République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de BEJAIA
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin d'étude

En vue de l'obtention d'un Master Professionnel en Informatique

Option : Administration et Sécurité des Réseaux

Thème

Etude et mise en place d'une messagerie électronique Exchange sécurisée

---

Réalisé par :

M^{lle} Ait amraoui Zina et M^{S} Hamzaoui Mohand.

Evalué le 10/09/2023 devant le jury composé de :

Président	*M^{me} Hamza Lamia*	*U. A/Mira Bejaia.*
Examinateur	*M^{me} Ait salah Sohila*	*U. A/Mira Bejaia.*
Encadrant	*M^{me} BACHIRI LINA*	*U. A/Mira Bejaia.*

Année Universitaire : 2022/2023

REMERCIEMENTS

À travers de ce modeste travail, nous tenons à remercier notre encadrant pour ses conseils, son orientation et son aide le long de notre projet de fin d'étude.

Mes remerciements s'adressent aussi aux président et membres de jury d'avoir accepté d'examiner et d'évaluer notre travail.

Mes plus vifs remerciements s'adressent à l'ingenieur de notre stage pour la réalisation de notre travail et à tout le cadre professoral et administratif de l'entreprise Ejitel.

Mes remerciements vont enfin à nos parents, nos amis et à toute personne qui a contribué de près ou de loin à l'élaboration de ce travail.

Table des matières

Table des figures

Introduction générale

Les technologies de l'information et de la communication sont les révolutions les plus importantes et les plus innovantes qui ont marqué la vie humaine le siècle dernier. En fait, ils nous apportent de multiples conforts révolutionnaires sur la façon dont les individus travaillent grâce à la puissance de traitement d'informations d'une part et de rapprochement des informations sur les distances d'autre part.

Parmi ces technologies, la messagerie électronique constitue leur application la plus visible et la plus déployée dans les environnements professionnels avec les avantages suivants : Le coût, la simplicité et l'efficacité qu'elle présente par rapport à la technologie au préalable, comme par fax ou par téléphone. En revanche, si le courrier électronique est également bénéfique pour une entreprise, il pourrait facilement conduire à la faillite de celle-ci, car le courrier électronique s'est avéré représenter un vecteur de menace considérable, fournit une voie pour une variété d'attaques, y compris les logiciels malveillants, le phishing et le spam. Ainsi, le système de messagerie devient un véritable défi.

Dans ce contexte, l'objectif principal de notre travail est d'assurer la sécurité et la disponibilité des systèmes de messagerie basés sur Microsoft Exchange Serveur 2019 .

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 et nous allons présenter l'organisme d'accueil.

— 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 existants 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 disponibilité proposée.

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

CHAPITRE 1

GÉNERALITÉS SUR LES RÉSEAUX INFORMATIQUES

1.1 Introduction

Actuellement, la société est dominée par la communication et la technologie, où l'avenir des réseaux informatiques continue de croître et de se développer. La sécurité informatique est donc devenue un enjeu majeur pour toute organisation utilisant un réseau informatique, qui vise à protéger les données et les systèmes contre les menaces potentielles. Dans cette optique, il est essentiel de comprendre les fondamentaux des réseaux et la sécurité informatique, notamment les différentes topologies, les modèles OSI et TCP/IP et équipements d'interconnexion, en outre les critères de la sécurité et les meilleures pratiques pour les garantir, et c'est le sujet de ce chapitre.

1.2 Les réseaux informatiques

1.2.1 Définition :

Un réseau informatique est un ensemble de dispositifs interconnectés, tels que des ordinateurs, des serveurs, des routeurs, des commutateurs, des imprimantes, des scanners, des périphériques de stockage et des appareils mobiles, qui peuvent communiquer et échanger des données entre eux. Les réseaux informatiques sont utilisés pour partager des ressources telles que des fichiers, des imprimantes, des connexions Internet et des applications, ainsi que pour faciliter la communication entre les utilisateurs. Les réseaux informatiques peuvent être configurés de différentes manières, en fonction des besoins et des objectifs spécifiques. Les réseaux peuvent être classés en fonction de leur taille et de leur portée géographique, tels que les réseaux locaux (LAN), les réseaux étendus (WAN) et les réseaux métropolitains (MAN). Les réseaux peuvent également être configurés en fonction de leur topologie, tels que les réseaux en étoile, les réseaux en bus, les réseaux en anneau et les réseaux en maillage. Les réseaux informatiques peuvent être utilisés dans de nombreux domaines, tels que l'entreprise, l'éducation, la recherche scientifique, les soins de santé, les services publics et les télécommunications. Ils sont devenus un élément essentiel de l'infrastructure de l'information moderne, permettant la communication, la collaboration et le partage des connaissances à l'échelle mondiale [28]. .

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 à relier ces ordinateurs entre eux afin de pouvoir échanger des informations.

Un réseau informatique a de divers intérêts :

- **Le partage de ressources :** Le partage de ressources (fichiers, applications ou matériels) est l'une des raisons justifiants 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 [11].

- **La communication entre personnes :** (courrier électronique, vidéo et conférences...).

- **La communication entre processus :** (entre des machines industrielles par exemple).

1.3.1 Classification des réseaux informatiques :

On distingue des différentes catégories des réseaux informatiques privés (des réseaux appartenants à une même organisation), selon leur taille (en termes de nombre de machines), leur vitesse de transfert de données ainsi que leur étendue :[22]

- **LAN :**(Local Area Network) .

- **MAN :**(Métropolitain Area Network) .

- **WAN :**(Wide Area Network).

- **PAN :**(Personal Area Network).

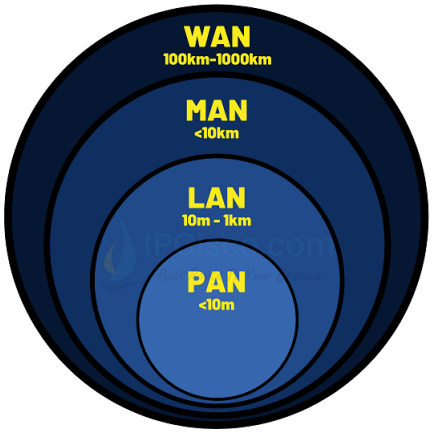


FIGURE 1.1 – Classification des réseaux informatiques.

LAN : Il s'agit d'un ensemble de machines appartenant à une même organisation et reliées entre eux dans une petite aire géographique ; il ne dépasse pas généralement les centaines de machines et un kilomètre de distance, la vitesse de transmission vont de 10 à 100 Mb/S. Ceux sont les plus nombreux, pour la très grande majorité privés, développés à l'échelle d'une entreprise ou d'un site industriel. (Mégabits par seconde).

MAN : Les réseaux métropolitains interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de kilomètres), ils ont des débits importants, ainsi un MAN permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local).

WAN : (Les réseaux étendus couvrent une grande zone géographique typiquement à l'échelle d'un pays, d'un continent, voire de la planète entière. Les débits disponibles sur un WAN résultent d'un arbitrage avec le cout des liaisons qui augmente avec la distance et peuvent être faibles. Les WAN fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un nœud du réseau, le plus connu des WAN est l'internet.

PAN : Désigne un type de réseau informatique restreint en terme d'équipements, généralement mis en œuvre dans un espace d'une dizaine de mètres. D'autres appellations pour ce type de réseau sont : réseau domestique ou réseau individuel .

1.3.2 Types de réseaux :

***Intranet :(Un réseau interne)** est un ensemble de services Internet (par exemple un serveur Web, un serveur de messagerie, un serveur de fichiers) mais à l'échelle d'un réseau local. On utilise donc des technologies Internet qui reposent sur le fameux protocole IP mais à l'échelle du réseau de l'entreprise. Ce réseau privé n'est pas visible du réseau Internet. Sa particularité est donc d'adopter les grands standards Internet mais de manière privée. L'Intranet est particulièrement adapté pour le travail collaboratif [10].

***Internet :(Un réseau ouvert)** Internet est le réseau informatique mondial que tout le monde connaît. Il correspond à une interconnexion d'un grand nombre de machines entre-elles. Ce réseau rend accessible au public un certain nombre de services hébergés, le point commun de tous ces services est le protocole IP (Internet Protocol) qui assure la communication entre toutes ces machines via un navigateur et une connexion [10].

***Extranet :(Un réseau privé)** Un Extranet est une extension du système d'information d'une entreprise à des partenaires situés au-delà du réseau de cette entreprise, cette extension est sécurisée de manière à n'autoriser l'accès uniquement qu'aux personnes désignées. Dans ce cas, le réseau Internet est mis à contribution pour véhiculer l'information, mais l'information n'est pas accessible du grand public. Un Extranet n'est donc ni un Intranet, ni un site Internet. Il s'agit d'un système supplémentaire offrant par exemple aux clients d'une entreprise, à ses partenaires ou à des filiales, un accès privilégié à certaines ressources informatiques de l'entreprise par l'intermédiaire d'une interface Web.

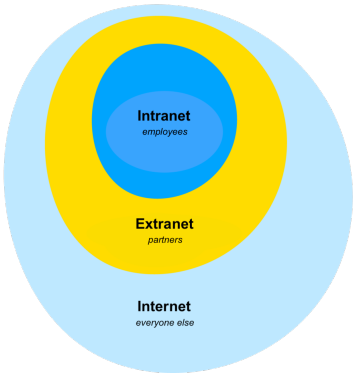


FIGURE 1.2 – Type de réseaux.

1.3.3 Les normes de communication réseau :

A. Le modèle OSI (Open System Interconnections) :
L'ISO a créé un modèle de références en 1984 appelé modèle OSI (Open System Interconnexion). Dont les constructeurs doivent respecter ses bases pour que leur produit soit vérifié et validé pour la vente [4].

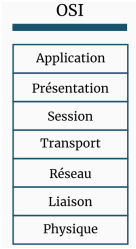


FIGURE 1.3 – Le modèle OSI.

- **La couche physique :** Cette couche définit les spécifications matérielles du réseau, tels que les câbles, les connecteurs et les signaux électriques utilisés pour transmettre les données.

- **La couche liaison de données :** Cette couche définit les protocoles qui permettent de transférer les données sur le support physique. Elle s'occupe de la gestion des erreurs de transmission, de la détection des collisions et de la gestion des adresses MAC (Media Access Control).

- **La couche réseau :** Elle permet de déterminer le chemin à emprunter pour acheminer les paquets de données entre les différents réseaux. Elle s'occupe également de la gestion des adresses IP (Internet Protocol).

• **La couche transport :** Cette couche permet d'assurer un transport fiable et efficace des données en découpant les données en paquets, en s'assurant de leur bonne réception et en gérant les retransmissions si nécessaire. Les protocoles TCP (Transmission Control Protocol) et UDP (User Datagram Protocol) sont utilisés à cette couche.

• **La couche session :** Cette couche permet d'établir, de gérer et de terminer les sessions entre les applications. Elle permet également de synchroniser les données échangées.

• **La couche présentation :** Cette couche permet de traduire les données dans un format compréhensible pour les applications. Elle gère également la compression et le chiffrement des données.

• **La couche application :** Cette couche permet aux applications de communiquer entre elles et d'accéder aux services du réseau. Elle regroupe les protocoles tels que HTTP, FTP et SMTP ...

B. Le modèle TCP/IP :

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait deux protocoles étroitement liés : un protocole de transport, TCP (Transmission Control Protocol) qu'on utilise « par-dessus » et un protocole réseau, IP (Internet Protocol). Ce qu'on entend par « modèle TCP/IP », c'est en fait une architecture réseau en quatre couches dans laquelle les protocoles TCP et IP jouent un role prédominant, car ils en constituent l'implémentation la plus courante.
Comme on peut le remarquer, les couches du mot TCP/IP ont des tâches beaucoup plus diverses que les couches du modèle OSI, étant donné que certaines couches du modèle TCP/P correspondent à plusieurs couches du modèle OSI [5].

Le modèle TCP/IP est composé de quatre couches principales :

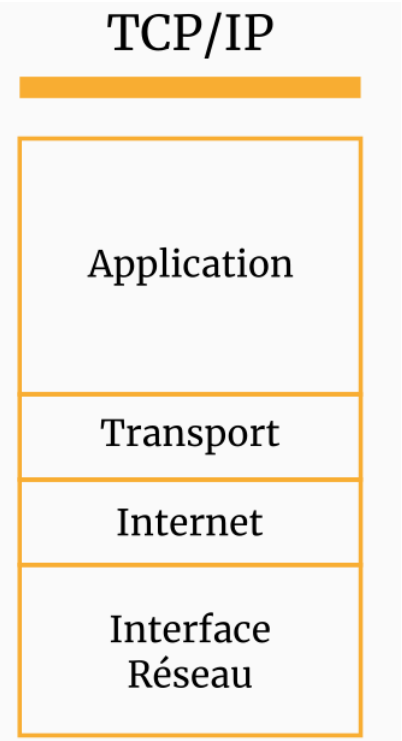


FIGURE 1.4 – Modèle TCP/IP.

- **La couche réseau (hôte réseau) :** Elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé.

- **La couche Internet :** Elle est chargée de fournir le paquet de données (datagramme).

- **La couche transport :** Elle assure l'acheminement des données, ainsi que les mécanismes qui permettent de connaître l'état de la transmission.

- **La couche application :** Elle englobe les applications standards du réseau (Telnet, SMTP et FTP...).

Le modèle TCP/IP est largement utilisé dans les réseaux informatiques, en particulier sur Internet. Il est plus simple que le modèle OSI et est plus adapté aux réseaux IP. Cependant, il est moins rigoureux que le modèle OSI en ce qui concerne la normalisation et la définition des couches. Parmi les organisations utilisant TCP/IP, on a les opérateurs de centres de données ; Ils l'utilisent pour gérer et contrôler le trafic réseau dans leurs données.

1.3.4 Architecture réseau :

Il existe deux types de réseaux LAN :

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

*** Les avantages d'une architecture P2P :**
- Un coût réduit.
- La simplicité.

*** Les inconvénients d'une architecture P2P :**
- Très difficile à administrer.
- La sécurité est très peu présente.
- Valable pour de petit nombre d'ordinateurs et pour des applications ne nécessitant pas une grande sécurité.

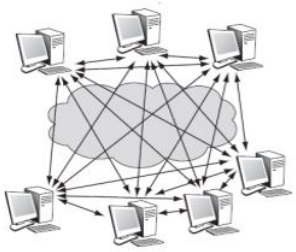


FIGURE 1.5 – Architecture Peer to Peer .

b) L'architecture client/serveur :L'architecture client-serveur est un modèle de fonctionnement logiciel qui se réalise sur tout type d'architecture matérielle (petites à grosses machines), à partir du moment où ces architectures peuvent être interconnectées. On parle de fonctionnement logiciel dans la mesure où cette architecture est basée sur l'utilisation de deux types de logiciels, à savoir un logiciel serveur et un logiciel client s'exécutant normalement sur deux machines différentes. [25]

*** Les types de l'architecture client/serveur :**

- **Architecture à deux niveaux :**

L'architecture à deux niveaux caractérise les systèmes clients/serveurs pour lesquels le client demande une ressource et le serveur la lui fournit directement, en utilisant ses propres ressources. Cela signifie que le serveur ne fait pas appel à une autre application afin de fournir une partie du service (sans passer par un service intermédiaire).

FIGURE 1.6 – Architecture client/serveur à deux niveaux .

- **Architecture à trois niveaux :**

Dans l'architecture à trois niveaux, il existe un niveau intermédiaire, c'est-à-dire que l'on a généralement une architecture partagée entre :
1. Un client, c'est-à-dire l'ordinateur demandeur de ressources, équipé d'une interface utilisateur (généralement un navigateur web) chargé de la présentation.
2. Le serveur d'application (appelé également middleware), chargé de fournir la ressource mais faisant appel à un autre serveur.
3. Le serveur de données, fournissant au serveur d'application les données.

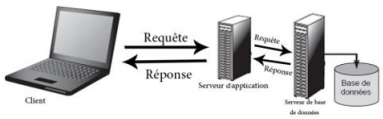


FIGURE 1.7 – Architecture client/serveur à trois niveaux .

- **Architecture multi-niveaux (à n-tiers) :**

Elle va plus loin dans le découpage de l'application sur différents serveurs. Elle est aussi appelée architecture distribuée du fait de la distribuion 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.

1.4 Présentation de l'entreprise

1.4.1 Introduction :

D'une manière générale, l'entreprise EGITEL, ou nous avons effectué notre stage pratique. On va commencer par la présentation du l'entreprise EGITEL (Entreprise Générale D'informatiques Des Télécommunications), en tant qu'organisme d'accueil, après on va présenter sa structure et ses moyens. Ensuite, on va présenter ses services et leur ambition, ainsi que l'équipe qu'on a intégrée pendant notre stage. Enfin, on va donner leur trophée et leur certification.

1.4.2 Présentation de L'EGITEL :

EGITEL (Entreprise Générale D'informatiques Des Télécommunications) est une entreprise SARL créé en 1995 par des ex cadres de l'entreprise étatique SONATITE, elle est l'une des toutes premières entreprises privées à investir le domaine des TIC. Elle est spécialisée dans les installations intégrées, Voix, données et image. Elle est aussi certifiée par des partenaires prestigieux de renommée mondiale reconnue, tels qu'Alcatel-Lucent ou Legrand ... Avec une expérience cumulée durant 22 années d'existence et son sérieux, elle a acquis un savoir-faire et un professionnalisme qui lui valent l'envergure des grandes entreprises. Une équipe dynamique, qualifiée dont les compétences avérées, accompagne les projets de sa clientèle à tous les niveaux. Rigueur dans sa méthodologie, des études approfondies, sont ses maitres mots pour répondre aux besoins et spécificités de chacun de ses clients.

FIGURE 1.8 – Logo (EGITEL) .

1.4.3 Situation géographique :

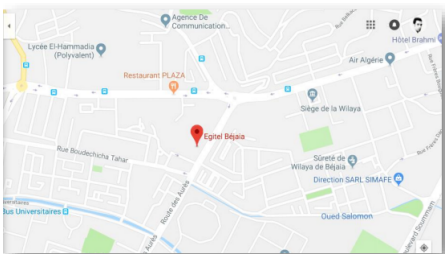


FIGURE 1.9 – Situation géographique de l'EGITEL a Béjaia .

1.4.4 Organigramme :

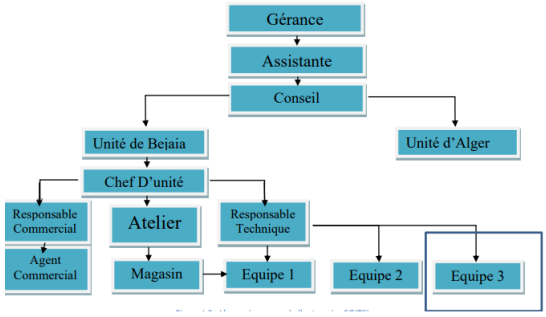


FIGURE 1.10 – L'organigramme de l'entreprise EGITEL. .

1.4.5 Structure :

-02 unités de réalisation de projets et d'intervention :

* Unité de Béjaia pour les régions Est /Sud.

*Unité d'Alger pour région Centre/Ouest.

FIGURE 1.11 – Unité de Béjaia et Alger

.

Gérées par des responsables techniques qualifiés et expérimentés. Avec un pool d'une douzaine de véhicules pour autant d'équipes d'interventions. L'EGITEL offre une qualité de service des plus performantes en célérité et professionnelle. Pour maintenir sa position, elle organise des stages aussi bien de perfectionnement que de recyclage pour son personnel.

1.4.6 Ateliers de maintenance et d'entretien :

L'EGITEL dispose :

***D'un atelier** équipé d'appareillages modernes, pour réparation et rénovation de modules, cartes et postes ainsi que le Service Apres Vente. Sous la responsabilité d'un technicien spécialisé.

*** D'un Magasin** Pour le stockage de la réserve en équipements, outillage, pièces de rechange et matériel de chantier géré par un magasinier chargé de la comptabilité matière.

*** 03 équipes** pour les travaux neufs et mise en œuvre de réseaux et solutions.

1.4.7 Qualifications et formations :

L'EGITEL est certifiée par ses partenaires, son personnel est recruté avec des formations de bases dans les domaines des TIC, puis perfectionne en continuant par des stages appropriés et des cycles de recyclage sur du nouveau matériel et les innovations techniques sont organisées. L'EGITEL utilise une demi-douzaine de véhicules fonctionnels pour son intervention.

