REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR

ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET D'INFORMATIQUE

DEPARTEMENT D'INFORMATIQUE

Mémoire

De fin d'étude

En vue de l'obtention du diplôme de Master en informatique

Options : Réseaux, Mobilités, et Systèmes Embarqués

Thème

Implémentation d'une solution de sécurité en utilisant Le Firewall Forefront TMG (Threat Management Gateway) Cas l'entreprise 2IntPartners

Encadré par :

M^me^ Chamek Lynda.

Réalisé et Présenté par :

M ^elle^ MAMERI Nouara

M^elle^ AIT AMAR Hayat

Promotion 2013/2014

Remerciements

Nous exprimons nos remerciements et nos gratitudes à notre promotrice M^{me} Chamek L. pour L'aide qu'il nous a apporté tout au long de ce travail.

Nos plus vifs remerciements vont aussi aux membres de jury pour nous avoir fait l'honneur De juger ce travail.

Nous réservons ici une place particulière pour remercier vivement nos familles pour leur Affection et leur soutien continu. Et à tous ceux qui, d'une manière ou d'une autre, nous ont Aidés et encouragés à la réalisation de ce modeste travail.

En bref, merci à tous et à toutes

Dédicaces

Je dédie ce travail :

A la mémoire de mon père

A ma très chère mère,

A Mon frères et mes sœurs,

A Toute ma famille,

A tout mes amis(es),

… Et tous ceux qui me connaissent !

Nouara. M

Dédicaces

Je dédie ce travail :

A mon père

A ma très chère mère,

A Mon frères et mes sœurs,

A Toute ma famille,

A tout mes amis(es),

… Et tous ceux qui me connaissent !

Hayat. A

Chapitre I : la sécurité des réseaux informatique

Chapitre II : Forefront Threat Management Gateway (TMG)

Chapitre III : Etude de l'existant

Chapitre IV: Solution Firewall

Chapitre V: Réalisation de l'application

Introduction Générale

De nos jours, les réseaux informatiques ont le but d'assurer le transfert de fichier, le partage des ressources (imprimantes et données), l'exploitation de la messagerie ou l'exécution et la maintenance des programmes à distance. Quelque soient le type système informatiques utilisés au sein d'une entreprise, leur interconnexion pour constituer un réseau est aujourd'hui indispensable.

Avec l'arrivé d'internet, le but premier est d'améliorer la vitesse de transmission des données, en ne se souciant pas de la sécurité dans un premier temps. Au début, il n'y avait que peu de personnes ayant accès à internet. De nos jours, ce n'est plus le cas chacun peut avoir accès à internet chez lui en n'ayant aucune connaissance informatique.

Internet se démocratisant de plus en plus, tout le monde en parle Que ce soit dans les journaux, à la télévision, dans les livres. Naviguer pour certains devient alors trop simple, trop commun, ils vont vouloir se démarquer. Ces internautes vont donc vouloir en connaître plus quelles sont les origines d'internet ? Comment fonctionne t-il ? Qu'est-ce qu'une adresse IP ? Comment fonctionne un serveur web ? Tant de questions auxquelles ils pourront bientôt répondre et devenir des pirates Hackers ou crackers, ils scrutent les ordinateurs du réseau dans l'espoir d'y déceler une faille, pour tenter une intrusion ou pour provoquer un plantage Et cela peut-être sur votre ordinateur ou votre entreprise.

Malgré tout ces risques, les entreprises utilisent l'internet pour accéder à la manne d'information disponible sur le réseau des réseaux, et de pouvoir communiquer avec l'extérieur. Cette ouverture vers l'extérieur est indispensable... et dangereuse en même temps. Ouvrir l'entreprise vers le monde signifie aussi laisser place ouverte aux étrangers pour essayer de pénétrer le réseau local de l'entreprise, et y accomplir des actions douteuses, parfois gratuites de destruction, vol d'information confidentielles. Pour parer à ces attaques, nous somme penché sur l'implémentation d'une solution de sécurité pour l'entreprise 2IntPartnrs. Le cœur d'une telle architecture est basé sur un Firewall Forefront TMG de Microsoft qui est l'objectif de notre projet. Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux possible. Cela représente une sécurité supplémentaire rendant le réseau ouvert sur Internet beaucoup plus sûr.

Pour mieux comprendre le sujet, nous allons d'abord parler dans le 1er chapitre sur la sécurité des réseaux informatique, on détaillera dans le 2^{éme} chapitre le Forefront TMG, et dans le 3^{éme} chapitre en fait une étude de l'existant et dans le 4$^{éme\ chapitre}$ on propose les solutions de sécurité, Enfin, dans le dernier chapitre, on illustrera notre application avec des captures d'écran

Chapitre I :

La sécurité des réseaux informatique

Introduction :

Les attaques informatiques ne cessent d'être dirigées contre les entreprise, petites ou grandes soient-elles. En effet, la menace qui plane sur un système est un fait ; plus l'entreprise possède des informations importantes, plus elle y sera soumise. Cependant, il existe des moyens qui permettent de garder élevé le seuil de sécurité des systèmes en mettant en place des contre-mesures pour réduire les risques d'attaques et la compromission des données.

La sécurité engendre généralement le déploiement de moyens techniques et surtout des solutions de prévention. Ces dernières doivent prendre en compte la formation et la sensibilisation de tous les acteurs de l'entreprise sur les risques encourus. Ainsi il faut mettre en place une bonne politique de sécurité fondée sur la collaboration de l'ensemble des employés et l'utilisation d'équipements et techniques qui répondent aux exigences du système tout en assurant un blocage d' attaques informatiques de tout genre. Dans ce chapitre, nous aborderons les réseaux informatiques, les types d'attaques et leurs mécanismes de protection.

I.1 Généralités sur les réseaux informatiques

I.1.1 Définition d'un réseau informatique :

Un réseau informatique est un ensemble d'ordinateur et périphérique connectés les uns des aux autre afin d'assurer des échange informatique tel que le transfert des fichiers, le partage de ressources (imprimantes et données), la messagerie ou l'exécution de programmes à distance. **[1]**

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

- Désigne l'ensemble des machines ou l'infrastructure informatique d'une organisation avec les protocoles qui sont utilisés.
- Décrire la façon dont les machines d'un site sont interconnectées.
- Spécifier les protocoles qui sont utilisés pour que les machines communiquent.

I.1.2 Les avantages de la mise en réseau:

Un réseau informatique a plusieurs buts distincts : **[1]**

- Partage des ressources logicielles (Applications).
- Partage des ressources matérielles (Imprimantes).
- Partage des données.
- Communication entre personnes distantes.
- Communication entre processus (Machine industrielles).
- Organisations efficaces.
- Accès aux données en temps réel.

I.1.3 Classification des réseaux: [1]

I.1.3.1 Classification selon l'étendue

- **LAN (Local Area Network)**

  Réseau local, intra entreprise permettant l'échange de données et le partage de ressources. Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

  La vitesse de transfert de données d'un réseau local varie entre 10 Mbps (pour un réseau Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire par 1000 utilisateurs.

- **MAN (Metropolitain Area Network)**

Réseau métropolitain qui permet la connexion de plusieurs sites à l'échelle d'une ville. Les MAN interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de Kms). Ainsi un MAN permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local. Dans un MAN on trouve des commutateurs ou des routeurs interconnectés par des liens hauts débits (en générale la fibre optique). **[1]**

- **WAN (Wide Area Network)**

Réseau à l'échelle d'un pays, généralement celui des opérateurs. Le plus connu des WAN est Internet. Un WAN (ou réseau étendu) interconnecte plusieurs LANs à travers de grandes distance géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le cout des liaisons (qui augment avec la distance). **[1]**

I.1.3.2 Classification selon la topologie

- **La topologie en bus**

Une topologie en bus est l'organisation la plus simple d'un réseau, elle désigne le fait que lors de l'émission de données sur le bus par une station de travail, l'ensemble des stations de travail connectées sur le bus la reçoivent. Seule la station de travail à qui le message est destiné la recopié.

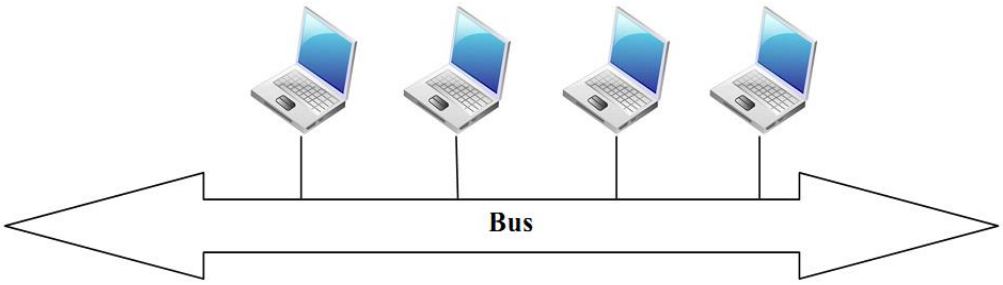


Figure I.1 : Topologie en bus.

Cette topologie a comme avantage d'être facile à mettre en œuvre et de fonctionner facilement, par contre elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, c'est l'ensemble du réseau qui est affecté.

- **La topologie en anneau**

L'information circule tout au longe de l'anneau dans un seul sens. A chaque passage d'un message au niveau d'une station de travail, celle-ci regarde si le message lui est destiné, si c'est le cas elle le recopie.

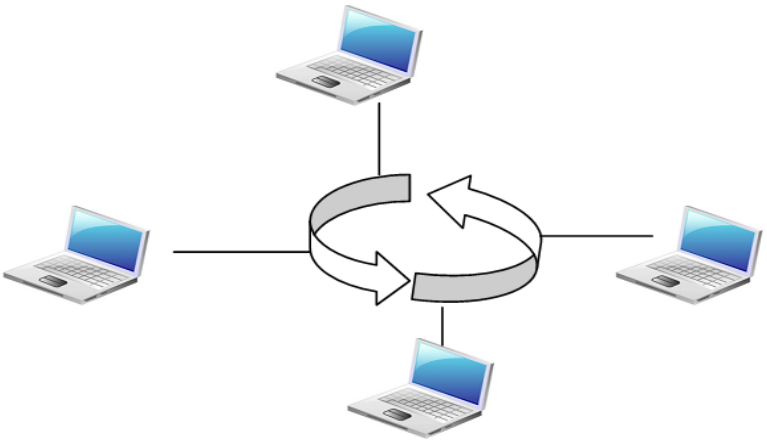


Figure I.2 : Topologie en anneau.

Dans cette topologie chaque ordinateur joue le rôle d'un répéteur en générale de nouveau le signe avant de le transmettre à l'ordinateur suivant, mais tout l'anneau doit être réinitialisé après chaque problème.

I.1.4 La communication sur un réseau:

La transmission d'information entre 2 programmes informatiques sur 2 machines différentes passe par deux modèles : le modèle OSI ou le modèle TCP/IP. Ces deux normes permettent à chaque partie de la communication de dialoguer. Chaque modèle inclut plusieurs couches. Le terme couches est utilisé pour évoquer le fait que les données qui transitent sur le réseau traversent plusieurs niveaux de protocole.

I.1.4.1 Le modèle OSI

OSI (Open System Interconnexion), est un modèle de base qui été défini par l'ISO (International Standard Interconnexions). Cette organisation revient régulièrement pour mettre en place un standard de communications entre les ordinateurs d'un réseau. **[2]**

Ce modèle a permis de standardiser la communication entre les machine afin que les différents constructeurs puise mettre au point des produits (logiciels ou matériel) compatible. Ce modèle définit 7 couches différentes pour le transport de donnée. L'architecture OSI est schématisée comme suit **: [3]**

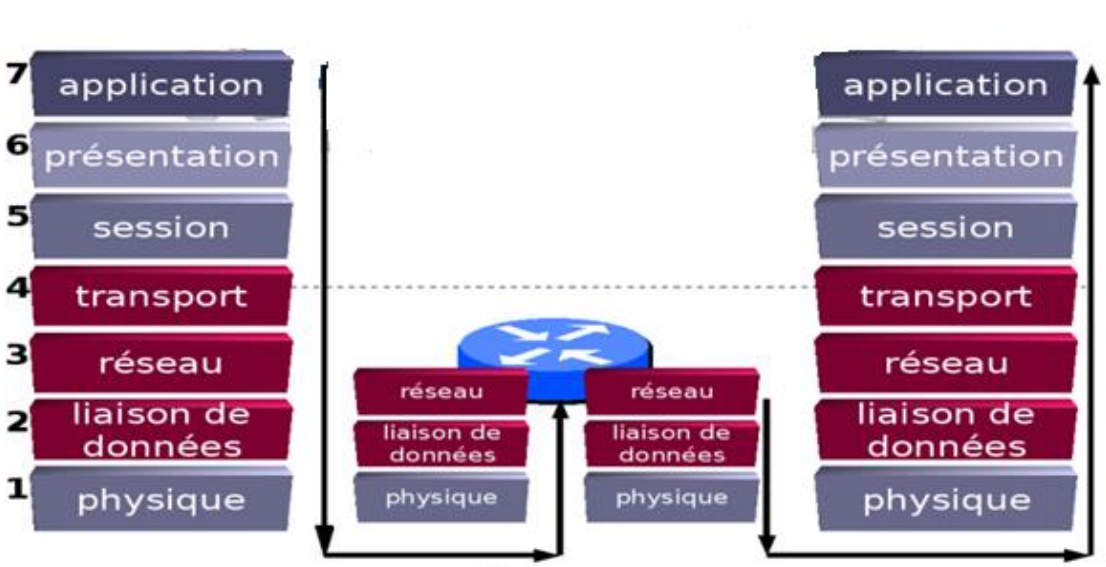


Figure I.3 : Le modèle OSI.

- **Couche application**: assure l'interface avec les applications ; il s'agit donc du niveau le plus proche des utilisateurs géré directement par les logiciels**.**
- **Couche présentation**: s'occupe de la mise en forme des données, éventuellement de l'en cryptage et de la compression des données, par exemple mise en forme des textes, images et vidéo.
- **Couche session**: la couche session, s'occupe de l'établissement, de la gestion et coordination des communications.
- **Couche transport**: la couche transport, gère la remise correcte des informations (gestion des erreurs), utilise notamment l'UDP et le TCP/IP
- **Couche réseau**: la couche réseau, détermine les routes de transport et s'occupe du traitement et du transfert de messages: gère IP et ICMP
- **Couche liaison**: la couche liaison de données, définit l'interface avec la carte réseau: hubs, Switch,…
- **Couche physique**: la couche physique, gère les connections matérielles, définit la façon dont les données sont converties en signaux numériques.

I.1.4.2 Le modèle TCP/IP (Transfert Control Protocol/Internet Protocol):

Le modèle TCP/IP est inspiré du modèle OSI. Il fournit un protocole standard pour résoudre le problème de connexion entre différents réseaux, mais ne contient que quatre couches. Ces couches ont des taches beaucoup plus diverses était donné qu'elles correspondent à plusieurs couche du modèle OSI**. [3]**

TCP (Transfert Contrôle Protocole) : se charge du transport de bout en bout pour toute application.

IP (Internet Protocole) : est responsable du routage à travers le réseau.

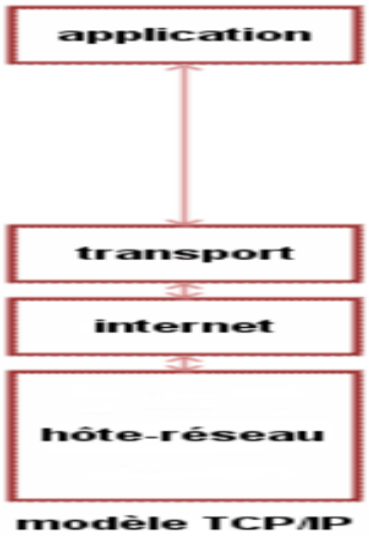


Figure I.4: L'architecture TCP/IP

Le modèle TCP /IP est structuré en quatre couches :

- **La couche application** : elle prend en charge les protocoles d'adressage et l'administration réseau. Elle comporte des protocoles assurant le transfert de fichiers, le courrier électronique et la connexion à distance.
- **La couche transport** : assure le transfert des données et les contrôles de flux qui permettent de vérifier l'état de la transmission**.**
- **La couche Internet :** traite le format des paquets envoyés à travers l'Internet, ainsi que des mécanismes qui permettent de propager les paquets échangées. Le protocole utilisé dans cette couche est : IP**.**
- **La couche accès réseau** : Assure l'interface physique avec le réseau. Elle formate les données aux normes du réseau et élabore les adresses des sous réseaux en tenant compte des adresses physiques des machines destinataires. Elle effectue les contrôles d'erreurs au niveau des données mises sur le réseau physique.

I.2 Internet:

Internet est un **réseau informatique** qui relie des ordinateurs du monde entier entre eux et qui leur perme d'échanger des informations. Les données sont transmises par l'intermédiaire de lignes téléphoniques, des câbles ou de satellites. Pour communiquer entre eux, les ordinateurs connectés à Internet utilisent un protocole de transmission et de communication constituant un langage commun. Ce langage s'appelle la Transmission Control Protocol / Internet Protocol (**TCP/IP). [4]**

I.2.1 Historiques et évolution d'Internet:

Internet est issu du réseau Arpanet, qui a été conçu dans les années 1960 par l'ARPA (Advanced Research Project Agency) pour le département américain de la Défense. A l'origine, il s'agit d'un réseau coopératif

d'ordinateurs permettant le partage de données stockées sur des serveurs distants, ainsi que l'échange de messages électroniques (E-mails). Réseau à usage militaire, Arpanet s'étend alors progressivement aux universités américaines dans les années 1970, notamment l'université de Californie a Los Angeles (UCLA) et l'université Stamford à Palo Alto, avant d'être remplacé en 1990 par le réseau Internet, destiné dans un premier temps à la recherche civile.

En 1991, Tim Berner-Lee du CERN à Genève met au point l'interface d'Internet appelée World Wide Web, qui permet d'ouvrir le réseau au grand public en simplifiant les procédures de consultation des sites. En janvier 1992, l'Internet Society (ISOC) voit le jour avec pour objectif de promouvoir et de coordonner les développements sur Internet. L'année 1993 voit l'apparition du premier navigateur ou butineur (Browser), supportant le texte et les images. Cette même année, la NSF (National Science Foundation) mandate une compagnie pour enregistrer les noms de domaine. D'un point de vue technologique, Tim Berner-Lee, l'inventeur du Web, crée en 1994 le consortium W3C (World Wide Web Consortium), qui a pour objectif de favoriser l'interopérabilité sur le Web, c'est-à-dire le développement de normes**. [4]**

I.2.2 Les protocole d'Internet :

- **Le protocole TCP :**

Responsable de l'établissement de la connexion et du contrôle de la transmission. C'est un protocole de remise fiable, au contraire d'UDP. Le protocole TCP utilise les services du protocole IP afin d'établir une communication fiable entre deux machines : ou les données d'une même transaction, fractionnées en paquets (ou datagrammes IP), sont acheminées de routeur en routeur d'une adresse à une autre.

- **Le protocole IP (protocole Internet) :**

C'est l'un des plus importants protocoles d'internet, il permet la détermination du destinataire du message, son rôle est la transmission d'un bloc de donnée appelé datagrammes d'une source vers une destination, sans toute fois assurer le contrôle du transfert.

- **Le protocole HTTP (Hyper Text Transfer Protocol) :**

Protocole mis en œuvre pour le chargement des pages web et transférer des messages entre un navigateur (client) et un serveur web. C'est le protocole le plus utilisé sur internet depuis 1990. Il se charge de la transmission des documents distribués et multimédia à travers un système d'information multi utilisateurs. Il fonctionne conjointement aux langages HTML.

- **Le protocole HTTPS** : HTTPs pour la navigation en mode sécurisé.

- **Le protocole FTP (File Transfer Protocol) :**

  Protocole utilisé pour le transfert de fichiers sur Internet. Ce transfert s'effectue en établissant une connexion entre un serveur FTP et un client FTP situé sur votre ordinateur. Les fichiers échangés sont des fichiers informatiques de tous types (texte, images, sons, logiciels, …).

- **Le protocole SMTP** (Simple Mail Transfer Protocol) : est conçu pour l'envoi et l'acheminement de courrier**.**

- **Le protocole POP3 (Post Office Protocol version 3) :**

  Le protocole de postage, le protocole POP désigne le service email quand un système est éteint ou n'est plus en ligne (offline). S'il existe une connexion physique du système client au serveur, ce dernier téléchargera les courriers électroniques qu'il détient. Dés lors les courriers détenus par ce serveur seront détruits après le transfert à la machine locale du client POP3 est la versions 3 de protocole de POP. **[11]**

- **Le protocole IMAP (Internet Message Access Protocol) :**

  L'IMAP permet la manipulation des messages distants il fournit des accès multiples aux boites aux lettres avec possibilité sur plusieurs serveurs et donne la possibilité aux utilisateurs de créer, de détruire et de renommer les boites aux lettres.

- **Le protocole IRC** (Internet Relay Chat) : protocole de discussion instantanée.

- **Le protocole UDP**:

  Le protocole UDP utilise IP pour acheminer, d'un ordinateur à un autre, on mode non fiable, des datagrammes qui lui sont transmis par une application. Il est situé au dessus d'IP. Le contrôle d'intégrité des données transmises est à la charge de l'application utilisant les services d'UDP.

- **Le protocole ICMP** (Internet Control Message Protocol) :

  Organise un échange d'informations permettant aux routeurs et aux machines d'envoyer des messages d'erreurs et de commande à d'autres ordinateurs ou routeurs. ICMP tourne au dessus de I, il est requis dans tous les routeurs. C'est pour cette raison qu'il est placé dans la couche IP le but de ICMP n'est pas de fiabiliser le protocole IP, mais de fournir à la couche IP, ou à une couche supérieure de protocole (TCP ou UDP).

I.2.3. Les services d'Internet :

L'internet offre plusieurs services qui sont relatifs aux différents protocoles de communication parmi ces services nous citons **: [4]**

- **E-MAIL (La messagerie électronique) :**

La messagerie électronique est devenue un élément clé des réseaux de communications de la plupart des bureaux modernes. Données et messages peuvent être transmis d'un ordinateur à un autre au moyen de lignes téléphoniques, de liaisons hertziennes, de satellites de communications ou d'autres équipements de télécommunications. Le même message peut être envoyé à un certain nombre d'adresses différentes.

 : L'arrobase, caractère indispensable dans l'adresse d'un courrier électronique

- **Accès à des sites d'information en mode World Wide Web (www) :**

Constitue une véritable bibliothèque virtuelle d'où un explorateur peut télécharger un très grand nombre de documents et de fichiers multimédias et des pages écrites en HTML (HyperText Markup Language). Une des forces du web est qu'il donne accès à tous les services d'Internet totalement ou en parties, il utilise le Protocol HTTP (HyperText Transfert Protocol) pour l'échange d'informations entre le logiciel client (le navigateur) et le serveur.

- **Les news (Forums Electroniques):**

Il s'agit d'un immense ensemble de forums. Les débats s'organisent sous forme de questions et de réponses animées par des abonnés à ces forums. Le protocole utilisé est NNTP (News Network Transfer Protocol).

- **Telnet & SSH:**

C'est un protocole permettant à un ordinateur de se brancher à un autre ordinateur comme s'il se trouvait face à lui. Cela ouvre par exemple des possibilités pour le travail à domicile, puisqu'il devient possible d'utiliser les machines se trouvant sur son lieu de travail depuis chez soi. Telnet est plus ancien, et commence à être abandonné au profit de SSH pour des raisons de sécurité: avec Telnet toutes les informations transmises transitent en clair sur le réseau, y compris les mots de passe, ce qui permet à un éventuel pirate simplement à l'écoute du réseau d'intercepter toutes les données sensibles qui transiteraient de cette manière. À l'inverse pour SSH toutes les données transmises sont cryptées et donc illisibles par toute autre personne que le destinataire.

I.3 La sécurité informatique

I.3.1Définition

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. **[05]**

I.3.2 critères de sécurité

- **La confidentialité :** La confidentialité consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.
- **L'intégrité de données:** Vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle). **[06]**
- **La disponibilité:** Permettant de maintenir le bon fonctionnement du système informatique.
- **Non répudiation :** Permettant de garantir qu'une transaction ne peut être niée.
- **L'authentification:** L'authentification consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.

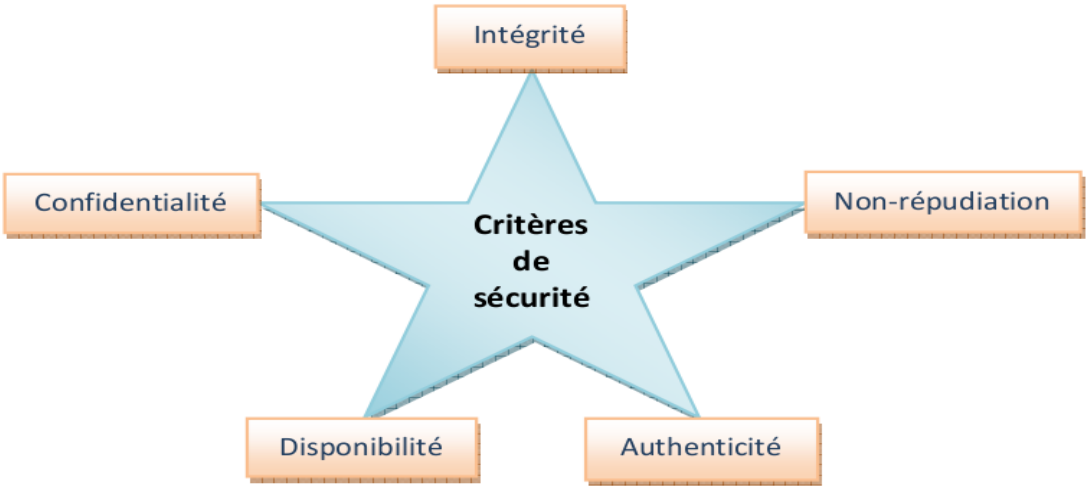


Figure I.5 : **Critères de sécurité.**

I.3.3 Différents types d'attaques

I.3.3.1 Les Attaques réseaux

Les attaques réseaux profitent des vulnérabilités du réseau. Voici quelques exemples d'attaques réseaux **: [06]**

1. Usurpation d'adresse IP

L'usurpation d'adresse IP (IP spoofing) est une technique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet. Le but peut être de masquer sa

propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque sorte l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès. **[06]**

2. DNS Spoofing

Elle consiste à fournir de fausses réponses aux requêtes DNS, c'est-à-dire indiquer une fausse adresse IP pour un nom de domaine, afin de rediriger, à leur insu, des internautes vers des sites pirates. Grâce à cette fausse redirection, l'utilisateur peut envoyer son identifiant en toute confiance.

I.3.3.2 Les attaques applicatives

Les attaques applicatives se basent sur des failles dans les programmes utilisés, ou encore des erreurs de configuration. Toutefois, il est possible de classifier ces attaques selon leur provenance :

1. Man in the middle

Cette attaque permet de détourner le trafic entre deux stations. Imaginons un client communiquant avec un serveur. Un pirate peut détourner le trafic du client en faisant passer les requêtes du client vers le serveur par sa machine, puis transmettre les requêtes de sa machine vers le serveur. Et inversement pour les réponses du serveur vers le client. Totalement transparente pour le client, la machine du pirate joue le rôle de proxy. Il accédera ainsi à toutes les communications et pourra en obtenir les informations sans que l'utilisateur s'en rende compte.

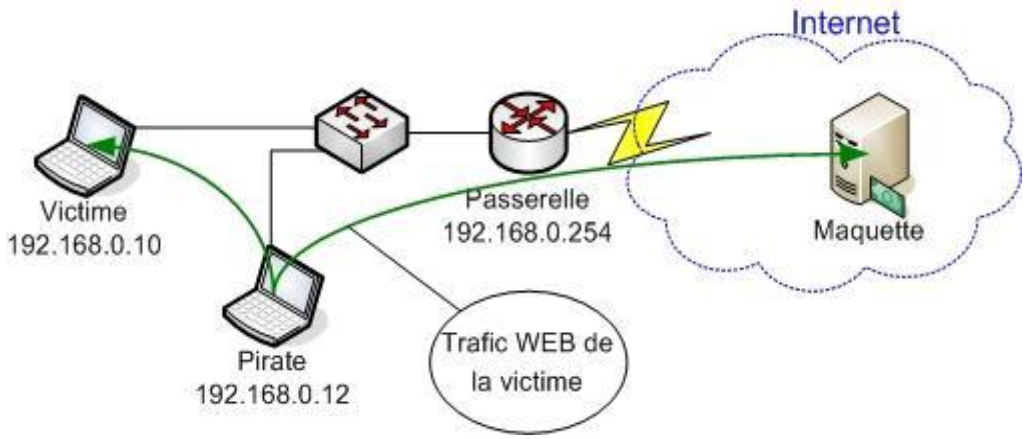


Figure I.6: Attaque Man in the middle.

2. Le Déni de service

Le déni de service est une attaque visant à rendre indisponible un service. Ceci peut s'effectuer de plusieurs manières, par le biais d'une surcharge réseau rendant ainsi la machine totalement injoignable, ou bien de manière applicative en crashant l'application à distance. Grâce à quelques instructions malicieuses et suite à une erreur de programmation, une personne mal intentionnée peut rendre indisponible un service (serveur web, serveur de messagerie) voire un système complet. Voici quelques attaques réseaux permettant de rendre indisponible un service :

3. Attaques de mots de passe

Il existe des moyens permettant au pirate d'obtenir les mots de passe des utilisateurs :

- **les keyloggers :** ou enregistreurs de touches, sont des logiciels lorsqu'ils sont installés sur le poste de l'utilisateur permettent d'enregistrer les frappes de claviers saisies par l'utilisateur.
- **l'ingénierie sociale :** consiste à exploiter la naïveté des individus pour obtenir des informations. Un pirate peut ainsi obtenir le mot de passe d'un individu en se faisant passer pour un administrateur du réseau ou bien à l'inverse appeler l'équipe de support en demandant de réinitialiser le mot de passe en prétextant un caractère d'urgence.
- **l'espionnage :** représente la plus vieille des méthodes. Il suffit en effet parfois à un pirate d'observer les papiers autour de l'écran de l'utilisateur ou sous le clavier afin d'obtenir le mot de passe. Par ailleurs, si le pirate fait partie de l'entourage de la victime, un simple coup d'œil par-dessus lors de la saisie du mot de passe peut lui permettre de le voir ou de le deviner.

4. Les virus

Un virus informatique est un programme doté des propriétés, infection, multiplication et possession d'une fonction nocive. La fonction d'infection permet au virus de s'introduire dans des programmes et données utilisant un langage de script. Lors de l'accès à ces derniers, le code du virus s'exécutera de façon d'abord silencieuse (phase de multiplication pendant laquelle il infectera d'autres fichiers) puis visible (activation de la fonction nocive). Cette dernière pourra être déclenchée par des facteurs très variables selon le virus (au bout de n réplications, à une date fixe, lors de l'exécution de certaines tâches précises…). Elle peut se limiter à l'affichage d'un message agaçant ou conduire à des perturbations graves de l'ordinateur (ralentissement du fonctionnement, effacement ou corruption de fichiers, formatage du disque dur...). **[13]**

5. Le cheval de Troie

Initialement un cheval de Troie désignait un programme se présentant comme un programme normal destiné à remplir une tâche donnée, voire ayant parfois un nom connu (en quelque sorte déguisé sous une fausse apparence) mais qui, une fois installé exerçait une action nocive totalement différente de sa fonction officielle. Actuellement le terme désigne à peu près tout programme qui s'installe de façon frauduleuse (souvent par le biais d'un mail ou d'une page web piégés) pour remplir une tâche hostile à l'insu de l'utilisateur. Les fonctions nocives peuvent être l'espionnage de l'ordinateur, l'envoi massif de spams, l'ouverture d'un accès pour un pirate. **[13]**

7. Les portes dérobées (backdoor)

Une porte dérobée peut être introduite soit par le développeur du logiciel ou un pirate informatique. La personne connaissant la porte dérobée peut l'utiliser pour surveiller les activités du logiciel, voire en prendre le contrôle par contournement de l'authentification.

