République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DU **G**ENIE **E**LECTRIQUE ET D'**I**NFORMATIQUE
DEPARTEMENT D'INFORMATIQUE

Mémoire de Fin d'Etudes de MASTER ACADEMIQUE

Domaine : **Mathématiques et Informatique**
Filière : **Informatique**
Spécialité : **Systèmes informatiques**

Présenté par :

Salmi Miliza

Thème

Mise en œuvre d'une solution de messagerie sécurisée et tolérante aux pannes avec Exchange Server

Mémoire soutenu publiquement le 26/09/2019 devant le jury composé de :

Président : Mr M.RAMDANE
Examinatrice : Mme N.SEGHIRI
Encadré par : Mr H.RADJA

Résumé

Notre travail s'inscrit dans le domaine de la sécurité de la messagerie électronique, plus particulièrement la messagerie au milieu professionnel. En effet, étant le moyen de communication le plus déployer et utiliser dans le monde professionnel, le courrier électronique représente un trésor d'informations commerciales sensibles et les données qu'il véhicule ont une valeur économique importante. C'est pourquoi qu'il est la cible préférée des attaquants et des concurrents. Afin de répondre aux besoins de sécurité dans un système de messagerie, nous avons donc choisi l'une des principales solutions de messagerie existante aujourd'hui sur le marché mondial des TICs, en l'occurrence MS Exchange Server, nous l'avons mis en œuvre sur un environnement de travail virtuel et nous avons effectué l'ensembles des tâches de configuration nécessaire pour une messagerie fonctionnelle. Ensuite, nous avons proposé une solution de sécurité et de haute disponibilité basée sur un environnement Exchange que nous avons implémenté et testé sur notre système de messagerie.

Mots clés : Exchange Server, messagerie électronique, Haute disponibilité, sécurité, cryptographie, Active Directory.

Table des matières

Table des figures

Introduction Générale

Les technologies de l'information et de la communication TIC ont profondément changé la méthode de travail à l'intérieur des entreprises avec l'émergence des outils facilitant l'échange et le partage d'informations entre ses différents services.

Parmi ces technologies, la messagerie électronique qui en constitue l'application la plus marquante et la plus déployée au milieu professionnel grâce aux avantages de cout, de simplicité et d'efficacité qu'elle présente par rapport aux technologies antérieurs comme le fax ou le téléphone.

En revanche, si la messagerie électronique peut être aussi bénéfique pour l'entreprise, elle peut facilement causer la faillite de celle-ci puisque le courrier électronique s'est révélé lui-même à représenter un vecteur de menace considérable, fournissant un itinéraire pour une variété d'attaques, y compris les logiciels malveillants, le Phishing et les spams. Assurer la sécurité et la disponibilité d'un système de messagerie devient donc un véritable défi.

Dans ce contexte, l'objectif principal de notre travail est d'assurer la sécurité et la tolérance aux pannes d'un système de messagerie basé sur Microsoft Exchange Server 2013.

Organisation du mémoire

Notre travail est reparti sur quatre chapitres :

— Le premier chapitre traite des concepts de base relatifs aux réseaux informatiques, leurs objectifs, classification, architectures, ... etc.

— Le deuxième chapitre est consacré à la messagerie électronique dont nous allons aborder son fonctionnement, son architecture générale, son usage au milieu professionnel ainsi que les différents protocoles qu'elle utilise et enfin nous allons présenter quelques outils existant sur le marché.

— Dans le troisième chapitre, nous allons aborder la notion de sécurité dans le monde de la messagerie électronique, les différentes menaces et la façon de se protéger.

— Dans le quatrième chapitre, nous détaillerons les différentes étapes nécessaires pour la mise en place de notre solution de messagerie, sa configuration

ainsi que l'implémentation de la solution de sécurité et de haute disponibilité proposé.

Nous terminerons ce mémoire par une conclusion générale qui contiendra une Synthèse et quelques perspectives envisagées pour ce travail.

Chapitre 1

Généralité sur les réseaux

1.1 Introduction :

En informatique le besoin est la source d'une créativité, et les réseaux informatiques sont le fruit du besoin de transporter une information d'une personne à une autre. Cette communication qui pendant longtemps s'est faite directement par l'homme, comme dans les réseaux postaux ou via des moyens sonores tel-que la téléphonie.

Autrefois réservés aux seules entreprises, les réseaux informatiques touchent aujourd'hui tous les utilisateurs d'ordinateurs, en particulier ceux connectés a internet. ils permettent de mettre en œuvre des applications très diverses, des plus simples aux plus sophistiquées.

Ce chapitre introductif décrit les concepts de base relatifs aux réseaux informatiques, leurs objectifs, leurs classification et bien d'autres notions.

1.2 Définition d'un réseau informatique :

Un réseau informatique est un ensemble de composants matériels ou logiciels reliés entre eux grâce a des lignes de communication (câbles réseaux, liaisons sans fils, etc.) dans le but de permettre aux utilisateurs de partager des ressources et d'échanger des informations sous forme de données numériques.[Dromard 09]

1.3 Intérêt d'un réseau informatique

Un ordinateur est une machine permettant de manipuler des données. L'homme en tant qu'être communiquant, a rapidement compris l'intérêt qu'il pouvait y avoir a relier ces ordinateurs entre eux afin de pouvoir échanger des informations. [Lemainque 12]

Un réseau informatique a divers intérêts :

— **Le partage de ressources :**

Le partage de ressources (fichiers, applications ou matériels) est l'une des raisons justifiant la mise en place d'un réseau informatique, il est en effet intéressant de rendre accessible a une communauté d'utilisateurs des ressources indépendamment de leur localisation.

— **La communication entre personnes** (courrier électronique, vidéo conférences,etc.).

— **La communication entre processus** (entre des machine industrielles par exemple).

1.4 Classification des réseaux informatiques

1.4.1 Classification selon l'étendu :

On distingue généralement quatre catégories de réseaux informatiques, différenciées par la distance maximale séparant les points les plus éloignés du réseau :

- Les réseaux personnels, ou PAN (Personal Area Network), Interconnectent sur quelques mètres des équipements personnels tels que les téléphones portables, PDA(Personal Digital Assistant), etc.
- Les réseaux locaux, ou LAN (Local Area Network), Un réseau local peut s'étendre de quelques mètres à quelques kilomètres et correspond au réseau d'une entreprise.
- Les réseaux métropolitains, ou MAN (Metropolitain Area Network), permettent l'interconnexion des entreprises ou éventuellement des particuliers sur un réseau spécialisé à haut débit qui est géré a l'échelle d'une métropole, il sert généralement à interconnecter des réseaux locaux distants de quelques kilomètres.
- Les réseaux étendus, ou WAN (Wide Area Network), permettent la communication sur des distances à l'échelle d'un pays, voire d'un continent ou de plusieurs continents. Le réseau est soit terrestre, et il utilise dans ce cas des infrastructures au niveau du sol, essentiellement de grands réseaux de fibre optique, soit hertzien, comme les réseaux satellites.

La figure suivante illustre sommairement ces grandes catégories de réseaux informatiques.

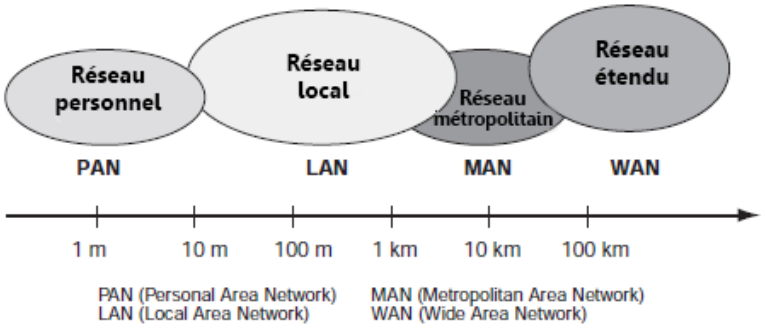

FIGURE 1.4.1 – Les grandes catégories de réseaux informatiques

1.4.2 Classification selon la topologie

La topologie décrit la manière dont les équipements réseau sont connectés entre eux. On distingue deux types de topologies :

1.4.2.1 Topologie physique

Cette topologie décrit l'arrangement physique, c'est-à-dire la façon dont les machines sont raccordées au réseau. On distingue généralement les topologies suivantes :

— **La topologie en Bus :**
Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus les ordinateurs sont reliés a une même ligne de transmission par l'intermédiaire de câbles, généralement de type coaxial.[Lemainque 12] Cette topologie a pour avantage d'être facile a mettre en œuvre. En revanche, elle est extrêmement vulnérable étant donné que si le bus tombe en panne, l'ensemble du réseau est affecté.

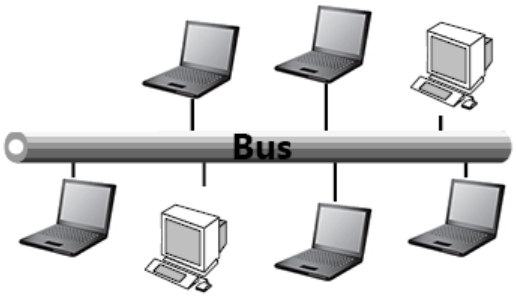

FIGURE 1.4.2 – La topologie en bus

— **La topologie en étoile :**
Dans une topologie en étoile, les ordinateurs du réseau sont reliés a un nœud central qui a pour rôle d'assurer la communication entre les différents ordinateurs. Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une connexion peut être débranchée sans paralyser le reste du réseau. Le point névralgique de ce réseau est le nœud central, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible.

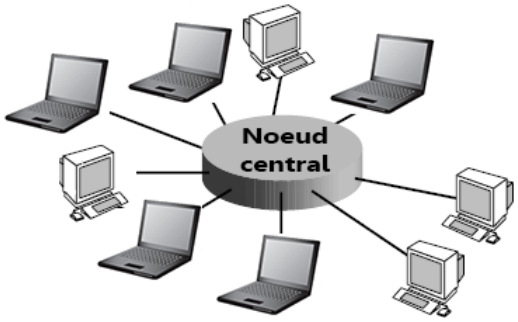

FIGURE 1.4.3 – La topologie en étoile

— **La topologie en anneau :**
Dans une topologie en anneau, les ordinateurs sont théoriquement situés sur une boucle et communiquent chacun a son tour, Ils sont en réalité reliés a un répartiteur (MAU, Multistation Acess Unit) qui va gérer la communication entre eux en affectant a chacun un temps de parole.[Lemainque 12] Cette topologie a pour avantage d'être moins couteuse et son implémentation ne nécessite pas beaucoup de temps. En revanche, le temps de transmission de l'information peut être très long puisqu'il est influencé par le nombre de machine du réseau.

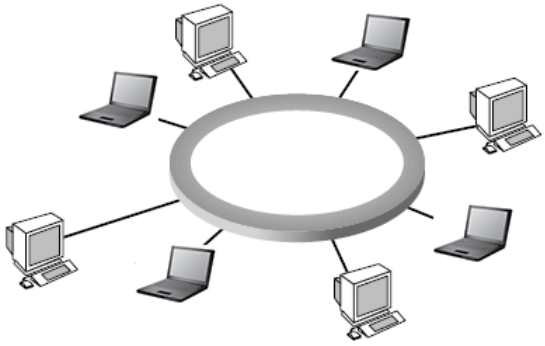

FIGURE 1.4.4 – La topologie en anneau

— **La topologie en arbre :**
Dans une topologie en arbre, le réseau est divisé en niveaux dont, le noeuds du sommet est relié aux nœuds du niveau inférieur qui eux même peuvent être relier a d'autres nœuds de niveau inférieur. Cette topologie a pour avantage d'être facile à gérer et représente un bon choix pour les grandes entreprises. L'inconvénient

majeur est que la panne des éléments centraux entraine la panne du réseau en entier.

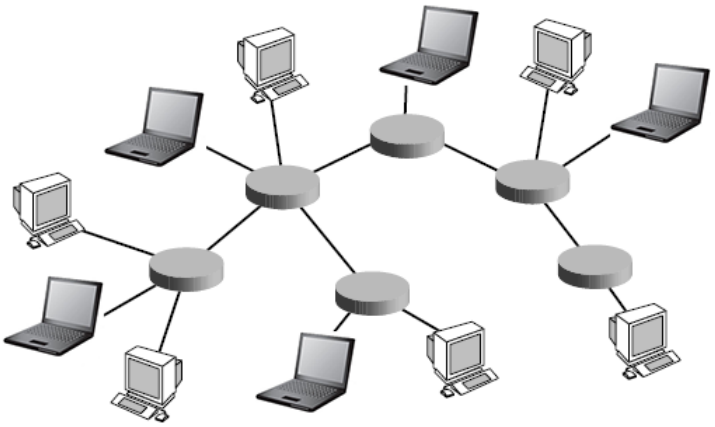

FIGURE 1.4.5 – La topologie en arbre

— **La topologie maillée :**
La topologie maillée est une topologie réseau hybride de type étoile mais avec différents chemins pour accéder d'un nœud à un autre. L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé lorsque le nombre de terminaux l'est.

FIGURE 1.4.6 – La topologie maillée

1.4.2.2 Topologie Logique

La topologie logique, par opposition a la topologie physique, représente la façon dont les données transitent dans les lignes de communication. Les topologies les plus courantes sont :

— **Ethernet :**
Le principe d'Ethernet repose sur un bus partagé : chaque station est autorisée à émettre sur la ligne à n'importe quel moment et sans notion de priorité entre les machines mais, quand deux stations émettent en même temps, il se produit une collision. Dans ce cas, les émissions sont stoppées et au bout d'un laps de temps aléatoire, une autre tentative est faite.

On distingue différentes variantes de technologies Ethernet suivant le diamètre des câbles utilisés :

Technologie	Type des câbles	Vitesse	Portée
10 Base-2	Câble coaxial de faible diamètre	10 Mb/s	185m
10 Base-5	Câble coaxial de gros diamètre	10 Mb/s	500m
10 Base-T	Double paire torsadée	10 Mb/s	100m
100 Base-Tx	Double paire torsadée	100 Mb/s	100m
1000 Base-Sx	Fibre optique	1000 Mb/s	500m

FIGURE 1.4.7 – Les technologies Ethernet

— **L'anneau à jeton :**
L'anneau à jeton (en anglais Token-Ring) est une technologie d'accès au réseau sur le principe de la communication au tour à tour, c'est-à-dire que chaque station attend de disposer d'un jeton (matérialisé par une trame d'un format particulier) avant d'émettre une trame. Le jeton circule de station en station, formant un anneau et lorsqu'un ordinateur est en possession du jeton il peut émettre pendant un temps déterminé, après lequel il remet le jeton à l'ordinateur suivant.

— **FDDI :**
FDDI (Fiber Distributed Data Interface) est une technologie d'accès au réseau sur des lignes de type optique. Un réseau FDDI est constitué d'un double anneau ce qui permet de garantir le fonctionnement du réseau en cas de défaillance d'un lien ou d'un nœud. [Servin 06]

Quel type de réseau retenir ? Ethernet (gestion des collisions sur un bus) ou Token-Ring (gestion d'un jeton sur un anneau) ?

Question performances, les deux se valent, même si, a débit égal, il y a un léger avantage a utiliser Token-Ring. En effet a l'inverse du bus partagé dont l'accès est aléatoire, la technique du jeton est plus déterministe : chaque station parle a tour de rôle au bout d'un laps de temps fixe qui dépend du nombre de stations (le temps pour le jeton de faire le tour de l'anneau). La bande passante est mieux exploitée avec Token-Ring, ce qui le rend plus performant. Cependant, Ethernet détient plus de 85% du marche et a toujours été en avance sur Token-Ring.

En résumé, si l'on doit créer soi-même un réseau a partir de rien, autant se lancer

dans Ethernet : c'est plus simple, plus évolutif et présente un meilleur compromis coût/performances.

Si dans une entreprise, Token-Ring est déjà bien implanté, on peut envisager de poursuivre dans cette voie. Mais une migration vers Ethernet est toujours envisageable.[Montagnier 01]

Token-Ring ou FDDI ?

Si vous êtes face a un tel choix procéder sans doute au FDDI car la disponibilité est un facteur très important dans les réseaux informatique et ce concept est implémenter dans le FDDI par la paire d'anneaux et absent dans le Token-Ring.

1.5 La transmission de données

1.5.1 Représentation des données :

Le but d'un réseau est de transmettre des informations d'un ordinateur a un autre. Pour cela il faut dans un premier temps décider du type de codage de la données a envoyer c'est-à-dire sa représentation informatique. Celle-ci sera différente selon le type de données, car il peut s'agir de : données sonores, textuelles, graphiques, vidéo, etc. On distingue deux types de représentations : La représentation numérique et la représentation analogique. [Lemainque 12]

La différence entre les deux représentations réside dans le fait qu'en analogique, les informations sont traduites en impulsions électriques d'amplitude variable. Dans la représentation numérique, l'information est codée en un ensemble de valeurs binaires dont chaque bit représente deux amplitudes distinctes.

1.5.2 Les supports de transmission :

Les supports de transmission sont les composants physiques permettant de transmettre les éléments binaires, suites de 0 et de 1, représentant les données a transmettre. Ces derniers sont nombreux, parmi ceux-ci, trois familles sont à distinguer : Les supports métalliques (comme les paires torsadées et les câbles coaxiaux qui servent a transmettre des courants électriques), immatériels (communications sans fil qui transmettent des ondes électromagnétiques), et les supports de verre ou de plastique (comme les fibres optiques, qui transmettent de la lumière)

— **Câbles coaxiaux :** Un câble coaxial est constitué d'une partie centrale (appelée âme), c'est-à-dire un fil de cuivre, enveloppé dans un isolant (permet de limiter les perturbations dues au bruit externe), puis d'un blindage métallique tresse et enfin d'une gaine extérieure. Il existe deux grandes catégories de câbles coaxiaux :

— **Câble coaxial fin (Thinnet) :** Le Thinnet ou simplement le 10Base2 est un câble fin de diamètre de 6mm, il permet de transporter un signal sur une distance d'environ 185 mètres sans affaiblissement.
— **Câble coaxial épais (Thicknet) :** Le Thicknet ou le 10Base5 est un câble épais de diamètre de 12mm, il permet de transporter un signal sur une distance d'environ 500 mètres sans affaiblissement.[Goupille 05]

Concernant la notation 10Base2 et 10Base5 : le 10 indique le débit en Mbps (mégabits par seconde), le B indique la façon de coder les 0 et les 1, soit ici la bande de Base, le dernier chiffre indique la taille maximale du réseau, exprimée en mètres et divisée par 100.

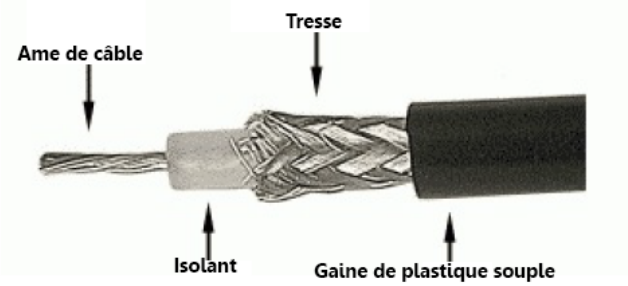

FIGURE 1.5.1 – Coupe d'un câble coaxial

Un câble coaxial a pour avantage d'être simple, peu couteux et facilement manipulable. Il est aujourd'hui obselet et remplacé par le câblage à paire torsadée.

— **Câble électrique à paire torsadée :**

Un câble à paire torsadée est le support de transmission le plus simple, il est souvent fabriqué a partir de plusieurs paires torsadées regroupées et placées à l'intérieur de la gaine protectrice.

Pourquoi on torsade les fils ?

Parce que cela permet une meilleure protection du signal électrique. En effet, on s'est rendu compte qu'en torsadant les fils, le câble était moins sujet a des perturbations électromagnétiques

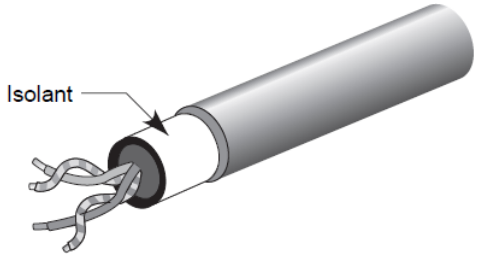

FIGURE 1.5.2 – Coupe d'un câble à paire torsadée

La paire torsadée est adaptée à la transmission de l'information sur de courtes distances. Si la longueur du fil est peu importante, de quelques centaines de mètres a quelques kilomètres, des débits de plusieurs mégabits par seconde peuvent être atteints. Sur des distances plus courtes, on peut obtenir des débits de plusieurs dizaines de mégabit par seconde voir quelques centaines de mégabits par seconde pour des distances plus réduite.[Pujolle 08]

La paire torsadée a aussi l'avantage d'être simple, peu couteuse et facilement manipulable mais, sur de longues distances la paire torsadée n'assure pas l'intégrité des données.

— **Fibre optique :**

Une fibre optique est un cylindre constitué d'un brin central en fibre de verre ou en plastique extrêmement fin et entourée d'une gaine protectrice. Chaque fibre optique gainée de plastique de manière a l'isoler des autres.

L'avantage des fibres optiques est qu'elles permettent de réaliser des liaisons a grandes distances et offrent l'avantage d'être pratiquement insensibles a un environnement électrique ou magnétique.[Goupille 05]

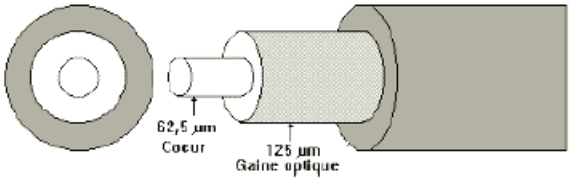

FIGURE 1.5.3 – La fibre optique

Quel type de câble choisir ?

Éternel débat que celui du choix des câbles, chaque constructeur ayant des arguments en faveur de son produit. De nombreuses combinaisons techniques viennent compliquer le choix. Pour résoudre ce dilemme, un certain nombre de questions sont à se poser.

— **Cuivre ou fibre optique ?**

L'avantage de la fibre optique est qu'elle permet de s'affranchir des contraintes de distance (plusieurs centaines de mètres au minimum contre quatre-vingt-dix mètres pour le cuivre). Cela tient a l'atténuation du signal, beaucoup plus importante sur un câble en cuivre.

En revanche, le coût global d'un système de câblage en fibre optique est plus élevé que son équivalent en cuivre. En effet, l'ingénierie nécessaire pour poser des câbles optiques (raccordement des connecteurs et test) est plus complexe et plus couteuse qu'avec des câbles en cuivre.

Il faut ajouter à cela le coût des équipements actifs (les commutateurs et cartes Ethernet), deux fois plus chers en version fibre optique, et pour une densité de ports deux fois moins élevée que leur équivalent en cuivre.

En conclusion, le câble en cuivre sera privilégié pour la distribution, et la fibre optique pour la connexion entre les locaux techniques.

— **Coaxial ou paire torsadée ?**

Le câble coaxial n'est plus utilisé pour les réseaux locaux. Il pourra cependant être posé pour des besoins spécifiques. En revanche, la paire torsadée est le standard pour l'informatique et la téléphonie.

1.6 Modèles de communication réseau

Afin de faire communiquer des machines entre elles, le plus simple était de partir de ce que nous connaissons déjà de la communication, en effet la communication nécessite la présence d'un émetteur, récepteur, un support de transmission et d'une langue. Les chercheurs ont travaillé pour faire passer les principes de communication humaines a des principes de communication pour ordinateurs. Ils ont ainsi regroupé l'ensemble de leurs recherches et de leurs résultats dans des normes que devront respecter toute personne qui communique. Il s'agit du modèle OSI et le modèle TCP/IP.

1.6.1 Le modèle OSI :

Le modèle OSI (Open System Interconnexion) a été mis en place par l'ISO (International Standard Organisation). Ce modèle est une norme qui préconise comment les ordinateurs devraient communiquer entre eux. Le modèle OSI est un modèle qui comporte 7 couches et chaque couche ne peut communiquer qu'avec une couche adjacente.

Les différentes couches du modèle OSI sont définies dans la figure suivante :

1.6.1.1 Les couches du modèle OSI :

— **La couche physique :**

Définit la façon dont les données sont physiquement converties en signaux numériques sur le média de communication, les unités de données sont des bits 0 ou 1.

— **La couche liaison de données :**

Cette couche permet le transfert de l'information sous forme de trames, détection et correction d'erreurs et le partage du média de transmission. L'unité de donnée à ce niveau est la trame.

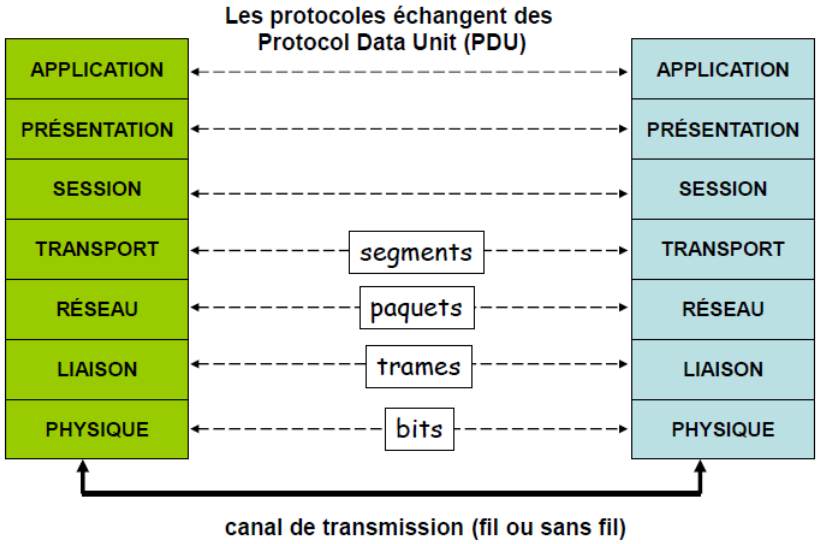

FIGURE 1.6.1 – Les couches du modèle OSI

— **La couche réseau :**
Permet de gérer l'adressage et le routage des données, c'est-à-dire leur acheminement via le réseau. L'unité de données s'appelle le paquet.

— **La couche transport :**
Assure le transport de données entre les entités de session, la procédure de connexion et déconnexion et le contrôle de flux. L'unité de donnée à ce niveau est le message.

— **La couche session :**
Assure l'ouverture et la fermeture de sessions de communication entre les machines du réseau.

— **La couche présentation :**
Cette couche met en forme les informations échangées pour les rendre compatibles avec l'application destinataire (traduction des formats, compression, encryptage, etc.). Elle s'intéresse à la syntaxe des informations.

— **La couche application :**
C'est la couche OSI la plus prés de l'utilisateur, elle fournit des services réseau aux applications de l'utilisateur (exemple : navigateur).

1.6.2 Le modèle TCP/IP :

Dans les années 70, le département de la défense américain, ou DOD (Department Of Defense), décide devant le foisonnement de machines utilisant des protocoles de communication différents et incompatibles, de définir sa propre architecture. Cette architecture, dite TCP/IP (Transmission Control Protocol / Internet

Protocol), est à la source du réseau Internet.[Pujolle 08]

Le modèle TCP/IP est un modèle qui comporte 4 couches.

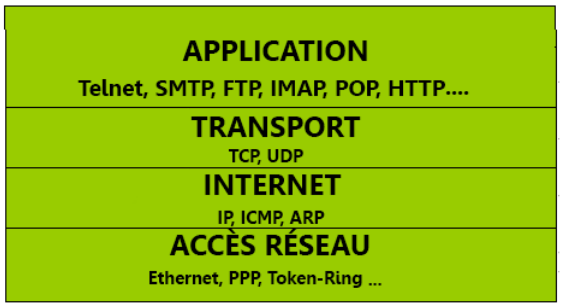

FIGURE 1.6.2 – Les couches du modèle TCP/IP

1.6.2.1 Les couches du modèle TCP/IP :

— **La couche Accès réseau :**

Elle regroupe toutes les fonctions des couches de niveaux 1 et 2 du modèle OSI. Les tâches réalisées par cette couche sont : La constitution de la trame, la gestion d'erreurs sur les trames fournies par la couche supérieure, l'accès au média de transmission et la transmission sur les supports physiques.

— **La couche Internet :**

Les rôles de cette couche sont similaires à ceux de la couche réseau du modelé OSI. Les trames crées par la couche internet porte ici le nom de trames IP.

— **La couche Transport :**

Selon les applications employées, les différents types de connexion, les protocoles TCP (Transmission Control Protocol) et UDP (User Data Protocol) permettent de mettre en place un transfert des données en mode connecté ou en mode sans connexion pour chacun des messages fournis par les applications.

— **La couche Application :**

Englobe les applications standard du réseau. Intègre aussi les services et présentation. Le modèle TCP/IP regroupe en une seule couche tous les aspects liés aux applications et suppose que les données sont préparées de manière adéquate pour la couche suivante.

1.7 Quelques protocoles utilisés par le modèle TCP/IP

Un protocole est un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau. Il en existe plusieurs selon ce que l'on attend de la communication.

Sur internet, les protocoles utilisés font partie d'une suite de protocoles, c'est-à-dire un ensemble de protocoles qui fonctionnent ensemble.La suite de protocole TCP/ IP, contient entre autres les protocoles suivants :

Le protocole IP :

Sur internet, les ordinateurs communiquent entre eux grâce au protocole IP (Internet Protocol) decrit dans la RFC 791, ce dernier utilise des adresses numériques, appelées adresses IP. C'est l'ICANN (Internet Corporation for Assigned Names and Numbers, remplaçant l'IANA, Internet Assigned Numbers Agency, depuis 1998) qui est chargée d'attribuer des adresses IP publiques, c'est-à-dire les adresses IP des ordinateurs directement connectés sur le réseau public Internet. Ces adresses servent aux ordinateurs du réseau pour communiquer entre eux, ainsi chaque ordinateur d'un réseau possède une adresse IP unique sur le réseau.

Les versions du protocole IP : Le protocole IP existe sous les versions suivantes :

— **IPV4 :**

Une adresse IPV4 est une adresse 32bits, généralement notée sous forme de 4nombres (4octets) compris entre 0 et 255. L'adresse est constituée de deux parties : un identificateur de réseau (désigne le réseau) et un identificateur de la machine pour ce réseau (désigne les ordinateurs de ce réseau). La séparation entre l'identificateur du réseau et celui de la machine se fait avec le masque de sous réseau.

Masque de sous-réseau : On appelle masque de sous-réseau (subnet mask), la séparation entre l'identificateur du réseau et celui de la machine dans une adresse IP. Le masque est précisé en binaire par des 1 pour la partie réseau et des 0 pour la partie ordinateur.

Les limites de L'IPV4 :

Le protocole IPV4 permet d'utiliser un peu plus de quatre milliard d'adresses différentes pour connecter les ordinateurs et les autres appareils reliés au réseau. Du temps des débuts d'internet, cela paraissait plus que suffisant, il était pratiquement impossible d'imaginer qu'il y aurait un jour suffisamment de machines sur un unique réseau pour que l'on commence a manquer d'adresses disponibles.

[Lemainque 12] Cette limite conduit à la transition d'IPV4 vers l'IPV6, actuellement en cours de déploiement, qui devrait progressivement le remplacer.

— **IPV6 :**

Une adresse IPV6 est une adresse 128bits, la représentation s'effectue par groupe de 16bits et se présente sous la forme suivante : xxxx : xxxx : xxxx : xxxx : xxxx : xxxx : xxxx : xxxx ou chaque x représente un chiffre hexadécimal et chaque xx représente 1 octet. On distingue 3 types d'adresses IPV6 : Adresse de monodiffusion (identifie un seul nœud), Adresse de multidiffusion (identifie un groupe de nœuds), Adresse Anycast (identifie un nœud parmi un groupe de nœuds).

Avantage de l'IPV6 :

–Supporter des billions de machines.

–Réduire les tailles des tables de routage.

–Offrir une meilleure sécurité.

–Simplifier le protocole pour accélérer le routage.

Le protocole TCP :

Le protocole TCP (Transmission Control Protocol) décrit dans la RFC 793 est l'un des principaux protocoles de la couche transport du modèle TCP/IP. Il permet, au niveau des applications, de gérer les données en provenance (ou a destination) de la couche inférieur du modèle. Lorsque les données sont fournies au protocole IP celui-ci les encapsule dans des datagrammes IP. TCP est un protocole fiable créant une connexion bidirectionnelle entre 2 ordinateurs. L'expéditeur s'attend à une confirmation du destinataire sur réception.

Le protocole UDP :

Le protocole UDP (User Data Protocol) est utilisé au-dessus du protocole IP et fonctionnant dans un mode sans connexion. UDP prend en charge toutes les applications n'ayant pas besoin de contrôle et demandant un temps de réaction faible, comme la parole téléphonique. C'est un protocole non fiable, ne garantissant pas la livraison du paquet, ne délivrant aucune confirmation de réception et ne maintient aucune connexion entre les ordinateurs.

Le protocole TELNET :

Le protocole TELNET est un protocole permettant à un équipement terminal de se connecter à un serveur distant.

Le protocole FTP :

Le protocole FTP (File Transfert Protocol) est un protocole de transfert de fichiers, il a été développé dans le cadre d'internet pour garantir une qualité de service, c'est-à-dire le fichier arrive correctement et en entier au récepteur. L'application FTP est de type client-serveur avec un client FTP et un serveur FTP. Le logiciel propose un mode avec connexion, de telle sorte que l'émetteur et le récepteur se mettent d'accord sur les caractéristiques de la transmission.

Le protocole SMTP :

Le courrier électronique au sein d'internet est géré par le protocole SMTP bâtis sur TCP. Il permet l'échange de message entre un émetteur et un ou plusieurs récepteurs pourvus que leurs adresses soient connues.

Le protocole HTTP :

Le protocole HTTP (HyperText Transfert Protocol) décrit dans la RFC 2616, est le protocole définit pour le web, c'est un protocole de gestion du transfert de fichier hypertexte entre serveur et client Web.

Le protocole ICMP :

Le protocole ICMP (Internet Control Message Protocol) est un protocole de notification d'erreurs (réseau coupé, échéances temporelles) permettant d'informer l'expéditeur en cas d'anomalies de fonctionnement.

1.8 Équipement d'interconnexion

Un réseau est constitué d'ordinateurs reliés par un ensemble d'éléments matériels et logiciels. Les éléments matériels permettant d'interconnecter les ordinateurs sont les suivants :

— **La carte réseau :**
La carte réseau (coupleur) est une carte connectée sur la carte mère de l'ordinateur ou partie intégrante de la carte mère qui relie a l'aide d'un câble ou d'ondes radios un ordinateur au reste du réseau.

— **Les commutateurs :**
Un commutateur (switch) est un équipement agissant au niveau 2 du modèle OSI qui offre une connexion directe entre les ordinateurs sources et destinations autrement dit le commutateur analyse les trames arrivant sur ses ports d'entrée et filtre les données afin de les aiguiller uniquement sur les ports adéquats.

— **Les concentrateurs :**
Un concentrateur (hub) est un équipement permettent de connecter entre eux plusieurs hôtes, son rôle est de récupérer les données binaires parvenant sur un port et de le diffuser sur l'ensemble des ports.

— **Les routeurs :**
Un routeur permet de relier de nombreux réseaux locaux de telles façons a permettre la circulation de données d'un réseau a un autre de la façon optimale c'est-à-dire il examine l'entête du paquet afin de déterminer le meilleur itinéraire par lequel acheminer le paquet.

— **Les passerelles :**
Afin qu'il y ai une communication entre deux réseaux il faut les interconnecter pour qu'ils puissent échanger des informations. Le nœud qui joue le rôle d'intermédiaire s'appelle la passerelle ou gateway.

— **Les ponts :**
Le pont est un équipement agissant au niveau 2 du modèle OSI qui permet de filtrer les trames et laisse passer les blocs destinés au réseau raccordé seulement. Ainsi le pont permet de segmenter un réseau en conservant au niveau du réseau local que les trames destinées au niveau local et en transmettant les trames destinées aux autres réseaux. Cela permet de réduire le trafic sur chacun des réseaux et d'augmenter le niveau de confidentialité car les informations destinées a un réseau ne peuvent pas être écouter par les autres réseaux.

— **Les répéteurs :**
Le répéteur est un équipement simple qui travaille au niveau de la couche 1 du modèle OSI et qui permet de régénérer le signal entre deux nœud du réseau, ce qui permet d'étendre la distance de câblage d'un réseau.

1.9 Architecture réseau

1.9.1 L'architecture Poste à Poste (Peer to Peer)

Dans l'architecture Peer to Peer (P2P) il n'y a pas de nœud central, chaque ordinateur fait office de client et de serveur a la fois, autrement dit chacun des ordinateurs du réseau est libre de partager ses ressources.

La figure suivante illustre l'architecture peer to peer :

Les avantages d'une architecture P2P

— Un coût réduit.
— La simplicité.

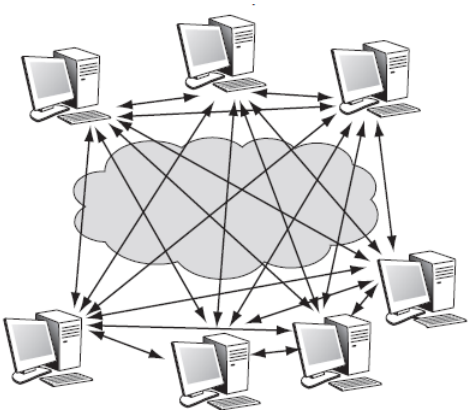

FIGURE 1.9.1 – L'architecture Peer to Peer

Les inconvénients d'une architecture P2P

les réseaux P2P ont énormément d'inconvénients.
— Très difficile a administrer.
— La sécurité est très peu présente.
— Valable pour de petits nombre d'ordinateurs et pour des applications ne nécessitant pas une grande sécurité.

1.9.2 L'architecture Client/Serveur

L'architecture client/serveur désigne un mode de communication entre un client et un serveur ou le client est un processus qui demande l'exécution d'un service au serveur qui accompli ces services et envoie en retour des réponses. Ces services sont des programmes fournissant des données.

1.9.2.1 Fonctionnement d'un système client/serveur

Un système client/serveur fonctionne selon le schéma suivant :
— Le client émet une requête vers le serveur dans laquelle il demande un service.
— Le serveur reçoit la demande, la traite et renvoie la réponse au client.
La figure suivante illustre ce fonctionnement :

1.9.2.2 Les notions de base de l'architecture client/serveur

Le client : est un processus qui demande l'exécution d'une tâche a un processus serveur par l'envoie de requête contenant le descriptif de l'opération a exécuter.

