RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE
LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU
FACULTE DE GENIE ELECTRIQUE ET INFORMATIQUE
DEPARTEMENT D'INFORMATIQUE

Mémoire de fin d'études

En vue de l'obtention du diplôme de Master II en Informatique

Option : Systèmes informatiques

Thème :

Mise en place d'une politique de sécurité dans un réseau

Cas d'une banque

Proposé et dirigé par :

M^me^: R. AOUDJIT
Mr: M. KIBOUH

Réalisé par :

M^lle^: CHENANE Kathia
M^lle^: FEDOUL Saloua

Promotion: 2012/2013

Remerciements

Nous tenons à exprimer notre profonde gratitude à notre promotrice Mme R. AOUDJIT et notre encadreur M M.KIBOUH et tous les employés de l'école 2INT Partners pour leurs suivis et leurs conseils précieux tout au long de l'élaboration de notre mémoire.

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

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

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

Dédicaces

Je dédie ce modeste travail à

Ma très chère mère, grâce à qui je suis ici aujourd'hui

Mes très chères sœurs et mon cher frère,

Mes chers amis(e)

Et toute notre promotion Master II SI.

Saloua

Dédicaces

Je dédie ce modeste travail à mes très chers parents et ma sœur, Linda, qui ont su croire en moi et pour leur soutien pendant toute la durée de mes études.

A tous mes amis qui ont toujours été là pour moisans oublier toute la promotion 2013.

Kathia

Table des matières

Table des matières

Table des matières

Table des matières

Table des matières

Table des figures

Table des figures

Table des figures

Table des figures

Table des figures

Glossaire

AAA	Authentication Authorization Accounting
ACE	Access Control List
ACL	Access Control Entry
AH	Authentication Heade
AIP SSM	Advanced Inspection and Prevention Security Services Module
ARP	Address resolution protocol
ASA	Adaptive Security Appliance
ASDM	Adaptive Security Device Manager
CA	Certificate Authority
CD /DVD	Compact Disc / Digital Versatile Disc
CSC SSM	Content Security and Control Security Services Module
DDoS	Distributed Denial-of-Service a
DMZ	Demilitarized zone
DNS	Domain Name System
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GNS3	Graphical Network Simulateur
HIDS	Host Intrusion Detection System
HTTPS	Hypertext Transfer Protocol secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection Services
IIS	Internet Information Services
IOS	Inter-network Operating System
IP	Internet Protocol
IPsec	Internet Protocol Security
IPS	Intrusion Prevention Services
ISA	Internet Security and Acceleration
KIPS	Kernel Intrusion Prevention System
LAN	Local Area Network
MAC	Media Access Control
MIB	Management information base
NAS	Network Attached Storage
NAP	Network Access Protection
NAT	Network Address Translation
NIDS	Network Intrusion Detection System
NLB	Network Load Balancing
NPS	Network Policy Server
NTFS	New Technology File System
OS	Operating System
OSI	Open Systems Interconnection

PAT	Port Address Translation
PGP	Pretty Good Privacy
PIX	Private Internet EXchange
PKI	public-key infrastructure
PKCS	Public-Key Cryptography Standards
POP3	Post Office Protocol version 3
PPP	Protocol Point-To-Point
QOS	Quality Of Service
RADIUS	Remote Authentification Dial In User Service
RAID	Rendundant Array of Independent Disks
RPV	Réseau privé virtuel
RPF	Reverse Path Forwarding
SSH	Secure Shell
SSL	Secure Socket Layer
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
TCP	Transfer Control Protocol
Telnet	TELecommunication NETwork
TMG	Threat Management Gateway
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
USM	User-based Security Module
VPN	Virtual Private Network
VLAN	Virtual Local Area Network
VACM	View Access Control Model
WAN	Wide Area Network

Introduction générale

Introduction générale

L'outil informatique, qui fut à une certaine époque, le luxe que s'offraient certaines entreprises, est devenu en l'espace d'une quarantaine d'années le moyen de communication par excellence. Cette vulgarisation matérielle a conduit à une expansion du réseau intense : qui a fait exploser le nombre de menaces informatiques très diverses.

Si, avant l'internet, il fallait au pirate un contact direct avec les données pour nuire à sa cible, depuis l'avènement de cette dernière, la compromission des données peut se faire d'un bout du monde à l'autre. En parallèle, si dans le passé la sécurité était réduite, aujourd'hui, elle ne cesse d'évoluer car des utilisateurs font de plus en plus face aux failles et menaces de la sécurité informatique. Ces derniers cherchent toujours à les réduire en se protégeant au maximum des cyberattaques.

La meilleure solution adoptée par les entreprises du monde est le renouvellement périodique de leurs moyens sécuritaires. Ce qui est le cas de la banque dont nous étudierons l'infrastructure réseau et système. Pour des raisons de sécurité, le nom de la banque sera omis tout au long de ce projet. Cette dernière a été mise à jour en 2007 avec la collaboration de l'école 2INT Partners. Notre étude consiste à énumérer les différentes vulnérabilités des réseaux et systèmes et proposer des solutions innovantes en tenant compte des nouvelles technologies tout en essayant de préserver cette banque des différents risques.

La démarche sécuritaire suivie consiste à mettre en place une politique de sécurité fiable. Pour y parvenir, nous étudierons en premier lieu, les différents aspects de la sécurité informatique, la sécurisation des interconnexions réseaux et les solutions matérielles disponibles sur le marché. En second lieu, nous nous pencherons sur l'étude de l'architecture existante pour déterminer les points critiques et ainsi proposer les solutions adéquates.

Chapitre I : La sécurité des réseaux informatiques

I.1.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 différents aspects liés à la sécurité, les types d'attaques et leurs mécanismes de détection et la protection des réseaux informatiques.

I.2. Récapitulatif des plus récentes attaques

Avant de nous lancer dans le thème de la sécurité nous avons recueilli quelques attaques perpétrées pendant l'année 2012 et le début de l'année 2013. Nous avons choisi les organismes les plus connus et sécurisés :

- ✓ Le 2 janvier 2012: huit sites gouvernementaux ou proches de la présidence tunisienne ont été mis hors services par saturations de leurs serveurs.

- ✓ 2012 : une série d'attaques DOS (Deny of Sevice) contre les banques américaines a été perpétrée par des hackers qui ont piraté les systèmes informatiques de Wells Fargo.

- ✓ Janvier 2013 : Google a été attaqué par un groupe de pirates identifiés sous le nom d'Eboz loin d'être un DOS. Ils ont bloqué durant des heures Google avec une image de deux manchots traversant un pont accompagné de messages énigmatiques.

- ✓ 19 février 2013 : après Facebook, Twitter, le New York Times ou encore le Wall Street Journal, Apple a reconnu à son tour avoir été victime d'une attaque informatique. Cette dernière a été répondue par l'intermédiaire d'un site internet pour les développeurs logiciels en utilisant une vulnérabilité dans le logiciel Java pour les navigateurs internet.

Comme nous pouvons voir, des attaques ne cessent d'être perpétrées. Elles sont motivées par l'appât du gain, pour dérober des informations industrielles ou juste pour le fun.

I.3. La sécurité informatique

I.3.1. Définition

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. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité. [01]

I.3.2.Les critères de la sécurité

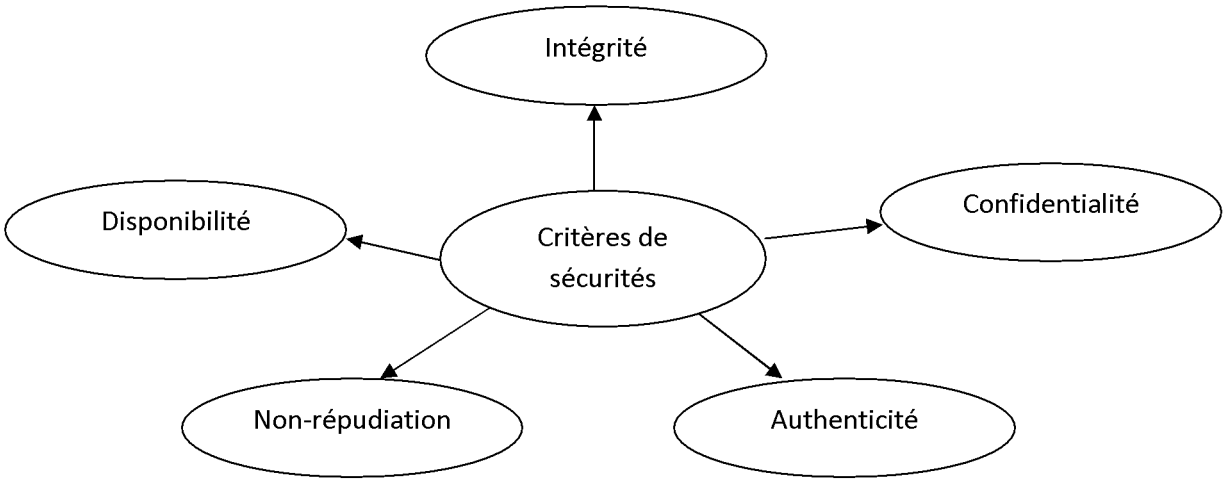

Figure1.1 : Critères de sécurité.

Intégrité: le critère d'intégrité des ressources physiques et logiques (équipements, données, traitements, transactions et services) est relatif au fait qu'elles n'ont pas été détruites (altération totale) ou modifiées (altération partielle) à l'insu de leurs propriétaires tant de manière intentionnelle qu'accidentelle. Une fonction de sécurité appliquée à une ressource pour contribuer à préserver son intégrité, permettra de la protéger plus ou moins efficacement contre une menace de corruption ou de destruction. [02]

Confidentialité: la confidentialité des données peut être définie comme la protection des données contre une divulgation non autorisée. Il existe deux types d'actions complémentaires permettant d'assurer la confidentialité des données :

- ✓ Limiter et contrôler leurs accès afin que seules les personnes habilitées à les lire ou à les modifier puissent le faire.
- ✓ Les rendre incompréhensibles en les chiffrant de telle sorte que seules les personnes ayant les moyens de déchiffrement puissent y accéder.

Disponibilité: le bon fonctionnement des services, systèmes et données doivent être accessibles aux ayants droits en continu sans interruption, sans retard, ni dégradation.

Non-répudiation: c'est le fait de ne pas pouvoir nier ou rejeter qu'un événement (actions, transactions) a eu lieu. A ce critère de sécurité peuvent être liées les notions suivantes :

- ✓ L'imputabilité est l'attribution d'une action (un événement) à une entité déterminée (ressources ou personnes).
- ✓ La traçabilité permet de grader une trace numérique de tout événement (message électronique, transaction commerciale, transfert de données…).
- ✓ L'auditabilité définie la capacité d'un système à garantir la présence d'informations nécessaires à une analyse ultérieure d'un événement (courant ou exceptionnel) effectué dans le cadre de procédure de contrôle spécifique et d'audit.

Authentification: doit permettre de vérifier l'identité d'une entité pour pouvoir assurer son authentification, ainsi seules les personnes autorisées auront accès aux ressources.

I.4. Politique de sécurité

I.4.1. Définition

Une politique de sécurité est un ensemble de règles qui fixent les actions autorisées et interdites dans le domaine de la sécurité, répondant à toutes les questions qu'un ingénieur en charge d'une étude se pose lorsqu'il aborde le volet de sécurité d'un projet informatique. La réussite de ce dernier dépend entre autres de la prise en compte dès le début des contraintes de sécurité.

Une politique de sécurité est donc un document confidentiel qui en faisant abstraction des contingences matérielles et techniques fournit une collection de directives de sécurité classées par thèmes. [04][03]

I.4.2. Les types de politique de sécurité

- ✓ **La politique qui interdit tout par défaut :** dans cette approche, tout ce qui n'est pas explicitement permis est interdit. Elle consiste à définir les services à autoriser (SMTP pour l'hôte serveur de courrier, http pour l'hôte devant accéder au web) et définir les droits de chaque utilisateur.
- ✓ **La politique qui autorise tout par défaut :** dans cette approche, tout est permis sauf ce qui est considéré comme dangereux donc tout ce qui n'est pas explicitement interdit est autorisé. Elle consiste à analyser les différents risques d'application qui doivent s'exécuter, en déduire les interdictions à appliquer et autoriser tout les reste. [05]

I.5.Terminologies de la sécurité informatique

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

- ✓ **Vulnérabilité** : c'est une faille de sécurité le plus souvent cachée touchant une infrastructure informatique. Ce terme est fréquemment associé aux logiciels mais il regroupe plus généralement toute faiblesse quelle qu'en soit la nature. Une erreur de configuration d'un équipement réseau constitue une vulnérabilité tout comme un mot de passe vide ou trivial.
- ✓ **Risque** : c'est la probabilité qu'un problème survienne lorsqu'une vulnérabilité est exposée à une population malveillante qui tentera de l'exploiter.
- ✓ **Attaque:** elle représente le moyen d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables.
- ✓ **Contre-mesure:** c'est la procédure ou technique permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique.
- ✓ **Menace:** c'est un adversaire déterminé capable de monter une attaque exploitant une vulnérabilité.

I.6. Les types de menaces

- ✓ **Menaces accidentelles:** ce sont celles qui existent sans qu'il y ait préméditation, exemples, défaillance de systèmes, bévues opérationnelles et bugs dans les logiciels.
- ✓ **Menaces intentionnelles:** ce sont des actions exécutées par une entité pour violer la sécurité de l'information et l'utilisation non autorisée des ressources. Les menaces intentionnelles peuvent être passives ou actives.
  - ☑ **Menaces passives** : ce sont celles qui, si elles se concrétisent, ne produiraient aucune modification d'informations contenues dans le(s) système(s) et avec lesquelles ni le fonctionnement, ni l'état du système ne change. Il est très difficile de détecter ce type de menaces car elles sont inoffensives par rapport aux fonctions normales du système. L'utilisation de branchements clandestins passifs pour observer des informations transmises via une ligne de communication (surveillance de réseau) est une concrétisation d'une menace passive.
  - ☑ **Menaces actives**: les menaces actives ou attaques envers un système comprennent l'altération d'informations contenues dans ce système, ou des modifications de l'état ou le fonctionnement du système. Les menaces actives sont, contrairement aux menaces passives, plus faciles à détecter si des précautions appropriées ont été prises au préalable.

Les exemples d'attaques sont la destruction, la modification, la fabrication, l'interruption ou l'interception de données. Le résultat d'une attaque est soit une divulgation de l'information (violation de la confidentialité de l'objet), soit une modification des objets (violation de l'intégrité de l'objet) ou un déni de service (violation de la disponibilité). [06]

I.6.1. Les attaques informatiques

I.6.1.1. Les types d'attaques

Les personnes malveillantes utilisent plusieurs techniques d'attaques qui peuvent être regroupées en trois familles différentes : [07]

a. Les attaques directes

C'est la plus simple des attaques. Le hacker attaque directement sa victime à partir de son ordinateur. En effet, les programmes de hacking qu'ils utilisent ne sont que faiblement paramétrable, et un grand nombre de ces logiciels envoient directement les paquets à la victime.

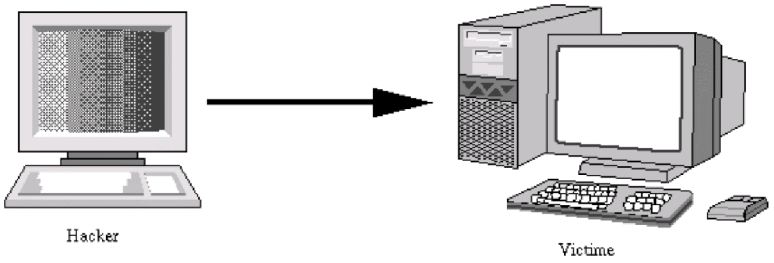

Figure1.2 : Attaque directe.

b. Les attaques indirectes par rebond

Cette attaque est très prisée des hackers. En effet, le rebond a deux avantages :

- ✓ Masquer l'identité (l'adresse IP) du hacker.
- ✓ Utiliser éventuellement les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante) pour attaquer.

Les paquets d'attaque sont envoyés à l'ordinateur intermédiaire qui répercute l'attaque vers la victime. D'où le terme de rebond.

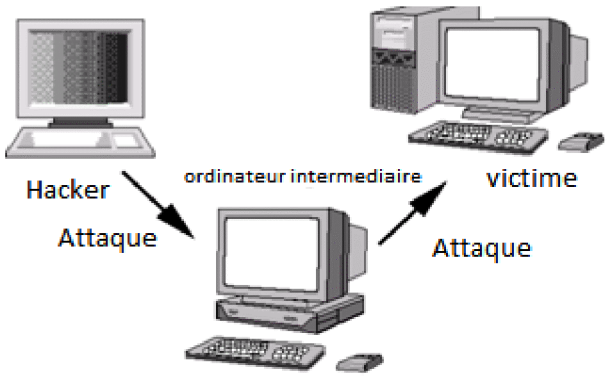

Figure1.3 : Attaque indirecte par rebond.

c. Les attaques indirectes par réponse

Cette attaque est dérivée de l'attaque par rebond. Elle offre les mêmes avantages, du point de vue du hacker, mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime.

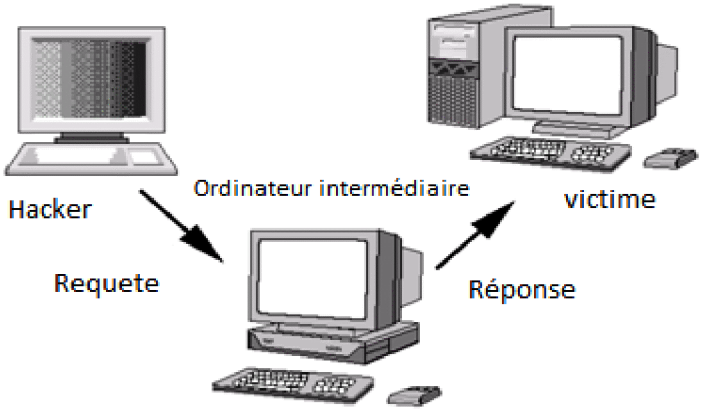

Figure1.4 : Attaque indirecte par réponse.

I.6.1.2. Les techniques d'attaques

I.6.1.2.a. Les attaques réseaux

Les attaques réseaux profitent des vulnérabilités du réseau. Voici quelques exemples d'attaques réseaux :

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. [08]

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. Il existe deux techniques pour effectuer cette attaque :

a. Empoisonnement du cache DNS

L'empoisonnement du cache DNS ou pollution de cache DNS (DNS cache poisoning) est une technique permettant de leurrer les serveurs DNS afin de leur faire croire qu'ils reçoivent une réponse valide à une requête qu'ils effectuent, alors qu'elle est frauduleuse. Une fois que le serveur DNS a été empoisonné, l'information est mise dans un cache, rendant ainsi vulnérable tous les utilisateurs de ce serveur. Ce type d'attaque permet, par exemple, d'envoyer un utilisateur vers un faux site dont le contenu peut servir à de l'hameçonnage (dans le cas du DNS) ou comme vecteur de virus et autres applications malveillantes.

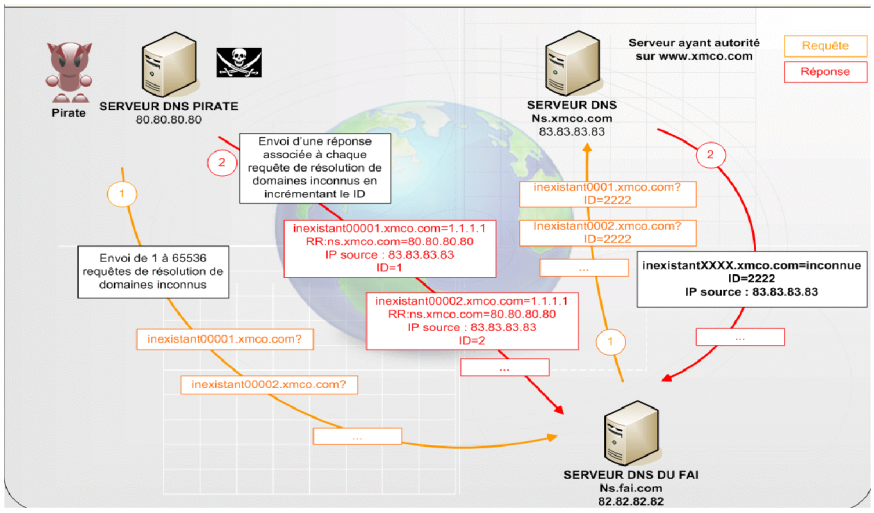

Figure1.5 : Le fonctionnement de DNS cache poisoning.

b. DNS ID Spoofing

Lors d'une requête pour obtenir l'adresse IP à partir d'un nom, un numéro d'identification est placé dans la trame afin que le client et le serveur puissent identifier la requête. L'attaque consiste ici à récupérer ce numéro d'identification (en sniffant le réseau) lors de la communication entre un client et un serveur DNS, puis, envoyer des réponses falsifiées au client avant la réponse du serveur DNS.

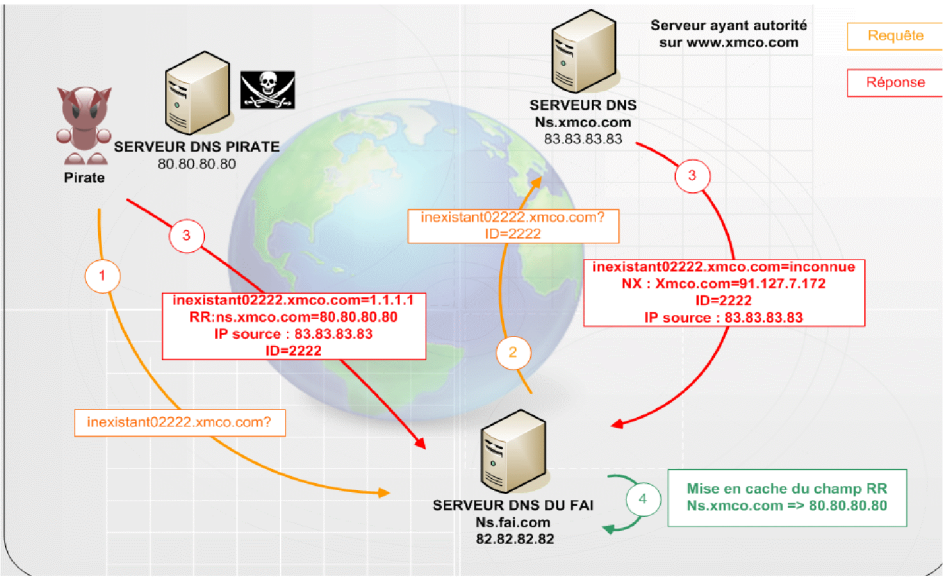

Figure 1.6: ID DNS Spoofing.

3. ARP Spoofing

Cette attaque consiste à rediriger le trafic d'une machine vers une autre. Grâce à cette redirection, une personne mal intentionnée peut se faire passer pour une autre. De plus, le pirate peut rerouter les paquets qu'il reçoit vers le véritable destinataire, ainsi l'utilisateur usurpé ne se rendra compte de rien. La finalité est la même que l'IP spoofing, mais ARP Spoofing (ARP Redirect) travaille au niveau de la couche liaison de données.

4. TCP Session Hijacking

Cette attaque consiste à rediriger un flux TCP afin de pouvoir outrepasser une protection par mot de passe. Ainsi le contrôle d'authentification s'effectuant uniquement à l'ouverture de la session, un pirate réussissant cette attaque parviendra à prendre possession de la connexion pendant toute la durée de la session. Dans un premier temps, le pirate doit écouter le réseau, puis lorsqu'il estime que l'authentification a pu se produire (délai de n secondes par exemple), il désynchronisera la session entre l'utilisateur et le serveur. Pour ce faire, il construit un paquet avec, comme adresse IP source, celle de la machine de l'utilisateur et le numéro d'acquittement TCP attendu par le serveur. En plus de désynchroniser la connexion TCP, ce paquet permettra au pirate d'injecter une commande via la session préalablement établie. [10]

5. Port scanning

Elle consiste à préciser quels ports sont ouverts afin de déterminer vulnérabilités du système. Le firewall va, dans tous les cas bloquer ces scans en annonçant le port comme fermé.

I.6.1.2.b. 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. Les problèmes de configuration

En général, les administrateurs réseau se contentent d'utiliser les configurations par défaut. Celles-ci sont souvent non sécurisées afin de faciliter l'exploitation du logiciel. De plus, des erreurs peuvent apparaître lors de la configuration d'un logiciel. Une mauvaise configuration d'un serveur peut entraîner l'accès à des fichiers importants ou mettre en jeu l'intégrité du système d'exploitation.

2. Les scripts

Les scripts s'exécutent sur un serveur qui renvoie les résultats de ces derniers au client. Cependant, lorsqu'ils sont dynamiques ils utilisent des entrées saisies par un utilisateur. Des failles peuvent apparaître si les entrées ne sont pas correctement contrôlées. L'exemple classique est l'exploitation de fichier à distance, tel que l'affichage du fichier mot de passe du système en remontant l'arborescence depuis le répertoire web.

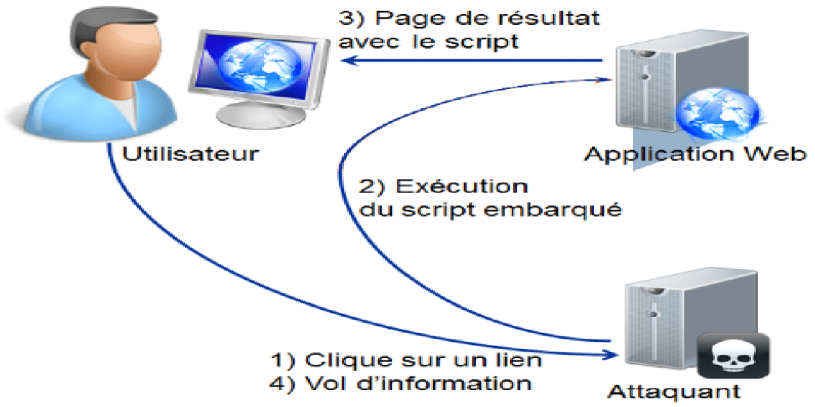

Figure1.7 : Attaque par script.

3. Les injections SQL

Tout comme les attaques de scripts, les injections SQL profitent de paramètres d'entrée non vérifiés. Le but des injections SQL est d'injecter du code SQL dans une requête de base de données. Ainsi, il est possible de récupérer des informations se trouvant dans la base (exemple : des mots de passe) ou encore de détruire des données. [12]

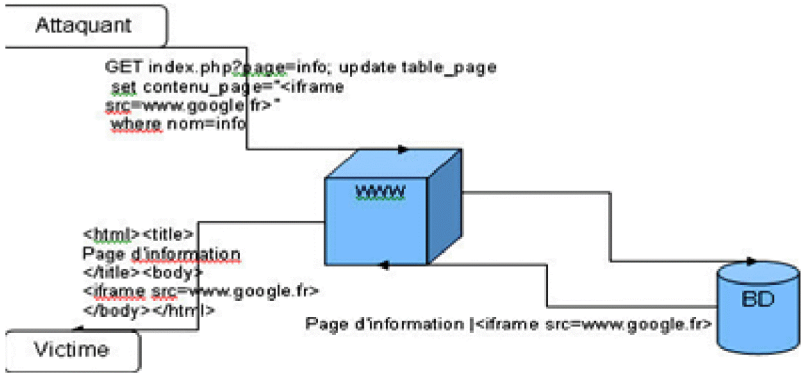

Figure1.8: Injection SQL.

4. 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.

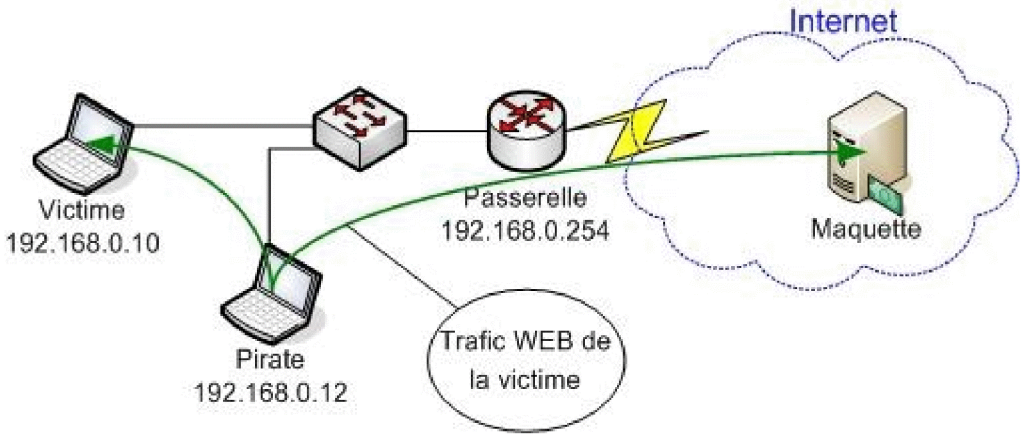

Figure1.9: Attaque Man in the middle.

5. 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 :

a. SYN Flooding

Le principe est de laisser un grand nombre de connexions TCP en attente. Le pirate envoie de nombreuses demandes de connexion (SYN), reçoit les SYN-ACK mais ne répond jamais avec ACK. Les connexions en cours occupent des ressources mémoire ce qui va entraîner une saturation et l'effondrement du système.

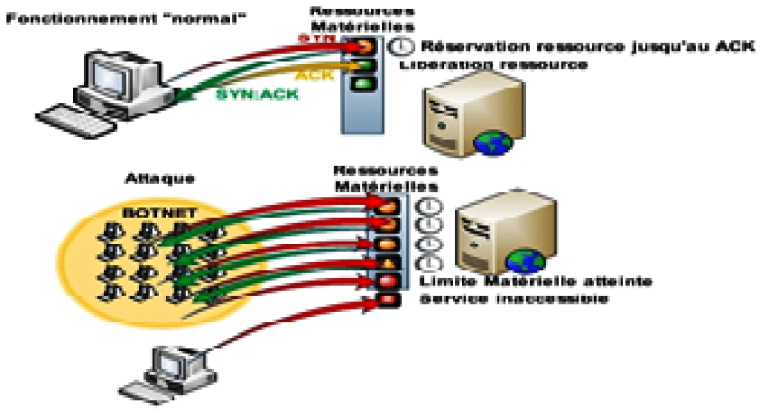

Figure1.10: SYN flooding.

b. UDP Flooding

Le trafic UDP est prioritaire sur TCP. Le but est donc d'envoyer un grand nombre de paquets UDP, ce qui va occuper toute la bande passante et ainsi rendre indisponible toutes les connexions TCP.

