MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE

DEPARTEMENT ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention
du Diplôme de Master II en Electronique

Option : Réseaux et télécommunication

Thème :

Mise en œuvre d'un système de messagerie Exchange sécurisé par la TMG

Proposé et dirigé par :

M^r R.ZIANI

M^r M.KIBOUH

Présenté par :

M^elle DAHOUMANE Lynda

M^elle CHEHEB Lilia

Année universitaire 2012/2013

Remerciements

Nous remercions en premier lieu Dieu tout puissant de nous avoir accordé la puissance et la volonté pour terminer ce travail.

Nous tenons à exprimer notre profonde gratitude à notre promoteur Mr.ZIANI pour ses orientations et ses conseils précieux.

Un grand merci à Mr.Kibouh et tous les employés de l'école 2int partners pour leurs suivis et leurs encouragements tout au long de l'élaboration de notre mémoire.

Notre parfaite considération à l'ensemble des enseignants qui ont contribué à notre formation.

Nos sincères salutations aux membres du jury qui nous font l'honneur d'examiner et de juger notre travail.

Enfin, nous tenons à remercier toutes les personnes qui ont contribué de prés ou de loin à la réalisation de ce mémoire.

Dédicaces

Je dédie ce travail À :

- *Mes très chers parents, pour leurs sacrifices et leurs dévouements pour mon bonheur, et leur soutient pendant toute la durée de mes études.* ***Que Dieu les gardes et les protèges***

- *Mes chères sœurs : Djamila (Nana), Karima, Samira et Lila et leurs maris : Karim, Hacene, Toufik, et Youcef*
  Qui ont su croire en moi

- *Mes chères et adorables nièces et neveux : Rima, Lisa, Melissa, Amine, Nadine, Said, Younesse, nour el Houda, mohamed.*
  Qui remplissent ma vie de bonheur

- *Ma chère binôme Lilia et sa famille, à qui je*
  Souhaite beaucoup de bonheur et de réussite

- *Mes chers Amis (es) qui ont toujours été là pour moi*
- *Toute la promotion : 2012-2013 et 2010-2011 ELN*

Lynda

Dédicaces

Je dédie ce travail À :

- *Mes chers parents, pour leurs sacrifices, leurs dévouements pour mon bonheur, et leur soutient dans ma vie.*
- *Mes chères sœurs : Fetta, Sonia et Sarah.*
- *Mes beaux-frères Naguib et Hakim.*
- *Mes adorables neveux : Ghiles et Anis.*
- *Mon cher fiancé Yazid et sa famille.*
- *Ma chère binôme Linda avec qui j'ai partagé ce travail et à sa famille.*
- *Mes chers Amis (es) qui ont toujours étai là pour moi.*
- *Mes anciens camarades ingénieurs de la promotion 2006-2007 ELN*
- *Mes collègues du département physique.*
- *Mes nouveaux camarades de la promotion : 2012-2013 ELN.*

QUE DIEU VOUS GARDE ET VOUS PROTEGE

Lilia

Liste des tableaux

Liste des tableaux

Liste des figures

Liste des figures

Chapitre I :

Chapitre II :

Liste des figures

Chapitre III :

Liste des figures

Chapitre IV:

Liste des figures

Liste des figures

Liste des figures

Sommaire

Sommaire

Chapitre II : la sécurité du système de messagerie électronique

Chapitre III : Présentation de la solution de messagerie

Chapitre IV : Publication d'Exchange avec la TMG

Sommaire

Introduction générale

Introduction générale

Lorsque les organisations ont commencé à implanter des systèmes de messagerie électronique, c'était dans le but de disposer d'une méthode de communication et d'information purement informelle. Cependant, le courrier électronique, ou courriel, a rapidement évolué pour devenir un des plus importants moyens de communication dans le cadre des activités organisationnelles. C'est un outil qui a transformé la manière dont les organisations mènent leurs tâches parce que c'est un moyen rapide, efficace et peu coûteux, que ce soit au niveau du réseau local ou du réseau étendu : dans certains cas, il a presque remplacé les notes internes et même les appels téléphoniques.

Un nombre grandissant d'organisations utilisent le système de messagerie électronique pour diffuser des informations générales, faire circuler des rapports, envoyer des notes, échanger des documents officiels, expédier de la correspondance à l'extérieur du réseau local, diffuser des directives et soutenir différents aspects de leurs opérations. Un service de courrier électronique adapté offre la possibilité d'augmenter la rapidité des communications organisationnelles, de diffuser massivement des informations, d'éliminer des opérations de surcharge, de faciliter la prise de décisions et d'automatiser certaines tâches courantes.

Cependant, ce système efficace qui permet l'échange de documents électroniques à une grande vitesse, peut également être une véritable source de perturbation pour une organisation. L'usage abusif du système à des fins privées, la perte de contrôle sur les documents d'archives, l'augmentation de la masse des messages sans intérêt, les problèmes de sécurité, le non respect de la vie privée et la perte des informations peuvent facilement diminuer, voire annuler les bénéfices offerts par l'usage du courrier électronique.

Les organismes, tant publics que privés, devraient établir des lignes directrices concernant l'usage du courrier électronique comme moyen de mener leurs activités, instaurer des prescriptions sur la confidentialité des données et l'accès aux informations et normaliser la création, la gestion et la conservation des messages électroniques. Une politique de gestion du courrier électronique bien établie définit également les responsabilités des usagers, des gestionnaires de système et des archivistes. Les politiques et procédures aident les employés à faire un usage efficace et cohérent du système de messagerie

Dans ce mémoire, nous présentons d'abord le système de messagerie électronique puis une solution de messagerie proposée par Microsoft nommée : Exchange. C'est une solution qui assure aux utilisateurs plusieurs objectifs tels que : un espace collaboratif, une simplicité d'administration, une sécurité avancée…etc.

Afin de comprendre ce système et son fonctionnement, nous avons jugé utile de structurer notre travail en quatre chapitres articulés comme suit :

Dans le premier chapitre, nous donnons un bref historique du courrier électronique et l'aspect technique de l'ensemble des modules constituant un système de messagerie.

Dans le deuxième chapitre, nous présentons les failles et les menaces qui pèsent sur la messagerie électronique et nous donnons quelques exemples des solutions retenues pour faire face à ces différents risques et menaces.

Dans le troisième chapitre, nous décrivons la solution de messagerie Exchange Serveur 2010 ainsi que l'environnement de son infrastructure.

Le quatrième chapitre est consacré à la présentation du travail réalisé au cours de ce mémoire. Nous proposons la création d'une architecture réseau interne, qui implémente la politique de sécurité et de messagerie dans Exchange, ainsi que la publication d'Exchange à l'aide du firewall TMG (Threat Management Gateway), qui permet aux utilisateurs et à des collaborateurs distants d'accéder aux ressources du réseau interne (applications, données…etc.) de façon sécurisée.

Enfin, nous terminons par une conclusion générale sur les travaux décrits dans ce document ainsi que des perspectives sur les suites à donner à notre travail.

Chapitre I

Le système de messagerie électronique

I.1.Introduction

Le système de messagerie est aujourd'hui le moyen de communication le plus utilisé sur Internet. C'est également l'un des moins chers à mettre en œuvre, parce que simple, rapide et fiable. En raison de sa popularité, le courrier électronique permet de communiquer avec un vaste auditoire. Il tend à prendre une place de plus en plus prépondérante par rapport aux moyens de communication traditionnels. Bien qu'il puisse incorporer des graphiques, des fichiers sonores et visuels, il sert principalement à l'envoi de textes avec ou sans documents annexés.

La messagerie électronique joue un rôle important au sein des entreprises car elle agit d'une manière directe ou indirecte sur leurs productivités et leurs évolutions. Elle est souvent considérée comme une application stratégique voir critique. Cependant, il est impératif de bien assimiler l'étude théorique et l'aspect technique de l'ensemble des modules constituant un système de messagerie.

I.2.Origines

Les premières messageries électroniques datent des années 60. Aujourd'hui, l'e-mail est l'application d'Internet la plus répandue.

✓ 1967-1968 : la première messagerie collective est créée par l'équipe de Douglas Engelbart, pionnier des interfaces, de l'hypertexte et inventeur de la souris. Son projet appelé NLS était un dispositif intégrant l'hypertexte, les interfaces graphiques et la messagerie collective c'est-à-dire un espace de travail collaboratif,... Le projet NLS est étroitement lié à la naissance du réseau Arpanet en 1969.

✓ Jusqu'en 1972, les programmes de messagerie fonctionnaient sur des machines à temps partagé, utilisées par plusieurs utilisateurs.

✓ En mars 1972, deux ans à peine après la création d'Arpanet, premier réseau distribué et ancêtre d'Internet, Ray Tomlinson, ingénieur chez BBN, écrit le premier programme de courrier électronique (E-Mail) entre deux machines, à partir de deux programmes qu'il venait de créer pour le courrier "intra-machine" : SNDMSG (SeND MeSsaGe), pour envoyer des messages et READMAIL, pour lire les messages. La création, par Tomlinson, d'un protocole expérimental de transfert de fichier appelé CPYNET a permit aux messages électroniques de "sortir" pour la première fois des machines locales pour

circuler sur le réseau. Le véritable courrier électronique à distance était né. Dans son programme, Ray Tomlinson voulait un caractère du clavier qui soit très peu utilisé par les informaticiens, pour séparer nettement l'adresse de l'utilisateur de celle de l'hébergeur et il a choisi l'@, symbole aujourd'hui connu du courrier électronique.

La première adresse de courrier électronique fût *tomlinson@bbn-tenexa.* Tenexa réfère à Tenex, le système d'exploitation utilisé.

I.3.La valeur de la messagerie électronique

I.3.1.Pourquoi le courrier électronique ?

Aujourd'hui tout tourne autour du courrier électronique (communication, inscription, authentification, etc.). C'est un portail collaboratif et un moyen pratique de communication pour quatre grandes raisons :

- ✓ Son fort taux d'utilisation (qui ne possède pas d'adresse électronique ?).
- ✓ Son accès régulier (tout le monde consulte son courrier électronique au moins une fois par jour).
- ✓ Son universalité (quel que soit le fournisseur de messagerie, il est compatible avec les autres).
- ✓ Sa pérennité (il y'a peu de risques que le courrier électronique disparaisse dans les années à venir).

Le courrier électronique est un bon outil de signalisation car il est asynchrone, soit ouvert au reste du monde (internet) ou fermé (à l'intérieur des groupes de travail professionnels).

I.3.2.Besoins des entreprises en termes de Technologie de l'information et de la communication

L'évolution des technologies, l'internationalisation des marchés, la concurrence des firmes d'un même secteur et les exigences toujours plus fortes des consommateurs sont autant de facteurs qui rendent instable et turbulent l'environnement des organisations. Il est dès lors vital pour les organisations de démontrer leurs aptitudes à réagir et à s'adapter à ces perturbations externes. La messagerie électronique est une solution qui s'est peu à peu imposée dans les organisations, au point d'y être aujourd'hui omniprésente et de constituer une technologie utilisée par les administrateurs.

I.3.3.Apports d'un système de messagerie à une entreprise

Dans le cadre de l'entreprise aujourd'hui, la messagerie électronique offre l'opportunité de prendre contact avec d'autres utilisateurs, clients et dirigeants. Dans les années 80, le dirigeant transmettait les décisions par la voie hiérarchique en s'assurant que les personnes intéressées avaient bien reçu les informations. De nos jours, le manager rédige ses notes depuis son logiciel de messagerie, vérifie l'orthographe (la plus part du temps elle se fait automatiquement), les relie, puis les envoie. La procédure est simple et fiable. Cependant la rédaction de notes de services n'est pas la seule fonctionnalité qui contribue à l'amélioration des communications internes. On peut citer de nombreuses potentialités techniques et organisationnelles que la messagerie électronique apporte aux entreprises :

- **La gestion du temps**
  - ✓ améliore les temps de réponse.
  - ✓ raccourcit les délais de prise de décision.
  - ✓ accélère l'exécution des tâches.
- **La gestion de l'information**
  - ✓ facilite le stockage de l'information.
  - ✓ augmente la circulation des documents.
  - ✓ permet le partage d'information et de documents de natures et de sources différentes.
  - ✓ unifie les dispositifs et procédures de diffusion d'informations.
- **L'exécution des tâches**
  - ✓ améliore la productivité.
  - ✓ allège le travail du manager.
  - ✓ permet de mieux organiser son travail.
- **La communication**
  - ✓ augmente l'accès à l'individu.
  - ✓ s'affranchit (en partie) des barrières spatiales et temporelles.
  - ✓ améliore la fréquence de communication.
- **Le travail en équipe**
  - ✓ améliore la constitution des équipes.
  - ✓ favorise le travail collaboratif.
  - ✓ permet de structurer le travail en équipe.
  - ✓ permet une meilleure coordination horizontale.

- **Les relations verticales**
  - ✓ réduit les barrières hiérarchiques.
  - ✓ permet une meilleure implication des collaborateurs.
  - ✓ permet une meilleure responsabilisation des collaborateurs.
  - ✓ peut être utilisé comme levier dans les dispositifs de motivation.

I.4.Définitions

I.4.1.La messagerie électronique

La messagerie électronique appelée parfois courriel, courrier électronique, ou encore e-mail provenant de « electronic mail », est un service de transmission de messages envoyés électroniquement via un réseau informatique dans la boîte aux lettres électronique d'un ou plusieurs destinataires simultanément. Le message envoyé est un ensemble d'informations constitué d'un texte auquel peuvent être joints tous types de fichiers (image, son, vidéo, logiciels, fichiers bureautiques…).

L'émission et la réception des messages par courrier électronique nécessitent la mise à disposition d'une adresse électronique et d'un programme d'accès, sous la forme d'un logiciel appelé client de messagerie. L'acheminement des courriels est régi par diverses normes concernant aussi bien le routage que le contenu.

I.4.2.Le réseau informatique

Un réseau informatique est un ensemble d'ordinateurs et périphériques connectés les uns aux autres afin d'assurer des échanges tels que le transfert de fichiers, le partage de ressources (imprimantes et données), la messagerie électronique ou l'exécution de programmes à distance.

Le terme réseau peut désigner plusieurs choses en fonction de son contexte :

- ✓ L'ensemble des machines ou l'infrastructure informatique d'une organisation avec les protocoles qui sont utilisés.
- ✓ Description de la façon dont les machines d'un site sont interconnectées.
- ✓ Spécification des protocoles utilisés par les machines pour communiquer.

Mise en réseau (Networking) : Mise en œuvre des outils et des tâches permettant de relier des ordinateurs afin qu'ils puissent partager des ressources.

I.4.3.L'organisation réseau utilisée par la messagerie électronique

Le courrier électronique est l'un des services réseau qui utilise le paradigme (client/serveur).

• L'environnement (client /serveur)

De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes (des machines faisant partie du réseau) contactent un serveur (une machine généralement très puissante en termes de capacités d'entrée/sortie) qui lui fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion…

C'est ce type d'architecture que l'on trouve sur les réseaux d'entreprises, qui peut parfaitement supporter plusieurs centaine de clients, voir plusieurs milliers.

Dans un environnement purement Client/serveur, les ordinateurs du réseau (les clients) ne peuvent voir que le serveur, c'est l'un des principaux atouts de ce modèle.

• Fonctionnement d'un système client/serveur

Un système Client/serveur fonctionne selon le schéma suivant

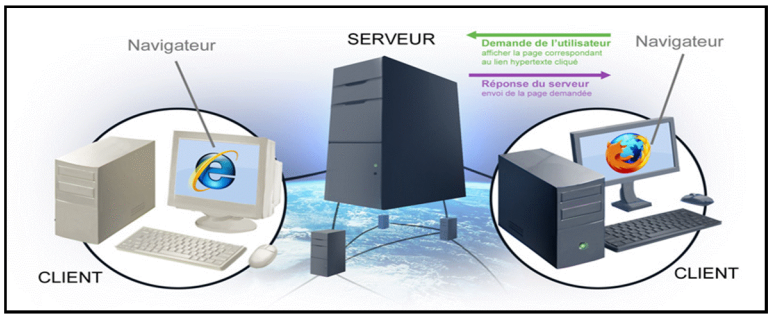


Figure I.1: principe de fonctionnement d'un système Client/serveur

- ✓ Le client émet une requête vers le serveur grâce à son adresse, qui désigne un service particulier du serveur.
- ✓ Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine client et son port.

I.4.4.La boîte aux lettres électronique

Une Boîte Aux Lettres ou inbox en anglais, est un espace dédié à un utilisateur, où sont stockés (dans une pile (stack)) les courriels qui lui parviennent, en attendant qu'il les lises. La taille des mails stockés est limitée par Les serveurs de messageries électroniques.

Afin d'accéder aux différentes applications proposées on désigne une adresse à partir de laquelle on peut émettre et recevoir des e-mails. Elle a la forme suivante :

nomd'utilisateur@domaine.extension.

I.4.5.Les éléments d'une adresse électronique

- **Le nom d'utilisateur**

L'utilisateur peut s'inspirer, pour cette partie de l'adresse, de son propre nom (« prénom-nom », « prenom.nom », « pnom », etc.) ou bien adopter un pseudonyme. Le nom d'utilisateur identifie l'utilisateur sur le réseau, le différenciant de tous les autres utilisateurs de ce réseau.

- **L'arobase @**

L'arobase, caractère indispensable de l'adresse électronique, sépare le nom de l'utilisateur du nom de domaine et signifie « chez ».

- **Le nom de domaine**

Le nom de domaine du fournisseur (« *provider* » en anglais) est en général l'hébergeur ou le nom du site qui fournit le service de messagerie : laposte, gmail, free, etc.

- **L'extension**

Elle désigne le type de domaine. Il existe des extensions géographiques pour tous les pays par exemple L'extension '.dz' désigne un DNS en Algérie ou encore '.fr' pour un DNS en France…, ainsi que des extensions qui désignent le domaine d'activité auquel le serveur est rattaché, par exemple, les universités ou une autre institution scolaire ont souvent pour extension '.edu', les entreprises commerciales utilisent l'extension '.com', le '.Org' indique que l'hôte est un organisme non commercial, les organismes gouvernementaux comportent une extension '.gouv' et '.net' est réservé aux organismes comme les fournisseurs de services Internet...etc.

Notons qu'une adresse électronique peut comporter les caractères suivants : les lettres minuscules de a à z, les chiffres, les caractères «-», «_» et «.».

I.5.Format et structure d'un e-mail

I.5.1.structure d'un e-mail

Un e-mail a une structure similaire à celle d'un courrier classique, il est composé d'une enveloppe (en-tête), comportant les données relatives aux adresses des expéditeurs et des destinataires, ainsi que le sujet du message, la date, , etc. A la suite de l'en-tête séparée par

une ligne vide s'ajoute le contenu de l'e-mail (corps du message), comprenant éventuellement des pièces jointes.

L'en-tête contient donc les informations suivantes :

- ✓ L'adresse e-mail de l'émetteur du message.
- ✓ L'adresse e-mail du (ou des) destinataires.
- ✓ Le chemin suivi par le message.
- ✓ Le type d'encodage du message.
- ✓ Des informations « subsidiaires » comme par exemple le type de logiciel qui a généré le message.

Lors de la lecture d'un e-mail, les champs visibles sont :

- ✓ L'expéditeur.
- ✓ L'objet.
- ✓ Le texte(ou corps) du message.

• Exemple de contenu brut d'un courrier électronique

```
Received: from 31.121.118.45 (EHLO serveur.fr)

  by mta1007.mail.ukl.yahoo.com with SMTP; Fri, 21 Sep 2012 21:31:16
+0000

Received: by serveur.fr (Postfix, from userid 106)

  id 3DF2F15A0CD; Fri, 21 Sep 2012 23:31:16 +0200 (CEST)

From: "Lilia" <lilia@serveur.fr>

To: lynda@yahoo.fr

Subject: Bonjour!

Date: Fri, 21 Sep 2012 23:31:16 +0200

MIME-Version: 1.0

Content-Transfer-Encoding: 8bit
```

I.5.2.Le format MIME (Multi-purpose Internet Mail Extension)

Le format MIME a été défini pour permettre la transmission de données non ASCII par courrier électronique. L'extension MIME offre un mécanisme complémentaire au service de courriel utilisant le SMTP.

MIME ajoute des lignes à l'en-tête d'un mail pour définir le type des données et la méthode de codage utilisé. Un message peut contenir plusieurs types de données différents. Ainsi la structure des messages appelée « RFC 822 » ou « 822 » utilise une ligne blanche pour séparer l'en-tête et le corps de l'image. MIME apporte à la messagerie les fonctionnalités suivantes :

- ✓ Possibilité d'avoir plusieurs objets (pièces jointes) dans un même message.
- ✓ Une longueur de message illimité.
- ✓ L'utilisation du jeu de caractère alphabet autre que le code ASCII.
- ✓ L'utilisation de texte enrichie (mise en forme des messages, police de caractère, couleur etc.).
- ✓ Des pièces jointe binaire (exécutable, image, fichier audio ou vidéo etc.).

- **Un Exemple d'utilisation des messages multiple MIME**

```
From:      lynda@master2.fr
To:        lilia@master2.fr
MIME-Version:1.0
Content-Type: Multipart/Mixed; Boundary=Nouvellepartie

--Nouvellepartie
Bonjour,
Ci-joint la photo que je t'avais promise.
A la prochaine,
Lili

--Nouvellepartie
Content-Type: image/gif
Content-Transfer-Encoding:    base64
                        ……  données de la photo  ……
```

- **Explication de l'exemple**

- ✓ MIME-Version: Il s'agit de la version du standard MIME utilisée dans le message.

- ✓ Content-type : Décrit le type et les sous-types des données. Un type MIME est constitué de la manière suivante :

Content-type: type_mime_principal/sous_type_mime. Dans la première partie de notre exemple « Content-Type: Multipart/Mixed » spécifie que chaque partie du message peut avoir un type de contenu différent et indépendant. Dans la seconde partie on trouve l'image gif qui possède le type MIME suivant : « Content-type: image/gif».

✓ Content-Transfer-Encoding : Définit l'encodage utilisé dans le corps du message qui est « base64».

✓ Le mot clé Boundary= définit la chaîne de caractères que l'on utilise pour séparer les différentes parties du message. Dans notre exemple, l'émetteur a choisi « Nouvellepartie» pour servir de frontière.

- **Les directives spécifiques de l'en-tête du MIME**

➢ **Content type**	➢ **Type MIME de base**	• Text / plain, html,rfc822 • Image /gif,jpeg,png… • Audio /basic, wav … • Video /mpeg… • Application/octet-stream, pdf… • Multipart /Mixed, Alternative, Parallel, Digest.
➢ **Content-transfert-Encoding**	➢ **Format de codage**	• 7bits (pour les messages non accentués) • 8bits • Quoted-printable (pour les messages utilisant un alphabet sur plus de 7bits « présence d'accents par exemple » • Based64 (recommandé pour les fichiers binaires en pièce jointe). • Binary(déconseillé).

Tableau I.1: directives spécifiques de l'en-tête du MIME**.**

I.6.Concepts clés de la messagerie électronique

I.6.1.Le serveur de messagerie électronique

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

La plupart des serveurs de messagerie possèdent ces deux fonctions (envoi/réception), mais elles sont indépendantes et peuvent être dissociées physiquement en utilisant plusieurs serveurs.

I.6.2.Les agents de la messagerie électronique

L'architecture de la messagerie repose sur un ensemble de constituants logiciels distincts qui travaillent ensemble pour assurer le transfert d'un message d'un utilisateur vers d'autres utilisateurs.

On peut distinguer trois types de constituants : MUA, MTA, MDA

I.6.2.1.MUA (Mail User Agent ou Agent de Gestion du Courrier « AGC »)

L'Agent de Gestion du Courrier est un logiciel client de messagerie qui fournit l'interface entre l'utilisateur et la messagerie. Il permet à l'utilisateur la gestion des courriels (saisie, suppression, réception…), il est également capable d'expédier le message au MTA le plus proche.

On trouve deux MUA distincts: un MUA installé sur le système de l'utilisateur qui est appelé client de messagerie lourd et un MUA accessible via un navigateur web appelé client de messagerie léger (webmail).

- **Le client de messagerie lourd**

Est un logiciel installé sur la machine de l'utilisateur qui sert à lire et à envoyer des courriers électroniques, il permet de stocker tous les messages sur la machine et d'écrire des messages hors connexions ou de lire ceux qui sont déjà stockés.

Les clients de messageries lourds les plus connus sont : Microsoft Outlook, Lotus Note (IBM), Mail (Apple), Mozilla Thenderbird, Zimbra Desktop, etc.

- **Client de messagerie léger**

Est un client de messagerie qui s'exécute sur un serveur web, il sert d'interface entre un serveur de messagerie et un navigateur web. Il faut absolument être connecté pour rédiger ou lire les messages.

Les logiciels de webmail les plus connu sont : MS Outlook Web Application, web mail ajax de zimbra, roundcube, etc.

I.6.2.2.MTA (Mail Transfer Agent ou Agent de Transfert de Courriers « ATC »)

L'Agent de Transfert de Courriers est un programme qui permet d'envoyer le message d'un serveur à un autre. Ce logiciel est situé sur chaque serveur de messagerie. Il est composé d'un agent de routage et d'un agent de transmission. Il envoie le message via des protocoles qui permettent de gérer la transmission du courrier entre les systèmes de messagerie. Le protocole le plus utilisé est le SMTP.

Le transfert des messages entre utilisateurs est assuré par une chaine de MTA selon la situation des utilisateurs sur le réseau. Cette chaîne peut être constituée d'un MTA ou de plusieurs MTA. A titre d'exemple, pour une société équipée d'un seul serveur de messagerie pour des échanges de messages en interne, la chaine est réduite à un seul MTA. Quand la chaîne comprend plusieurs MTA, les messages sont « relayés » de MTA en MTA, du MTA d'émission au MTA de réception comme le montre la figure I.2. Le MTA est souvent appelé « relai SMTP ». Il existe plusieurs logiciels serveurs de messageries : Sendmail, MS Exchange, Postfixe, etc.

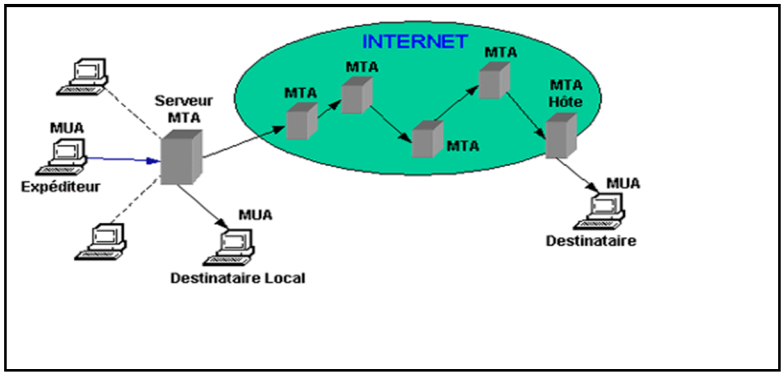


Figure I.2 : Les différents relais de MTA

I.6.2.3.MDA (Mail Delivery Agent ou Agent de Distribution de Courriers « ADC »)

L'Agent de Distribution de Courriers est un programme utilisé par l'Agent de Transfert de Courriers ATC pour mettre en charge la gestion des boîtes aux lettres. Son rôle est de trier les messages en fonction de leurs en-têtes ou de leurs contenus. Il prélève les courriers dans les files d'attentes du MTA et les dépose dans le répertoire de boîtes aux lettres de l'utilisateur à l'aide du protocole POP et IMAP qui viendra les consulter en utilisant le MUA de son poste de travail. Pour cela il est souvent considéré comme le point final d'un système de messagerie. Sous Linux, procmail est très utilisé, et sous Windows on utilise Exchange.

La figure I.3 met l'accent sur la récupération du courrier de la boîte aux lettres par le MDA.

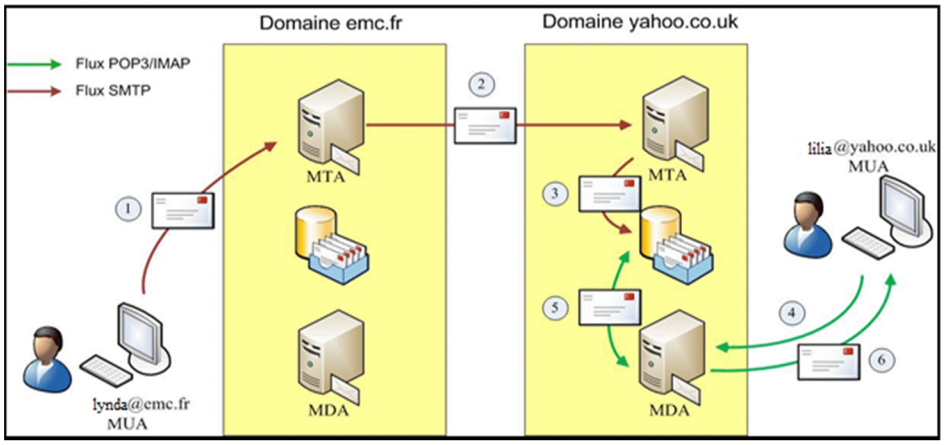


Figure I.3 : la récupération du courrier de la boîte aux lettres par le MDA

I.6.3.Les protocoles de la messagerie électronique

L'acheminement de l'e-mail se fait en plusieurs étapes. Tout d'abord, le courrier est envoyé à un serveur de mail qui va se charger de l'acheminement à bon port. Le serveur source transmet le message au serveur destinataire qui le stocke en attendant que l'utilisateur destinataire le récupère à partir de sa boîte aux lettres personnelle.

Contrairement au courrier postal, l'acheminement d'un message électronique est beaucoup plus rapide et il peut être distribué automatiquement à plusieurs destinataires à la fois.

La transmission du courrier électronique utilise différents protocoles applicatifs : TELNET, SMTP, POP et IMAP. Ces derniers font partie d'une suite de protocoles appelée TCP/IP.

Un protocole est une méthode standard qui permet la communication entre des processus (s'exécutant éventuellement sur différentes machines), c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau. Il en existe plusieurs selon ce que l'on attend de la communication. Certains protocoles seront par exemple spécialisés dans l'échange de fichiers (le FTP), d'autres pourront servir à gérer simplement l'état de la transmission et des erreurs (c'est le cas du protocole ICMP), ... etc.

On classe généralement les protocoles en deux catégories selon le niveau de contrôle des données que l'on désire:

- **Les protocoles orientés connexion** : Il s'agit des protocoles opérant un contrôle de transmission des données (paquets) pendant une communication établie entre deux machines. Dans un tel schéma, la machine réceptrice envoie des accusés de réception lors de la communication, ainsi la machine émettrice est garante de la validité des données qu'elle envoie en assurant l'ordre de remise des paquets, leur retransmission en cas de perte ou d'erreur et la vérification de l'intégrité de l'en-tête des paquets.

- **Les protocoles non orientés connexion** : Il s'agit d'un mode de communication dans lequel la machine émettrice envoie des données (datagrammes) sans prévenir la machine réceptrice, et la machine réceptrice reçoit les données sans envoyer d'avis de réception à la première. Ce protocole ne garantit ni la remise ni l'ordre des paquets délivrés.

I.6.3.1.Le protocole Telnet

Le premier protocole historique est Telnet. C'est un protocole standard permettant à un ordinateur de se connecter à distance à un autre ordinateur, via l'Internet, en mode caractère uniquement : une fois que l'on est connecté à la machine distante, les touches tapées au clavier sont directement transmise à celle-ci et à partir du Telnet la machine nous renvoie les réponses. Généralement, la machine distante commence la communication par nous demander un mot de passe d'accès, puis nous donne accès à un shell sur lequel nous pouvons lancer nos commandes.

Le protocole Telnet s'appuie sur une connexion TCP pour envoyer des données au format ASCII entre lesquelles s'intercalent des séquences de contrôle Telnet. Il fournit ainsi un système orienté communication, bidirectionnel. C'est un protocole de base, sur lequel s'appuient certains autres protocoles de la suite TCP/IP (FTP, SMTP, POP3, ...). Ainsi, Telnet

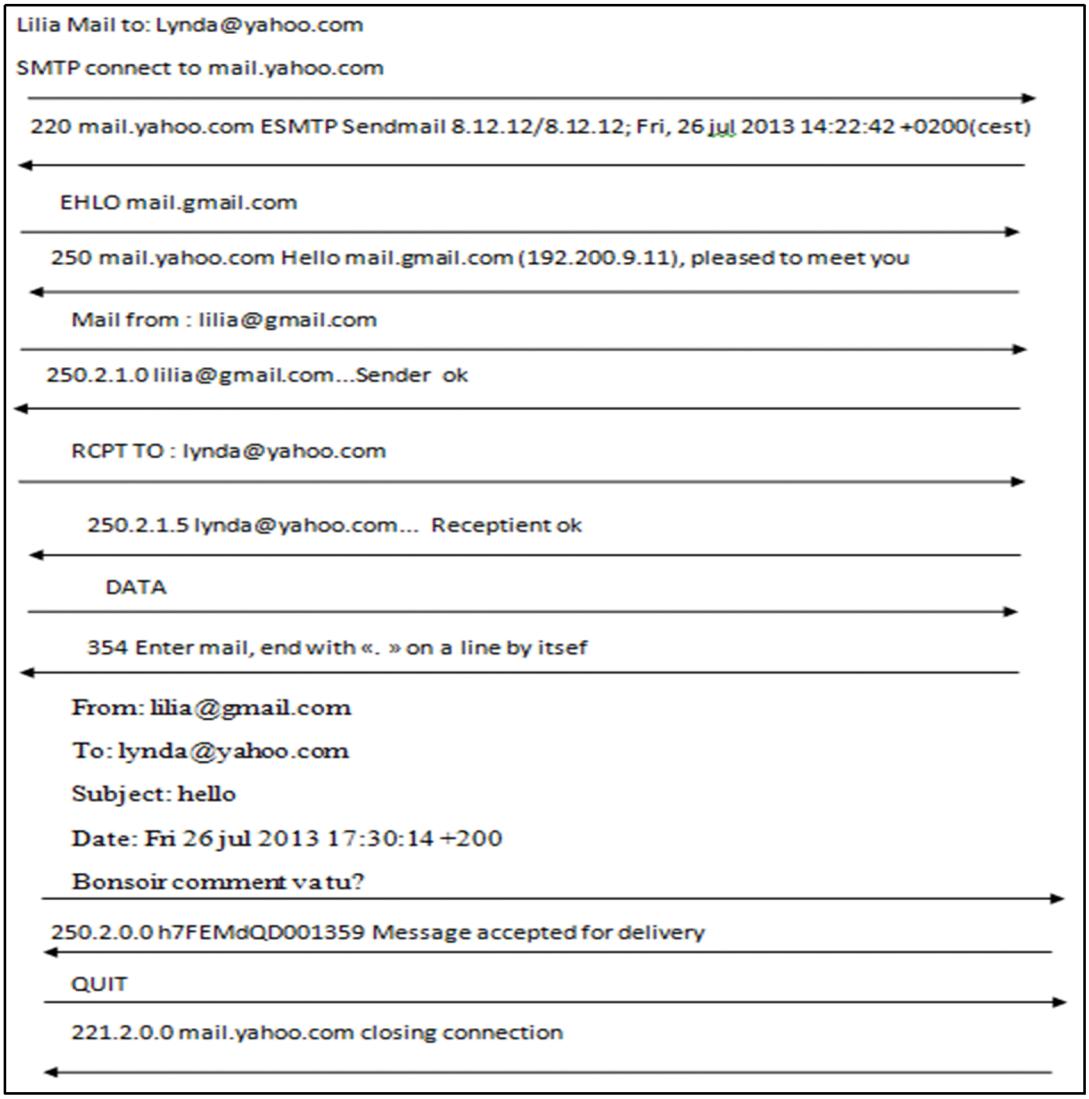
permet de transférer des fichiers FTP, de lire le courrier électronique et de visionner des documents HTML.

Le serveur TELNET n'est pas sécurisé, toutes les informations (y compris le compte d'utilisateur et le mot de passe) circulent en clair dans le réseau.

I.6.3.2.Le protocole SMTP (Simple Mail Transfert Protocol)

Est un protocole de communication utilisé pour transférer le courrier électronique soit d'un client à un serveur soit d'un serveur à un autre. L'utilisation de ce protocole est assez simple, il fonctionne en mode commuté encapsulé dans des trames TCP/IP, grâce à des commandes textuelles (chaine de caractère ASCII terminé par le caractère CR/LF qui est une séquence de deux octets qui indique la fin de ligne dans un texte).

Dans un dialogue, par exemple entre un client et un serveur de messagerie, chaque commande envoyée du client est suivie d'une réponse du serveur SMTP. Une réponse est composée d'un numéro et d'un message afin de signaler si la commande est prise en compte ou non par le serveur.



Dans cet exemple les numéros apparus sont : 220, 250 et 354 qui signifient respectivement : service prêt, action exécutée et début de saisie du message fin avec un point «.».

D'autres codes de messages de services peuvent être interceptés dans les messages tels que :

211(état du système), 214(message d'information), 221(fermeture du canal de transmission) 251(utilisation non local, message transféré), etc. Et les codes d'erreurs tels que 450(requête non prise en compte, boite inaccessible ou occupée), 452(requête non prise en compte, espace mémoire insuffisant), 500(erreur de syntaxe, commande non reconnue, ligne de commande trop langue), etc.

• **Récapitulatif des principales commandes SMTP**

Commande	Exemple	Description
HELO	HELO 121.12.54.75	Identification à l'aide de l'adresse IP ou du nom de domaine de l'ordinateur expéditeur
MAIL FROM:	MAIL FROM:expediteur@domaine.com	Identification de l'adresse de l'expéditeur
RCPT TO:	RCPT TO:destinataire@domaine.com	Identification de l'adresse du destinataire
DATA	DATA message	Partie de l'entête et Corps du mail
QUIT	QUIT	Permet de quitter la connexion sur le serveur SMTP
HELP	HELP	Liste des commandes SMTP supportées par le serveur

Tableau I.2 : Récapitulatif des principales commandes SMTP

I.6.3.3.Le protocole ESMTP (Extended Simple Mail Transfert Protocol)

Il est une amélioration du protocole SMTP avec lequel il est compatible, il fournit des options supplémentaires d'authentification et de cryptage. La commande « HELO » est remplacée par la commande « EHLO » (Extended Helo). Le destinataire ne répond plus seulement « OK» mais donne aussi la liste des extensions qu'il est capable de traiter.

Dans le cas où le destinataire ne supporte pas le protocole ESMTP, il retourne un message d'erreur. Le poste émetteur envoie alors la commande HELO pour initier une communication SMTP.

• **Récapitulatif des principales commandes ESMTP**

Commande	Description
8BITMIME	Permet au client d'envoyer des messages comportant des caractères 8 bits
DSN	(Delivery Status Notification) : Génère et envoie une notification d'état de remise à l'ordinateur expéditeur en cas d'échec de la remise.
SIZE	Indique avant l'envoie par le client, la taille maximale des messages admissibles par le serveur.

Tableau I.3 : Récapitulatif des principales commandes ESMTP

I.6.3.4.Le protocole POP (Post Office Protocole)

Est un protocole qui permet de récupérer les courriers électroniques situés sur un serveur de messagerie électronique. Ce protocole a été réalisé en plusieurs versions respectivement POP1, POP2 et POP3. Actuellement, c'est POP3 (Post Office Protocol Version 3) qui est utilisé de façon standard.

Tout comme dans le cas du protocole SMTP, le protocole POP (POP2 et POP3) fonctionne grâce à des commandes textuelles envoyées au serveur POP. Chacune des commandes envoyées par le client (validée par la séquence CR/LF) est composée d'un mot-clé, éventuellement accompagné d'un ou plusieurs arguments et est suivie d'une réponse du serveur POP (soit +OK ou – ERR).

• **Récapitulatif des principales commandes POP3**

Commande	Description
USER identifiant	Cette commande permet de s'authentifier. Elle doit être suivie du nom de l'utilisateur, c'est-à-dire une chaîne de caractères identifiant l'utilisateur sur le serveur. La commande USER doit précéder la commande *PASS*.
PASS mot_de_passe	La commande *PASS*, permet d'indiquer le mot de passe de l'utilisateur dont le nom a été spécifié lors d'une commande *USER* préalable.
STAT	Informations sur les messages contenus sur le serveur.
RETR	Numéro du message à récupérer.

DELE	Numéro du message à supprimer.
LIST [msg]	Numéro du message à afficher.
NOOP	Permet de garder les connexions ouvertes en cas d'inactivité.
TOP <message_ID> <n>	Commande affichant *n* lignes du message, dont le numéro est donné en argument. En cas de réponse positive du serveur, celui-ci renvoie les en-têtes du message, puis une ligne vierge et enfin les *n* premières lignes du message.
UIDL [msg]	Demande au serveur de renvoyer une ligne contenant des informations sur le message éventuellement donné en argument. Cette ligne contient une chaîne de caractères, appelée *listing d'identificateur unique*, permettant d'identifier de façon unique le message sur le serveur, indépendamment de la session. L'argument optionnel est un numéro correspondant à un message existant sur le serveur POP, c'est-à-dire un message non effacé).
QUIT	La commande QUIT demande la sortie du serveur POP3. Elle entraine la suppression de tous les messages marqués comme effacés et renvoie l'état de cette action.

Tableau I.4 : Récapitulatif des Principales commandes POP3

Le protocole POP3 gère ainsi l'authentification à l'aide d'un nom d'utilisateur et d'un mot de passe, il n'est par contre pas sécurisé car les mots de passe, au même titre que les mails, circulent en clair sur le réseau. D'autre part le protocole POP3 bloque la boîte aux lettres lors de la consultation, ce qui signifie qu'une consultation simultanée par deux utilisateurs d'une même boîte aux lettres est impossible.

I.6.3.5.Le protocole IMAP (Internet Message Acces Protocole)

Ce protocole permet de récupérer les courriers électroniques déposés sur des serveurs de messagerie. Son but est similaire à POP3, l'autre principal protocole de relève du courrier. Mais contrairement à ce dernier, il présente les avantages suivants :

- ✓ Possibilité de stocker les messages sur le serveur de manière structurée.
- ✓ Gestion de plusieurs boîtes aux lettres.
- ✓ Permet l'accès direct à des parties du message (par exemple les en-têtes sans le corps du message).