Le serveur : est un processus accomplissant une opération sur demande d'un client, et lui transmettant la réponse.

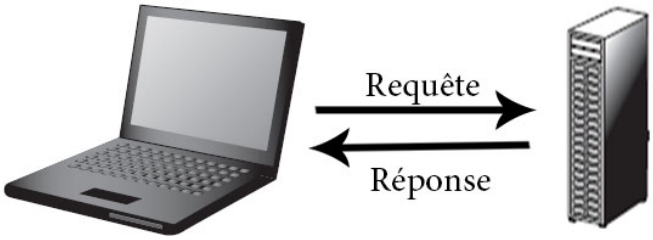

FIGURE 1.9.2 – Communication Client/Serveur

La requête : désigne le message envoyer du client au serveur décrivant l'opération a exécuter.

La réponse : désigne le message transmit par un serveur à un client suite à l'exécution d'une opération. contenant le résultat de l'opération.

Le service : c'est le travail fourni par le serveur suite a la requête du client. Le serveur est fournisseur de services aux clients qui sont des consommateurs.

1.9.2.3 Les différentes architectures Client/Serveur

L'architecture client/serveur à 2-tiers :

Cette architecture caractérise les systèmes clients/serveurs pour lesquels le client demande une ressource et le serveur la lui fournit directement, en utilisant ses propres ressources, sans faire appel à d'autres intermédiaires.

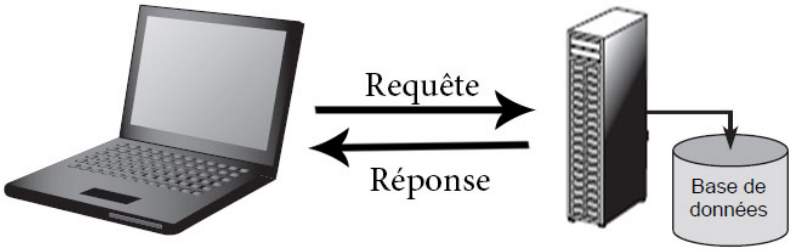

FIGURE 1.9.3 – Architecture client/serveur à 2-tiers

L'architecture client/serveur à 3-tiers :

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

— Le client (niveau 1) : demandeur de ressource.

— Le serveur d'application (niveau 2) : est chargé de fournir la ressource au client mais qui fait appel a un autre serveur pour certaines demandes de

ressources. Le niveau deux lui-même est le client d'un serveur de base de données.
— Le serveur de base de données (niveau 3) : fournit les ressources au serveur d'application.

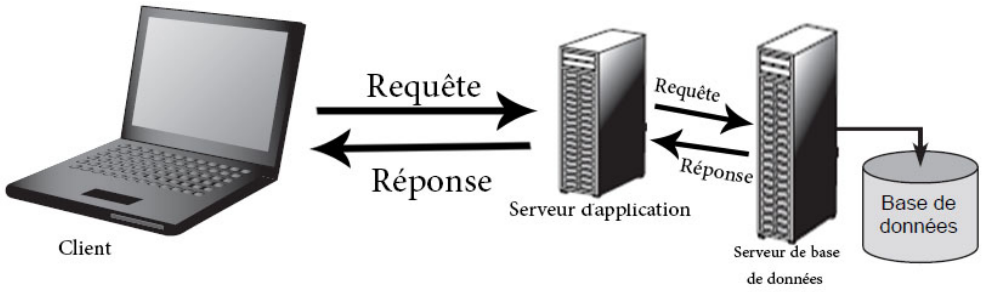

FIGURE 1.9.4 – Architecture client/serveur à 3-tiers

L'architecture client/serveur à n-tiers :

Une architecture à n-tiers va plus loin dans le découpage de l'application sur différents serveurs. Elle est également appelée architecture distribuée du fait de la distribuions des traitements et des données sur différents serveurs. Le découpage de base du système reste toujours le même, toutefois les deux parties développées côté serveur vont pouvoir être déployées chacune sur plusieurs serveurs.

L'objectif général de ce type d'architecture est de permettre l'évolutivité du système sous plusieurs aspects :
— la quantité de données stockée
— La disponibilité du serveur
— ...etc.

1.9.2.4 Les différents types de serveur

Les serveurs jouent de nombreux rôles dans l'environnement client/serveur dont certains sont configurés pour l'authentification, certains pour exécuter des applications et d'autres fournissent des services aux utilisateurs. En tant qu'administrateur système, la connaissance des principaux types de serveurs et les fonctions qu'ils exécutent sur le réseau est une chose indispensable.

Il existe plusieurs types de serveurs dont les plus utilisés sont les suivants :

Serveur de fichiers :

Un serveur de fichier permet de partager des données a travers un réseau, il désigne généralement l'ordinateur sur lequel est installé le logiciel applicatif . Cet ordinateur possède généralement un gros espace disque (plusieurs centaines de GO, voire TO), ou sont déposés les fichiers, que les utilisateurs peuvent récupérer au moyen d'un protocole de partage de fichiers.

Serveur DNS :

DNS (Domain Name System) est le service de résolution de nom d'hôte, il permet d'associer un nom d'une machine a une adresse IP et inversement d'associer une adresse IP a un nom de domaine. Le service DNS est essentiel aux réseaux et surtout à Internet. Il est utilisé par tous même si les utilisateurs ne le réalisent pas.

Par exemple, lorsque vous ouvrez un navigateur et vous pointez sur `http://www.google.fr`, votre PC envoie une requête à votre serveur DNS qui lui dit `www.google.fr=216.58.205.36` et votre navigateur sollicite en réalité `http://216.58.205.36`.

Serveur DHCP :

Un serveur DHCP (Dynamic Host Configuration Protocol) est un serveur qui délivre dynamiquement des adresses IP aux ordinateurs qui se connectent sur le réseau. Le processus d'attribution d'adresses se déroule en quatre phases :

- **Découverte (DHCP DISCOVER) :** Le client envoie une demande de configuration sur le réseau en diffusion, cette demande comporte entre autres l'adresse physique (MAC) du client.
- **Offre (DHCP OFFER) :** Tout serveur DHCP ayant reçu cette demande, s'il est en mesure de proposer une adresse sur le réseau auquel appartient le client, diffuse une offre DHCP. Cette offre comporte l'adresse IP du serveur, ainsi que l'adresse IP et le masque de sous réseau. Il se peut que plusieurs offres soient adressées au client.
- **Demande (DHCP REQUEST) :** Le client retient une des offres reçues (la première qui lui parvient), et diffuse sur le réseau un datagramme de requête.
- **Accusé de réception (DHCP ACK pour acknowledgement) :** Le serveur DHCP choisi élabore un datagramme d'accusé de réception qui assigne au client l'adresse IP et son masque de sous réseau, la durée du bail et éventuellement d'autre paramètres :
  - adresse Ip de la passerelle par défaut.
  - adresse IP des serveurs DNS.

— adresse IP des serveurs WINS.

D'autres paramètres et options peuvent être gérés par un serveur DHCP.

Serveur d'impression :

Un serveur d'impression est un serveur qui permet de partager une imprimante entre plusieurs utilisateurs située sur un même réseau informatique.

Serveur de Messagerie :

Un serveur de messagerie électronique permet a ses utilisateurs d'envoyer et de recevoir des courriers électroniques, l'utilisateur a recours a un logiciel client capable de gérer l'envoie et la réception des courriels. Nous allons voir plus en détail le serveur de messagerie et toutes ses caractéristiques dans les chapitres a suivre, qui est le but de notre projet.

Serveur de Base de données :

Un serveur de base de données répond à des demandes de manipulation de données stockées dans une ou plusieurs bases de données. Il s'agit typiquement de demandes de recherche, de tri, d'ajout, de modification ou de suppression de données.

1.9.2.5 Les avantages de l'architecture Client/Serveur

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

— **Un réseau évolutif :** grâce a cette architecture il est possible de supprimer ou de rajouter des clients sans perturber le fonctionnement du réseau.
— **Une meilleure sécurité :** car le nombre de points d'entrée permettant l'accès aux données est moins important.
— **Une meilleure fiabilité :** En cas de panne, seul le serveur fait l'objet d'une réparation, et non le PC du client.
— **Une administration au niveau du serveur :** l'administrateur de serveur s'occupe de la gestion du réseau.

1.9.2.6 Les inconvénients de l'architecture Client/Serveur

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

— Coût élevé : dû à la technicité du serveur.
— La panne du serveur central paralyse la suite du réseau, étant donné que tout le réseau est architecturé autour de lui.

1.9.2.7 Problématiques de la gestion et de l'administration des réseaux client/serveur

Un réseau informatique est une entité complexe qui propose divers services et renferme un grand nombre d'utilisateurs et d'équipements de différents types. Dans ces conditions la gestion de son fonctionnement s'avère une lourde tâche d'administration. Dans le soucis d'être plus compétitif avec un système d'information plus efficace, sécurisé et mieux adapté aux besoins, de plus en plus plusieurs entreprises implémentent de multiples technologies afin d'améliorer et d'organiser l'environnement de travail de leurs employés. Ainsi parmi ces technologies celles de la firme Microsoft a savoir les systèmes d'exploitation Windows server et le service d'annuaire Active Directory.

1.10 Conclusion

A l'issue de ce chapitre nous avons introduit les réseaux informatiques, nous avons parler de modèles de communication, d'architecture, de classification et d'autres concepts décrivant les réseaux informatique. Cependant lorsqu'on construit un réseau, c'est dans le but de l'exploiter et ceci est possible grâce aux applications. Ces applications sont en nombre infini, et durant ce travail nous nous somme intéresser a l'une des application client/serveur existante depuis très longtemps a savoir la messagerie électronique.

Chapitre 2

La messagerie électronique

2.1 Introduction

Sorti des laboratoires il y a environ 50ans comme une simple application de transmission de messages entre deux ordinateurs, s'impose de nos jours comme un outil indispensable aux grands public mais surtout aux plus grandes entreprises.

La messagerie électronique a effectivement commencé comme simple outil de transmission de messages court pour évoluer en douceur, quasiment silencieusement, en suivant régulièrement les évolutions technologiques et fait partie aujourd'hui de ces instruments d'efficacité dont la vocation majeure est de permettre à l'entreprise de fonctionner mieux.

Au cours de ce chapitre nous allons aborder quelques notions sur la messagerie (origines, fonctionnement, protocole, etc) nous allons voir par la suite son usage dans le milieu professionnel et nous clôturons le chapitre par le choix de la solution de messagerie la plus adéquate suite à une analyse des outils existants sur le marché.

2.2 Définition de la messagerie électronique

La messagerie électronique est avant tout un outil technique de communication, utilisée au domicile comme sur le lieu de travail dans le but de véhiculer des informations de nature privée et professionnelle. C'est un service de transmission d'émail par le biais d'un réseau informatique et des logiciels de messagerie. [Fernando 16]

2.3 Les origines de la messagerie électronique

La messagerie électronique existe depuis environ 50 ans. L'histoire de cette technologie qui s'est imposée au fil des années comme un outil de communication incontournable n'est pour autant pas très connue.

La messagerie électronique est arrivée en 1971 avec Ray Tomlinson, un ingénieur chez BBN (Bolt Beranek And Newman) qui met au point une application spécifique a l'envoie des messages SNDMSG (Send Message) ainsi qu'une application dédiée a la lecture de ces derniers, READMAIL. Avec SNDMSG/READMAIL les utilisateurs qui travaillent sur une même machine peuvent s'y laisser des messages les uns aux autres.

Tomlinson travaillait parallèlement sur un protocole de transfert de fichier, le CPYNET qui permettait de copier simultanément un fichier sur tous les ordinateurs d'Arpanet. Une idée traverse l'esprit de Ray : si on pouvait échanger des fichiers entre ordinateurs, pourquoi ne pas adresser des messages ?

Pour ce faire, Tomlinson retient alors l'arobase @ (se prononce at, c'est-a-dire chez) pour séparer nettement l'adresse de l'utilisateur de celle de l'hébergeur. C'est ainsi que tomlison@bbn-tenexa (tenexa pour indiquer le système d'exploitation utilisé) devint la première adresse de courrier électronique de l'histoire et le premier message de l'histoire qui avait comme contenu "QWERTYUIOP" soit la première ligne de caractère du clavier anglophone. Depuis cette fois, La messagerie électronique a été, et continue d'être.[Turner 08]

2.4 Les RFCs (Request For Comments)

2.4.1 Définition

Les RFC ont été inventés par Steve Crocker en 1969 pour aider a enregistrer des notes non officielles sur le développement de l'ARPANET, un des premiers prédécesseurs d'internet. Depuis, ils sont devenus le registre officiel des spécifications, protocoles, procédures et évènements Internet. Ce sont en effet un ensemble de documents et de rapports dont les chercheurs ont rapporté leurs propres résultats, théories et leurs activités.

Par qui ces RFCs ont elles été écrites ? N'importe qui peut soumettre un document en tant que RFC a l'IETF (Internet Engineering Task Force), si celle-ci est acceptée, elle apparaitra après avoir été critiquée et examinée. La RFC 1543, intitulée instructions to RFC authors, explique comment rédiger une RFC. Les RFCs sont disponible sur le site officiel de l'IETF `http://www.ietf.org/`. [Costales 08]

2.4.2 Les RFCs relatives au courrier électronique

Plusieurs RFCs relatives au courrier électronique existent sur Internet, celles-ci concernent tout administrateur d'un système de messagerie électronique. Les RFCs les plus intéressantes a ce sujet sont :

- **La RFC 5321 :** qui traite la façon dont les E-mails sont transférés entre les systèmes.
- **La RFC 1939 :** qui détaille le protocole de retrait d'émail POP dans sa version 3.
- **La RFC 2822 :** qui indique la manière dont les messages doivent apparaitre.
- **Les RFCs (2045, 2046, 2047, 2048, 2049) :** qui detaillent le standard MIME (Multipurpose Internet Mail Extensions).[Loshin 99]

2.5 Les notions indispensables de la messagerie électronique

2.5.1 Adresse électronique

Une adresse électronique permet d'identifier de façon unique le propriétaire d'une boite de courrier électronique qui peut être une personne physique ou morale, un service d'entreprise, une entreprise etc. Elle se présente sous la forme `Utilisateur@Domaine` ou :

— Utilisateur identifie l'utilisateur qui s'est inscrit auprès du serveur de messagerie.
— Le signe @ se prononce at et signfie chez, c'est un caractère réservé qui sert de séparateur entre le code.
— Domaine identifie le serveur de messagerie.[Silva 06]

La RFC 5322 décrit de façon détaillée le format des adresses électroniques.

2.5.2 Structure d'un courrier électronique

Dans le contexte du courrier électronique un message est composé de deux parties, une enveloppe et le message proprement dit.

2.5.2.1 L'enveloppe du message

Contient toutes les informations nécessaires pour assurer la transmission et la livraison du message.

2.5.2.2 Le message

Composé de deux éléments les champs d'entêtes et le corp du message.

— **Les champs d'entêtes :** fournissent des informations de nature variée sur le message. Les champs d'entêtes peuvent être classés selon leurs catégorie d'usage.
  — **Le champ de date :** correspond a la date et l'heure d'envoi du message, selon le fuseau horaire de l'expéditeur.
    — **Les champs d'entêtes qui indiquent la boite aux lettres de l'expéditeur :** sont au nombre de trois champs et permettent de renseignés la(es) adresse(s) source(s) de l'émail.
      — **Le champ from :** indique l'auteur du message.
      — **Le champ sender :** spécifie la boite au lettre de l'agent responsable de la transmission réelle du message.

  - **Le champ reply-to :** indique l'adresse électronique suggérée par l'auteur pour recevoir une réponse, si ce champ est vide ou inexistant, la réponse sera envoyée a l'adresse électronique spécifiée dans le champ from.
- **Les champs d'entêtes qui indiquent la boite aux lettres du destinataire :** spécifient les destinataires du message et se composent de trois champs.
  - **Le champ to :** contient la(es) adresse(s) du destinataire(s) primaire(s) du message.
  - **Le champ cc (carbon copy) :** doit être réservé aux personnes que vous désiriez tenir informées du contenu du message, mais qui ne sont pas directement concernées.
  - **Le champ bcc (blind carbon copy) :** contient les adresses des destinataires du message mais que les adresses ne doivent pas être révélées a d'autre destinataire du message.
- **Le champ d'identification :**
  - **Le champ message-id :** permet d'identifier un message de façon unique. L'unicité du message-id est garantie par l'hôte qui le génère.
- **Les champs d'information :** ce sont des champs facultatifs et sont au nombre de trois champs.
  - **Le champ subject :** contient une courte chaine identifiant le sujet du message, lorsqu'il est utilisé dans une réponse, le corps du champ peut commencer par la chaine Re suivis du contenu du champ subject.
  - **Le champ keywords :** contient une liste de mots et de phrases qui pourraient être utiles pour le destinataire.
  - **Le champ comments :** contient des commentaires supplémentaires sur le texte du corps du message.
- **Les champs de traces :** sont un groupe de champs d'entête consistant en un champ facultatif Return-Path et un ou plusieurs champs Received.
  - **Le champ Return-Path :** si le message ne peut être délivré a son destinataire, un message sera envoyé a cette adresse mail.
  - **Le champ Received :** correspondent a la liste de tous les intermédiaires qui ont servis à transmettre le message au destinataire, soit le chemin emprunté depuis l'expéditeur au destinataire.[Resnick 01]

  Notez que selon la RFC 2822, seuls les champs from et date sont réellement indispensables.
- **Le corps du message :** contenant le message, séparé de l'entête par

une ligne vide, le message peut être du texte brut (code ASCII) ou un message formaté (HTML par exemple), il prendra alors la forme d'un encodage MIME décrit dans le point suivant.

2.5.3 MIME (Multipurpose Internet Mail Extensions)

Lorsque la messagerie électronique a fait ses débuts, la technologie du moment ne permettait que l'envoie du texte au format ASCII ceci était déjà une belle réussite pour un début. Au fils du temps les besoins ont changé, on ne veut plus se contenter d'envoyer du texte seulement mais plutôt des images, du son, de la vidéo, ce qui a fait la naissance d'un nouveau standard à savoir MIME.

2.5.3.1 Définition

MIME (Multipurpose Internet Mail Extensions) est un standard défini par de nombreuses RFCs (RFC 2045, RFC 2046, RFC 2047, RFC 2048, RFC 2049), proposé afin d'étendre les capacités limitées du courriel en permettant l'insertion des documents (tel-que les images, du son, des fichiers...) dans les messages.

Comment ?

MIME permet de décrire dans des entêtes le type de contenu du message et le codage utilisé. Un message basé sur ce format contient en plus des champs standards (From, To ...), de nouveaux champs faisant partie des extensions, ce sont en effet des directives d'entête spécifiques afin de décrire le format utilisé dans le corps du message, celles-ci permettent aux clients de messagerie de pouvoir interpréter le message correctement.

2.5.3.2 Les directives d'entête de MIME

Cinq champs d'entêtes sont utilisés afin de décrire la structure des messages MIME.

- **MIME-Version :** indique la version du standard MIME utilisé dans le message.
- **Content-type :** le but de ce champ est de décrire les données contenues dans le corps pour que l'agent utilisateur destinataire puisse traiter les données de manière appropriée. Ce champ possède la syntaxe suivante : Content-Type : Type/Sous-type ; paramètre=”valeur”. Il existe deux catégories de types MIME :
  - **Les types de données discrets :** ce sont les types principaux de données a savoir text, audio, video, application (utilisé pour les données qui ne rentre dans aucune des autres catégories).

- **Les types de données composites :** permettent la structuration de différentes entités au sein du même message et sont deux types : message et multipart.
  - **message :** permet d'encapsuler dans un émail un autre émail.
  - **multipart :** permet de composer un messages avec différentes entités, pour ce faire MIME insert un séparateur appelée Boundry, il s'agit d'une chaine arbitraire définie en attribut de l'entête Content-Type et permet de délimiter un contenu, plusieurs type de séparateurs existent dont :
    - **multipart/mixed :** définit un ensemble d'objets distincts.
    - **multipart/alternative :** définit différentes alternatives pour une même information et le système devrait choisir le type adéquat selon l'environnement local de l'utilisateur.
    - **multipart/parallel :** le contenu des objets sera exécuté en parallèle. [Borenstein 96]
- **Content-Transfer-Encoding :** définit l'encodage utilisé dans le corps du message. Ce champ possède la syntaxe suivante : Content-Transfer-Encoding : "valeur", avec valeur = '7bit'/ '8bit'/ 'binary'/ 'quoted-printable'/ 'base64'.

Et l'encodage de l'entête du message ?

Pour permettre d'encoder les entêtes avec un alphabet de plus de 7bit afin d'avoir par exemple un sujet de message accentué, MIME propose le format suivant : `mot-codé='=?'jeudecaractères'?'encodage'?'textecodé'?='`.

encodage définit l'encodage souhaité (Q pour quoted-printable et B pour base64).

Par exemple :

`Subject:=?ISO-8859-1?Q?=pi-E8ce_jointe?=` (Ici le sujet du message a été encodé en quoted-printable et doit être décodé selon le codage ISO-8859-1.[Moore 96]

- **Content-ID et Content-Description :** deux champs d'entête supplémentaires peuvent être utilisés pour décrire plus en détails les données contenues dans le corps, le content-id (sert a identifier de façon unique un contenu) et le content-description (permet d'accompagner le corps avec des informations supplémentaire). [Freed 16]

Afin de voir plus clair le fonctionnement de MIME voici un émail au format MIME :

From : "Alice" <AL@test.com>
To : <Bob@test.com>
Date : Mon, 22 Mar 1993 09 :41 :09 -0800 (PST)
Subject : test d'encodage MIME
MIME-Version : 1.0
Content-Type : multipart/alternative ; boundary=PartieSuivante
ceci est un message multipart au format MIME.
--PartieSuivante

Content-Type : text/plain ; charset="us-ascii"
Content-Transfer-Encoding : 7bit
ceci est un message au format texte
--PartieSuivante
Content-Type : text/html ; charset="us-ascii"
Content-Transfer-Encoding : quoted-printable
<!DOCTYPE HTML>
<HTML><HEAD>
<TITLE>Message</TITLE>
</HEAD><BODY>
<DIV>ceci est un message au format html </DIV>
</BODY></HTML>
--PartieSuivante--

2.5.4 Serveur et client de messagerie

2.5.4.1 Serveur de messagerie

Un serveur de messagerie est un ordinateur dédié qui offre le service de messagerie électronique. Le serveur de messagerie joue, en particulier, un rôle de stockage et de transmission :

— Il contient des espaces sur les disques durs pour le stockage des comptes de messagerie des utilisateurs.
— Il assure l'envoi et la réception des messages.[Silva 06]

Les serveurs de messagerie les plus courants sont : Exchange Server de Microsoft, Sendmail, Postfix, Qmail, Zimbra ou encore IBM Dominos.

2.5.4.2 Client de messagerie

On distingue deux types de clients :

— **Les clients lourds :** Un client lourd est un logiciel qui s'installe sur le poste client et se connecte au serveur de messagerie. Ce type de client présente les avantages suivants :
  — **La disponibilité :** même si le serveur cesse de fonctionner les messages existent toujours sur le disque dur.
  — **Accès hors ligne :** les messages déjà lus sont téléchargés et stockés dans un ou plusieurs dossiers personnels et sont accessibles à tout instant.

  En revanche, les inconvénients majeurs sont :
  — **L'accès à distance :** un client de messagerie doit être installé et configuré sur un ordinateur. Une fois téléchargé, installé et configuré sur un ordinateur particulier, il n'est accessible que sur cet ordinateur.

  - **Les mise à jour :** même si le logiciel a été installée et configuré correctement, il doit être maintenu à jour a chaque nouvelle version afin d'assurer son bon fonctionnement.
  - **Les problèmes de sécurité :** du point de vue de la sécurité, le stockage des émail sur l'ordinateur de l'utilisateur peut mettre les données en danger car si une personne réussit a obtenir un accès non autorisé à l'ordinateur (en cas de vol par exemple), elle pourrait être en mesure d'accéder à tous les courriels stockés sur cet ordinateur.
- **Les clients légers :** Un client léger également appelée Webmail est un programme ou une série de scripts exécutés sur un serveur, accessible sur le web et permettant d'accéder a des fonctions de messagerie similaires à celles d'un client de messagerie classique.[Haycox 09] Ce type de client présente les avantages suivants :
  - **Accès à distance :** Avec un Webmail, il est possible d'accéder à la messagerie électronique depuis n'importe quel endroit disposant d'une connexion internet.
  - **Pas de mise à jour ou de maintenance :** contrairement au logiciels de messagerie qui doivent être mis à jour régulièrement, un Webmail est maintenu et administré de manière centralisée.
  - **Pas d'installation ou de configuration :** Accès aux mails avec un simple navigateur sans la moindre installation ou configuration.

  En revanche, les inconvénients majeurs sont :
  - **le Webmail n'est accessible qu'en ligne :** La lecture, l'écriture et l'envoie des mails nécessitent une connexion internet.
  - **Les problèmes de performance :** L'accès simultané d'un grand nombre de clients au serveur de messagerie peut avoir pour conséquence que les pages soient plus lentement ou dans des circonstances extrêmes, le serveur ne répond pas.
  - **Les problèmes de sécurité :** l'avantage de l'accès a distance cède la place a l'insécurité potentielle des machines sur lesquelles l'utilisateur accède à son courrier surtout si elles ne sont pas les siennes, parmi les problèmes de sécurité les plus fréquents nous citons :
    - La présence des keyloggers sur l'appareil entraine la capture et l'enregistrement de vos informations d'identification sur l'appareil qui peuvent être interceptées et utilisées par des tiers pour un accès non autorisé.
    - De nombreux navigateurs web modernes offrent la possibilité de sauvegarder un mot de passe chaque fois qu'il est entré. Un enregistrement accidentellement du mot de passe sur l'appareil le rend accessible à tout utilisateur ayant accès a cet appareil.

— Les utilisateurs peuvent se laisser connectés par oublie ce qui rend votre compte accessible à tout utilisateur ayant accès à l'appareil.

Faut-il choisir le logiciel de messagerie ou le Webmail ?

Il n'y a pas de choix meilleur que l'autre, tout dépend de vos besoins et vos moyens cependant il faut retenir que l'usage de ces outils nécessite de la prudence afin de ne pas mettre ses données entre les mains des personnes mal intentionnées.

2.5.5 Les protocoles de messagerie

2.5.5.1 SMTP pour la gestion du courrier

SMTP (Simple Mail Transfert Protocol) que l'on traduit par protocole simple de transfert de courrier, c'est un protocole de couche 7 du modèle OSI spécifié en 2008 par la RFC 5321, utilisé pour le transfert de message entre les nœuds du réseau. Le dialogue SMTP utilise des commandes d'envoi constituées de quatre lettres et des commandes de réponse du serveur constituées d'un code sur trois chiffres suivi d'un messages texte (un premier chiffre a 1,2 ou 3 signifie une réussite ; une valeur 4 ou 5 un échec). Les transactions de courrier SMTP se déroulent en trois étapes :

1. **Établissement de la connexion et identification des expéditeurs et destinataires du message :** l'expéditeur doit émettre la commande HELO ou EHLO avant de commencer une transaction par courrier. Ces commandes, ainsi qu'une réponse "250 OK" a l'une d'elles, confirment que le client SMTP et le serveur SMTP sont tous les deux à l'état initial, c'est-à-dire il n'y a pas de transaction en cours. Ensuite la transaction commence MAIL FROM qui permet d'identifier l'expéditeur. Dans le cas ou le serveur répond 250 OK, une série d'une ou plusieurs commandes RCPT TO suivent donnant des informations sur les destinataires, si le serveur renvoi 250 OK l'émetteur transfert le message.
2. **Transfert du message :** l'émetteur initie le transfert du message par l'envoie de la commande DATA. Si la commande est acceptée, le serveur SMTP renvoie une réponse 354 intermédiaire et considère que toutes les lignes suivantes font partie du mail jusqu'à arriver a la ligne contenant uniquement un " . " qui marque la fin de l'émail.
3. **Libération de la connexion :** l'émetteur envoie la commande QUIT au récepteur, cette commande spécifie que le destinataire doit envoyer une réponse 221 OK puis fermer le canal de transmission.

D'autre commande existent tel que RESET qui permet d'annuler le mail en cours, NOOP qui permet de demander au récepteur l'envoie d'une réponse OK, etc. [Morimoto 16][Klensin 08]

La figure montre un exemple de dialogue SMTP entre client et serveur dans lequel Bob envoie un émail via le serveur smtp.emetteur.org vers Alice et Jones sur le serveur smtp.recepteur.org. Le courrier est accepté pour Alice. Refusé pour Jones qui lui ne possède pas de boite aux lettre dans le serveur smtp.recepteur.org. Ce dialogue suppose que le serveur est prêt a recevoir une demande de connexion.

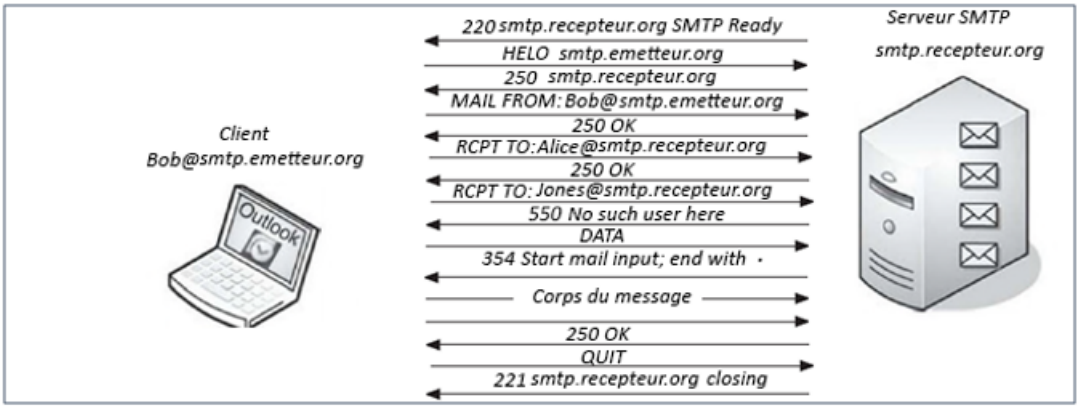

FIGURE 2.5.1 – Exemple de dialogue SMTP.

A partir des spécifications SMTP, a été définie une version étendue appelée ESMTP qui intègre les extensions MIME.

2.5.5.2 POP et IMAP pour le retrait du courrier

POP (Post Office Protocol) : que l'on traduit par protocole de bureau de poste, c'est un protocole de couche 7 du modèle OSI, utilisé pour le retrait de mail, il permet de télécharger le courrier électronique depuis le serveur de messagerie et de le repartir chez le client. La version 3 de POP (POP3) est spécifiée en 1996 par la RFC 1939. Tout comme le protocole SMTP, le protocole POP3 fonctionne grâce a des commandes textuelles sur quatre lettres émises du client au serveur POP, les réponses du serveur sont transmises sous forme d'une chaine de caractères précédée des caractères +OK ou -RR suivant que celle-ci est positive ou négative. Les clients POP ont recours par défaut au port 110 lors de la phase de connexion au serveur via le TCP/IP.[Morimoto 16][Myers 96]

La figure montre un exemple de transmission entre client et serveur POP3. Le dialogue commence par une réponse +OK du serveur suite a une demande de connexion du client indiquant qu'il est prêt, le client quant à lui s'identifie au prés du serveur en utilisant son nom d'utilisateur et son mot de passe. Après acceptation, le client peut lister le nombre de mails en attente (la commande STAT) il peut aussi récupérer un des messages et le supprimer (les commandes RETR et

DELE respectivement) et en dernier le client ferme la connexion en faisant appel a la commande QUIT.

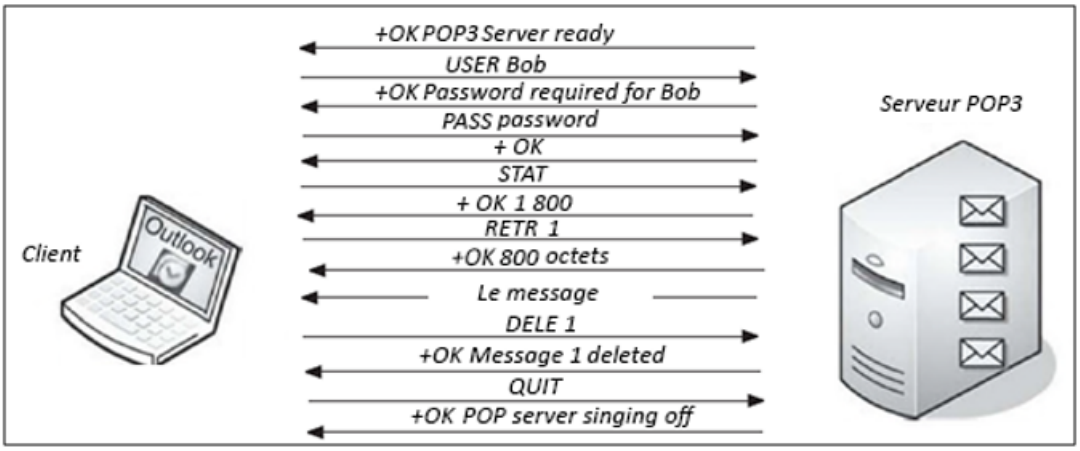

FIGURE 2.5.2 – Exemple de dialogue POP.

Il faut noter que les commandes POP3 ne se limitent pas à celles citées dans l'exemple.

IMAP (Internet Message Access Protocol) : est un protocole de couche 7 du modèle OSI, utilisé pour la lecture d'émail il a été conçu pour consulter les messages directement depuis le serveur de messagerie. La version 4 d'IMAP (IMAP4rev10 est spécifiée en 2003 par la RFC 3501.

La figure montre une transaction entre client et serveur IMAP, dans laquelle le client s'authentifie puis sélectionne la boite de réception (INBOX), le serveur lui renvoie le contenu de la boite sélectionnée dont :

La liste des indicateurs (FLAGS) possibles sur les messages (message lu, réponse envoyée, message marqué, etc).

Le nombre de messages dans la boite (1 EXIST).

Le nombre de messages récents (0 RECENT)...

Le client demande ensuite la lecture du contenu du mail 1 et se déconnecte à l'aide de la commande Logout.[Morimoto 16]

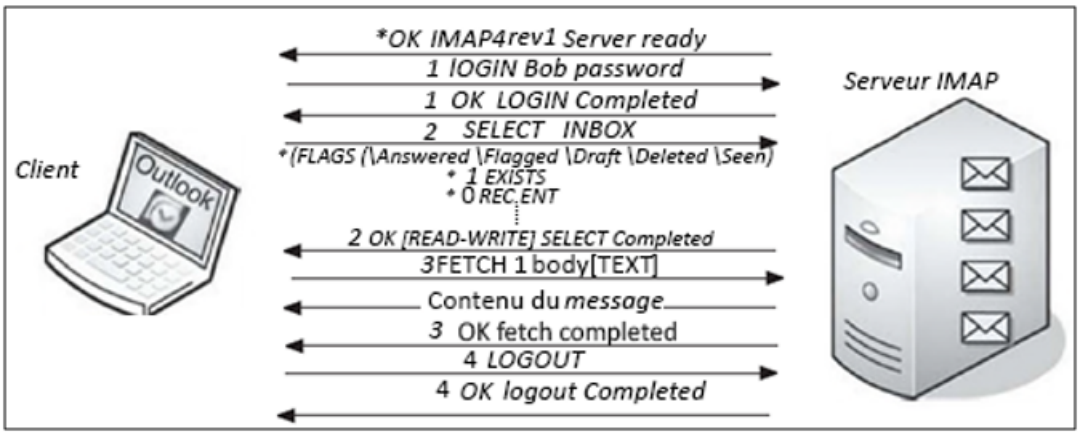

FIGURE 2.5.3 – Exemple de dialogue IMAP.

Le protocole IMAP est assez complexe comparé a POP et beaucoup d'autre commandes existent autres que celle citées dans l'exemple.

Faut-il choisir POP ou IMAP ?

Généralement les contraintes les plus courantes avec le courrier électronique varies entre la mobilité, l'accès multiple, espace de stockage. Afin de voir quel protocole choisir analysons la réaction des deux envers ces contraintes.

–**L'espace de stockage :** Avec IMAP le fait que les messages sont conservés sur le serveur et non sur votre ordinateur, à tendance à faire augmenter l'espace occupé par vos messages sur votre espace d'hébergement qui est sans doute limité, vous serez ainsi obligés d'effacer de temps en temps les messages qui vous sont pas utiles. POP de son côté présente l'avantage de télécharger les émails sur votre disque dur, ce qui vous donne ainsi la capacité de garder autant de mails que vous voulez.

–**L'accès multiple :** Le protocole POP fournit un accès bloqué à la boite mail c'est-à-dire qu'aucune autre connexion n'est permise en même temps que la connexion déjà en cours. IMAP quant à lui permet de gérer plusieurs accès simultanés ainsi par exemple si plusieurs utilisateurs partagent une boite aux lettres ils peuvent y accéder au même temps.

–**La mobilité :** Avec IMAP vous gérer vos émails depuis n'importe quel équipement connecté à internet quel que soit le lieu ou vous soyez. POP quant à lui récupère vos messages sur votre équipement ce qui ne les rends accessible que sur cet équipement.

–**La connexion Internet :** Avec IMAP il faudra être connecté pour gérer ses émails. Ce qui peut poser des difficultés si la connexion à internet n'est pas stable. POP de son côté n'utilise la connexion que pour télécharger les émails récents sur votre machine et donc fonctionne bien, même avec une connexion internet très

lente bien que la connexion n'est qu'une contrainte très mineure dans un monde de plus en plus connecté.

En conclusion les deux protocoles se valent et chacun présente des avantages que, l'autre n'a pas, la chose qu'il faut retenir est qu'avant de choisir POP ou IMAP il faudra considérer vos besoins quant à l'utilisation de votre messagerie et vos ressources informatiques.

2.6 L'acheminement du courrier électronique

La technologie s'inspire de la vie quotidienne, tout comme la messagerie électronique d'ailleurs qui elle s'est inspirée du courrier postal. Le courrier électronique passe exactement par les même étapes qu'un courrier postal néanmoins il n'y a pas de poste locale ni de facteur mais plutôt un ensemble d'agents ayant les même rôles.