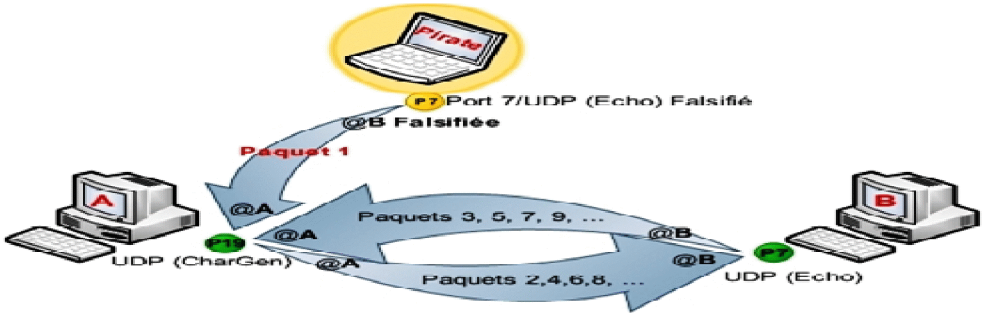

Figure1.11: UDP flooding.

c. Smurfling

Le pirate fait des requêtes ICMP ECHO à des adresses de broadcast en spoofant l'adresse source (en indiquant l'adresse de la machine cible). Cette machine cible va recevoir un nombre énorme de réponses, car toutes les machines vont lui répondre, et ainsi utiliser toute sa bande passante. [10]

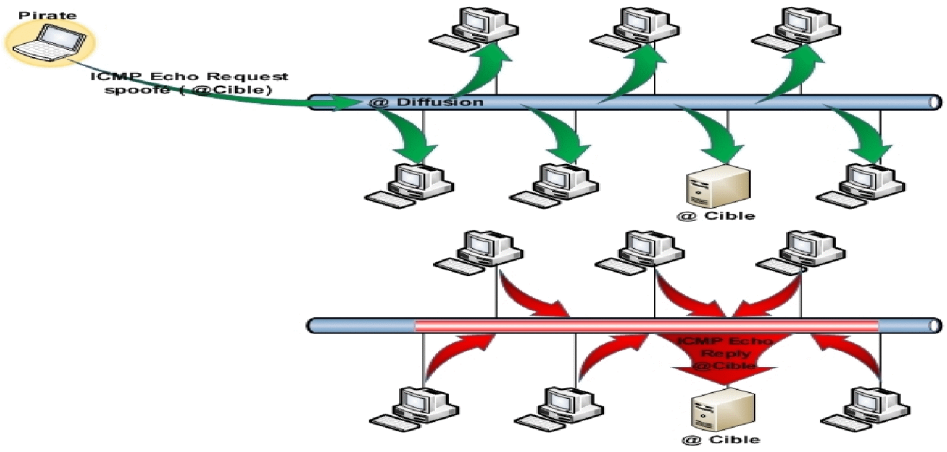

Figure1.12: Smurfling.

d. Déni de service distribué (DDoS)

Le but de DDoS est de reproduire une attaque normale à grande échelle. Pour ce faire, le pirate va tenter de se rendre maître d'un nombre important de machines. Grâce à des failles il va pouvoir prendre le contrôle de machines à distance et ainsi pouvoir les commander à sa guise. Une fois ceci effectué, il ne reste plus qu'à donner l'ordre d'attaquer à toutes les machines en même temps, de manière à ce que l'attaque soit reproduite à des milliers d'exemplaires. Ainsi, une simple attaque comme un SYN Flooding pourra rendre une machine ou un réseau totalement inaccessible.

7. 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 son épaule lors de la saisie du mot de passe peut lui permettre de le voir ou de le deviner.

8. 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]

9. 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]

10. Un ver

Un ver est un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique. Contrairement à un virus informatique, un ver n'a pas besoin d'un programme hôte pour se reproduire, il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction. L'objectif du ver est d'espionner l'ordinateur où il se trouve, offrir une porte dérobée à des pirates informatiques, détruire les données de l'ordinateur infecté et envoyer de multiples requêtes vers un serveur internet dans le but de le saturer (déni de service). Il a pour effet le ralentissement de la machine infectée.

11. Hameçonnage

L'hameçonnage (phishing) est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. Elle repose sur l'ingénierie sociale consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance afin de

lui soutirer des renseignements personnels comme numéro de carte de crédit, date de naissance. L'hameçonnage peut se faire par courrier électronique, par des sites Web falsifiés ou autres moyens électroniques.

12. 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. Parmi les motivations amenant les développeurs de logiciel à créer des portes dérobées, il y a :

- ✓ l'intérêt pratique d'un accès facile et toujours ouvert au logiciel pour pouvoir mener efficacement les actions de maintenance.
- ✓ la possibilité de désactiver secrètement le logiciel en cas de désaccord avec son client (non-paiement de licence).

Parmi les motivations amenant les pirates informatiques à installer une porte dérobée :

- ✓ La possibilité de surveiller ce que fait l'utilisateur légitime et de copier ou détruire des données ayant une valeur (mots de passe, clé privée pour déchiffrer des messages privés, coordonnées bancaires, secrets commerciaux).
- ✓ La possibilité de prendre le contrôle d'un ordinateur et de pouvoir l'utiliser pour mener des actions malfaisantes (envoi de courriels notamment pour l'hameçonnage, de virus informatiques, déni de service).
- ✓ Le contrôle d'un vaste réseau d'ordinateurs, qui peut être utilisé pour du chantage au déni de service distribué (DDoS), ou revendu à des criminels.

I.6.2. Les mécanismes de prévention et détections d'attaques

La sécurité contre les attaques distantes se renforce, notamment par le biais d'équipements réseaux plus puissants, mais les attaques locales restent toutefois encore fort efficaces. Les risques de failles applicatives sont, de ce fait, très grands et peuvent s'avérer dangereux pour des applications largement répandues. [17]

I.6.2.1. Les systèmes de prévention d'intrusion

Un système de prévention d'intrusion (ou IPS, Intrusion Prevention System) est un ensemble de composants logiciels et matériels dont la fonction principale est d'empêcher toute activité

suspecte détectée au sein d'un système. Les IPS sont des outils aux fonctions actives, qui en plus de détecter une intrusion, tentent de la bloquer. Parmi les types d'IPS :

- ✓ **Les systèmes de prévention d'intrusion kernel (KIPS) :**l'utilisation d'un préventeur d'intrusions au niveau noyau peut s'avérer parfois nécessaire pour sécuriser une station. Prenons l'exemple d'un serveur web, sur lequel il serait dangereux qu'un accès en lecture ou écriture dans d'autres répertoires que celui consultable via http, soit autorisé. En effet, cela pourrait nuire à l'intégrité du système. Grâce à un KIPS, tout accès suspect peut être bloqué directement par le noyau, empêchant ainsi toute modification dangereuse pour le système.

I.6.2.2. Les systèmes de détection d'intrusion

Afin de détecter les attaques que peut subir un système, il est nécessaire d'avoir un logiciel spécialisé dont le rôle serait de surveiller les données qui transitent sur ce système, et qui serait capable de réagir si des données semblent suspectes. Plus communément appelé IDS (Intrusion Detection Systems), les systèmes de détection d'intrusions conviennent parfaitement pour réaliser cette tâche. Il existe différents types d'IDS qui sont :

- ✓ **Les systèmes de détection d'intrusions :** c'est l'ensemble de composants logiciels et matériels dont la fonction principale est de détecter et analyser toute tentative d'effraction (volontaire ou non).Son fonctionnement consiste à la détection des techniques de port scanning, des tentatives de compromission de systèmes, d'activités suspectes internes ou encore des activités virales. Certains termes sont souvent utilisés quand on parle d'IDS :
  - ☑ **Faux positif** : une alerte provenant d'un IDS mais qui ne correspond pas à une attaque réelle.
  - ☑ **Faux négatif** : une intrusion réelle qui n'a pas été détectée par l'IDS.

- ✓ **Les systèmes de détection d'intrusions réseaux (NIDS) :** écoute tout le trafic réseau, puis l'analyse et génère des alertes si des paquets semblent dangereux. Le but des NIDS est d'analyser de manière passive les flux transitant sur le réseau et détecter les intrusions en temps réel.
- ✓ **Les systèmes de détection d'intrusions de type hôte (HIDS) :** se base sur une unique machine, n'analysant cette fois plus le trafic réseau mais l'activité se passant sur celle-ci. Il analyse en temps réel les flux relatifs à une machine ainsi que les fichiers journaux.

- ✓ **Les systèmes de détection d'intrusions hybrides :** généralement utilisés dans un environnement décentralisé, ils permettent de réunir les informations de diverses sondes placées sur le réseau. Leur appellation « hybride » provient du fait qu'ils sont capables de réunir aussi bien des informations provenant d'un système HIDS qu'un NIDS.

I.7. Les mécanismes de sécurité

I.7.1.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. [09]

I.7.1.1. 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 décrypter les messages.

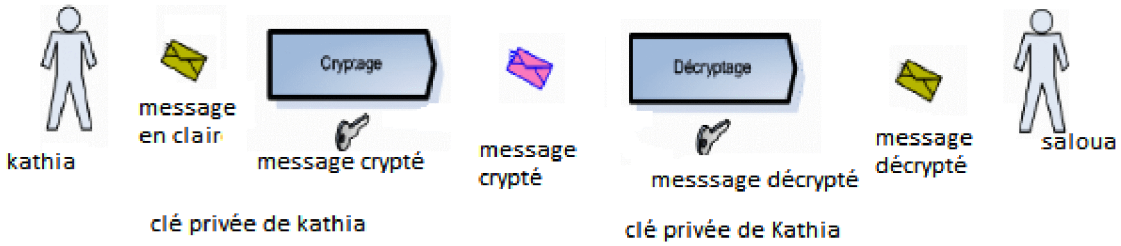

Figure1.13 : Cryptage symétrique.

I.7.1.2.Le cryptage asymétrique

Pour pallier la complexité induite par la gestion de la distribution des clés par cryptographie symétrique. Un autre type de cryptage qualifié d'asymétrique a été conçu et utilisé largement dans le monde de l'internet.

Ce système de cryptage utilise deux clés différentes pour chaque utilisateur, une privée et n'est connue que de l'utilisateur, l'autre publique et donc accessible par tout le monde.

Les clés publiques et privées sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante. Une clé est donc utilisée pour le cryptage et l'autre pour le décryptage. Ce cryptage présente l'avantage de permettre le placement de signatures numériques dans le message et ainsi permettre l'authentification de l'émetteur.

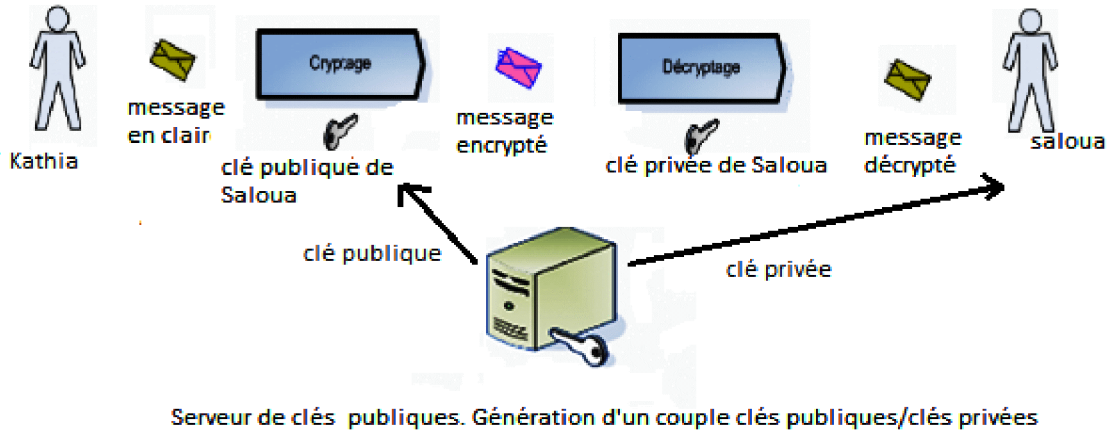

Figure1.14 : Le cryptage asymétrique.

I.7.1.3.Le cryptage à clé mixte

Il combine la cryptographie symétrique et asymétrique. La cryptographie asymétrique est intrinsèquement lente à cause des calculs complexes qui y sont associés, alors que la cryptographie symétrique brille par sa rapidité. Toutefois, cette dernière souffre d'une grave lacune, on doit transmettre les clés de manière sécurisée (sur un canal authentifié). Pour pallier ce défaut, la cryptographie hybride combine les deux systèmes afin de bénéficier des avantages (rapidité de la cryptographie symétrique pour le contenu du message) et utilisation de la cryptographie lente uniquement pour la clé.

I.7.2. 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.

I.7.2.1. 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.

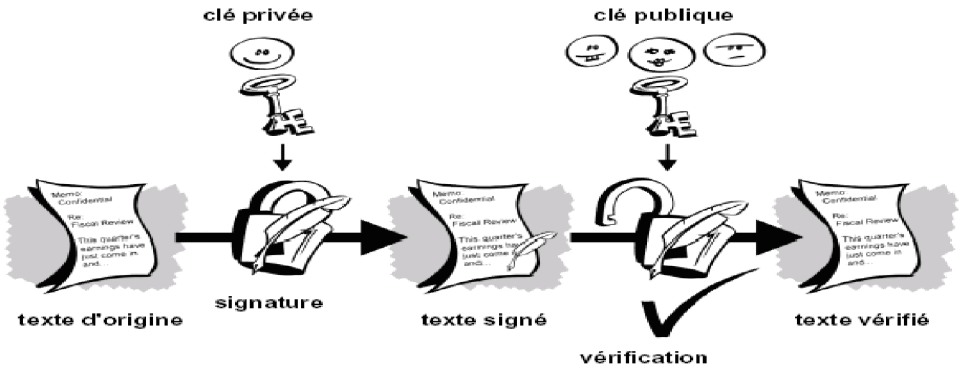

Figure1.15 : La technique de signature numérique.

I.7.2.2.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. [11]

I.7.3. Les Antivirus

Un antivirus est un logiciel informatique destiné à identifier et à effacer des logiciels malveillants (malwares), également appelés virus, Chevaux de Troie ou vers selon les formes. [12] L'antivirus analyse les fichiers entrants (fichiers téléchargés ou courriers électroniques), la mémoire vive de l'ordinateur et les périphériques de stockage comme les disques durs, internes ou externes, les clés USB et les cartes à mémoire Flash. La détection d'un logiciel malveillant peut reposer sur trois méthodes :

- ✓ reconnaissance d'un code déjà connu (appelé signature) et mémorisé dans une base de données.
- ✓ analyse du comportement d'un logiciel.
- ✓ reconnaissance d'un code typique d'un virus.

I.8. Les protocoles de sécurité

I.8.1.Protocole IPsec

IPSec (Internet Protocole Security) est un protocole de niveau 3. Il est très utilisé lors de la création de réseaux privés virtuels et pour la sécurisation des accès distants à un intranet. Les services IPSec sont basés sur des mécanismes cryptographiques qui leur confèrent un niveau de sécurité élevé. La sécurisation se faisant au niveau IP, IPSec peut être mis en œuvre sur tous les équipements du réseau et fournir un moyen de protection unique pour les échanges de données.

IPSec s'insère dans la pile de protocoles TCP/IP au niveau d'IP. Ceci présente l'avantage de le rendre exploitable par les niveaux supérieurs et d'offrir un moyen de protection unique pour toutes les applications. [12]

IPSec distingue deux niveaux de protection à travers deux protocoles :

- ✓ Authentification Header (AH) qui ne prend en charge que l'authentification, le contrôle d'intégrité et l'anti-rejeu. Le rejeu est une technique, utilisable par un intrus, qui consiste à renvoyer des paquets capturés lors d'une communication réseau légale.
- ✓ Encapsulating Security Payload (ESP) qui ajoute la fonction de confidentialité.

I.8.2.Protocole SSL

SSL (Secure Sockets Layer) est un protocole assurant la sécurité des échanges indépendamment du protocole applicatif utilisé. Il permet de chiffrer les communications entre deux machines et d'assurer la confidentialité des données, l'authentification de l'utilisateur et du serveur, ainsi que l'intégrité des données par signature électronique.

Le principe d'une authentification du serveur avec SSL est le suivant :

- ✓ Le navigateur du client fait une demande de transaction sécurisée au serveur.
- ✓ Suite à la requête du client, le serveur envoie 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 choisit l'algorithme.
- ✓ Le serveur envoie son certificat avec les clés cryptographiques correspondantes au client.

- ✓ Le navigateur vérifie que le certificat délivré est valide.
- ✓ Si la vérification est correcte alors le navigateur du client envoie au serveur une clé secrète chiffrée à l'aide de la clé publique du serveur qui sera donc le seul capable de déchiffrer puis d'utiliser cette clé secrète. [02]

I.8.3. Protocole HTTPs

HTTPs (HTTP sécurisé) est un procédé de sécurisation des transactions HTTP utilisé pour la navigation sécurisée**.** Il offre des possibilités d'authentification et de chiffrement pour les sites web nécessitant un certain niveau de sécurité dans leurs échanges avec les navigateurs web. Pour garantir cette sécurité, il fait usage de méthodes de cryptographie asymétrique pour l'authentification et de méthodes de cryptographie symétrique pour le chiffrement des échanges.

Contrairement à SSL au niveau de la couche de transport, HTTPs procure une sécurité basée sur des messages au dessus du protocole HTTP, en marquant individuellement les documents html à l'aide de certificats. SSL permet de sécuriser la connexion internet tandis que HTTPs permet de fournir des échanges HTTP sécurisé.

I.8.4. Le protocole PGP

PGP (Pretty Good Privacy) utilise la cryptographie Hybride, il est classé dans les systèmes à clés de session. C'est un système qui utilise à la fois le principe de chiffrement à clés privées et le principe de chiffrement à clés publiques. [12]

I.8.5. Le protocole SSH

Le SSH (Secure Shell) permet de répondre à la principale problématique posée par la sécurité des informations et la confidentialité. En effet, grâce à ce protocole, il est possible de chiffrer des données par un système de clés privées et publiques. Ces données transitent dans un tunnel, une sorte de canal sécurisé où 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 sécurité suivantes :

- ✓ Après avoir effectué une connexion initiale, le client peut s'assurer de s'être connecté au même serveur lors des sessions suivantes.
- ✓ Le client peut transmettre ses données d'authentification au serveur, telles que son nom d'utilisateur et son mot de passe, en format crypté.
- ✓ Toutes les données envoyées et reçues pendant la connexion sont transférées de façon chiffrée, ce qui les rend extrêmement difficiles à déchiffrer et impossible à lire.

I.8.6. Le protocole PKI

PKI (Public Key Infrastructure) se base sur le chiffrement asymétrique. Selon cette formule, une organisation ou une personne s'adresse à un tiers de confiance appelé autorité de certification ou CA (Certification Authority) pour lui demander une paire de clés de chiffrement. L'une de ces clés est privée (secrète) et l'autre publique (disponible dans une base de données accessible par le public).Une fois en possession de ses clés, l'organisation ou la personne peut communiquer sur tout type de réseau de manière sécurisée. Les PKI sont des structures précises assurant en particulier la création et la gestion des certificats. [18]

I.8.7. Le protocole Kerberos

Le protocole d'authentification Kerberos est un exemple d'authentification des applications par un serveur dédié. Ce service est réalisé par un serveur central d'authentification qui permet d'authentifier serveurs et utilisateurs de serveurs via des mots de passes. Serveurs et clients doivent êtres enregistrés auprès des serveurs Kerberos. Celui-ci stocke dans sa base de données des informations relatives à leurs identifications, mots de passe, permissions et droits d'accès. Il partage avec chacun d'entre eux une clé secrète. Un serveur dessert plusieurs utilisateurs et serveurs qu'il connait et qui appartiennent à son domaine. L'authentification inter-domaine Kerberos est assurée par un mécanisme de dialogue entre différents serveurs Kerberos, à condition qu'ils se connaissent et qu'ils partagent pour cet échange une clé secrète. [02]

I.9.Gestion du rôle Serveur NPS

Le serveur NPS (Network Protection Server) permet de créer et de mettre en œuvre des stratégies d'accès réseau à l'échelle d'une entreprise pour assurer l'intégrité des clients, l'authentification et l'autorisation des demandes de connexion. Il permet aussi de configurer et de gérer de manière centralisée l'authentification d'accès réseau, l'autorisation et les stratégies d'intégrité des clients avec les trois fonctionnalités suivantes :

- ✓ **Serveur RADIUS** :(Remote Authentication Dial-In User Service), est un service d'authentification standard, il est utilisé pour authentifier les postes de travail sur les réseaux locaux, qu'ils soient filaires ou sans fils. Son fonctionnement est basé sur un système client/serveur chargé de définir les accès d'utilisateurs distants à un réseau. Il repose principalement sur le serveur RADIUS, relié à une base d'identification comme une base de données et un client RADIUS, appelé **NAS** (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur. L'ensemble des transactions entre le

client RADIUS et le serveur RADIUS est chiffrée et authentifiée grâce à un secret partagé. **[19]**

- ✓ **Serveur de stratégie NAP** : lorsque le serveur NPS est configuré en tant que serveur de stratégie NAP, NPS évalue les déclarations d'intégrité envoyées par les ordinateurs clients compatibles avec la protection d'accès réseau (NAP) qui tentent de se connecter au réseau en assurant l'authentification et l'autorisation des demandes de connexion. Il peut configurer des stratégies NAP et des paramètres dans le serveur NPS, y compris les programmes de validation d'intégrité système, la stratégie de contrôle d'intégrité et les groupes de serveurs de mise à jour qui permettent aux ordinateurs clients de mettre à jour leur configuration afin de se conformer à la stratégie réseau de l'organisation.
- ✓ **Proxy RADIUS** : le serveur NPS utilisé en tant que proxy RADIUS permet de configurer des stratégies de demande de connexion qui spécifient, les demandes de connexion transmises par le serveur NPS à d'autres serveurs RADIUS et les serveurs RADIUS auxquels on souhaite transmettre les demandes de connexion. Il est également possible de configurer le serveur NPS de manière à ce qu'il transmette les données de comptes à un ou plusieurs ordinateurs dans un groupe de serveurs RADIUS distants à des fins de journalisation.

I.10.Les VPN

VPN (Virtual Private Network) ou RPV (Réseau privé virtuel) est une technique permettant à un ou plusieurs postes distants de communiquer de manière sure, tout en empruntant les infrastructures publiques. Ce type de liaison est apparu suite à un besoin croissant des entreprises de relier les différents sites, et ce de façon simple et économique.

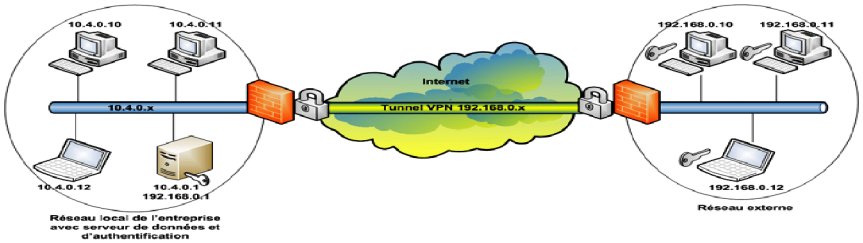

Figure1.16 : Réseau privé virtuel.

Un réseau VPN repose sur le protocole de tunneling. Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets de l'entreprise, les VPN d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagé, comme internet. [13]

I.10.1.Les différents types de VPN

Selon les besoins, on distingue trois types de VPN :

- ✓ **Le VPN d'accès** : il est utilisé pour permettre à des utilisateurs nomades d'accéder au réseau de leur entreprise. L'utilisateur se sert d'une connexion internet afin d'établir une liaison sécurisée.
- ✓ **L'intranet VPN** : il est utilisé pour relier deux ou plusieurs intranets d'une même entreprise entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants .Cette technique est également utilisée pour relier des réseaux d'entreprise, sans qu'il soit question d'intranet (partage de données, de ressources, exploitation de serveurs 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 cas, il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès. De plus, seul une partie des ressources sera partagée, ce qui nécessite une gestion rigoureuse des espaces d'échange.

I.11. Les VLAN

Un VLAN permet de créer des domaines de diffusion (domaines de broadcast) gérés par les commutateurs indépendamment de l'emplacement où se situent les nœuds, ce sont des domaines de diffusion gérés logiquement. [14]

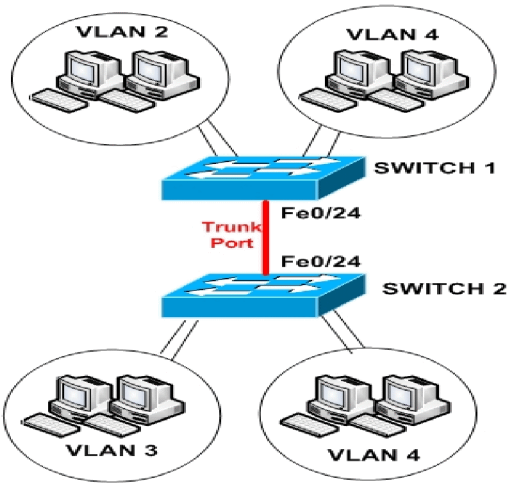

Figure1.17 : Exemple de VLAN.

I.11.1.Les différents types de VLAN

Pour répondre aux objectifs des VLAN, la règle suivante doit être impérativement respectée, une trame doit être associée à un VLAN et un seul et ne peut pas sortir du VLAN, sinon l'étanchéité du niveau 2 n'est plus respectée.

Les méthodes de construction d'un VLAN doivent donc déterminer la façon dont le commutateur va associer la trame à un VLAN. Usuellement on présente trois méthodes pour créer des VLAN : les vlan par port (niveau 1), les Vlan par adresses MAC (niveau 2), les VLAN par adresses IP (niveau 3) ainsi que des méthodes dérivées.

- ✓ **Les VLAN par port (Vlan de niveau 1) :** chaque port des commutateurs est affecté à un VLAN. L'appartenance d'une trame à un VLAN est alors déterminée par la connexion de la carte réseau à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN. Si une station est physiquement déplacée, il faut désaffecter son port du Vlan puis affecter le nouveau port de connexion de la station au bon Vlan. Si une station est logiquement déplacée, il faut modifier l'affectation du port au Vlan.
- ✓ **Les Vlan par adresse MAC (Vlan de niveau 2) :** chaque adresse MAC est affectée à un VLAN. L'appartenance d'une trame à un VLAN est déterminée par son adresse MAC. En effet il s'agit, à partir de l'association Mac/VLAN, d'affecter dynamiquement les ports des commutateurs à chacun des VLAN en fonction de l'adresse MAC de l'hôte qui émet sur ce port. L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation géographique. Si une station est déplacée sur le réseau physique, son adresse physique ne changeant pas, elle continue d'appartenir au même VLAN (ce fonctionnement est bien

adapté à l'utilisation de machines portables). Si on veut changer de Vlan il faut modifier l'association Mac / Vlan.

- ✓ **Les Vlan par adresse de Niveau 3 (VLAN de niveau 3) :** une adresse IP est affectée à un VLAN. L'appartenance d'une trame à un VLAN est alors déterminée par son adresse IP .En effet, il s'agit à partir de l'association adresse IP/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLAN. Dans ce type de VLAN, les commutateurs apprennent automatiquement la configuration des VLAN en accédant aux informations de couche 3. Ceci est un fonctionnement moins rapide que le Vlan de niveau 2. Quand on utilise le protocole IP on parle souvent de Vlan par sous-réseau.

I.12. Le NAT

Dans les entreprises de grandes taille, différents réseaux interconnectés peuvent utiliser les mêmes adresses IP .Pour que la communication soit possible entre nœuds des deux coté, il est nécessaire de modifier les références de l'émetteur de paquets afin qu'il n'y ait pas de conflits et que la transmission soit fiable.

Des équipements de translation d'adresse NAT (Network Address Translation) sont chargés d'adopter cette fonctionnalité .Ils permettent le changement d'une adresse IP par une autre.

Trois types d'adresse sont possibles :

- ✓ La translation de port PAT (Port Address Translation), joue sur une allocation dynamique des ports TCP ou UDP, en conservant l'adresse IP d'origine.
- ✓ La conversion dynamique d'adresses (NAT dynamique) change à la volée d'adresse IP par rapport à une externe disponible dans une liste.
- ✓ La conversion statique d'adresse (NAT statique), effectue également un changement d'adresse IP, mais une table est maintenue, permettant à une adresse IP interne de toujours être remplacée par la même adresse IP externe. [15]

I.13. Les ACL

Les listes de contrôle d'accès (Access Control List) ont pour objectif de disposer d'une fonction de filtrage prenant en compte l'historique des connexions en cours, afin de ne pas accepter du trafic qui n'aurait pas été demandé à partir d'une zone précise du réseau. [04]

Les ACL semblent avoir toujours existé sur les routeurs et rares sont les configurations où elles n'apparaissent pas. Elles servent principalement au filtrage des paquets sur les interfaces physiques. Cependant leur mode de définition est employé pour catégoriser les réseaux en vue, entre autre, de les injecter dans un protocole de routage ou de les soumettre à une règle de qualité de service.

Il existe deux types d'ACL :

- ✓ **Les ACL standard :** permettent d'autoriser ou de refuser le trafic en provenance d'adresse IP source et la destination du paquet, tandis que les ports n'ont aucune incidence.
- ✓ **Les ACL étendues :** filtrent les paquets IP en fonction de plusieurs attributs, dont le type de protocole, l'adresse IP source, l'adresse IP destination, les ports TCP ou UDP source et destination et les informations facultatives sur le type de protocole pour une meilleure précision du contrôle.

Lors de la configuration des ACL, chaque liste est identifiée par un numéro unique attribué. Ce numéro permet d'identifie le type d'ACL créé et doit être compris dans les plages suivantes :

- ✓ Les ACL standard : 1-99 ,1300-1999.
- ✓ Les ACL étendues : 100-199, 2000-2699.

I.14.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 selon l'entreprise comme le souligne Rivière, le Pdg de Lexsi (laboratoire d'expertise en sécurité informatique) : « Une politique de sécurité ne se met pas en place en fonction du nombre de postes, mais du métier de l'entreprise, de la valeur des données qui circulent et de ce que représente l'outil informatique pour sa pérennité ». Donc une politique de sécurité comprend un ensemble de bases définissant une stratégie, des directives, des procédures, des codes de conduite, des règles organisationnelles et techniques.

Dans le deuxième chapitre nous aborderons les mécanismes de sécurité, toujours, pour augmenter le niveau de sécurité.

Chapitre II : Sécurisation des interconnexions réseaux

II.1.Introduction

Un réseau est soumis régulièrement à de nombreuses évolutions et modifications avec le développement de la technologie et le besoin de sécurité qui l'accompagne. Le moins que l'on puisse affirmer, c'est que ces dernières années le domaine de la sécurité a explosé. Les petites et grandes entreprises en passant par les particuliers, tout ce grand monde revendique les moyens à la pointe de la technologie pour mieux protéger leurs systèmes d'informations et l'interconnexion réseaux. Les solutions d'interconnexions réseaux étant diverses et variées avec l'internet, l'avènement de la téléphonie IP et les réseaux sans fil. La mise en place d'une sécurisation des réseaux informatiques efficace n'est pas chose simple face à la variété de choix auquel on est confronté.

Dans ce chapitre, nous présenterons ces différents choix, nous expliquerons la vision de Cisco qui a introduit le self-defending Network, la notion de découpage en zone qui est un moyen incontournable, et nous introduirons le système ou l'ensemble de différents composants matériels et logiciels permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers, notamment internet.

II.2. L'architecture réseau et sécurité

II.2.1. L'auto défense du réseau

Le concept d'auto défense du réseau (self-defending Network) est une approche de la sécurité des réseaux introduite par Cisco. Ce concept s'étend à toutes les couches du modèle OSI et offre des services sécuritaires aux équipements, utilisateurs et applications. Connecté à des systèmes de contrôle et de surveillance, il en résulte une architecture réseau sécurisée.[04]

Cette approche consiste à scinder l'architecture globale en zones fonctionnelles recevant chacune un niveau de sécurité en fonction de sa position et de son rôle. Les zones sont :

- ✓ Zone infrastructure qui représente le réseau interne. Ce dernier est à son tour divisé en trois zones.
  - les filiales.
  - les réseaux longue distance (WAN).
  - la zone DMZ.
- ✓ Zone applicative (Datacenter) qui comprend les aires de stockage, les centres applicatifs et les services de téléphonie sur IP.

II.2.1.1.Découpage en zones de sécurité

Le découpage en zones fonctionnelles facilite considérablement les tâches de surveillance et d'administration en ciblant les mesures de sécurité en fonction de la zone concernée. De plus, chaque zone obtient une certaine indépendance dans sa gestion ce qui ne remet pas en cause la gestion de la sécurité des autres zones qui l'entourent. Toutefois, il faut garder en mémoire que la sécurité d'une zone est étroitement dépendante de celle des zones qui l'entourent. La création et l'exploitation des zones de sécurités doivent être soumises aux règles suivantes :

- ✓ Un équipement ou un hôte qui viendrait à changer de zone doit se conformer aux règles de sécurité de la nouvelle zone.
- ✓ Le trafic ne doit pas transiter entre deux zones dans le sens de la zone la moins sécurisée vers la zone la plus sécurisée.

II.2.1.1.a. La zone infrastructure

La zone infrastructure est la première des zones de sécurité à considérer car elle est au centre du système d'information. L'étendue de cette zone comprend, le cœur du réseau et la zone d'accès. Il existe trois zones de base :

- ✓ **La zone d'accès** : c'est l'extrémité du réseau qui comprend les commutateurs sur lesquels sont connectés les postes de travail. Elle est dérivée en deux familles :
  - Les zones dans lesquelles sont fournis des accès filaires.
  - Les zones dans lesquelles sont fournis des accès sans fil.