Un serveur IMAP est un système de fichiers dont les répertoires sont des classeurs, chaque classeur contient des messages. A chaque message est associé des informations (en plus du corps et de l'en-tête des messages) tels que :

- ✓ Un numéro unique.
- ✓ Une série de drapeaux (message lu, réponse envoyée, message à effacer, brouillon...).
- ✓ Une date de réception du message.

• Récapitulatif des principales commandes IMAP

Commande	Description
LOGIN	Connexion au serveur IMAP
LIST	List des dossiers
SELECT	Sélection d'un dossier
SEARCH	Recherche de messages dans un dossier en fonction de critère
FETCH	Récupération d'un message
STORE	Association de drapeaux à un message
LOGOUT	Déconnection du serveur IMAP

Tableau I.5 : Récapitulatif des principales commandes IMAP

• Les ports associés aux protocoles

Un port est un numéro associé à un service ou une application réseau. La fonction du port est de déterminer à quel programme la communication est destinée.

De nombreux programmes peuvent être exécutés simultanément sur Internet (on peut par exemple naviguer sur des pages web tout en consultant une messagerie électronique). Chacun de ces programmes travaille avec un protocole de communication, toutefois l'ordinateur doit pouvoir distinguer les différentes sources de données.

Ainsi, pour faciliter ce processus, chacune de ces applications se voit attribuer une adresse sur la machine, codée sur 16 bits : la combinaison adresse IP + port de communication est alors une adresse unique au monde, elle est appelée socket.

L'adresse IP sert donc à identifier de façon unique un ordinateur sur le réseau local ou sur le réseau internet tandis que le numéro de port indique l'application à laquelle les données sont destinées. De cette manière, lorsque l'ordinateur reçoit des informations destinées à un port de communication, les données sont envoyées vers l'application correspondante. Le tableau I.6 montre les ports des protocoles de messagerie.

Protocole (application):	Port:
TELNET	23
SMTP	25
IMAP	143
POP3	110

Tableau I.6 : Les ports liés à la messagerie électronique

I.7.Architecture et principe de fonctionnement

Les différents éléments d'un système de messagerie sont agencés selon une architecture logique, pour en assurer le fonctionnement. L'architecture d'un système de messagerie peut être représentée de la sorte

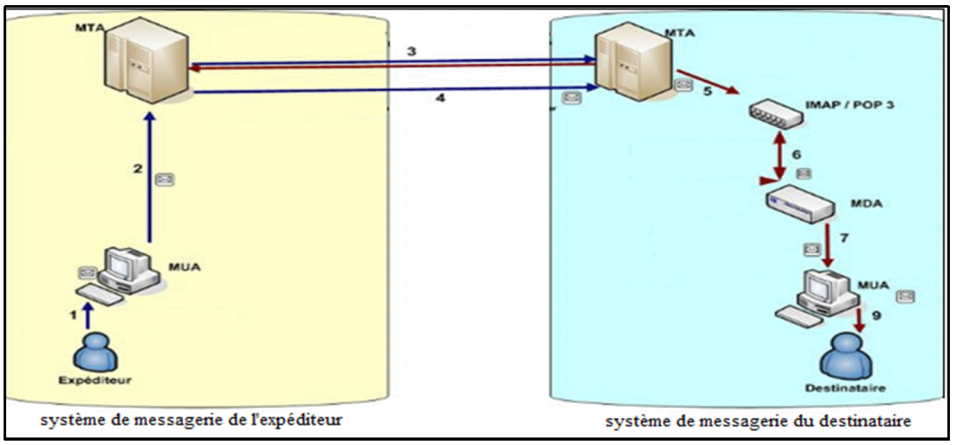


Figure I.4 : Architecture d'un système de messagerie

- **Les étapes de fonctionnement du système de messagerie**
  - ✓ **Etape 1 :** L'expéditeur saisit et valide l'envoie de son courrier.

✓ **Etape 2 :** Le MUA transmet le courriel au MTA (la plupart des MUA intègrent des clients SMTP).

✓ **Etape 3 :** Le MTA du système de l'émetteur établit un canal de transmission avec le MTA du système du destinataire, par émission successives de requêtes bidirectionnelles.

✓ **Etape 4 :** Une fois le canal établi, le courriel est transmis d'un système à un autre par le MTA.

✓ **Etape 5 :** Dans le système du destinataire, le MTA transmet le courrier reçu au serveur IMAP ou POP3.

✓ **Etape 6 :** Le MDA récupère le courriel du serveur IMAP/POP3 par émissions successives de requêtes.

✓ **Etape 7 :** Le MDA récupère le courriel du serveur IMAP/POP3 par émissions successives de requêtes, et le met à disposition du MUA.

✓ **Etape 8 :** Le MUA dépose le courriel dans la boîte aux lettre du destinataire qui pourra le consulter à tout moment sur authentification.

I.8.Le contexte d'utilisation de la messagerie électronique en entreprise

On distingue trois cas d'utilisation de la messagerie électronique dans une entreprise

✓ Une utilisation via le réseau privé de l'entreprise purement interne appelée : l'intranet.

✓ Une utilisation étendue à des fournisseurs ou partenaires appelée : Extranet.

✓ Une utilisation ouverte vers l'extérieur via des réseaux publics appelée : Internet.

I.8.1.L'utilisation de l'e-mail au sein d'un Intranet

Un intranet est un ensemble de services internes à un réseau local, c'est-à-dire accessible uniquement à partir des postes d'un réseau local, ou bien d'un ensemble de réseaux bien définis, et invisible de l'extérieur. Ces services sont basés sur les mêmes technologies que l'internet (protocoles de communication TCP/IP, messagerie électronique, partage des données, serveur web interne, etc.).

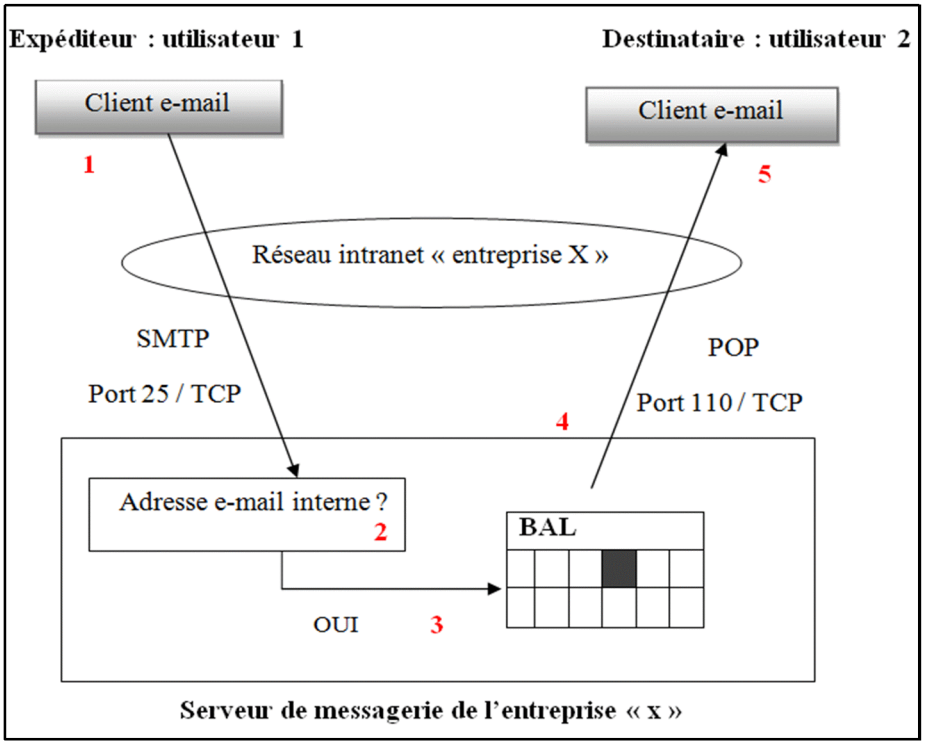


Figure I.5 : Illustration de l'acheminement d'un e-mail entre deux correspondants appartenant à la même entreprise

- **Les étapes**

1. L'utilisateur 1 expédie un e-mail avec comme adresse de destination celle de l'utilisateur, il utilise un client de messagerie configuré pour dialoguer avec le serveur de messagerie de son entreprise « entreprise x ».
2. Le serveur de messagerie analyse l'adresse de destination de cet e-mail, il reconnait que celle-ci correspond à une adresse interne de l'entreprise (utilisateur2@entreprisex. extension).
3. L'email est donc déposé dans la boîte aux lettres assignée à l'utilisateur 2.
4. L'utilisateur 2 destinataire de cet e-mail doit périodiquement interroger le serveur de messagerie (manuellement ou automatiquement), afin de savoir s'il a du courrier en attente.
5. Dans le cas positif, les e-mails en attente sur le serveur de messagerie peuvent être rapatriés sur le poste de travail du destinataire (utilisateur 2).

I.8.2.L'utilisation de l'e-mail au sein d'un extranet

Un extranet est une extension du système d'information de l'entreprise à des partenaires situés au-delà du réseau. L'accès à l'extranet doit être sécurisé dans la mesure où cela offre un accès au système d'information à des personnes situées en dehors de l'entreprise. Il peut s'agir soit d'une authentification simple (authentification par nom d'utilisateur et mot de passe) ou d'une authentification forte (authentification à l'aide d'un certificat). Il est conseillé d'utiliser HTTPS pour toutes les pages web consultées depuis l'extérieur.

De cette façon, un extranet n'est 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.

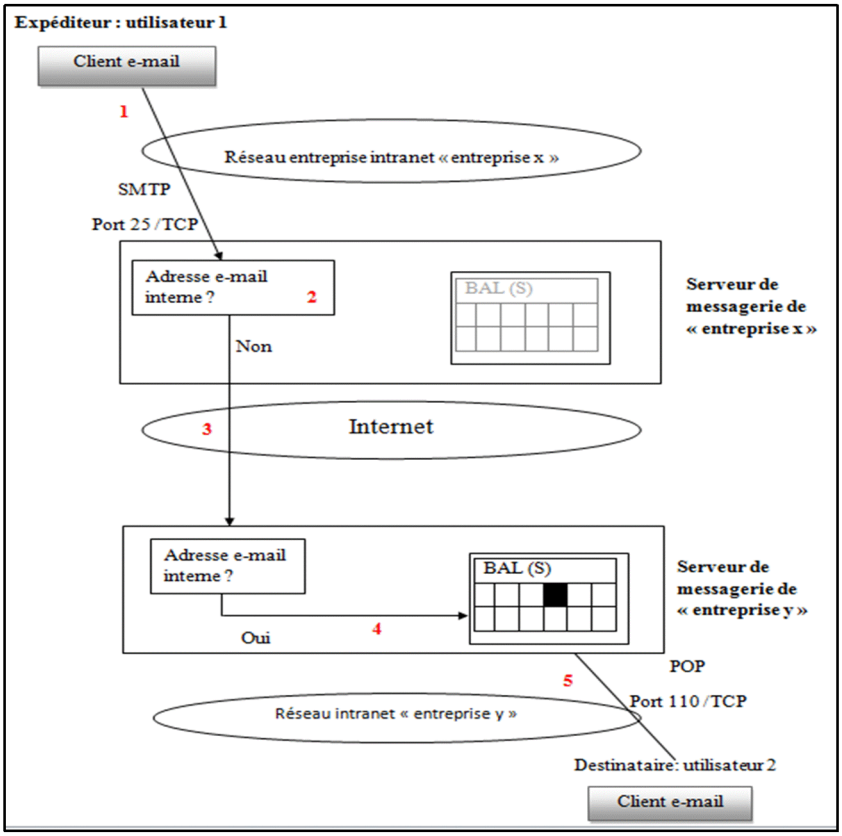


Figure I.6 : Illustration de l'acheminement d'un e-mail entre deux correspondants appartenant à des entreprises différentes (internet ou extranet)

- **Les étapes**

1. L'utilisateur 1 expédie un e-mail, avec comme adresse de destination celle de l'utilisateur 2 à l'extérieur de l'entreprise. Il utilise un client de messagerie configuré pour dialoguer avec la messagerie de son entreprise « entreprise x ».
2. Le serveur de messagerie analyse l'adresse de destination.
3. Compte tenu que l'adresse de destination ne correspond pas à une adresse interne, le serveur de la messagerie « entreprise x » oriente le message via Internet vers le serveur de la messagerie de la société « entreprise y ». Une recherche de l'adresse IP du serveur de messagerie de l'entreprise destinataire est alors nécessaire. Il s'agit d'une interrogation du DNS (Domain Name Service). La résolution DNS s'obtient à partir du nom de domaine situé à la droite du signe @ de l'adresse de l'expéditeur « utilisateur2@entreprisey.extension ». Eventuellement, l'email peut transiter par plusieurs serveurs de messagerie intermédiaire.

4. Le serveur de messagerie de la société « entreprise y » analyse l'adresse de destination de l'e-mail, il constate que cette adresse correspond à l'une des adresses internes, il place donc l'e-mail dans la boite aux lettres du destinataire.
5. L'utilisateur 2 destinataire de cet e-mail, doit interroger périodiquement le serveur de messagerie (manuellement ou automatiquement), afin de savoir s'il a du courrier en attente.
6. Les e-mails en attente sur le serveur de messagerie peuvent être rapatriés sur le poste de travail du destinataire (utilisateur2).

I.8.3.L'utilisation de l'e-mail au sein d'un internet

L'internet forme une gigantesque toile d'araignée (en anglais "web") formant le réseau le plus vaste, puisqu'il contient l'interconnexion des différents réseaux (LAN, MAN, et WAN). Sur Internet il existe différents protocoles qui permettent de faire plusieurs applications:

- **IRC (Internet Relay Chat)**

Qui signifie discussion relayée par Internet. Elle utilise un protocole qui sert à la communication instantanée (en temps réel) principalement sous la forme de discussions en groupe par l'intermédiaire de canaux de discussion. IRC correspond en fait à un service de conférence électronique improvisée qui s'articule autour d'un contexte questions et réponses. Les paquets IRC arrivent sur le port 6667 (ou un autre situé généralement autour de 7000).

- **HTTP (HyperText Transfer Protocol)**

La version du protocole HTTP 0.9 était uniquement destinée à transférer des données sur Internet mais La version 1.0 permet un transfert de fichiers (essentiellement au format HTML) localisés grâce à une chaîne de caractères appelée URL entre un navigateur (le client) et un serveur Web mais également un transfert des messages avec des en-têtes décrivant le contenu du message en utilisant le codage MIME. Les paquets http arrivent sur le port 80 et sont transmis au navigateur internet à partir duquel la page a été appelée.

- **FTP (file Transfert protocol)**

Est un protocole de communication dédié à l'échange informatique de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur de copier des fichiers depuis ou vers un autre ordinateur du réseau ou encore de supprimer ou modifier des fichiers sur cet ordinateur.

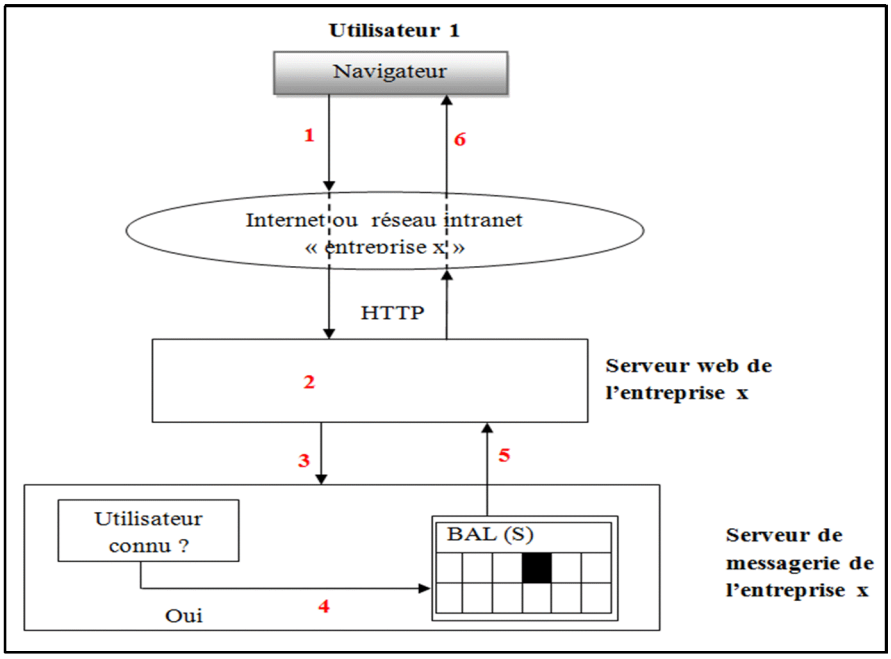


Figure I.7 : Illustration de l'accès à un serveur de messagerie à partir d'un navigateur (webmail) pour le retrait d'un e-mail

- **Les étapes**

1. L'utilisateur 1 se connecte au serveur web de son entreprise à l'aide de son navigateur. Il accède à une page http permettant de solliciter le service webmail d'accès à sa messagerie. Un dialogue initial permet d'identifier et d'authentifier l'utilisateur.
2. Le serveur web élabore une requête destinée au serveur de messagerie.
3. La requête est transmise au serveur de messagerie de l'entreprise x.
4. Le serveur de messagerie de l'entreprise x authentifie le propriétaire de la boite aux lettres.
5. Tous les messages reçus sont transmis au serveur web qui les reformate dans une page web.
6. Le résultat est transmis en retour au navigateur de l'utilisateur 1 qui peut alors consulter le contenu de ses e-mails.

I.9.Conclusion

Nous avons fait le tour des différents éléments théoriques impliqués dans la réalisation d'un système de messagerie. Nous avons commencé par présenter le service de messagerie électronique, son architecture et les différents agents intervenant dans son fonctionnement. Nous avons ensuite présenté le format d'un message électronique et le standard MIME qui normalise la structure et le codage des messages. Enfin, nous avons exposé un ensemble de protocoles intervenant dans les communications entre les différents agents du service de messagerie.

Nous avons constaté à travers notre étude théorique que cette forte utilisation de la messagerie électronique constitue l'une de ses principales faiblesses car le courrier des utilisateurs est devenu la ressource la plus sensible d'un système informatique obligeant ceux-là à sécuriser leurs systèmes de messagerie en particulier celles des entreprises.

Dans le deuxième chapitre nous allons exposer les failles de la messagerie et les solutions standards de sa sécurisation.

Chapitre II

La sécurité du système de messagerie électronique

II.1.Introduction

La messagerie est un vecteur de communication, de productivité et de production. Sa sécurité et sa disponibilité sont les préoccupations des entreprises. Toutefois, lors de leurs conceptions, les protocoles de messageries n'ont pas intégré les procédures de sécurité actuelles. C'est ce qui explique la multiplication des menaces qui pèsent sur la messagerie: virus, leurres, spam, déni de service, usurpation d'adresse, etc. De plus, parce que c'est un outil virtuel, simple et rapide, des dérives de son utilisation engendrent des risques tels que l'interception des messages électroniques par des tiers non autorisés ou encore la répudiation d'un acte d'échange (contrat, paiement, factures, bons de commandes, etc.).

Dans ce chapitre, nous commençons par présenter les failles et les menaces qui pèsent sur la messagerie électronique. Ensuite, nous donnons quelques exemples des solutions retenues actuellement pour faire face aux différents risques et menaces. À titre d'exemple, nous citons le chiffrement, les réseaux privés virtuels, les systèmes pare-feu, etc.

II.2.Récapitulatif des attaques les plus répondues exploitant le système de messagerie

Avant de nous lancer dans le thème de la sécurité nous avons recueilli quelques attaques répondus qui exploitent les failles de la messagerie pour se propager. Cela dans le but d'illustrer l'importance d'une prise en compte sérieuse de la sécurité du système de messagerie :

- ✓ Le virus CIH dit Chernobyl a obligé des milliers d'utilisateurs, en 1998, a changé la carte mère de leurs ordinateurs après en avoir détruit le programme BIOS.
- ✓ Le ver « ouvrez-ça » en pièce jointe d'un courrier électronique a infecté en 1999 plus de 45 millions d'ordinateurs dans le monde. Plus récemment, le ver Sapphire/Slammer a infecté plus de 75 000 serveurs sur toute la planète, en dix minutes environ.
- ✓ En mars 2007, un programme malveillant a fait subir aux utilisateurs d'ordinateurs personnels et d'entreprises une attaque par pourriel. Au cours de ces attaques, certaines entreprises canadiennes qui exploitent leurs propres serveurs de courriel risquaient de voir leurs ordinateurs détournés pour servir de relais à l'envoi de pourriel à tous leurs contacts. Elles risquaient également que le cheval de Troie télécharge un logiciel malveillant qui pourrait avoir comme effet de ralentir ou de surcharger leur réseau.
- ✓ Un autre cas qui utilise de simples rumeurs (hoax), plaisanteries, relayées par la messagerie électronique qui faisait croire que la présence dans le répertoire C:\windows du fichier kerne132-d11 trahissait la présence d'un virus. La fausse alerte conseillait alors

de le supprimer, ce qui rendait tout redémarrage ultérieur du système impossible. L'ignorance des utilisateurs a fait le reste.

II.3.Les failles et les menaces de la messagerie électronique

Nous avons choisi de segmenter les menaces et risques potentiels touchant au système de messagerie autour de 3 problématiques :

- ✓ Les atteintes aux messages autorisés au sein de l'entreprise.
- ✓ Les atteintes à l'infrastructure et au système d'information « SI » sur lesquels repose le système d'échange.
- ✓ Les atteintes à l'organisation et à l'utilisation du système de messagerie de l'entreprise.

II.3.1.Les atteintes aux messages autorisés au sein de l'entreprise

II.3.1.1.Perte d'un message électronique

Une mauvaise configuration et une non sécurisation d'un serveur de messagerie qu'il soit en relais ou en serveur interne, qui résiste mal à la charge et à des dénis de service peut provoquer une perte de message. Une mauvaise configuration d'un serveur antivirus peut également conduire à tort à la perte d'un message contaminé ou non contaminé dû à sa suppression sans en informer l'expéditeur et le destinataire.

II.3.1.2.Perte d'intégrité

Le protocole standard le plus utilisé pour la messagerie électronique est SMTP, cependant ce protocole ne satisfait pas à l'intégrité des messages étant donné qu'il n'effectue aucun contrôle sur l'expéditeur du message. Ainsi un message peut être altéré, accidentellement ou par malveillance pendant sa transmission ou son stockage, sur un serveur de messagerie ou sur le poste destinataire.

II.3.1.3.Perte de confidentialité

Une autre faiblesse du protocole SMTP réside dans le fait que les messages envoyés ou reçus sont transmis en clair sur le réseau, c'est à dire qu'ils ne sont pas chiffrés. Ainsi, toute personne écoutant sur le réseau a la possibilité de voir l'entête et le contenu du message.

S'ajoute à cela la faiblesse du protocole POP3 et IMAP qui utilise par défaut une méthode d'authentification appelée « Clear ». Un utilisateur s'authentifie au serveur en envoyant son

nom d'utilisateur et son mot de passe, qui circulent en clair sur le réseau, puis le serveur envoie les messages requis à l'utilisateur, toujours en clair. Ainsi un espionnage des messages à l'aide d'un logiciel spécialisé (sniffer) peut permettre, de recueillir les échanges de messagerie et prendre connaissance sans difficulté des mots de passe et du contenu des messages reçus ou transmis.

II.3.1.4.Usurpation de l'identité de l'émetteur

Le protocole SMTP standard ne fournit pas de moyen d'authentifier de façon sûre l'émetteur d'un message. Il est ainsi très simple de forger un message SMTP en se faisant passer pour n'importe quel émetteur, que celui-ci existe ou non. Cette possibilité est très souvent utilisée par les virus et les pourriels (spamming) afin de camoufler la source réelle de l'envoi.

II.3.1.5.La répudiation

La répudiation est le risque de reniement de l'envoi ou de la réception d'un message en absence d'un dispositif de sécurisation. Les messages reçus ou envoyés sont archivés soit sur un serveur, soit sur le poste de l'utilisateur qui n'est en général pas sauvegardés. En cas de perte du disque, la perte de ces archives peut être préjudiciable (perte de trace d'envoi ou de l'historique des échanges, perte de pièces jointes). Dans ce cas l'émetteur peut nier l'envoi d'un message ou d'un document et le destinataire peut nier la réception de celui-ci.

II.3.2.Les atteintes à l'infrastructure et au Système d'Information

II.3.2.1.Malveillance informatique

La messagerie électronique constitue un vecteur important de diffusions de programmes malveillants car elle permet d'introduire différents types de fichiers dans les machines des utilisateurs.

- **Infections informatiques**

Ce sont des programmes simples ou autoreproducteurs, à caractère offensif, s'installant dans un système d'information, à l'insu du ou des utilisateurs, en vue de porter atteinte à la confidentialité, l'intégrité ou la disponibilité du système, ou susceptible d'incriminer à tort son processus ou l'utilisateur dans la réalisation d'un crime ou d'un délit. La figure II.1 détaille les différents types d'infections informatiques.

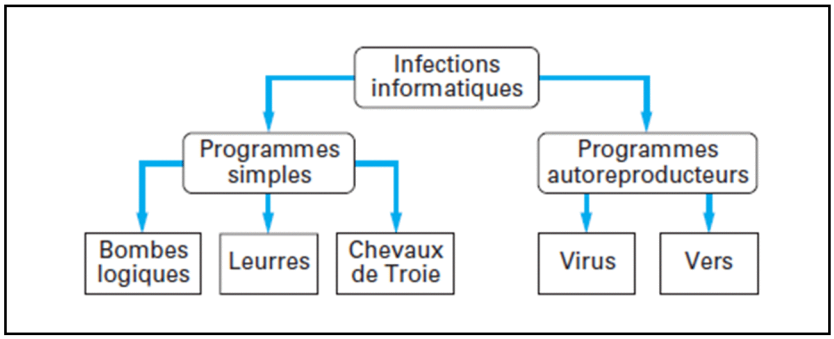


Figure II.1: classification des infections informatiques

- **Infections simples**

Le mode propre de ces programmes, comme leur nom l'indique, est de simplement s'installer dans le système. L'installation se fait généralement :

✓ **En mode résident**

Le programme est résident (processus actif en mémoire de façon permanente) afin de pouvoir agir tant que le système fonctionne.

✓ **En mode furtif**

L'utilisateur ne doit pas se rendre compte qu'un tel programme, puisque résident, est présent dans son système.

✓ **En mode persistant**

En cas d'effacement ou de désinstallation, le programme infectant est capable par différentes techniques de se réinstaller dans la machine indépendamment d'un dropper (sous Windows généralement, plusieurs copies de ce programme sont cachées dans les répertoires systèmes et une ou plusieurs clefs dans la base de registres sont ajoutées par le programme lors de l'installation initiale, afin d'assurer la réinstallation). Ce mode permet également, au démarrage de la machine, de lancer le programme infectieux en mode résident.

Au final, il est essentiel de noter qu'une seule erreur de l'utilisateur suffit. Tant que le programme infectieux n'aura pas été complètement éradiqué, le système sera corrompu.

On peut citer les programmes simples infectants suivants :

- **Bombe logique**

Programme infectant simple s'installant dans le système et qui attend un événement (date, action, données particulières, etc.) appelé en général « gâchette », pour exécuter sa fonction offensive. Ces programmes constituent assez souvent la charge finale d'un virus (par exemple,

le virus Vendredi 13). C'est la raison pour laquelle les bombes logiques sont souvent assimilées par erreur aux virus et aux vers.

- **Cheval de Troie**

Programme simple composé de deux parties, le module serveur et le module client (figure II.2). Le module serveur, installé dans l'ordinateur de la victime, donne discrètement accès à tout ou à une partie de ses ressources à l'attaquant, qui en dispose via le réseau (en général), grâce à un module client (il est le « client » des « services » délivrés inconsciemment par la victime). Le module client recherche sur le réseau, grâce à la commande ping, les machines infectées par le module serveur puis en prend le contrôle, lorsqu'il a obtenu en retour l'adresse IP et le port (TCP ou UDP) des machines accessibles. Cette prise de contrôle lui permet de mener un nombre plus ou moins grand, selon la nature du Cheval de Troie, d'actions offensives : redémarrage de la machine, transfert de fichiers, exécution de code, destruction de données, etc. L'exemple le plus célèbre de Cheval de Troie est le logiciel Back Orifice.

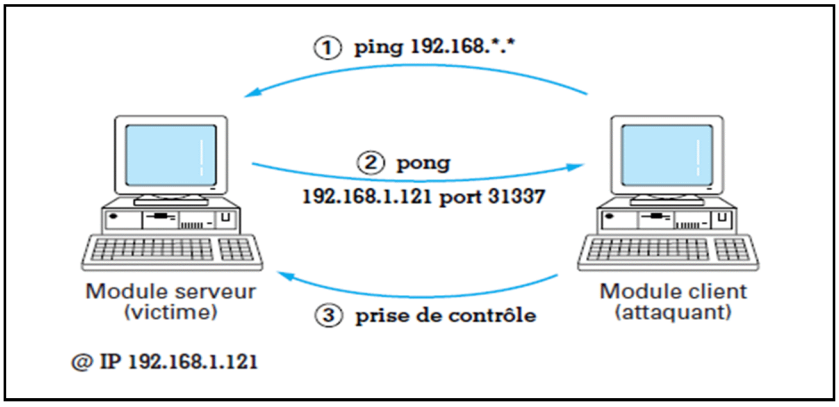


Figure II.2: Mécanisme d'action d'un cheval de Troie

- **Leurres (Hoax)**

On peut classer dans cette catégorie les faux virus (hoax), qui propagent de fausses informations ou qui font perdre beaucoup de temps de lecture aux destinataires. Ces faux virus peuvent être dangereux. Certains d'entre eux recommandent de supprimer des fichiers supposés être des virus alors qu'il s'agit de fichiers indispensables au fonctionnement du système d'exploitation.

- **Programmes autoreproducteurs**

La finalité d'un programme autoreproducteur est identique à celle d'un programme simple. Il s'agit de perturber ou de détruire. A sa première exécution, le programme cherche à se reproduire. Il sera donc généralement résidant en mémoire et dans un premier temps discret.

Comme leur nom l'indique, leur finalité est de se dupliquer, afin de se diffuser et de se propager, via les vecteurs pour lesquels ils ont été programmés.

- **Virus**

Un virus informatique est un programme, intégré dans un programme hôte ou localisé dans un champ spécifique de la mémoire, capable lors de son exécution de créer une copie de lui-même. Un virus doit contenir au moins deux parties pour pouvoir se reproduire lui-même :

Un algorithme de recherche d'un fichier hôte à infecter, et un algorithme de recopie sur le fichier hôte. On y ajoute éventuellement une troisième étape (destruction, espionnage, etc.).

La messagerie électronique offre un principal vecteur de transmission des virus par le biais d'une pièce jointe ou par l'utilisation du carnet d'adresse d'un utilisateur pour envoyer des messages à tous les contacts. De nombreux types de fichiers joints dans un courriel sont susceptibles de contenir ces programmes exécutables. Il s'agit naturellement des programmes (extensions .exe, .dll, .bat, .vbs,…etc), mais également de toutes sortes de fichiers de données « évolués » (extensions .doc, .xls, .pdf, .pps,…etc) qui contiennent des macro-instructions exécutées à l'ouverture ou lors de l'activation de certaines fonctions.

- **Vers**

Le ver peut être défini comme un virus de réseau, il profite en effet des fonctionnalités des réseaux informatiques pour se propager. Il infecte un réseau et non pas un simple ordinateur, il n'est de plus présent qu'en un seul exemplaire sur le système. Étant donné qu'il utilise les possibilités offertes par les réseaux, généralement le courrier électronique, pour se propager, il expédie une copie de lui-même à d'autre systèmes lorsque celui-ci est dans un format de page web incluant des scripts (appelé les vers de courriers électroniques ou « mass-mailing worm »). Son pouvoir infectieux est donc beaucoup plus important, pouvant faire le tour du monde en quelques minutes.

II.3.2.2.L'indisponibilité du serveur de messagerie

La messagerie fait de plus en plus partie intégrante du processus de l'entreprise. L'indisponibilité de la messagerie doit être prise en compte au même titre que les applications métiers, car elle peut conduire à une forte dégradation, voire à une interruption de service. Cette interruption peut être accidentelle (panne, destruction de locaux…) ou malveillante

(attaque de type « déni de service » du serveur de messagerie, d'une attaque virale ou de l'envoie de spam).

II.3.2.3.Le déni de service (DOS)

Le but d'une telle attaque n'est pas de dérober des informations sur une machine distante, mais de paralyser durant une certaine période les services ou les ressources d'une organisation. Ce déni de service peut être réalisé en sollicitant excessivement des ressources. Ne possédant pas la capacité de traiter un tel afflux de demandes, les systèmes ciblés, surchargés par un trop grand nombre de requêtes, s'effondrent et deviennent indisponibles, ou encore en exploitant une faille du système distant afin de le rendre inutilisable. Voici quelques attaques qui exploitent des failles de la messagerie et qui causent un déni de service.

- **Messages non sollicités (Spams)**

Un spam est un message reçu par un utilisateur sans qu'il l'ait sollicité, souvent envoyé en masse par des logiciels automatisés. Ces logiciels utilisent des listes d'adresses de messagerie collectées sur les sites web et les services de messagerie instantanée (newsgroups), etc.

Certains virus récents ont même été conçus pour la collecte de telles adresses ainsi que pour la transmission de spam. Les deux conséquences principales du spam sont la réduction des ressources informatiques (bande passante du réseau et performances des serveurs), ainsi que la perte de temps pour les utilisateurs (lecture et suppression de spam).

- **Inondation de messages (Mailbombing)**

Le mail bombing consiste à envoyer plusieurs milliers de messages identiques à une boîte aux lettres électronique afin de la saturer. En effet les mails sont stockés sur un serveur de messagerie, jusqu'à ce qu'ils soient relevés par le propriétaire du compte de messagerie. Ainsi lorsque celui-ci relèvera le courrier, ce dernier mettra beaucoup trop de temps et la boîte aux lettres deviendra alors inutilisable...

II.3.2.4.Vulnérabilités des clients de messagerie

Comme tout logiciel, un client de messagerie peut comporter des vulnérabilités. Si celles-ci concernent les fonctions de décodage ou d'affichage des messages, on peut aboutir à des vulnérabilités exploitables à distance par l'envoi d'un simple message, avec exécution de code en local. Un exemple simple serait un client de messagerie qui provoquerait un débordement de tampon lorsque le sujet d'un message dépasse 1024 caractères. Un attaquant peut alors forger

un message avec un sujet très long, et faire exécuter le code de son choix par la machine vulnérable qui recevrait ce message.

II.2.2.5.Vulnérabilités du webmail

L'utilisation du webmail expose l'entreprise à divers menaces (espionnage, usurpation d'identité, intrusion, virus, ver…) car Lorsque les utilisateurs du réseau interne ont accès à Internet via le protocole HTTP, ils peuvent utiliser les interfaces Web de nombreux fournisseurs pour envoyer et recevoir des messages personnels. Ces messages sont émis et reçus à partir d'un serveur situé sur Internet. En dehors du réseau interne, Les échanges de données circulent donc en clair à travers le réseau et ne sont pas analysés par la passerelle de filtrage des messages.

II.3.2.6.L'utilisation abusive des relais ouvert « open relay »

Une bonne configuration d'un serveur de messagerie n'accepte que des expéditeurs et des destinataires appartenant à son domaine local ou à sa plage d'adresse IP. L'absence ou l'insuffisance d'une sécurisation permet à des tiers non autorisés appartenant à des réseaux quelconques d'envoyer des courriers électroniques, qui se sert de ce serveur de messagerie pour expédier des mails souvent illicites (spams), on parle alors de relais ouverts. Par conséquent, Le risque est d'être inscrit chez les fournisseurs d'accès Internet contenant une liste des relais ouverts « black-list » (son adresse IP publique devient inutilisable tant que le relai reste ouvert), afin d'interdire la réception de messages provenant de tels serveurs.

II.3.3.Les atteintes à l'organisation et à l'utilisation du système de messagerie de l'entreprise

II.3.3.1.Les contenus illicites ou offensants

La loi interdit la diffusion de certains contenus (racistes, trafics divers…). Les auteurs mais également les entreprises qui offrent les services de messagerie peuvent être sévèrement condamnés. Un autre risque de la messagerie est la diffusion de messages offensants, anonymes (utilisation d'une adresse d'émetteur factice) ou au nom d'une autre personne.

II.3.3.2.L'utilisation abusive

La messagerie d'entreprise est mise à disposition des employés pour les besoins de service. La jurisprudence reconnaît cependant un droit à son utilisation à des fins privées. Si elle reste marginale, cette pratique est supportable par l'entreprise.

Une utilisation abusive peut cependant être la source de nuisance : encombrement des espaces disques par des fichiers volumineux (musique, vidéo…), encombrement de la bande passante, sans compter la perte de temps consacrée à ces activités.

II.3.3.3.Accomplissement d'actes frauduleux par la messagerie

L'utilisation de la messagerie à des fins d'extorsion, de racket ou de chantage entrainant des préjudices pour l'entreprise (perte financière, atteinte à l'image, divulgation d'informations confidentielles, , etc.).

II.3.3.4.Hameçonnage (phishing)

La technique du phishing est une technique d'«ingénierie sociale» c'est-à-dire consistant à exploiter non pas une faille informatique mais la «faille humaine» en dupant les internautes par le biais d'un courrier électronique semblant provenir d'une entreprise de confiance (une banque, un site de commerce, etc.).

Le mail envoyé par ce pirate usurpe l'identité d'une entreprise et les invite à se connecter en ligne par le biais d'un lien hypertexte et de mettre à jour des informations les concernant dans un formulaire d'une page web factice, copie conforme du site original, en prétextant par exemple une mise à jour du service, une intervention du support technique, etc. Ainsi, par le biais du formulaire, les pirates réussissent à obtenir les identifiants et mots de passe des internautes ou bien des données personnelles ou bancaires (numéro de client, numéro de compte en banque, etc.).

II.4.La Sécurité informatique

La sécurité informatique est l'ensemble des moyens mis en œuvre dans le but de diminuer le risque à un niveau acceptable dans un contexte donné, et dépend de l'importance accordée par les administrateurs aux ressources à protéger et aux risques encourus. Pour ce faire, il faut bien connaitre toutes les composantes du risque et avoir une vision globale et cohérente des valeurs et mesures de sécurité. Elle passe par la définition d'une politique de sécurité, la motivation et la formation du personnel, la mise en place des mesures ainsi que l'optimisation des solutions.

II.4.1.Définition de la politique de sécurité

La politique de sécurité est le document de référence définissant les objectifs poursuivis en matière de sécurité et les moyens mis en œuvre pour les assurer.

La politique de sécurité définit un certain nombre de règles, de procédures et de bonnes pratiques permettant d'assurer un niveau de sécurité conforme aux besoins de l'organisation. Un tel document doit nécessairement être conduit comme un véritable projet associant des représentants des utilisateurs et conduit au plus haut niveau de la hiérarchie, afin qu'il soit accepté par tous. Lorsque la rédaction de la politique de sécurité est terminée, les clauses concernant le personnel doivent leur être communiquées, pour donner à la politique de sécurité le maximum d'impact.

II.4.2.Objectifs de la sécurité et fonctions associées

Tout programme de sécurité a pour objectif de protéger des éléments d'informations. Trois caractéristiques clés composent ce qu'on appelle le triangle CID (ou le triangle des fonctionnalités de sécurité) : Confidentialité, Intégrité et Disponibilité. Associés, ils doivent être au cœur et à l'origine de toutes les décisions de sécurité. De même, les risques, menaces et vulnérabilité se mesurent par leur capacité à compromettre un ou plusieurs principes du triangle CID.

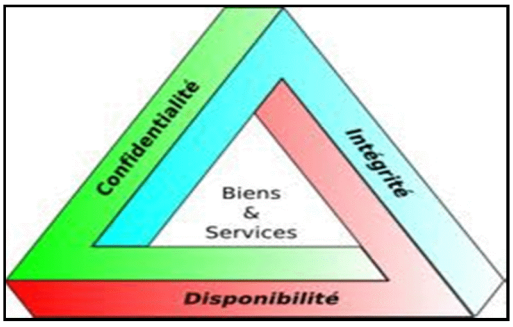


Figure II.3: Triangle CID

- **Confidentialité**

Garantir la confidentialité des données empêche une entité tierce non autorisée, de récupérer ces données et de les exploiter. Seuls les utilisateurs autorisés doivent être en mesure de prendre connaissance du contenu des données. Un message ou un échange de messages à sa confidentialité garantie dès lors que tout utilisateur non autorisé qui aurait pu le récupérer ne peut pas l'exploiter.

- **Intégrité**

L'intégrité garantit l'état inchangé des données afin de maintenir la précision et la fiabilité des informations, elle englobe deux concepts importants :

- ✓ **Intégrité des sources :** assure que l'expéditeur est celui qui prétend être.
- ✓ **Intégrité des données :** assure que les informations reçues n'ont pas été modifiées lors de la transmission.

Les agents de sécurité liés à l'intégrité assurent une protection contre des interventions malveillantes ou la contamination des informations. Les attaques contre l'intégrité susceptibles d'altérer les informations lors de la transmission(ou avant la réception) ou d'apparaitre comme provenant d'une source fiable alors que ce n'est pas le cas. Par exemple, le phénomène d'hameçonnage (phishing) redirige les utilisateurs vers un site web qui semble être approuvé, mais qui est en réalité dirigé par un utilisateur malveillant.

- **Disponibilité**

La disponibilité garantit l'accès fiable des données aux utilisateurs autorisés, dans un intervalle de temps raisonnable. Cela signifie la probabilité de pouvoir mener correctement à terme une session de travail. La disponibilité d'une ressource est indissociable de son accessibilité, elle est mesurée sur la période de temps pendant laquelle le service offert est opérationnel. Le volume potentiel de travail susceptible d'être pris en charge durant la période de disponibilité d'un service, détermine la capacité d'une ressource par exemple dans le cas du service de messagerie.