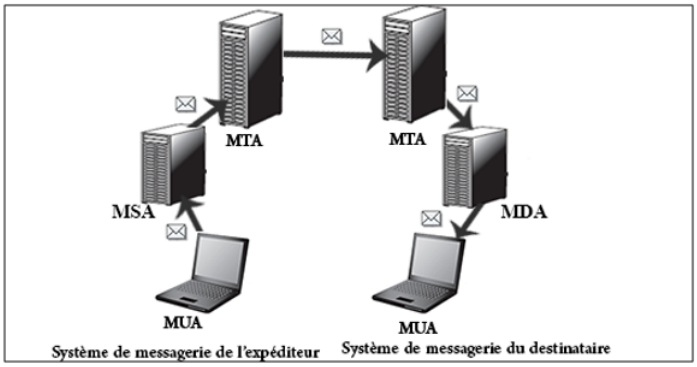

FIGURE 2.6.1 – L'acheminement du courrier électronique

–**Le MUA (Mail User Agent : client de messagerie) :** Un MUA est une application qui vous permet de retirer des mails de votre boite de réception et d'en écrire, le client de messagerie (logiciel ou Webmail) tout comme Outlook ou Thunderbird. Comparé au système du courrier postal, le MUA représente le papier et le stylo que vous utilisez pour écrire une lettre.

–**Le MSA (Mail Submission Agent : agent de soumission de courrier) :** Le rôle d'un facteur est de conduire la lettre que vous rédigez vers la poste. Le MSA n'est rien d'autre qu'un facteur de transmission, c'est un logiciel qui sert d'intermédiaire entre le client de messagerie et le serveur de messagerie.

–**Le MTA (Mail Transfert Agent : agent de Transfert de courrier) :** Le MTA est un serveur de messagerie, il correspond au bureau de poste dans le courrier postal dont le rôle est de recevoir votre courrier et de l'expédier au destinataire.

dans le cas où l'adresse du destinataire appartient à un autre domaine que celui de l'émetteur, le courrier passe par un autre MTA. Cependant, lorsqu'il s'agit d'un mail interne à un même domaine, il est directement pris en charge par le MDA (Mail Delivery agent) sans passer par le second MTA. Il est possible de fusionner un MTA et un MSA, dans ce cas on parle seulement de MTA mais ce dernier assure également le rôle d'un MSA. Comme si vous décidiez d'aller vous même déposer votre lettre à la poste local au lieu de passer par un facteur.

–**Le MDA (Mail Delivery Agent : agent de livraison du courrier) :**

Comparant au courrier postal le MDA correspond au facteur de réception qui vient déposer le courrier dans votre boite aux lettres.

Comment les différents agents communiquent entre eux ?

Afin d'acheminer le courrier du rédacteur au destinataire, les différents agents doivent dialoguer entre eux pour cela le système de messagerie fait appel aux protocoles de messagerie : SMTP, POP et IMAP.

Du MUA de l'expéditeur au dernier MTA par lequel passe le courrier, c'est le protocole SMTP qui est utilisé et entre le MDA et le MUA du destinataire on fait appel aux protocoles de réception IMAP ou POP.

Autrement dit, les serveurs de messagerie utilisent le SMTP pour la transmission et la réception, tandis que les clients utilisent SMTP pour l'envoie et un autre protocole (POP ou IMAP) pour la réception.

2.7 La messagerie électronique et son usage en entreprise

Avec les innovations technologiques, divers outils de communication ont fait leurs apparitions pour le monde professionnel : des applications de collaborations, des réseaux sociaux professionnels. Malgré cette diversité d'outils, la messagerie électronique reste un des moyens de communication les plus indispensables aux entreprises. La popularisation des émails en entreprise a commencé vers les années 80 et ne cesse d'augmenter.

L'émail professionnel en quelques chiffres :

Radicati group en collaboration avec des sociétés mondiales fournit des études quantitatives et qualitatives sur les technologies de communication dont la messagerie électronique, voyons quelques statistiques au sujet de l'utilisation de l'émail dans le monde et en entreprise :

— Plus de la moitié de la population mondiale utilise l'émail, le nombre d'utilisateurs de messagerie dans le monde est de l'ordre de 3,9 milliards en 2019 avec une prévision de 4,3 milliards pour 2023.[Group 19]

— 293 milliards d'émails sont téléchargés chaque jour dans le monde en 2019 sans compter les spams. Une prévision de 347 milliards est faite pour l'an 2023.[Group 19]
— En 2015, un salarié recevait en moyenne 88 émails et envoyait 34 émails liés au travail par jour dont 12 sont identifiés par les usagers comme étant du spam.[Group 15]
— En 2015, on comptait plus de 4,3 milliards de comptes émails dans le monde, avec une prévision de plus de 5,5 milliards en 2019.[Group 15]

Pourquoi l'émail est étant populaire au milieu professionnel ?

Le courrier électronique a réussi l'épreuve du temps et de la concurrence et s'est imposé comme outil incontournable en entreprise grâce aux diverses fonctionnalités qu'il fournit à savoir :

— La possibilité de transmission simultanée d'un message à plusieurs personnes et l'envoie des pièces jointes.
— La facilite d'usage de cet outil ainsi que la rapidité d'envoie et de réception des émails.
— Le courrier électronique est un outil de coopération, il permet de faire circuler et d'échanger des documents en cours d'élaboration.
— Les logiciels de messagerie électronique permettent de garder trace des différentes interactions via des sauvegardes.
— Et enfin parce que lorsque les émails sont utilisés avec modération et parcimonie, ils sont très bénéfiques pour les entreprises.

Néanmoins tout comme l'usage de l'émail au milieu professionnel peut être aussi bénéfique, un système de messagerie électronique non sécurisé nuira a la société. En effet la messagerie électronique est le canal par lequel transite les informations les plus importantes d'une entreprise ce qui fait des serveurs de messagerie des sources d'informations exceptionnelle pour les pirates et les concurrents. Voyons un aperçu des risques d'une messagerie non sécurisée :

— **Perte d'informations :** le dysfonctionnement du serveur entraine la perte des émails et donc des informations de l'entreprise.
— **Perte d'intégrité :** un émail peut être intercepté, modifié puis relayé à son destinataire dans le but de tromper l'utilisateur et de nuire le système.
— **Les menaces :** l'émail est un moyen de diffusion des menaces tel que : les virus, les spams, le phishing, les ransomwares, les tentatives de fraude, l'ingénierie sociale etc.
— **Perte de confidentialité :** lorsque les émails sont transmis en clair sur le réseau, des personnes non autorisées peuvent avoir accès aux informations confidentielles de l'entreprise.
— **Usurpation d'identité :** un attaquant peut prendre l'identité d'une personne en fabriquant un émail ayant son identité dans le but de déstabiliser

l'entreprise.
Beaucoup d'autres risques existent ce qu'il faut retenir, c'est que toute la société qui est mise en jeu avec la messagerie électronique.

Afin de pallier à ces problèmes et de faire de la messagerie un outil sure et fiable, des mesures de sécurité doivent être établies ceci fera l'objet du prochain chapitre. Néanmoins si la solution de messagerie elle-même n'étant pas fiable et sure, les pirates utiliseront souvent ses failles pour exécuter leurs actions malveillantes et aucune mesure de sécurité ne serait suffisante pour se protéger.

Quelle est la solution de messagerie la plus sure et la plus fiable ? Nous allons le découvrir à travers une analyse des outils disponible sur le marché.

2.8 Analyse des outils de messagerie électronique

Depuis l'adoption du courrier électronique pour le monde professionnel, la concurrence augmente en termes de logiciels de messagerie, chacun des producteurs favorise son produit qui se distingue par ses fonctionnalités et la qualité de service qu'il fournit. Il n'y a certes pas de produit parfait en milieu professionnel, les points qui peuvent faire la différence sont la sécurité et la fiabilité.

Après cette analyse le choix se portera sur la solution de messagerie la plus fiable et qui donne plus d'opportunité a un administrateur d'un système de messagerie d'établir des mesures de sécurité.

2.8.1 Les principales solutions de messagerie

- **Zimbra Collaboration Suite ZCS :** est une solution de messagerie et de travail collaboratif prenant en charge les e-mails, contacts, calendriers, tâches et partage de documents. la suite ZCS fait son apparition sur le marché en 2005, achetée en 2007 par Yahoo et revendu à VMware en 2010. Zimbra est à la base une solution gratuite néanmoins pour bénéficier des fonctionnalités supplémentaires il faut passer vers la version payante.[Touitou 07][Déon 08]t
- **IBM Lotus Domino :** à l'origine nommée Lotus Notes racheté par IBM depuis 1995 est rebaptisé IBM Domino depuis sa version 9. Lotus est un outil unique doté de plusieurs composants permettant d'accomplir différentes tâches dont la messagerie électronique, la gestion de bases de données et le développement d'application notes et web. Lotus Notes est autant connu dans le monde de la messagerie car il possède autant de fonctionnalités que les logiciels spécialisés dans la messagerie notamment le calendrier et la planification.[Déon 08]
- **GroupWise :** est une solution de messagerie professionnelle et de travail collaboratif développée par Novell. GroupWise est un système multi plate-

forme qui fournit les fonctions de messagerie, d'agenda et de planification. Il inclut également des fonctions de gestion des tâches, des contacts et des documents, ainsi que d'autres outils de productivité.

— **Microsoft Exchange Server :** est un produit Microsoft conçu des le départ comme une solution mail professionnelle. Il prends en charge les agendas, les contacts, les tâches. Suivant la vague du cloud computing, Mirosoft Exchange est, depuis 2009 disponible au travers d'une offre SaaS (Software as a service) appelé Microsft Online Services sous le nom d'Exchange Online. Cette offre a desormais été remplacée par Microsoft Office 365.[Lohier 13]

— **Open Business Management OBM :** est un logiciel de travail collaboratif développé en 1998 par la société AliaSOure. OBM fournit une multitude de fonctionnalités dont la messagerie, les outils de travail collaboratif, etc. [Déon 08]

2.8.2 Quelle solution de messagerie choisir ?

Les solutions de messagerie ne manquent pas, chacune se distingue par ses fonctionnalités. Pour notre projet nous avons opté pour Microsoft Exchange server.

Pourquoi Exchange ?

Parce que Microsoft Exchange Server est bien meilleur que ses concurrents, en effet la part de marché qu'occupe Exchange server est de plus de 50% et continue à enregistrer une croissance ces dernières années, contrairement à Lotus Notes et GroupWise qui ont effectivement perdu des parts de marché tandis que VMware est tout juste entrain de redessiner la stratégie de Zimbra vers le marché selon Gartner.

Microsoft Exchange est une solution messagerie taillée pour un environnement professionnel. S'il est vrai que le choix en termes de solutions de messagerie parait assez large, en y regardant de plus prés on se rend rapidement compte qu'un outil spécialisé dans la messagerie depuis son apparition, crée et suivi par un géant comme Microsoft et fonctionnant avec les meilleurs technologies en terme de stockage et de routage notamment Active Directory. Un outil qui a passé l'épreuve du temps et de la concurrence pour garder la place de leadeur durant plus de 23 ans prendra souvent une longueur d'avance sur ses concurrents.

Et enfin parce que dans la messagerie électronique la sécurité est avant tout, le pari pour la sécurité de Microsoft Exchange server est dédiée de manière qu'elle implémente des systèmes surs pour la protection des différentes données et les relations qu'elle administre. Le programme surveille tout, du stricte contrôle d'accès depuis les appareils mobiles aux différentes autorisations des utilisateurs.

2.9 Conclusion

Le but de ce chapitre est de comprendre le fonctionnement de la messagerie électronique et de choisir la solution de messagerie la plus adapter à nos besoins à savoir Exchange Server. Néanmoins un bon logiciel ne suffit pas pour se protéger contre la multitude de menaces auxquelles est affrontée cette technologie. Au cours du prochain chapitre nous allons d'une part voir plus en détails les dangers et les menaces véhiculées par la messagerie et d'autre part la stratégie de sécurité à mettre en place afin de se protéger et de fermer la porte contre toute tentative de piratage notamment dans un environnemnt Exchange server 2013.

Chapitre 3

La sécurité dans la messagerie électronique

3.1 Introduction

La messagerie électronique avec tous les avantages et bénéfices qu'elle peut apporter à l'entreprise, elle peut causer la faillite de celle-ci. En effet étant le moyen de communication le plus déployé et utilisé dans le monde professionnel, le courrier véhicule les informations les plus importantes de l'entreprise, ce qui fait de lui la cible préférée des attaquants et des concurrents. Il est donc essentiel d'accompagner sa messagerie d'une bonne stratégie de sécurité. Nous allons au cours de ce chapitre aborder la notion de sécurité dans le monde de la messagerie électronique et la façon de se protéger.

3.2 Définition de la sécurité informatique

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.[Belattaf]

3.3 Les objectifs de la sécurité de la messagerie électronique

Un administrateur de messagerie vise à assurer les services de sécurité fondamentaux que vise tout autre administrateur d'un système informatique à savoir :

- **La disponibilité :** permet de garantir l'accès aux serveurs de messagerie et à l'ensemble des ressources du système de messagerie.
- **L'intégrité :** s'assurer que le contenu de l'e-mail ne peut être altéré avant d'atteindre sa destination.
- **La confidentialité :** s'assurer que le contenu de l'e-mail reste secret entre les acteurs de la transaction et n'est pas divulgué à une personne tierce.
- **L'authentification :** consiste à s'assurer de l'identité d'un utilisateur, c'est-à-dire garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.
- **La non-répudiation :** est la garantie qu'aucun des correspondants ne pourra nier qu'il ait envoyé ou reçu le mail.
- **Le contrôle d'accès :** est un service qui contrôle et consigne les accès aux systèmes, aux ressources et aux applications. [Dowland 10] [Turner 08]

3.4 Menaces et attaques par courrier électronique

Un système de messagerie comme tout autre système d'information d'ailleurs est vulnérable à une variété de risques, de menaces et d'attaques qui peuvent en fonction des contres mesures établies affecter le système d'un degré plus ou moins grand. Cependant, afin de pouvoir se protéger, il est nécessaire de prendre connaissances des risques auxquels notre système est exposé.

3.4.1 Les courriers électroniques non sollicités

Un courrier non sollicité est comme son nom l'indique un courriel envoyé a un destinataire sans qu'il le sollicite, ce mail peut prendre différentes forme et peut avoir différents buts.

3.4.1.1 Les types de courriers non sollicités

Les courriers non sollicités peuvent prendre différentes appellations en fonction du but qu'ils accomplissent dont les principaux sont :

— **Les Spams :**

le Spam également appelé pollupostage, pourriel, courrier indésirable ou encore junk mail désigne l'envoi massif de courrier électronique à des destinataires ne l'ayant pas sollicité à des fins publicitaires. Le premier spam de l'histoire date de 1978 envoyé par Gray Thuerk, un employé de digital équipement corporation. Gray souhaitait faire connaitre l'un des nouveaux produits de sa société, il récupèrera pour cela les adresses mails des 393 personnes, connectés à l'époque sur le réseau pour leur transmettre le mail.

Comment travaille les spammeurs ? les spammeurs collectent des adresses électroniques un peu partout sur internet grâce à des logiciels appelés robots parcourant les différentes pages et stockant au passage dans une base de données toutes les adresses e-mail y figurant. Il ne reste ensuite au spammeur qu'à lancer une application envoyant successivement à chaque adresse le message publicitaire.[Bay 15] [Bloch 09]

— **Les Scams :**

Le Scam également appelé fraude 419 est une sorte d'arnaque dont l'attaquant promet une grosse somme d'argent à la victime en contrepartie d'une aide financière. [Dowland 10]

— **Les canulars (Hoax) :**

On appelle hoax un courrier électronique propageant une fausse information et poussant le destinataire à diffuser la fausse nouvelle à tous ses proches, collègues et au grand publique. Le but de ce genre d'attaque dépend de son contenu : il

peut s'agir de faire passer une idée dans l'opinion publique, accroître le sentiment d'insécurité informatique, dénigrer un produit ou une personne, etc. [Bay 15]

— **Le Phishing (hameçonnage) :**
le Phishing consiste à envoyer des courriels qui semblent provenir de sources réputées dans le but d'influencer ou d'obtenir des informations personnelles. L'attaquant pourrait impliquer une pièce jointe au courrier électronique qui charge des logiciels malveillants sur votre ordinateur. Il pourrait également inclure un lien vers un site Web illégitime. [Hadnagy 15]

3.4.1.2 Comment se protéger des courriers indésirables ?

Les courriers non sollicités sont le type de risques dont ne nous pouvons se protéger que si nous sommes assez prudents et vigilent. Afin d'éviter les courriers indésirables, il est important d'adopter des bons réflexes à ce titre :

— Divulguer son adresse électronique le moins possible pour cela : éviter au maximum la publication des adresses e-mails sur des forums ou des sites internet et créer des adresses servant uniquement à s'inscrire ou s'identifier sur les sites jugés non dignes de confiance.
— Vérifier les informations de l'expéditeur et la présence d'erreur ou des fautes d'orthographes sur les emails suspects.
— Ne jamais répondre au spam, scam et aux messages de phishing même pour demander de ne plus recevoir ceux-ci, car cela indique à l'attaquant que votre adresse est une adresse valide ce qui aura pour conséquence l'augmentation du nombre de courriers indésirables que vous recevrez.
— Afin de lutter efficacement contre la propagation de fausses informations via des canulars, ne pas diffuser l'information si elle n'est pas accompagnée d'un lien vers un site précisant sa véracité.
— Sensibilisation et formation du personnel.
— Ne jamais donner ses identifiants et ses informations personnelles à quiconque.

Outre les bonnes pratiques énumérées, il existe des logiciels permettant de repérer les messages non sollicités tel que les antispam.

3.4.2 Les Attaques par déni de service

3.4.2.1 Présentation de l'attaque par déni de service

Une attaque par déni de service (DoS, Denial of Service) fait référence à des tentatives malveillantes visant à empêcher les utilisateurs légitimes d'accéder aux ressources demandées en réduisant la bande passante ou en rendant indisponible pendant un temps indéterminé les services ou ressources d'une organisation. Il

existe une variante de Dos dite DDos (Distributed DeniaI of Service) qui est similaire au DoS, mais qui se fait à partir de plusieurs machines.[Amiri 16][Bancal 09]

3.4.2.2 Les types d'attaques DOS

Les attaques Dos peuvent être classées en attaque par saturation qui consiste à saturer une machine de fausse requête et en attaque par exploitation de vulnérabilité qui exploite une faille d'un système afin de le rendre inutilisable. Différentes techniques d'attaques Dos existent dont les principales sont :

— **Attaque par réflexion (smurf) :** est un exemple d'attaque par saturation dans laquelle, l'attaquant envoie des paquets a des serveurs de diffusion en indiquant comme adresse IP source l'adresse de la cible, les serveurs vont donc diffuser les paquets sur l'ensemble des utilisateurs du réseau, puis rediriger l'ensemble des paquets émis en réponse vers la cible. [Amiri 16]

— **Attaque SYN (TCP/SYN Flooding) :** Une attaque SYN se base sur le principe de fonctionnement du TCP/IP qui opère en trois temps pour l'établissement de connexion entre le client et le serveur comme le montre la figure suivante :

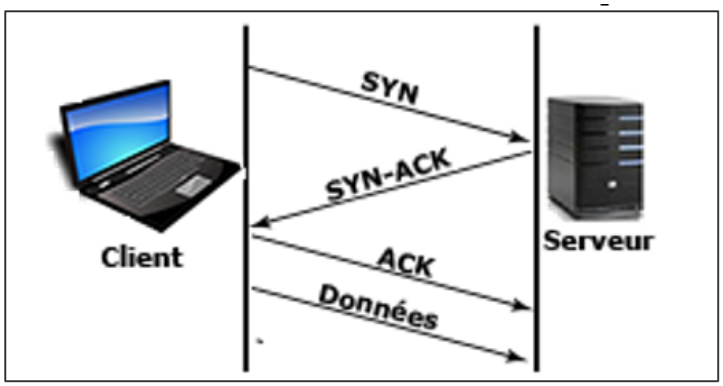

FIGURE 3.4.1 – Etablissement de connexion TCP/IP

L'attaque SYN consiste à inonder la cible par des requêtes SYN avec des adresses IP source erronées, la machine cible ne pourra donc pas répondre, ce qui fait que la connexion est mise en file d'attente en attendant l'ACK de l'utilisateur, qui une fois saturée, provoquera le plantage ou redémarrage de la machine.

— **Attaque du Ping de la mort (Ping of death) :** consiste à créer un datagramme IP dont la taille est supérieure à la taille maximale autorisée, ce qui provoquera un plantage sur la machine cible.

— **Attaque par fragmentation :** est une variante d'attaque par saturation dont le principe est de falsifier les informations de décalage des datagrammes IP, ainsi le destinataire ne sera pas capable de réassembler le paquet ce qui peut provoquer l'instabilité du système.
— **Attaque LAND :** consiste à envoyer vers la cible un paquet possédant la même adresse IP et le même numéro de port dans les champs source et destination des paquets IP. Ce paquet provoquera un plantage ou une instabilité du système.[Bay 15]
— **Attaque par downgrade :** L'attaquant demande au serveur d'utiliser une version d'un protocole plus ancienne afin d'exploiter les failles qu'elle comporte. Cette attaque peut s'effectuer sur toutes les applications réseau qui comportent des fonctionnalités de compatibilité avec d'anciennes versions. [Bay 15]

En résume, il existe de nombreuses autres techniques d'attaque Dos, l'attaque Dos n'en finissent d'évoluer, il n'est tout de même pas possible de faire le tour sur toutes ses techniques, néanmoins elles fonctionnent toutes pour un but commun qui est de rendre un système indisponible.

3.4.2.3 Les outils utilisés et les contremesures

Afin d'aboutir à leurs objectifs, les pirates utilisent des outils spécialisés dans le déni de service qui permettent d'envoyer des paquets TCP/IP sur commande, les principaux outils de Dos sont : L'outil hping3, Scapy, Metaspoit et LOIC.

Comment se protéger contre le déni de service ? Les attaques déni de service sont difficiles à combattre néanmoins, il existe certaines méthodes pour diminuer l'effet que peut produire ce type d'attaques sur notre système.

— Mise en place d'un pare-feu pour bloquer les connexions illégitimes.
— Absorber l'attaque en rajoutant des ressources.
— Implémenter la redondance des serveurs.
— Analyse constante du réseau et du trafic entrant et sortant.

3.4.3 L'attaque de l'homme au milieu

3.4.3.1 Présentation de l'attaque l'homme au milieu

L'attaque de l'homme au milieu ou Man in the middle (MiTM), est une attaque dans laquelle un pirate casse la liaison entre deux interlocuteurs et se fait passer pour l'autre entité, il intercepte et renvoie les communications et peut les modifier. [Bancal 09]

Les attaque MITM, peuvent avoir différents buts, un pirate peut se contenter d'intercepter le paquet et de le retransmettre tel quel, dans ce cas en parle d'attaque

par rejeu, ou de le modifier et l'altérer.

3.4.3.2 Principe de fonctionnement de l'attaque de MITM

Dans une attaque MITM, le pirate se place au milieu de la communication, et toute information va transiter par le pirate avant d'aller vers l'un des interlocuteurs. Cette transition est transparente, les deux communicants ne savent pas qu'il y a une personne tierces qui intercepte et lit leurs conversations, mais la question qui se pose est **comment le pirate peut-il se trouver au milieu des interlocuteurs ?**

Afin de réaliser son attaque, le pirate utilise ce qu'on appelle l'ARP Spoofing ou l'empoisonnement ARP (Protocole de Résolution d'Adresse), c'est en effet de l'usurpation d'adresse via le protocole ARP, la procédure que suit le pirate dans l'attaque MITM est la suivante :

Le pirate se trouvant sur le même réseau des deux interlocuteurs, commence par envoyer une requête ARP vers l'un des interlocuteurs pour lui indiquer que l'adresse IP du destinataire correspond à l'adresse MAC du pirate, ce qui fait que toutes les communications doivent passer par cette adresse MAC. La victime croit cette requête forgée et fait transiter ses données par l'adresse mac de l'attaquant. Le pirate effectue la même procédure avec le deuxième interlocuteur, ce qui fait que l'ensemble des échanges vont transiter par le pirate avant de passer vers les interlocuteurs. La figure suivante illustre un exemple de ce type d'attaque.

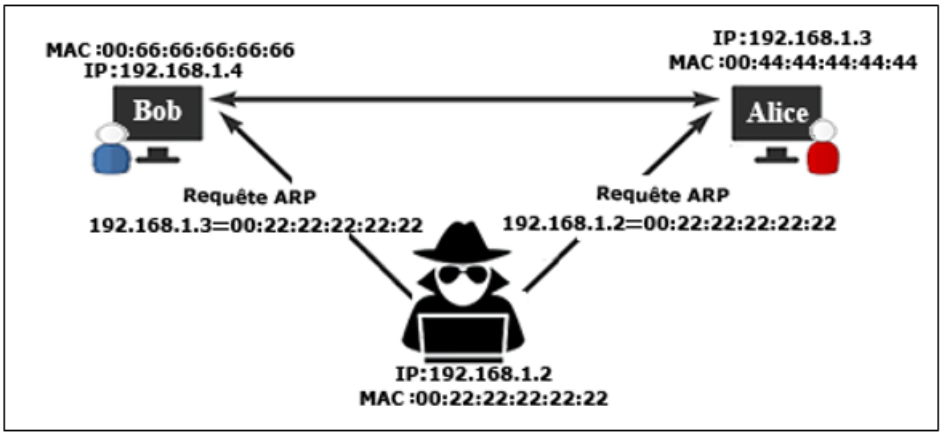

FIGURE 3.4.2 – L'attaque de l'homme au milieu

Dans le cadre des attaques MITM sur la messagerie électronique, le principe est quasiment le même, le pirate se positionne entre le client et le serveur de messagerie pour intercepter le trafic circulant, il fait croire au client qu'il fait office de serveur de messagerie, et il se prend pour le client auprès du vrai serveur de messagerie.

3.4.3.3 Les outils utilisés et les contremesures

Afin de réaliser une attaque Man in the middle, le pirate utilise des outils spécifiques dont :

- **Ettercap :** est une suite d'outils qui permet d'écouter sur le réseau et récupérer les informations et d'enregistrer dans un fichier les données récupérées.
- **DriftNet :** un autre outil d'attaque MITM qui permet de récupérer toutes les images du trafic réseau et de les afficher dans une fenêtre lorsqu'il est couplé à ettercap.
- **3vilTwinAttacker :** un autre outil d'attaque MITM, écrit en python et intègre un bon nombre d'outil permettant de faciliter l'attaque MITM.

Comment se protéger contre les attaque MITM ? Les attaques de l'homme au milieu sont des attaques très difficiles à détecter et très dangereuses, et afin de protéger ses données il est nécessaire de :

- Chiffrer les communications en utilisant de la cryptographie.
- Se servir des intermédiaires de confiance à savoir les autorités de certification.
- Faire une seconde vérification via un autre canal de communication.

3.4.4 Attaques de mots de passe

L'accès à un système informatique est dans la plupart du temps protégé par un mot de passe, celui-ci représente d'ailleurs la première défense contre les attaques. Néanmoins la plupart des utilisateurs, estiment qu'ils n'ont rien de secret à partager, ils choisissent pour cela des mots de passe simple facile à retenir et ils ignorent qu'ils mettent en danger le système en entier.

3.4.4.1 Techniques d'attaques de mot de passe

Il existe deux types d'attaques par mot de passe : les attaques par force brute, et les attaques par dictionnaire.

- **Attaque par force brute :** est la technique la plus utilisée qui consiste à essayer toutes les combinaisons possibles jusqu'à trouver le mot de passe.
- **Attaque par dictionnaire :** est une variante de la force brute qui consiste à essayer les mots prélevés dans un dictionnaire qui contient les mots susceptibles de constituer un mot de passe. [Belattaf]

Il est possible de combiner les deux techniques d'attaques afin de casser le mot de passe.

3.4.4.2 Les outils utilisés et les contremesures

Pour effectuer une attaque par mot de passe, les pirates utilisent une variété d'outils dont :

Les keyloggers : un keylogger ou un enregistreur de frappe, est un programme informatique qui surveille et enregistre sur un fichier journal, toutes les frappes effectuées par un utilisateur pour obtenir un accès non autorisé à des mots de passe ou d'autres informations confidentielles. Le fichier est envoyé discrètement vers l'adresse e-mail du pirate, une fois la victime connectée à internet.[Dewett 15] [Norman Alan 17]

L'ingénierie sociale et l'espionnage : L'ingénierie sociale consiste à exploiter la naïveté des individus pour obtenir des informations. Un pirate peut ainsi obtenir le mot de passe d'un individu en se faisant passer par exemple pour un administrateur du réseau. L'espionnage quant à lui représente la plus vieille des méthodes. Il suffit en effet parfois à un pirate d'observer les papiers autour de l'écran de l'utilisateur ou sous le clavier afin d'obtenir le mot de passe.[Bay 15] [Dewett 15]

Comment se protéger des attaques par mot de passe ?

— Choisir des mots de passe complexe long et difficile à casser, éviter les mots de passe facile à deviner dont l'identifiant, le nom et prénom, etc.
— Faire un scan avec un antivirus pour détecter les keyloggers et utiliser des anti-keyloggers tel que Spyshelter et keyscrambler qui permettent de chiffrer les touches tapées, empêcher les keyloggers de les récupérer et les déchiffrer avant de les placer dans l'application concerner.
— Utiliser des site comme `https://www.virustotal.com/`ou `https://www.malwr.com/` pour scanner avec une variétés d'antivirus les fichiers que vous jugez keylogger ou autres logiciels d'espionnage.
— Utiliser les outils de cassage de mot de passe pour tester la sécurité de sa politique de mot de passe tel que John The Ripper (JTR), Hashcat, crunch et Ophcrack, ce sont des logiciels qui permettent de craquer les mots de passe à partir de leurs hashs.
— Et enfin le meilleur moyen de prévention est la vigilance et la prudence.

3.5 Les mécanismes de sécurité

Afin de pouvoir réduire la probabilité que notre système soit infecter ou au moins de réduire les dommages que peuvent causés ces risques, il est nécessaire de mettre en place des mécanismes de sécurité.

3.5.1 La cryptographie

Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages. Le message chiffré est appelé cryptogramme (ciphertext) par opposition au message initial, appelé message en clair

(plaintext). La cryptographie peut être utiliser pour garantir la confidentialité, l'intégrité, l'authentification et la non répudiation.

3.5.1.1 Le chiffrement

Le cryptage ou chiffrement consiste à faire subir à un texte clair une transformation plus ou moins complexe pour en déduire un texte inintelligible, dit chiffré. On distingue généralement deux types de chiffrement :

— **Le chiffrement symétrique :** également appelé chiffrement à clé privée ou chiffrement à clé secrète, ce type de chiffrement repose sur deux éléments : une fonction mathématique et une clé secrète qui est utilisée à la fois pour le chiffrement et pour le déchiffrement et qui est pré-partagée entre les communicants via un canal sécuriser.

— **Le chiffrement asymétrique :** également appelé chiffrement à clés publiques, repose sur l'utilisation d'une paire de clés : une clé publique pour le chiffrement et une clé secrète pour le déchiffrement. Ainsi lorsqu'un utilisateur désire envoyer un message à un autre utilisateur, il lui suffit de chiffrer le message à envoyer au moyen de la clé publique du destinataire Le destinataire sera en mesure de déchiffrer le message à l'aide de sa clé privée. [Bay 15][Lehning 13]

Afin d'illustrer le fonctionnement du chiffrement symétrique et asymétrique voyant la figure ci-dessus.

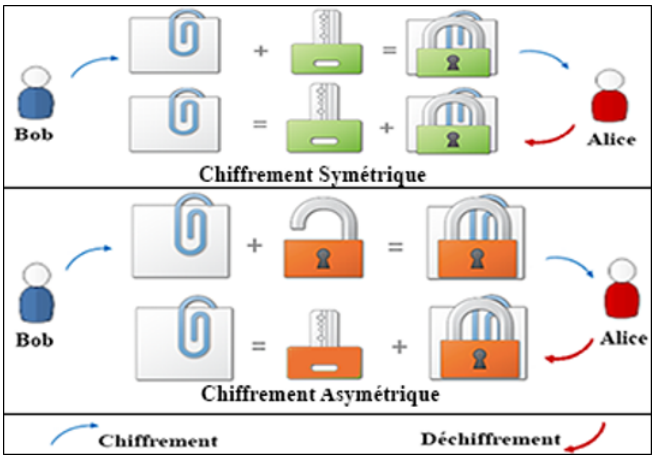

FIGURE 3.5.1 – Le chiffrement symétrique et asymétrique

Le chiffrement assure la confidentialité du fait que seul les personnes ayant la clé privée peuvent décrypter le message et donc accéder à son contenu.

3.5.1.2 La signature numérique

La signature numérique également appelée signature électronique est un procédé permettant de garantir l'authenticité de l'expéditeur, de vérifier l'intégrité du message reçu et d'assure la fonction de non répudiation.

Principe de la signature numérique

La signature se base sur les principes du chiffrement asymétrique. La procédure que suit l'émetteur pour signer un message est la suivante :

1. Il produit un haché du message par une fonction de hachage choisie. Une fonction de hachage permet d'obtenir un condensé d'un texte, c'est-à-dire une suite de caractères assez courte représentant le texte qu'il condense.
2. Il chiffre ensuite le digest en utilisant sa clé privée et un algorithme de chiffrement.
3. Le résultat qui constitue la signature numérique ainsi que la clé publique sont envoyés au récepteur.

Une fois le message reçu le récepteur suit une autre procédure pour la vérification.

1. Il commence par déchiffrer la signature numérique en utilisant la clé publique de l'émetteur et le même algorithme de chiffrement, il aura comme résultat le digest de l'émetteur.
2. Il recalcule ensuite le condensé en utilisant la données et la même fonction de hachage.
3. Enfin Il compare les deux condensés, s'ils sont identiques cela veut dire que le message n'a pas été modifié durant le transfert et que l'émetteur est authentifié.

La figure ci-dessus illustre le principe de la signature numérique.

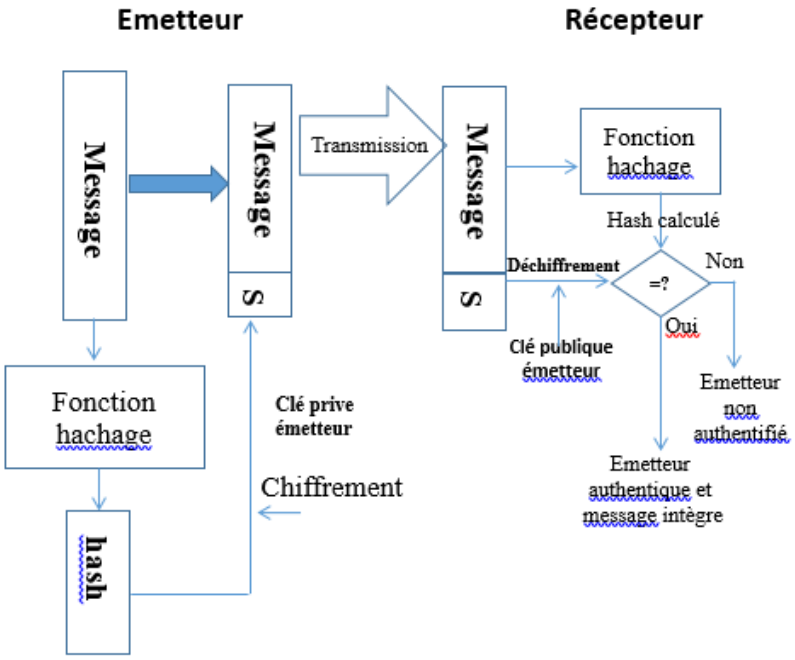

FIGURE 3.5.2 – La signature numérique

Pourquoi l'émetteur chiffre avec sa clé privé et non pas avec la clé publique du destinataire comme c'était le cas avec la confidentialité ? La réponse est simple, signer un message, reviens à s'assurer que la personne émettrice est bien celle qu'on prétend être. Pour ce faire, il est nécessaire de posséder une information unique de l'expéditeur, dont personne d'autre ne peut posséder et c'est bien la clé privée.

3.5.1.3 Les certificats numériques

Le chiffrement asymétrique est basé sur l'utilisation d'une clé publique partagée entre les interlocuteurs. Le problème avec ces clés est que rien ne garantit que la clé est bien celle de l'utilisateur à qui elle est associée. Un pirate peut corrompre une clé publique en la remplaçant par sa clé publique, il sera donc en mesure de déchiffrer tous les mails chiffrés avec sa clé publique.

Comment s'assurer de la validité de la clé publique ? c'est justement au travers des certificats numériques. Un certificat est un document qui permet d'associer une clé publique à une entité, c'est en quelque sorte la carte d'identité de la clé publique, il contient la clé publique du propriétaire du certificat, la date de validité du certificat, l'algorithme de chiffrement utilisé pour signer le certificat, la signature de l'émetteur du certificat, etc.

Comment obtenir ce certificat ? Les utilisateurs peuvent obtenir des certificats grâce à des PKI. Une PKI (Public Key Infrastructure), également appelée IGC (Infrastructure de Gestion de Clés) est un système de gestion de clés et de certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique, autrement dit une PKI a pour fonction d'assister les utilisateurs pour obtenir les clés publiques nécessaires. Une PKI se compose de quatre éléments essentiels :

- **Une Autorité d'Enregistrement (RA) :** permet de traiter les demandes de certificat et de générer les clés publique et privée.
- **Une Autorité de Certification (CA) :** reçoit les demandes de certificats, génère les certificats et les signe avec sa clé privée.
- **Une Autorité de Dépôt (Annuaire) :** charger de diffuser les certificats aux utilisateurs.
- **Les utilisateurs de la PKI :** désignent les utilisateurs ayant effectué la demande de certificat ainsi que les utilisateurs qui souhaitent vérifier l'identité d'un certificat qu'ils ont reçu.

