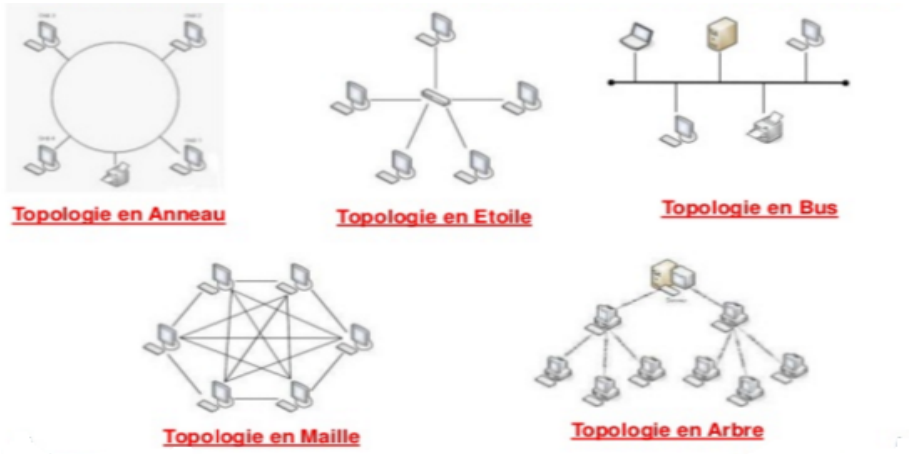

FIGURE 1.2 – Topologies des réseaux

1.2.5 Composants matériels d'un réseau d'entreprise

1.2.5.1 Equipements d'interconnexion

Voici les équipements qui peuvent rentrer dans la composition d'un réseau d'entreprise [4] :

- **La carte réseau**
  Elle constitue l'interface physique entre l'ordinateur et le câble réseau. Les données transférées du câble à la carte réseau sont regroupé en paquets composé d'un entête qui contient les informations d'emplacement et des données d'utilisateurs. Souvent la carte réseau est intégrée dans la carte mère.
- **Le concentrateur**
  Le concentrateur (appelé Hub en anglais) est un élément matériel qui permet de relier plusieurs ordinateurs entre eux. Son rôle c'est de diffuser la donnée sur l'ensemble des ports.
- **Le répéteur**
  Le répéteur (en anglais repeater) est un équipement utilisé pour régénérer le signal entre deux noeuds du réseau, afin d'étendre la distance du réseau. On peut l'utiliser pour relier des câbles de même types et de types différents.
- **Les ponts**
  Le pont (bridge) est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole. Il reçoit la trame et analyse l'adresse de l'émetteur et du destinataire et la dirige vers la machine destinataire.
- **Le commutateur**
  Comme le concentrateur, le commutateur (en anglais switch) est un élément matériel qui permet de relier plusieurs ordinateurs entre eux. Sa seule différence avec le Hub, c'est qu'il est capable de connaître l'adresse physique des machines qui lui sont connectées et d'analyser les trames reçues pour les diriger vers la machine de destination.

- **La passerelle**

  La passerelle permet à des architectures réseau différentes de communiquer entre elle. Une passerelle joue le rôle d'un interprète par exemple deux réseaux peuvent être physiquement connectés, mais ils peuvent avoir besoin d'une passerelle pour traduire les données qu'ils s'échangent.

- **Le routeur**

  Le routeur est un appareil qui relie des réseaux et achemine les informations d'un émetteur vers un destinataire selon une route, il examine l'en-tête de chaque paquet pour déterminer le meilleur itinéraire par lequel acheminer le paquet. Le routeur connaît l'itinéraire de tous les segments du réseau grâce aux informations stockées dans sa table de routage.

- **Le modem (modulateur démodulateur)**

  Le modem est un périphérique qui permet de transmettre et de recevoir les données sous forme d'un signal. il transforme les signaux analogiques en numériques et inversement, ces signaux sont acheminés par une ligne téléphonique.

1.2.5.2 Supports de transmissions

Il existe plusieurs types de support de transmission nous allons décrire quelques-uns ci-dessous [5] :

1. **câble coaxial**

   Un câble coaxial se compose d'un conducteur de cuivre entouré d'une couche de matériau isolant flexible.

   - Un câble coaxial se compose d'un conducteur de cuivre entouré d'une couche de matériau isolant flexible.
   - Vitesse et débit : 10 à 100Mbit/s.
   - Cout : économique
   - Taille du connecteur et du média : moyenne.
   - Longueur de câble maximale : 500 m.

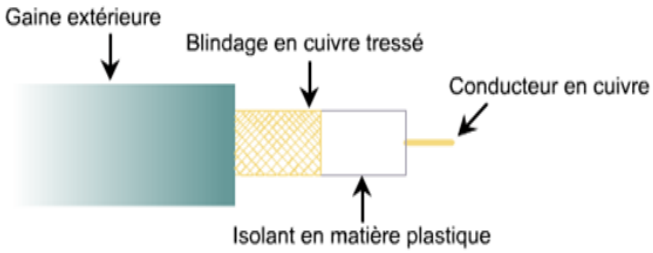

FIGURE 1.3 – câble coaxial

2. **Câble à paires torsadées blindées (STP)**

   Le câble à paires torsadées blindées allie les techniques de blindage, d'annulation et de torsion des fils. Chaque paire de fils est enveloppée dans une feuille métallique et les deux paires sont enveloppées ensemble dans un revêtement tressé ou un film métallique.

   - Vitesse et débit : 0 à 100Mbit/s.
   - Cout : modéré.
   - Taille du connecteur et du média : moyenne a grande.
   - Longueur de câble maximale : 100 m.

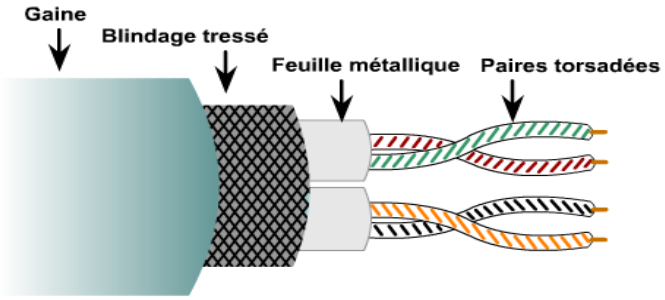

FIGURE 1.4 – Câble à paires torsadées blindées (STP).

3. **Câble à paires torsadées non blindées (UTP)**

   Est un média constitué de quatre paires de fils, présent dans divers types de réseau. Chacun des huit fils de cuivre du câble est protégé par un matériau isolant. De plus, les paires de fils sont tressées entre elles. Ce type de câble repose uniquement sur l'effet d'annulation produit par les paires torsadées pour limiter la dégradation du signal due aux interférences électromagnétiques et radio.

   - Vitesse et débit : 10-100-1000 Mbit/s.
   - Cout : le moins onéreux.
   - Taille du connecteur et du média : petite.
   - Longueur de câble maximale : 100 m.

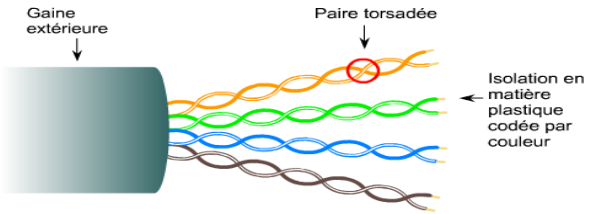

FIGURE 1.5 – Câble à paires torsadées non blindées (UTP).

4. **Fibre optique**

   Le coeur d'une fibre optique est la partie dans laquelle circulent les rayons lumineux. Chaque câble à fibre optique utilisé dans les réseaux comprend deux fibres de verre logées dans des enveloppes distinctes. Une fibre transporte les données transmises depuis l'équipement A vers l'équipement B. Il existe deux types de fibre monomode et multimode.

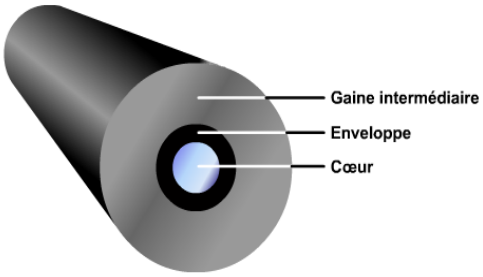

FIGURE 1.6 – Fibre optique.

5. **Transmission sans fil**

   Le Wi-Fi ou wifi est un ensemble de protocoles de communication sans fil régis par les normes du groupe IEEE 802.11 (ISO/CEI 8802-11). Un réseau Wi-Fi permet de relier par ondes radio plusieurs appareils informatiques (ordinateur, routeur, smartphone, décodeur Internet, etc.) au sein d'un réseau informatique afin de permettre la transmission de données entre eux.

1.2.5.3 Périphériques finaux

Les périphériques réseau auxquels les gens sont le plus habitués sont appelés périphériques finaux, ou hôtes. Ces périphériques forment l'interface entre les utilisateurs et le réseau de communication sous-jacent. Voici quelques exemples de périphériques finaux [6] :

- Ordinateurs.
- Imprimantes réseau.
- Téléphones VoIP.
- Terminal TelePresence.
- Caméras de surveillance.
- Appareils mobiles (tels que les smartphones, tablettes, PDA, les lecteurs de cartes bancaires et les scanners de codes-barres sans fil).
- Serveur (physique ou virtuel).

1.3 La sécurité des réseaux d'entreprise

1.3.1 Les attaques réseaux

Les attaques réseaux sont très nombreuses, il est donc très difficile de les recenser. Il est cependant possible de dresser une typologie des faiblesses de sécurité afin de mieux appréhender ces attaques, qui ont pour point commun d'exploiter des faiblesses de sécurité. Ces dernières peuvent être classifiées par catégories comme suit :

1.3.1.1 Faiblesse des protocoles

Quelques protocoles réseaux n'ont pas été conçus pour tenir compte des problèmes de sécurité. Les principales attaques qui se propagent dans ce type de faiblesse sont :

- **Attaque par fragmentation**

  une attaque par fragmentation est une attaque réseau par saturation exploitant le principe de fragmentation du protocole IP. En effet, le protocole IP est prévu pour fragmenter les paquets de taille importantes en plusieurs paquets IP possédant chacun un numéro de séquence et un numéro d'identification commun. A la réception des données, le destinataire rassemble les paquets grâce aux valeurs de décalages qu'il contienne [7] .

- **Attaque par déni de service**
  le déni de service consiste à empêcher les utilisateurs légitimes d'accéder aux informations ou d'obtenir les services auxquels ils ont droits, c'est une attaque contre la disponibilité. C'est souvent le type d'attaque le plus facile, puisqu'il suffit d'émettre des requêtes valide ou non,en très grand nombre (on parle alors d'inondation ou flooding, de façon à saturer les ressources disponible pour un service donné [8].

1.3.1.2 Faiblesse d'authentification

Les versions actuelles des protocoles IP ou ICMP, ne dispose pas de mécanisme d'authentification, de ce fait elles subissent des attaques qui s'appuient sur ces faiblesses. Parmi les principales attaques on trouve :

- **Attaque ARP**
  C'est une technique d'attaque simple qui consiste à exploiter les lacunes du protocole ARP, c'est ce qu'on appelle couramment l'empoisonnement de cache ARP, elle exploite la lacune de non authentification des requêtes. En effet, rien n'indique à une machine qu'une requête provient effectivement d'une machine avec laquelle elle communique [9].

- **Attaque man-in-the-middle**
  dite en français l'homme au milieu, elle consiste à passer les échanges entre deux personnes par le biais d'une troisième, sous le contrôle de l'entité pirate, ce dernier intercepte et transforme les données, toute en masquant à chaque acteur la réalité de son interlocuteur [10].

- **Attaque par réflexion**
  des milliers de requêtes sont envoyées par l'attaquant au nom de la victime. Lorsque les destinataires répondent, toutes les réponses convergent vers l'émetteur officiel, dont les infrastructures se trouvent affectées [11].
- **Attaque par Rejeu de message**
  Les attaques par " rejeu " (en anglais " replay attaque ") sont des attaques de type " Man in the middle " consistant à intercepter des paquets de données et à les rejouer, c'est-à-dire les retransmettre tels quel (sans aucun déchiffrement) au serveur destinataire [12].

1.3.1.3 Faiblesse d'implémentation

Parmi les attaques qui exploitent ce genre de faiblesse on trouve :

- **Attaque du ping de la mort**
  "L'attaque du ping de la mort " est une des plus anciennes attaque réseau. Le principe consiste tout simplement à créer un datagramme IP dont la taille totale excède la taille maximum autorisée (65536 octets). Un tel paquet envoyé à un système possédant une pile TCP/IP vulnérable, provoquera un plantage [12].

1.3.1.4 Faiblesse de configuration

Une mauvaise configuration des équipements réseau, pare-feu, routeur...etc. est souvent exploitée pour mener des attaques. Les erreurs de configuration peuvent être de plusieurs natures, incluant l'erreur humaine, par conséquent les équipements réseau ne doivent accédés ou configurés que par des acteurs autorisés [13].

1.3.2 Conduire une politique de sécurité réseau

La politique de sécurité d'une entreprise se base sur une analyse des risques décrivant les ressources critiques de l'entreprise, les probabilités de menace ainsi que leurs conséquences.

1.3.2.1 Les objectifs d'une politique de sécurité

Une politique de sécurité consiste à mettre en place un ensemble de procédures et d'opérations suivies par l'entreprise, tel que [14] :

- ✓ S'assurer que les utilisateurs observent les bonnes pratiques et les règles concernant l'utilisation des technologies de l'information.
- ✓ S'assurer que les normes en matière de sécurité informatique soient dûment mises en application.
- ✓ Réviser périodiquement les résultats des vérifications et contrôles, notamment pour y relever les anomalies et autres incidents.
- ✓ Recommander les actions à prendre pour corriger les situations anormales ou dangereuses, notamment, les processus opérationnels et les grandes stratégies en matière informatique et les achats d'équipement.

- ✓ Informer le comité de Direction du Collège des travaux, activités et incidents en matière de sécurité informatique.
- ✓ S'assurer que les éléments opérationnels qui requièrent une approbation des différentes directions soient respectés.

1.3.2.2 Principe générique d'une politique de sécurité réseau

Quelle que soit la nature des biens produit par l'entreprise, sa politique de sécurité réseau vise à satisfaire les critères suivants :

- Identification : information permettant d'indiquer qui vous prétendez être.
- Authentification : information permettant de valider l'identité pour vérifier que vous êtes celui que vous prétendez être.
- Autorisation : information permettant de déterminer quelles sont les ressources de l'entreprise auxquelles l'utilisateur identifié aura accès ainsi que les actions autorisées sur ces ressources.
- Confidentialité : ensemble des mécanismes permettant qu'une communication de données reste privée entre un émetteur et un destinataire.
- Intégrité : ensemble des mécanismes garantissant qu'une information n'a pas été modifiée.
- Disponibilité : ensemble des mécanismes garantissant que les ressources de l'entreprise sont accessibles.
- Non-répudiation : mécanisme permettant de trouver qu'un message a bien été envoyé par un émetteur et reçu par un destinataire.
- Traçabilité : ensemble des mécanismes permettant de retrouver les opérations réalisées sur les ressources de l'entreprise.
- Continuité : a pour but de garantir la survie de l'entreprise après un sinistre important touchant le système informatique. Il s'agit de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données.

1.3.2.3 Les différents types de politiques de sécurité

Une politique de sécurité couvre les éléments suivants :

- Sécurité de l'infrastructure : couvre la sécurité logique et physique des équipements et des connexions réseau.
- Sécurité des accès : couvre la sécurité logique des accès locaux et distants aux ressources de l'entreprise, ainsi que la gestion des utilisateurs et de leurs droits d'accès aux systèmes d'information de l'entreprise.
- Sécurité de l'Intranet face à Internet ou aux tierces parties de confiance : couvre la sécurité logique des accès aux ressources de l'entreprise (Extranet) et l'accès aux ressources extérieurs (Internet).

1.3.3 Stratégie de sécurité réseau

1.3.3.1 Méthodologie pour élaborer une stratégie de sécurité réseau

Il existe plusieurs méthodes permettant d'élaborer des stratégies de sécurité, nous pouvons citer :

- Prédiction des attaques potentielles et analyse de risque.
- Analyse des résultats et amélioration des stratégies de sécurité.

1.3.3.2 Proposition de stratégies de sécurité réseau

Les parties qui suivent détaillent un ensemble de stratégies de sécurité focalisées sur des domaines spécifiques, ces stratégies doivent être considérées comme des briques de bases pour avoir une bonne politique de sécurité [15] :

- **Authentification**
  L'authentification selon le contexte utilise des informations contextuelles pour vérifier si l'identité d'un utilisateur est authentique ou non. Grâce aux profils de risque, les entreprises ont les moyens de restreindre l'accès à des systèmes spécifiques ou à des éléments de contenu selon les critères d'un utilisateur.
- **Cryptographie (chiffrement et signature)**
  Le chiffrement des données fut inventé pour assurer la confidentialité des données. Il est assuré par un système de clé (algorithme) appliqué sur le message. Ce dernier est décryptable par une clé unique correspondant au cryptage. Dans toute transaction professionnelle, La signature numérique est un moyen d'identification de l'émetteur du message.
- **Contrôles d'accès aux ressources**
  Méthode pour restreindre l'accès à des ressources. On n'autorise que certaines entités privilèges.
- **Firewalls**
  Afin d'éviter que des attaques puissent venir d'Internet par le routeur, il convient d'isoler le réseau interne de l'entreprise. La méthode la plus connue est le firewall et le serveur proxy ; Le firewall, placé à l'entrée du réseau, constitue ainsi un unique point d'accès par où chacun est obligé de passer. Le serveur Proxy, lui, permet de faire le relais au niveau des applications pour rendre les machines internes invisibles à l'extérieur.
- **Audit**
  L'audit de sécurité permet d'enregistrer tout ou partie des actions effectuées sur le système. L'analyse de ses informations permet de détecter d'éventuelles intrusions. Les systèmes d'exploitation disposent généralement de systèmes d'audit intégrés, certaines applications aussi. Les différents évènements du système sont enregistrés dans un journal d'audit qui devra être analysé fréquemment, voire en permanence. Sur les réseaux, il est indispensable de disposer d'une base de temps commune pour estampiller les évènements.

- **Logiciels anti-virus**
  Deux tiers des attaques se font par virus : chaque poste doit disposer d'un logiciel anti-virus mis à jour régulièrement ! Les virus se transmettent principalement par flash disk, mais peuvent aussi se faire par mail. Les fichiers les plus susceptibles d'en contenir sont bien sûr les exécutables (.com, .exe).
- **Programmes de tests de vulnérabilité et d'erreurs de configuration**
  Utiliser des logiciels permettant de façon automatique de chercher les erreurs de configuration ou les vulnérabilités du système tel que Cops et Satan.
- **Détection d'intrusion**
  Utiliser un logiciel de détection des comportements anormaux d'un utilisateur ou des attaques connues. Ce logiciel émet une alarme lorsqu'il détecte que quelqu'un de non-autorisé est entré sur le réseau.
- **Les réseaux privés virtuels (VPN : Virtual Private Network)**
  Permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Avec le développement d'Internet, il est intéressant de permettre un transfert de données sécurisé et fiable. Grâce à un principe de tunnel (tunnelling) dont chaque extrémité est identifiée, les données transitent après avoir été chiffrées.
- **Les DMZ (zone démilitarisé)**
  Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur Web, serveur de messagerie, serveur FTP public,...etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau a part, accessible aussi bien du réseau interne que de l'extérieur sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de zone démilitarisé (noté DMZ pour Demilitarized zone) pour designer cette zone isolée hébergeant des applications mises à disposition du public [16].

1.4 Conclusion

Ce chapitre a introduit les premiers concepts des réseaux informatiques, ainsi qu'une analyse des besoins de sécurité et les étapes capitales qui précèdent la mise en place des stratégies de sécurité dans un réseau d'entreprise. Le chapitre suivant va porter sur une étude du réseau existant au sein de l'entreprise ainsi qu'une synthèse de ses faiblesses et leurs solutions.

CHAPITRE 2

ETUDE DE L'EXISTANT ET PROPOSITION DE NOUVELLES AMÉLIORATIONS

2.1 Introduction

Ce chapitre sera réservé à l'étude du réseau existant dans l'EPB et aux améliorations proposées, d'abord nous allons évoquer un bref aperçu de l'entreprise pour mieux connaitre sa structure et ses objectifs. Ensuite, nous allons étudier le réseau et ses composants pour pouvoir proposer d'éventuelles améliorations.

2.2 Présentation générale de l'organisme d'accueil

Le port de Bejaia joue un rôle très important dans les transactions internationales vu sa place et sa position géographique. Aujourd'hui, il est classé 2ème port d'Algérie en marchandises générales et 3ème port pétrolier. Il est également le 1er port du bassin méditerranéen certifié par ISO 9001 pour l'ensemble de ses prestations et pour avoir ainsi installé un système de management d'une grande qualité. Cela est très important pour le processus d'amélioration des prestations, pour le bénéfice de ses clients. L'Entreprise Portuaire a connu d'autres succès depuis, elle est notamment certifiée à la Norme ISO 14001 et au référentiel BS OHSAS 18001, respectivement pour l'environnement et l'hygiène et sécurité au travail.

2.2.1 Missions et activités de l'Entreprise Portuaire de Bejaïa

Les missions et les activités sont représentées dans la figure 2.1.

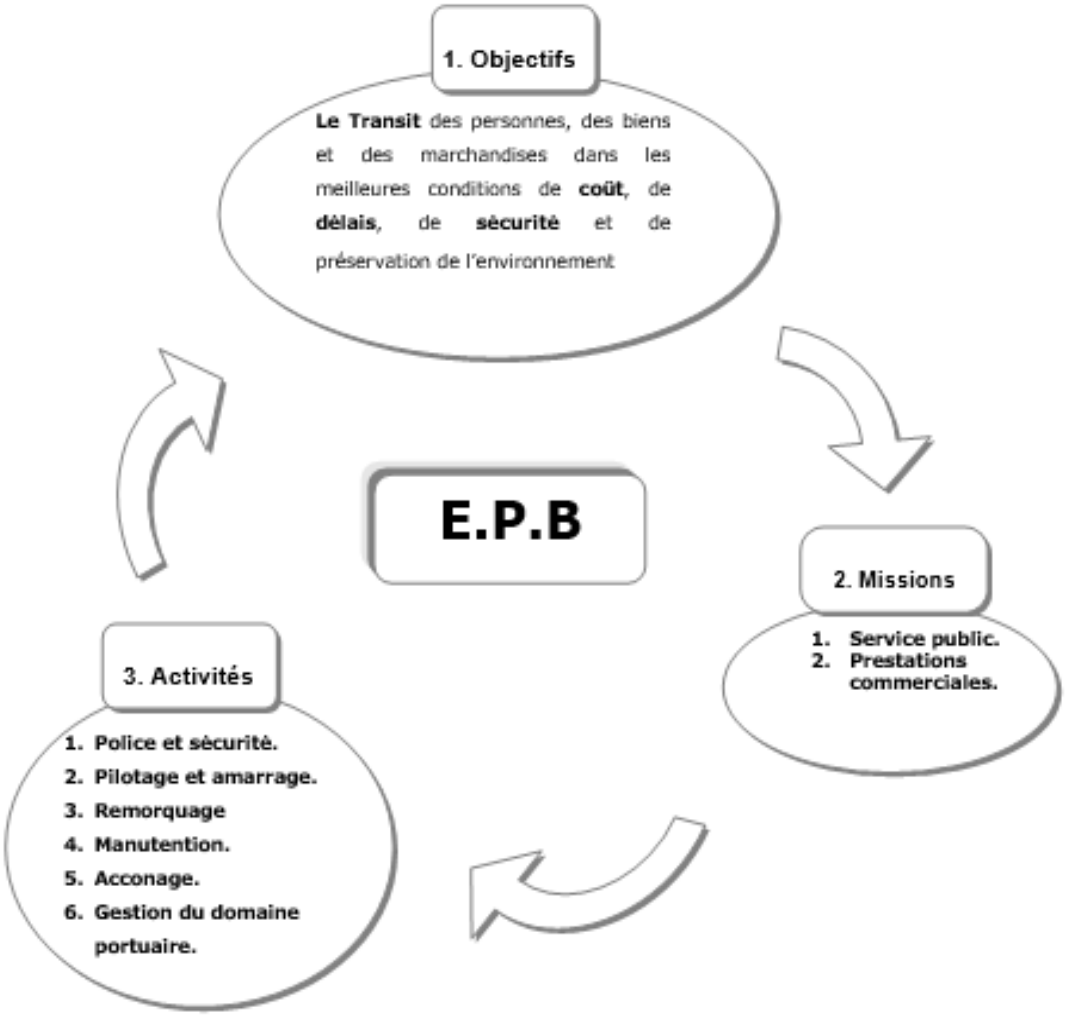

FIGURE 2.1 – Missions et Activités de l'EPB

2.2.2 Organisation de la structure générale de l'entreprise

Organigramme :

L'EPB est organisée selon des directions fonctionnelles et opérationnelles dirigées par une Direction Générale qui est chargée de concevoir, coordonner et contrôler les actions liées à la gestion et au développement de l'entreprise (voir figure 2.2).