  Elle est essentiellement sécurisée. C'est la qu'intervient l'authentification obligatoire avant toute possibilité de communiquer. Elle permet aussi la protection contre les attaques par déni de service et par usurpation de session.
- ✓ **La zone d'agrégation** : elle est située immédiatement à la suite de la zone d'accès à laquelle elle peut être combinée à des fins de simplification. Ce sont donc les techniques de sécurité au niveau 3 qui prévalent comme le filtrage inter VLAN, les ACL de tous types et la protection des protocoles de routage.
- ✓ **La zone de cœur du réseau** : elle ne reçoit pas à proprement parler de fortes mesures de sécurité car, étant au centre de la zone d'infrastructure, elle bénéficie de la sécurité des zones qui l'entourent. Malgré tout, la sécurité de cette zone existe. Elle se concentre autour des principes de sécurité des équipements, des protocoles de routage et de la sûreté de fonctionnement grâce aux multiples techniques de redondance.

La zone d'infrastructure bénéfice donc d'une sécurité physique renforcée. Le schéma suivant représentant un exemple de zone d'infrastructure.

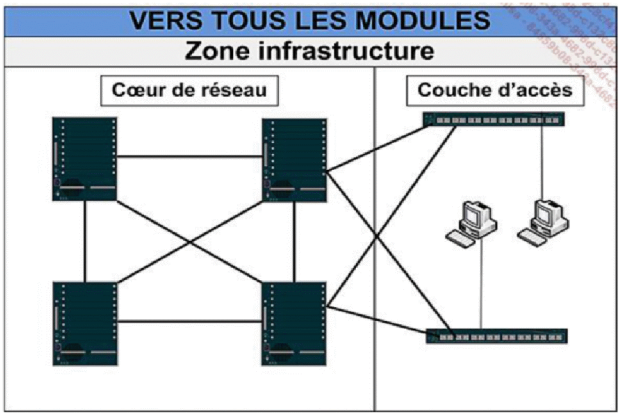

Figure2.1 : Zone infrastructure.

II.2.1.1.b. Les filiales

Une filiale est une zone à part entière de l'entreprise et dispose en règle générale de moyens limités pour assurer sa propre sécurité. L'efficacité maximale est recherchée avec un nombre réduit d'équipements. Elle est généralement traitée comme une extension du réseau local et à ce titre bénéficie de tous les services applicatifs.

La sécurité d'une filiale est sensiblement identique à celle des zones d'accès. Des protocoles sont chargés d'assurer une stricte authentification des utilisateurs ainsi que la distribution de droits d'accès réseau sous la forme d'ACL reçues après le processus de connexion.

Les communications de la filiale vers le site central sont habituellement chiffrées. Cette mesure se justifie pleinement, si le réseau Internet est voué à cette tâche d'interconnexion. La suite IPSec est tout naturellement indiquée pour accomplir cette tâche entre un équipement de la filiale et un équipement dédié sur le site central.

La figure ci-dessous montre une zone filiale simple pour laquelle deux équipements sont en service.

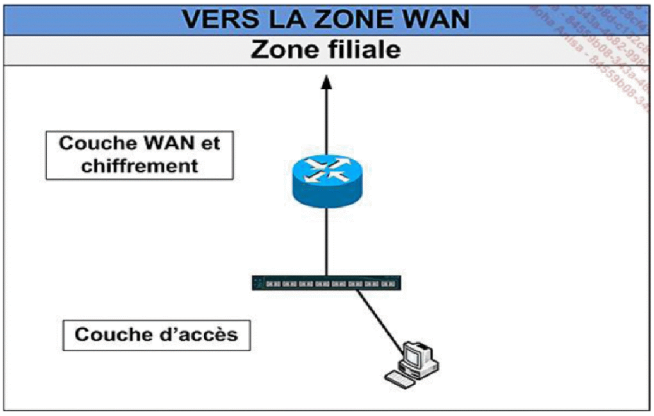

Figure2.2 : Zone filiale.

II.2.1.1.c. WAN

La zone WAN est raccordée aux diverses interfaces qui la relient au monde extérieur. Ainsi, un sous-réseau est attribué au recueil des collaborateurs nomades, un autre correspond aux arrivées Internet et un dernier est dédié aux filiales. La sécurité sur cette zone comprend les ACL qui écartent du réseau tous les trafics indésirables en provenance d'Internet et la protection logique des équipements. Il est primordial de prendre les mesures de protection visant à limiter certains types de trafic en fonction de leur débit afin de se prémunir contre les attaques par saturation.

Le schéma ci-dessous illustre un exemple d'un WAN :

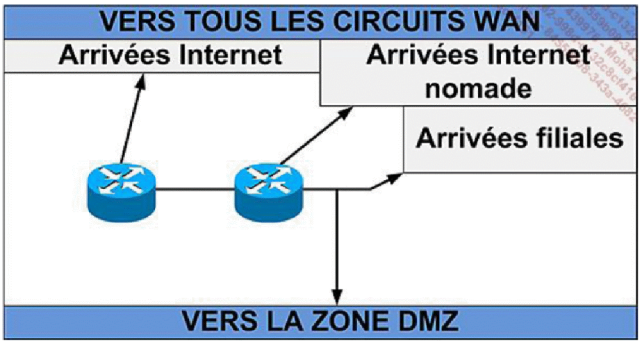

Figure2.3 : Zone WAN.

II.2.1.1.d. La zone DMZ

Les DMZ (De-Militarized Zone) est un sous réseau qui forme une zone tampon entre la partie privée du réseau local et le monde extérieur. Son rôle consiste à assurer la défense contre les tentatives d'intrusions en prévenance de l'internet, qu'elles concernent le trafic intranet, extranet ou internet. Elle se compose d'un ou plusieurs ordinateurs formant l'infrastructure d'un système de défense du périmètre qui sécurise l'essentiel des communications. [18]

L'installation de la DMZ ne pose pas de problème de sécurité intrinsèque, en effet, toutes ses communications sont contrôlées et autorisées par le firewall de la passerelle. Les problèmes de sécurité sont donc en grande partie gérés en amont. D'autre part, l'utilisation du NAT rend très difficile (souvent impossible) l'accès direct à la DMZ par un éventuel pirate.

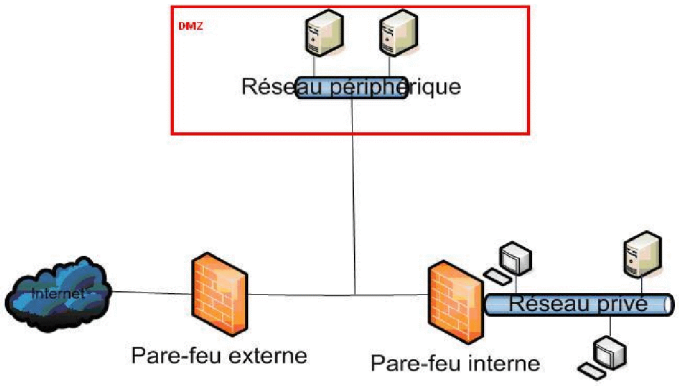

Figure2.4 : Zone DMZ.

II.2.1.1.e. La zone Datacenter

La zone Datacenter (centre de traitement de données) héberge les serveurs centraux et des baies de stockage de grande capacité. Cette notion implique une concentration des moyens en un lieu unique dont la sécurité logique est l'une des composantes fortes. Un Datacenter combine en effet toutes les composantes de la sécurité et requiert un niveau de disponibilité à la hauteur de la criticité des informations qu'il héberge. Les mesures de protections associées à ce dernier vont de la protection physique des accès, à la redondance électrique en passant par la protection contre les incendies.

La sécurité au niveau réseau du Datacenter repose principalement sur le déploiement d'ACL qui vise à garantir que le trafic entrant autorisé correspond aux services fournis par le Datacenter. Il en va de même en sens inverse en s'assurant de la correspondance du trafic sortant avec les requêtes émises de l'extérieur. Etant une zone interne, le trafic qui y transite n'est habituellement pas chiffré. Cette disposition favorise le déploiement de dispositif d'analyse et de surveillance comme les sondes de détections d'intrusions finement ajustées sur les trafics caractéristiques de la zone. S'il est

décidé de chiffrer le trafic, il conviendra de disposer de relais si la surveillance est souhaitée. La figure suivante montre un exemple d'architecture d'une zone Datacenter.

Figure2.5 : Zone Datacenter.

II.2.2. Les Firewalls

II.2.2.1.Définition

Le ciment entre les diverses zones est le firewall (pare-feu). C'est un système ou un ensemble de différents composants matériels et logiciels permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers, notamment Internet. Il permet le filtrage des paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

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

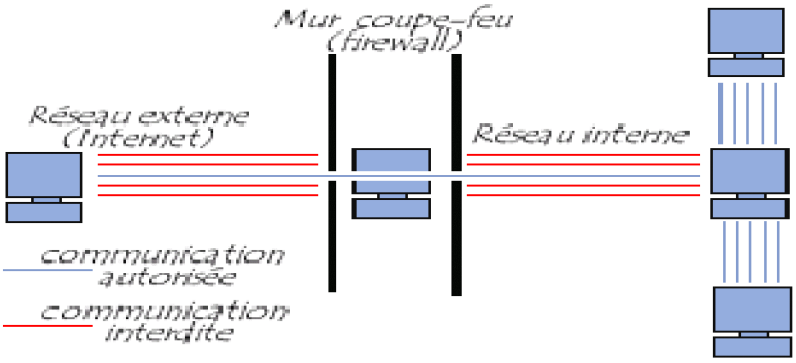

Figure2.6 : Exemple de firewall.

Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. Il est possible de mettre un système firewall sur n'importe quelle machine et avec n'importe quel système à condition que :

- ✓ La machine soit suffisamment puissante pour traiter le trafic.
- ✓ Le système soit sécurisé.
- ✓ Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.

II.2.2.2. Les fonctions d'un firewall

Un firewall dispose de plusieurs fonctions dont :

- ✓ Autoriser la connexion (*allow*)
- ✓ Bloquer la connexion (*deny*).
- ✓ Rejeter la demande de connexion sans avertir l'émetteur (*drop*).
- ✓ Autoriser ou interdire l'ouverture d'un service.
- ✓ Utiliser un protocole.
- ✓ Autoriser ou bannir une adresse IP source/destination.
- ✓ Vérifier ou inspecter la conformité du trafic.

II.2.2.3.Les différents types de firewall

a. 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 à une autre en leur appliquant les règles prédéfinies. En effet, quand une requête ARP est émise sur le câble réseau, le firewall ne répond jamais et comme il ne fait que transmettre les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirigée directement contre le firewall, étant donné qu'aucun paquet ne sera traité par ce dernier comme étant sa propre destination. Donc, la seule façon de le contourner est de passer outre ses règles. Toute attaque devra donc faire avec ses règles, et essayer de les contourner. [20]

Comme tous les firewalls ce dernier contient des avantages et des inconvénients :

Avantages

- ✓ Impossible de l'éviter (les paquets passeront par ses interfaces).
- ✓ Peu coûteux.

Inconvénients

- ✓ Possibilité de le contourner (il suffit de passer outre ses règles).
- ✓ Configuration souvent contraignante.
- ✓ Les fonctionnalités présentes sont très basiques (filtrage sur adresse IP, port, le plus souvent en Stateless).

b. Les firewalls matériels

Ils sont 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 interaction avec les autres fonctionnalités du routeur est simplifiée par leur présence sur le même équipement réseau. Souvent relativement peu flexibles en termes de configuration, ils sont aussi peu vulnérables aux attaques. De plus, étant souvent très liés au matériel, l'accès à leur code est assez difficile. Leur administration est souvent plus aisée que les firewalls bridges. Et leur niveau de sécurité est de plus très bon sauf découverte de failles éventuelles comme dans tous firewalls.

Avantages

- ✓ Intégré directement dans la machine.
- ✓ Administration relativement simple.

Inconvénients

- ✓ Dépendant du constructeur pour les mises à jour.
- ✓ Souvent peu flexibles car seules les spécificités prévues par le constructeur du matériel sont implémentées.

c. Les firewalls logiciels

Présents à la fois dans les serveurs et les routeurs, ils peuvent être classés en plusieurs catégories :

c.1. Les firewalls personnels

Ils ont pour but de sécuriser un ordinateur particulier, et non pas un groupe d'ordinateurs. Souvent payants, ils peuvent être contraignants et quelque fois très peu sécurisés. En effet, ils s'orientent plus vers la simplicité d'utilisation plutôt que vers l'exhaustivité, afin de rester accessible à l'utilisateur final.

c.2. Les firewalls plus

Tournant généralement sous linux, ils ont généralement le même comportement que les firewalls matériels des routeurs, à ceci près qu'ils sont configurables à la main.

II.2.2.4. Les types de filtrage des paquets

II.2.2.4 .a. Le filtrage simple de paquets

Le filtrage de paquets sans état (Stateless Packet Filtering) est un système firewall qui fonctionne sur le principe du filtrage simple de paquets. Il analyse les en-têtes de chaque paquet de données (datagramme) échangé entre une machine du réseau interne et une machine externe. Les en-têtes analysés sont :

- ✓ 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.

II.2.2.4 .b. Le filtrage dynamique de paquets

Le filtrage de paquets avec état ou (Stateful Packet Filtering) est la méthode de filtrage la plus simple, elle opère au niveau de la couche réseau et transport du modèle OSI. La plupart des routeurs d'aujourd'hui permettent d'effectuer du filtrage simple de paquet. Cela consiste à accorder ou refuser le passage de paquet d'un réseau à un autre en se basant sur :

- ✓ L'adresse IP Source/Destination.
- ✓ Le numéro de port Source/Destination.
- ✓ Le protocole de niveau 3 ou 4 du modèle OSI.

II.2.2.4 .c. Le filtrage applicatif

Le filtrage applicatif permet de filtrer les communications application par application. Il opère au niveau de la couche application du modèle OSI, il suppose une connaissance des protocoles utilisés par chaque application sur le réseau, et notamment de la manière dont elle structure les données échangées.

Un firewall effectuant un filtrage applicatif est appelé passerelle applicative ou proxy, car il sert de relais entre deux réseaux en s'interposant et en effectuant une validation fine du contenu des

paquets échangés. Le proxy représente donc un intermédiaire entre les machines du réseau interne et externe, subissant les attaques à leur place. De plus, le filtrage applicatif permet la destruction des en-têtes précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire.

Il s'agit d'un positionnement, assurant une bonne protection du réseau, pour peu qu'il soit correctement administré. En contrepartie, une analyse fine des données applicatives requiert une grande puissance de calcul et se traduit donc souvent un ralentissement des communications, chaque paquet devant être finement analysé.

Par ailleurs, le proxy doit nécessairement être en mesure d'interpréter une vaste gamme de protocoles et de connaître les failles pour être efficace. Le but d'un serveur proxy est d'isoler une ou plusieurs machines pour les protéger, comme l'illustre la figure ci-dessous :

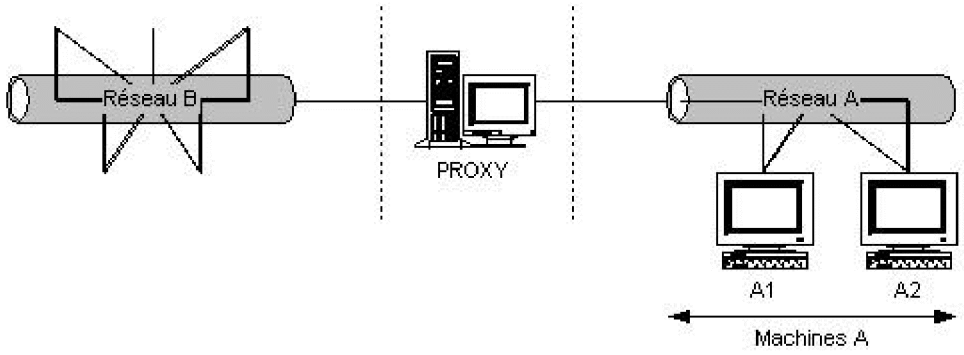

Figure2.6 : Proxy.

II.3.Conclusion

Le partage en ligne d'informations, l'utilisation de plus en plus courante et indispensable de la toile nous amène à nous protéger des risques d'insécurité liés à l'internet. Il est donc devenu impératif de protéger l'infrastructure des réseaux informatiques. Les moyens définis dans ce chapitre permettent une grande liberté de l'usage du net, le transfert de données secret, le recours à la vidéo conférence et la téléphonie IP dans des conditions optimales et sécurisées. Certes il ne faut pas oublier qu'une sécurité inviolable n'est qu'éphémère. Mais les moyens comme découpage en zone, le data-center et le firewall qui permet d'isoler des environnements, masquer des ressources, filtrer le flux entrant et sortant, renforcent la protection des systèmes internet donc des réseaux informatiques en réalisant des périmètres de sécurités optimaux.

Ayant vu les fonctionnalités et types de firewall, on pourrait se demander quels sont les plus utilisés, les nouveautés dans ce domaine et le quel utiliser. Dans le prochain chapitre nous présenterons les firewalls les plus récents comme TMG, ASA et d'autres.

Chapitre III : Les solutions matérielles

III.1. 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, des passerelles VPN, et des systèmes de détection d'intrusion. Dans ce chapitre nous présenterons les firewalls, PIX, ASA, TMG, FortiGate et SideWinder.

III.2. Le firewall PIX

III.2.1. Présentation

Le Cisco PIX (Private Internet eXchange) est une appliance prenant en charge les fonctions de firewall et NAT. Installé sur un réseau, il détermine si le trafic est autorisé, dans un sens ou dans l'autre. Le cas échéant, il active la connexion, celle-ci aura un impact quasiment nul sur les performances du réseau. Les données d'un trafic non autorisé sont détruites.

La gamme PIX étant disponible dans de nombreux formats, peut s'adapter à tous les types de réseaux. Il est mis en place au niveau des passerelles du réseau. Il est généralement installé sur le périmètre du réseau, entre le réseau externe et l'intranet d'une autre entreprise ou le réseau public Internet. Ainsi aucun équipement supplémentaire n'est nécessaire au bon fonctionnement de ce produit. [21]

Figure 3.1: Le firewall PIX.

III.2.2. Principaux avantages et fonctionnalités

Le PIX possède plusieurs avantages et fonctionnalités parmi eux :

- ✓ **Sécurité:** Cisco PIX Firewall utilise un système d'exploitation sécurisé dédié à la protection du routeur et des réseaux.
- ✓ **Performances:** le PIX prend en charge plusieurs fois la capacité des routeurs concurrents et assure un niveau de sécurité sans égal, avec un impact minimum sur les performances du réseau.
- ✓ **Stabilité:** le PIX étant dédié à un objectif unique, la sécurité, il est particulièrement stable. La stabilité est un point essentiel pour un dispositif d'une telle importance dans l'architecture du réseau. Le temps moyen entre les défaillances d'un PIX est supérieur à six ans.
- ✓ **Evolutivité:** les plates-formes PIX sont disponibles dans de nombreux formats afin de s'adapter parfaitement aux divers contextes possibles, de la PME ou succursales au siège social. Toutes les plates-formes PIX sont équipées du même logiciel et utilisent les mêmes solutions de gestion, disposant ainsi d'une évolutivité et d'une intégration optimales.
- ✓ **Installation et maintenance simplifiées:** Cisco a créé PIX Device Manager, un utilitaire web intégré et sécurisé pour configurer simplement et graphiquement le firewall.

- ✓ **VPN conforme aux normes:** la fonctionnalité VPN selon les normes IPsec compte parmi les fonctions de sécurité du PIX Firewall. Outre ses performances hors du commun, le PIX est doté des fonctions VPN site-à-site et à accès distant.

III.3. Le firewall ASA

III.3.1.Présentation

L'idée de la conception de l'Adaptative Security Appliance (ASA) est apparue lors de la mise en place, par Cisco, de la solution Self-Defending Network (le réseau qui se défend tout seul). En effet, en associant un firewall très puissant à un système qui offre les services VPN, l'ASA est la solution idéale pour garantir un réseau accessible de l'extérieur et sécurisé. Il met en place une défense face aux menaces et bloque les attaques avant qu'elles ne se propagent dans le reste du réseau. Grâce à une interface graphique (ASDM) et une utilisation simplifiée des fonctionnalités, l'ASA offre aux entreprises qui souhaitent sécuriser leur réseau un outil complet et raisonnablement facile à utiliser.

Figure 3.2: Le firewall ASA.

III.3.2. Les principaux avantages et fonctionnalités de l'ASA

L'ASA offre de nombreuses fonctionnalités de sécurité :

- ✓ **NAT (Network Address Translation):** comme l'ASA est en partie un routeur, il offre du NAT, ce qui permet d'avoir un accès à des réseaux externes comme internet.
- ✓ **QoS (Quality of Service) :** c'est un gestionnaire de trafic qui permet d'allouer les ressources réseau aux applications selon leur poids et leur priorité. En effet, dans le cas d'une vidéoconférence, il doit faire de telle sorte à fournir un débit suffisamment important pour obtenir une image et une voix acceptable. Pour implémenter la QoS, il faut spécifier des classes de trafic et associer des actions à chaque classe afin de former une politique QoS.
- ✓ **Security Context :** l'ASA peut être partitionné en de multiples périphériques virtuels, appelés « Security Context ». Chaque contexte est un périphérique indépendant, ayant ses propres règles de sécurité, interfaces, et administrateurs. Il contient donc plusieurs appareils

indépendants. Plusieurs fonctionnalités peuvent y être utilisées, comme les tables de routage, les fonctionnalités de firewall, l'IPS et l'administration.

- ✓ **ACL (Access Control List):** à chaque interface connectée à l'ASA, un numéro de sécurité (entre 0 et 100) est attribué. Le réseau intérieur se voit attribué par défaut le numéro 100 et le réseau extérieur le numéro 0. Sans aucune spécification de la part de l'utilisateur, l'ASA interdit le trafic d'une interface vers une autre interface dont le numéro de sécurité est supérieur. Il autorise d'un autre coté le trafic vers un niveau de sécurité inférieur. Les ACL ont été mises en place pour pouvoir interdire ou autoriser certains trafics d'une interface vers une autre. Elles sont composées d'ACE (Access Control Entries). Chaque ACE autorise ou refuse un trafic, en spécifiant l'adresse source et destination ainsi que le protocole.
- ✓ **IPS (Intrusion Prevention Services)** : l'ASA peut utiliser l'AIP SSM, un module de prévention d'intrusion qui surveille et effectue des analyses en temps réel du trafic sur le réseau. Il cherche les anomalies et les mauvais usages basés sur une bibliothèque de signatures étendue. Ainsi lorsque le système repère une activité non-autorisée, il peut mettre fin à la connexion en cours, bloquer l'hôte attaquant, enregistrer l'incident, et envoyer une alerte au gérant du réseau. Les autres connexions légitimes continuent à fonctionner indépendamment, sans interruption.
  - ☑ **AIP SSM :** il utilise un logiciel d'IPS (Intrusion Prevention Services) avancé qui fournit un service de protection pour stopper le trafic malicieux, notamment les vers et les virus réseau, avant qu'ils n'affectent le reste du réseau.
  - ☑ **CSC SSM :** il fournit une protection contre les virus, les spywares (logiciels espions), les spams et tout autre trafic non-désiré en scannant les paquets FTP, HTTP, POP3, et SMTP que l'utilisateur lui demande de scanner.
- ✓ **La détection de menace :** l'ASA fournit une fonctionnalité très importante sous deux formes, la détection basique de menaces, celle qui est installée par défaut sur l'ASA. Et la détection de menaces celle à configurer par l'utilisateur. La détection basique de menaces détecte les activités qui pourraient être liées à une attaque, comme une attaque DoS. Elle surveille le taux de paquets abandonnés et les évènements liés à la sécurité. Lorsque l'ASA détecte une menace, il envoie un log au système. La détection basique de menaces n'a un impact, sur les performances de l'ASA, que lorsqu'il y a des abandons de paquets ou qu'une menace est détectée. Mais même dans ce cas, l'impact est quasi-insignifiant.
- ✓ **Protection contre l'IP Spoofing :** afin de se protéger contre cette menace, l'ASA inclut l'Unicast Reverse Path Forwarding (Unicast RPF), que l'on peut activer sur une interface.

L'Unicast RPF donne l'instruction à l'ASA de regarder également l'adresse source (et non pas uniquement l'adresse de destination). En effet, pour chaque trafic que l'on autorise l'ASA à laisser passer, il crée une table de routage qui contient également la route vers l'adresse source. Il lui suffit donc d'observer l'adresse source et la table de routage afin de détecter les menaces.

- ✓ **Normalisation TCP :** la normalisation TCP est une fonctionnalité qui permet à l'administrateur réseau de rajouter des critères à la liste de ceux existants pour le scan d'un paquet TCP. En effet, cela offre la possibilité par exemple d'autoriser les paquets dont la taille des données dépasse la limite des paquets TCP ou abandonner les paquets SYN contenant des données.
- ✓ **AAA (Authentication, Authorization, Accounting):** AAA permet à l'ASA de savoir qui est l'utilisateur (authentification), ce qu'il est autorisé à faire (autorisations), ainsi que ce qu'il fait. Il offre ainsi une sécurité supplémentaire. En effet, supposons que l'ACL autorise le trafic Telnet du réseau interne vers un réseau externe. N'ayant pas accès aux adresses IP des quelques utilisateurs étant autorisés à se connecter par Telnet, AAA permet l'authentification au moment de la connexion.
  - ☑ **Authentification:** elle vérifie le nom d'utilisateur et le mot de passe. On peut configurer l'ASA à mettre en place par exemple l'authentification des connexions administratives tel que SSH, Telnet, Console série, ASDM (avec https), gestion du VPN, la commande enable, l'accès au réseau et/ou au VPN.
  - ☑ **Autorisation :** elle vérifie les autorisations pour chaque utilisateur après authentification pour les sessions, les commandes de management et l'accès au réseau et/ou au VPN.
  - ☑ **Surveillance :** elle permet de garder des traces du trafic qui passe à travers l'ASA. En activant l'authentification, l'ASA peut surveiller le trafic d'un ou plusieurs utilisateurs spécifiques.
- ✓ **Les filtres HTTP, HTTPS, FTP :** étant donnée la grande taille et la nature dynamique du net, l'utilisation des ACL n'est pas suffisante pour filtrer les sites web ou les serveurs ftp. Il est donc conseiller d'utiliser l'ASA en parallèle avec un serveur utilisant un produit de filtrage internet. Ainsi les performances du réseau peuvent être réduites considérablement par le serveur externe. Plus il est éloigné du réseau, plus son impact est important.

- ✓ **Limites de connexions :** l'ASA offre la possibilité de limiter le nombre de connexions TCP et UDP, le nombre de connexions à l'état embryonnaire, le nombre de connexions par utilisateur, ainsi que détecter les connexions mortes.

III.3.3.Le système d'exploitation Cisco IOS

Cisco IOS (Inter-network Operating System) fournit des fonctionnalités qui permettent à un périphérique Cisco d'envoyer et de recevoir du trafic réseau à l'aide d'un réseau filaire ou sans fil. Il est proposé sous la forme de modules appelés images. Ces images prennent en charge diverses fonctionnalités pour des organisations de toutes tailles. L'image IOS de base est appelée l'image de base IP. Cette dernière prend en charge le routage entre différents réseaux en ajoutant des services. Par exemple, l'image Advanced Security offre des fonctionnalités de sécurité avancée, telles que la création de réseaux privés et les firewalls. Un grand nombre de types et de versions d'images Cisco IOS sont disponibles. Ces images sont conçues pour fonctionner sur des modèles spécifiques de routeurs et de commutateurs. Il est important de savoir quelle image et quelle version sont chargées sur un périphérique avant de commencer le processus de configuration. [21]

III.4.Le firewall TMG

III.4.1.Présentation de firewall TMG

Le firewall Forefront TMG (Threat Management Gateway) est une passerelle Web qui permet aux entreprises d'utiliser Internet de façon sécurisée et efficace, sans crainte des logiciels malveillants ou autres menaces. Pour mieux bloquer les menaces récentes en provenance du Web, ce produit multiplie les couches de protection (filtrage d'URL, recherche de logiciels malveillants et prévention des intrusions) et les met à jour en permanence. Il protège les utilisateurs contre les menaces du Web en intégrant plusieurs couches de sécurité dans une solution simple à administrer. Placé comme passerelle dans le réseau de l'entreprise, il inspecte le trafic Web aux niveaux réseau, application et contenu pour assurer une sécurité Web cohérente. De plus, il améliore les performances du firewall en répartissant la charge de certaines fonctions sur plusieurs processeurs, comme l'inspection des logiciels malveillants. [24][25]

III.4.2.Les composants du firewall TMG

Le firewall TMG se compose de quatre composants :

- ✓ **Le serveur Forefront TMG** : il fournit plusieurs technologies d'inspection, des firewalls applicatifs et réseau, une prévention d'intrusion et un filtrage de logiciels malveillants. Il se connecte à Forefront TMG Web Protection Service pour le filtrage des URL et les mises à jour des signatures des logiciels malveillants.

- ✓ **Forefront TMG Web Protection Service :** il assure les mises à jour des signatures et le filtrage des URL Internet en temps réel, il peut aussi servir à surveiller ou à bloquer l'usage fait par les employés du Web.
- ✓ **La console d'administration :** il permet une gestion locale et à distance des serveurs.
- ✓ **Un serveur d'administration :** inclus dans Forefront TMG Enterprise Edition, il permet la création de stratégies à l'échelle de toute l'entreprise et les applique à des ensembles des serveurs TMG.

III.4.3.Les principaux avantages et fonctionnalités de la TMG

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

a. Protection complète

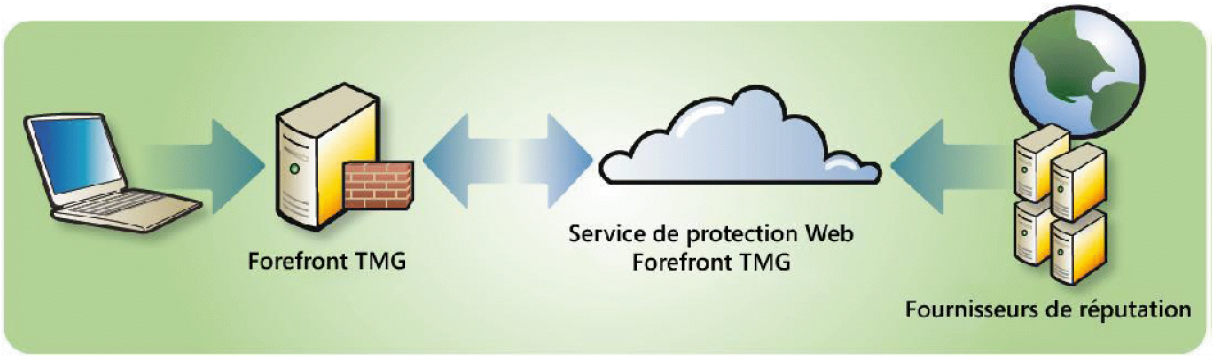

Figure 3.3 : Le filtrage des URL dans TMG Web Protection Service consolide les données en provenance de plusieurs fournisseurs.