A) Activités et services de L'EGITEL :

a- Installation des PBX Small/Moyen/Large.
b- Installation des réseaux informatiques et téléphoniques.
c- Installation des caméras de surveillance.
d- Mise en place d'une stratégie de sécurité.

B) Ambition de L'EGITEL :

Son ambition est de développer au mieux les NTIC, les applications et l'intégration des innovations, pour une communication souple et optimisée dans la gestion des établissements et des entreprises économiques et administratives.

Son objectif est de satisfaire sa clientèle en lui apportant une qualité de service appropriée et surtout, répondre à ses besoins et exigences à tout moment et en tous les lieux.

C) Evènements, certifications et trophées :

1- Certification :

L'EGITEL est certifiée par ses partenaires, ses certificats, sont obtenus par des examens.

* Commercial.

*Technique : Cette certification est renouvelée et actualisée de la même façon à chaque nouveauté ou évolution dans les équipements.

2-Les trophées :

L'EGITEL a obtenu 03 trophées de meilleur revendeur indirecte **(fourniture et installation de solutions de communication)** discerné par le partenaire **Alcatel-Lucent**, 2012-2013-2015.

D)Clientèle et partenaire de L'EGITEL :

1- La Clientèle de L'EGITEL :

La clientèle de l'EGITEL est comptée aussi bien dans les entreprises privées, que dans les entreprises, établissements ou administrations publiques. L'EGITEL intervient sur tout le territoire national.

FIGURE 1.12 – La clientèle de l'EGITEL.

.

2- Les Partenaires de L'EGITEL :

FIGURE 1.13 – Les Partenaires de L'EGITEL.

Ce stage nous est bénéfique sur plusieurs volets :

* Par la mise en pratique de nos connaissances acquises.

* Nous avons touché au domaine réel des applications et fonctions étudiées.

* Nous avons découvert aussi le monde du travail, les relations et l'organisation.

* Il faut signaler aussi, le bon accueil au niveau de la société que la disponibilité des techniciens pour nous accompagner.

1.4.8 Conclusion :

A l'issu de ce chapitre, nous avons présenté l'entreprise d'accueil et nous nous sommes parti d'une brève définition sur les réseaux, leurs architectures, et de classification et d'autres concepts décrivants les réseaux informatiques. Cependant, le but de construire des réseaux c'est de les exploiter. Durant notre travail, nous nous sommes intéressés à l'une des application client/serveur existante depuis très longtemps à savoir la messagerie électronique.

CHAPITRE 2

LA MESSAGERIE ÉLECTRONIQUE

2.1 Introduction

Sorti du laboratoire il y a environ 50 ans sous la forme d'une simple application. La transmission de messages entre deux ordinateurs s'impose désormais à un outil indispensable pour le grand public, mais surtout pour les grandes entreprises. Le courrier électronique a en fait commencé comme un simple outil. La transmission de messages courts s'est développée en douceur et presque silencieusement en suivant régulièrement les évolutions technologiques et constitue aujourd'hui l'un des outils d'amélioration de l'efficacité, dont la principale fonction est de permettre que les affaires marchent mieux. Dans ce chapitre, nous discuterons de quelques concepts sur la transmission de messages (origine, fonctionnement et protocole ...). Nous verrons son utilisation plus tard dans un cadre professionnel, on termine le chapitre en choisissant une solution de la messagerie la plus adaptée basée sur une analyse des outils existants marché.

2.2 Définition de la messagerie électronique :

Une messagerie électronique est un logiciel dont le but est de recevoir, de classer et d'envoyer vos courriers électroniques (e-mails). Parmi les plus connus on retrouve Outlook (de la suite logicielle Microsoft office), Windows Mail (anciennement Outlook Express, et installé par défaut sur Windows) mais aussi ThunderBird (par Mozilla). Une messagerie que l'on consulte directement sur Internet s'appelle également webmail [12].

L'intérêt de la messagerie électronique pour les entreprises : Elle est un outil de communication très important pour les entreprises et son utilisation est un enjeu pour eux car elle répond à leurs besoins techniques et opérationnels. Cependant, elle peut modifier complètement le travail et la productivité. Il est donc important d'utiliser cet outil avec précaution et de manière efficace et c'est pour cela que nous allons citer certaines de ses intérêts [13].

1) RAPIDITÉ :

- Plus rapide que la télécopie (fax).
- Fonction priorité pour signaler à un destinataire que le message a une priorité haute qu'il ne manquera pas de voir grâce à une icône (avec Outlook Express).

2) ÉCONOMIE :

- Plus économique que les interurbains, la télécopie.

3)RAPPROCHEMENT :

- Entretien de contacts avec des personnes, sans contrainte d'ordre géographique (brise l'éloignement).

4)ÉTENDUE :

- Réseau Internet implanté dans un grand nombre de pays.
- Serveurs disponibles en tout temps, indépendamment du décalage horaire.

5)PIÈCES JOINTES :

- Possible de joindre des fichiers de toutes natures à un message.

6) NOMBRE DE DESTINATAIRES :

- Transmission simultanée d'un message à plusieurs personnes.

7) LECTURE À DISTANCE :

- À partir d'une page Web (ex : Hotmail, Yahoo et GMail...), il est possible de lire ses messages sur n'importe quel ordinateur, n'importe où dans le monde, sans devoir modifier la configuration du logiciel de courrier installé sur l'ordinateur.

8) ARCHIVES :

- Archivage des messages expédiés et reçus.
- Archivage des messages dans des dossiers.

9) FIABILITÉ :

• Fonction « Demander une confirmation de lecture » d'un message expédié (menu Outils avec Outlook Express).
• Expédition automatique d'un message d'erreur si le courrier ne se rend pas.
• Longuement fiable.

2.3 Les RFCs (Request For Comments) :

2.3.1 Définition :

Les RFC (Request For Comments) sont un ensemble de documents qui font référence auprès de la Communauté Internet et qui décrivent, spécifient, aident à l'implémentation, standardisent et débattent de la majorité des normes, standards, technologies et protocoles liés à Internet et aux réseaux en général.

Par qui ces RFC ont elles été écrites ?

La suite de protocoles TCP/IP représente un ensemble de normes établies par un organisme qui s'appelle l'IETF (Internet Engineering Tasking Force). Ceux-ci publient officiellement leurs rapports sous formes de requêtes, disponibles pour tous, permettant d'éclaircir un grand nombre de sujets relatifs à TCP/IP. Chacun de ces documents représente une proposition de spécification qui peut à tout moment être rendue obsolète par un nouveau document RFC. Ainsi, les RFCs sont des fichiers textes dont le nom est"rfcxxxx.txt" dont xxxx est un nombre incrémenté pour chaque nouveau RFC. Il en existe actuellement plus de 2000, représentant une taille d'environ 130 Mo (25 Mo une fois compressés). Toutefois, un nombre de ces fichiers ont été remplacés par des fichiers plus récents. En réalité, n'importe qui peut écrire une RFC et la soumettre à l'IETF en la transmettant au responsable : rfc.editor@rfc.editor.org. Si celle-ci est acceptée, elle paraîtra après avoir été critiquée par les responsables. La RFC1543, intitulée instructions to RFC authors, explique comment rédiger une RFC [19].

2.3.2 Les RFCs relatives au courrier électronique :

Les normes RFCs (Request for Comments) qui se rapportent à la messagerie comprennent notamment [7] :

- RFC 821 : Spécification de base du protocole de messagerie SMTP (Simple Mail Transfer Protocol).
- RFC 822 : Format de message pour les courriels.
- RFC 2821 : Spécification actualisée de SMTP.
- RFC 2822 : Spécification actualisée du format de message pour les courriels.
- RFC 3501 : Définit le protocole de communication IMAP (Internet Mail Access Protocol).
- RFC 5321 : Spécification actualisées de SMTP.
- RFC 5322 : Spécification actualisée du format de message pour les courriels.

Ces normes sont développées et maintenues par l'Internet Engineering Task Force (IETF) et, sont largement utilisées pour assurer l'interopérabilité entre les serveurs de messagerie et les clients de messagerie.

2.4 Les notions indispensables de la messagerie électronique :

2.4.1 Adresse électronique :

Une adresse électronique est une chaîne de caractères qui permet de recevoir du courrier électronique dans une boîte de réception. Cela permet aux utilisateurs d'envoyer et de recevoir des messages électroniques à partir de n'importe quel endroit dans le monde, à condition qu'ils aient accès à Internet et un compte de messagerie électronique. Les adresses électroniques sont généralement composées d'un nom d'utilisateur suivi du symbole @ et d'un nom de domaine correspondant au fournisseur de messagerie électronique, par exemple monnomutilisateur@exemplaire.com. Les adresses électroniques sont largement utilisées pour la communication personnelle et professionnelle, ainsi que pour l'inscription à des services et la réception de bulletins d'information [3].

2.4.2 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 [6].

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

2) Le message :
Composé de deux éléments les champs d'entêtes et le corps du message.
Les champs d'en-tête (en anglais header fields), un ensemble de lignes décrivants les paramètres du message, tels que l'expéditeur, le destinataire et la date ...
Les champs d'entêtes peuvent être classés selon leurs catégorie d'usage :
— **Le champ de date :** correspond à la date et l'heure d'envoi du message, selon le fuseau horaire de l'expéditeur.
— **Les champs des entêtes qui indiquent la boite aux lettres de l'expéditeur :** sont au nombre de trois champs et permettent de renseignér 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 à l'adresse électronique spécifiée dans le champ from.
— **Les champs des 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 à 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 :** ceux 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 suivi 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 à son destinataire, un message sera envoyé a cette adresse mail.
— **Le champ Received :** correspond à la liste de tous les intermédiaires qui ont servis à transmettre le message au destinataire, soit le chemin emprunté depuis l'expéditeur au destinataire. 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.

2.4.3 MIME (Multipurpose Internet Mail Extensions) :

Multipurpose Internet Mail Extensions (MIME) a été développé par Bell Communications au début des années 1990 et plus tard standardisé par l'Internet Engineering Task Force (IETF) en 1996. La possibilité d'envoyer des pièces jointes et des médias riches dans les messages électroniques a considérablement élargi l'utilité et la polyvalence du courrier électronique, lui permettant d'être utilisé pour un plus large éventail d'objectifs au-delà de

la simple communication textuelle de base. MIME est désormais une norme largement utilisée et est pris en charge par tous les principaux clients et serveurs de messagerie [16].

DEFINITION MIME :

Multipurpose Internet Mail Extensions (MIME) est une norme Internet qui étend le format des messages électroniques pour prendre en charge le texte dans des jeux de caractères autres que ASCII, ainsi que des pièces jointes d'audio, de vidéo, d'images et de programmes d'application. MIME est une partie importante de l'infrastructure de messagerie, car il permet aux clients de messagerie d'envoyer et de recevoir des messages avec un contenu non textuel, et garantit que les messages peuvent être correctement interprétés et affichés par différents logiciels et systèmes de messagerie.
De plus, MIME fournit un moyen standard d'envoyer et de recevoir des messages avec plusieurs parties ou avec des versions alternatives du même contenu, telles que les versions HTML et texte brut d'un message électronique. Les spécifications MIME définissent également les procédures d'enregistrement des types de médias ou des formats de fichiers utilisés sur Internet [26].

2.4.4 Serveur et client de la messagerie :

2.4.4.1 Serveur électronique :

Un serveur de messagerie électronique est un ordinateur qui gère les envois et les réceptions de courriers électroniques (e-mails) pour les utilisateurs d'un système de messagerie électronique. Les serveurs de messagerie électronique peuvent être configurés pour fonctionner de différentes manières, mais en général, ils suivent un modèle client-serveur. Les exemples de serveurs de messagerie couramment utilisés incluent Microsoft Exchange Server 3, Gmail, Yahoo Mail et Zimbra. Les serveurs de messagerie peuvent être auto-hébergés ou gérés par des fournisseurs de services de messagerie en tiers [8].

2.4.4.2 Client de messagerie :

***Les clients lourds de la messagerie :**

Un client lourd de messagerie électronique est un logiciel de messagerie installé localement sur votre ordinateur, qui vous permet de gérer vos e-mails hors ligne. Les clients lourds de messagerie sont également connus sous le nom de clients de messagerie de bureau, car ils sont installés sur votre ordinateur et fournissent une interface utilisateur dédiée pour gérer vos e-mails. Voici quelques exemples de clients lourds de messagerie électronique : Microsoft Outlook, Mozilla Thunderbird, Apple Mail et IBM Notes.

Avantages :

— 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.

Inconvénients :

— 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 installé et configuré correctement, il doit être maintenu à jour à chaque nouvelle version afin d'assurer son bon fonctionnement.
— Les problèmes de sécurité : du point de vue de la sécurité, le stockage des émails sur l'ordinateur de l'utilisateur peut mettre les données en danger car si une personne réussit à 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 lourds de messagerie électronique sont particulièrement utiles pour les utilisateurs qui ont besoin de gérer des volumes importants d'e-mails hors ligne et qui souhaitent avoir un contrôle total sur la sécurité de leurs données de messagerie.

***Les clients légers de la messagerie :**

Un client léger de messagerie électronique est une application web qui permet de gérer les e-mails à partir d'un navigateur web, sans qu'il soit nécessaire d'installer un logiciel de messagerie sur l'ordinateur. Les clients légers de messagerie sont souvent utilisés dans les environnements professionnels et d'entreprise, où les utilisateurs ont besoin d'accéder à leur compte de messagerie depuis plusieurs appareils ou emplacements différents.
Voici quelques exemples de clients légers de messagerie électronique : Gmail, Yahoo ! Mail et Outlook.com, .

Avantages

Les clients légers de messagerie sont des ordinateurs qui sont conçus pour être utilisés avec un serveur centralisé pour stocker et gérer les données. Ils sont souvent utilisés dans les entreprises car ils permettent aux responsables informatiques de mieux contrôler les installations logicielles, les mises à jour et la gestion des appareils. Les clients légers présentent également un très bon rapport coût/efficacité pour une prestation fournie par les services informatiques.
Les avantages de l'accès à distance sont échangés contre la sécurité potentielle de la machine à partir de laquelle l'utilisateur accède à son courrier électronique, surtout si ce n'est pas le sien.

Les clients légers de messagerie électronique sont pratiques pour les utilisateurs qui ont besoin d'accéder à leur compte de messagerie à partir de plusieurs appareils ou emplacements différents, sans avoir besoin d'installer un logiciel de messagerie sur chaque appareil. Ils sont également souvent plus simples et plus faciles à utiliser que les clients lourds de messagerie électronique, ce qui les rend populaires auprès des utilisateurs occasionnels.

2.4.5 Les protocoles de messagerie :

1.SMTP pour la gestion du courrier :

SMTP signifie Simple Mail Transfer Protocol. Il s'agit d'un protocole de communication standard utilisé pour transférer des messages électroniques entre des serveurs de messagerie via Internet. SMTP est principalement responsable de l'envoi du courrier, tandis que d'autres protocoles, tels que

POP3 et IMAP, sont utilisés pour recevoir et récupérer le courrier d'un serveur. Dans SMTP, un serveur est chargé d'envoyer ou de transférer des messages à d'autres serveurs pour livrer le courrier au serveur de messagerie du destinataire prévu. SMTP utilise le port TCP 25 par défaut pour la communication, mais il peut également utiliser d'autres numéros de port, tels que 587 ou 465 [17].

2. Établissement de la connexion et identification des expéditeurs et destinataires du message :
Le client (serveur d'envoi) initie une connexion TCP au serveur (serveur de réception) sur le port 25 (port SMTP par défaut). Alors Le client doit envoyer la commande EHLO (Extended HELO) pour s'identifier et spécifier ses capacités avant de commencer une transaction. Le serveur répond avec son nom et les fonctionnalités prises en charge. Le client envoie la commande MAIL FROM pour spécifier l'adresse e-mail de l'expéditeur. Le serveur répond par un code 250 OK. Le client envoie la commande RCPT TO pour spécifier l'adresse e-mail du destinataire. Le serveur répond par un code 250 OK.

3.Transfert du message :
Le client envoie la commande DATA pour indiquer le début de la transmission du message. Le client envoie l'en-tête du message (y compris From, To et Subject...) et le corps. Le client envoie lui-même un point (.) sur une ligne pour indiquer la fin du message.

4.Libération de la connexion :
Le serveur répond avec un code 250 OK et stocke le message pour livraison. Au cours de ce processus, le serveur peut effectuer un filtrage anti-spam et une analyse antivirus pour s'assurer que le message est légitime et sûr. De plus, le cryptage peut être utilisé pour sécuriser la communication entre le client et le serveur.

2.5 Analyse des outils de messagerie électronique :

Depuis l'adoption de l'e-mail dans le monde professionnel, la concurrence sur les logiciels de messagerie s'est intensifiée, chaque constructeur privilégiant son propre produit, reconnu pour ses fonctionnalités et la qualité du service rendu. Il n'y a certainement pas de produit parfait dans un environnement professionnel. La différence est la sécurité et la fiabilité. Après l'analyse, la solution de messagerie la plus fiable est sélectionnée. Cela offre plus d'opportunités aux administrateurs de systèmes de messagerie pour établir des mesures de sécurité.

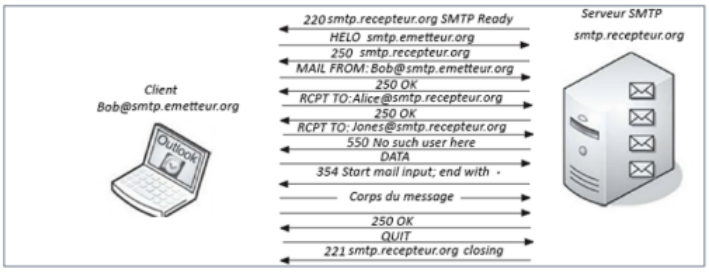


FIGURE 2.1 – Exemple de dialogue SMTP .

2) POP et IMAP pour le retrait du courrier :

POP (Post Office Protocol) : Le Post Office Protocol (POP) est un protocole Internet standard de la couche application utilisé par les clients de messagerie pour récupérer les e-mails d'un serveur de messagerie. POP version 3 (POP3) est la version couramment utilisée, et avec IMAP, les protocoles les plus courants pour la récupération des e-mails. Le but du protocole POP est de fournir un accès via un réseau IP (Internet Protocol) à une application cliente utilisateur à une boîte aux lettres (maildrop) maintenue sur un serveur de messagerie. Le protocole est défini par une série de demandes de commentaires (RFC), y compris la RFC 1939 qui définit la version 3 de POP. D'autres extensions et spécifications ont également été proposées pour prendre en charge les extensions générales ainsi que pour annoncer de manière organisée la prise en charge des commandes facultatives, telles que comme TOP et UIDL. POP3 est un protocole plus ancien qui a été initialement conçu pour être utilisé sur un seul ordinateur. Contrairement aux protocoles modernes qui utilisent la synchronisation bidirectionnelle, POP3 télécharge uniquement les e-mails du serveur, puis les

supprime du serveur. Cela signifie qu'une fois qu'un e-mail est téléchargé via POP3, il n'est accessible qu'à partir de l'appareil sur lequel il a été téléchargé. Si vous accédez à votre messagerie à partir de plusieurs appareils, POP3 n'est peut-être pas le meilleur choix [20].

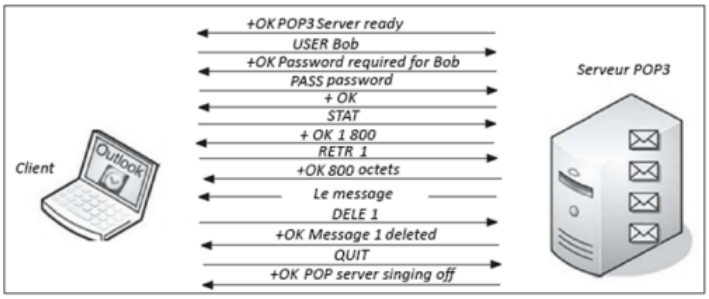


FIGURE 2.2 – Exemple de dialogue POP .