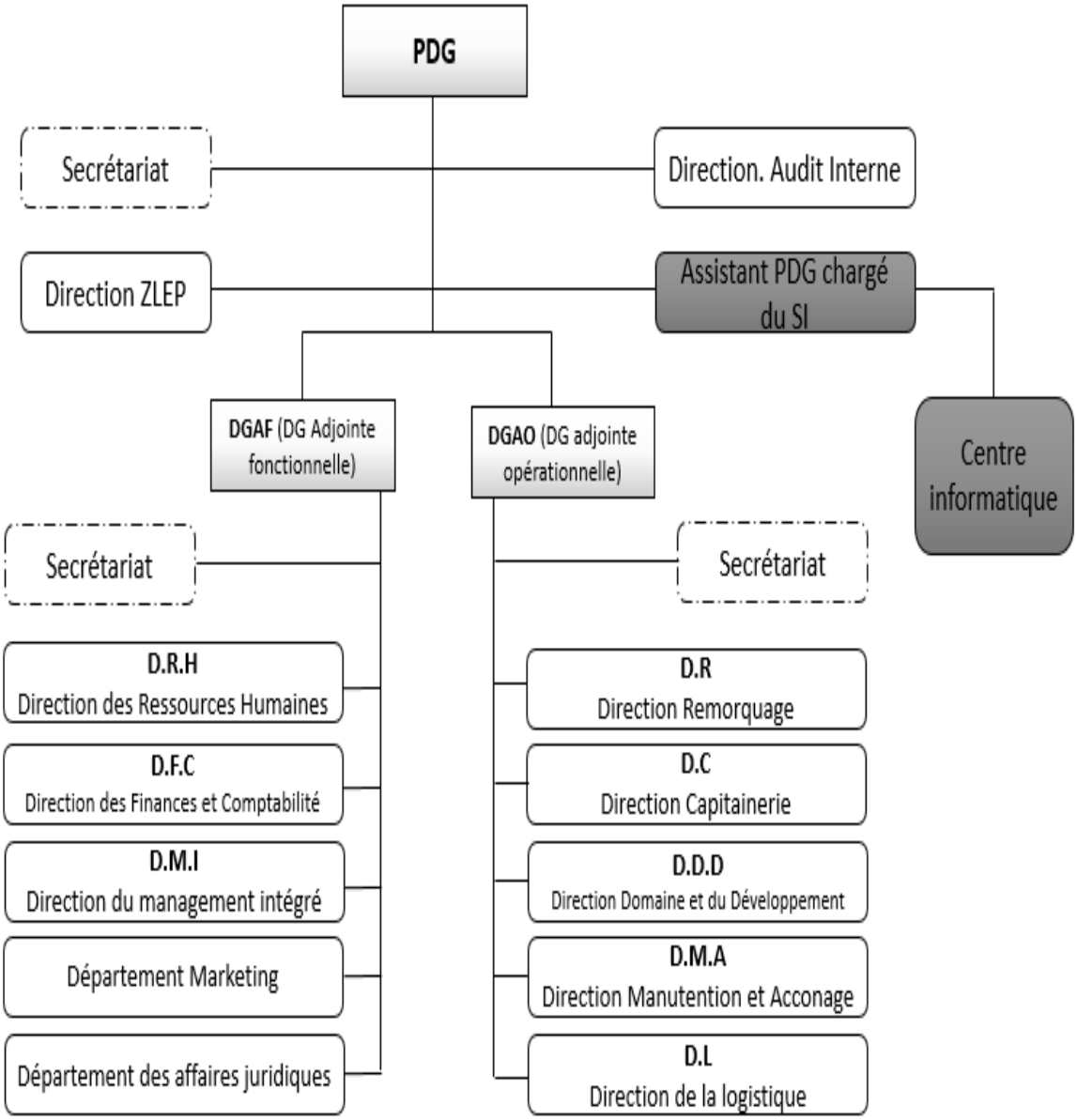

FIGURE 2.2 – organigramme de l'EPB

2.3 Présentation du centre informatique

La structure informatique de l'EPB est un département rattaché à la direction générale adjointe ; il a été créé en 1989 et c'est à cette époque que les premières applications de l'entreprise ont vu le jour. En 1995 la micro-informatique a été introduite à l'EPB et les premières applications sont écrites sous DBASE 5. A partir de 2001 l'entreprise portuaire a lancé un plan pour développer les applications métiers sous PHP et DELPHI 5 et comme système de gestion de bases de données MYSQL.

2.3.1 les missions du centre informatique

- L'informatique a pour mission l'automatisation des métiers de l'Entreprise Portuaire de Bejaia, et cela en mettant en place les logiciels et l'infrastructure nécessaires pour la gestion du système d'information.
- L'EPB déploie des systèmes d'informations pour accroitre la productivité, automatiser les processus métiers et fournir un meilleur service aux clients. Ces systèmes intègrent de plus en plus des fonctionnalités réseau pour relier tous les utilisateurs à l'entreprise ou établir des liens avec la clientèle et les fournisseurs.
- Le réseau apporte aujourd'hui une réelle valeur ajoutée en permettant d'intégrer de nouveaux partenaires, fournisseurs et clients.

2.3.2 Organisation humaine du centre informatique

la figure 2.3 représente l'organisation humaine du département informatique

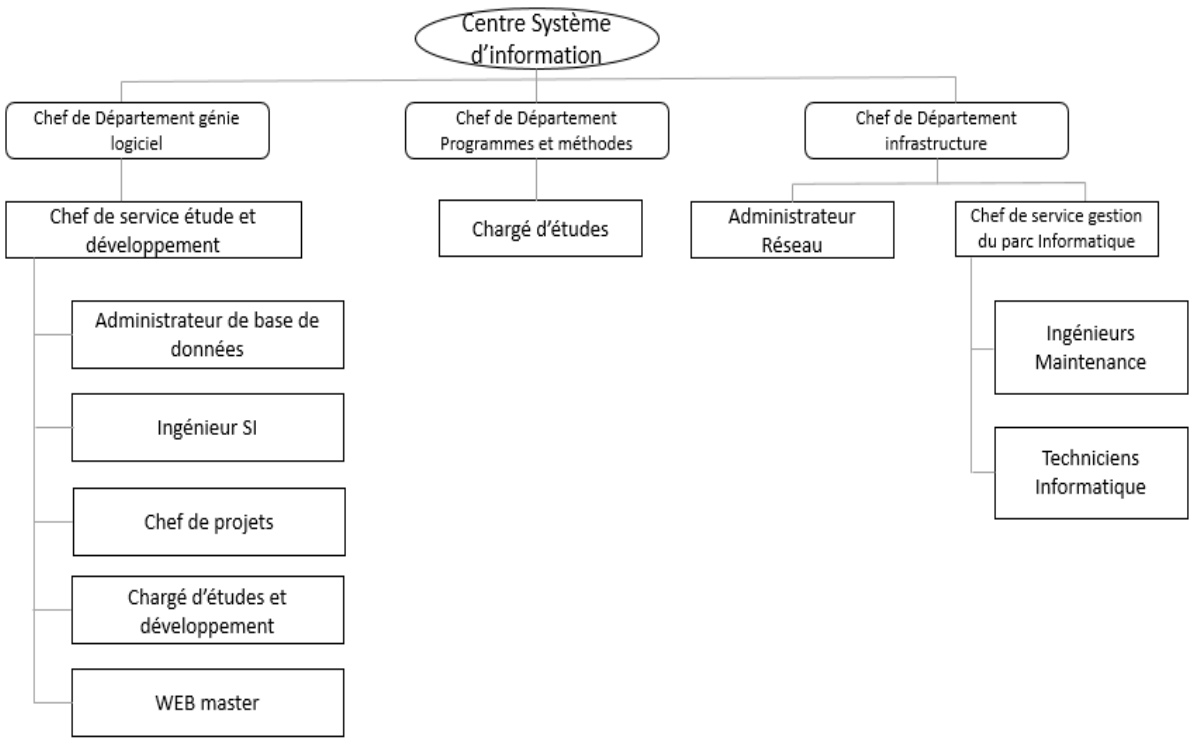

FIGURE 2.3 – l'organigramme de la structure informatique

2.4 L'infrastructure informatique

2.4.1 Le réseau informatique de l'EPB

Le réseau du port de Bejaia s'étend du port pétrolier (n°16) aux ports 13 et 16 (port à bois). La salle machine du réseau local de l'EPB contient principalement une armoire de brassage et une autre armoire optique de grande taille, éventuellement l'ensemble des serveurs, ces deux armoires servent à relier les différents sites de l'entreprise avec le département informatique par des fibres optiques de type 4, 6, 8 et 12 brins (voir figure 2.4). Chaque site a une armoire de brassage contenant un/des convertisseur(s) media, un/plusieurs Switch où sont reliés les différents équipements par des câbles informatiques.

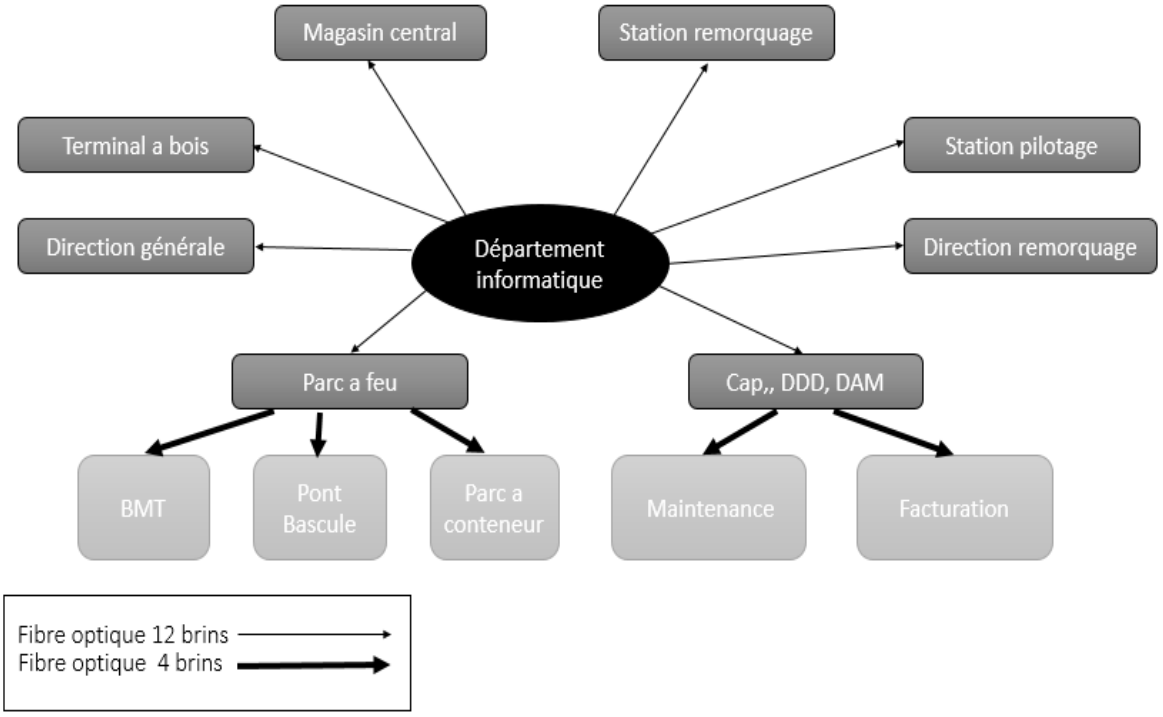

FIGURE 2.4 – réseau fibre optique de l'EPB

2.4.2 Presentation de l'architecture de l'EPB

Dans cette partie nous allons décrire les differents composants de l'architecture de l'EPB (figure 2.5)

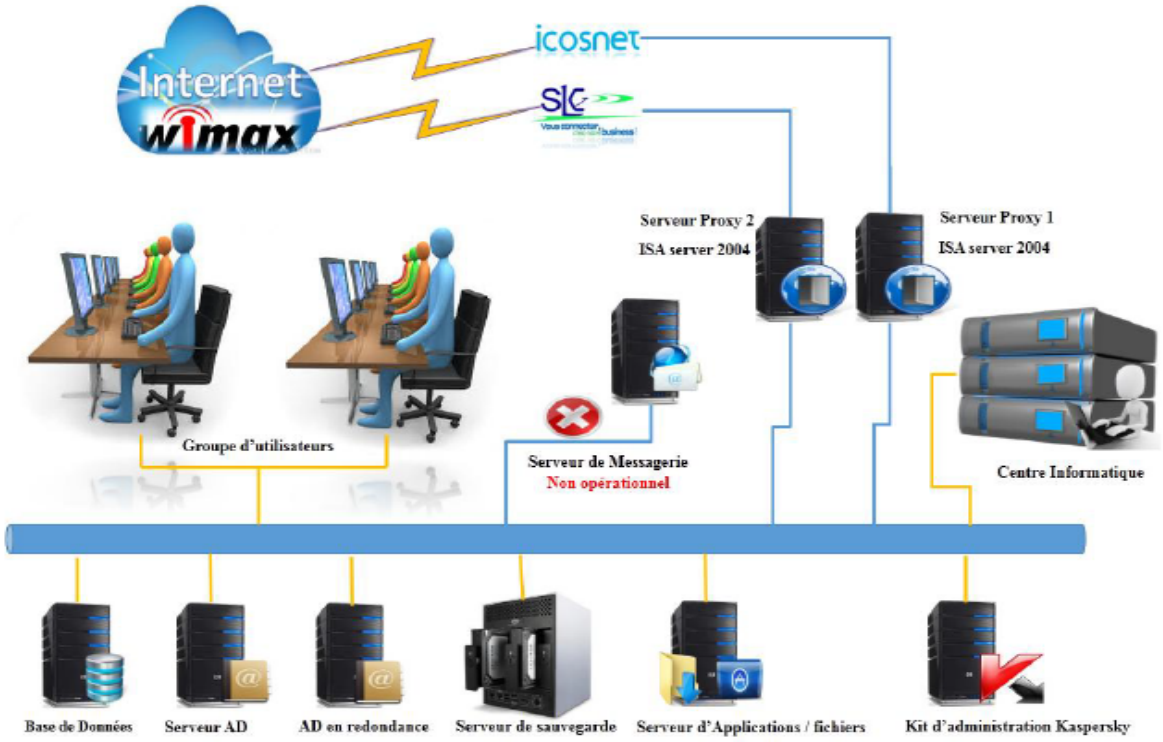

FIGURE 2.5 – Architecture de l'EPB

2.4.2.1 Etude de l'architecture

- **Connexion Internet** - L'entreprise portuaire de Bejaia s'est dotée de deux connexions Wimax à savoir icosnet et Algérie télécom. Ce type de connexions permet de se connecter à Internet haut débit grâce à une antenne outdoor qui communique par des ondes hertzienne via une station de base située au mont Gouraya, d'une très grande fiabilité permettant ainsi d'éviter l'usage du câble et le risque d'une panne physique par conséquent.

- **Sécurité** - La sécurité est assurée par deux serveurs Proxy qui agissent comme un filtre afin de définir les règles d'accès à un réseau comme Internet à cause des risques que peut représenter une connexion normal dans certain cas, d'une part et de deux pare-feu logiciels ISA server 2004 (Internet Security and Acceleration Server) pour appliquer les stratégies d'accès et les règles de routages déterminant la manière dont les clients accèdent à Internet.

- **Salle machine** - La salle machine est le coeur du réseau toutes les activités du port reposent sur cette salle, elle regroupe en un seul endroit les ressources nécessaires au bon fonctionnement du LAN, en plus des Switchs elle comporte les différentes machines serveurs :

  ✓ Serveur de base de données (SQL server 2003 and My SQL) : un serveur de base de données répond à des demandes de manipulation de données stockées dans une ou plusieurs base de

données. Il s'agit de demande de recherche, de tri, d'ajout, de modification ou de suppression de données. Ces données sont utilisées par des serveurs web et des utilisateurs.

- ✓ Serveur de contrôleur de domaine DC1 (Active Directory) : sous Windows Server 2003 l'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateur utilisant le système Windows. Il répertorie les éléments de ce réseau administré tel que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes...etc.
- ✓ Serveur de contrôleur de domaine redondant DC2 (Active Directory) : il permet de conserver des réplicas de données de l'annuaire sur un autre contrôleur de domaine, cela garantie la disponibilité et la continuité.
- ✓ Serveur application/fichier : c'est un serveur sur lequel sont installées les applications utilisées par les usagers. ces applications sont chargées sur le serveur d'application pour y accéder à distance. Un serveur d'application peut être un serveur qui centralise toutes les applications utilisées par les postes clients.
- ✓ Serveur de sauvegarde : il a pour rôle de sauvegarder en continue les données générées par l'entreprise. Si un employé efface par erreur un document, ou qu'il y a un dysfonctionnement d'un ordinateur, le serveur est en mesure de récupérer le fichier perdu.
- ✓ Kit d'administration Kaspersky : Kaspersky Administration Kit est un outil de gestion de protection contre les programmes malveillants dans une entreprise. Quelle que soit la taille de l'organisation, il permet de surveiller et de contrôler chaque aspect de l'infrastructure de sécurité. Kaspersky Administration Kit augmente le niveau de protection et réduit le coût total de propriété des produits de Kaspersky Lab. C'est la démarche de haute valeur adoptée par Kaspersky Lab.

2.4.2.2 Diagnostique de l'architecture de l'EPB

L'étude que nous avons menée sur l'architecture nous a permis de retirer des faiblesses réseaux et qui sont les suivantes.

Plateforme dépassée quant à l'utilisation de Windows serveur 2003

- Fin du support technique des mises à jour et le support des applications utilisées sur ces serveurs ne seront plus garanti.
- Explosion des coûts de maintenance de serveurs obsolètes à long terme.
- Arrêt des patchs de sécurité : le réseau et exposé aux failles de sécurité (pour rappel, 37 mises à jour critiques sur Windows serveur 2003 en 2013).
- Des risques potentiellement importants liés à la non-conformité avec les standards et les règlementations.

Pare-feu logiciels ne sont plus supportés ISA serveur 2004

- Protection obsolète contre les nouvelles menaces.
- fin de support produit 2009.
- Fonctionnalités limités et basique.
- Control de flux entrant et sortant restreint.

Technologie de stockage dépassés DAS

- dans le cadre d'un réseau d'entreprise on comprend vite les limitations induites par une architecture DAS.
- les périphériques de stockages sont gérés indépendamment les uns des autres, ce qui complique l'administration et la gestion de parc.
- Sauvegarde décentralisée et non sécurisée des données, et difficulté de gestion.

Plan d'adressage statique

- Un adressage par IP fixe du style 10.0.0.0/24, qui ne permettait que de connecter qu'un maximum de 254 machines, cette plage a atteint ses limites vu le nombre croissants de machines clientes au réseau de l'EPB, cet adressage ne permet pas une évolutivité du parc informatique de l'EPB, De ce fait, une nouvelle machine ne peut avoir d'adresse IP ni se connecter au réseau.

Un seul domaine de diffusion

- Un seul et unique domaine de diffusion ce qui implique une surcharge du réseau de l'entreprise, les machines communiquent sans cesse entre elles, le trafic réseaux devient lourd, ce qui ralenti nettement la communication sur le réseau et engendre une lourdeur mêmes sur les applications et machines clients.

Architecture plate

- Besoin de segmentation du réseau en plusieurs VLAN.
- Changements et Configuration des Switch au niveau des armoires pour mettre à niveau le réseau VLAN de l'entreprise.

Messagerie non opérationnelle

- L'EPB dispose d'une messagerie externe qui dépond entièrement d'Internet. Dans le cas de coupure de connexion Internet les utilisateurs ne pourront plus s'envoyer des e-mails.
- L'entreprise ne dispose pas de serveur de messagerie interne.
- Relais de messagerie ouvert, cependant il peut être utilisé pour envoyer ou recevoir des e-mails commerciaux non sollicités ou des Spams, également appelé courriers indésirables.

Absence des liaisons VPN

- manque de liaisons sécurisées entre les plates-formes extra-portuaires et le site principal de l'EPB.

Absence de serveurs en redondances pour assurer la tolérance aux pannes

- Pour assurer la disponibilité et la continuité des données et des ressources dans une entreprise un serveur en redondance est important.
- Le serveur en redondance prend en charge tous les services défectueux du premier serveur.

Aucun mécanisme de détection et de prévention d'intrusion.

La salle des serveurs non conforme avec le programme de management intégré.

2.4.2.3 Les objectifs du centre informatique

Afin d'assurer les besoins de l'entreprise il est nécessaire d'améliorer les performances du réseau, et pour cela il faudra passer en revue tous les aspects intervenant dans ce système, notamment :

1. Amélioration de la sécurité, de la disponibilité et des performances réseau.
2. Amélioration du câblage interne.
3. Amélioration du plan d'adressage IP.
4. Mise à niveau des systèmes d'exploitation.
5. Amélioration de la qualité du matériel (serveurs, commutateurs et hôtes).
6. Maitrise de l'impact des trafics générés par les serveurs d'authentification - des médias d'interconnexion.

1. **Amélioration de la sécurité, de la disponibilité et des performances réseau**
   Les performances d'un réseau dépendent de nombreux facteurs :
   - le débit pratique maximal du câblage, c'est à dire la quantité d'octets transmissible sur le câble par seconde. Plus le nombre d'octets par seconde est élevé, plus le réseau est performant. On dit que le réseau " s'effondre " quand plus aucune machine ne peut transmettre de message.
   - la quantité (petite ou élevée) de machines connectées au même segment.
   - le tunneling (VPN).
   - les cartes réseaux.

   Améliorer les performances d'un réseau informatique consiste donc à accélérer la transmission des données (le débit) ou à augmenter la capacité des supports de transmission tout en assurant l'intégrité des informations transmises.

   ♣ **Déploiement de firewalls pour contrôler le trafic réseau**
   - Éviter les intrusions grâce aux filtres.

- Mettre en oeuvre une stratégie de cyber sécurité.
- Déployer des firewalls PFsense.
- Surveillance du réseau en temps réel et génération de rapports journaliers.
- Equilibrage de la charge des connexions internet.
- Contrôle total des flux entrants et sortants.

♣ **Assurer la confidentialité du réseau et la Confidentialité des connexions externes**

- Observation illicite du réseau.
- Partitionnement pour éviter les pertes de données.
- Valider les entrées utilisateur (active directory).
- Contrôler la fuite d'informations en gérant les menaces provenant du réseau local (Sécurisation des communications avec IPSec, Confidentialité grâce au chiffrement).
- La segmentation et la virtualisation sont un atout pour les clients du système d'information, pour les exploitants et pour le management.
- Gérer la sécurité des serveurs, des applications, d'un système d'information complexe et évolutif.

♣ **Virtualiser les serveurs logiques dans les serveurs physiques**

- VMware, etc.
- Inutile de multiplier le nombre de serveurs physiques et leur maintenance.

2. **Amélioration du plan d'adressage IP**
   - Mise à niveau de l'adressage IP en mettant en oeuvre l'adressage dynamique et des adresses de classe B.
   - Segmentation du réseau en plusieurs domaines de diffusion.
3. **Mise à niveau des systèmes d'exploitation**

♣ **Mise à niveau des contrôleurs du domaine**

- Migration vers une nouvelle plateforme Active Directory (système et paramétrages réseaux) sur les deux contrôleurs.
- Création de sessions contrôlables organisées selon les organigrammes des structures de l'entreprise.
- Mise en place de règles de contrôle d'accès.
- Mise en place de stratégies de groupe.
- Gestion des partages.
- Paramétrages du deuxième contrôleur pour la tolérance aux pannes.

♣ **Mise en place d'un nouveau Serveur de BDD en redondance**

- Allocation des espaces disque et installation de l'ensemble des BDD de l'entreprise.

♣ **Mise à niveau des différents serveurs**

- Serveur d'application.
- Serveur de fichier.
- Serveur de sauvegarde.
- Deux serveurs d'accès Internet (Proxy).

4. **Amélioration de la qualité du matériel (serveurs, commutateurs et hôtes)**
   - Acquisition de nouveaux serveurs puissants et remplacement des anciens serveurs ne supportant plus.
   - Assurer la disponibilité et la tolérance aux pannes en mettant en place un serveur redondant pour chaque serveur.
   - Amélioration de la politique de stockage : Configuration des RAID pour une Meilleure gestion du stockage et garantir la disponibilité des données
   - Facilité de déploiement de nouvelles machines et optimisation de la consommation des ressources matérielles
   - Facilité de maintenance et d'accès aux données.
   - Réduction de la consommation d'énergie et meilleur gestion de l'espace...
   - Possibilités de test, de retour en arrière lors des configurations grâce aux snapshots.

2.4.3 Les améliorations apportées par l'EPB

- Migration de Windows serveur 2003 vers une nouvelle plate-forme Windows serveur 2012 R2 essentiellement pour les contrôleurs du domaine principal et secondaire, et vers une nouvelle plate-forme Windows serveur 2008 pour les autres serveurs.
- Mise en place de liaisons sécurisées VPN pour répondre aux besoins d'interconnexion de l'Entreprise Portuaire de Bejaia aux différents sites distants..
- Mise en place d'une console d'administration KVM et une autre console IDS qui permettent à l'administrateur réseau de faciliter la gestion des différents serveurs existants dans l'entreprise.
- Mise en place de deux zones démilitarisées DMZ publiques (serveur Web) et privé (antivirus, analyse, FTP, http, SMTP).
- L'ajout d'un serveur physique en redondance pour tous les serveurs logiques pour assurer la disponibilité des données.
- Mise à niveau du système d'adressage IP de classe A vers la classe B/22 avec le masque de sous réseau suivant : 255.255.252.0.
- Remplacer l'antivirus Kaspersky par ESET.
- Utilisation d'un environnement virtuel qui permet de faire fonctionner, en même temps, plusieurs systèmes d'exploitation et plusieurs applications sur la même plate-forme physique.