- ✓ **TMG bloque efficacement l'accès aux sites malveillants :** il utilise des données en provenance de différents fournisseurs de filtres d'URL, et des technologies contre les logiciels malveillants et l'usurpation d'identité qui équipent déjà Internet Explorer 8. Le filtrage des sites Web permet aussi de bloquer l'accès aux sites inappropriés selon les choix d'entreprise.
- ✓ **Empêche l'exploitation de vulnérabilités :** il empêche les intrusions qui exploiteraient des vulnérabilités du navigateur ou de ses modules additionnels.
- ✓ **Détecte les logiciels malveillants du Web :** il assure une détection précise grâce à un moteur d'analyse qui combine des signatures génériques pour anticiper la diffusion de nouvelles variantes n'ayant pas de signatures spécifiques.

b. Interface de sécurité Web unifiée

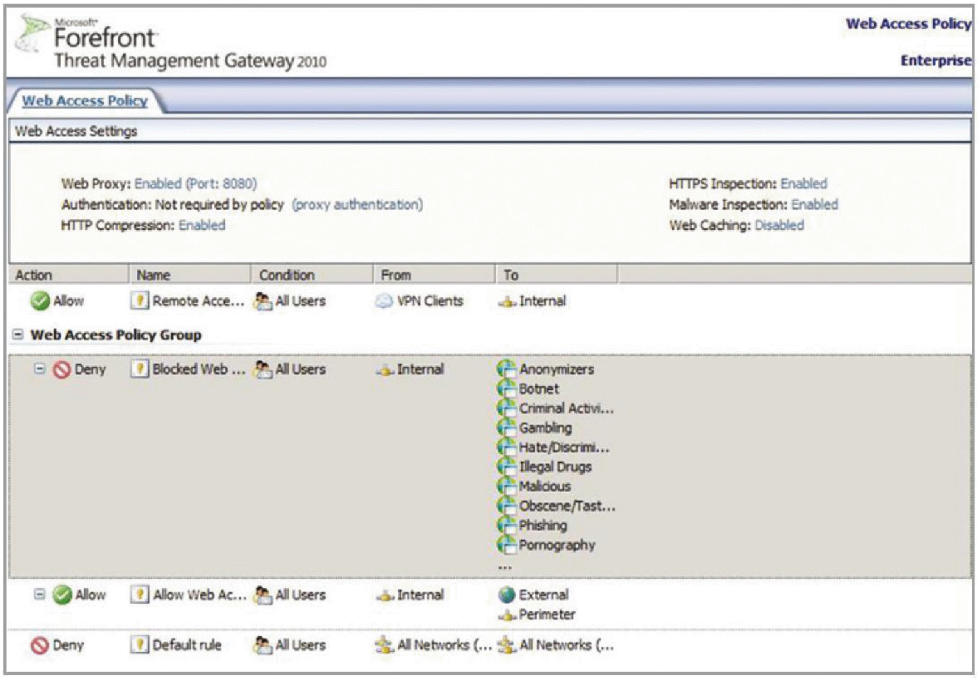

Figure 3.4: La console d'administration Forefront TMG simplifie la création de stratégies.

- ✓ **Assure les principales fonctions de protection du réseau :** il reprend les technologies de protection du réseau de Microsoft ISA Server 2006, la version précédente de Forefront TMG. Cela permet de déployer un firewall de périmètre et une passerelle sécurisée pour des applications comme Microsoft Exchange Server.
- ✓ **Inspecte le trafic Web chiffré :** il examine le trafic Web chiffré SSL, ce que ne fait pas un firewall. Dans ces sessions chiffrées, Forefront TMG peut détecter un logiciel malveillant et contrôler l'accès à des sites interdits par l'entreprise.

c. Sécurité intégrée

- ✓ **Une source unique pour la sécurité Web :** il combine sur un seul serveur le filtrage des URL, des services de réputation, le blocage des intrusions, le proxy Web, des firewalls applicatifs et réseau, la détection de logiciels malveillants et l'inspection HTTP/HTTPS.
- ✓ **Réduit les coûts :** il assure un rôle de cache pour améliorer la rapidité de navigation et réduire les coûts en bande passante. La possibilité de déployer Forefront TMG comme une appliance virtuelle permet d'économiser sur le matériel.
- ✓ **Exploite les investissements d'infrastructure existants :** il simplifie l'authentification et l'application des stratégies en s'intégrant dans Active Directory. Par exemple, Forefront TMG simplifie l'inspection HTTPS en distribuant son certificat via Active Directory. Il

utilise aussi l'infrastructure Windows Update pour diffuser rapidement de nouvelles protections à tous les serveurs Forefront TMG.

d. Administration simplifiée

- ✓ **Centralise la gestion sur une seule console simple d'emploi :** il permet aux administrateurs de créer et de gérer toutes les fonctions de sécurité Web à partir d'une seule console dans des environnements distribués.
- ✓ **Fournit des rapports complets** : il génère rapidement des rapports de sécurité qui peuvent être adaptés pour répondre à des besoins spécifiques de l'entreprise.

III.5. Le firewall FortiGate de Fortinet

III.5.1. Présentation

La gamme FortiGate déploie une protection économique et exhaustive contre les menaces qui pèsent sur le réseau, les applications et les contenus. Elle a été conçue pour gérer le réseau de façon à optimisé l'ensemble des fonctions de sécurité, des couches réseaux aux couches applicatives.

L'appliance FortiGate est un boîtier entièrement dédié à la sécurité. Il est convivial et fournit une gamme complète de services, que ce soit:

- ✓ Au niveau des applications (comme le filtrage antivirus, la protection contre les intrusions, les filtrages anti-spam, contenu web …).
- ✓ Au niveau du réseau (comme le firewall, la détection et prévention d'intrusion, les VPN IPSec et VPN SSL et la qualité de service).
- ✓ Au niveau de l'administration (comme l'authentification d'un utilisateur, la journalisation, les profils d'administration, l'accès sécurisé au web et SNMP).

Les composants premiers de FortiGate sont la puce FortiAsic et le système d'exploitation FortiOS. [26]

Figure 3.5 : Le firewall FortiGate.

III.5.2.FortiAsic

Le FortiAsic est un asic spécialisé dans le traitement des contenus applicatifs et la comparaison par rapport à des bases de données. La puce FortiAsic dispose de quatre moteurs d'analyse de contenu qui accélèrent les traitements antivirus, VPN, pare-feu, IPS et filtrage Web et anti-spam.

- ✓ Le moteur de recherche est capable d'identifier des données de différents types parmi des milliers de signatures de virus, d'attaques, de mots clés, d'URL, d'adresse emails et d'adresses de serveurs SMTP.
- ✓ Le moteur de chiffrement supporte entre autre les algorithmes de chiffrements. Un FortiGate peut délivrer un très haut débit VPN, tout en analysant les flux déchiffrés au niveau antivirus.
- ✓ Le moteur firewall accélère l'analyse des en-têtes réseau, et le moteur de gestion de flux exécute les opérations de trafic.

III.5.3. Le système FortiOS

Le système d'exploitation FortiOS est un système propriétaire mis au point par Fortinet. Il a été développé autour des critères:

- ✓ de sécurité,
- ✓ de performance nécessaire à l'analyse temps réel des applications,
- ✓ de portabilité sur différents type de matériel. Il peut être exécuté sur des déférents types de processeurs, dent le processeur Intel.

Le cœur de ce système d'exploitation est un noyau sécurisé, temps réel et optimisé au traitement des paquets. Il supporte des APIs permettant l'intégration aisée d'applications qui tournent sur des systèmes d'exploitation standards comme Linux tels Secure Shell, ou serveur Web.

III.6.Le firewall SideWinder

III.6.1.Présentation

Le firewall d'entreprise Sidewinder G2 assure la protection de haut niveau des réseaux, en fournissant une solution de sécurité prête à l'emploi qui s'intègre de manière transparente à n'importe quel réseau IP. Il représente la passerelle VPN et firewall, il permet de constituer un bouclier multicouche impénétrable grâce au système d'exploitation SecureOS supprimant ainsi tout patch de sécurité.

L'architecture hybride de Sidewinder G2 regroupe en une solution unique et économique, tous les mécanismes de sécurité des firewalls, dont le filtrage dynamique, les proxies au niveau circuit, les proxies d'application, les serveurs sécurisés et les alertes en temps réel.

Avec ses fonctionnalités de déploiement facile, ses capacités de sauvegarde et restauration à distance, sa journalisation centralisée, sa surveillance exhaustive d'état/analyse et sa fonctionnalité précurseur de détection d'intrusion et de réponse automatisée, il se positionne parmi les meilleures solutions Firewall de niveau 7.

Figure 3.6 : Le firewall SideWinder.

III.6.2.Les principaux avantages et fonctionnalités

- ✓ **Antivirus et anti-spyware :** protection contre les logiciels espions, les chevaux de Troie et les vers, analyse heuristique, mise à jour automatiques des signatures.
- ✓ **Visibilité et contrôle sur les applications :** grace à son moteur combinant hautes performances et proxies applicatifs transparents, McAfee Firewall Enterprise permet de bénéficier du plus haut niveau de sécurité en analysant le contenu des applications critiques plus finement que les firewalls traditionnels. Capable de reconstituer les communications et d'y appliquer des traitements intelligents (filtrage antivirus, cryptage, IPS/IDS,..), McAfee Firewall Enterprise, il garantit le fonctionnement sécurisé des applications particulièrement vulnérables aux attaques Internet les plus récentes.
- ✓ **Système d'exploitation McAfee SecureOS :** en son cœur, McAfee Firewall Enterprise bénéficie du système d'exploitation rapide et sécurise McAfee SecureOS, équipé de la technologie brevetée McAfee Type Enforcement qui offre un haut niveau de sécurité de plate-forme.
- ✓ **Géolocalisation:** la fonctionnalité de géolocalisation de Firewall Enterprise limite encore plus les menaces en permettant un filtrage du trafic basé sur le code du pays. De nombreuses entreprises gaspillent de la bande passante et des ressources système en traitant le trafic provenant de pays et de continents entiers avec lesquels ils n'ont aucune relation commerciale, s'exposant par la même à des risques de sécurité inutiles. La géolocalisation permet d'accepter uniquement la connexion au trafic mondial directement lie à entreprise.
- ✓ **McAfee Firewall Profiler :** appliance distincte de la gamme Firewall Enterprise, Firewall Profiler identifie en temps réel comment les règles du firewall sont liées aux utilisateurs et

aux applications. Il permet aux administrateurs de constater l'impact de la création ou modification des règles du firewall, tout en diminuant les coûts d'exploitation.

- ✓ **McAfee Firewall Enterprise Control Center:** vendu séparément, il offre une gestion centralisée des stratégies de firewalls Enterprise.

III.7. Les critères de choix d'un firewall

Il n'existe pas de bon produit en soi. Il existe des produits qui ont un bon rapport qualité/prix, des produits qui répondent plus ou moins bien aux besoins spécifiques d'une entreprise et des produits qui s'intègrent plus ou moins bien dans l'existant. Avant de faire un choix de produit, il est nécessaire d'avoir connaissance des critères suivant pour effectuer le choix d'un firewall.

- ✓ La nature, le nombre des applications appréhendées (FTP, messagerie, HTTP, SNMP, Real Audio, vidéoconférence…).
- ✓ Le type de filtres, le niveau de filtrage (niveau applicatif, niveau TCP, niveau IP, possibilité de combiner ces niveaux).
- ✓ Les facilités d'enregistrement des actions à des fins d'audit, login, complet des paramètres de connexion, l'existence d'outils d'analyse, d'audit actif et détection d'activités suspectes.
- ✓ Les outils et facilités d'administration (interface graphique ou lignes de commandes, administration distante après authentification du gestionnaire…).
- ✓ La simplicité de système, proxy facile à comprendre et à vérifier (facilité de configuration).
- ✓ La capacité à supporter un tunnel chiffré permettant de réaliser, si nécessaire, un réseau privé virtuel (VPN).
- ✓ La disponibilité d'outils de surveillance, d'alarmes, d'audit actif.
- ✓ La possibilité d'effectuer de l'équilibrage de charge.
- ✓ L'existence dans l'organisation de compétences en matière d'administration du système d'exploitation du firewall.

III.8. Conclusion

Le firewall constitue un des outils de la réalisation de la politique de sécurité et n'est qu'un des composants de sa mise en œuvre. En effet le firewall ne suffit pas à bien protéger le réseau et le système d'une organisation. Il doit être également accompagné d'outils de mesure et de procédure répondant à des objectifs de sécurité préalablement déterminés par la politique de sécurité.

L'efficacité d'un firewall dépend aussi du choix du type des firewalls à utiliser. Avec toutes les différentes gammes qu'il y a sur le marché avant de prendre une décision, il faut avoir connaissance des critères de choix d'un firewall. Etant choisi, son positionnement par rapport aux systèmes qu'il doit protéger, sa configuration et sa gestion déterminent son efficience.

Chapitre IV : Etude de l’existant

IV.1. Introduction

Les attaques informatiques constituent aujourd'hui l'un des fléaux de notre civilisation moderne. Il ne se passe plus 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 d'une banque. Nous allons, pour lever toute ambiguïté, découvrir son architecture réseau et ses différents sites.

Tout au long de ce chapitre, nous présenterons et étudierons les principaux points critiques qui dévoilent les risques potentiels encourus en décrivant les causes qui les engendrent. Puis nous proposerons une nouvelle structure de l'architecture réseaux de la banque avec les solutions à mettre en place pour avoir une meilleure sécurité.

IV.2. Présentation de l'architecture existante

Notre infrastructure existante est constituée de deux sites:

Le **site 1** est constitué de :

- ✓ 19 Serveurs dont 12 protégés par les IPS.
- ✓ 1 base de données.
- ✓ 11 zones
- ✓ 5 types de VLAN
- ✓ 6 Firewalls :
  - 2 SideWinder.
  - 3 Fortigate.
  - 1 PIX.
- ✓ 2 Routeurs
- ✓ 8 Commutateurs dont l'un est un commutateur VPN.
- ✓ 5 postes :
  - 2 postes de stations d'administration.
  - 1 poste pour le superviseur réseau.
  - 2 postes pour le service réseau.

Le **site 2** est constitué de :

- ✓ 8 Serveurs dont 6 sont protégés par des IPS.
- ✓ 1 base de données.
- ✓ 10 zones.
- ✓ 5 types de VLAN.
- ✓ 6 Firewalls :
  - 2 SideWinder.
  - 1 PIX.
  - 3 Fortigate

    .
- ✓ 2 Routeurs.
- ✓ 8 Commutateurs dont l'un est un commutateur VPN.
- ✓ 4 postes :
  - 2 postes de stations d'administration.
  - 2 postes pour le service réseau.

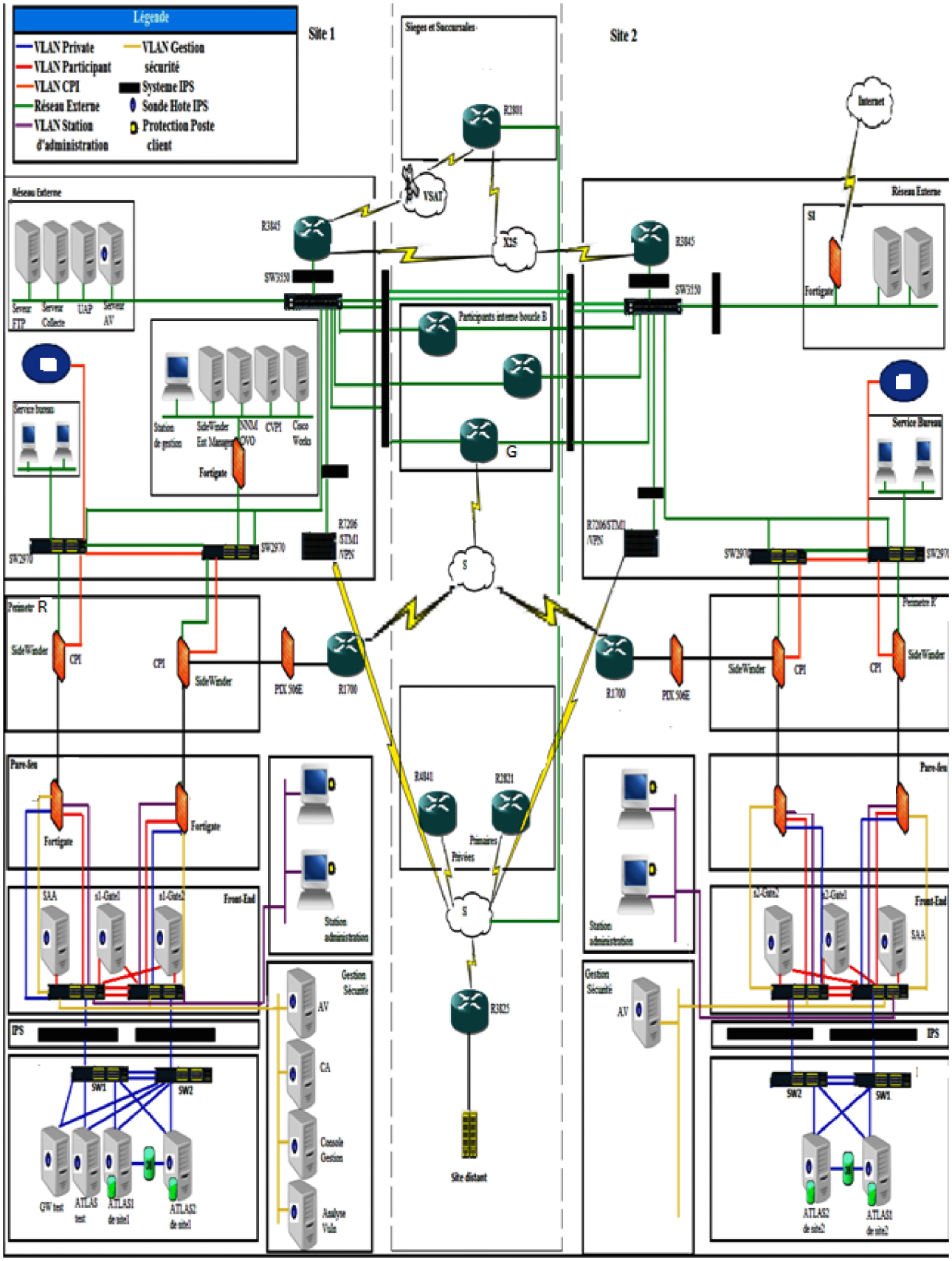

Figure IV.1: L'architecture existante.

Cette infrastructure est constituée de deux sites, qui contiennent comme nous pouvons le voir dans la figure ci-dessus une architecture identique (les seules différences résident dans le nombre de serveur et la connexion internet). Dans notre étude identifierons les différentes failles du site 1 et la faille qui réside dans la zone SI du réseau externe du site 2.

En ce qui concerne la dorsale qui sépare les deux sites, vu qu'elle est prise en charge par A Télécom, nous n'allons pas la prendre en considération dans cette étude.

IV.2.1. Les vulnérabilités de l'architecture réseau

1. Le firewall PIX506^{E}

A sa sortie le PIX, un des premiers sur le marché, était un excellent firewall mais le paysage depuis la sécurité à bien changé. Aujourd'hui, pour protéger un réseau un PIX n'est plus suffisant au vu du nombre de type d'attaques possibles comme les virus, les vers, ainsi que les applications non désirées (P2P, jeux, messageries instantanée), car il n'offre pas de protection multi-threat ni Anti X. C'est pour cela que la gamme PIX a été suspendue en juillet 2008.

Comme illustré dans la figure ci-dessous le firewall Cisco PIX 506^{E} qui lie le réseau S et le périmètre R même si cette liaison est secondaire, (la liaison primaire est effectuée à travers une ligne spécialisée au niveau du site de G), PIX constitue un point critique qui ne peut être négligé.

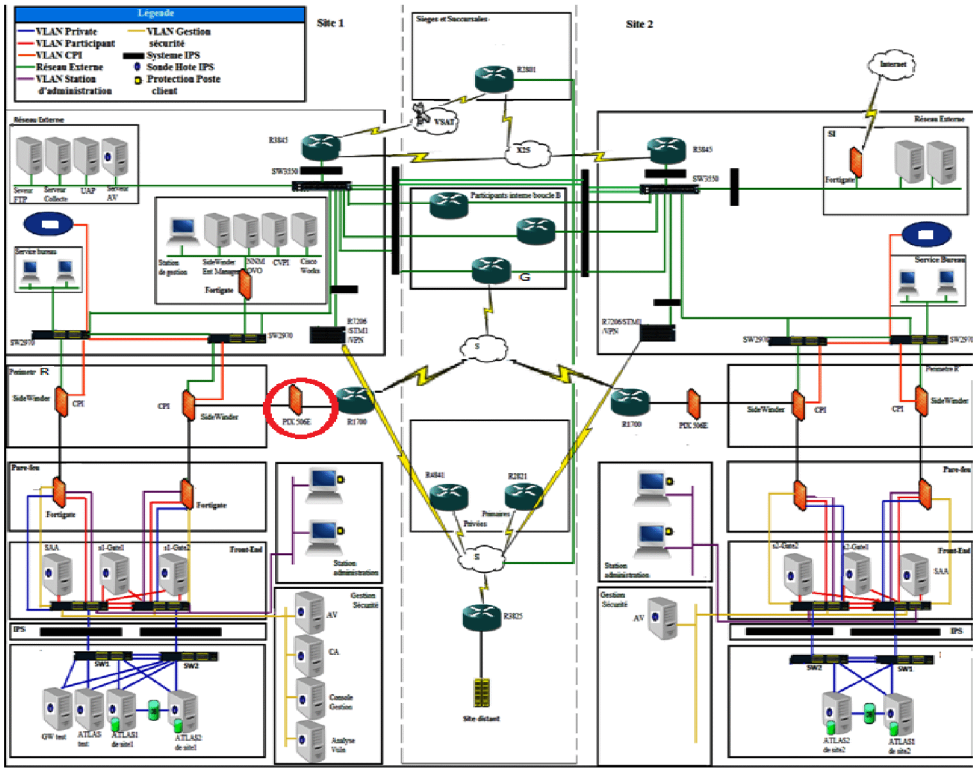

Figure IV.2 :La vulnérabilité de PIX506E.

2. L'utilisation de type identique de firewalls

La vulnérabilité de l'utilisation de deux firewalls identiques au même niveau, dans notre cas, deux SideWinder dans la zone R et deux Fortigate dans la zone pare-feu, est due à la non optimisation de la sécurité. Même si ces firewalls sont performants, il n'en reste qu'ils ne sont pas infaillibles car chaque type de firewall travaille sur des couches précises qui ne sont pas forcement les même.

Mettre deux firewalls Sidewinder dans la même zone constitue un risque car ces deux firewalls fonctionnent au niveau de la même couche qui est la couche application. Si le premier firewall ne détecte pas la présence d'un virus le deuxième ayant les mêmes caractéristiques ne pourra pas non plus le détecter.

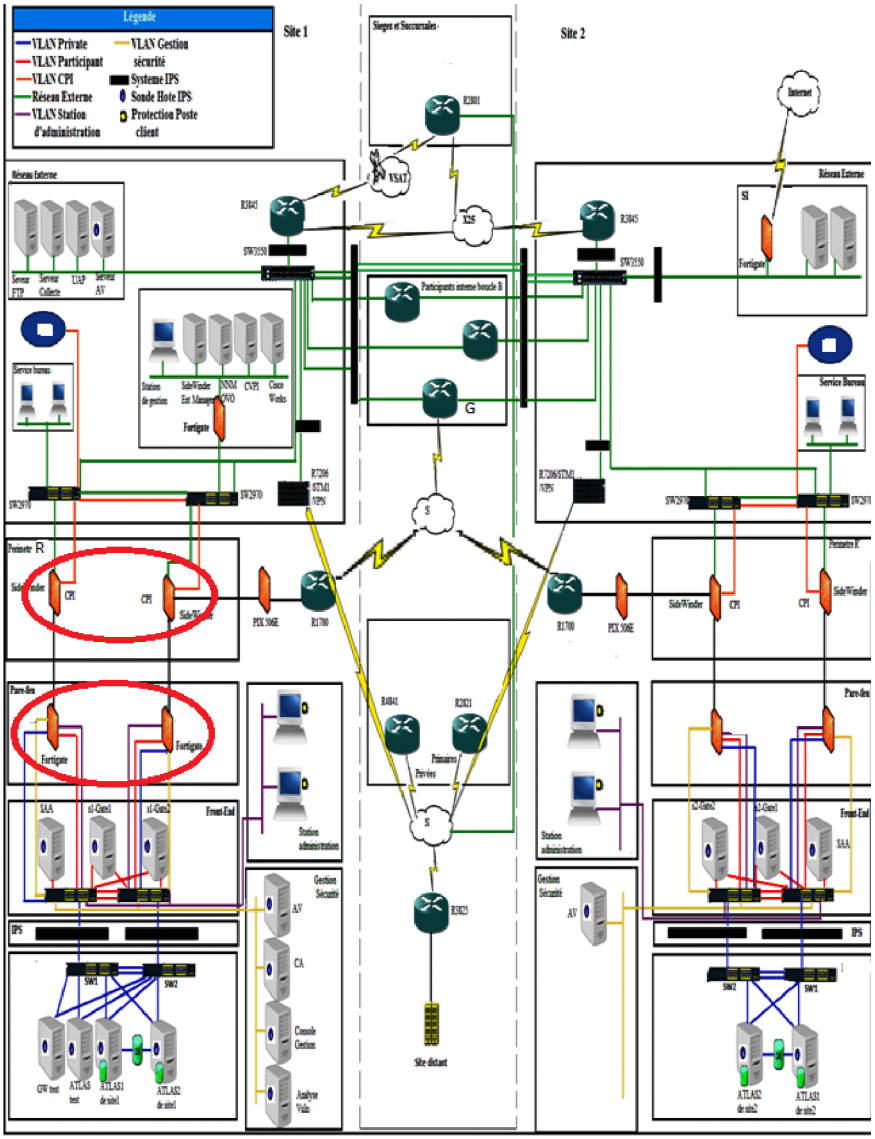

Figure IV.3: La vulnérabilité de type identique de firewalls.

3. Le system de prévention d'intrusion IPS

Les IPS possèdent de nombreux inconvénients qui sont énumérés comme suit :

✓ Un IPS bloque toute activité qui lui semble suspecte même si elle ne constitue pas un danger. Comme exemple, un IPS peut détecter une tentative de déni de service alors qu'il s'agit simplement d'une période chargée en trafic. Les faux positifs sont donc très dangereux pour les IPS.

✓ Le deuxième inconvénient est qu'un pirate peut utiliser sa fonctionnalité de blocage pour mettre hors service un système. Prenons l'exemple d'un individu mal intentionné qui attaque un système protégé par un IPS, tout en spoofant son adresse IP, si l'adresse IP spoofée est celle d'un nœud important du réseau comme un routeur ou service Web, les conséquences seront catastrophiques.

✓ Le troisième inconvénient et non le moindre : un IPS est peu discret. En effet, à chaque blocage d'attaque, il montre sa présence. Cela peut paraître anodin, mais si un pirate remarque la présence d'un IPS, il tentera de trouver une faille dans celui-ci afin de réintégrer son attaque mais cette fois en passant inaperçu.

Donc son utilisation aux points sensibles de la banque peut engendrer des portes ouvertes aux malveillants que ce soit au niveau interne ou externe de la banque.

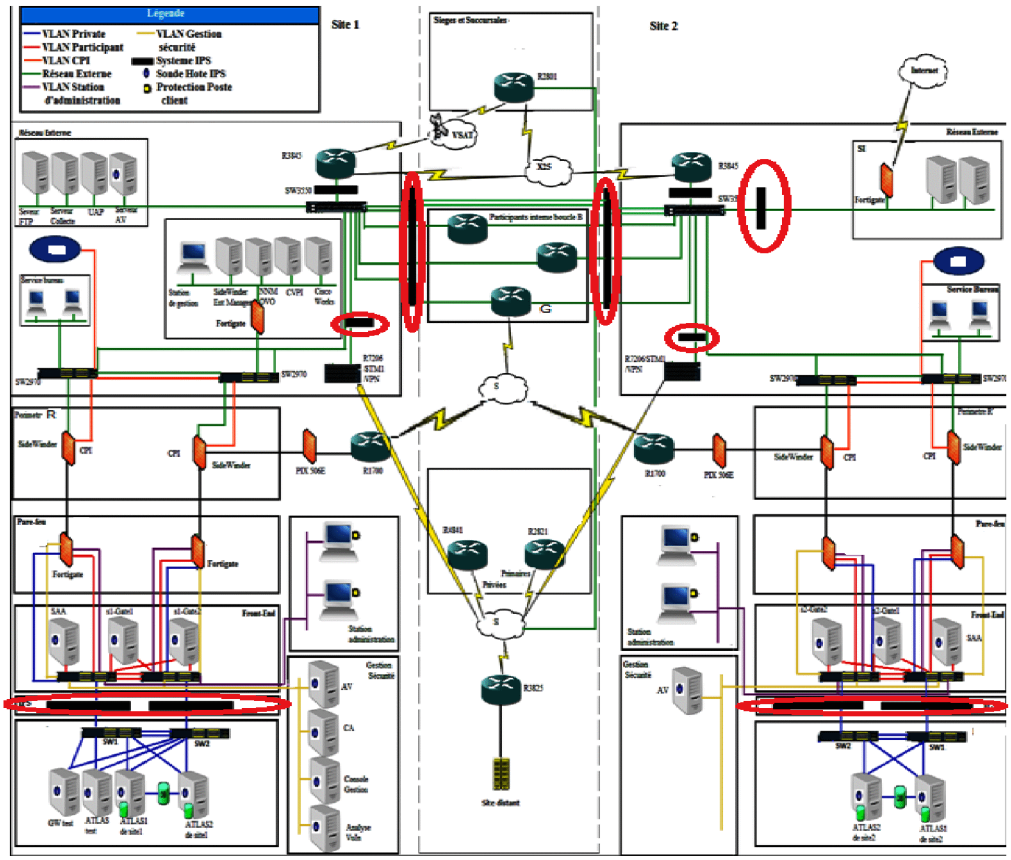

Figure IV.4 : La vulnérabilité IPS.

4. Le commutateur SW3550

Comme illustré dans le schéma ci-dessous le commutateur SW3550 représente un point de défaillance, vu que toute l'infrastructure R est connectée directement ou indirectement à ce seul commutateur. Donc la panne de ce commutateur causera la déconnexion de tous les utilisateurs sauf ceux connectés à travers le réseau S puisqu'il y a une liaison secondaire à travers le PIX 506^{E}. Sans oublier aussi que ce commutateur connecte le système R au réseau SI. En cas de faillite du commutateur, il n'y aura aucune connectivité avec le réseau SI.

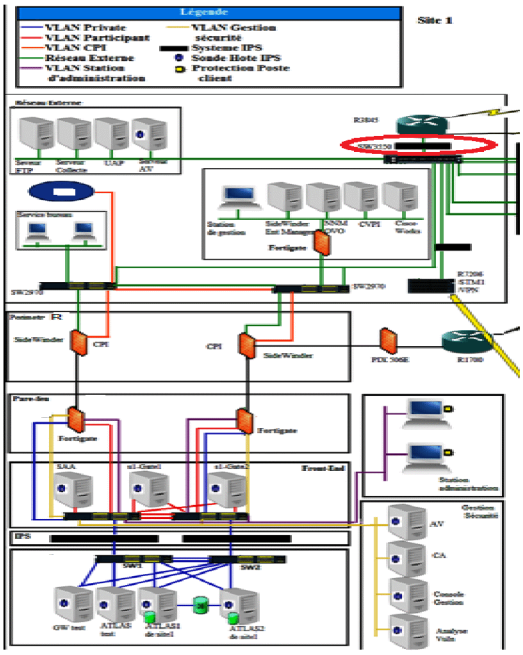

Figure IV.5 : La vulnérabilité du commutateur SW3550.

5. Plusieurs points d'entrée du réseau (Multiple Entry Points)

Dans le réseau de télécommunication de la banque, il existe plusieurs points d'entrée du réseau avec les entités externes, comme le montre la figure ci-dessous:

- ✓ Le pare-feu Cisco PIX 506^{E} qui connecte les participants externes directement à la zone Périmètre R du réseau interne.
- ✓ Le routeur Cisco 3845 qui fournit l'accès aux sièges et succursales, à travers le réseau X.25 et la connexion VSAT.
- ✓ Le routeur Catalyste 7206 qui fournit la connexion vers le site 2, aux participants internes à travers la boucle B, et aussi au réseau S puisque la connexion primaire du réseau S se trouve au niveau de G qui est accessible à travers la boucle B.
- ✓ La connexion internet, qui se trouve au niveau du réseau SI dans le site 2.

Le fait d'avoir plusieurs points d'entrée constitue une faille car il est difficile d'assurer une bonne politique de contrôle d'accès sur toutes les entités externes utilisant le réseau de la banque et les services fournis.