3) IMAP (Internet Message Access Protocol) :

Il est conçu pour permettre la gestion complète d'une boîte de messagerie par plusieurs clients de messagerie, ce qui signifie que les clients laissent généralement des messages sur le serveur jusqu'à ce que l'utilisateur les supprime explicitement. IMAP a été créé en 1986 par Mark Crispin en tant que protocole de boîte aux lettres d'accès à distance et est depuis devenu l'un des protocoles standard les plus répandus pour la récupération des e-mails, aux côtés de POP3 (Post Office Protocol). IMAP permet d'accéder aux parties de message MIME et à la récupération partielle, aux informations sur l'état des messages, à plusieurs boîtes aux lettres sur le serveur, aux recherches côté serveur, au mécanisme d'extension intégré et aux notifications push du serveur. Bien qu'il remédie à de nombreux défauts de POP, il introduit une complexité supplémentaire. Pour des raisons de sécurité, IMAPS sur le port TCP 993 peut être utilisé pour protéger de manière cryptographique les connexions IMAP entre le client et le serveur [23].

FIGURE 2.3 – Exemple de dialogue IMAP .

Faut-il choisir POP ou IMAP ? :

En général, les restrictions les plus courantes dans les e-mails sont variées selon la mobilité, l'accès multiple et l'espace de stockage. Pour voir, Analysons les deux réponses à ces contraintes :

–**Stockage :** En IMAP, le fait que les messages soient stockés à tendance à augmenter l'espace disque lorsqu'il est utilisé sur un serveur plutôt que sur un ordinateur peut être occupé par des messages dans un espace d'hébergement limité. Par conséquent, nous sommes obligés de supprimer certains messages de temps en temps, cela n'aide pas. POP a l'avantage que le courrier électronique peut être téléchargé sur le site. Un disque dur pouvant stocker autant d'e-mails que nécessaire vouloir.

– **Accès multiple :** le protocole POP permet un accès verrouillé au box. Autrement dit, aucune autre connexion n'est autorisée en même temps que le courrier. Vous êtes déjà connectés. Avec IMAP, en revanche, vous pouvez gérer plusieurs accès simultanés. Par exemple, lorsque plusieurs utilisateurs partagent une boîte aux lettres, elles Peuvent être consultées en même temps.

– **Mobilité :** Avec IMAP, vous pouvez gérer votre messagerie depuis n'importe quel appareil connecté à Internet, où que vous soyez. Pop pour l'instant peut restaurer vos messages sur votre appareil.

– **Connexion Internet :** Pour gérer IMAP, vous devez être connectés à IMAP. E-mail. Cela peut causer des problèmes si votre connexion Internet n'est pas stable. Pour cette partie, POP utilise uniquement la connexion pour télécharger les e-mails récents. Votre machine fonctionne bien même avec une connexion Internet très lente, mais votre connexion est une très petite limitation dans un monde de plus en plus en réseau.

En résumé, les deux protocoles sont équivalents et chacun a ses avantages. Ce que les autres n'ont pas, c'est un POP ou vous devez tenir compte de vos besoins concernant l'utilisation du courrier IMAP. et de vos ressources informatiques .

2.6 L'acheminement du courrier électronique :

L'acheminement du courrier électronique est le processus de transmission d'un e-mail d'un expéditeur à un ou plusieurs destinataires via un réseau informatique, généralement Internet. Le courrier électronique est envoyé en utilisant des protocoles de courrier électronique standard tels que SMTP (Simple Mail Transfer Protocol) pour l'envoi et POP3 (Post Office Protocol 3) ou IMAP (Internet Message Access Protocol) pour la réception.

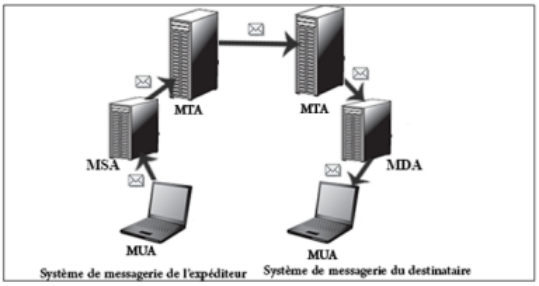


FIGURE 2.4 – L'acheminement du courrier électronique .

–Le MUA (Mail User Agent : client de messagerie)
Un Mail User Agent (MUA) est une application logicielle utilisée pour lire et gérer les messages électroniques. Il est également appelé client de messagerie ou lecteur de messagerie. Microsoft Outlook, Gmail et Apple Mail sont des exemples de MUA populaires. Le MUA permet aux utilisateurs de composer, envoyer, recevoir et organiser leurs messages électroniques. Il fournit également des fonctionnalités telles qu'un carnet d'adresses, la gestion des dossiers et le filtrage des spams. Le MUA communique avec un serveur de messagerie, soit via les protocoles standard SMTP, POP3 et IMAP, soit via un protocole propriétaire.

-Le MSA (Mail Submission Agent : agent de soumission de courrier) : Un agent de soumission de courrier électronique (MSA), ou agent de soumission de courrier, est un programme informatique ou un agent logiciel qui reçoit des messages électroniques d'un agent utilisateur de courrier (MUA) et coopère avec un agent de transfert de courrier (MTA) pour la livraison du courrier.

-Le MTA (Mail Transfert Agent : agent de Transfert de courrier) : Un agent de transfert de message (ATM) ou agent de transfert de courrier (MTA), est une application logicielle chargée de transférer des messages électroniques d'un ordinateur à un autre. Il reçoit le courrier entrant de l'agent d'utilisateur de messagerie (MUA) d'un utilisateur et transfère le courrier sortant pour livraison à un autre MTA ou au MUA d'un utilisateur. Le MTA utilise un protocole tel que le protocole SMTP (Simple Mail Transfer Protocol) pour échanger des messages avec d'autres MTA ou MUA. Certains exemples courants de MTA incluent Sendmail, Postfix et Microsoft Exchange.

–Le MDA (Mail Delivery Agent : agent de livraison du courrier) : Le facteur de réception du MDA par rapport au courrier postal est : Venez déposer le courrier dans votre boîte aux lettres.

Comment les différents agents communiquent entre eux ? Afin d'acheminer le courrier de l'éditeur au destinataire, divers mandataires doivent communiquer entre eux, pour cela, le message passant l'appel système Protocoles de messagerie : SMTP, POP et IMAP. Du MUA de l'expéditeur au dernier MTA traversé par le message, qui est Le protocole SMTP utilisé et celui que nous utilisons entre le MDA et le MUA du destinataire est appelé le protocole de réception IMAP ou POP. Autrement dit, le serveur de messagerie utilise SMTP pour le transport et recevoir, tandis que le client utilise SMTP pour envoyer et un autre Protocole de réception (POP ou IMAP).

2.7 Les principales solutions de messagerie

— **Cisco Webex :** Plateforme de collaboration en ligne permettant les réunions, la messagerie et le partage de fichiers en équipe. Il permet des réunions virtuelles avec des individus et des équipes, ainsi que des webinaires, et permet aux utilisateurs de partager facilement des fichiers et des écrans. De plus, Cisco Webex offre une intégration avec d'autres outils tels que Microsoft Teams et Slack. Cisco Webex est disponible pour Windows, macOS, iOS et Android, et peut être téléchargé à partir du site Web de Cisco ou des magasins d'applications. Cisco propose également un plan gratuit pour Webex qui est disponible dans certains pays et régions [30].
— **Google Workspace :** Solution de messagerie professionnelle de Google offrant des fonctionnalités comme Gmail, Google Drive, Google Docs et bien plus encore Google Workspace est une suite d'outils de productivité et de collaborations basés sur le cloud développés par Google. Il comprend une gamme d'applications Web telles que Gmail, Google Drive, Google Docs, Google Sheets, Google Slides et Google Meet ...
Google Workspace est conçu pour aider les équipes à travailler ensemble plus efficacement et à collaborer sur des projets en temps réel depuis n'importe où dans le monde. Il propose de différents plans tarifaires qui offrent de différentes fonctionnalités, stockage et options de support pour les entreprises de toutes tailles et de tous besoins, des petites startups aux grandes entreprises [1].
— **Zoho Mail :** Solution de messagerie professionnelle de Zoho offrant un stockage de messagerie en ligne sécurisé, un calendrier, un gestionnaire de tâches et une suite bureautique en ligne. Il est un service d'hébergement de messagerie pour les entreprises fourni par la société Zoho. Il offre une variété de fonctionnalités, notamment des adresses e-mail basées sur un domaine, l'intégration d'e-mails et de calendriers et une protection anti-spam. Il est disponible sur les plates-formes de bureau et mobiles, permettant aux utilisateurs de rester connectés et productifs lors de leurs déplacements. Le service est également personnalisable, avec des options de filtrage des e-mails, de signature d'e-mail personnalisée ... Zoho Mail propose un modèle de tarification à l'utilisation, sans contrat à long terme, une authentification des e-mails et d'autres fonctionnalités de sécurité pour garantir la sécurité des comptes de messagerie des utilisateurs [18].

— **Microsoft Exchange Server :** C'est un serveur de messagerie et un serveur de calendrier développé par Microsoft qui s'exécute exclusivement sur les systèmes d'exploitation Windows Server. Exchange Server est concédéré sous licence à la fois en tant que logiciel sur site et logiciel en tant que service (SaaS) (Software as a service), et Exchange Online est un Exchange Server fourni en tant que service cloud hébergé par Microsoft lui-même. En outre, Microsoft Exchange Server utilise un protocole propriétaire d'appel de procédure distante (RPC) appelé MAPI/RPC, qui a été conçu pour être utilisé par Microsoft Outlook [27].
— **Open Business Management OBM :** En affaires, OBM signifie « Online Business Manager ». Un gestionnaire d'entreprise en ligne est un professionnel de l'assistance virtuelle qui fournit une assistance au niveau de la gestion aux propriétaires d'entreprise en ligne. Leurs tâches peuvent varier, mais incluent souvent la gestion des opérations, des projets, des membres de l'équipe et des mesures. Ils peuvent aider les entreprises à se développer et à évoluer en rationalisant les processus, en mettant en œuvre des systèmes et l'automatisation, et en libérant du temps aux propriétaires d'entreprise pour se concentrer sur les tâches génératrices de revenus [21].

2.8 Quelle solution de messagerie choisir ?

Les solutions de messagerie ne manquent pas, chacune étant connue pour ses capacités. Pour notre projet, nous avons choisi Microsoft Exchange Server.

Pourquoi Exchange ?
Microsoft Exchange est une solution de messagerie adaptée à un environnement professionnel. Bien que les choix de solutions de messagerie semblent assez larges pour qu'en y regardant de plus près, on se rende vite compte qu'il est un outil dédié à la messagerie depuis sa création, porté par un géant comme Microsoft, il opère en utilisant la meilleure technologie stockage et routage, y compris Active Directory, un outil testé Temps et course pour rester en tête sur Les années 23 qui ont tendance à avoir une longueur d'avance sur les concurrents. Enfin, parce que dans la messagerie électronique, la sécurité est une priorité absolue, les enjeux pour la sécurité de

Microsoft Exchange Server sont privés, il met en place des systèmes de sécurité pour protéger les différentes données et relations qu'il gère. Le programme surveille tout, des contrôles d'accès stricts des appareils mobiles aux différentes autorisations d'utilisateur.

2.9 Conclusion

Le but de ce chapitre est de comprendre le fonctionnement de la messagerie Email et de choisir la solution de messagerie qui correspond le mieux à nos besoins. Autrement dit, le serveur Exchange. Cependant, même le meilleur logiciel ne suffit pas à vous protéger en faite face aux nombreuses menaces qui pèsent sur cette technologie.Dans le chapitre suivant, nous verrons plus en détails les dangers, les menaces de messagerie et un autre aspect de la politique de sécurité mis en place pour se protéger et fermer la porte pour empêcher toute tentative surtout le piratage dans un environnement Exchange Server 2019.

CHAPITRE 3

LA SÉCURITÉ DE LA MESSAGERIE ÉLECTRONIQUE

3.1 Introduction

La sécurité de la messagerie électronique est une préoccupation majeure dans le monde numérique d'aujourd'hui. Avec l'essor de la communication électronique, les courriels sont devenus un canal essentiel pour les échanges professionnels et personnels, mais ils sont également devenus une cible privilégiée pour les cybercriminels. L'enjeu de la sécurité de la messagerie est donc de protéger les informations sensibles et confidentielles transmises par courriel contre les menaces telles que les attaques de phishing, les logiciels malveillants, la perte de données et les violations de la vie privée. Dans cette optique, de nombreuses stratégies, pratiques et solutions technologiques ont été développées pour garantir la confidentialité, l'intégrité et l'authenticité des messages électroniques, assurant ainsi une communication sûre et fiable.

3.2 Définition de la sécurité informatique :

La sécurité informatique est l'ensemble des mesures, des technologies et des pratiques qui sont mises en place pour protéger les systèmes informatiques, les réseaux, les données et les utilisateurs contre les attaques, les dommages, les intrusions et les pertes d'informations. Elle vise à prévenir les menaces telles que les virus informatiques, les logiciels malveillants, les attaques de phishing, les attaques de déni de service, les vols de données et les violations de la confidentialité. La sécurité informatique implique souvent l'utilisation de logiciels de sécurité tels que des pare-feux, des antivirus, des antispam, des outils de chiffrement et des outils de détection d'intrusion. Elle implique également la mise en place de politiques de sécurité informatique et de pratiques de gestion des risques pour protéger les systèmes informatiques et les données contre les menaces [14].

3.3 Les objectifs de la sécurité de la messagerie électronique

1) Confidentialité : l'objectif principal de la sécurité de la messagerie électronique est de protéger le contenu des messages contre les accès non autorisés. Le contenu du message doit être illisible pour toute personne autre que le destinataire légitime.

2) Intégrité : il est important de s'assurer que le contenu du message n'a pas été modifié ou altéré pendant la transmission. L'objectif de l'intégrité est de garantir que le message est arrivé dans son état d'origine.
3) Disponibilité : la sécurité de la messagerie électronique doit garantir que les messages sont disponibles pour les destinataires légitimes lorsqu'ils en ont besoin. Il ne doit pas y avoir de déni de service ou de perturbation de la disponibilité des messages.
4) Authenticité : l'objectif de l'authenticité est de s'assurer que le message provient de la personne ou de l'entité prétendant l'avoir envoyé. Elle peut être assurée à l'aide de signatures électroniques, de certificats numériques ou d'autres méthodes d'authentification.
5) Non-répudiation : l'objectif de la non-répudiation est de garantir que l'expéditeur ne peut pas nier avoir envoyé un message une fois qu'il a été envoyé. Cela est important dans les transactions commerciales ou légales, où la preuve de l'envoi et de la réception des messages est essentielle.
6) Protection contre les menaces internes et externes : garantir que les messages ne sont pas compromis par des acteurs malveillants, tels que des virus, des logiciels malveillants, des attaques de phishing ou des attaques de type homme du milieu [2][14].

3.4 Vulnérabilités de la messagerie électronique

Il existe plusieurs types de menaces et risques que nous pouvons segmenter par rapport à leur niveau potentiel en trois problématiques :
- La sécurisation des messages autorisés au sein de l'entreprise .
- La sécurisation de l'infrastructure sur laquelle repose le système d'échange.
- La définition des règles d'utilisation du système de messagerie de l'entreprise.

3.4.1 Les atteintes aux flux identifiés par l'entreprise comme légitimes/autorisés :

Il y a deux scénarios :
-La perte d'un e-mail au cours de sa transmission, due à plusieurs éléments qui créent le problème du serveur, suppression par oubli ou à tort par un anti spam.

- La disparition d'un ou de tous les messages reçus, c'est surtout lorsqu'on stocke les e-mails dans son propre ordinateur.

1) Perte de confidentialité :

Elle peut être due à plusieurs événements :

· Une divulgation accidentelle.

· Une divulgation par négligence ou méconnaissance des règles.

· Une divulgation volontaire.

· Un espionnage des messages lors de la transmission sur un réseau local à partir d'un logiciel spécialisé « SNIFFER ».

2) Perte d'intégrité :

Un message peut être altéré accidentellement (par dysfonctionnement d'équipements, modification de format) ou par malveillance pendant sa transmission ou son stockage dans un serveur de messagerie ou sur le poste destinataire, cette perte peut également provenir de modifications, de suppressions ou d'ajouts volontaires effectués au niveau du serveur.

3) Usurpation de l'identité de l'émetteur :

Dans un système de messagerie, l'adresse e-mail est un élément vulnérable car elle est diffusée à tous les destinataires et est stockée dans des milliers de carnets d'adresses ; des gens ou organisations malveillants exploitent des failles de sécurité via des vers ou des virus pour récupérer ces adresses en accédant aux données personnelles de l'utilisateur et dans son carnet d'adresse lors de divulgation sur le web.

4) Répudiation :

C'est le risque de reniement de l'envoi ou de la réception d'un message, c'est qu'on n'a pas de garantie sur l'émission ou la réception d'un message.

3.4.2 Les atteintes à l'infrastructure et au système d'information :

1)Programme malveillant :

La messagerie permet d'introduire les fichiers dans un ordinateur donc c'est un bon vecteur de diffusion des programmes malveillants (Virus, Cheval de Troie et Spyware ...), alors on a trois types d'attaque :

· L'introduction d'un virus par le biais d'une pièce jointe, en contenant des instructions exécutables avec extension (.exe, .dll, .bat, .vbs, ...).

· L'introduction d'un code malicieux dans le corps du message, lorsque celui-ci est dans un format de page web incluant des scripts.

· L'introduction des faux virus (hoax) qui propagent de fausses informations ou qui font perdre inutilement le temps de lecture aux destinataires [9].

2)Spam :

Le spam est l'opération qui consiste à inonder les boîtes aux lettres (BAL) de courriers indésirables et non sollicités, son but est soit la publicité pour les sites marchands plus ou moins recommandables, soit simplement de nuire aux systèmes de messagerie par saturation des réseaux et des BAL (mail bombing).

3) L'interruption de service :

C'est l'indisponibilité du service de messagerie alors qu'elle fait partie intégrante du processus de l'entreprise, elle peut être accidentelle ou malveillante (panne, destruction de locaux et déni de service), elle peut provenir d'une inscription en Black-list suite à des attaques opérées à partir des serveurs de l'entreprise.(* 24 Club de la sécurité des systèmes d'information Français, Op. cit).

3.5 Les mécanismes de sécurité

3.5.1 La cryptographie

La cryptographie est une technique d'écriture qui consiste à rédiger un message crypté, via l'utilisation de codes secrets ou de clés de décryptage. Elle est principalement utilisée pour protéger un message jugé confidentiel. La cryptologie est la théorie qui étudie les techniques de la cryptographie et de la cryptanalyse.

a) Le chiffrement :

Le chiffrement est un procédé de cryptographie qui permet de rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement. Le terme « chiffrement » est utilisé depuis le XVIIe siècle dans le sens de chiffrer un message. L'opération inverse, qui suppose que l'on connaisse la clé, est donc le « déchiffrement ». Le chiffrement est un moyen de brouiller les données afin que seules les parties autorisées puissent comprendre les informations.

-Le chiffrement asymétrique :

Le chiffrement asymétrique est un procédé de cryptographie qui utilise des

clés différentes : une paire composée d'une clé publique, servant au chiffrement, et d'une clé privée, servant à déchiffrer. Le point fondamental soutenant cette décomposition publique/privée est l'impossibilité calculatoire de déduire la clé privée de la clé publique.

-Le chiffrement symétrique

C'est un algorithme cryptographique qui utilise la même clé secrète pour le chiffrement et pour le déchiffrement d'un message. Il s'agit d'une clé partagée. Le chiffrement symétrique est particulièrement rapide mais nécessite que l'émetteur et le destinataire se mettent d'accord sur une clé secrète commune ou se la transmettent par un autre canal.

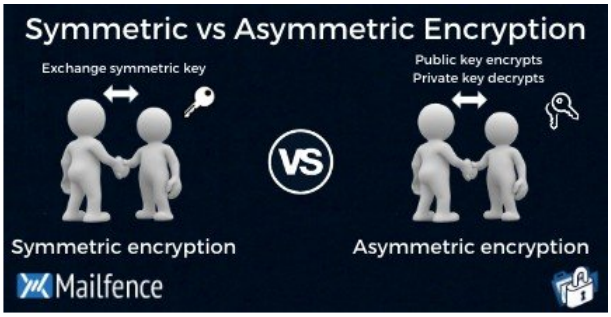


FIGURE 3.1 – Le chiffrement asymetrique et symetrique.

b) La signature numérique :

La signature numérique est un procédé cryptographique qui permet de garantir l'intégrité et l'authenticité d'un document électronique. Elle est utilisée pour s'assurer que le document n'a pas été modifié depuis sa signature et que l'auteur de la signature est bien celui qu'il prétend être [15].