I.4 Les mécanismes de sécurité

I.4.1.Cryptographie

Les données qui peuvent être lues et comprises sans mesures spéciales sont appelées texte clair. Le procédé qui consiste à dissimuler du texte clair de façon à cacher sa substance est appelée cryptographie ou chiffrement. Le chiffrement des données fut inventé pour assurer la confidentialité des données. Il est assuré par un système de clé (algorithme) appliqué sur le message. Ce dernier est décryptable par une clé unique correspondant au cryptage. Il existe à l'heure actuelle deux grands principes de cryptage : le cryptage symétrique basé sur l'utilisation d'une clé privée et le cryptage asymétrique qui repose sur un codage à deux clés, une privée et l'autre publique**. [13]**

- **Le cryptage symétrique**

Le cryptage à clé privée ou symétrique est basé sur une clé(ou algorithme) partagée entre les deux parties communicantes. Cette même clé sert à crypter et à décrypter les messages. Les algorithmes de chiffrement les plus connus sont : Kerberos, DES (Data Encryptions Standard)

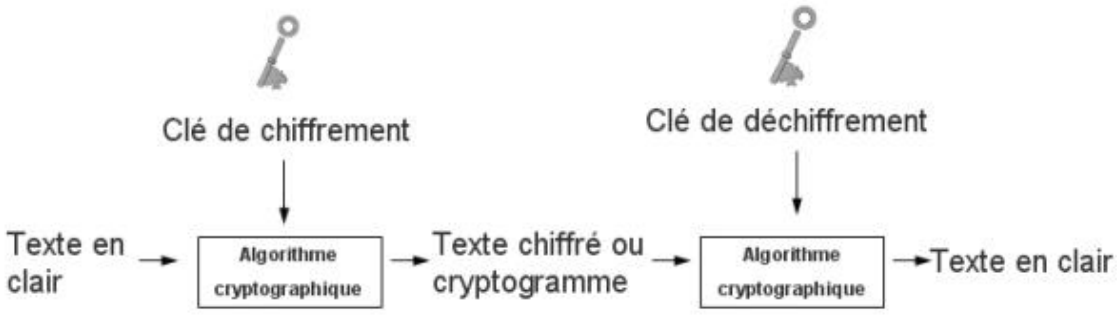


Figure I.7: Les clés symétriques

- **Le cryptage asymétrique**

Ce système de cryptage utilisent deux clé différent pour chaque utilisateur : une est privée et n'est connue que par l'utilisateur l'autre est publique et donc accessible par tout le monde.

Les clés publiques et privé sont mathématiquement liées par un algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privé correspondant. Une clé (la clé publique) est donc utilise pour le cryptage et l'autre (la clé privé) pour le décryptage. Ce cryptage présent l'avantage de permettre le placement des signatures numériques dans le message et ainsi permettre l'authentification de l'émetteur. le principale avantage du cryptage à clé publique est de résoudre le problème de l'envoi de clé privée sur un réseau non sécurisé.

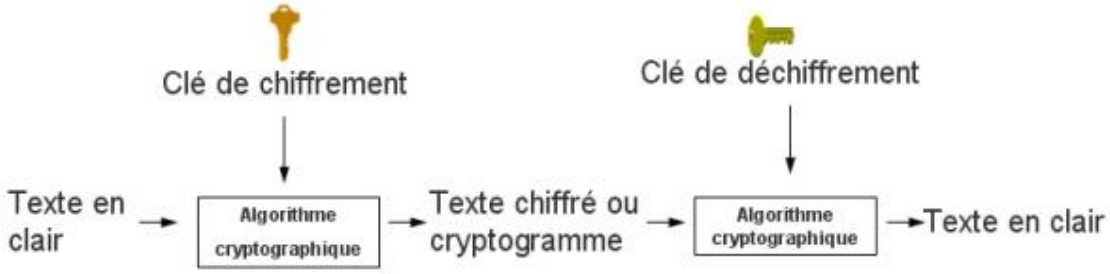


Figure I.8: Les clés asymétriques

I.4.2. La Signature

Dans toute transaction professionnelle, les deux parties doivent offrir une garantie de leurs identités. La signature numérique et le certificat sont des moyens d'identification de l'émetteur du message**. [12]**

I.4.2.1 La Signature numérique

Le principe de la signature numérique consiste à appliquer une fonction mathématique sur une portion du message. Cette fonction mathématique s'appelle fonction de hachage et le résultat de cette fonction est appelé code de hachage. Ce code fait usage d'empreinte digitale du message. Il faut noter que la fonction est choisie de telle manière qu'il soit impossible de changer le contenu du message sans altérer le code de hachage. Ce code de hachage est ensuite crypté avec la clé privée de l'émetteur et rajouté au message. Lorsque le destinataire reçoit le message, il décrypte ce code grâce à la clé publique de la source puis il compare ce code à un autre code qu'il calcule grâce au message reçu. Si les deux correspondent, le destinataire sait que le message n'a pas été altéré et que son intégrité n'a pas été compromise. Le destinataire sait aussi que le message provient de l'émetteur puisque seul ce dernier possède la clé privée qui a crypté le code.

Ce principe de signature fût amélioré avec la mise en place de certificats permettant de garantir la validité de la clé publique fournie par l'émetteur.

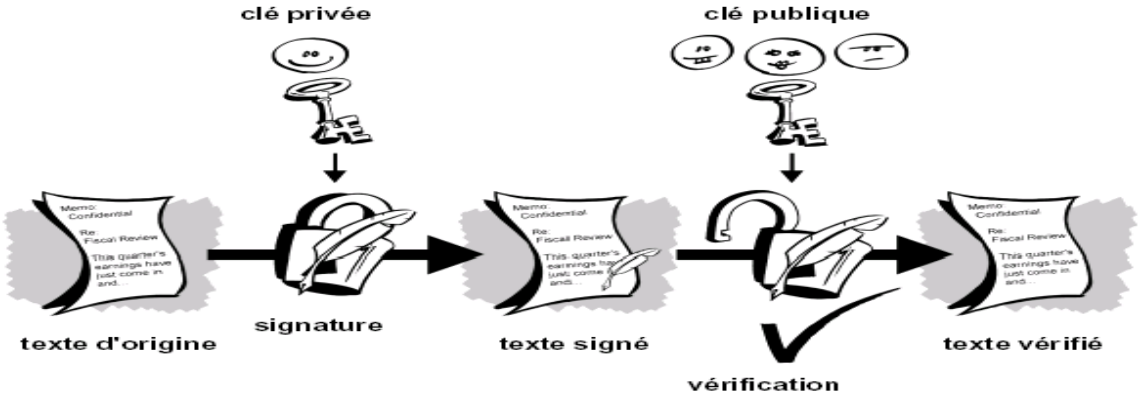


Figure I.9: La signature numérique

I.4.2.2 Les certificats

Pour assurer l'intégrité des clés publiques, celles-ci sont publiées avec un certificat. Un certificat (ou certificat de clés publiques) est une structure de données qui est numériquement signée par une autorité certifiée (CA : Certification Authority). Il contient une série de valeurs, comme le nom du certificat et son utilisation, des informations identifiant le propriétaire de la clé publique et la clé publique elle-même, la date d'expiration et le nom de l'organisme de certificat. La CA utilise sa clé privée pour signer le certificat et assurer ainsi une sécurité supplémentaire.

Si le récepteur connaît la clé publique de la CA, il peut vérifier que le certificat provient vraiment de l'autorité concernée et assurer que le certificat contient des informations viables et une clé publique valide. **[12]**

I.4.3 Réseau Privé Virtuel

Le VPN pour (Virtual Private Network) est une technologie de « réseau Privé Virtual ».il permet à un ordinateur distant d'avoir, via Internet, un accès direct et totalement sécurisé à un autre ordinateur ou à un réseau local. Cette technologie dispense d'avoir recours à de couteuses solutions de location de connexions privées et spécifique.les réseaux privés virtuels permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Grâce à un principe de tunnel (tunnelling) dont chaque extrémité est identifiée, les données transitant après avoir été éventuellement chiffrées**. [07]**

Figure I.10: VPN

- **Le VPN d'accès :** permet à des utilisateurs d'accéder au réseau privé
- **L'intranet VPN :** est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants.

- **L'extranet VPN** : une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans Ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les Droits de chacun sur celui-ci.

I.4.4 les logiciels antivirus :

Il s'agit d'un logiciel capable de détecter et de détruire les virus contenus sur un disque. Le logiciel a pour charger de surveiller la présence de virus et éventuelle de nettoyer et de supprimer ou mettre en quarantaine.

I.4.5 Les protocole de sécurité :

I.4.5.1 Le protocole SSH :

Le SSH (Secure Shell) grâce à ce protocole, il est possible de chiffrer des données par un système de clé privées et publique. Ces données transitent dans un 'tunnel', une sorte de canal sécurisé ou il est impossible de savoir ce qui se passe à l'intérieur. Dans le protocole SSH un ordinateur client peut initier une connexion avec un ordinateur serveur et profiter des mesures de sécurités suivantes :

- Après avoir effectué une connexion initiale, le client peut s'assurer de se connecter au même serveur lors des sessions suivant.
- Le client peut transmettre ses données d'authentification au serveur, telles que son nom d'utilisateur et son mot de passe, en format crypté.
- Tous les données envoyées et reçues pendant la connexion sont transférées de façon chiffrée, ce qui les rendre extrêmes difficile à déchiffre et a lire.

I.4.5.2 Le protocole SSL :

Le protocole SSL (Secure Socket Layer) permet de sécuriser tout protocole applicatif s'appuyant sur TCP/IP (http, FTP, etc. …). Le protocole SSL permet non seulement de fournir les services d'authentification du serveur, mais également les services de confidentialité et d'intégrité. Le principe d'une authentification du serveur avec SSL est le suivant :

- Le navigateur du client fait une demande de transaction sécurisé au serveur.
- Suite à la requête du client, le serveur envoi son certificat au client.
- Le serveur fournit la liste des algorithmes cryptographiques qui peuvent être utilisés pour la négociation entre le client et le serveur.
- Le client choisi l'algorithme.

- Le serveur envoie son certificat avec les clés cryptographiques correspondant au client.
- Si la vérification est correct alors le navigateur du client envoie au serveur une clé secrète chiffré à l'aide de la clé publique du serveur qui sera donc le seul capable de déchiffré puis d'utiliser cette secrète .cette clé est un secret uniquement partagé entre le client et le serveur afin d'échanger des données en toute sécurité. **[07]**

I.4.5.3 Le protocole Secure HTTP :

S-HTTP (http sécurisé) est un procédé de sécurisation des transactions http utilisé pour la navigation sécurisé sur le www. Il offre des possibilités d'authentification et de chiffrement pour les sites web nécessaire un certain niveau de sécurité dans leurs échanges avec les navigateurs web. Pour garantir cette sécurité, S-HTTP fait usage de méthode de cryptographie asymétrique pour l'authentification et des méthodes de cryptographie symétrique pour le chiffrement des échanges. Contrairement à SSL qui se trouve au niveau de la couche transport, S-HTTP procure une sécurité basée sur des messages au dessus du protocole http.Ainsi, alors que SSL est indépendant de l'application utilisé et crypte l'intégralité de la communication, S-HTTP est très fortement lié au protocole http et crypte individuellement chaque massage. Les messages S-http sont basés sur Troie composant **: [06]**

- Le message HTTP.
- Cryptographie de l'envoyeur.
- Cryptographie du destinataire

I.4.6. Firewall :

Un pare-feu (**Firewalls** en anglais) : C'est un système de protection qui est placé entre le réseau d'entreprise et l'internet. Il filtre les informations entrantes et sortantes. Son rôle principal est de protéger l'entreprise contre la fraude, le piratage des informations stockées. Il comportant au minimum deux interfaces réseau.

- une interface pour le réseau à protéger (réseau interne)
- une interface pour le réseau externe.

Le pare-feu représente ainsi généralement dans les entreprises un dispositif à l'entrée du réseau qui permet de protéger le réseau interne d'éventuelles intrusions en provenance des réseaux externes (souvent internet).

Figure I.11 : Le firewall entre le réseau LAN et Internet.

I.4.6.1 Le fonctionnement d'un système pare-feu

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- Soit d'autoriser uniquement les communications ayant été explicitement autorisées : **"Tout ce qui n'est pas explicitement autorisé est interdit".**
- Soit d'empêcher les échanges qui ont été explicitement interdits.

I.4.6.2 Les différents types de filtrages :

- **Le filtrage simple de paquet (Stateless) :** Le fonctionnement des systèmes pare-feu, historiquement assuré par les routeurs, est basé sur le principe du filtrage de paquets IP, c'est-à-dire sur l'analyse des en-têtes des paquets IP (aussi appelé datagrammes) échangés entre deux machines. En effet les machines d'un réseau relié à Internet sont repérées par une adresse appelée adresse IP. Ainsi, lorsqu'une machine de l'extérieur se connecte à une machine du réseau local, et vice-versa, les paquets de données passant par le firewall contiennent les en-têtes suivants, qui sont analysés par le firewall.

  - L'adresse IP de la machine émettrice
  - L'adresse IP de la machine réceptrice
  - Le type de paquet (TCP, UDP, ...)
  - Le numéro de port.

Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé.

- **Le filtrage de paquet avec état (Stateful) :**

Permettant d'effectuer un suivi des transactions entre le client et le serveur et donc d'assurer la bonne circulation des données de la session en cours. Si le filtrage Stateful est plus performant que le filtrage de Stateless basique, il ne protège pas pour autant de failles applicatives, c'est-à-dire les failles liées aux logiciels, représentant la part la plus importante des risques en termes de sécurité.

- **Le filtrage applicatif (ou pare-feu de type proxy ou proxying applicatif)**

Le filtrage applicatif est comme son nom l'indique réalisé au niveau de la couche Application. Pour cela, il faut bien sûr pouvoir extraire les données du protocole de niveau 7 pour les étudier. Les requêtes sont traitées par des processus dédiés, par exemple une requête de type Http sera filtrée par un processus proxy Http. Le pare-feu rejettera toutes les requêtes qui ne sont pas conformes aux spécifications du protocole. Cela implique que le pare-feu proxy connaisse toutes les règles protocolaires des protocoles qu'il doit filtrer.

I.4.6.3 Les différents types de firewall :

- **Les firewalls bridge :**

Ces derniers sont relativement répandus. Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus, d'où leur appellation de firewall. Leurs interfaces ne possèdent pas d'adresse IP, et ne font que transférer les paquets d'une interface a une autre en leur appliquant les règles prédéfinies. Cette absence est particulièrement utile, car cela signifie que le firewall est indétectable pour un hacker. En effet, quand une requête ARP est émise sur le câble réseau, le firewall ne répondra jamais. Ses adresses Mac ne circuleront jamais sur le réseau, et comme il ne fait que « transmettre » les paquets, il sera totalement invisible sur le réseau.

- **Les firewalls matériels**

Ils se trouvent souvent sur des routeurs achetés dans le commerce par de grands constructeurs comme Cisco. Intégrés directement dans la machine, ils font office de « boite noire », et ont une intégration parfaite avec le matériel. Leur configuration est souvent relativement ardue, mais leur avantage est que leur interaction avec les autres fonctionnalités du routeur est simplifiée de par leur présence sur le même équipement réseau.

Figure I.12: Quelques firewalls "matériels"

- **Les firewalls logiciels :** Présents à la fois dans les serveurs et les routeurs

Conclusion :

La dépendance des particuliers et des organisations aux réseaux informatique et aux technologies internet amènent ces dernières à se confronter à différents degrés de vulnérabilités qui sont loin d'être négligeables. La maîtrise des nouvelles technologies par le grand public engendre un accroissement des menaces et une diversification d'outils d'attaques qui ne cessent de se perfectionner.

Il devient donc urgent de mettre en place des mécanismes pour satisfaire au mieux les besoins de la sécurité. Et l'un des mécanismes incontournables, est la mise en place d'une politique de sécurité qui doit être au préalable bien réfléchit et étudiée.

Dans le deuxième chapitre nous aborderons le firewall TMG, toujours, pour augmenter le niveau de sécurité.

Chapitre II:

Forefront Threat Management Gateway (TMG)

Introduction :

Face à des activités basées sur internet et au nombre considérable de réseaux d'entreprise qui y connectés, il est plus jamais nécessaire de disposer d'une passerelle puissante et facile à administrer qui fournisse une connexion sécurisée tout en augmentant et en améliorant les performances réseau. Microsoft Forefront Threat Management Gateway (TMG) répond à ces exigences par une solution de connectivité Internet contenant un pare-feu qui protège les ressources réseau des accès non autorisé provenant de l'extérieur du réseau d'entreprise, tout en permettent des accès autorisé efficaces.

II.1 Présentation de la technologie UTM (Unified Threat Management) :

En sécurité informatique, **UTM** (Unified Threat Management) est un terme inventé par Charles Kology du cabinet de conseil IDC (International Data Corporation) en 2004 et utilisé pour décrire des pare-feu réseaux qui possèdent de nombreuses fonctionnalités supplémentaire qui ne sont pas disponibles dans les pare-feux traditionnels. Avec la technologie UTM Microsoft a développé TMG et parmi les caractéristique de UTM on trouve : Routage, Antivirus, Anti Spam, IPs, Web Filtering**. [14]**

II.2.Présentation de Forefront Threat Management Gateway (TMG) :

Forefront Threat Management Gateway (successeur d'ISA Server 2006) est conçu pour répondre aux besoins des entreprises qui disposent d'un accès à internet, Forefront TMG est une passerelle de haute sécurité qui protège votre informatique contre les menaces d'Internet, tout en offrant à vos utilisateurs un accès à distance rapide et sécurisé aux données et aux applications. Forefront TMG se charge de la sécurité du périmètre à l'aide d'un **firewall intégré**, d'un **VPN**, d'un **filtrage URL** et d'un **IPS/IDS** (Intrusion Prevention System / Intrusion Detection System).

La solution Forefront Threat Management Gateway inclut deux composants :

- **Forefront Threat Management Gateway Server**

  Fournit un filtrage d'URL, une protection Anti malware, un pare feu agissant au niveau applicatif et au niveau du réseau, une protection des flux HTTP et HTTPS, une passerelle VPN et un reverse Proxy (publication Web sécurisée).

- **Forefront Threat Management Gateway Web Protection Service**,

Fournit des mises à jour continuelles pour le filtrage des malwares et l'accès aux données concernant le filtrage d'URL (disponible uniquement avec la souscription à un abonnement Web Protection service). **[15]**

II.3 Objectif de Forefront TMG :

- contrôle les accès entrants et sortants au niveau du périmètre de votre réseau.
- Protège les utilisateurs lors de navigation sur le web, quelque soient le navigateur (Internet explore, Mozila …).
- Protège les infrastructures de messagerie, pas forcément Exchange mais toute messagerie SMTP aussi bien sur la patrie Anti-Spam.
- protège les machines contre les exploits à travers le réseau.
- Faciliter l'administration et le déploiement**. [16]**

II.4.Les édition de Forefront Threat Management Gateway (TMG) :

Forefront TMG est disponible en 2 versions : Enterprise et Standard. Les fonctionnalités de protections de ces 2 versions sont les mêmes, seuls les besoins de déploiement selon l'infrastructure réseau orienteront le choix**. [25]**

II.5. Les caractéristiques de Forefront Threat Management Gateway (TMG) :

Parmi les caractéristiques présentes dans TMG, on cite généralement Routage sécurisé, VPN, le filtrage Anti- Spam, serveur proxy, web Filtering, un système de prévention d'intrusion (IPS), publication des serveurs**. [25]**

II.5.1 Routage :

Dans Forefront TMG a la fonctionnalité de routage au minimum entre deux réseau au plus.

II.5.2. Un système de prévention d'intrusion (IPS) : [18]

C'est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP. La mise en œuvre d'un nouveau protocole Internet (IPV6) intégrant en natif des fonctions de sécurité n'est pas aisée. et le Forefront TMG intègre la fonctionnalité de IPS.

II.5.3 Proxy

Les Proxy permettent d'une part, de relayer le trafic entre Internet et un réseau protégé et d'autre part, ils effectuent un enregistrement intermédiaire de données à des points définis d'Internet.

- **Filtrage :**

D'autre part, grâce à l'utilisation d'un proxy on assure un suivi des connexions (En anglais tracking). Il est possible de filtrer les connexions d'Internet en analysant d'une part les requêtes des clients, d'autre part les réponses des serveurs. Lorsque le filtrage est réalisé en comparant la requête du client à une liste de requête réalisé, on parle d'une liste blanche, lorsqu'il s'agit d'une liste des sites interdits on parle de liste noire. Enfin l'analyse des réponses des serveurs conformément à une liste de critères est appelé filtrage de contenu.

- **Authentification :**

Dans la mesure où le proxy est l'intermédiaire indispensable des utilisateurs du réseau interne pour accéder à des ressources externes, il est parfois possible de l'utiliser pour authentifier les utilisateurs, c'est-à-dire de leur demander de s'identifier à l'aide d'un nom d'utilisateur et d'un mot de passe par exemple. Il est ainsi aisé de donner l'accès aux ressources externes aux seules personnes autorisées à le faire et de pouvoir enregistrer dans les fichiers journaux des accès identifiés.

II.5.4. L e Web Filtering :

Web Filtering permettant de scanner en temps réel les pages web à la recherche des virus, malwares ou autres menaces. Avec le Forefront TMG on peut bloquer des sites web pare exemple (www.facebook.com).

II.5.5. Anti-Spam:

Le terme **« spam »** désigne l'envoi massif de courrier électronique (souvent de type publicitaire) à des destinataires ne l'ayant pas sollicité et dont les adresses ont généralement été récupérées sur internet. Le but premier du spam est de faire de la publicité à moindre prix par « envoi massif de courrier électronique non sollicité ».

Le **« Anti-Spam »** c'est un dispositif qui permet de repérer et , et de supprimer les messages indésirables sur la base de règles évoluées. On distingue généralement deux familles de logiciels anti spam :

- **Les dispositifs Anti Spam côté client :** situé au niveau du client de messagerie. I l s'agi t généralement de systèmes possédant des filtres permettant d'identifier, sur la base de règles prédéfini es ou d'un apprentissage.

- **Les dispositifs Anti Spam côté serveur :** permettant un filtrage du courrier avant remise aux destinataires. Ce type de dispositif est le meilleur car il permet de stopper le courrier non sollicité et éviter l 'engorgement des réseaux et des boîtes aux lettres.

II.5.6. Publication des serveurs:

La publication des serveurs c'est d'exposer des serveurs comme des serveurs web ou exchange sur l'internet donc l'utilisateur se connecte au Forefront TMG qui se charge de l'authentification du client en fonction de la stratégie mise en place si l'authentification est concluant, TMG crée le lien entre ce client et le serveur.

II.5.7 Les réseaux privés virtuels (VPN) : le Forefront TMG intègre les réseaux privés virtuelle, un client externe pour avoir accès aux réseaux locaux via VPN il faut avoir des configurations dans le Forefront TMG qui autorise au non l'accès aux réseaux internes

II.6. Les nouveautés Forefront TMG par rapport à ISA serveur 2006:

II.6.1.Microsoft Internet Security and Acceleration Server (ISA Server):

ISA serveur est décrite par Microsoft comme une "passerelle de sécurité périphérique intégrée". Appelé précédemment **Microsoft Proxy Server**, **ISA** est un produit de sécurité de type pare-feu basé sur Microsoft Windows conçu initialement pour présenter (publier) sur Internet des serveurs Web et d'autres systèmes serveur de manière sécurisée.

Il fournit un système pare-feu au niveau de la couche application gérant l'état des sessions mode dit Stateful, un service d'accès VPN et l'accès Internet pour les ordinateurs clients dans un réseau d'entreprise.

II.6.2.Les nouveautés

TMG ajoute quelques nouvelles fonctionnalités intéressantes qui n'étaient pas disponibles dans ISA Server.

- **Filtrage des URL :** Autorise ou refuse l'accès à certains sites selon les catégories d'URL autorisées ou non par l'administrateur TMG.
- **Inspection HTTPS :** des sessions établies à l'aide du protocole encrypté HTTPS pourront être inspectées à la recherche de menaces. De plus, pour des raisons de respect de la vie privée, certaines sessions (sites bancaires par exemple) peuvent être exclues de cette inspection.
- **Protection E-mail :** Forefront TMG fonctionne en collaboration avec Microsoft Exchange server pour scanner les e-mail à la recherche des virus, menaces, etc.
- **Network Inspection System(NIS) :** permet d'analyser le trafic réseau à l'aide d'une analyse par protocole pour prévenir de l'utilisation d'exploits. Le système NIS se base sur des signatures de vulnérabilités connues pour détecter et bloquer le trafic malveillant.

- **Web Anti malware :** TMG permet de scanner en temps réel les pages web à la recherche de virus, malwares ou autre menaces.

II.7 La topologie du réseau dans Forefront Threat Management Gateway(TMG) :

II.7.1 Edge Firewall :

Le hot bastion est l'ordinateur qui constitue le principal point de contact des clients des réseaux internes lorsqu'ils accèdent à internet. En tant que pare-feu, l'hôte bastion est conçu pour défendre le réseau interne des attaques. Un hôte bastion contient deux cartes réseau, l'une est connectée au réseau interne et l'autre est connecter au réseau externe.

- **Avantage liés à l'utilisation d'un hôte bastion:**

Il permet de réduire le cout et le volume des taches administratives requises pour un pare-feu. Cependant, un hôte bastion dépend d'un seul pare-feu pour protéger l'ensemble du réseau. si un internaux compromet le pare-feu, il peut accéder au réseau interne de l'entreprise.

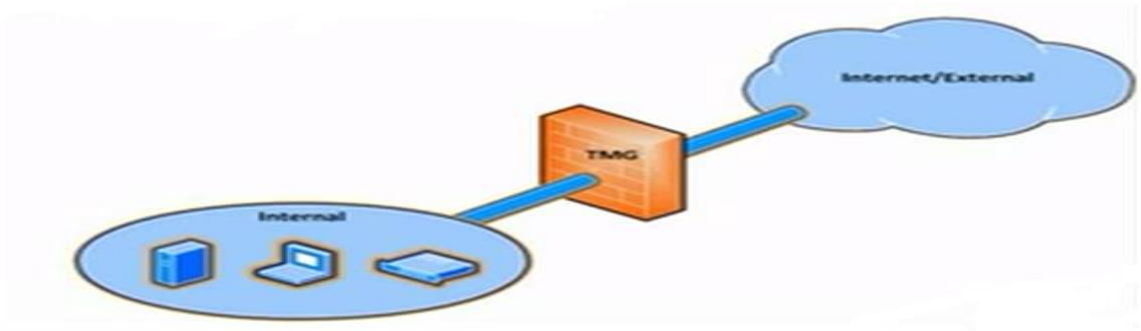


Figure II.1 Edge Firewall

II.7.2 Réseau périphérique équipé d'un pare-feu tri-résident :

Un réseau périphérique est un petit réseau qui contient les ressources qui peuvent être mises à la disposition des internautes tout en assurant la sécurité de ces ressources. Un réseau périphérique est séparé de réseau interne et d'Internet. Ce dernier permet aux clients externes d'accéder à des serveurs spécifiques situés sur le réseau périphérique tout en empêchant totalement l'accès au réseau interne. Un tel réseau sert généralement à déployer des serveurs Web ou des serveurs de messagerie. Le pare-feu est configurer avec trie carte réseau chaque carte réseau est connecté à l'un des réseaux suivants :

- Internet.
- les serveurs du réseau interne situés sur le réseau périphérique.
- Les clients du réseau interne.

Bien que les serveurs du réseau périphérique aient chacun des adresse IP auxquelles les clients externes peuvent accéder, l'ordinateur pare-feu ne permet pas d'accéder directement aux ressources qui sont situées sur le réseau interne.la stratégie de sécurité d'une entreprise peut également autoriser un trafic réseau restreint et très contrôlé entre les ordinateurs du réseau périphérique et des ordinateurs sélectionnés sur le réseau interne.

- **Avantage liés à l'utilisation des pare-feu tri-résidents :**

Un pare-feu tri-résident fournit une meilleure sécurité, il permet un accès sécurisé à certaines ressources réseau à partir d'Internet sans autoriser le trafic réseau entre Interne et le réseau interne. Un pare-feu tri-résident fournit un seul point d'administration permettant de configurer l'accès à votre réseau périphérique et au réseau interne. Toutefois, un pare-feu tri-résident fournit aussi un seul point d'accès à toutes les parties de réseau, ce qui signifie qu'il doit être particulièrement attentif à la conception des règles d'accès.

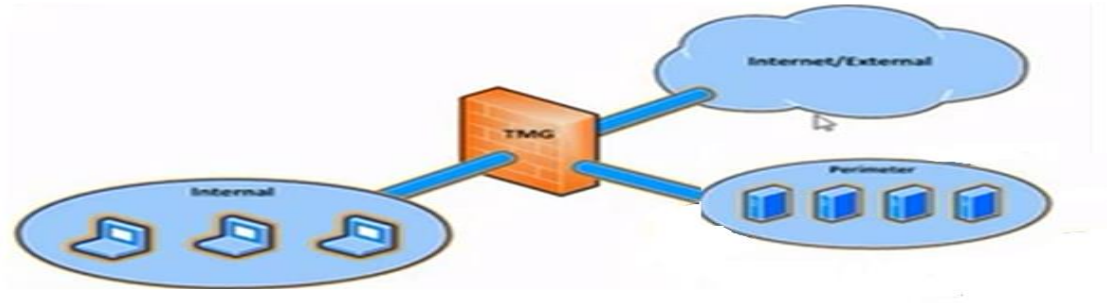


Figure II.2 schéma d'un Réseau équipé d'un pare-feu tri-résident.

II.7.3 Réseau périphériques équipé de pare-feu dos-à-dos:

Un réseau périphérique équipé d'un pare-feu tri-résident, on peut configurer un réseau périphérique avec des pare-feu dos-à-dos.sur un réseau périphérique équipé de pare-feu dos-à-dos, deux pare-feu sont situés de chaque coté du réseau périphérique.

Ces deux pare-feu sont connectés au réseau périphérique, l'un étant également connecté à Internet et l'autre au réseau interne. Donc pour atteindre le réseau interne, un utilisateur doit traverser les deux pare-feu.

- **Avantage liés à l'utilisation des pare-feu dos-à-dos :**

On peut configurer des règles de sécurité plus strictes sur des pare-feu dos-à-dos que sur un pare-feu tri-résident, ce qui permet de protéger votre réseau interne de façon plus fiable.il est également plus facile de configuré des règles pour des pare-feu dos-à-dos si la stratégie d'accès de l'entreprise autorise un trafic réseau restreint et très contrôlé entre des ordinateurs du réseau périphérique et des ordinateurs sélectionné sur le réseau interne.

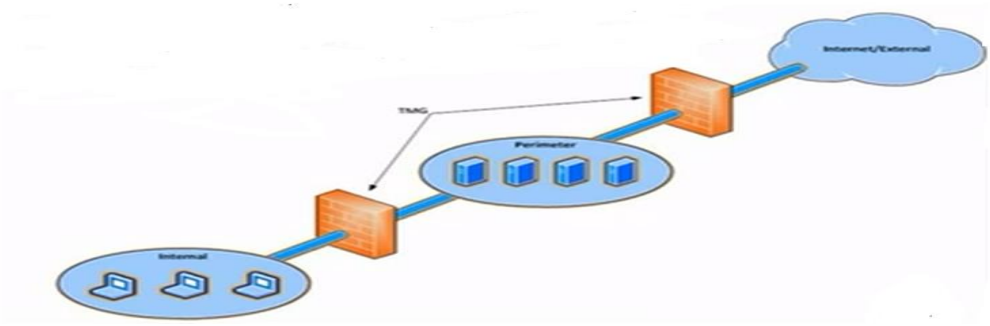


Figure II.3 schéma d'un Réseau équipé d'un pare-feu dos-à-dos.

Conclusion:

Avec internet, de nouvelles opportunités s'offrent aux entreprises pour se connecter à leurs clients, leurs partenaires et leurs employés. Toutefois, Internet s'accompagne de nouveaux risque et de nouvelles préoccupations portant sur la sécurité, les performances et l'amélioration de la gestion. Forefront TMG est conçu pour répondre aux besoins actuels des entreprises présentes sur Internet. Forefront TMG apporte un pare-feu d'entreprise multicouche qui permet de protéger les ressources réseau contre les virus, les pirates informatiques et les accès frauduleux.

Chapitre III:
Etude de l’existant

Introduction

Les attaques informatiques constituent aujourd'hui l'un des fléaux de notre civilisation moderne. Il ne se passe plus d'une semaine sans que l'on apprenne que telle entreprise ou tel institut a essuyé de lourdes pertes financières en raison d'une déficience de la sécurité de son réseau. Par conséquent les entreprises ne peuvent plus ignorer ces risques et se croire à l'abri de telles épreuves. C'est pour cela que nous nous sommes penchées sur la sécurité de l'entreprise 2IntPartenrs. Et pour découvrir toute ambiguïté nous allons découvrir les problèmes liés à l'architecture existant de 2IntPartnrs.