Bien que la fonction d'enregistrement puisse être mise en œuvre directement avec l'autorité de certification, il est parfois utile dans les grandes entreprises de décharger la fonction d'enregistrement vers un composant distinct.[Adams 02]

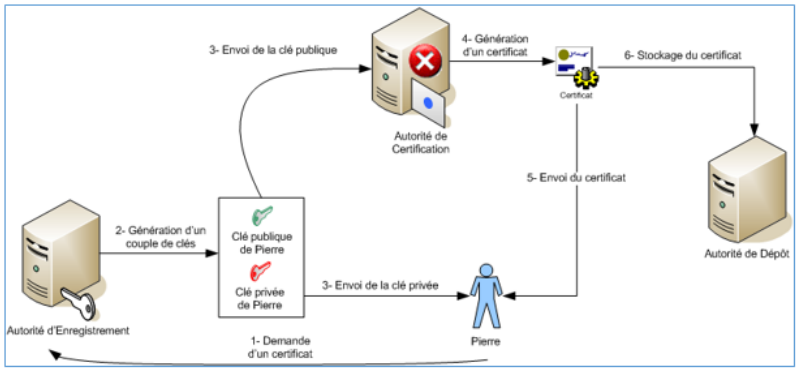

FIGURE 3.5.3 – La signature numérique

Ainsi lorsqu'un utilisateur désire communiquer avec une personne, il lui suffit de récupérer le certificat du destinataire et de vérifier sa signature pour s'assurer que ce document n'a pas été falsifié et provient de la CA. Après avoir vérifié que la signature est valide, l'utilisateur peut donc récupérer la clé publique contenue dans ce certificat et l'utiliser avec confiance.

3.5.2 Les protocoles de sécurité

3.5.2.1 Le protocole S/MIME

Protocole S/MIME (Secure Multipurpose Mail Extension) est un protocole pour l'envoie des messages chiffrés et signés numériquement, il permet de ce fait de garantir la confidentialité, l'intégrité, l'authentification et la non répudiation des messages électronique. [Ramsdell 99]

Fonctionnement du protocole S/MIME : Le protocole S/MIME est basé sur le chiffrement asymétrique pour offrir deux services de sécurité : la signature numérique et le cryptage des messages, nous avons vu dans la partie cryptographie comment fonctionne séparément chacune des méthodes, néanmoins il faut savoir que ces deux services ne s'excluent pas mutuellement au contraire ils sont conçus pour être utilisés conjointement. Avec le protocole S/MIME, il est possible d'implémenter un de ces services seulement, tout comme il est possible de les combiner.

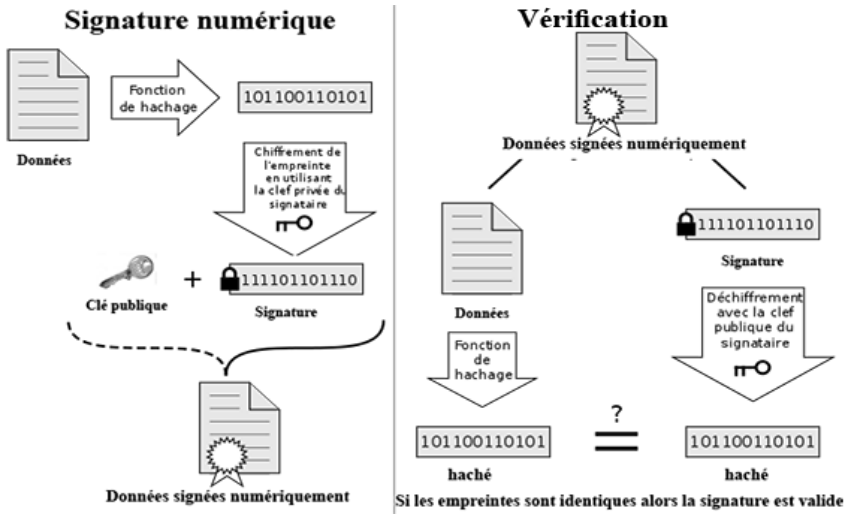

FIGURE 3.5.4 – Fonctionnement du protocole S/MIME

Le protocole S/MIME version 3 utilise le triple traitement et un message S/MIME soumis au triple traitement est signé, crypté, puis resigné. Il a noté aussi qu'il est possible de signer le message avec une clé de session crypté avec la clé publique afin d'améliorer les performances.

3.5.2.2 Le protocole PGP

PGP (Pretty Good Privacy) est un protocole développé par Phil Zimmermann en 1991. PGP combine chiffrement à clé publique et la signature numérique pour offrir

un bon niveau de confidentialité, d'intégrité, de non-répudiation et d'authenticité. [Garance 06]

Fonctionnement du PGP : PGP est un système de cryptographie hybride, utilisant une combinaison du chiffrement symétrique et asymétrique. Cette combinaison permet de chiffrer rapidement et de manière sécurisée. La procédure que suit le protocole PGP est illustrer dans la figure suivante :

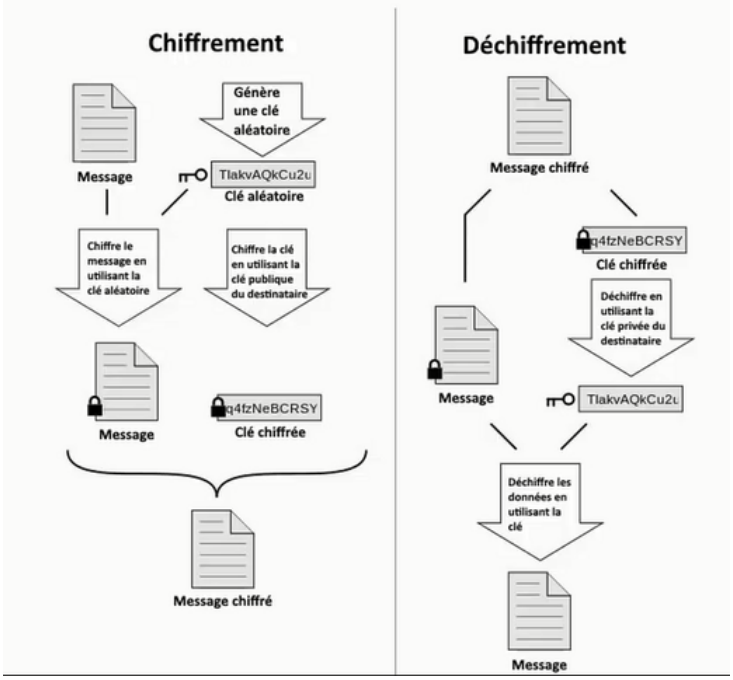

FIGURE 3.5.5 – Fonctionnement du protocole PGP

PGP crée une clef de session qui est une clef secrète à usage unique et s'en sert pour chiffrer le message en suivant un algorithme symétrique. Il chiffre ensuite cette clé aléatoire, en utilisant un algorithme asymétrique, grâce à la clé publique du destinataire. Le message est enfin transmis chiffré, accompagné de la clé chiffrée. Pour décrypter, il commence par déchiffrer la clé de session avec sa clé privée puis déchiffre les données avec cette clé de session. Lorsque l'on souhaite signer un message avec PGP, on chiffre le message avec la clé privée du destinataire.

3.5.2.3 Le protocole SSL

Le protocole SSL (Secure Sockets Layer) crée par Netscape, racheté l'IETF et rebaptisé en TLS (Transport Layer Security). SSL repose sur la cryptographie a clé publique afin de garantir la sécurité des communications entre un client et un serveur, en établissant un canal de communication sécurisé (chiffré) assurant ainsi la confidentialité et l'intégrité des données échangées et l'authentification au serveur. [Bay 15]

Fonctionnement du protocole SSL :

L'établissement de la liaison SSL entre le client et l'hôte se produit en deux temps : la négociation SSL et La communication SSL.

- **Protocole TLS Handshake (phase de négociation) :** est la phase au cours de laquelle les parties négocient les paramètres de connexion et effectuent l'authentification, la négociation SSL se déroule de la manière suivante.
  - Le client se connecte au serveur sécurisé par SSL et lui demande de s'authentifier. Il lui envoie également la liste des méthodes de chiffrement qu'il supporte.
  - À la réception de la requête le serveur envoie un certificat au client contenant la clé publique du serveur, signée par la CA, ainsi que le protocole de chiffrement le plus puissant dans la liste avec lequel il est compatible.
  - Le client vérifie la validité du certificat, extrait la clé publique puis génère une clé secrète aléatoire qu'il chiffre avec la clé publique du serveur, puis envoie le résultat au serveur.
  - Le serveur est en mesure de déchiffrer la clé de session avec sa clé privée. Ainsi, les deux entités sont en possession d'une clé commune dont ils sont les seuls connaisseurs. [Stephen 00], [Bay 15]

Voici un exemple de négociation SSL entre un client et un serveur :

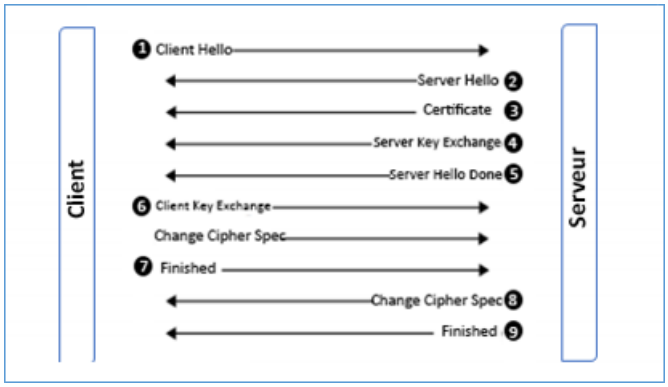

FIGURE 3.5.6 – Exemple de négociation SSL

— **TLS Record Protocol (phase de communication) :** permet d'encapsuler les messages et d'assurer la confidentialité et l'intégrité via la signature et le chiffrement.

SSL pour le web : HTTPs

Avec http la communication entre le client et le serveur n'étant pas chiffrée, les données transitent en clair ce qui fait que toutes les données que vous entrez sur un site seront envoyées en format texte brute et seront, par conséquent, vulnérables aux interceptions et à l'espionnage. Néanmoins lorsque l'http est encapsulé dans l'SSL il offre une certaine sécurité, il permet d'une part au visiteur de vérifier l'identité du site web auquel il accède garantissant ainsi l'authenticité du serveur et d'autre part il assure la confidentialité et l'intégrité des données envoyées par l'utilisateur en chiffrant la connexion entre le serveur web et le navigateur. [Stephen 01]

3.5.2.4 Le protocole Kerberos

Kerberos est un protocole d'authentification réseau créé par MIT (Massachusetts Institute of Technology) qui repose sur la cryptographie à clés symétriques et l'utilisation de tickets pour authentifier les utilisateurs auprès des services réseau. [Red Hat 05]

Fonctionnement du Kerberos :

Le protocole Kerberos repose sur l'utilisation d'un tiers de confiance appelé centre de distribution de clés (KDC : Key Distribution Center) qui est constitué de deux composants :

— **Un serveur d'authentification(AS) :** qui effectue l'authentification de l'utilisateur.

— **Un serveur de Ticket-octroi(TGS) :** qui permet d'autoriser un utilisateur d'accéder à des services réseau en lui accordant un ticket de service (TGS : Ticket Granting System).

Les étapes de l'authentification kerberos sont présentées dans la figure suivante :

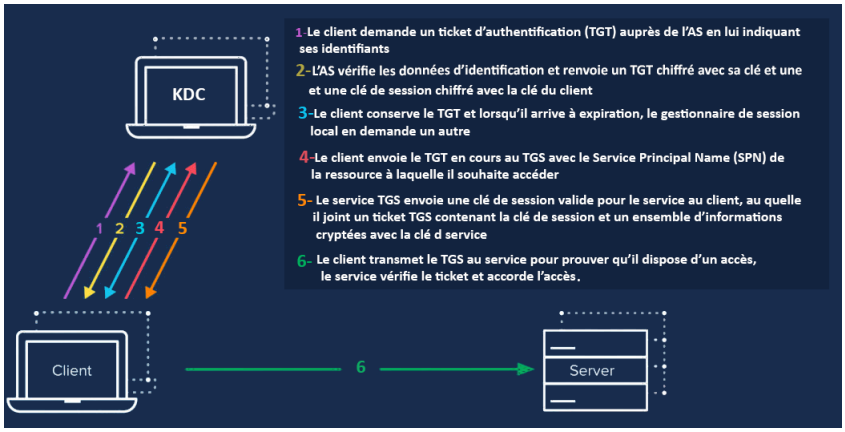

FIGURE 3.5.7 – Exemple de négociation SSL

Le TGT prouve que le client s'est bien adressé au KDC, la première clé de session envoyer au client par l'AS lui servira pour communiquer de manière sécurisée avec le KDC (pour les futures demandes de tickets au TGS), la seconde clé de session envoyer par le TGS servira pour crypter les communications entre le client et le service

3.6 La sécurité de la messagerie Exchange

La procédure de sécurité et les différentes étapes à entreprendre pour la sécurité de sa messagerie d'entreprise dépend grandement du produit à utiliser. Cela dépend en effet de son architecture, des technologies qu'il peut prendre en charge, des menaces auxquels il est vulnérable et de beaucoup d'autres facteurs. Nous allons de ce fait aborder dans cette partie la politique de sécurité que nous mettrons en place sur notre messagerie Exchange.

3.6.1 La sécurité du transport des messages

L'email transite par différents équipements avant d'atteindre sa destination et éventuellement par une variété de risques. Le transport du courrier se base sur les protocole Smtp, Pop et http, néanmoins ces protocoles permettent de transiter les mails en clair sur le réseau. Afin de se protéger il est donc nécessaire d'établir un canal de transmission sécurisé et chiffré. Pour la sécurité des échanges au sein d'exchange nous allons créer un canal de transmission sécurisé via le protocole TLS permettant d'encapsuler les protocoles d'échanges d'emails et de sécuriser la communication entre les MTA et entre le serveur et client de messagerie et ainsi garantir le transport des e-mails en toute sécurité.

3.6.2 La protection du contenu des Emails

Les entreprises ont souvent recours à la messagerie électronique pour échanger des informations sensibles, telles que les rapports financiers, des analyses de concurrence, des informations sur les clients et les employés, etc. La fuite de ces informations peut donc représenter une sérieuse menace pour les entreprises et causée entre autre des dommages financiers, détérioration de l'image de l'entreprise auprès de ses clients, perte de l'avantage concurrentiel, etc. Il est donc indispensable de protéger le contenu des emails contre la divulgation et la modification. Pour ce faire nous allons combiner deux technologies différentes : S/MIME et IRM au sein de l'organisation Exchange.

3.6.2.1 Le protocole S/MIME

S/MIME est un protocole de cryptage de bout en bout également appelé cryptage d'écrivain à lecteur, car les messages sont cryptés de l'expéditeur au destinataire et le cryptage est préservé tout au long du transfert du message. En plus du cryptage, S / MIME prend également en charge la signature numérique des messages. [Neil 13]

Afin de garantir l'intégrité, l'authenticité et la non-répudiation des messages nous allons utiliser dans le cadre de ce projet le protocole S/MIME en sa 3ème version.

Le protocole SSL assure déjà le chiffrement de la communication pourquoi utiliser un autre mécanisme ? Il ne faut pas confondre la protection de la communication de la protection du contenu, le protocole SSL protège les données pendant leurs transports mais une fois reçu dans la boîte aux lettres rien ne vous garantit leurs confidentialités et leurs intégrités.

3.6.2.2 La gestion des droits relatifs à l'information (IRM)

Le service Gestion des droits relatifs à l'information (IRM) permet de restreindre les actions qui peuvent être effectuées par les utilisateurs sur les courriers électroniques (telles que l'impression, la copie, le transfert et la réponse, les dates d'expiration, etc.), il permet également d'assurer le chiffrement des emails. IRM est donc un moyen de garantir une protection permanente au courrier durant toute sa durée de vie.[Neil 13]

S/MIME permet déjà de protéger le contenu de l'email ?

Avec S/MIME le message est protégé pendant son transit ainsi que dans l'application de messagerie de l'utilisateur, ce qui fait qu'entre l'expéditeur et le destinataire, le message est très sécurisé. Mais une fois le courrier déchiffré la protection ne persiste pas, il n'y a aucun contrôle sur ce que le destinataire peut faire avec les informations qu'il contient.

3.6.3 La protection contre les pertes de données

Les services basés sur une architecture centralisée dont la messagerie permettent de faciliter le déploiement, l'administration et la maintenance des services. Ils posent toutefois le soucis de la disponibilité. Ainsi lorsque l'on souhaite sécuriser une architecture, on doit donc penser à vérifier l'ensemble des composants pouvant entraîner une panne complète du système. L'objectif est d'envisager une panne de n'importe lequel de ces composants sans que cela empêche l'accès au service. [Russel 15]

3.6.3.1 Le DAG, Le load Balacing et le Safety Net

Dans Exchange 2013 trois services doivent être hautement disponible : le service d'accès client, le service de transport de courrier et le service de stockage de mails puisque la panne d'un de ces composants entraine la panne du système en entier. Exchange 2013 rend la haute disponibilité de ces services possible grâce aux technologies suivantes : Le DAG pour le service de boites aux lettres, le Load Balancing pour l'accès client et le Safety Net pour le service de transport et d'autres concepts que nous allons aborder au cours du chapitre 4.

3.6.3.2 La sauvegarde et la restauration

Exchange Server 2013 automatise le processus de protection et récupération des données des serveur grâce aux technologie de la haute disponibilité. Cependant, il existe encore des situations où une panne matérielle, une erreur humaine, voir une catastrophe naturelle, peut nécessiter une intervention manuelle pour restaurer les données et ramener le système à des conditions de service normales. Exchange 2013 met à disposition des administrateurs différents mécanismes permettant d'assurer la sauvegarde, la restauration de bases de données, ainsi que les mécanismes nécessaires pour assurer une reprise après sinistre.

3.7 Conclusion

La messagerie électronique est l'un des nombreux domaines dans lesquels la technologie seule ne peut pas fournir la solution complète de sécurité. Une messagerie sécurisée dépend grandement du sens de responsabilité de ses usagers et de l'efficacité des solutions de sécurité proposées par les administrateurs de messagerie. Après avoir fait le tour sur la messagerie électronique et sa sécurité, nous allons à présent passer au chapitre 4 dont nous allons voir la procédure à suivre pour une messagerie efficace avec le moindre risque possible.

Chapitre 4

Implémentation de la solution de messagerie sécurisée et tolérante aux pannes

4.1 Introduction

Ce chapitre sera consacré à la partie pratique de notre projet, nous allons décrire étape par étape et de manière explicite la démarche que nous allons suivre pour la mise en œuvre d'une solution de messagerie sécurisée et hautement disponible sous Exchange server 2013. Pour ce faire nous allons travailler en six phases :

- Dans la phase 1 nous allons faire une introduction d'Exchange Server, son architecture, ses clients et les technologies avec lesquelles il travaille.
- Dans la phase 2 nous allons décrire l'architecture réseau a déployer.
- Dans la phase 3 nous allons installer et préparer Active Directory en vue de la préparation de l'installation d'Exchange et ensuite nous allons procéder a l'installation d'exchange
- Dans la phase 4 nous allons configurer les différents composants d'exchange afin d'avoir un environnement de messagerie fonctionnel et fiable.
- Dans la phase 5 nous allons présenter et implémenter la sécurité de la messagerie Exchange.
- Dans la phase 6 nous allons présenter et implémenter la haute disponibilité d'Exchange.

4.2 Introduction à Exchange 2013

Après 17 ans d'expérience avec la plateforme de messagerie Exchange, Microsoft publie la huitième version du produit, une version qui a apporté d'importantes modifications en comparaison à ses prédécesseurs, notamment au niveau architectural. Les modifications visaient essentiellement à simplifier Exchange Server et à le rendre plus redondant et plus fiable.

4.2.1 Architecture technique d'Exchange 2013

Exchange 2013 contrairement à ses prédécesseurs, ne possède plus que deux principaux rôles :

1. **Rôle d'accès au client (Client Access role : CAS) :** ce rôle permet de gérer les accès des clients auprès de leurs comptes Exchange. Un serveur CAS se contente d'authentifier le client et d'acheminer la requête par proxy au serveur de boites aux lettres du destinataire.
2. **Rôle de boite aux lettres (Mailbox : MBX) :**Ce rôle permet d'héberger l'ensemble des boites aux lettres. Un serveur de boites aux lettres est l'endroit où s'effectue tout le traitement concernant les e-mails.[Microsoft 16], [Wesselius 14a]

Pourquoi Microsoft a-t-elle réduit le nombre de rôles a deux ?

Avant Exchange 2013 les fonctions d'Exchange étaient segmentées sur 5 rôles distincts :

- **Le rôle CAS :** pour la gestion des accès client aux comptes Exchange.
- **Le rôle MBX :** pour le stockage des boites aux lettre.
- **Le rôle transport HUB :** pour le routage des messages à l'intérieur et vers l'extérieur de l'organisation.
- **Le rôle Edge :** pour la gestion des messages en provenance et à destination d'internet, dans le cas de la présence d'un serveur Edge, le serveur hub n'aura pour rôle que la gestion du routage d'e-mails à l'intérieur de l'entreprise
- **Le rôle de messagerie unifiée (UM) :** pour la gestion des messages vocaux et fax dans la boite aux lettre. Il joue le rôle d'intermédiaire entre l'infrastructure téléphonique et l'organisation Exchange, il permet entre autre la réception des messages vocaux et fax dans la boite aux lettre de l'utilisateur et la consultation des boites au lettres via une messagerie vocales.

Néanmoins, par retour d'expérience on s'est aperçu que les entreprises travaillaient sur des serveurs multi-rôles et souvent les administrateurs mettaient en place une topologie CAS/Edge dans la DMZ (Zone démilitarisée) et une topologie Mailbox/Hub en local et donc la forte diminution des rôles est issue du retour d'expérience utilisateurs et administrateurs d'Exchange.

Ou sont-il passé l'ensemble des fonctionnalités assurées par les rôles supprimés ?

Avec Exchange 2013, Microsoft a conservé les fonctionnalités en revanche elle a réduit la présence des rôles. Cependant le service de transport est assuré par les serveurs MBX et CAS, le service de messagerie unifiée quant à lui est assuré par le serveur MBX, le rôle Edge a été abandonné par la version RTM d'exchange 2013 puis revenu comme rôle distinct avec le service pack1.

4.2.2 Les clients Exchange

Les clients Exchange constituent la partie la plus importante de tout système de messagerie vus que c'est l'interface par laquelle les utilisateurs accèdent à leurs comptes et une des raisons du succès d'Exchange est justement la connectivité client puisque Exchange est désormais capable de prendre en charge une très grandes variété de clients de messagerie et d'offrir différents types d'accès à savoir :

- **Le client Outlook :** est le client lourd d'Exchange fonctionnant via la fonctionnalité Outlook Anywhere qui permet aux clients Ms Outlook de se connecter à leurs serveurs Exchange en interne tout comme a l'extérieur du réseau d'entreprise ou via internet.

— **Outlook Web App (OWA) :** connu sous le nom Outlook Web Access dans les versions antérieurs à Exchange 2010, OWA est le Webmail d'Exchange permettant aux utilisateurs d'accéder à leurs boites aux lettres via différents navigateur Web sur différents systèmes d'exploitation
— **Les clients Exchange ActiveSync :** Exchange ActiveSync (EAS) est le protocole utilisé par les clients mobiles pour se connecter à l'environnement Exchange, il permet de synchroniser votre appareil avec votre boite aux lettre Exchange via la fonction Direct Push qui permet d'informer le périphérique mobile lorsque de nouvelles informations sont prêtes à être synchronisées.
— **Les clients de messagerie tiers :** étant donné qu'exchange 2013 prend en charge les protocoles Pop et Imap, les utilisateurs peuvent utiliser n'importe quel client de messagerie compatible avec ces protocoles afin d'établir une connexion au serveur Exchange. Ces applications incluent Gmail, Mozilla Thunderbird, Eudora, MailPeek et beaucoup d'autres. [Microsoft 16], [Wesselius 14a], [Winters 13]

4.2.3 Exchange server et Active Directory

Avec la messagerie électronique, nous devons conserver tant d'informations qu'il est devenu indispensable de se fier à des annuaires. Exchange server lui qui ne sais jamais en passer, il embraquait depuis son apparition son propre annuaire jusqu'à ce que Active Directory vois le jour en 1996 et devient alors la base d'Exchange server, mais **c'est quoi Active Directory ?**[Wesselius 14a], [Crawford 08]

4.2.3.1 Introduction à Active Directory

Définition d'Active Directory

Apparus en 1996, utilisable depuis 1999 avec Windows Server 2000 jusqu'à nos jours. Active Directory est un annuaire crée par Microsoft, il permet de centraliser toutes les informations relatives aux ressources réseau au sein de l'annuaire dans le but de faciliter leur implantation ainsi que leur gestion. Active Directory est composé d'une suite de rôles :

— **Les services de domaine Active Directory (ADDS, Active Directory Domain Services) :** constituent un annuaire centralisé destiné à la gestion et à l'authentification des utilisateurs et des ordinateurs.
— **Les Services de certificats Active Directory (AD CS, Active Directory Certificate Services) :** ce rôle permet d'installer une autorité de certification au sein du réseau d'entreprise pour pouvoir délivrer des certificats de façon aisée aux utilisateurs et ordinateurs.
— **Les Services de federation Active Directory (AD FS, Active Directory Federation Services) :** ce rôle permet d'établir une relation d'appro-

bation entre différents environnements AD, afin d'ouvrir un accès sécurisé a certains de vos services pour vos partenaires externes.
- **Les services AD LDS (Active Directory Lightweight Directory Service) :** procurent un service d'annuaire aux applications, il permet de répertorier des informations nécessaires aux applications dans un annuaire plutôt qu'individuellement dans chaque application.
- **Les services AD RMS (Active Directory Rights Management Services) :** permet de renforcer la sécurité d'une organisation. Avec AD RMS l'émetteur accompagne l'objet par une licence de publication, le serveur AD RMS assure le respect de cette licence par le récepteur.[Crawford 08], [Deman 08]

Terminologie et concepts d'Active Directory :

Comme Active Directory est la base d'Exchange il est important de connaitre les termes utilisés pour décrire des concepts d'AD que nous utiliserons par la suite lors de la mise en place d'Exchange. Nous présenterons dans ce qui suit les termes et les concepts fondamentaux d'Active Directory.

- **Objet active directory :** Un objet est un ensemble particulier d'attributs qui représente quelque chose de concret, par exemple un utilisateur, une imprimante, un serveur, un domaine, etc. [Deman 08]
- **Domaines et sites :** Un domaine est l'unité de base chargée de regrouper de façon logique les objets qui partagent un même espace de nom et une même base de données d'annuaire. Un site contrairement à un domaine mappe la structure physique de l'organisation, il désigne la combinaison d'un ou plusieurs sous-réseaux IP.[Deman 08]
- **L'unité d'organisation (OU) :** est un conteneur Active Directory qui permet de renfermer des objets et d'autres unités d'organisation.[Crawford 08]
- **Arborescences et forêts :** Une arborescence de domaines est le regroupement hiérarchique de plusieurs domaines partageant un espace de nom contigu. La forêt quant à elle consiste à regrouper plusieurs arborescences de domaine.[Deman 08]
- **Contrôleurs de domaine (DC) :** Un DC est chargé de stocker l'ensemble des données et de gérer les interactions entre les utilisateurs et le domaine (recherche dans l'annuaire, ouverture de session, etc).[Deman 08]
- **La base de données Active Directory :** contient l'ensemble des informations relatives à l'annuaire, elle est représentée par le fichier NTDS.DIT et subdivisée en 4 partitions logiques :
  - **Partition de schéma :** Le schéma AD détermine quels types d'objets sont disponibles et quels attributs ont ces objets. Par exemple, si un nouvel utilisateur est créé, un objet utilisateur est instancié à partir du schéma, les propriétés requises sont renseignées et le compte utilisateur

est stocké dans la base de données Active Directory.
- **Partition de configuration :** est l'endroit où se trouvent toutes les informations qui doivent être disponibles dans toute la forêt Active Directory.
- **Partition de domaine :** stocke des objets spécifiques à un domaine, ainsi que leurs attributs.
- **Partition d'application :** stocke les données sur les applications utilisées dans Active Directory.

Les contrôleurs de domaine d'une même forêt ont des partitions de configuration et de schéma commune, ceux du même domaine partagent la partition de domaine, la partition d'application quant à elle se réplique sur des DCs choisis et faisant partie de la même forêt.

- **Le catalogue global :** Comporte une copie partielle de chacun des objets de l'annuaire Active Directory avec une petite partie des attributs des objets d'origine. Les attributs repris dans le catalogue global sont les attributs les plus communément utilisés dans les opérations de recherche (les nom et prénoms de l'utilisateur, etc.) ainsi que les attributs requis pour localiser le réplica complet de l'objet.

4.2.3.2 Intégration d'Exchange dans Active Directory

Exchange 2013 est étroitement intégré à Active Directory, il s'en sert principalement pour le stockage et le routage. Il inscrit dans chacune des partitions de la base de données Active Directory des éléments :

- **Dans la partition de schéma :** Lors de l'installation du premier serveur Exchange de la forêt, le processus de préparation d'AD en ajoute une multitude de classes d'objets et attributs spécifiques à Exchange dans le schéma AD. Cela permet de créer les objets d'Exchange et d'étendre certains objets existants avec de nouveaux attributs.
- **Dans la partition de configuration :** stocke toute la configuration Exchange, la configuration décrit la structure de l'organisation Exchange.
- **Dans la partition de domaine :** Lors de l'installation du premier serveur Exchange de la forêt, les objets Exchange sont créés dans la partition de domaine.[Stanek 13b]

En plus du stockage Exchange 2013 utilise la topologie de routage d'annuaire pour déterminer comment acheminer les messages au sein de l'organisation.

4.2.4 Exchange server et Windows PowerShell

PowerShell est à la fois un interpréteur de commandes et un puissant langage de scripts, développé par Microsoft et conçu initialement pour la gestion et l'adminis-

tration des systèmes d'exploitation, il sert maintenant aussi pour l'administration de certains produits tels que Microsoft Exchange Server, Microsoft SQL Server, Active directory, SharePoint, etc.

Avec PowerShell nous ne manipulerons plus uniquement du texte, comme c'est le cas avec la plupart des autres shells, mais le plus souvent des objets, c'est d'ailleurs cette facilité de manipuler les objets qui fait de PowerShell un shell d'exception !

Pourquoi utiliser les scripts ?

Depuis toujours les administrateurs système utilisent des scripts pour automatiser la réalisation des tâches fastidieuses. En effet, quoi de plus inintéressant que la répétition de tâches d'administration, telle que la création de comptes utilisateurs sans compter les erreurs commises et tout le temps perdu alors qu'il est possible d'écrire un petit script qui réalisera tout le travail à notre place. Vous l'avez compris L'intérêt principal du scripting réside dans l'automatisation des tâches en supprimant les erreurs induites par un traitement manuel. [Lemesle]

Et Exchange dans tout cela ?

PowerShell est le langage de script que nous utiliserons au cours de ce travail pour l'ensemble des tâches d'installation et de configuration de notre solution de messagerie.

4.3 Conception de l'architecture réseau à déployer

Notre projet a pour but de déployer une solution de messagerie sécurisée et tolérante au pannes avec Microsoft exchange 2013 et afin de réaliser ce travail nous avons fait appel à un Lab virtuel pouvant être adapter facilement aux besoins des entreprises. Dans ce qui suit nous allons dans un premier temps présenter la maquette réseau, puis nous présenterons en détail les différents éléments de celle-ci ainsi que son plan d'adressage.

Schéma du Lab :

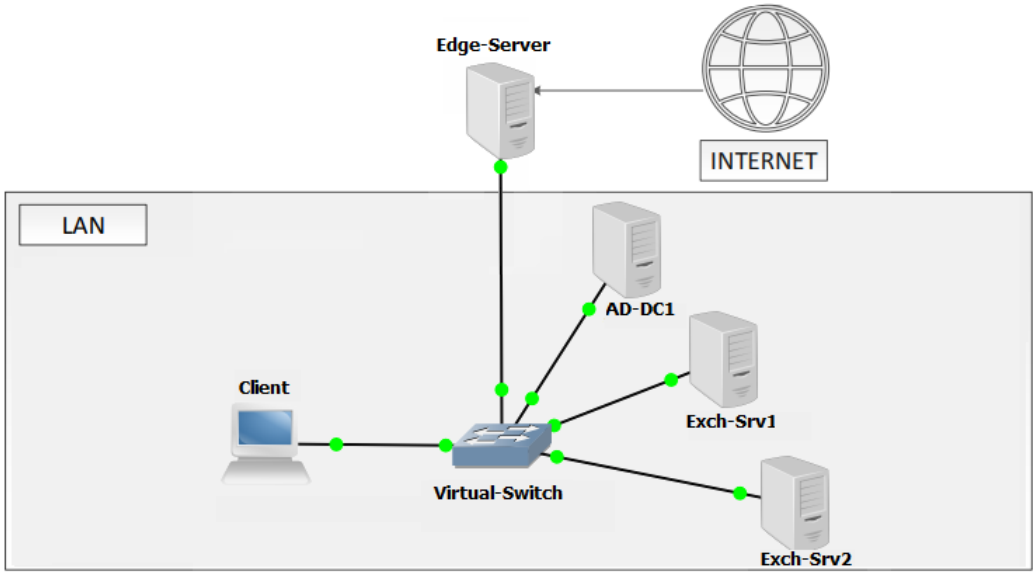

FIGURE 4.3.1 – Schéma du lab

Pour concevoir et déployer notre architecture, nous avons opté pour l'environnement de virtualisation VMware Workstation pour héberger nos machines clientes et nos serveurs, le lab est constitué des machines suivantes :

- **La machine AD-DC01 :** fait office d'un contrôleur de domaine Active Directory, d'un serveur AD RMS, d'une autorité de certification ainsi qu'un serveur DNS avec un nom de domaine Lab.local.
- **La machine Exch-Srv01 :** serveur Exchange 2013 disposant des rôles serveur d'accès client et boîtes aux lettres.
- **La machine Exch-Srv02 :** serveur Exchange 2013 disposant des rôles serveur d'accès client et boîtes aux lettres et mis en œuvre dans le cadre de la haute disponibilité.
- **La machine Edge-Server :** serveur Exchange 2013 disposant du rôle Edge mis en œuvre dans le cadre de la sécurité de la messagerie.
- **La machine Client :** utilisée pour tester le fonctionnement de la messagerie avec différents accès sur différentes plateformes.

Tableau des serveurs et plan d'adressage

Nom du server	Adresse IP	Disque	RAM	Système d'exploitation
AD-DC01	10.10.10.5/24	50GO	1GO	Windows 2012 Datacenter
Exch-Srv01	10.10.10.6/24	50GO	2GO	Windows 2012 Datacenter
Exch-Srv02	10.10.10.7/24	50GO	2GO	Windows 2012 Datacenter
Edge-Server	10.10.10.9/24	50GO	2GO	Windows 2012 Datacenter
Client	10.10.10.8/24	20GO	1GO	Windows 7

FIGURE 4.3.2 – Tableau des serveurs et plan d'adressage

4.4 Prérequis et Installation d'Exchange 2013

Pour l'installation d'Exchange server 2013 nous allons travailler en deux temps, l'installation et la préparation d'Active Directory en vue de la préparation de l'installation d'Exchange et ensuite l'installation de l'exchange lui-même mais avant tout voyons l'ensemble des prérequis matériels et logiciels nécessaire pour Exchange 2013.

4.4.1 Identification des prérequis nécessaires à l'installation d'Exchange 2013

Avant de procéder à l'installation d'Exchange 2013, nous devons nous assurer d'avoir rempli les conditions ci-après sur les serveurs Active Directory et Exchange.

4.4.1.1 La configuration matérielle requise

Exchange 2013 doit être déployé sur un serveur ayant au minimum la configuration matérielle suivante :

- **Processeur :** doit être basé sur l'architecture X64.
- **Mémoire :** La mémoire requise varie en fonction du rôle à installer et de la charge du serveur, néanmoins la quantité de RAM recommandée est de :
  - 8 Go de RAM pour le serveur de boîtes aux lettres.
  - 4 Go de RAM pour le serveur d'accès au client.
  - 8 Go de RAM pour le serveur de boîtes aux lettres et le serveur d'accès au client combinés.
- **Disque :** Au minimum 30 Go d'espace libre sur le disque sur lequel Exchange 2013 sera installé

4.4.1.2 La configuration logicielle requise

Exchange 2013 requière le respect de certains critères relatifs au système d'exploitation où Exchange Server sera déployé, au service d'annuaire Active Directory (AD DS) et nécessite l'installation de certains logiciels supplémentaires.

- **Prérequis du système d'exploitation :** Exchange 2013 peut être installé sur les systèmes d'exploitation Windows suivants : Windows Server 2008 R2, 2008 R2 SP1, 2012 et 2012R2.
- **Prérequis de l'annuaire Active Directory :** Exchange 2013 s'appuie grandement sur Active Directory d'où la nécessité d'avoir un environnement AD fonctionnel et répondant aux exigences d'exchange 2013. Les critères requis par exchange 2013 sur Active Directory sont :
  - Le maitre de schéma, le serveur de catalogue global et les contrôleurs de domaine du domaine où vous souhaitez déployer Exchange 2013 doivent être au minimum en Windows Server 2003 SP2.
  - Le niveau fonctionnel de la forêt AD doit être à Windows Server 2003 natif ou supérieur.
  - L'annuaire doit aussi être préparé pour Exchange 2013.
- **Les composants additionnels :** Exchange 2013 requière l'installation de trois logiciels supplémentaires :
  - Microsoft Unified Communications Managed API 4.0 (UCMA).
  - Microsoft Office 2010 Filter Pack 64 bit (facultatif).
  - Microsoft Office 2010 Filter Pack SP1 64 bit (facultatif).

Les filterpacks servent à afficher dans un navigateur web des documents de type office sans avoir à disposer d'un office localement sur la machine tandis que l'UCMA sert a à utiliser Microsoft Exchange pour faire de la téléphonie sur IP. [Microsoft 16], [Wesselius 14a] Il faut noter que seul le UCMA est nécessaire pour une installation du rôle CAS uniquement.

4.4.2 Installation et préparation d'Active Directory

4.4.2.1 Installation d'Active Directory

L'installation d'Active Directory commence par l'ajout du rôle ADDS y compris les outils d'administration graphiques et PowerShell permettant de gérer et déployer Active Directory.