-Le principe de la signature numérique :

Le principe de fonctionnement de la signature numérique est le suivant :

• Le document à signer est haché à l'aide d'une fonction de hachage cryptographique pour obtenir une empreinte unique du document.

• L'empreinte est ensuite chiffrée à l'aide de la clé privée de l'auteur de la signature pour obtenir la signature numérique.

• Le document signé et la signature numérique sont ensuite transmis au destinataire.

* Le destinataire peut vérifier l'intégrité et l'authenticité du document en effectuant les étapes suivantes :

• Il hache le document à l'aide de la même fonction de hachage crypto-

graphique pour obtenir une empreinte unique du document.
• Il déchiffre la signature numérique à l'aide de la clé publique de l'auteur de la signature pour obtenir l'empreinte originale.
• Il compare l'empreinte originale avec l'empreinte calculée à partir du document pour s'assurer que le document n'a pas été modifié depuis sa signature et que l'auteur de la signature est bien celui qu'il prétend être [9].

3.6 protocole S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) est un protocole de cryptographie et de signature numérique de courriels encapsulés au format MIME. Il assure l'intégrité, l'authentification, la non-répudiation et la confidentialité des données. S/MIME est une méthode largement acceptée pour envoyer des messages signés numériquement et chiffrés [24].

3.6.1 fonctionnement du protocole S/MIME

Le S/MIME est basé sur la cryptographie asymétrique qui fonctionne avec une paire de clés mathématiquement liées : une clé publique et une clé privée. Sur le plan informatique, il est impossible de déterminer la clé privée à partir de la clé publique. Les e-mails sont chiffrés à l'aide de la clé publique du destinataire. Le destinataire utilise ensuite sa clé privée pour déchiffrer le message. Il est largement utilisé pour envoyer des messages signés numériquement et chiffrés.

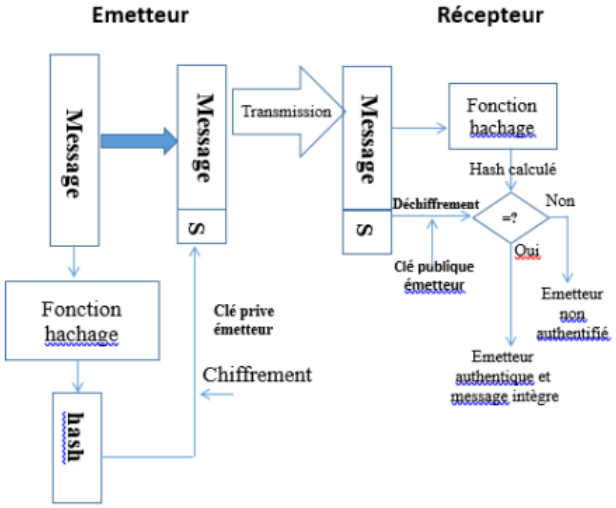


FIGURE 3.2 – fonctionnement du protocole S/MIME .

3.6.2 Protocole PGP

Le protocole PGP (Pretty Good Privacy) est un protocole de sécurité qui permet de garantir la confidentialité et l'authentification pour la communication des données. Il est souvent utilisé pour la signature de données, le chiffrement et le déchiffrement des textes, des courriels, fichiers, répertoires et partitions de disque entier pour accroître la sécurité des communications par courriel [24].

-Le fonctionnement de PGP pour assurer la confidentialité des données est le suivant :

1. PGP génère une paire de clés : une clé publique, qui ne sert qu'à chiffrer, et une clé privée, également appelée clé de session, qui sert à déchiffrer.
2. Le destinataire de l'e-mail transmet la clé publique à ses contacts.
3. Le contact utilise la clé publique pour chiffrer l'e-mail, puis l'envoie.
4. Le destinataire utilise sa clé privée, dont il est seul détenteur, pour déchiffrer l'e-mail.

3.6.3 Protocole SSl

Le protocole SSL (Secure Sockets Layer) est un protocole de chiffrement utilisé pour sécuriser les communications sur Internet. Il a été remplacé par

le protocole TLS (Transport Layer Security), qui est une version plus récente et plus sûre. La négociation SSL (également appelée handshake) est le processus qui amorce une session de communication utilisant le chiffrement SSL. Elle se compose d'une série de datagrammes (ou messages) échangés par un client et un serveur. Elle implique plusieurs étapes, car le client et le serveur échangent les informations nécessaires pour terminer la négociation et rendre la conversation possible [29].

-Protocole tls (phase de negociation) : C'est la phase au cours de laquelle les parties négocient les paramètres de connexion et effectuent l'authentification, la 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.

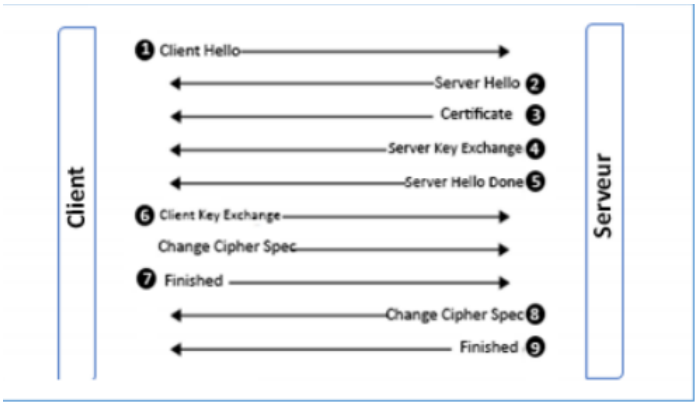


FIGURE 3.3 – Fonctionnement du protocole S/MIME .

-SSl pour le web : http

utiliser HTTPS sur votre site Web, vous devez disposer d'un certificat SSL ou TLS installé sur votre site Web. SSL signifie « Secure Sockets Layer », c'est un protocole de sécurité qui crée un lien chiffré entre un serveur Web et un navigateur Web3. Les entreprises doivent ajouter des certificats SSL à leur site Web pour sécuriser les transactions en ligne et sécuriser la confidentialité des informations client.

3.7 La sécurité de la messagerie Exchange

3.7.1 La sécurité de transport des messages

Les e-mails transitent par différents appareils avant d'atteindre leur destination, et peuvent être soumis à divers risques. Transport de courrier basé sur protocoles SMTP, Pop et http, mais ces protocoles permettent la transmission de E-mail en texte clair sur le Web. Par conséquent, afin de vous protéger, il est nécessaire d'établir Canal de transmission sécurisé et crypté. Pour la sécurité des échanges internes Échange Nous allons créer un canal de transmission sécurisé via le protocole TLS encapsule les protocoles d'échange d'e-mails et protège Communication entre les MTA et entre les serveurs de messagerie et les clients ... Assurer la transmission sécurisée des e-mails.

3.7.2 La protection du contenu des Emails

Les entreprises utilisent souvent le courrier électronique pour échanger des informations sensibles telles que des rapports financiers, des analyses de performances, informations sur la concurrence, les clients et les employés .... Par conséquent, les informations peuvent constituer une menace sérieuse pour l'entreprise et entraîner des pertes financières, une détérioration de l'image de l'entreprise et la relation avec les clients et la perte d'avantage concurrentiel ... Par conséquent, il est crucial de protéger le contenu des e-mails contre la divulgation et la modification. Pour cela, nous allons combiner deux technologies différentes : S/MIME et IRM au sein de l'organisation Exchange.

Le protcole SSL assure déjà le chiffrement de la communication, pourquoi utiliser un autre mécanisme ?

Il ne faut pas confondre protection Communication protégée par contenu, données protégées par SSL pendant leur expédition, mais une fois que vous recevez quelque chose dans la boîte aux lettres sa confidentialité et son intégrité sont garanties.

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

La gestion des droits relatifs à l'information (IRM) est un outil qui permet de restreindre l'accès aux documents sensibles en empêchant leur impression, leur transfert ou leur copie par des personnes non autorisées. Les autorisations sont stockées dans le document où elles sont authentifiées par un serveur IRM. L'IRM est disponible sur Windows, MacOS, iOS et Android. Vous pouvez utiliser Rights Management d'informations dans Word pour restreindre l'accès aux documents.

S/MIME permet déjà de protéger le contenu de l'email ?
Les messages S/MIME sont protégés non seulement en transit, mais également au sein de l'application de messagerie de l'utilisateur, offrant un degré élevé de protection des messages entre l'expéditeur et le destinataire. Mais dès que l'e-mail est déchiffré, la protection est supprimée ne persiste pas et vous ne pouvez pas contrôler ce que le destinataire peut en faire les informations qu'il contient.

3.8 La protection contre les pertes de données

La protection contre les pertes de données (DLP) est une stratégie pour s'assurer que les données sensibles ou confidentielles ne sont pas perdues, volées ou accidentellement divulguées. Elle permet d'identifier l'endroit où les données sont en danger, puis de prendre des mesures pour les protéger. Il existe plusieurs outils pour protéger les données sensibles, tels que la protection contre les pertes de données (DLP), la gestion des droits relatifs à l'information (IRM) et le chiffrement des emails avec S/MIME.

3.8.1 Le DAG, Le load Balacing et le Safety Net

Le DAG (Directed Acyclic Graph) est une structure de données qui est utilisée pour représenter les dépendances entre les tâches. Le load balancing est une technique qui permet de distribuer la charge de travail sur plusieurs ressources informatiques. Le Safety Net est un mécanisme de sécurité qui permet de récupérer des données en cas de perte ou de corruption.

3.8.2 La sauvegarde et la restauration

Exchange Server 2019 automatise le processus de protection et de récupération des données du serveur utilisant la technologie de haute disponibilité. Mais il panne matérielle, erreur humaine ou même catastrophes naturelles. La récupération peut nécessiter une intervention manuelle, effacer les données et restaurer le système à l'état de fonctionnement normal. Echange 2013 fournit aux administrateurs une variété de mécanismes pour sauvegarder et restaurer les bases de données et les mécanismes nécessaires pour assurer la reprise après sinistre .

3.9 Conclusion

Le courrier électronique est l'un des nombreux domaines où la technologie ne peut à elle seule fournir une solution de sécurité complète. Une messagerie sécurisée dépend largement de la responsabilité de l'utilisateur et de l'efficacité des solutions de sécurité fournies par l'administrateur de messagerie. Alors nous allons à présent passer au quatrième chapitre 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

4.1 Introduction

Ce chapitre sera consacré pour la partie pratique de notre projet qui a été au sein de l'entreprise EGITEL, ou nous allons essayer d'expliquer pas par pas la démarche à suivre pour la mise en œuvre d'une solution de messagerie, nous allons apprendre à mettre en place un serveur de messagerie Microsoft Exchange Server 2019 sous Windows Server 2022. Vous pouvez aussi l'installer sur Windows Server 2019 (mais pas une version plus ancienne). Même si Microsoft 365 est une solution très à la mode et qu'elle intègre Exchange Online, de nombreuses entreprises se tournent encore vers un serveur de messagerie Exchange "classique". D'ailleurs, Microsoft souhaite poursuivre l'aventure avec Exchange puisqu'une nouvelle version est prévue pour 2025 afin de prendre le relais avec Exchange Server 2019.

Voici quelques informations sur la VM qui va accueillir Exchange 2019 :
Nom : AZ-EXCHANGE
Adresse IP : 10.10.100.211/24
Système d'exploitation : Windows Server 2022 Datacenter.
RAM : 16 Go
vCPU : 4
Stockage : un volume NTFS pour le système et un volume ReFS pour la base de données et les logs.

Microsoft Exchange est un sujet très vaste. Dans cet article, nous nous concentrons sur les prérequis, la préparation du serveur, l'installation et une première connexion sur les différentes consoles.

4.2 Présentation de l'environnement de travail

1- Définition de GNS3 :

GNS3, ou Graphical Network Simulator 3, est un logiciel de virtualisation de réseaux largement utilisé dans le domaine des technologies de l'information. Il permet aux professionnels des réseaux de créer des topologies de réseaux virtuelles en utilisant des images d'équipements réseaux réels

(tels que des routeurs, des commutateurs et des pare-feu ...) pour simuler et tester des configurations de réseaux. GNS3 est un outil précieux pour l'apprentissage, la formation et le développement de solutions réseau, car il permet aux utilisateurs de concevoir, configurer et dépanner des réseaux informatiques de manière pratique et sans avoir besoin d'équipements matériels coûteux.

2- Définition de VMWAR

VMware est une société informatique qui propose une gamme de solutions de virtualisation, de gestion de cloud et d'infrastructure logicielle. Le terme "VMware" est souvent associé à VMware vSphere, l'un de leurs produits phares, qui permet la création et la gestion des machines virtuelles (VM) sur des serveurs physiques. Les VM sont des environnements informatiques isolés et autonomes qui fonctionnent sur un même serveur physique, ce qui permet de maximiser l'utilisation des ressources matérielles et de simplifier la gestion des systèmes informatiques. En résumé, VMware facilite la virtualisation des infrastructures informatiques pour améliorer l'efficacité, la flexibilité et la gestion des environnements de serveurs.

3- Définition de Windows serveur 2022

Windows Server 2022 est la dernière version du système d'exploitation serveur de Microsoft, conçue pour fournir des services informatiques aux entreprises. Il offre des fonctionnalités avancées de gestion, de stockage, de sécurité et de virtualisation pour soutenir les besoins de l'entreprise en matière d'informatique serveur.

4- iOs Web

iOS Web est un terme généralement utilisé pour désigner les applications web spécialement conçues pour fonctionner sur les appareils Apple, tels que l'iPhone et l'iPad. Ces applications web sont accessibles via un navigateur web sur les dispositifs iOS et sont souvent optimisées pour une expérience utilisateur mobile. Elles offrent généralement un accès à des

services en ligne, des informations ou des fonctionnalités via Internet sans nécessiter de téléchargement ou d'installation depuis l'App Store.

5- Exchange 2019

Exchange 2019 est la version de Microsoft Exchange Server sortie en 2018, et c'est une solution de messagerie et de collaboration pour les entreprises. Elle permet aux utilisateurs de gérer leurs courriels, calendriers, contacts et tâches, tout en offrant des fonctionnalités avancées de sécurité, de gestion des boîtes aux lettres et de communication. Exchange 2019 est conçu pour être déployé localement sur les serveurs de l'entreprise, offrant ainsi un contrôle total sur l'infrastructure de messagerie.

4.3 Présentation de l'architecture proposée

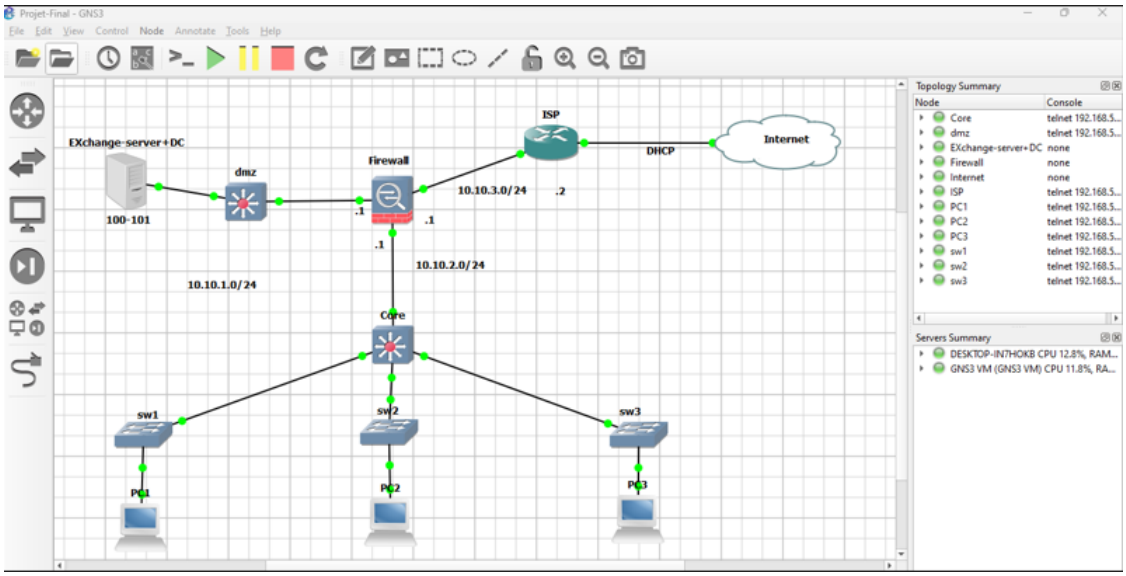


FIGURE 4.1 – Architecture proposée pour simuler le travail

Pour concevoir et déployer notre architecture, nous avons opté pour l'environnement de virtualisation VMware Workstation pour héberger nos machines clientes et nos serveurs. L'architacture est constituée des machines suivantes :

-Serveur DC (domain controlleur) : Il fait office d'un contrôleur de domaine ActiveDirectory, d'un serveur AD , d'une autorité de certification ainsi qu'un serveur DNS avec un nom de domaine .

-Serveur Exchange : Serveur Exchange 2013 disposant des rôles serveur d'accès client et boîtes aux lettres et dans le cadre de la haute disponibilité et de la sécurité de la messagerie.

4.4 Tableau d adressage des réseaux

Type	Adresse réseaux	Adresse	Type
DMZ	10.10.1 .0/24	255.255.255.0	1
LAN	10.10.2.0/24	255.255.255.0	1
WAN	10.10.3.0/24	255.255.255.0	2

FIGURE 4.2 – Tableau d'adressage des réseaux

4.5 Tableau d'adressage des équipements

Nom d'équipement	Interface	Adresse IP	Le masque	Gateway
Firewall	DMZ	10.10.1.1	255.255.255.0	/
	LAN	10.10.2.1	255.255.255.0	/
	WAN	10.10.3.1	255.255.255.0	/
Serveur	CART1	10.10.1.100	255.255.255.0	1

FIGURE 4.3 – Tableau d'adressage des équipements

4.6 Prérequis Microsoft Exchange 2019

Avant d'installer Microsoft Exchange 2019 (ou une autre version), il convient de prendre connaissance de certains prérequis. C'est ce que nous vous proposons en premier lieu. Ensuite, nous allons passer à la phase de préparation du serveur Exchange, toujours avant d'installer Exchange en lui-même.

*** Prérequis pour le stockage Exchange**

Exchange Server supporte aussi bien les volumes formatés en NTFS qu'en ReFS, en fonction de l'usage qui est fait du volume, car ReFS n'est pas utilisable pour le système et les binaires d'Exchange. Dans la documentation de Microsoft, on peut lire :

* Au moins 30 Go de libres sur la partition où est installé Exchange.
* Au moins 200 Mo de libres sur la partition du système.
* Au moins 500 Mo de libres sur la partition qui contient la base de données de file d'attente des messages.

En réalité, il faudra prévoir beaucoup plus large en espace disque pour la base de données : tout dépend du nombre d'utilisateurs et de leur manière d'utiliser la messagerie..

*** Créer les enregistrements DNS (MX) correspondants à ce serveur Exchange**

Vous devez configurer les enregistrements DNS suivants pour que votre serveur Exchange soit localisable. Les valeurs ci-dessous sont données à titre d'exemple.

L'idéal étant d'avoir des enregistrements DNS différents pour les accès publics et pour les accès privés. Quand l'accès provient de l'extérieur, on fera en sorte de résoudre sur l'adresse IP publique sur laquelle est joignable votre serveur Exchange (à moins que vous utilisiez un service tiers pour l'analyse des e-mails), tandis pour que quand l'accès provient de l'intérieur (exemple : un PC avec Outlook connecté au réseau local), on fera en sorte de faire la résolution de noms avec l'adresse IP privée.