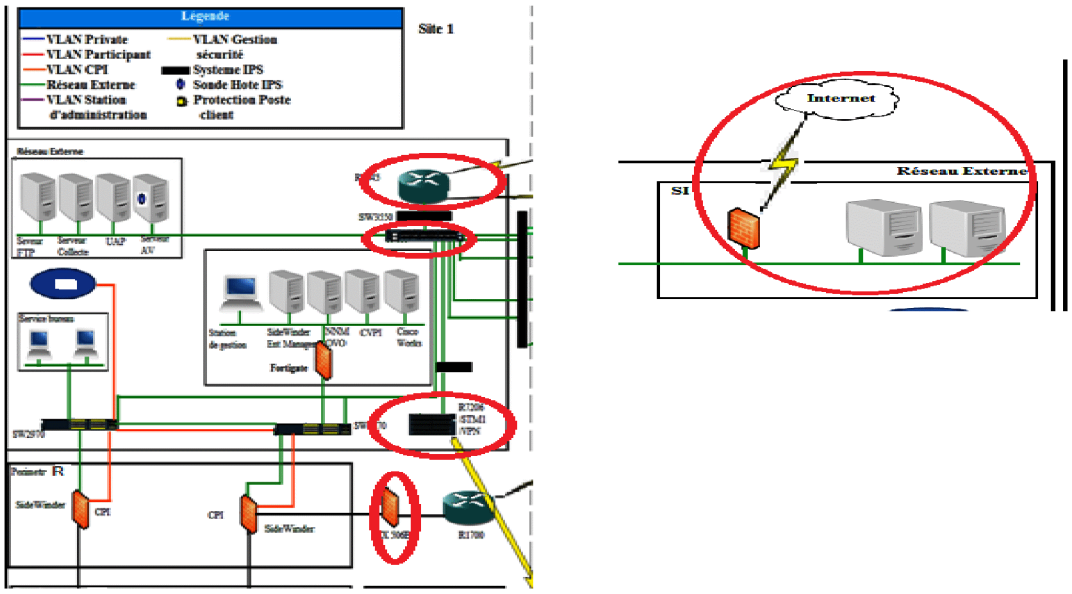

Figure IV.6: Les multiple points d'entrée du réseau.

IV.2.2. Vulnérabilités de configuration et de gestion du réseau

1. Utilisation de protocoles à texte clair (ClearText)

Des protocoles à texte clair sont utilisés pour gérer le réseau, comme Telnet et HTTP qui sont activés sur les routeurs. Cela signifie que les comptes utilisateur et les mots de passe, de même que les commandes de configuration sont transmis à travers le réseau en texte clair. Les protocoles SNMPv1 et SNMPv2 sont non sécurisés parce qu'ils permettent l'échange des informations critiques en texte clair pour gérer les éléments du réseau.

L'une des plus grandes faiblesses du protocole SNMPv1 est l'absence d'un mécanisme adéquat pour assurer la confidentialité et la sécurité des fonctions de gestion. Les faiblesses comprennent aussi l'authentification et le cryptage, en plus de l'absence d'un cadre administratif pour l'autorisation et le contrôle d'accès. En résumé le protocole SNMPV1 utilise SNMP pour l'acquisition des données de gestion, mais pour effectuer le contrôle on utilise le protocole Telnet.

La deuxième version SNMPV2 a introduit quelques nouveaux types, mais sa nouveauté majeure est l'opération GETBULK, qui permet à une plate forme de gestion de demander en bloc de plusieurs variables consécutives dans la MIB de l'agent. Généralement, on demande autant de variables que l'on peut mettre dans un paquet SNMP. Ceci règle un problème majeur de

performance dans SNMPv1. Il y a eu certes des changements avec cette nouvelle version mais pas dans le domaine de la sécurité, ce qui fait que l'utilisation de ces protocoles constitue une vulnérabilité.

2 .Mots de passe faibles

Les routeurs sont protégés par des mots de passe faibles comme « cisco » et « rtgs ». Les intrus auront ainsi des diverses options qui leur permettront de causer des dommages et d'interrompre les activités métier. Cette vulnérabilité existe à cause du manque de lignes directrices de sécurité de mot de passe, et la mauvaise appréciation des conséquences de l'utilisation de mots de passe faibles.

IV.2.3. Vulnérabilités de configuration et de gestion des firewalls

1. La dépendance de la gestion et la configuration des firewalls avec le fournisseur

Pour la gestion et la configuration des firewalls, la banque dépend toujours du fournisseur de celui-ci. En effet il y a un manque de compréhension vis-à-vis de la configuration du firewall et de ce qui est permis ou non. De même, la présence du fournisseur est toujours nécessaire pour répondre aux questions techniques. Ce qui peut causer un problème de configuration si le fournisseur n'est pas joignable.

2. Trafic sortant non restreint

Les règles du firewall n'interdisent pas aux IP internes, de se connecter au réseau externe. Ceci peut permettre à un intrus d'initier un « reverse tunnel » de l'intérieur de la banque vers sa machine, et ainsi lui permettre de dévier les règles « externes » du firewall.

3. Compte partagé pour la gestion du firewall

Les comptes d'administration des firewalls SideWinder sont partagés par au moins deux employés de la banque et le fournisseur. Ainsi, les responsabilités ne sont pas bien définies, il est impossible d'auditer les changements des configurations des firewalls. Et le manque de documentations des changements effectués, constitue une vulnérabilité sérieuse du mécanisme de défense de la banque. Comme exemple il se peut que des ports soient ouverts pour faire des testes et que les administrateurs oublient de les fermer et les biens protégés par le firewall seront exposés.

IV.2.4. Vulnérabilités de gestion et de configuration du système

1. Le manque d'une bonne politique de mot de passe

L'inexistence d'une bonne politique de mot de passe imposée au niveau du domaine est en soit une vulnérabilité car il n'y a aucune manière de garantir un niveau minimum de complexité de mot de passe.

2. Anti-virus McAfee n'est pas totalement configuré

Bien que la direction des systèmes de paiements ait apparemment fortement investi pour obtenir une solution d'Anti-virus de McAfee, l'efficacité cette solution est affaiblie par le fait qu'elle n'est pas totalement configurée ou qu'elle n'est pas étroitement surveillée. McAfee ePolicy Orchestrator n'est pas encore configuré pour informer les administrateurs en cas de production d'un incident relatif à un virus ou d'un problème relatif au logiciel comme l'échec de la mise à jour. Ainsi la console d'Anti-virus n'est pas étroitement surveillée à cause de sa présence dans la salle du serveur et de l'inexistence d'un responsable de sécurité chargé de la surveiller et de la mettre à jour régulièrement.

3. Ports ouverts et services démarrés

Beaucoup de ports ouverts sur les serveurs sont relatifs à des services inutiles. Ils constituent des risques de points d'entrée au réseau qui peuvent être utilisés par des intrus. Ceci rend la gestion de la sécurité de ces serveurs plus difficile puisque tous ces services doivent être régulièrement mis à jour et leur configuration doit être périodiquement revue.

4. Activités d'administrateurs non surveillées

Les administrateurs ont le privilège d'arrêter la journalisation, supprimer des événements du journal système ou même supprimer le journal. L'installation actuelle rend pratiquement impossible de détecter la falsification des journaux système ou toutes autres activités non autorisées d'administrateur.

5. Stations non verrouillées

Les postes de travail utilisés pour administrer les systèmes R et les postes de travail appartenant au service bureau ne sont pas verrouillés quand ils ne sont plus utilisés. Ceci peut permettre aux intrus d'avoir un accès non autorisé aux privilèges administratifs attribués à ces postes.

IV.3. Les solutions proposées

IV.3.1. L'architecture proposée

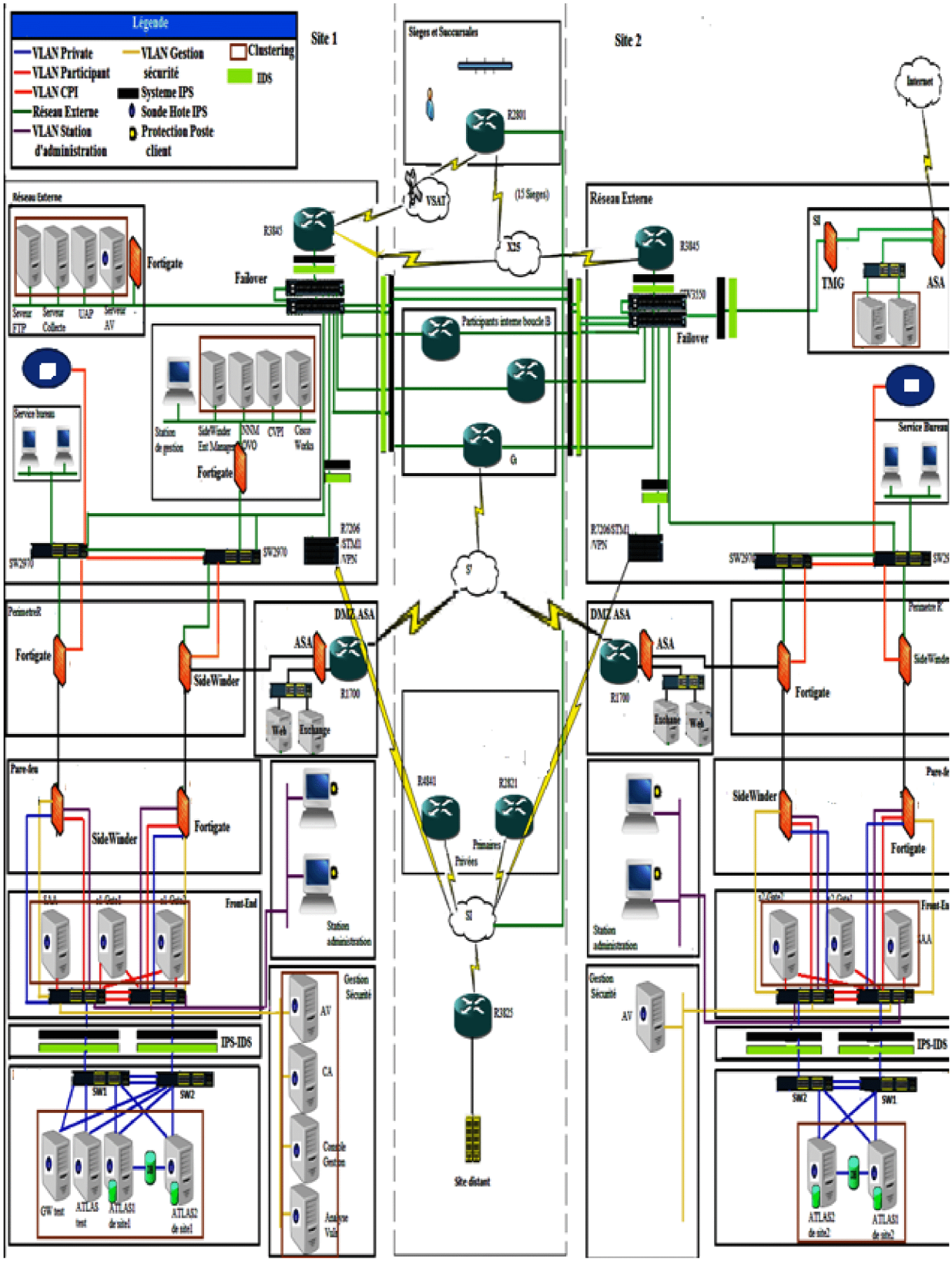

Figure IV.7 :L'architecture proposée.

IV.3.1.a. Les changements de l'architecture réseau

1. Remplacer le PIX par ASA

Après que le firewall PIX eut été suspendu, une autre gamme dite ASA a vu le jour. Dans l'impossibilité d'effectuer une mise à jour du firewall PIX qui n'existe plus, il doit être remplacé par un autre Firewall. Nous proposons le Firewall ASA.

Ce dernier regroupe trois éléments de la gamme Cisco en une seule plate-forme, le Cisco PIX firewall, le Cisco VPN 3000 Series Concentrator, le Cisco IPS 4000 Series Sensor et le module qui le différencie vraiment du PIX, le CSC SSM, Content Security and Control Security Service Module pour ajouter ces fonctions « Anti X » alors que le PIX n'était qu'un firewall avec quelques fonctions VPN et sonde IPS assez limitées.

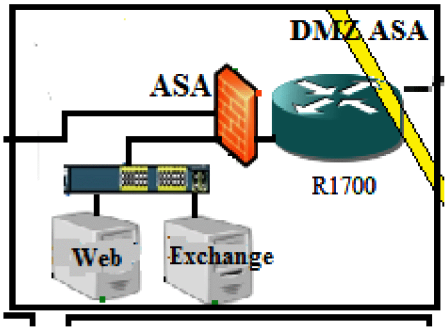

Figure IV.8 : Le remplacement de PIX par ASA.

2. Repositionnement des firewalls de type identique

Pour remédier aux vulnérabilités de l'utilisation de firewalls de type identique et mieux exploiter les fonctionnalités des firewalls disponibles, nous proposons de permuter les firewalls comme le montre la figure ci-dessous pour une meilleure sécurité.

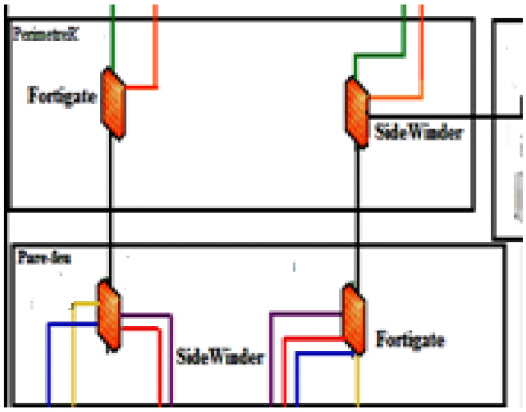

Figure IV.9 : La permutation des firewalls.

3. L'ajout des IDS

Malgré les inconvénients des IPS, on peut retenir que ces derniers sont actifs, pour cette raison nous proposons d'utiliser en plus des IPS existants des IDS qui permettront d'accentuer la sécurité des IPS à tous les niveaux, que ce soit système ou réseau. (l'emplacement des IPS et IDS est montré dans la figure ci-dessous).

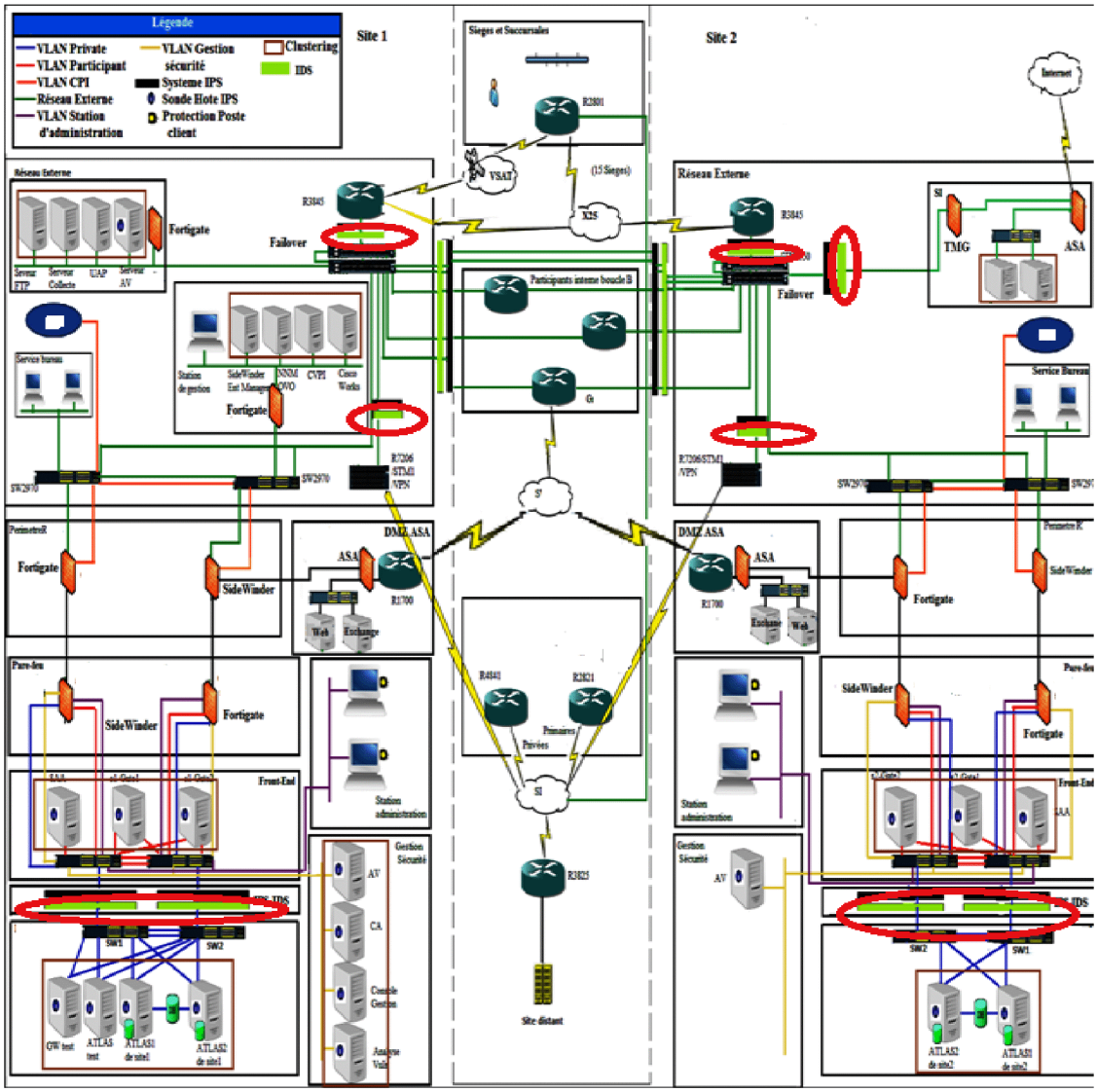

Figure IV.10:L'ajout des IDS.

4. L'implémentation du failover

Pour remédier au point de défaillance que constitue le commutateur dans l'architecture réseau, la solution que nous proposons est l'ajout d'un commutateur pour implémenter la technique de tolérance aux pannes (failover). Le failover consiste à mettre en marche un seul commutateur à la fois. Le déclenchement du deuxième commutateur ne s'effectuera qu'après la panne du premier.

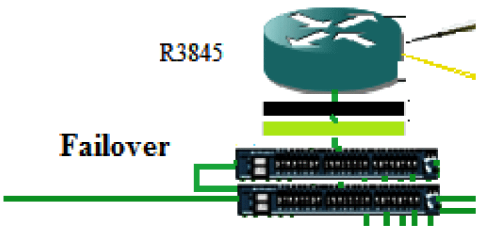

Figure IV.11 :L'implémentation de failover**.**

5. La sécurisation des points d'entrées réseau

Nous proposons des solutions pour sécuriser les points d'entrées selon la chronologie citée dans les vulnérabilités liées à ce titre.

- ✓ La solution à apporter pour sécuriser le premier point d'entrée que constitue PIX, remplacé par ASA, est la création d'une DMZ.

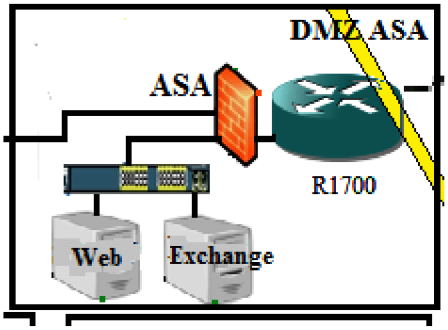

Figure IV .12 : La création de la DMZ ASA.

Cette DMZ englobera, un serveur Exchange et un serveur Web.

- ✓ Pour l'échange des mails aux niveaux interne et externe de la banque, nous utiliserons le serveur de messagerie Exchange 2010.
- ✓ Pour la publication web, nous ajouterons un serveur web, qui contiendra le site de la banque.

Comme ces deux serveurs sont connectés à l'aide d'un commutateur, la banque a la possibilité d'effectuer une extension si besoin.

- ✓ Pour le deuxième point d'entrée que constitue le routeur Cisco 3845, nous avons proposé l'ajout de l'IDS comme vu plus haut.
- ✓ Pour le troisième point d'entrée, le routeur Cisco Catalyst 7206, notre solution consistera à configurer une liaison VPN SSL site à site d'ASA.

- ✓ Pour le quatrième point d'entrée, la connexion internet qui se trouve au niveau du réseau SI dans le site 2.Nous proposons de créer une DMZ qui contiendra les serveurs existants dans SI raccordés par un commutateur à un firewall ASA et un firewall TMG. L'ASA gère le trafic entrant et sortant de la banque et la protège de l'extérieur. La TMG définit et contrôle tout le trafic interne. Ces derniers comme nous l'avions dit, offrent une meilleure protection pour l'internet. Quant au firewall Fortigate existant, nous proposons au lieu de le supprimer du réseau, de le placer au niveau du SI du site 1, afin protéger les serveurs de cette zone.

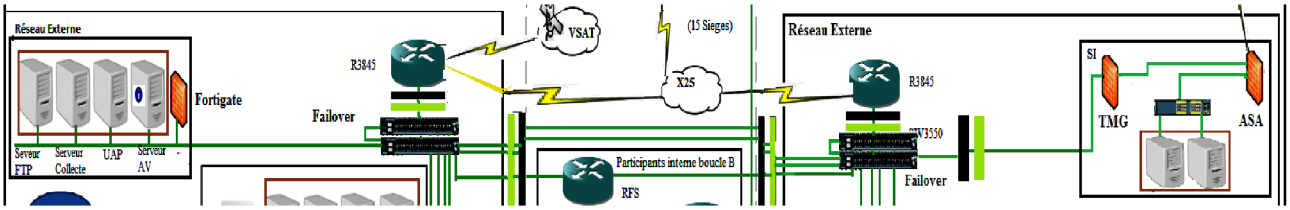

Figure IV.13 : La création de la DMZ SI.

IV.3.1.b. Les solutions de configuration et de gestion du réseau

1. Utilisation de protocoles sécurisés pour la gestion du réseau.

Comme on ne peut pas complètement empêcher quelqu'un d'intercepter les données qui transitent sur l'internet, le moyen trouvé pour sécuriser les transactions de la banque est le cryptage. Dans le cas où un pirate récupère le mot de passe crypté il ne peut rien faire avec. La solution consiste à utiliser pour gérer le réseau les protocoles chiffrés, HTTPS, SSL et IPSe.

- ✓ Utiliser le protocole HTTPs pour sécuriser des transactions HTTP adopté pour permettre une navigation sécurisée sur le web.
- ✓ Afin d'assurer la sécurité des échanges indépendamment du protocole applicatif utilisé. Nous proposons l'utilisation du protocole SSL pour chiffrer les communications entre les différents points entités à l'intérieur et l'extérieur de la banque et protéger les données.
- ✓ Pour vérifier l'intégrité des ordinateurs avant de leurs accorder un accès au réseau interne de la banque, nous proposons d'implémenter la protection d'accès réseau (Network Access Protection), cette dernière combinée avec le serveur DHCP (Dynamique Host Configuration Protocol) attribue dynamiquement les adresses IP aux clients internes conformes. Parmi les règles de conformité qui peuvent être spécifiées par l'utilisateur nous trouvons, l'activation du pare-feu, l'installation d'un anti-virus et les mises à jour. Si le client n'est pas conforme il ne se verra pas attribuer une adresse IP interne jusqu'à ce qu'il soit conforme. Et s'il contient

une adresse IP et qu'entre temps il n'est plus conforme il se verra retirer l'adresse IP interne au prochain bail. Donc pour des questions de sécurité le bail doit être au maximum valable 8 jours.

- ✓ Pour la gestion des équipements du réseau le protocole SNMP Version 3. La version SNMPV3 contrairement aux versions citées auparavant, inclue la sécurité des transactions. La sécurité comprend l'identification des parties qui communiquent et l'assurance que la conversation soit privée, même si elle passe par un réseau public. Cette sécurité est basée sur deux concepts :

a. USM (User-based Security Model)

Trois mécanismes sont utilisés. Chacun de ces mécanismes a pour but d'empêcher un type d'attaque.

- L'authentification : Empêche quelqu'un de changer le paquet SNMPv3 en cours de route et de valider le mot de passe de la personne qui transmet la requête.
- Le cryptage : Empêche quiconque de lire les informations de gestions contenues dans un paquet SNMPv3.
- L'estampillage du temps : Empêche la réutilisation d'un paquet SNMPv3 valide déjà transmis par quelqu'un.

b. VACM (View Access Control Model)

Permet le contrôle d'accès au MIB. Ainsi on a la possibilité de restreindre l'accès en lecture et/ou écriture pour un groupe ou pour un utilisateur.

Pour mettre en place un système de cryptographie capable d'implémenter l'ensemble des protocoles de sécurité HTTPS, SSL et assurer les fonctions de cryptage/décryptage en toute sécurité, nous installons des certificats PKI.

Pour confirmer l'identité et l'intégrité d'un serveur ou un utilisateur, nous proposons l'utilisation des certificats PKI. Pour utiliser un certificat nous pouvons soit l'acheter auprès d'une autorité de confiance ou de créer notre autorité de certificat. Ayant choisit de le créer, il nous faut mettre en œuvre des processus administratifs pour être certain de l'identité de chaque personne qui reçoit un certificat. Garantissant ainsi un monde de confiance dans un environnement incertain. Voulons certifier les accès web et messagerie de la banque, nous proposons d'installer la CA sur

Microsoft exchange 2010. Comme exchange est divisé en plusieurs rôles, Transport Hub, Accès aux clients et qu'il transporte des informations privées sur les connexions TCP/IP. Apres avoir générer un certificat crypté autant qu'administrateur de sécurité, nous pouvons le déployer sur l'ensemble des serveurs et utilisateurs authentifiés de la banque.

En suite, grâce à ces certificats, le courrier est acheminé sur des connexions sécurisées. Cette solution permet de sécuriser entièrement le transfert des informations et garantit que les données ne seraient en aucune manière compromises.

2 .Utilisation de mots de passe fort

Les solutions proposées pour une bonne politique de sécurité de mot passe est la suivante :

- ✓ Avant toute chose souligner l'importance de changer les mots de passe par défaut.
- ✓ Choisir un login qui soit différent de Admin, mieux vaut choisir un mot qui n'existe pas dans le dictionnaire, car la plus part des pirates utilise la méthode du dictionnaire.
- ✓ l'administrateur ne doit pas choisir un mot de passe qui fait référence à son nom, prénom, ou même ces deux combinés avec des caractères spéciaux.
- ✓ Le mot de passe doit être changé et renouveler au moins tous les 45 jours.
- ✓ Utiliser lors de la configuration un mot de passe crypté.
- ✓ Le mot de passe doit contenir au moins 7 caractères
- ✓ La complexité du mot de passe doit inclure trois des quartes catégories :
  - ➢ Lettres minuscules (a-z)
  - ➢ Lettres majuscules (A-Z)
  - ➢ Chiffres (0-9)
  - ➢ Caractères spéciaux ($,#, %..)

IV.3.1.c. Solutions de configuration et de gestion du firewall

1. La formation des équipes de travail

Afin de remédier au problème de la dépendance du fournisseur pour la configuration et la gestion des firewalls, nous suggérons d'organiser périodiquement des formations pour améliorer les compétences des équipes de travail et les connaissances sur les technologies actuellement utilisées au niveau de l'infrastructure de la banque.

2. La restriction du trafic sortant

Les règles du firewall doivent être bien réfléchies pour bien exploiter ses fonctionnalités, comme exemple, la configuration des ACL, de sorte à limiter le trafic sortant du réseau interne vers le réseau externe.

3. L'utilisation d'un seul compte pour la gestion du firewall et la documentation de changement

Pour ne pas permettre des accès non autorisés, des changements non contrôlés et l'impossibilité de surveiller des activités de l'administrateur, la solution proposée est de désigner un seul administrateur pour gérer le compte, et s'il a besoin de subordonnés ils doivent avoir chacun leurs comptes différents de l'administrateur pour exécuter les charges de gestion.

Pour pallier au manque de documentations sur les changements effectués, tous changement dans la configuration du firewall doit être documenté et archivé par l'administrateur. Les modifications doivent être autorisées si les conditions suivantes sont assurées :

- ✓ Le changement a été examiné méthodiquement et avec succès.
- ✓ Les impacts du changement sur le fonctionnement du système ont été testés.
- ✓ Les impacts du changement sur la sécurité du système ont été vérifiés.
- ✓ Toutes les entités affectées par le changement ont été informées.

IV.3.1.d. Solution de gestion et de configuration du système

1. La mise en place d'une bonne politique de mot de passe

Le service d'annuaire Active Directory de Microsoft serveur 2008, prend en charge toutes les exigences citées plus haut pour mettre en place une bonne politique de sécurité. Il permet aussi de spécifier la durée de validité de mot de passe, s'il doit être changé à la première utilisation ou non.

2. L'utilisation antivirus Kaspersky

La sécurité d'une entreprise s'évalue par la capacité de protection de son anti-virus, suite aux failles de sécurité de McAfee, nous proposons l'utilisation de l'anti-virus Kaspersky 8 Administration Kit qui nous semble plus avantageux. Parmi les fonctionnalités dont il dispose qui nous ont convaincu de son bon fonctionnement nous pouvons citer :

- ✓ Former une structure des groupes d'administration qui assure la protection antivirus de la société.

- ✓ Effectuer l'installation à distance et centraliser et la désinstallation des applications de la protection antivirus de l'entreprise.
- ✓ Recevoir et diffuser de façon centralisée sur les ordinateurs les mises à jour des bases et des modules de programme des applications antivirales.
- ✓ Recevoir les notifications sur les événements critiques dans le fonctionnement des applications de la protection antivirus.
- ✓ Recevoir les statistiques et les rapports de fonctionnement des applications de la protection antivirus.
- ✓ Administrer les licences de toutes les applications antivirales installées.
- ✓ Travailler avec les applications d'autres fabricants dans le réseau.

Ces fonctionnalités facilitent la mise en place d'un responsable de sécurité chargé d'administrer, surveiller, déployer et mettre à jour régulièrement Kaspersky Admin Kit. [27]

3. La suspension des ports ouverts et services démarrés

Les systèmes devraient seulement démarrer les services nécessaires pour effectuer leurs fonctions. Tous les autres services doivent être suspendus. La documentation de système devrait inclure tous les ports nécessaires au fonctionnement et devrait souligner l'importance de fermer tout autre port.

En se basant sur la documentation mise à notre disposition, nous utilisons la TMG et l'ASA afin de créer des règles pour fermer les ports et les services inutiles et se limiter aux besoins de la banque, comme les protocoles de messagerie et web (TCP, POP3, IMAP4, SMTP, HTTPS, DNS…).

4. La surveillance d'activités d'administrateurs

Les activités de l'administrateur devraient être surveillées étroitement afin de s'assurer que les privilèges ne sont pas mal utilisés. L'Active Directory se charge de cette tâche. Il permet d'activer la journalisation, définir sa durée et de l'appliquer aux administrateurs à travers une stratégie de groupe. Ceci permet de revoir régulièrement les activités d'administrateur et d'agir immédiatement si le compte d'administrateur a été compromis. Cette configuration est typiquement administrée et surveillée par une personne autre que l'administrateur de réseau, précisément un membre de l'équipe d'audit de sécurité.

5. Le verrouillage des stations et ports physiques

Afin de ne pas avoir un accès non autorisé aux privilèges administratifs attribués aux postes de travail. Nous implémentons des stratégies de groupe permettant le verrouillage des stations hors des horaires de travail. Pour éviter tous vol de données, introduction de virus intentionnel ou accidentel et craquage de mot de passe, nous bloquons l'ensemble des ports physiques (USB, CD/DVD, lecteur carte mémoire) grâce aux stratégies de groupe.

6. La mise en place des clusters

Afin d'assurer l'intégrité et la disponibilité des données, nous avons pensé à utiliser les clusters. Un cluster est un groupe logique de serveurs qui exécutent simultanément des applications ou des services tout en donnant l'impression au monde extérieur de ne constituer qu'un seul serveur. Ces derniers peuvent ou non communiquer avec leurs homologues du cluster. Dans cette étude nous appliquerons les deux solutions proposées par le clustering qui sont la tolérance aux pannes et la réparation de charge réseau.

- ✓ Un cluster tolérant aux pannes (failover) afin d'éviter toute indisponibilité des applications et services sélectionnés. Les serveurs mis en cluster appelés nœuds sont connectés via des câbles physiques les uns aux autres et au stockage disque partagé. Si l'un des nœuds est défaillant, un autre nœud prend le relais (basculement). Les serveurs d'un cluster de basculement peuvent fonctionner dans différents rôles, y compris les rôles d'un serveur de fichier, un serveur d'impression, un serveur de messagerie ou un serveur de bases de données, et proposent la haute disponibilité pour un grand nombre d'autres services et applications.
- ✓ Un cluster avec répartition de charge (Network Load Balancing) distribue en toute transparence les demandes clients entre les serveurs du cluster NLB, évitant ainsi toute surcharge sur un seul serveur, cela en utilisant des adresses IP virtuelles et un nom partagé. Du point de vue du client, le cluster NLB apparait comme un serveur unique. Nous proposons de l'utiliser pour créer une batterie web avec un groupe de serveurs travaillant pour prendre en charge le site web de la banque.