III.1 Présentation de l'organisme d'accueil

Le but principale de 2IntPartnrs est l'intégration des nouvelles technologies et des standards Internet au sein des systèmes d'information de ses utilisateurs toute la démarche est fondée sur une compréhension approfondie de l'activité des utilisateurs des enjeux et contraints afin de garantir la mise en œuvre d'une solution fiable.

L'offre du 2int est centrée sur les systèmes et réseaux, le développement d'applications, les bases de données et les environnements « Open Source ».

III.1.1 Architecture d'organisme d'accueil :

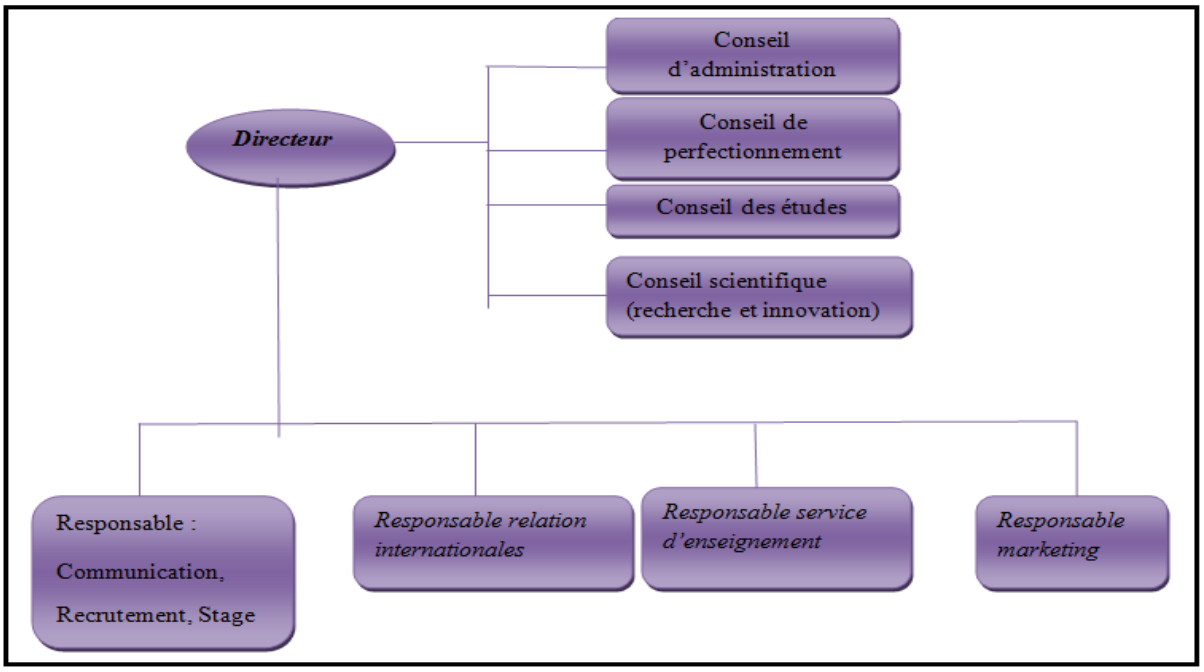


Figure III.1 L'organigramme de 2intPartenrs.

III.2 Situation actuelle

2IntPartenrs a pour vocation d'intégrer de nouvelles technologies et des standards Internet au sein des systèmes d'information de ses clients. Dans ce cadre, nous allons décrire la situation actuelle de 2IntPartnrs qui

souhaite adopter une solution de firewall qui satisfait ses exigences vis-à-vis à la gestion des accès de ses employés au réseau internet et pour améliorer la sécuriser de son système d'information.

Dans ce qui suit, on va détailler les composants du système d'information existant de l'entreprise 2IntPartnrs:

III.2.1 Produit de messagerie « Exchange 2010 »

La messagerie électronique est l'un des applications d'internet les plus anciennes : les premières messageries électronique datent des années 60 et le premier protocole de messagerie sur Arpanet a été crées 1972 aujourd'hui l'e-mail est l'application d'internet la plus populaire et la plus répandus au monde.

Exchange Server 2010 nous permet d'atteindre des niveaux inédits de fiabilité et de performance en offrant des fonctionnalités qui simplifient l'administration, protègent les communications **[24]**

III.2.2 Active Directory (AD)

Est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows. L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs**. [19]**

III.2.3 Contrôleur de domaine : Windows Server 2008

Le contrôleur de domaine permet d'héberger le service d'annuaire (authentification des utilisateurs, validation des accès aux ressources,…).Lorsqu'on crée un contrôleur de domaine dans l'entreprise, on crée également le premier domaine, la première forêt, le premier site et on installe Active Directory.

III.2.4 Certain éléments d'interconnexion comme le Switch et des routeurs.

- **Le Switch :** c'est un système assurant l'interconnexion de stations ou de segments de LAN en leur attribuant l'intégralité de la bande passante à l'inverse de concentrateur qui la partage.
- **Le routeur :** ils travaillent au niveau de la couche 3 du modèle OSI, et s'occupent du routage des unités de données. Ils permettent d'interconnecter deux réseaux de types différents. Un routeur transfère des paquets en les analysants au niveau 3 du modèle ISO.

Parmi les éléments d'interconnexion utiliser au sien de l'entreprise 2IntPartnrs en trouve des Switch et des router CISCO.

III.2.5 Architecture et composants du réseau de l'entreprise

Topologie du réseau de l'entreprise est en étoile: Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur.

III.3 Présentation de l'architecture existante

L'infrastructure existante de 2IntPartnrs est constituée :

- D'un réseau local qui contient des postes des utilisateurs.
- D'un Firewall TMG (Windows Server 2008 R2 64 Bits).
- D'un serveur Active Directory (Windows Server 2008 R2 64 bits)
- Certain éléments d'interconnexion comme les Switch et les routeurs.
- D'un serveur Exchange 2010 externe.
- D'un réseau externe (Internet).

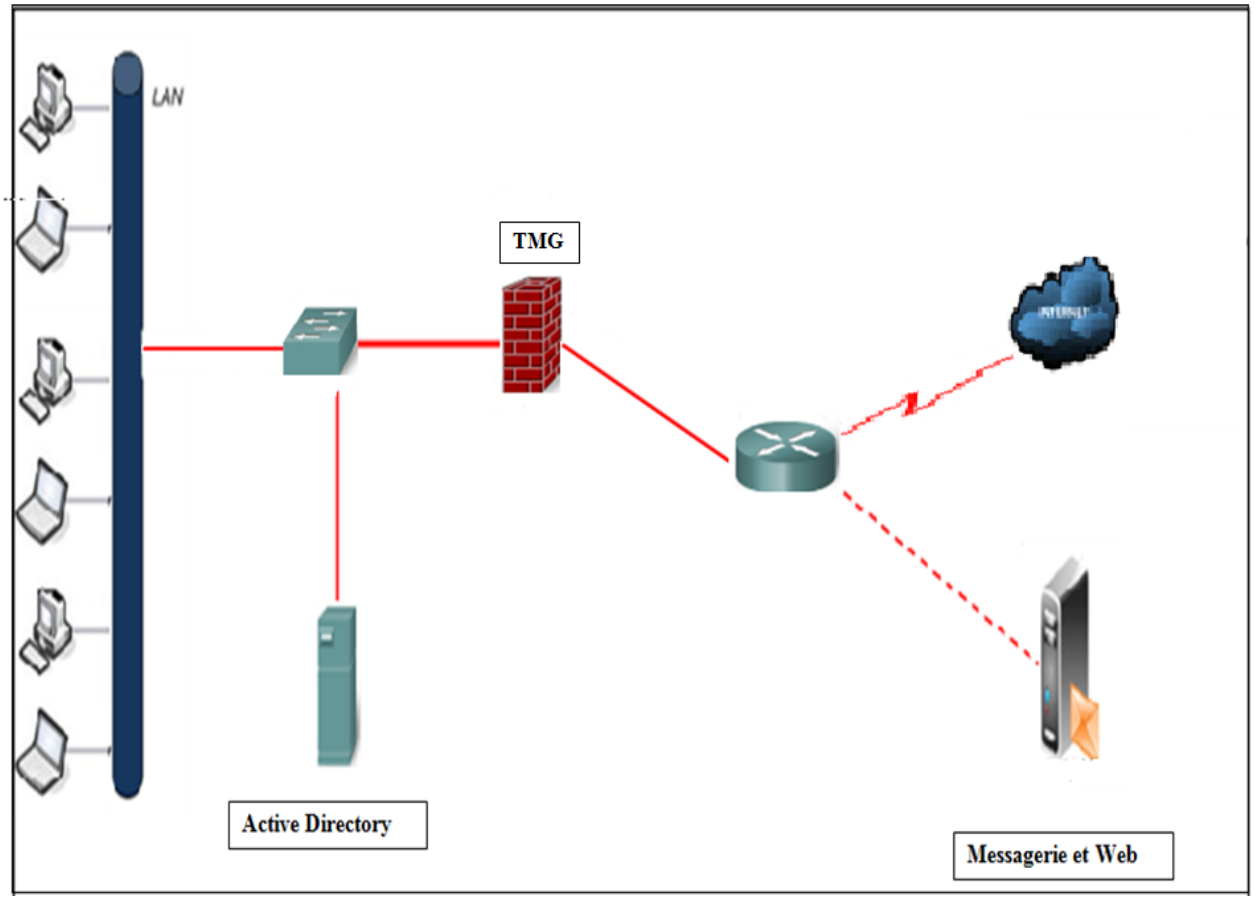


Figure III.2: L'architecture existant de 2IntPartners.

III.3.1 Problème liés a cette architecteur :

Cette architecteurs possède plusieurs problèmes dont on cite :

- Absence de sécurité
- Un seul Firewall peut être attaqué par un Déni de service.
- Volume accru du trafic générer par chaque utilisateur
- Trafic web important
- N'importe quelle employer peut accéder et même pirate le serveur Active Directory
- Le serveur Exchange n'est pas sécurisé
- Absence des certificats.
- Les données rechanger entre le serveur Exchange et le réseau interne peut être Intercepter par un pirate (Main In The Middle).
- Le Firewall TMG est membre de domaine.

III.3.2 Matrice des besoins

Cette matrice résume les exigences de l'entreprise en une liste de règles devant être respectés par la future solution proposés et pour résoudre les problèmes lies a leurs architecteur existant et qui fera l'objet de notre projet :

- **Règle 1 :** Autorisé juste pour certain groupe d'utilisateur d'accéder a Internet et même vers des sites web précise.
- **Régle2 :** Blocage de certain site web par exemple (http://www.Facebook.com)**.**
- **Règle 3 :** Installation de deux Firewall TMG, le premier sera intégrer dans le domaine et le deuxième Workgroups
- **Règle 4 :** Création de deux zones DMZ (Zone Démilitarisé).
- **Règle 5 :** Mettre les serveurs Active Directory et les serveurs de base de données dans DMZ1
- **Règle 6 :** Mettre les serveurs accessibles depuis l'extérieur (Serveur Exchange et Serveur Web) dans la DMZ 2.
- **Règle 7 :** Mettre en place de deux serveurs Exchange 2010.

- **Règle 8 :** Les rôles « **HUB** » et le « **CAS »** d'Exchange Server 2010 seront installé dans des serveurs différents.
- **Règle 9 :** Publication d'Exchange Serveur 2010, le serveur qui contient le rôle « **CAS** ».
- **Règle 10 :** publication de serveur Web (IIS).
- **Règle 11** : l'utilisation des certificats d'Authority.
- **Règle 12** : l'authentification via le protocole LDAP.

Conclusion

La complexité des attaques, la facilité de se renseigner sur les logiciels et les moyens d'intrusions via le net, font que n'importe qu'elle architecture aussi sécurisée soit-elle peut être confrontée à d'innombrables défaillances. C'est le cas de notre architecture, qui doit être protégée des attaques informatiques pouvant nuire à son bon fonctionnement. La présentation de notre solution sera l'objectif de prochain chapitre.

Chapitre IV

Solution proposée

Introduction :

Aux débuts de l'informatique, la sécurité physique était au cœur des préoccupations pour protéger les données sensibles. Mais avec l'arrivé des réseaux les pirates ont porté leurs attentions sur les protocoles de communication. Ils ont développé des méthodes ciblant à attaquer les connexions réseaux pour récupérer ou compromettre les données privées des entreprises. Parmi les méthodes utilisées on retrouve le spoofing d'adresses, la recherche de mots de passe et les dénis de services.

La prévention de ces attaques a conduit les plus grandes maisons de l'informatique à mettre en place des outils permettant un degré de sécurité satisfaisant pour les entreprises. Parmi ces moyens nous retrouvons, le développement des firewalls. Dans ce chapitre nous présenterons la solution proposée pour résoudre les problèmes liés à l'architecteur existant de l'entreprise 2 IntPartenrs.

IV.1 La Solution proposée :

Après avoir entamé l'étude de l'existant et l'analyse de différent problème liées a l'architecteur existant de 2IntPartnrs on a aboutit à la représentation de notre solution qui basé sur le firewall TMG et qui respecte au plus la matrice des règle imposée par 2IntPartenrs.

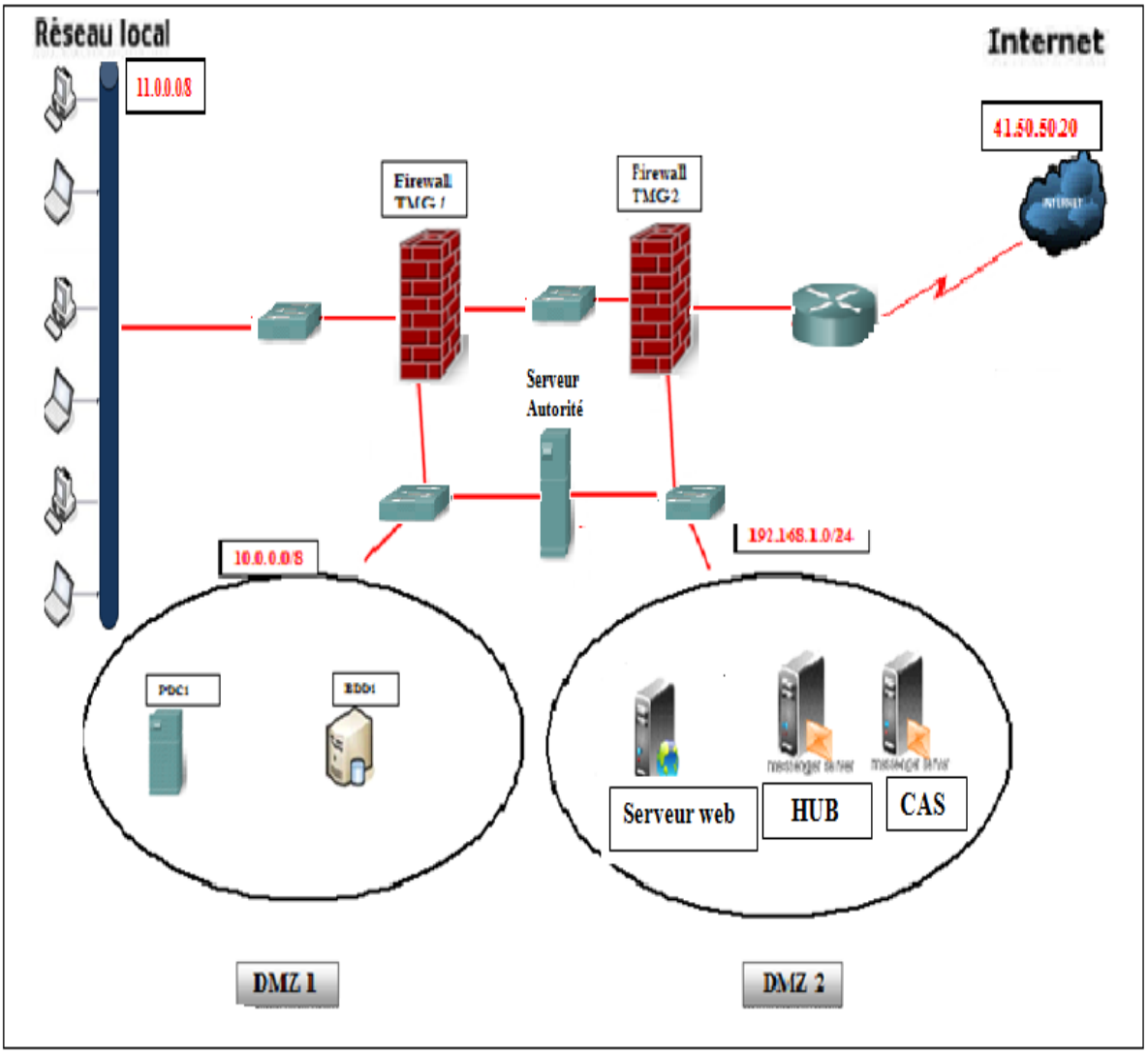


Figure IV.1: La solution proposée

IV.2 Les composant de l'architecteur proposée :

Dans ce qui suit, on va détailler les composants du la solution proposée pour 2IntPartnrs. Avec ajouté de nouveau matériels qui doivent être utilisés par l'entreprise dans le but d'assurer le fonctionnement optimal de

ses ressources réseaux et assurer à ses membres un accès rapide à l'information et un partage facile des données. Notre solution est constituée :

- **Deux firewall TMG (Thread Mangement Gateway),** chaque firewall contient 3 interfaces:
  - Une interface interne.
  - Une interface externe.
  - Une interface DMZ.
- **Deux Zones DMZ :**
  - **DMZ 1** contient :
    - Une base de donnes (BDD).
    - Un Contrôleurs de domaine (ADC).
    - Un Active directory (PDA).
  - **DMZ 2** contient :
    - Un serveur web.
    - Deux serveurs Exchanges (Exchange1 ; Exchange2).
- Un serveur d'Autorité de certificat.
- Un réseau interne LAN contient des postes des utilisateurs
- Un réseau externe (Internet).
- Certaine élément d'interconnexion comme les Switch et les routeurs.

IV.2.1 Une Zone DMZ (Zone démilitarisé) :

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, un serveur FTP public, etc.), 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 Demilitarized Zone) 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. Les serveurs situés dans la DMZ sont appelés « **bastions** » en raison de leur position d'avant poste dans le réseau de l'entreprise. La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

- Traffic du réseau externe vers la DMZ **autorisé**.
- Traffic du réseau externe vers le réseau interne **interdit**.
- Traffic du réseau interne vers la DMZ **autorisé**.
- Traffic du réseau interne vers le réseau externe **autorisé**.

- Traffic de la DMZ vers le réseau interne **interdit**.
- Traffic de la DMZ vers le réseau externe **refusé**.

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise.

IV.2.2 Un serveur Web

On appelle serveur web aussi bien le matérielle informatique que le logiciel, qui joue le rôle de serveur informatique sur un réseau local ou sur le World Wide Web. Et dans la solution proposée nous avons sécurisé le site web avec SSL.

IV.3 Les étapes à suivre pour la réalisation de la solution

Etape 1 :L'ajoute d'un Firewall TMG

Dans l'architecteur existant de 2IntPartnrs on trouve un seul firewall TMG qui placer entre le réseau local et le réseau externe, et si un pirate arrive à pénétrer ce firewall la premier victime si le réseau local et l'Active Directory parce que le firewall est un membre de domaine (intégrer dans le domaine). Et pour cela nous avons choisi d'ajouter un autre Firewall TMG qui sera placé entre le réseau externe (Internet) et le firewall TMG de l'entreprise. Et ce nouveau firewall ajouter sera installé comme Workgroups. Comme le montre la figure suivant :

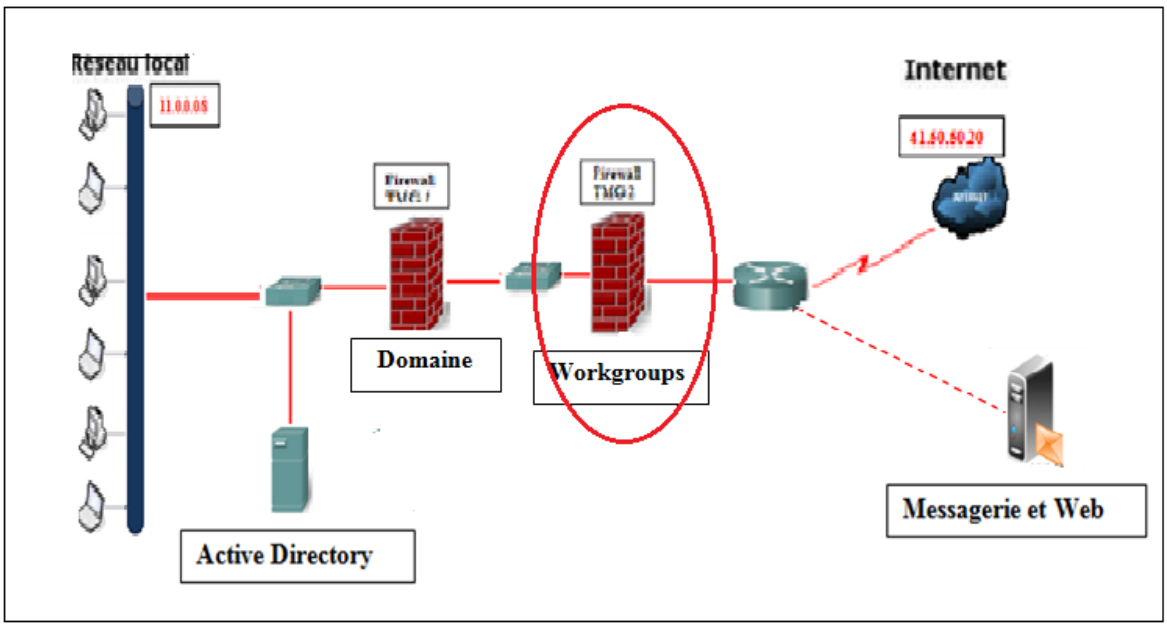


Figure IV.2: l'ajoute de firewall TMG

Etape 2 : Création de deux zones DMZ

Nous avons chois de mettre deux zone DMZ, dans le firewall TMG1 on créer une interface DMZ1 avec l'adresse IP 10.0.0.0/8 et dans le firewall TMG 2 on créer l'interface DMZ 2 avec l'adresse IP 192.186.1.0/24

La création de ces deux zone nous permettre de sécurisé en plus les donnés sensible de l'entreprise (Active Directory, les base de donner) est si un pirate arrive au réseau local de l'entreprise ce dernier il ne peut pas arriver au donner sensible de l'entreprise

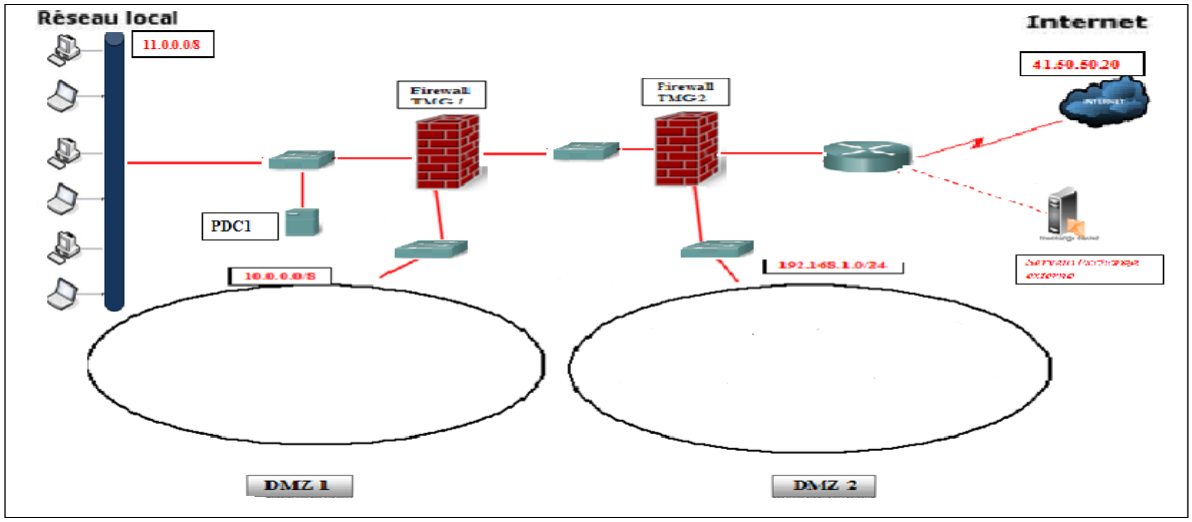


Figure IV.3: l'ajoute de deux zones DMZ

Etape 3 : Ajoute de serveur Exchange externe dans la DMZ 2 :

Dans notre solution proposée nous avons choisi de mettre le serveur Exchange interne (DMZ 2) et en installe le rôle « HUB » et « CAS » dans des serveurs différent et de faire publier le serveur qui contient le « CAS ». Parce que la publication des deux rôles est risquer d'être pirater, le « HUB » contient la base de donner Comme le montre la figure suivant :

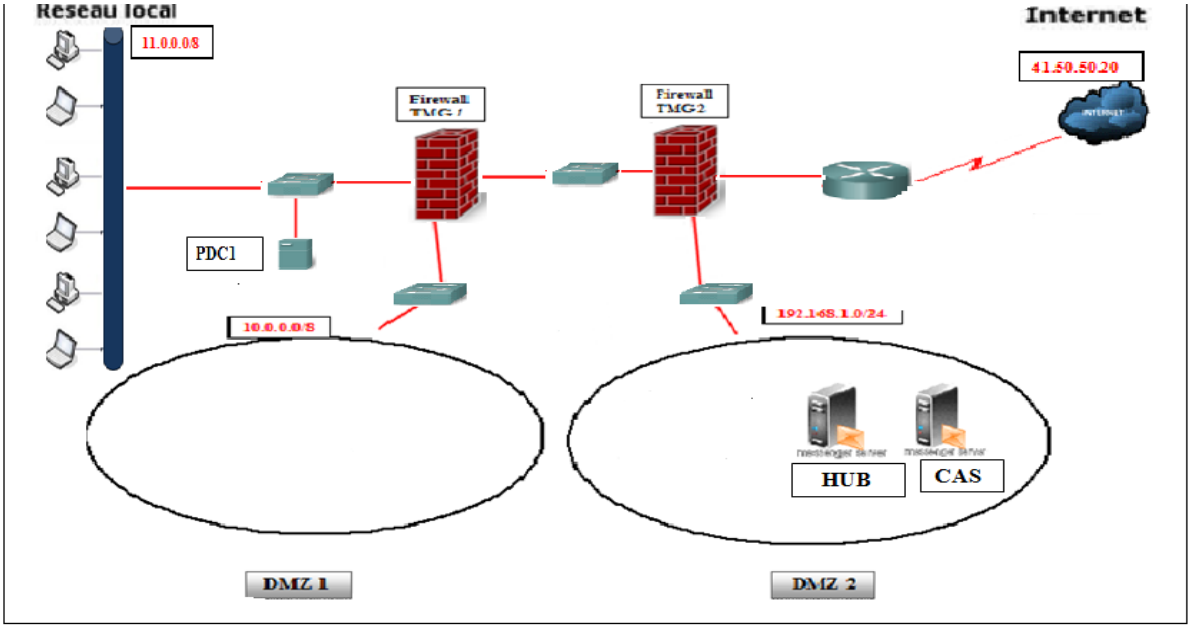


Figure IV.4: l'ajoute de serveur Exchange dans la DMZ 2

Etape 4 : Ajoute le Serveur Active Directory dans la DMZ 1 :

Dans l'architecteur existant de 2IntPartnrs le serveur active directory n'est pas sécurisé et n'importe qu'il utilisateur de réseau interne peut accéder au donner sensible de l'entreprise.et pour cela nous avons choisi de l'intégrer dans la DMZ1.

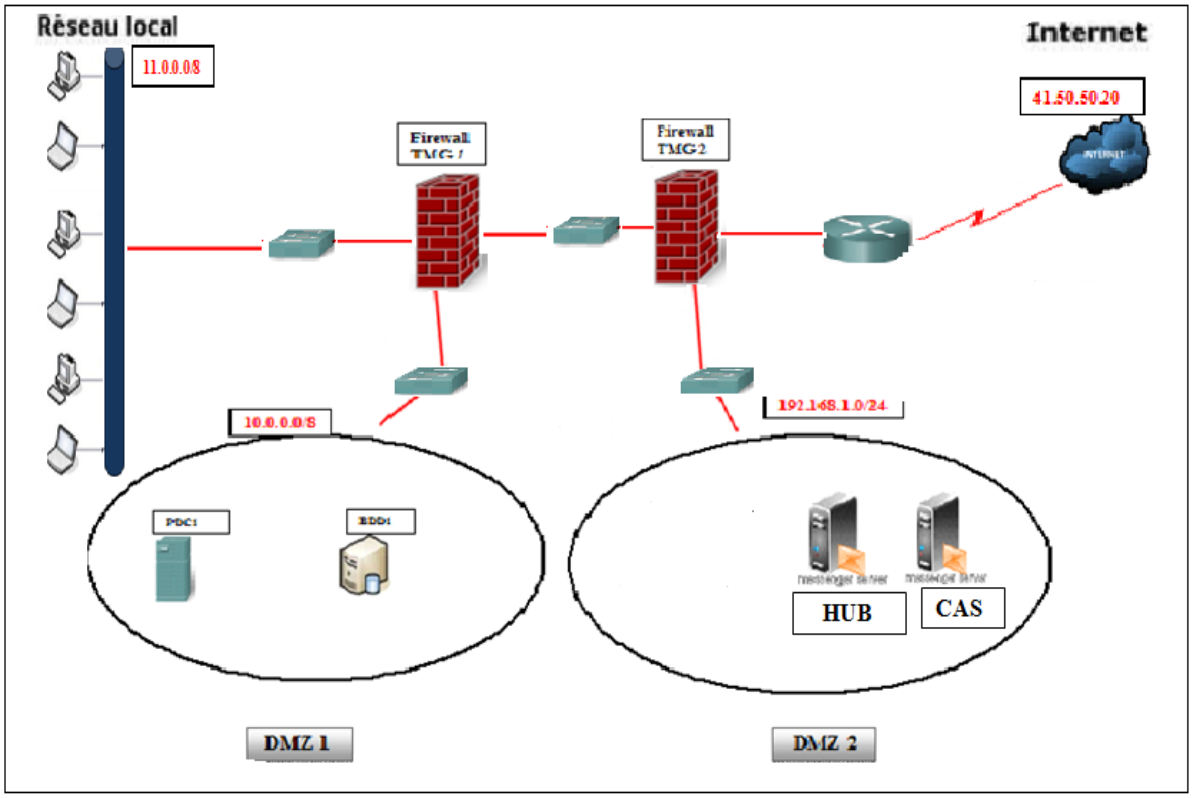


Figure IV.5: l'ajoute de serveur Active Directory dans la DMZ

Etape 5 : L'ajoute de Serveur Web:

Dans la solution proposée nous avons choisi de maitre le serveur web dans la DMZ parce que ce serveur sera accessible de l'extérieur (Internet) il aura des échange avec les clients externe et de publier le serveur web en tout sécurité en utilisant le SSL.

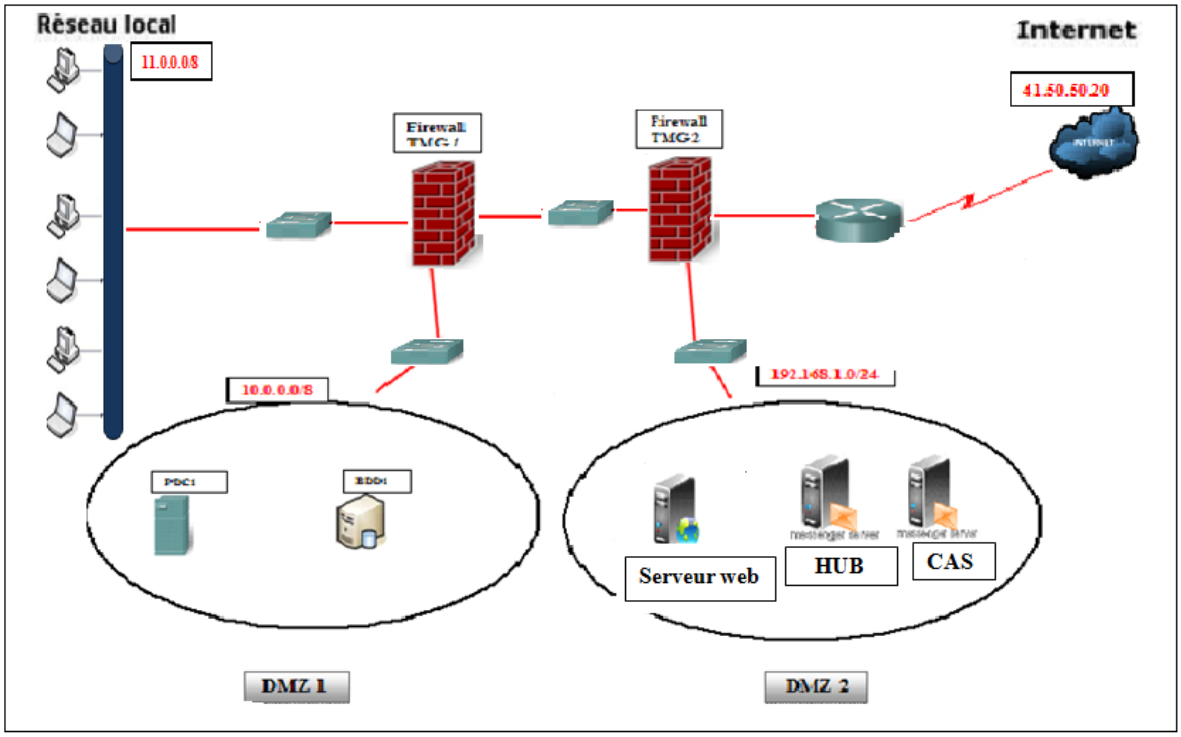


Figure IV.7: L'ajoute de serveur Web sécurisé.