- Réaménagements de la salle des serveurs et la mettre en conformité avec le programme de management intégré.
- Mise en place d'une autorité de certification dans l'objectif de renforcer la sécurité du système.
- Mise en place de deux pare feux matériels.
- Mise en place d'un nouveau Serveur de BDD en redondance.
- Mise à niveau des différents serveurs, tels que serveur d'application, serveur de sauvegarde, serveur de fichier, et deux serveurs d'accès Internet.
- Amélioration de la connexion Internet en changeant la connexion WiMax par une autre connexion WiMax à meilleur débit.

Les améliorations vues précédemment effectuées par l'EPB ont donné l'architecture suivante (figure 2.6) :

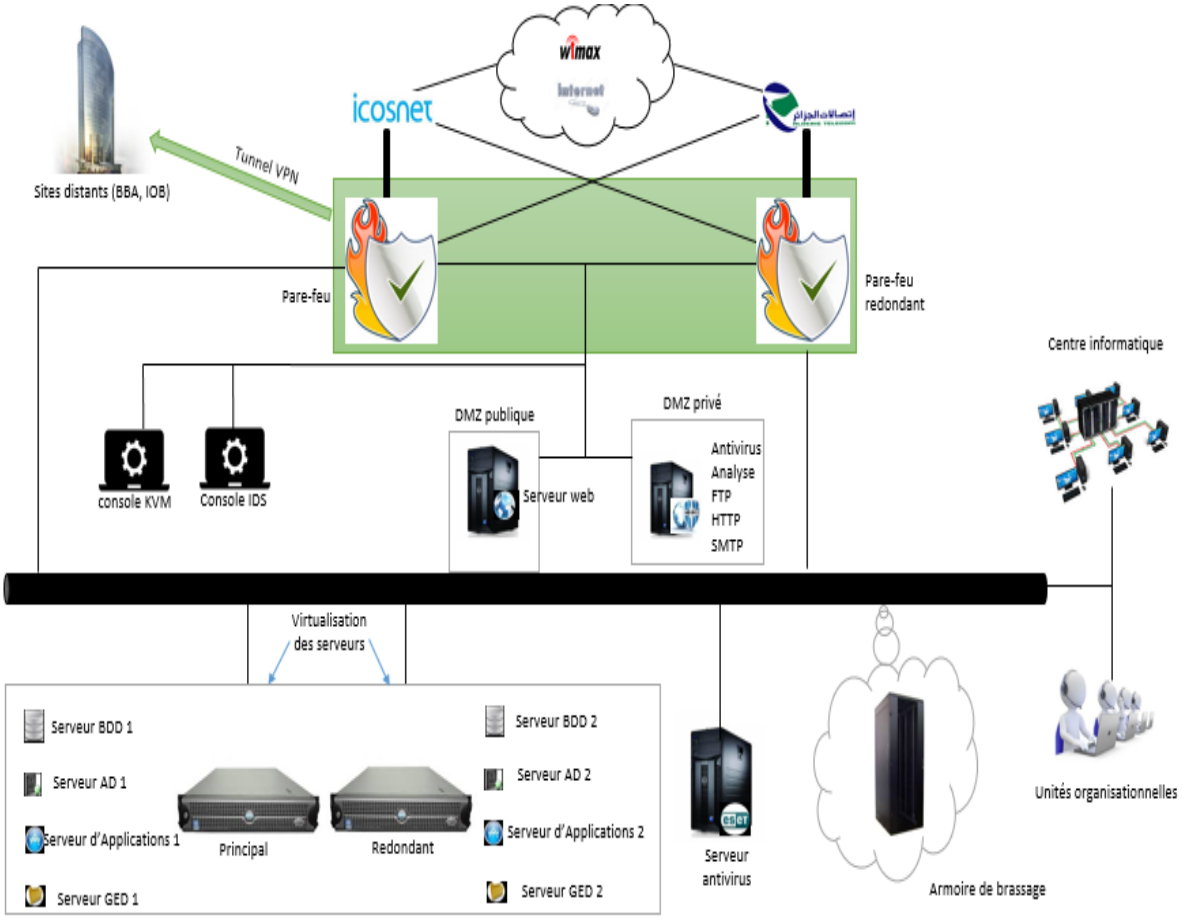

FIGURE 2.6 – l'architecture réseau de l'EPB

Cette architecture répond à la majorité des besoins exprimés et faiblisses recensées néanmoins certains points n'ont pas fait l'objet d'une amélioration d'où la nécessité de mise à niveau.

2.5 Contexte du projet à réaliser

Notre travail consiste à mettre en oeuvre d'autres améliorations à cette architecture pour un meilleur fonctionnement et pour assurer la continuité de quelques services.

2.5.1 Présentation du projet à réaliser

Le projet à réaliser s'intitule "Etude et amélioration de l'architecture réseau et sécurité de l'EPB". Apres avoir étudié les faiblesses et les améliorations effectuer à l'architecture réseau, nous allons pouvoir continuer le travail qui a déjà été initié auparavant en améliorant encore plus le fonctionnement du système et la sécurité du réseau de l'EPB.
La mise en oeuvre de ce projet permet d'apporter une amélioration au réseau de l'entreprise en mettant l'accent sur la réalisation d'un serveur de messagerie plus la configuration du relai SMTP, pour une meilleur gestion des mails des utilisateurs de l'entreprise tout en assurant la fluidité et la sécurité de la communication. et nous allons aussi amélioré quelques parties tel que la segmentation du réseau et la sécurité des systèmes.

2.5.2 Contraintes

Toute en respectant les objectifs, il est bien sur nécessaire d'assurer la continuité du service réseau et que les besoins des clients soient assurés, pendant et après la mise en oeuvre du projet. Les performances du réseau ne doivent pas non plus être altérées. En outre, les utilisateurs ne doivent pas s'apercevoir qu'un changement a été opéré sur leur réseau.

2.5.3 Cahier des charges

- Déploiement d'un serveur de messagerie exchange 2013, c'est un logiciel de groupware (travail collaboratif) de Microsoft pour serveur de messagerie électronique, il permet la gestion d'agendas, de contacts et de taches qui assurent le stockage des informations, il permet des accès à partir des clients mobiles tels qu'OMA (Outlook mobile Access) et de client web (navigateurs tel que : internet explorer, Mozilla, Firefox...). Il constitue une puissante plateforme de travail collaboratif [17]. En fait, le travail collaboratif permet d'assurer la cohérence des activités et la coordination des taches, en accord avec la politique globale de l'entreprise, pour cela il est doté d'outils qui permettent :
  - D'échanger des informations à l'intérieur d'un réseau de collaborateurs.
  - De partager des ressources dans un même contexte.
  - De travailler sur des documents en groupe et en temps réel.
- Configuration d'un relai SMTP : est un service qui est utilisé comme un moyen de transport de messages électroniques entre les différents serveurs. Il est principalement utilisé quand un e-mail doit être livré à un domaine différent du domaine de l'utilisateur. Le Service de relais

SMTP permet de filtrer les messages en bloquant le spam et les virus avant qu'ils n'atteignent les contacts externes et d'appliquer les paramètres de sécurité de messagerie.

- Utilisation des ACL (Access Control List) Une ACL est une liste séquentielle de critères utilisée pour du filtrage des paquets. Les ACLs sont capables d'autoriser ou d'interdire des paquets, que ce soit en entrée ou en sortie [18].
  - o Le filtrage se fait en fonction de certains critères (IP source, IP destination, port source, port destination, protocole,...).
  - Une ACL permet soit d'autoriser du trafic (permit) ou de le bloquer (deny).
  - Il est possible d'appliquer au maximum une ACL par interface et par sens (input/output).
  - Une ACL est analysé par l'IOS de manière séquentielle.
  - Dès qu'une règle correspond au trafic, l'action définie est appliquée, le reste de l'ACL n'est pas analysé.
  - Toute ACL par défaut bloque tout trafic. Donc tout trafic ne correspondant à aucune règle d'une ACL est rejeté.
- Utilisation des VLAN pour alléger et assurer la fluidité du réseau. L'assignation de groupes d'utilisateurs à des VLAN permet d'améliorer l'administration et la sécurité du réseau local entier. Ils permettent de réaliser les opérations suivantes :
  - Création de divisions logiques de groupes de travail.
  - Application de stratégies de sécurité différentes selon les groupes de travail.
  - Les VLAN réduisent la taille des domaines de diffusion et améliorent ainsi l'efficacité du réseau.
- Utilisation d'un serveur LMS (LAN Management Solution) est constitué d'une suite de composants logiciels spécifiquement conçu pour augmenter l'efficacité opérationnelle des équipements dans de nombreux domaine d'administration [19] :
  - Gestion de parc matériel.
  - Gestion des systèmes d'exploitation.
  - Surveillance du bon fonctionnement des équipements (alerte en cas de défaillance).
  - Sauvegarde et historisation des configurations...etc.
- Mise en place de deux serveur IDS (Intrusion Detection System) et IPS (Intrusion Prevention System) pour surveiller le trafic transitant dans le réseau [20].
  - IDS : Comme son nom l'indique, un système de détection d'intrusion permet de détecter différentes tentatives d'intrusion et ce en se basant sur une base de signatures des attaques connues.
  - IPS : La différence principale entre un IDS et un IPS, est que le système de prévention ne se contente pas de détecter les intrusions, mais se charge, en plus, de les stopper.

- Intégration de la technologie en RAID (Redundation Array of Inexpensive Disks), permet de construire une unité de stockage à partir de plusieurs disques durs. Unité ainsi créé appelée (grappe) a donc une grande tolérance aux pannes (haute disponibilité), ou bien une plus grande capacité (vitesse d'écriture). La répartition des données sur plusieurs disques durs permet donc d'en augmenter la sécurité et fiabiliser les services associes [21]. Les disques assemblés selon la technologie RAID peuvent être utilisés de différentes façon, appelées niveaux RAID. Chacun de ces niveaux constitue un mode d'utilisation de la grappe, en fonction des performances, du cout et des accès disques :
  - Niveau 0 : le niveau RAID-0 appelé stripping consiste à stocker les donnes en les répartissant sur l'ensemble des disques de la grappe. De cette façon il ne y'aura pas de redondance. En effet en cas de défaillance de l'un des disques, l'intégrité des données reparties sur les disques sera perdue.
  - Niveau 1 : il a pour but de dupliquer l'information à stocker sur plusieurs disques cette technologie est appelée mirroring, elle permet d'assurer une plus grande sécurité des données, car si l'un des disques tombe en panne les données sont sauvegardées sur l'autre, d'autre part, la lecture peut être beaucoup plus rapide lorsque les deux disques sont en fonctionnement. En contre partie cette technologie est très onéreuse étant donné que seule la moitié de la capacité de stockage n'est effectivement utilisée.
  - Niveau 2 : le niveau RAID-2 est désormais obsolète, car il propose un contrôle d'erreur par code de Hamming (code ECC- Erorr Correction Code), or ce dernier est désormais directement intégré dans les contrôleurs de disques durs. Cette technologie consiste à stocker les données selon le même principe qu'avec RAID-0 mais en écrivant sur une unité distincte les bits de contrôle ECC, généralement 3 disques ECC sont utilisés pour 4 disques de données. Cette technologie offre de piètre performance mais un niveau de sécurité élevé.
  - Niveau 3 : le niveau 3 propose de stocker les données sous formes d'octets sur chaque disque et de dédier un des disques au stockage de bit de parité. De cette manière, si l'un des disques venait à défaillir, il sera possible de reconstituer l'information à partir des autres disques. Apres la reconstitution le contenu du disque défaillant est de nouveau intégré. Par contre, si deux disques venaient à tomber en pannes simultanément, il serait alors impossible de remédier à la perte de données.
  - Niveau 4 : le niveau 4 est très proches du niveau 3, la différence se trouve au niveau de la parité, qui est faite sur un secteur (appelé bloc) et non au niveau du bit, et qui est stockée sur un disque dédié. C'est-à-dire plus précisément que la valeur du facteur d'entrelacement est différente par rapport au RAID-3.
  - Niveau 5 : le niveau 5 est similaire au niveau 4, c'est-à-dire que la parité est calculée au niveau d'un secteur, mais repartie sur l'ensemble des disques de la grappe. De cette façon, il améliore grandement l'accès aux données car l'accès aux bits est reparti sur les différents disques de la grappe.

- Niveau 6 : il définit l'utilisation de deux fonctions de parité, et donc leur stockage sur deux disques dédiés. Ce niveau permet aussi d'assurer la redondance en cas d'avarie simultanée de deux disques. Cela signifie qu'il faut au moins 4 disques pour mettre en oeuvre un système RAID-6.

- Mise en place d'un outil de sécurité EMET (Enhanced Mitigation Experience Toolkit) pour empêcher l'exploitation des vulnérabilités logicielles de Windows (serveur ou client).

2.5.4 Architecture proposée pour le réseau de l'EPB

Nous pouvons regrouper les améliorations proposées dans l'architecture suivante (voir figure 2.7).

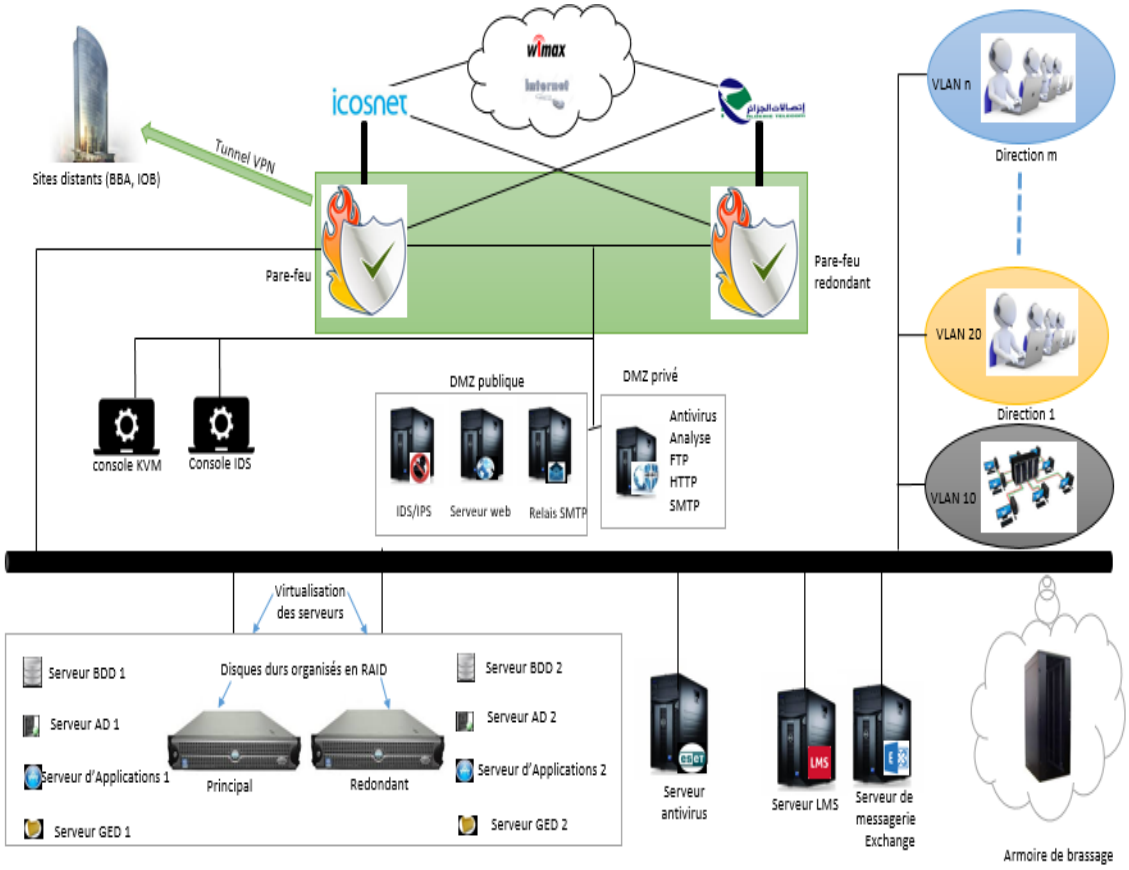

FIGURE 2.7 – architecture proposée pour le réseau de l'EPB

2.6 Conclusion

L'étude de l'existant nous a permis de se familiariser avec le réseau actuel de l'EPB, et de comprendre l'utilité de chaque détail profondément, et c'est ce qui nous a permis de voir les lacunes et les faiblesses du réseau. L'étude de ces lacunes nous a conduits à proposer une solution pour palier à ses dernières. Apres avoir choisi la solution à adopter nous avons tracé nos objectifs ensuite nous avons défini un plan de travail pour mettre en oeuvre cette solution. La prochaine partie va être réservée à la description et à la réalisation de quelques étapes citées précédemment, à savoir l'installation du matériel et des logiciels ainsi que les configurations appropriées.

CHAPITRE 3

MISE EN OEUVRE DE LA SOLUTION

3.1 Introduction

Ce chapitre est consacré à l'amélioration de l'architecture réseau de l'EPB, nous allons définir les différents outils que nous utiliserons ainsi que les installations et les configurations requises, où nous allons citer les différentes étapes à suivre pour la mise en oeuvre de la solution proposée dans le chapitre deux.

3.2 Mise en place de la messagerie électronique

La messagerie électronique est un moyen de communication différé ou asynchrone entre utilisateurs d'un réseau informatique. Différé car contrairement à la messagerie instantanée (le Chat), le récepteur du message n'est pas censé répondre immédiatement à l'émetteur et vice-versa. La messagerie électronique a été le second service après l'émulation de terminal (Telnet) et le FTP à connaitre un développement avant même le service Web. Aujourd'hui encore ce service est très utilisé par les entreprises et les particuliers.

- **Fonctionnement du courrier électronique**
  Le fonctionnement du courrier électronique est basé sur l'utilisation d'une boîte aux lettres électronique. Lors de l'envoi d'un email, le message est acheminé de serveur en serveur jusqu'au serveur de messagerie du destinataire. Plus exactement, le message est envoyé au serveur de courrier électronique chargé du transport (nommé MTA pour Mail Transport Agent), jusqu'au MTA du destinataire cela en utilisant une recherche DNS de type MX du domaine de destinataire (voir figure 3.1) [22]. Sur internet, les MTA communiquent entre eux grâce au protocole SMTP et sont logiquement appelés serveurs SMTP (parfois serveur de courrier sortant).
  Le serveur MTA du destinataire délivre alors le courrier au serveur de courrier électronique en-

trant (nommé MDA pour Mail Delivery Agent), qui stocke alors le courrier en attendant que l'utilisateur vienne le relever. Il existe deux principaux protocoles permettant de relever le courrier sur un MDA :

- Le protocole POP3 (Post Office Protocol), le plus ancien, permettant de relever son courrier et éventuellement d'en laisser une copie sur le serveur.
- Le protocole IMAP (Internet Message Access Protocol), permettant une synchronisation de l'état des courriers (lu, supprimé, déplacé) entre plusieurs clients de messagerie. Avec le protocole IMAP une copie de tous les messages est conservée sur le serveur afin de pouvoir assurer la synchronisation.

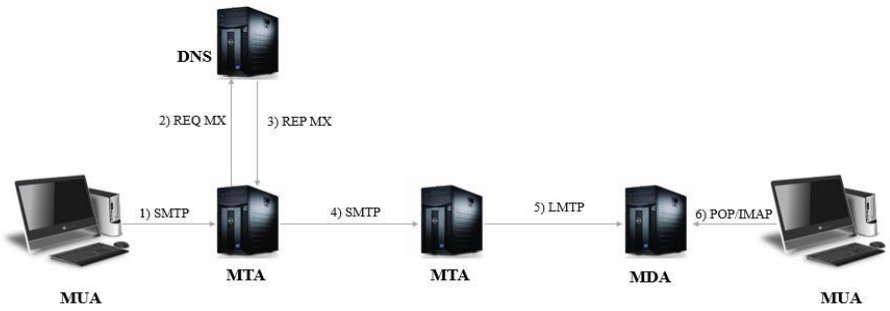

FIGURE 3.1 – Acheminement des e-mails

Par analogie avec le monde réel, les MTA font office de bureau de poste (centre de tri et facteur assurant le transport), tandis que les MDA font office de boîte aux lettres, afin de stocker les messages (dans la limite de leur capacité en volume), jusqu'à ce que les destinataires relèvent leur boîte. Ceci signifie notamment qu'il n'est pas nécessaire que le destinataire soit connecté pour pouvoir lui envoyer du courrier. Pour éviter que chacun puisse consulter le courrier des autres utilisateurs, l'accès au MDA est protégé par un nom d'utilisateur et un mot de passe.
La relève du courrier se fait grâce à un logiciel appelé MUA (Mail User Agent). Lorsque le MUA est installé sur le système de l'utilisateur, on parle de client de messagerie (par exemple Mozilla Thunderbird, Microsoft Outlook, Eudora Mail, Incredimail ou Lotus Notes). Lorsqu'il s'agit d'une interface web permettant de s'interfacer au serveur de courrier entrant, on parle alors de Webmail.

- **Relais SMTP**

  Le relais permet de transférer des messages depuis le domaine interne vers des domaines externe ou vice versa. Il existe deux cas d'utilisations de relais SMTP soit un relais interne dans le cas où l'entreprise choisit d'internalisé son relais ou externe dans le cas où il est en externe sur le provider ou le fournisseur d'accès, donc il n'est pas au niveau de l'entreprise (voir figure 3.2) [23].

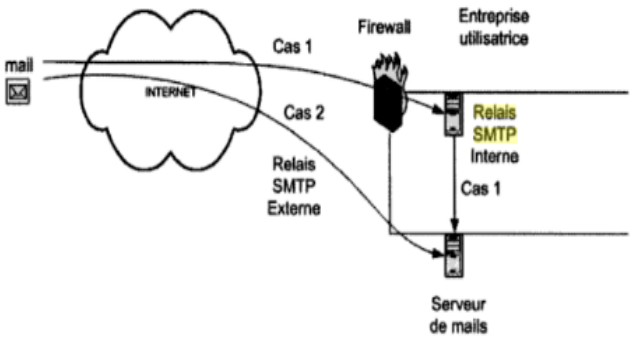

FIGURE 3.2 – Différents cas du relais SMTP

- **Modes de relayage SMTP**
  Le relayage n'a de répercussions que sur l'envoi d'e-mails, il n'influence aucunement la façon dont le courrier est reçu sur le serveur. Il existe trois modes de relayage :

  - Relais ouvert, ou open Relay, est un serveur de messagerie qui accepte le courrier en provenance de n'importe qui, et à destination de n'importe quelle adresse. De tels relais sont souvent utilisés par les spammeurs pour transmettre leur spams. Il faut donc absolument éviter que son propre serveur se comporte en relais ouvert. Sans cela, il serait rapidement utilisé pour transmettre du pourriel, et risquerait de finir sur des listes de blocage, puis de voir tout son courrier sortant refuser par les autres serveurs de l'Internet. Donc il faudra refuser tout le courrier reçu de l'extérieur à destination de l'extérieur, pour éviter d'être un relais ouvert de pourriel.
  - Relais fermé : ce mode de relayage permet uniquement l'envoi et la réception d'e-mails localement (depuis et vers des domaines hébergés sur le serveur). L'unique exception concerne les hôtes figurant dans la Liste blanche et signalés comme bénéficiant d'une autorisation.
  - Relais avec autorisation : ce mode de relayage permet à n'importe quel ordinateur hôte d'utiliser les services de messagerie d'un domaine sur le serveur à condition que les utilisateurs de la messagerie utilisent les bons noms de login et mot de passe pour s'authentifier.

  Afin qu'un relais ne sois pas ouvert il doit être sécurisé et configuré pour accepter et transmettre uniquement les messages suivants :

  - Messages à partir d'adresses IP locales à des boîtes aux lettres locales.
  - Messages à partir d'adresses IP locales à des boîtes aux lettres non-locales.
  - Messages à partir d'adresses IP non locales à des boîtes aux lettres locales.
  - Messages de clients qui sont authentifiés et autorisés.

3.2.1 Présentation de Windows serveur 2012

Windows Server 2012 R2 est le résultat de toute l'expérience de Microsoft dans la fourniture de services dans le Cloud à l'échelle mondiale. Il représente à la fois un serveur de haut niveau pour les entreprises et une plateforme dans le Cloud. Il permet d'optimiser les performances pour les scénarios les plus stratégiques et protège contre des ruptures de services par l'utilisation d'options de récupération très fiables. Il réduit la complexité et les coûts grâce à une automatisation complète et à des solutions de virtualisation du réseau et du stockage sur du matériel standard. Enfin, il permet aux utilisateurs un accès à distance de n'importe où, à partir de n'importe quel appareil, tout en protégeant les informations de l'entreprise [24].
La gamme de produits Windows Server 2012 a été simplifiée afin de choisir plus facilement l'édition qui convient le mieux :

- Édition Datacenter pour les environnements de Clouds privés fortement virtualisés.
- Édition Standard pour les environnements peu ou pas virtualisés.
- Édition Essentials pour les petites entreprises comptant jusqu'à 25 utilisateurs, avec un serveur à 1 ou 2 processeurs.
- Édition Foundation pour les petites entreprises comptant jusqu'à 15 utilisateurs avec un serveur monoprocesseur.