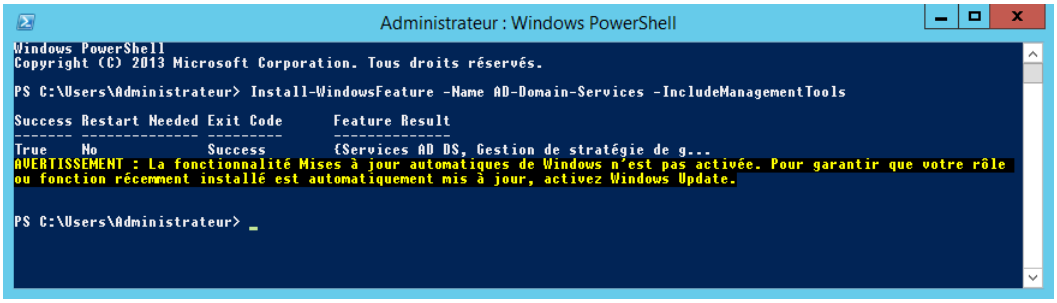

FIGURE 4.4.1 – Installation du rôle AD DS

Viens par la suite l'installation du nouveau domaine racine qui constitue l'unique domaine de la forêt Active Directory.

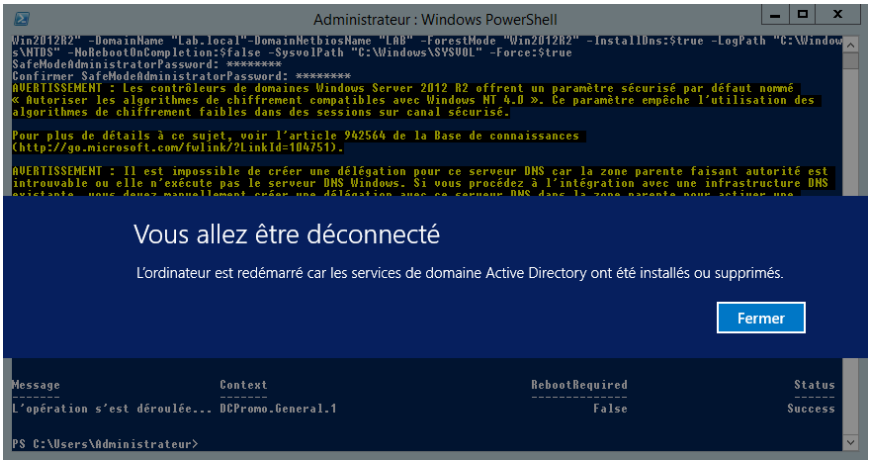

FIGURE 4.4.2 – Configuration d'Active Directory

4.4.2.2 Préparation d'Active Directory pour recevoir Exchange

La préparation de l'annuaire se déroule en trois 3 étapes et doit être réalisée avant le déploiement des premiers serveurs Exchange.

1. **Préparation du schéma Active directory :** cette phase permet d'étendre le schéma Active Directory pour y ajouter de nouveaux attributs et classes d'objets spécifiques à Exchange. La préparation du schéma se fait via la commande suivante : **Setup.exe /PrepareSchema /IAcceptExchangeServerLicenseTerms** [Wesselius 14a]
2. **Préparation d'Active Directory :** Au cours de cette étape, Exchange crée son organisation c'est à dire le conteneur stockant les paramètres d'Exchange dans la partition de configuration AD, puis prépare le domaine racine

en créant une unité d'organisation contenant les groupes universels de sécurité nécessaires à Exchange. La préparation d'AD se fait via la commande suivante : **Setup /PrepareAD /OrganizationName :MonLab /IAcceptExchangeServerLicenseTerms**

3. **Préparation des domaines Active Directory :** cette étape permet de préparer le domaine actuel en créant une unité d'organisation contenant le ou les groupes nécessaires au bon fonctionnement d'Exchange. Cette étape est inutile dans un environnement mono-domaine ou le /PrepareAD prépare déjà le domaine racine qui constitue l'unique domaine de la forêt, en revanche elle sert dans les environnements multi-domaine afin de préparer chacun des domaines enfants. La préparation des domaines se fait via la commande suivante : **Setup.exe /PrepareDomain /IAcceptExchangeServerLicenseTerms**

Il est possible de remplacer le /PrepareDomain par un PrepareAllDomains qui permet de préparer tous les domaines de la forêt en une seule opération. [Microsoft 16]

Comme l'infrastructure de notre lab est une infrastructure mono-domaine, nous allons lancer uniquement la commande /PrepareAD qui est un cumule d'un /PrepareSchema et d'un /PrepareDomain.

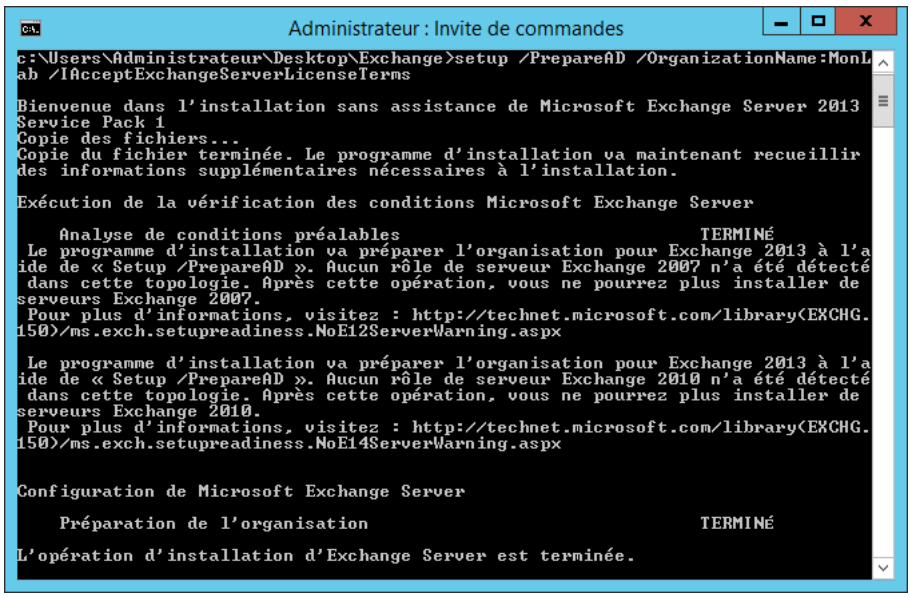

FIGURE 4.4.3 – Préparation d'Active Directory

Comment vérifier que cela a fonctionné ?

Lors de la préparation d'AD pour Exchange, plusieurs propriétés sont mises à jour et avant d'entamer l'installation d'Exchange, il est nécessaire de les vérifiées afin de s'assurer que tout a fonctionné comme prévu, pour ce faire nous allons vérifier trois propriétés :

1. La propriété rangeUpper sur l'objet ms-Exch-SchemaVerision-Pt qui est de 15292 pour la version d'exchange 2013 SP1 et qui définit la nouvelle version du schéma.
2. La propriété objectVersion dans le conteneur d'objets système Microsoft Exchange qui est de 13236.
3. La propriété objectVersion sur le conteneur de l'organisation Exchange qui est de 15844 pour exchange 2013.

La vérification est faite via ce script PowerShell :

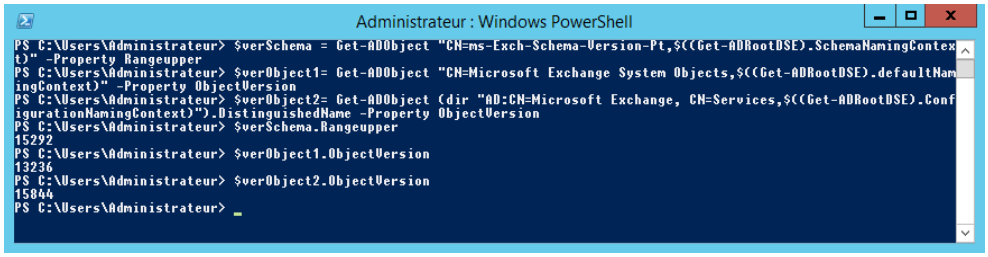

FIGURE 4.4.4 – Vérification de la préparation d'Active Directory

4.4.3 Installation d'Exchange 2013

Après avoir préparé l'environnement Active Directory, il ne reste plus qu'à installer les prérequis Exchange et enfin, déployer Exchange 2013. Mais avant il faut savoir qu'Exchange 2013 peut être déployé de 3 façons différentes :

- **Déploiement sur un serveur unique :** ou un seul serveur Exchange hébergera les deux rôles tel sera le cas dans le cadre de notre lab.
- **Déploiement sur plusieurs serveurs :** il est possible de segmenter les rôles CAS et MBX sur deux serveurs différents.
- **Déploiement hybride :** dont une partie se situe en local et une partie chez office 365 que Microsoft gère, il existe aussi des déploiements complètement office online ou il n'y a pas de serveur exchange en local tout est situé chez Microsoft.

4.4.3.1 Installation des prérequis

L'installation des prérequis consiste en l'installation des composants additionnels que nous avons identifié au préalable ainsi que des fonctionnalités du système

d'exploitation sur lequel le déploiement d'Exchange aura lieu, Exch-Srv01 dans notre cas, mais avons nous allons commencé par l'intégration de ce serveur dans Active Directory.

Intégration de la machine au domaine : l'ajout du serveur au domaine se fait de la manière suivante :

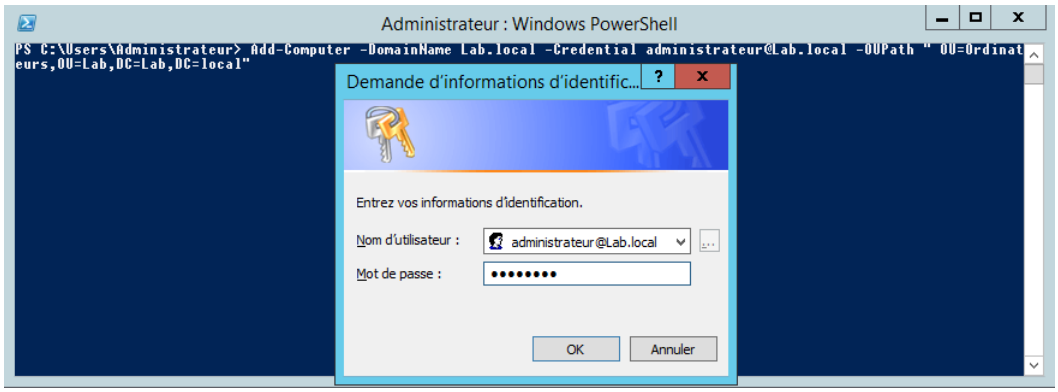

FIGURE 4.4.5 – La jonction au domaine Lab.Local

Suite au redémarrage du serveur, nous devons retrouver la machine dans AD au sein de l'Unité d'Organisation nommée "ordinateurs ".

Installation des fonctionnalités : L'installation des fonctionnalités requise pour une installation combinée des rôles Cas et Mbx se déroule ainsi :

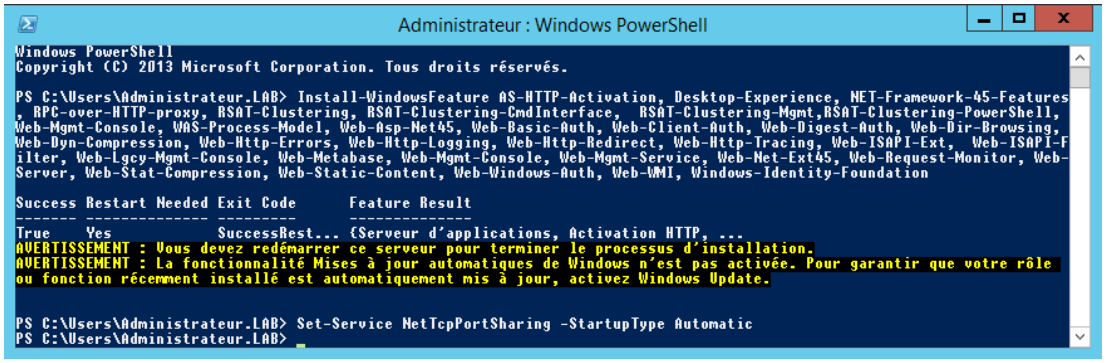

FIGURE 4.4.6 – Installation des fonctionnalités

Ensuite, il est nécessaire d'installer les composants additionnels à savoir UCMA et les filters packs.

4.4.3.2 Installation des rôles Exchange 2013

Après avoir remplis tous les prérequis d'Exchange, Il ne reste plus qu'à lancer l'installation d'Exchange a travers cette commande : **Setup.exe /mode :Install /role :ClientAccess, Mailbox /OrganizationName :MonLab /IAcceptExchangeServerLicenseTerms**

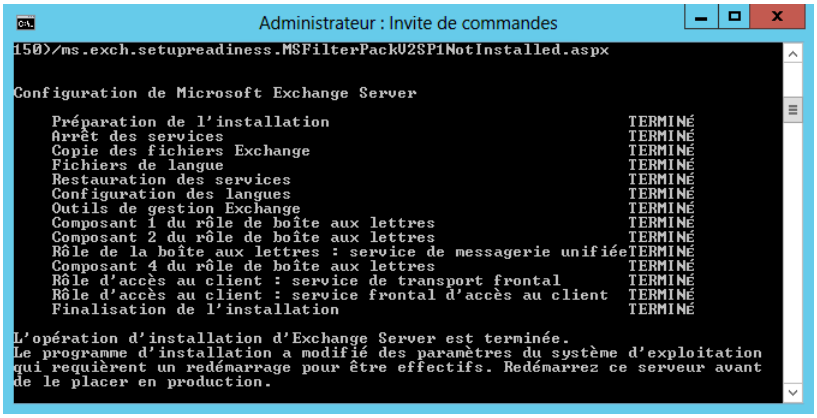

FIGURE 4.4.7 – Installation de Microsoft Exchange 2013

La durée d'exécution estimée est de 60 minutes et une fois terminée, un redémarrage est nécessaire.

Vérification de l'installation d'Exchange 2013

Une fois l'installation achevée, il est nécessaire de vérifier que tout s'est déroulée correctement grâce à la commande PowerShell **Get-ExchangeServer** qui permet de lister les serveurs Exchange installés.

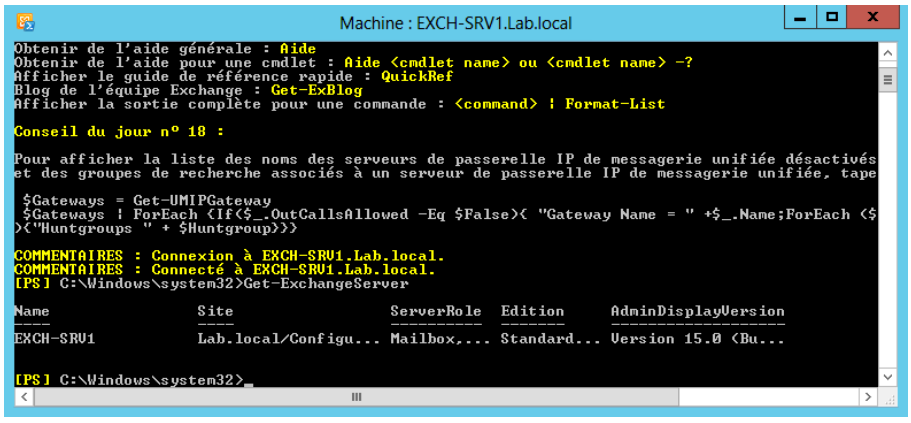

FIGURE 4.4.8 – Vérification de l'installation d'Exchange 2013

4.5 Configuration d'exchange 2013

Avant d'entamer la partie sécurité et haute disponibilité de la messagerie exchange, il est nécessaire dans un premier temps de configurer les différents composants d'exchange afin d'avoir un environnement de messagerie fonctionnel.

4.5.1 Configuration du rôle serveur de boîtes aux lettres

Le serveur de boîtes aux lettres joue un rôle crucial dans la mesure où il fournit la quasi-totalité des services d'une plateforme Exchange à savoir le stockage des boîtes aux lettres et des dossiers publics ainsi que les protocoles d'accès client pour le rendu des informations, les services de transport et la messagerie unifiée.[Pfeiffer 14b]

4.5.1.1 Administration des bases de données de boites aux lettres

L'implémentation des services de boîtes aux lettres passe par l'implémentation des bases de données Exchange. Une base de données Exchange est l'endroit où les boites aux lettres sont créées et stockées. Cette base est stockée sous forme de fichier .edb sur le disque dur local du serveur de boite aux lettres. [Microsoft 16]

Création d'une base de données de boite aux lettres :

Pour des besoins de test, nous allons créer et monter une base de données nommée Lab-BD.

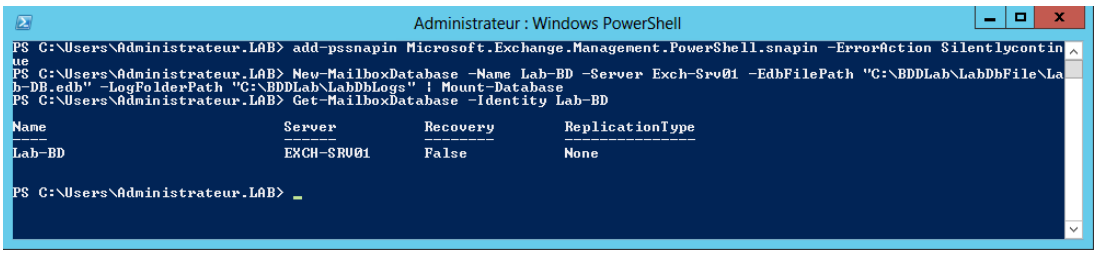

FIGURE 4.5.1 – Création d'une base de données de boites aux lettres

Paramétrage de la base de données :

Les paramètres des bases de données comprennent les éléments relatifs à la gestion des limites de la base ainsi que les quotas, la rétention de suppression et la journalisation circulaire. Les limites de la base permettent de limiter la quantité de stockage attribuée aux utilisateurs ainsi si un utilisateur dépasse la limite désignée il sera soumis à certaines restrictions. La rétention des éléments supprimés permet de conserver les éléments supprimés pendant une période donnée avant

la suppression définitive. La journalisation circulaire quant à elle permet de réduire considérablement l'espace de stockage occupé par les fichiers journaux en s'écrasant les uns par-dessus des autres.[Stanek 13a]

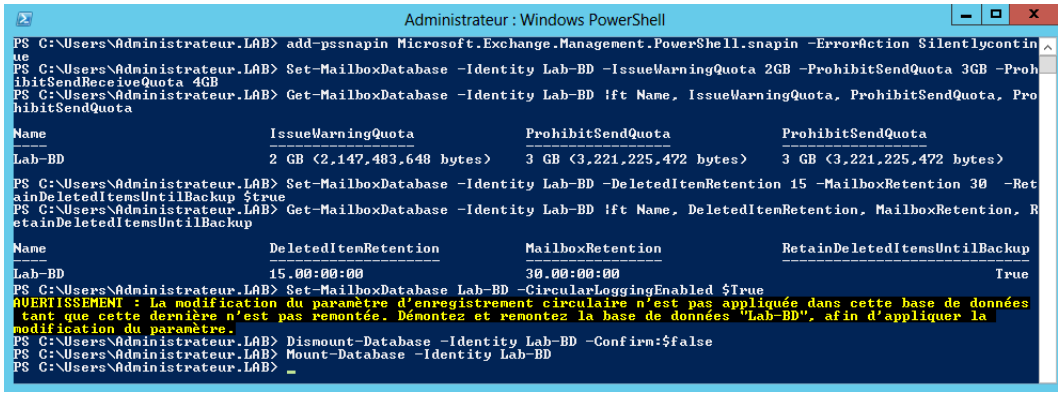

FIGURE 4.5.2 – Paramétrage de la base de données de boites aux lettres

4.5.1.2 Gestion des objets destinataires et des listes d'adresses

La notion d'objet destinataire fait référence à tout objet a extension de messagerie dans Active Directory utilisé pour émettre ou recevoir des courriers électroniques au sein d'une organisation Exchange. Il existe différents types d'objets destinataires sous Exchange 2013 dont : les boites aux lettres, les utilisateurs de messagerie, les contacts, les groupes de distribution et les dossiers publiques.

Présentation et Gestion des boites aux lettres :

Les boîtes aux lettres constituent le type de destinataire le plus couramment utilisé par les utilisateurs et administrateurs d'Exchange qui se servent principalement pour l'envoie, la réception et le stockage des e-mails, des tâches, des documents, etc. Chaque boîte aux lettres est associée à un compte utilisateur Active Directory. Il existe plusieurs types de boîtes aux lettres disponibles dans Exchange 2013 dont :

- **Les Boîte aux lettres d'utilisateur :** utilisées par des utilisateurs individuels pour l'envoie et la réception des e-mails, des tâches, des documents, etc. [Wesselius 14a]
- **Boîte aux lettres de ressources :** sont utilisées pour représenter des ressources matérielles et planifier leur utilisation dans l'entreprise .
- **Boîte aux lettres partagées :** boite aux lettres commune dont plusieurs personnes peuvent y accéder.

La gestion des boites aux lettres utilisateur consiste à effectuer les actions de création, déplacement, Activation, suppression, etc.

Création des boites aux lettres utilisateur

Les boites aux lettres dans exchange 2013 peuvent être associer à des utilisateurs existants dans Active directory tout comme elles peuvent être créer sur de nouveaux comptes AD. Pour les boites aux lettre que nous utiliserons dans le Lab nous allons activer la messagerie pour l'ensemble des comptes utilisateurs dans Active Directory.

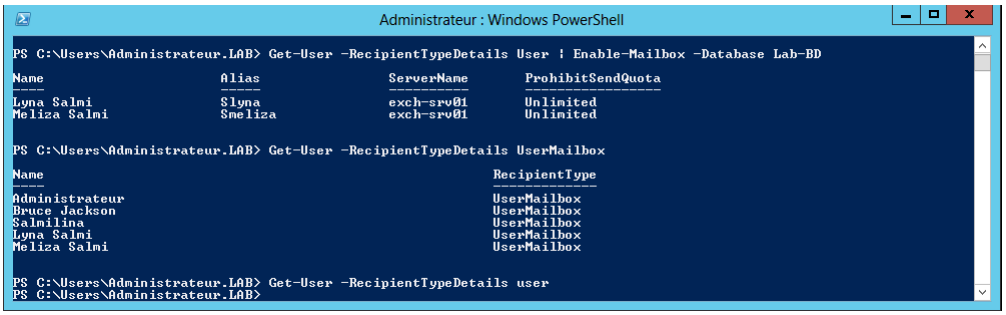

FIGURE 4.5.3 – Création des boites aux lettres

Présentation et Gestion des utilisateurs et contacts de messagerie :

Un utilisateur de messagerie représente un compte utilisateur de l'annuaire Active Directory n'ayant pas de boîte aux lettres hébergée par l'organisation Exchange. Un contact de messagerie quant à lui représente un destinataire fréquent de messagerie pour les utilisateurs de l'organisation Exchange, mais une entité ne possédant ni de compte dans l'annuaire, ni boîte aux lettres sur les serveurs Exchange.

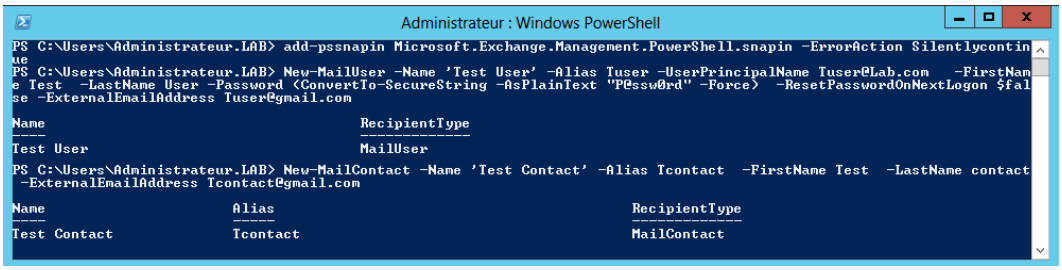

FIGURE 4.5.4 – Gestion des contacts et utilisateurs de messagerie

Quelle est la différence entre un utilisateur de messagerie et un contact ?
C'est justement la possession du compte au sein de l'annuaire AD, les utilisateurs

de messagerie ont besoin d'accéder au réseau de l'entreprise tout en continuant à recevoir les mails via leur adresses emails existantes. Les contacts quant à eux remplissent un besoin spécifique : la nécessité de faire apparaître les contacts externes afin d'éviter à ce que les utilisateurs de l'entreprise saisissent ou importent les mêmes destinataires dans leurs dossiers de contacts personnels.

Gestion des groupes de distribution

Un groupe de distribution est une collection d'objets destinataires définie par un administrateur qui permet de distribuer un message à l'ensemble des membres à travers l'adresse de messagerie du groupe. Il y a cependant un autre type de groupe de distribution, qui est le groupe de distribution dynamique et auquel la liste des membres est calculée à chaque fois qu'un message est destiné au groupe, en fonction des filtres et conditions spécifiés.[Carraz 14]

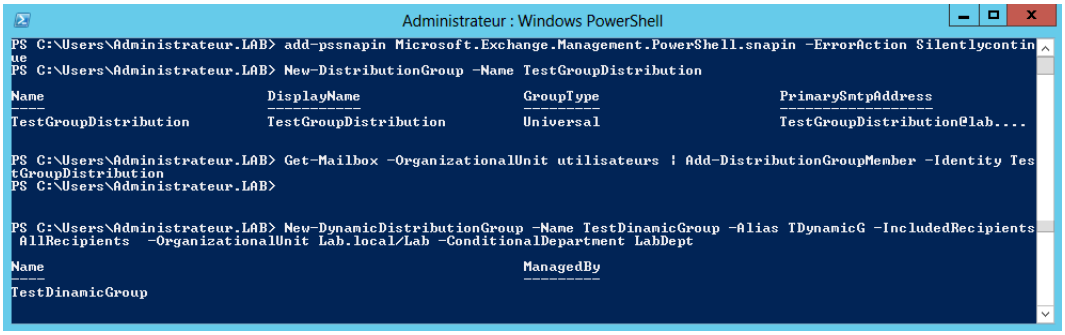

FIGURE 4.5.5 – Gestion des groupes de distribution

Il existe de ce fait un troisième type de groupe qui est le groupe de sécurité utilisé pour distribuer des messages et accorder des autorisations d'accès aux ressources dans Exchange et Active Directory. [Microsoft 16]

Présentation et gestion des listes d'adresses

Les listes d'adresses sont des objets Exchange qui permettent de regrouper et de trier des objets destinataires selon des critères définis par l'administrateur de manière à faciliter leurs recherche par un utilisateur. [Carraz 14] Exchange 2013 permet de gérer différentes listes d'adresses :

— **Liste d'adresses globale (GAL) :** Inclut tous les objets à extension de messagerie dans la forêt AD. La Gal est mise à jour régulièrement pour lui ajouter ou retirer les objets destinataires nouvellement créés ou supprimés.

— **Listes d'adresses :** sont des sous-ensembles de destinataires qui sont regroupés en une seule liste, ce qui les rend plus faciles à trouver par les utilisateurs. [Microsoft 16]
— **Le carnet d'adresses en mode hors connexion (OAB) :** est une copie d'un ensemble de listes d'adresses qui a été téléchargé de façon à ce qu'un utilisateur puisse accéder aux informations qu'il contient tout en étant déconnecté du serveur Exchange. [Pfeiffer 14b]

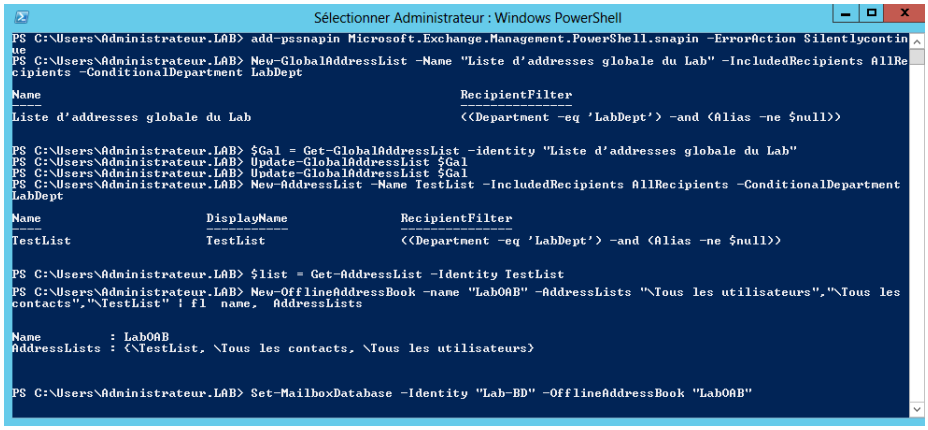

FIGURE 4.5.6 – Gestion des listes d'adresses

Une fois l'ensemble des listes d'adresses sont créés et configurées, il est nécessaire à présent de mettre en place une stratégie de carnet d'adresses qui permet de fournir une vue personnalisée du carnet d'adresse qui est ni plus ni moins qu'un ensemble de listes d'adresses. Une fois la stratégie créé nous allons l'associer à l'ensemble des boites aux lettres dans exchange 2013.

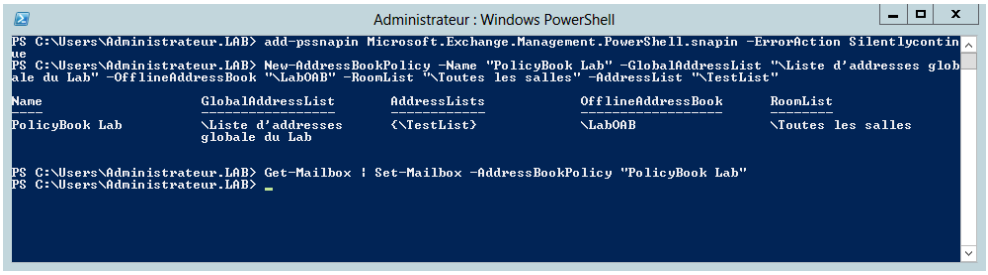

FIGURE 4.5.7 – Une stratégie de carnet d'adresses

4.5.2 Configuration du rôle serveur d'accès client

4.5.2.1 Introduction au serveur d'accès client

Il est vrai que le serveur de boite aux lettre offre la quasi-totalités des services Exchange, néanmoins le serveur d'accès client reste plus important dans la mesure où il représente le serveur auquel les clients se connectent. Lorsqu'un utilisateur tente de se connecter à l'environnement Exchange, il passe obligatoirement par le serveur d'accès client qui lui l'authentifie, localise le serveur de boite aux lettres hébergeant sa boite aux lettres et redirige la demande vers le serveur en question. Le serveur d'accès client offre un ensemble de services dont :

La découverte automatique de votre profil Outlook (Autodiscover) : est le service permettant aux clients Outlook d'être configurés automatiquement en utilisant un nombre de paramètres réduit qui se résume à l'adresse de messagerie et au mot de passe. L'opération se déroule en quatre étapes :

1. Le client envoie une requête au contrôleur de domaine pour localiser le serveur d'accès client.
2. Le Service d'annuaire renvoie l'URL du serveur CAS au client.
3. Apres obtention de l'URL, le client se connecte au serveur CAS.
4. Le serveur CAS récupère la configuration de la boite aux lettres auprès d'Active Directory et génère un fichier XML qu'il remet au client. Le client a son tour applique les paramètres contenus dans le fichier XML. [Pfeiffer 14b][Pfeiffer 14a]

La fonction Outlook Anywhere : Outlook Anywhere est la méthode de connexion adaptée par Exchange 2013. Au travers d'Outlook Anywhere, nous allons pouvoir accéder à la boîte aux lettres et a l'intégralité des fonctionnalités de messagerie depuis un client Outlook où qu'il soit.[Pfeiffer 14a]

4.5.2.2 Configuration du serveur d'accès client

Un déploiement réussi d'Exchange dépend fortement du déploiement d'espaces de noms pour la connectivité client, sans cela les problèmes de connectivité Lors de cette étape de configuration nous allons configurer deux éléments importants à savoir : les répertoires virtuels et Outlook Anywhere.

Configuration des répertoires virtuels

Lors de L'installation du rôle serveur d'accès client, les Url internes utilisées par les client internes de l'organisation afin de se connecter à l'environnement Exchange sont configurées de sorte à utiliser le nom de domaine complet du serveur, les URL externes quant à elles ne sont pas configurer et sont laissées nulles. La première étape de la configuration du serveur CAS consiste à configurer les Url externe sur les différentes répertoires virtuels (OWA, ECP, EWS, EAS, OAB...) de manière à rendre disponible l'accès client en externe via ces Url.

Pour ce qui est de notre Lab nous allons utiliser l'url mail.Lab.com comme url externe et interne, pour ce faire nous allons en premier lieu configurer le DNS.

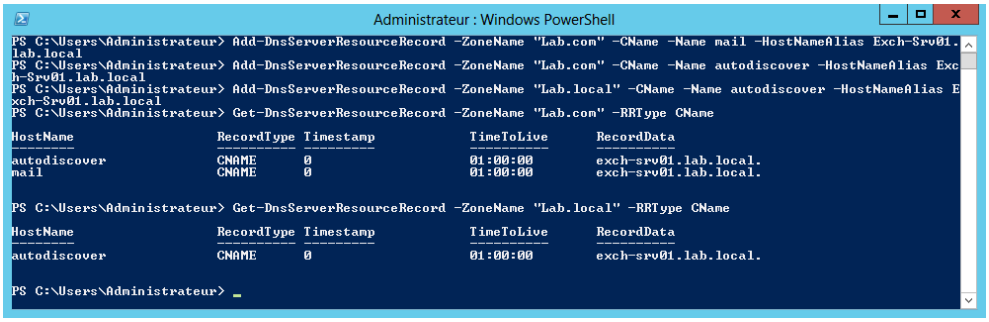

FIGURE 4.5.8 – Configuration des entrées DNS

Viens par la suite la configuration les répertoires virtuels et Outlook Anywhere.

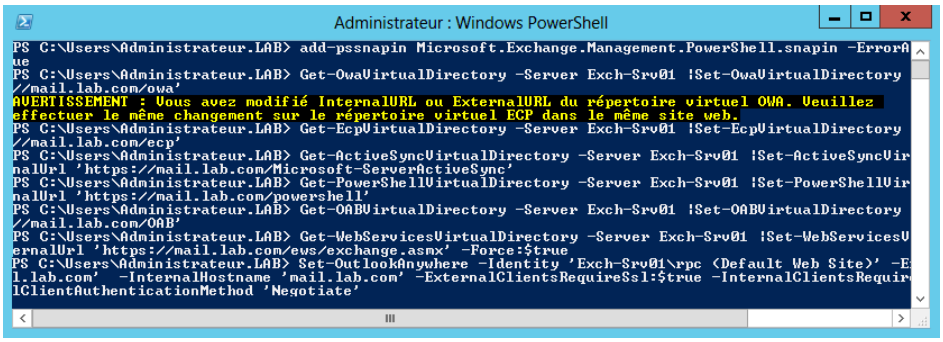

FIGURE 4.5.9 – Configuration des répertoires virtuels et d'Outlook Anywhere

4.5.3 Implémentation et configuration du transport

Le système de transport d'emails dans exchange 2013 qui était un rôle à part dans les versions antérieures se repartis sur les rôles d'accès au client et de boîte aux lettres. Comprendre comment concevoir, gérer et configurer le transport est une condition essentielle pour la gestion d'Exchange.

4.5.3.1 Architecture du transport au sein d'Exchange 2013

Le service de transport se compose de deux parties distinctes :

1. **Le service de transport frontal :** situé sur le serveur ayant le rôle Cas, permet de gérer l'ensemble du trafic Smtp externe a l'entreprise.

2. **Le service de transport Hub :** situé sur le serveur exécutant le rôle de boite aux lettres et est constitué de deux composants :
   a) **Le service de transport :** permet de gère tous les flux de messagerie Smtp de l'organisation. Lorsqu'un message est reçu, il est transmis au catégoriseur qui inspecte son contenu et détermine s'il doit être remis localement ou à distance, puis une fois classé il est transféré vers la file d'attente de remise en attendant son envoi.
   b) **Le rôle de service transport de boite aux lettres :** Ce service se compose de deux services distincts :
      i. **Le service de remise du transport de boîtes aux lettres :** reçoit les messages Smtp à partir du service de Transport sur le serveur de boîtes aux lettres local ou sur d'autres serveurs de boîtes aux lettres et établie une connexion avec la base de données pour la remise du mail.
      ii. **Le service de dépôt du transport de boîte aux lettres :** récupère le message depuis la base de données et l'envoie, via Smtp, au service de transport sur le serveur de boîtes aux lettres local ou sur d'autres serveurs de boîtes aux lettres.

Le schéma ci-dessus identifie les différents composants du système de transport ainsi que l'acheminement des emails entre les différents composants.

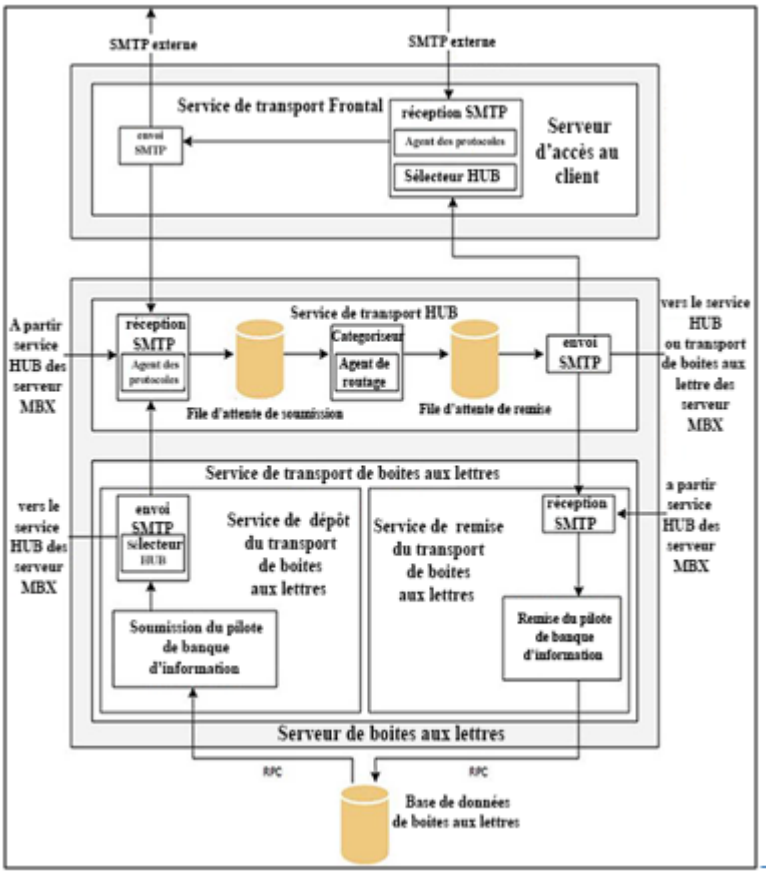

FIGURE 4.5.10 – Architecture du service de transport d'exchange 2013

4.5.3.2 Acheminement d'un flux de messagerie Exchange 2013

Dans tout système de messagerie les courriels peuvent parvenir d'un expéditeur interne ou externe via internet. Avec Exchange 2013 la façon dont le flux est géré dépend grandement de sa source dont deux cas se présente :

— **Messages provenant d'expéditeurs externes :** Les messages ne provenant pas de l'organisation accèdent serveur Exchange via un connecteur de réception du service de transport frontal du serveur d'accès au client et sont acheminés vers le service de transport d'un serveur de boîtes aux lettres.