Etape 6 : Maitre en place d'un serveur de certificat d'Authority

Maitre en place d'un serveur d'Authority de certificat pour sécurisé tout les échange de donner et l'utilisation des certificats pour la publication de l'exchange en tout sécurité. Et l'accès sécurisé entre le serveur web publier les clients externes.

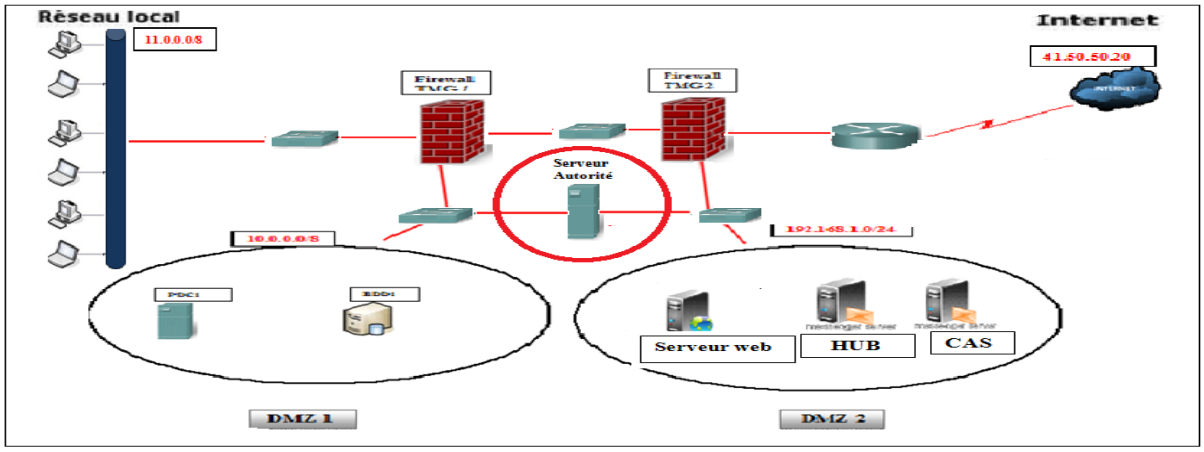


Figure IV.8: L'ajoute de serveur d'Authority de certificat

Conclusion :

Dans ce chapitre nous avons proposé une solution de sécurité en base sur l'architecteur existant de l'entreprise 2IntParterns et nous avons essayé d'améliorer la sécurité au niveau de cette entreprise et de minimiser les risques des attaques externes on utilisant le pare-feu TMG de Microsoft.

Chapitre V
Réalisation de l’application

Introduction :

Quelle que soit la performance et l'efficacité des outils et techniques utilisés pour la mise en place d'une solution de sécurité, il reste difficile, voire impossible, d'assurer la sécurité à 100%. L'avènement d'internet et des nouvelles technologies donnent une raison et une curiosité motivante aux pirates et aux malveillants de pénétrer de plus en plus dans les réseaux que ce soit par fun ou pour usurper des données et informations confidentielles.

Dans cette solution nous essaierons le maximum d'amélioré la sécurité d'entreprise en accordant aux différents administrateurs la responsabilité de sensibiliser les membres de l'entreprise au secret professionnel.

Dans ce chapitre, nous présenterons les différentes étapes suivies afin d'implémenter la solution citées précédemment.

V.1. Présentation des outils utilisés :

V.1.1. La VMware Workstation 8.0.0

Pour l'émulation de notre réseau, nous avons choisi d'utiliser la VMware Workstation 8.0.0. Cette dernière permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique. Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'hôte physique. Cette version exécute les applications les plus exigeantes, elle utilise le dernier matériel pour répliquer l'environnement des serveurs postes de travail tout en étant accessible de n'importe quel périphérique grâce à son interface Web. **[22]**

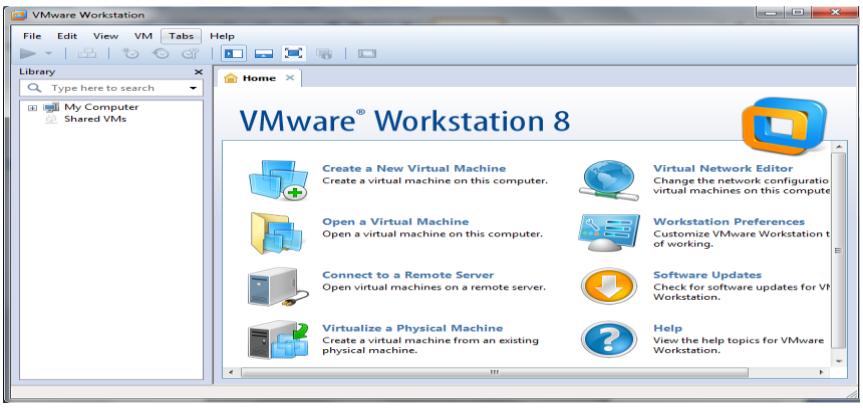


Figure V.1: VMware Workstation 8.

V.1.2. Microsoft Windows Server 2008

Microsoft Windows Server 2008 est conçu pour fournir aux entreprises la plate-forme la plus productive pour virtualiser les charges de travail en utilisant la virtualisation Microsoft intégrée, alimenter des applications et protéger des réseaux. Il propose aussi une plate-forme sécurisée et facile à gérer servant à développer et héberger de façon fiable des applications et des services Web. **[23]**

Figure V.2 : Server 2008.

V.1.3. Active Directory

Pour réaliser la gestion des objets sans liens avec la disposition réelle des protocoles réseaux employés, nous avons utilisé Active Directory qui est un annuaire des objets du réseau. Il permet aux utilisateurs de localiser, gérer et utiliser facilement les ressources, en organisant l'annuaire en sections, ce qui permet de suivre le développement d'une société allant de quelques objets à des millions d'objets. Combiné aux stratégies de groupes, Active directory permet une gestion des postes distants de façon complètement centralisée.

Figure V.3: Active Directory.

V.1.4 Les étapes suivies pour la mise en place de notre application

Etape I : la préparation des machines

Nous avons préparé les machines suivantes :

- ✓ Un contrôleur de domaine.
- ✓ Deux serveurs membre pour l'installation de la TMG.
- ✓ Un serveur membre pour l'installation de Microsoft Exchange Server 2010.
- ✓ Un serveur membre pour l'installation de serveur Web (IIS).
- ✓ Un serveur membre pour l'installation de serveur des certificats d'autorité (CA).
- ✓ Une machine membre client interne qui fait office de machine test.

- ✓ Une machine (internet) client externe qui fait office de machine test.

1. L'installation du contrôleur de domaine :

Après préparation de la machines virtuelles Windows Server 2008, nous avons installé un contrôleur de domaine (PDC), **www.tmg.com.**

Dans l'annexe 1, vous trouverez l'installation et le fonctionnement de l'Active Directory sous le Windows serveur 2008.

1.1 L'ajout d'un serveur ou machine membre

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

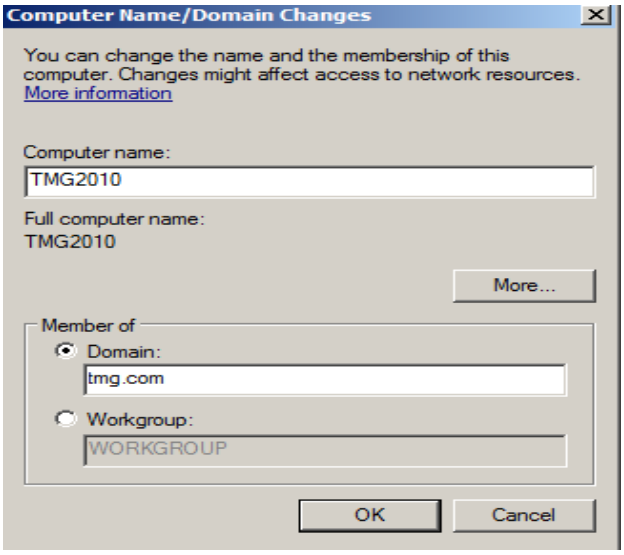


Figure V.4: Ajout de la TMG1 au domaine www.tmg.com.

Etape II : Installation du serveur Web IIS :

IIS (Internet Information) Services propose bien évidemment la prise en charge de ce protocole pour sécuriser les données transmises sur le réseau entre le serveur Web et un client.

Le rôle du serveur Web l'IIS 7.0 de Windows Server 2008 est de partager des informations avec des utilisateurs sur internet, intranet ou extranet. IIS nous permet d'avoir une plateforme web unifiée, améliorée et permet de personnaliser les sites web.

Après l'installation de service IIS dans un serveur web, on créer un site Web comme suit :

Dans le menu démarrer→ outils d'administration→ gestionnaire des services Internet (IIS)→ une fenêtre de dialogue s'ouvre→on clique sur « Ajouter un site Web », comme montre le figure suivant :

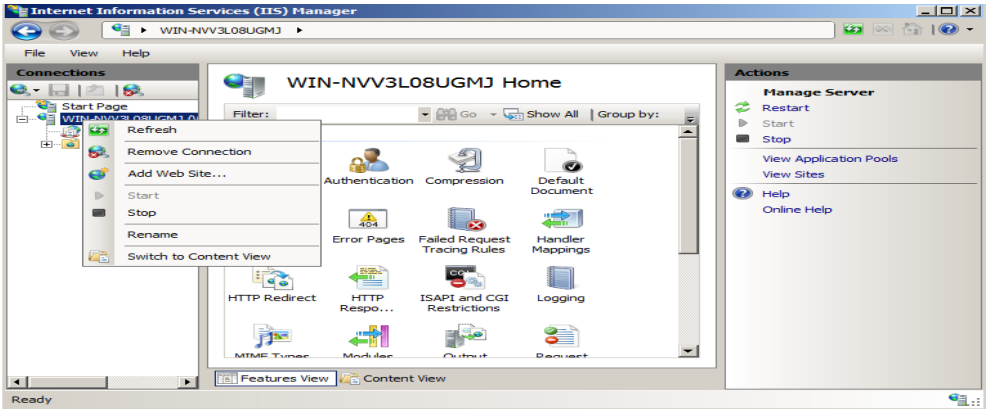


Figure V.5: création un nouveau site

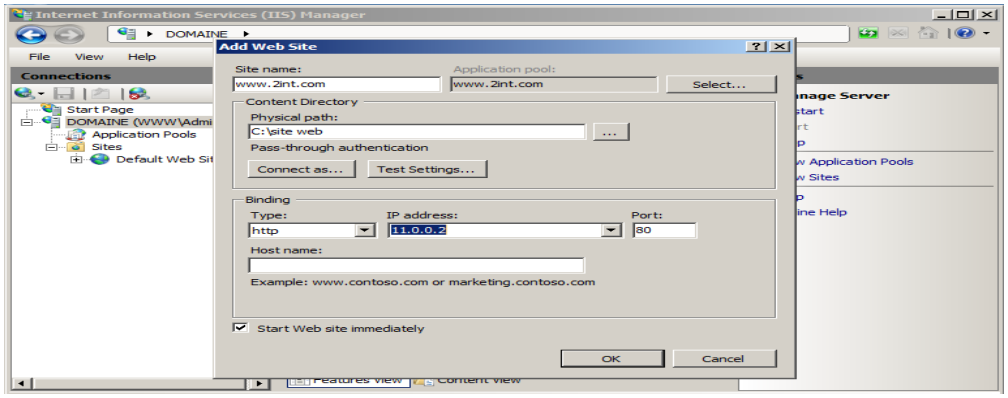


Figure V.6: les informations de nouveau site

Etape III : Installation et configuration du Server Exchange 2010

1. Installation de Microsoft Exchange Server 2010

L'ensemble des étapes d'installation de l'exchange sont détaillées dans l'annexe C**.**

3. Configuration de Microsoft Exchange 2010

3.1. Configuration des bases de données

3.1. a. Création d'une base 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-> boite aux lettres->Nouvelle base de données de boite aux lettres.

Puis nous indiquons le nom de la base de données ainsi que le serveur Exchange qui l'héberge.

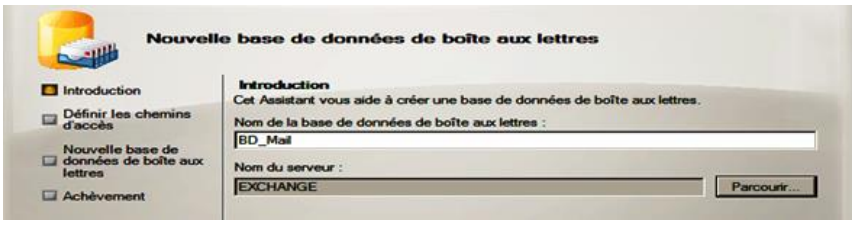


Figure V.7: Création de la base de données de boite aux lettres.

3.1. b. Création d'un compte de messagerie utilisateur

Il existe différents types de boîtes aux lettres :

- ✓ **Boite aux lettres utilisateur** : boîte classique pour un utilisateur.
- ✓ **Boite aux lettres de salle** : permet de réserver des salles de réunion.
- ✓ **Boite aux lettres d'équipements**: permet de réserver des équipements (vidéoprojecteurs).
- ✓ **Boite aux lettres liée**: permet d'associer une adresse mail avec un compte situé par exemple dans une forêt différente.
- ✓ **Autodiscover** : permet d'activer la recherche d'un mail depuis les boîtes aux lettres.

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

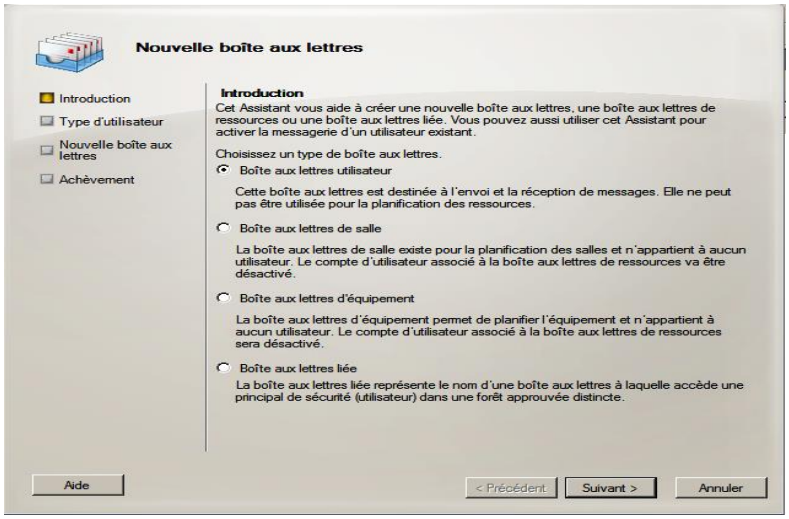


Figure V.8: Création de boite aux lettres utilisateur.

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

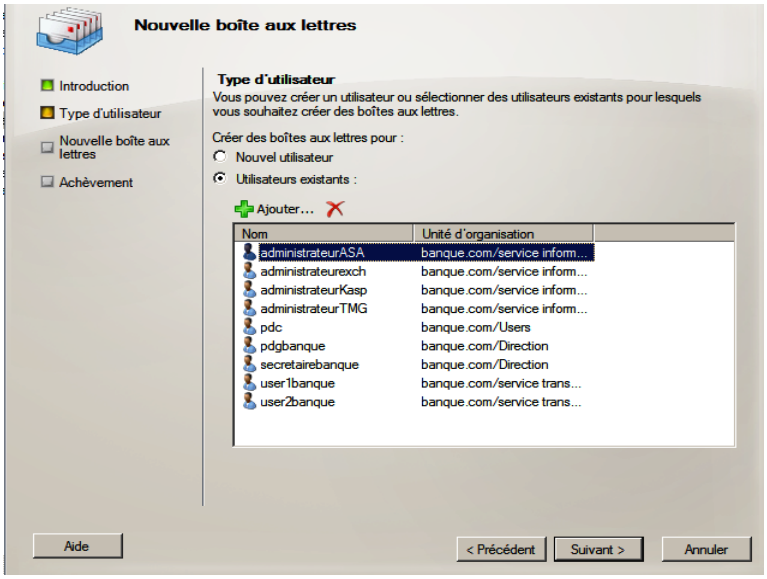


Figure V.9: Sélection des utilisateurs.

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

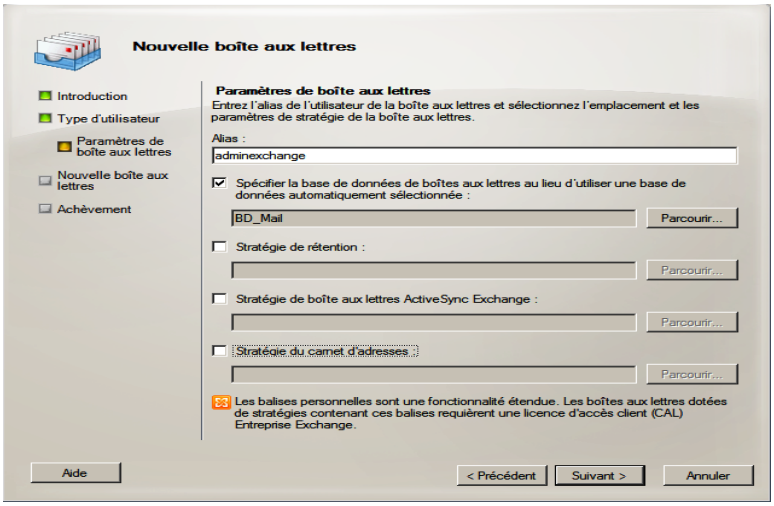


Figure V.10: Paramétrage de boite aux lettres.

Etape IV : L'installation et configuration de la TMG1 et TMG2 :

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

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 fichiers NTFS.
- ✓ 2,5 Go d'espace disque disponible.

2. Configuration des cartes réseau dans TMG1 :

L'installation préalable de la TMG exige l'ajout et la configuration de 3 cartes réseaux :

- ✓ Une interne avec l'adresse 11.0.0.0/8 (11.0.0.200)
- ✓ Une externe avec l'adresse 13.0.0.0 /8 (13.0.0.10)
- ✓ Une pour la DMZ avec l'adresse 170.100.100.1/16

3. Configuration des cartes réseau dans TMG2 :

Même nombres de carte réseau (3 cartes réseaux) dans TMG2 mais avec des adresses IP différents :

- ✓ Une interne avec l'adresse 10.0.0.0/8 (10.0.0.100)
- ✓ Une externe avec l'adresse 41.10.10.10/24
- ✓ Une pour la DMZ avec l'adresse 192.168.0.1/24

4. Lancement de l'installation de la TMG

Les différentes étapes d'installation de la TMG sont définies dans l'annexe 1**.**

La fenêtre suivante présente l'interface principale de Forefront TMG 2010 :

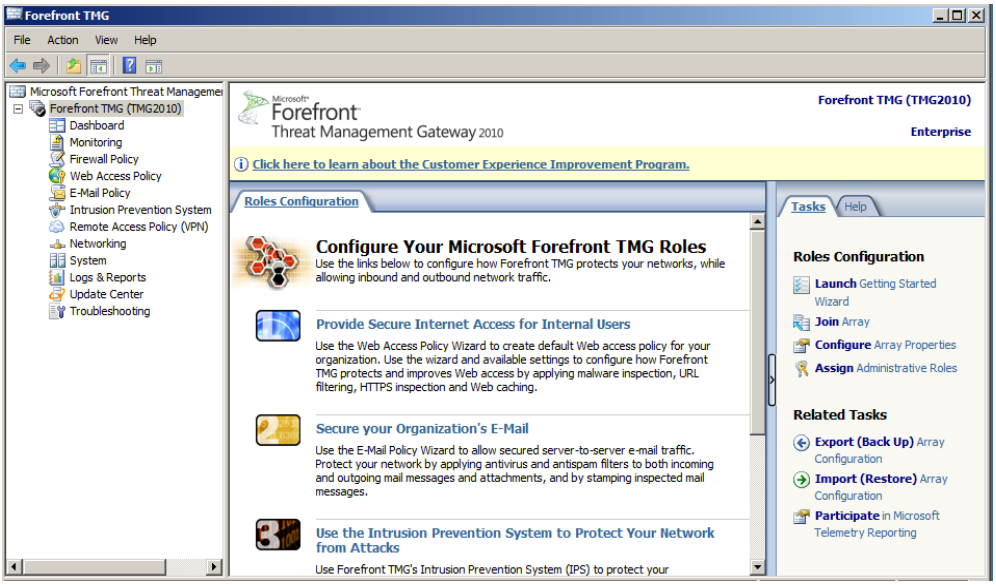


Figure V.11 : La console de gestion de la TMG.

Après l'installation on remarque que le TMG divise en 5 réseaux :

- Local Host (TMG lui même).
- Internal (Réseau LAN).
- External (Internet).
- VPN (Les personnes qui connecté de l'extérieur)
- VPN Quarantin (NAP: Network Access Protection).

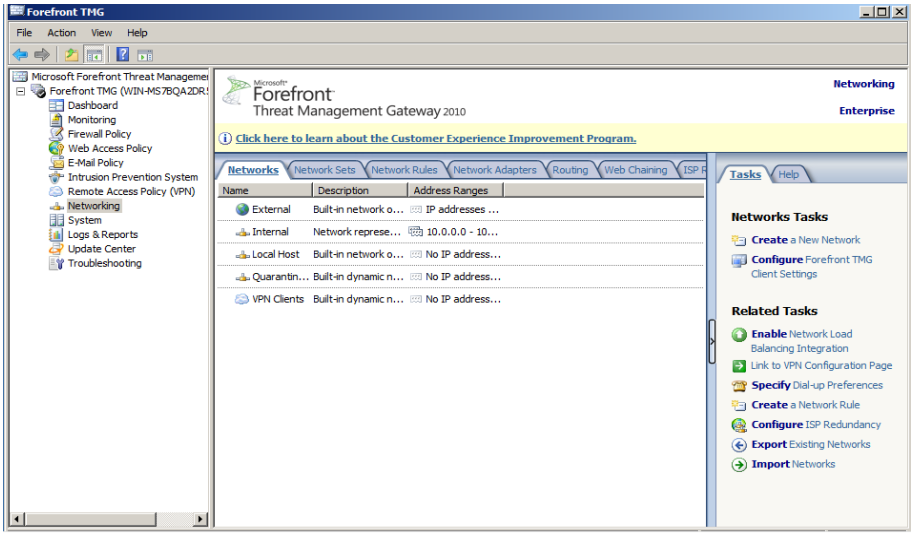


Figure V.12: les 5 réseaux de TMG

5. La création des règles d'accés :

Le Forefront TMG interdit par défaut tout le trafic entrant et sortant sur tous les réseaux (internes, externes et locaux). La première et seul règle qui existe par défaut au niveau du serveur TMG est celle qui dit que tout le trafic est refusé depuis tous les réseaux vers tous les réseaux, donc il faut autoriser les trafics supplémentaires.

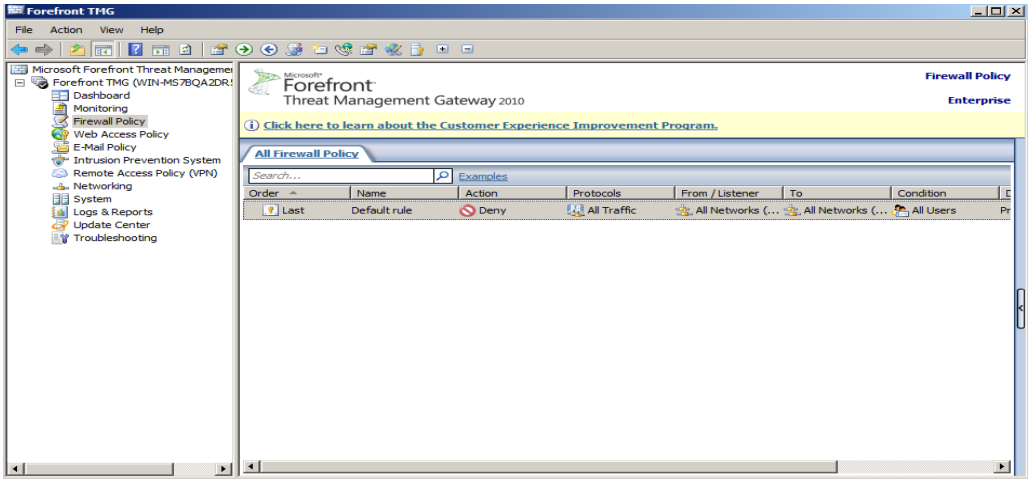


Figure V.13: la première règle excite dans TMG par défaut

Nous avons autorisé les règles, DNS, HTTP /HTTPS, SMTP en spécifiant, pour chacun d'eux le réseau interne, et la destination et les utilisateurs sur les quels elles seront appliquées. Dans la machine TMG1 on crée les règles suivantes : la règle DNS qui permet de spécifier un ordinateur sur le quel elle s'applique, et la règle HTTP, HTTPS. Et afin nous créons une règle pour empêcher l'accès au site www.facebook.com.

Dans la machine TMG2 on crée la règle SMTP

- **Création de la règle DNS**

Pour la création de la règle d'accès DNS, Firewall Policy -> entrons le nom DNS.

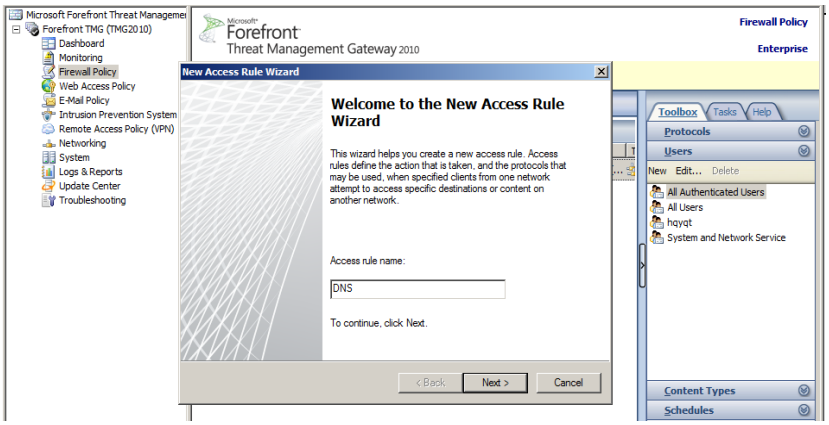


Figure V.14 : création de la règle d'accès DNS.

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

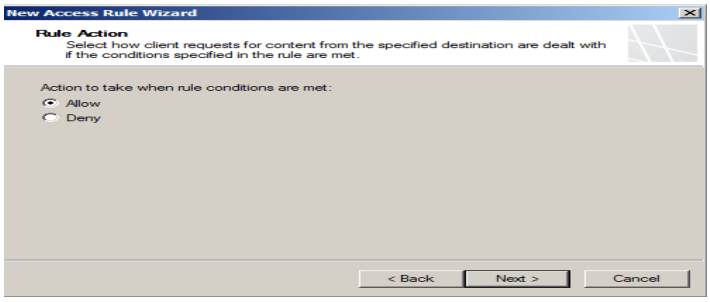


Figure V.15: Choix de l'action de la règle.

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

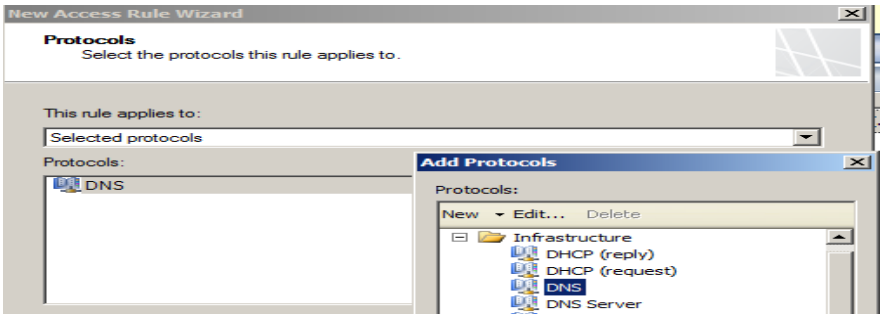


Figure V.16: Sélection des protocoles.

Cette règle s'appliquant sur le serveur DNS, **domaine.www.tmg.com**, dans l'ajout des entités réseau, nous sélectionnons ce serveur avec son adresse IP (11.0.0.0.1) comme source de règle d'accès.

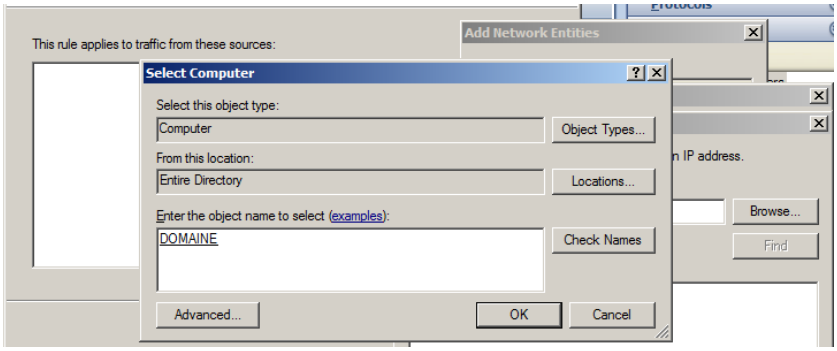


Figure V.17: Chercher la machine DOMAINE

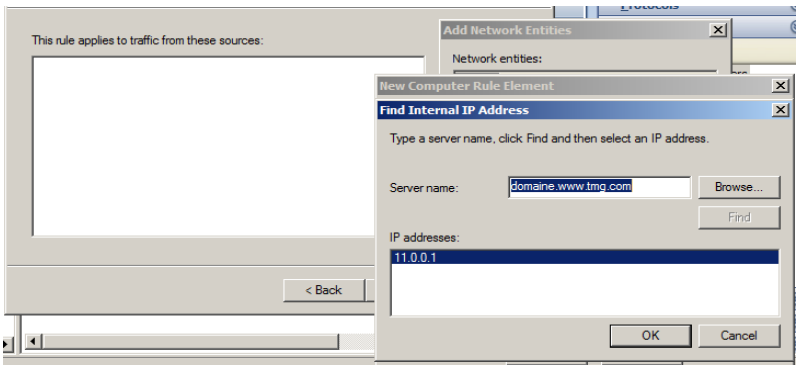


Figure V.18: ajouter la machine domaine.www .tmg.com et son adresse dans TMG

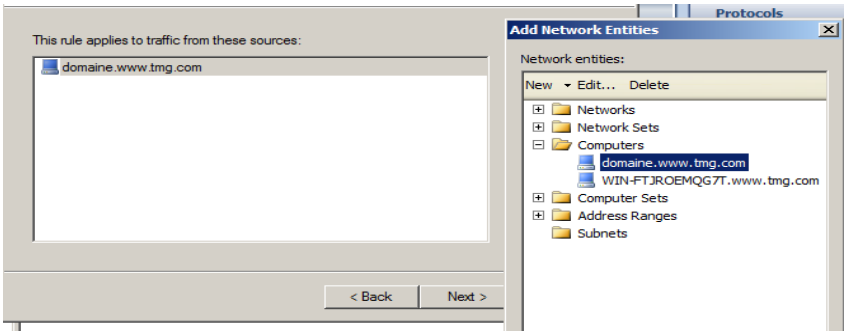


Figure V.19: Sélection de la source de règle d'accès.

Le trafic destinataire étant le réseau local séléctionnons l'hote local.