A ces trois critères s'ajoute celle qui permet de prouver l'identité des entités (notion d'authentification) et celle qui indique que des actions ou événements ont bien eu lieu (notion de non-répudiation).

- **Authentification**

L'authentification permet de vérifier l'identité annoncée et de s'assurer de la non usurpation de l'identité d'une entité. Pour cela, l'entité devra reproduire une information spécifique telle que : un code, un mot de passe, une empreinte biométrique, etc. Ce critère assure :

- ✓ La confidentialité et l'intégrité des données : seules les entités identifiées et authentifiées peuvent accéder aux ressources ou les modifier.
- ✓ La non-répudiation : seules les entités identifiés et authentifiées ont pu réaliser telle action (preuve de l'origine d'un message ou d'une transaction, preuve de la destination d'un message...etc.).

- **Non-répudiation**

La non-répudiation est le fait de ne pouvoir nier ou rejeter qu'une action a eu lieu. A ce critère de sécurité sont associées les notions d'imputabilité, traçabilité et éventuellement d'auditabilité.

✓ **L'imputabilité** : est l'affectation certaine d'une entité à une action ou à un événement, elle est liée à la notion de responsabilité. Cette action est réalisée par l'ensemble des exigences garantissant l'enregistrement des informations pertinentes sur l'utilisateur agissant.

✓ **La traçabilité :** elle mémorise l'origine d'un message, d'un événement, d'une information ou d'une donnée. Elle permet par exemple, de retrouver l'adresse à partir de laquelle ces données ont été envoyées.

✓ **L'auditabilité :** se définit par la capacité d'un système à garantir la présence des informations nécessaires à une analyse ultérieure d'un événement dans le cadre de procédures de contrôle, afin de déterminer s'il y'a effectivement eu violation de la sécurité, et dans ce cas, quelles informations ou autres ressources ont été compromises. C'est également la fonction destinée à examiner les événements susceptibles de constituer une menace pour la sécurité. Afin de garder la trace des événements, on a recourt à des solutions informatiques qui permettent de les enregistrer (journaliser) sous des fichiers logs.

II.5.La sécurisation de la messagerie électronique

Compte tenu de tous les problèmes cités précédemment, un réseau utilisant la messagerie doit se protéger pour réduire les risques au minimum. Le niveau de protection et les contraintes associées doivent être adaptés aux besoins de sécurité du système protégé, notamment en termes de disponibilité, de confidentialité et d'intégrité. Bien sûr, toute mesure de protection doit aussi être compatible avec les besoins des utilisateurs pour que le service soit opérationnel.

II.5.1.Protocoles de messagerie sécurisés

La sécurisation des échanges par les protocoles de messagerie SMTP, POP et IMAP et le protocole HTTP est réalisée via le protocole Couche Points d'Accès Sécurisés (SSL : Secure Socket Layer). C'est une couche protocolaire qui s'intercale entre un protocole d'une couche réseau orientée connexion (TCP/IP) et une couche protocolaire d'application de messagerie. Il

fournit une communication sécurisée entre client et serveur en permettant l'authentification mutuelle, l'utilisation des signatures numériques pour la vérification de l'intégrité des données, et le chiffrement pour la confidentialité. Elle utilise deux mécanismes :

- ✓ **Négociation (Poignée de main « handshake »)** : Les deux entités communicantes s'authentifient par la certification, et négocient le niveau de sécurité à appliquer au transfert (la version SSL, la méthode de chiffrement, la langueur de clé…).
- ✓ **Communication (record)** : Les données transmises sont alors découpées, compressées, chiffrées puis envoyées. Et à la réception les données subissent le processus inverse.

Il existe plusieurs versions du protocole SSL dont la version TLS (Transport Layer Security).

II.5.1.1.Intégration du protocole TLS au protocole SMTP(SMTPS)

L'intégration du TLS dans le protocole SMTP se fait grâce à une extension de commande STARTTLS qui permet :

- ✓ l'authentification forte des serveurs SMTP (via un certificat).
- ✓ l'établissement d'une session TLS (chiffrée) entre 2 serveurs (MTA-MTA).
- ✓ l'authentification forte des clients SMTP (via un certificat).
- ✓ l'établissement d'une session TLS (chiffrée) entre le client et le serveur (MUA-MTA).

L'authentification entre client et serveur est réalisé grâce à l'utilisation du certificat X.509. Lors de la phase de négociation de départ (EHLO), le serveur indique qu'il supporte le mode sécurisé STARTTLS, le client peut alors utiliser le mode TLS qui permet de sécuriser l'échanges des informations.

II.5.1.2.La sécurisation des protocoles IMAP et POP3 (IMAPS/POPS3)

Les protocoles POPS3 et IMAPS répondent au problème de la transmission des mots de passes en clair, en introduisant l'extension STLS pour POP3 et STARTTLS pour IMAP. Tout comme pour SMTP, ces commandes permettent de passer en mode TLS une fois la connexion établie. Elles permettent également, d'authentifier de façon forte le client et de remplacer le couple username/password par un certificat client.

II.5.1.3.Le Webmail sécurisé par HTTPS

Les solutions retenues pour sécuriser le webmail sont : l'utilisation du HTTPS qui est la variante de HTTP utilisé pour l'accès sécurisé à un serveur Web. Si on indique HTTPS dans

l'URL au lieu de la mention HTTP normale, le message sera adressé vers un port d'entrée sécurisé du serveur. Le dialogue entre le navigateur Web et le serveur sera alors géré avec les contraintes de sécurité. En particulier, les échanges de données seront cryptés et l'utilisateur sera généralement identifié. Pour obtenir une protection homogène, il est nécessaire d'appliquer le même type de filtrage sur les fichiers téléchargés par les protocoles HTTPS et FTP que sur les pièces jointes des messages reçus par SMTP.

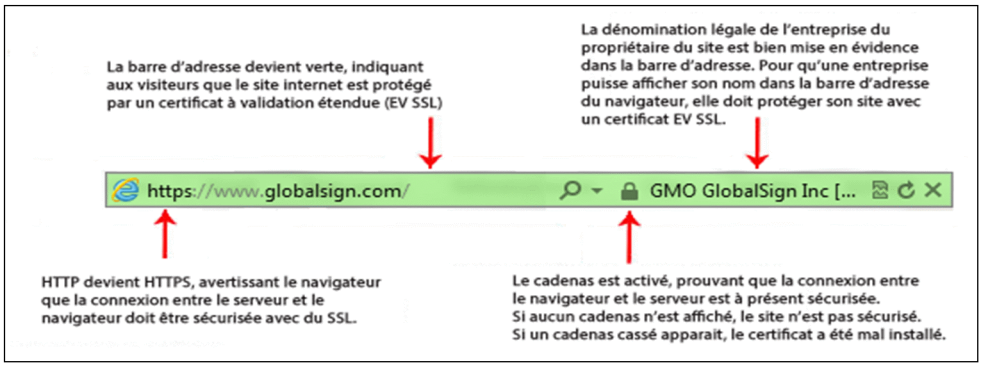


Figure II.4 : la connexion HTTPS

II.5.1.4.TELNETS

Telnet est sécurisé par un tunnel SSH**,** qui est un protocole permettant d'établir une session interactive chiffrée entre un client et un serveur. Ainsi, les flux d'informations entre ces deux entités sont cryptés, ce qui garantit la confidentialité. De plus, il permet l'identification de la machine distante. L'algorithme utilisé pour la négociation des clés est RSA. Une fois l'échange des clés effectué la communication entre les deux machines se fait en utilisant un chiffrage symétrique. Les principaux algorithmes utilisés dans SSH sont le triple DES (3DES) et le Blowfish.

II.5.1.5.Le protocol PGP (Pretty Good Privacy)

Est une solution utilisée pour rendre confidentielle la transmission des messages et authentifier l'émetteur. Cette alternative pose le problème de sa compatibilité avec le format des messages du système de messagerie MIME, mais s'exécute sur un grand nombre de plates-formes dont Windows et Unix.

PGP passe par cinq étapes permettant de renforcer la sécurité des messages transférés, à savoir : l'authentification par signature digitale, la confidentialité par chiffrement, la compression ZIP, la compatibilité par des mécanismes de conversions de formats, la segmentation et le réassemblage.

Cette solution se base sur l'algorithme IDEA pour le chiffrement des messages, sur MD5 pour le hash du résumé, sur RSA pour le chiffrement du résumé et pour l'échange de la clé privée nécessaire à IDEA. Cette dernière est générée de façon aléatoire au moment du chiffrement et utilisée une seule fois. PGP utilise optionnellement la compression ZIP d'un message avant son chiffrement.

Le tableau II.1 illustre les ports liés aux protocoles sécurisés.

Protocole sécurisé	**Port**	Application
HTTPS	**443**	Web sécurisé
SMTPS	**465**	sécurisation du Transport de courrier
IMAPS	**993**	Accès sécurisé aux boîtes aux lettres
POPS3	**995**	
TELNETS	**992**	Connexion interactive sécurisée

Tableau II.1: Les ports liés aux protocoles sécurisés

II.5.2.S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) est une norme de cryptographie de courriel encapsulé en format MIME. Elle propose des services d'authentification par signature et de confidentialité par chiffrement.

La signature du message est réalisée par chiffrement via la clé privée de l'émetteur (RSA, DSS) d'un résumé du message (message digest) créé par SHA-1 ou MD5. Les clés de sessions sont générées via l'algorithme Diffie-Hellman. Les algorithmes de chiffrement RSA, DES, RC2/40 sont supportés par S/MIME.

II.5.3.La Cryptologie

II.5.3.1.Chiffrement du message électronique

Le chiffrement apporte la sécurisation des messages. Il permet d'assurer la confidentialité et l'intégrité de ceux-ci, l'authentification de l'émetteur et la garantie de la non répudiation des échanges. L'opération de chiffrement consiste à coder le message à l'aide d'algorithmes de chiffrement afin de le transmettre sur un réseau non sécurisé sans être intercepté par un tiers non autorisé qui ne possède pas la clé de déchiffrement.

Les algorithmes de chiffrement peuvent être classés en deux catégories

- **Les algorithmes symétriques**

Les algorithmes symétriques utilisent la même clé pour chiffrer puis déchiffrer un message. L'émetteur et le destinataire doivent posséder la même clé secrète pour rendre confidentielles les données du message et pour pouvoir les comprendre. Les principaux algorithmes symétriques sont : AES, DES, TRIPLE DES, IDEA, etc.

- **Les algorithmes asymétriques**

Un système de chiffrement asymétrique est basé sur l'usage d'un couple unique de deux clés complémentaires, l'une est une clé publique et l'autre est une clé privée. Avec ce système de chiffrement, l'émetteur chiffre un message avec la clé publique et le destinataire le déchiffre avec sa clé privée. Ainsi le message est confidentiel pour le destinataire dans la mesure où lui seul peut le déchiffrer. Le principal algorithme asymétrique est RSA.

II.5.3.2.Signature électronique du message

Au même titre que la signature manuscrite, la signature électronique est un procédé qui permet, l'authentification d'un signataire ainsi que la manifestation de son consentement par rapport au contenu du document signé. La signature électronique est un dispositif dérivé du cryptage, l'émetteur doit disposer d'une bi-clé (clé privée et clé publique associé).

Le message de l'émetteur est crypté avec sa clef privée et ne peut être lu par les destinataires qu'avec la clé publique de celui-ci. Un document à signer est tout d'abord traité par une fonction de Hachage qui permet d'obtenir une empreinte digitale de l'émetteur, celle-ci est ensuite cryptée avec la clé privée du signataire. Le résultat obtenu constitue la signature électronique du document.

La signature électronique procure la non répudiation et l'intégrité du document et produit sur le système de messagerie un environnement de confiance lors des échanges de documents.

- **Etapes**

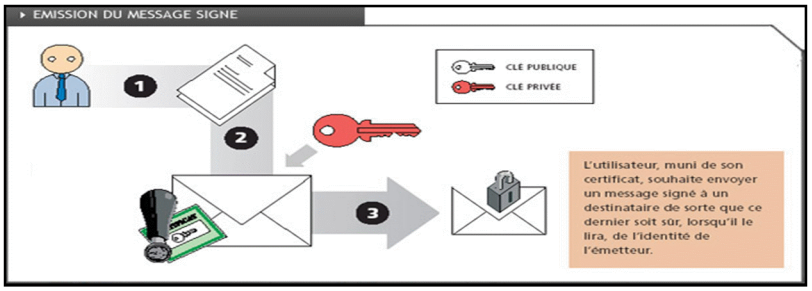


Figure II.5 : transmission d'un message signé

1. Le titulaire du certificat rédige le message qu'il souhaite adresser.

2. Il signe son message avec sa clé privée.

3. Le message transmis au destinataire est composé à la fois du message rédigé par l'expéditeur, de la signature chiffrée de ce message et du certificat de l'expéditeur comportant sa clé publique.

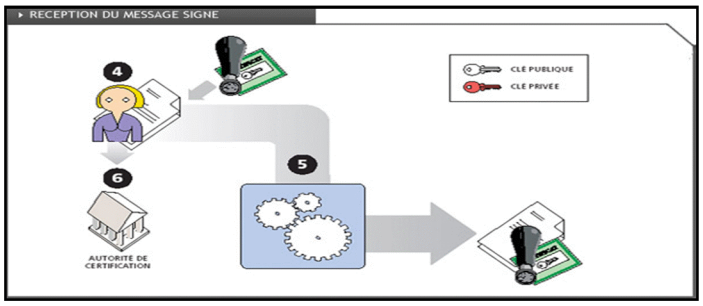


Figure II.6: réception d'un message signé

4. Le destinataire reçoit le message signé de l'expéditeur.

5. Son logiciel de messagerie commence la vérification de la signature.
6. La deuxième vérification consiste à contrôler que le certificat est toujours valide et n'est pas révoqué.

II.5.3.3.PKI (public key infrastructure ou Infrastructure de Gestion de clés « IGC »)

Le chiffrement des messages et la réalisation des signatures électroniques nécessitent la certification. Un certificat électronique constitue la carte d'identité numérique d'une entité (utilisateur) ou d'une ressource informatique à qui il appartient (serveur web, routeur, etc.). Ce certificat est émis par une infrastructure appelée PKI, qui est une entité responsable de l'émission, de la délivrance et de gestion des certificats pour garantir l'identité de son

propriétaire et l'établissement d'un environnement de confiance entre des entités distantes lors d'un échange de messages annexés par des documents importants.

Les autorités de certification nécessitent trois rôles principaux :

- **l'Autorité de Certification** (AC), dont la fonction est de définir la Politique de Certification, de la faire appliquer et de garantir ainsi un certain niveau de confiance aux utilisateurs. Elle est juridiquement responsable des certificats émis.

- **l'Autorité d'Enregistrement** (AE), dont la fonction est de mettre en œuvre les procédures d'identification des personnes physiques conformément aux règles définies par l'Autorité de Certification. Son but est d'établir que le demandeur a bien l'identité et les attributs qui seront indiqués dans le certificat. L'Autorité d'Enregistrement est le lien entre l'Autorité de Certification et le Titulaire.

- **l'Opérateur de Certification** (OC), qui assure la partie technique de la fourniture et de la gestion du cycle de vie des certificats ainsi que leur archivage. Son rôle consiste à mettre en œuvre, sous la responsabilité de l'AC, une plate-forme opérationnelle, fonctionnelle et sécurisée, dans le respect des exigences énoncées dans la Politique de Certification.

- **Etapes**

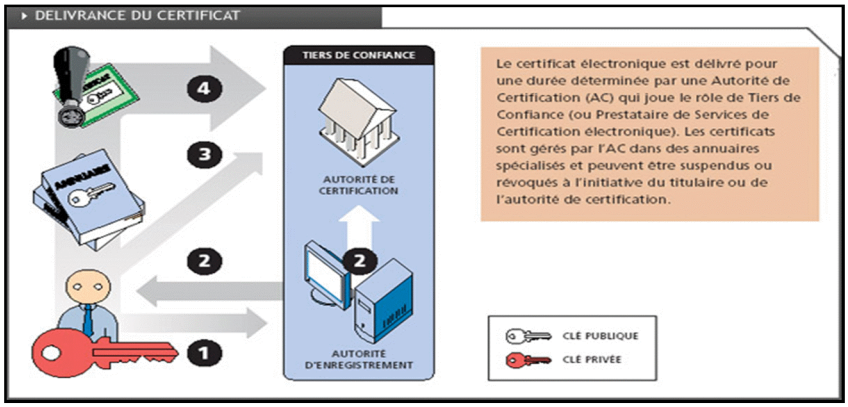


Figure II.7 : délivrance du certificat.

1. L'utilisateur prend contact avec une Autorité d'Enregistrement (AE) et fournit un dossier permettant de l'identifier (nom, prénom, adresse, etc.).
2. Après vérification, l'AE valide la demande de certificat et en informe l'utilisateur, puis transmet les informations à l'Autorité de Certification (AC) qui gérera le certificat. Celle-ci génère le certificat, le signe avec sa clé privée et lui ajoute son identification en tant qu'AC.

3. L'utilisateur se connecte auprès du Tiers de Confiance. Une procédure permet de s'assurer que la délivrance du certificat sera réalisée exclusivement auprès de celui-ci.
4. Le certificat signé par l'AC est expédié à l'utilisateur.

II.5.4.Traçabilité des échanges

La traçabilité a pour objectif de conserver la preuve des échanges c'est-à-dire la non répudiation. Dans la messagerie électronique, la preuve se construit autour des étapes d'identification et d'authentification de l'émetteur et destinataire, du contrôle d'intégrité des échanges, de confidentialité, d'horodatage et d'archivage.

La garantie de la traçabilité nécessite l'enregistrement de certains paramètres (émetteur, destinataire, taille du message, date et heure…) lorsque les courriels passent par le serveur, puis archivés et indexés de sorte qu'ils puissent être retrouvés et restitués en cas de besoin. De ce fait l'intégrité du système d'archivage est indispensable.

L'étape d'horodatage consiste à attacher un temps certain à un événement (création, signature, envoie, réception, etc.), elle sera fournie par une autorité de confiance choisie par les émetteurs et les destinataires.

II.5.5.Sécurisation des infrastructures

Pour protéger un système utilisant un service de messagerie connecté à Internet, on utilise différentes technologies : des techniques de filtrage, qui consiste à placer une passerelle de messagerie en coupure entre Internet et le serveur interne. Cette passerelle peut être constituée d'un pare-feu applicatif ou bien d'une DMZ. Suivant le résultat des divers filtres mis en œuvre, un message peut être accepté tel quel, placé en quarantaine ou bien modifié. Et une technique appelée les réseaux privés virtuels (VPN : virtuel private network) qui relie les réseaux internes par une liaison privé via internet en implémentant des tunnels chiffrés. La figure II.5 illustre l'architecture générale des différentes technologies.

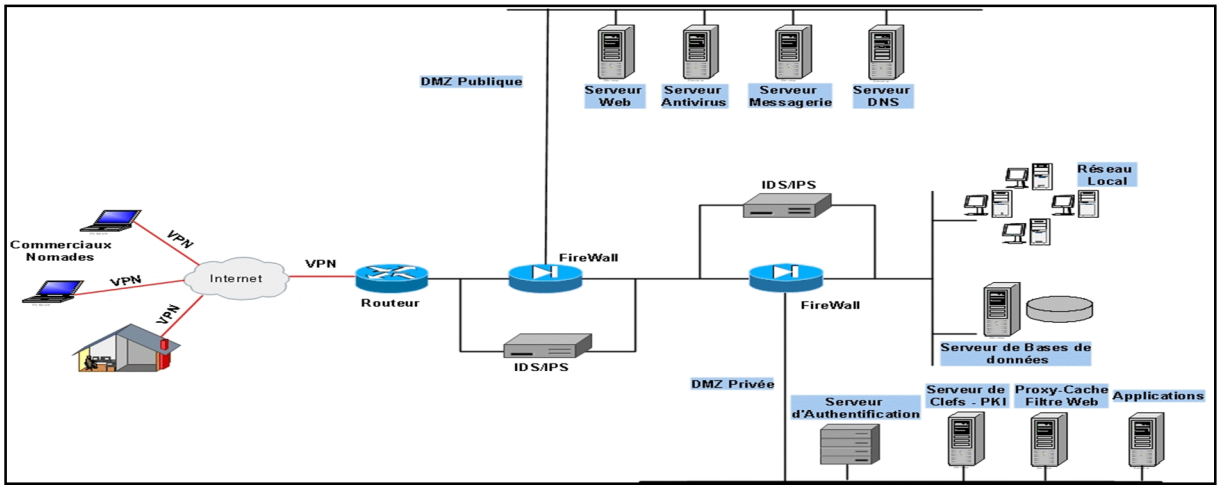


Figure II.8 : Architecture générale

II.5.5.1.Les logiciels antivirus

Il s'agit de logiciels capables de détecter et de détruire les différentes infections informatiques contenues sur des unités de stockage (disque, périphériques…). Leur utilisation reste importante car ils sont principalement installés sur les postes de travail des utilisateurs qui restent un maillon faible de la sécurité. Le logiciel a pour charge de surveiller la présence de virus et éventuellement de nettoyer, supprimer ou mette en quarantaine le ou les fichiers infectés. Le programme est composé de trois parties ayant chacune un rôle essentiel :

- ✓ Un « moteur » qui a pour rôle la détection des virus.
- ✓ Une base de données contenant des informations sur les virus connus.
- ✓ Un module de nettoyage qui a pour but de traiter le fichier infectés.

Les virus peuvent être combattus à plusieurs niveaux. On distingue Deux modes de protection:

- ✓ Généralisation de l'antivirus sur toutes les machines, il faut absolument prévoir une mise à jour automatique de tous les postes via le réseau.
- ✓ Mise en place d'un antivirus sur les points d'entrée/sortie de données du réseau (au niveau du serveur de messagerie, serveur relai…) après avoir parfaitement identifiés tous ces points la rigueur de tout le personnel pour les procédures doit être acquise.

II.5.5.2.présentation d'un pare-feu

Un pare-feu (appelé aussi coupe-feu, garde-barrière ou firewall en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un

réseau tiers (notamment internet). Le pare-feu est en réalité un système permettant de bloquer des ports TCP, c'est-à-dire en interdire l'accès aux personnes provenant de l'extérieur.

Il existe deux types de pare-feu ceux qui opèrent au niveau des paquets, en acceptant ou rejetant ceux-ci selon le contenu des informations dans l'en-tête de paquet. Et ceux qui opèrent au niveau d'une application, fournissant des proxies d'application fiables, il s'agit ainsi d'une passerelle filtrante comportant au minimum une interface pour le réseau à protéger (réseau interne) et une interface pour le réseau externe. Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. Le pare-feu permet de :

- ✓ Contrôler le trafic sortant d'un réseau, et notamment éviter que les utilisateurs accèdent à certains nœuds du réseau.
- ✓ Sécuriser le trafic entrant d'un réseau, et empêcher certains nœuds extérieurs de se connecter un réseau local.
- ✓ Pour une question de vigilance, éviter que certaines machines mal configurées du réseau local n'envoient des données vers l'extérieur.

• Pare-feu applicatif

Un pare-feu applicatif joue un rôle de filtre des flux applicatifs. Pour le paramétré correctement il faut connaitre l'ensemble des applications qui le traverseront. Il peut également jouer le rôle de passerelle applicative, de proxy (serveur proxy, pare-feu proxy). Il établit en lieu et place de l'utilisateur le service invoqué par celui-ci en masquant certaines informations et en validant chaque contenu.

L'objectif d'un système qualifié de proxy est de réaliser un masquage d'adresse par relais applicatif, et de rendre transparent l'environnement interne de l'organisation. Il est censé constituer un point de passage obligé pour toutes les applications qui nécessitent un accès internet. Cela suppose qu'une application « relai » soit installé sur le poste de travail de l'utilisateur et sur le pare-feu.

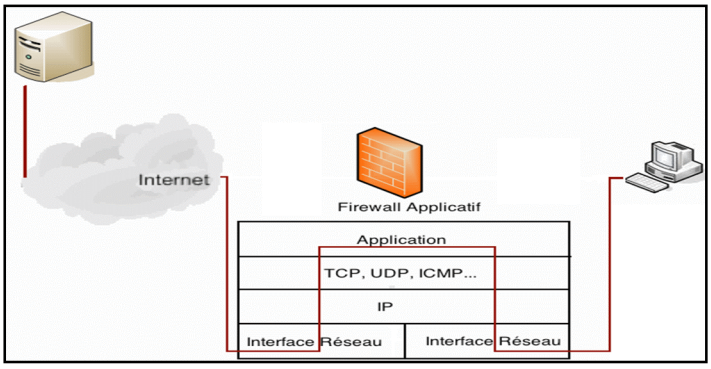


Figure II.9 : le pare-feu applicatif

II.5.5.3.Mise en place d'une architecture sécurisée en DMZ

Lorsque le serveur de messagerie du réseau interne a besoin d'être accessibles de l'extérieur, il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de « **Zone Démilitarisé** » (notée **DMZ**) pour désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile.

Cette architecture devrait comporter deux serveurs de messagerie minimum pour limiter les risques d'attaques, le premier serveur est positionné au niveau de la zone démilitarisée (DMZ) et sert de relais entre le réseau local et l'extérieur. Le deuxième serveur est positionné dans le réseau local.

La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

- ✓ Trafic du réseau externe vers la DMZ autorisé.
- ✓ Trafic du réseau externe vers le réseau interne interdit.
- ✓ Trafic du réseau interne vers la DMZ autorisé.
- ✓ Trafic du réseau interne vers le réseau externe autorisé.
- ✓ Trafic de la DMZ vers le réseau interne interdit.
- ✓ Trafic de la DMZ vers le réseau externe refusé.

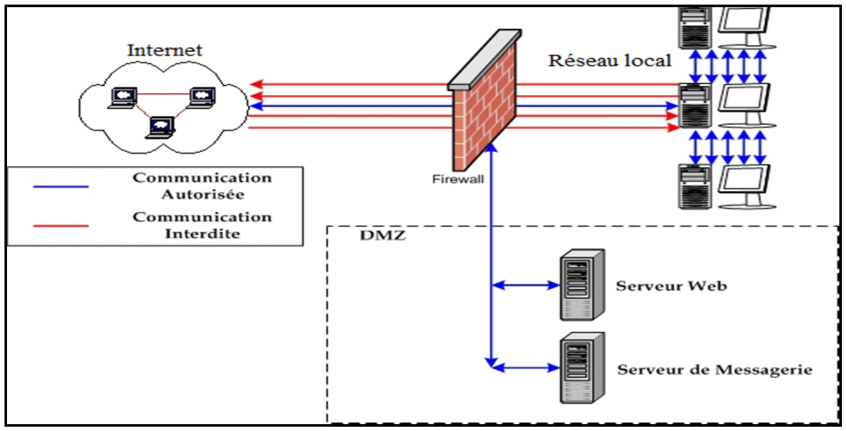


Figure II.10 : Architecture en DMZ

II.5.5.4.Mise en place des liaisons sécurisées VPN

Les réseaux locaux de type LAN permettent de faire communiquer les différents utilisateurs d'une société (exemple : partage de données par le biais de la messagerie électronique). Ces réseaux sont relativement sûr car ils sont quasiment toujours derrière une série de pare-feu ou coupés d'Internet et que le chemin emprunté par les données ne quitte pas l'entreprise. Il arrive souvent, que les entreprises aient besoin de communiquer avec des filiales, des clients, mais aussi du personnel géographiquement éloignées, et cette communication passe par le biais d'Internet.

Cependant sur Internet, les données sont plus vulnérables et peuvent être interceptées car elles ne suivent pas le même chemin. De ce fait, connecter deux réseaux LAN entre eux par le biais d'Internet n'est pas concevable sans sécurité. La solution de chiffrer message par message serait très inefficace : on choisira plutôt de chiffrer le flux de l'ensemble du trafic sur un ou plusieurs itinéraires donnés, cela constituera un réseau privé virtuel sécurisé, un VPN.

- **Définition**

Ce réseau virtuel à la capacité de relier deux réseaux locaux, dits « physiques » par une liaison privée (Internet) car seuls les ordinateurs de ce réseaux peuvent accéder aux données. Cette solution consiste à utiliser Internet comme support de transmission en utilisant un protocole de « tunnelisation», les données sont alors transmises de manière chiffrée. De ce fait la liaison est sécurisée, elle permet d'authentifier et d'identifier l'interlocuteur tout en assurant la confidentialité des données puisque le chiffrement les rend inutilisables par une tierce.

- **Les différents types de VPN**
  - **Le VPN d'accès**

Il est utilisé pour permettre à des utilisateurs d'accéder au réseau privé. Grâce à une connexion Internet, l'utilisateur établit la connexion VPN. On peut définir deux méthodes d'accès aux VPN :

✓ L'utilisateur demande à son fournisseur d'accès de lui établir une connexion vers un serveur dit distant. Cela lui permet de communiquer sur différents réseaux en créant plusieurs tunnels.

✓ L'utilisateur à son propre logiciel client pour le VPN et établit directement la connexion de manière codée vers le réseau de l'entreprise. Dans ce cas la totalité des informations est cryptée dès le début de la connexion.

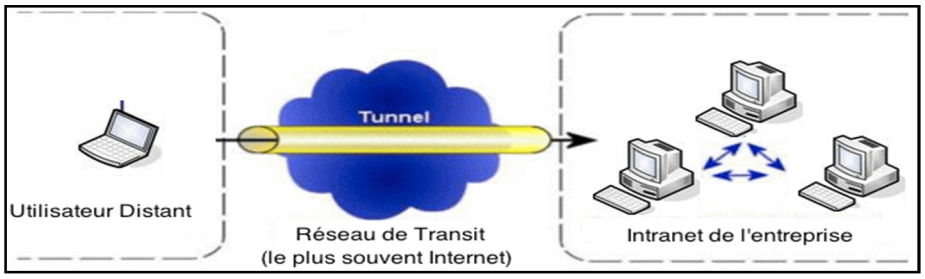


Figure II.11 : Le VPN d'accès

- **L'intranet VPN**

Il est utilisé pour relier au minimum deux Intranets entre eux. C'est un réseau particulièrement utile pour une entreprise qui possède des agences à travers le monde, car il facilite la communication. Le plus important c'est qu'il garantit la sécurité des données. Des techniques d'authentification comme la cryptographie sont mises en œuvre pour assurer la validité des données et l'authentification de la source.

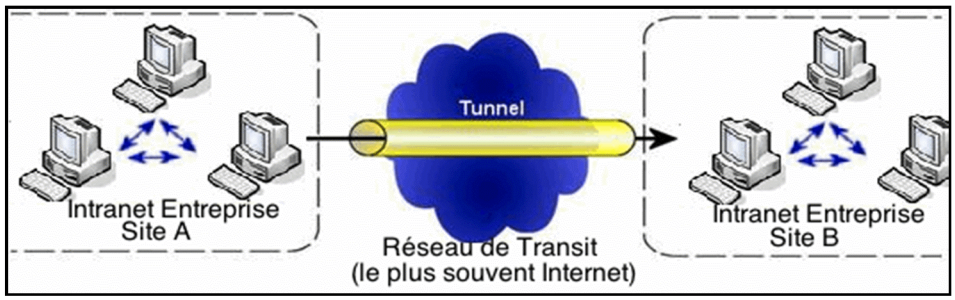


Figure II.12 : L'Intranet VPN

- **L'Extranet VPN**

Dans le but d'échanger et de communiquer avec ses clients et ses partenaires, l'entreprise a la possibilité de mettre en place un Extranet VPN qui ouvre l'accès aux réseaux locaux pour des personnes extérieurs.

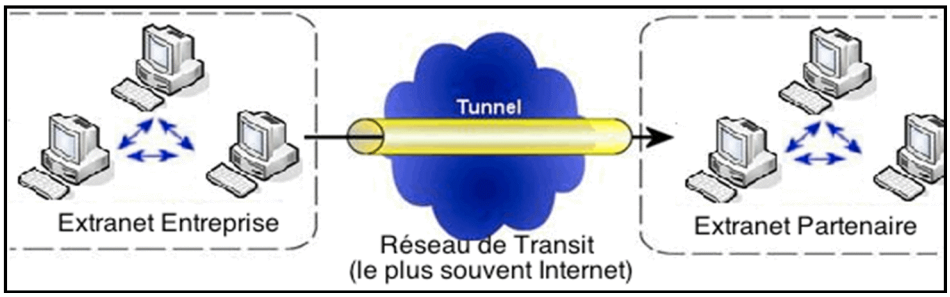


Figure II.13 : L'Extranet VPN

- **Exemple de protocoles de tunnelisation utilisés**

- **PPTP (Point-to-Point Tunneling Protocol)**

Est un protocole qui utilise une connexion PPP à travers le réseau IP en créant un réseau privé virtuel. Le tunnel PPTP se caractérise par une initialisation du client, une connexion de contrôle entre le client et le serveur ainsi que par la clôture du tunnel par le serveur. Au départ, le client effectue d'abord une connexion avec son fournisseur d'accès Internet, c'est une connexion de type PPP qui permet de faire circuler les données. Par la suite, une deuxième connexion est établie qui permet d'encapsuler les paquets PPP dans le datagramme IP. C'est cette deuxième connexion qui forme le tunnel PPTP.

Ce protocole permet l'encryptage des données, leur compression et leur authentification grâce au protocole Ms-Chap.

- **IPSec (IP Security protocols) :**

Est un protocole qui vise à sécuriser l'échange de données au niveau de la couche réseau. C'est un mécanisme de protection des données commune à IPv4 et IPv6. IPSec est basé sur deux mécanismes. Le premier, AH (Authentification Header) qui vise à assurer l'intégrité et l'authenticité des datagrammes IP. Il ne fournit par contre aucune confidentialité puisque les données qu'il fournie ne sont pas encodées. Le second, ESP (Encapsuling Security Payload) qui est utilisé principalement pour le cryptage des données.

II.5.6.Comparaison des procédés de sécurisation

Procédés	Explications
Chiffrement	Si utilisateur 1 envoie à utilisateur 2 un message électronique chiffré avec la clé publique de l'utilisateur 2, seul utilisateur 2 pourra lire le message, même si utilisateur 1 par erreur à également envoyé le message à utilisateur 3, celle-ci ne pourra pas le déchiffrer. Si un jour le responsable de l'entreprise veut lire ce message qui contient un plan contre cette entreprise, il devra obtenir la clé privée de l'utilisateur 2 pour lire le contenu de sa boîte à lettres.
Le SMTP et POP sécurisés	Si l'utilisateur 1 et l'utilisateur 2 ne chiffrent pas les messages électroniques qu'ils échangent, mais que les serveurs de messagerie des réseaux locaux de leurs employeurs respectifs utilisent les versions sécurisées par TLS des protocoles électroniques SMTP et POP, les échanges seront chiffrés pendant la circulation des messages sur le réseau, mais pas sur leurs postes de travail. Les messages seront protégés contre l'espionnage de l'utilisateur 3 si celui-ci a accès au réseau, mais pas dans les boites aux lettres respectives si l'utilisateur 3 a accès à leurs ordinateurs. De même, le responsable de l'entreprise, lorsqu'il prendra les disques durs, pourra lire les messages sans difficultés.
VPN IPSec	L'Utilisateur 1 et l'utilisateur 2 peuvent aussi disposer de VPN IPSec pour accéder aux réseaux qui abritent leurs serveurs de messagerie respectifs, qui ne sont accessibles que par ce procédé. Ce dispositif garantit que l'utilisateur 3 ne pourra pas accéder à ces serveurs, car seuls les utilisateurs autorisés et authentifiés par IPSec le peuvent. ce type d'accès permet à l'utilisateur 1, et à l'utilisateur 2 d'accéder à tous les services du réseau local, pas uniquement à la messagerie.

Tableau II.2 : Comparaison des procédés de sécurisation

II.5.7.Solutions organisationnelles

Comme dans tout autre domaine de la sécurité, les mesures retenues pour la messagerie électronique doivent, pour être efficaces, s'inscrire dans un cadre globale cohérent « la politique de sécurité ». L'efficacité des dispositifs techniques de sécurité dépend également en grande partie du comportement des utilisateurs, celui-ci devra être encadré dans une charte d'utilisation.

II.5.7.1.La messagerie électronique et la politique de sécurité

La politique de sécurité de l'entreprise énonce des principes et des règles dont certains sont directement applicables à la messagerie électronique:

- ✓ Les principes de classification des informations et les règles de conservation, de transmission et de destruction de ces informations selon leur nature (utilisation de moyens de chiffrement, règles d'archivage…).
- ✓ Les règles de protection antivirale (interdiction de certaines pièces jointes, formats de messages admis…).
- ✓ Les règles visant l'efficacité du système (taille des fichiers transmis,…).
- ✓ Les principes de filtrage et de contrôle d'utilisation de la messagerie (filtre antispamming, quarantaine…).

II.5.7.2.La charte d'utilisation

Les règles d'utilisation de la messagerie seront consignées dans une charte d'utilisation de la messagerie, ou incluses dans une charte plus globale d'utilisation des moyens d'informatiques. Ce document, signé par chaque utilisateur, informe également le destinataire des différents types de contrôle susceptible d'être effectué, dans les limites fixées par la réglementation.

La charte d'utilisation est un document qui doit être présenté aux instances représentatives du personnel avant diffusion. La diffusion de ces documents pourra s'intégrer dans un plan de sensibilisation des utilisateurs (réunions, vidéos ou tout autre support).

II.6.Conclusion

Après avoir clairement analysé les menaces et défini une politique de sécurité, nous avons constaté que la sécurisation de la messagerie est relativement complexe en raison des nombreux standards, protocoles et formats de fichiers mis en jeu et aux limites des techniques de sécurité proposées. La recherche de nouvelles solutions plus efficaces s'impose d'où l'apparition de plusieurs solutions de messagerie telles que : Zimbra, postfix, IBM Notes Domino, Exchange, etc.

Dans le troisième chapitre nous allons présenter la solution du serveur de messagerie Exchange en vue de sa forte utilisation dans le milieu du travail et de sa facilité d'administration ainsi que d'autres options que nous développerons.

Chapitre III

Présentation de la solution de messagerie

III.1.Introduction

Nous avons choisi de présenter Exchange serveur 2010 de Microsoft et l'environnement de son infrastructure. Cette solution de Microsoft est très utilisée dans les entreprises, elle possède l'avantage d'avoir un réseau uniforme et ainsi éviter d'éventuelles sources de conflits.

Exchange permet d'atteindre de nouveaux niveaux de performance et de fiabilité en mettant à disposition des fonctionnalités qui simplifient l'administration, aident à protéger les communications et répondent aux besoins des utilisateurs en mobilité.

III.2.Présentation de Microsoft Exchange Serveur

III.2.1.Qu'est-ce que Microsoft Exchange serveur ?

Microsoft Exchange serveur est un logiciel de messagerie. Il permet le stockage et la gestion du courrier électronique, ses principales caractéristiques sont les suivantes :

- ✓ Accès en mobilité, il permet à chaque utilisateur d'accéder à son courrier électronique, à sa messagerie vocale, à son calendrier et à ses contacts via des clients mobiles (Outlook web Application, Exchange ActiveSync) installés sur son ordinateur, et sur son téléphone portable, ou via des clients Web (navigateurs tels que Internet Explorer, Mozilla Firefox…) et ce depuis tout endroit connecté à Internet.
- ✓ Une bonne sécurité qui sauvegarde et archive les données critiques.
- ✓ Une bonne efficacité permettant le partage d'agenda et de contact professionnel avec des collègues ou des collaborateurs.
- ✓ Une multitude d'outils de gestions facilitant son d'administrations...

III.2.2.Historique des versions d'Exchange Serveur

- **Microsoft-Mail 3.5**

Microsoft Mail est le premier système de messagerie client/serveur, il dispose de son propre service d'annuaire et les emails sont accessibles sous la forme d'un partage de fichiers.

L'utilisation de Microsoft Mail dans de grandes organisations pose problème car une seule instance était limitée à 500 utilisateurs et la synchronisation de l'annuaire (et des listes d'adresses) n'est pas efficace.

- **Exchange Server 4.0**

Apparu en 1996, Exchange Server 4.0 est le remplaçant de Microsoft Mail. Il est basé sur le protocole de messagerie X.400. Comme avec Microsoft Mail, de nombreux connecteurs sont disponibles pour fournir une interaction avec les autres protocoles de messagerie tels que SMTP.

- **Exchange Server 5.0**

Apparu le 23 Mai 1997, ses principales nouveautés sont : Intégration du protocole SMTP en standard, apparition d'un webmail nommé Exchange Web Access, puis Outlook Web Application et une nouvelle console d'administration.

- **Exchange Server 5.5**

A partir de la version 5.5 (novembre 1997), Exchange est proposé en deux éditions : standard et entreprise, Sur la version standard les bases de données sont limitées à 16Go alors que sur la version entreprise la limite est de 8To (même si Microsoft recommande de ne pas dépasser les 100Go...). Exchange 5.5 apporte le support du protocole IMAP4, le support du clustering à deux nœuds (uniquement sur la version entreprise) et intègre la fonction calendrier dans Outlook Web Access.

- **Exchange Server 2000**

Apparu le 29 novembre 2000, Exchange 2000 ne dispose plus de son propre annuaire LDAP. Il est dorénavant intégré à Active Directory ce qui complique le processus de migration à partir des versions précédentes. Exchange 2000 apporte aussi son lot d'amélioration sur les fonctions existantes (support des clusters à 4 nœuds, amélioration d'Outlook Web Access...).

- **Exchange Server 2003**

Apparu 3 ans plus tard, Exchange 2003 reste dans la lignée d'Exchange 2000. Ses principales nouveautés concernent le domaine de la mobilité :

✓ Intégration d'Outlook Mobile Access (interface Web conçue pour le réseau WAP) et d'ActiveSync qui est un logiciel de synchronisation, utilisant le protocole propriétaire ActiveSync Exchange qui permet de synchroniser une boîte aux lettres avec le serveur Exchange en synchronisant un périphérique portable avec un ordinateur de bureau.