— **Messages provenant d'expéditeurs internes :** Les messages SMTP provenant de l'intérieur de l'organisation accèdent au serveur Exchange via le service de transport d'un serveur de boîtes aux lettres soit via un connecteur de réception ou via le service de transport de boîtes aux lettres.

4.5.3.3 Les connecteurs d'envoi et de réception Exchange 2013

Avec Exchange Le transfert d'email au sein de l'organisation ou en dehors repose sur l'utilisation des connecteurs. Les connecteurs sont les éléments les plus importants sur le service de transport parce que c'est bien à travers eux que l'on va pouvoir envoyer ou recevoir des emails. Ce sont en effet des objets logiques stockés dans Active Directory créés pour que les messages prennent un certain chemin. Exchange 2013 comporte deux types principaux de connecteurs : les connecteurs d'envoi et les connecteurs de réception.

— **Les connecteurs de réception :** sont responsables de l'acceptation des messages Smtp provenant d'autres serveurs de messagerie internes ou externes. Par défaut Exchange 2013 crées un ensemble de connecteurs pour la réception des messages en interne tout comme à l'extérieur de l'entreprise, il n'y a donc rien à configurer pour la réception des emails.

— **Les connecteurs d'envoi :** sont responsables de la transmission des messages Smtp sortant. Par défaut Exchange 2013 ne crée aucun connecteur d'envoi, Il est donc requis d'en créer un avant qu'une organisation Exchange 2013 puisse envoyer des messages en dehors de l'organisation.

Création d'un connecteur d'envoi

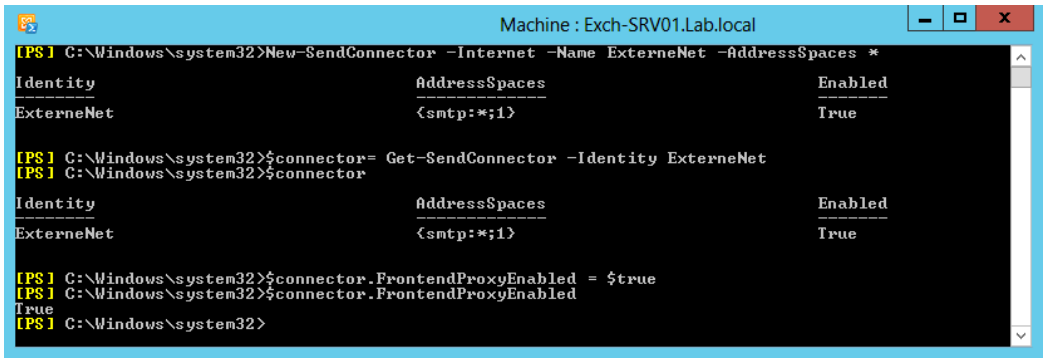

FIGURE 4.5.11 – Création et configuration d'un connecteur d'envoi

4.6 Implémentation de la sécurité de la messagerie

4.6.1 Présentation de la solution de sécurité à déployer

4.6.1.1 La sécurité des données et de la communication au sein d'Exchange 2013

Pour minimiser les accès non autorisés sur les courriers électroniques et afin d'assurer un haut niveau de sécurité sur les données circulant dans la messagerie électronique, nous proposons de combiner quatre technologies de sécurité que nous avons aborder dans le chapitre 3 : S/MIME, SSL/TLS, IRM et Kerberos. Le tableau ci-dessus illustre les services de sécurité assurés par chacune des technologies.

Technologie	Contrôle d'accès	Confidentialité	Non répudiation	Intégrité	Authentification
SSL/TLS	×	√	×	√	√
S/MIME	×	√	√	√	×
IRM	√	√	×	×	×
Kerberos	√	×	×	×	√

FIGURE 4.6.1 – Les services de sécurité assurés par S/MIME, IRM, SSL et kerberos

Combiner toutes ces technologies sur un émail offrent un haut niveau de sécurité. Malheureusement dans Exchange server il n'est pas possible de combiner la solution S/MIME avec l'IRM, La protection IRM ne peut pas être appliquée à un message déjà signé ou crypté à l'aide de S/MIME, Il en va de même pour les messages protégés par IRM. Bien qu'ils représentent deux normes qui se complètent au lieu de se faire directement concurrence. Il est cependant dommage de préférer une technologie sur l'autre tandis que S/MIME et AD RMS peuvent être très utiles dans les bons contextes.

Quand utiliser AD RMS ou S/MIME ?

Il est recommandé d'utiliser IRM lorsque l'on souhaite appliquer des restrictions d'utilisation ainsi qu'un cryptage. En revanche, il est recommandé d'utiliser S/MIME lorsque la communication requiert un véritable cryptage de bout en bout, autrement dit lorsque l'on souhaite un haut niveau de confidentialité et d'intégrité des données.

Dans le cadre de notre environnement de test, nous allons combiner les trois technologies ensemble, le choix entre l'application du S/MIME ou d'AD RMS dépend de la situation et de l'importance de la donnée. Néanmoins nous appliquerons

la protection IRM sur l'ensemble des courriers par défaut avec possibilité de suppression de la protection pour une application de S/MIME selon le cas et le besoin d'utilisation.

Le schéma général de la solution de protection des données que nous déploierons sur Exchange 2013 est illustré dans la figure suivante :

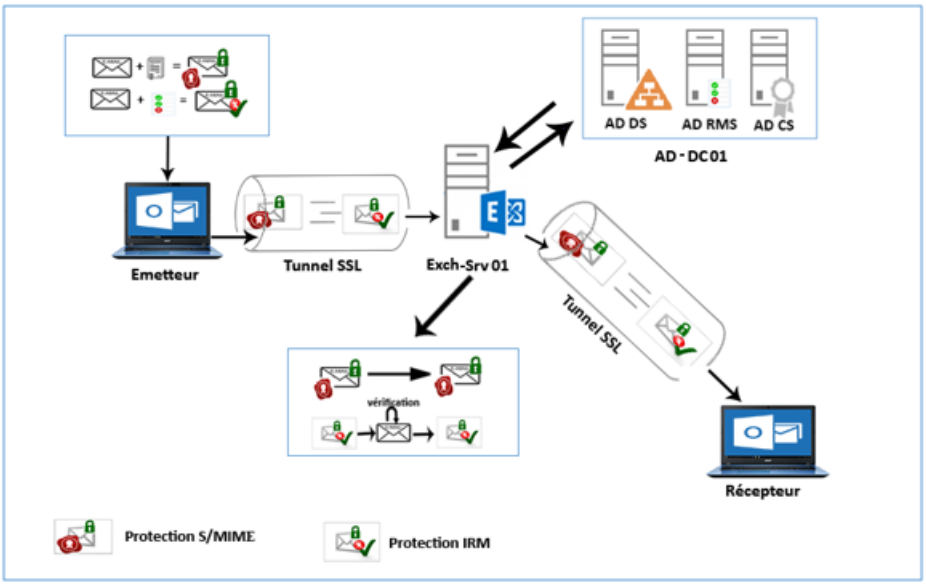

FIGURE 4.6.2 – Le schéma général de la solution de protection des données

4.6.1.2 La protection contre les courriers non sollicités et les programmes malveillants

Les expéditeurs du courrier indésirable et des malwares utilisent une variété de technique et d'outils pour exécuter leurs actions malveillantes dans l'organisation Exchange. Il n'est certainement pas possible d'éliminer la totalité du courrier indésirable et des malwares mais de réduire leurs risques via des techniques de protection basé sur des filtres.

Quand un e-mail est reçu par le service de transport Hub du serveur de boite aux lettres ou via le serveur Edge, il est soumis à de multiples couches de filtrage et de défense de la manière suivante :

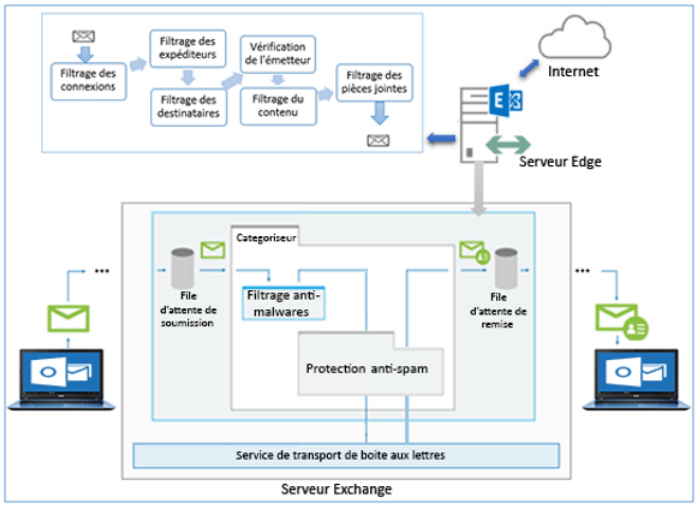

FIGURE 4.6.3 – Protection contre les courriers non sollicités et les programmes malveillants

Pour ce qui est de notre Lab, nous déploierons la solution de protection anti-spam et anti-malware sur le service de transport Hub du serveur de boites aux lettres pour le filtrage des mails internes à l'entreprise ainsi que sur le serveur Edge pour les mails externes.

4.6.1.3 La protection contre les pertes de données

La prévention contre les pertes de données est une fonctionnalité conçu pour empêcher l'envoi des messages contenant des informations confidentielles, elle examine le contenu des messages pour rechercher des séquences de données qui pourraient être considéré comme données sensibles.[Wesselius 14b]

Ce type de solution permet de contrôler ce qui peut transiter dans les emails de ce qu'il ne doit pas transiter, il est donc important lors de la conception d'une solution DLP pour une entreprise d'identifier soigneusement les données ne devions pas transiter par mail.

4.6.2 Mise en place d'une infrastructure à clés publique (PKI)

Pour rappel, une PKI (Public Key Infrastructure) est une infrastructure réseau qui a pour but de sécuriser les échanges réseau en utilisant des certificats numériques. Une entreprise peut mettre en œuvre sa propre PKI, tout comme elle peut utiliser des services de certificats tiers tel que OpenCA, VeriSign, Digicert, etc.

Dans le cadre de la messagerie Exchange, les services des autorités de certification sont principalement utilisés dans le cadre de :

— La sécurisation des communications, autrement dit la sécurité de la transmission de données d'un expéditeur à un destinataire via le protocole Transport Layer Security (TLS) utilisé par exemple pour sécuriser les communications web (HTTPS) ou email (SMTP, POP3, IMAP... sur TLS).[Adams 02]
— La sécurisation du contenu des courriers électroniques via le protocole S/MIME ou PGP.

Pour ce qui est de notre Lab, la mise en œuvre de cette PKI consiste à mettre en place une autorité de certification d'entreprise pour le domaine Lab.local sur notre contrôleur de domaine AD-DC01.

4.6.2.1 Mise en place d'une autorité de certification d'entreprise

La mise en place d'une autorité de certification (CA) s'effectue par l'intermédiaire du rôle ADCS (Active Directory Certificate Services) qui permet de créer une hiérarchie de PKI complète pour émettre et gérer des certificats dans l'organisation. La mise en place de la CA commence donc par l'ajout du rôle ADCS, viens par la suite la création et la configuration de l'autorité de certification Lab-CA.

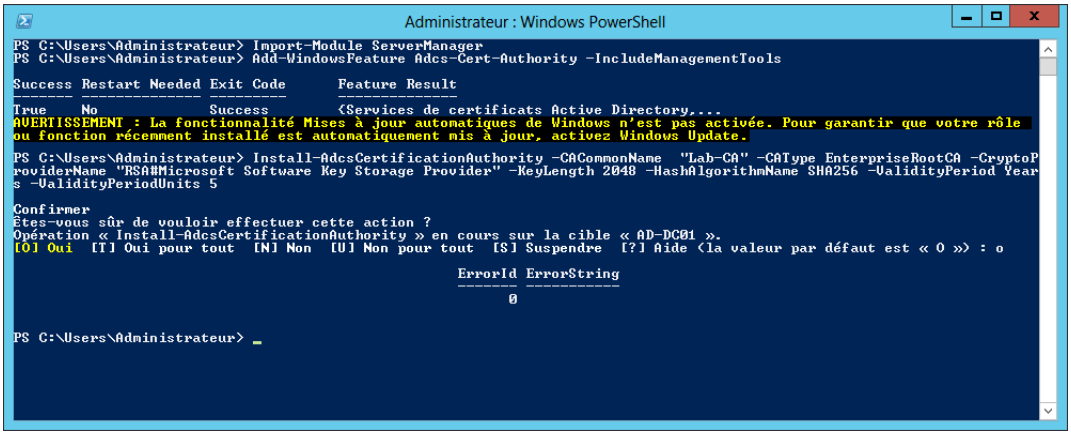

FIGURE 4.6.4 – Mise en place d'une autorité de certification d'entreprise

Notre PKI étant mise en place, nous pouvant l'utiliser afin de sécuriser l'infrastructure Exchange.

4.6.3 Sécuriser la communication à l'aide du protocole SSL

Afin de sécuriser la communication entre le serveur et les clients dans exchange, nous allons s'en servir des certificats afin de créer un canal SSL chiffré utilisé pour protéger les communications entre les clients et notre serveur Exchange.

4.6.3.1 Création et configuration d'un certificat SSL

Lors de l'installation d'Exchange 2013, des certificats auto-signés sont automatiquement générés et installés pour chiffrer les données transmises entre les serveurs, néanmoins les certificats auto-signés ne sont pas des certificats de confiance et les utilisateurs recevront des avertissements de certificat les informant que les certificats ne sont pas émis à partir d'une source approuvée ce qui peut créer une certaine confusion pour les utilisateurs finaux. Il est donc recommandé de remplacer ces certificats par de nouveaux certificats émis par une autorité de certification approuvée.

Pour la création d'un nouveau certificat, il est nécessaire dans un premier lieu de générer une demande de certificat.

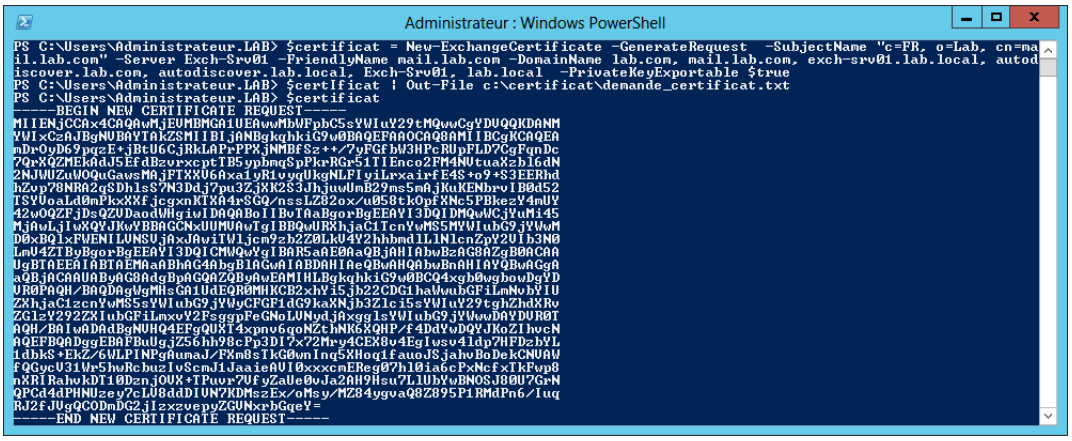

FIGURE 4.6.5 – Création et configuration d'un certificat SSL

Viens par la suite la soumission de notre demande auprès de notre autorité de certification, pour ce faire nous allons accéder à l'autorité de certification via l'url `http://AD-DC01/certsrv`, lui soumettre la demande de certificat et télécharger le certificat une fois qu'il est prêt.

Une fois le certificat est près, la prochaine étape consiste à installer ce certificat sur le serveur d'accès client.

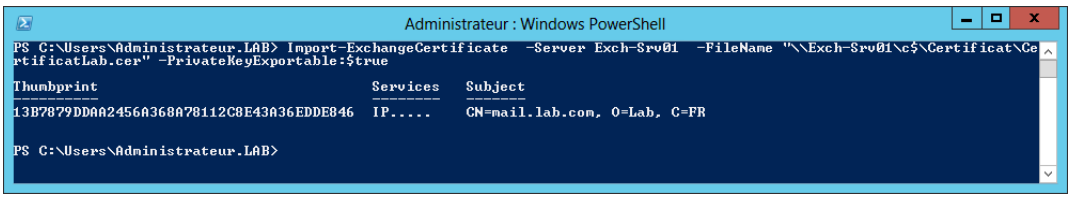

FIGURE 4.6.6 – Installer un certificat SSL sur le serveur d'accès client

Une fois notre certificat généré, la dernière étape consiste à l'affecter au services POP, IMAP, SMTP et IIS pour une communication sécurisée entre les clients et notre serveur Exchange.

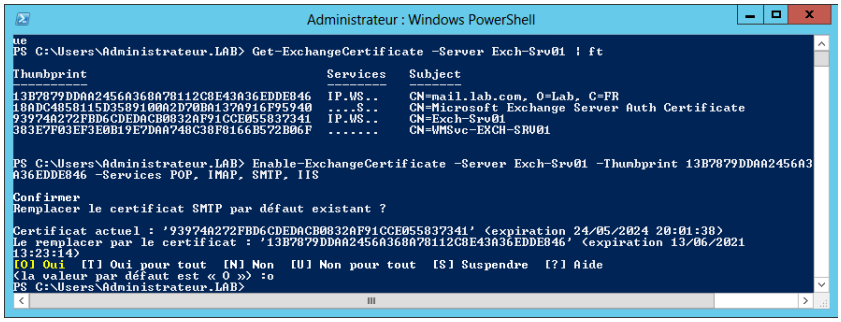

FIGURE 4.6.7 – Sécurisation des protocoles de transport

A ce niveau le protocole TLS est bien configuré et les communications sécurisées peuvent être établie avec notre serveur Exchange, mais que ce passe-t-il si le serveur de destination ne prend pas en charge le protocole TLS ?

Il est important de mentionner que lorsque le serveur Exchange est configuré avec TLS, il est configuré par défaut avec l'option TLS opportuniste, c'est-à-dire qu'il essaie toujours d'établir une liaison de communication sécurisée, mais dans le cas où l'autre partie ne prend pas en charge TLS, le serveur Exchange "acceptera" d'utiliser un canal de communication non chiffré à l'aide du protocole SMTP ce qui mettra les données en danger.

Afin de remédier à ce problème nous allons configurer l'option Force TLS sur les connecteurs d'envoi et de réception ainsi Si le serveur de messagerie de destination ne prend pas en charge TLS, la communication par courrier électronique ne se poursuivra pas et le message ne sera pas remis.

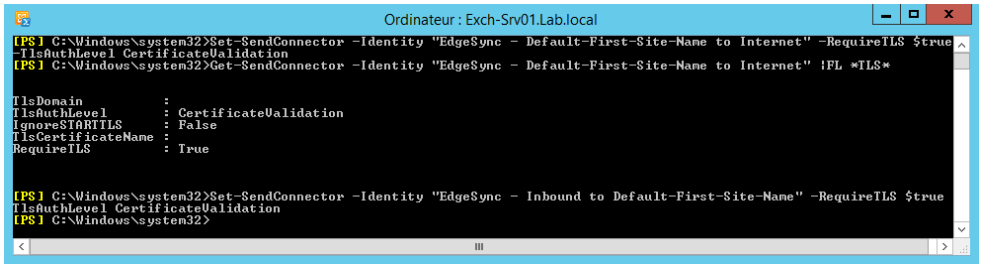

FIGURE 4.6.8 – Configuration du force TLS

4.6.3.2 Analyse du traffic TLS avec Wireshark

Afin de vérifier la bonne mise en place du protocole TLS, nous avons utilisé l'analyseur de réseau Wireshark pour capturer le trafic entre le client outlook et le serveur Exchange.

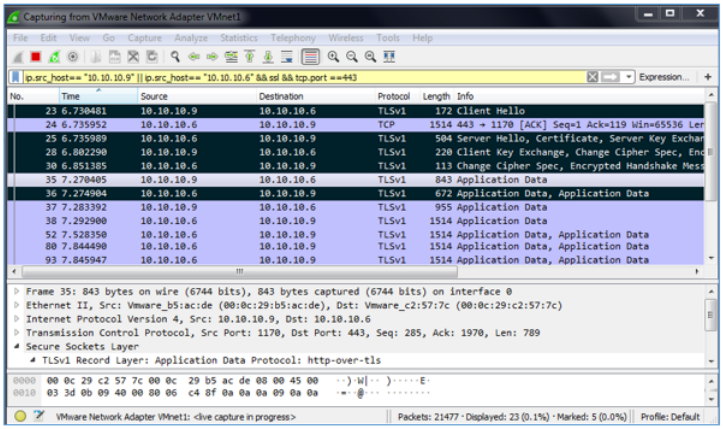

FIGURE 4.6.9 – Analyse du traffic TLS avec Wireshark

4.6.4 Sécuriser les e-mails à l'aide du protocole S/MIME

Pour rappel S/MIME est un protocole pour l'envoi de messages chiffrés et signés numériquement, et afin de permettre aux client d'utiliser S/MIME, les utilisateurs doivent disposer des certificats délivrés à des fins de signature et de chiffrement et doivent configurer leurs clients de messagerie pour qu'ils prennent en charge ce certificat. Ce processus doit être effectuer périodiquement sur chaque système et selon le niveau de connaissance, les utilisateurs peuvent avoir des difficultés. Pour leurs simplifier la tâche, nous allons automatiser ce processus en utilisant l'inscription automatique et les GPO (Group Policy Object).

4.6.4.1 Configuration des certificats d'utilisateur Exchange

Pour délivrer des certificats aux utilisateurs, la meilleure pratique consiste à configurer le serveur de certificats pour émettre automatiquement des certificats aux utilisateurs dans Active Directory, Ceci est connu sous le nom d'inscription automatique des certificats.

L'inscription automatique s'effectue en trois étapes :

— Création d'un modèle de certificat pour la signature et le chiffrement.
— Ajouter le modèle à l'autorité de certification.

— Créer une stratégie de groupe pour déployer automatiquement les certificats aux utilisateurs.

Création d'un modèle de certificat :

Un modèle de certificat est une liste pré-configurée de paramètres qui permet aux utilisateurs et aux ordinateurs d'obtenir des certificats sans avoir à créer des demandes de certificat complexes. [Microsoft 18]

Pour configurer un modèle de certificat à déployer sur les utilisateurs, nous allons dupliquer le modèle de certificat **Utilisateur Exchange** présent dans le conteneur modèle de certificat, le modifier et lui définir les paramètres nécessaires (périodes de validité, de renouvèlement, objectifs du certificat, etc.).

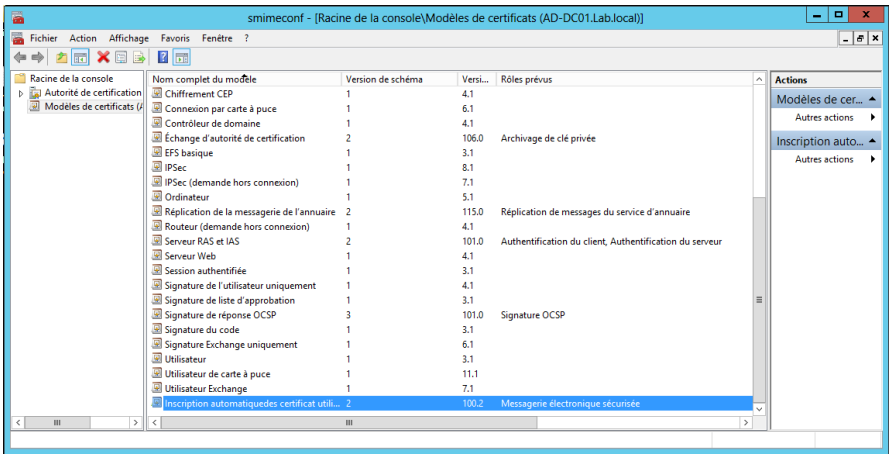

FIGURE 4.6.10 – Modèle de certificat utilisateur

Ajouter le modèle au serveur de l'autorité de certification :

Après avoir créé le modèle, la prochaine étape consiste à l'ajouter au serveur de l'autorité de certification à l'aide de la commande Add-CATemplate.

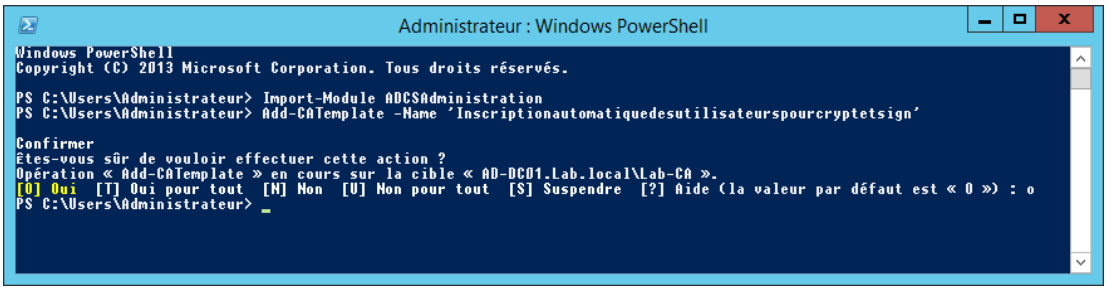

FIGURE 4.6.11 – Ajout du modèle dans la CA

Déploiement des certificats :

Le déploiement des certificats sera fait par GPO, nous allons donc créer un nouvel GPO, le lier au domaine, l'éditer pour le déploiement automatique des certificats.

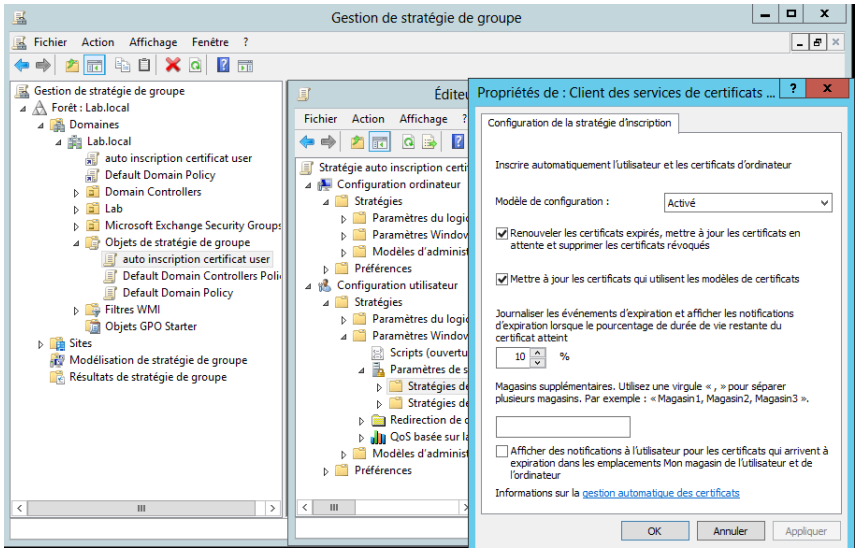

FIGURE 4.6.12 – Déploiement des certificats

Comment vérifier que cela à fonctionner ?

Pour vérifier le fonctionnement du déploiement des certificats, il suffit de charger la console MMC Certificates sur le compte d'un utilisateur du domaine et contrôler la présence du certificat dans le dossier personnel.

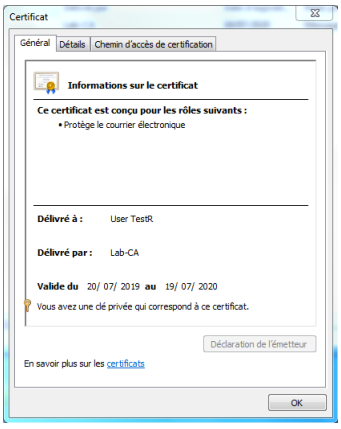

FIGURE 4.6.13 – Le certificat utilisateur

Une fois que l'inscription automatique a délivré un certificat à l'utilisateur et que celui-ci a confirmé sa réception, Microsoft Outlook détecte automatiquement le certificat d'inscription automatique correct et configure Outlook pour qu'il utilise ce certificat pour la signature et le cryptage des courriers électroniques, pour le client OWA une étape de configuration sur le serveur Exchange est nécessaire.

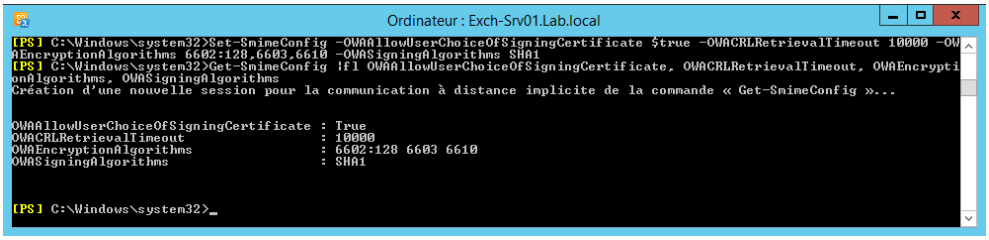

FIGURE 4.6.14 – Configuration de S/MIME pour OWA

4.6.4.2 Tester le protocole S/MIME

Afin de tester le protocole S/MIME, nous avons envoyer un mail d'Alice vers Bob de la manière suivante.

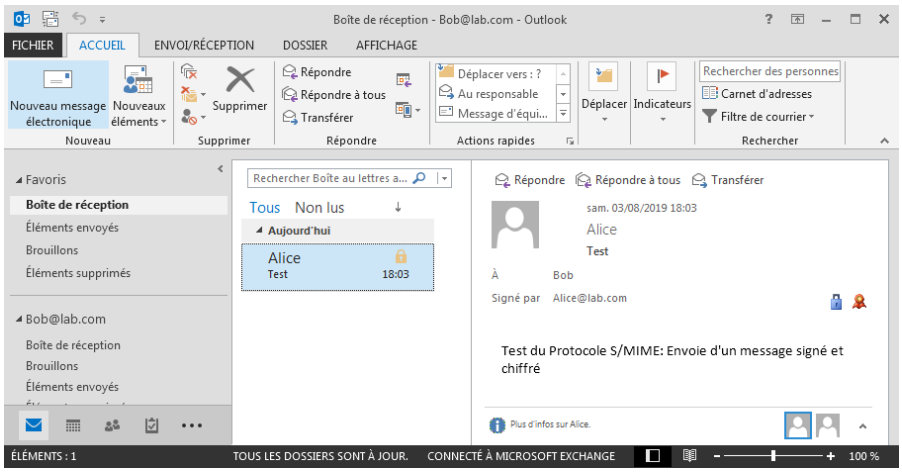

FIGURE 4.6.15 – Test du protocole S/MIME

4.6.5 La gestion des droits relatifs à l'information (IRM)

En plus de vouloir protéger le flux des communications et le contenu des courriers, une organisation peut avoir besoin de protéger les informations contenues dans les mails et ce que les destinataires peuvent faire d'elles, pour permettre par exemple d'empêcher un destinataire d'imprimer, transférer ou de copier-coller le

contenu d'un message en raison de la sensibilité de ses informations et c'est là que la gestion des droits d'information (IRM) entre en jeu.[Wesselius 14b]

Pour permettre l'utilisation d'IRM pour protéger les données Exchange, un serveur AD RMS doit être déployé dans la forêt Active Directory, les modèles de stratégie de droits doivent ensuite être définis, viens par la suite la configuration d'AD RMS pour Exchange et enfin déployer le méthode d'application de l'IRM choisie.

4.6.5.1 Déploiement du rôle AD RMS

Le rôle AD RMS doit être déployer sur un serveur membre du domaine Active Directory, ou carrément sur le contrôleur de domaine pour les petites entreprises. Dans le cadre de notre Lab nous allons l'installer sur notre contrôleur de domaine AD-DC01.

Le déploiement AD RMS commence par l'ajout du rôle AD RMS ainsi que les outils d'administration.

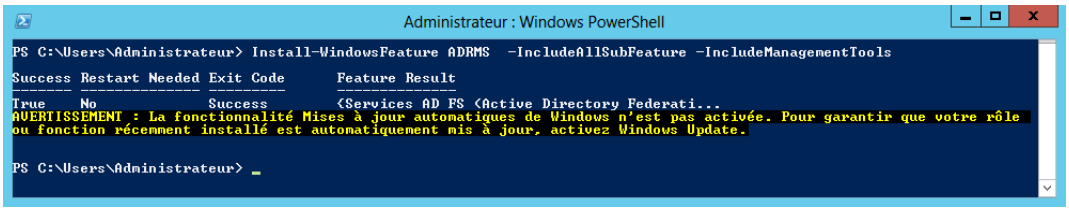

FIGURE 4.6.16 – Installation du rôle AD RMS

Une fois le rôle RMS installé sur le serveur, l'étape suivante consiste à configurer le service de rôle.

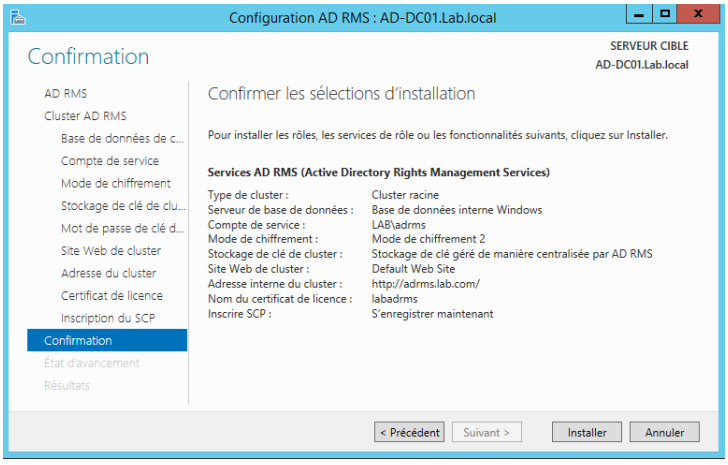

FIGURE 4.6.17 – Configuration du rôle AD RMS

4.6.5.2 Modèles de stratégie de droits AD RMS

La protection IRM est appliquée via un modèle de stratégie de droits AD RMS. Les modèles de stratégie de droits permettent de contrôler les droits d'un utilisateur ou d'un groupe sur le contenu d'un émail.

Création d'un modèle AD RMS

Afin de simplifier l'administration d'AD RMS nous allons créer un modèle de stratégie de droits qui va permettre à l'auteur d'un document de définir les conditions appliquées au contenu protégé. Dans le cadre de notre environnement de test, nous avons créé un modèle de stratégie de droits via la console AD RMS que nous avons nommé ''Lab Template" dans lequel nous avons défini les actions à entreprendre pour protéger le courrier.

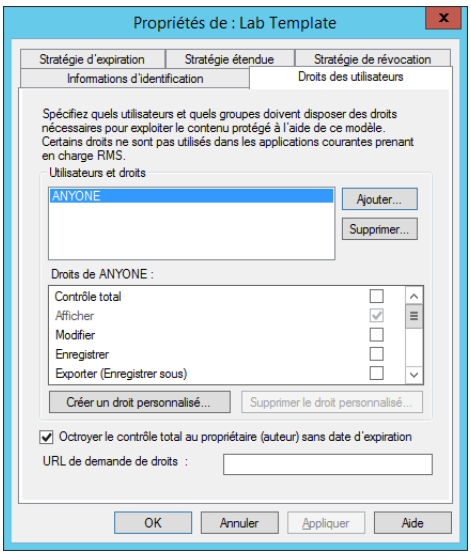

FIGURE 4.6.18 – Modèle de stratégie de droits

Une fois le modèle créé, nous allons a présent le publier pour l'ensemble des utilisateurs du domaine via la technologie SMB (Server Message Block).

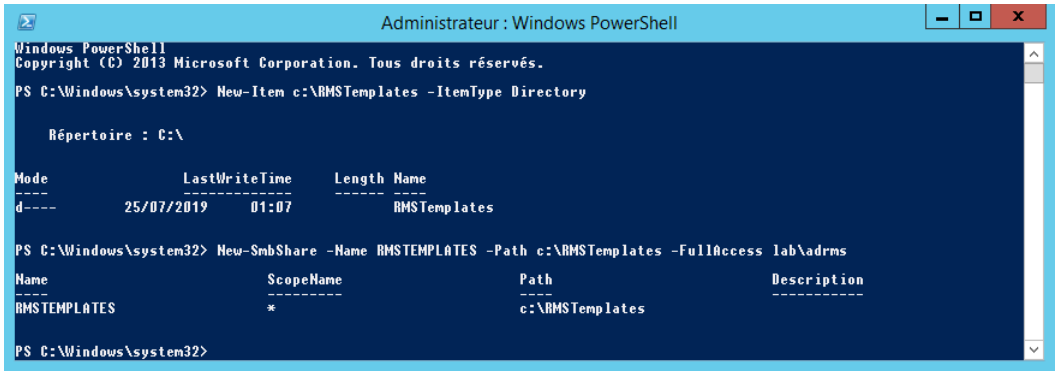

FIGURE 4.6.19 – Publication du modèle aux utilisateurs de domaine

4.6.5.3 Configurer AD RMS pour Exchange 2013

Pour intégrer RMS dans un environnement Exchange Server 2013, certaines configurations sur les serveurs AD RMS et Exchange doivent être effectuées pour octroyer des droits et un accès entre les deux systèmes et permettre au serveur Exchange de récupérer le modèle et de l'appliquer aux courriers. Il est nécessaire par la suite de tester la configuration IRM et de l'activer une fois le test réussit.