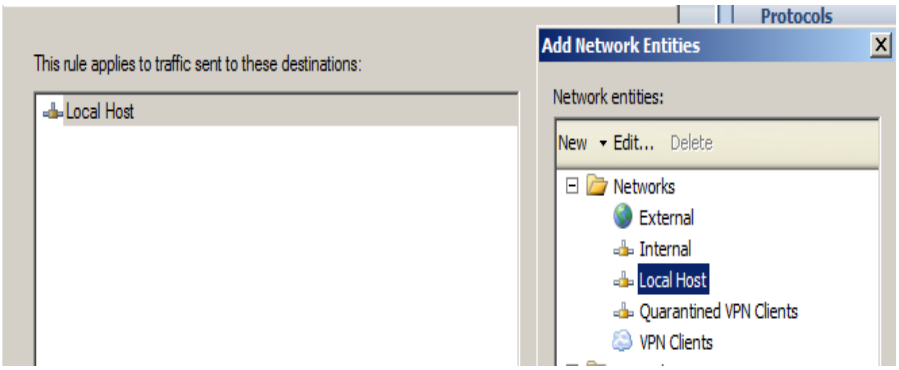


Figure V.20: Spécification de la destination de la règle d'accès.

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

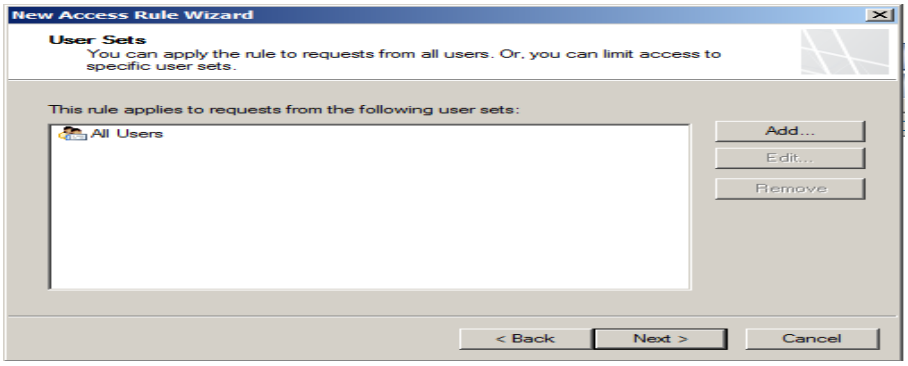


Figure V.21: Ensemble des utilisateurs concernés par la règle d'accès.

- **Création de la règle HTTP, HTTPS :**

Cette règle d'accès permet aux ordinateurs du réseau interne de se connecter à Internet a travers le protocole http, https depuis le réseau local.

Test avant la création de la règle :

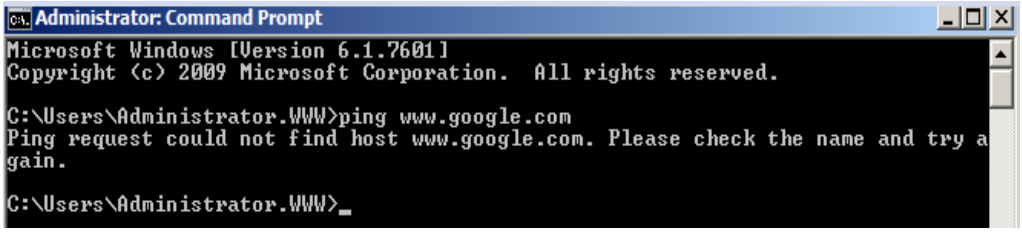


Figure V.22: test avant de crée la règle d'accès

Pour la création de la règle d'accès HTTP, HTTPS Firewall Policy -> entrons le nom HTTP, HTTPS.

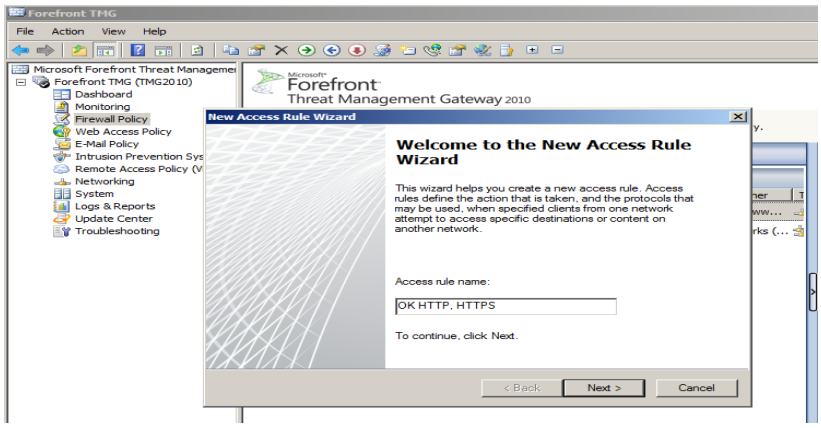


Figure V.23: création de la règle d'accès HTTP, HTTPS.

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

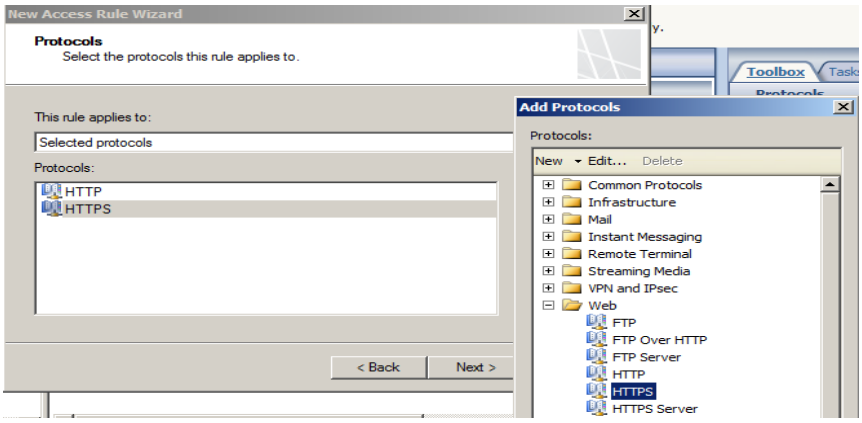


Figure V.24: Sélection des protocoles.

Le trafic source étant le réseau interne séléctionnons Internal.

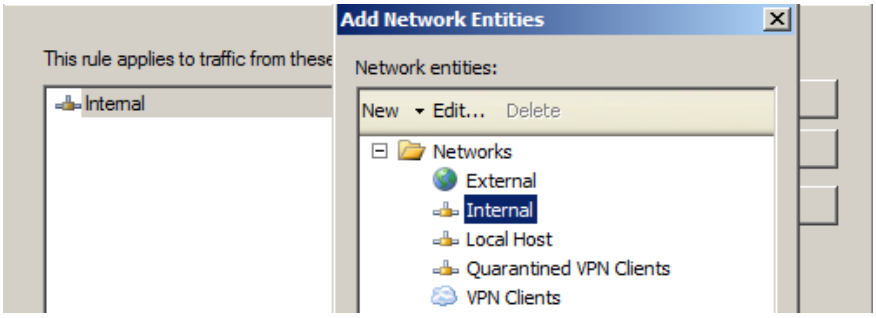


Figure V.25: Sélection de la source de règle d'accès.

Le trafic destinataire étant le réseau externe (Internet) séléctionnons External.

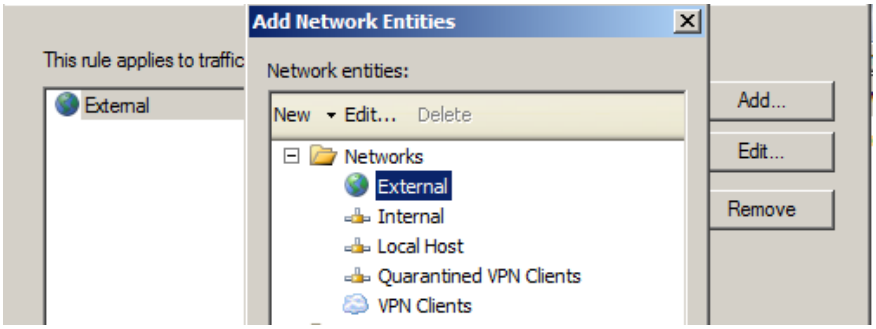


Figure V.26: Spécification de la destination de la règle d'accès

Test après la création de la règle.

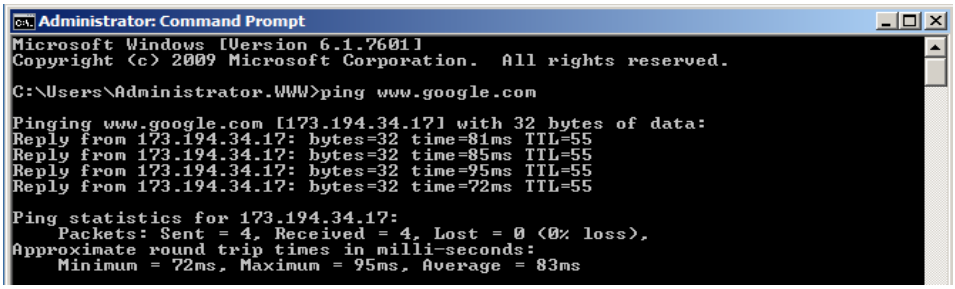


Figure V.27: Teste de ping réussie

- **Création de la règle pour empêcher l'accès à site www.facebook.com:**

Dans ajout des protocoles nous spécifions sur quels protocoles s'applique cette règle « Refuse Facebook ».

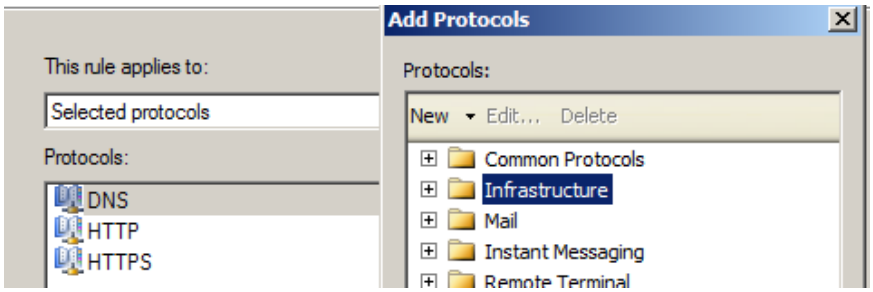


Figure V.28: Sélection des protocoles.

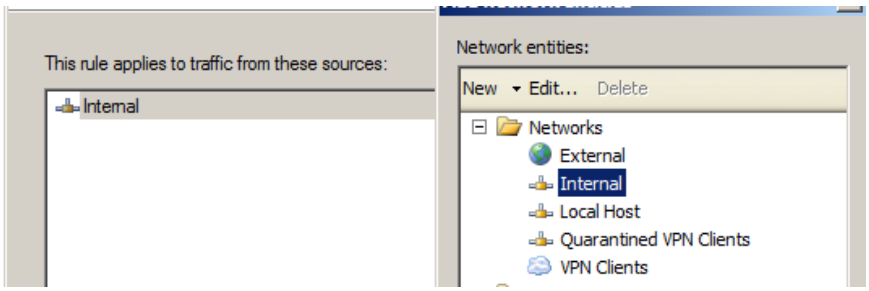


Figure V.29 : Sélection la source de la règle.

On définie le nom de site a refusé www.facebook.com et d'ajouter les URL incluent dans ce site (http://*.facebook.com, http://www.facebook.*/).

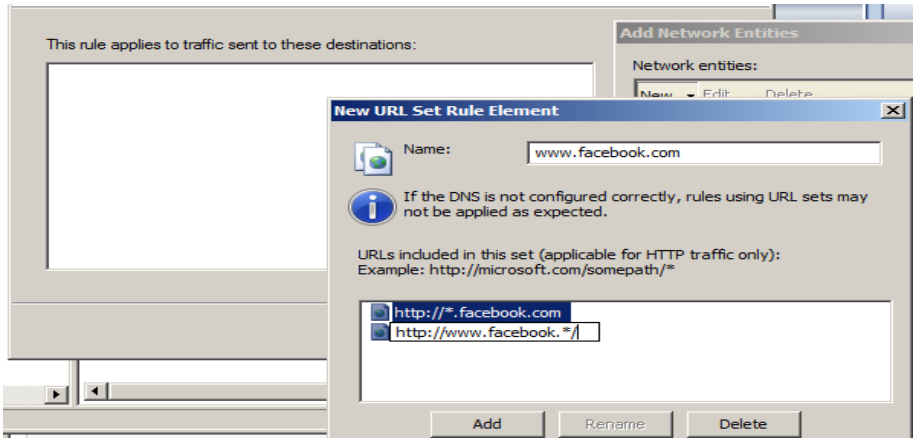


Figure V.30: création de site a refusé.

Ajouter le site refusé comme une destination dans cette règle (refuse Facebook)

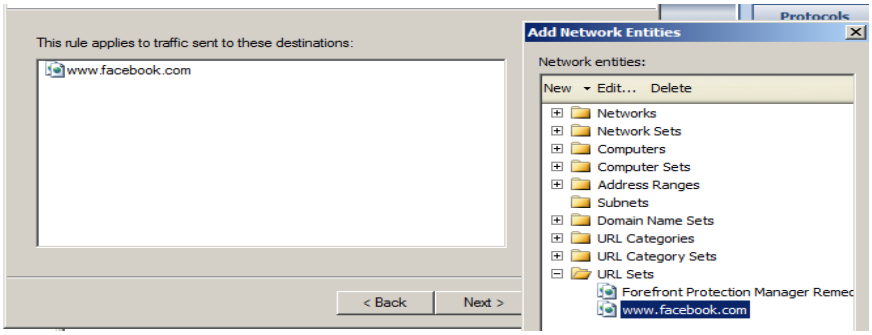


Figure V.31 : Spécification de la destination de la règle d'accès refusé.

Afin de valider et enregistrer toute modification apportée à la TMG, nous cliquons sur Appliquer.

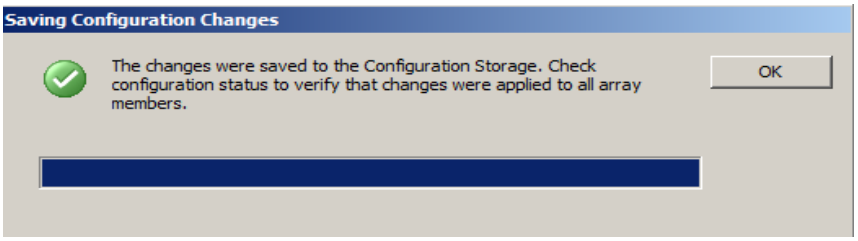


Figure V.32: Enregistrement des modifications.

Le récapitulatif des règles TMG1 configurées est montré sur la figure ci-dessous :

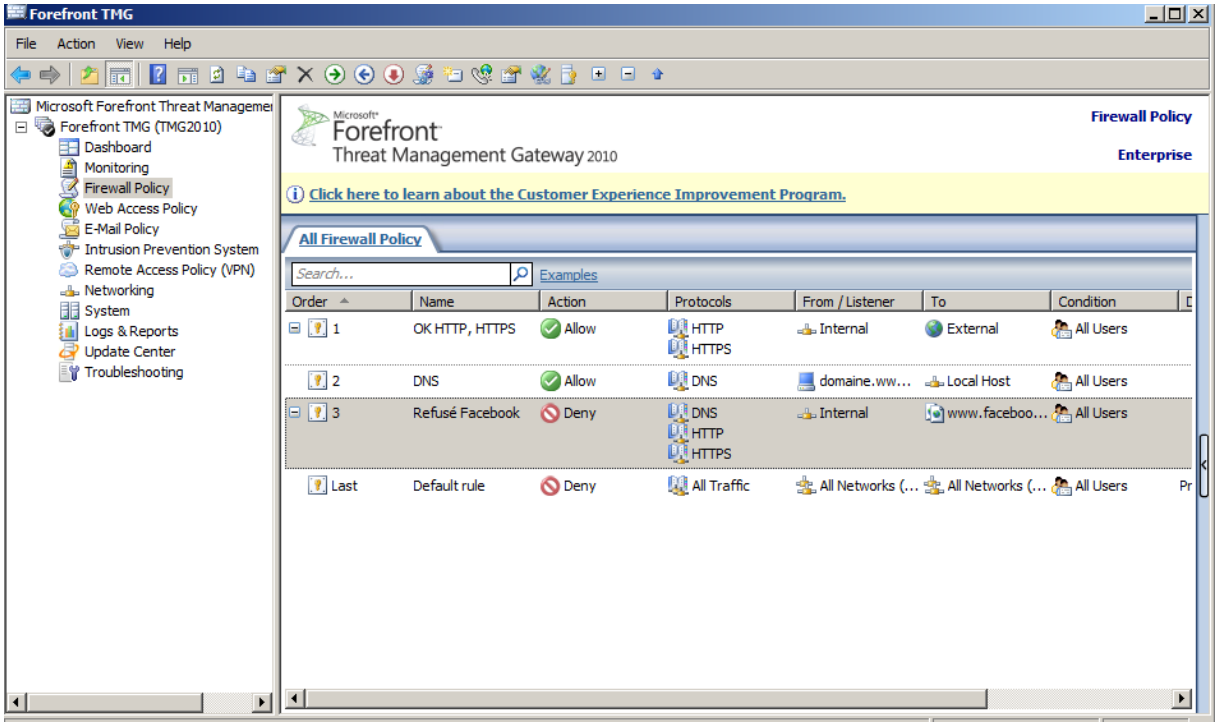


Figure V.33: Récapitulatif des règles TMG.

- **Configuration LDAP (Lightweight Directory Access Protocol):**

Les annuaires LDAP se situent au cœur des fonctions de communication et de collaboration de l'entreprise à travers son Intranet car ils en simplifient la gestion et l'administration. La mise en œuvre d'un annuaire LDAP au sein d'un Intranet apporte donc une gestion optimale des utilisateurs et de leurs profils, des ressources, et la possibilité de partager.

Le principal avantage du protocole LDAP réside dans la possibilité de réunir les informations concernant toute une organisation dans un lieu central. Par exemple, plutôt que de gérer des listes d'utilisateurs pour chaque groupe au sein d'une organisation, LDAP peut être utilisé comme un répertoire central accessible sur tout le réseau. De plus, puisque LDAP prend en charge les fonctions Secure Sockets Layer (SSL) et Transport Layer Security (TLS), des données confidentielles peuvent être protégées contre toute intrusion.

Dans cette partie nous avons fait la configuration au niveau d'actif directory et au niveau de TMG1 (Pour ouvrir la connexion entre TMG1 et AD).

Etape 1: Au niveau Active directory :

Pour que TMG1 connecte à LDAP, Dans la machine AD→ outils administrateur→ ADSI Edit→ Connecte to→ CN-Windows NT → CN-Directory service→ Propriété → Sélectionner le type de basse de données AD (configuration)

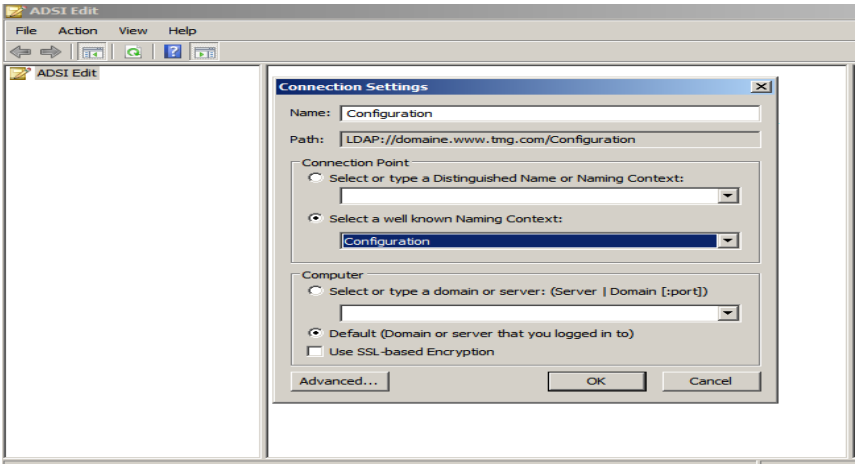


Figure V.34: sélectionner le type de BDD d'Active Directory

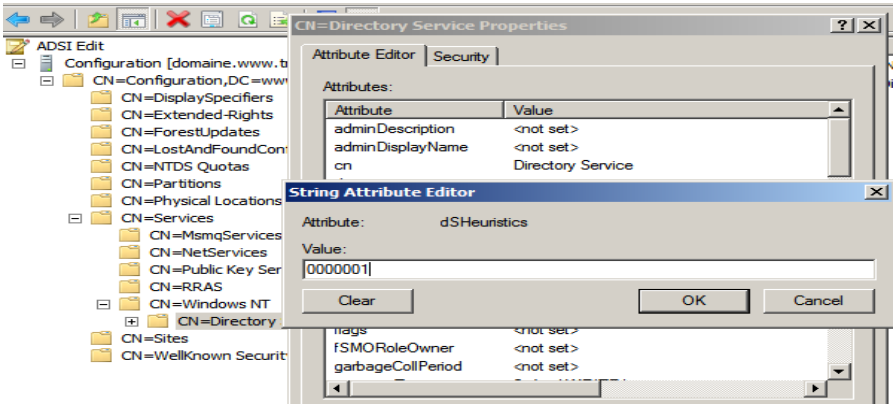


Figure V.35: configure l'attribut dSHeuristics

Ajouter le groupe d'utilisateur de type « ANONYMOUS LOGON » dans ADSI et active directory user and computer, C'est-à-dire tout les personnes qui incluent dans le contrôleur de domaine

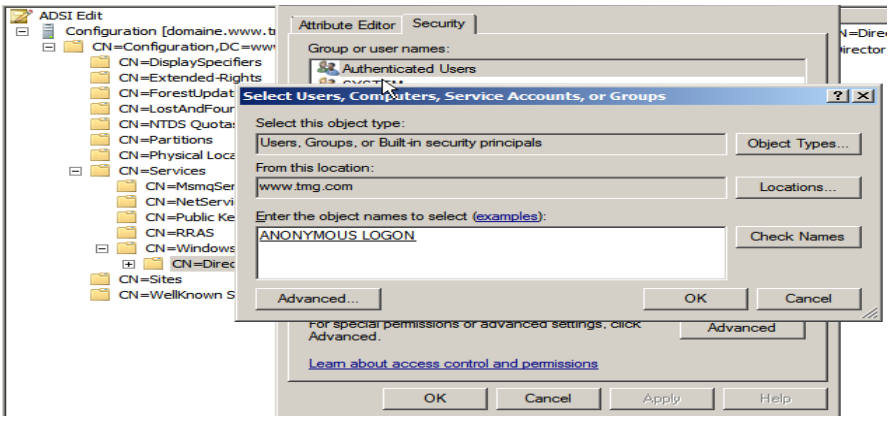


Figure V.36: Ajouter groupe ou le nom d'utilisateur

Etape 2: Au niveau TMG1

Pour configure le serveur LDAP au niveau TMG1.(ce résume en deux action).

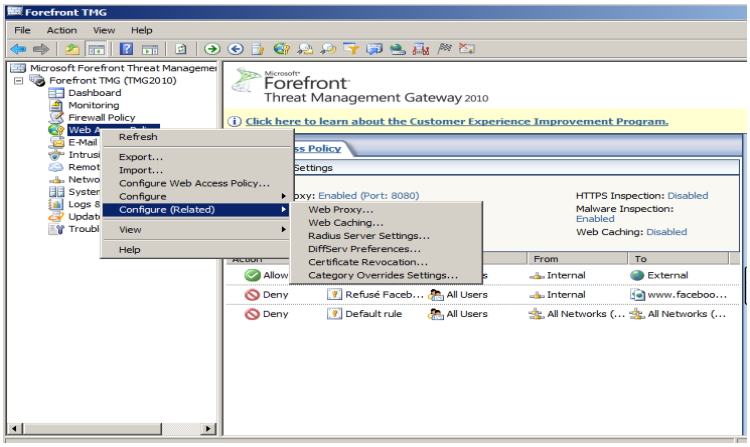


Figure V.37: l'emplacement LDAP dans TMG1

La première action à faire dans TMG1 est de donner le nom pour le serveur LDAP (c'est le nom de la machine contrôleur de domaine), « **domaine.www.tmg.com** », le nom de domaine « **www .tmg.com** », et donner le nom et le mot de passe qu'il va données l'autorisation d'entré dans l'active directory comme montre le figure suivant :

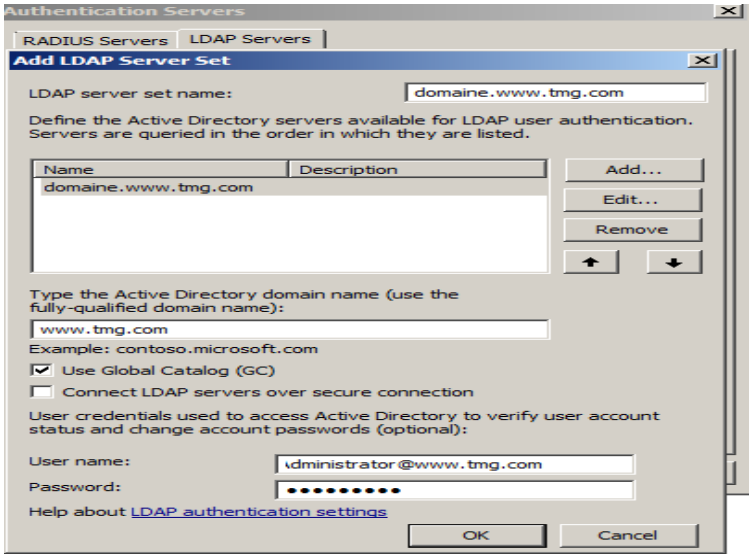


Figure V.38: configuration de serveur LDAP

La deuxième action est d'ajoute les utilisateurs dans le serveur LDAP comme suit :

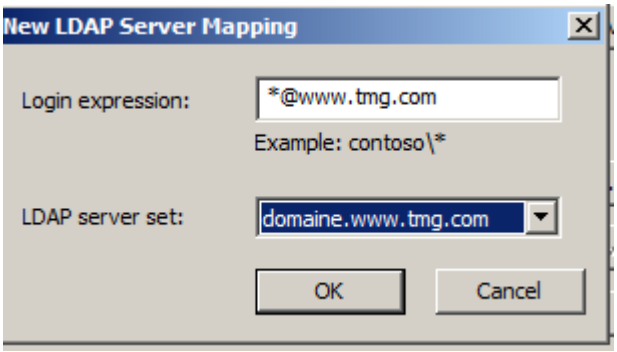


Figure V.39: la première catégorie d'utilisateur

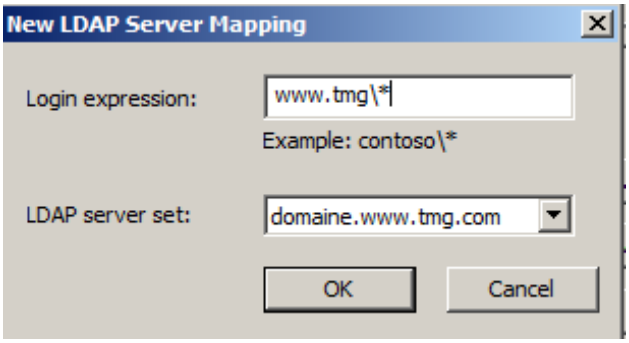


Figure V.40: la deuxième catégorie d'utilisateur

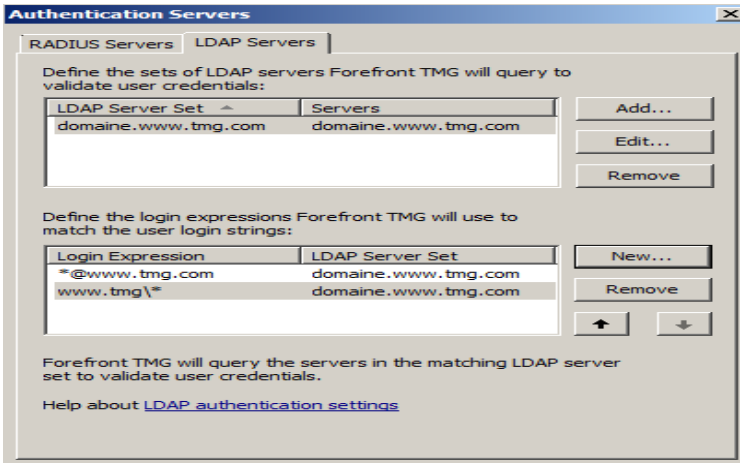


Figure V.41: résume les deux actions

Ces deux étapes assurent la connectivité entre TMG1 et l'Active Directory.

Après ces étapes la connexion entre TMG1 et Active directory est ouvert. Pour vérifier cette connexion on créons des nouveaux connections de vérification dans TMG1 comme suite : Monitoring (surveillance)→vérifier les connectivites→création nouveau connexion de vérification→nommé cette connexion «LDAP »→ donner l'adresse IP de l'active directory (11.0.0.1) et le type de service.

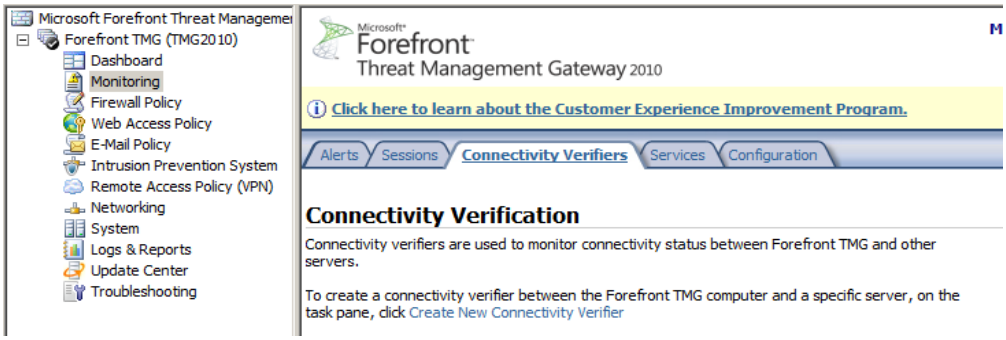


Figure V.42: création une connections de vérification

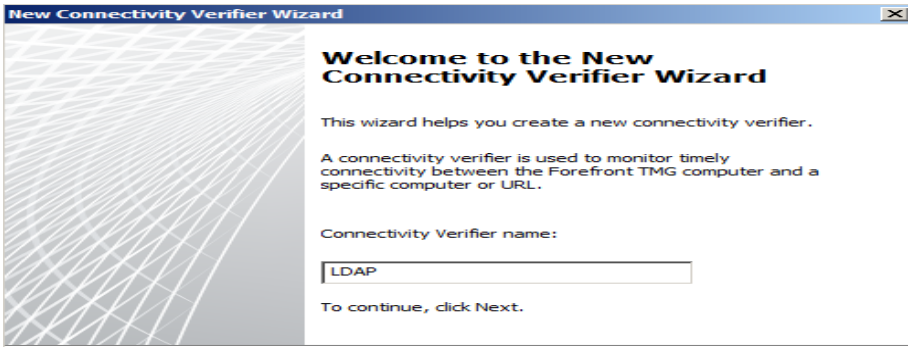


Figure V.43: le nom de la connexion

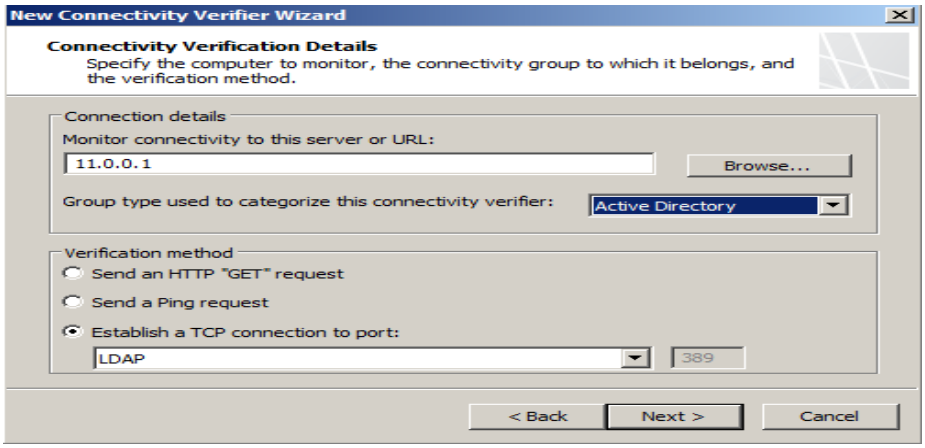


Figure V.44: Le nom et la catégorie de connexion

Pour vérifier que LDAP fonctionner entre TMG1 et Active directory on ajouter des utilisateurs et des groupes dans l'Active Directory et on va joindre ses utilisateurs dans la TMG1.