Avec PowerShell, vous pouvez vérifier les enregistrements DNS :

*** Resolve-DnsName -Type A mail.domaine.fr | ft -AutoSize**

*** Resolve-DnsName -Type MX domaine.fr | ft -AutoSize**

***Le futur serveur Exchange doit être membre du domaine Active Directory.**

*** Add-Computer -DomainName domaine.local**.

Les contrôleurs de domaine Active Directory de la forêt doivent exécuter Windows Server 2012 R2 au minimum et La forêt Active Directory doit avoir un niveau fonctionnel en "Windows Server 2012 R2" au minimum.

*** Get-ADForest | fl Name,ForestMode**

*** Microsoft Outlook 2013 au minimum, que ce soit sur Windows ou macOS, afin d'être compatible Exchange 2019** .

Il y a également des composants et fonctionnalités de Windows Server à installer sur le serveur de messagerie avant de lancer l'installation de Microsoft Exchange. Ceux sont, en quelque sorte, des prérequis. Nous allons voir quels sont ces éléments et comment les installer dans l'étape suivante. Pour des détails supplémentaires sur les prérequis, consultez cette documentation :

*** Microsoft Learn - Exchange Server system requirements** .

4.7 Préparer le futur serveur de messagerie

Sur le serveur de messagerie sur lequel Microsoft Exchange 2019 va être installé, nous devons installer certains composants. Voici les étapes à réaliser :

A. Installer .NET Framework 4.8

Le premier composant à installer, c'est .NET Framework 4.8. Toutefois, sur Windows Server 2022 il est déjà installé donc c'est inutile d'essayer de l'installer à nouveau. Au cas où vous l'auriez supprimé, voici le lien :
Télécharger .NET Framework 4.8

B. Installer Visual C++ Redistributable Package

Vous devez installer sur le serveur Visual C++ Redistributable Package pour Visual Studio 2012 et Visual Studio 2013. Voici les liens de téléchargements :
Télécharger Visual C++ Visual Studio 2012
Télécharger Visual C++ Visual Studio 2013

C. Installer UCM API 4.0

Vous devez installer le runtime "Unified Communications Managed API 4.0" sur le serveur également. Le téléchargement s'effectue aussi depuis le site Microsoft, via ce lien :
*** Télécharger Unified Communications Managed API 4.0 Runtime**

D. Installer des composants de Windows Server

Microsoft Exchange a besoin de nombreux composants de Windows Server. Pour les installer, le plus simple est d'utiliser une console PowerShell et d'exécuter la commande "Install-WindowsFeature" avec la liste des fonctionnalités à installer. Par exemple, il y a des consoles d'administration ainsi que des fonctionnalités propres à IIS (serveur Web pour le Webmail Exchange).
Personnellement, je préfère réaliser toutes les étapes préparatoires avant d'installer Exchange, mais sachez que celle-ci peut être réalisée pendant l'installation d'Exchange, car c'est proposé par l'assistant.

Voici la commande à exécuter sur un serveur Windows Server avec une interface graphique :

Install-WindowsFeature Server-Media-Foundation, NET-Framework-45-Features, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering -CmdInterface, RSAT-Clustering-Mgmt, RSAT-Clustering-PowerShell, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation, RSAT-ADDS

Sur un Server Core, la liste est légèrement différente. Voici la commande à exécuter :

Install-WindowsFeature Server-Media-Foundation, NET-Framework-45-Features, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-Clustering-PowerShell, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth,
Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Metabase, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, RSAT-ADDS

L'installation prend quelques minutes... Un peu de patience. Il n'est pas nécessaire de redémarrer le serveur à la fin de l'installation.

E. Installation d'URL Rewrite pour IIS

Avant-dernière étape de préparation : l'installation du module "URL Rewrite 2.1" pour IIS. Le Webmail d'Exchange a besoin de ce composant pour fonctionner. Il suffit de télécharger le package d'installation et d'installer le module en quelques clics.

F. Installer les dernières mises à jour du système

Vous devez installer les dernières mises à jour cumulatives sur votre serveur avant de procéder à l'installation de Microsoft Exchange. Un tour dans Windows Update suffira pour lancer une recherche de mises à jour.

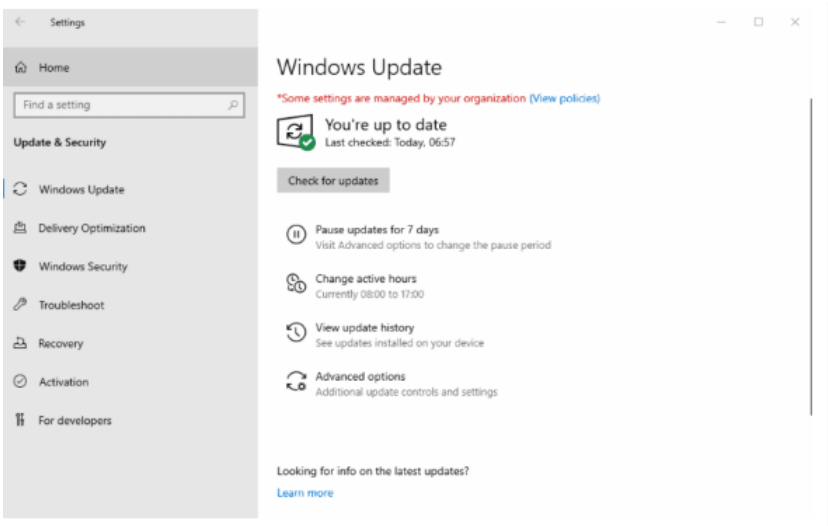


FIGURE 4.4 – Installer les dernières mises à jour du système.

4.8 Installation de Microsoft Exchange 2019

Avant de continuer : nous allons nous connecter sur notre serveur Exchange avec un compte "Administrateur du domaine". Je vous recommande aussi de redémarrer le serveur avant de procéder à l'installation (au cas où un reboot serait en attente suite à une mise à jour, par exemple).

Pour réaliser l'installation de Microsoft Exchange 2019, vous devez télécharger les sources. Utilisez un site officiel de Microsoft pour réaliser cette action. Voici un lien :

*** Télécharger - Microsoft Exchange 2019 - Cumulative Update 12**.

L'ISO d'installation de Microsoft Exchange 2019 pèse environ 5,8 Go. Pour ce tutoriel, j'utilise l'image ISO suivante **"Exchange Server 2019 Cumulative Update 12".** Commencer par monter l'image ISO via un double-clic. Accédez à l'image disque. Exécutez le **"setup"** en tant qu'administrateur

via un clic droi **"Exécuter en tant qu'administrateur"** .

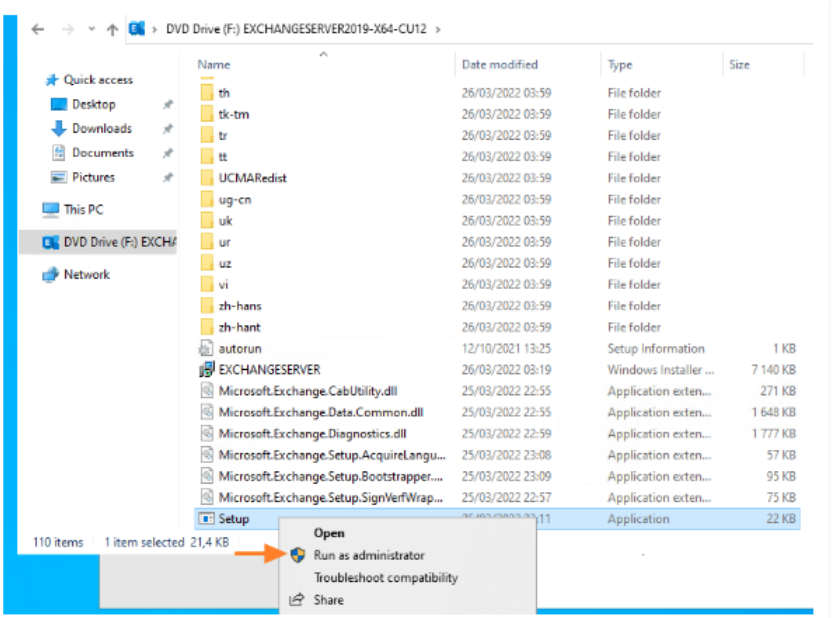


FIGURE 4.5 – Installer les dernières mises à jour du système.

Choisissez "Connect to the internet and check for updates" lorsque la première étape s'affiche. L'objectif étant de vérifier s'il y a une mise à jour plus récente. À ce jour, c'est non, car c'est la version la plus récente.

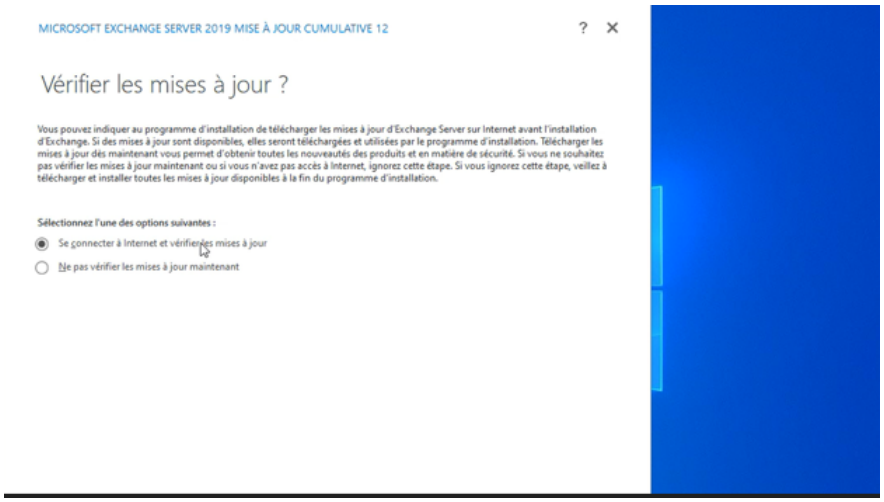


FIGURE 4.6 – Vérifier les mise à jou .

Poursuivez. L'étape **"Copying files"** apparaît : patientez pendant la copie des fichiers.

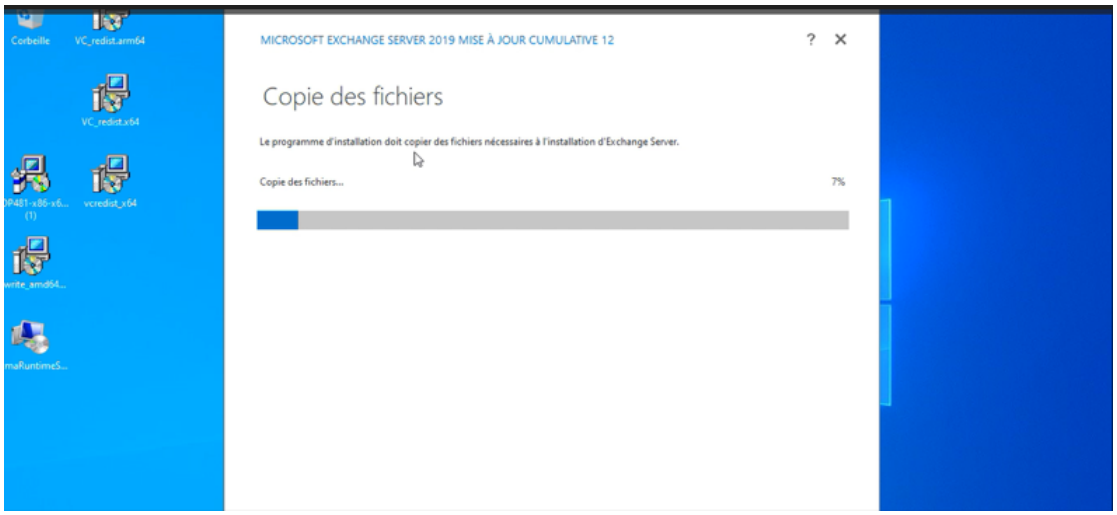


FIGURE 4.7 – Copier les fichier pour l'installation de Exchange .

Une fois que c'est fait, l'étape **"Introduction"** apparaît. Poursuivez.

Acceptez la licence (première ou deuxième option) et continuez

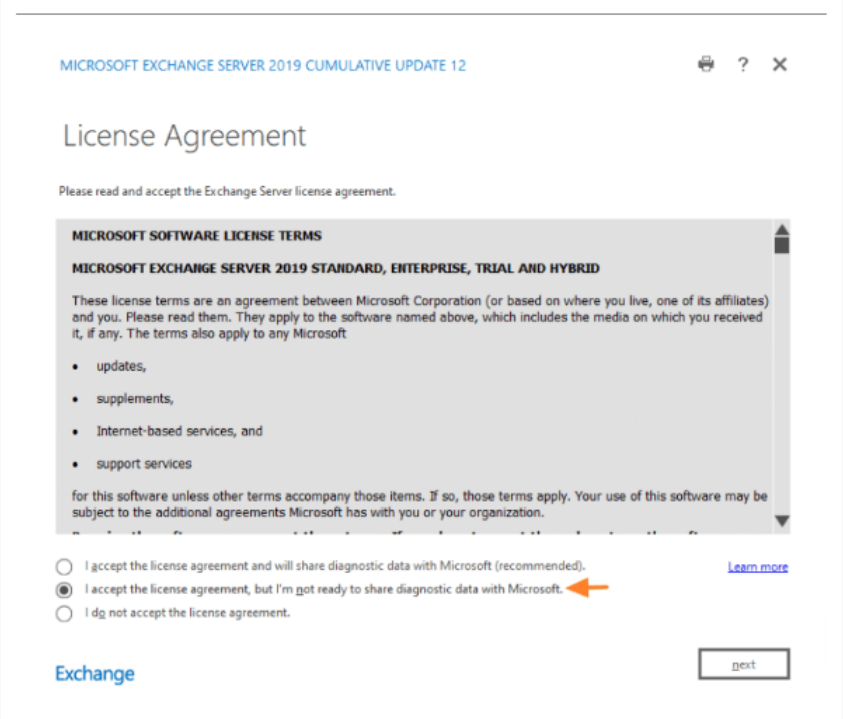


FIGURE 4.8 – Utiliser les paramètres d'installation recommandés .

Cochez l'option **"Use recommended settings"** pour utiliser les paramètres d'installation recommandés. Pour tout configurer, partez sur la seconde option :

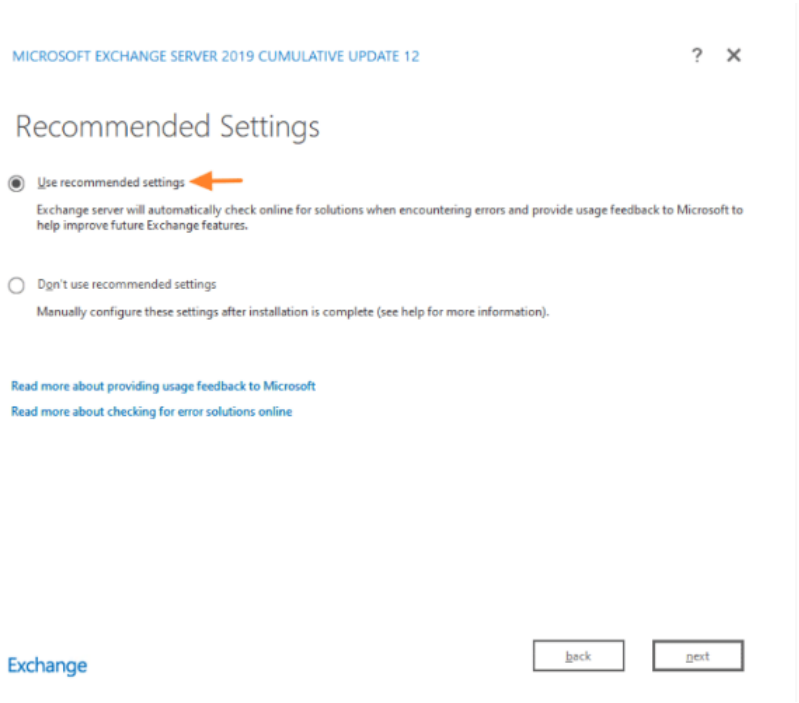


FIGURE 4.9 – Choose Use recommended settings.

Au moment de choisir les rôles, sélectionnez **"Mailbox role"** , car il s'agit du premier serveur de notre environnement Exchange. L'option **"Automatically install Windows Server roles and features that are required to install Exchange Server"** n'est pas nécessaire, car nous avons déjà installé les différents rôles avec la commande PowerShell exécutée lors de la préparation du serveur.

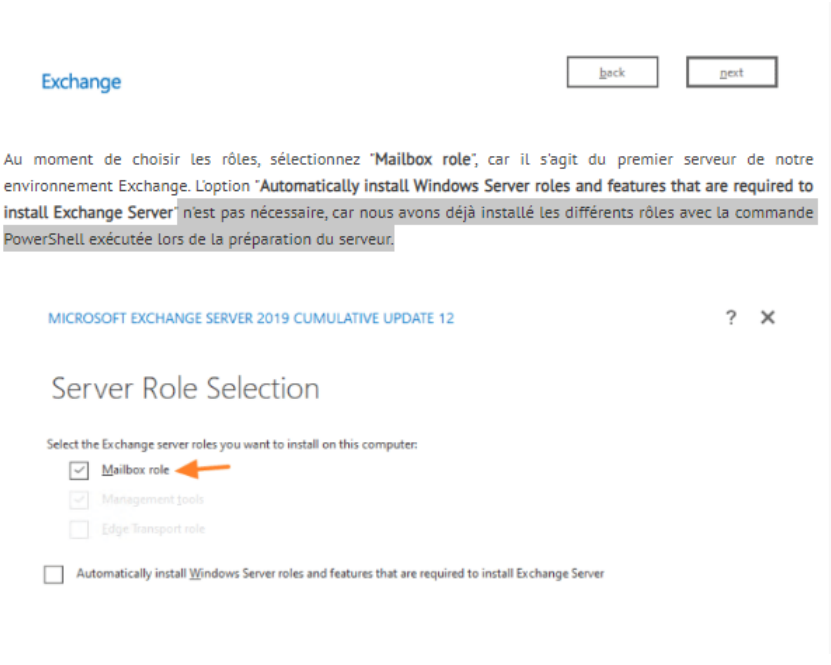


FIGURE 4.10 – Choisir Mailbox role.

Exchange Server en lui-même va s'installer dans "C :" et nécessite 5,7 Go d'espace disque.

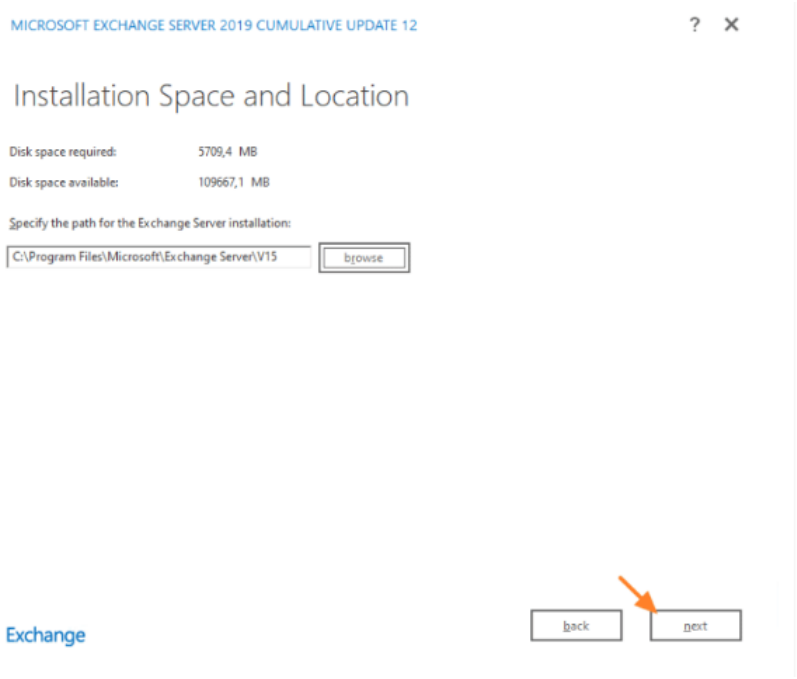


FIGURE 4.11 – Installation de Exchange Server.

Nommez l'organisation Exchange, ce qui sera probablement le nom de votre entreprise. L'option **"Apply Active Directory split permissions security model to the Exchange organization"** est nécessaire principalement avec des services informatiques où il y a une répartition des rôles. Par exemple, si la personne qui administre l'Active Directory n'est pas la même que celle qui gère l'Exchange.