✓ Ajout d'un mode « Exchange mis en cache » pour les clients MAPI, qui fournit une copie de la boîte aux lettres qui est stockée sur l'ordinateur. Cette copie fournit un accès rapide aux données et est fréquemment mise à jour avec le serveur de messagerie.

✓ Intégration du protocole RPC sur HTTP qui permet de synchroniser un client MAPI (Outlook) via des requêtes HTTP (ou HTTPS).

✓ Intégration de deux fonctions liées à ActiveSync : le mode Direct Push qui permet de recevoir ses mails en temps réel, et la fonction RemoteWipe qui permet d'effacer le contenu des périphériques mobiles volés ou perdus qui sera effectué par l'administrateur via une interface Web spécifique.

✓ Il apporte aussi des fonctionnalités de filtrage anti-spam performantes.

- **Exchange Server 2007**

La version 2007 correspond à une mise à jour majeure, elle est intégralement redéveloppée en 64 bits avec la plateforme .net, introduisant de nouveaux concepts tels que :

✓ Les différentes fonctions d'Exchange sont éclatées en rôles pouvant être déployés de manière indépendante.

✓ Ajout du cluster de la réplication locale continue (LCR) : permet de créer une copie des groupes de stockage (une seule base par groupe de stockage) sur le même serveur physique. Le système est de type copie passive, en effet la copie n'est pas sollicitée par les utilisateurs mais permet la diminution de la charge pour le groupe de stockage actif.

✓ La fonctionnalité appelée la réplication continue en cluster (RCC) : fonctionne au moins avec deux serveurs Actif/Passif, chaque nœud à son propre espace de stockage et ses propres bases. Néanmoins il faut une troisième machine jouant le rôle de tiers de confiance appelé quorum MNS qui détermine le nœud actif qui est celui qui communique avec ce troisième nœud. Le MNS résout le problème d'avoir deux serveurs ayant les mêmes services sur le réseau.

✓ De nouveaux outils d'administration qui sont Exchange Management Console et Exchange Management Shell qui permettent une nouvelle architecture d'administration.

✓ Intégration d'un système de messagerie vocale basée sur la Voix sur IP (VoIP).

III.2.3.Introduction à la notion de rôle

III.2.3.1.Notion de serveur dorsal et serveur frontal

Dans un système de messagerie basé sur Exchange Server 2003, on distingue deux types de serveurs : les serveurs dorsaux (principaux) et les serveurs frontaux.

- **Serveur dorsal**

Un serveur dorsal héberge les boîtes aux lettres des utilisateurs, les dossiers publics et fournit l'accès aux clients MAPI.

- **Serveur frontal**

Le serveur frontal accepte les requêtes des clients et les achemine en agissant en tant que proxy jusqu'au serveur dorsal approprié, en vue de leur traitement ainsi il offre une couche de sécurité supplémentaire pour les boîtes aux lettres. Cette architecture est mise en place si plusieurs protocoles d'accès non MAPI (POP3, IMAP4, Webmail,…) sont utilisés par les clients pour accéder au serveur Exchange.

L'architecture frontal/dorsal permet d'équilibrer la charge de travail entre les machines et de fournir une meilleure sécurité puisque seul le serveur frontal est publié sur Internet. La figure III.1 illustre une architecture de serveur frontal/dorsal.

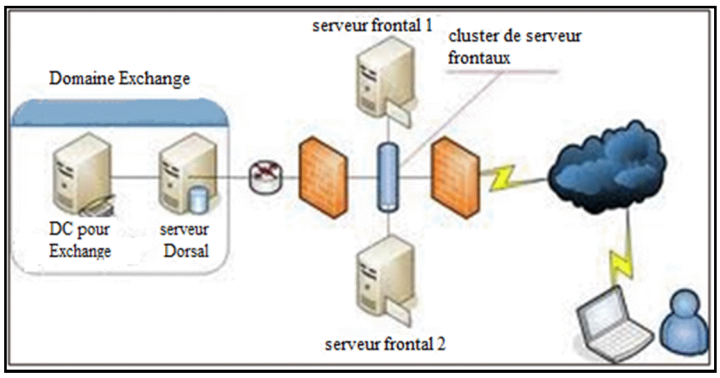


Figure III.1 : Infrastructure d'exchange 2003

III.2.3.2.Les rôles

C'est avec l'arrivée d'Exchange Serveur 2007 que la notion de rôle est apparue. C'est une unité qui regroupe logiquement les fonctions et les composants requis pour exécuter une fonction spécifique dans l'environnement de messagerie.

- **Rôle serveur de boîtes aux lettres (Mailbox server)**

Le rôle serveur de boîtes aux lettres est le rôle qui se trouve au cœur d'une organisation Exchange. Il est l'équivalent du serveur dorsal dans une topologie Exchange 2003. Ce serveur héberge les bases de données des boîtes aux lettres et des dossiers publics. Il héberge également les carnets d'adresses et permet la planification de réunions et des ressources associées.

Les serveurs de boîtes aux lettres exécutent aussi les fonctions suivantes :

- ✓ Fournir un stockage de courrier électronique.
- ✓ Générer des listes d'adresses et des carnets d'adresses en mode hors connexion.
- ✓ Rechercher dans plusieurs boîtes aux lettres.
- ✓ Fournir une haute disponibilité et une résilience de site.
- ✓ Fournir l'indexation de contenu.

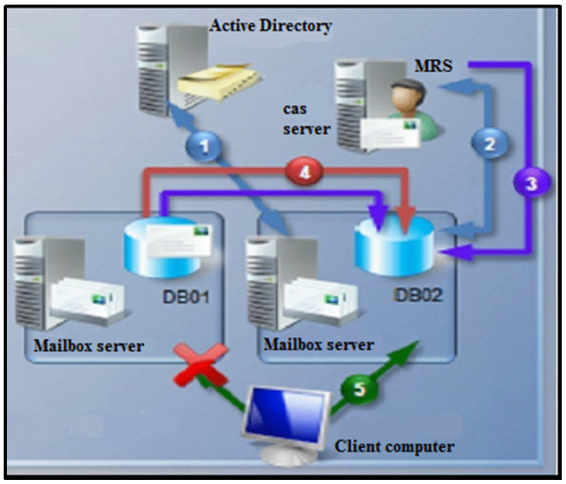


Figure III.2 : Rôle serveur de boîtes aux lettres

- **Rôle serveur d'accès client (Client Access Server)**

Ce serveur héberge les protocoles clients ainsi il leurs permet de se connecter au serveur Exchange. Il est l'équivalent du serveur frontal dans une topologie Exchange 2003.

Des clients logiciels tels que Microsoft Outlook Express et Eudora utilisent des connexions POP3 ou IMAP4 et les clients matériels, tels que les téléphones mobiles, utilisent ActiveSync, POP3 ou IMAP4 pour communiquer avec le serveur Exchange. Il prend aussi en charge Outlook Web Application qui permet d'accéder à la messagerie à partir de n'importe quel navigateur Web.

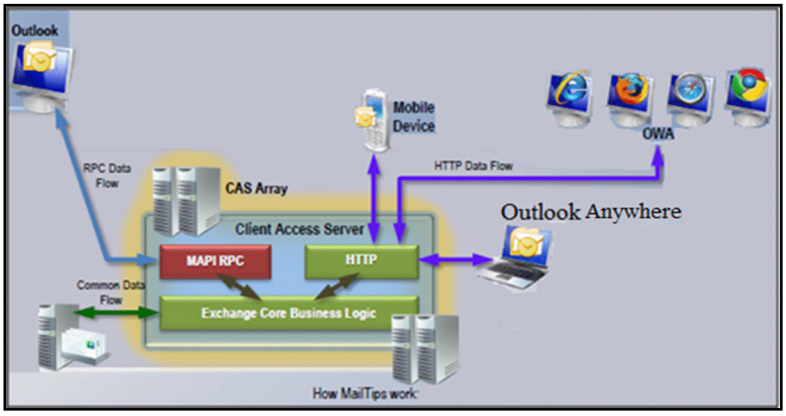


Figure III.3 : Rôle serveur d'accès client

- **Rôle Serveur Transport Hub (Hub transport Server)**

Le rôle de serveur de transport Hub traite tout le flux des messages au sein de l'organisation, applique les règles de transport, les stratégies de journalisation et remet les messages à la boîte aux lettres d'un destinataire. Les messages qui sont envoyés à Internet sont relayés par le serveur de transport Hub sur le rôle serveur de transport Edge déployé dans le réseau de périmètre ou vers une passerelle SMTP. Les messages reçus d'Internet sont traités par le serveur de transport Edge avant d'être relayés sur le serveur de transport Hub.

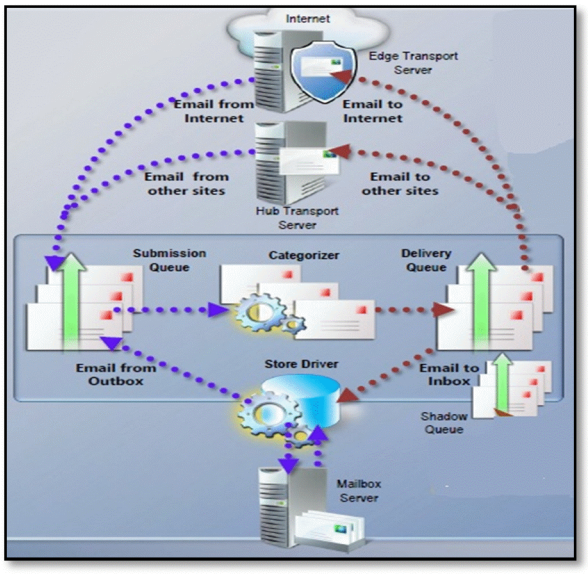


Figure III.4 : Rôle Serveur Transport Hub

- **Rôle serveur de transport Edge (Edge Transport Server)**

Ce serveur de routage se trouve généralement dans le périmètre de la topologie placé en DMZ, et route les messages à l'intérieur et en dehors de l'organisation Exchange conçu pour réduire la surface d'attaque. Le serveur de transport Edge gère tout le flux de messagerie côté Internet ou de serveurs d'organisations externes clairement identifiés, offrant ainsi des services de relais SMTP et d'hôte actif pour l'organisation Exchange.

Des couches supplémentaires de protection des messages et de sécurité sont assurées par une série d'agents qui s'exécutent sur le serveur de transport Edge et agissent sur les messages lors de leur traitement par les composants de transport de messages. Ces agents prennent en charge les fonctions qui fournissent une protection contre les virus et le courrier indésirable et appliquent des règles de transport pour contrôler le flux de messages grâce à un firewall nommé Forefront Protection for Exchange, Les emails entrants ayant passé l'hygiène de messagerie seront routés vers les serveurs Transport Hub de l'organisation.

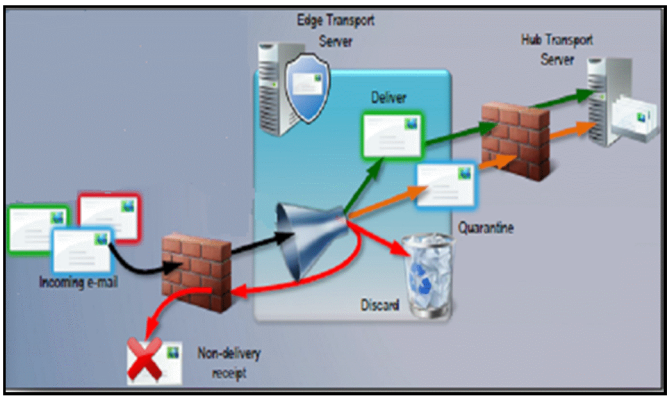


Figure III.5 : Rôle serveur de transport Edge

- **Le rôle serveur de messagerie unifiée (Unified Messaging Server)**

Ce serveur connecte un système PBX (Private Branche Xchange) à Exchange 2010. La messagerie unifiée (MU) associe la messagerie vocale et la messagerie électronique en une seule infrastructure de messagerie c'est-à-dire dans une seule boîte aux lettres Exchange qui est accessible depuis divers périphériques. Une fois les serveurs de messagerie unifiée déployés sur le réseau, les utilisateurs peuvent accéder à leurs messages à l'aide d'Outlook, depuis un téléphone, un appareil mobile ou un ordinateur.

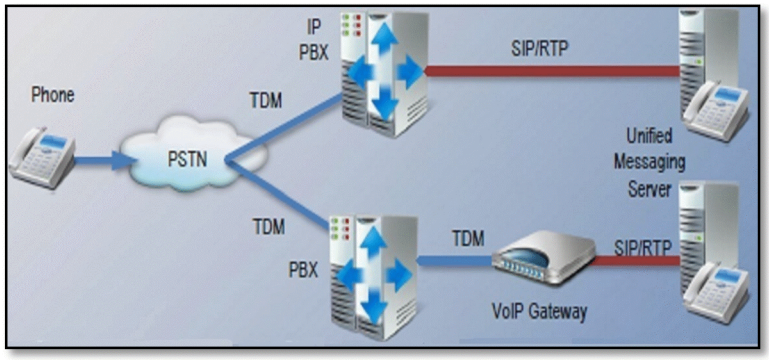


Figure III.6 : Le rôle serveur de messagerie unifiée

III.2.4.La solution d'annuaire d'Exchange

Avec le développement des réseaux, les services offerts se sont multipliés. On trouve ainsi couramment sur un même réseau un service de messagerie, un serveur de fichiers, un agenda partagé, etc. Avant d'accéder à un quelconque service, il est souvent demandé aux utilisateurs de s'authentifier, afin de se faire reconnaitre du service en question. De même, chaque utilisateur d'un service disposera de ses propres données, de ses propres paramètres, pour l'utilisation du service. En prenant l'exemple de la messagerie, un utilisateur devra s'authentifier auprès du serveur de messagerie, au moyen d'un identifiant et d'un mot de passe et éditer ses données personnelles (au minimum nom, prénom et adresse personnelle).

Plus le réseau est vaste et plus les services se multiplient. Il est par conséquent difficile, sur un réseau étendu, de contrôler finement et efficacement l'ensemble des ressources avec une telle approche. C'est là que le concept d'annuaire prend son sens. Un annuaire va permettre de centraliser les informations d'un utilisateur, d'un service pour en simplifier l'administration.

Chaque utilisateur disposera d'une entrée dans l'annuaire, entrée dans laquelle seront conservées toutes les données le concernant. Les services n'auront alors plus qu'à consulter l'annuaire pour fournir à l'utilisateur les données qu'il attend.

Le serveur Exchange a besoin d'Active Directory (au minimum sur Windows Server 2003) pour fonctionner. Active Directory va servir à stocker différentes données et également les comptes utilisateurs activés pour la messagerie. Par exemple un serveur Exchange pourra localiser rapidement le serveur contenant la boite aux lettres d'un utilisateur Lorsque celui-ci essaye d'y accéder.

III.3.Active Directory

III.3.1.Définition

Active Directory est un annuaire au sens informatique et technique chargé de répertorier tout ce qui touche au réseau comme le nom des utilisateurs, des imprimantes, des serveurs, des dossiers partagés,, etc. L'utilisateur peut ainsi trouver facilement des ressources partagées, et les administrateurs peuvent contrôler leurs utilisations grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation des accès aux ressources répertoriées. Il offre aussi les avantages suivant :

- **Intégration DNS**

Active Directory utilise les conventions d'attribution de noms DNS pour créer une structure hiérarchique qui fournit une vue familière, ordonnée et évolutive des connexions réseau. Le DNS est la base d'Active Directory, c'est grâce aux DNS que les postes utilisateurs ou serveurs membre du domaine peuvent trouver le ou les serveur(s) Active Directory. DNS sert également à faire correspondre les noms d'hôtes tels que 2int.com à des adresses numériques TCP/IP telles que 192.168.19.2

- **Évolutivité**

Active Directory est organisé en sections qui permettent de stocker un très grand nombre d'objets. Active Directory peut de ce fait évoluer en fonction des besoins de l'entreprise. Une organisation qui dispose d'un seul serveur avec quelques centaines d'objets peut évoluer vers des milliers de serveurs et des millions d'objets.

- **Administration centralisée**

Active Directory permet aux administrateurs d'administrer les ordinateurs distribués, les services réseau et les applications à partir d'un emplacement central tout en utilisant une interface d'administration cohérente.

Active Directory fournit également un contrôle centralisé de l'accès aux ressources réseau en permettant aux utilisateurs d'ouvrir une fois une session et d'obtenir un accès complet aux ressources d'Active Directory.

- **Administration déléguée**

La structure hiérarchique d'Active Directory permet de déléguer le contrôle d'administration sur des parties spécifiques de la hiérarchie. Un utilisateur autorisé par une autorité administrative plus élevée peut effectuer des tâches d'administration dans la partie de la structure qui lui a été affectée.

III.3.2.les Rôles d'Active Directory

- **Services de domaine de l'Active Directory (ADDS)**

Il s'agit du rôle principal d'Active Directory, c'est un service d'annuaire qui fournit les services d'authentification et d'autorisation des utilisateurs, des ordinateurs et d'autres périphériques sur le réseau. Les AD DS fournissent également des services de gestion et de partage des informations qui permettent aux utilisateurs de trouver n'importe quel composant

(Serveur de fichiers, imprimantes, groupes et autres utilisateurs) en le cherchant dans l'annuaire ainsi ils facilitent le partage des ressources et la collaboration entre les utilisateurs.

- **Services LDAP de l'Active Directory (ADLDS)**

Il s'agit d'un service d'annuaire avec des accès gérés par le protocole LDAP (Lightweight Directory Access Protocol) qui fournit une prise en charge flexible des applications utilisant des annuaires, sans l'authentification des utilisateurs. ADLDS ne compromet pas à la sécurité de la base de données d'AD DS.

- **Services de Certificat de l'Active Directory (ADCS)**

Est un rôle d'Active Directory proposant la délivrance des certificats numériques dans le cadre d'une infrastructure à clé publique (PKI : Public Key Infrastructure) qui lie l'identité d'une personne, d'un équipement ou d'un service à une clé privé correspondante. Elle est utilisée pour la protection des logiciels, des utilisateurs et du réseau, ainsi que pour leur sauvegarde dans la base de données dans ADDS. ADCS délivre aussi des certificats pour l'authentification des courriers électroniques et leur chiffrage (SMIME).

- **Service de gestion des droits et la protection des documents (AD RMS)**

Ce rôle fournit une technologie de protection des informations qui permet de mettre en œuvre des modèles de stratégie permanents qui définissent des usages autorisés ou interdits, par exemple configurer un modèle qui permet aux utilisateurs de lire un document annexé à un message électronique, mais d'interdire son impression et la copie de son contenu. Ainsi ce rôle protège les documents, les courriers électroniques et les sites web contre tout accès, ou utilisation non autorisée dans le but de leur confidentialité et leur intégrité. Ce service nécessite des applications qui gèrent les protections de type DRM (Digital Rights Management).

- **Services de Fédération de l'Active Directory (ADFS)**

Il s'agit du composant permettant la fédération de services entre différents environnements Active Directory (qui ne partagent pas leurs services d'annuaire AD DS) en fournissant une authentification Web unique SSO (Single Sign On). Cela permet de donner un accès à certains des services internes de manière contrôlée et sécurisée.

III.3.3.Structure d'Active Directory

III.3.3.1.Définitions

- **Schéma**

Le schéma Active Directory contient les définitions de tous les objets, comme les utilisateurs, les ordinateurs et les imprimantes stockés dans Active Directory. Il n'y a qu'un seul schéma pour l'ensemble de la forêt, ce qui permet une homogénéité de l'ensemble des domaines. Ainsi, tous les objets créés dans Active Directory se conforment aux mêmes règles.

Le schéma possède deux types de définitions : les classes d'objets et les attributs. Les classes d'objets comme utilisateur, ordinateur et imprimante décrivent les objets d'annuaire possibles qu'on peut créer. Chaque classe d'objet est un ensemble d'attributs.

Les attributs sont définis séparément des classes d'objets. Chaque attribut n'est défini qu'une seule fois et peut être utilisé dans plusieurs classes d'objets.

Le schéma est stocké dans la base de données d'Active Directory ce qui permet des modifications dynamiques exploitables instantanément.

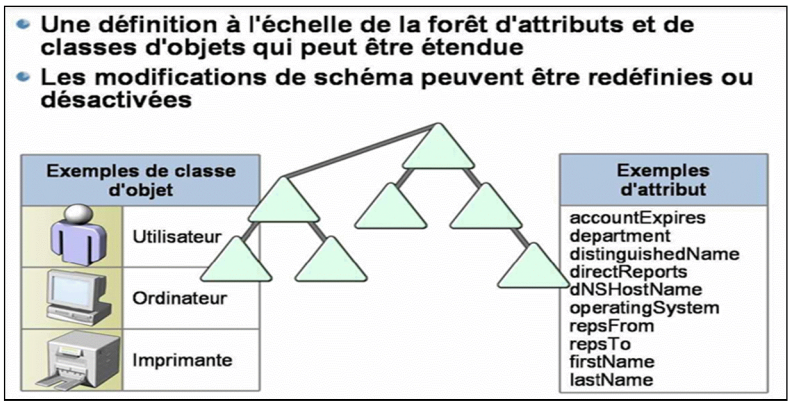


Figure III.7 : Le schéma d'Active Directory

- **catalogue global**

Dans Active Directory, les ressources peuvent être partagées parmi des domaines et des forêts. Le catalogue global d'Active Directory permet de rechercher des ressources parmi des domaines et des forêts de manière transparente pour l'utilisateur. Par exemple, si vous recherchez toutes les imprimantes présentes dans une forêt, un serveur de catalogue global traite la requête dans le catalogue global, puis renvoie les résultats. En l'absence de serveur de catalogue global, cette requête exigerait une recherche dans chaque domaine de la forêt.

Figure III.8 : Le catalogue global d'Active Directory

III.3.3.2.L'infrastructure physique

Contrairement à la structure logique, qui modélise des exigences administratives, la structure physique d'Active Directory optimise le trafic réseau en déterminant où et quand se produit un trafic de connexions et de réplications. Pour optimiser l'utilisation par Active Directory de la bande passante du réseau, on doit comprendre la structure physique. Les éléments de la structure physique d'Active Directory sont :

- **Le Contrôleur de Domaine**

Un contrôleur de domaine est un serveur qui exécute des fonctions de stockage et de réplication. Un contrôleur de domaine ne peut gérer qu'un seul domaine.

Pour assurer une disponibilité permanente d'Active Directory, chaque domaine doit disposer de plusieurs contrôleurs de domaine.

- **Le Site**

Un site est un emplacement d'un réseau qui contient des serveurs Active Directory. Un site est défini comme un ou plusieurs sous-réseaux IP connectés entre eux par une liaison à haut débit fiable (liaison LAN). Définir des sites permet à Active Directory d'optimiser la duplication et l'authentification afin d'exploiter au mieux les liaisons les plus rapides. Les

sites sont généralement symbolisés par des ovales comme le montre l'exemple de la figure III.9.

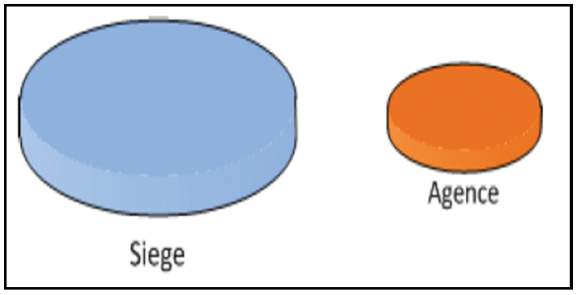


Figure III.9 : Représentation des sites

III.3.3.3.L'infrastructure logique

Active Directory offre un stockage sécurisé pour les informations concernant les objets dans sa structure logique hiérarchique. Les objets Active Directory représentent des utilisateurs et des ressources, tels que des ordinateurs et des imprimantes. Certains objets en contiennent d'autres. La structure logique d'Active Directory inclut les composants suivants :

- **Les objets**

Il s'agit des composants les plus élémentaires de la structure logique. Les classes d'objets sont des modèles pour les types d'objets qu'on crée dans Active Directory. Chaque classe d'objet est définie par une liste d'attributs, qui définit les valeurs possibles qu'on associe à un objet. Chaque objet possède une combinaison unique de valeurs d'attributs.

- **Les unités d'organisation (OU, Organizational Unit)**

On utilise ces objets conteneurs pour organiser d'autres objets de telle manière qu'ils prennent en compte les objectifs administratifs. La disposition de ces objets par unité d'organisation simplifie la recherche et la gestion des objets. On peut également déléguer l'autorité de gestion d'une unité d'organisation.

Les unités d'organisation peuvent être imbriquées les unes dans les autres, ce qui simplifie d'autant la gestion d'objets.

- **Le Domaine**

Est une unité fonctionnelle centrale dans la structure logique d'Active Directory qui est le plus souvent liée a la hiérarchie, c'est un ensemble d'objets définis administrativement qui partagent la base de données d'annuaire commune, des stratégies de sécurité et des relations

d'approbation avec d'autres domaines. Les domaines disposent des trois fonctions suivantes : une limite d'administration pour objets, une méthode de gestion de la sécurité pour les ressources partagées et une unité de réplication pour les objets. Un domaine est généralement symbolisé par un triangle comme le montre la figure III.10.

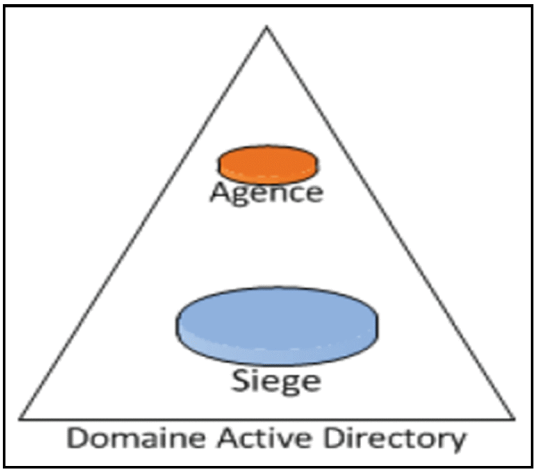


Figure III.10 : Représentation d'un domaine

Ce qu'il faut retenir, c'est qu'un domaine peut être sur plusieurs sites mais qu'un site (au sens Active Directory) ne peut pas avoir plusieurs domaines.

- **Les arborescences de domaines**

Les domaines regroupés en structures hiérarchiques sont appelés arborescences de domaines. Lorsqu'on ajoute un second domaine à une arborescence, il devient enfant du domaine racine de l'arborescence. Le domaine auquel un domaine enfant est attaché est appelé domaine parent. Un domaine enfant peut à son tour avoir son propre domaine enfant.

Le nom d'un domaine enfant est associé à celui de son domaine parent par exemple (developpez.adds) pour former son nom DNS unique, par exemple (corp.developpez.adds).

De cette manière, une arborescence a un espace de noms contigu, comme le symbolise la figure III.11.

- **La Forêt**

Une forêt est une collection d'un ou plusieurs domaines c'est-à-dire une instance complète d'Active Directory, n'ayant pas le même nom commun. Le premier domaine installé dans celle-ci est appelé le domaine racine de la forêt. Active Directory ne réplique aucune donnée au-delà des frontières de la forêt c'est-à-dire les informations ne sont partagées qu'à l'intérieur

de celle-ci. Ainsi, la forêt est une limite de sécurité pour les informations contenues dans l'instance d'Active Directory.

Une forêt peut comprendre plusieurs arborescences. Par exemple La forêt developpez.adds présentée dans la figure III.11 comporte quatre arborescences. Les arborescences d'une même forêt peuvent partager des ressources et des fonctions administratives. Comme pour les domaines, il est conseillé d'être, le plus possible dans la configuration idéale, c'est-à-dire en mono-forêt. La configuration idéale est donc un Active Directory mono-domaine mono-forêt.

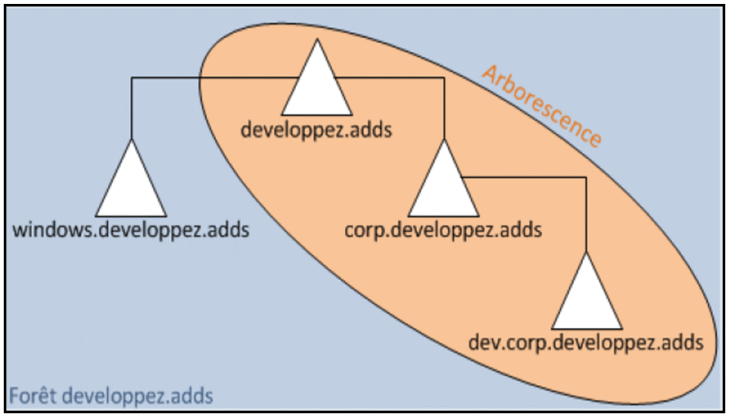


Figure III.11 : forêt et arborescence

III.3.4.Partitions Active Directory

Chaque contrôleur de domaine contient les partitions Active Directory suivantes :

1. **La partition de domaine** : contient les réplicas de tous les objets de ce domaine. La partition de domaine n'est répliquée que dans d'autres contrôleurs appartenant au même domaine.
2. **La partition de configuration** : contient la topologie de la forêt. La topologie est un enregistrement de tous les contrôleurs de domaine et des connexions entre eux dans une forêt.
3. **La partition de schéma** : contient le schéma étendu au niveau de la forêt. Chaque forêt comporte un schéma de sorte que la définition de chaque classe d'objet soit cohérente. Les partitions de configuration et de schéma sont répliquées dans chaque contrôleur de domaine dans la forêt.
4. **Les partitions d'applications facultatives** : contiennent des objets non liés à la sécurité et utilisés par une ou plusieurs applications. Les partitions d'applications sont répliquées dans des contrôleurs de domaine spécifiés dans la forêt.

III.4.Les nouveautés d'Exchange 2010

Grâce aux nouvelles options de déploiement et de stockage, aux capacités améliorées de gestion de la boîte de réception et à l'archivage intégré des messages électroniques, Exchange 2010 est considéré comme une évolution importante comparée aux versions ultérieures.

- **Disponibilité Continue**

Exchange Server 2010 offre une approche simplifiée de la disponibilité continue et de la reprise sur incident afin de permettre de délivrer une continuité de service :

Le rôle serveur de boîtes aux lettres intègre les fonctionnalités de disponibilité Par le moyen d'une nouvelle technologie appelé (DAG) « Database Availability Group ». Il s'agit d'un ensemble de serveurs de bases de données qui utilise la fonctionnalité Windows Failover Clustering de manière transparente afin de faire basculer automatiquement les composants de l'infrastructure Exchange, sur une copie de la base en état de fonctionnement (au niveau des disques, des serveurs et des centres de données). La DAG permet la réplique automatique des bases de données avec seulement deux serveurs, maintien la disponibilité et la reprise sur incident rapide avec jusqu'à 16 répliques de la base de données à un temps de basculement de 30 secondes.

Permet aux administrateurs de déplacer les boîtes aux lettres entre les bases de données pendant que les utilisateurs se connectent à leurs boîtes aux lettres et d'envoyer ou de recevoir du courrier. Les administrateurs peuvent aussi effectuer les activités de maintenance du système pendant les heures d'ouverture.

Les rôles Hub-Transport et Edge-Transport intègrent des fonctionnalités de disponibilité et la Protection contre la perte des messages électroniques par l'intermédiaire de deux technologies. La première appelée Transport Redundancy qui consiste à conserver les messages sur le serveur précédent jusqu'à ce qu'il soit délivré plus loin, lorsqu'une erreur est détectée (timeout), le serveur précédent délivre de nouveau les messages à un autre HUB par exemple. La deuxième appelée Transport Dumpster reçoit les informations de la file d'attente de réplication entre les bases pour déterminer quels sont les messages qui ont été remis et répliquées. Tant qu'un message n'est pas répliqué sur l'ensemble des bases de données du DAG, un exemplaire est conservé dans la file d'attente du hub-transport ou de l'Edge Transport qui en assurent la remise par sécurité.

- **Contrôle et Protection de l'Information**

Exchange Server 2010 étend également la prise en charge de la protection et du contrôle des informations, afin de pouvoir facilement chiffrer, transmettre ou bloquer les messages électroniques sensibles ou inappropriés en fonction d'attributs spécifiques d'expéditeur, de récepteur et de contenu, on peut :

- ✓ combiner Exchange Server 2010 et ADRMS (Active Directory Rights Management Services) afin que les utilisateurs puissent appliquer automatiquement la protection IRM (Gestion des droits d'informations) pour limiter l'accès et l'utilisation des informations d'un message, quelle que soit sa destination.
- ✓ autoriser les collaborateurs et les clients à lire et à répondre au courrier protégé par IRM, même s'ils ne disposent pas des services ADRMS (Active Directory Rights Management Services) sur site.
- ✓ permettre aux responsables de consulter le courrier et approuver ou bloquer la transmission.

- **Archivage centralisé des fichiers**

Exchange Server 2010 offre une nouvelle fonction intégrée d'archivage de la messagerie, y compris la recherche détaillée sur plusieurs boîtes aux lettres et des stratégies de sauvegarde au niveau de l'élément, ce qui permet

- ✓ Aux administrateurs de bénéficier d'un contrôle centralisé sur toutes les archives.
- ✓ Aux utilisateurs d'obtenir l'accès direct à leur courrier archivé. L'expérience d'archivage reste privée et ne perturbe pas leur façon de gérer quotidiennement leurs boîtes de réception.
- ✓ Déplacer de volumineux fichiers de données vers une boîte d'archivage d'Exchange en ligne d'obtenir une réduction des lectures ou écritures sur le disque allant jusqu'à 50 % par rapport à ceux d'Exchange 2007.

- **Administration Simplifiée**

Nouvelles fonctionnalités de service permettant aux utilisateurs de gérer certaines tâches sans faire appel à l'assistance informatique. C'est une délégation d'administration afin d'être plus souple et utilisable par des populations autre que l'administrateur de messagerie. Elle repose sur le principe RBAC (Rôle Based Access Control) dont l'objectif est d'utiliser des modèles prédéfinis mais personnalisables de délégation. Chaque model correspond à un rôle

d'administration d'exchange et sera affecté à une population d'utilisateurs.

La création d'une règle RBAC se fait avec l'outil de contrôle d'accès Exchange appelé ECP(Exchange Contrôle Panel) qui permet à des groupes d'utilisateurs spécialisés et définis d'effectuer des tâches spécifiques, comme autoriser les responsables des ressources humaines à mettre à jour les informations personnelles des utilisateurs dans l'annuaire de l'entreprise ou rechercher à travers de multiples boîtes aux lettres pour un service juridique.

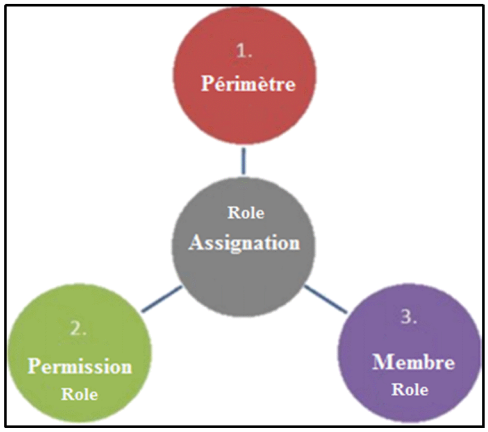


Figure III.12 : triangule du pouvoir de délégation RBAC

Le principe de mise en place d'une délégation RBAC passe par la configuration de trois éléments(le périmètre d'application, le rôle (ou les permissions) et les membres).

- ✓ **Le périmètre**

Il s'agît du périmètre d'assignation c'est-à-dire une OU (unité d'organisation). Par défaut tous les rôles ont un périmètre d'application donc lorsque on crée un nouveau RBAC, il est forcément un enfant d'un rôle déjà existant et hérité donc du périmètre de son parent. Il est aussi possible de spécifier un périmètre spécifique lors de sa création ou de le modifier par la suite.

- ✓ **Les permissions**

Une fois que l'on sait dans quel périmètres appliquer notre rôle il faut encore définir ce qu'il va pouvoir faire. Par défaut Exchange Server possède 65 rôles prédéfinis (dans le but de couvrir le maximum de scénario). On peut alors créer des rôles personnalisés enfant de rôle existant mais forcement ayant moins de droits. L'attribution des droits se fait par sélection des cmdlets powershell que le rôle pourra exécuter au final.

✓ **Les membres**

Maintenant que le périmètre de notre rôle et les actions qu'il peut réaliser sont connus, il ne reste plus qu'à définir les membres de ce rôle. On peut assigner le rôle aussi bien à un utilisateur unique qu'a un groupe entier (il est recommandé d'utilisé des groupes dans l'administration).

Chaque élément étant un objet dans l'Active Directory, le tout forme également un nouvel objet « Management Role Assignment »défini par le principe RBAC.

✓ **Assignations**

L'assignation est le lien entre un rôle et un groupe de rôles. Lorsqu'un rôle est ajouté à un groupe de rôle, le processus crée silencieusement une assignation. Elle se présente sous la forme suivante : « Rôle » - « Groupe de rôles ».

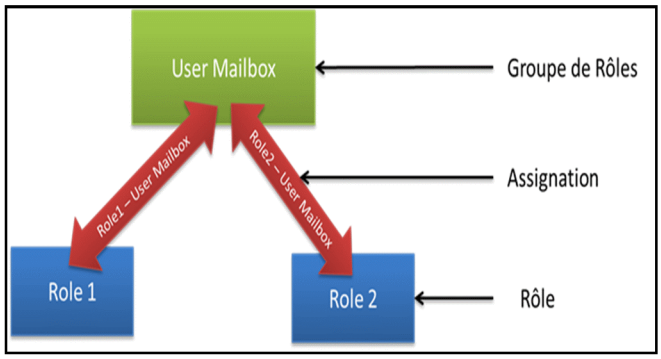


Figure III.13 : création de l'assignation de rôles

- **Accès à distance et en tout lieu**

Les améliorations d'Exchange 2010 fournissent aux utilisateurs un accès à toutes leurs communications depuis un emplacement unique tout en facilitant la collaboration entre utilisateurs et avec les partenaires externes. Ces améliorations permettent entre autres :

✓ Un accès en mobilité qui permet à chaque utilisateur d'accéder à l'ensemble de ses communications (messagerie électronique vocale et instantanée, calendrier et contacts) depuis presque toutes les plateformes, navigateurs ou terminaux, via des clients mobiles (Outlook web Application, ActiveSync) installés sur son ordinateur ou sur son téléphone portable, ou via des clients Web (navigateurs tels que Internet Explorer, Mozilla Firefox…) et ce depuis tout endroit connecté à Internet.

✓ De partager des informations de disponibilité du calendrier avec des partenaires extérieurs pour une planification rapide et efficace, et de choisir le niveau de détail qu'ils souhaitent partager, etc.

III.5. Topologie de la messagerie d'Exchange 2010

La figure III.14 illustre une topologie de messagerie unifiée Exchange Server 2010.

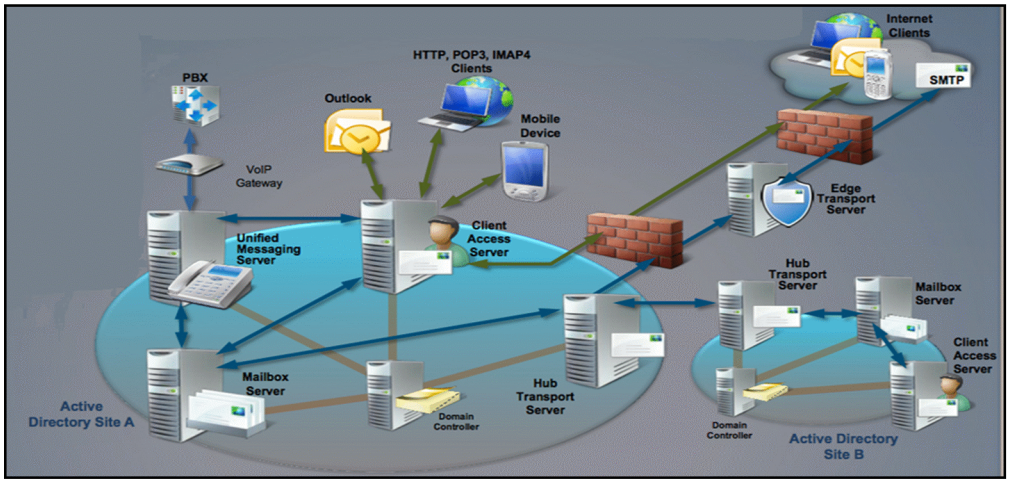


Figure III.14: La topologie de la messagerie d'Exchange 2010

Les rôles serveur de boîte aux lettres, serveur d'accès client (CAS), serveur de transport Hub et serveur de messagerie unifiée (UM) sont installés sur des machines distinctes. On remarque bien que le serveur UM interagit avec le PBX (Private Branch Exchange) de l'entreprise. Enfin le serveur de transport Edge est placé en DMZ de manière à filtrer de manière sécurisée tous les mails entrant et sortant de l'organisation. Seul le serveur Edge et le serveur CAS doivent être accessibles depuis Internet.

Pour harmoniser le réseau, faciliter la répartition et l'envoie de courriels au sein des entreprises en autorisant aux utilisateurs de façon sécuritaire et productive l'utilisation d'internet pour le travail sans se soucier des logiciels malveillants et autres menaces. Il est recommandé de faire appel à une solution de filtrage applicatif comme Le pare-feu Forefront TMG (Threat Management Gateway).

III.6.Présentation du pare-feu TMG

Le firewall Forefront TMG (Threat Management Gateway) est une passerelle Web qui permet aux entreprises d'utiliser internet de façon sécurisée. Il fonctionne en collaboration

avec le système de messagerie Exchange pour scanner les e-mails pour mieux bloquer les menaces récentes en provenance du Web. Le TMG multiplie les couches de protection (filtrage d'URL, recherche de logiciels malveillants et prévention des intrusions) et les met à jours en permanence dans une solution simple à administrer. De plus, il améliore les performances du pare-feu en répartissant la charge de certaines fonctions sur plusieurs processeurs.