IV.4. 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. Mais comme nous l'avons vu, en nous basant uniquement sur les documents fournis sur l'infrastructure de la banque, il existe diverses vulnérabilités que nous avons découvertes et expliquées dans ce chapitre. Nous tenons à souligner que cette liste de failles n'est pas exhaustive car nous nous sommes limitées aux données qui ont été mises à notre disposition.

Apres avoir examiné les différentes failles, nous avons proposé des solutions qui permettront de pallier ces différentes vulnérabilités qu'elles soient réseaux ou systèmes. Ce que nous pouvons affirmer après notre étude c'est qu'il faut mettre à jour l'infrastructure réseau (réseau et systèmes) avec des moyens récents et effectuer des tests en tenant compte des nouvelles techniques de piratages pour optimiser les chances de sécurités.

Dans le chapitre suivant nous allons mettre en pratique la plupart des solutions mentionnées dans celui-ci.

Chapitre V : Réalisation de l’application

V.1. 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 de minimiser au maximum les risques d'attaques et les points vulnérables de la banque 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 les solutions citées précédemment.

V.2. Présentation des outils utilisés

V.2.1. Le simulateur graphique de réseaux

Dans le but de se rapprocher le plus possible de la mise en place d'une architecture réseau réelle, nous avons opté pour l'utilisation de GNS3 (Graphical Network Simulateur). Un logiciel open source qui est à la fois simulateur et émulateur, simulateur de réseaux LAN et WAN et émulateur de routeurs et firewalls CISCO et Juniper. Autant que simulateur il imite le comportement de l'équipement, comme émulateur il exécute directement le système d'exploitation de l'équipement, ce qui permet d'assurer les mêmes résultats dans le cas réel. (Dans l'annexe A, vous trouverez plus d'information sur le fonctionnement et l'installation de GNS3).

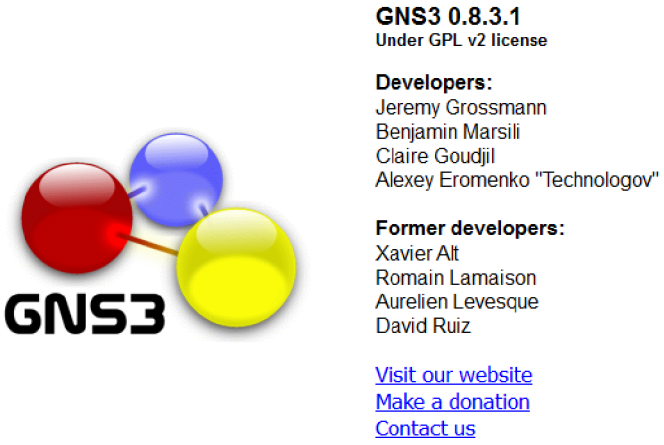

Figure V.1 : GNS3.

V.2.2. La VMware Workstation 9.0.0

Pour l'émulation de notre réseau, nous avons choisi d'utiliser la VMware Workstation 9.0.0. 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.

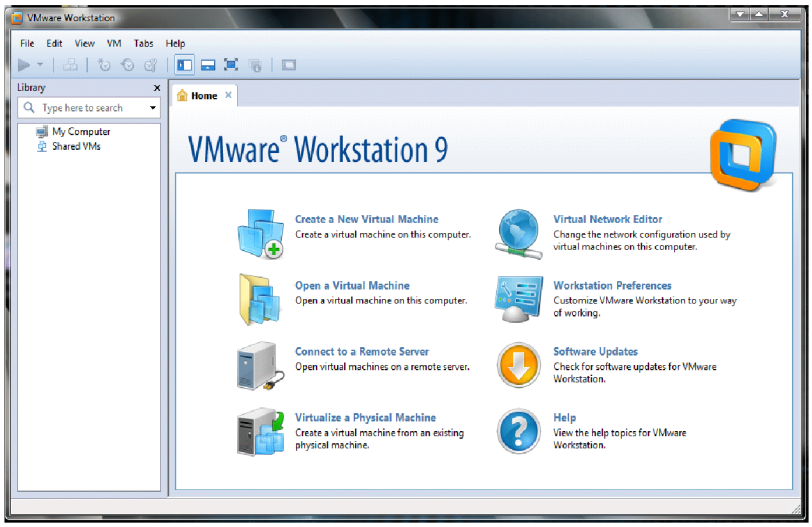

Figure V.2: VMware Workstation 9.

V.2.3. 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.

Figure V.3 : Server 2008.

V.2.4. 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.4: Active Directory.

V.2.5. Les caractéristiques du PC utilisé

Vu que notre application exige de grandes ressources matérielles, l'utilisation d'un PC professionnel était primordiale pour regrouper les solutions proposées, réseaux et systèmes. Les caractéristiques du PC portable professionnel utilisé sont :

- ✓ Processeur I5 x64 bits
- ✓ RAM 5G
- ✓ Disque dur 560 G
- ✓ Système Windows 7 professionnel x64 bits
- ✓ Prise en charge de la virtualisation.

V.3. Les étapes suivies pour la mise en place de notre application

Vu qu'il est impossible d'implémenter toute l'infrastructure réseau de la banque avec les solutions réseaux et systèmes proposées. Nous avons simplifié l'architecture de sorte à permettre la mise en place de notre politique de sécurité. La figure suivant montre l'architecture simplifiée.

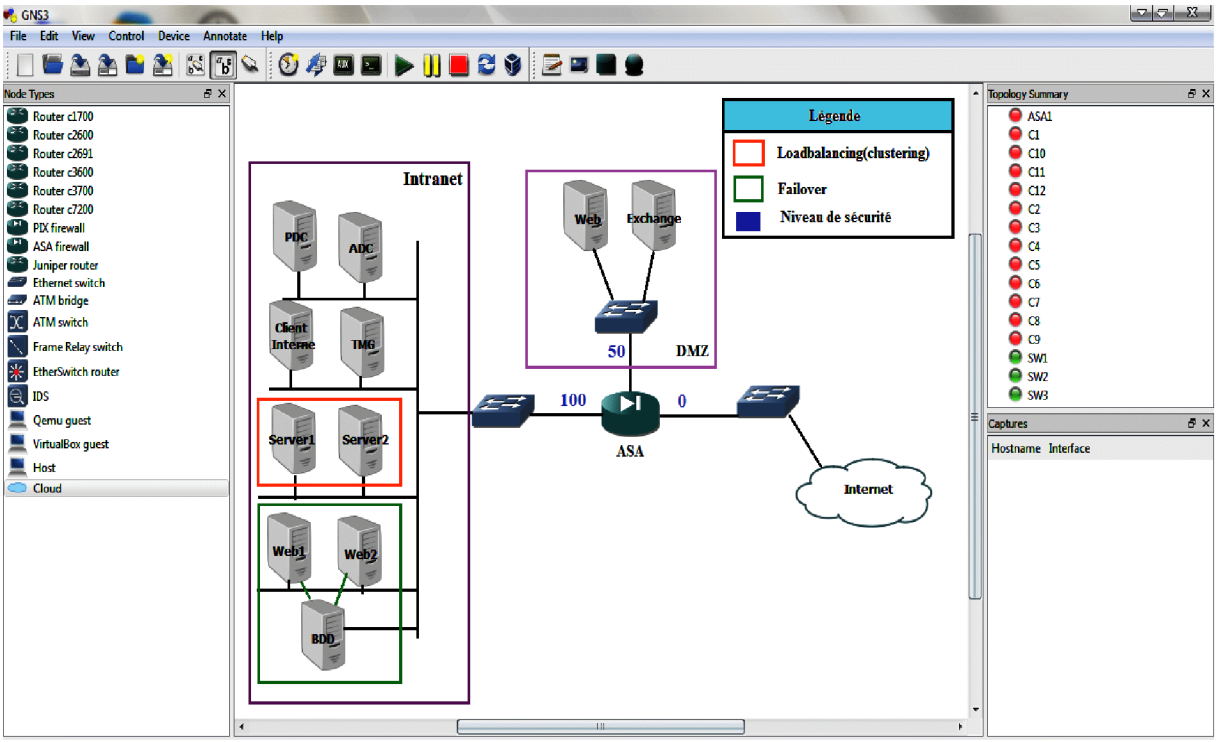

Figure V.5 : L'infrastructure réseau mise en place sous GNS3.

Dans ce qui suit, nous présentons les différentes étapes suivies pour la réalisation de notre application.

Etape I : la préparation des machines

Nous avons préparé les machines suivantes :

- ✓ Un contrôleur de domaine principal.
- ✓ Un contrôleur de domaine secondaire.
- ✓ Un serveur 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.
- ✓ Une machine membre client interne qui fait office de machine test.
- ✓ Deux machines membres pour l'implémentation de la solution load balancing.
- ✓ Deux machines membres pour l'implémentation de la solution failover.
- ✓ Une machine membre pour la base de données.
- ✓ Une machine (internet) client externe qui fait office de machine test.

1. L'installation du contrôleur de domaine principal et secondaire

Après préparation de deux machines virtuelles Windows Server 2008, nous avons installé sur la première machine un contrôleur de domaine principal (PDC), **banque.com.** Sur la deuxième

machine nous avons effectué le déploiement du contrôleur de domaine pour avoir un contrôleur de domaine secondaire (ADC). Ce dernier sert à la réplication du PDC.

L'installation des deux contrôleurs est la même à la différence du choix de l'étape montrée ci-dessous. La première figure montre le choix de la création d'un nouveau domaine principal et la deuxième l'installation d'un contrôleur de domaine secondaire.

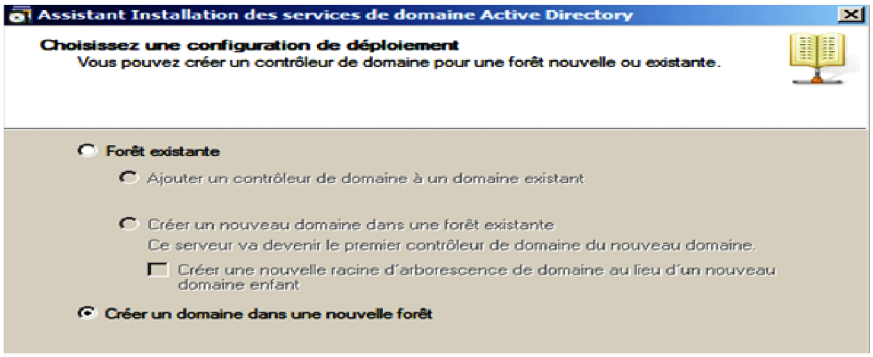

Figure V.6 : La création du domaine principal.

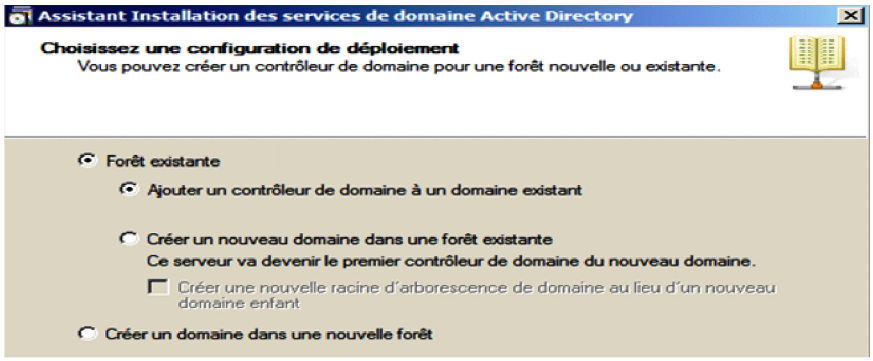

Figure V.7 : L'ajout du domaine secondaire.

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

2. 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 :

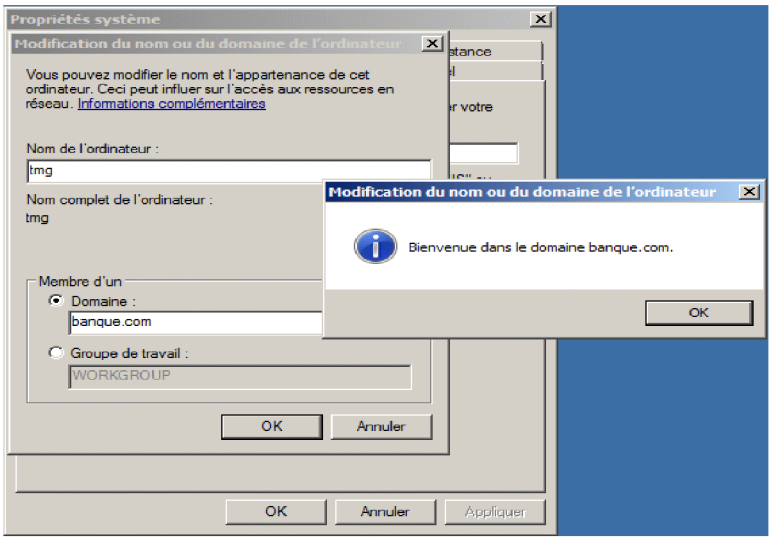

Figure V.8 : Ajout de la TMG au domaine banque.com.

Etape II : L'installation et configuration de la TMG

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

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

- ✓ Une interne avec l'adresse 10.0.0.5/8
- ✓ Une externe avec l'adresse 192.168.0.1/24
- ✓ Une pour la DMZ avec l'adresse 170.100.100.1/16

3. Installation du serveur Web IIS

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. (Voir annexe C).

4. Lancement de l'installation de la TMG

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

Figure V.9 : La console de gestion de la TMG.

5. La création des règles de la TMG

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

- **Exemple de la règle DNS**

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

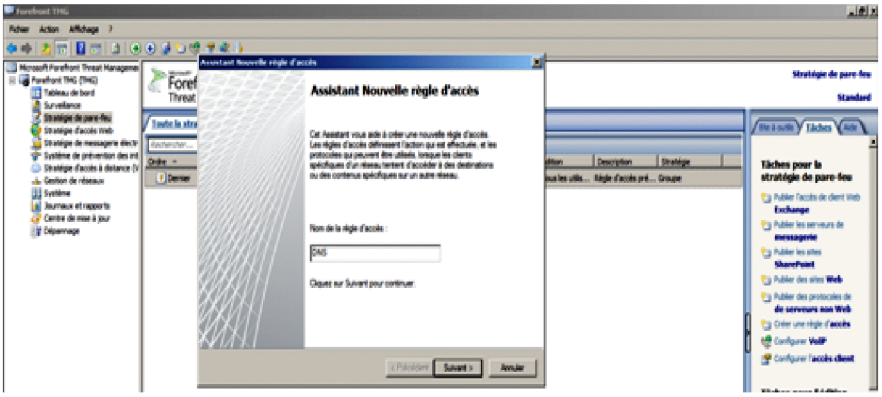

Figure V.10: création de la règle d'accès DNS.

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

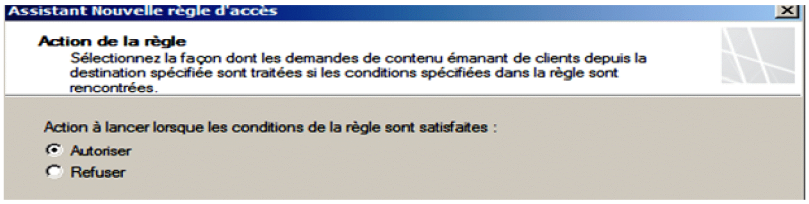

Figure V.11: Choix de l'action de la règle.

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

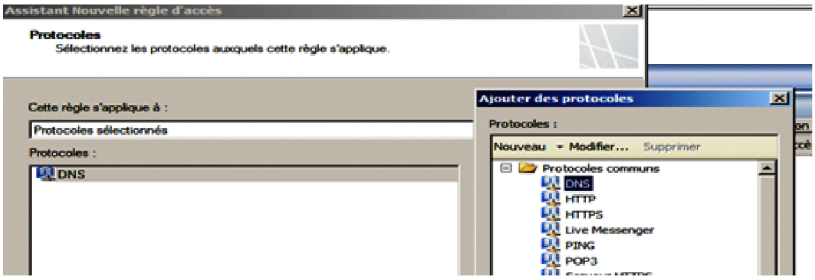

Figure V.12: Sélection des protocoles.

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

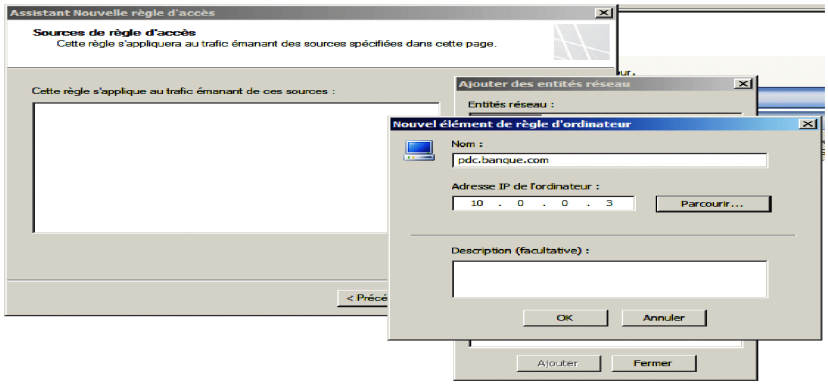

Figure V.13 : Sélection de la source de règle d'accès.

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

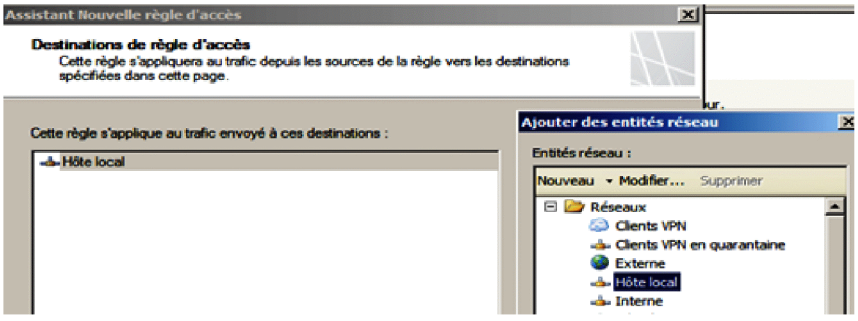

Figure V.14 : Spécification de la destination de la règle d'accès.

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

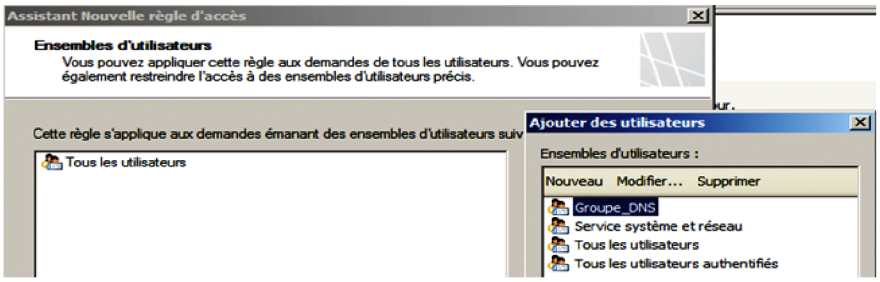

Figure V.15: Ensemble des utilisateurs concernés par la règle d'accès.

- **Exemple de la règle pour empêcher l'accès à certain sites**

Définissons les utilisateurs sur lesquels s'applique cette règle.

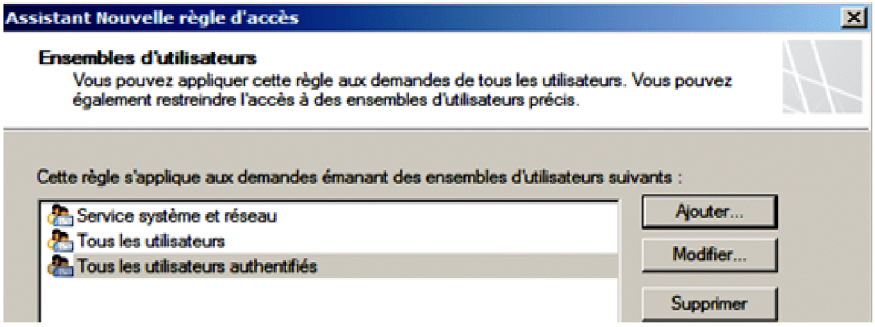

Figure V.16: L'ensemble des utilisateurs concernés par la règle de refus.

Choisissons les sites à exclure, comme les réseaux sociaux, les sites d'achat e-commerce et autres.

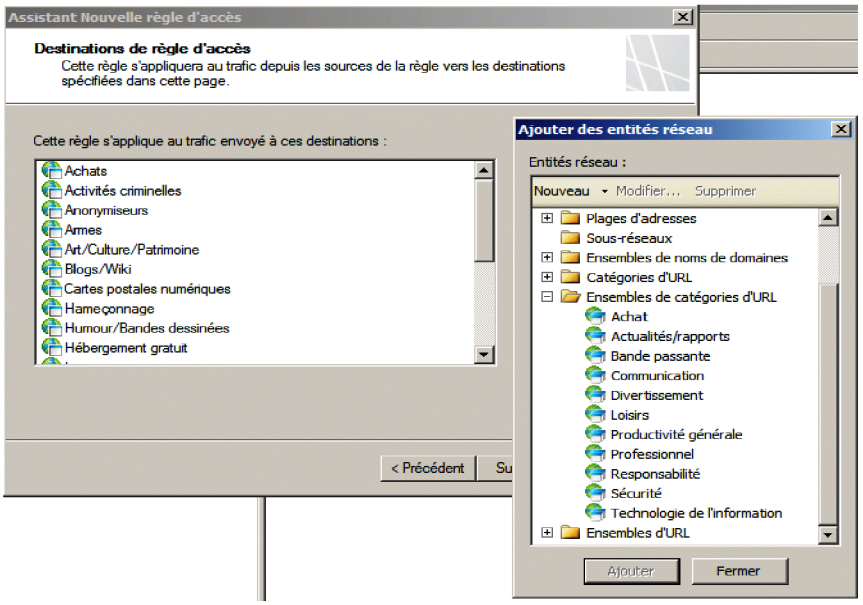

Figure V.17 : La sélection des catégories d'URL non autorisées.

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

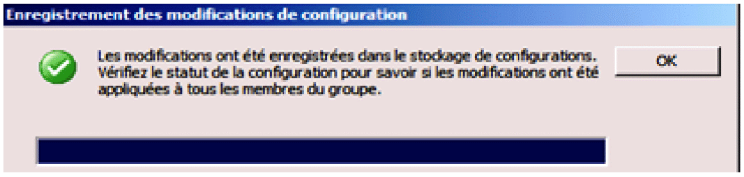

Figure V.18: Enregistrement des modifications.

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

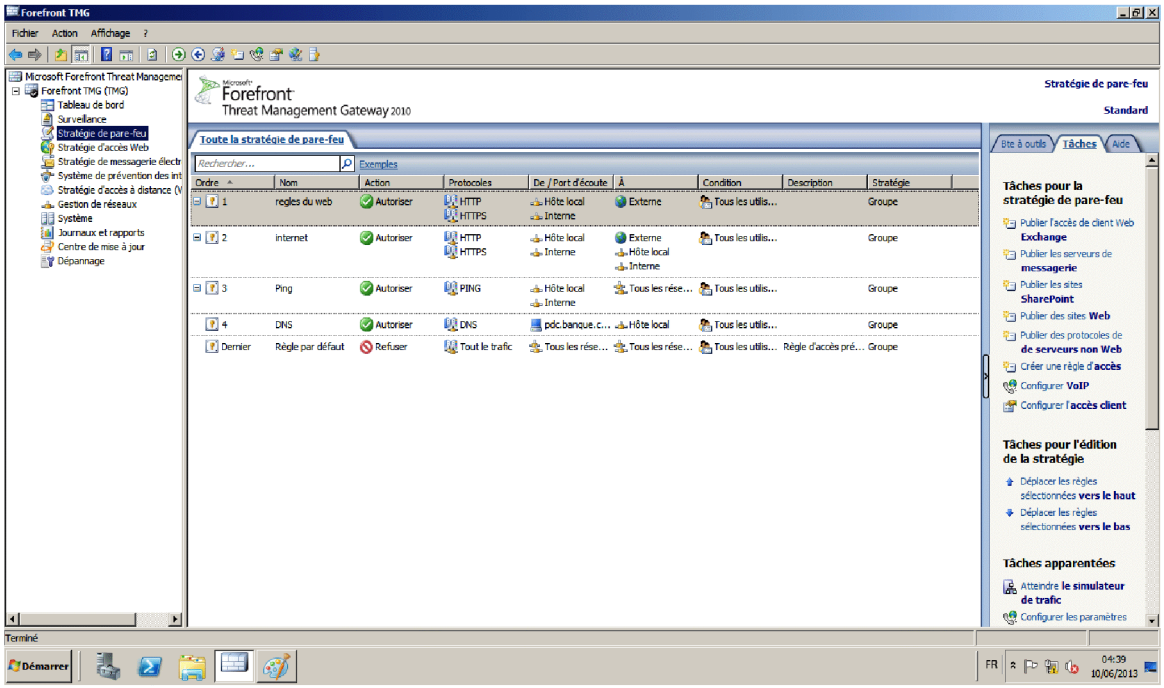

Figure V.19: Récapitulatif des règles TMG.

Etape III : Installation et configuration du Server Exchange 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.

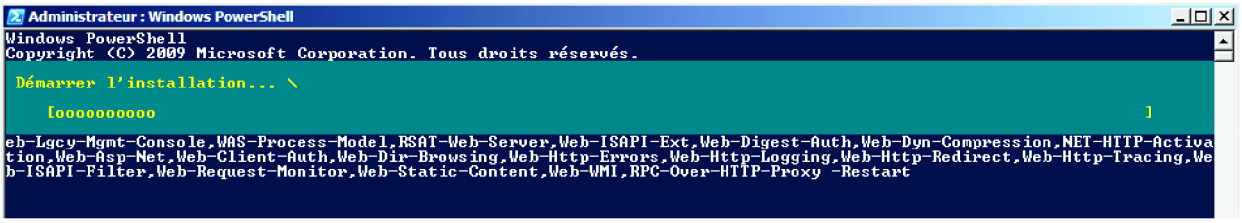

Figure V.22: Installation des pré-requis.

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 banque.com

Command: C:\>Setup /PrepareAD /OrganizationName:banque.

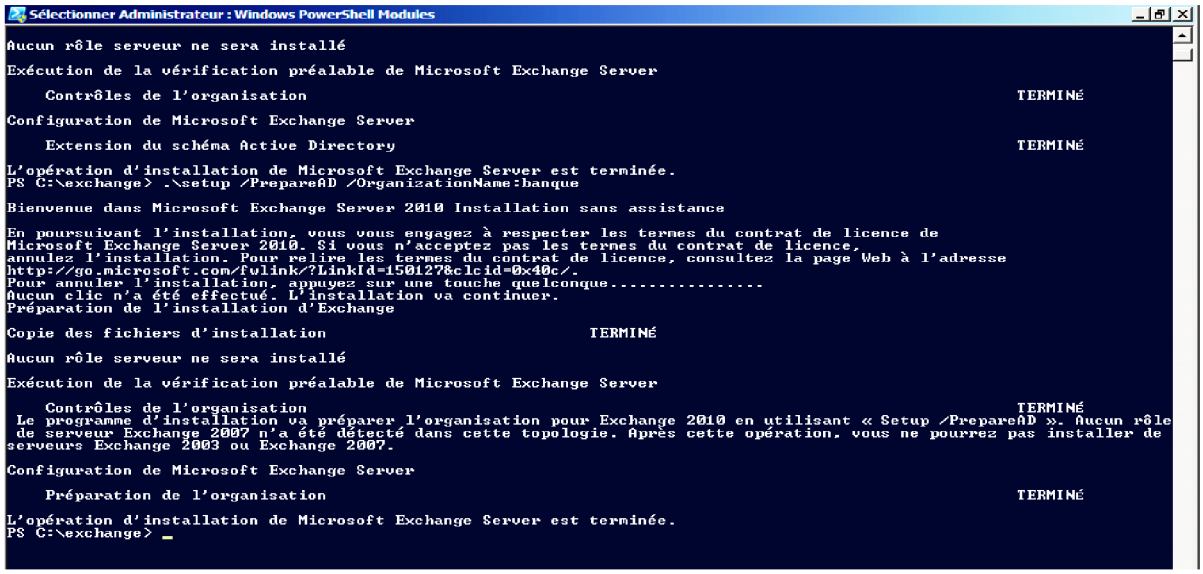

Figure V.25: Préparation de la forêt.

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

Commande : C:\>Setup /PrepareDomain.

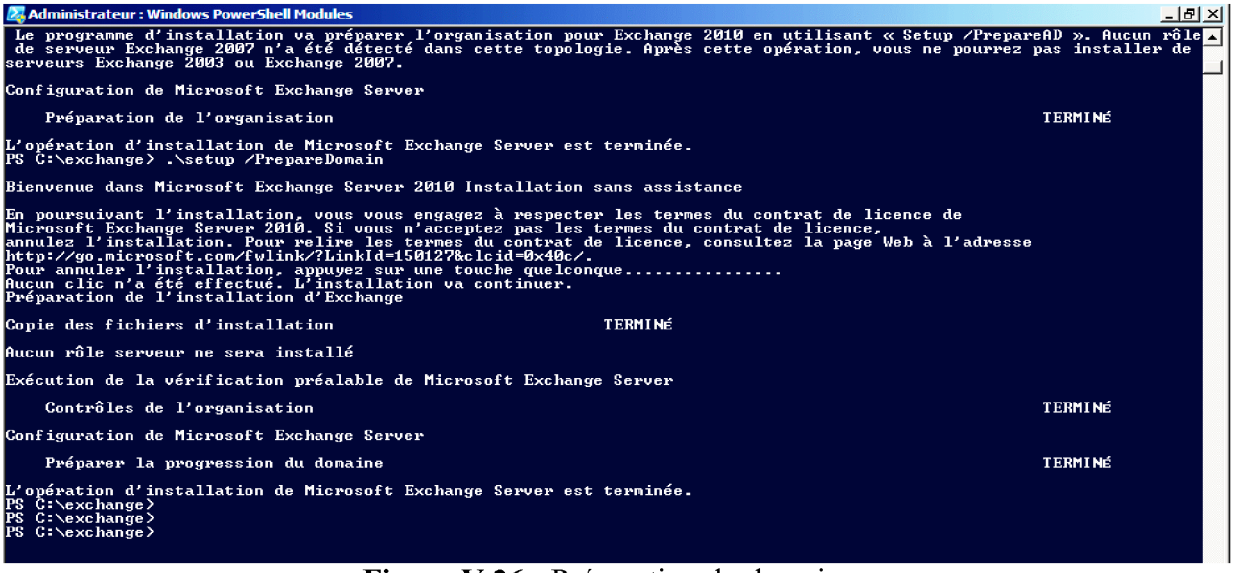

Figure V.26 : Préparation du domaine.

2. 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.

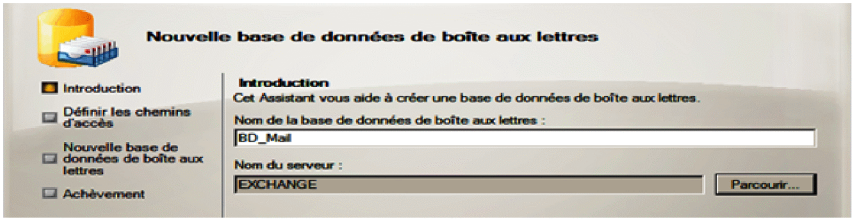

Figure V.27 : Création de la base de données de boite aux lettres.

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.