Dans notre cas nous avons utilisé l'édition standard car c'est la mieux adaptée à notre environnement.

3.2.2 Présentation et configuration du serveur Active Directory

3.2.2.1 Définition de l'Active Directory

Active Directory est le service d'annuaire de la famille Windows Server 2012. C'est un service réseau qui identifie toutes les ressources d'un réseau et met ces informations à la disposition des utilisateurs ainsi que des applications. Les services d'annuaires sont importants, car ils fournissent un moyen cohérent de nommer, décrire, localiser, administrer et sécuriser les informations relatives à ces ressources et d'y accéder. Lorsqu'un utilisateur recherche un dossier partagé sur le réseau, le service d'annuaire identifie la ressource et fournit l'information à l'utilisateur [25].

3.2.2.2 les composants de l'Active Directory

Active directory se compose de plusieurs services dont [26] :

- **Active Directory Certificate Services (AD CS)** Ces services fournissent les fonctions nécessaires pour émettre et révoquer les certificats numériques des utilisateurs, des ordinateurs clients et des serveurs.
- **Active Directory Domain Services (AD DS)** Ces services AD DS procurent les services d'annuaire essentiels à l'établissement d'un domaine.

- **Active Directory Federation Services (AD FS)** Ces services AD FS complètent les fonctionnalités d'authentification et de gestion d'accès des Services AD DS en les développant pour le World Wide Web.
- **Active Directory Lightweight Directory Services (AD LDS)** Ces services AD LDS fournissent un magasin de données pour les applications fonctionnant avec l'annuaire qui ne nécessitent pas les Services AD DS et qui n'ont pas besoin d'être déployées sur des contrôleurs de domaine.
- **Active Directory Rights Management Services (AD RMS)** Ces services AD RMS procurent une couche destinée à protéger les informations d'une organisation et qui peut s'étendre hors de l'entreprise, protégeant ainsi les messages électroniques, les documents et les pages Web de l'intranet, contre tout accès non autorisé.

3.2.2.3 Utilisateurs et groupes dans active directory

Chaque utilisateur dans l'AD est associé à un objet. Cet objet contient plusieurs attributs qui décrivent l'utilisateur (nom, prénom, login, adresse e-mail, téléphone, département... Etc.), lorsque le nombre d'utilisateurs augmente, nous pouvons les gérer par groupe.
Il existe deux types de groupes. Le premier est le groupe de sécurité. Ce type permet de gérer la sécurité pour l'accès et l'utilisation des ressources du réseau. Le deuxième type est le groupe de distribution. Ce type permet de gérer des listes de distribution d'e-mails dans un serveur de messagerie (Exchange).

3.2.2.4 Sites et domaines dans active directory

Dans la conception d'AD, Microsoft a tenté d'être le plus proche possible de la structure d'une entreprise. La structure d'une entreprise se compose de deux parties distinctes : physique et logique. Physique par son organisation géographique en différents sites et logique par sa hiérarchie.

- Sites : un site désigne la combinaison d'un ou plusieurs sous-réseaux IP. Bien souvent, nous attribuons un sous-réseau IP à un site physique d'une entreprise. Cela permet de désigner les postes sur le réseau de l'entreprise.

- Domaine : contrairement à un site, il représente la structure logique de l'organisation. C'est à dire bien souvent la hiérarchie. Le domaine n'a aucun lien avec le réseau IP : c'est un ensemble d'ordinateurs et d'utilisateurs partageant le même annuaire.
  L'espace de nommage est réalisé grâce au système DNS. Un domaine peut avoir plusieurs sous-domaines : nous créons ainsi une arborescence, le séparateur est le point. Si l'on souhaite par exemple créer un sous domaine Des (directions générales adjointes) dans un domaine existant PORTDEBEJAIA.AD, alors le domaine se nommera DGA. PORTDEBEJAIA.AD.

3.2.2.5 Arborescences et forets dans active directory

Une arborescence est une notion qui découle du système DNS et des domaines AD. Comme nous l'avons vu précédemment, il est possible de créer des sous-domaines dans des domaines. Le sous-domaine DGA fait partie du domaine PORTDEBEJAIA.AD et portera donc le nom DGA.PORTDEBEJAIA.AD. Cette notion d'arborescence est différente de celle de forêt. Une forêt peut comprendre plusieurs arborescences. La forêt PORTDEBEJAIA.AD présentée ci-dessous (voir aussi figure 3.3) comporte quatre arborescences :
De PORDEBEJAIA.AD a DGA.PORTDEBEJAIA.AD ;
De : PORTDEBEJAIA.AD à DFC.PORTDEBEJAIA.AD ;
De : PORTDEBEJAIA.AD à MKT.DGA. PORTDEBEJAIA.AD ;
MKT pour département marketing
DFC pour direction finances et comptabilité
DGA pour direction générale adjointe

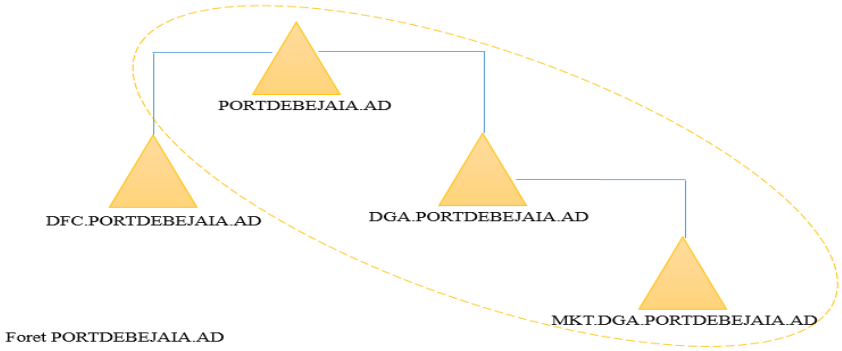

FIGURE 3.3 – Exemple de foret " foret POTDEBEJAIA "

Les arborescences de même forêt peuvent partager des ressources et des fonctions administratives.

3.2.2.6 Unités d'organisation d'active directory

C'est un conteneur utilisé à l'intérieur du domaine. Les UO sont des conteneurs logiques dans lesquels les utilisateurs, des groupes, des ordinateurs et d'autres UO sont placés. Elles ne peuvent contenir que des objets de leur domaines parent.

3.2.2.7 Relations d'approbations dans ative diectory

C'est un mécanisme permettant à un utilisateur d'un domaine d'accéder aux ressources d'un autre domaine, et à un administrateur de pouvoir gérer les utilisateurs de l'autre domaine. En se basant sur la direction et la transitivité.

3.2.2.8 Configuration d'Active Directory

La première étape consiste à configurer le nom de la machine et l'@ IPv4 du serveur local

- Le nom de la machine est SRVDC01 (figure 3.4).
- L'adresse IPv4 c'est une adresse statique de classe A : 10.0.0.5 (figure 3.4)

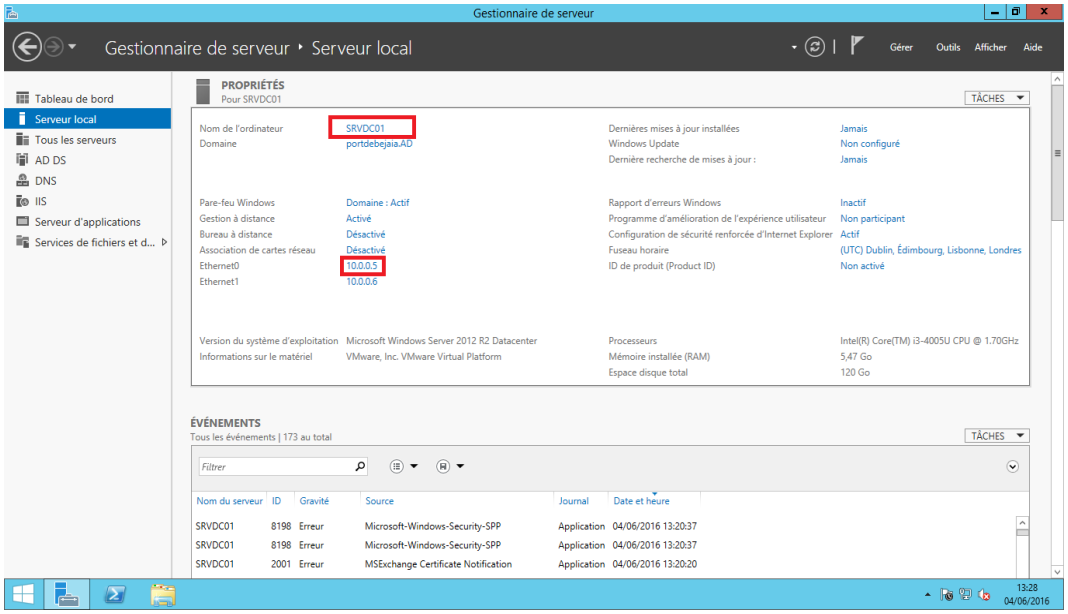

FIGURE 3.4 – Configuration du serveur local

La deuxième étape comprend l'ajout du rôle d'Active Directory au serveur local (voir figure 3.5), pour cela nous allons :

- Depuis le gestionnaire de serveur, cliquer sur ajouter des rôles et fonctionnalités.
- Sélectionner le type d'installation " installation basée sur un rôle ou fonctionnalité ".
- Notre serveur et le seul du réseau, le choisir dans le pool de serveurs.
- Cocher le rôle service AD DS (Active Directory Domain Service).

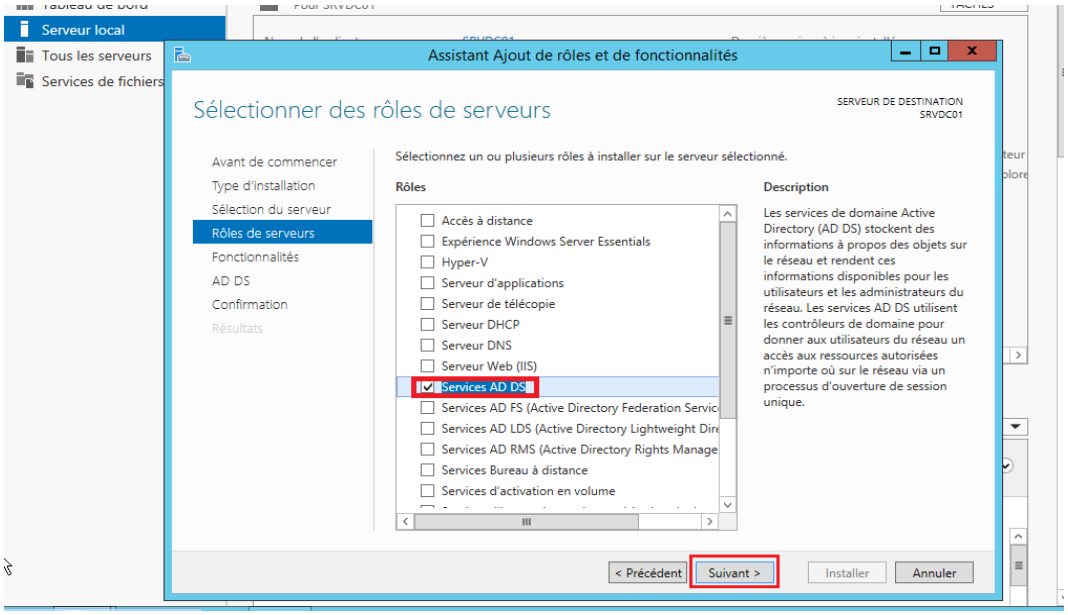

FIGURE 3.5 – l'ajout du rôle AD DS

Apres l'installation d' Active Directory Domain Service, le système va redémarrer automatiquement. Dans la troisième étape figure 3.6, nous devons promouvoir ce serveur en tant que contrôleur de domaine sinon le domaine ne sera pas créé.

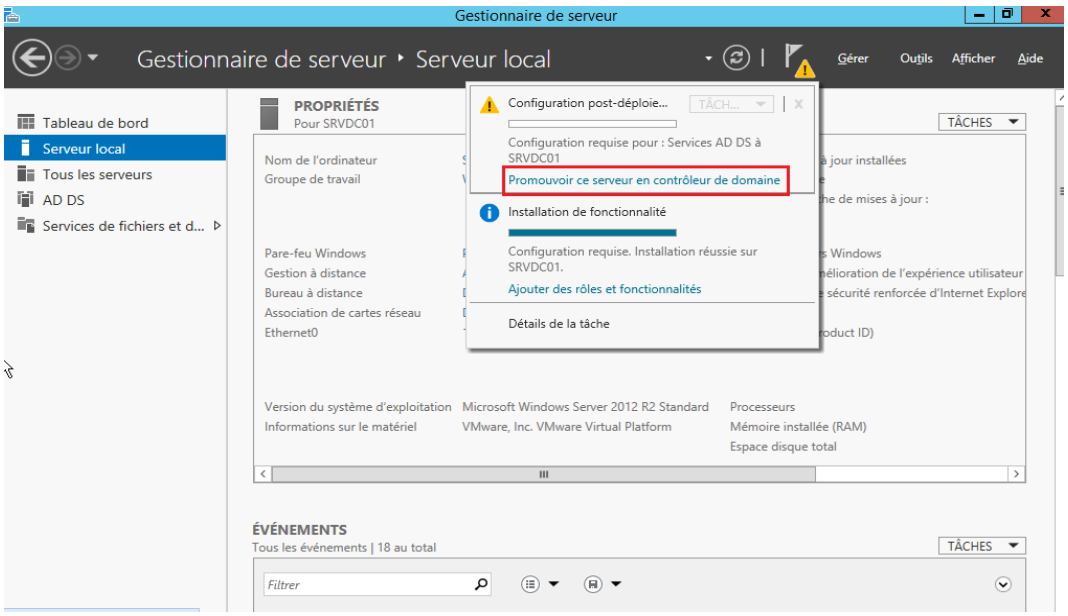

FIGURE 3.6 – Promouvoir le serveur en contrôleur de domaine

Apres avoir cliqué sur " promouvoir ce serveur en contrôleur de domaine ", dans la figure 3.7 l'assistant nous demande de créer une nouvelle forêt sous le nom "portdebejaia.AD "

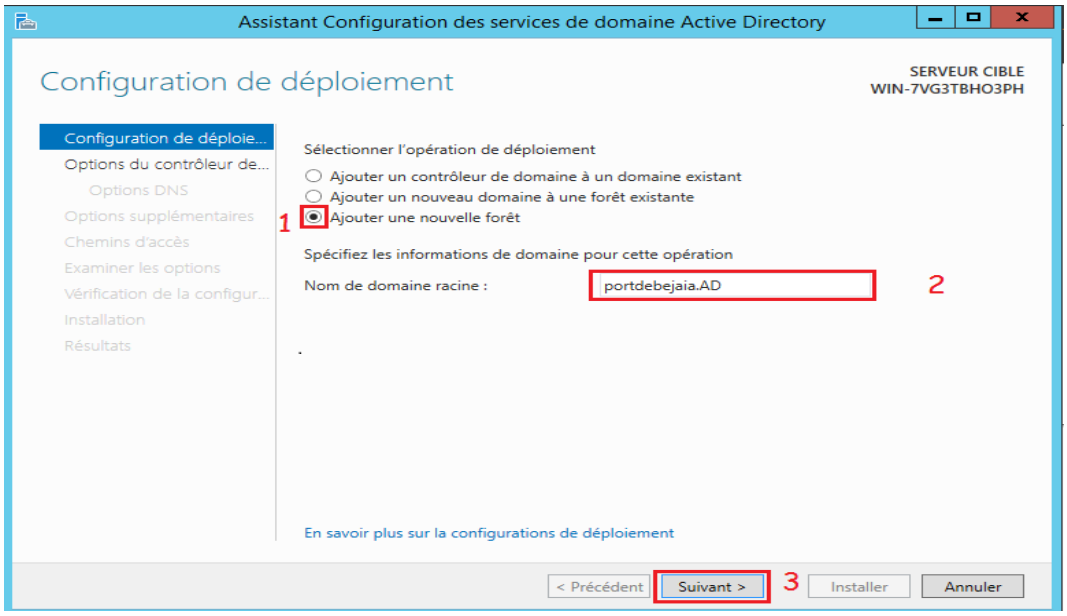

FIGURE 3.7 – Ajout d'une nouvelle forêt

Lorsque la forêt et le domaine seront créés, le niveau fonctionnel de la nouvelle forêt est sélectionné par défaut, et nous laissons cocher l'ajout de la fonctionnalité du serveur DNS. Puis insérer le mot de passe du mode de restauration du service d'annuaire (DSRM) (figure 3.8).

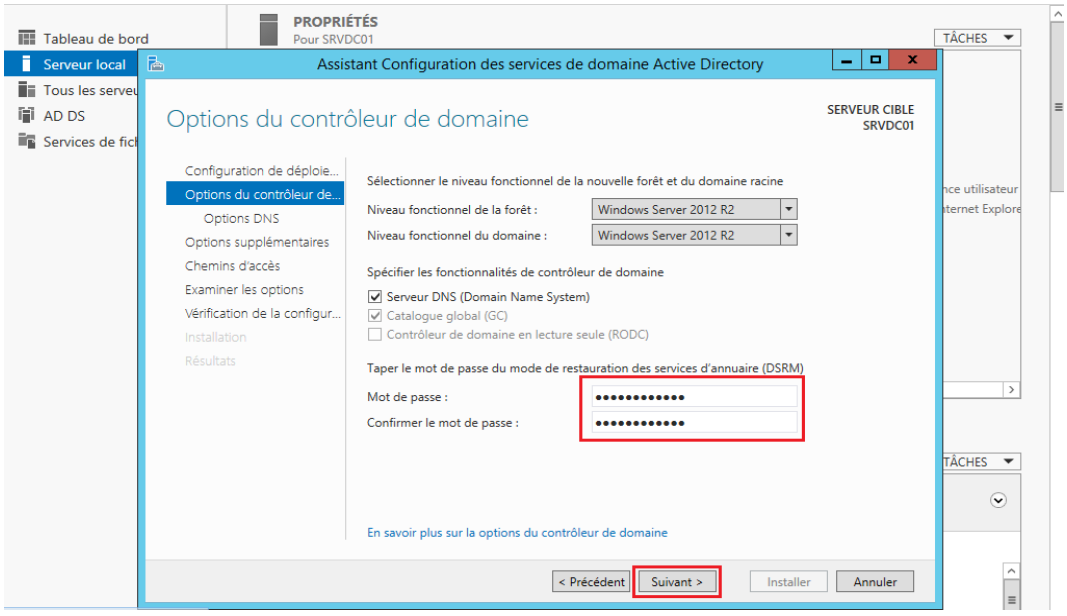

FIGURE 3.8 – Options de contrôleur de domaine

Une erreur apparait sur l'écran suivant, ce message survient car aucun serveur DNS n'est installé sur la machine, nous cliquons simplement sur suivant pour le créer automatiquement, car c'est grâce à lui que les clients (postes utilisateurs ou serveurs membres du domaine) vont pouvoir trouver le(s) serveur(s) AD.

- Indiquer un nom NetBIOS au domaine " PORTDEBEJAIA ".
- Laisser les valeurs suivantes par défaut (NTDS et SYSVOL).
- L'installation est prête et un récapitulatif est affiché dans la figure 3.9 pour vérifier la configuration.

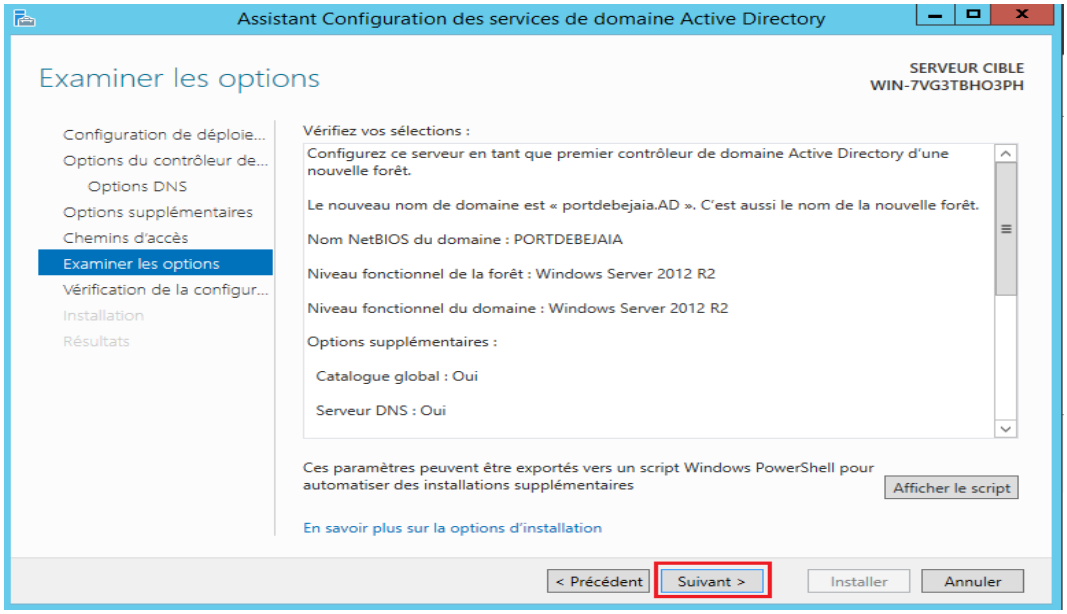

FIGURE 3.9 – Examiner les options

Après configuration le serveur redémarre automatiquement, à présent, les outils de gestion d'active directory sont présents dans le menu outils, notre domaine est créé et l'ouverture de session se fait avec le compte administrateur du domaine " portdebejaia/Administrateur ".

3.2.3 Présentation et installation d'exchange 2013

3.2.3.1 Présentation d'exchange

Microsoft Exchange (existe en deux versions, standard et entreprise) est un logiciel serveur de messagerie très utilisé dans le monde entier par de nombreuses entreprises et organisations. La multiplication des plateformes Exchange dans le monde entier est due à la popularité croissante du "Hosted Exchange " dans le " Cloud " à bas prix (société OVH par exemple). Il a été important de définir qu'il est préférable d'utiliser la version d'Exchange 2013 par rapport aux versions précédentes pour les raisons suivantes [27] :

- Nombre de rôles moindres.
- Outlook WebApp optimisée pour Smartphones, tablettes, PCs.
- Protection contre la perte de données sensibles (DLP) grâce à une analyse de contenus.

Microsoft Exchange 2013 est disponible en deux versions : Standard et Entreprise.

3.2.3.2 Rôles dans Exchange 2013

Exchange 2013 ne possède que 2 rôles. Pour des raisons de sécurité notamment, il est conseillé de séparer les différents rôles fournis par Exchange sur deux serveurs différents. Exchange 2013, contrairement à ses prédécesseurs, ne possède plus que 2 grands rôles au lieu de 5 [27] : Client Access Server (CAS) et Mailbox Server (MBX).

- **Client Access Server rôle** Comme son nom l'indique, ce rôle sert d'intermédiaire entre le client et le Mailbox Server lors d'une connexion avec Outlook, OWA etc...
  - Il est responsable d'authentifier et de fournir une connexion sécurisée SSL.
  - Il est responsable de rediriger et de router les différentes requêtes vers le bon Mailbox Serveur contenant la boîte mail de l'utilisateur.
  - Il offre également de différents protocoles tels que le POP, SMTP, IMAP, RPC over HTTPS.

  Il assure ces différents services :
  - Client Access Service : gère les connexions entre les clients et la boîte mail.
  - Front End Transport Service : il assure le filtrage des mails et le routage des mails entre les serveurs Exchange et les serveurs externes.
  - AutoDiscovery : Permet de configurer le client de messagerie (Outlook 2007 et plus) automatiquement.
- **Mailbox Server** Ce rôle permet au serveur Exchange de :
  - Stocker la base de données concernant les boîtes mails des clients.
  - Stocker les dossiers publics.
  - il est Responsable du stockage et du traitement des données.
  - le Service Hub Transport permet le routage des mails dans l'organisation et la connexion entre le Front End Transport Service et le Mailbox Transport Service.
  - le Service Mailbox Transport assure la connexion entre le Hub Transport Service et les bases de données de mails.

  Aucune connexion n'a lieu entre un client mail (Outlook, OWA...) et ce serveur et il ne doit pas être accessible depuis l'extérieur ou l'intérieur (excepté le CAS). Ce rôle est étroitement lié avec Active Directory, le Client Access Server et la base de données des boîtes mails. Ce rôle peut également bénéficier d'une redondance en ayant plusieurs Mailbox Server formant un Database Availability Group (DAG).