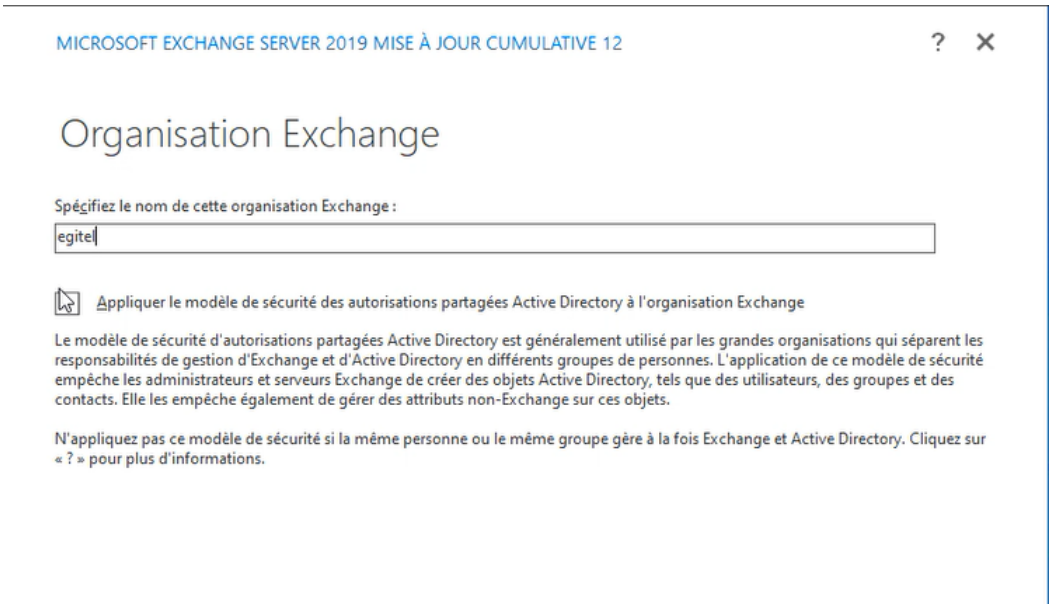


FIGURE 4.12 – Nommez l'organisation Exchange .

Laissez cette option sur **"No"** pour que **la protection anti-malware reste active.** Ici, on vous propose de la désactiver. Cela peut s'avérer utile si vous avez déjà une autre solution qui effectue ce travail à la place d'Exchange.

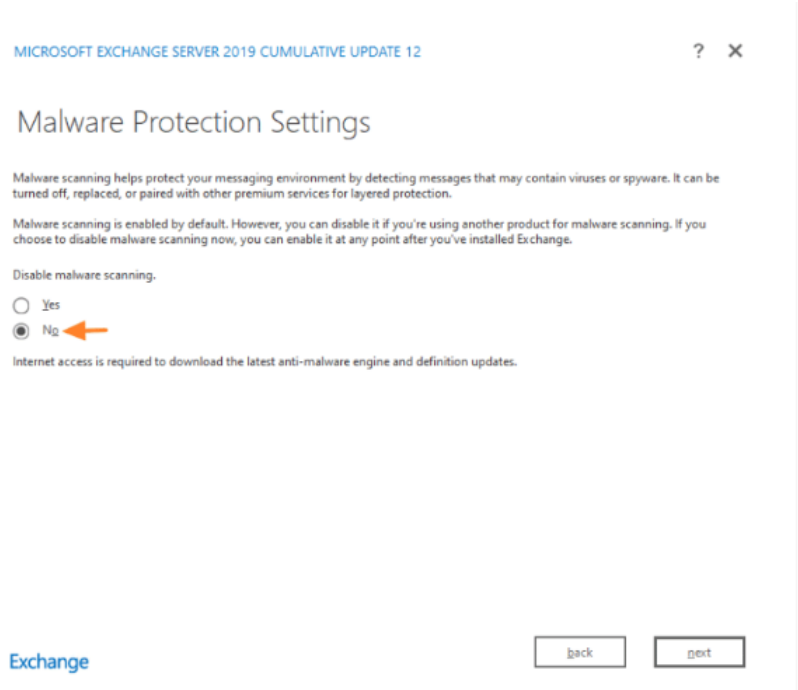


FIGURE 4.13 – Pour la protection anti-malware reste active.

Avant de lancer l'installation, le setup vérifie si vous respectez les différents prérequis...

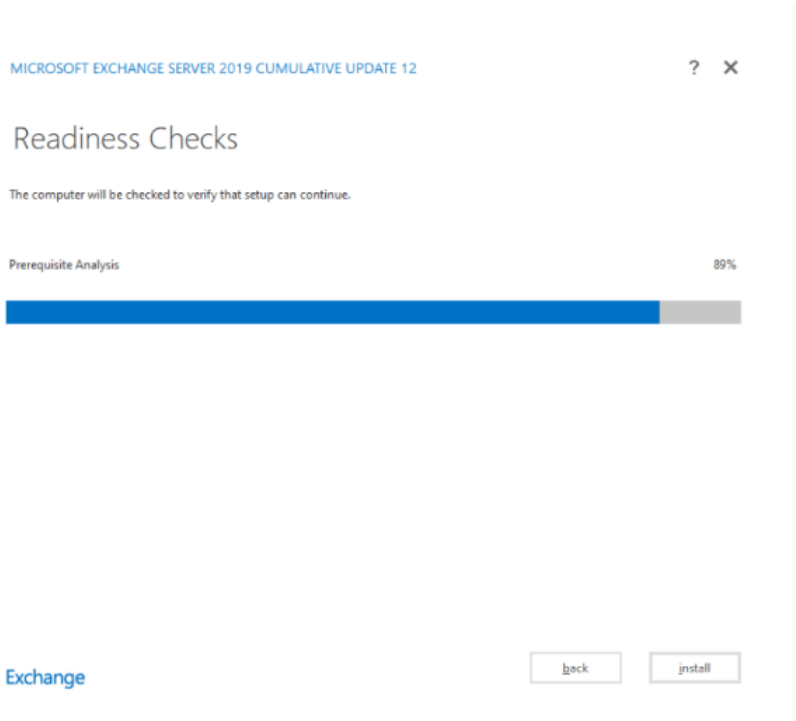


FIGURE 4.14 – Vérification du respect des prérequi.

Normalement, vous devez avoir **uniquement 2 warnings** : l'installeur d'Exchange vous informe qu'il va procéder à la préparation de l'annuaire Active Directory, ce qui implique notamment de mettre à jour le schéma Active Directory. **Cliquez sur "Install" pour lancer l'installation d'Exchange Server 2019.**

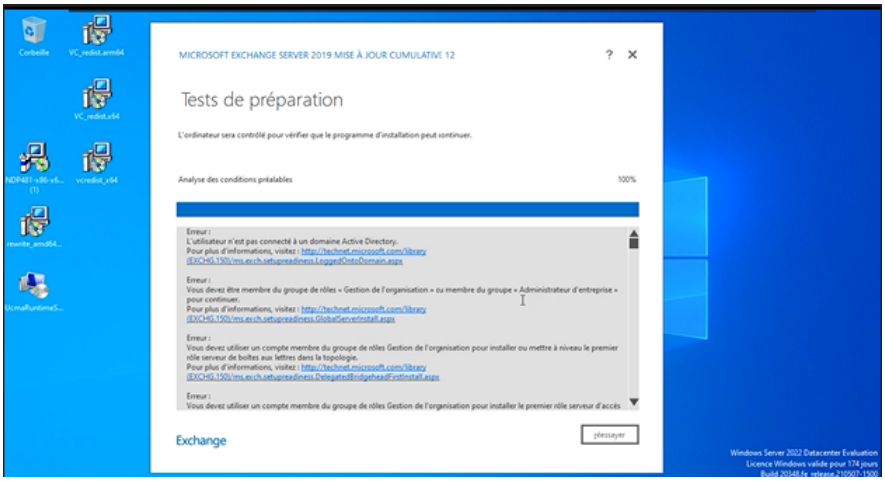


FIGURE 4.15 – L'installation d'Exchange Server 2019

Patientez pendant l'installation... **Elle dure au moins 30 minutes...** Et la durée dépend des performances de votre machine. Pas de panique, donc.

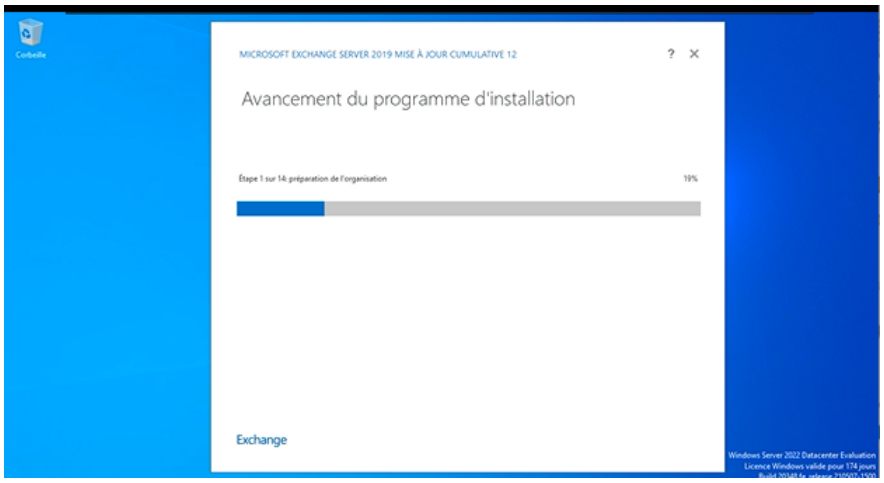


FIGURE 4.16 – Avancement du programme d'installation.

Nous avons installer Microsoft Exchange Server 2019. Maintenant, il faut redémarrer le serveur.

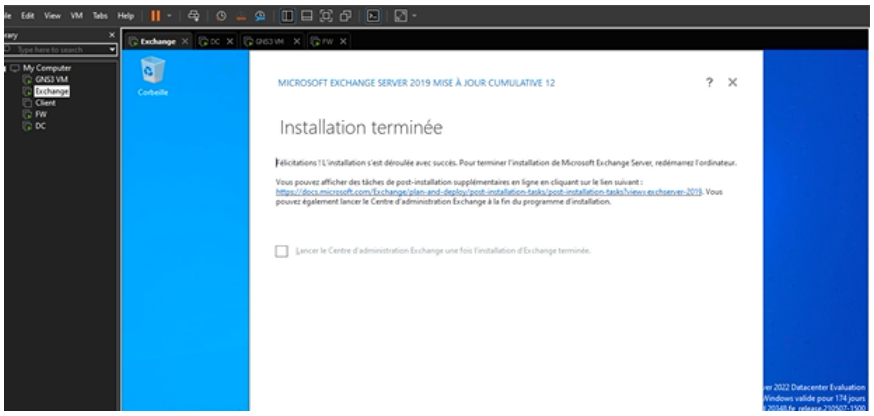
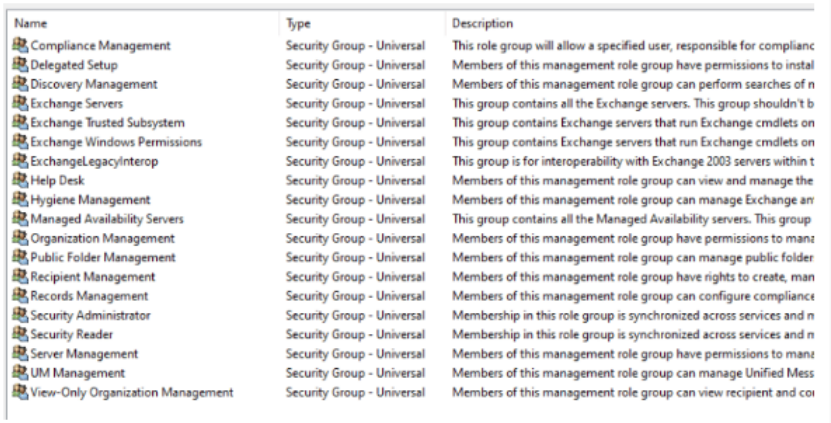


FIGURE 4.17 – Réussite de l'installation d'Exchange Server 2019

Suite à l'installation, une nouvelle OU est visible à la racine de l'Active Directory. Nommée **Microsoft Exchange Security Groups"**, elle contient les groupes d'administration suivants :



Name	Type	Description
Compliance Management	Security Group - Universal	This role group will allow a specified user, responsible for complianc
Delegated Setup	Security Group - Universal	Members of this management role group have permissions to instal
Discovery Management	Security Group - Universal	Members of this management role group can perform searches of n
Exchange Servers	Security Group - Universal	This group contains all the Exchange servers. This group shouldn't b
Exchange Trusted Subsystem	Security Group - Universal	This group contains Exchange servers that run Exchange cmdlets on
Exchange Windows Permissions	Security Group - Universal	This group contains Exchange servers that run Exchange cmdlets on
ExchangeLegacyInterop	Security Group - Universal	This group is for interoperability with Exchange 2003 servers within t
Help Desk	Security Group - Universal	Members of this management role group can view and manage the
Hygiene Management	Security Group - Universal	Members of this management role group can manage Exchange ar
Managed Availability Servers	Security Group - Universal	This group contains all the Managed Availability servers. This group
Organization Management	Security Group - Universal	Members of this management role group have permissions to mana
Public Folder Management	Security Group - Universal	Members of this management role group can manage public folder
Recipient Management	Security Group - Universal	Members of this management role group have rights to create, man
Records Management	Security Group - Universal	Members of this management role group can configure compliance
Security Administrator	Security Group - Universal	Membership in this role group is synchronized across services and n
Security Reader	Security Group - Universal	Membership in this role group is synchronized across services and n
Server Management	Security Group - Universal	Members of this management role group have permissions to mana
UM Management	Security Group - Universal	Members of this management role group can manage Unified Mess
View-Only Organization Management	Security Group - Universal	Members of this management role group can view recipient and co

FIGURE 4.18 – Création des groupes.

4.9 Première utilisation d'Exchange

A. Centre d'administration Exchange et Exchange Management Shell
L'administration d'Exchange s'effectue à travers d'un portail d'administration en mode Web, ainsi que des commandes PowerShell. Le portail d'administration appelé **"Centre d'administration Exchange"** est accessible à cette adresse :

```
# En local sur le serveur
https://localhost/ecp

# À partir d'une machine du réseau local (via le nom du serveur)
https://az-exchange/ecp

# À partir de l'extérieur
https://mail.domaine.fr/ecp
```

FIGURE 4.19 – Microsoft Exchange Security Groups.

Sur cette interface, vous pouvez vous authentifier avec un compte administrateur du domaine.
En complément, il y a **'Exchange Management Shell'** qui contient des commandes PowerShell pour gérer Exchange. Des raccourcis sont disponibles dans le menu Démarrer du serveur.

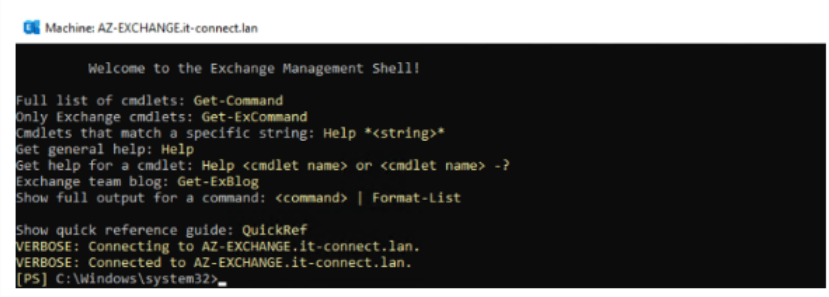


FIGURE 4.20 – Microsoft Exchange Security Groups.

B. Webmail d'Exchange Server 2019

En ce qui concerne les utilisateurs, ils ont le choix entre un client de messagerie type Outlook, ou un accès via le webmail. Ce dernier étant accessible à l'adresse suivante (c'est mieux d'avoir une seule adresse en interne et en externe) .

FIGURE 4.21 – Webmail d'Exchange Server 2019

Le sigle "OWA" fait référence à Outlook Web Access. L'utilisateur doit se connecter avec ses identifiants Active Directory (au préalable, vous devez créer la BAL).

FIGURE 4.22 – Outlook

Ah, mon utilisateur a bien reçu l'e-mail de test que je lui ai envoyé !

Si cela ne fonctionne pas, vérifiez vos enregistrements DNS, les règles de pare-feu (notamment le pare-feu en sortie de réseau) ainsi que l'adresse e-mail utilisée.

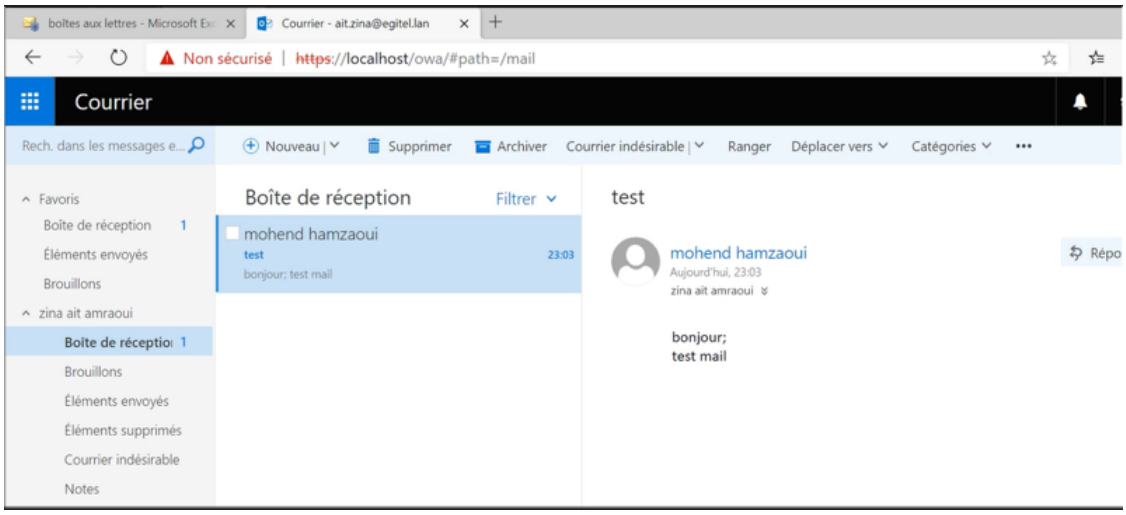


FIGURE 4.23 – Boite de réception.

C. Déplacer la base de données Exchange

Suite à l'installation de Microsoft Exchange, la base de données (au format EDB) et les journaux sont stockés à l'emplacement par défaut aux côtés des binaires d'Exchange :

```
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 0780012571\Mailbox Database 0780012571.edb
```

FIGURE 4.24 – Commande pour déplacer la base de données Exchange.

Nous pouvons déplacer la base de données Exchange sur un autre volume, ainsi que les logs sur un volume différent (soit 3 volumes au total). Au minimum, utilisez un volume séparé pour stocker la base de données et les journaux. Nous venons d'installer notre serveur Exchange, donc c'est aisé et rapide de déplacer les données maintenant.
L'objectif va être de déplacer la base de données et les journaux vers le volume ReFS, au chemin suivant :

```
E:\MsExchange_DB\
```

FIGURE 4.25 – Commande pour déplacer la base de données Exchange.

Nous allons en profiter pour renommer la base de données, car **"Mailbox Database 0780012571.edb"** n'est pas un nom très parlant.. **Ouvrez l'Exchange Management Shell.**
Cette première commande définit le nom **"Mailbox IT-Connect"** pour la

base de données (à la place du nom mentionné précédemment).

```
Get-MailboxDatabase "Mailbox Database 0780012571" | Set-MailboxDatabase -Name "Mailbox
IT-Connect"
```

FIGURE 4.26 – Commande qui permet de lister les bases de données.

La commande **"Get-MailboxDatabase"** permettra de vérifier l'opération puisqu'elle sert à lister les bases de données. Dès que c'est fait, on enchaîne avec la commande **"Move-DatabasePath"** pour déplacer la base de données **EdbFilePath** et les journaux **(-LogFolderPath)** , ce qui donne :

```
Move-DatabasePath "Mailbox IT-Connect" -EdbFilePath
"E:\MsExchange_DB\MailboxITConnect.edb" -LogFolderPath "E:\MsExchange_DB\Logs\"
```

FIGURE 4.27 – Commande qui permet de lister les bases et déplacer les bases de données.