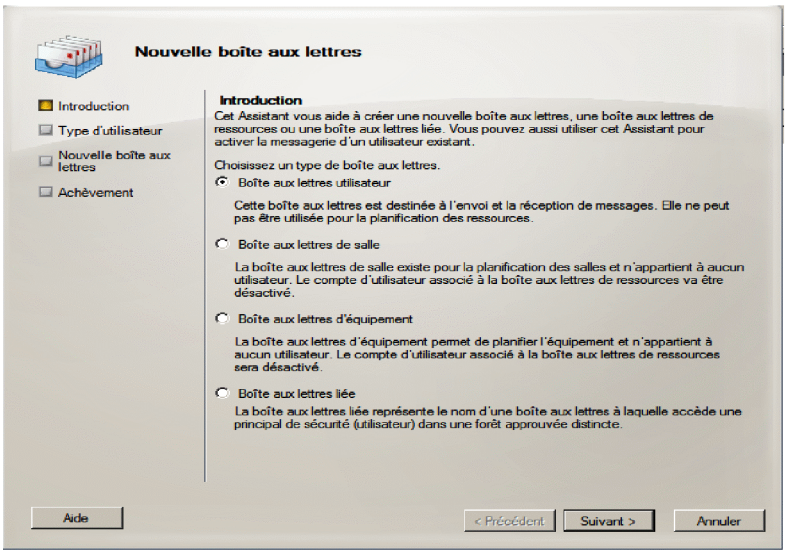

Figure V.28: Création de boite aux lettres utilisateur.

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

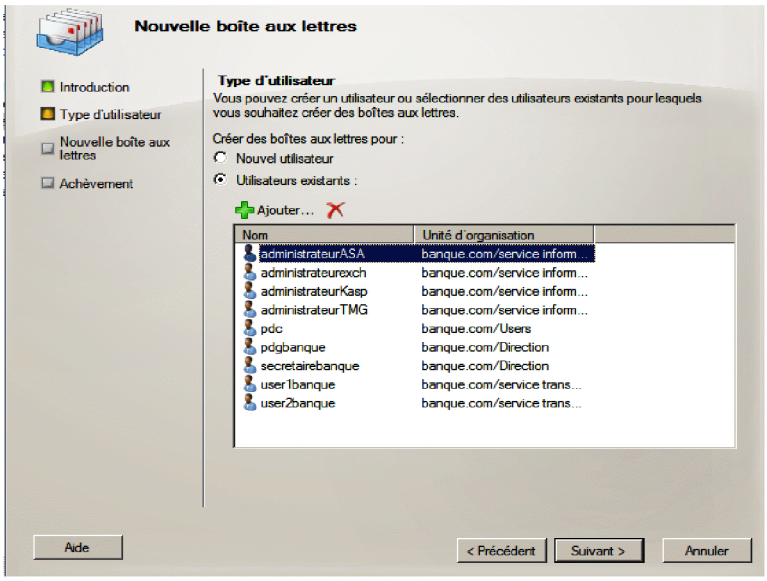

Figure V.29: Sélection des utilisateurs.

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

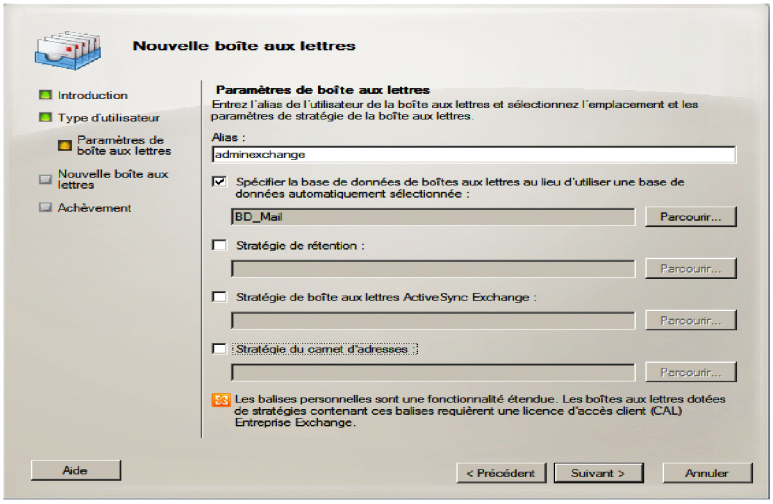

Figure V.30 : Paramétrage de boite aux lettres.

Etape IV : 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

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.

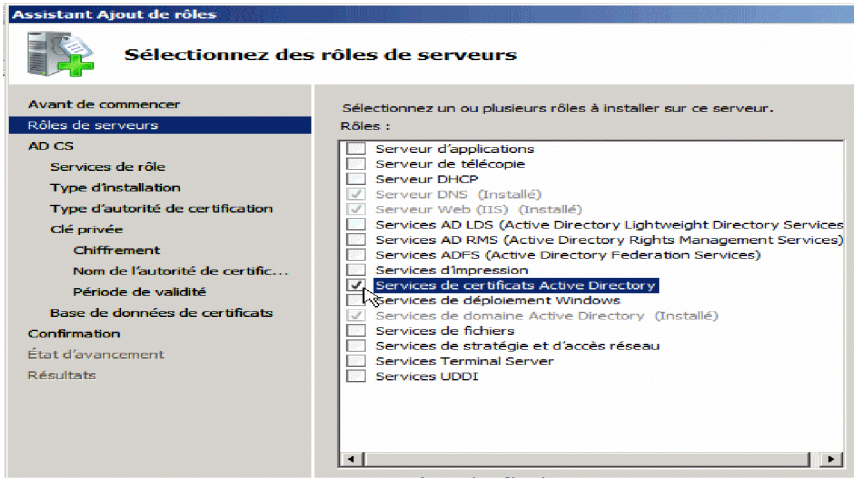

Figure V.31: Ajout du service de certificats Active Directory.

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.

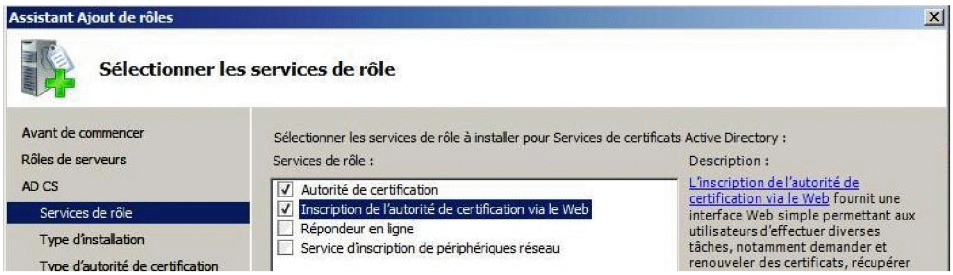

Figure V.32 : Les services de rôle.

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.

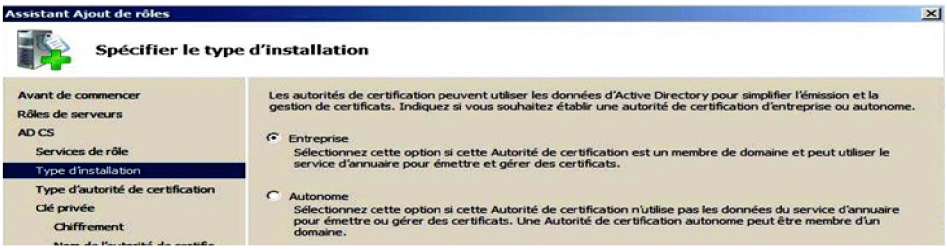

Figure V.33: Spécification du type d'installation.

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).

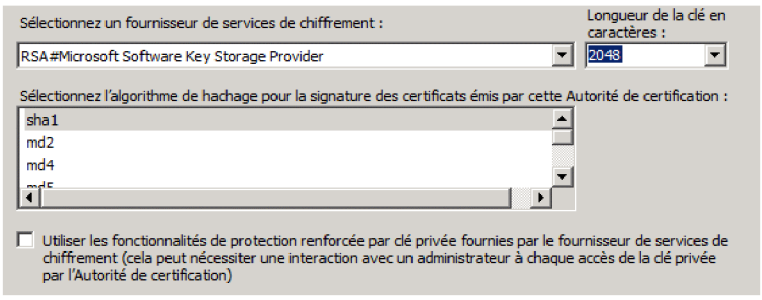

Figure V.34: Création d'une nouvelle clé privée.

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

Figure V.35: Nomination de l'Autorité de certificat.

A la fin de cette installation, création de l'autorité **banque-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.

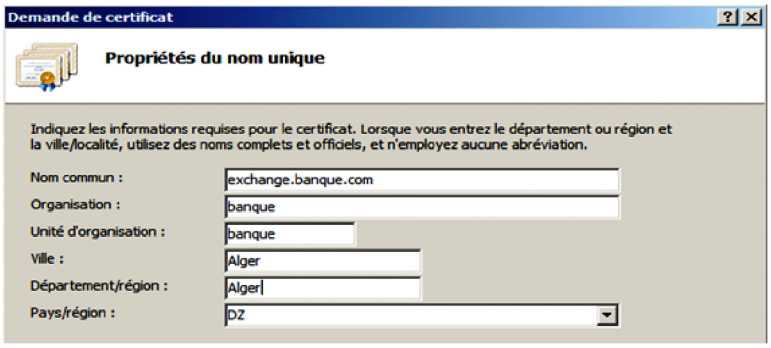

Figure V.36 : Demande de certificat.

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

Figure V.37: Propriétés du fournisseur de services de chiffrement.

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

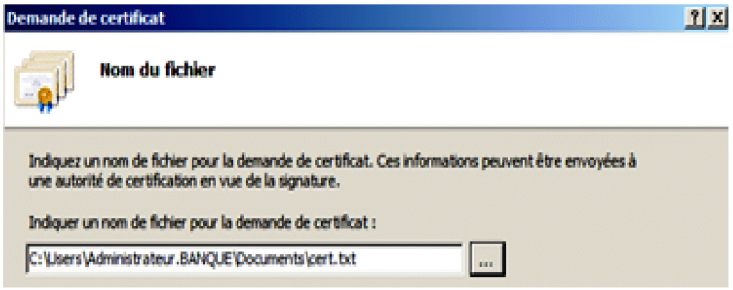

Figure V.38: Fichier de demande de certificat.

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

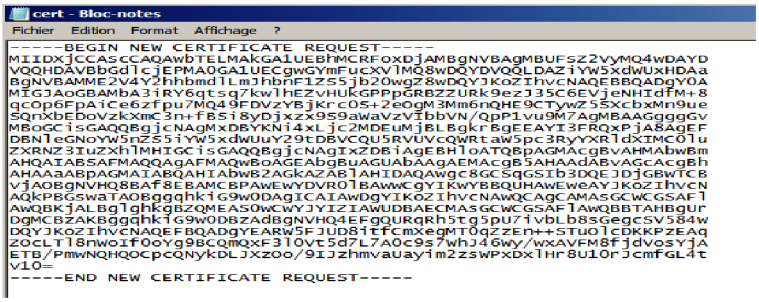

Figure V.39 : clé privée de certificat.

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 :

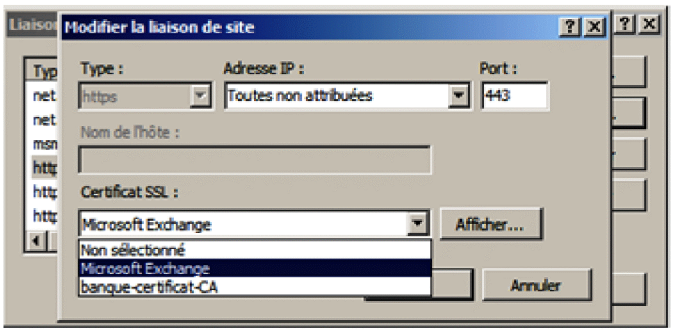

Figure V.40: Liaison avec HTTPS.

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.

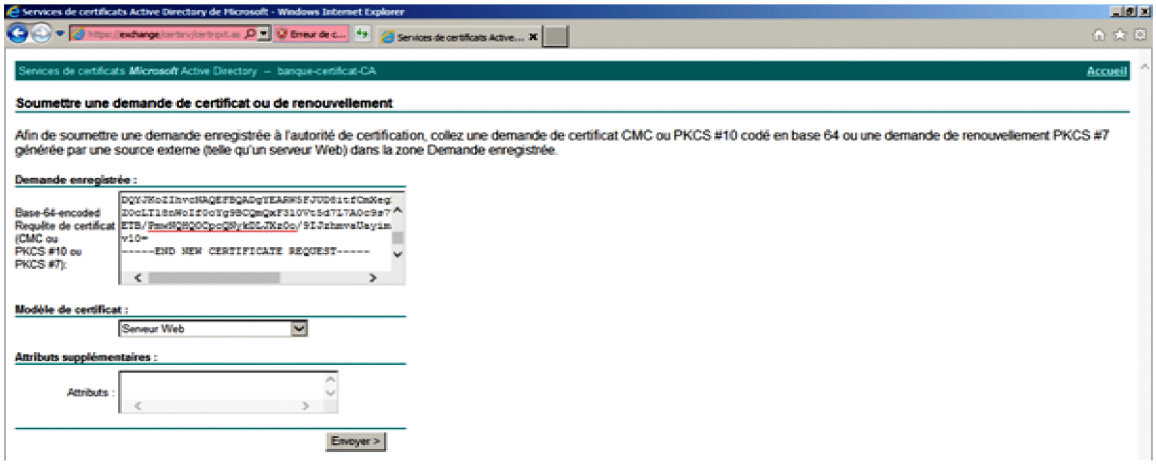

Figure V.41 : Soumettre une demande de certificat.

Téléchargeons le certificat en spécifiant son emplacement.

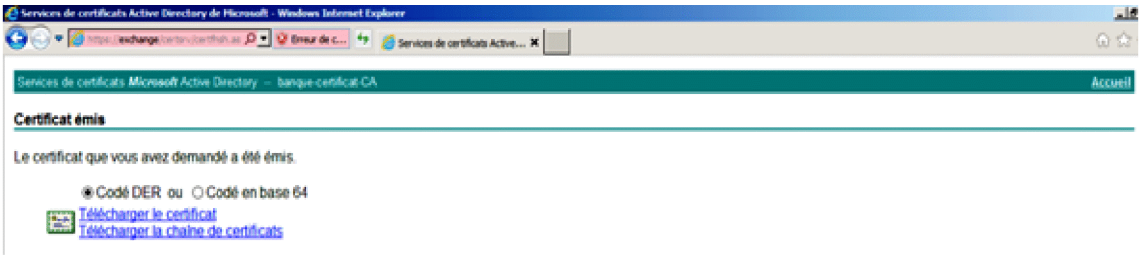

Figure V.42 : Téléchargement de certificat.

3. Terminer la demande de certificat

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

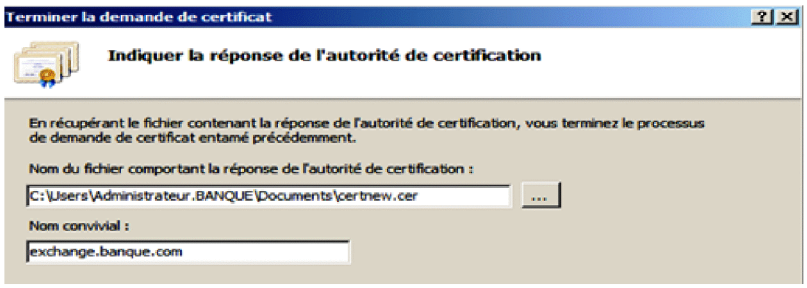

Figure V.43: Terminer la demande de certificat.

La demande de certificat exchange.banque.com étant finalisée nous pouvons modifier la liaison du site par défaut en utilisant cette fois le nouveau certificat signée par notre CA, banque-certificat-CA.

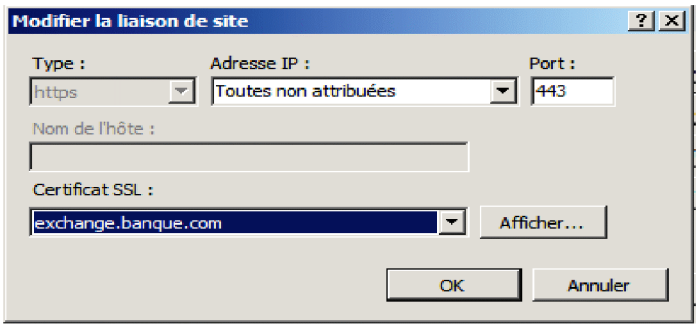

Figure V.44: Modification de la liaison de site.

4. Création des zones DNS sous Active Directory

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

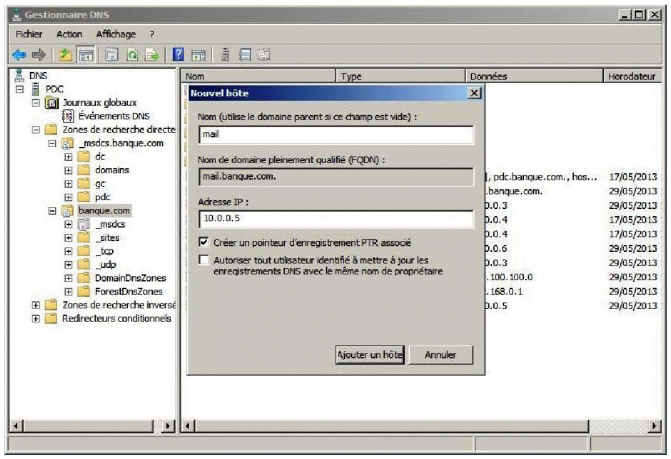

Figure V.45: Enregistrement de serveur de messagerie Exchange.

Afin de permettre l'accès au serveur de messagerie à partir de l'extérieur, nous avons ajouté un autre enregistrement avec l'adresse de l'interface externe de la TMG avec le nom de **mail.banque.com**.

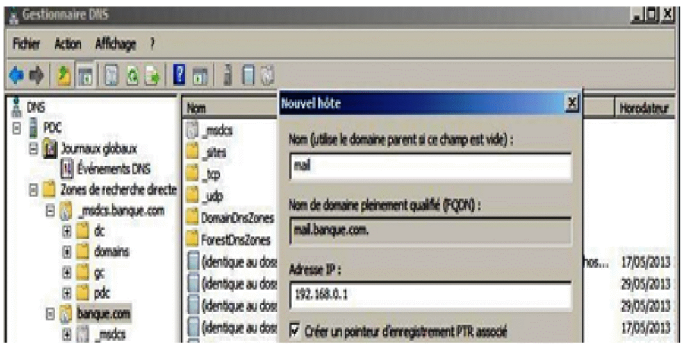

Figure V.46 : Enregistrement de l'interface externe.

5. La publication du serveur de messagerie via TMG

A ce stade si nous essayons d'accéder avec l'adresse https://mail.banque.com/certsrv à partir de la TMG, nous ne le pourrons pas car la TMG ne détient pas de certificat. Afin de permettre un accès sécurisé via les certificats, nous procédons comme suit :

Depuis l'exchange :

- ✓ Exportons l'autorité de certificat banque-certificat-CA et le certificat exchange.banque.com. L'exportation se fera d'une manière sécurisée avec l'utilisation de l'administrateur et d'un mot de passe.
- ✓ Mettons ces certificats exportés dans un dossier et partageons les avec pour seule autorisation la lecture par l'administrateur.
- ✓ Ayant été partagé, le dossier peut être lu depuis la TMG, où il sera copié.

5. 1. L'exportation de banque-certificat-CA

La manière d'exporter les certificats étant la même nous illustrons juste l'exportation de la CA avec des figures. L'exportation se fait avec l'exécution de la commande MMC. Après exécution nous voyons apparaitre la Console de Microsoft Management (MMC) que voici :

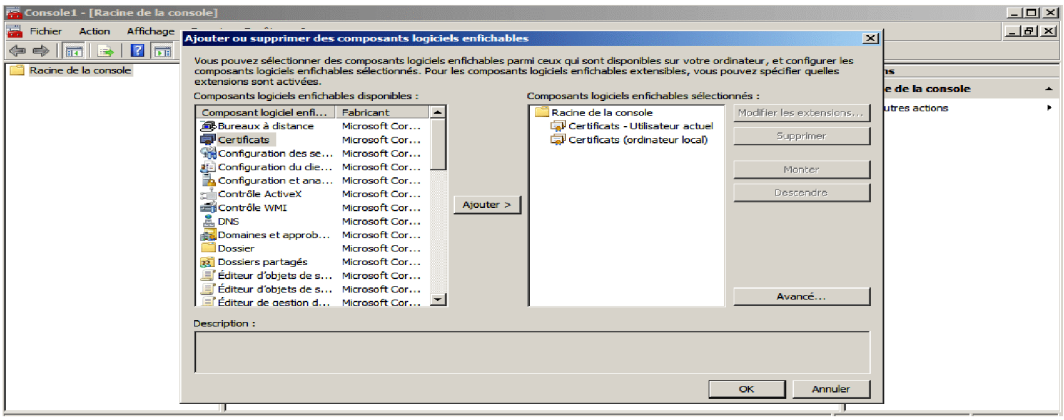

Figure V.47: Les certificats avec la Console Microsoft Managment.

Dans certificat (ordinateur local) -> dossier autorité de certificat -> banque-certificat-CA -> exportons la clé privée comme suit :

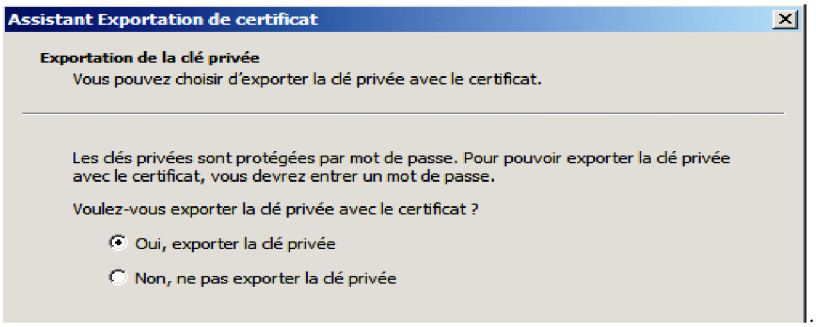

Figure V.48 : exportation de la clé privée.

Définir le type de format de fichier d'exportation, PKCS #12.

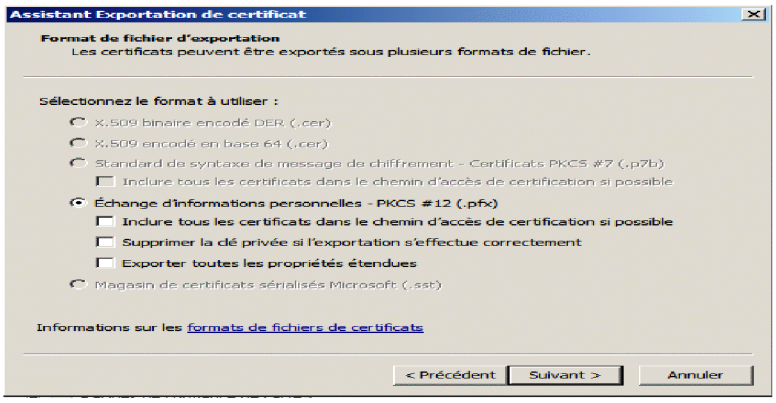

Figure V.49: format du fichier d'exportation.

Entrons le mot de passe qui permet de protéger la clé privée.

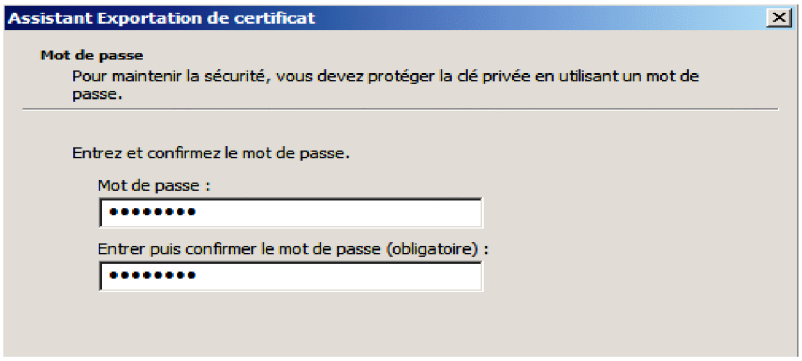

Figure V.50 : Mot de passe.

Pour finir l'exportation, définissons un emplacement pour finaliser l'exportation du fichier .pfx.

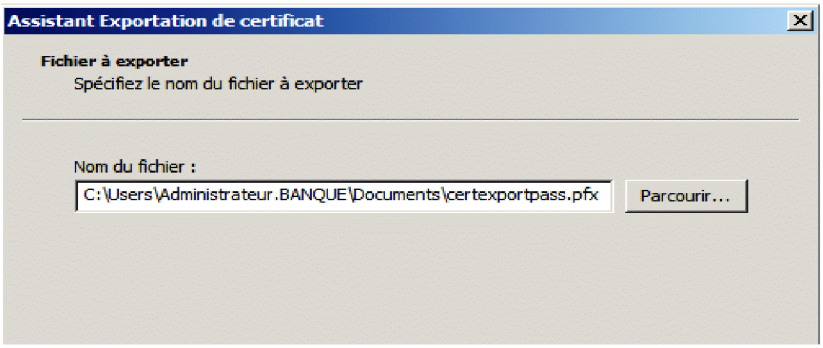

Figure V.51: Fichier à exporter.

5. 2. Importation du certificat

Maintenant que la CA et le certificat exchange.banque.com ont été exportés et copiés dans la TMG comme expliqué plus haut, passons à l'importation de ces derniers dans la TMG. Toujours avec l'utilisation de la commande MMC, nous importons les certificats dans l'ordinateur local et l'utilisateur actuel et à chaque fois dans le dossier personnel et le dossier autorité de certificats. Comme suit :

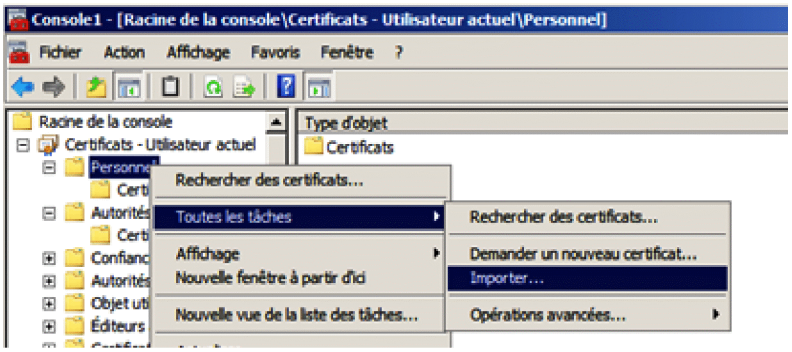

Figure V.52: La console MMC.

Sélectionnons le fichier à importer.

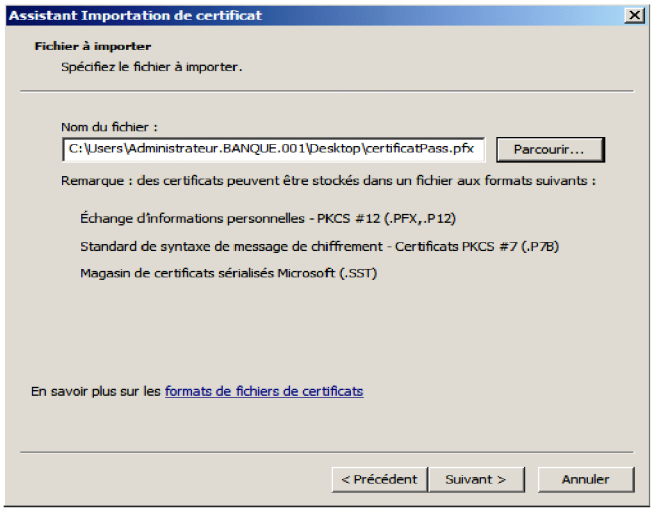

Figure V.53: Fichier à importer.

Entrons le mot de passe qu'on avait utilisé pour protéger la clé privée et finaliser l'importation de la CA.

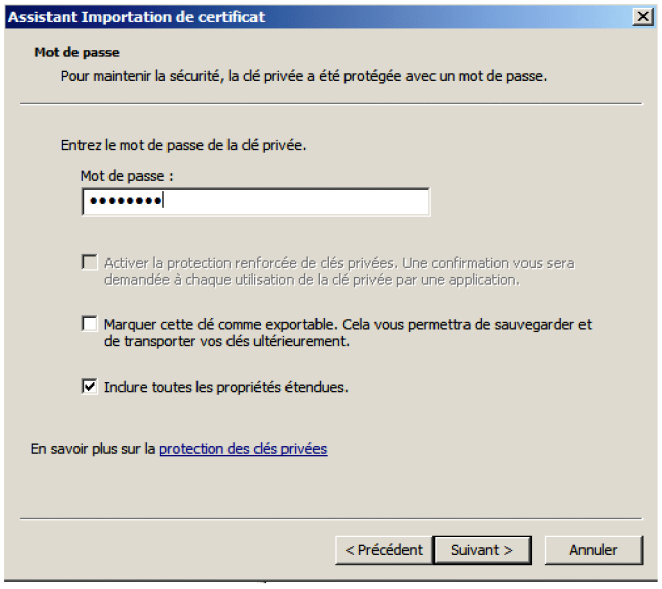

Figure V.54: Mot de passe.

6. Création du certificat mail.banque.com

Si nous avons exporté l'autorité de certificat, banque-certificat-CA, c'est pour signer avec cette autorité le certificat qui va être créé pour certifier le site **mail.banque.com** de la messagerie OWA. Pour ce faire nous allons suivre les étapes suivantes :

Dans MMC mais cette fois seulement dans l'ordinateur local et dans personnel ->toutes les tâches ->opérations avancées -> gérer les stratégies d'inscription.

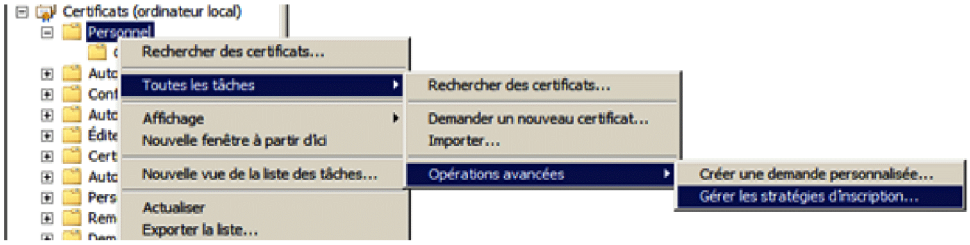

Figure V.55: Gestion des inscriptions d'inscription.

Nous voyons s'afficher la page, Inscription de certificat, ayant configuré les certificats à l'aide de l'AD, la stratégie sélectionnée est donc Stratégie d'Inscription à Active Directory.

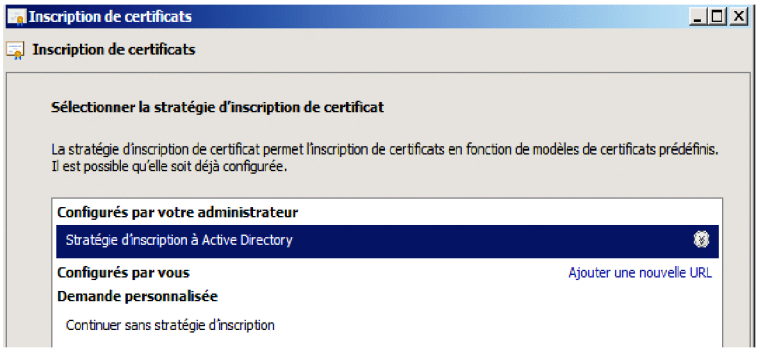

Figure V.56 : Sélection de la stratégie d'inscription de certificat

Voulons utiliser le certificat pour l'échange de mail via le web, le modèle choisi est donc Serveur Web avec le format PKCS #10.

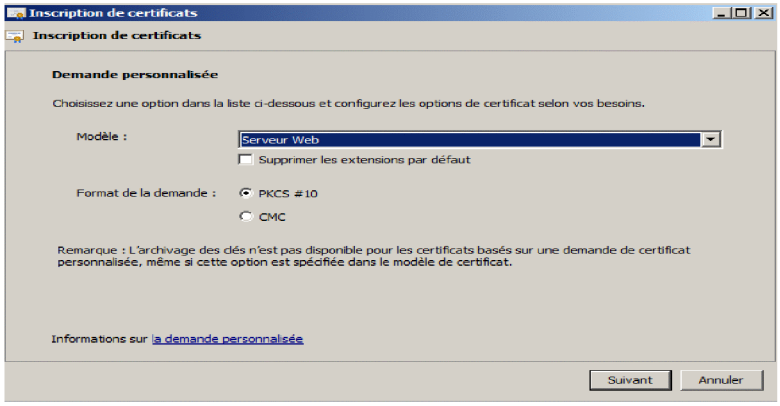

Figure V.57 : demande personnalisée.