III.6.1.Les composants de la TMG

Le pare-feu TMG se compose de quatre composantes :

- ✓ **Le serveur Forefront TMG** : il fournit plusieurs technologies d'inspection, des firewalls applicatifs et réseau, une prévention d'intrusion et un filtrage de logiciels malveillants.
- ✓ **Forefront TMG Web Protection Service** : il assure les mises à jours des signatures et le filtrage des URL Internet en temps réel, il peut aussi servir à surveiller ou à bloquer l'usage fait par les employés du Web.
- ✓ **La console d'administration**: il permet une gestion locale et à distance des serveurs.
- ✓ **Le serveur d'administration**: inclus dans Forefront TMG Entreprise Edition, il permet la création de stratégies à l'échelle de toute l'entreprise et les applique à des ensembles de serveurs TMG.

III.6.2.Les principaux avantages et fonctionnalités de la TMG

Forefront TMG fournit aux entreprises plusieurs avantages en matière de connectivité à Internet

a. Protection complète

- ✓ **TMG bloque efficacement l'accès aux sites malveillants**

Il utilise des données en provenance de différents fournisseurs de filtres d'URL, et des technologies contre les logiciels malveillants et usurpation d'identité. Le filtrage des sites Web permet aussi de bloquer l'accès aux sites inappropriés selon les choix d'entreprise.

- ✓ **Empêche l'exploitation des vulnérabilités**

Il empêche les intrusions qui exploiteraient des vulnérabilités du navigateur ou de ses modules additionnels.

✓ **Détecte les logiciels malveillants du Web**

Il assure une détection précise grâce à un moteur d'analyse qui combine des signatures génériques pour anticiper la diffusion de nouvelles variantes n'ayant pas de signatures spécifiques.

b. Interface de sécurité Web unifiée

✓ **Assure les principales fonctions de protection du réseau**

Il reprend les technologies de protection du réseau de Microsoft ISA Server 2006, la version précédente du Forefront TMG. Cela permet de déployer un pare-feu de périmètre et une passerelle sécurisée pour des applications.

✓ **Inspecte le trafic Web chiffré**

Il examine le trafic Web chiffré SSL, ce que ne fait pas un pare-feu. Dans ces sessions chiffrées, Forefront TMG peut détecter un logiciel malveillant et contrôler l'accès à des sites interdits par l'entreprise.

c. Sécurité intégré

✓ **Une source unique pour la sécurité Web**

Il combine sur un seul serveur le filtrage des URL, le blocage des intrusions, le proxy Web, des pare-feu applicatifs et réseau, la détection de logiciels malveillants et l'inspection http/ https.

✓ **Réduit les couts**

Il assure un rôle de cache pour améliorer la rapidité de navigation et réduire les couts en bande passante. La possibilité de déployer Forefront TMG comme une Application virtuelle permet d'économiser sur le matériel.

✓ **Exploite les investissements d'infrastructure existants**

Il simplifie l'authentification et l'application des stratégies en s'intégrant dans Active Directory. Par exemple, Forefront TMG simplifie l'inspection HTTPS en distribuant son certificat via Active Directory. Il utilise aussi l'infrastructure Windows Update pour diffuser rapidement de nouvelles protections à tous les serveurs Forefront TMG.

d. **Administration simplifiée**

✓ **Centralise la gestion sur une seule console simple d'emploi**

Il permet aux administrateurs de créer et de gérer toutes les fonctions de sécurité Web à

partir d'une seule console dans des environnements distribués.

- ✓ **Fournit des rapports complets**

Il génère des rapports de sécurité qui peuvent être adaptés pour répondre à des besoins spécifiques de l'entreprise.

III.7.Conclusion

Apres avoir présenté la solution de messagerie Exchange et ces différents modules. Nous avons mis en évidence l'importance de l'intégration d'Active Directory à Exchange qui fournit des services de centralisations et d'authentification, et sa collaboration avec le pare-feu TMG qui renforce ces paramètres de sécurité pour une éventuelle publication. Ainsi nous comprenons mieux pourquoi Exchange est un système de messagerie collaboratif avec un réseau uniforme.

Dans le prochain chapitre nous allons mettre en pratique les installations et configurations requises pour créer une architecture Exchange complète pour ensuite passer à sa publication.

Chapitre IV

Publication d'Exchange avec la TMG

IV.1.Introduction

Les entreprises doivent permettre à leurs employés et à leurs partenaires d'accéder aux applications, aux données et aux documents appropriés de façon sécurisée, quel que soit l'ordinateur ou le matériel utilisé. La publication d'applications sécurisée avec la TMG procure un contrôle accru des ressources de l'intranet, tout en améliorant l'efficacité grâce à la mise à disposition de ces ressources aux utilisateurs distants. La TMG est dotée de fonctions d'inspection des paquets par état et de filtrage au niveau applicatif, combinées à un ensemble complet d'outils de publication qui aident à protéger les applications, les services et les données de l'entreprise sur toutes les couches du réseau.

Avant de publier le serveur Exchange, nous allons créer au préalable une architecture réseaux interne, qui implémente la politique de messagerie d'Exchange et ses différents paramètres.

IV.2.Présentation du matériel Utilisé

IV.2.1.La VMware Workstation 9.0.0

IV.2.1.1.Principe de fonctionnement de VMware Workstation

Pour l'émulation de notre réseau, nous avons choisi d'utiliser la VMware Workstation 9.0.0. Cette dernière permet l'exécution simultanée, sur un même ordinateur physique, de plusieurs systèmes d'exploitation et de leurs applications. Ces systèmes d'exploitation et applications sont isolés dans des machines virtuelles sécurisées qui co-existent sur le même matériel. La couche de virtualisation VMware alloue les ressources matérielles aux ressources de la machine virtuelle. Ainsi, chaque machine virtuelle a ses propres ressources CPU, mémoire, disques, unités d'E/S, etc.

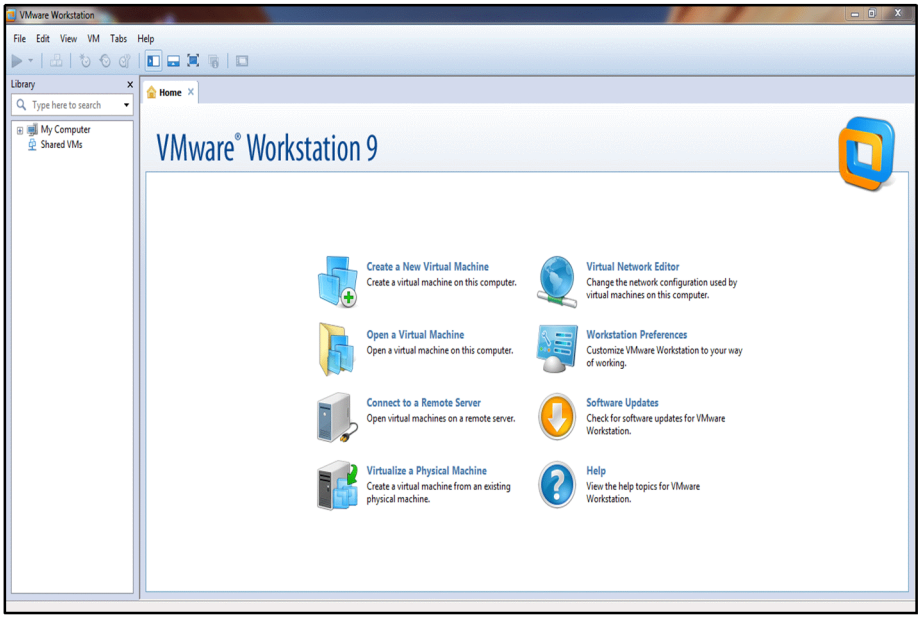


Figure IV.1 : VMware Workstation 9.0.0

IV.2.1.2.Objectifs de la virtualisation

La virtualisation permet :

- ✓ de diminuer le nombre de machines physiques, ce qui entraine une réduction d'énergie, d'espace et de temps de maintenance.
- ✓ de construire des réseaux complexes, développer, tester et déployer de nouvelles applications sur une seule et même machine sans impact sur celle-ci.
- ✓ d'effectuer des solutions efficaces pour les tests d'intrusions et failles en sécurité informatique.
- ✓ de prendre en charge des applications existantes tout en assurant une migration sécurisée vers un nouveau système d'exploitation.
- ✓ de tester les nouveaux systèmes d'exploitation dans des machines virtuelles sécurisées avant tout déploiement.

IV.2.2.Microsoft Windows Server 2008 R2

Microsoft Windows server 2008 R2 est le successeur de Windows server 2008 SP1, il apporte des fonctionnalités optionnelles. La Game Windows server 2008 a été conçu pour fournir aux entreprises des plates-formes réduisant les charges de travail en utilisant la gestion centralisé et la virtualisation intégrée. Il propose aussi des plates-formes sécurisée et facile à gérer servant à développer et à héberger de façon fiable des applications et des services Web.

Figure IV.2 : Windows serveur 2008 R2

IV.2.3.Les caractéristiques du PC utilisé

Vu que notre pratique exige l'installation de plusieurs machines virtuelles afin de simuler un réseau d'entreprise, l'utilisation d'un PC professionnel est primordiale pour installer notre système de messagerie sécurisé. Les caractéristiques du PC portable professionnel utilisées sont :

- ✓ Processeur i5 x64bits.
- ✓ RAM 8 G (4 G de base, plus l'ajout d'une extension de 4 G de RAM pour les besoins de l'application).
- ✓ Disque dur 300 G.
- ✓ Système d'exploitation Windows 7 professionnel.
- ✓ Prise en charge de la virtualisation.

IV.3.Présentation de l'Architecture

Pour l'implémentation de notre service de messagerie sécurisé via un pare-feu, nous allons mettre en place un réseau d'entreprise (LAN) avec une architecture (client/serveur) dotée d'un contrôleur de domaine Active Directory pour le DNS, et d'un deuxième contrôleur de domaine pour assurer la continuité du système en cas de panne. La figure IV.3 présente l'architecture répondant aux besoins.

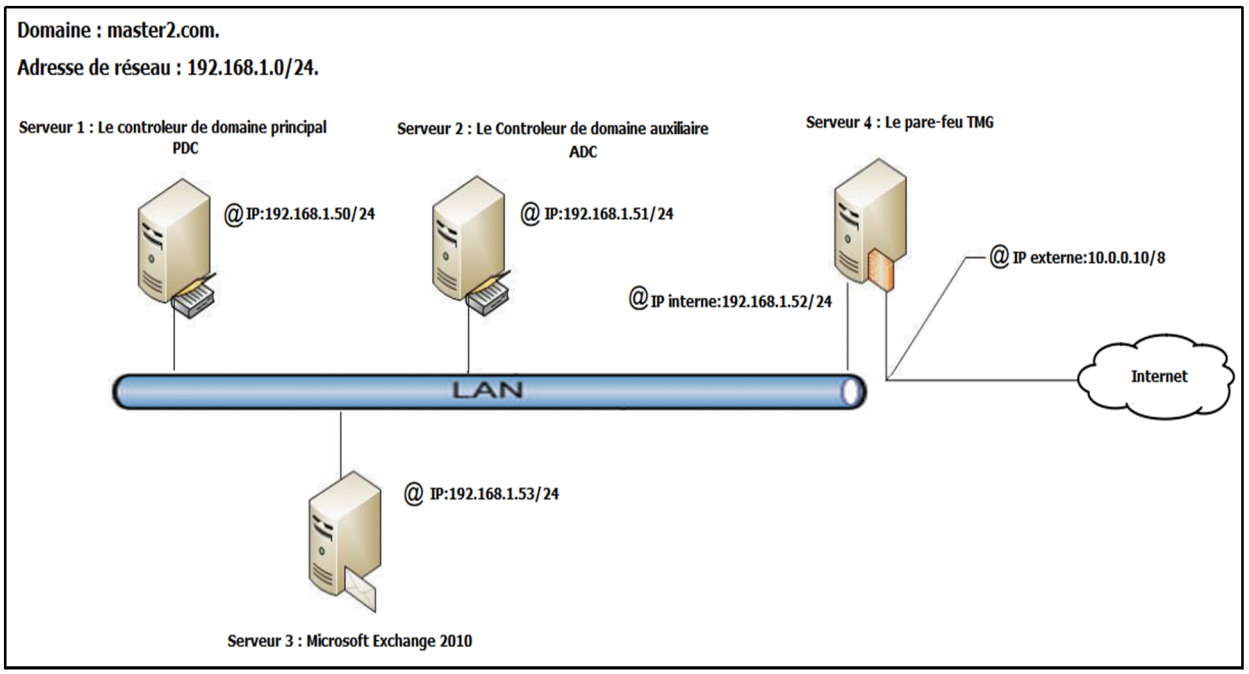


Figure IV.3 : l'architecture répondant aux besoins

IV.4.Présentation des machines

Pour la réalisation de l'architecture de notre application, nous avons préparé les machines suivantes :

- ✓ Serveur 1 : Le contrôleur de domaine principal (PDC).
- ✓ Serveur 2 : Le contrôleur de domaine auxiliaire (ADC).
- ✓ Serveur 3 : Microsoft Exchange 2010.
- ✓ Serveur 4 : Le pare-feu TMG.

IV.5.Les étapes suivies pour la mise en place de notre application

IV.5.1.Installation d'Active Directory

- **Installation du contrôleur de domaine principal (PDC)**

Le rôle principal de l'Active Directory est ADDS, qui sert à organiser les éléments du réseau (utilisateurs, ordinateurs, périphérique…) en une structure hiérarchique. Un serveur qui exécute ADDS est nommé contrôleur de domaine.

Etant donné qu'on installe Active Directory dans la première machine virtuelle et qu'on choisit de créer un domaine dans une nouvelle forêt, Active Directory le prendra comme domaine principal par défaut.

- **Les étapes**

✓ Menu Démarrer ->dans l'exécuteur de commande on saisit « DCPROMO ».

✓ Lancement de l'assistant d'installation du rôle ADDS-> on choisit « utiliser l'installation en mode avancé » : ce mode permet de fournir un fichier de réponse issu d'une autre installation, dans notre cas c'est la création d'un ADC pour la réplique du PDC.

✓ On choisit " Nouveau Domaine dans une nouvelle forêt".

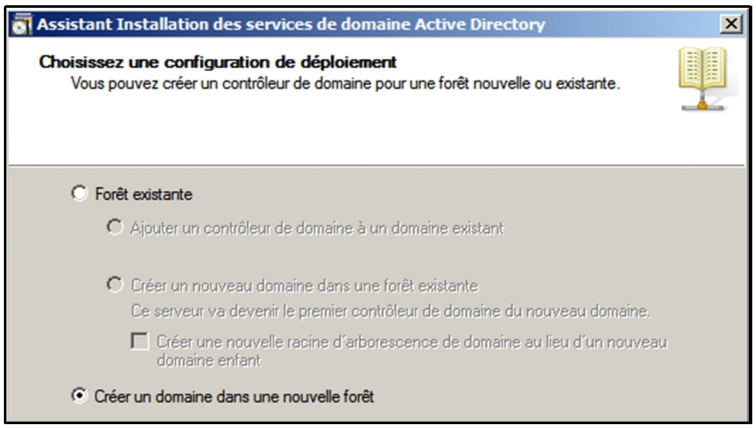


Figure IV.4 : création d'une forêt

✓ On nomme notre domaine : master2.com.

✓ L'assistant va détecter si le domaine DNS est déjà utilisé ou non sur notre réseau.

✓ on choisit le niveau fonctionnel de la forêt « Windows server 2008 ».

✓ Par défaut Active Directory crée un serveur DNS et un catalogue global. Le catalogue global est utilisé dans la réplication : il contient un sous ensemble des attributs de tous les objets de l'Active Directory.

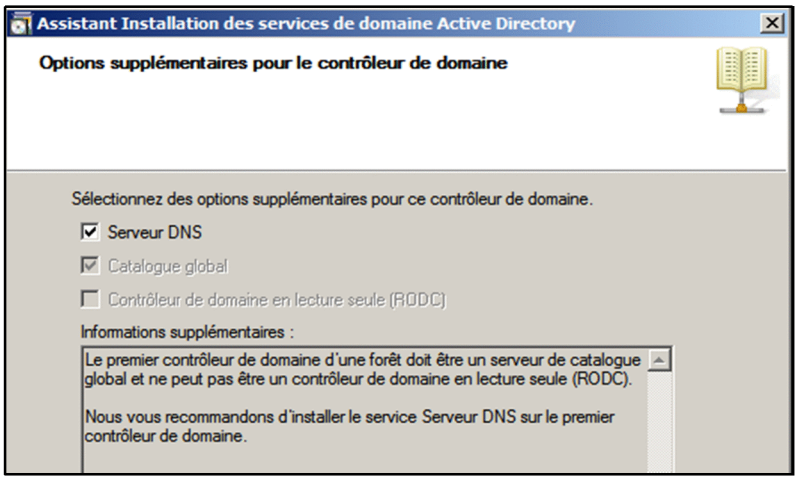


Figure IV.5 : Option pour le contrôleur de domaine

✓ Ensuite on indique le futur emplacement des fichiers servant à Active Directory.

✓ on fournit un mot de passe de restauration, pour protéger notre serveur et ainsi éviter des restaurations non souhaitées en cas de panne.

✓ Le résumé de l'installation s'affiche avant l'installation puis le serveur redémarre.

✓ Après le redémarrage, on vérifie l'installation du PDC dans le Gestionnaire de serveur.

Figure IV.6 : vérification des paramètres de l'installation du PDC

- **Installation du contrôleur de domaine auxiliaire (ADC)**

Tous les contrôleurs du même domaine se répliquent leur contenu dans une base de réplication. On assure ainsi la tolérance aux pannes car, si un contrôleur n'est pas disponible les utilisateurs ne peuvent pas s'authentifier et ne pourront pas, par conséquence, accéder à leurs ressources.

Pour cela on installe dans la deuxième machine virtuelle un contrôleur de domaine auxiliaire (ADC) qui reste passif.

- **Etapes**

Même procédure que pour le premier contrôleur de domaine à la différence des étapes suivantes :

✓ On ajoute un contrôleur de domaine à un domaine existant.

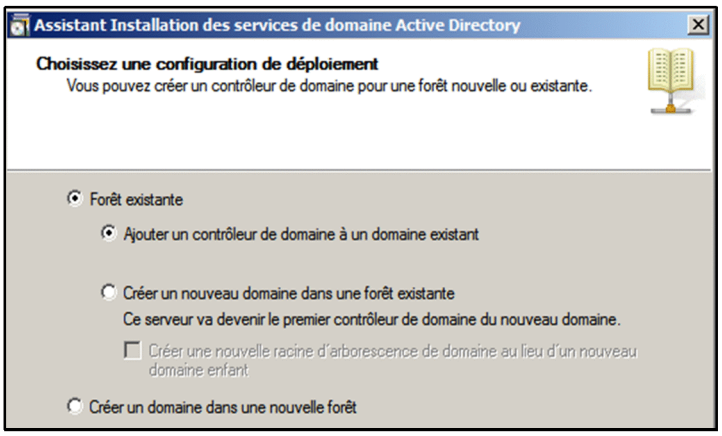


Figure IV.7 : L'ajout du contrôleur domaine auxiliaire

✓ On fournit le nom du domaine auquel on veut ajouter ce contrôleur de domaine.

✓ Dans la fenêtre « Options supplémentaires pour le contrôleur de domaine », on doit préciser si ce contrôleur de domaine est aussi un serveur DNS et un catalogue global.

✓ On précise à partir de quel contrôleur de domaine la réplication doit se faire.

✓ On choisit de répliquer les données sur le réseau à partir d'un contrôleur de domaine existant.

✓ Le résumé de l'installation s'affiche avant l'installation puis le serveur redémarre.

✓ Après le redémarrage, on vérifie l'installation de l'ADC dans le Gestionnaire de serveur.

- **Test**

Nous avons effectué un test pour savoir si les deux contrôleurs de domaine sont joignables avec la commande ping. Elle permet de tester l'accessibilité d'une autre machine à travers un réseau IP. Elle mesure également le temps mis pour recevoir une réponse, appelé round-trip time (temps aller-retour).

```
PS C:\Users\Administrateur> ping adc.master2.com

Envoi d'une requête 'ping' sur ADC.master2.com [192.168.1.51] avec 32 octets de données :
Réponse de 192.168.1.51 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.51 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.1.51 : octets=32 temps=3 ms TTL=128
Réponse de 192.168.1.51 : octets=32 temps=2 ms TTL=128

Statistiques Ping pour 192.168.1.51:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 3ms, Moyenne = 1ms
PS C:\Users\Administrateur> _
```

Figure IV.8 : Test Ping à partir du PDC

✓ Test Ping réussi.

- **Configuration et optimisation DNS**

L'assistant Active Directory a préconfiguré le DNS, cela reste une configuration par défaut insuffisante. Pour une question de sécurité et d'optimisation, nous allons créer une zone de recherche directe qui permettra de traduire les noms DNS en une adresse IP à partir d'un nom d'hôte.

- **Etapes**

✓ Menu Démarrer ->outils d'administration -> On ouvre la console de gestion DNS, on trouve les zones de recherche directe.

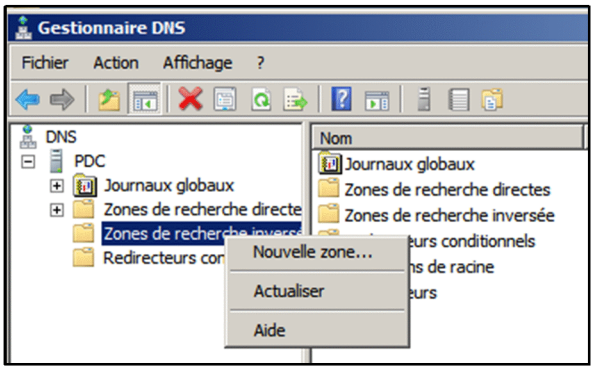


Figure IV.9 : console de gestion DNS

✓ On crée une nouvelle zone de recherche directe en zone principale et intégrée à Active Directory qui se répliquera vers tous les serveurs du domaine.

✓ On doit entrer le nom de notre zone.

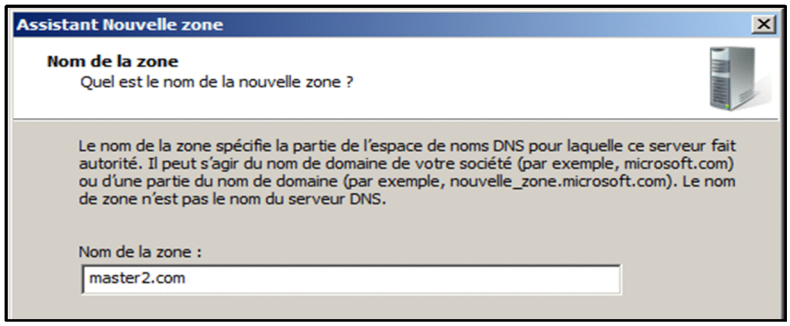


Figure IV.10 : Inscription de l'identifiant de réseau

✓ Enfin, un résumé s'affiche. La zone sera créée lorsqu'on termine l'assistant de création.

Figure IV.11 : résumé de la création de zone directe

- **Configuration et optimisation DHCP**

Ayant affecté au PDC une adresse IP statique compatible avec la plage d'adresse prévue pour le sous réseau local (192.168.1.0/24), on lance l'assistant Ajout de rôles depuis le Gestionnaire de serveur.

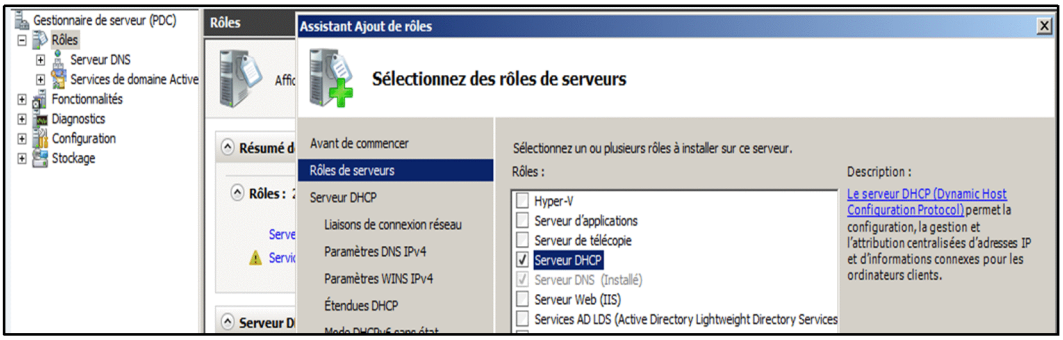


Figure IV.12 : Ajout du rôle DHCP

On sélectionne l'adresse IP affecté manuellement, qui sera le sous réseau logique des adresses qui seront affectées aux clients.

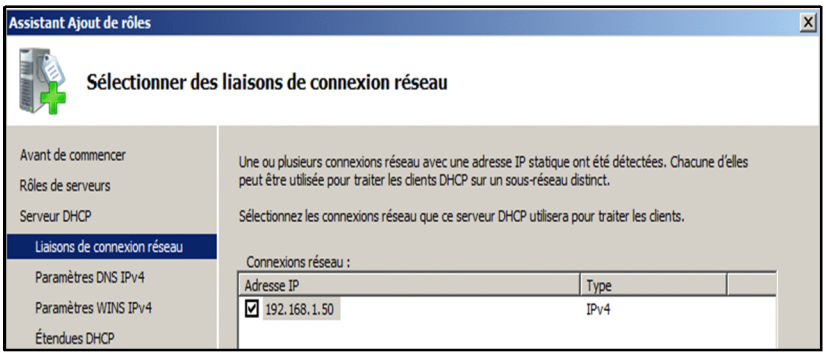


Figure IV.13: Sélection des liaisons de connexion réseau

La spécification des paramètres IPv4 du serveur DNS IPv4 permet de configurer les options DNS Domaine Name et DNS Servers pour les étendues à créer sur le serveur DHCP.

✓ L'option DNS Domaine Name permet de définir un suffixe DNS pour les connexions du client qui obtient un bail d'adresse DHCP. Elle est dans notre cas spécifiée par la valeur saisie dans la zone de texte Domain Parent master2.com.

✓ L'option DNS Server permet de configurer la liste d'adresses de serveurs DNS pour les connexions clients. Dans notre cas nous avons un seul serveur DNS qui appartient à notre domaine et dont l'adresse est 192.168.1.50.

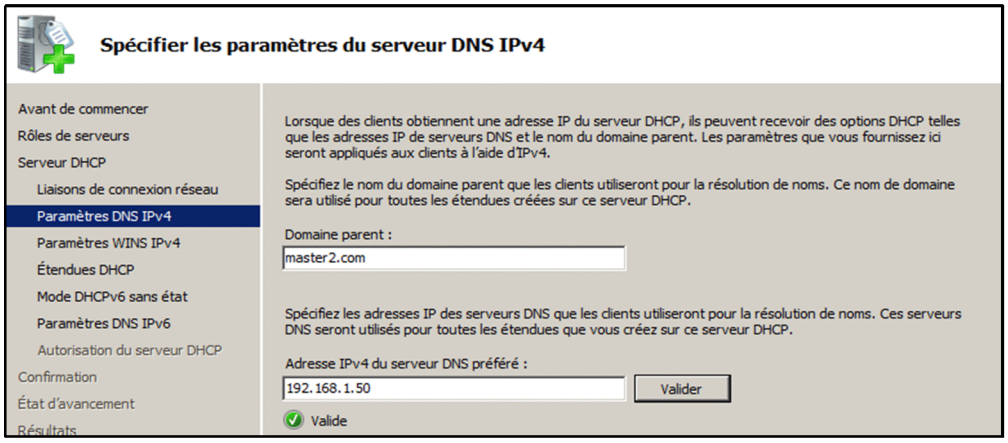


Figure IV.14 : Spécification des paramètres du serveur DNS IPv4

La spécification des paramètres du serveur WINS IPv4 permet de configurer l'option WINS, grâce à laquelle nous pouvons affecter une liste de serveurs WINS aux clients. Le serveur WINS est l'ancêtre du serveur DNS, utilisé pour les clients Windows 95 ou 98. Dans notre cas n'ayant pas de serveur WINS, cette option n'a pas été validée.

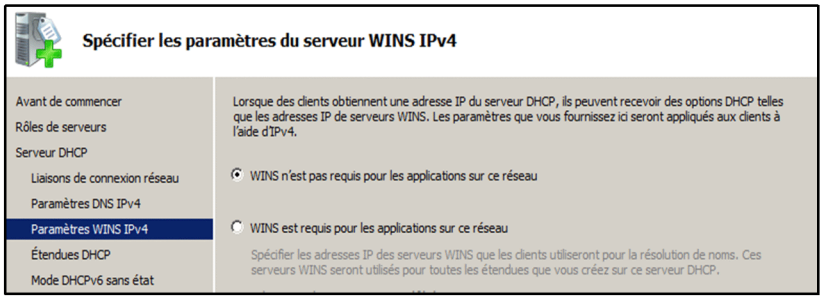


Figure IV.15 : Spécification des paramètres du serveur WINS IPv4

L'ajout d'étendues DHCP permet de définir ou de modifier les étendues sur le serveur DHCP. Notre étendu d'adresses IP pour les ordinateurs du sous–réseau DHCP est 192.168.1.60-254/24. N'utilisant que le mode DHCP IPv4, nous désactivons le mode IPv6.

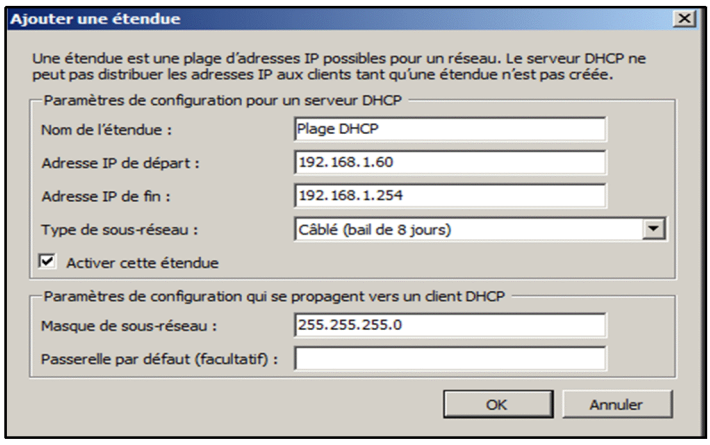


Figure IV.16 : Ajout des étendues DHCP

Dans l'environnement de domaine Active Directory, un serveur DHCP n'allouera des adresses IP à des clients que s'il est autorisé. Pour cela nous avons spécifié l'utilisateur (administrateur) qui aura tous les pouvoirs et qui gèrera le serveur DHCP.

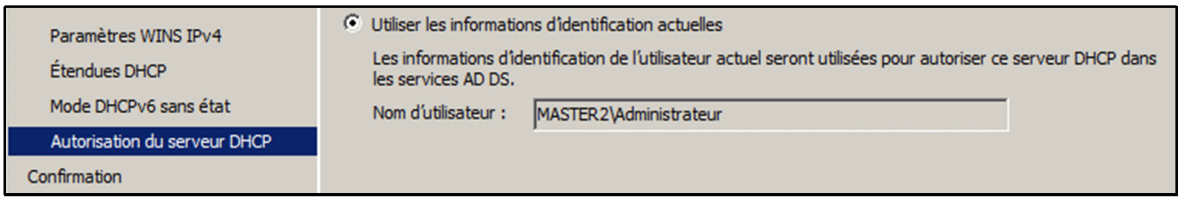


Figure IV.17: Autorisation du serveur DHCP

On aura après un récapitulatif avant le lancement de l'installation du DHCP. Et pour vérifier si le serveur est bien installé on entre dans Gestionnaire de serveur.

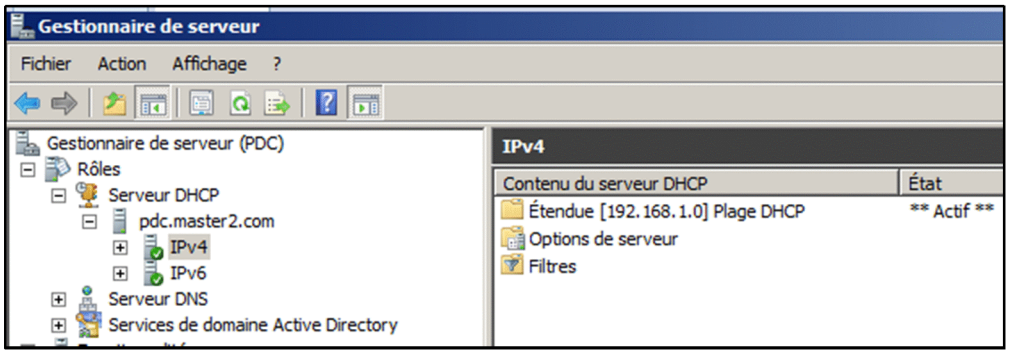


Figure IV.18 : Vérification de l'installation du DHCP

- **Installation d'une machine client test**

Pour savoir si notre serveur DHCP et bien mis en service, nous installons une machine client sous Windows XP. Cette machine ne sera pas membre du domaine, elle pourra juste communiquer avec les autre machines virtuelles via notre logiciel de simulation, cela en

spécifiant lors de la création de la carte réseau la commande host-only. D'une certaine manière comme si on avait relié nos machines via un Switch.

Nous allons dans : favoris réseau->propriétés->connexion au réseau local->Statut->Support ->Détails.

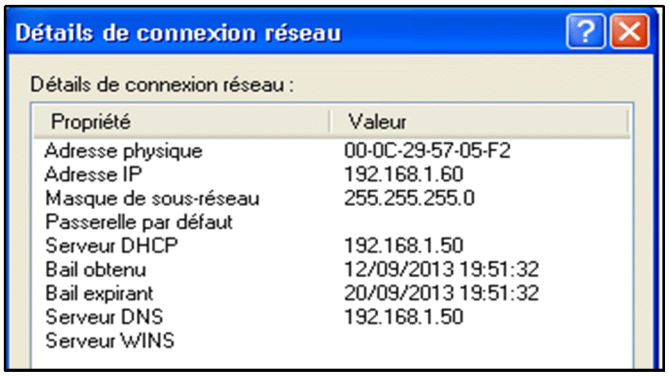


Figure IV.19 : Attribution d'adresse par serveur DHCP au client test

Notre machine a bien reçu l'adresse par notre serveur DHCP et a bien été enregistré dans les baux d'adresses que nous lui avions attribué.

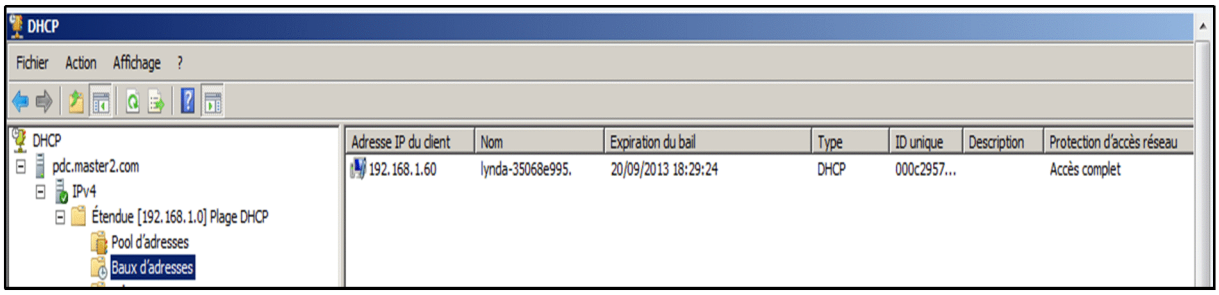


Figure IV.20 : Enregistrement au niveau du serveur DHCP

IV.5.2.Installation des applications

Avant de procéder à l'installation d'Exchange et de la TMG sur les machines, il est important de préciser qu'il faut effectuer une mise à jour au système d'exploitation via Microsoft Update.

IV.5.2.1.Installation et configuration du serveur Exchange 2010

- **Matériels exigés**
  - ✓ Un ordinateur avec un processeur 64 bits.
  - ✓ Système d'exploitation Windows Server 2008 R2 64-bits.
  - ✓ 4,6 GO ou plus de mémoire.
  - ✓ Une partition de disque dur local, formatée avec le système de fichier NTFS.
  - ✓ 2 GO d'espace disque disponible.

- **Installation des pré-requis**

L'installation du serveur de messagerie Exchange 2010 exige des pré-requis. Pour cette étape, nous avons le choix soit d'installer les prérequis en ajoutant des fonctionnalités à notre serveur via le Gestionnaire de serveur, soit se servir de l'interpréteur de commande PowerShell.

✓ Via le PowerSell :

Figure IV.21 : L'importation des modules du Gestionnaire de serveur

Figure IV.22 : Ajout des modules

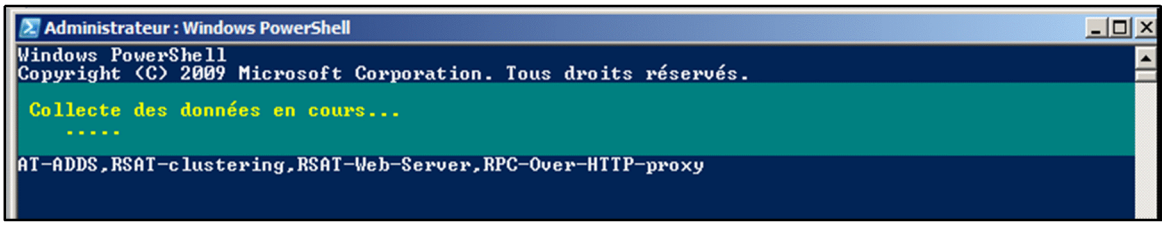


Figure IV.23 : Installation des pré-requis

Aprés un redemarrage de l'ordinateur à la fin de l'installation des fonctionnalités, on passe au paramétrage du port TCP en changant le mode de démarrage du service de partage de ports TCP.Net, afin de le passer en mode automatique.

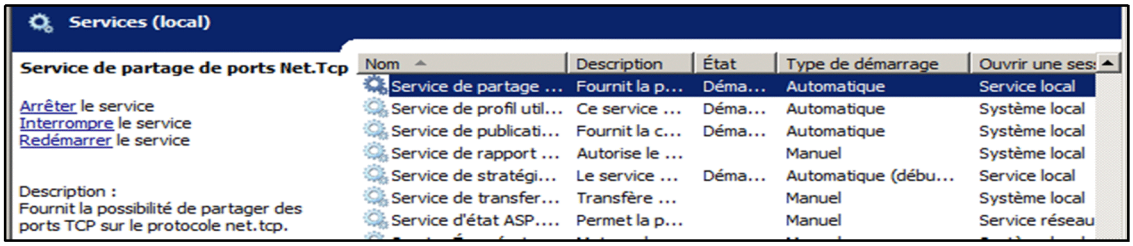


Figure IV.24 : le passage en mode automatique du service Net.Tcp

- **Préparation d'Active Directory**

Exchange 2010 nécessite un Active Directory de niveau fonctionnel 2003 au minimum pour fonctionner. Pour ce faire nous allons ouvrir l'invite de commande et se positionner à l'emplacement du programme d'installation de Microsoft Exchange server 2010. Dans notre cas on effectue l'extraction des fichiers d'exécution dans un document qu'on nomme Exchange comme le montre la figure suivante :

Figure IV.25 : Emplacement des fichiers d'exécutions

Cette partie se déroule en trois étapes :

✓ **Etape1**

Consiste à préparer le schéma d'Active Directory et cela en exécutant la commande : C:\>Setup /PrepareSchema

Cette commande permet de modifier le schéma Active Directory et d'y ajouter toutes les classes et tous les attributs nécessaires au bon fonctionnement d'Exchange 2010. On exécute cette commande dans le même domaine et dans le même site Active Directory que le contrôleur de schéma.

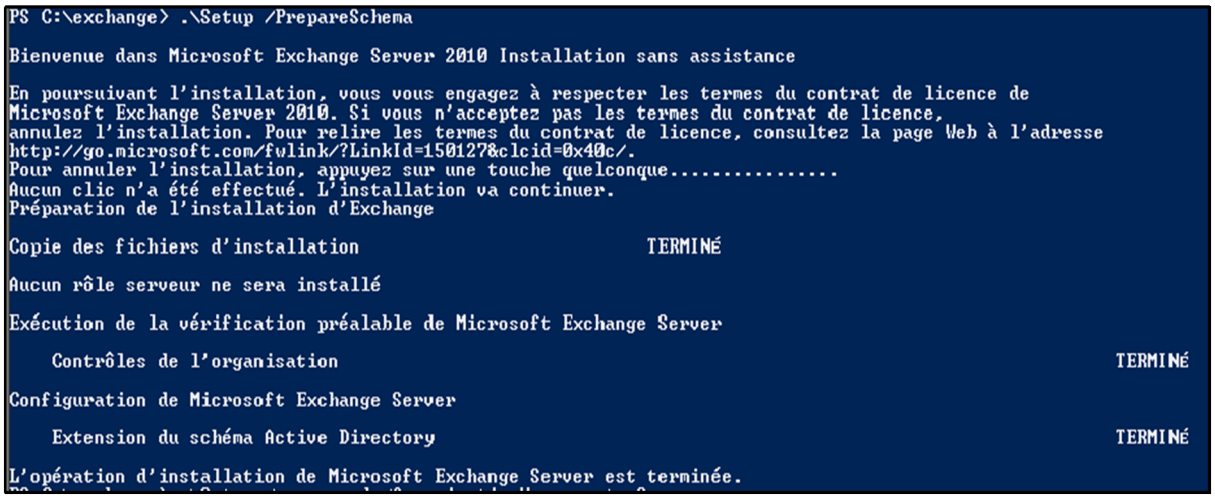


Figure IV.26 : Préparation du schéma d'Active Directory

✓ **Etape2**

Consiste à préparer la forêt master2.com et cela en exécutant la commande :

C :\> Setup /PrepareAD /OrganizationName:master2

Cette commande permet de créer l'organisation Exchange (c'est à dire le conteneur stockant les paramètres d'Exchange dans la partition de configuration Active Directory). Dans un second temps, il prépare le domaine en créant une unité d'organisation contenant les groupes universels de sécurité nécessaires à Exchange.