Dans le domaine nommé « www.tmg.com » on a créé une unité d'organisation nommé «**tmg** » dont on a produire Deux utilisateurs « **Mameri Nouara, Ait Amar Hayat** » et un groupe nommé « **Réseau** ».

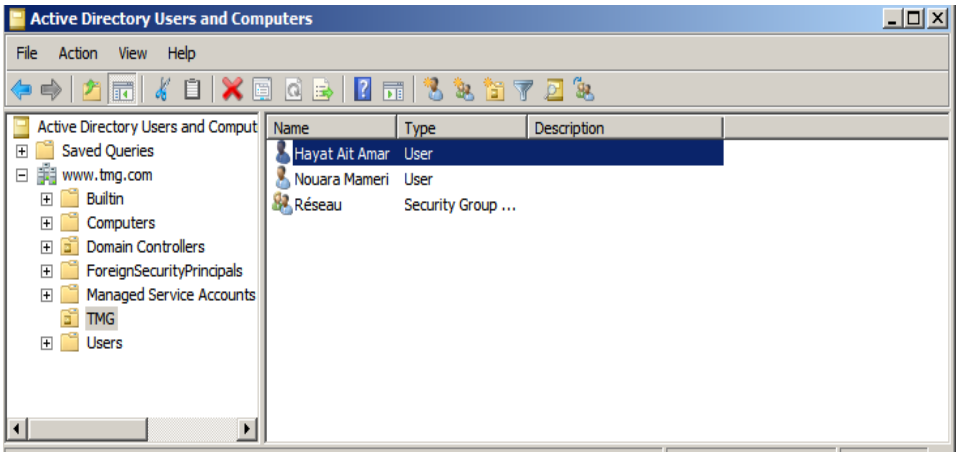


Figure V.45: Utilisateur et ordinateur Active Directory

Pour joindre les utilisateurs à partir de TMG1 on crée nouvel utilisateur nommé LDAP comme suit :

Figure V.46: création nouvel utilisateur

Sélectionner le type **LDAP** comme un utilisateur établi

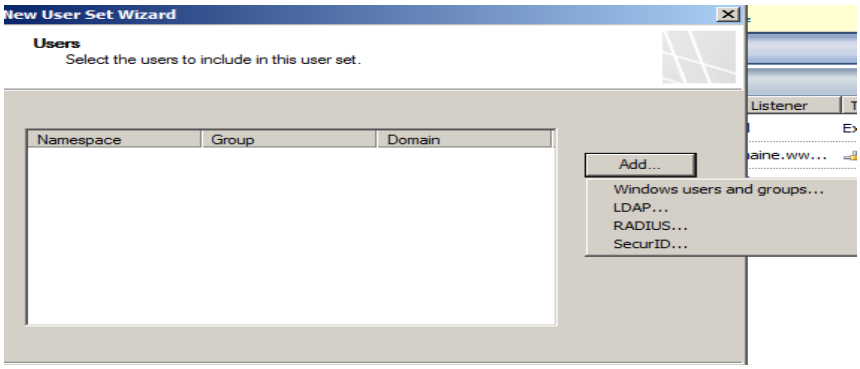


Figure V.47: Sélectionner le type d'utilisateur

La fenêtre de dialogue suivante donner le nom et le mot de passe « **Administrator@www.tmg.com, Passw0rd**» qu'elle accorder l'accès au serveur LDAP dans L'active directory

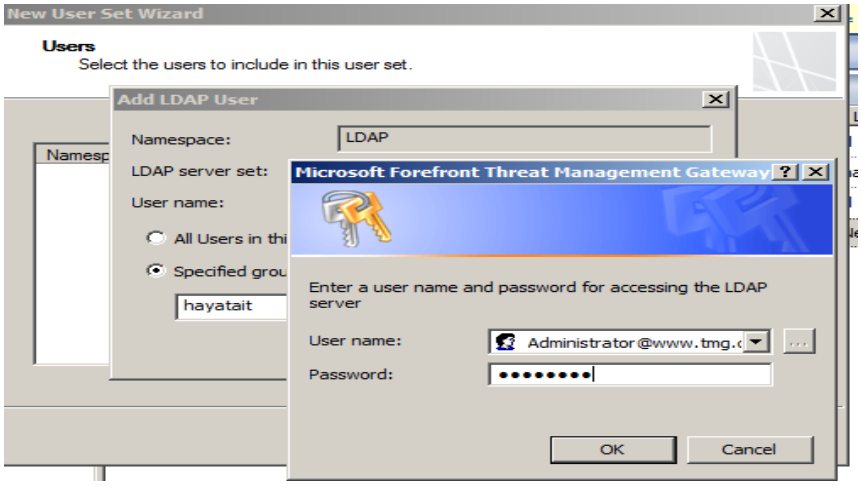


Figure V.48: L'accès à l'Active Directory

Ajouter automatiques les utilisateurs qui incluent dans l'Active directory

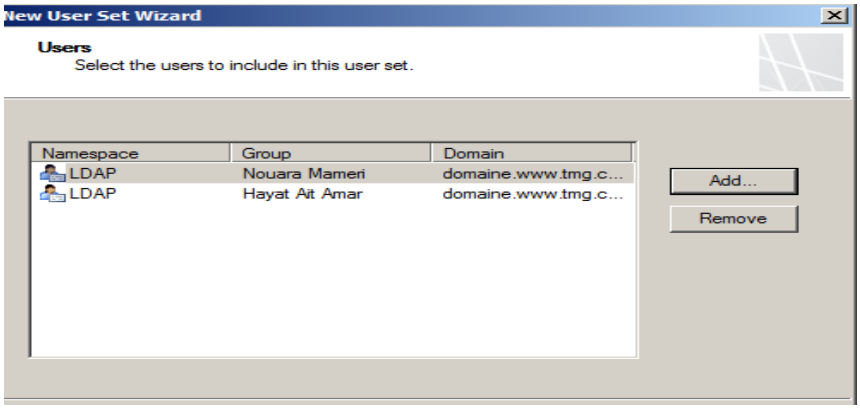
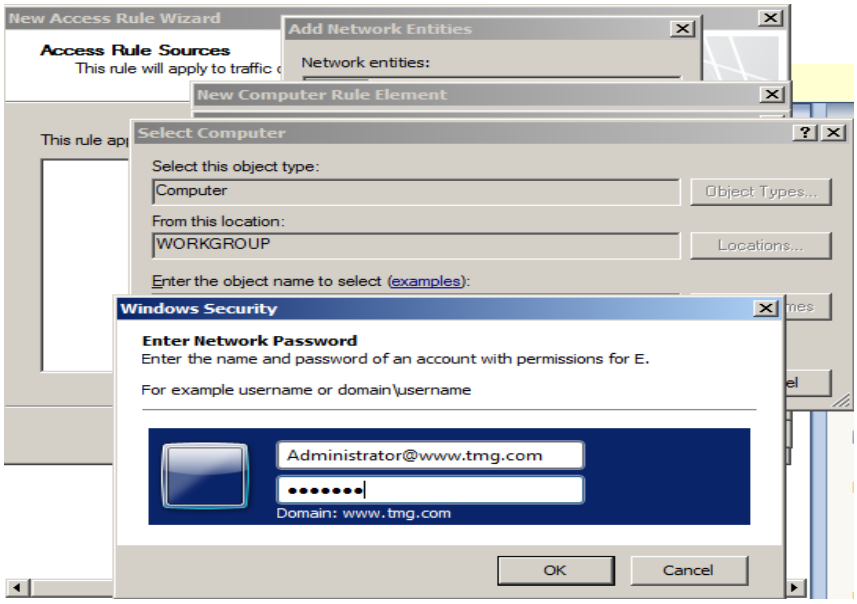


Figure V.49: les résultats de LDAP

- **Création de la règle SMTP :**

Dans notre application, on s'intéresse aux règles de publication de ce dernier en toute sécurité avec le Forefront TMG. Et pour cela on crée une règle dont on configure les accès sur le Forefront TMG server afin que le serveur Exchange SMTP puis envoyer des messages sur internet et de l'autre coté les recevoir depuis internet.

Etape1: on crée un nouvel objet de type ordinateur on lui effectue le nom « **Exchange.www.tmg.com »,** une adresse IP et une description comme le montre la figure suivant :



Etape2 : ajouter la machine Exchange dans une zone DMZ (les deux machine aient même carte réseau).

Pour exécuter cette étape avec succès, on crée nouveau réseau dans TMG2 comme suite :

News Network, donné le nom de réseau « DMZ », ajouter son carte réseau « DMZ (192.168.0.10) »

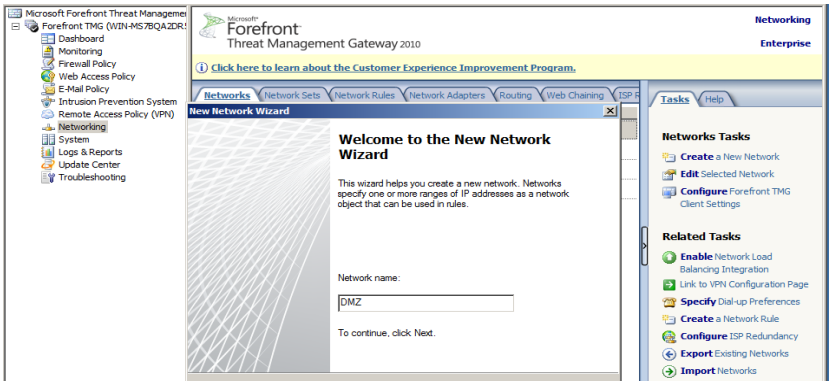


Figure V.50: création de réseau DMZ

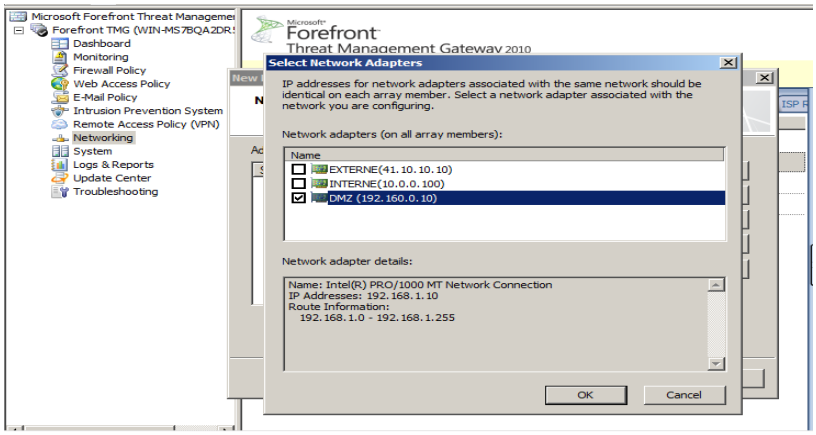


Figure V.51: sélectionner la carte réseau DMZ

Afin de valider et enregistrer toute modification apportée à la TMG2, nous cliquons sur Appliquer.

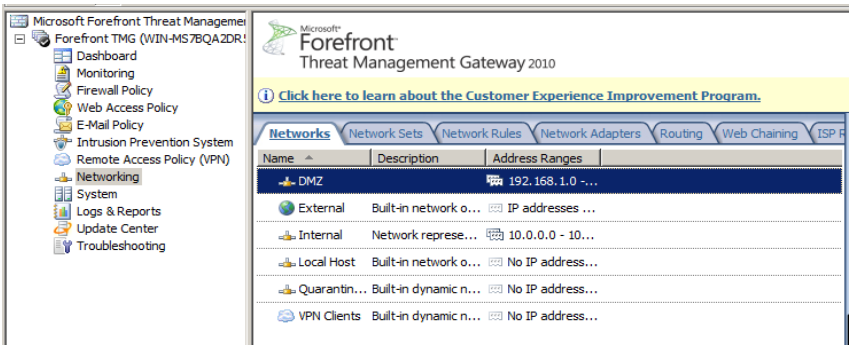


Figure V.52: résultat de création de réseau DMZ

Maintenant on va créer la première règle qui permet à TMG2 server d'envoyer des messages SMTP du réseau DMZ vers l'Internet (réseau externe).

Cette règle est une règle de sortie (règle d'accès) qui porte le nom « OK SMTP », elle autorise un trafic qu'on sélectionne en cliquant sur ajouter et dans les protocoles commun on sélectionne le protocole SMTP.

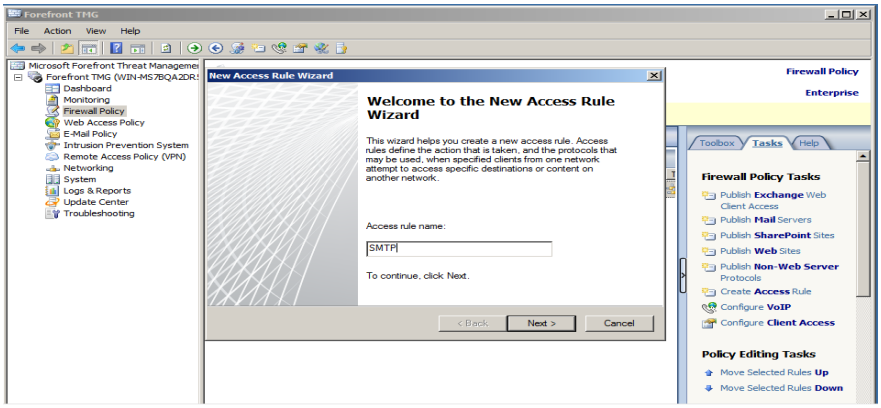


Figure V.53: Création de la règle SMTP

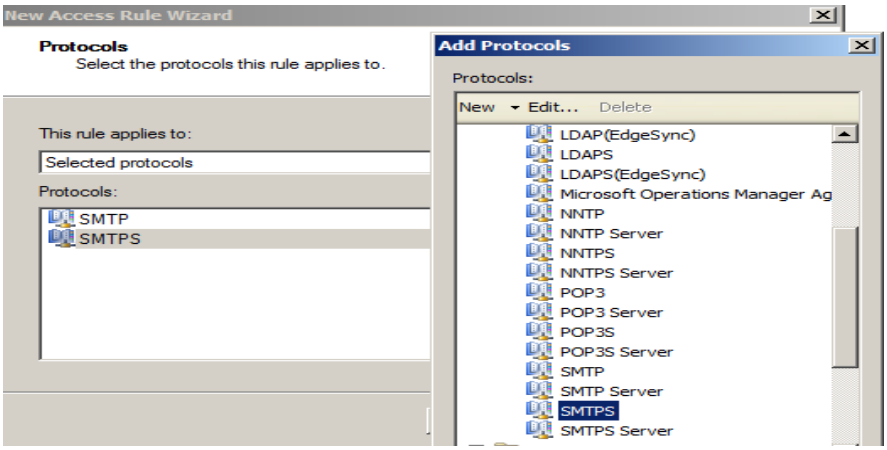


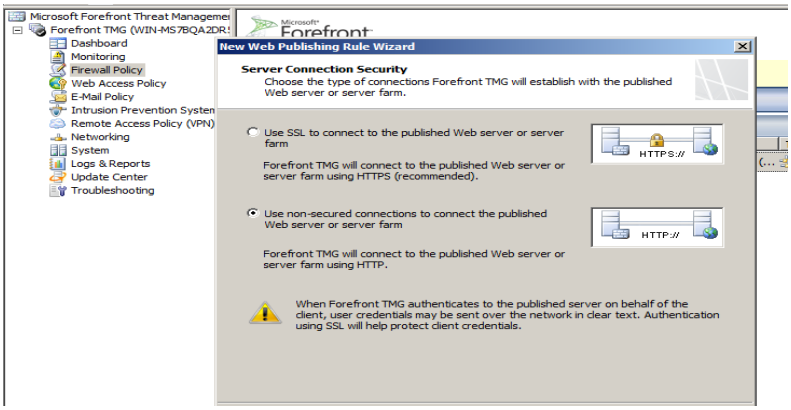
Figure V.54: Sélectionner les protocoles de la règle

La création de la première règle est réalisée et on passe maintenant à la création de la deuxième règle.

- **Création de la règle de publication du serveur Exchange :**

Pour créer cette règle on ouvre la console de gestion TMG2 et dans Le Firewall Policy, bouton droit on sélectionne une nouvelle règle de publication de serveur de courrier.

- **Création de la règle de publication du serveur Web :**



Etape V : La publication des serveurs Web et messagerie

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

1. Installation de l'Autorité de Certification

Les différentes étapes d'installation de l'autorité certificat sont définies dans l'annexe 2**.**

A la fin de cette installation, création de l'autorité **tmg-certificat-CA**, en 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). Le certificat étant auto-signé, il est réputé comme n'étant pas de confiance car il provoque constamment des erreurs de validation SSL lors des différents accès au serveur. L'étape suivante consiste à la demande de création de certificat, certifiée par notre CA.

2. Demande de certificat

Après avoir créé le modèle de certificat, nous générons des certificats en effectuant une demande comme suit : certificats de serveur -> créer une demande de certificat. Sur la page qui s'affiche nous remplissons les informations de sorte à être précis car plus les informations sont précises plus les personnes détenant le certificat seront rassurées de sa provenance.

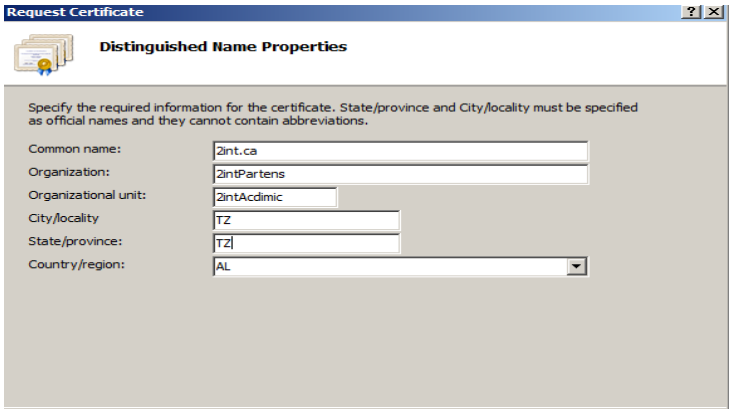


Figure V.55 : Demande de certificat.

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

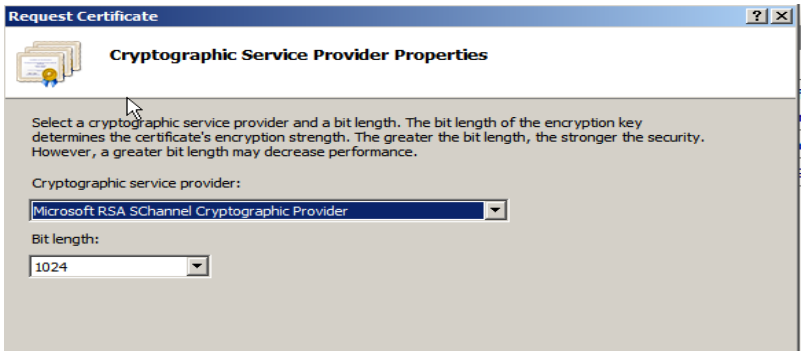


Figure V.56: Propriétés du fournisseur de services de chiffrement.

Ensuite, nous spécifions l'emplacement du fichier d'exportation du certificat.

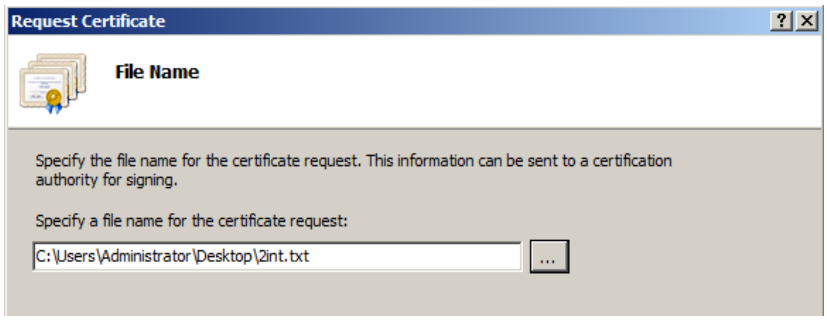


Figure V.57: Fichier de demande de certificat.

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

Figure V.58: 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 suit :

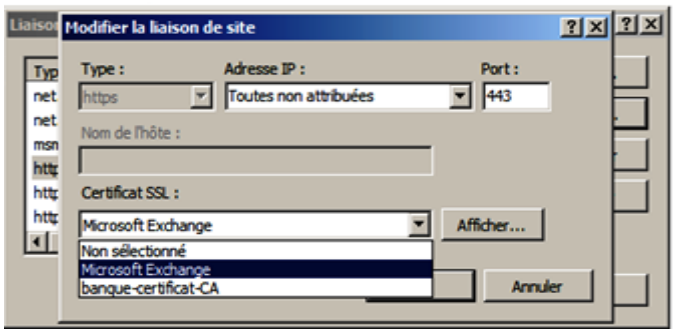


Figure V.59: Liaison avec HTTPS.

Pour soumettre la demande de certificat via internet explore suivant ces étapes : **https://Exchange/certsrv** -> demande de certificat -> demande de certificat avancée-> soumettez une demande en utilisant un fichier

PKCs#7 codé en base 64. Dans la page ouvrante collons la clé privée obtenue et spécifions le modèle de certificat, Serveur Web.

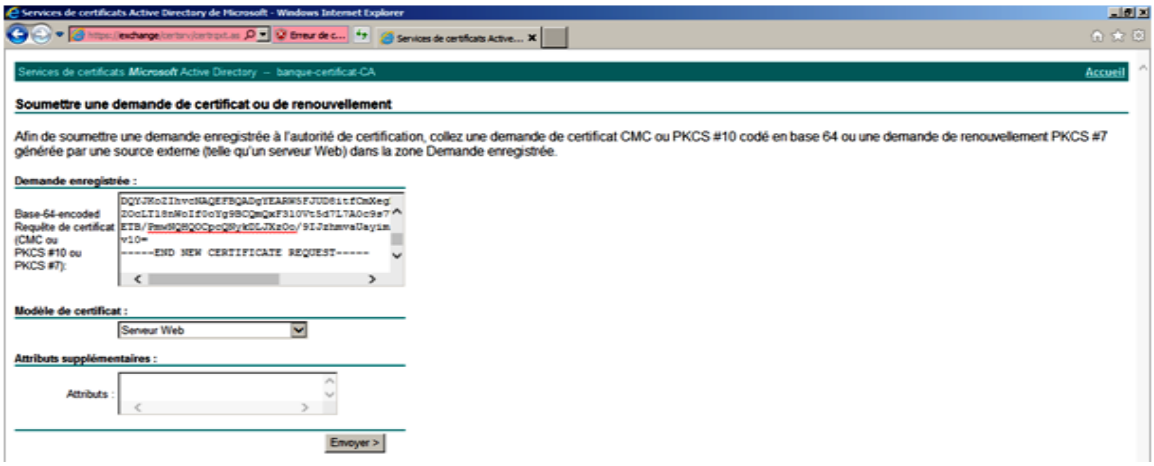


Figure V.60: Soumettre une demande de certificat.

Téléchargeons le certificat en spécifiant son emplacement.

Conclusion :

La connexion de réseau et d'utilisateur à internet soulève des questions de sécurité et rapide, exploitant les puissantes fonctions de gestion de Windows 2008. Il apporte aux entreprises des capacités complètes de contrôles d'accès et de surveillance d'utilisation comme il protège les réseaux contre les accès frauduleux, inspecte le trafic et alerte les administrateurs en cas d'attaques.

Les organisations qui souhaitent ouvrir leurs réseaux à internet doivent considérer TMG Server comme composant stratégique de leur infrastructure de communication.

Conclusion générale

La sécurité du système d'information d'une entreprise est un requis important pour la poursuite de ses activités. Qu'il s'agisse du vol de ses secrets de fabrication ou de la perte de ses données clients, et ca nous a ramené de la nécessité de garantir certains besoins de sécurisation : l'intégrité et la confidentialité des données transmises, l'authentification des utilisateurs, ainsi que la non répudiation des actes.

Dans notre mémoire nous sommes intéressés à l'installation et la configuration du pare-feu TMG server dans le but de faire faces aux différents actes de malveillance dont la nature et la méthode d'intrusions sont sans cesse changeantes.

Le Forefront TMG Server propose un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécuriser et de gérer le trafic réseau.

Ce projet nous a permis d'acquérir des connaissances dans de nombreux domaines. En effet, il nous a initiés au monde de la recherche sur les réseaux surtout en ce qui concerne la sécurité. Il nous a également permis de découvrir le logiciel de simulation VMware Workstation, Windows server 2008, service d'annuaire Active Directory et Microsoft Exchange 2010.

Dans les grande entreprise le Forefront TMG seul reste insuffisant pour garantir la sécurité de ses ressources, alors il est nécessaire de l'inclure dans une démarche qui prendre en compte d'autre paramètres tel que des pare-feux matériels, des antis virus ainsi des mises à jour de leurs applications.

Annexe

2.1 Installation de serveur Web IIS

Le serveur Web IIS fournit une infrastructure d'application web fiable et gérable et évolutive, pour l'ajouter comme fonctionnalité sous le contrôleur de domaine principal, aller au menu démarrer -> outil d'administration -> gestionnaire de serveur, et l'ajouter comme rôle, les figures suivantes illustrent la procédure.

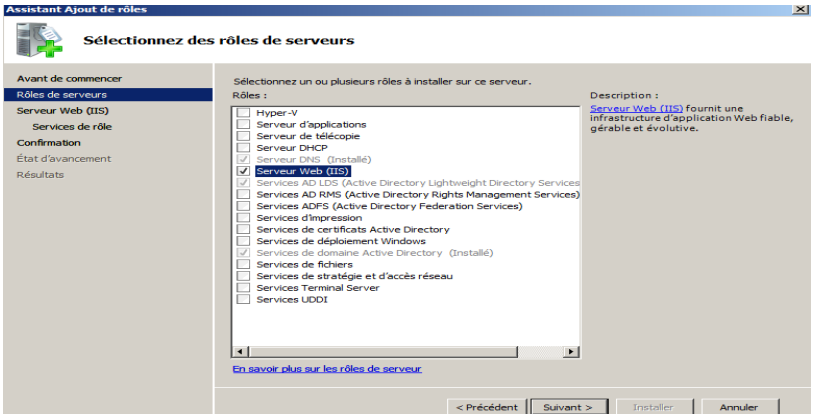


Figure 2.1: Illustration 1.

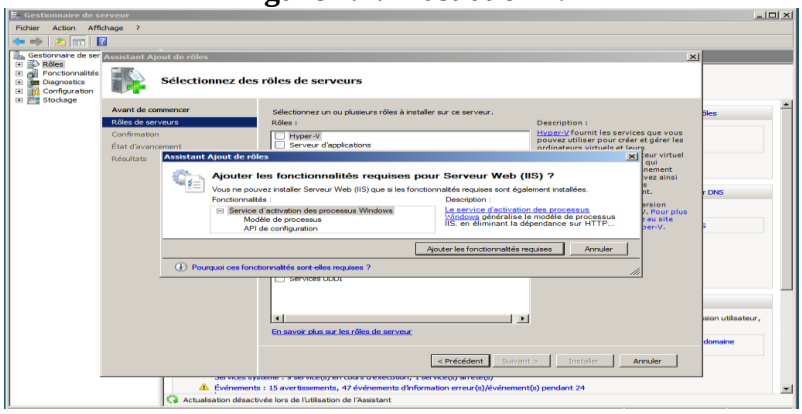


Figure 2.2: Illustration 2.

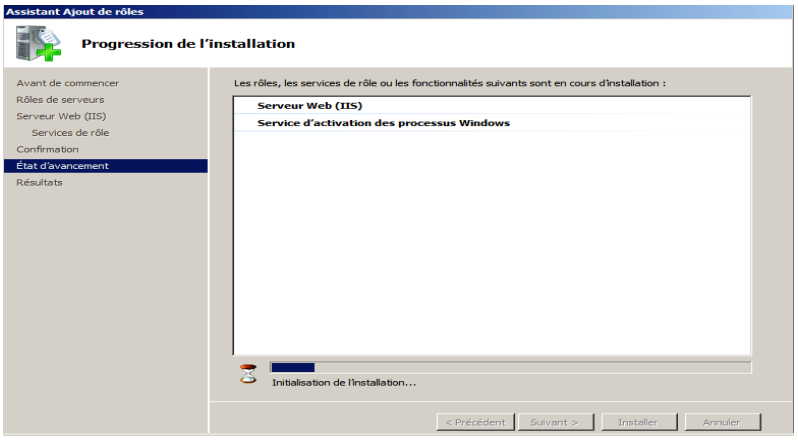


Figure 2.3: Illustration 3.

2.2 Installation de Microsoft Exchange Server 2010

L'installation du serveur de messagerie Exchange exige des pré-requis.

1. Installation des pré-requis et préparation d'Active Directory

Microsoft exchange 2010 nécessite un Active Directory de niveau fonctionnel 2003 au minimum pour fonctionner. Pour vérifier et installer les pré-requis nous avons le choix de les ajouter au serveur via le gestionnaire de serveur ou bien comme nous l'avons fait via l'interpréteur de commande PowerShell.

✓ **Via le PowerShell:**

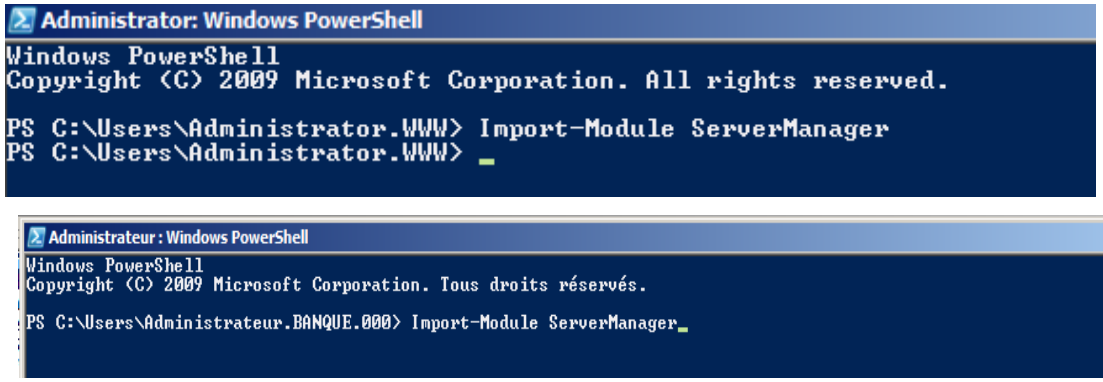


Figure V.20: L'importation des modules de gestionnaire de serveur.

Figure V.21: L'ajout des modules.

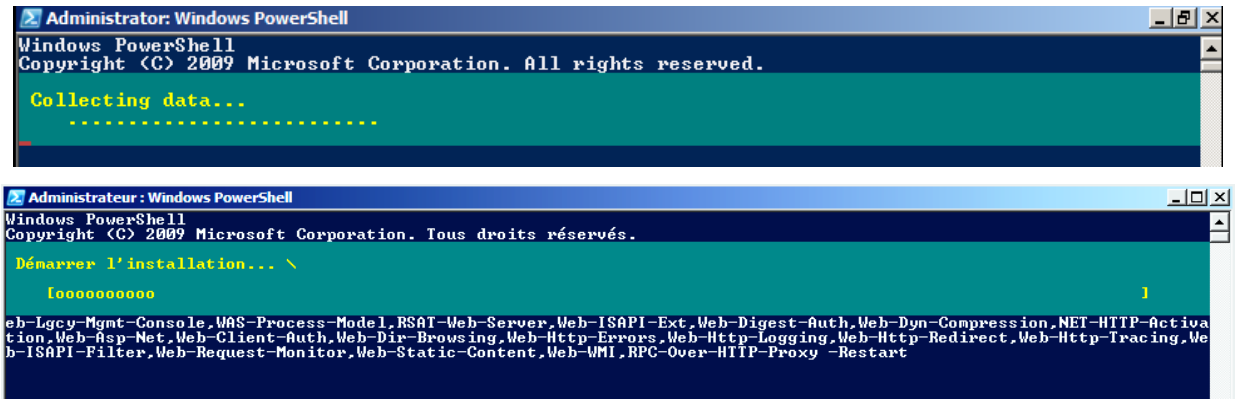


Figure V.22: Installation des pré-requis.

Après un redémarrage de l'ordinateur à la fin de l'installation des fonctionnalités, il faut changer le mode de démarrage du service de partage de ports net.TCP, afin de le passer en mode automatique.