Quelques secondes plus tard, le tour est joué (attention, pendant l'opération la base de données est démontée et donc inutilisable).

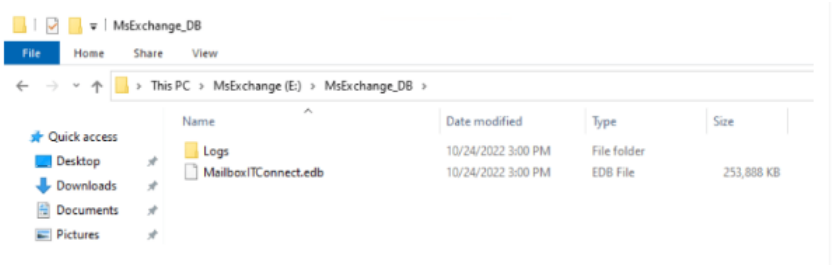


FIGURE 4.28 – Démonter la base de donnée

D. Créer une nouvelle boite aux lettres Exchange

Pour créer une boîte aux lettres (appelée aussi "BAL") pour un utilisateur, vous devez suivre ce chemin : **destinataire > boîtes aux lettres > "+"** Ici, vous devez renseigner un formulaire : soit vous sélectionnez un utilisateur existant dans votre annuaire Active Directory, soit vous créez l'utilisateur en même temps. **Gardez à l'esprit que les comptes utilisateurs et les boîtes aux lettres Exchanges sont liés** à tel point que si vous supprimez une boîte aux lettres dans Exchange, l'utilisateur AD correspondant sera supprimé .

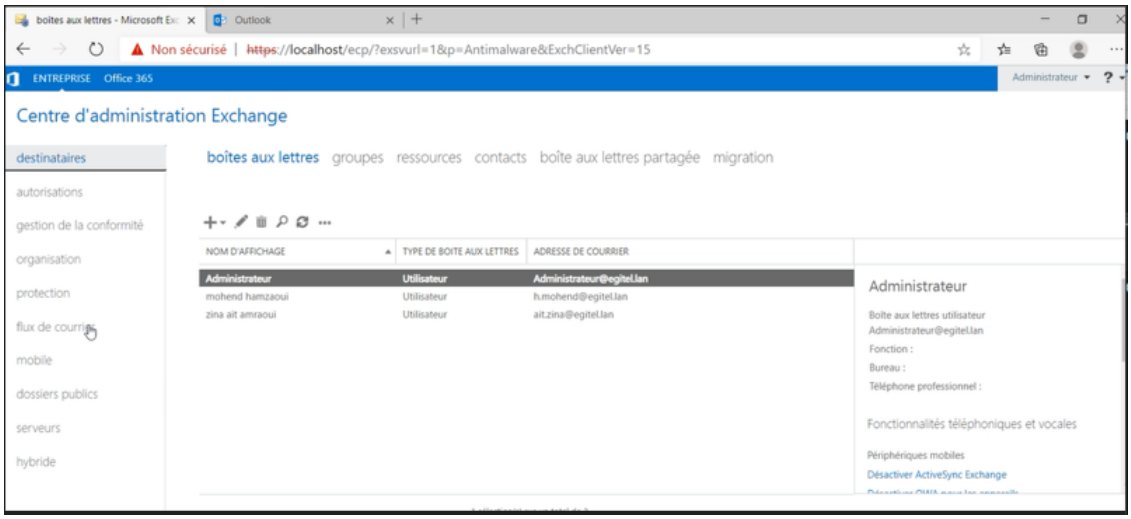


FIGURE 4.29 – Création de boite aux lettres Exchange.

Si votre Exchange est mis en place sur un domaine Active Directory avec un domaine non routable (exemple ".local" ou ".lan"), **le domaine de l'adresse e-mail ne correspondra pas à votre domaine de messagerie** pour communiquer avec l'extérieur.
Dans ce cas, vous devez déclarer un nouveau domaine dans Exchange puis l'attribuer dans une politique d'adresses e-mails.

***Pour ajouter le domaine :**

1 - Cliquez sur **"Flux de courrier"** (Mail flow).

2 - Cliquez sur l'onglet **"Domaines acceptés"** .

3 - Ajoutez un nouveau domaine de messagerie avec l'option **"Le domaine accepté fait autorité"** .

4 - Validez.

5 - Editez le domaine pour cocher l'option **"Définir ce domaine comme domaine par défaut".**

*** Pour éditer la stratégie d'adresse de courrier :**

Soit il faut modifier la stratégie par défaut (qui s'applique sur tous les éléments) ou créer une nouvelle stratégie :

1 - Cliquez sur **"Flux de courrier"** (Mail flow).

2 - Cliquez sur l'onglet **"Stratégies d'adresses de courrier"** .

3 - Editez la **"Default Policy"** .

4 -Cliquez sur **"Format de l'adresse de courrier"** et modifiez le domaine

de **"SMTP"** pour que ça corresponde au nouveau domaine.

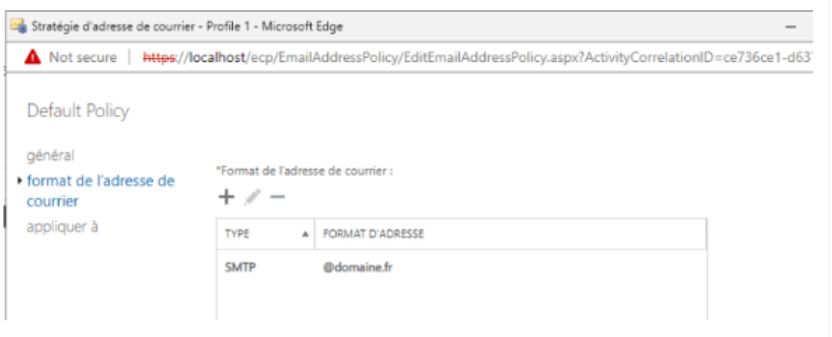


FIGURE 4.30 – Interface du centre management Exchange.

5 -Validez.

Pour que **l'identifiant de l'utilisateur (d'un point de vue Active Directory) hérite aussi de ce domaine de messagerie** (ce qui est idéal), vous devez déclarer un nouveau suffixe UPN dans votre annuaire Active Directory.

E- Créer des certificats pour Exchange

Nous allons maintenant créer et gérer notre certificat pour Egitel.dz à fin de mettre en production notre serveur de messagerie pour qu'il soit joignable sur les réseaux public comme la figure montre :

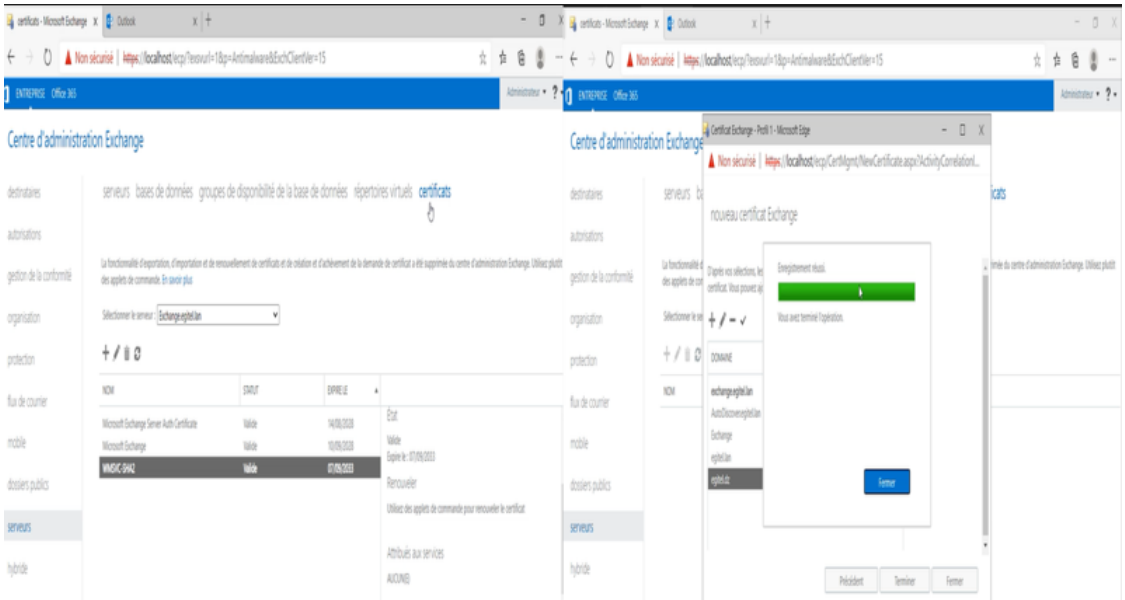


FIGURE 4.31 – Création des certificats.

F -Le firewall

Tous d'abord, nous allons configurer les interfaces et le routage et les règles de filtrage . Voici les captures de configuration de base :

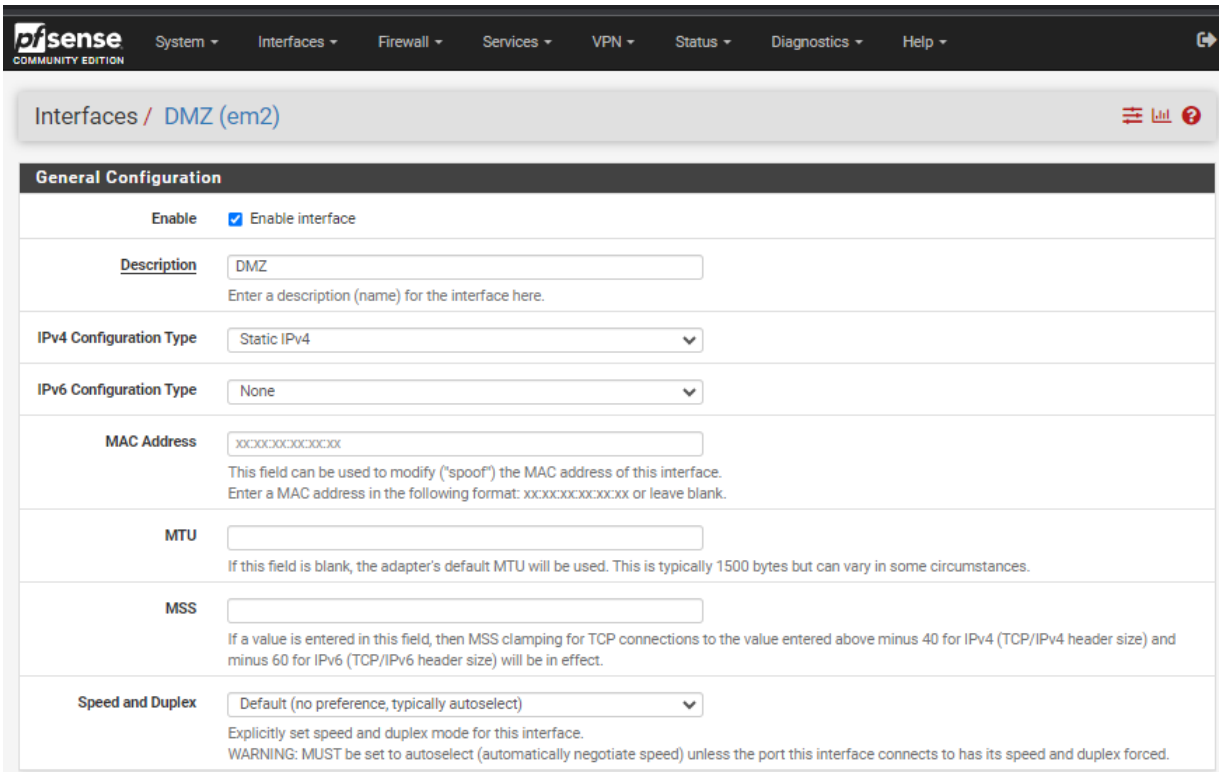


FIGURE 4.32 – Configuration de la DMZ.

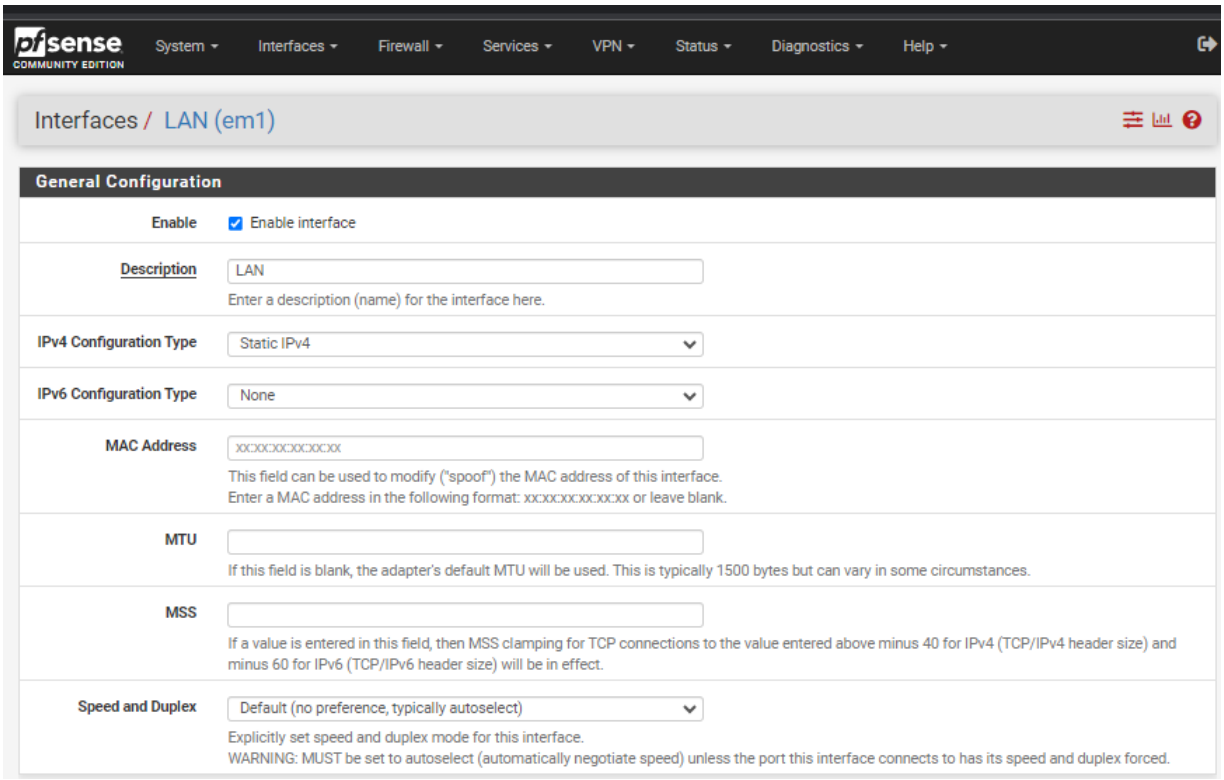


FIGURE 4.33 – Configuration de LAN.

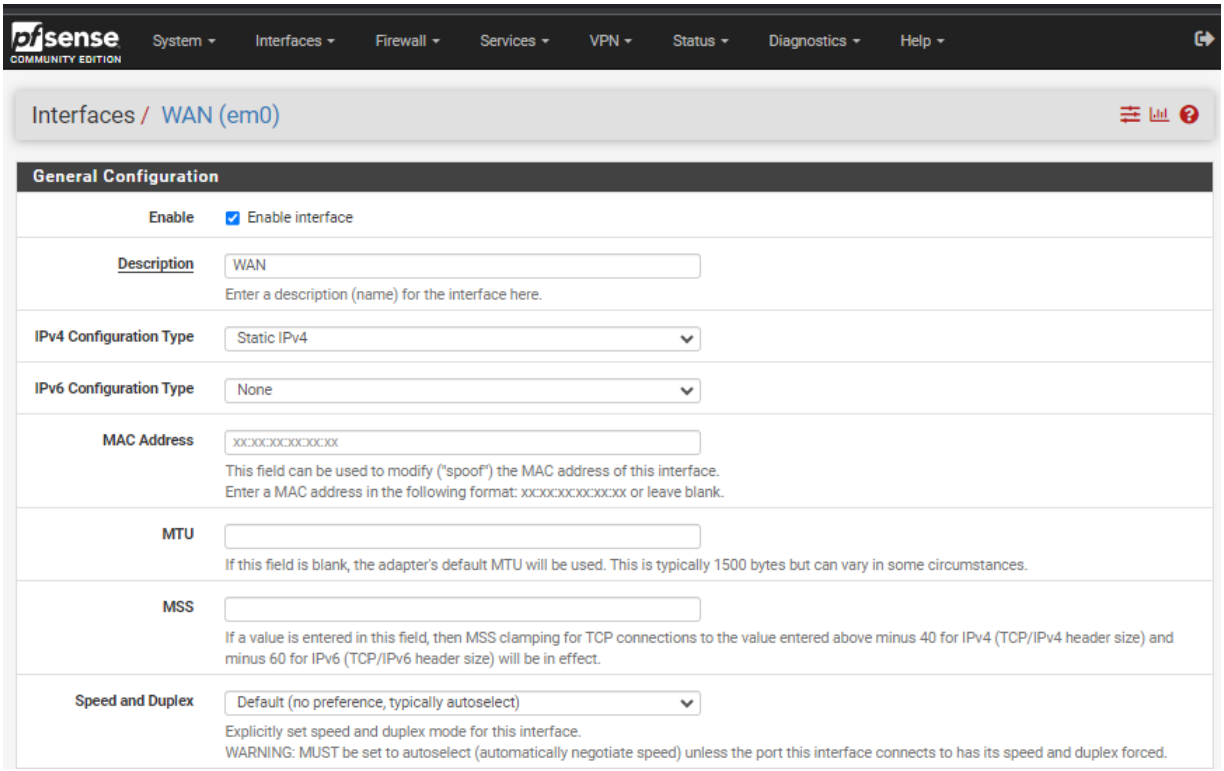


FIGURE 4.34 – Configuration de WAN.

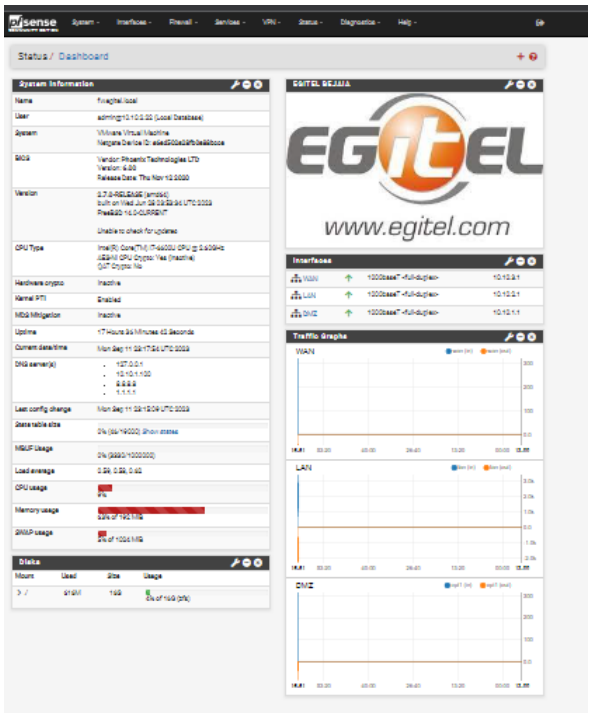


FIGURE 4.35 – Tableau de bord.