3.2.3.3 Installation et configuration d'exchange

Pour installer Exchange 2013 nous avons besoin des prérequis matériels et logiciels

1. **Prérequis matériel**
   - Processeur : serveur basé sur une architecture x64 équipé d'un processeur Intel.
   - Mémoire : Minimum 8 Go pour les rôles " Boîte aux lettres " et " Accès au client " combinés.
   - Espace disque : Minimum de 40 Go.
2. **Prérequis logiciels**
   - Plateforme de virtualisation : nous avons utilisé VMware comme plate-forme de virtualisation.
   - Serveur : Windows serveur 2012 R2.
   - Outils et fonctionnalités Windows : Active Directory, IIS et DNS.
   - Installation des prérequis pour les rôles Mail box et client Access.
   - Unified Communications Managed API 4.0 Runtime.
   - Microsoft Office 2010 Filter Packs 64 bits.
   - Service Pack 1 for Microsoft Office Filter Pack 2010 (KB2460041) 64-bit Edition.
3. **Installation**

   Dans la première partie nous avons pu installer et configurer Windows serveur 2012 et Active Directory, nous allons maintenant pouvoir commencer l'installation des prérequis pour Mail box et client Access. Pour l'installation des rôles Mail box et client Access, nous allons ouvrir Power Shell en mode administrateur et y ajouter ces lignes (voir figure 3.10) :
   - Install-WindowsFeature RSAT-ADDS
   - Install-WindowsFeature AS-HTTP-Activation, Desktop-Experience,NET-Framework-45-Features, RPC-over-HTTP-proxy, RSAT-Clustering,Web-Mgmt-Console, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth,Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression,Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracin,Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase,Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor,Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation
   - Add-WindowsFeature Server-Media-Foundation

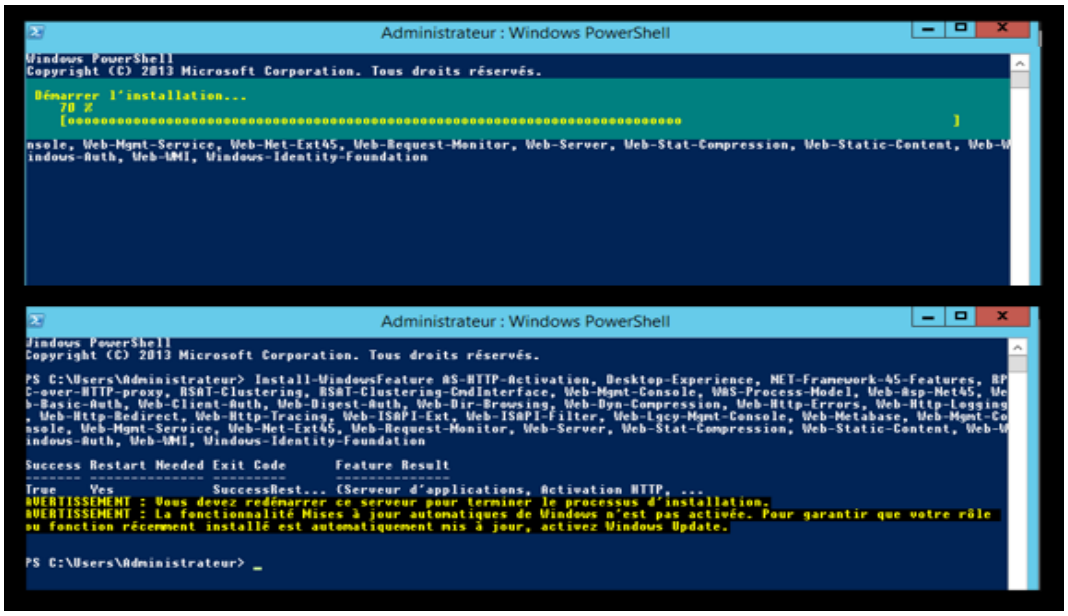

FIGURE 3.10 – Installation des prérequis Mail box et client Access

Une fois l'installation terminée, il faudra redémarrer le serveur. Pour terminer l'installation des prérequis, nous allons installer les composants suivant :

- Unified Communications Managed API 4.0 Runtime.
- Microsoft Office 2010 Filter Packs 64 bits.
- Service Pack 1 for Microsoft Office Filter Pack 2010 (KB2460041) 64-bit Edition.

Si des erreurs surgissent lors de l'installation cela veut dire que les programmes sont déjà disponibles.
Ensuite nous allons lancer le Setup Exchange setup.exe et télécharger les dernières mises à jour du logiciel puis poursuivre l'installation (voir figure 3.11).

FIGURE 3.11 – Vérifications des mises à jour exchange 2013

Une fois les mises à jour terminées, l'installation continue avec la copie des fichiers (figure 3.12).

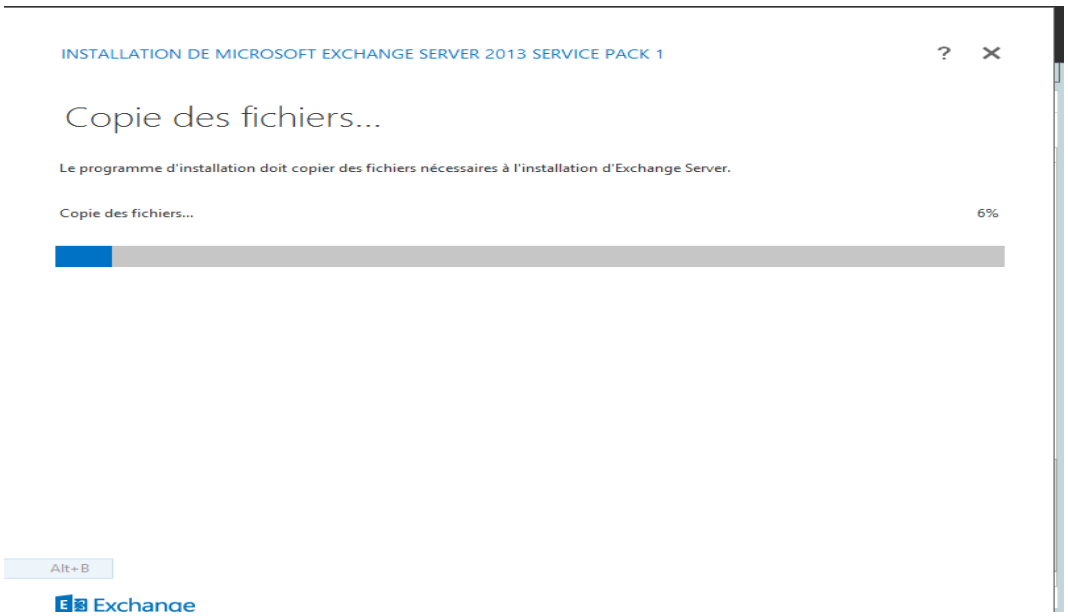

FIGURE 3.12 – Copie des fichiers

Quand la copie des fichiers est terminée, nous allons cliquer sur suivant et accepter le contrat de licence puis choisir l'option n'utilisez pas les paramètres recommandés pour configurer manuellement les paramètres.
Ensuite sélectionner les rôles serveur exchange à installer comme l'indique la figure 3.13 :

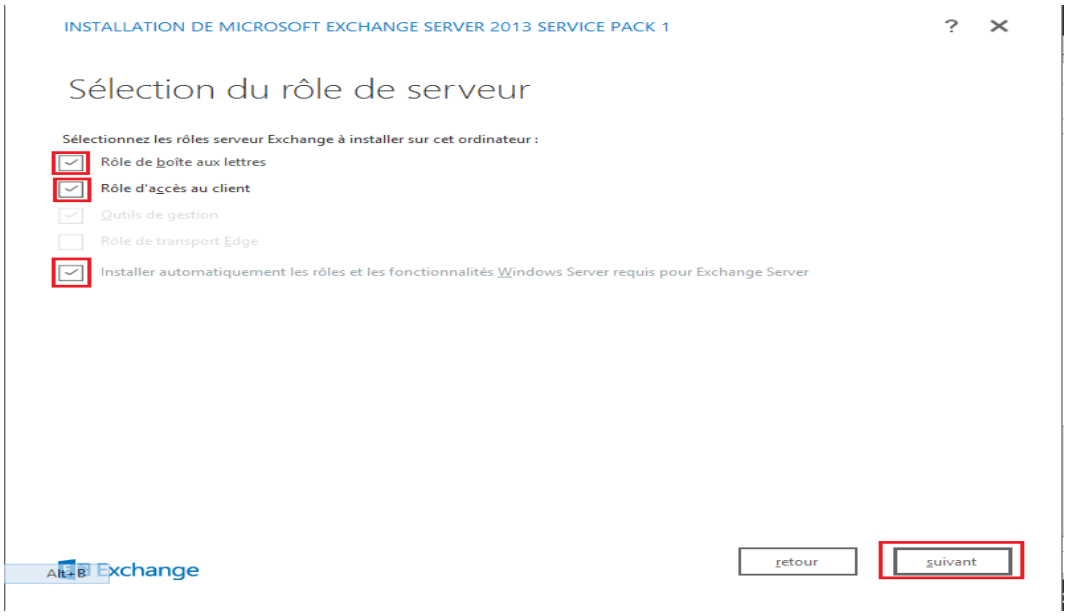

FIGURE 3.13 – Sélection du rôle de serveur

Nous devons maintenant choisir dans la figure suivante (figure 3.14) où installer Exchange :

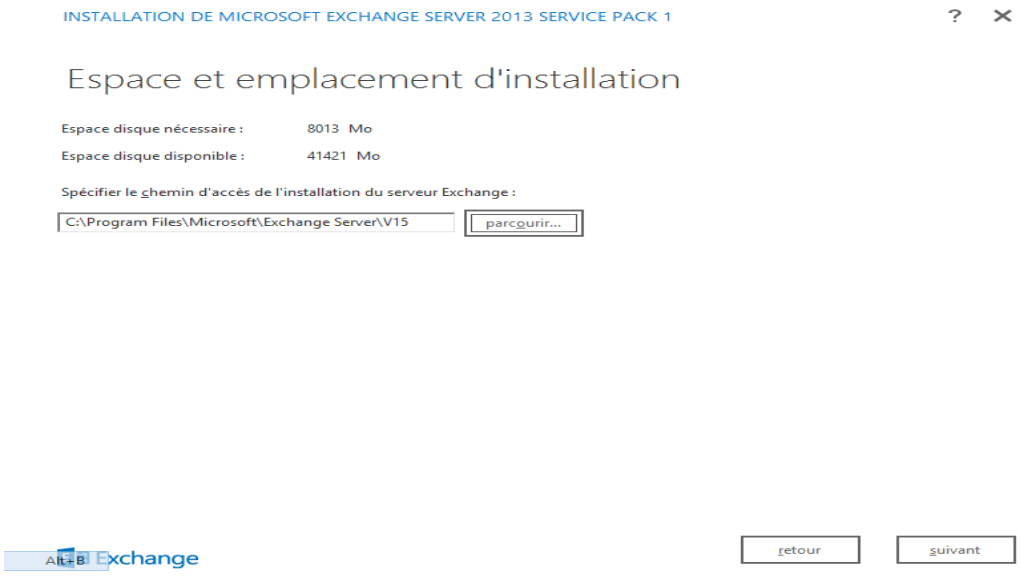

FIGURE 3.14 – Espace et emplacement d'installation.

Nous allons ensuite sélectionner le nom de l'organisation : portdebejaia.
La page d'après concerne les paramètres de protection des anti-programmes Malveillant. Nous allons désactiver la recherche de programmes malveillants.
L'ordinateur sera contrôlé pour vérifier que le programme d'installation peut continuer, puis cliquer sur installer.
Une fois l'installation terminée, nous utilisons exchange Admin Center pour l'administration.

4. **Configuration**

(a) **Centre d'administration Exchange (EAC)** L'administration d'Exchange 2013 s'effectue maintenant depuis une console Web appelée l'EAC (Exchange Administration Center) ou bien sûr toujours à l'aide du Powershell, mais en version 3.0. Il n'est plus possible, ni nécessaire, de déployer les consoles d'administration Exchange sur les postes des administrateurs. L'utilisation d'un simple navigateur Internet permet l'accès à l'interface d'administration Exchange 2013 EAC (voir figure 3.15).

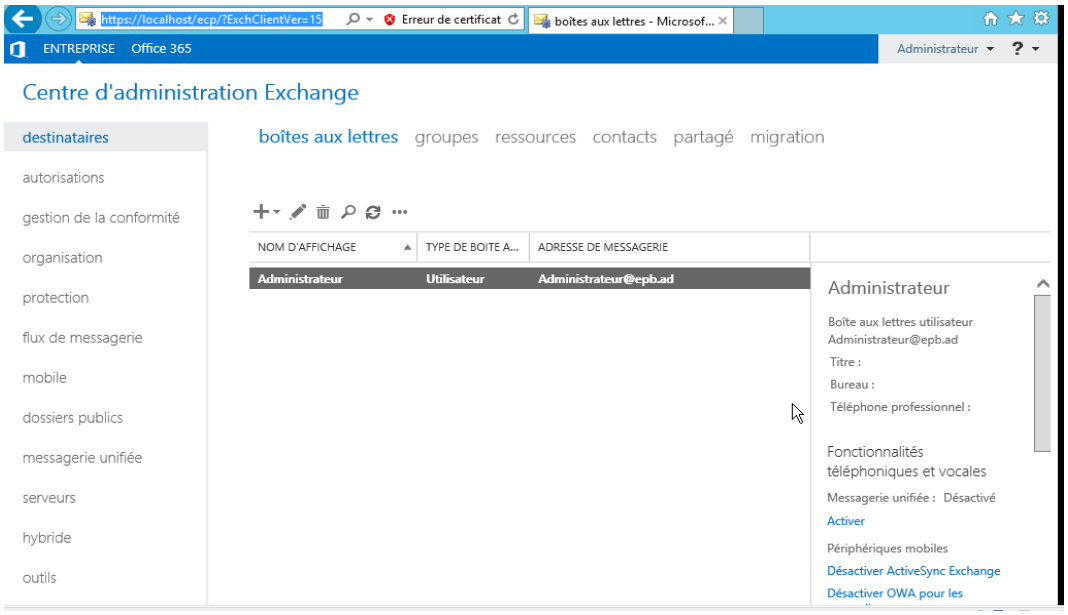

FIGURE 3.15 – Centre d'administration Exchange (EAC).

(b) **Configuration du domaine accepté et de stratégie d'adresses**

Pour configurer un nom de domaine externe nous avons besoin de configure un domaine accepté et une stratégie d'adresse de messagerie.

Par défaut, lorsque le premier serveur de boîtes aux lettres Exchange 2013 est installé, un domaine accepté est configuré comme faisant autorité pour l'organisation Exchange. Le domaine accepté par défaut est le nom de domaine complet de notre domaine racine de la forêt. Souvent, le nom de domaine interne diffère du nom de domaine externe. Par exemple notre nom du domaine interne est portdebejaia.AD, alors que notre nom de domaine externe portdebejaia.dz, L'enregistrement du serveur de messagerie (MX) DNS (Domain Name System) de notre organisation va faire référence à portdebejaia.dz. Ce dernier est l'espace de noms SMTP que nous affecterons aux utilisateurs lorsque nous créerons une stratégie d'adresse de messagerie. Nous devrons créer un domaine accepté qui correspond au nom de domaine externe. Les configurations citées précédemment sont représentées dans les figures suivantes (voir figure 3.16 et figure 3.17) :

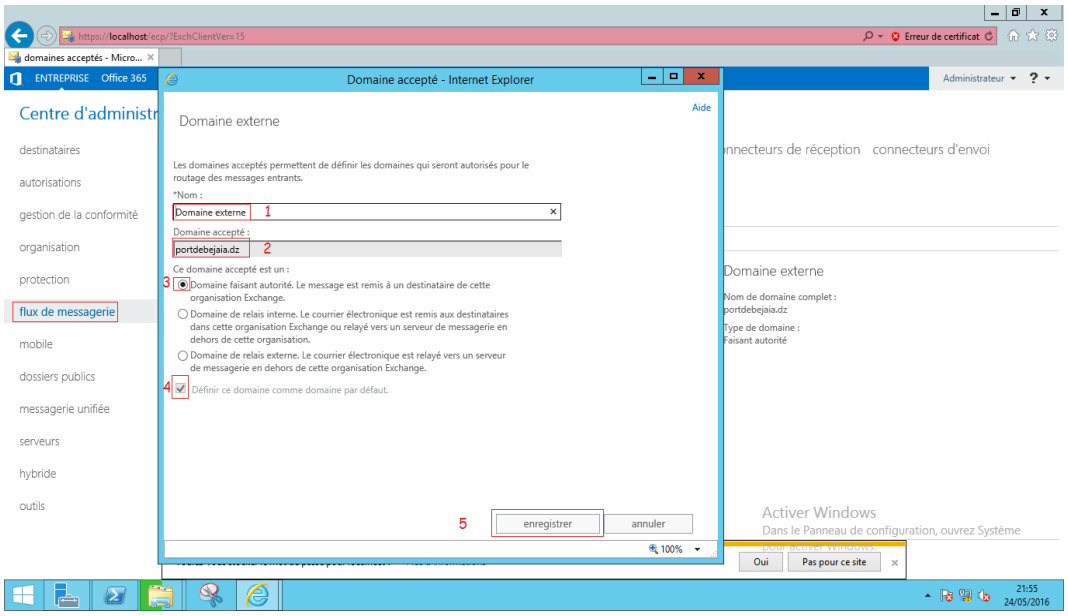

FIGURE 3.16 – Configuration d'un domaine accepté.

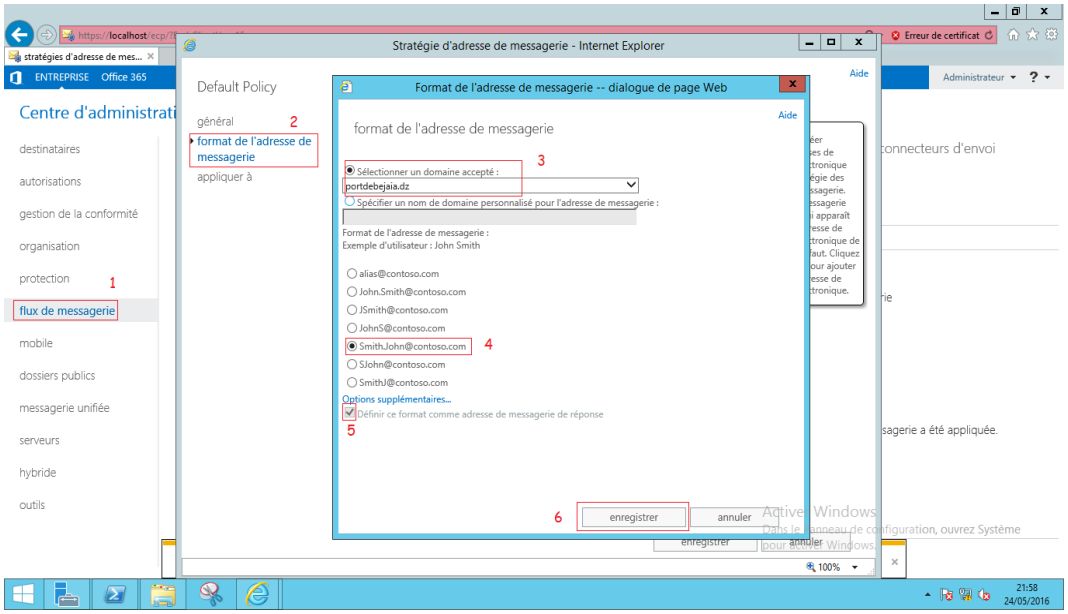

FIGURE 3.17 – Création d'une stratégie d'adresse de messagerie.

Donc la configuration du domaine accepté et de stratégie d'adresses est terminé.

(c) **La création des boites aux lettres** Il existe deux méthodes de création des boites aux lettres :

- Si l'utilisateur figure dans la liste des utilisateurs ADDS, on lui associe directement une boite aux lettres en utilisant le centre d'administration (EAC), pour cela il faudra cocher utilisateur existant et le lien se fera automatiquement, (voir figure 3.18).
- Si l'utilisateur ne figure pas dans la liste des utilisateurs nous pouvons lui créer une boite aux lettres directement à partir de l'EAC en cochant nouvel utilisateur, ensuite il sera ajouté automatiquement dans la liste des utilisateurs ADDS, (voir figure 3.18).

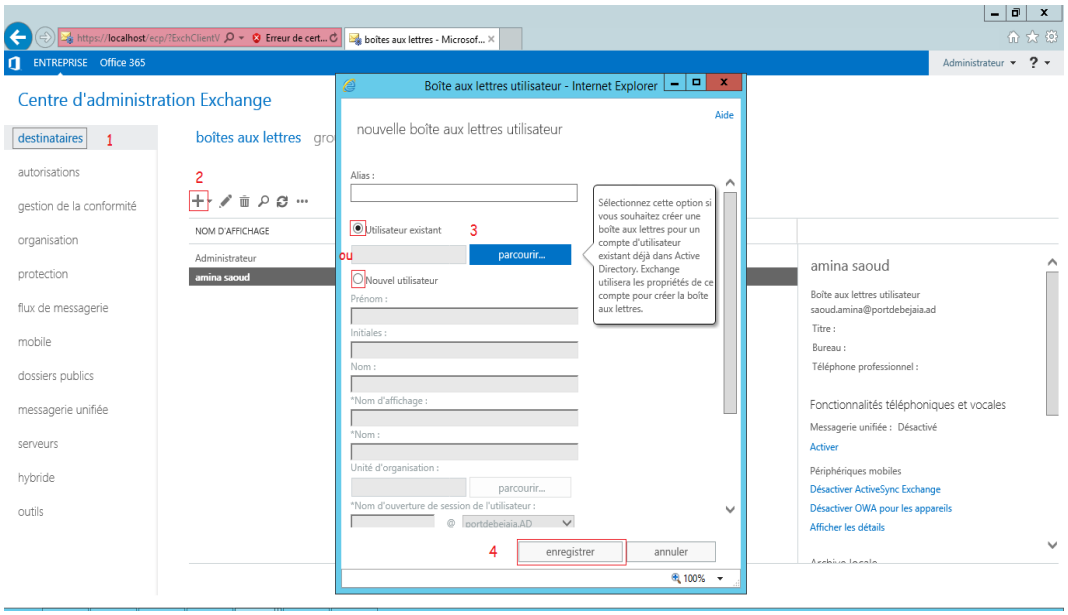

FIGURE 3.18 – Création des boites aux lettres.

(d) **Ouverture de boites aux lettres**

Pour qu'un utilisateur ouvre sa propre boite aux lettres depuis un client de messagerie tel que Outlook, il doit utiliser un navigateur web ou une application, dans notre cas nous avons utilisé internet explorer.

Les utilisateurs doivent pouvoir ouvrir leurs boites aux lettres depuis leur ordinateur personnel, pour cela nous devons effectuer des modifications dans les paramètres SSL du site web par défaut (OWA), à l'intérieur du gestionnaire des services internet (IIS) (voir figure 3.19), Et pour enregistrer les modifications nous cliquons sur appliquer.

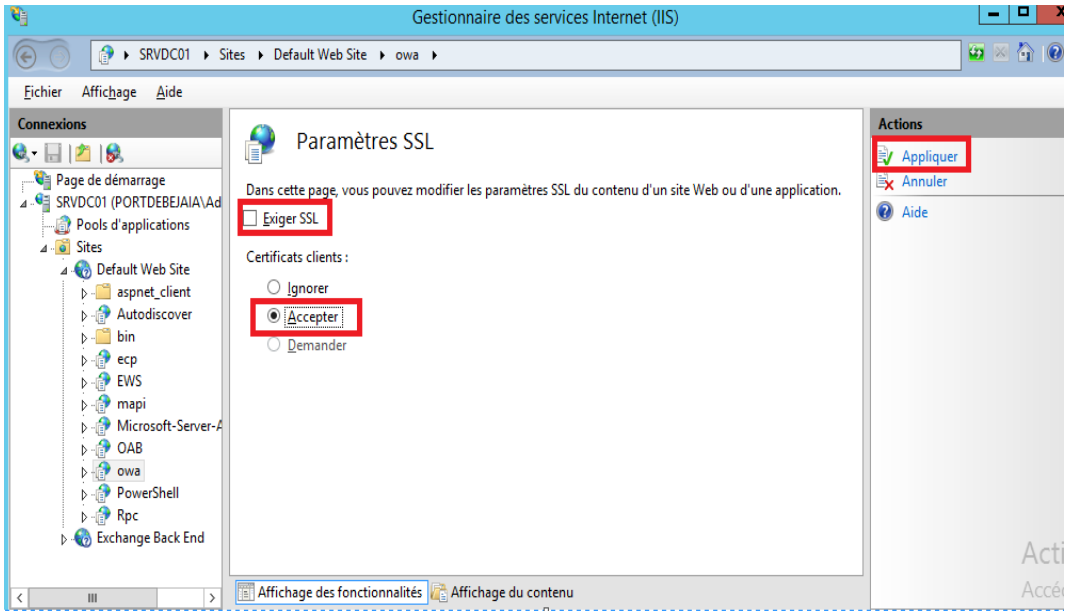

FIGURE 3.19 – Configuration owa.

(e) **Tester l'envoi de message entre des utilisateurs locaux**

Nous allons maintenant tester notre configuration en envoyant des messages entre des utilisateurs de notre réseau local il existe deux méthodes pour effectuer l'envoi soit en utilisant le client Outlook soit en utilisant le power Shell Windows. Nous avons opté pour la deuxième méthode (voir figure 3.20).

Nous avons déjà créé deux boites aux lettres de deux utilisateurs locaux :

Saoud.amina@portdebejaia.dz

Saoud.siham@portdebejaia.dz

Donc nous allons envoyer un message de teste d'un utilisateur vers un autre, la console d'administration ne retourne pas une erreur donc cela veut dire que tout fonctionne parfaitement en interne.