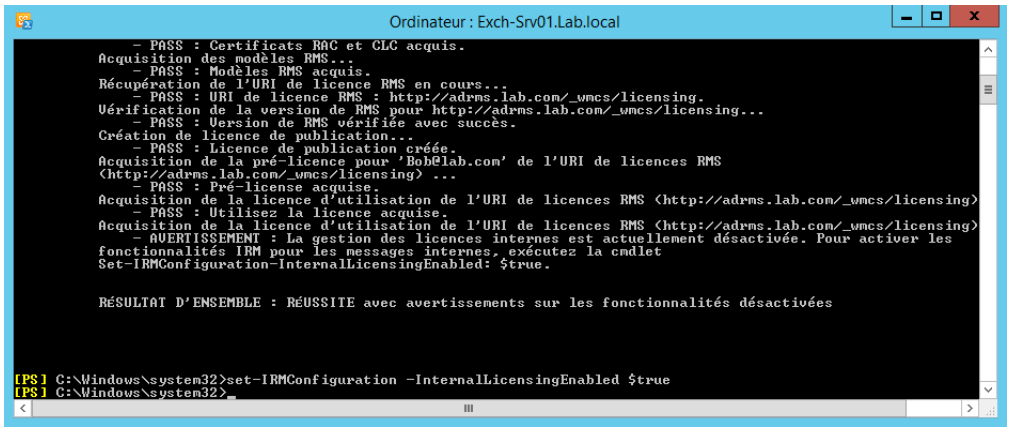

FIGURE 4.6.20 – Tester et activer la configuration IRM

4.6.5.4 Appliquer un modèle AD RMS sur les courriers

Il existe trois façons d'appliquer la protection IRM sur un message :

— La protection IRM peut être appliquée manuellement par les utilisateurs lors de la composition d'un message.

— La protection IRM peut être basée sur les stratégies de messagerie de votre organisation et appliquées à l'aide de règles de protection de transport ou de règles de protection Outlook.
  — **Les règles de protection transport :** La protection IRM est appliquée une fois que le message arrive au service de transport d'Exchange Server.
  — **Les règles de protection Outlook :** La protection IRM est appliquée par Outlook 2013 lorsque l'utilisateur compose un message.

Quelle méthode choisir ?

Dans Microsoft Exchange 2013, les utilisateurs peuvent appliquer la protection IRM aux messages en appliquant un modèle AD RMS. Toutefois, lorsque le choix est laissé aux utilisateurs, ceux-ci ont la possibilité d'envoyer les messages en texte clair sans protection IRM, ce qui peut mettre en danger les informations contenues dans les mails. Les règles de protection Outlook et transport permettent de remédier à ce problème en appliquant la protection IRM automatiquement aux messages dans Exchange 2013. Néanmoins la protection basée sur les règles de protection Outlook s'applique uniquement à Outlook et non à Outlook Web App, ce qui rend la protection basée sur les règles de transport plus avantageuse, celle que nous avons choisis d'ailleurs pour notre environnement de test.

Création des règles de protection de transport

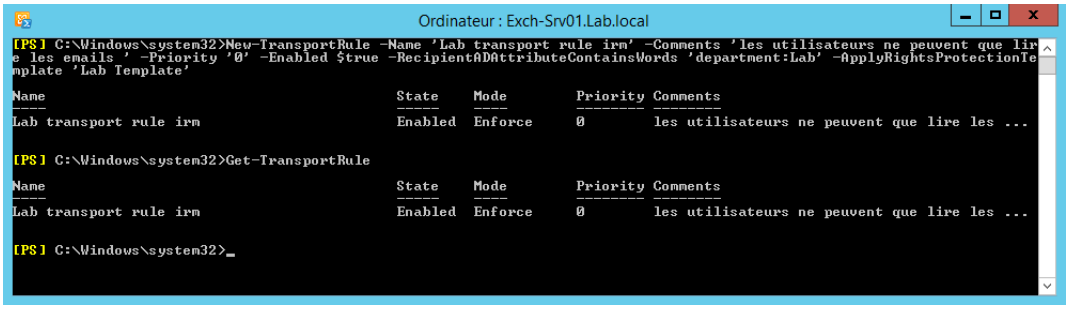

FIGURE 4.6.21 – Création des règles de protection de transport

4.6.5.5 Tester la protection des droits relatifs a l'information

Afin de tester la protection IRM, nous avons envoyer un mail de Bob vers Alice de la manière suivante.

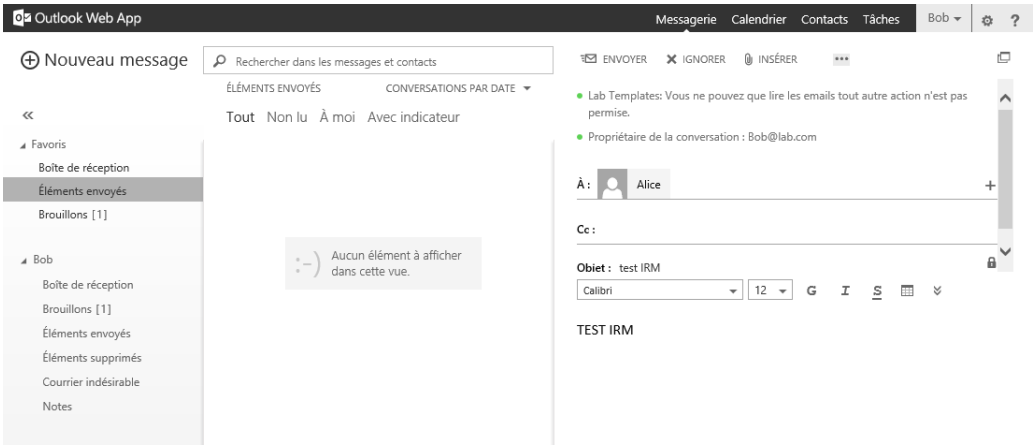

FIGURE 4.6.22 – Tester la protection des droits relatifs a l'information

4.6.6 Sécuriser les accès clients via le protocole Kerberos

Exchange utilise par défaut l'authentification NTLM (NT Lan Manager) pour la gestion des accès des clients.NTLM est un protocole utilisant le mécanisme challenge-réponse, le processus que suit ce protocole dans un environnement Exchange est le suivant :

1. L'utilisateur lance Outlook et envoie ses identifiants au serveur spécifié dans le profil Outlook.
2. Le trafic est dirigé vers un serveur CAS qui lui va vérifier ces informations en envoyant un trafic vers le contrôleur de domaine auquel il est associé.
3. Suite à la réponse du DC, le serveur CAS génère un jeton d'accès et répond à la demande. [Microsoft 11]

En plus d'être plus simple et moins sécurisé que kerberos, Ntlm apporte une charge plus lourd sur Active Directory puisqu'il effectue une vérification d'authentification pour chaque connexion à chaque serveur auquel le client se connecte ce qui signifie que les identifiants du client transiteront partout sur le réseau du moment que l'authentification n'est pas transmise entre les serveurs.

4.6.6.1 Configuration du Kerberos

La configuration du Kerberos dans exchange 2013 s'effectue en 3 étapes principales : la configuration des répertoires virtuels et d'Outlook Anywhere que nous avons déjà faite dans la partie configuration du Cas, la création du compte ASA et l'activation de l'authentification kerberos pour les clients.

Création de l'Alternate Service Account (ASA)

Dans un déploiement Exchange avec plusieurs serveurs Cas tel est le cas dans notre environnement, un client obtient un ticket de service kerberos dans le contexte du groupe. Toutefois, sur un serveur d'accès au client particulier, les services Exchange s'exécutent dans le contexte du système ou du compte de service réseau local et tenteront d'authentifier les tickets de service Kerberos dans ces contextes plutôt que dans le contexte du groupe. Cela provoque une incompatibilité de contexte et entraîne un échec de l'authentification Kerberos.

Pour que l'authentification Kerberos réussisse, le membre du groupe du serveur d'accès au client doit utiliser une autre information d'identification partagée (compte d'ordinateur, etc.) par tous les membres du groupe. Pour ce faire nous allons créer un objet dans Active Directory puis le propager dans toute la forêt.

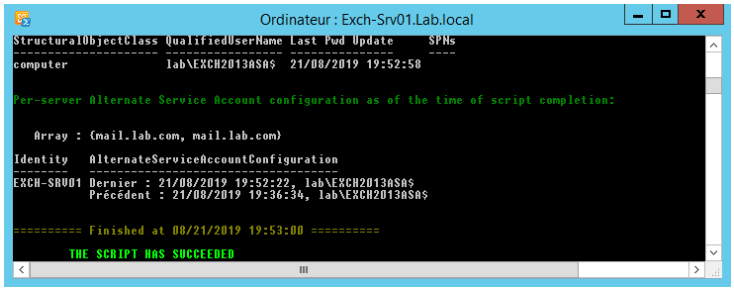

FIGURE 4.6.23 – Création de l'Alternate Service Account

Nous pouvons désormais créer les SPN pour notre compte ASA.

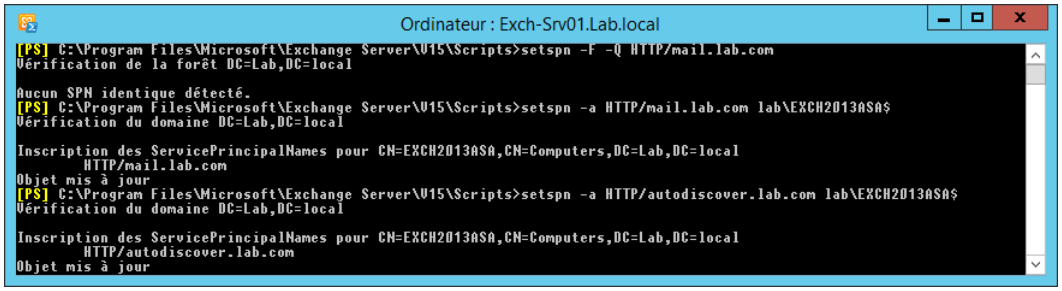

FIGURE 4.6.24 – Configuration des SPN pour le compte ASA

Activation de l'authentification Kerberos pour les clients Outlook

La dernière étape de la configuration du kerberos consiste à redéfinir le mode d'authentification des clients du Ntlm vers Kerberos, nous devons pour cela reconfigurer chaque serveur Cas afin de basculer l'authentification au mode Negociate.

Pour ce qui est de notre lab nous allons configurer kerberos forcé en interne et configurer kerberos avec fail-back en Ntlm en externe.

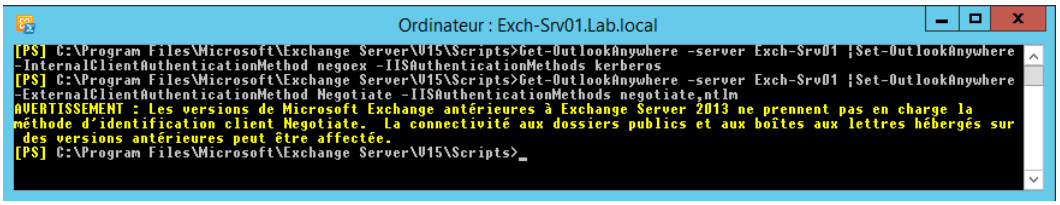

FIGURE 4.6.25 – Activation de l'authentification Kerberos

4.6.7 La protection contre les courriers indésirables et les programmes malveillants

4.6.7.1 Mise en place d'un serveur de transport Edge

Le serveur de transport Edge constitue la première ligne de défense du système de messagerie, son objectif principal est de fournir une protection supplémentaire face aux menaces toujours plus nombreuses sur Internet. Le serveur Edge se positionne en amont des services de transport de l'infrastructure Exchange ainsi il devient la passerelle en charge des entrées/sorties en provenance et à destination des réseaux extérieurs à l'entreprise.

La mise en place d'un serveur Edge implique quatre étapes principales :

Préparation du serveur :

L'installation du rôle Transport Edge demande l'installation de deux prérequis logiciels : le Framework .NET 4.5 (intégré a Windows Server 2012 R2) et le composant Active Directory Lightweight Directory Services (AD LDS).

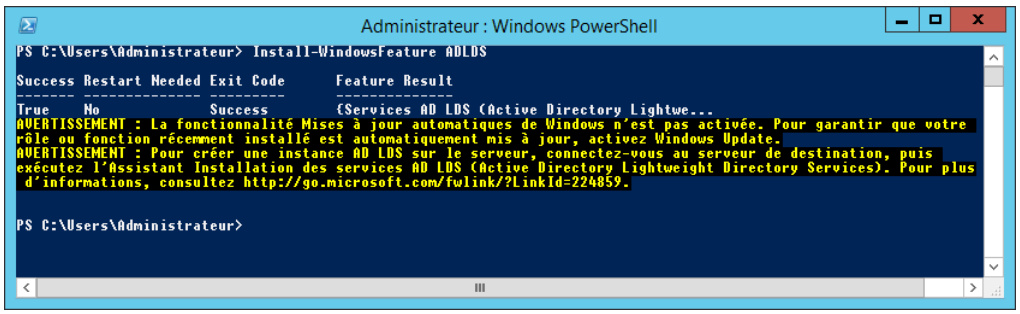

FIGURE 4.6.26 – Installation du rôle AD LDS

Installation du serveur de transport Edge :

Une fois les prérequis installés, le rôle Transport Edge peut être installé.

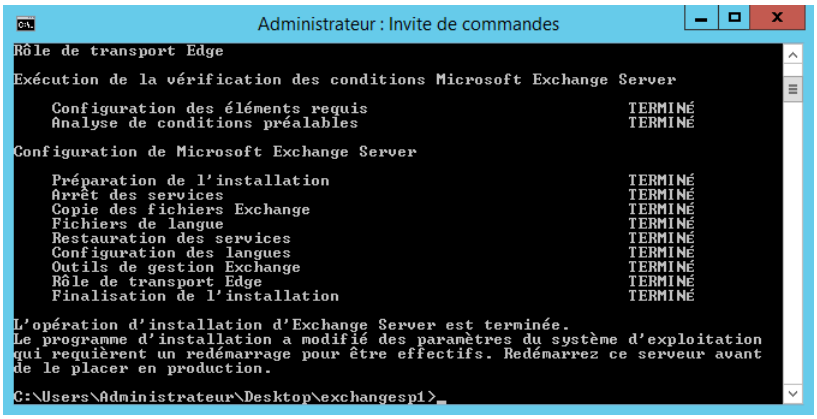

FIGURE 4.6.27 – Installation du serveur de transport Edge

Création de l'abonnement Edge :

Un serveur Edge ne dispose pas d'un accès direct à Active Directory. Toutes les informations de configuration et de destinataire que le serveur de transport Edge utilise pour traiter les messages sont stockées dans AD LDS. La création d'un abonnement Edge établit une réplication automatique et sécurisée des informations d'AD vers AD LDS ainsi le service Microsoft Exchange EdgeSync qui s'exécute sur les serveurs de boîtes aux lettres effectue périodiquement une synchronisation unidirectionnelle pour transférer des données à jour vers AD LDS. La création d'un abonnement Edge s'effectue de la manière suivante :

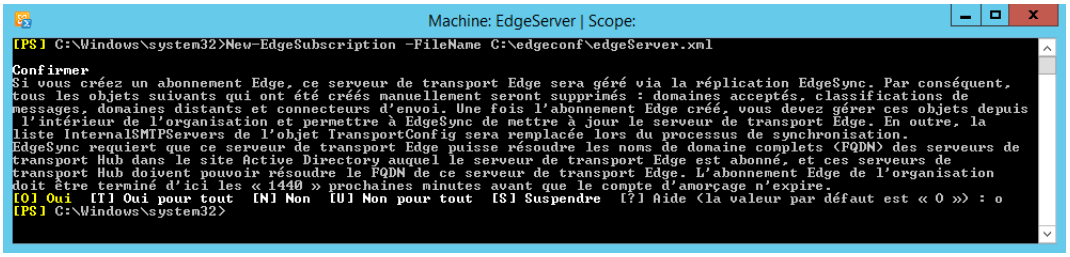

FIGURE 4.6.28 – Installation du serveur de transport Edge

Ainsi le fichier edgeServer.xml contient toutes les informations du serveur Edge requises par le serveur Exchange. Il est nécessaire donc de copier le ficher dans le serveur exchange et de lancer l'abonnement Edge de la manière suivante :

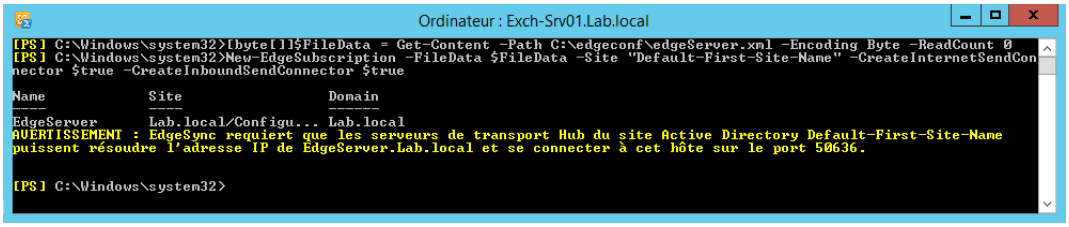

FIGURE 4.6.29 – Abonnement Edge

Démarrage de la synchronisation Edge :

Une fois l'abonnement créé nous allons a présent lancer la synchronisation entre le serveur Edge et Exchange afin de récupérer automatiquement la configuration requise.

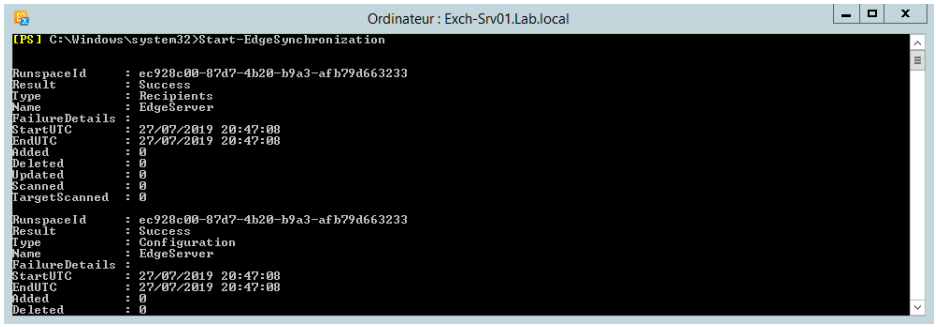

FIGURE 4.6.30 – la synchronisation Edge

4.6.7.2 Mise en place d'une protection anti-spam et anti-malware sur les messages internes

Protection contre les courriers indésirables

Exchange 2013 propose une approche de protection anti-spam basé sur des agents de transport pour réduire les spams dans une organisation, cette protection s'applique au niveau du serveur de boite aux lettre sur le service de transport Hub.

Activation des agents anti-spam

Nous allons dans un premier temps activer les agents anti-spam sur le service de boite aux lettre, une fois terminé un redémarrage du service de transport Microsoft Exchange est requis.

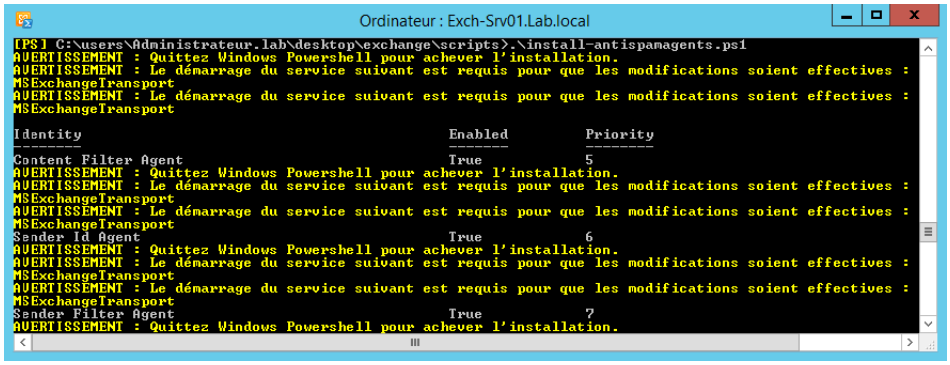

FIGURE 4.6.31 – Activation de l'agent anti-spam

Nous devons ensuite informer les agents anti-spam de nos serveurs Exchange, pour notre Lab les serveurs Exch-rv01 et Exch-Srv02 doivent être renseigner.

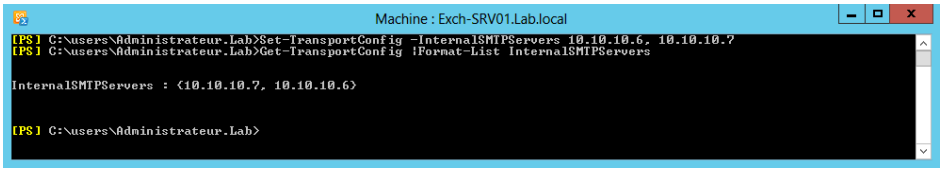

FIGURE 4.6.32 – Spécifier les serveurs internes

Lorsque d'autres agents anti-spam agissent sur les messages avant qu'ils n'atteignent le serveur de boîtes aux lettres, des en-têtes X anti-spam sont ajoutées aux messages et les messages passent sans être à nouveau analysés par les agents anti-spam présents sur le serveur de boîtes aux lettres à l'exception de l'agent de filtrage des destinataires.

Configuration des agents anti-spam

Une fois l'installation de l'agent anti-spam achevé, viens l'étapes de configuration des filtres anti-spam.

Configuration de l'agent de filtrage des expéditeurs

L'agent de filtrage des expéditeurs permet comme son nom l'indique de filtrer les expéditeurs des mails sur la base de la commande Mail From : et d'une liste d'émetteur, de domaine ou de sous-domaine définit par l'administrateur, ainsi un émail émit par un utilisateur figurant dans cette liste sera rejeter.

La politique de filtrage d'émetteur varie d'une entreprise a une entre, dans le cadre de notre Lab nous allons configurer une liste d'expéditeurs et de domaines bloqués ainsi que le blocage des mails dont l'en-tête de commande SMTP MAIL FROM est vide, le filtrage est activé en interne tout comme à l'extérieur de l'entreprise.

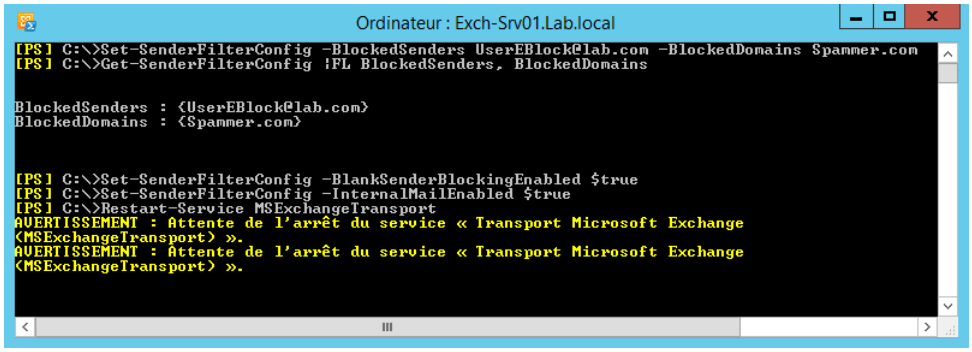

FIGURE 4.6.33 – Filtrage d'expéditeurs

Tester l'agent de filtrage des expéditeurs

Afin de tester le filtrage des expéditeurs, nous allons envoyer un émail depuis l'utilisateur UserEBlock vers l'administrateur Exchange.

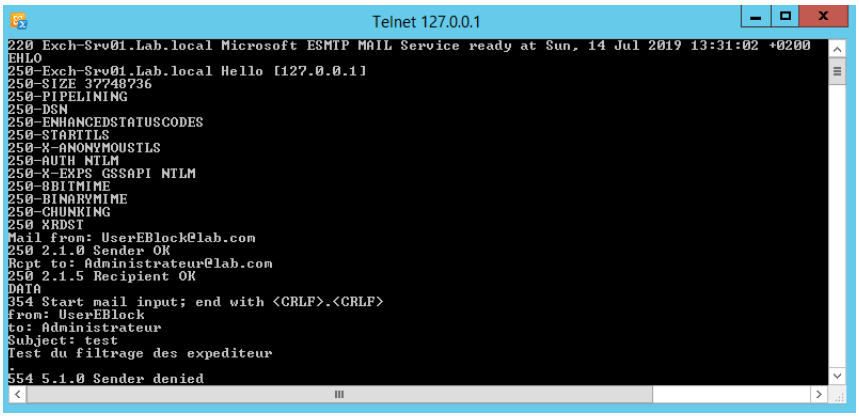

FIGURE 4.6.34 – Tester l'agent de filtrage des expéditeurs

Configuration de l'agent de filtrage des destinataires

L'agent de filtrage des destinataires : compare les destinataires des messages de la commande RCPT TO : SMTP à une liste de blocage de destinataires définie par l'administrateur, si une correspondance est trouvée ou si l'adresse ne correspond pas à un destinataire valide, le message n'est pas autorisé à entrer dans l'organisation, il sera donc rejeté.

Dans le cadre de notre Lab, nous allons configurer une liste de destinataire bloqués et bloquer les destinataires non présents dans le carnet d'adresse.

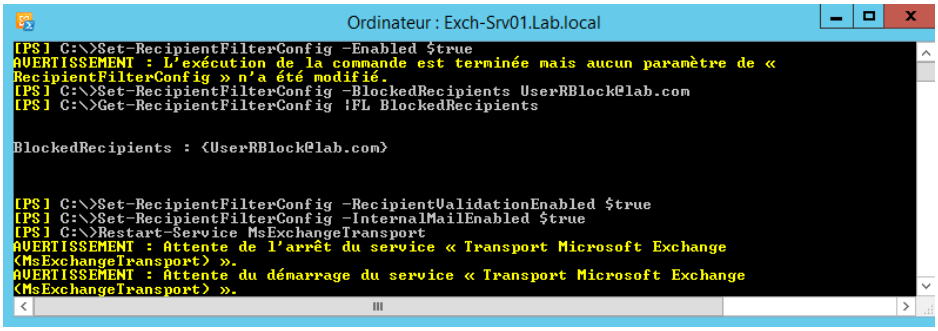

FIGURE 4.6.35 – Configuration de l'agent de filtrage des destinataires

Tester l'agent de filtrage des destinataires

Afin de tester le filtrage des expéditeurs, nous allons envoyer un émail depuis l'utilisateur UserEBlock vers l'administrateur Exchange.

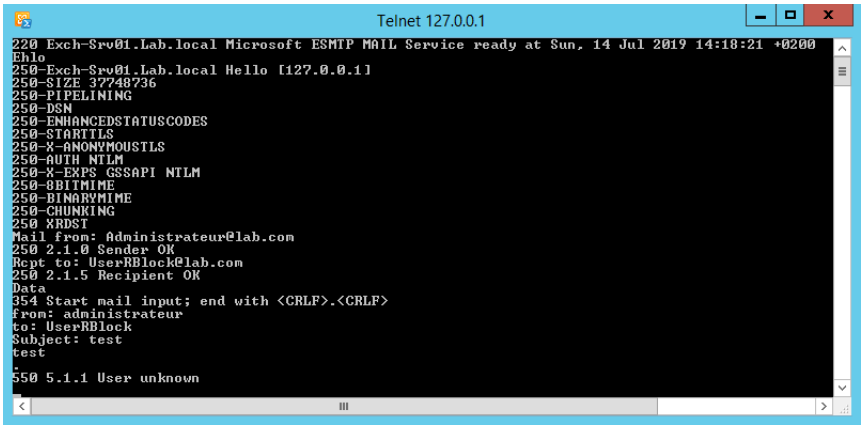

FIGURE 4.6.36 – Tester l'agent de filtrage des destinataires

Configuration de l'agent d'ID de l'expéditeur

Conçu par Microsoft pour lutter contre l'usurpation d'identité en vérifiant l'expéditeur d'un message électronique. Il s'appuie sur l'en-tête SMTP reçu et une requête pour le service DNS du système d'envoi. En effet lorsqu'un mail est reçu, le serveur Exchange interroge le serveur DNS de l'expéditeur pour vérifier que l'adresse IP à partir de laquelle le message a été reçu est autorisée à envoyer des messages pour le domaine spécifié dans les en-têtes de message et elle correspond bien à celle se trouvant dans l'entête SMTP.

FIGURE 4.6.37 – Configuration de l'agent d'ID de l'expéditeur

Configuration de l'agent de contenu

L'agent de filtrage du contenu permet de filtrer les messages en provenance de tous les connecteurs de réception et évalue la probabilité qu'un message entrant soit légitime ou indésirable, ce filtrage permet aussi d'identifier des messages contenant un contenu jugé inacceptable pour l'organisation.[Lohier 13]

L'agent de filtrage du contenu affecte une valeur de seuil de probabilité SCL (Spam Confidence Level) de courrier indésirable à chaque message. En fonction du seuil le message peut être supprimer, rejeter ou mis en quarantaine . Pour le Lab nous allons configurer cet agent de sorte à supprimer tous les mails dont la valeur SCL dépasse 8, rejeter les mails entre 6 et 7 et mettre en quarantaine les mails dont SCL égale à 5 et enfin placer les mails dont la SCL vaut 4 dans le dossier spam, puis configurer la SCL sur l'ensemble de l'organisation et donc sur toutes les boites aux lettres.

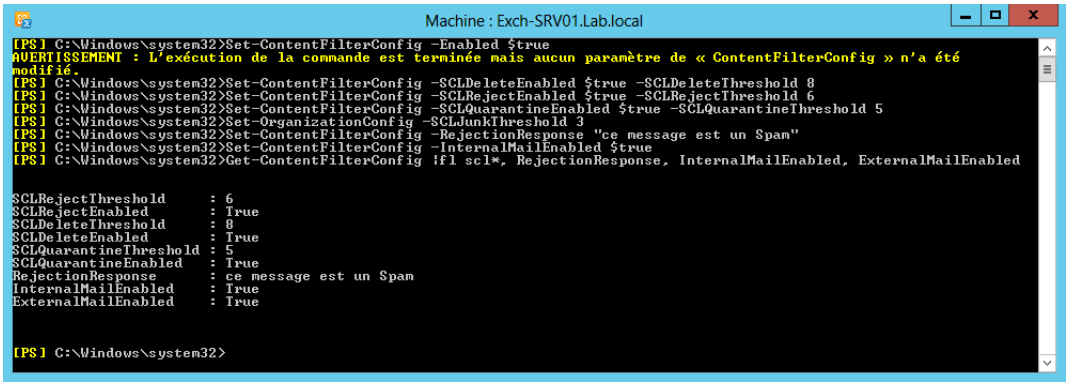

FIGURE 4.6.38 – Configuration de l'agent de contenu

Protection contre les programmes malveillants

Exchange 2013 intègre une solution de protection anti-malwares, conçue pour aider les organisations à lutter contre les virus et les logiciels d'espions dans leur

environnement de messagerie. Afin de mettre en œuvre une solution anti-malware, il est nécessaire dans un premier temps d'activer cette protection sur exchange 2013 et de redémarrer le service MicrosoftExchangeTransport.

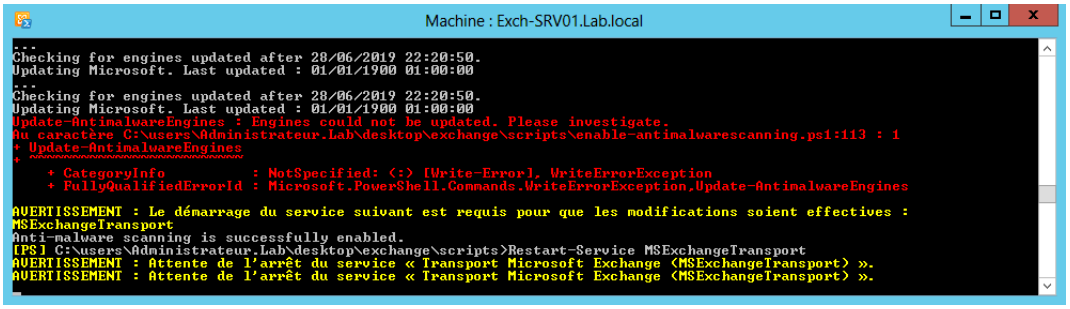

FIGURE 4.6.39 – Activer la protection anti-malware

Création d'une stratégie anti-malware

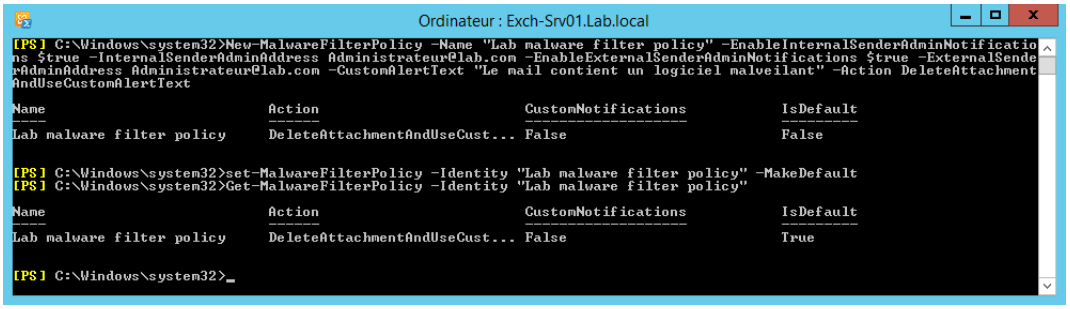

FIGURE 4.6.40 – Stratégie anti-malware

Tester la protection anti-malware

Afin de tester la protection anti-malware, nous allons utiliser le fichier de test d'antivirus EICAR.TXT pour tester le filtrage des programmes malveillants.

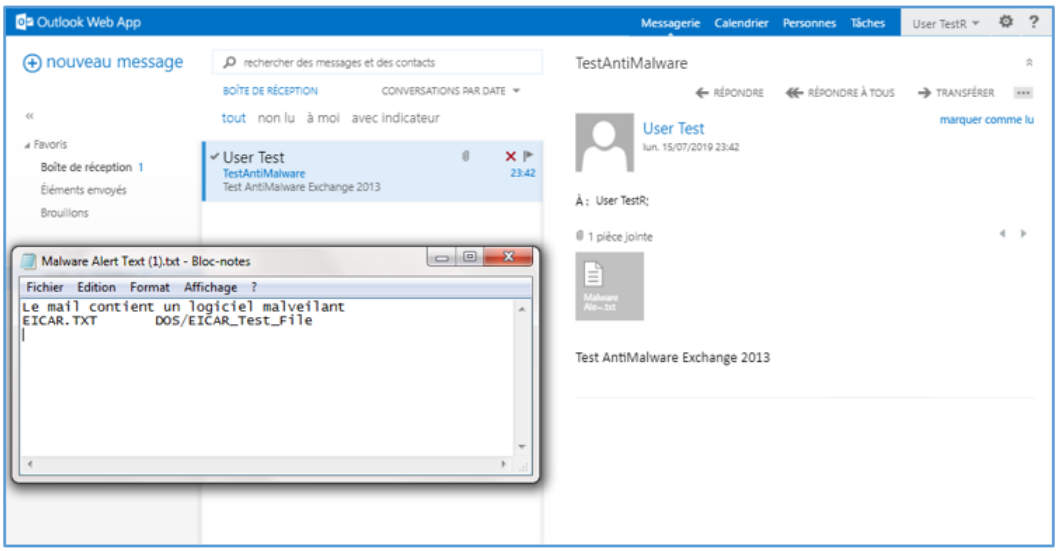

FIGURE 4.6.41 – Tester la protection anti-malware

4.6.7.3 Mise en place d'une protection anti-spam sur les messages externes

L'ensemble des messages externes à l'organisation exchange arrivent sur le serveur de transport Edge, lorsque les messages réussissent tous les filtres, ils sont remis au serveur. Le serveur de transport Edge 2013 possède en plus des filtres anti-spam existants dans un serveur de boite aux lettre deux autres filtres : le filtrage des connexions et le filtrage des pièces jointes.

Configuration des agents anti-spam

Filtrage des connexions : est la première couche de défense, lorsqu'un hôte tente de délivrer un message depuis internet sur le serveur de transport Edge, l'adresse IP source de la connexion Smtp est comparée aux adresses IP autorisées ou bloquées et en fonction de l'existence de l'adresse source du mail dans une des listes la connexion est acceptée ou refusée. La politique de filtrage des connexion se configure selon les besoins de l'entreprise, nous allons dans notre lab configurer un exemple de liste de blocage et d'autorisation.

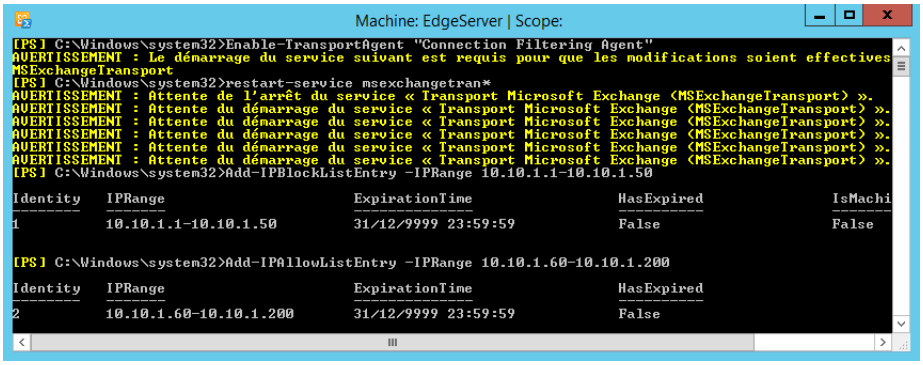

FIGURE 4.6.42 – Filtrage des connexions

Filtrage des pièces jointes : permet d'empêcher les fichiers joints aux messages électronique d'entrer dans l'organisation, Edge propose une approche de filtrage par type de contenu ou par nom de fichier, nous allons configurer l'agent de sorte à rejeter les messages contenant une liste de fichiers interdite.

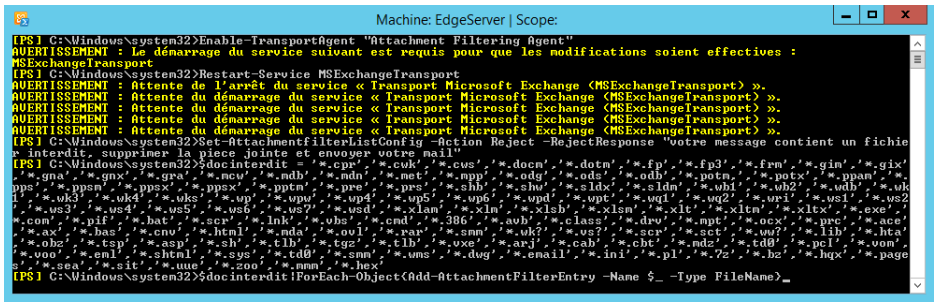

FIGURE 4.6.43 – Filtrage des connexions

Dans Exchange server 2013, la lutte contre les courriers indésirables passe par une implémentation de différents composants qui une fois réunis limiteront fortement les spams et les malwares dans l'organisation. Dans le cadre de notre Lab nous avons opté pour les solutions anti-malware et anti-spam intégrées de Microsoft qui sont déjà assez efficace mais rien n'empêche d'utiliser dans les entreprises des protections tierces lorsque le budget le permet.