Afin de joindre notre serveur Exchange depuis internet, nous allons configurer la redirection des ports pour la messagerie et pour le serveur web :

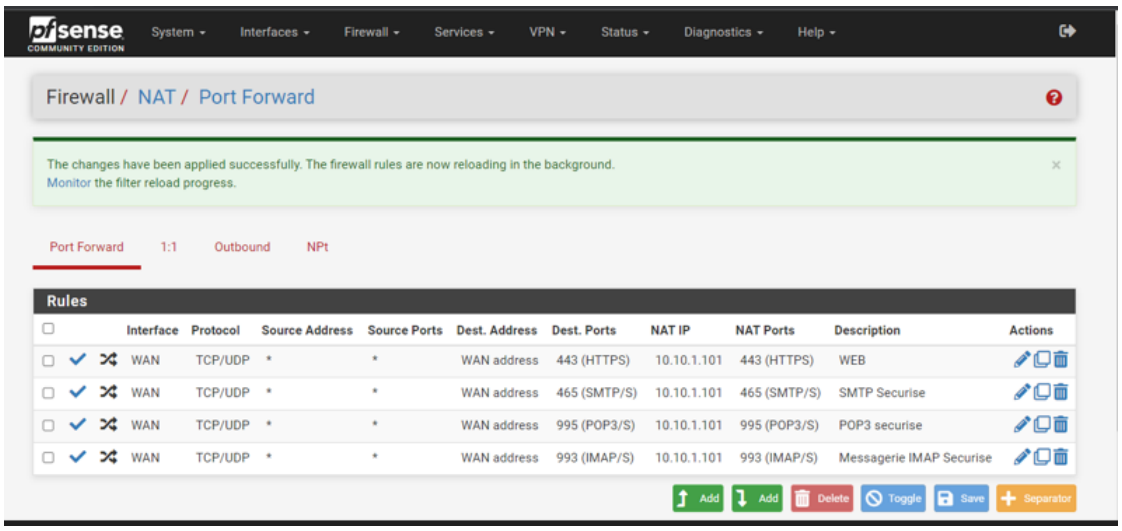


FIGURE 4.36 – La redirection des ports vers internet.

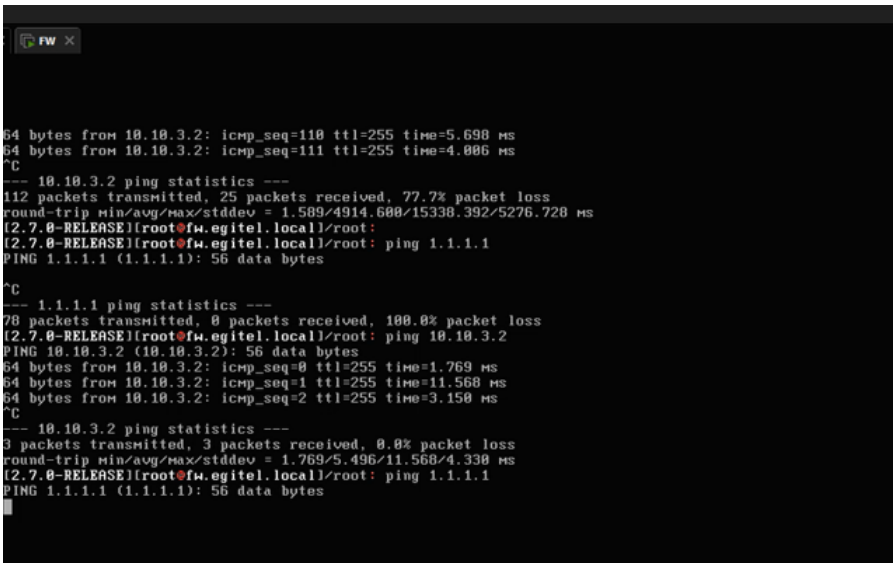


FIGURE 4.37 – Ping réussi vers internet.

4.10 Conclusion

Le serveur de messagerie Exchange est en place. Bien que la configuration ne s'arrête pas là pour qu'il soit prêt à la production (Exchange est un sujet conséquent), la première grosse étape d'installation est terminée, et en soit, il est utilisable.
IL faut maintenir à jour le serveur Exchange, pas seulement au niveau du système Windows Server, mais aussi au niveau de l'applicatif en lui-même. En effet, Microsoft met en ligne des mises à jour Exchange par **"Cumulative Update"**appelée aussi **"CU"**. Il est important de procéder à l'installation pour bénéficier des derniers correctifs de sécurité.

4.11 Comment protéger un serveur Microsoft Exchange avec CrowdSec

I. Présentation

Nous allons voir comment sécuriser un serveur de messagerie Microsoft Exchange avec le pare feu collaboratif CrowdSec. Le fait d'installer CrowdSec sur un serveur Microsoft Exchange va permettre de se protéger contre les attaques courrantes, mais également contre les nouvelles menaces. Par exemple, je pense à la faille de sécurité ProxyNotShell qui a fait parler d'elle en octobre 2022 : CrowdSec est capable de détecter les tentatives

d'exploitation et de bloquer les adresses IP malveillantes, grâce au fait qu'il existe une collection pour IIS et les attaques basées sur les protocoles HTTP/HTTPS.

On peut également citer des cas plus classiques :

Une brute force sur l'interface du webmail d'Exchange. Par sa fonction, un serveur Exchange sera plus ou moins exposé sur Internet selon l'architecture de votre SI (par exemple, la présence ou non d'un reverse proxy). Toutefois, il a besoin de pouvoir communiquer vers l'extérieur et être joignable depuis l'extérieur pour envoyer et recevoir les e-mails à destination des boîtes aux lettres de vos utilisateurs.
Ce même serveur sera aussi joignable par l'intermédiaire d'un Webmail qui permet aux utilisateurs de consulter leurs e-mails à partir d'un navigateur. Ceci implique la présence d'un serveur Web IIS qui héberge à la fois le Webmail et le Centre d'administration d'Exchange. D'ailleurs, lorsqu'il y a la compromission d'un serveur Exchange dans le cadre d'une cyberattaque, cela passe majoritairement par les accès HTTP/HTTPS : d'où l'intérêt de se désactiver les accès externes au Centre d'administration Exchange.

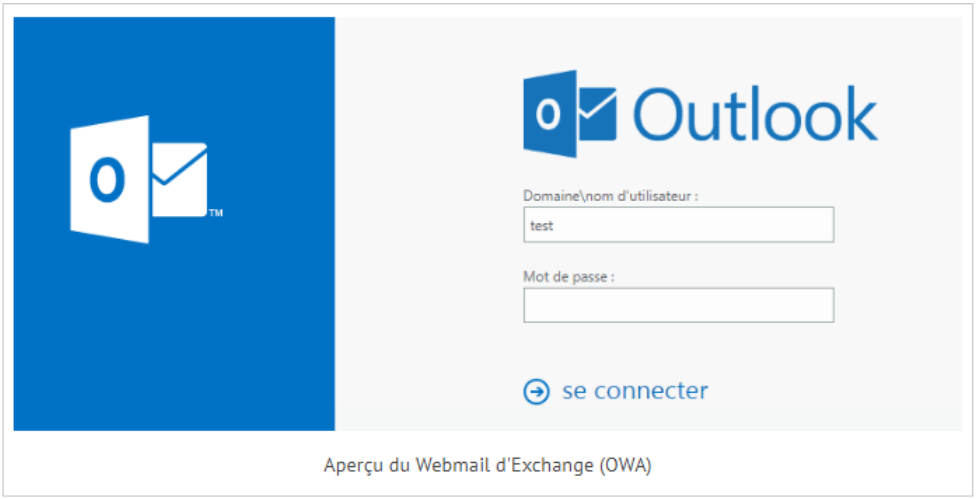


FIGURE 4.38 – Interface client Outlook.

4.12 Mise en place de CrowdSec sur Windows

A. Installation de l'agent CrowdSec

Désormais, l'agent CrowdSec pour Windows est disponible en version stable, ce qui signifie qu'il est prêt pour être mis en place en production.
Lors de l'installation, le package MSI de CrowdSec va réaliser les actions suivantes :

* Installation de CrowdSec en lui-même.
* Intégration de la collection Windows (les détails sont disponibles ici).
* Inscription de l'instance CrowdSec avec l'API Central.
* Inscription du service CrowdSec au sein de Windows (démarrage automatique).

Une fois que c'est fait, démarrez l'installation. Il suffit de suivre les étapes sans apporter de modifications... Ensuite, comptez deux minutes environ pour l'installation de l'agent.

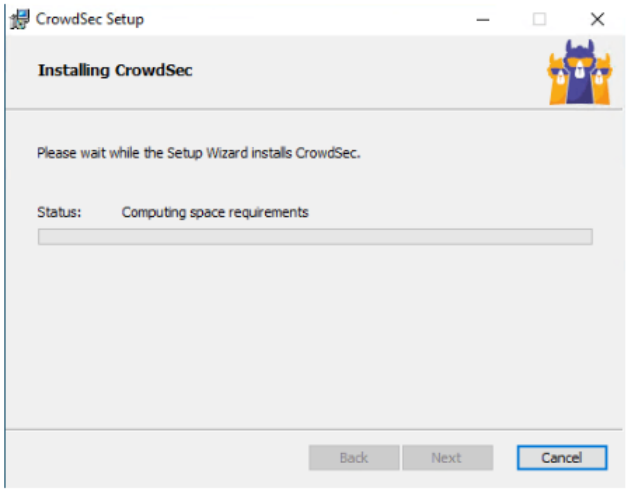


FIGURE 4.39 – l'installation de l'agent CrowdSec.

Dès que l'agent CrowdSec est en place, nous avons accès à la ligne de commande "cscli" qui permet de manager son instance CrowdSec en ligne de commande.

Pour lister les collections actuelles :

```
cscli collections list
```

FIGURE 4.40 – Ligne de commande pour lister les collections.

Pour lister les bouncers actuels (aucun par défaut) :

```
cscli bouncers list
```

FIGURE 4.41 – Ligne de commande pour lister les bouncers actuels.

```
PS C:\> cscli collections list
COLLECTIONS
-------------------------------------------------------------------------------------------------------------
 NAME                  ☒  STATUS   VERSION  LOCAL PATH
-------------------------------------------------------------------------------------------------------------
 crowdsecurity/windows  ✔  enabled  0.1      C:\ProgramData\CrowdSec\config\collections\windows.yaml
-------------------------------------------------------------------------------------------------------------
PS C:\> cscli bouncers list
-------------------------------------------------------------------
 NAME  IP ADDRESS  VALID  LAST API PULL  TYPE  VERSION  AUTH TYPE
-------------------------------------------------------------------
-------------------------------------------------------------------
PS C:\>
```

FIGURE 4.42 – Ligne de commande pour lister les bouncers actuels

B. Installation de la collection IIS

Sur Windows, CrowdSec met en place nativement la collection "crowdsecurity/windows", mais ce n'est pas suffisant pour protéger notre serveur Exchange. Nous devons ajouter la collection pour IIS, ce qui va implicitement ajouter deux autres collections permettant de détecter les attaques Web.

Cette collection s'installe à partir de cette commande :

```
cscli collections install crowdsecurity/iis
```

FIGURE 4.43 – Ligne de commande pour installer d'autres collections.

Quelques secondes plus tard, nous pouvons lister les collections installées afin de constater la présence des nouvelles collections :

```
PS C:\> cscli collections list
COLLECTIONS
NAME                                  STATUS   VERSION  LOCAL PATH
crowdsecurity/base-http-scenarios     enabled  0.6      C:\ProgramData\CrowdSec\config\collections\base-http-scenarios.yaml
crowdsecurity/http-cve                enabled  1.6      C:\ProgramData\CrowdSec\config\collections\http-cve.yaml
crowdsecurity/iis                     enabled  0.1      C:\ProgramData\CrowdSec\config\collections\iis.yaml
crowdsecurity/windows                 enabled  0.1      C:\ProgramData\CrowdSec\config\collections\windows.yaml
```

FIGURE 4.44 – Lister les collections installées.

D'ailleurs, pour justifier ce que je disais en introduction au sujet de la vulnérabilité ProxyNotShell, nous pouvons regarder le détail de la collection **"crowdsecurity/http-cve"**. Ici, on peut constater la présence d'un scénario de**"crowdsecurity/CVE-2022-41082"** correspondant à cette vulnérabilité :

```
cscli collections inspect crowdsecurity/http-cve
```

FIGURE 4.45 – Ligne de commende qui montre la vulnérabilité.

C. Installation du bouncer firewall Windows

Nous devons mettre en place le bouncer **"firewall"** pour Windows, sinon les attaques seront détectées, mais pas bloquées.

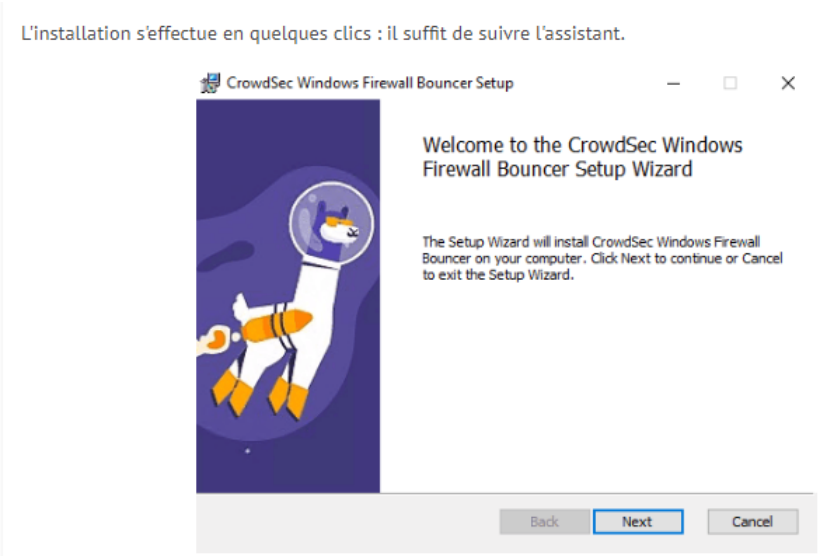


FIGURE 4.46 – Installation du bouncer firewall Windows.

Une fois que c'est terminé, la commande ci-dessous permettra de visualiser la présence du bouncer.

```
cscli bouncers list
```

FIGURE 4.47 – Commande permet de visualiser la présence du bouncer.

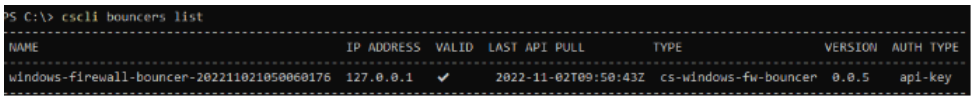


FIGURE 4.48 – Commande permet de visualiser la présence du bouncer.

D. Ajouter la prise en charge des logs IIS

Pour que CrowdSec s'intéresse aux journaux générés par IIS, et par extension correspondant aux accès sur les portails OWA et ECP d'Exchange, nous devons lui indiquer les chemins vers les fichiers journaux à analyser.

Vous devez modifier le fichier suivant :

```
C:\ProgramData\CrowdSec\config\acquis.yaml
```

FIGURE 4.49 – Commande pour modifier le fichier.

Afin d'ajouter les lignes suivantes à la suite :

```
---
use_time_machine: true
filenames:
  - C:\inetpub\logs\LogFiles\*\*.log
labels:
  type: iis
```

FIGURE 4.50 – Commande d'ajouter.

Vous pouvez voir la présence d'un chemin "dynamique" qui se caractérise par la présence du caractère wildcard.

"C :.log" : Cette valeur va permettre à CrowdSec de trouver et lire les fichiers de logs situés dans l'arborescence **"C :¨"** et de les analyser. Ce qui signifie que si vous utilisez un autre chemin, voire même un autre volume pour les logs, vous devez adapter cette valeur.

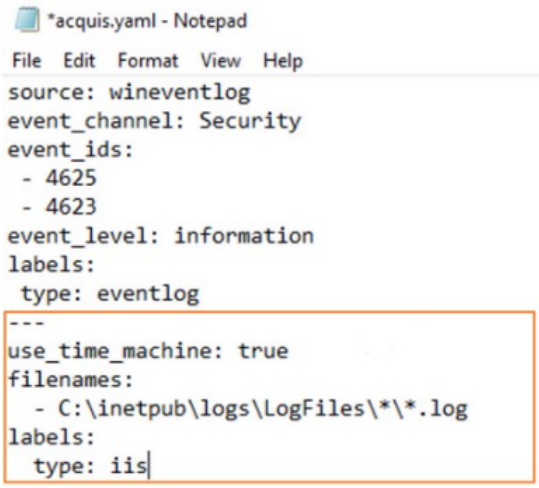


FIGURE 4.51 – La présence d'un chemin dynamique.

Au-delà du chemin vers les fichiers journaux, ce bloc de configurations que l'on vient d'ajouter contient un paramètre nommé **use-time-machine**. Il est important, car IIS n'écrit pas les logs en temps réel dans le fichier journal, mais il écrit les nouveaux événements en bloc chaque minute. Grâce à ce paramètre, CrowdSec va lire la date et l'heure de chaque ligne pour se repérer et traiter les événements chronologiquement, ceci évite de faux positifs.

Par contre, si vous n'utilisez pas les fichiers de logs, mais l'observateur d'événements, vous devez utiliser ce bout de code et non celui mentionné précédemment :

```
---
source: wineventlog
event_channel: Microsoft-IIS-Logging/Logs
event_ids:
  - 6200
event_level: information
labels:
  type: iis
```

Pour finir, nous devons redémarrer le service CrowdSec. Cette opération s'effectue en PowerShell avec cette commande :

```
Restart-Service crowdsec
```

FIGURE 4.52 – La commande qui permet de redémarrer le service CrowdSec.

4.13 Conclusion

Nous venons de voir comment mettre en place l'agent CrowdSec sur Windows de manière à protéger un serveur de messagerie Microsoft Exchange.

Nous avons pris l'exemple d'Exchange Server 2019, mais cela s'applique aussi aux versions précédentes. Avec ces deux exemples rapides, mais concrets, nous avons pu voir l'efficacité de CrowdSec.

Nous profitons de cet article pour vous rappeler l'existence de la console CrowdSec qui vous permet de suivre les alertes remontées par un ou plusieurs agents CrowdSec à partir d'une console en mode Web.

Conclusion générale

La communication électronique a résisté à l'épreuve du temps et de la compétition, s'imposant désormais comme l'outil privilégié au sein du milieu professionnel, grâce à ses innombrables avantages et fonctionnalités. Cependant, lorsque les courriels transportent des informations sensibles de l'organisation, ce qui est fréquemment le cas, ils présentent un danger réel pour celle-ci.

Dans ce contexte, l'objectif de notre travail consistait à concevoir et mettre en œuvre une solution de sécurité fiable afin de minimiser les risques associés au système de messagerie basé sur Microsoft Exchange Server. Pour atteindre cet objectif, nous avons d'abord examiné les concepts fondamentaux et les notions théoriques liés aux réseaux informatiques, à la messagerie électronique et à la sécurité dans un environnement de messagerie.
Ensuite, nous avons déployé la solution de messagerie basée sur Exchange Server au sein d'un environnement de travail virtuel, en accomplissant toutes les tâches de configuration et d'administration nécessaires pour garantir une messagerie fiable et opérationnelle.

Enfin, nous avons mis en œuvre et testé la solution de sécurité et disponibilité que nous avons proposée, dans le but de réduire les vulnérabilités auxquelles la messagerie est exposée.

Résumé

Notre projet s'inscrit dans le domaine de la sécurité de la communication électronique, en se concentrant plus spécifiquement sur la messagerie électronique au sein de l'environnement professionnel. En effet, en tant que moyen de communication le plus répandu et utilisé dans le monde des affaires, le courrier électronique contient une quantité considérable d'informations commerciales sensibles, conférant ainsi une valeur économique significative aux données qu'il transporte. C'est pourquoi il représente une cible privilégiée pour les attaquants et les concurrents.

Pour répondre aux impératifs de sécurité inhérents à un système de messagerie, nous avons fait le choix d'adopter l'une des principales solutions de messagerie actuellement disponibles sur le marché mondial des technologies de l'information et de la communication, à savoir MS Exchange Server. Nous l'avons déployée au sein d'un environnement de travail virtuel, réalisant toutes les opérations de configuration requises pour garantir le bon fonctionnement de la messagerie.

Par la suite, nous avons élaboré une solution de sécurité hautement fiable et de disponibilité élevée, basée sur l'environnement Exchange que nous avons implémentée et soumise à des tests approfondis au sein de notre système de messagerie.

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

Abstract

Our project falls within the field of electronic communication security, focusing specifically on electronic messaging within the business environment. This make it a prime target for attackers and competitors alike. We deployed MS Exchange Server in a virtual work environment, then we developed a high availability security solution based on the Exchange environment, which we implemented and tested carrying out all the configuration operations required to ensure the smooth running of the messaging system.

Key words : Exchange Server, electonic messaging, availability, security, cryptography, Active Directory.