FIGURE 3.20 – Envoi de message depuis le Shell.

(f) **Configuration du FQDN dans le DNS privé**

Le but est non plus de parler avec le serveur exchange par son nom interne portdebejaia.AD mais un nom qui est aussi utilisable sur Internet de cette manière les utilisateurs (Outlook) n'ont qu'un nom à retenir le FQDN publique (mail.portdebejaia.dz).

Dans ce cas nous allons déclarer ce nom dans le DNS de notre Active Directory. Pour cela nous ouvrons le gestionnaire DNS et nous choisissons une nouvelle zone dans une zone de recherche directe, voir figure 3.21.

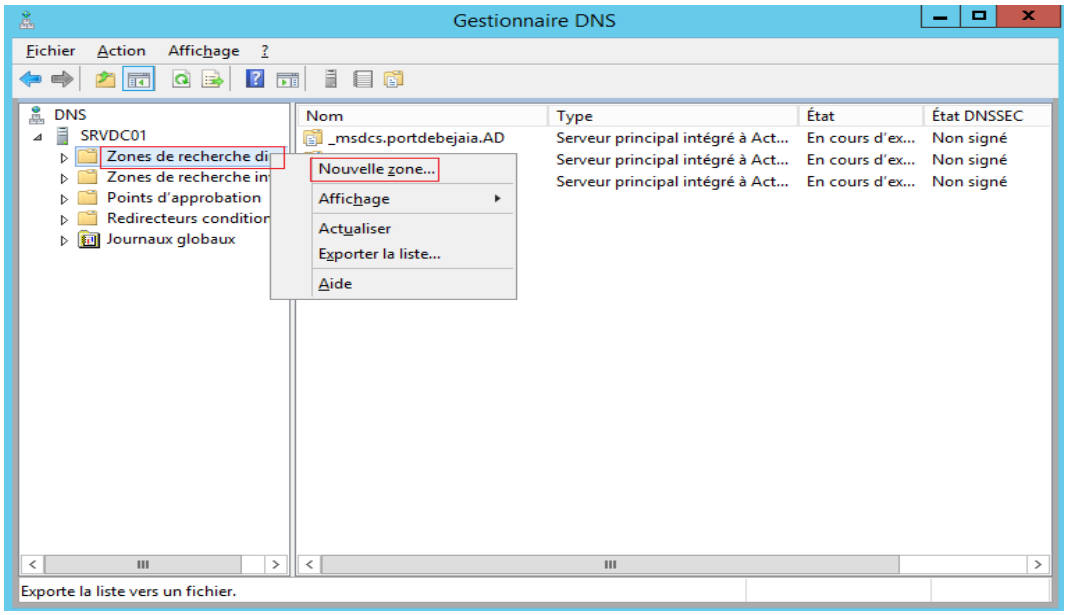

FIGURE 3.21 – Déclaration dans le DNS interne.

Puis nous choisissons zone principale comme type de zone et nous cliquons sur suivant, ensuite nous devons sélectionner la façon dont les données DNS doivent être répliquées sur le réseau, et nous cochons la case vers tous les serveurs DNS exécuter sur des contrôleurs de domaine dans ce domaine : portdebejaia.AD, après cela nous insérons le FQDN publique comme nouvelle zone de recherche directe : mail.portdebejaia.dz et nous autorisons que les mises à jour dynamiques sécurisées.

Une fois la zone est créé un enregistrement de type A doit être créer afin d'affecter l'IP privé suivante : 10.0.0.5 au FQDN. Figure 3.22.

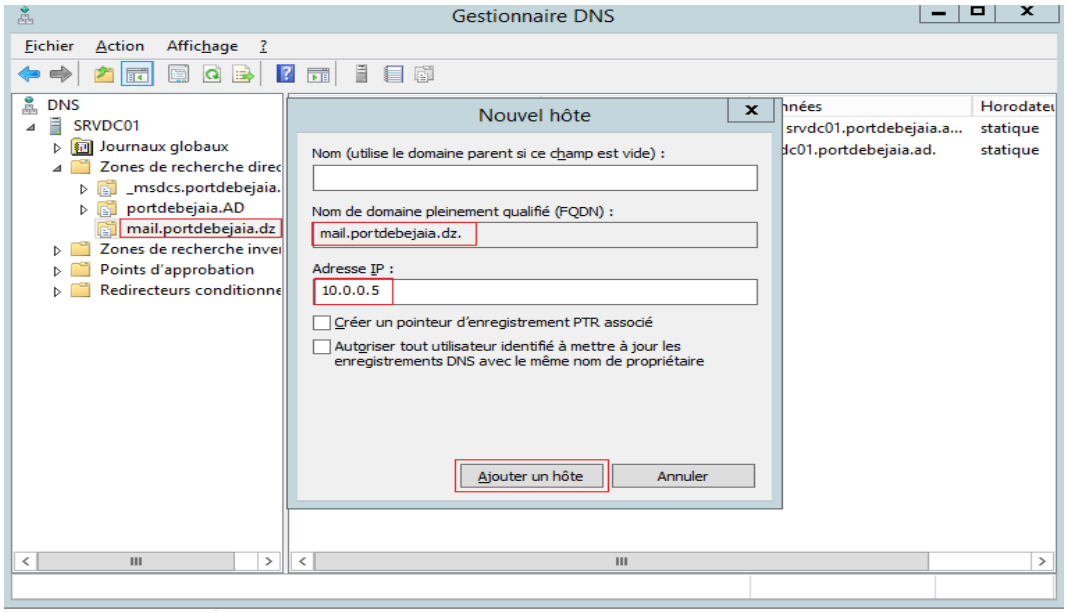

FIGURE 3.22 – Ajout d'un hôte de type A.

Une fois la configuration est faite la connectivité peut être vérifiée depuis le power Shell avec la commande Ping mail.portdebejaia.dz

Nous allons maintenant configurer Exchange pour utiliser le nom d'hôte externe (mail.portdebejaia.dz) que cela soit en internet ou en externe. Pour cela il existe deux manières, soit en utilisant une interface graphique soit en utilisant le power Shell. Etant donné le nombre d'occurrences à remplacer il est préférable de mettre de côté l'EAC et de réaliser cette opération uniquement en power Shell :

- Get-OABVirtualDirectory|Set-OABVirtualDirectory-InternalUrlhttps : //mail.portdebejaia.dz/OAB-ExternalUrlhttps ://mail.portdebejaia.dz/OAB
- GetWebServicesVirtualDirectory|SetWebServicesVirtualDirectoryInternalUrlhttps : //mail.portdebejaia.dz/EWS/Exchange.asmx-ExternalUrlhttps : //mail.portdebejaia.dz/EWS/Exchange.asmx
- Get-EcpVirtualDirectory|Set-EcpVirtualDirectory-InternalUrlhttps : //mail.portdebejaia.dz/ecp-ExternalUrlhttps ://mail.portdebejaia.dz/ecp
- Get-OwaVirtualDirectory|Set-OwaVirtualDirectory-InternalUrlhttps : //mail.portdebejaia.dz/owa-ExternalUrlhttps ://mail.portdebejaia.dz/owa
- Get-ActiveSyncVirtualDirectory|Set-ActiveSyncVirtualDirectory-InternalUrlhttps : //mail.portdebejaia.dz/Microsoft-Server-ActiveSync-ExternalUrlhttps : //mail.portdebejaia.dz/Microsoft-Server-ActiveSync
- Get-ReceiveConnector"DefaultFrontendportdebejaia.AD"|Set-ReceiveConnector-Fqdnmail.portdebejaia.dz
- Get-ClientAccessServer|Set-ClientAccessServer-AutodiscoverServiceInternalUrihttps :

//mail.portdebejaia.dz/Autodiscover/Autodiscover.xml

(g) **Configuration des connecteurs d'envoie et de réception**

Pour que les utilisateurs internes puissent communiquer avec l'extérieur des connecteurs d'envois et de réceptions sont exigées car c'est les passerelles vers le monde extérieurs.

- **Configuration du connecteur d'envoi**

  Le connecteur d'envoi comme son nom l'indique permet d'envoyer les e-mails vers l'extérieur. Avant de le créer, il va falloir se poser la question de comment notre Exchange va distribuer le courrier sur internet, dans notre cas comme nous l'avons précisé précédemment, nous avons choisi la résolution MX. Mais cette méthode est un peu délicate donc nous devons prendre en considération certaines choses :

  -L'adresse IP publique ne doit pas être blacklistée, il faudra vérifier cela périodiquement.
  -La disposition d'un Reverse DNS qui pointe sur notre domaine, son paramétrage s'effectue par le fournisseur d'accès internet (FAI).

  Pour créer le connecteur d'envoi, nous ouvrons l'EAC, nous cliquons sur " flux de messagerie", dans le volet " connecteur d'envoi " nous appuyons sur " Ajouter " (+). Une boite de dialogue sera affichée, nous devrons donc insérer le nom " internet " et cocher le type " internet ". voir figure 3.23.

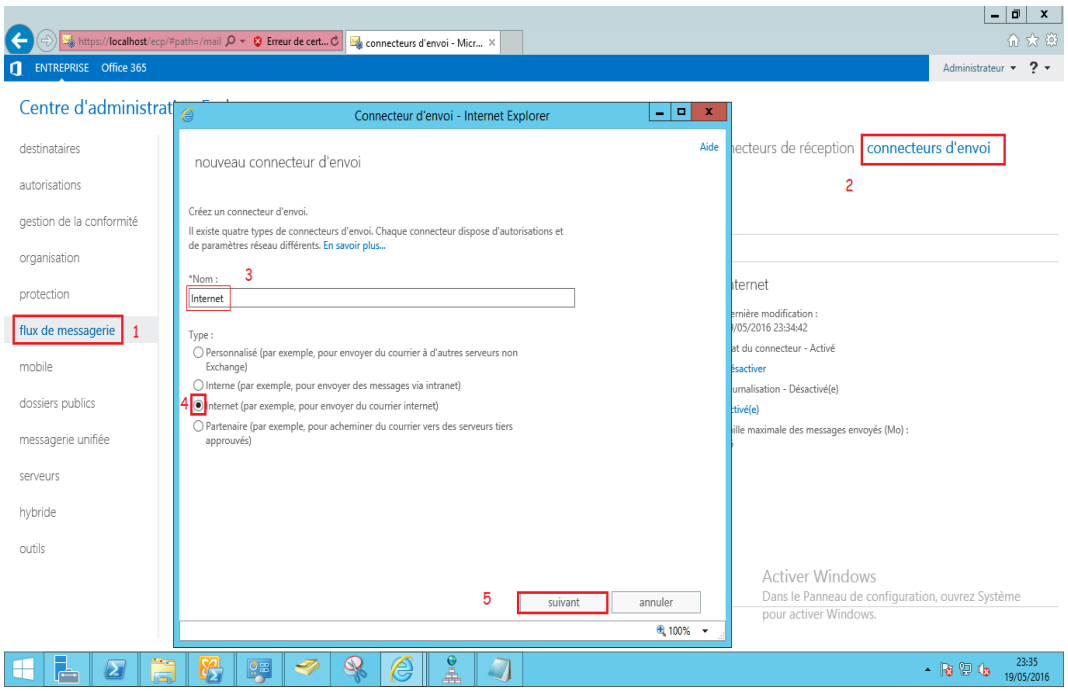

FIGURE 3.23 – Nouveau connecteur d'envoi.

Une autre boite de dialogue sera affichée, dans ce cas-là nous devons cocher la résolution MX. (Nous avons choisi la résolution MX car notre serveur SMTP et locale donc nous ne pouvons pas l'utiliser comme hôte actif). voir figure 3.24.

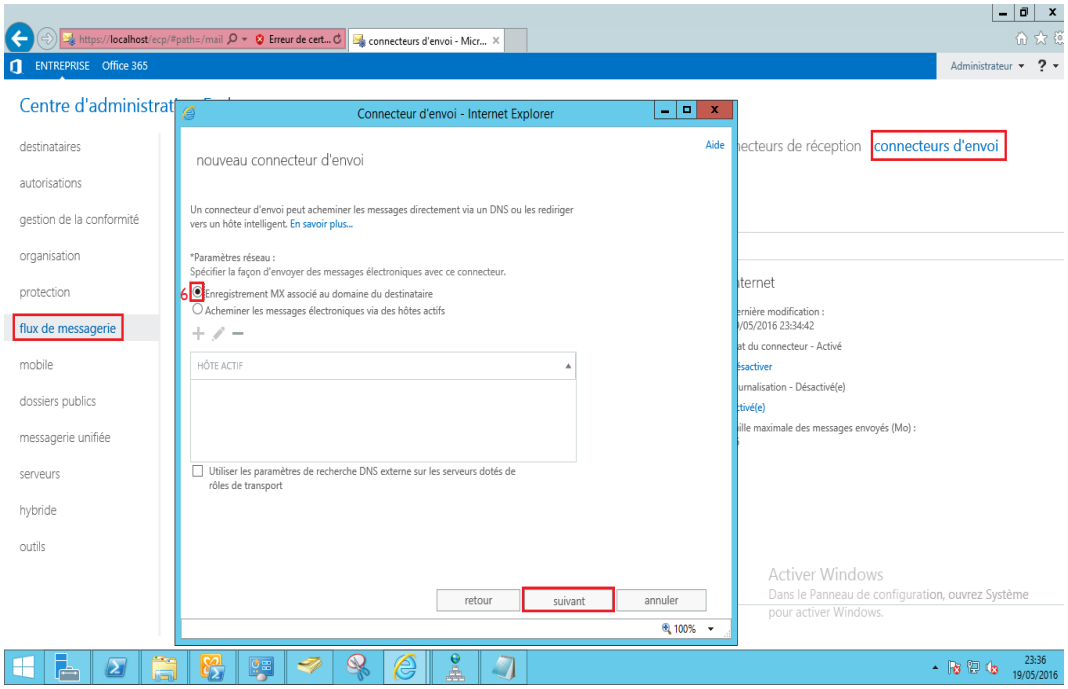

FIGURE 3.24 – Configuration des paramètres réseau.

Ensuite nous spécifions l'espace d'adresse vers lequel ce connecteur acheminera les messages électronique : (+) => type " SMTP ", domaine " * ", cout " 1 ". voir figure 3.25

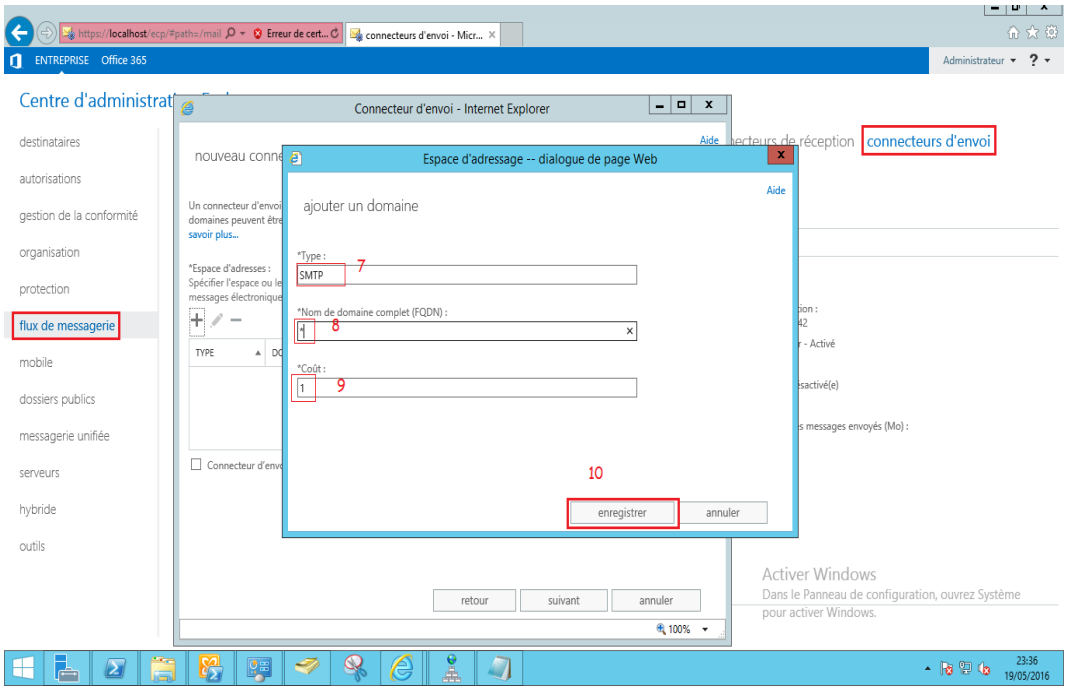

FIGURE 3.25 – Ajouter un domaine.

Enfin nous sélectionnons notre serveur Exchange (seul et unique serveur dans notre topologie) qui est SRVDC01. voir figure 3.26

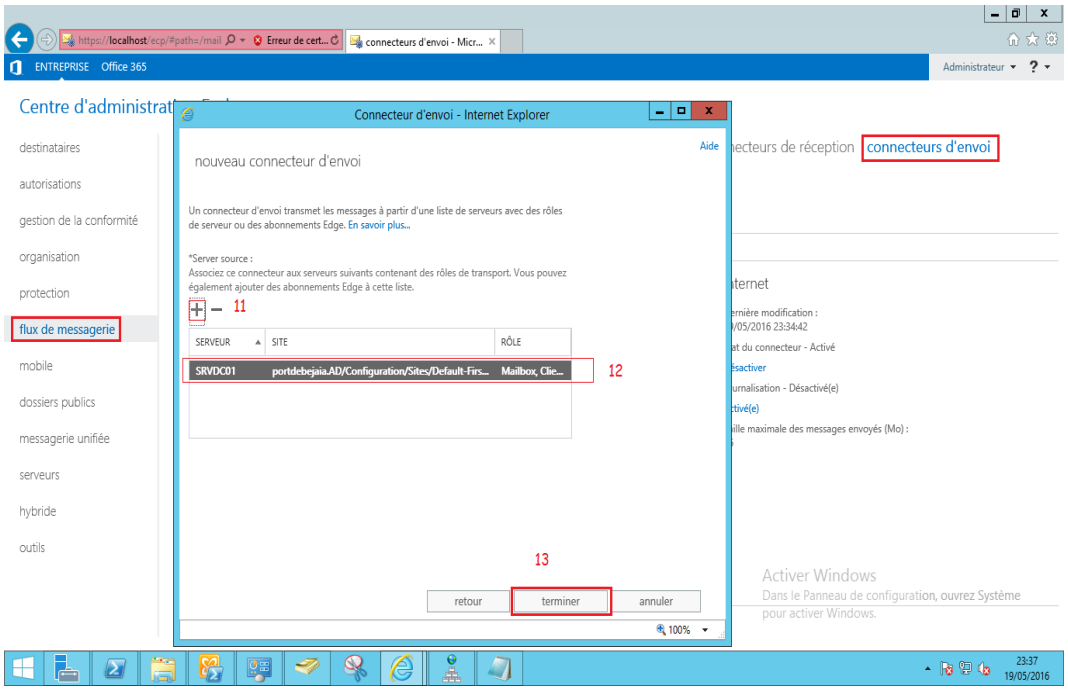

FIGURE 3.26 – Choisir le serveur source.

Enfin le connecteur est prêt nous pouvons envoyer des e-mails vers l'extérieur.

- **Configuration du connecteur de réception** Il existe plusieurs connecteurs de réception créés dès l'installation d'Exchange : Client Frontend, Client Proxy, Default, Default Frontend et Outbound Proxy Frontend Le plus important pour nous est le Default Frontend, Ce connecteur écoute le port 25 et a pour but de recevoir le courrier en provenance d'Internet. Cependant, il y a une petite modification à effectuer dessus afin de pouvoir fixer son nom d'hôte convenablement.
  Nous allons nous connecté à l'EAC, dans " Flux de messagerie " > " Connecteurs de réception " nous allons modifier le connecteur " Default Frontend SRVDC01 ". Dans l'onglet " Sécurité " nous décochons la case " Authentification du serveur Exchange ". voir figure 3.27.

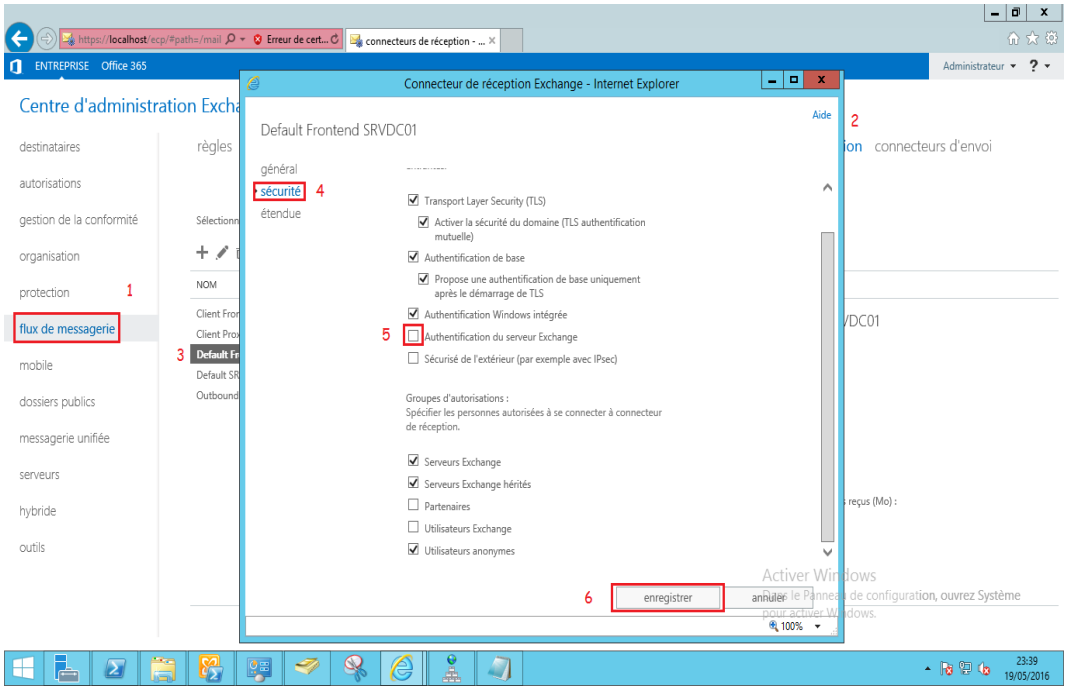

FIGURE 3.27 – Modifier la sécurité de default frountend du connecteur de réception.

Ensuite dans l'onglet " Étendue " nous insérons le nom d'hôte externe : mail.portdebejaia.dz voir figure 3.28.

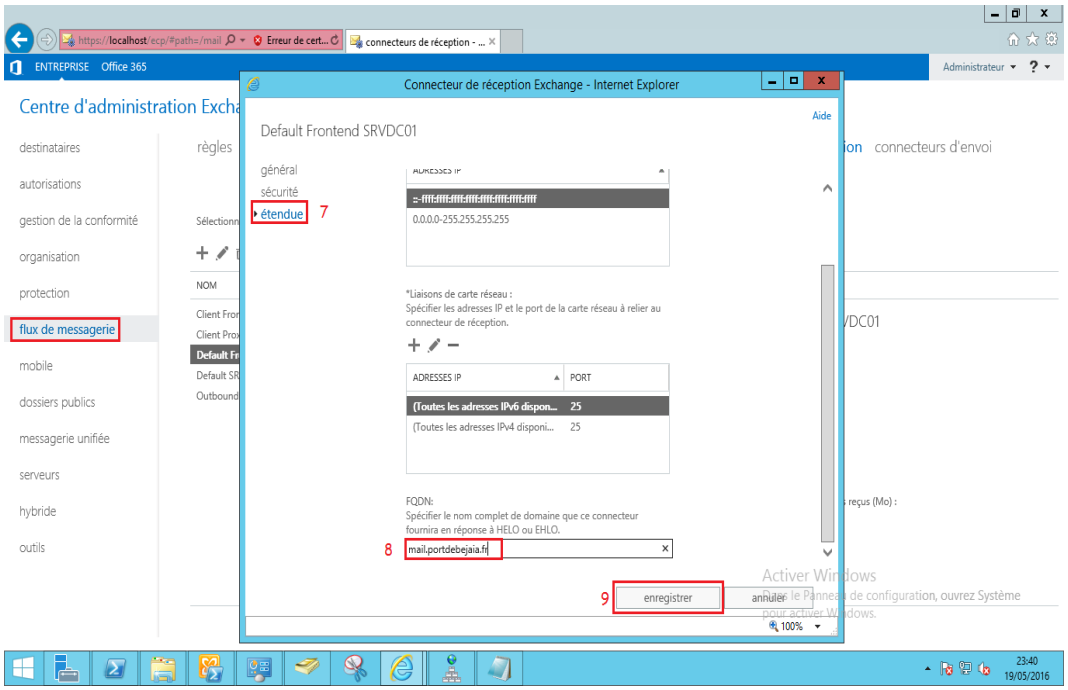

FIGURE 3.28 – Modifier l'etendue de default frountend du connecteur de réception.

(h) **Configuration du serveur SMTP** Pour configurer le serveur SMTP, Dans le Gestionnaire IIS 6, nous développons le nom du serveur, dans notre exemple SRVDC01, puis clique-droit sur le serveur SMTP et nous sélectionnons Propriétés, voir figure 3.29.