✓ **Via le PowerShell:**

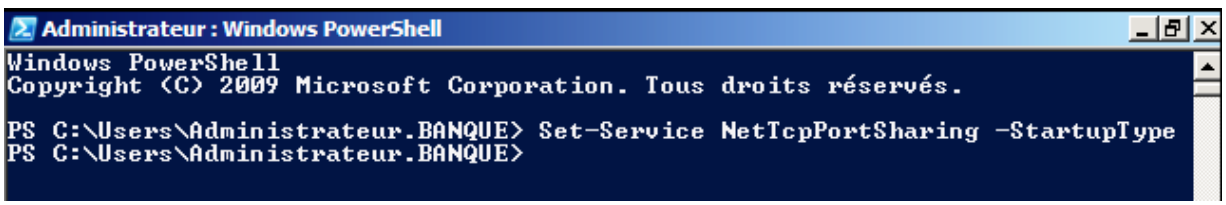


Figure V.23: Le passage au mode automatique.

Nous allons maintenant commencer à préparer l'Active Directory pour installer Exchange Server 2010. 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. Cette partie se déroule en trois étapes :

1. La première étape consiste à préparer le schéma d'Active Directory.

Command: C:\>Setup /PrepareSchema.

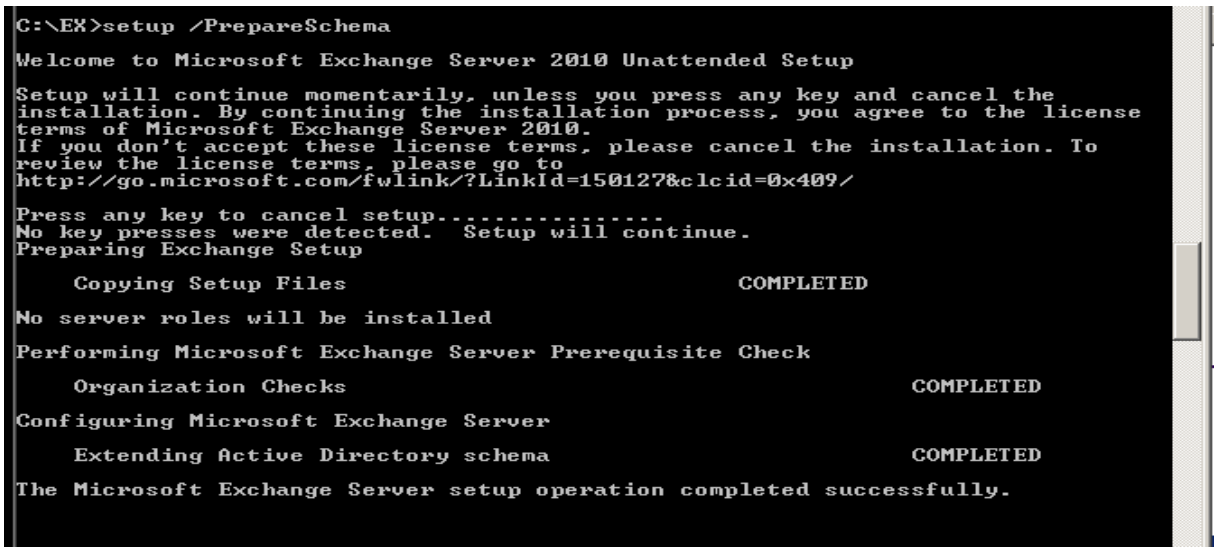


Figure V.24 : Préparation de schéma Active Directory.

2. La seconde étape consiste à préparer la forêt www.tmg.com

Command: C:\>Setup /PrepareAD /OrganizationName:2int.

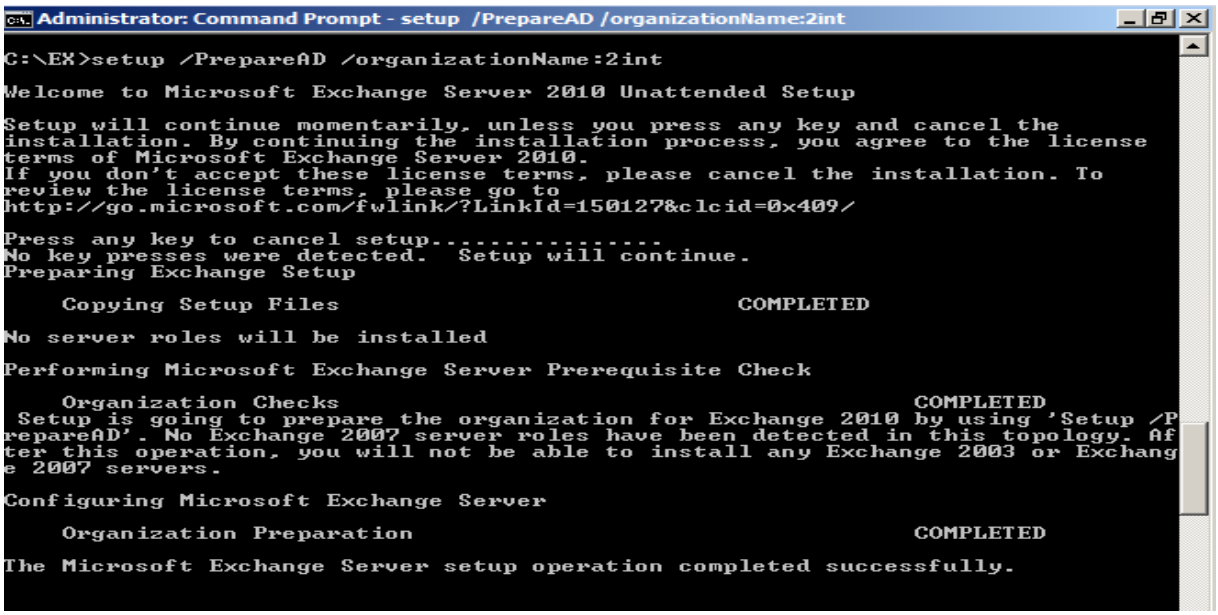
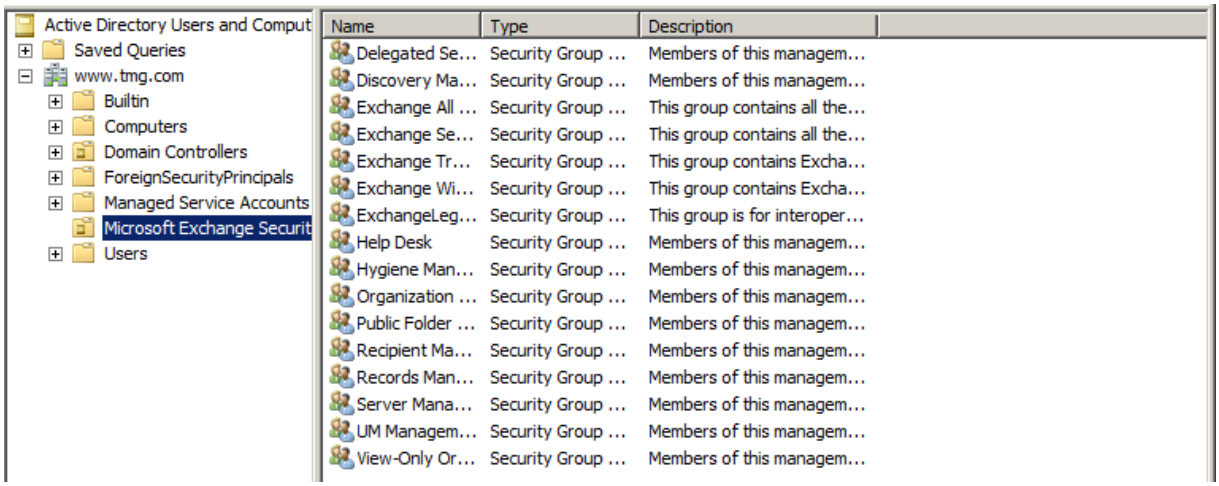


Figure V.25: Préparation de la forêt.

Vérifiez ensuite que la commande s'est bien déroulée. Pour cela ouvrez la console AD sur votre serveur et vérifiez la création de l'OU « **Microsoft Exchange Security Groups** » avec les groupes de sécurités suivantes :



3. La dernière étape nous permet de préparer le domaine.

Commande : C:\>Setup /PrepareDomain.

```
C:\EX>setup /PrepareDomain

Welcome to Microsoft Exchange Server 2010 Unattended Setup

Setup will continue momentarily, unless you press any key and cancel the
installation. By continuing the installation process, you agree to the license
terms of Microsoft Exchange Server 2010.
If you don't accept these license terms, please cancel the installation. To
review the license terms, please go to
http://go.microsoft.com/fwlink/?LinkId=150127&clcid=0x409/

Press any key to cancel setup.....................
No key presses were detected.  Setup will continue.
Preparing Exchange Setup

    Copying Setup Files                                COMPLETED

No server roles will be installed

Performing Microsoft Exchange Server Prerequisite Check

    Organization Checks                                           COMPLETED

Configuring Microsoft Exchange Server

    Prepare Domain Progress                                       COMPLETED

The Microsoft Exchange Server setup operation completed successfully.

C:\EX>
```

Figure V.26 : Préparation du domaine.

2. Installation de Microsoft Exchange Server 2010 :

Une fois tous les pré-requis validés, nous passons à l'étape d'installation d'Exchange 2010. Pour cela nous exécutons le fichier « setup » situé dans le dossier d'installation.

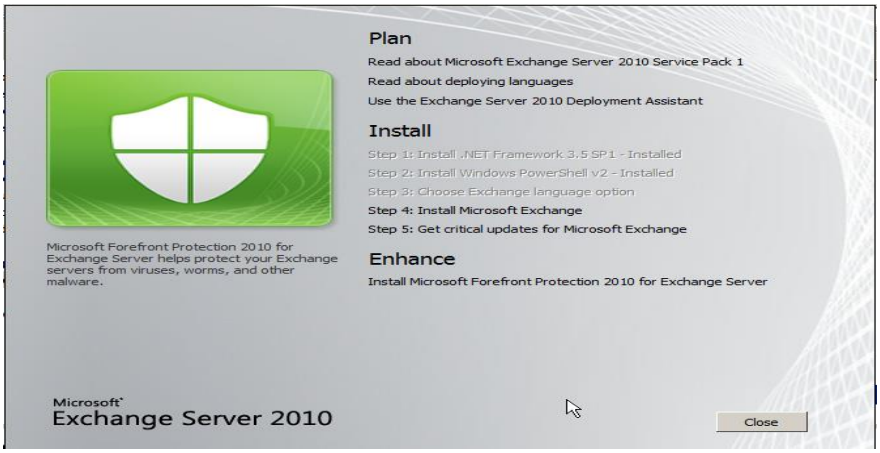


Figure 2.4: Lancement d'installation de l'Exchange.

Figure 2.5: Introduction.

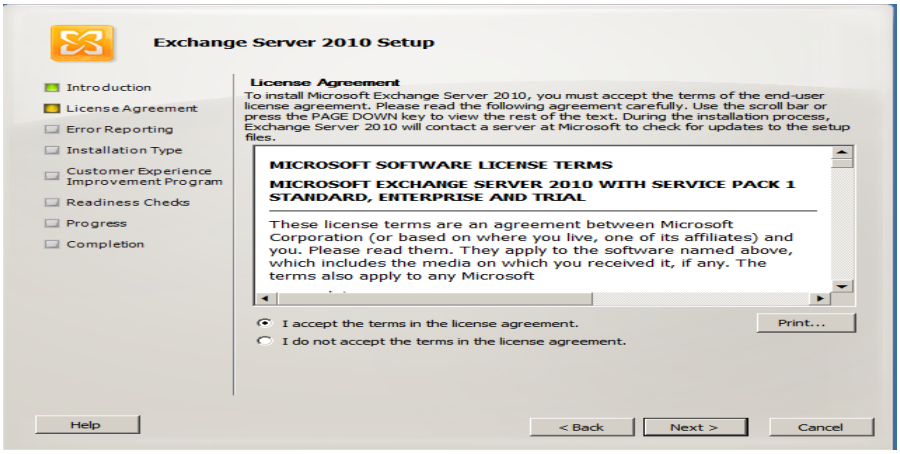


Figure 2.6: Acceptation de la licence.

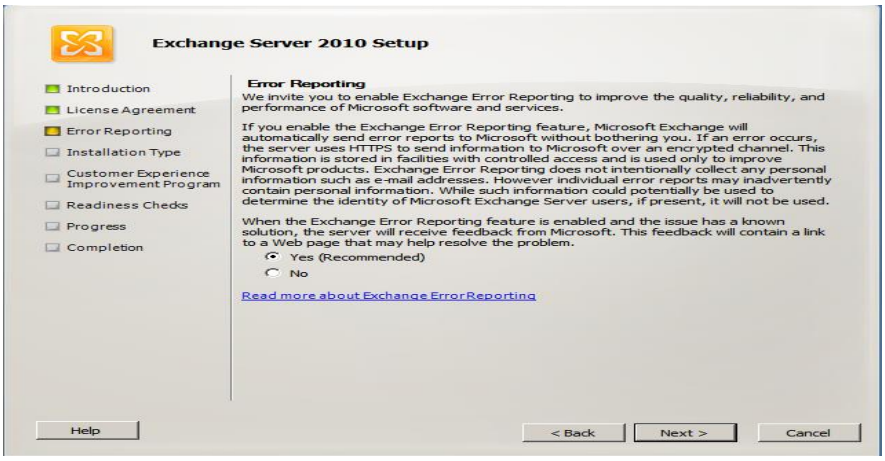


Figure 2.7: Le choix de rapport d'erreur.

Après avoir passé l'introduction, accepté le contrat de licence et choisi notre mode de rapport d'erreur, nous avons le choix entre une installation typique ou personnalisée. L'installation personnalisée nous permet d'installer les rôles dont nous avons besoin alors que l'installation typique installera les rôles CAS, Hub et Mailbox ainsi que les outils de gestion Exchange. Nous avons procédé à l'installation typique.

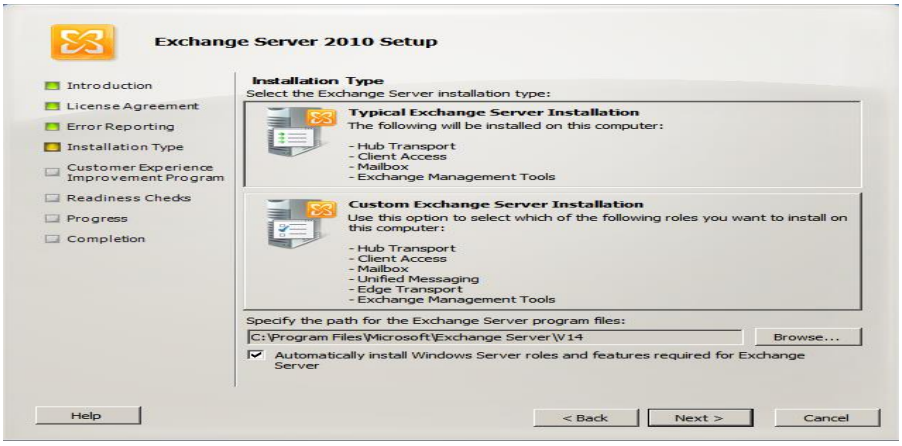


Figure 2.8: Le choix de type d'installation.

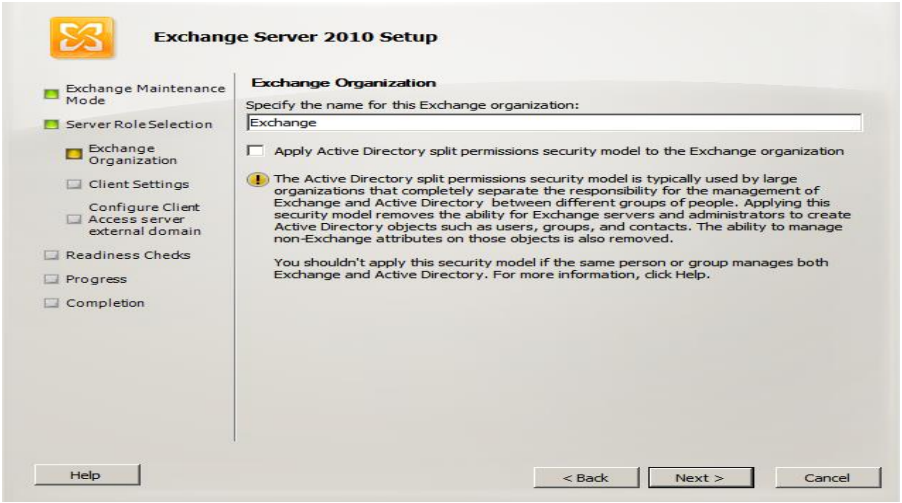


Figure 2.9 : Spécification de nom de l'organisation.

L'assistant nous demande ensuite si notre réseau contient des clients Outlook 2003 ou Entourage (Mac OS). Cela permet d'assurer une compatibilité pour les anciens clients. Dans notre cas l'entreprise n'a pas ce genre de clients donc nous avons fait le choix correspondant.

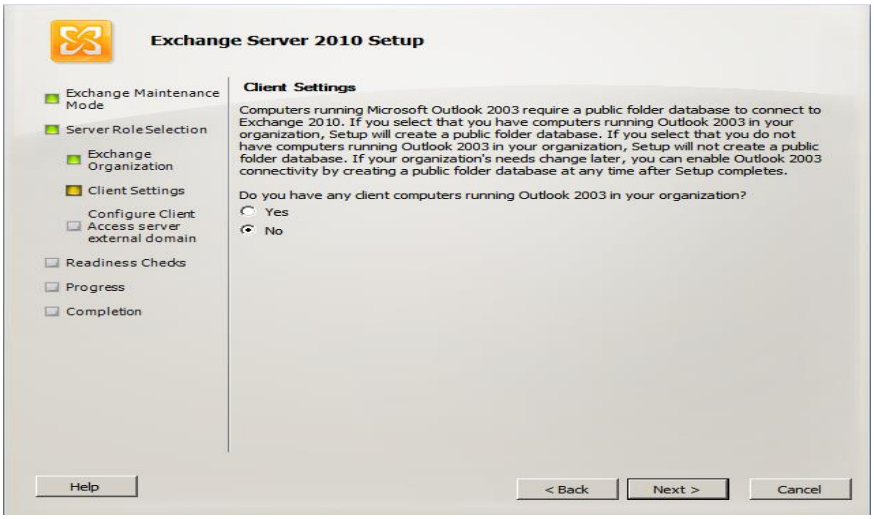


Figure 2.10 : Paramètre client.

A cette étape, nous avons configuré l'adresse du webmail qui sera accessible depuis l'extérieur.

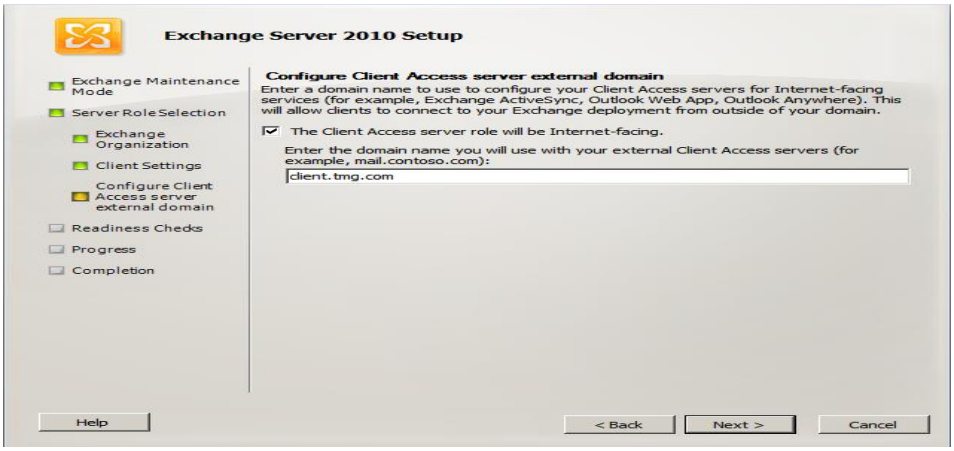


Figure 2.11: Configuration de domaine externe du serveur d'accès client.

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

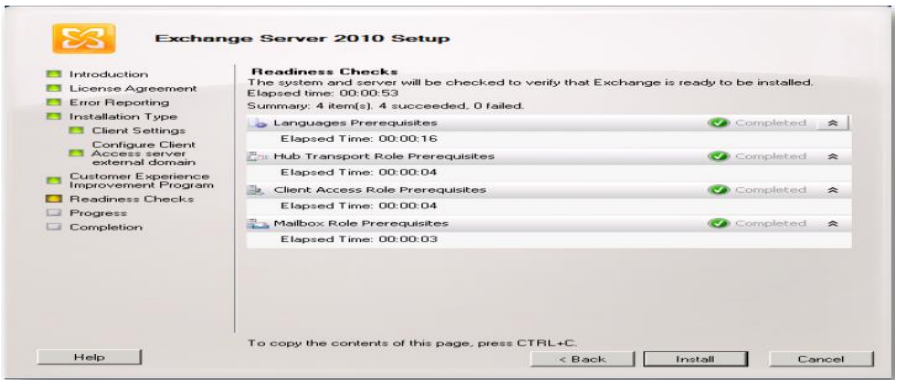


Figure 2.12: Les tests de préparation.

Une fois les tests effectués, nous pouvons lancer l'installation. Elle peut durer plus ou moins longtemps selon le serveur et les rôles à installer. Dans notre cas, Exchange a mis 1h39mn07s à s'installer.

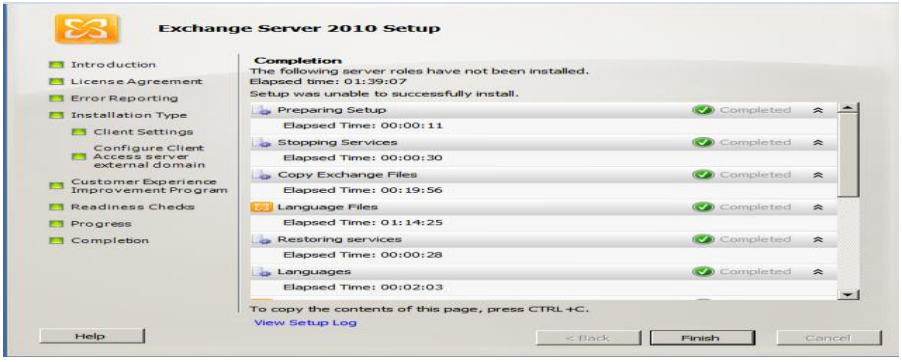


Figure 2.13 : Achèvement.

Avant de finaliser cette installation à l'aide de la console de gestion, il faut effectuer une mise à jour à l'aide du logiciel PackRollUp. Au démarrage de l'Exchange un message s'affiche pour nous prévenir que notre produit est sans licence afin de l'enregistrer.

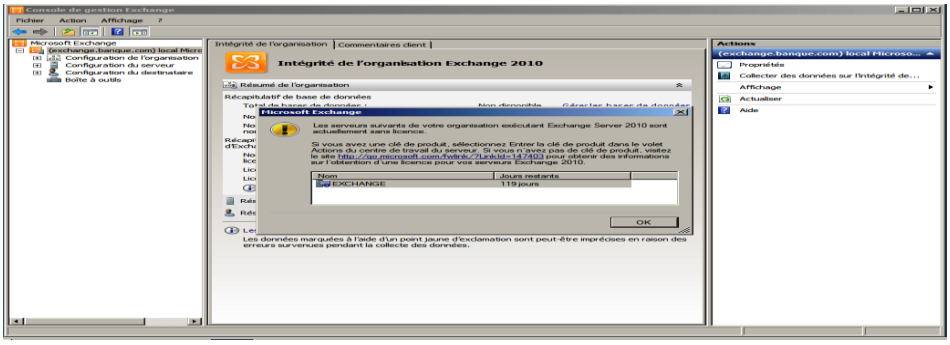


Figure 2.14: La console de gestion Exchange.

2.3 Installation de l'Autorité de Certification

Pour installer le service de certificats Active Directory, nous suivons les étapes que voici : Gestionnaire de serveur -> Ajouter des rôles-> Service de certificats Active Directory.

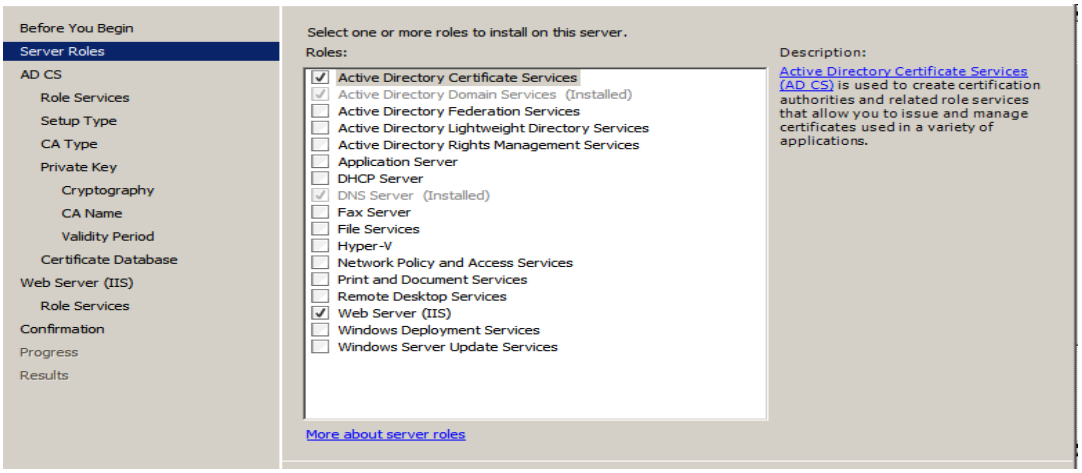


Figure 2.15: Ajout du service de certificats Active Directory.

Ajout des rôles autorité de certification (CA) pour émettre et gérer les certificats et l'inscription web qui permet aux utilisateurs de se connecter à la CA via un navigateur web pour demander des certificats.

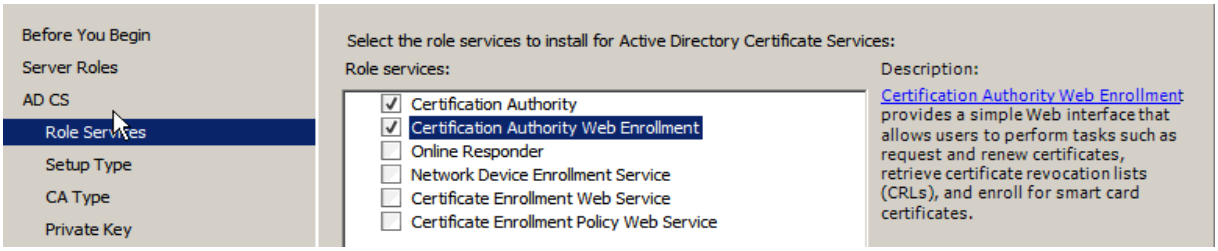


Figure 2.16 : Les services de rôle.

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

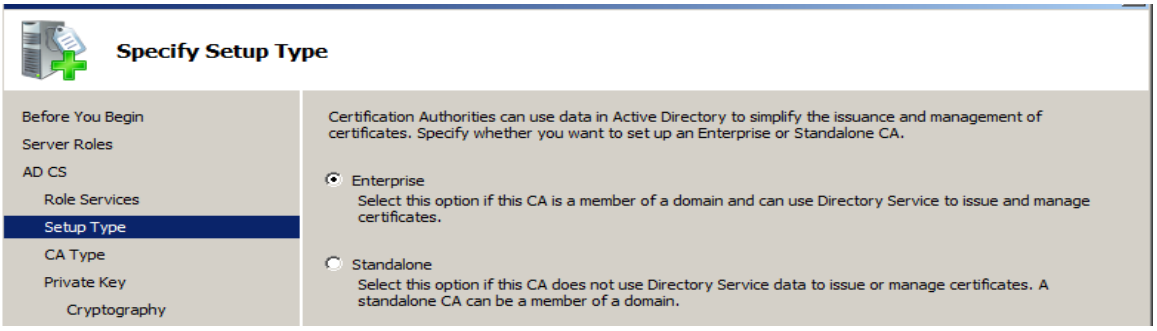


Figure 2.17: Spécification du type d'installation.

Ayant opté pour une CA entreprise dans cette étape nous créons une nouvelle clé privée, en spécifiant le fournisseur de service de chiffrement (RSA), l'algorithme de hachage (sha1) et la longueur de la clé en caractère (2048).

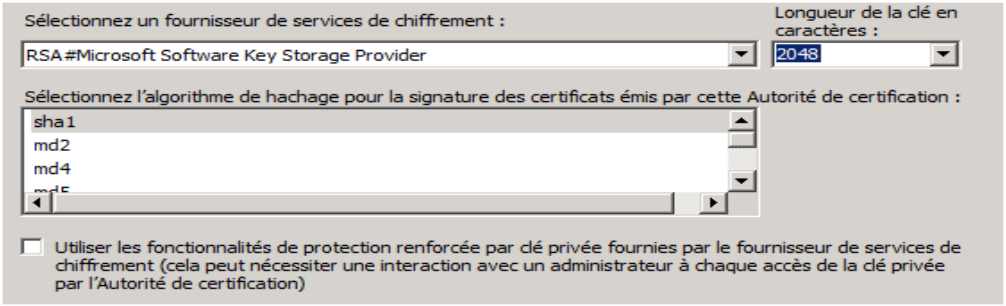


Figure 2.18: Création d'une nouvelle clé privée.

Définissons le nom de l'autorité de certificat, **2intpartners-certificat-CA**.

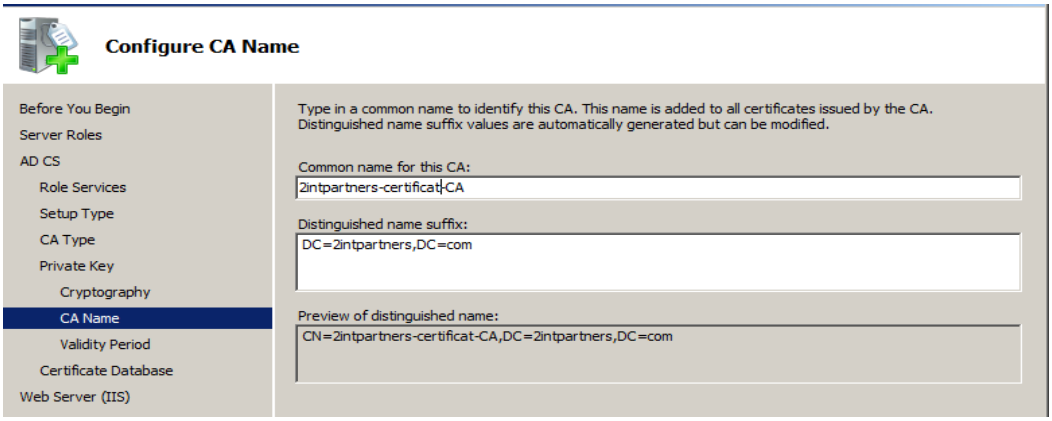


Figure 2.19: Nomination de l'Autorité de certificat.

1.1 Présentation d'Active Directory

Active Directory est le nom du service d'annuaire de Microsoft apparu dans le système d'exploitation Microsoft Windows Server 2000. Le service d'annuaire Active Directory est basé sur les standards TCP/IP, DNS, LDAP, Kerberos,...

Il doit être entendu au sens large, c'est-à-dire qu'Active Directory est un annuaire référençant les personnes (nom, prénom, numéro de téléphone,...) mais également toute sorte d'objet, dont les serveurs, les imprimantes, les applications, les bases de données, …Il permet de recenser toutes les informations concernant le réseau, que ce soient les utilisateurs, les machines ou les applications. Ainsi il constitue le moyeu central de toute l'architecture réseau et a vocation à permettre à un utilisateur de retrouver et d'accéder à n'importe quelle ressource identifiée par ce service.

Active Directory est donc un outil destiné aux utilisateurs mais dans la mesure où il permet une représentation globale de l'ensemble des ressources et des droits associés, il constitue également un outil d'administration et de gestion du réseau. Il fournit à ce titre des outils permettant de gérer la répartition de l'annuaire sur le réseau, sa duplication, la sécurisation et le partitionnement de l'annuaire de l'entreprise.

Figure 1.1: Active Directory.