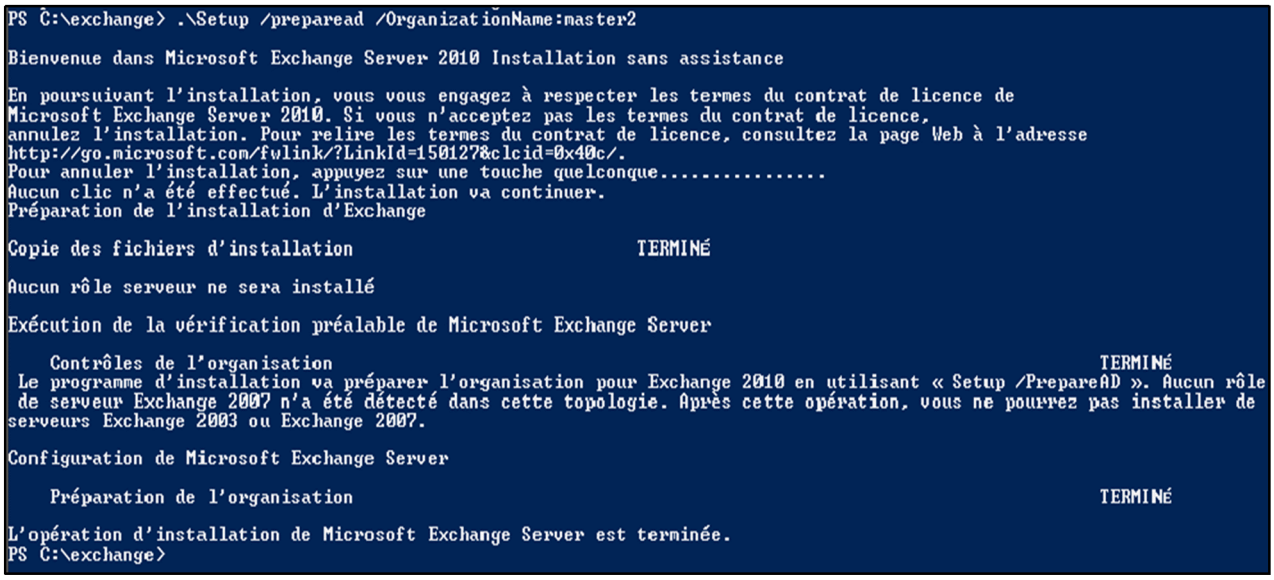


Figure IV.27 : Préparation de la forêt

✓ **Etape3**

Consiste à préparer le domaine et cela en exécutant la commande :

C:\>Setup /PrepareDomain

Cette commande prépare le domaine actuel en créant une unité d'organisation contenant le ou les groupes nécessaires au bon fonctionnement d'Exchange 2010.

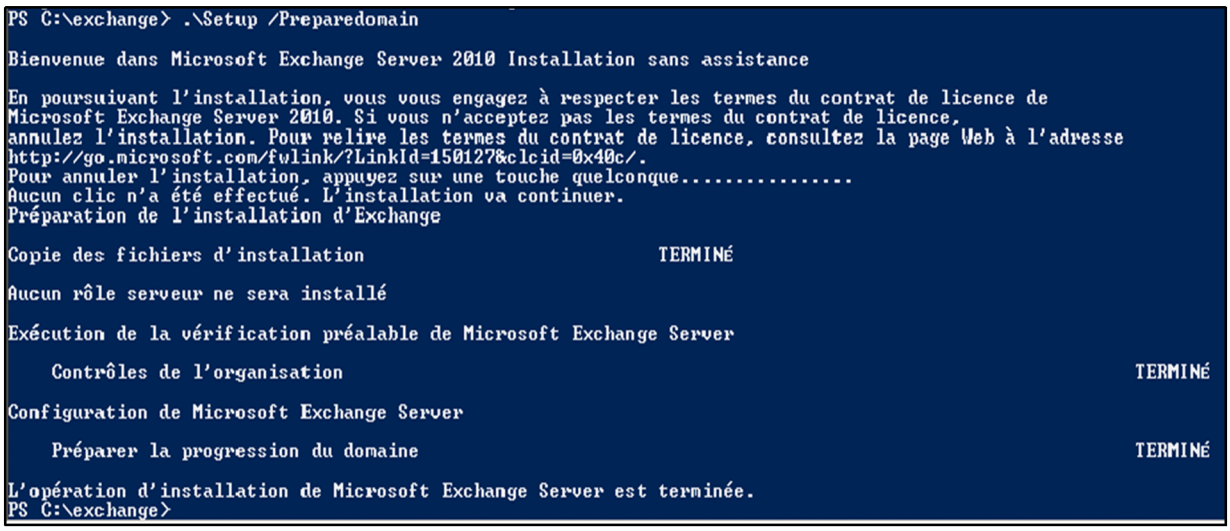


Figure IV.28 : Préparation du domaine

Une fois tous les pré-requis validés, on passe au déploiement d'Exchange. Pour cela on exécute le fichier « setup » situé dans le dossier d'installation.

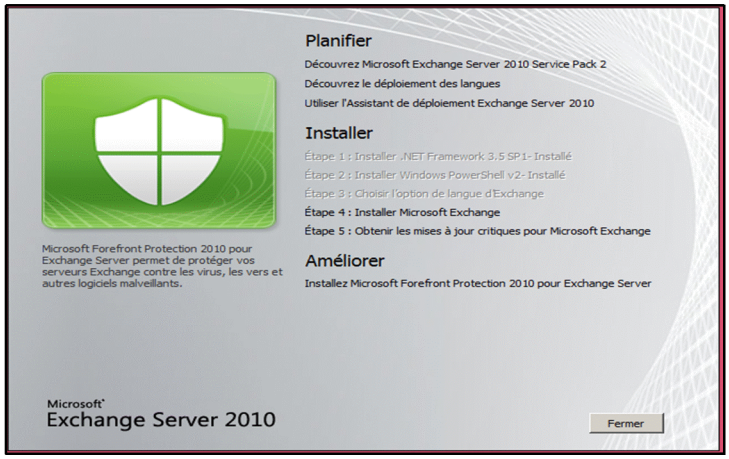


Figure IV.29 : Lancement d'installation d'Exchange

Après avoir passé l'introduction, accepté le contrat de licence et choisi un mode de rapport d'erreur, on a le choix entre une installation typique ou personnalisée. L'installation personnalisée permet d'installer les rôles choisis alors que l'installation typique installera les rôles CAS, Hub et boîte aux lettres ainsi que les outils de gestion Exchange. On procède à l'installation typique.

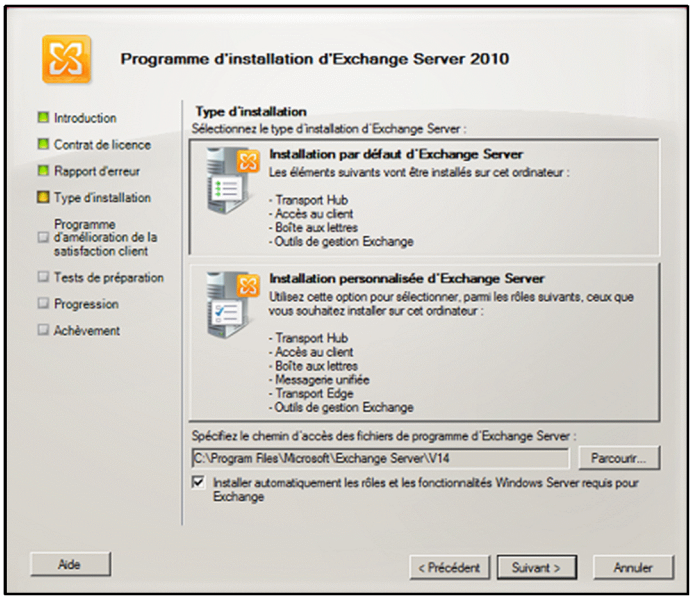


Figure IV.30 : Le choix du type d'installation

L'assistant nous demande ensuite si notre réseau contient des clients Outlook 2003 ou Entourage (Mac OS). Cela permet d'assurer une compatibilité pour ces clients anciens. Nous n'avons pas ces clients donc on fait le choix correspondant.

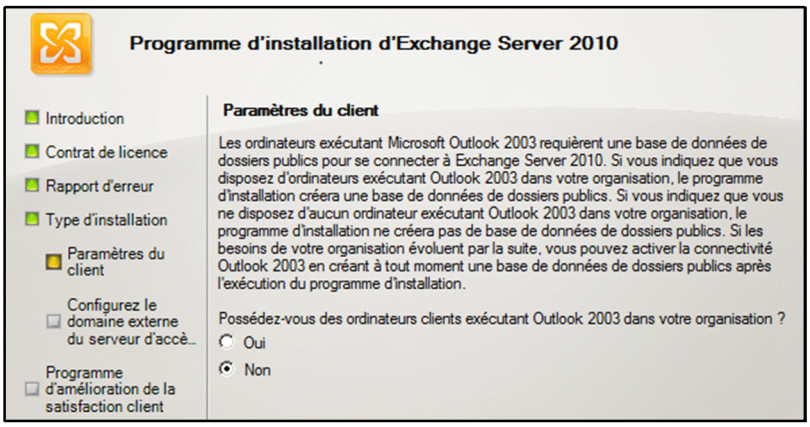


Figure IV.31 : Paramètres du client

Afin de rendre le rôle d'accès client disponible depuis Internet pour OWA, Outlook Anywhere ou Active Sync, on indique le nom externe qu'aura notre serveur.

Figure IV.32 : Configuration de domaine externe du serveur d'accès client

Avant de lancer l'installation, Exchange procède à quelques tests afin de s'affranchir d'éventuels problèmes lors de l'installation.

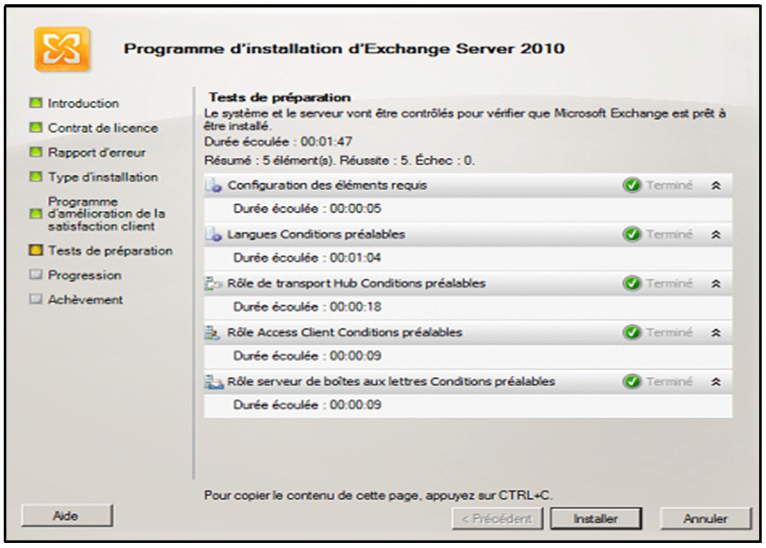


Figure IV.33 : Les tests de préparation

Une fois les tests effectués, on lance l'installation. Elle peut durer plus ou moins longtemps selon le serveur et les rôles à installer. Dans notre cas, Exchange a mis 45 minutes car on utilise un lab d'essai, il n'est donc pas adapté aux besoins d'Exchange. Sur un serveur dimensionné correctement, l'installation sera plus rapide.

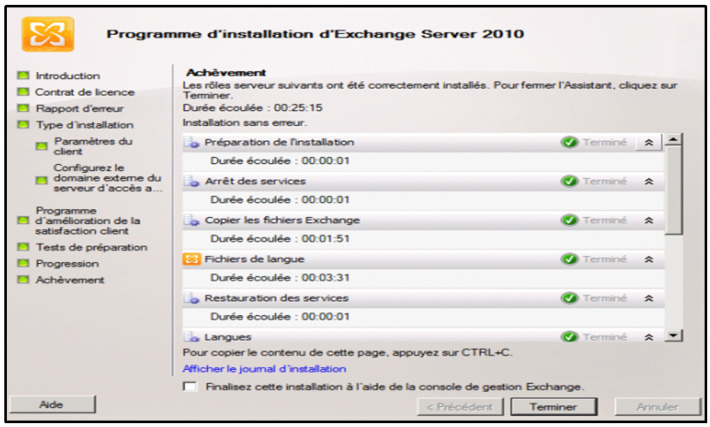


Figure IV.34 : Achèvement de l'installation d'Exchange

Avant de lancer la console de gestion d'Exchange : il est préférable de mettre à jour le serveur Exchange via Microsoft Update.

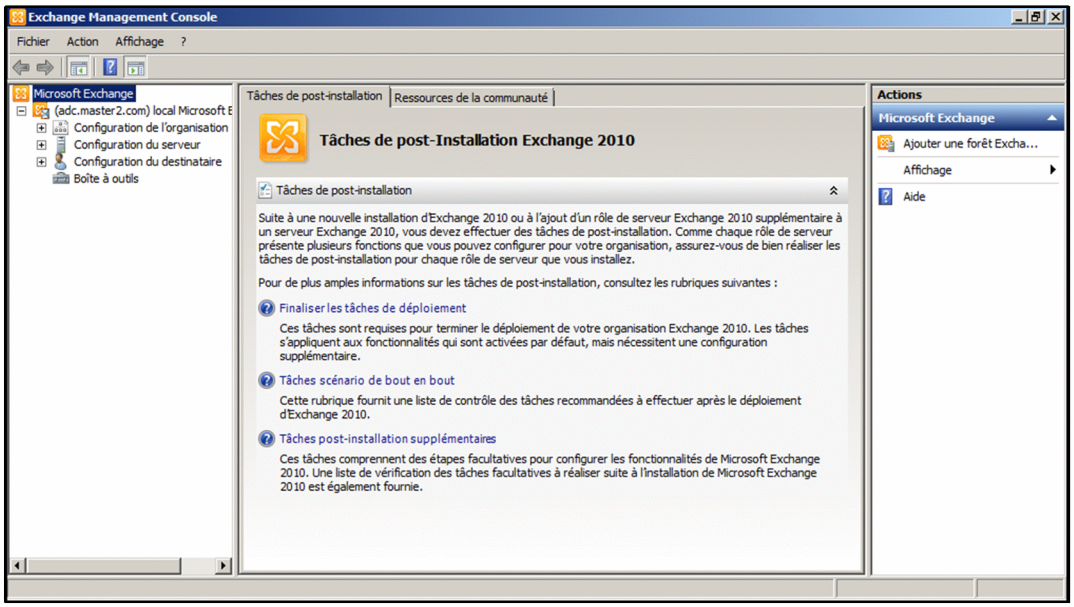


Figure IV.35 : La console de gestions Exchange

- **Configuration du serveur Exchange**

  ✓ **Création des bases de données**

Lors de son installation, Exchange crée automatiquement une base de données par défaut. Néanmoins nous allons créer une nouvelle, pour une question de sécurité, depuis la console, configuration de l'organisation->boîte aux lettres->nouvelle base de données de

boîte aux lettres. Puis on indique le nom de la base de données ainsi que le serveur Exchange qui l'héberge.

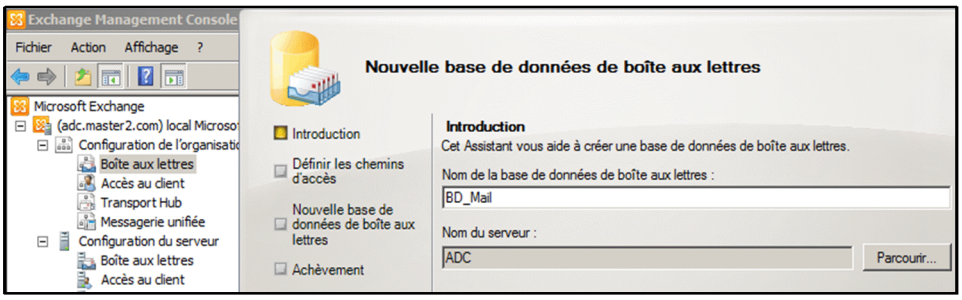


Figure IV.36 : Création de la base de données de boite aux lettres

✓ **Création d'un compte de messagerie utilisateur**

Il existe différents types de boîtes aux lettres :

1. **Boite aux lettres utilisateur :** boîte classique pour un utilisateur.
2. **Boite aux lettres de salles :** permet de réserver des salles de réunions.
3. **Boite aux lettres d'équipements :** permet de réserver des équipements (vidéoprojecteurs).
4. **Boîtes aux lettres liée** : permet d'associer une adresse mail avec un compte situé par exemple dans une forêt différente.
5. **Autodiscover** : permet d'activer la recherche d'un mail depuis les boites aux lettres.

Pour créer un compte de messagerie, on utilise les boites aux lettres utilisateurs. Pour ce faire, Configuration de destinataire->boîte aux lettres->nouvelle boîte aux lettres.

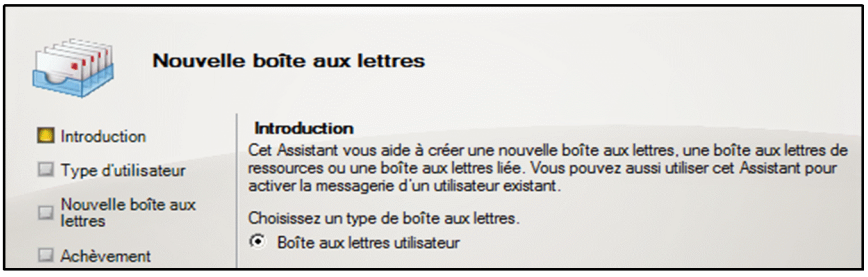


Figure IV.37 : Création de boite aux lettres utilisateur

L'étape suivante nous permet de sélectionner les utilisateurs existants.

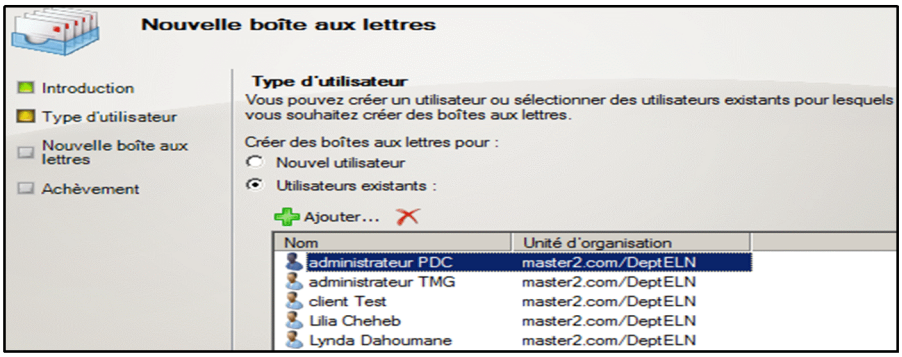


Figure IV.38 : seléction des utilisateurs

Sélectionnons la base de données BD_Mail où seront sauvegardés les mails des utilisateurs.

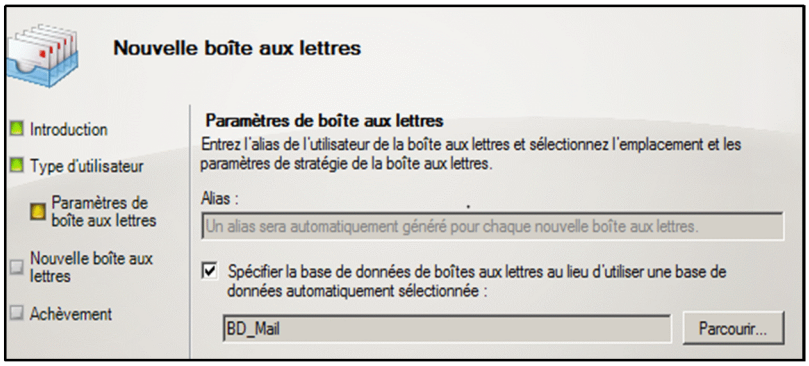


Figure IV.39 : paramétrage de boite aux lettres

IV.5.2.2.Installation et configuration de la TMG

- **L'ajout de la TMG comme serveur membre**

Un serveur ou une machine membre ne sont pas des contrôleurs de domaine mais seulement des membres du domaine. Pour ajouter la TMG comme membre, il faut accéder aux propriétés systèmes et modifier le domaine de l'ordinateur comme le montre la figure suivante :

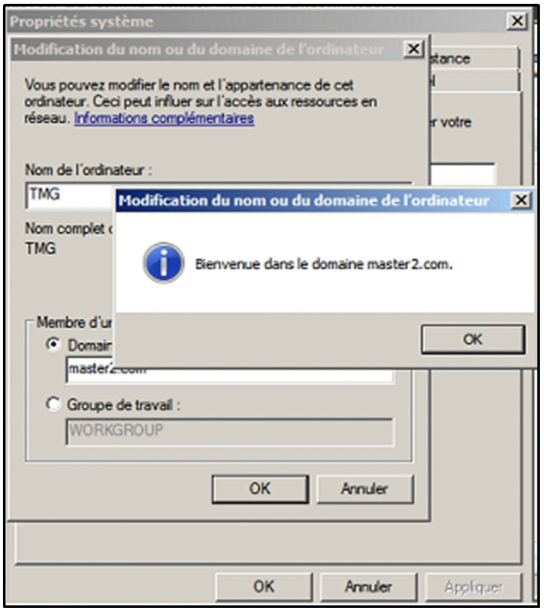


Figure IV.40 : Ajout de la TMG au domaine master2.com

Pour éviter tout problème pendant l'installation de Forefront TMG 2010, avant de commencer, nous avons pris en compte les conditions suivantes :

- **Condition d'installation**

1. Matériels exigés

- ✓ Un ordinateur avec un processeur 64 bits.
- ✓ Système d'exploitation Windows Server 2008 R2 64-bits.
- ✓ 2 GO ou plus de mémoire.
- ✓ Une partition de disque dur local, formatée avec le système de fichier NTFS.
- ✓ 3 GO d'espace disque disponible.

2. Configuration des cartes réseaux

L'installation préalable de la TMG exige l'ajout et la configuration de 2 cartes réseaux :

- ✓ Une interne avec l'adresse IP 192.168.1.52/24.
- ✓ Une externe avec l'adresse IP 10.0.0.10/8.

- **Lancement de l'installation**

Au lancement du programme d'installation, le processus d'installation nous recommande d'installer les dernières mises à jour puis d'exécuter l'outil de préparation pour installer l'ensemble des pré-requis nécessaires pour le déploiement de la plate-forme TMG.

Figure IV.41: Lancement de Forefront TMG 2010

Après avoir lancé l'outil de préparation, on choisit le mode d'installation que l'on souhaite effectuer. On installe les services et fonctionnalités de la TMG et la console de gestion pour une installation complète de celle-ci.

Figure IV.42 : Le type d'installation de la TMG

Les rôles et les fonctionnalités essentiellement installés sont :

- ✓ Serveur NPS (Network Policy Server).
- ✓ Outils des services AD LDS (Active Directory Lightweight Directory Service).
- ✓ Outils d'équilibrage de la charge réseau (Network Load Balancing).
- ✓ Windows Power Shell.
- ✓ Microsoft .NET Framework 3.5 SP1.
- ✓ API des Services Web Windows.
- ✓ Microsoft Windows Installer 4.5.
- ✓ Microsoft Chart Controls for Microsoft .NET Framework 3.5 and 3.5 SP1.

Ensuite, il nous ait demandé d'ajouter les cartes réseau, dans notre cas pour gérer le réseau interne on sélectionne la carte interne.

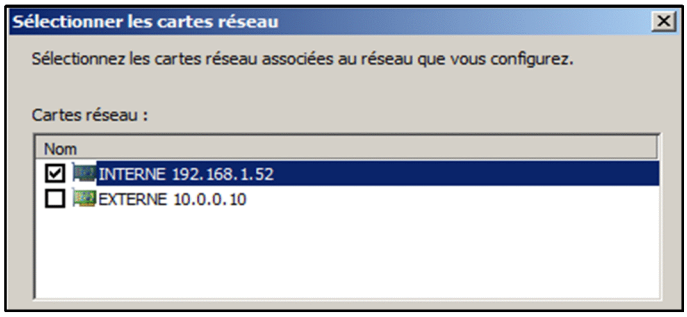


Figure IV.43 : sélection des cartes réseau

Aprés la seléction de la carte interne, la plage d'adresses de celle-ci sera calculée et listée.

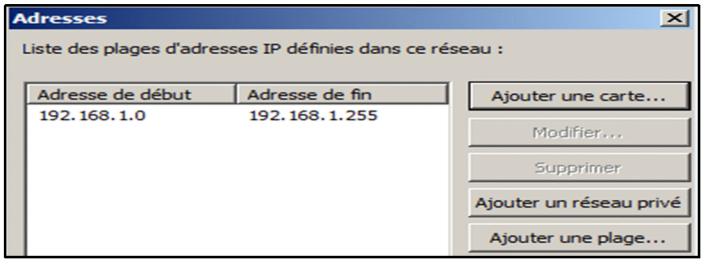


Figure IV.44 : La plage d'adresse IP du réseau interne

A la fin de l'installation de Forefront TMG, on lance la console de gestion.

Figure IV.45 : la console de gestion de la TMG

- **La création des règles de la TMG**

Il est indispensable de configurer les règles qu'il faut autoriser avant d'entreprendre n'importe qu'elle configuration au niveau interne, car la TMG interdit par défaut tout le trafic entrant et sortant sur tous les réseaux (internes, externes et locaux). Nous avons autorisé les règles DNS, PING, HTTP/HTTPS en spécifiant, pour chacun d'eux le réseau entrant, sortant et les utilisateurs sur lesquels elles seront appliquées. Comme exemple de création d'une règle TMG, nous prenons celle du DNS qui permet de spécifier un ordinateur sur lequel elle s'applique.

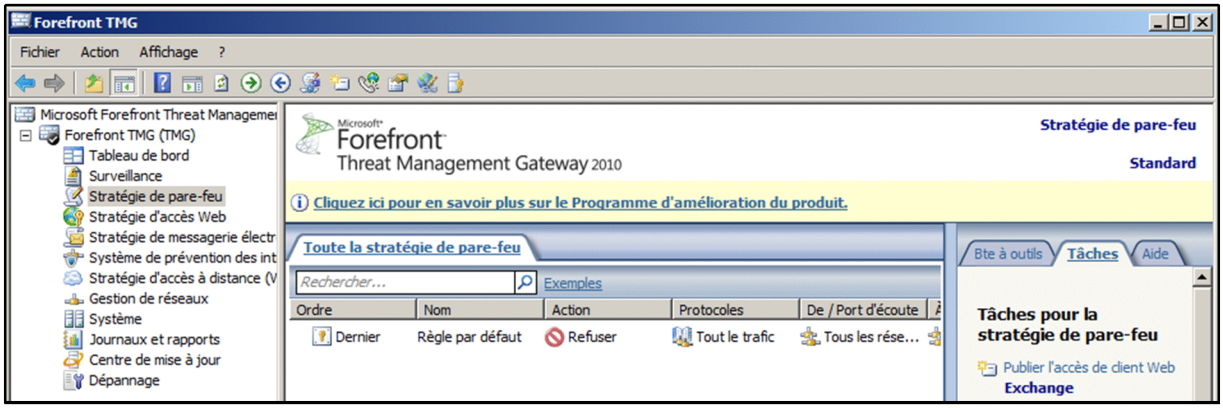


Figure IV.46 : La configuration par défaut du trafic de la TMG

- **Exemple de la règle DNS**

Pour la création de la règle d'accès DNS, stratégie de pare-feu->entrons le nom DNS.

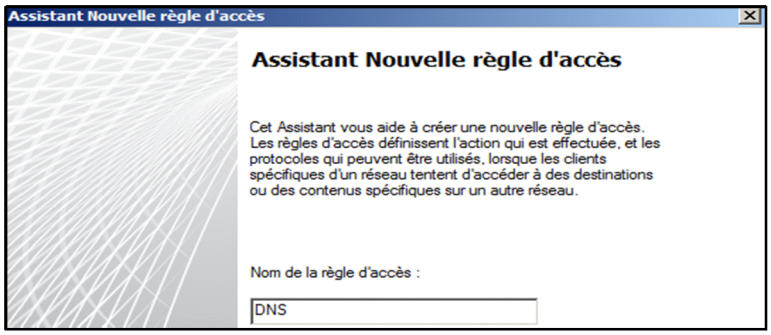


Figure IV.47 : Création de la règle d'accès DNS

Notre objectif étant d'autoriser la règle DNS, sélectionnons autoriser.

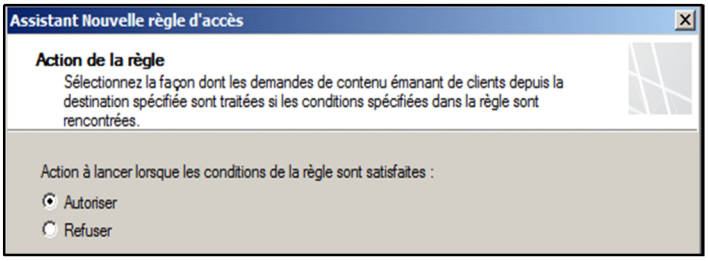


Figure IV.48 : Choix de l'action de la règle

Dans ajout de protocoles nous spécifions sur quels protocoles s'applique cette règle (DNS).

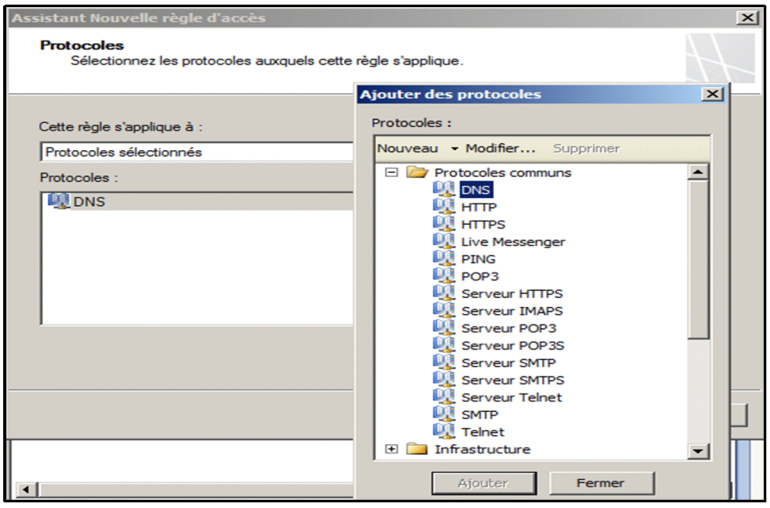


Figure IV.49 : Sélection des protocoles

Cette règle s'appliquant sur le serveur DNS, **pdc.master2.com.** Dans l'ajout des entités réseau, nous sélectionnons ce serveur avec son adresse IP comme source de règles d'accès.

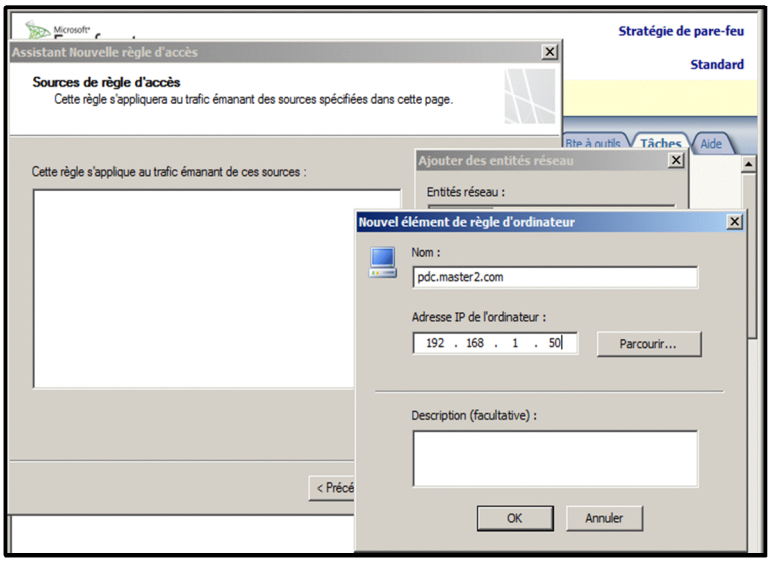


Figure IV.50 : Sélection de la source de règle d'accès

Le trafic destinataire étant le réseau local, on sélectionne l'hôte local.

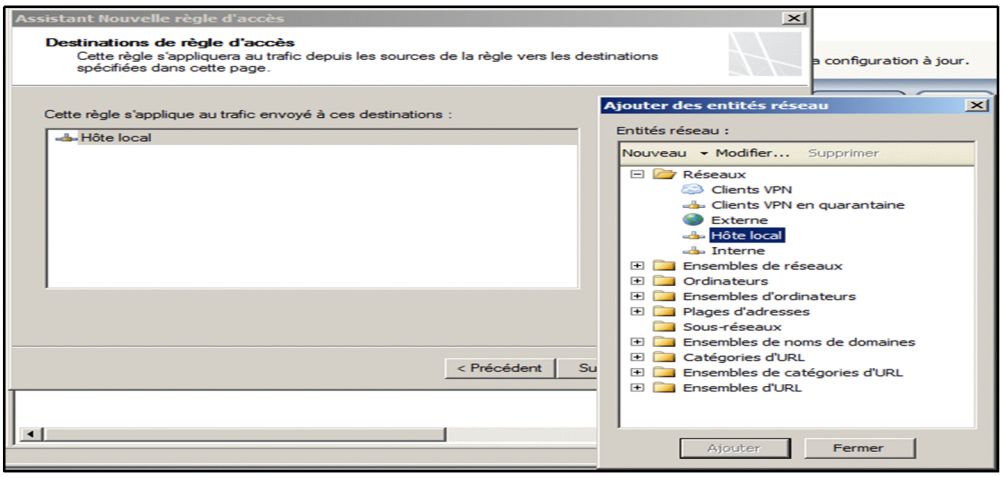


Figure IV.51 : Spécification de la destination de la règle d'accès

Spécifions sur quels utilisateurs s'applique cette règle, dans ce cas tous sont concernés par le DNS.

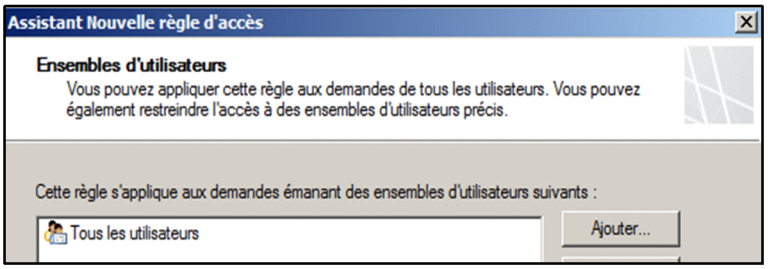


Figure IV.52: Ensemble des utilisateurs concernés par la règle d'accès

Afin de valider et d'enregistrer toute modifications apportées à la TMG, nous cliquons sur Appliquer.

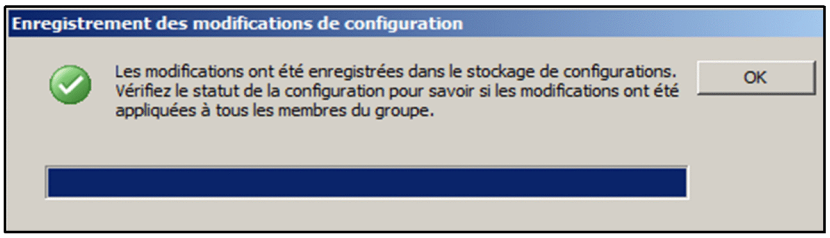


Figure IV. 53: Enregistrements des modifications

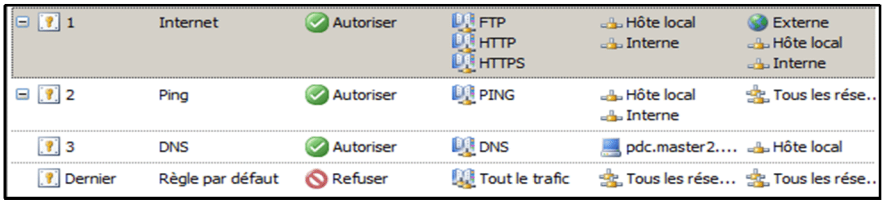


Figure IV. 54: Récapitulatif des règles de la TMG

IV.5.3.Publication du serveur Exchange

IV.5.3.1.Publication du serveur Exchange via les certificats

Pour sécuriser les échanges au niveau interne et limiter les accès depuis l'extérieur aux personnes autorisées. Nous allons dans ce qui suit publier un certificat.

- **Installation de l'autorité de certification (rôle ADCS)**

L'ADCS est un rôle d'Active Directory proposant différents services configurables pour créer et gérer des clés et certificats pour la protection des applications utilisés dans les réseaux.

L'installation du service certificat nécessite une installation préalable d'un service Web IIS, qui propose la prise en charge du protocole SSL pour sécuriser les données transmises sur le réseau entre un serveur web et le client. Le tout nous fournit une infrastructure d'application web sécurisé et fiable.

- **Etapes**

✓ Pour l'ajout du serveur Web IIS comme fonctionnalité, on effectue les étapes suivantes : menu démarrer-> outils d'administration->gestionnaire de serveur et l'ajouter comme rôle, à la fin le résultat d'installation s'affiche.

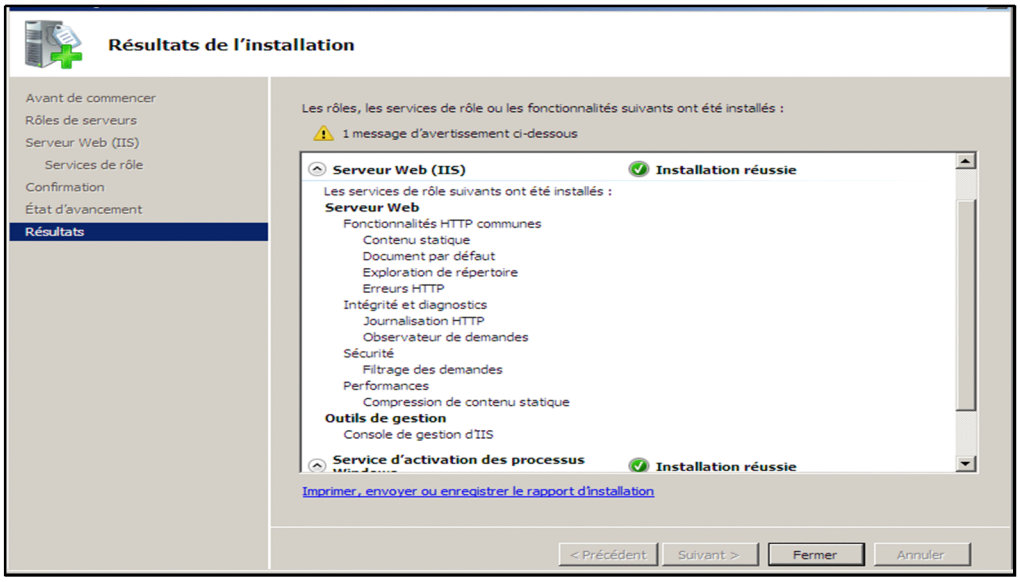


Figure IV.55: Fin d'installation du serveur web IIS

✓ Maintenant on passe aux étapes de l'installation de l'ADCS.

✓ Menu Démarrer->Gestionnaire de serveur->ajouter des rôles->on ajoute le rôle services certificat Active Directory, puis une page nous propose les différents services disponibles pour ADCS et on choisit deux services qui sont Autorité de certification (AC) et Inscription de l'autorité de certification via le web.

✓ Lors de l'installation, il faut spécifier le type de l'installation de la AC, **Autonome** ou **Entreprise**, Autonome signifie que la AC n'est pas nécessairement intégrée dans un service d'annuaire AD alors que l'entreprise exige d'avoir un service d'annuaire, comme Exchange est membre de l'Active Directory, notre choix s'est porté sur cette AC qui sera utilisée comme émettrice. Elle sera subordonnée à une autre AC dans une hiérarchie, fournissant de ce fait des certificats aux utilisateurs autorisés, intérieurs et extérieurs.

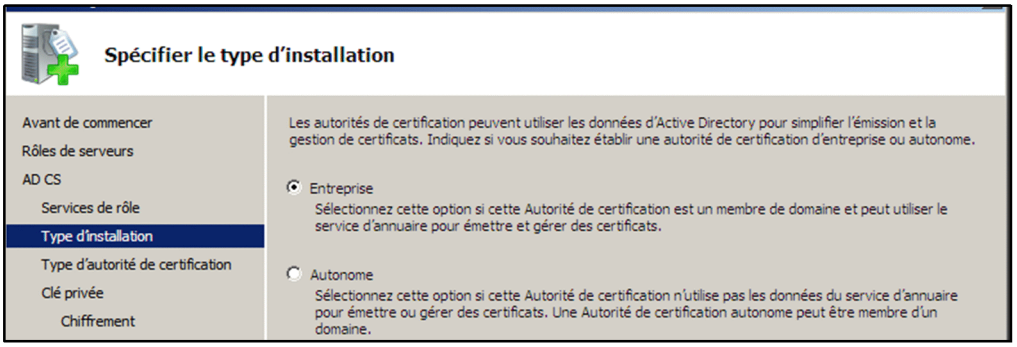


Figure IV.56 : Spécification du type d'installation

✓ On doit créer une nouvelle clé privée, en spécifiant le fournisseur de service de chiffrement (RSA), l'algorithme de hachage (Sha1) et la langueur de la clé en caractère (2048).