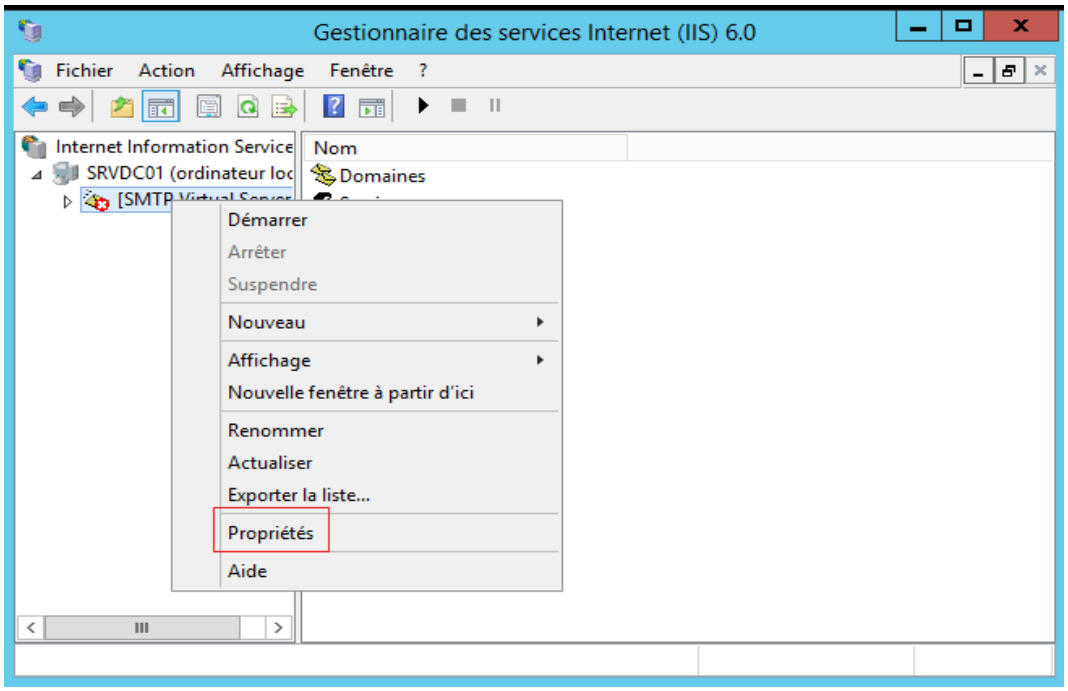

FIGURE 3.29 – Configuration du serveur SMTP.

Dans l'onglet " Général " nous activons la case " activer l'enregistrement " et nous choisissons le format de fichier journal étendu du W3C.

Puis dans l'onglet " Accès " nous nous assurons que dans " l'authentification " " l'accès anonyme " est cochée, et que la " connexion " au serveur SMTP n'est possible que du serveur local pour des raisons de sécurité, et aussi que la " restriction du relais " ne soit possible que par le serveur local sinon il sera un relais ouvert.
Pour les autres onglets nous laissons la configuration telle quelle est.

(i) **Envoie de mail vers l'extérieur** Apres avoir configuré les connecteurs d'envoie et de réception nous pouvons maintenant tester l'envoie de mail vers l'extérieure en utilisant une des boites aux lettres existantes.
Nous remarquons que le message transite bien mais quand le serveur de messagerie de destinataire le reçoit il envoie un mail de refus (voir figure 3.30) cela arrive parce que notre adresse publique n'est pas fixe et notre domaine n'est pas déclaré chez le fournisseur d'accès.

FIGURE 3.30 – Message d'erreur.

3.3 Mise en place d'EMET (Enhanced Mitigation Experience Toolkit)

3.3.1 Definition

EMET (Microsoft Enhanced Mitigation Experience Toolkit) est une trousse à outils mise à disposition gratuitement par Microsoft, qui s'applique au système et à n'importe quelle application tournant sous Windows.
EMET protège contre certaines techniques d'exploitation des vulnérabilités logicielles grâce à des technologies de réduction des risques de sécurité. En ce sens, il est parfois classé dans les HIPS (Host-based Intrusion Prevention System). Ces technologies fonctionnent comme des protections spéciales et des obstacles que l'auteur de l'attaque doit mettre en échec pour exploiter les vulnérabilités logicielles et progresser dans son attaque [28]. Ces technologies de réduction des risques de sécurité ne garantissent pas à 100% de la non-exploitation des vulnérabilités. Toutefois, elles font en sorte que l'exploitation soit aussi difficile que possible. Il arrive fréquemment qu'une exploitation pleinement fonctionnelle pouvant contourner l'utilitaire EMET ne puisse jamais se développer. Il s'agit de perdre l'attaquant dans un labyrinthe. EMET est donc un outil de durcissement du système et de défense. EMET 5.5 est compatible avec :

- Tous les postes de travail Microsoft Windows à partir de Windows Vista SP2.
- Tous les serveurs à partir de Windows Server 2003 SP2.

Il existe plusieurs mécanismes sous Windows permettant de renforcer la sécurité [29] :

- **Data Execution Prevention (DEP)** c'est un mécanisme interdisant l'exécution de code depuis une zone mémoire non exécutable.
- **Address Space Layout Randomization (ASLR)** c'est un mécanisme de sécurité permettant de rendre aléatoire l'adresse de chargement des éléments comme les bibliothèques.
- **SafeSEH/SEHOP** offre un vrai gestionnaire d'exception, interdisant ou plutôt rendant difficile l'utilisation des exceptions dans l'exécution de code arbitraire.

3.3.2 Installation et configuration d'EMET

L'installation d'EMET est rapide et nous permet d'être protégés dès le début contre les failles de sécurité des navigateurs internet, Office et autres applications. Bien qu'il s'agisse d'un outil technique et puissant, son utilisation est simple. Voici comment installer et configurer EMET sur Windows.

3.3.2.1 Installation

Tout d'abord, nous allons télécharger EMET à partir du site Web de Microsoft et l'installer comme tout autre logiciel. Lors de l'installation, nous sélectionnons l'option "Utiliser Paramètres Recommandé " dans la fenêtre de configuration et nous cliquons sur le bouton "Terminer" pour continuer.

3.3.2.2 Configuration

la figure 3.31 représente l'outil EMET. En cliquant sur le bouton "Apps" sur le ruban, nous pouvons voir toutes les applications qui sont protégés par EMET. Dans la fenêtre Configuration de l'application, nous pouvons aussi activer ou désactiver chaque politique d'atténuation individuellement pour chaque application. Pour ajouter notre propre application pour EMET, nous cliquons sur le bouton "Ajouter une application" sur le ruban, nous sélectionnons l'application et cliquons sur le bouton "Ouvrir" pour terminer la procédure. Par exemple, nous avons pris Google chrome comme exemple pour l'ajouter à EMET. Apres avoir lancé le navigateur Google nous pouvons maintenant le voir dans la liste des processus en cours d'exécution. L'icône verte indique que le programme est protégé par EMET.

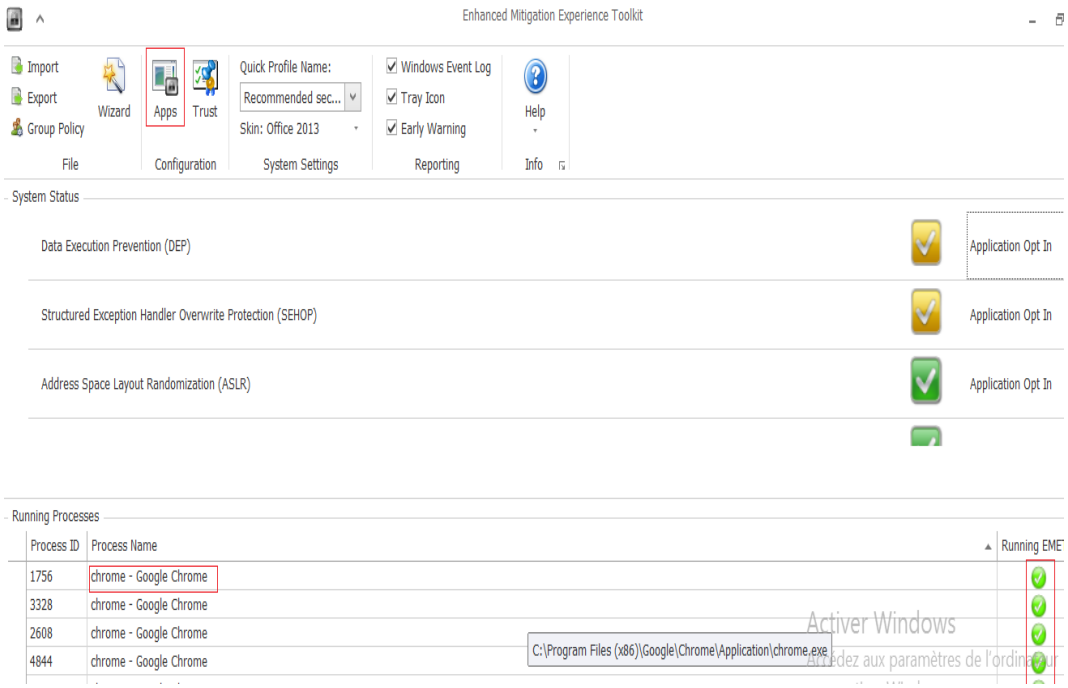

FIGURE 3.31 – Interface de gestion d'EMET.

3.4 Segmentation du réseau en VLANs

Les performances réseau constitue un facteur important dans la productivité d'une entreprise, l'une des technologies permettant de les améliorer consiste à diviser de vastes domaines de diffusions en domines plus petits.
Dans un inter-réseau commuté, les VLANs permettent la segmentation et assouplissent l'organisation. Les VLANs offrent un moyen de regrouper des périphériques dans un LAN. Un groupe de périphériques dans un VLAN communiquent comme si ils étaient reliés au même câble. Les VLANs reposent sur des connexions logiques, et non de connexions physiques.

3.4.1 Matériel et équipements utilisés

- Câble RJ45 droit et croisé.
- Câble fibre optique.
- 22 switchs cisco 2960.
- 1 switch fédérateur optique.
- Des ordinateurs

Attribution des adresses IP aux VLANs (voir tableau 3.32)

Nom de Vlan	ID	Adresse Réseau	première adresse utilisable	Dernière adresse utilisable	passerelle
Vlan DC	3	172.16.3.0/24	172.16.3.1	172.16.3.254	172.16.3.1
Vlan DDD	4	172.16.4.0/24	172.16.4.1	172.16.4.254	172.16.4.1
Vlan DFC	5	172.16.5.0/24	172.16.5.1	172.16.5.254	172.16.5.1
Vlan DG	6	172.16.6.0/24	172.16.6.1	172.16.6.254	172.16.6.1
Vlan DGAF	7	172.16.7.0/24	172.16.7.1	172.16.7.254	172.16.7.1
Vlan DL	8	172.16.8.0/24	172.16.8.1	172.16.8.254	172.16.8.1
Vlan DMA	9	172.16.9.0/24	172.16.9.1	172.16.9.254	172.16.9.1
Vlan DMI	10	172.16.10.0/24	172.16.10.1	172.16.10.254	172.16.10.1
Vlan DR	11	172.16.11.0/24	172.16.11.1	172.16.11.254	172.16.11.
Vlan DRHM	12	172.16.12.0/24	172.16.12.1	172.16.12.254	172.16.12.1
vlan TEXTER	13	172.16.13.0/24	172.16.13.1	172.16.13.254	172.16.13.1

FIGURE 3.32 – Tableau des adresses IP.

3.4.2 Logiciel de simulation utilisé Packet Tracer

Packet Tracer est un simulateur de réseau puissant développé par Cisco système pour faire des plans d'infrastructure de réseau au temps réel. Il offre la possibilité de créer, visualiser et de simuler les réseaux informatiques. L'objectif principal de simulateur est de schématiser, configurer et de voir toutes les possibilités d'une mise en oeuvre. Cisco Packet Tracer est un moyen d'apprentissage et de la réalisation de divers réseaux et découvrir le fonctionnement des différents éléments constituant un réseau informatique.

3.4.3 Architecture physique de l'EPB

Nous avons pris quelques switches seulement pour la simulation, l'architecture est représentée dans la figure 3.33 :

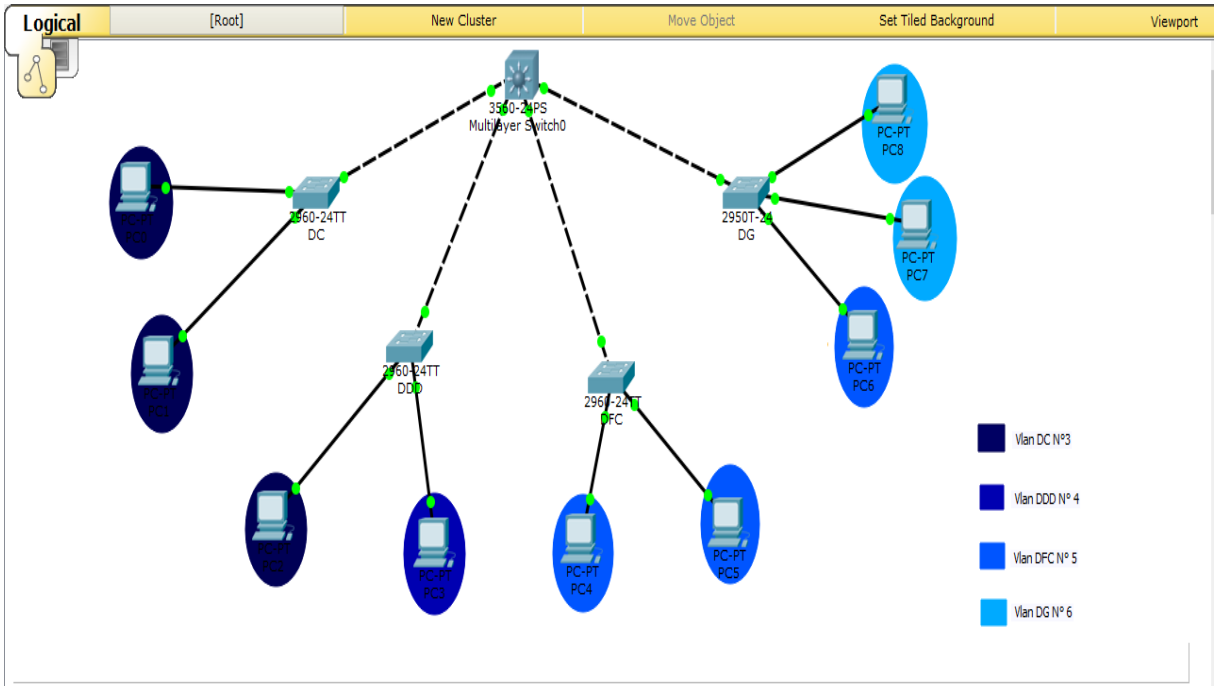

FIGURE 3.33 – Exemple d'architecture de l'EPB sous Packet Tracer.

3.4.4 Configuration de base des équipements

3.4.4.1 Affectation des noms aux switchs

Nous exécutons ces lignes de commandes sur tous les switchs pour affecter à chaque switch son propre nom :

Switch #config t

Switch (config) #hostname DC

3.4.4.2 Configuration des mots de passes

Maintenant pour sécuriser tous les accès aux équipements, il faudrait configurer les mots de passes pour chaque switch. Le mot de passe privilégier, le mot de passe console (configuration globale) et le mode de configuration Telnet voir figure 3.34 : (ex switch DC)

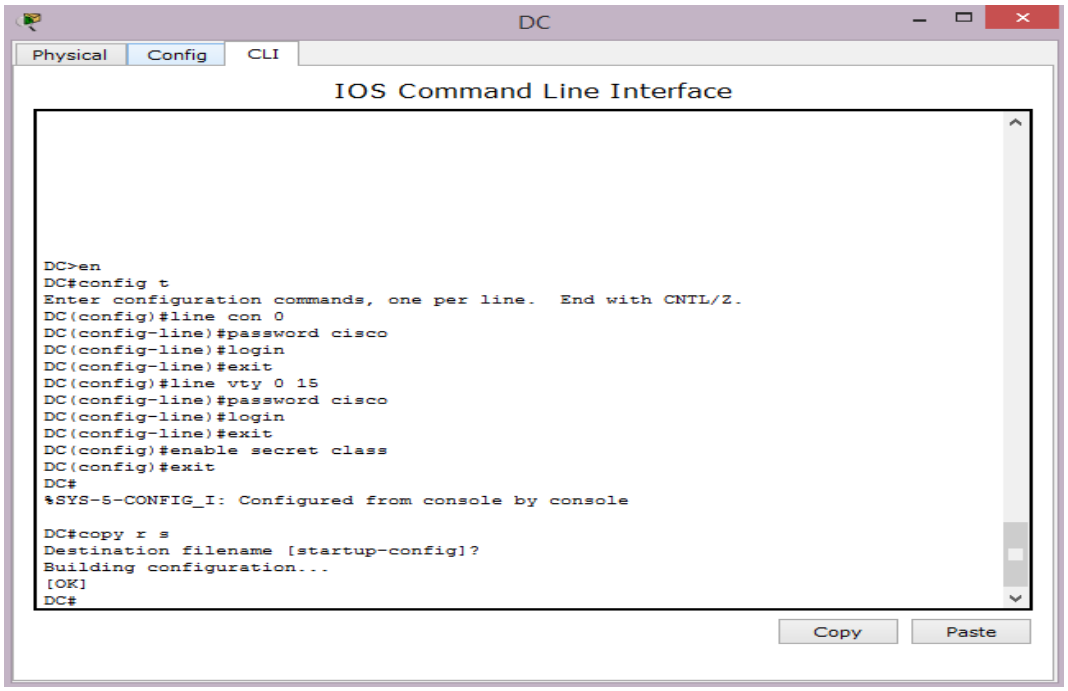

FIGURE 3.34 – Configuration des mots de passe (ex : switch DC).

Apres avoir créé les mots de passes, nous utilisons la commande suivante pour les chiffrés :
DC (config) #service password-encryption

3.4.4.3 Configuration du VTP

Le protocole VTP permet à un administrateur réseau de configurer un commutateur pour qu'il propage des configurations VLAN à d'autres commutateurs du réseau. Les commutateurs peuvent être en trois modes différents :

- Commutateur en mode serveur : Il diffuse ses informations sur les VLANs à tous les autres commutateurs appartenant au même VTP domaine.
- Commutateur en mode client : Il stocke uniquement les informations sur les VLANs transmises par le commutateur en mode VTP server sur le même domaine.
- Commutateur en mode transparent : Il transmet les informations VTP aux autres commutateurs mais ne les traitent pas. Ces commutateurs sont autonomes et ne participent pas aux VTP.

Dans ce cas-là, Le commutateur Multilayer sera configurer en mode server, et le reste des commutateurs seront configurés en mode client.

- **Mode VTP Server** Nous allons configure notre Switch Mutlilayer en mode serveur (voir figure 3.35)

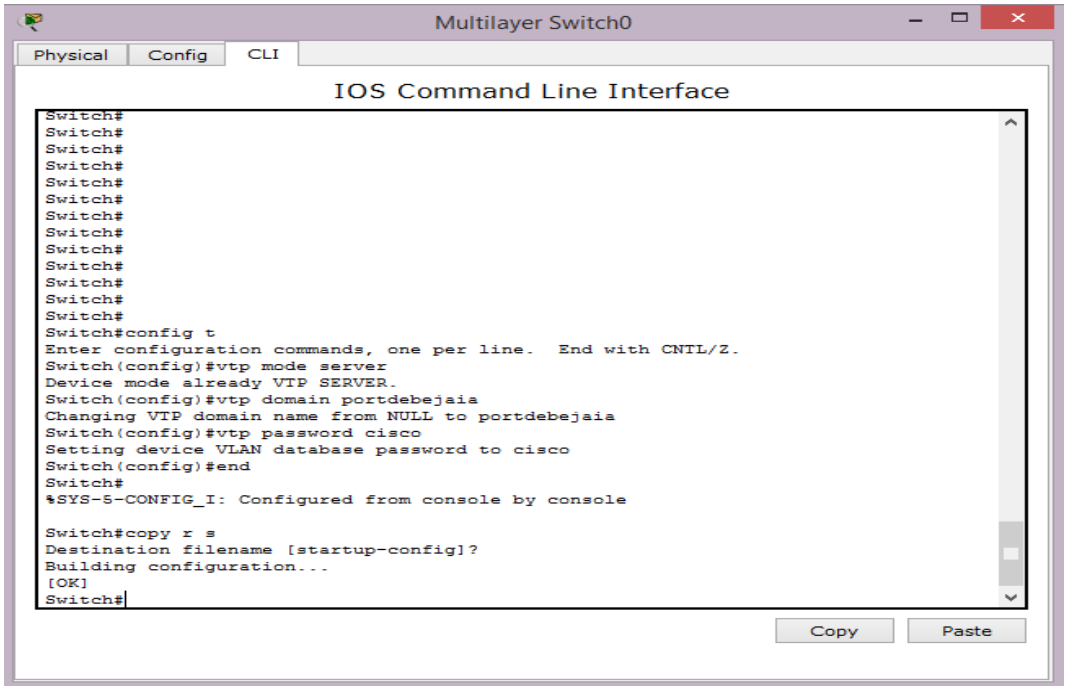

FIGURE 3.35 – Configuration du VTP server.

- **Mode VTP Client** La configuration des clients-VTP sera au niveau de chaque commutateur (ex : switch DFC) (voir figure 3.36)

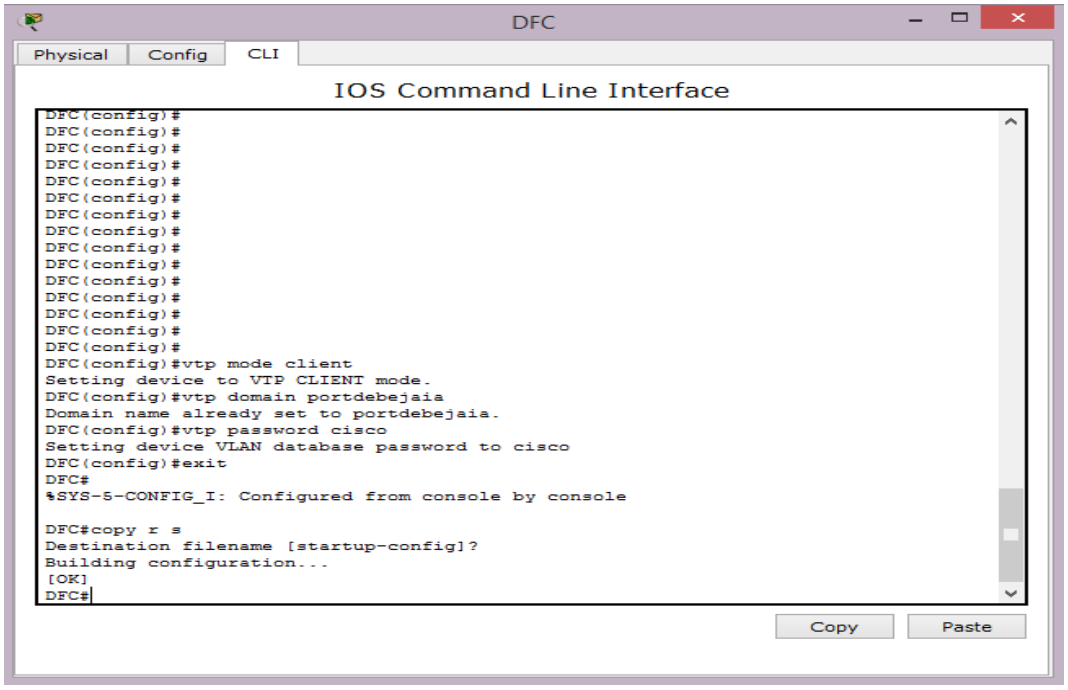

FIGURE 3.36 – Configuration du VTP server.