1.2 L'installation d'Active Directory sous Windows 2008

1.2.1 Procédure

Dans le menu « Démarrer. Tous les Programmes. Outils d'administration. Gérer votre serveur ». Cliquer sur le lien « Ajouter un rôle (add roles)»

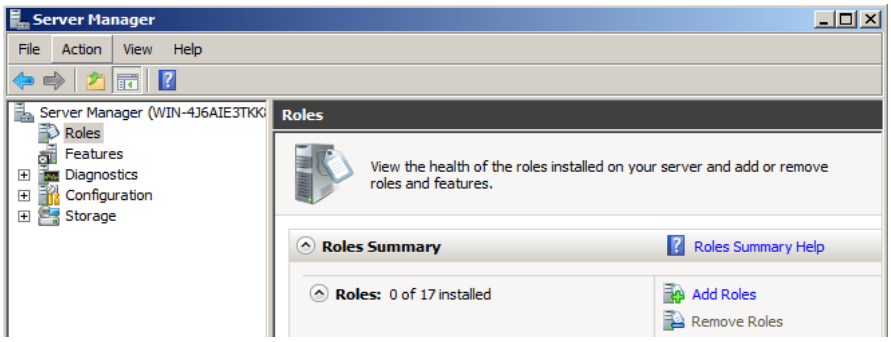


Figure1.1 : Ajouter des rôles dans server Manager

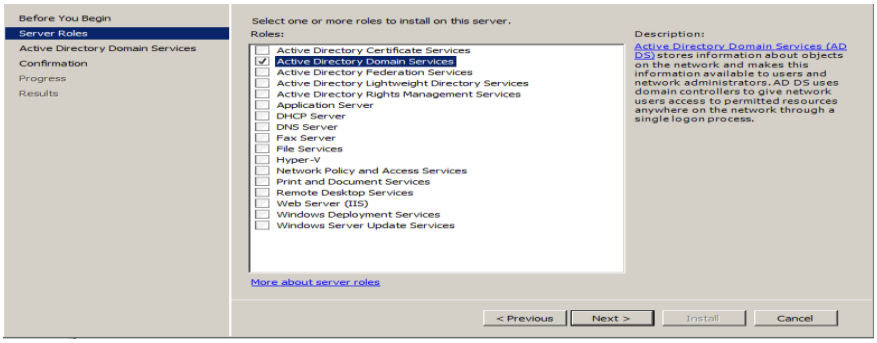


Figure1.2 : Sélectionner le rôle Active Directory Domaine Service

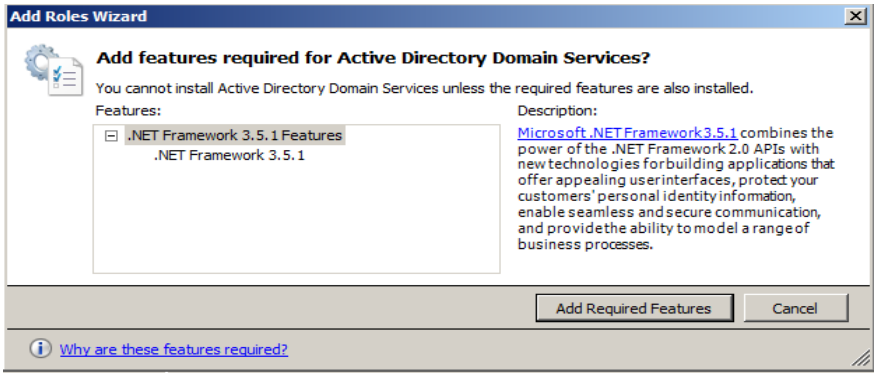


Figure1.3 : Ajouter des fonctions pour AD DS

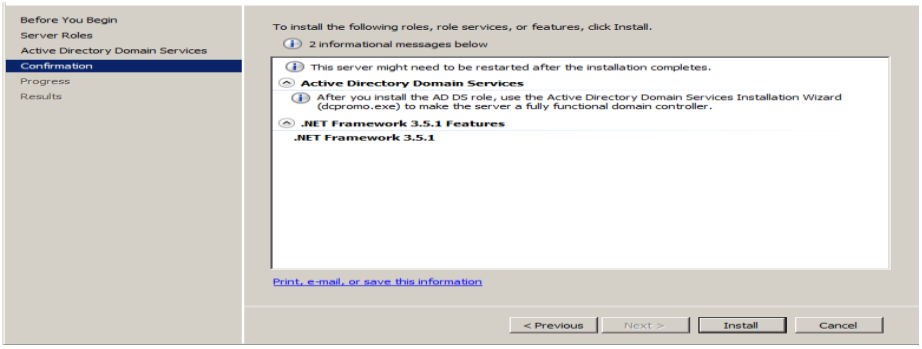


Figure1.4: installation de service AD DS et la fonction NET framework 3.5.1

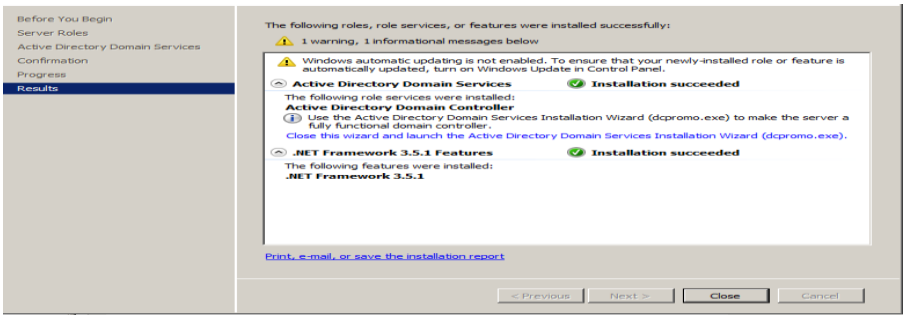


Figure1.5 : Fin d'installation de service AD D

Après l'installation de service Active Directory Domaine Service et ses fonctions, on installe le contrôleur de domaine à l'aide de la commande **« dcpromo.exe »**

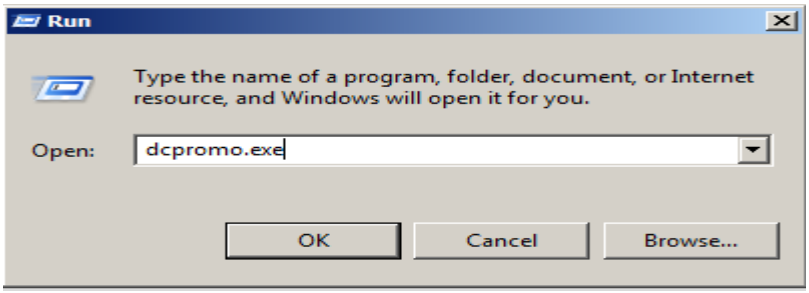


Figure 1.6 : Commande Dcpromo

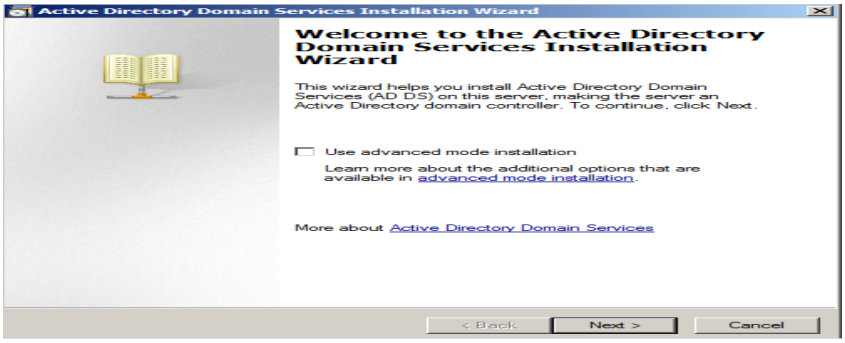


Figure 1.7 : Lancement de l'assistant d'installation d'Active Directory.

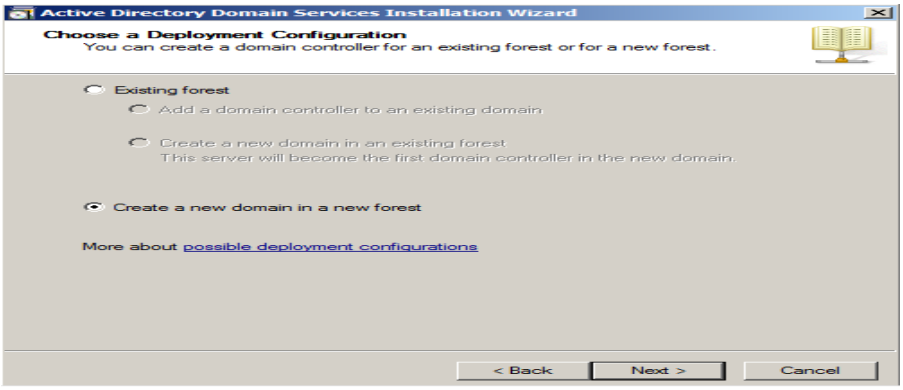


Figure 1.8 : Nouveau nom dans nouvelle forêt.

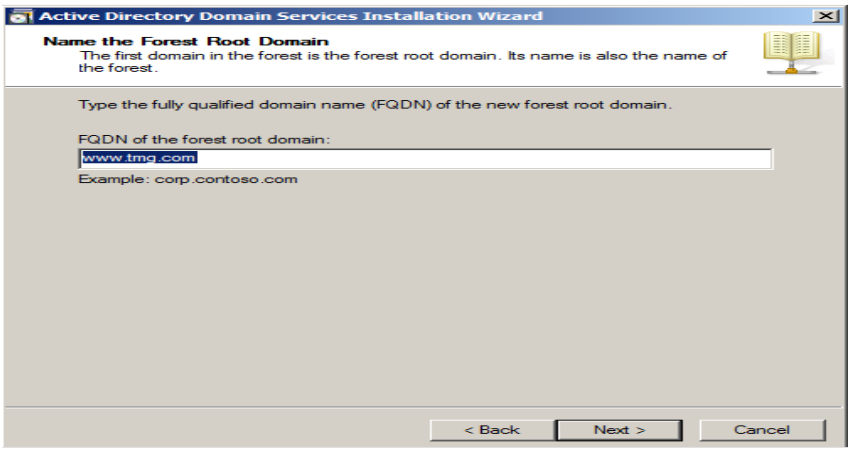


Figure 1.9 : Nom DNS du domaine.

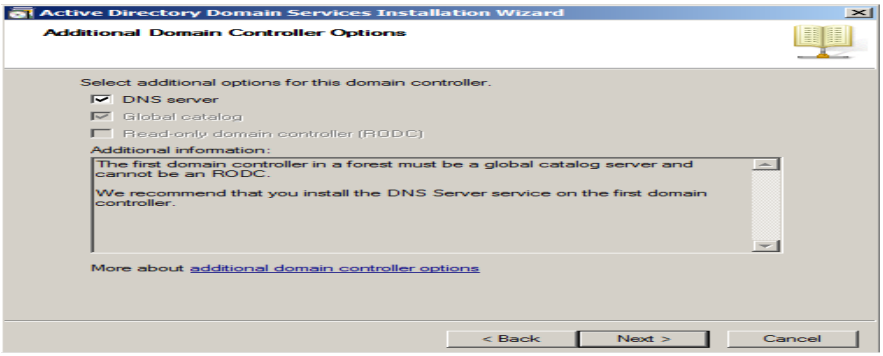


Figure 1.10 : Addition DNS dans le contrôleur de domaine.

Ensuite donner le chemin de la base de données, du journal Active Directory, et emplacement du dossier SYSVOL. Microsoft préconise des disques durs différents pour des raisons de performances et de meilleure récupération

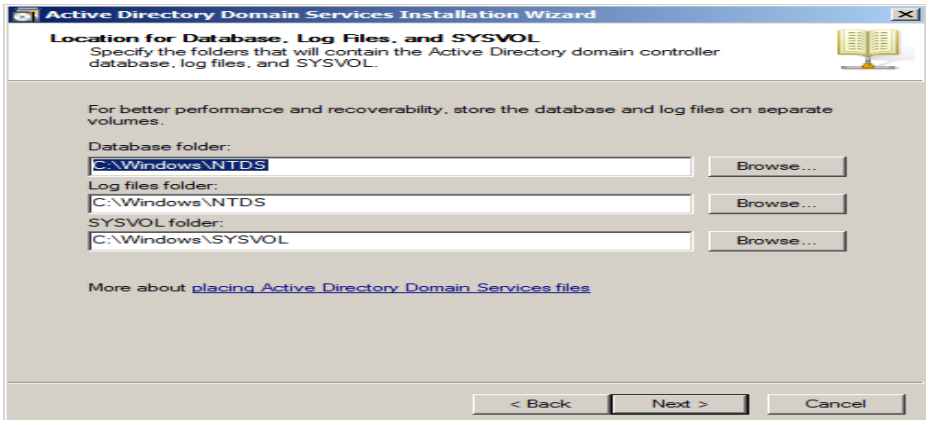


Figure 1.11 : Emplacement du dossier SYSVOL et la base de données NTDS

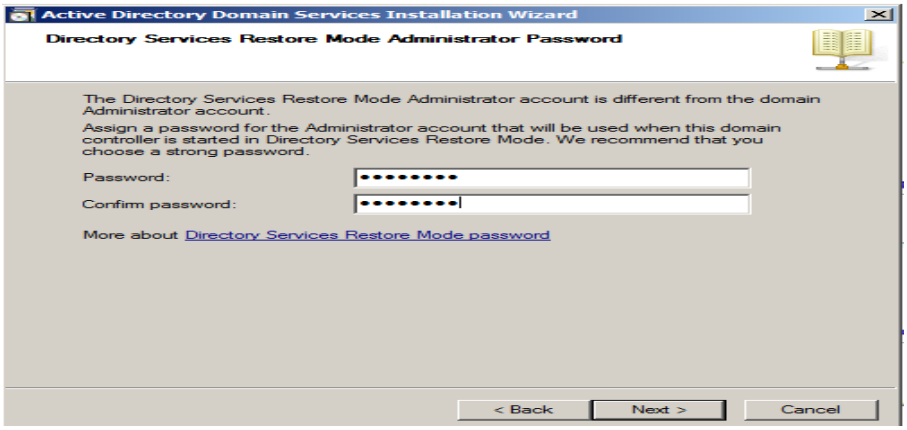


Figure 1.12 : Saisie du mot de passe administrateur.

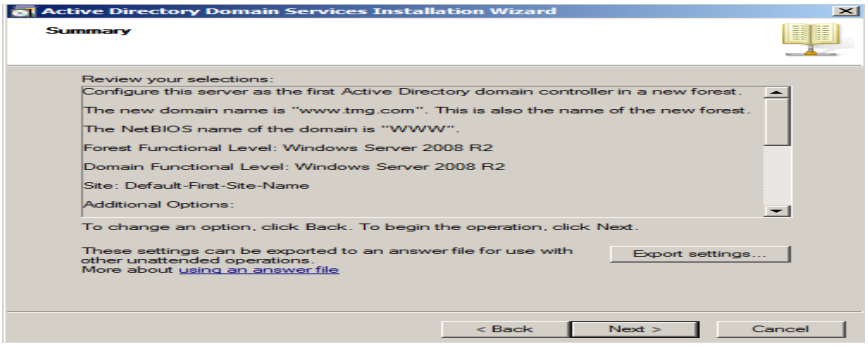


Figure 1.13: Affichage du résumé.

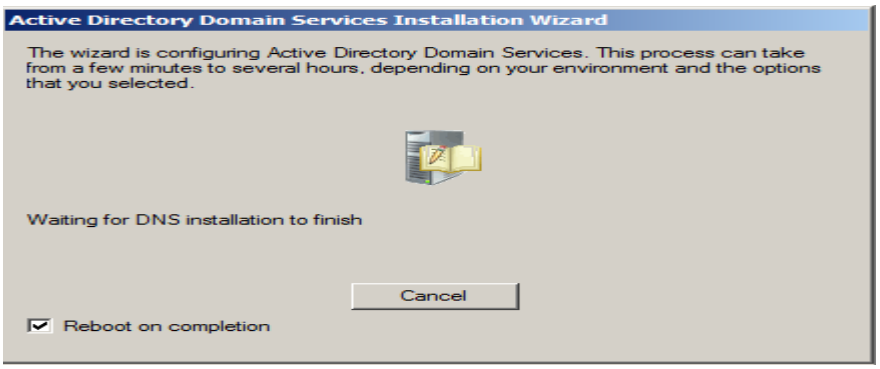


Figure 1.14 : Configuration d'Active Directory.

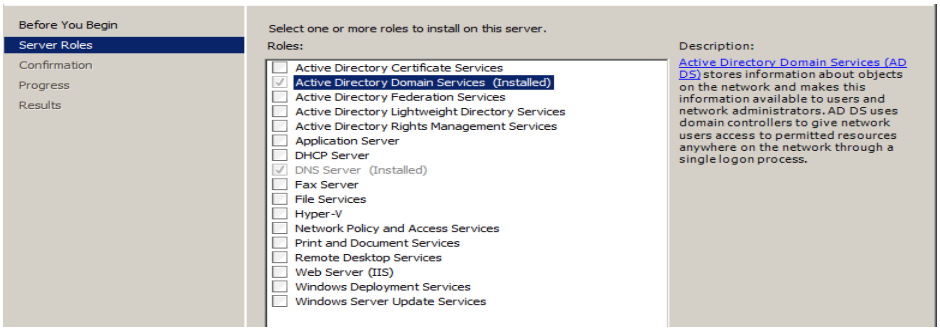


Figure 1.15 : le résultat d'installation de service AD DS.

1.3 Installation de la TMG

1.3.1 Les Pré-requis Matériels et logiciels de TMG

La configuration nécessaire à l'installation de TMG serveur 2010 dépend du nombre de machines connectées en même temps et des services utilisé. Il nécessaire un environnement comportant les caractéristiques minimales suivant :

- **Pré-requis Matériels :**

  - Un ordinateur avec un processeur 64 bits.
  - Système d'exploitation Windows Server 2008 64-bits. Vous ne pouvez pas installer Forefront TMG sur les versions 32 bits de Windows Server 2008.
  - 2 giga-octets (Go) ou plus de mémoire

- Une partition de disque dur local, qui est formaté avec le système de fichiers NTFS.
- 2,5 Go d'espace disque disponible. Ceci est exclus l'espace disque que vous souhaitez utiliser pour la mise en cache ou de stocker temporairement les fichiers lors de l'inspection malware.
- Une carte réseau qui est compatible avec le système d'exploitation, pour la communication avec le réseau interne.
- Une carte réseau supplémentaire pour chaque réseau connecté à l'ordinateur Forefront TMG.

➢ **Pré-requis Logiciels:**

Vous devez installer les programmes suivants sur votre serveur avant d'installer TMG

- Dot Net Framework 3.5
- Deux fonctionnalités de Windows Server 2008 doivent être ajoutées:
    - Windows Powershell
    - Message Queuing Service - Integration du service d'annuaire

Au lancement du programme d'installation en obtient la fenêtre suivante :

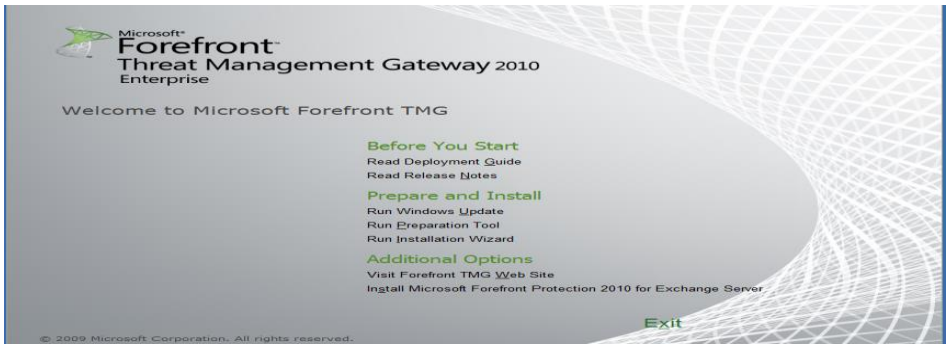


Figure 1.15 : Lancement de l'installation de la TMG.

Comme nous le voyons, le processus d'installation est subdivisé en trois étapes :

- ✓ **Etape 1:** Exécuter Windows Update cela permettra d'installer les dernières mises à jour.
- ✓ **Etape 2:** Exécuter l'outil de préparation pour installer l'ensemble des Pré-requis nécessaires pour le déploiement de la plate-forme TMG comme suit :

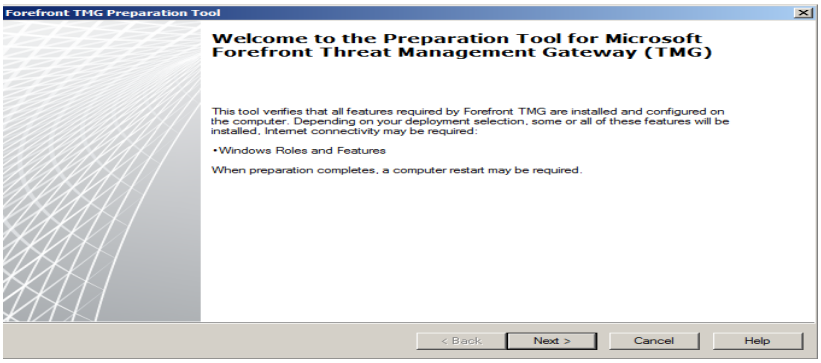


Figure 1.16 : Lancement de l'exécution des outils de préparation.

Apres avoir cliqué sur suivant nous choisissons d'installer les services et fonctionnalités de TMG et la console de gestion.

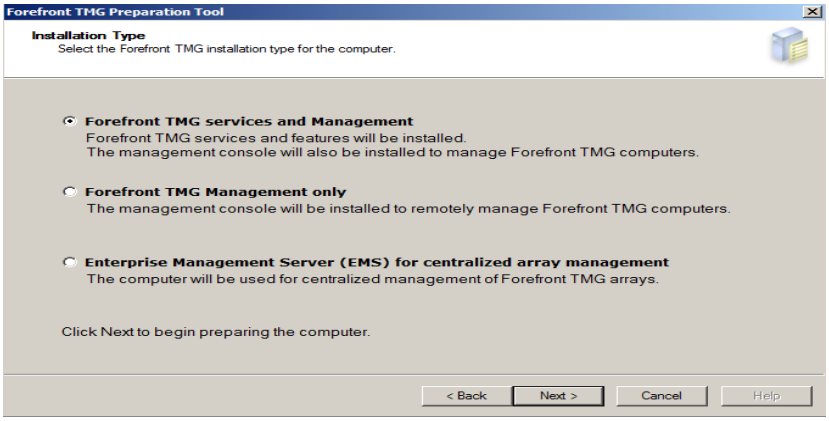


Figure 1.17: Le choix des fonctionnalités de la TMG.

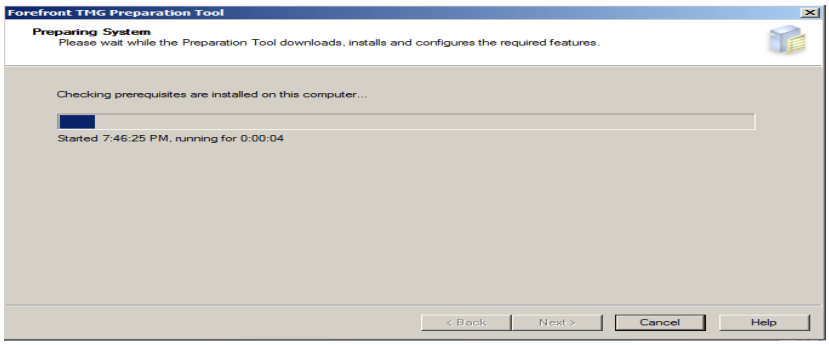


Figure 1.18 : Préparation des outils.

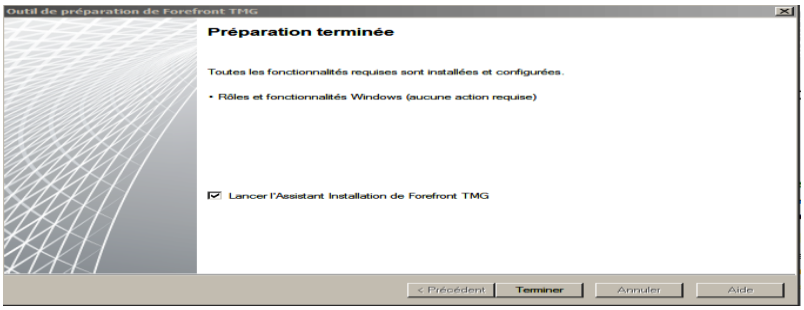


Figure 1.19 : Fin de préparation des outils et lancement d'assistant d'installation de la TMG.

- ✓ **Etape 3 : Exécuter l'assistant d'installation.**

Après le lancement de l'assistant d'installation nous obtenons la figure suivante :

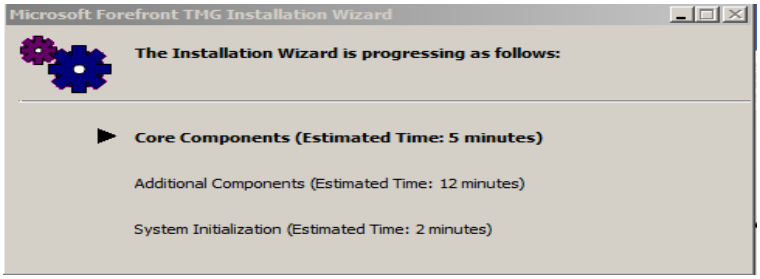


Figure 1.20 : Assistant d'installation de la TMG.

Pour valider la licence du produit il nous ait demandé d'introduire le nom de l'utilisateur et la compagnie.

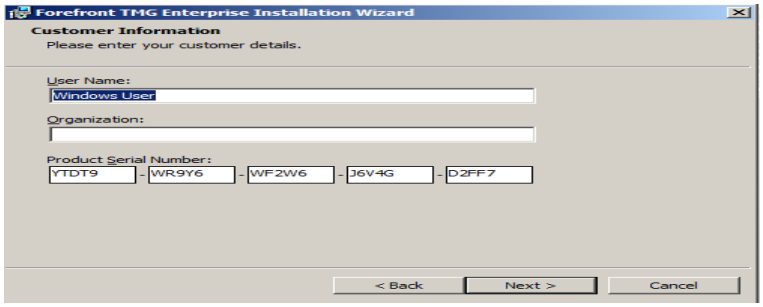


Figure 1.21 : Validation de la licence.

Le produit étant validé, il nous ait demandé d'ajouter les cartes réseau, dans notre cas pour gérer le réseau interne nous sélectionnons la carte interne.

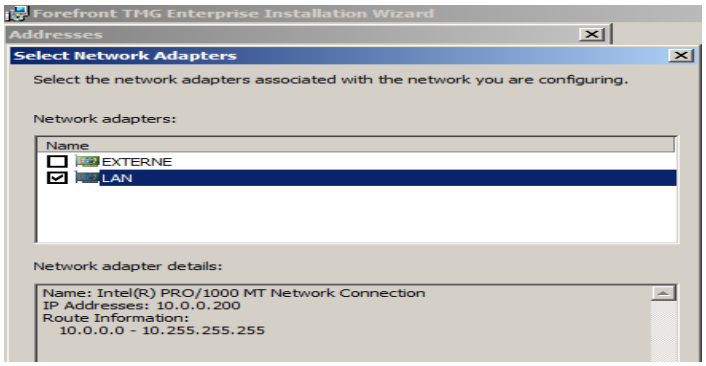


Figure 1.22 : Sélection des cartes réseau.

Après la sélection de la carte interne la plage d'adresse de celle-ci sera calculée et listée il ne reste plus qu'à la valider.

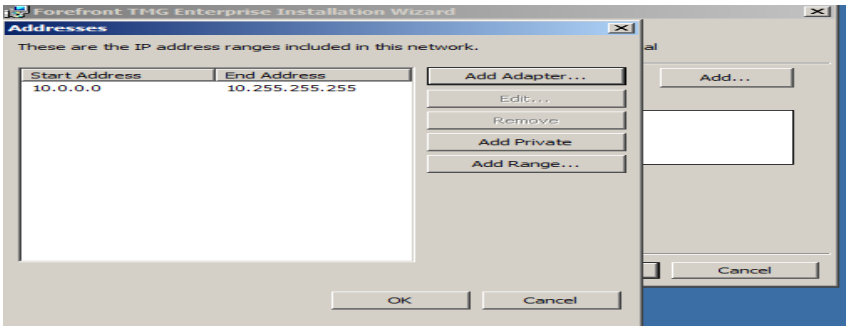


Figure 1.23: Liste de la plage des valeurs.

A la fin de l'installation de Forefront TMG, nous pouvons lancer la gestion de la TMG.

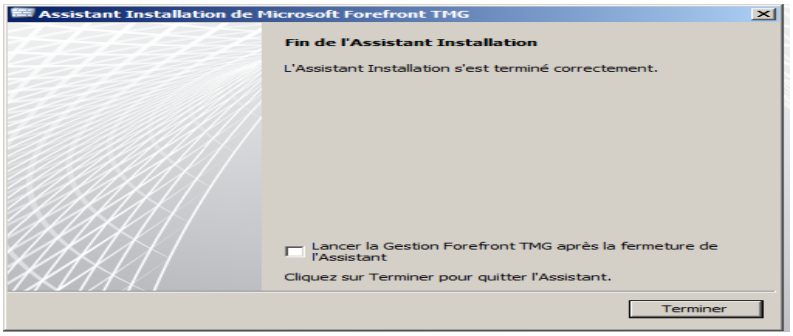


Figure 1.24 : Fin d'assistant d'installation.

Bibliographie

[1] : Guy PUJOLLE, les réseaux, livre de l'édition EYROLLES, (2008).

[2] : Laurent BLOCH et Christophe WOLFHUGEL, 2ème édition de Sécurité Informatique, de l'édition EYROLLES, (2009).

[03]: Douglas Comer « TCP/IP Architecture, Protocoles, Applications », 4e édition DUNOD.

[04]: Dominique MANIE, Intégré la dimension éthique et le respect de la déontologie, Cours de « Certification Informatique et Internet » à l'université de lyon2, (2005).

[05]: Ibrahim HAJJEH, Sécurité des échanges. Conception et validation d'un nouveau protocole pour la sécurisation des échanges, thèse doctorat à l'école national des télécommunications de Paris, (décembre 2004).

[06]: Eric Maiwald« Sécurité des réseaux », Edition CampusPress, paris 2001.

[07]: Joseph Steinberg, SSL VPN accès web et extranets sécurisés, Eyrolles, 2006.

[08]: Solange Ghernouatu-Hélie, Sécurité informatique et réseaux, Dunod, 2008.

[09]: ACISSI, Sécurité informatique Ethical Hacking apprendre l'attaque pour mieux se défendre, ENI, 2012.

[10]: Thierry Evangelista, Les systèmes de détection d'intrusions informatiques, Dunod, 2004.

[11] : Université de Nice, Le livre sécuritéinfo.com, (2010).

[12]: Gary Hallen, CCNP security IPS 642-627 quick reference, Cisco Presse Library of Bolovan Calin Borgdan, 2011

[13]: Guillaume Desgeorge, La sécurité des réseaux, 2000.

[14]: Yuri Diogenes, Dr Tom Shinder, Forefront Threat Management Gateway (TMG), Micrsoft Forefront TMG Team, Administrator's Companion, 2010

[15]: Vladimir Holostov, Forefront TMG 2010 Common Criteria Evaluation Guidance Documentation Addendum Microsoft Forefront Threat Management Gateway Team, Microsoft Corp, 2010.

[16]: Jim Harrison, Yuri Diogenness, Microsoft Forefront Threat Management Gateway (TMG),

[17]:J.F.PILLOU 'tout sur la sécurité informatique', édition, Paris : duons 2009 2 éme

[18] : D.HOLME : « Configuration d'une infrastructure active Directory avec Windows 2008 » : Paris : DUNOD, 2008

[19] : http:// www.Microsoft.com

[20] :http://www.technet .microsoft.com

[21] :http:// www.Vmware.com

[22] :http:/ /www.google.com/windows serveur 2008**.**

[23] : http:// www.google.com / Microsoft Exchange serveur 2010.com

[24]:http://www.laboratoir mocrosoft.com

DMZ Demilitarized Zone

DNS Domain Name System

FTP File Transfert Protocol

HTTP HyperText Transfert Protocol

HTTP-S HyperText Transfert Protocol Secure

ICMP Internet Control Message Protocol

IP Internet Protocol

ISO International Standard and Acceleration

LAN Local Area Network

OSI Open System Interconnection

POP Post Office Protocol

POP3 Post Office Protocol version 3

SMTP Simple Mail Transfert Protocol

VPN Virtual Private Network

UDP User Datagram Protocol

SSH Secure Shell

SSL Secure Socket Layer

TCP Transfert Control Protocol

ARPA Advanced Research Project Agency

NCF National Science Foundation

IRC Internet Relay Chat

NNTP News Network Transfert Protocol