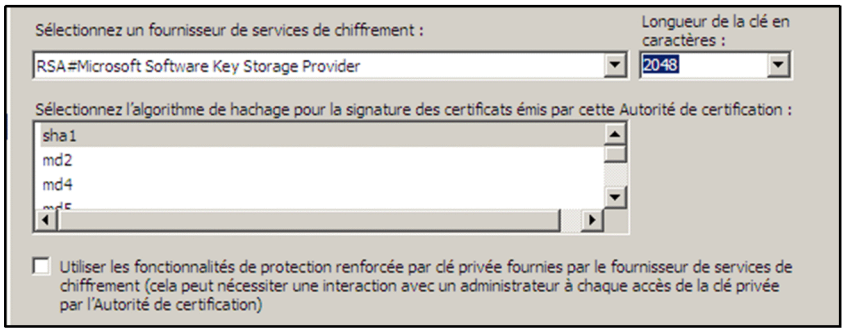


Figure IV.57 : Création d'une nouvelle clé privé

✓ On définit ensuite le nom de l'autorité de certification qu'on nomme **master2-ADC-CA** et ensuite on spécifie la période de validité du certificat. Et on termine par une confirmation de fin d'installation.

Figure IV.58: Nomination de l'Autorité de certification

A la fin de la création de l'autorité **master2-ADC-CA,** nous nous rendons au serveur IIS, nous remarquons qu'un certificat auto-signé est aussi créé automatiquement, d'exchange pour exchange (du nom d'hôte pour le nom d'hôte). Par défaut, Exchange se crée un certificat auto-signé qu'il assigne aux différents services. Le problème de ce genre de certificat est qu'on ne peut pas lui faire confiance. Par exemple, si notre serveur vous dit qu'il s'est auto-proclamé www.votredomaine.com (alors qu'en réalité c'est www.voleur-de-domaine.com), allez-vous lui faire confiance ? Le certificat étant auto-signé, il est réputé comme n'étant pas de confiance on aura alors constamment des erreurs de validation SSL lors des différents accès au serveur.

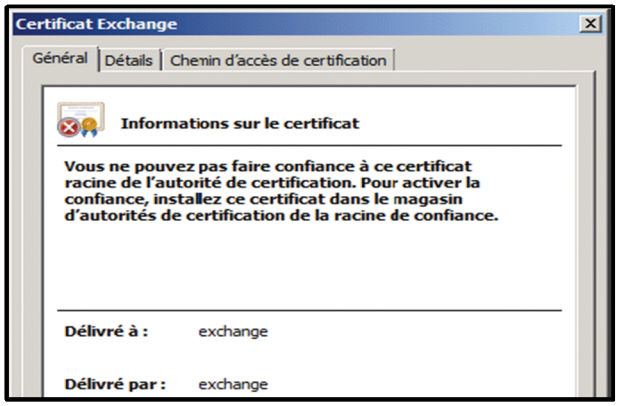


Figure IV.59: Certificat auto-signé

L'étape suivante consiste à la demande de création de certificat, certifiée par notre CA.

- **Préparation de la Demande de certificat**

Après avoir créé le modèle de certificat, nous allons dans le serveur IIS pour générer des certificats en effectuant une demande comme suit : certificat de serveur-> créer une demande

de certificat. Sur la page qui s'affiche on doit remplir les informations de sorte à être précis car les personnes détenant le certificat doivent être rassurées de sa provenance.

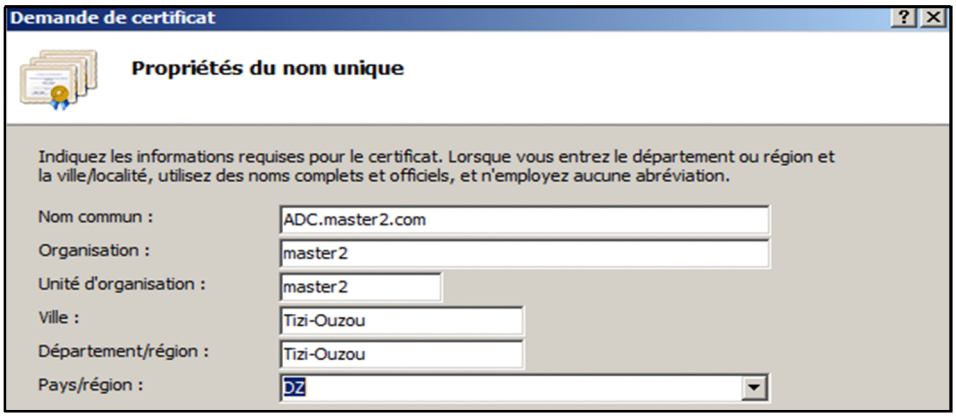


Figure IV.60 : Demande de certificat.

L'étape suivante consiste à sélectionner le fournisseur de services de chiffrement ainsi que la longueur de la clé de chiffrement.

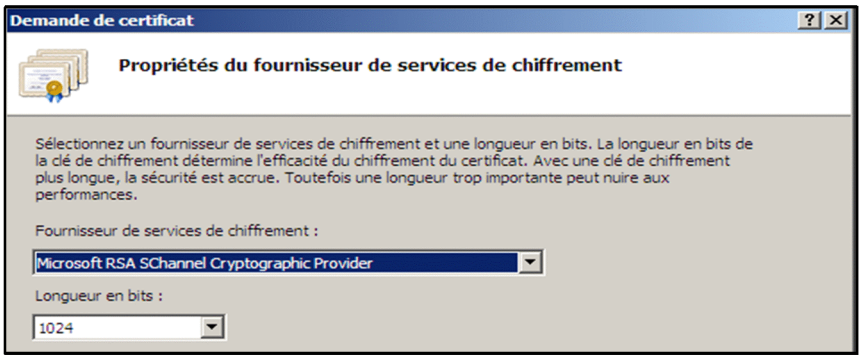


Figure IV.61: Propriétés du fournisseur de services de chiffrement

Ensuite on spécifie l'emplacement du fichier d'exportation du certificat.

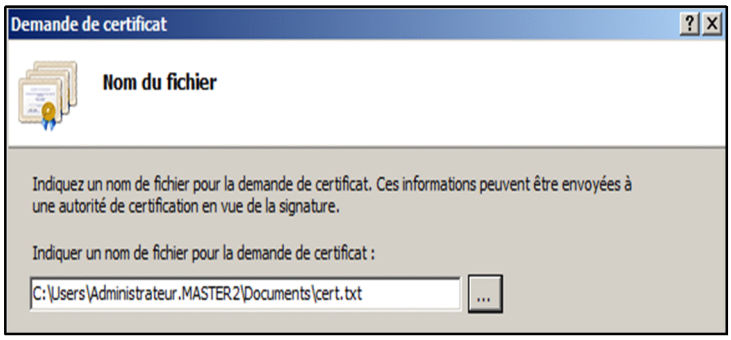


Figure IV.62 : Fichier de demande de certificat

A la fin en allant à l'emplacement du fichier d'exportation, nous trouvons la clé privé que voici :

Figure IV.63 : Clé privée de certificat

Apres avoir effectué la demande de certificat, allons à IIS, en utilisant le site par défaut, en exigeant le SSL dans paramètre SSL modifiant la liaison de ce dernier pour utiliser le HTTPS avec le certificat auto-signé comme suite :

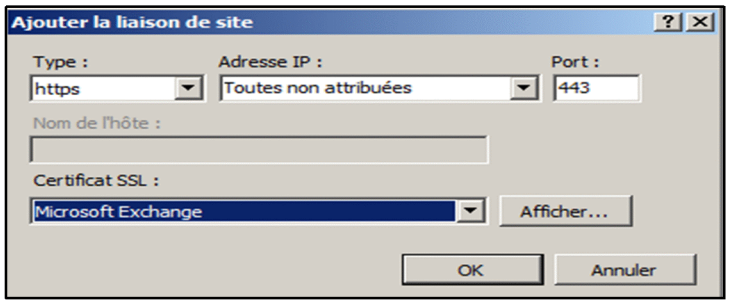


Figure IV.64: Modification de la liaison de site

Pour soumettre la demande de certificat via internet explore, nous suivons ces étapes : **https://adc.master2.com/certsrv** -> demande de certificat -> demande de certificat avancée -> soumettre une demande en utilisant un fichier PKCs#7 codé en base 64. Dans la page qui s'ouvre, nous écrivons la clé privée obtenue et nous spécifions le modèle de certificat, serveur web.

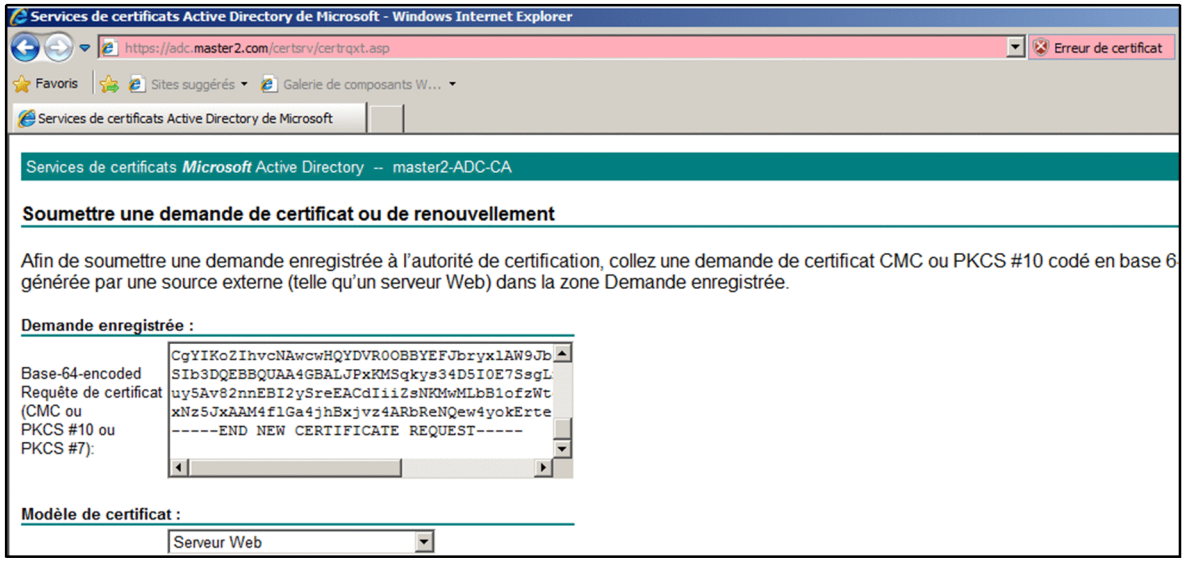


Figure IV.65: Soumettre une demande de certificat

Le site n'étant pas encore certifiée par notre CA, provoque des erreurs de certificat en HTTPS qui apparait en rouge.

Et enfin Pour finir la demande, on télécharge le certificat en spécifions son emplacement.

- **Terminer la demande de certificat**

Une fois la demande faite, terminons cette dernière en allant à IIS->serveur certificat-> terminer une demande de certificat, ou nous spécifions l'emplacement du certificat que nous venons de télécharger ainsi que son nom convivial, **IIScertsuradc.**

Figure IV.66: terminer la demande de certificat

Pour finaliser notre configuration, nous pouvons modifier la liaison du site par défaut en utilisant cette fois le nouveau certificat signée par notre CA, master2-PDC-CA.

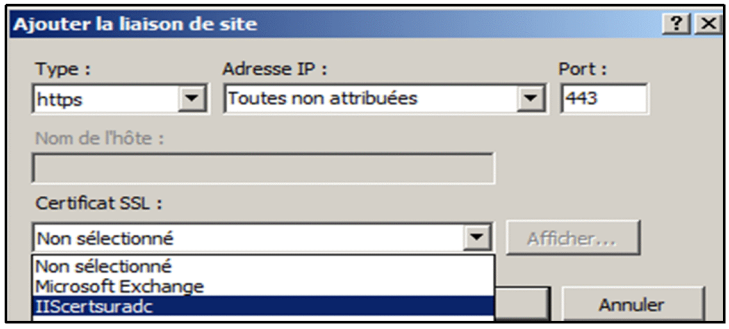


Figure IV.67: Modification de la liaison de site

Pour vérifier que notre certificat ne présente pas d'erreur, nous nous connectons une autre fois au site adc.master2.com avec HTTPS.

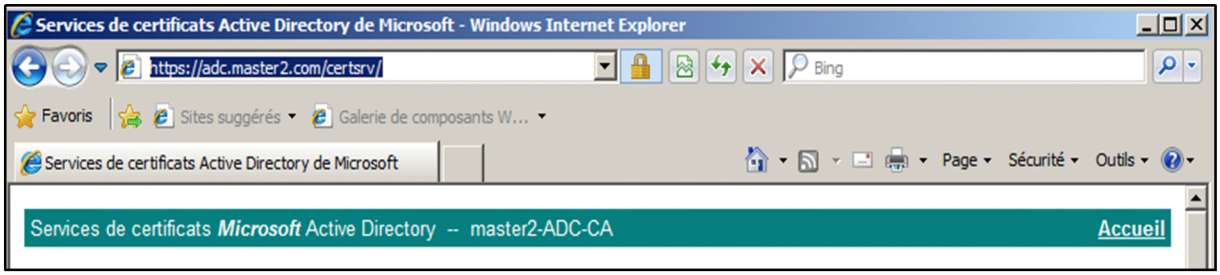


Figure IV.68 : Installation du certificat

Le cadenas bleu apparait, il n'y a donc pas d'erreur de certificat, notre site est bien en HTTPS.

- **Création des zones DNS sous Active Directory**

Maintenant, dans le contrôleur de domaine faisons un enregistrement de notre serveur de messagerie exchange, pour le faire, accédons au service DNS du PDC puis créons un nouvel enregistrement de l'hôte. Dans la fenêtre de création nous saisissons le nom que nous voulons donner à notre serveur de messagerie et l'adresse IP interne de la TMG vu que tout le trafic sera analysé par ce pare-feu.

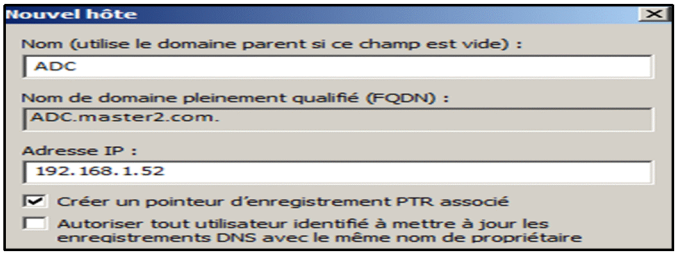


Figure IV.69 : Enregistrement de serveur de messagerie Exchange

Afin de permettre l'accès au serveur de messagerie à partir de l'extérieur, nous ajoutant un autre enregistrement avec l'adresse de l'interface externe de la TMG avec le nom ADC.master2.com.

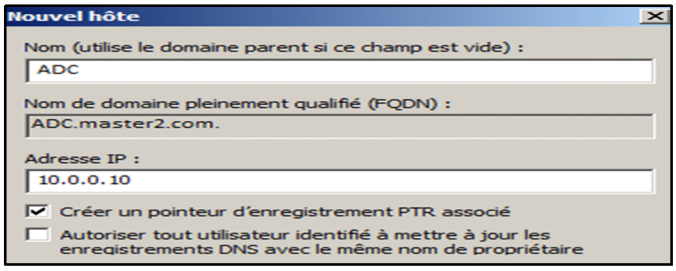


Figure IV.70 : Enregistrement de l'interface externe

IV.5.3.2.La publication du serveur Exchange via la TMG

- **Ajout de règle pour la TMG permettant un accès à OWA**

Dans le but de vérifier ce qui se passe lorsqu'un utilisateur se connecte à OWA, nous utilisons un port d'écoute qui va écouter le trafic et vérifier si le bon certificat est utilisé.

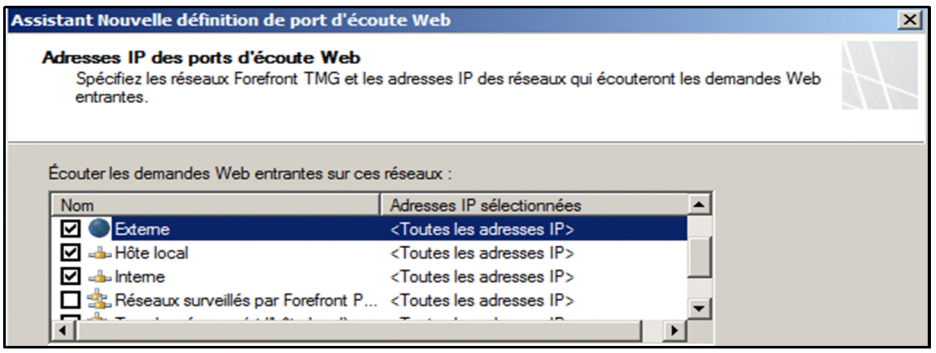


Figure IV.71 : définir les réseaux à écouter

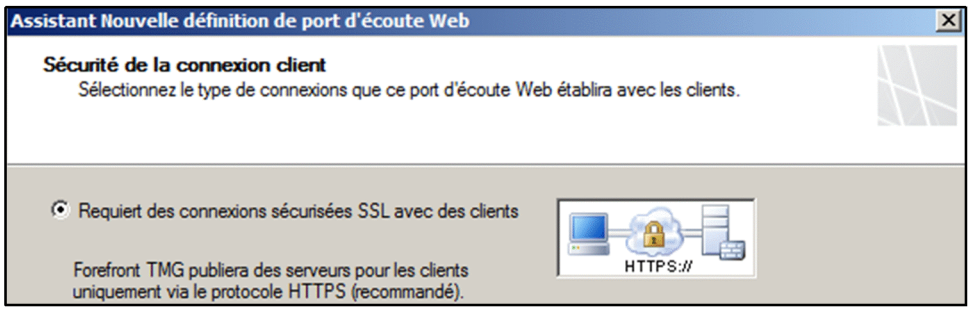


Figure IV.72 : Définir le type de connexions du port

Sélectionnons le certificat qui sera utilisé par tous les utilisateurs internes et externes.

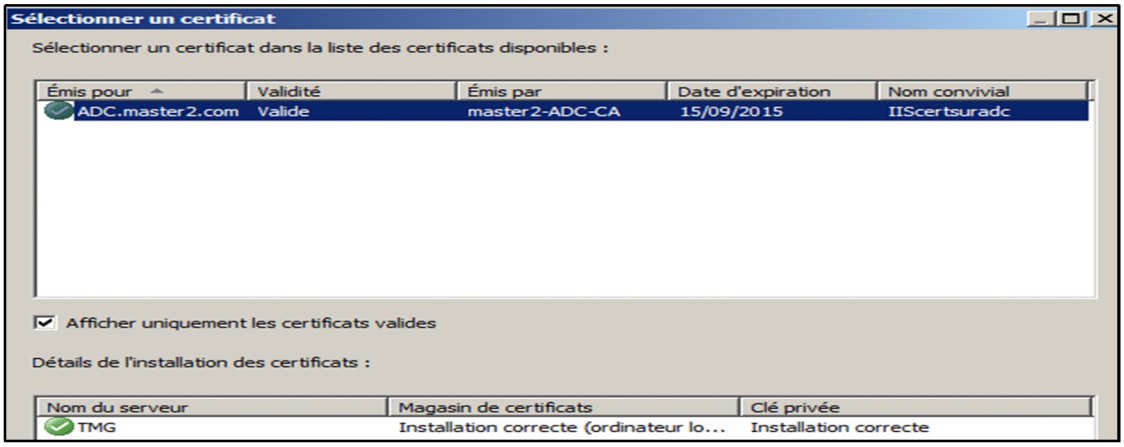


Figure IV.73 : définir quel certificat utilisé

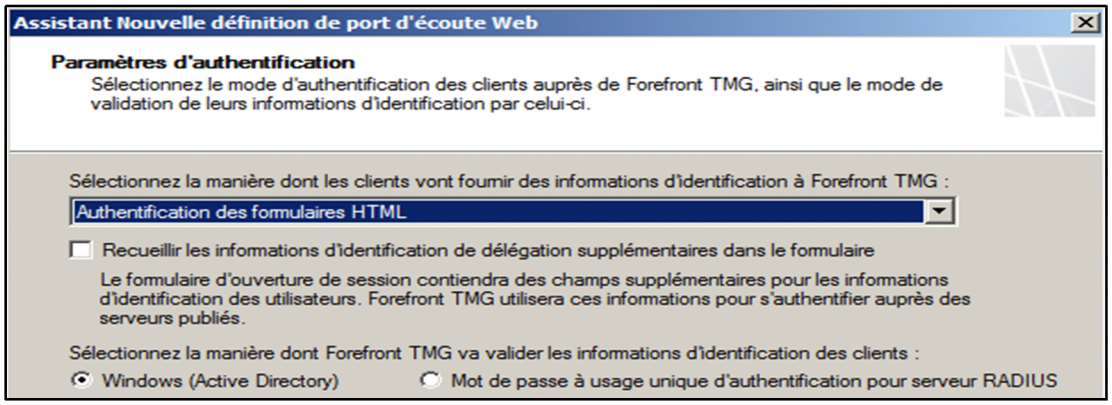


Figure IV.74 : le mode d'authentification utilisé.

Maintenant que le port d'écoute est configuré, nous pouvons créer la règle qui permettra un accès autorisé avec SSL et le certificat ADC.master2.com en utilisant le port d'écoute précédemment configuré suivant ces étapes :

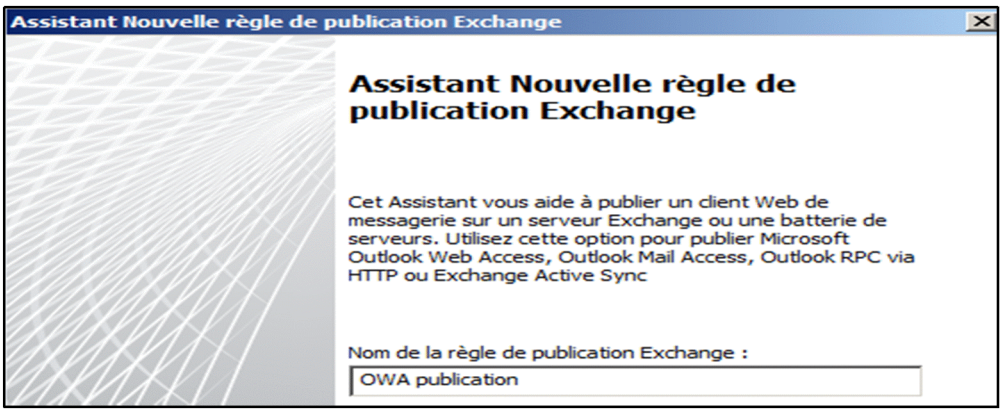


Figure IV.75 : Spécification du nom du site local

Entrons le nom du site local.

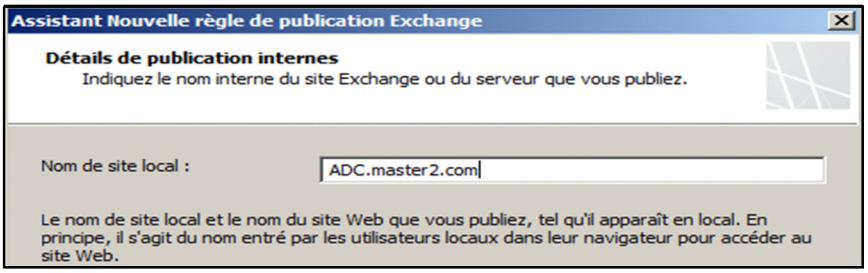


Figure IV.76 : Spécification du nom du site local

Saisissons le nom public du site OWA.

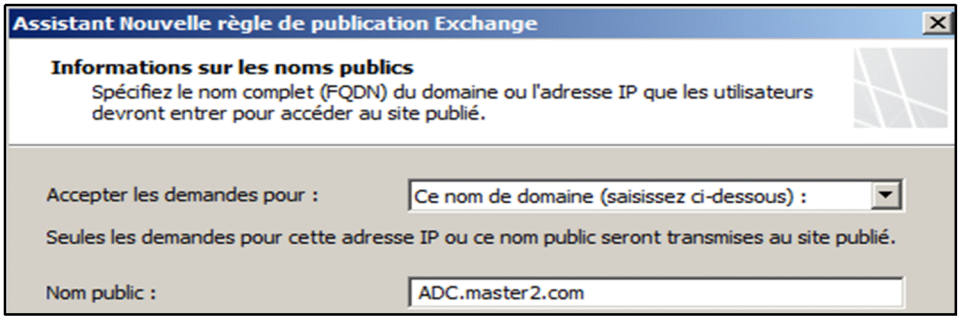


Figure IV.77 : Spécification des informations sur les noms publics

Créons une règle pour sélectionner tous les services sécurisés autorisés pour l'utilisation de la messagerie comme POP3, IMAP4 et SMTP.

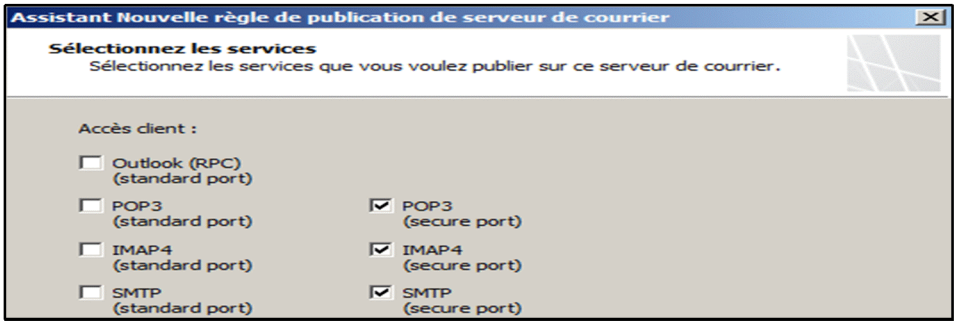


Figure IV.78 : Sélection des services

Le récapitulatif des règles TMG qui permettent aux utilisateurs de se connecter au site de messagerie OWA avec le nom DNS **ADC.master2.com** d'une façon chiffrée en utilisant le certificat ADC.master2.com et le protocole SSL.

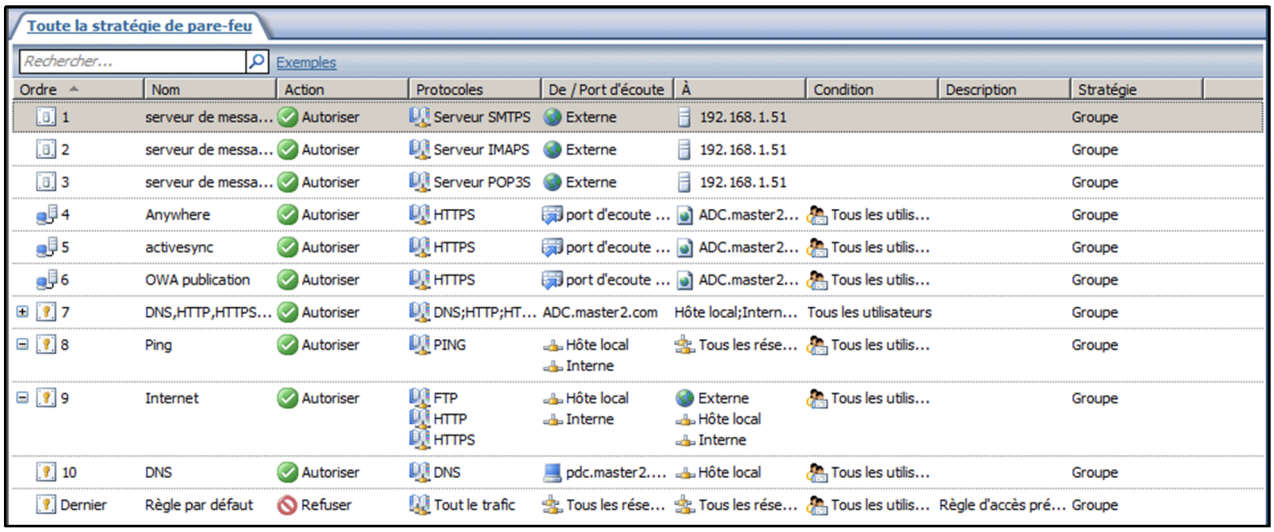


Figure IV.79 : Récapitulatif des règles TMG

IV.5.3.3.Configuration d'Exchange pour l'accès au site web de l'extérieur

- **Configuration des connecteurs**

Les connecteurs sont des éléments clé de l'Exchange, ils permettent l'envoie et la réception des mails.

- **Connecteur d'envoi**

Pour créer un connecteur d'envoi vers internet, nous cliquons sur Configuration de l'organisation->Transport Hub-> nouveau connecteur d'envoi.

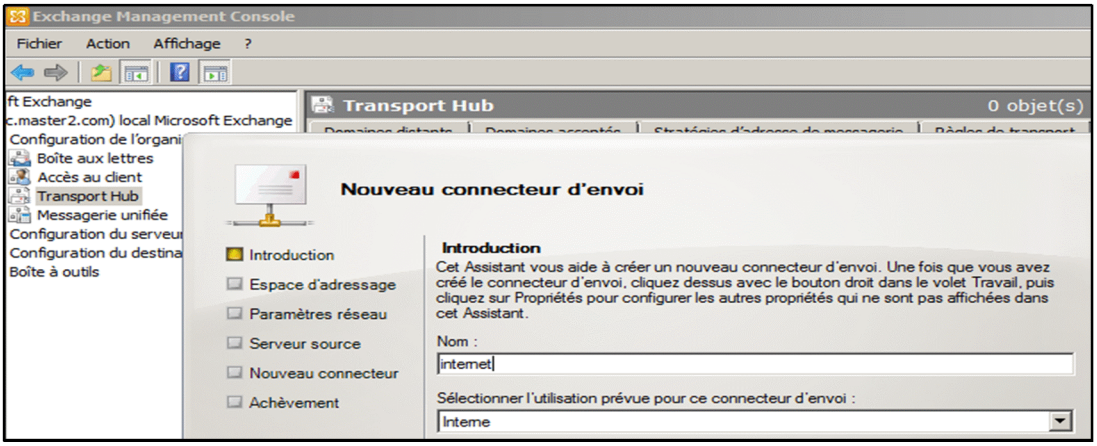


Figure IV.80 : Création d'un nouveau connecteur d'envoie

L'étape suivante permet de spécifier l'espace d'adressage, nous pouvons également indiquer un domaine en particulier ou bien insérer le champ « * » pour autoriser l'envoi vers tous le domaine et indiquer un coût pour spécifier des priorités des connecteurs dans le cas où il y'aurait plusieurs.

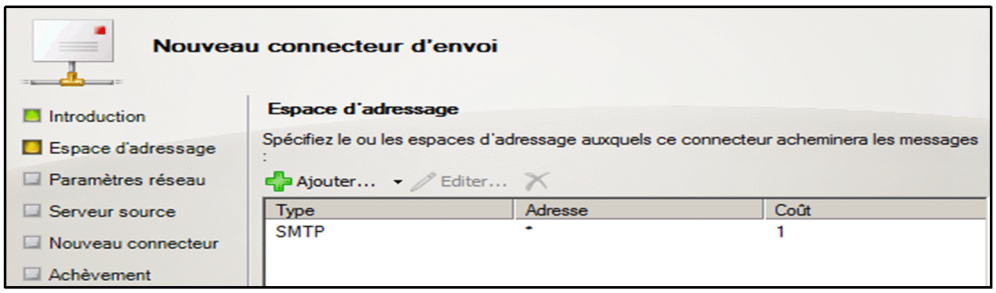


Figure IV.81 : Espace d'adressage

Ensuite, nous configurons les paramètres d'authentification de l'hôte actif en spécifiant le nom et le mot de passe de l'utilisateur et l'authentification du serveur exchange.

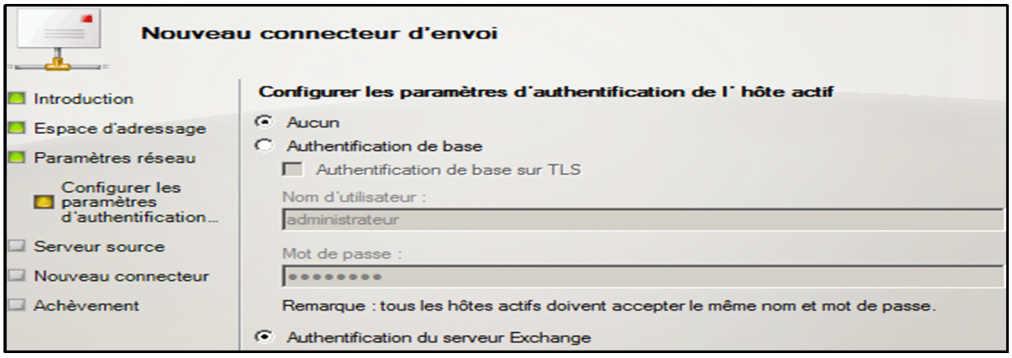


Figure IV.82 : Configuration des paramètres d'authentification

Nous finissons par la spécification du serveur source qui est le HUB de transport, **ADC.master2.com**, qui permet l'envoi des mails.

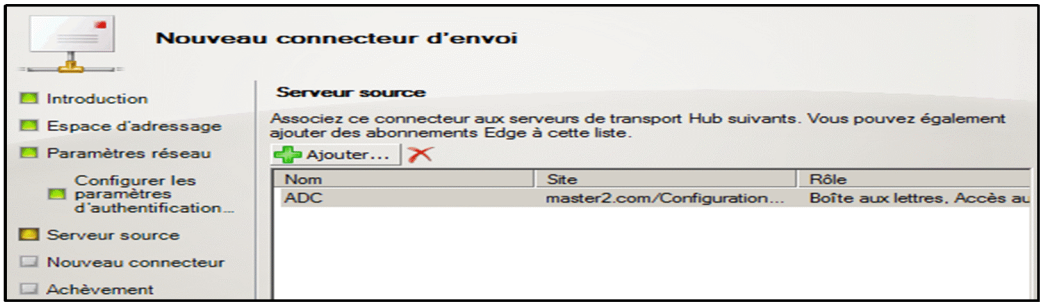


Figure IV.83 : La spécification du serveur source

- **Connecteur de réception**

Les connecteurs de réception sont gérés par le serveur, à l'inverse des connecteurs d'envoi. Il existe deux connecteurs de réception par défaut.

Le premier connecteur par défaut « Client ADC» permet les communications SMTPS uniquement pour les utilisateurs Exchange. Le second, « Default ADC» permet les communications SMTP pour les utilisateurs et les serveurs Exchange. Pour permettre aux serveurs SMTP externes d'envoyer des emails à notre serveur Exchange, il va falloir modifier les autorisations du connecteur. Pour cela, on ouvre les propriétés du connecteur « Default ADC» on va dans Groupes d'autorisation.

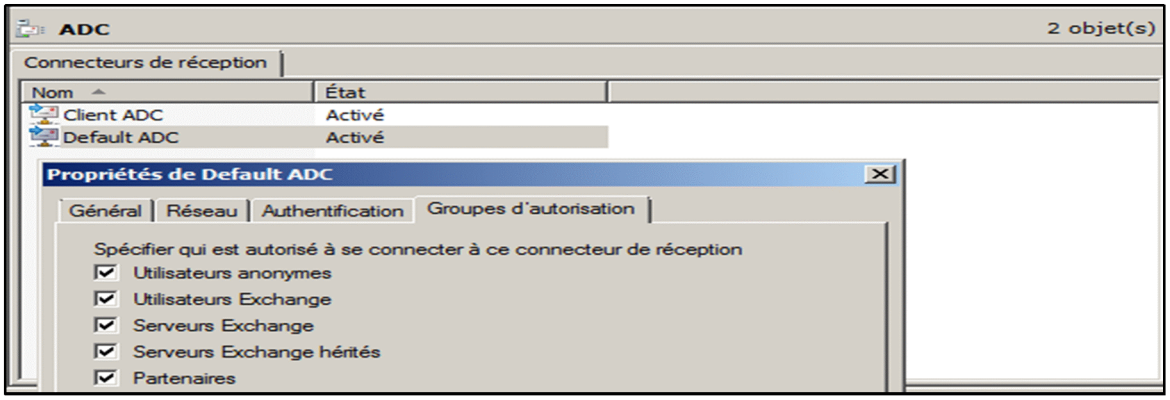


Figure IV.84 : Configuration des connecteurs de réception

- **Configuration d'Outlook Anywhere**

Pour permettre à OWA d'être vu de l'extérieur, nous activons l'Outlook Anywhere. Dans configuration du serveur->accès au client->activer Outlook Anywhere.

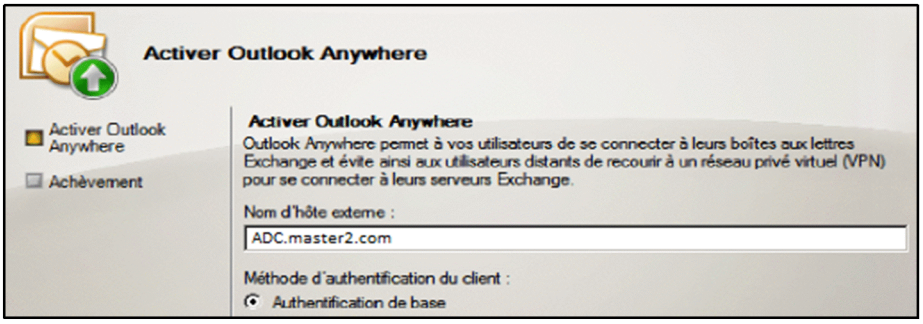


Figure IV.85 : Activation d'OWA

- **Tester l'envoie et la réception de mail**

Après avoir fourni la clé privée à l'administrateur et installé la CA, nous testons si l'échange se fait correctement avec le chiffrement des PKI. En suivant les étapes suivantes :

✓ Ouvrir le navigateur Web, puis accédez au serveur OWA à l'aide de l'adresse suivante : https://adc.master2.com/owa , cela ouvrira une session sur le Webmail en interne. On entre le nom d'utilisateur et le mot de passe.

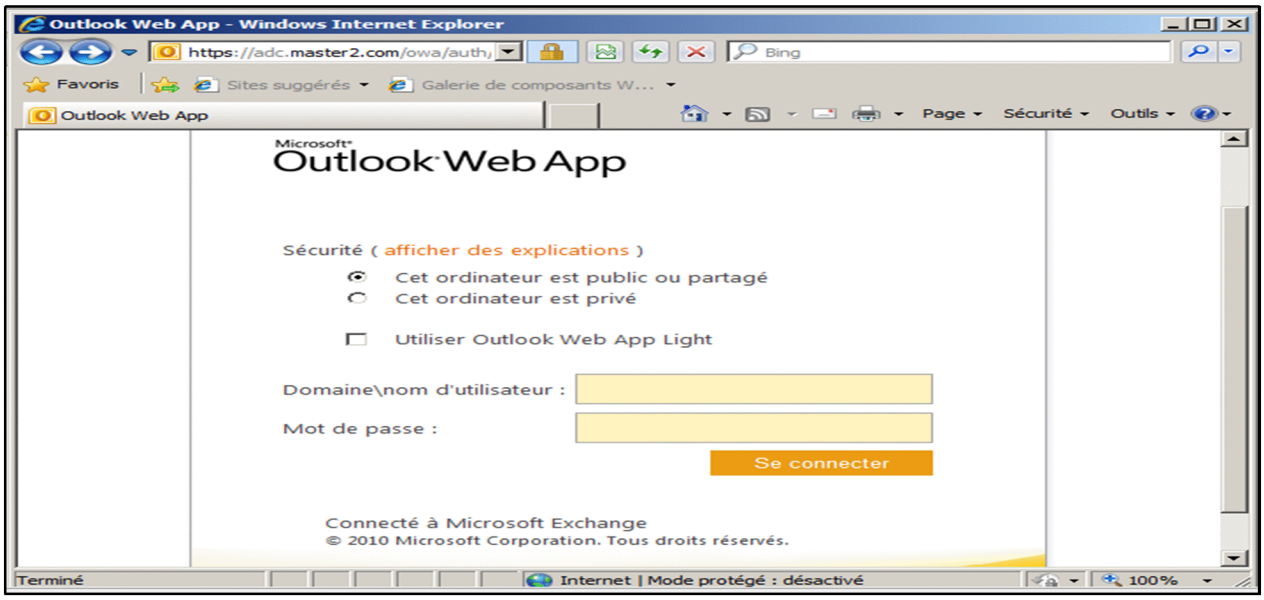


Figure IV.86 : Connexion à Outlook Web App

Comme nous le voyons dans la figure suivante l'accès a la boite mail de l'administrateur se fait d'une manier sécurisée.