3.4.4.4 Création et configuration des VLANs au niveau des switchs

- création des VLANs au niveau du multilayer
  Multilayer #vlan database
  Multilayer (vlan) #vlan 3 name DC
  Multilayer (vlan) #vlan 4 name DDD
  Multilayer (vlan) #vlan 5 name DFC
  Multilayer (vlan) #vlan 6 name DG
  Multilayer (vlan) #exit

- Configuration des adresses IP et du masque sur les interfaces des VLANs :
  Multilayer (config) #interface vlan 3
  Multilayer (config-if) #ip address 172.16.3.1 255.255.255.0
  Multilayer (config-if) #no shutdown
  Multilayer (config-if) #exit

  Multilayer (config) #interface vlan 4
  Multilayer (config-if) #ip address 172.16.4.1 255.255.255.0
  Multilayer (config-if) #no shutdown
  Multilayer (config-if) #exit

  Multilayer (config) #interface vlan 5
  Multilayer (config-if) #ip address 172.16.5.1 255.255.255.0
  Multilayer (config-if) #no shutdown
  Multilayer (config-if) #exit
  Multilayer (config) #interface vlan 6
  Multilayer (config-if) #ip address 172.16.6.1 255.255.255.0
  Multilayer (config-if) #no shutdown
  Multilayer (config-if) #exit

- Exécution de la commande qui permet le routage inter-vlan :
  Multilayer (config) #ip routing

- Configuration des agrégations, implémentation des trunk 802.1q sur le switch Multilayer :
  Multilayer (config) #interface range fa0/1-24
  Multilayer (config-if) #switchport mode trunk
  Multilayer (config-if) #switchport trunk encapsulation dot1Q
  Multilayer (config-if) #no shutdown

- Attribution des ports de switchs aux VLANs :
  - Au niveau du switch DC voir figure 3.37

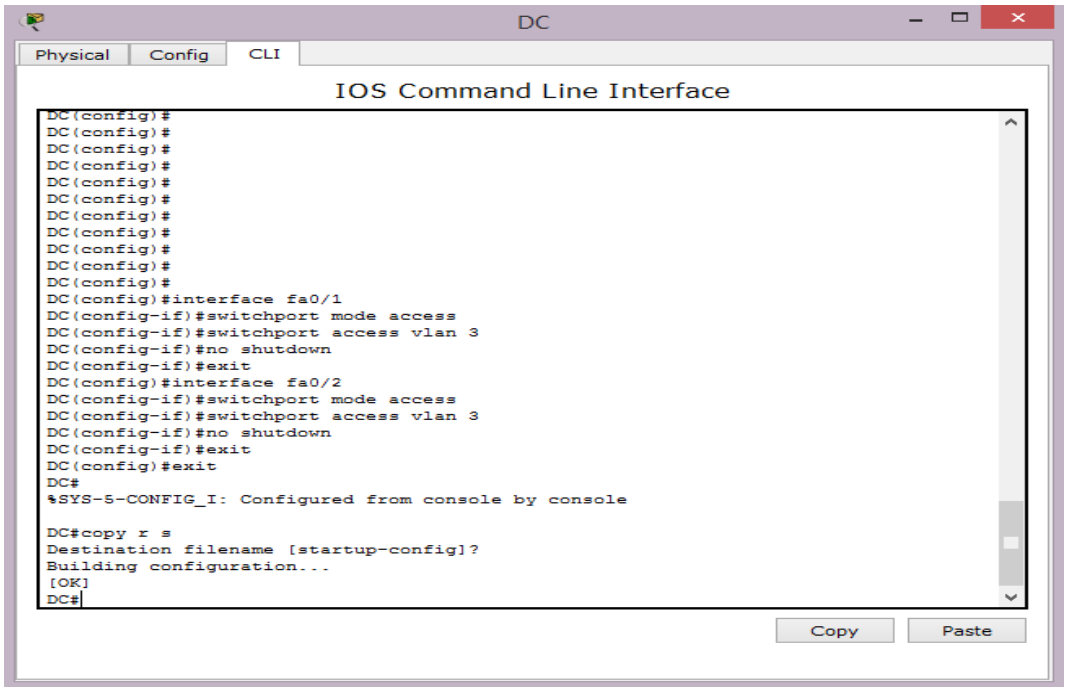

FIGURE 3.37 – Attribution des ports au niveau du switch DC.

  - Au niveau du switch DDD voir figure 3.38

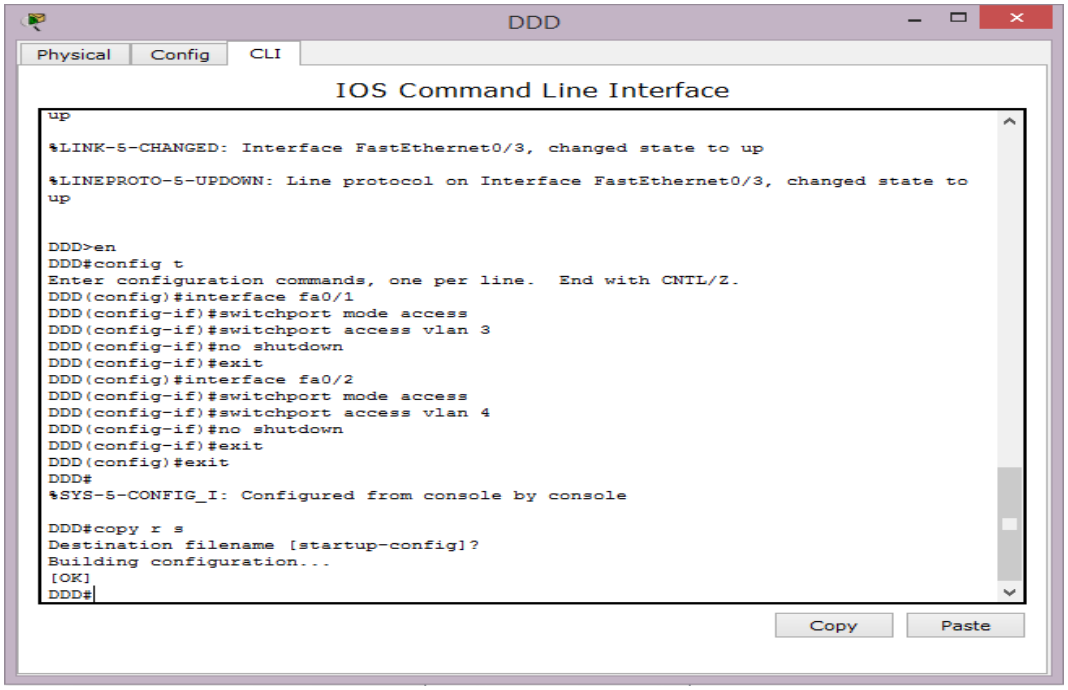

FIGURE 3.38 – Attribution des ports au niveau du switch DDD.

- Au niveau du switch DFC voir figure 3.39

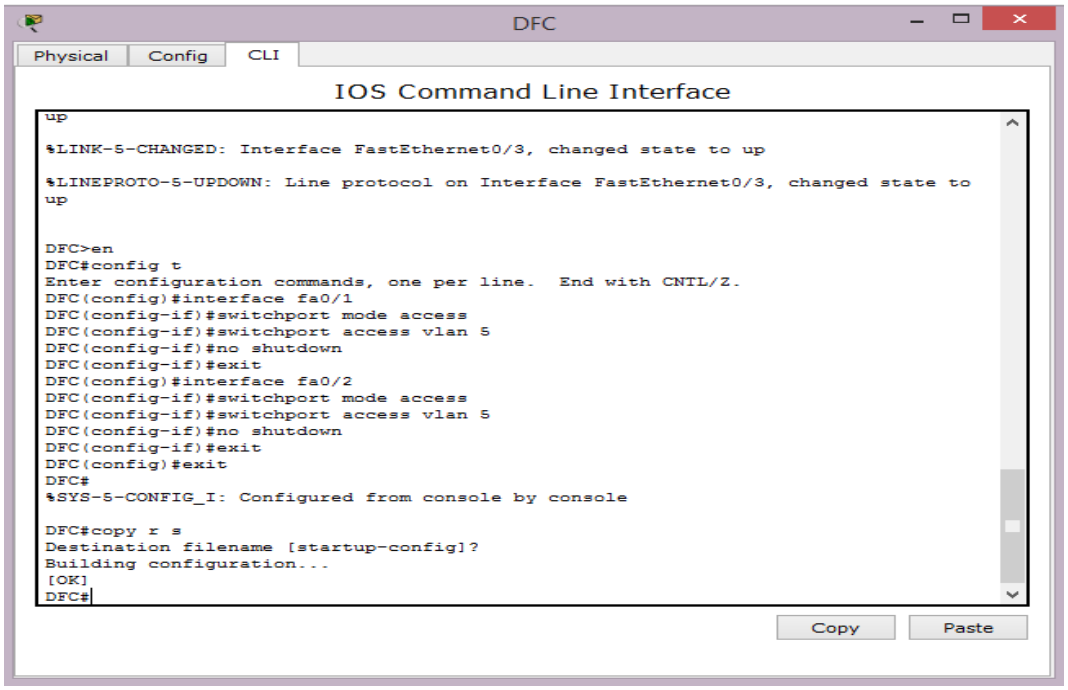

FIGURE 3.39 – Attribution des ports au niveau du switch DFC.

- Au niveau du switch DG voir figure 3.40.

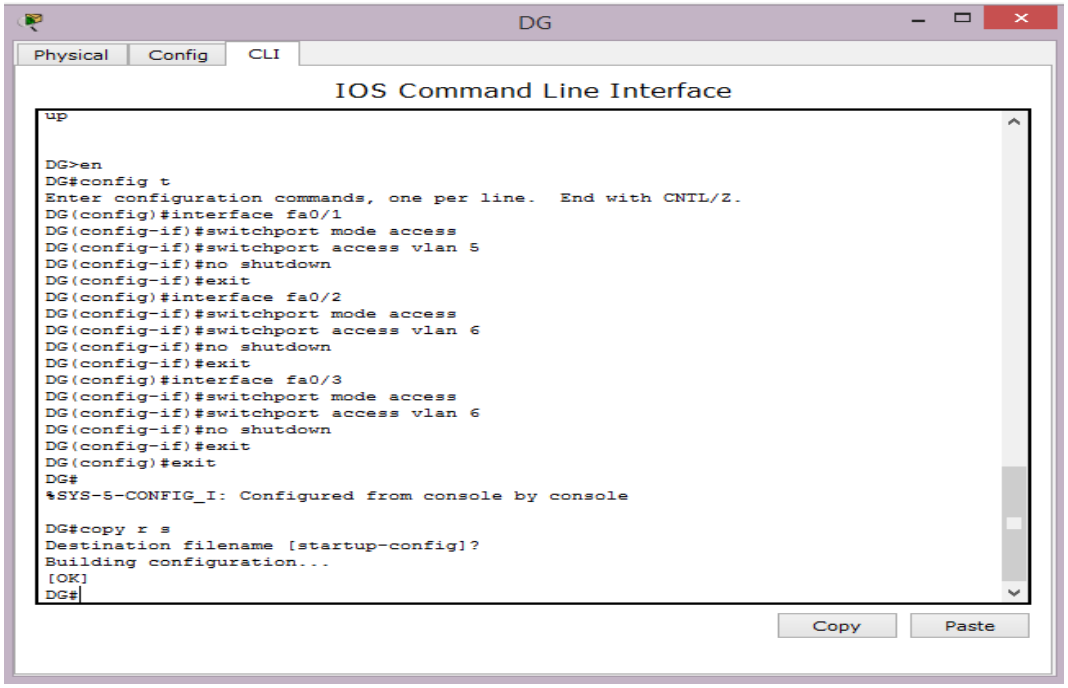

FIGURE 3.40 – Attribution des ports au niveau du switch DG.

3.4.4.5 La sécurité des ports

Avec les Switchs Cisco, il est possible de faire un contrôle sur les ports en limitant l'accès à certaines adresses MAC, cela permet de sécuriser l'accès. Pour cela, il faut utiliser l'option " Port-security ".
Il y a deux méthodes, la première consiste à enregistrer manuellement l'adresse MAC autorisée et la seconde consiste à prendre comme adresse MAC autorisée celle de l'hôte qui va se connecter et envoyer une trame en premier à ce port du Switch Cisco.

- **Sécurisation manuelle de l'accès** Dans un premier temps, on va sécuriser manuellement l'accès en définissant une adresse MAC précise pour un port. Dans le but d'empêcher n'importe quel poste de travail de se connecter.
  Switch # Configure terminal
  Switch (config) #interface FastEthernet 0/2
  Switch (config-if) #switchport mode access
  Switch (config-if) #switchport port-security
  Switch (config-if) #switchport port-security mac-address @MAC

- **Sécurisation automatique de l'accès** Il est possible de sécuriser l'accès de manière automatique c'est-à-dire que l'on active le " port-security " et c'est le premier hôte qui va se connecter et envoyer une trame qui va en être en quelque sorte le propriétaire. Tout le temps qu'il n'y a pas de trame, l'adresse MAC du PC connecté n'est pas enregistrée.
  Switch>enable
  Switch #Configure terminal
  Switch (config) #interface Fa0/3
  Switch (config-if) #switchport mode access
  Switch (config-if) #switchport port-security
  Switch (config-if) #switchport port-security mac-address sticky

- **Augmenter le nombre d'adresses MAC autorisées sur un port** Par défaut, il est possible d'autoriser une seule adresse MAC sur chacun des ports mais il est possible d'augmenter le nombre d'adresses grâce à la commande :
  Switch (config-if) #switchport port-security maximum x

  Sachant que X est le nombre d'adresses MAC que nous voulons autorisées.

- **La réaction des équipements lors de la violation de la sécurité** Le switch se doit de réagir lorsqu'un hôte non autorisé se connecte sur un port sécurisé, pour cela la commande " switch port-Security violation " doit être utilisé, en trois options différentes :

- La méthode " protect " : toutes les trames ayant des adresses MAC sources inconnues sont bloquées et les autres autorisées. Pour la réactiver, il faut désactiver le port manuellement et le réactiver manuellement pour qu'il redevienne actif. Pour cela, allez dans la configuration de l'interface et saisissez la commande " shutdown " pour désactiver puis " no shutdown " pour activer l'interface.
- La méthode " shutdown " : elle désactive l'interface lorsque il y'a violation.
- La méthode " restrict " : alerte SNMP envoyer et le compteur de violation est incrémenté.

Apres avoir choisi la méthode convenable, nous insérons les lignes de commandes suivantes :
DFC #config t
DFC (config) #interface fa0/2
DFC (config) #switchport mode access
DFC (config) #switchport port-security violation protect

3.4.5 Teste de connectivité

- La figure 3.41 représente un Ping entre le PC8 qui appartient au VLAN 6 et le PC6 qui appartient au VLAN 5.

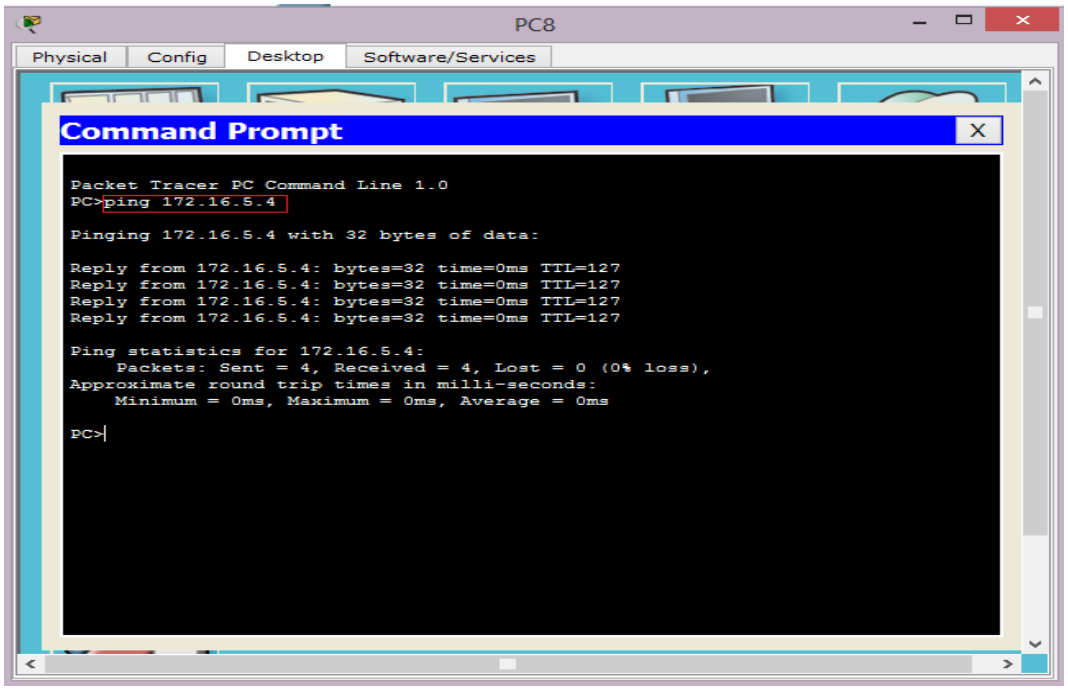

FIGURE 3.41 – Teste de connectivité entre le PC8 et le PC6.

- La figure 3.42 représente un Ping entre le PC3 qui appartient au VLAN 4 et le PC1 qui appartient au VLAN 3.

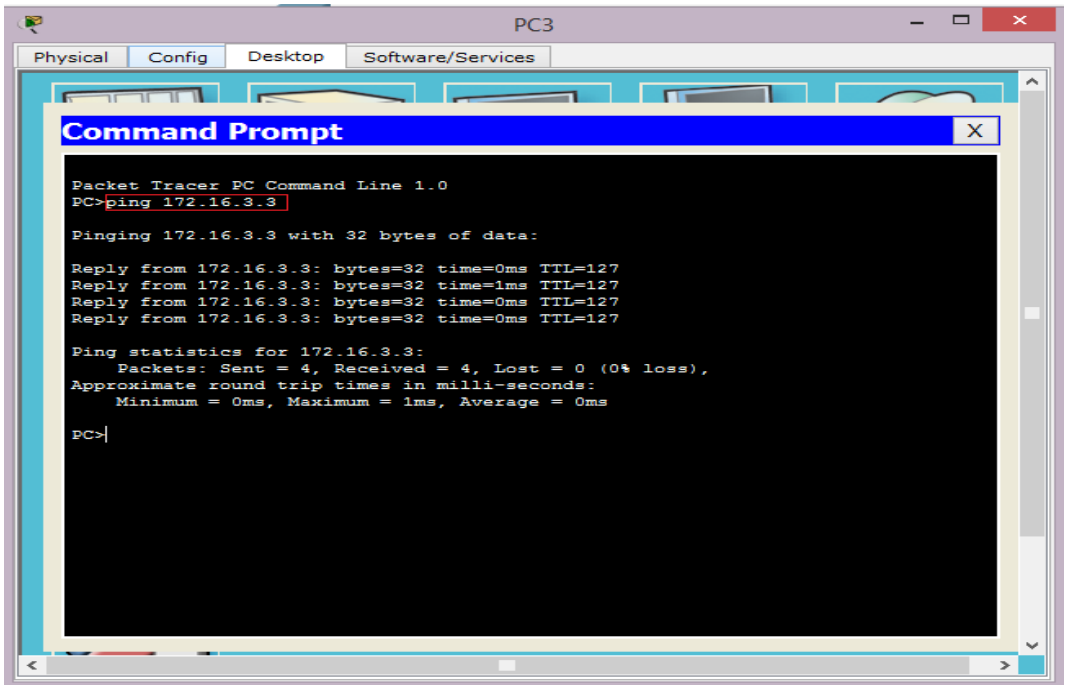

FIGURE 3.42 – Teste de connectivité entre le PC3 et le PC1.

3.5 Conclusion

Dans ce chapitre nous avons apporter des améliorations dans le réseau de l'EPB pour donner un plus au fonctionnement de l'entreprise. Pour cela nous avons opté pour exchange 2013 comme serveur de messagerie locale car il est très facile à manipuler, et nous avons aussi mis en place un outil de sécurité de Microsoft très performant EMET pour empêcher l'exploitation des vulnérabilités logicielles et pour endurcir et sécuriser les systèmes, et nous avons segmenté le réseau de l'entreprise en VLAN dans un switch Fédérateur d'une manière à avoir un réseau fluide, une bande passante optimisée et une organisation souple.

CONCLUSION GÉNÉRALE

Au terme de ce projet, nous avons pu exploiter nos connaissances théoriques et pratiques pour améliorer l'architecture réseau et système de l'entreprise portuaire de Bejaia. Ainsi, Après la présentation du présent projet suivie de l'étude générale de l'architecture réseau de l'EPB, nous avons élaboré la solution à retenir pour avoir une architecture mieux adaptée aux besoins de l'entreprise et nous avons pu mettre en oeuvre quelques-unes.

La mise en oeuvre d'une messagerie électronique interne ou externe, devient de plus en plus la solution de communication et d'échange de données aux seins des grandes entreprises, des grandes institutions. Et c'est le cas de l'entreprise portuaire de Bejaia.

la mise en place du réseau local virtuel (VLAN) nous a permis de segmenter le réseau de l'EPB. Ce travail d'une part n'a pas été facile du point de vu conception car il fallait comprendre le fonctionnement des équipements Cisco et leur fonctionnalité, afin d'augmenter les performances du réseau.

Sachant de plus que l'installation d'EMET offre la protection dès le début contre les failles de sécurité des systèmes, navigateurs internet, Office et autres applications. C'est pour cela son implémentation est importante au sein de l'entreprise.

Durant le stage pratique, la mise en oeuvre de la solutions retenues, n'a pu se faire au niveau de la Direction des Systèmes d'Informations et de la Télécommunication. Néanmoins, une phase de démonstration pratique a été possible grâce à notre ordinateur personnel, nous pouvons noter que notre mise en oeuvre peut etre améliorée en lui rajoutant la mise en place du serveur LMS pour la maintenance des équipements Cisco, l'implémentation des systèmes de détection et de prévention d'intrusion, la configuration des ACL pour le filtrage du trafic sortant et entrant, la configuration du relais SMTP dans la DMZ de l'entreprise après l'implémentation du serveur de messagerie Exchange.

L'intérêt principal que nous avons tiré de cette étude est que nous avons bien affronté la vie professionnelle de notre domaine. Nous avons évalué les différentes étapes de réalisation d'un projet ainsi que les techniques développées par les spécialistes du domaine pour assurer l'efficacité et la bonne réalisation des travaux en se limitant aux ressources et à des durées de temps exactes. Nous avons pu voir la complexité de la mise en route d'un nouveau projet et de sa rapide évolution qui nous a appris à mieux nous organiser afin d'être capable de finaliser notre travail.

BIBLIOGRAPHIE

[1] Dean .T. *Réseaux Informatique, 2ème édition.* les Editions RYNALD GOULET, 2001.

[2] LEMAINQUE Fabrice PILLOU Jean-François. *Tout sur les Réseaux et Internet,3e édition.* Dunod, 2012.

[3] *Http//mtyas.com/2009/05/11/pourquoi-le-web-30-sera-p2p-ou-ne-sera-pas.consulté-le-02/05/2016.*

[4] MOINDJIE Said Mouhamed. *cours sur les réseaux informatique, les équipements d'interconnexions.* site de la technologie, consulté le 04/04/2016.

[5] *COUR CISCO CCNA1,chapitre 3 Médias réseau.* netacad, 2016.

[6] *Cours CISCO CCNA1, chapitre1, les périphériques finaux.* netacad, 2015.

[7] PILLOU jean-François BAY jean philippe. *Tous sur la sécurité informatique.* dunod, 2005.

[8] DESWARTE Ludovic ME Yves. *sécurité des réseaux et système repartis.* Lavoisier, février 2002.

[9] EVENGELISTA Thierry. *les IDS (intrusion detection system).* dunod, 2004.

[10] LORENS Cedric LEVIER laurent. *Tableaux de bord de la sécurité réseau.* Edition eyrolles, 2003.

[11] *DNS, types d'attaques et techniques de sécurisation,p4.* AFNIC, 2009.

[12] CHAIKHI DOUAS Youssef. *les types d'attaques informatiques, module veille et technologie.* 2010.

[13] DENIS Valois BENJAMIN Morin CEDRIC Liorens, LAURENT Levier. *tableaux de bord de la sécurité réseau.* 3eme édition,Edition eyrolles, 2010.

[14] COLLEGE Lionel-Groulx. *publication, politique de sécurité informatique, Page 5.*

[15] Guillaume Desgeorge. *La sécurité des réseaux, Disponible sur http//www.guill.net/.* 2000.

[16] HAMZATA Gueye. *mise en place d'un IDS en utilisant Snort.* Etudes Supérieur en Informatique et Réseau, Diplôme Européen, 2011.

[17] *http//www.supinfo.com/articles/single/338-projet-laboratoire-microsoft-nouveautes-microsft-exchange-server-2013.* consulté-le-09/04/2016.

[18] *COURS CCNA 2 les ACL.consulté-le-10/04/2016.*

[19] *http//www.cisco.com/web/FR/documents/pdfs/datasheet/ios/ciscoworks-lanmanagement-21.pdf.* consulté-le-12/04/2016.

[20] *http//igm.univ-mlv.fr/dr/XPOSE2009/Sonde-de-securite-IDS-IPS/IDS.html.consulté-le-15/04/2016.*

[21] *http//www.commentcamarche.net/contents/966-protection-les-systemes-raid.consulté-le-15/04/2016.*

[22] *http//www.commentcamarche.net/contents/172-fonctionnement-du-courrier-electronique-mta-mda-mua.* consulté-le-03/06/2013.

[23] *file :///D :/M220informatique/mC3A9moire202016/pages20web/relai20avan/livre20RELAIS20smtp.html.* consulté-le-02/06/2016.

[24] *Fiche sur la licence de Windows Server 2012 R2.* Microsoft.

[25] *Service d'annuaire Active Directory.* DIRECTION RECHERCHE ET INGENIERIE DE FORMATION, p 6.

[26] WILLIAM R. STANEK. *Guide de l'administrateur Windows Server 2012.* Microsoft.

[27] JARDON El Hiny Noureddine. *MICROSOFT EXCHANGE.* Thèse en Télécommunications, Ingénierie des Technologies de l'Information, 2014.

[28] *https//support.microsoft.com/fr-fr/kb/2458544.* Consulté-le-01/06/2016.

[29] *https//forum.security-x.fr/tutoriels-317/enhanced-mitigation-experience-toolkit-emet-6874.* Consulté-le-01/06/2016.

[30] M. LIHAN LI NDJOM Hans. *cours sur Les Topologies Physiques des réseaux informatiques, ecole normale supérieur du cameroun.* Consulté-le-26/03/2016.