4.6.8 La protection contre les pertes de données

Les DLPs fonctionnent via des stratégies DLPs, ce sont des packages contenant un ensemble de conditions composées de règles, d'actions et d'exceptions. Une fois les stratégies créés et activés, elles commenceront à analyser et filtrer les e-mails.

4.6.8.1 Création et configuration d'une stratégies DLP

La conception d'une stratégie DLP varie d'une entreprise a une autre en fonction des informations que l'entreprise veut protéger, pour notre Lab nous allons implémenter un exemple de stratégie DLP permettant d'empêcher les utilisateurs de transmettre des données sensibles en dehors de l'organisation et de les informer qu'ils sont en train d'infanger la politique de sécurité et que le mail sera refusé.

Pour ce faire nous allons donc tout d'abord transmettre à Exchange un exemple de document que l'on juge confidentiel.

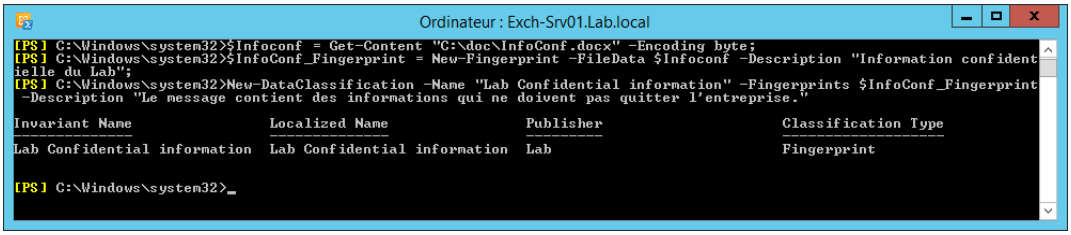

FIGURE 4.6.44 – Création des données sensibles

Puis nous allons créer la stratégie DLP et commencer à ajouter des règles de transport personnalisées.

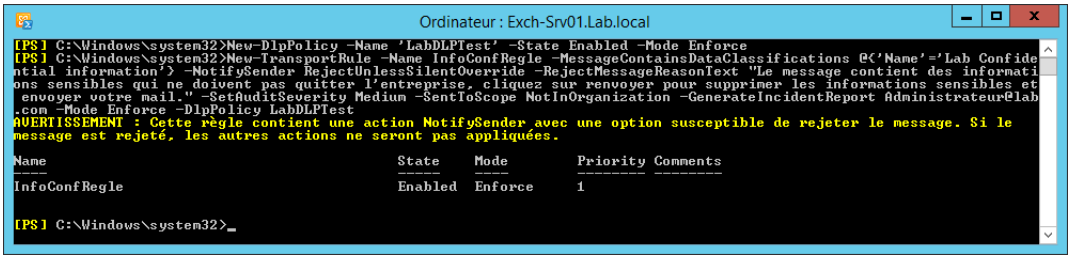

FIGURE 4.6.45 – Création d'une stratégie DLP

4.6.8.2 Test de la stratégie DLP

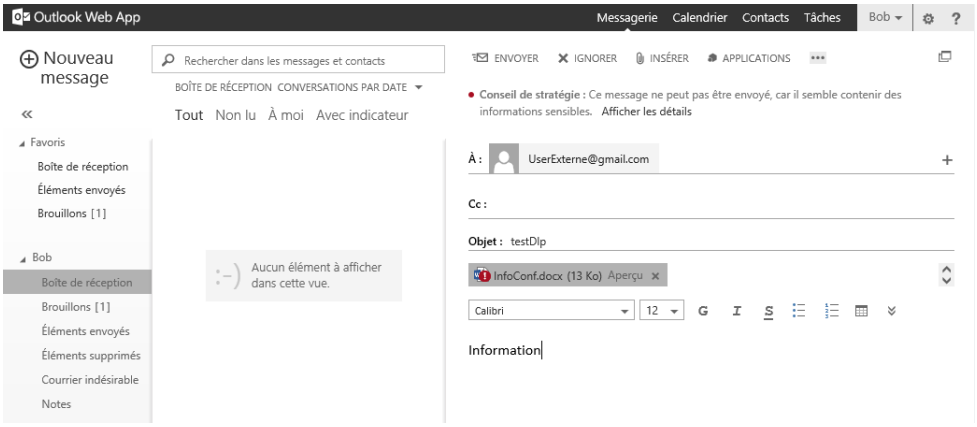

FIGURE 4.6.46 – Test de la stratégie DLP

4.7 Mise en place d'une solution de haute disponibilité

Lors du déploiement d'une plate-forme critique telle que la messagerie, la probabilité que ce système reste disponible sans interruption est quasiment nulle. La maintenance de tels systèmes complexes sans aucune interruption de service constitue un véritable défi.

4.7.1 Introduction a la Haute disponibilité

Dans le monde des technologies de l'information (IT), le terme haute disponibilité ou high availability désigne généralement un système ou un service conçu et mis en œuvre pour atteindre le niveau souhaité de performance et de disponibilité. Un service est dit disponible lorsqu'il est accessible par les utilisateurs finaux et exécute avec succès les tâches pour lesquelles il est conçu. Une haute disponibilité ne signifie pas nécessairement un service toujours disponible, mais elle signifie généralement un pourcentage très élevé de disponibilité pendant les heures de la journée où le service est requis. [Cunningham 15]

Que signifie la haute disponibilité pour Exchange Server 2013 ?

Bien que Microsoft Exchange Server 2013 soit un produit unique, il est composé de nombreux composants différents, cependant afin d'avoir une solution Exchange hautement disponible il est nécessaire de rendre disponible chacun de ses composants à savoir : le serveur d'accès client, le service de transport et le serveur de boites aux lettres.

4.7.2 Présentation de la solution de Haute disponibilité a déployer

4.7.3 Haute disponibilité du serveur de boite aux lettres

Dans Exchange 2013 la haute disponibilité d'un serveur de boites aux lettres repose sur le concept de DAG (Database Availability Group).

4.7.3.1 Présentation et fonctionnement du DAG

Le DAG symbolise la réunion d'un ensemble de serveurs de boites aux lettres qui vont répliquer entre eux un ensemble de base de données de boites aux lettres. Cependant en cas de pannes ou défaillance d'un disque ou du réseau ou encore lorsqu'une base de données n'est plus accessible, le DAG assure la continuité du système de messagerie en basculant vers une base de données fonctionnelle.[Cunningham 15]

A-t-on une limite en terme de serveurs membres du DAG ?

La solution DAG fonctionne avec un nombre de serveurs allons de 3 jusqu'à 16 serveurs, le minimum inclut deux serveurs de boites aux lettres hébergeant des bases de données de boites aux lettre et qui sont membres du DAG et un troisième serveur qui aura pour fonction le témoignage du bon fonctionnement du DAG entre les différents serveurs, ce serveur est appelé serveur de témoin, c'est un serveur membre du domaine AD et il ne doit être en aucun cas membre du DAG.

Comment fonctionne le DAG ?

Afin de comprendre le fonctionnement du DAG supposons qu'une solution DAG est mise en place, un des serveurs membre du DAG que l'on note Exch1 est mis en mode maintenance, cela entraine une permutation de serveur qui active la copie de base de données active sur Exch1 sur un autre serveur membre au bout d'un délai de 30s. Une fois le serveur est réparé et mis en ligne les autres serveurs membres du DAG sont notifiés et les copies de base hébergée sur le serveur Exch1 sont synchronisées avec les copies des autres membres. Une fois la synchronisation achevée, les copies de bases initialement active sur Exch1 se réactive et se mettent dans un l'état passive sur les serveurs ayant pris la relève d'Exch1.

Qui s'en charge du basculement et de l'activation des bases de données ?

Le basculement et la permutation des bases de données repose sur un composant nommé Active Manager . En effet le service de réplication Microsoft Exchange contrôle régulièrement l'état de toutes les bases de données montées, lorsqu'il détecte une défaillance, il notifie le Gestionnaire Active Manager qui a son tour détermine quelle copie de base de données doit être monté.

4.7.3.2 Mise en œuvre d'une solution de DAG

Dans le cadre de notre Lab nous déploierons une solution de DAG pour notre base de données de boite aux lettres Lab-BD de la manière suivante :

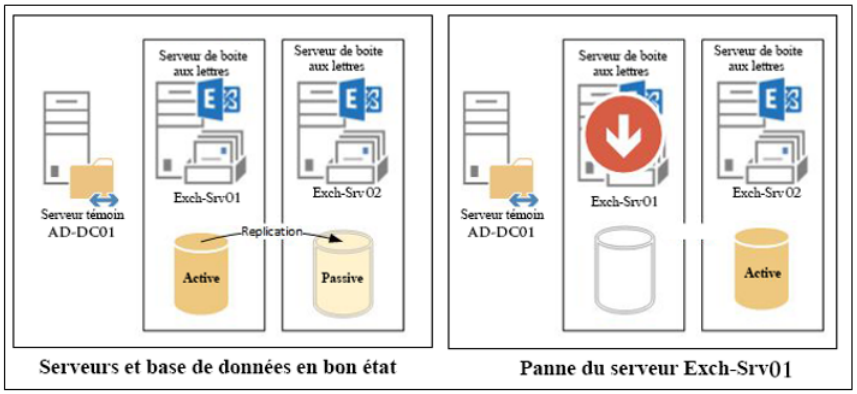

FIGURE 4.7.1 – Groupe de disponibilité des bases de données

Le processus de création du DAG :
La création d'un groupe de disponibilité de base de données (DAG) comprend plusieurs étapes. La première étape du processus consiste à créer le DAG lui-même puis ajout des serveurs de boîtes aux lettres au DAG et enfin l'ajout des copies de la base de données de boîtes aux lettres.

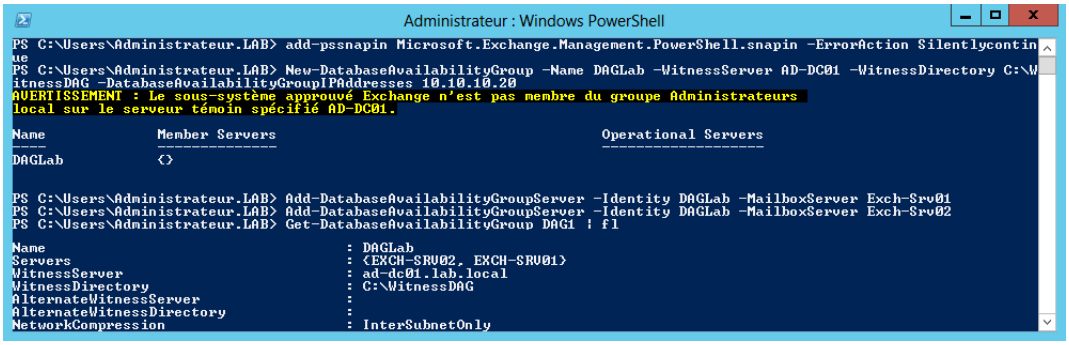

FIGURE 4.7.2 – Création du groupe de disponibilité des bases de données

4.7.4 Haute disponibilité du serveur d'accès au client

Le serveur d'accès au client (CAS) est le point d'entrée principal de toutes les connexions client au serveur Exchange, Il est donc important, lors de la conception ou de la configuration de la haute disponibilité, de prendre en compte les services

d'accès au client vus que la panne de ce service entrain la panne du système de messagerie en entier.[Cunningham 15]

La haute disponibilité du rôle CAS consiste donc à offrir une alternative de connexion aux client en cas de panne du serveur principal. Pour y parvenir, la méthode la plus courante consiste à repartir la charge entre plusieurs serveur CAS en utilisant : des solutions logicielles tel que la fonctionnalité NLB (Network Load Balancing) disponible nativement sous Windows Server, des équilibreurs de charge tiers dédiés, ou l'équilibrage de la charge matérielle qui est plus performant, mais a un coût élevé. [Lohier 13]

Dans le cadre de notre projet la solution qui s'offre à nous est la solution NLB et qui n'est malheureusement pas compatible avec le DAG. Nous proposons en revanche une solution de haute disponibilité du serveur CAS via le Round Robin.

4.7.4.1 Présentation du Round Robin DNS

Round Robin (RR) également appelé Tourniquet est une technique qui consiste à parcourir tous les serveurs Exchange et acheminer le trafic vers chaque serveur CAS. Le tourniquet DNS dépend entièrement du DNS et de la façon dont les ordinateurs clients et les périphériques traitent plusieurs enregistrements DNS pour le même hôte.

Le principe est simple, Il faut associer chaque serveur d'accès au client à l'espace de noms Exchange, ainsi à chaque fois qu'un client effectue une requête DNS pour l'espace de noms Exchange, il reçoit une liste ordonnée de tous les différents enregistrements A pour cet espace de noms spécifique. Lors de chaque requête DNS suivante, cette liste sera réorganisée de sorte que le prochain serveur d'accès au client du groupe constitue désormais la première entrée de la réponse DNS.

4.7.4.2 Mise en œuvre d'une solution Tourniquet DNS

Dans le cadre de notre Lab nous déploierons une solution de haute disponibilité du service d'accès client de la manière suivante :

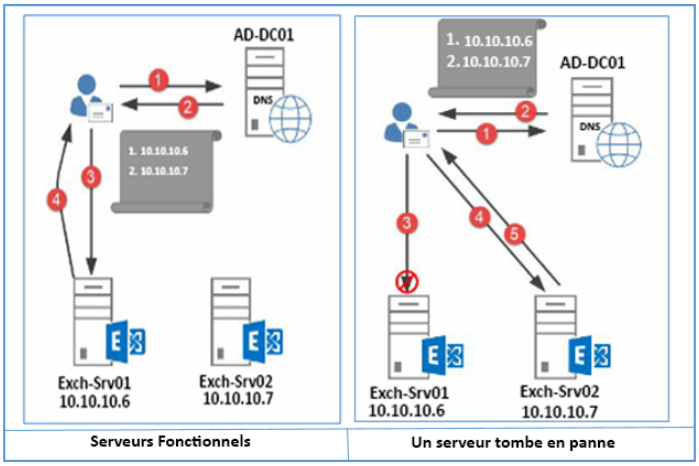

FIGURE 4.7.3 – Tourniquet DNS

1. Le client effectue une requête DNS pour l'espace de noms Exchange mail.lab.com.
2. Le serveur DNS répond avec une liste ordonnée.
3. Le client se connecte à la première adresse IP de la liste
4. Le serveur Exch-Srv01 répond à la demande du client.
5. Le client continuera à dialoguer le serveur Exch-Srv01 aussi longtemps qu'il sera disponible ou jusqu'à ce que la durée de vie de l'enregistrement DNS (TTL) expire. Ce dernier obligera le client à effectuer une nouvelle requête DNS et éventuellement à obtenir une liste ordonnée différente.

Dans le cas où le serveur Exchange en tête de liste n'est pas disponible, le client passe vers le deuxième serveur de la liste à savoir Exch-Srv02.

Configuration du tourniquet DNS :

Lors de la configuration du tourniquet DNS il est nécessaire de définir l'option TTL (Time-To-Live) de l'enregistrement DNS sur une valeur faible de 5 à 10 minutes, ainsi les clients enregistreront les modifications plus rapidement.

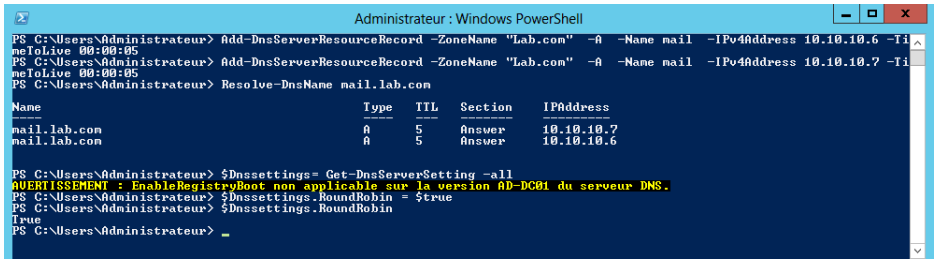

FIGURE 4.7.4 – Configuration du Tourniquet DNS

Une fois le tourniquet configuré, il est nécessaire de configurer le serveur Exch-Srv02 par le même certificat du serveur Exch-Srv01. Dans le cadre de la production il est recommandé d'accompagner la solution tourniquet DNS d'une solution de load balancing tierce ou d'un équilibreur de charge matérielle.

4.7.5 Haute disponibilité du service de transport

La haute disponibilité du service de transport Exchange est cruciale pour garantir qu'aucun courrier électronique ne soit perdu pendant le transit. Afin de rendre hautement disponible le service de transport.

4.7.5.1 Présentation et fonctionnement des Snapshots et du Safety Net

Exchange 2013 introduit deux notions importantes et complémentaires à savoir les snapshots et le Safety Net. En combinons ces deux notions nous pouvons rendre disponible le service de transport de sorte qu'aucun courrier électronique ne soit perdu pendant le transit.

- **Les clichés instantanés (snapshot) :** La redondance des clichés instantanés génère une copie redondante d'un courrier électronique sur un serveur différent avant son acceptation ainsi si le serveur émetteur ne reçoit pas d'accuser de réception du courrier au bout d'un certain temps, il soumettrait à nouveau le courrier.
- **Le Safety Net :** également nommé benne de transport ou dispositif de sécurité est une file d'attente associée au service de transport d'un serveur de boîtes aux lettres qui stocke temporairement les courriers électroniques traités avec succès par le service de transport.

Le Safety Net commence là où se termine la redondance des clichés instantanés, en d'autres termes, la redondance des clichés instantanés est chargée de garantir la livraison des e-mails en transit, tandis que Safety Net est chargé de garantir la resoumissions des messages précédemment envoyés lors de scénarios de récupération et de défaillance de la base de données de boîtes aux lettres.

Le diagramme ci-dessous présente un aperçu de la haute disponibilité du transport que nous allons configurer dans le cadre de notre Lab :

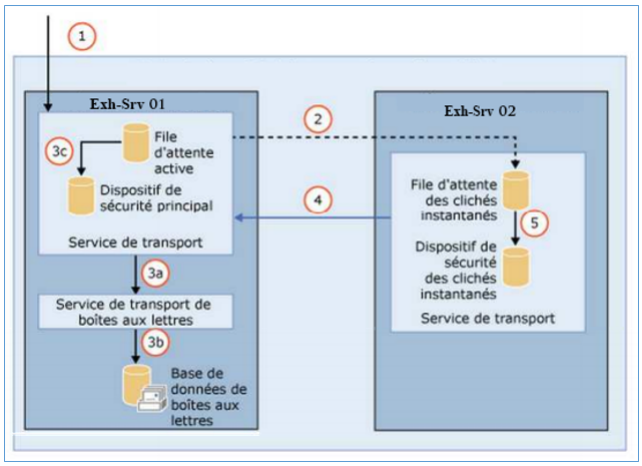

FIGURE 4.7.5 – La benne de transport et les clichés instantanés

1. Le serveur de boîtes aux lettres Exch-Srv01 reçoit un courrier électronique.
2. Avant d'accuser réception du courrier électronique, il démarre une session SMTP sur le serveur Exh-Srv02 qui lui crée un cliché instantané du courrier électronique.
3. Sur Exch-Srv01, le service de transport traite le courrier électronique principal et le remet à la base de données locale, il met en suite en file d'attente un statut pour Exch-Srv02, indiquant que le courrier électronique principal a été traité avec succès, et déplace une copie du courrier électronique principal vers le Safety net principal.
4. Exch-Srv02 interroge périodiquement le serveur principal pour obtenir le statut du courrier.
5. Une fois qu'il détermine que le courrier a été traité avec succès, il déplace le courrier vers le Safety Net local.

Le courrier électronique est conservé à la fois dans le Safety net primaire et dans le Safety net secondaire jusqu'à son expiration, sur la base d'une valeur de délai d'expiration configurable.

Pour les courriers envoyés le principe est quasiment le même, le serveurs Exch-Srv01 avant d'envoyer un email il contacte le serveur EXch-Srv02 qui lui créer une copie du mail, une fois l'accuse de réception sur le mail reçu le message est mis dans la fille d'attente.

Il faut noter que si un basculement de base de données se produit avant que ce délai ne soit atteint, le Safety Net principal sur Exch-Srv01 soumet à nouveau le courrier électronique. Si le serveur principal n'est pas disponible Exch-Srv02 le feras via le Safety Net secondaire.

4.7.5.2 Configuration de la Haute disponibilité du service de transport

Dans le cadre de notre Lab afin de rendre le service de transport hautement disponible nous allons configurer les connecteurs d'envoi et le Safety Net puisque le fonctionnement des snapshots est natif.

Configurer le connecteur d'envoi :

Nous allons configurer le connecteur d'envoi qui est en charge de l'envoi des mails en dehors de l'organisation avec deux serveurs Exchange, ainsi dans le cas de l'indisponibilité de l'un des serveurs le connecteur sollicitera l'autre serveur. La configuration du Safety Net requière que la redondance des clichés instantanés soit activée.

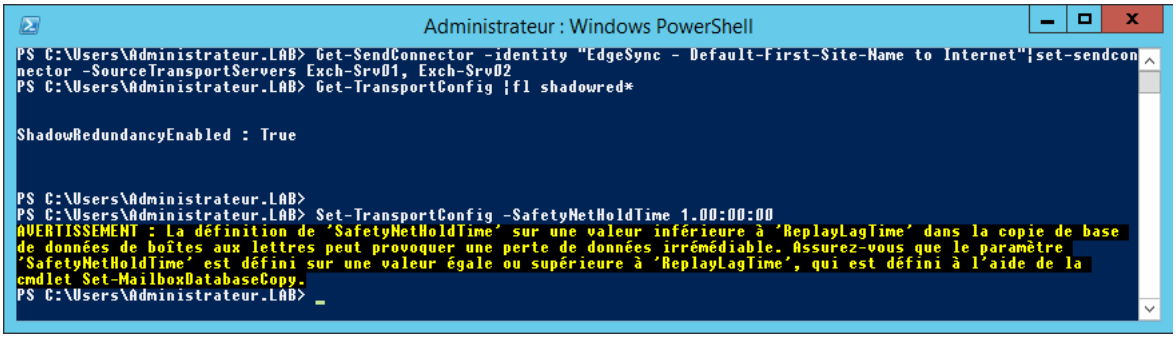

FIGURE 4.7.6 – Configuration de la benne de transport

4.7.6 La sauvegarde et la restauration d'Exchange Server

Aucune donnée informatique n'est à l'abri du risque de perte et ceci en raison de plusieurs causes matérielles et logiciels tel qu'un crash de disque, une suppression intentionnelle, des infections, un manque de vigilance, etc. Les causes peuvent être très diverses et peuvent couter très chères. Il est donc primordial de protéger ses données en gardant des copies dans des lieux surs grâce à des sauvegardes.

4.7.6.1 La sauvegarde d'Exchange Server 2013

La sauvegarde dans Exchange 2013 est le processus de stockage des éléments les plus importants du système de messagerie, telles que les bases de données de boîtes aux lettres, les fichiers journaux, les certificats SSL ou peut-être l'intégralité du serveur Exchange 2013, permettant ainsi une récupération des données suite à une perte. [Wesselius 14a]

Plusieurs niveaux de sauvegardes peuvent être créés :

La sauvegarde complète : représente une copie complète des données à protéger, une sauvegarde complète inclue toutes les bases de données de boîtes aux

lettres ainsi que tous les fichiers journaux nécessaires.

La sauvegarde incrémentale : permet de stocker uniquement les modifications enregistrées depuis la dernière sauvegarde complète ou incrémentale. Une restauration incrémentale nécessite l'ensemble des sauvegardes précédentes.

La sauvegarde différentielle : permet de stocker uniquement les modifications enregistrées depuis la dernière sauvegarde complète. Une restauration différentielle ne nécessite que la dernière sauvegarde complète. [Nelson 11]

Mise en place de la sauvegarde d'Exchange 2013 :

La sauvegarde dans Exchange server 2013 peut être mise en œuvre via divers solution de sauvegarde Microsoft ou tierce. Pour notre environnement de test nous avons opté pour l'outil de sauvegarde de Windows Server et nous l'avons utilisé de la manière suivante :

Commençons par l'installation de la fonctionnalité de sauvegarde de Windows server et ensuite la protection des bases de données via une sauvegarde quotidienne.

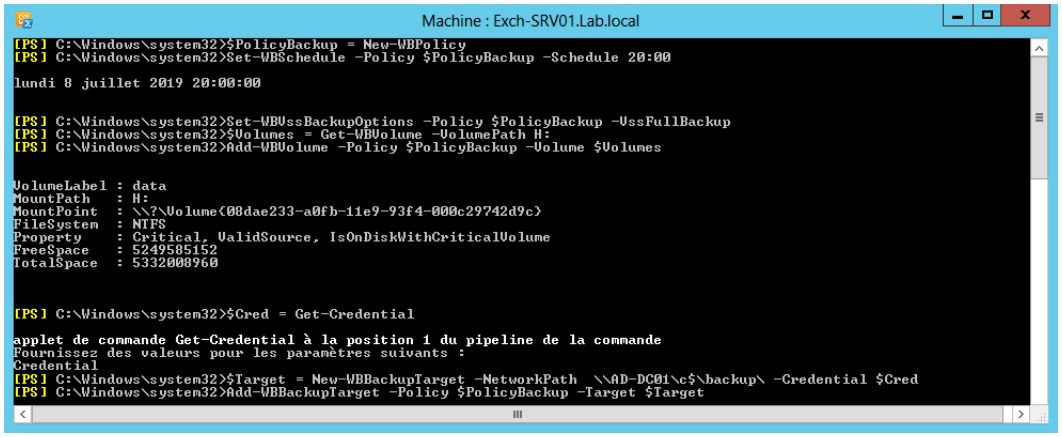

FIGURE 4.7.7 – La sauvgarde d'Exchange server 2013

La sauvegarde démarrera lors du prochain cycle automatiquement.

4.7.6.2 La restauration d'Exchange Server 2013

La récupération consiste à rendre accessible aux administrateurs, aux applications et aux utilisateurs un ensemble de données préservées par des sauvegardes. Exchange 2013 offre un ensemble d'outils intégrées permettant de restaurer entre autre des emails, des boites aux lettres supprimées ou déconnectées, etc. La solution de sauvegarde déployées permet aussi de récupérer des bases de données de boites aux lettres et des fichiers journaux.

La récupération de la base de données de boites aux lettres s'effectue via l'outil de sauvegarde Windows server de la même manière qu'une sauvegarde. Il est donc nécessaire de suivre les mêmes étapes de la restauration pour récupérer une base de données de boites aux lettres, puis vérifier son état via la commande Eseutil /mh <Fichier-BDD.edb> pour enfin la montée et la rendre accessible aux utilisateurs.

4.8 Conclusion

Dans ce dernier chapitre, nous avons illustré l'ensemble des tâches nécessaires, à la mise en place du système de messagerie basé sur Exchange Server, de sa sécurité et de sa disponibilité.

Conclusion générale et perspectives

La messagerie électronique a réussi l'épreuve du temps et de la concurrence pour s'imposer aujourd'hui comme l'outil le plus populaire au milieu professionnel et ceci grâce aux multiples avantages et fonctionnalités qu'elle fournit. Néanmoins, lorsque l'email véhicule des informations sensibles de l'organisation ce qui est souvent le cas, il représente un réel danger pour celle-ci.

Dans ce contexte l'objectif de notre travail était de proposer et d'implémenter une solution de sécurité et de haute disponibilité de sorte à éliminer le moindre risque possible sur le système de messagerie basé sur Microsoft Exchange Server.

Afin d'aboutir à cet objectif, nous avons dans un premier temps passé en revue les généralités et les notions théoriques relatives aux réseaux informatiques, la messagerie électronique ainsi que la sécurité dans un environnent de messagerie.

Ensuite, nous avons mis en place la solution de messagerie basé sur Exchange server sur un environnement de travail virtuel et nous avons réalisé l'ensembles des tâches de configuration et d'administration nécessaire pour une messagerie fiable et fonctionnelle.

Enfin, nous avons implémenté et testé la solution de sécurité et de la disponibilité que nous avons proposé de sorte à réduire les risques auxquels la messagerie est exposée.

Par ailleurs, les perspectives dégagées pour ce travail sont :

— Etude des scenarios de migration de systèmes de messagerie depuis les versions antérieures et depuis d'autres solutions.
— Etude et mise en place du rôle de messagerie unifie et de sa sécurité.
— Mise en production de notre solution au sein d'une organisation.

Bibliographie

[Adams 02] C. Adams & S. Lloyd. *Understanding PKI : Concepts, Standards, and Deployment Considerations*. Addison-Wesley Professional, 2002.

[Amiri 16] IS. Amiri & MR. Khalifeh Soltanian. *Theoretical and Experimental Methods for Defending Against DDOS Attacks*. Published by Syngress, 2016.

[Bancal 09] D. Bancal, D. Dumas & P. Puche. *Sécurité informatique Ethical Hacking : Apprendre l'attaque pour mieux se defendre*. Éditions ENI ,2éme édition, 2009.

[Bay 15] JP. Bay & JF. Pillou. *Tout sur la sécurité informatique*. Éditions Dunod ,4éme édition, 2015.

[Belattaf] S. Belattaf. *Sécurité informatique : introduction a la sécurité informatique*. 2016.

[Bloch 09] L. Bloch & C. Wolfhugel. *Sécurité informatique Principes et méthode à l'usage des DSI, RSSI et administrateurs*. Éditions EYROLLES ,2éme édition, 2009.

[Borenstein 96] N. Borenstein & N. Freed. *RFC 2046 : Multipurpose Internet Mail Extensions(MIME) Part Two : Media Types*, November 1996.

[Carraz 14] P. Carraz. *Exchange Server 2010 : Exploitation d'une plateforme de messagerie*. Editions ENI, 2014.

[Costales 08] B. Costales, G. Jansen & C. Aßmann. *Sendmail*. Édition O'Reilly,4éme édition, 2008.

[Crawford 08] S. Crawford & C. Russel. *WINDOWS SERVER® 2008 Volume 1 Installation et mise en réseau*. by Microsoft® Corporation, 2008.

[Cunningham 15] P. Cunningham, M. van Horenbeeck & S. Goodman. *Deploying and Managing Exchange Server 2013 High Availability*. 2015.

[Deman 08] T. Deman & M. Elmaleh F.and Chateau. *Windows Server 2008 : Administration avancée*. Éditions Eni, 2008.

[Dewett 15] A. Dewett. *How To Hack Email*. 2015.

[Déon 08] Sébastien Déon. *Zimbra : Messagerie collaborative d'entreprise Open source*. 2008.

[Dowland 10] P. Dowland & S. Furnell. *E-mail Security : A pocket guide*. by IT Governance Publishing, 2010.

[Dromard 09] Danièle Dromard & Dominique Seret. L'architecture des réseaux, collection synthex, 2éme édition. 2009.

[Fernando 16] Lagraña Fernando. *E-mail and Behavioral Changes : Uses and Misuses of Electronic Communications*. Wiley-ISTE,1ére édition, 2016.

[Freed 16] N. Freed. *RFC 2045 : Multipurpose Internet Mail Extensions(MIME) Part One : Format of Internet Message Bodies*, mars 2016.

[Garance 06] D. Garance & JM. Thomas. *PGP GPG Assurer la confidentialité de ses e-mails et fichiers*. ÉDITIONS EYROLLES, 2006.

[Goupille 05] Pierre-Alain Goupille. Technologie des ordinateurs et des réseaux, Éditions dunod, 8éme édition. 2005.

[Hadnagy 15] C. Hadnagy & M. Fincher. *Phishing Dark Waters : The Offensive and Defensive Sides of Malicious E-mails*. Published by John Wiley Sons, 2015.

[Haycox 09] L. Haycox, A. McDonald, R. Hildebrandt & C. Taylor. *Linux E-mail : up, maintain, and secure a small office e-mail server*. Packt Publishing, 2009.

[Klensin 08] J. Klensin. *RFC 5321 : Simple Mail Transfer Protocol*, October 2008.

[Lehning 13] H. Lehning. *Cryotographie codes secrets : L'art de cacher*. Éditions POLE, 2013.

[Lemainque 12] F. Lemainque & JF. Pillou. *Tout sur les réseaux et internet*. Éditions Dunod, 4éme édition, 2012.

[Lemesle] R. Lemesle & A. Petitjean. *Windows PowerShell (v1 et 2) : Guide de référence pour l'administration système*. eni editions.

[Lohier 13] S. Lohier, M. Noel, G. Yardeni, A. Abbate & C. Amaris. *Microsoft Exchange Server 2013 Unleashed*. by Pearson Education, 2013.

[Loshin 99] P. Loshin. *Essential Email Standards RFCs and Protocols*. Wiley Sons, 1999.

[Montagnier 01] Jean-Luc Montagnier. Construire son réseau d'entreprise, Éditions dunod. 2001.

[Moore 96] k. Moore. *RFC 2047 : Multipurpose Internet Mail Extensions(MIME) Part Three : Message Header Extensions for Non-ASCII Text*, November 1996.

[Morimoto 16] R. Morimoto & D. Présent. *Réseaux et transmissions : Protocoles, infrastructures et services*. Pearson Education, 2016.

[Myers 96] J. Myers & M. Rose. *RFC 1939 : Post Office Protocol - Version 3*, Mai 1996.

[Nedjmi 13] B. Nedjmi & L. Thobois. *Microsoft Exchange Server 2013 PowerShell Cookbook*. Packt Publishing, Second Edition, 2013.

[Neil 13] J. Neil & W. Blank. *Microsoft Exchange Server 2013 : Design, Deploy, and Deliver an Enterprise Messaging Solution*. Éditions Sybex, 2013.

[Nelson 11] S. Nelson. *Pro Data Backup and Recovery*. Éditions Apress, 2011.

[Norman Alan 17] T. Norman Alan. *HACKING HOW TO MAKE YOUR OWN KEYLOGGER in C++ Programming Language*. Éditions Kindle, 2017.

[Pfeiffer 14a] M. Pfeiffer & J. Andersson. *Exchange Server 2010 : Préparation à la certification MCSE Messaging - Examen 70-341*. Editions ENI, 2014.

[Pfeiffer 14b] M. Pfeiffer & J. Andersson. *Exchange Server 2013 : Préparation à la certification MCSE Messaging - Examen 70-341*. Editions ENI, 2014.

[Pujolle 08] GUY Pujolle. Les réseaux, Éditions eyrolles. 2008.

[Ramsdell 99] B. Ramsdell. *RFC 2633 : S/MIME Version 3 Message Specification*, June 1999.

[Resnick 01] P. Resnick. *RFC 2822 : Internet Message Format*, Avril 2001.

[Russel 15] C. Russel. *Deploying and Managing Active Directory with Windows PowerShell : Tools for Cloud-Based and Hybrid Environments*. Microosoft Press, 2015.

[Servin 06] S. Servin. *Réseaux télécoms*. Éditions Dunod, 2éme édition, 2006.

[Silva 06] G. Silva & V. Meunier. *Utilisez Thunderbird 2 ! : La messagerie intelligente et performante*. Éditions In Libro Veritas, 2006.

[Stanek 13a] R. Stanek & J. Andersson. *Microsoft Exchange Server 2013 Databases, Services, Management : Pocket Consultant*. Microsoft Press, 2013.

[Stanek 13b] W. Stanek. *Microsoft Exchange Server 2013 Pocket Consultant : Configuration Clients*. Microsoft Press, 2013.

[Stephen 00] A. Stephen & Thomas. *SSL TLS Essentials : Securing the Web*. ÉDITIONS Wiley, 2000.

[Stephen 01] A. Stephen & Thomas. *HTTP Essentials Protocols for Secure, Scaleable Web Sites*. Published by John Wiley Sons, 2001.

[Touitou 07] D. Touitou & M. Resnick. *Zimbra : Implement, Administer and Manage*. Packt Publishing, 2007.

[Turner 08] S. Turner & R. Housley. *Implementing Email Security and Tokens : Current Standards, Tools, and Practices*. Wiley Publishing, 1ére édition, 2008.

[Wesselius 14a] J. Wesselius. *Pro Exchange Server 2013 Administration*. Apress, 2014.

[Wesselius 14b] J. Wesselius & M. Rooij. *Pro Exchange 2013 SP1 PowerShell* $Administration_{F}orExchangeOn - PremisesandOffice365 - Apress. Apress$, 2014.

[Winters 13] N. Winters, N. Blank & N. Johnson. *Microsoft Exchange Server 2013 Design Deploy and Delivry an entreprise messaging solution*. Cybex, 2013.

Webographie

[Group 15] Radicati Group. *Email Statistics Report, 2011-2015*, mars 2015. http://www.radicati.com/wp/wpcontent/uploads/2011/05/Email-Statistics-Report-2011-2015-Executive-Summary.PDF[consulté:11mai2019]

[Group 19] Radicati Group. *Email Statistics Report, 2019-2023*, février 2019. http://www.radicati.com/wp/wpcontent/uploads/2011/05/Email-Statistics-Report-2019-2023-Executive-Summary.PDF[consulté:11mai2019]

[Hat 05] Red Hat. *Kerberos*, 2005. http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-fr-4/ch-kerberos.html[consulté:15août2019)

[Microsoft 11] Microsoft. *Enabling Kerberos Authentication*, avril 2011. https://techcommunity.microsoft.com/t5/Exchange-Team-Blog/Recommendation-Enabling-Kerberos-Authentication-for-MAPI-Clients/ba-p/585924[consulté:19août2019]

[Microsoft 16] Microsoft. *Exchange Server 2013*, Decembre 2016. http://technet.microsoft.com/fr-fr/library/bb124558(v=exchg.150).aspx[consultéle:10/06/2019]

[Microsoft 18] Microsoft. *Windows Server 2012 R2 PowerShell.*, Janvier 2018. https://docs.microsoft.com/fr-fr/powershell/windows/get-started?view=winserver2012r2-ps[consultéle16/06/2019]