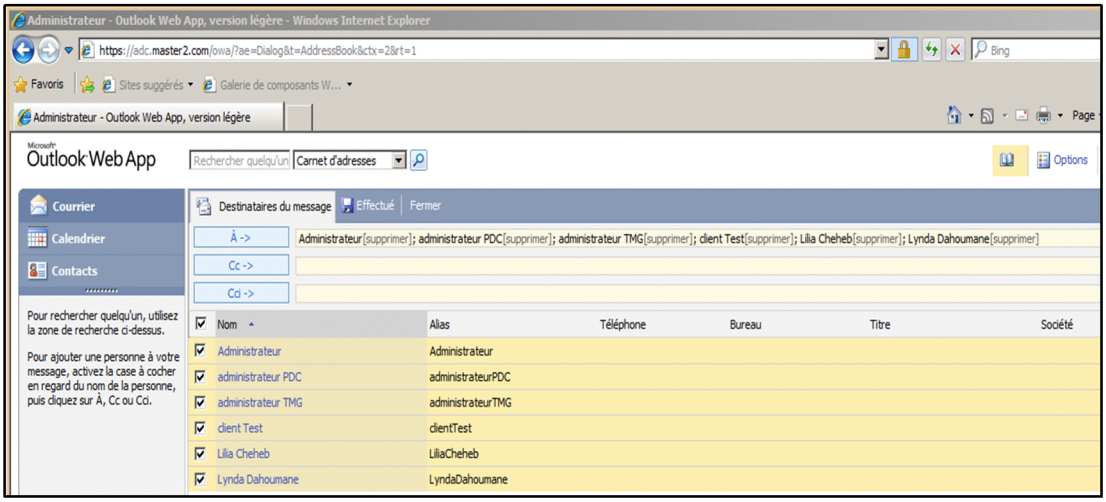


Figure IV.87 : La sélection des contacts du domaine master2.com

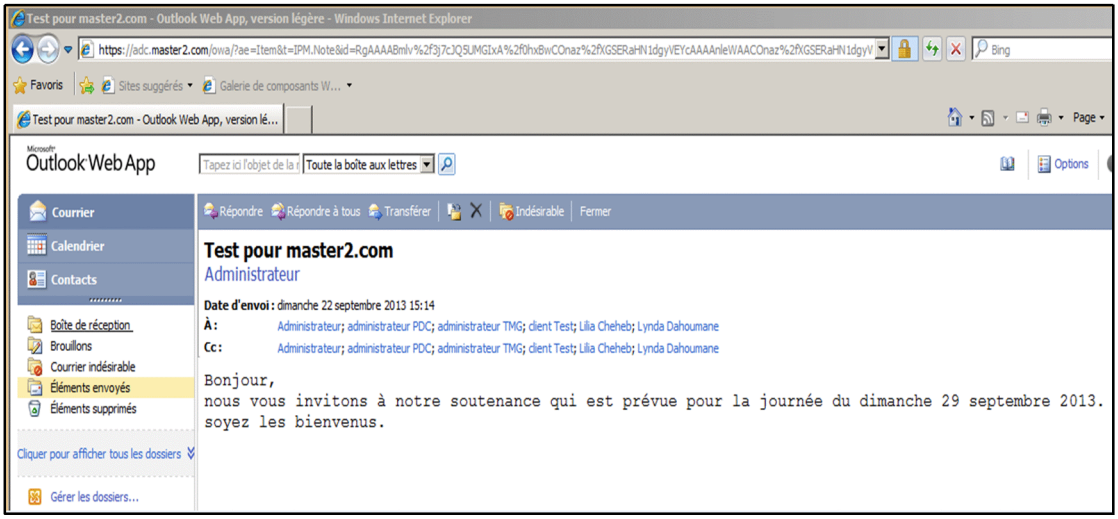


Figure IV.88 : Message envoyé

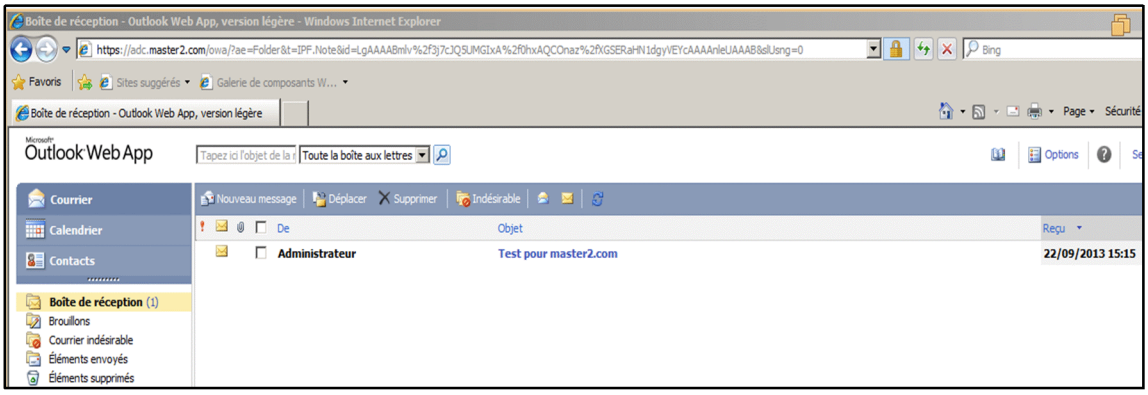


Figure IV. 89: Message reçu

IV.6.Problèmes rencontrés

Serveurs/Problèmes	Sources du problème	Solutions apportées
Exchange/Impossibilité d'accéder à Outlook Web Application (OWA).	La mise à jour du Rollup 4 d'Exchange ne s'est pas correctement installée.	Configuration de Microsoft Exchange 2010 Server, et enfin installation des mises à jour.
Exchange /PDC / Impossibilité d'envoyer et recevoir des mails. (configuration sans TMG)	Les requêtes DNS échouent (code : 451 4.4.0 DNS Query Failed).	Faire pointer l'enregistrement MX sur master2.com
Exchange / **TMG/** Impossibilité d'envoyer et recevoir des mails.	Les requêtes DNS échouent (code : 451 4.4.0 DNS Query Failed).	Création d'une règle de publication des serveurs de messagerie
PDC/Impossibilité de faire des résolutions de noms (via la commande nslookup)	DNS request time out.	Radicale : formatage et configuration du serveur avec Active Directory et DNS

Tableau IV.1 : problèmes rencontrés

IV.7.Conclusion

L'installation d'Exchange et de la TMG nous a permis d'apprendre et de comprendre les différents modules d'une infrastructure réseau sécurisée, nous avons créé un domaine et nous l'avons structuré selon nos besoins. Nous somme passé ensuite à l'installation des applications, à la création d'utilisateurs, de base de donnée, de boîtes aux lettres pour les comptes Exchange, et des connecteurs d'envoie et de réception pour l'envoie de mail à partir de clients internes ou externes.

Notre objectif principal était d'authentifier notre serveur Exchange et les clients approuvé par notre domaine en sécurisant les échanges de données via SSL, puis de sécuriser notre réseau interne y compris notre système de messagerie via le pare-feu TMG, qui est une sorte de porte d'entrée qui bloque tout les flux par défaut et dont nous devons spécifier les autorisations à travers des règles d'accès. Nous avons montré les différentes étapes nécessaires à la publication d'Exchange et comment le sécuriser via la TMG à travers les différentes règles de publication.

La publication d'applications sécurisée est une solution et une source de production importante pour les organisations car elle permet un accès simple et rapide au différentes ressources du réseau.

Conclusion générale

Conclusion

Ce mémoire est pour nous l'occasion d'aborder un des domaines de recherche d'actualité qui est le domaine de la sécurité informatique et d'étendre nos connaissances au monde professionnel qui nous était jusqu'à lors inconnu.

Nous avons constaté à travers notre travail que la mise en œuvre d'un système de messagerie électronique, devient de plus en plus la solution de communication et d'échange de données au sein des organisations, car elle offre des accès mobiles ou distants dans un environnement simple et rapide. Dans ce contexte, il est essentiel que seuls les utilisateurs authentifiés puissent accéder à ce système de messagerie pour garantir une réelle sécurité.

Afin de répondre à cet objectif, nous avons porté notre choix sur la mise en place d'un service de messagerie Microsoft Exchange 2010, nous l'avons implémenté sur un réseau LAN que nous avons créé. Nous avons effectué des configurations de base comme la création des utilisateurs, d'une base de donnée, des boîte aux lettres pour les compte Exchange, et des connecteurs d'envoie et de réception pour l'envoie de mail à partir des clients internes ou externes.

Pour la publication sécurisée, nous avons créé des certificats pour l'authentification du serveur et des clients en exigeant une connexion chiffrée via SSL pour passer en HTTPS. Nous l'avons ensuite associé au pare-feu Forefront TMG 2010 qui nous a permit de sécuriser l'ensemble du réseau interne et plus particulièrement notre système de messagerie via des règles de publication que nous avons configuré pour un accès sécurisé.

L'élaboration de ce mémoire nous a initié au monde de la gestion et de l'administration réseaux, ce qui nous a permis de comprendre l'importance de notre domaine d'étude. Il nous a permis d'abord de revoir certaines notions comme par exemple le DNS, les protocoles TCP/IP et les protocoles de messagerie tels qu'IMAP, POP et SMTP.

Nous avons rencontré différents problèmes principalement liés à la préparation des machines, à la configuration du domaine et à l'installation des applications, que nous avons résumé dans un tableau accompagné des solutions trouvées. L'autre difficulté été liée au manque de ressources matérielles exigées par les logiciels à savoir le logiciel de simulation VMware et les applications utilisées.

En choisissant ce thème nous avons pu explorer une infime partie de la sécurité. Nous aurions aimé approfondir le sujet, configurer bien plus d'avantage de paramètres, de

développer certains algorithme de chiffrement à travers leurs mécanismes de calcule et surtout de déployer d'autre solutions.

En conclusion, nous souhaitons que ce thème malgré les contraintes temporelles et matérielles soit enrichi et approfondi à l'avenir.

ANNEXES

Annexe I

I.1.Introduction

Il est important que tous les termes significatifs soient clairement définis, c'est pour cette raison que nous avons consacré une partie importante aux annexes. Dans cette annexe nous avons pris le temps de bien définir les différents protocoles de communication utilisés par les systèmes d'informations. La transmission d'information entre deux programmes informatiques sur deux machines différentes passe par deux modèles de base le modèle OSI et le modèle TCP/IP.

I.2.Les protocoles réseaux

I.2.1.Le modèle OSI

OSI signifie (Open Système Interconnexion, ce qui se traduit par interconnexion de systèmes ouverts). Ce modèle a été mis en place par l'ISO (International Standardization Organisation) afin de mettre en place un standard de communications entre les ordinateurs d'un réseau, c'est-à-dire les règles qui gèrent les communications entre des ordinateurs. En effet, aux origines des réseaux chaque constructeur avait un système propre (on parle de système propriétaire), ainsi de nombreux réseaux incompatibles coexistaient. C'est la raison pour laquelle l'établissement d'une norme a été nécessaire.

Le rôle du modèle OSI consiste à standardiser la communication entre les machines afin que différents constructeurs puissent mettre au point des produits (logiciels ou matériels) compatibles (pour peu qu'ils respectent scrupuleusement le modèle OSI).

- **L'intérêt d'un système en couches**

Le but d'un système en couches est de séparer le problème en différentes parties (les couches) selon leur niveau d'abstraction.

Chaque couche du modèle communique avec une couche adjacente (celle du dessus ou celle du dessous). Chaque couche utilise ainsi les services des couches inférieures et en fournit à celle de niveau supérieur

- **Les couches du modèle OSI**

Le modèle OSI est un modèle qui comporte 7 couches qui sont les suivantes :

- ✓ **La couche physique :** définit la façon dont les données sont converties en signaux numériques.
- ✓ **La couche liaison de données :** définit l'interface avec la carte réseau.

- ✓ **La couche réseau :** permet de gérer les adresses et le routage des données.
- ✓ **La couche transport :** elle est chargée du transport des données et de la gestion des erreurs.
- ✓ **La couche session :** définit l'ouverture des sessions sur les machines du réseau.
- ✓ **La couche présentation :** définit le format des données (leur représentation, éventuellement leur compression et leur cryptage).
- ✓ **La couche application :** assure l'interface avec les applications

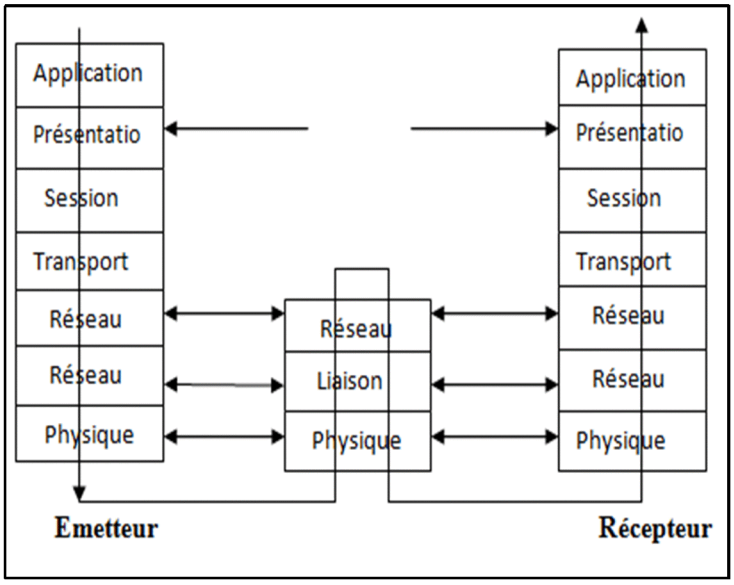


Figure I : Les couches du modèle OSI

I.2.2.Le Modèle TCP/IP

TCP/IP est une suite de protocoles. Le signale TCP/IP signifie « transmission control Protocol/ Internet Protocol ». Il provient des noms des deux protocoles majeurs de la suit de protocoles, c'est-à-dire le Protocole TCP et le protocole IP.

TCP/IP représente d'une certaine façon l'ensemble des règles de communication sur Internet et se base sur la notion adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données. Etant donné que la suite du protocole TCP/IP a été créée a l'origine dans un but militaire, elle est conçue pour répondre à un certain nombre de critères parmi lesquels :

- ✓ Le fonctionnement des messages en paquets.
- ✓ L'utilisation d'un système d'adresses.
- ✓ L'acheminement des données sur le réseau (routage).
- ✓ Le contrôle des erreurs de transmission de données.

Annexe I

La connaissance de l'ensemble des protocoles TCP/IP n'est pas essentielle pour un simple utilisateur, au même titre qu'un téléspectateur n'a pas besoin de connaitre le fonctionnement de son téléviseur, ni des réseaux audiovisuels. Toutefois, sa connaissance est nécessaire pour les personnes désirant administrer ou maintenir un réseau TCP/IP.

• **Les couches du modèle TCP/IP**

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à quatre couches :

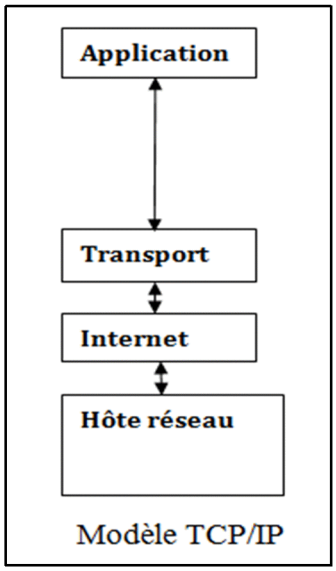


Figure II : Les couches du modèle TCP /IP

✓ **Couche application :** elle englobe l'application standard du réseau (Telnet, SMTP, FTP…).

✓ **La couche transport (TCP) :** Elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaitre l'état de transmission.

✓ **La couche internet (IP) :** elle est chargée d'assurer le transport des paquets de données (datagramme).

✓ **La couche hôte réseau :** elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type du réseau.

- **Remarque :** Les données sont transmises vers le bas du modèle lorsqu'il s'agit d'une émission sur le réseau, et vers le haut lors d'une application.

• **Transposition des deux modèles**

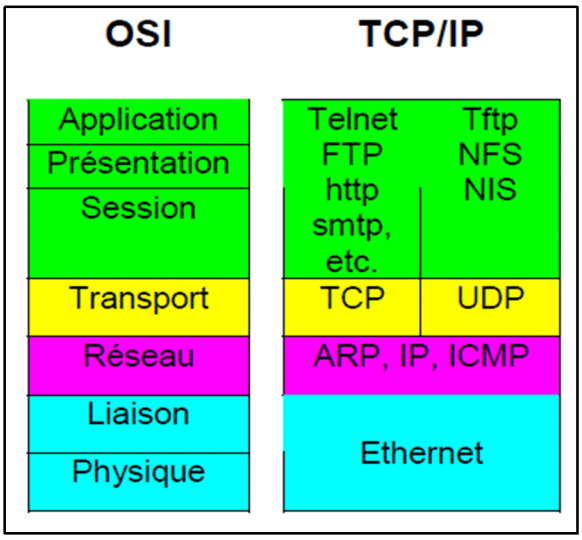


Figure III: transposition TCP/IP et OSI

Le modèle OSI a été mis à coté du modèle TCP pour faciliter la comparaison entre les deux modèles.

• **Le protocole UDP**

Le protocole UDP (User Datagramme Protocol) est comme le protocole TCP, c'est un protocole de transport de données. Cependant, contrairement au TCP, on qualifie l'UDP de transmission « en mode non connecté et non fiable » ou encore de protocole « non orienté connexion ».

• **Le protocole ARP**

Le protocole ARP (Address Resolution Protocol) a un rôle important parmi les protocoles de la couche internet de la suite TCP/IP ; car il permet de connaitre l'adresse physique d'une carte réseau correspondant à une adresse IP, d'où son nom protocole de résolution d'adresse.

• **Le protocole IP**

Le protocole IP (Internet Protocol) fait partie de la couche internet, c'est l'un des protocoles les plus importants d'internet car il permet l'élaboration et le transport des datagrammes IP, sans toutefois en assurer la livraison. Le protocole IP traite les datagrammes IP indépendamment les un des autres en définissant leur représentation, leur routage et leur expédition.

Le protocole IP détermine le destinataire du message grâce à trois champs :

- ✓ Adresse IP
- ✓ Le masque de sous-réseau
- ✓ Passerelle par défaut

• Le protocole ICMP

Le protocole ICMP (Internet Control Message Protocol) est un protocole qui permet de gérer les informations relatives aux erreurs des machines connectées. Etant donné le peu de contrôles que le protocole IP réalise, il permet non pas de corriger ces erreurs mais de faire état de celles-ci aux protocoles des couches voisines. Ainsi, le protocole ICMP est utilisé par tous les routeurs pour rapporter une erreur (appelé *Delivery Problem*).

I.3.Autres protocoles de la suite TCP/IP

I.3.1.Le protocole NNTP

Le fonctionnement général de NNTP (Network News Transfert Protocol) est très similaire à celle du protocole SMTP. NNTP utilise TCP sous le port 119 pour les connexions entrantes, soit à partir d'hôtes client ou d'autres serveurs NNTP. Comme dans SMTP, lorsque deux serveurs de nouvelles (appelée serveur de news) communiquent, celui qui initie la connexion joue le rôle de client.

NNTP est le protocole d'échange des nouvelles ou forums de discussions à travers Usenet. Il assure l'échange des nouvelles entre les serveurs et également la communication entre serveur et postes clients aussi bien pour la lecture que pour l'écriture de messages. Lorsqu'un utilisateur poste un article dans un groupe de news, il est dans un premier temps déposé sur le serveur de news auquel le poste client est relié. Puis, ce serveur va réexpédier cet article aux différents serveurs auxquels il est relié, qui eux-mêmes procéderont de la sorte, ce qui explique la rapidité de la diffusion des messages.

• Récapitulatif des principales commandes NNTP

Commande	**Description**
ARTICLE <n°>	Le numéro attribué selon un simple compteur propre à chaque groupe de discussions
LIST	Cette commande permet d'obtenir la liste des groupes disponibles sur le

	serveur avec des indications sur le nombre de messages et l'intervalle des numéros de messages
GROUP <id>	permet de sélectionner le groupe de discussion désiré. la commande retourne « 211 » (en cas de réussite) suivi du nombre d'articles dans le groupe et les indices du premier et du dernier article.
LAST	permet d'obtenir le dernier article stocké par le serveur
SLAVE	indique au serveur qu'il ne communique pas avec un utilisateur final mais avec un serveur
NEWGROUPS date heure	permet d'obtenir les nouveaux groupes apparus depuis la date indiquée,
XGTITLE	fournit l'intitulé d'un groupe de newsgroups

Tableau 1 : Récapitulatif des principales commandes NNTP.

I.3.3.Le protocole X.400

Est un protocole de courrier électronique normalisé par l'UIT (Union International des Télécommunications). Il n'a jamais connu de déploiement réellement significatif. Toutefois il est toujours utilisé aujourd'hui en tant que réseau à valeur ajoutée (réseau de télécommunication qui offre des services bien défini) dans les échanges EDI (Echange de Données Informatisé). Sa principal particularité et d'utilisé un MTA privé. Il a fait l'objet de nombreuses polémiques, à propos de sa comparaison avec SMTP, ce dernier l'ayant nettement emporté.

I.3.4.Le protocol LDAP (Lightweight Access Directory Protocol)

Est un protocole reposant sur TCP/IP qui permet d'interroger et modifier des services d'annuaire. Un service d'annuaire est une sorte de base de données électronique permettant de définir des utilisateurs, des groupes, des applications, des ressources, etc. Mais contrairement à une base de données, l'organisation des données n'est pas relationnelle mais hiérarchique, c'est à dire telle une arborescence. Ainsi, grâce à son annuaire, LDAP sera capable de gérer de manière souple un grand nombre de données le rendant bien adapté pour le monde d'Entreprise. Mais surtout, ce qui fait sa force, est qu'il offre un support d'authentification qui centralise tous les utilisateurs pour un grand nombre de services

I.3.5.Le protocole WAP (Wireless Application Protocol)

Est un protocole de communication qui permet d'accéder à Internet à partir d'un appareil de transmission sans fil, comme un téléphone portable. Afin d'atteindre cet objectif, une passerelle (en anglais *gateway*) est connectée au réseau mobile, routant les connexions WAP vers Internet (la passerelle effectue également une compression des données envoyée vers le téléphone portable, afin de faciliter la transmission). Grâce à cette passerelle, le client, c'est-à-dire dans ce cas le téléphone portable, se connecte à un serveur WAP, capable de lui envoyer des données au format WML, qui est le format spécifique du WAP, dérivé de HTML. La version 2.0 du WAP (destinée par exemple à l'UMTS « Univesal Mobile Télécommunications Système ») marque l'abandon de WML au profit de XHTML (Extensible Hyper Text Markup Language).

I.3.6.Le protocole RPC (Remote Procedure Call)

Est un protocole réseau permettant de faire des appels de procédures sur un ordinateur distant à l'aide d'un serveur d'applications. Ce protocole est utilisé dans le modèle client-serveur pour assurer la communication entre le client, le serveur et des éventuels intermédiaires.

Annexe II

I. Introduction

Dans cette annexe, nous présentons la Terminologies de la sécurité informatique suivie des principaux points à inclure dans une politique de gestion du courrier électronique, c'est-à-dire les objectifs et consigne de la politique des mots de passe, firewall, DMZ, et antivirus. Puis un exemple de charte et des règles de bon usage de la messagerie électronique.

II. Terminologies de la sécurité informatique

Parmi les mots-clés de la sécurité qui sont largement repris dans la littérature informatique nous trouvons :

- ✓ **Vulnérabilité :** c'est une faille de sécurité le plus souvent caché touchant une infrastructure informatique. Ce terme est fréquemment associé aux logiciels mais il regroupe plus généralement toute faiblesse qu'elle qu'en soit la nature. Par exemple un mot de passe vide ou trivial constitue une vulnérabilité.
- ✓ **Risque :** c'est la probabilité qu'un problème survienne lorsqu'une vulnérabilité est exposée à une population malveillante qui tentera de l'exploiter
- ✓ **Attaque :** c'est le moyen d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables.
- ✓ **Contre-mesure :** c'est la procédure ou technique permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique**.**
- ✓ **Menace :** c'est une violation potentielle capable d'exploiter une vulnerabilité d'une manière active ou passive, accidentelle ou intentionnelle.

III. La politique de gestion du courrier électronique

III.1. Politique des mots de passe

Les mots de passe sont un aspect important de la sécurité informatique. Ils sont la première protection pour les comptes d'utilisateur. Un mot de passe mal choisi peut aboutir au compromis du réseau entier de l''entreprise

- **Objectif**

L'objectif de cette politique est d'établir un standard pour la création de mots de passes compliqués, pour la protection des mots de passe et pour la fréquence de changement

- **Consignes**

  ✓ Tous les mots de passe de niveau de système (par exemple : racine, NT admin, etc) doivent être changés sur au moins une base trimestrielle.

  ✓ Tous les mots de passe de niveau utilisateur (par exemple : email, web, bureau,etc.) doivent être changés au moins tous les six mois. L'intervalle recommandé est tous les quatre mois.

  ✓ Les mots de passe ne doivent pas être transmis par email ou par toute autre forme de communication électronique.

  ✓ Ne pas utiliser les mêmes mots de passe pour les comptes de la société et les comptes personnels.

  ✓ Ne pas partager les mots de passe avec personne, y compris avec des aides administratifs ou des secrétaires. Tous les mots de passe doivent être traités comme sensibles et Confidentiels.

III.2. Politique de modification des règles de filtrage du Firewall

Cette politique décrit les procédures à effectuer lors de l'ajout, du retrait ou de modification de règles de filtrage sur le Firewall. Elle s'adresse aux administrateurs du réseau informatique.

- **Objectif**

Pour éviter de dégrader les relations entre employés à l'intérieur de l'entreprise. Toute modification des règles de filtrage au niveau du Firewall devra respecter la politique suivante.

- **Consignes**

  ✓ Toute modification ne pourra être réalisée qu'en accord avec son équipe et son supérieur, la seule exception restant l'ajout d'une règle temporaire. Une fois la règle clairement définie, l'ensemble des utilisateurs du système devront être mis au courant de l'intervention sur le Firewall au moins une journée à l'avance.

  ✓ En cas d'impératif précis et temporaire (virus exploitant une nouvelle faille pouvant être bloquée par l'ajout d'une règle), et si cela n'entraîne pas de gêne majeur pour le système, les administrateurs sont autorisés à mettre en place des règles de filtrage rapidement. Ils devront tout fois en référer dans la journée à leur supérieur.

  ✓ Toute modification devra être référencée dans l'espace réservé à cet effet par les administrateurs.

- ✓ Avant la mise en place d'une règle de filtrage 'critique', risquant d'engendrer de lourdes conséquences sur l'utilisation du système, une maquette de test devra être mise en place, et l'utilisation courante du système devra être testée.

III.3. Politique de la DMZ

- **Consignes**

✓ Les relais de messagerie ouverts sur l'extérieur doivent être placés dans la DMZ. On les appellera par la suite "relais principaux".

✓ Les serveurs de boites aux lettres qui contiennent les comptes des utilisateurs seront dans la zone protégée.

✓ Les relais principaux sont les seules machines habilitées au dialogue SMTP avec le monde extérieur : le relais du courrier entrant vers les serveurs de boîtes aux lettres et du courrier sortant vers l'extérieur s'effectue par les relais principaux.

✓ Les serveurs de boîtes aux lettres qui contiennent les comptes des utilisateurs seront dans la zone protégée.

III.4. Politique de l'antivirus

- **Consignes**

✓ Des logiciels antivirus et antispams sont installés au niveau des relais de messagerie ou au niveau des boites aux lettres. Il est possible de mettre en place une protection au niveau des postes clients.

✓ Toute pièce jointe à un courrier électronique doit être contrôlée par un logiciel antivirus au moins une fois avant d'être ouverte (virus, troyens, malwares divers).

✓ Tout courrier électronique doit être modifié s'il contient un virus. Le virus est supprimé du courrier et le destinataire en est prévenu

IV. La charte

L'intérêt principal d'une charte d'entreprise est d'obliger les employés à lire et signer un document précisant leurs droits et devoirs et par la même de leur faire prendre conscience de leur responsabilité individuelle. La mise en œuvre d'une charte peut être envisagé de différente façon selon le type le besoin et le bute des organisations. Voila ainsi un exemple de contenue d'une charte pour un bon usage de la messagerie électronique dans un cadre professionnel :

IV.1. Gérer au mieux l'envoi des messages

IV.1.1 envoie d'un message

- ✓ S'interroger sur la pertinence du media utilisé
- ✓ Ne pas utilisé la messagerie a des fin extra professionnels ou pour des motif prohibés par la loi.

IV.1.2 Contenu du message

- ✓ Indiquer de manier explicite l'objet du message
- ✓ S'obliger a une rigueur formelle dans la rédaction du message
- ✓ Ne pas abuser des pièces jointes

IV.1.3 Identification du (des) destinataire (s)

- ✓ S'interroger sur le (s) destinataire (s) principal (aux) du message
- ✓ Utiliser avec modération les fonctions « copie conforme » et « copie cachée »

IV.1.4 Moment d'envoi du message

- ✓ S'interroger sur le moment le plus opportun pour l'envoi d'un message
- ✓ Préparer les messages en mode brouillions ou hors connexion et de les envoyer pendant les heures habituelles du travail

IV.2. Gérer au mieux la réception des messages

IV.2.1 La réception d'un message

- ✓ Assurer l'expéditeur de la réception du message
- ✓ Gérer au mieux la réception du message en cas d'absence prolongée
- ✓ Limiter le nombre d'interruption

IV.2.2 Réponse aux messages

- ✓ Ne pas traiter immédiatement un message
- ✓ Appréhende le niveau de complexité de la réponse
- ✓ S'interroger pour répliquer la liste de diffusion utilisée par l'expéditeur

IV.2.3 Archivage des messages

- ✓ Définir une stratégie de conservation des messages

V. Les Règles de bon usage de la messagerie électronique

V.1.Les bonnes pratiques de l'utilisateur

Ce paragraphe ne reprend pas les obligations de l'utilisateur consignées dans une charte de bonne utilisation, mais propose quelques conseils pour une bonne utilisation de sa messagerie.

- **Dans la protection de son matériel, en absence d'une fonction d'administrateur**
  - ✓ S'assurer que son « antivirus » est bien à jour.
  - ✓ Utiliser les fonctionnalités de « pare-feu » et d' « anti-spam » lorsqu'elles sont disponibles.
- **Dans l'utilisation générale de la messagerie**
  - ✓ Eviter de déléguer l'utilisation de sa messagerie.
  - ✓ Protéger sa boite aux lettres par un mot de passe.
  - ✓ Limiter l'utilisation privée de son adresse professionnelle.
  - ✓ Ne pas laisser son adresse e-mail professionnelle sur n'importe quel site Web, sur des forums…
  - ✓ Ne pas répondre aux spam.
  - ✓ Désactiver les options d'envoi systématique d'informations sur les sites web.
- **Dans la gestion de sa messagerie**
  - ✓ Eviter l'envoi de messages de taille importante.
  - ✓ Classer à l'arrivée ses messages dans des dossiers prédéfinis.
  - ✓ Veiller à ce que les messages importants soient régulièrement sauvegardés.
  - ✓ Faire un archivage périodique de ses messages.
  - ✓ Supprimer les messages inutiles.
  - ✓ Activer les fonctionnalités de sécurité offertes par le client de messagerie (exemple : chiffrement des données locales et de la liaison avec le serveur.
- **Dans la réception des messages**
  - ✓ Ne pas ouvrir des messages ou des pièces attachées venant des personnes ou des sociétés non identifiées.
  - ✓ Se méfier des messages dont l'objet est en langue étrangère.
  - ✓ Ne pas porter crédit à des messages de type « Hoax ».

- **Dans l'envoi des messages**
  - ✓ Ne pas envoyer de messages qui demandent de relayer un message vers un grand nombre de personnes.
  - ✓ Pour l'envoi de messages à plusieurs personnes et pour éviter la divulgation des adresses, utiliser «copie caché».
- **Dans la gestion de son carnet d'adresse**
  - ✓ Crypter son carnet d'adresse si le client de messagerie le permet.
  - ✓ Rajouter une fausse adresse en tête de son carnet d'adresse pour être averti en cas d'envoi en masse à partir de son carnet d'adresse.

V.2. Les bonnes pratiques de l'administrateur

Le système de messagerie de l'entreprise doit être placé sous la responsabilité d'un « propriétaire » qui en validera les règles d'utilisation. L'administrateur à la charge le maintient opérationnel de la messagerie conformément aux règles d'utilisation décidées. Il est un acteur clé de la sécurité de la messagerie. Parmi les bonnes pratiques à appliquer, l'administrateur veillera particulièrement à :

- ✓ Limiter l'usage des listes de diffusion : l'abus de listes de diffusion génère un encombrement des boites aux lettres avec des messages mal ciblés. Un autre risque est l'envoie d'informations sensibles à des destinataires non désirés car la liste de diffusion n'est pas toujours maitrisée par l'utilisateur.
- ✓ Supprimer les certificats d'autorités non utilisés, les clients de messagerie intègrent automatiquement, lors de leurs installations des certificats d'autorités ayant une certaine notoriété au niveau mondial. Il est souhaitable de ne conserver que les certificats d'autorités qui ont été retenus dans la politique de sécurité de l'entreprise.
- ✓ Mettre en place un système de trace et de surveillance en conformité avec les exigences légales en termes de protection des données. Les logs doivent être régulièrement exploités, permettre l'identification des comportements anormaux et répondre au besoin d'archivage légal.
- ✓ Mettre en place des points de contrôle continu de l'efficacité des dispositifs techniques mis en œuvre.

Bibliographie

Webographie

www.Mémoireonligne.com

www.commentçamarche.com

www.supinfo.com

www.labo-microsoft.org

www.wikipedia.com

www.Technet.com

www.Developpez.com

http://www.commentcamarche.net/contents/authentification/radius.php3

http://technet.microsoft.com/fr-fr/library/cc753528.aspx

Glossaire

Glossaire

A

AES (Advanced Encryption Standard) : est un algorithme de chiffrement symétrique qui a été publié pour la première fois en 1998 par Vincent Rijmen et Joan Daemen, L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutés selon une table définie au préalable. Ces octets sont ensuite placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite. L'incrément pour la rotation varie selon le numéro de la ligne. Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d'une matrice auxiliaire, cette multiplication est soumise à des règles spéciales selon $GF(2^8)$ (groupe de Galois ou corps fini).

ARPANET (Advanced Research Project Agency NETwork) : premier réseau à commutation de paquets, à l'origine d'internet développé par le département de la défense américaine.

ASCII : (American Standard Code for Information Interchange) : qui signifie en français "Code américain normalisé pour l'échange d'information". La norme **ASCII** est largement utilisée en informatique pour coder les caractères.

L'ASCII est la norme de codage la plus répandue et compatible avec le plus de supports. Il contient l'ensemble des caractères alphanumérique utilisé en anglais. Initialement, il est codé sur 7 bits (plus un code de parité).

B

BAL (Boîte Aux Lettres).

BBN (Bolt Beranek and Newman) : est une société américaine créée en 1948 par deux professeurs du Massachusetts Institute of Technology (MIT) :Richard Bolt et Leo Beranek et d'un ancien étudiant de Richard Bolt : Robert Newman. La société doit son nom à ses fondateurs : ce sont leurs trois initiales.

Cette sociéte a été pionnière dans l'histoire de l'informatique, on lui doit pêle-mêle : le langage Logo, le système d'exploitation TENEX, la mise en place du réseau ARPANET et l'envoi du premier courrier électronique.

C

CR/LF (Carriage Return /de Line Feed) : (ou CR+LF), est une séquence de deux octets qui indique une fin de la ligne (et surtout une nouvelle ligne) dans un texte. Le sigle **CRLF** provient de la juxtaposition du sigle de **C**arriage **R**eturn (retour chariot) et de **L**ine **F**eed (saut de ligne).

D

DES (Data Encryption Standard) : est un algorithme de chiffrement symétrique (chiffrement par bloc) utilisant des clés de 56 bits. Son emploi n'est plus recommandé aujourd'hui, du fait de sa lenteur à l'exécution et de son espace de clés trop petit permettant une attaque systématique en un temps raisonnabl. DES a notamment été utilisé dans le système de mots de passe UNIX.

DHCP (Dynamic Host Configuration Protocol) : c'est un service qui permet d'attribuer dynamiquement des paramètres TCP/IP aux clients qui ont font la demande.

DMZ (Demilitarized Zone).

DNS (Domain Name System) : il s'agit d'un service disponible dans un environnement TCP/IP permettant de résoudre des noms du type www.google.fr en adresse IP

E

ESMTP (Extended Simple Mail Transfert Protocol).

F

Forum (newsgroup) : ce sont des messageries qui permettent à un groupe d'acteurs de structurer leurs échanges d'informations et de messages selon des dossiers thématiques ou des groupes de travail partagés. Selon les cas, les forums peuvent être publics ou privés et structurés autour de thématiques ou de projets opérationnels.

FTP (File Transfert Protocol).

H

Hachage : dans le contexte de chiffrement, cette fonction est également de fonction digest. Elle permet de générer, à partir des données qui lui sont fournies en entrée, leur résumé (sorte d'empreinte numérique (digest)), plus court que le message original et incompréhensible. Ce résumé peut être ensuite chiffré avec la clé privée de l'émetteur et associée au message à transmettre. Sur réception du message et de son empreinte, le destinataire déchiffre cette dernière avec la clé publique de l'émetteur puis, recalcule à partir du message reçu avec la même fonction hash, l'empreinte et la compare ensuite avec celle reçue. Si le résultat est identique, le destinataire a ainsi vérifié l'identité de l'émetteur et est assuré de l'intégrité du message. En effet, si le message est altéré, même légèrement, son empreinte est alors considérablement modifiée.

Hébergeur web (ou hébergeur internet) : est une entité ayant pour vocation de mettre à disposition des internautes des sites web conçus et gérés par des tiers. Il donne ainsi accès à tous les internautes au contenu déposé dans leurs comptes par les webmestres souvent via un logiciel FTP ou un gestionnaire de fichiers. Pour cela, il maintient des ordinateurs allumés et connectés 24 heures sur 24 à Internet (des serveurs web par exemple) par une connexion à très haut débit (plusieurs centaines de Mb/s), sur lesquels sont installés des logiciels : serveur HTTP (souvent Apache), serveur de messagerie, de base de données...

HTML (Hyper **T**ext **M**arkup **L**anguage**) :** langage de mise en forme de données utilises pour effectuer des présentations en mode graphique à travers un navigateur Internet.

HTTP (Hyper**T**ext **T**ransfer **P**rotocol**).**

Hypertexte : Les liens hypertextes (ancrages) sont des éléments d'une page HTML (soulignés lorsqu'il s'agit de texte) permettant aux internautes de naviguer vers une nouvelle adresse lorsque l'on clique dessus. Ce sont les liens hypertextes qui permettent de lier des pages Web entre elles.

Glossaire

I

ICMP (Internet **M**essage **A**ccess **P**rotocole**).**

IDEA (International **D**ata **E**ncryption **A**lgorithm**) :** est un algorithme de chiffrement symétrique par blocs utilisé pour chiffrer et déchiffrer des données. Il manipule des blocs de texte en clair de 64 bits. Une clé de chiffrement longue de 128 bits (qui doit être choisie aléatoirement) est utilisée pour le chiffrement des données. La même clé secrète est requise pour les déchiffrer.

IMAP (Internet **M**essage **A**cces **P**rotocole**).**

Index : est une structure de données utilisée et entretenue par le système de gestion de base de données (SGBD) pour lui permettre de retrouver rapidement les données. L'utilisation d'un index simplifie et accélère les opérations de recherche, de tri, de jointure ou d'agrégation effectuées par le SGBD. L'index placé sur une table va permettre au SGBD d'accéder très rapidement aux enregistrements, selon la valeur d'un ou plusieurs champs.

Infrastructure : Cette expression désigne l'ensemble des éléments de type matériel et logiciel composant le système informatique d'une entreprise ou d'une organisation.

IP (Internet **P**rotocol**).**

IPsec (Internet **P**rotocols **S**ecurity**).**

IRC (Internet **R**elay **C**hat**).**

ISA (Internet **S**ecurity and **A**cceleration**).**

L

LAN (Local **A**rea **N**etwork**)** : Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

M

MAN (Metropolitan **A**rea **N**etwork**)** : interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux noeuds distants de communiquer comme si ils faisaient partie d'un même réseau local. Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

MD5 (Message **D**igest 5): est une fonction de hachage cryptographique qui calcule, à partir d'un fichier numérique, son empreinte numérique (en l'occurrence une séquence de 128 bits ou 32 caractères en notation hexadécimale) avec une probabilité très forte que deux fichiers différents donnent deux empreintes différentes.

MDA (Mail **D**elivery **A**gent**).**

MTA (Mail **T**ransfer **A**gent**).**

MUA (Mail **U**ser **A**gent**).**

N

NLS (o**N-L**ine **S**ystem**).**

P

PBX : est un autocommutateur téléphonique privé qui sert principalement à relier les postes téléphoniques d'un établissement (lignes internes) avec le réseau téléphonique public (lignes externes). Il permet en plus la mise en œuvre d'un certain nombre de fonctions, notamment (relier plus de lignes internes qu'il n'y a de lignes externes, permettre des appels entre postes internes sans passer par le réseau public , programmer des droits d'accès au réseau public pour chaque poste interne, proposer un ensemble de services téléphoniques (conférences, transferts d'appel, renvois, messagerie, appel par nom…).

PGP (Pretty **G**ood **P**rivacy**).**

PKI (public **k**ey **I**nfrastructure**).**

POP (**P**ost **O**ffice **P**rotocol**).**

PPTP (Point-to-Point Tunneling Protocol).

R

RFC (Requests For Comments) : littéralement « demande de commentaires », sont une série numérotée de documents officiels décrivant les aspects techniques d'Internet, ou de différents matériels informatiques (routeurs, serveur DHCP). Peu de RFC sont des standards, mais tous les documents publiés par l'IETF (**L'Internet Engineering Task Force)** sont des RFC.

Routage : est le mécanisme par lequel des chemins sont sélectionnés dans un réseau pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires. Le routage est une tâche exécutée dans de nombreux réseaux, tels que le réseau téléphonique, les réseaux de données électroniques comme l'Internet, et les réseaux de transports. Sa performance est importante dans les réseaux décentralisés, c'est-à-dire où l'information n'est pas distribuée par une seule source, mais échangée entre des agents indépendants.

RSA nommé par les initiales de ses trois inventeurs(**R**ivest **S**hamir **A**dleman) : Le chiffrement RSA est asymétrique, il utilise une paire de clés (des nombres entiers) composée d'une clé publique pour chiffrer et d'une clé privée pour déchiffrer des données confidentielles.

S

SI (Système d'Information)

SMTP (Simple Message Transfer Protocol).

SSH (Secure Shel).

SSL (Secure Sockets Layer).

SSO (Single Sign-On) : est une méthode qui permet de centraliser l'authentification afin de permettre à l'utilisateur d'accéder à toutes les ressources (machines, systèmes, réseaux) auxquels il est autorisé d'accéder, en s'étant identifié une seule fois sur le réseau. L'objectif du SSO est ainsi de propager l'information d'authentification aux différents services du réseau, voire aux autres réseaux et d'éviter ainsi à l'utilisateur de multiples identifications par mot de passe.

T

TCP (Transfer **C**ontrol **P**rotocol**).**

TELNET (**TEL**ecommunication **NET**work).

U

UDP (User **D**atagram **P**rotocol**).**

URL (Uniform **R**essource **L**ocator**) :** chemin réseau permettant d'identifier une ressource TCP/IP de manière unique.

V

VoIP (Voice **o**ver **I**nternet **P**rotocol).

VPN (**V**irtuel **P**rivate **N**etwork**).**

W

WAN (Wide **A**rea **N**etwork **ou réseau étendu)** : interconnecte plusieurs LANs à travers de grandes distances géographiques. Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un nœud du réseau.