Dans les propriétés du certificat nous saisissons le nom du certificat, mail.banque.com, en spécifiant son type. Ayons utilisé la zone DNS, le type n'est autre que DNS.

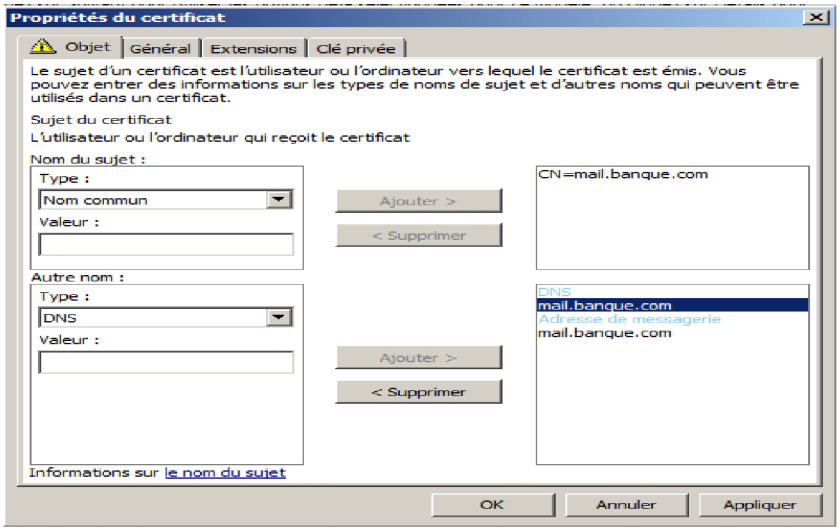

Figure V.58: Objet de propriétés du certificat.

Dans l'étape qui suit, nous spécifions le rôle du certificat, à l'aide de l'extension de ce certificat web. Ces types sont le chiffrement de clé et signature numérique de la clé.

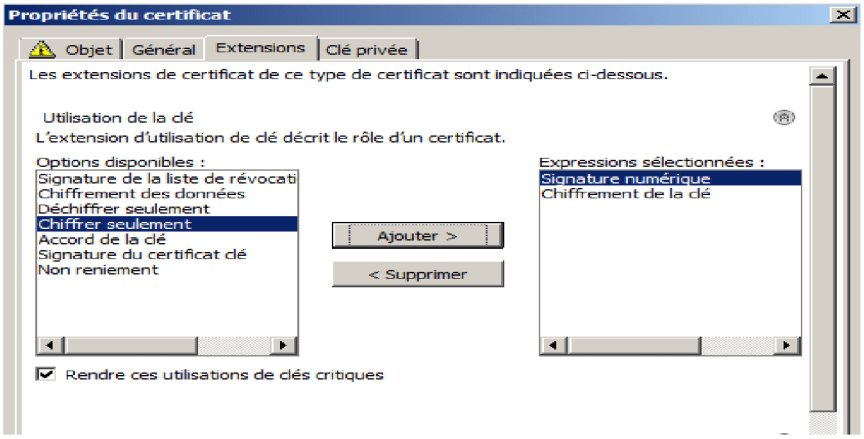

Figure V.59: Extension de propriétés du certificat.

Le certificat sera utilisé pour authentifier les serveurs et authentifier les clients.

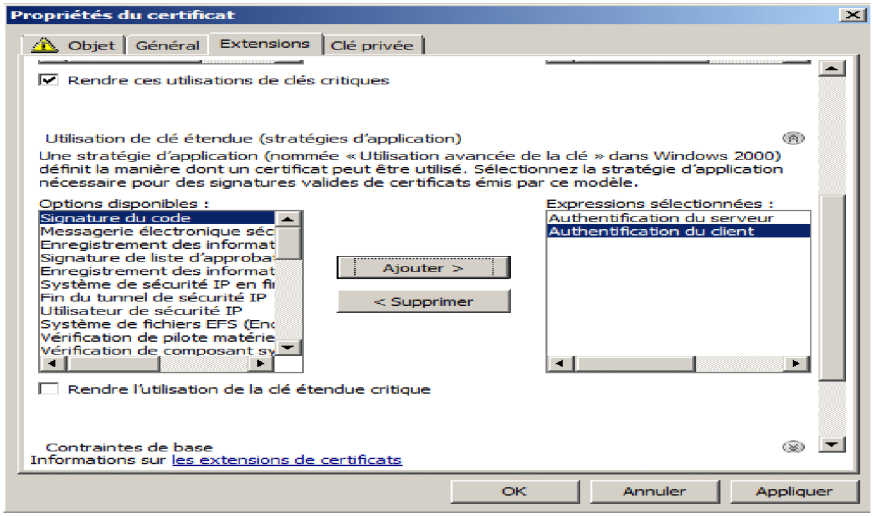

Figure V.60: Stratégie application de propriétés du certificat.

Dans cette étape nous sélectionnons le fournisseur du chiffrement et la taille de la clé.

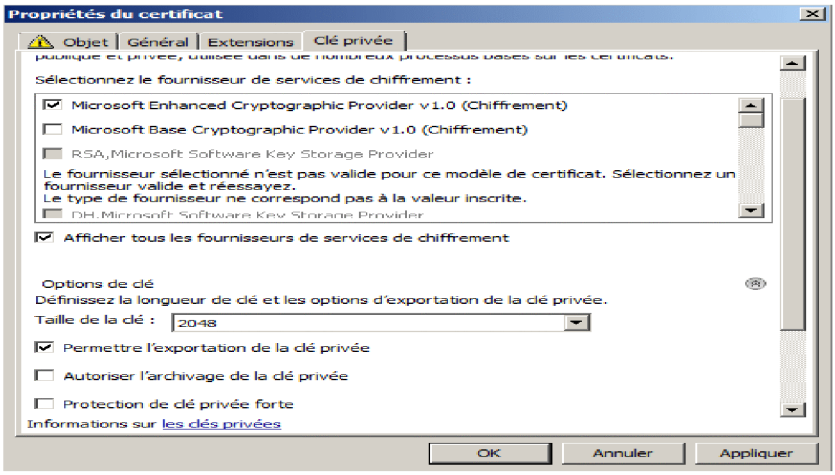

Figure V.61: Clé privée de propriétés du certificat.

Dans cette dernière étape d'inscription de certificats, nous enregistrons la clé privée dans un fichier en définissons son format en base 64.

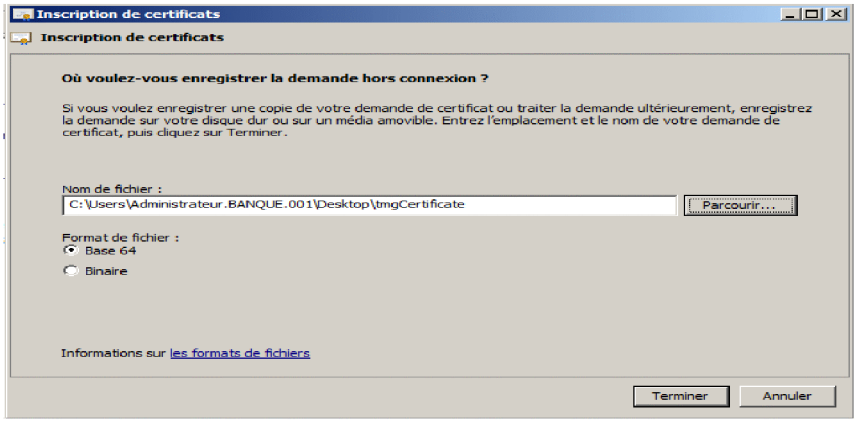

Figure V.62 : Format fichier.

Pour finaliser la demande de certificat, nous utilisons le web comme suit :

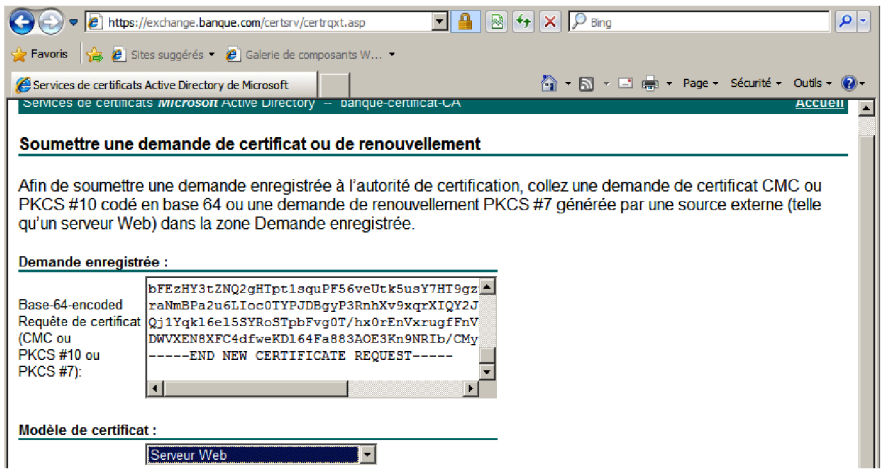

Figure V.63: soumettre une demande de certificat.

Après l'envoie de la demande, la clé est prête à être installée dans la TMG.

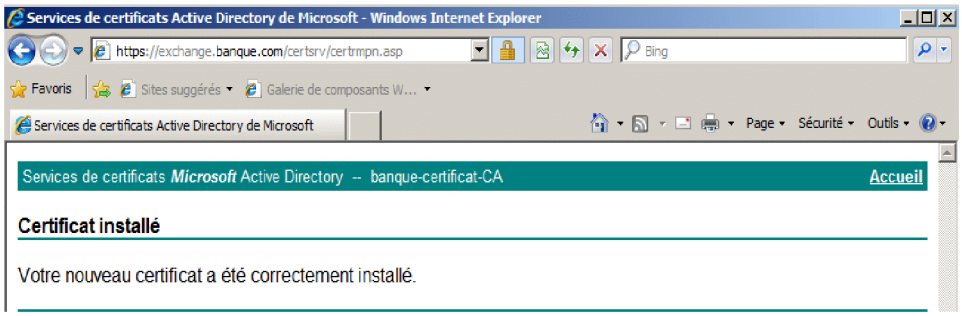

Figure V.64: Installation du certificat.

Après installation, le certificat mail.banque.com est prêt à être importé, comme fait plus haut.

7. Ajout de règles d'accès TMG

7. 1. Ajout de règles pour la TMG permettant un accès à OWA :

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

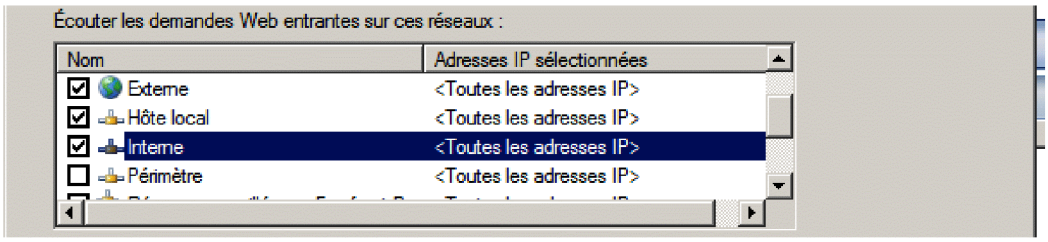

Figure V.65 : Définir les réseaux à écouter.

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

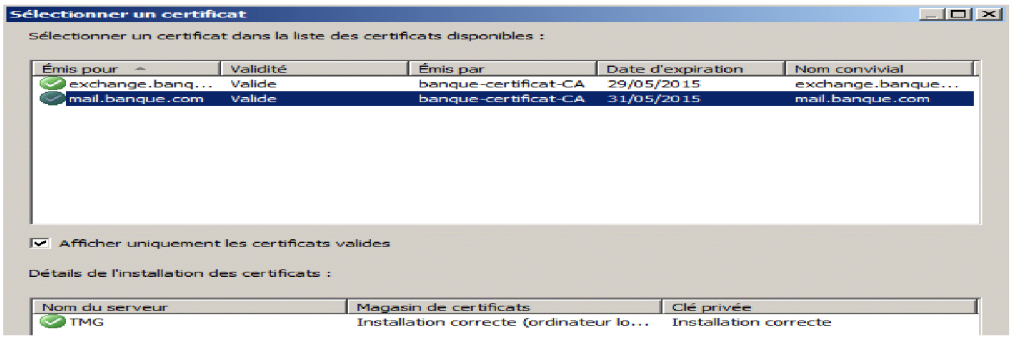

Figure V.66: Définir quel certificat utilisé.

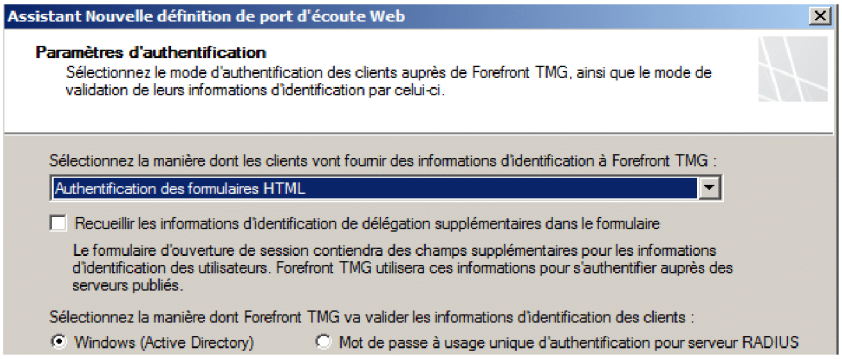

Figure V.67 : Le mode d'authentification utilisée.

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

Entrons le nom du site local.

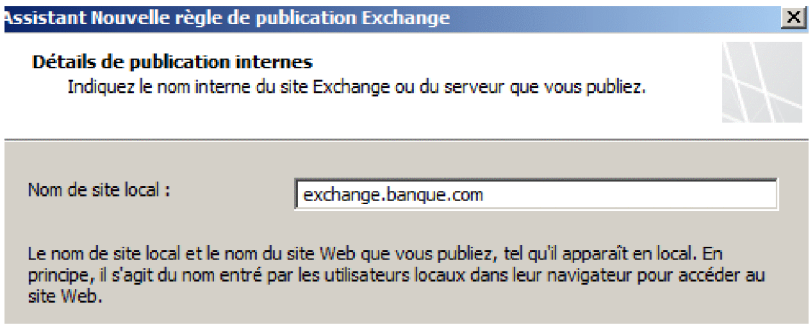

Figure V.68: Spécification du nom du site local.

Saisissons le nom public du site OWA, mail.banque.com.

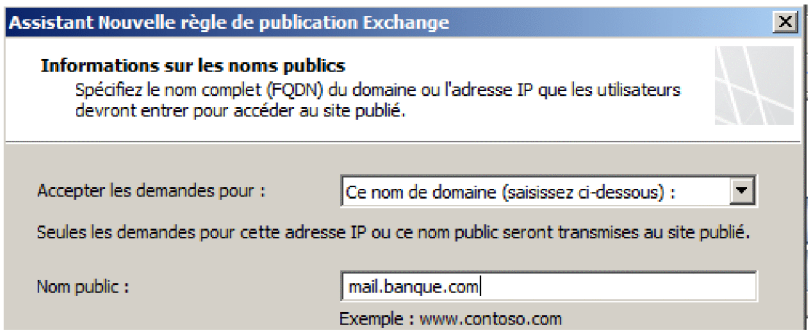

Figure V.69: Spécification des informations sur les noms publics.

Créons une règle pour sélectionner tous les services sécurisés autorisés pour l'utilisation de la messagerie comme le POP3, IMP4 et SMTP.

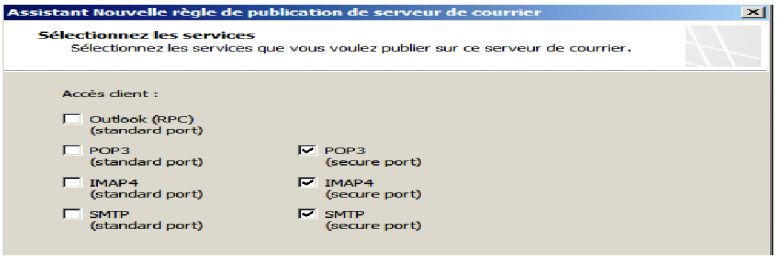

Figure V.70 : Sélection des services.

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

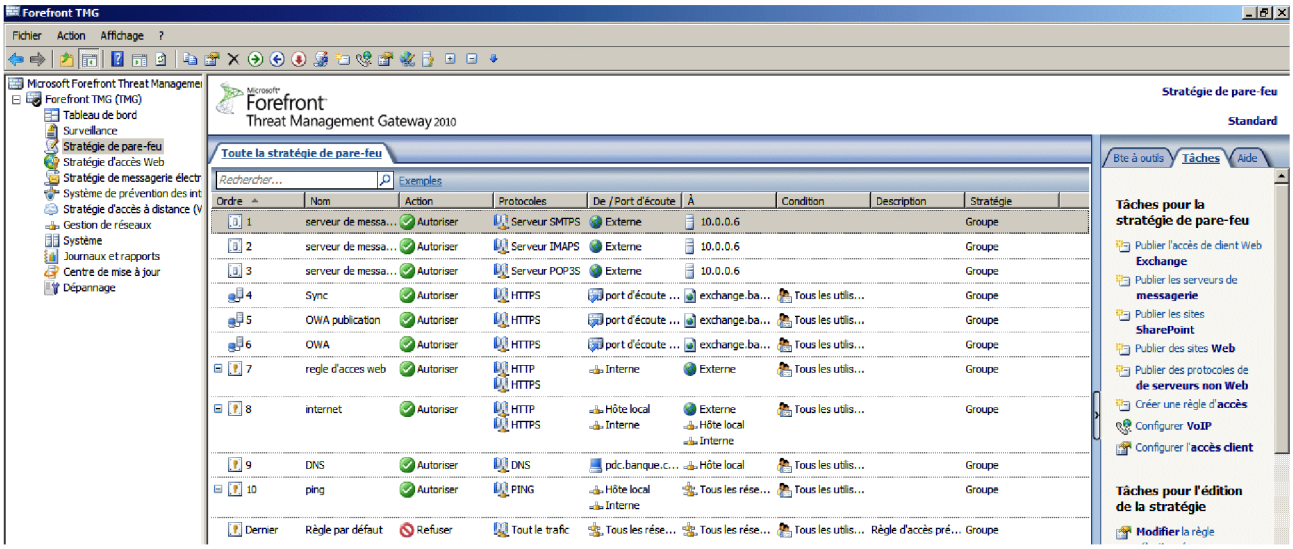

Figure V.71: récapitulatif des règles TMG.

7. 2. Configuration d'Exchange pour l'accès au site web de l'extérieur.

7.2.1. Configuration des connecteurs

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

7.2 .1. a. Connecteur d'envoi

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

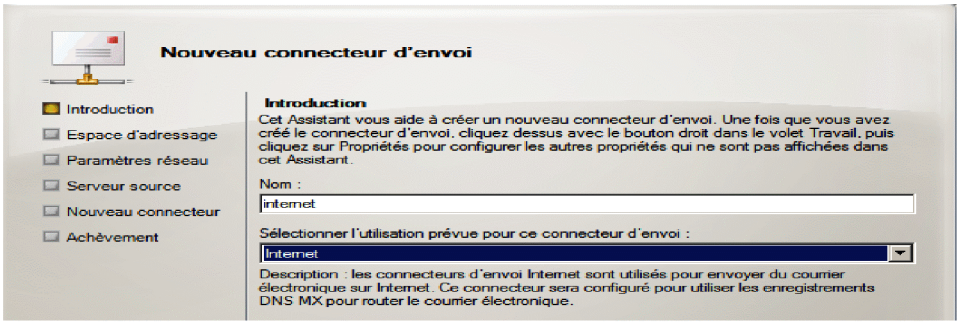

Figure V.72 : Création d'un nouveau connecteur d'envoi.

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

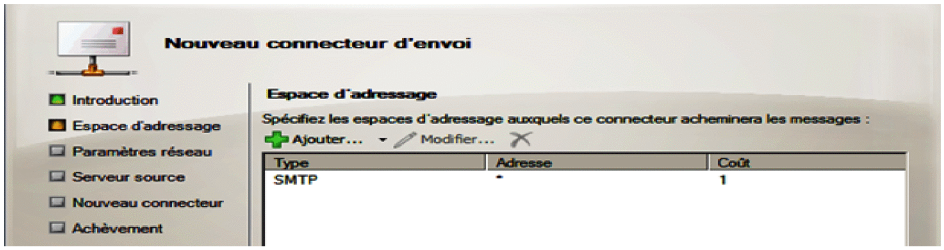

Figure V.73 : Espace d'adressage.

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

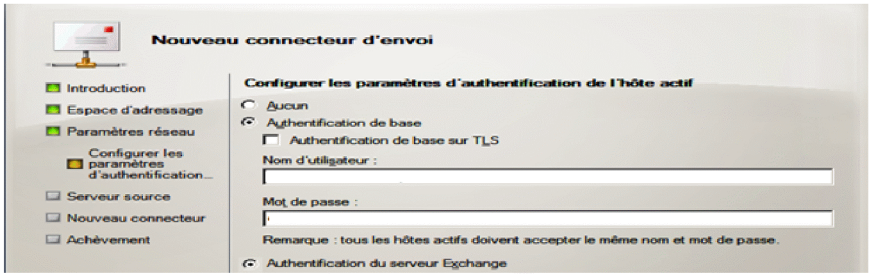

Figure V.74: Configuration des paramètres d'authentification.

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

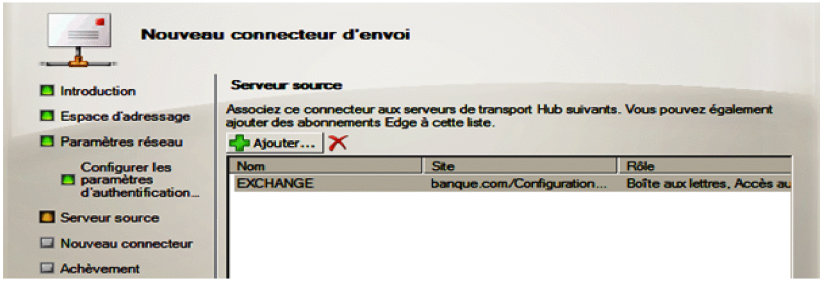

Figure V.75 : La spécification du serveur source.

7.2 .1. b. Connecteur de réception

Pour la création du connecteur de réception, nous cliquons sur Configuration du serveur -> Transport Hub -> nouveau connecteur de réception.

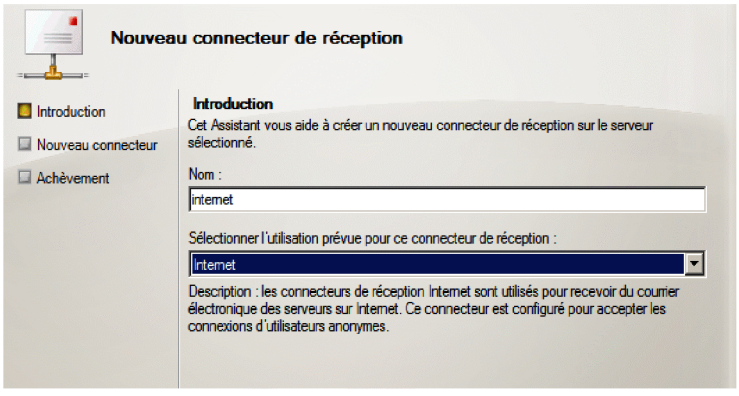

Figure V.76: Nouveau connecteur de réception.

7.3. Configuration d'Outlook Anywhere

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

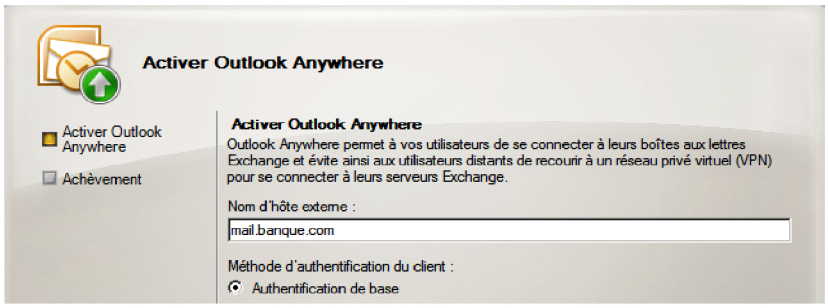

Figure V.77: Activation d'OWA.

8. Tester l'envoi et la réception de mails depuis un client interne et externe

Apres avoir fourni la clé privée à l'administrateur et installé la CA, nous testons si l'échange se fait correctement avec le chiffrement des PKI. Dans cet exemple, l'administrateur du réseau envoie par mail un document en pièces jointes à tous les employés de la banque en annonçant une réunion.

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

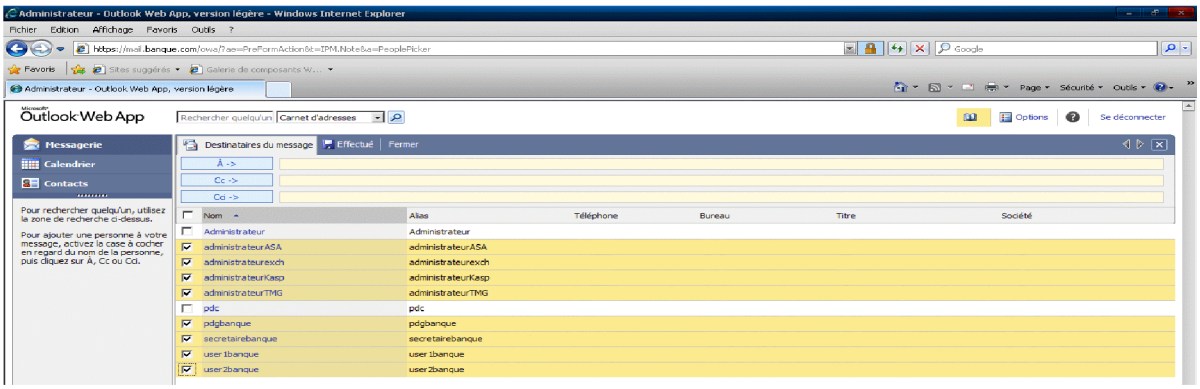

Figure V.78: La sélection des contacts de la banque.

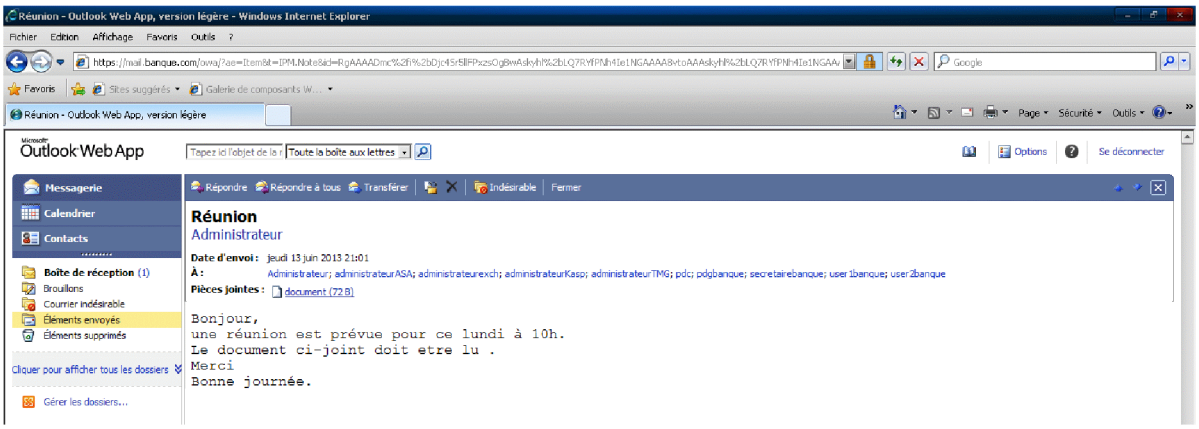

Figure V.79: Message envoyé.

La réception par l'administrateur de la TMG du mail.

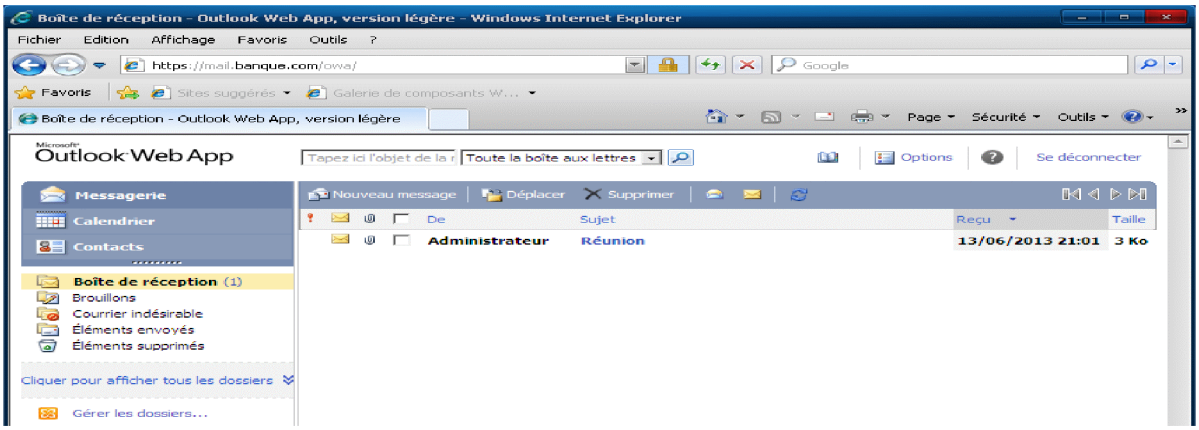

Figure V.80: Message reçu.

Etape V : Configuration du stockage serveur et des clusters de serveurs

1. Installation et configuration du stockage

Dans une banque comme dans toute entreprise, l'indisponibilité des données est un point critique nécessitant une solution bien réfléchie. Après avoir étudié les différentes méthodes de stockage, nous avons choisi d'utiliser la méthode iSCSI SAN (Storage area network). Son principe de fonctionnement, installation et utilisation sont détaillés dans l'annexes C.

1.1. Configuration de stockage

Pour assurer la disponibilité de la BDD à tout moment même en cas de panne d'un disque, nous avons choisi de configurer le volume tolérant aux pannes RAID 5 qui combine des zones libre d'au moins trois disques durs physiques en un seul volume logique. Il agrège les données par bandes avec des informations sur la parité (paire ou impaire) sur une baie de disques. Quand un disque est défaillant, Windows server 2008 se base sur ces informations de parité pour recréer les données du disque défaillant.

Pour créer un volume RAID 5, nous avons créé trois disques virtuels dans Starwind, disk1, disk2, disk3 (Annexe C). Pour accéder à ces disques nous avons configuré le iSCSI Initiateur, pour le faire allons dans outils d'administration choisissons iSCSI Initiateur.

Dans la fenêtre qui apparait, sélectionnons Découvert, ajoutons comme portail l'adresse du serveur de stockage **BDD.banque.com**.

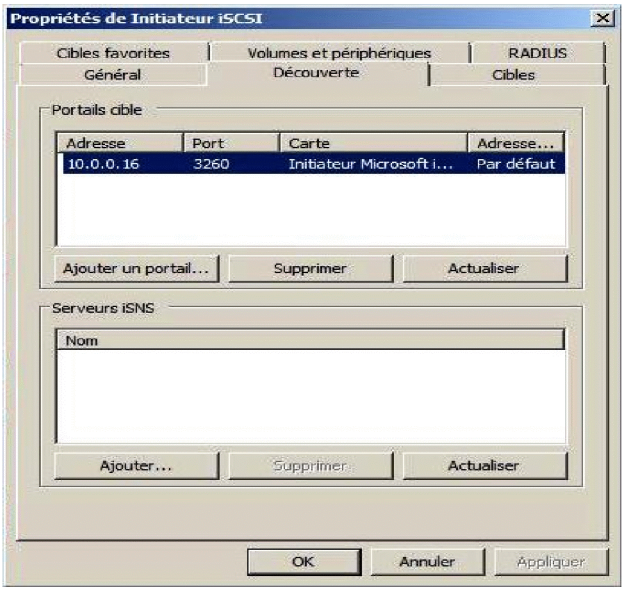

Figure V.81: L'ajout d'un portail.

Sur cibles nous trouvons l'ensemble des disques que nous avons créé inactifs, pour les activer cliquons sur ouvrir une session.

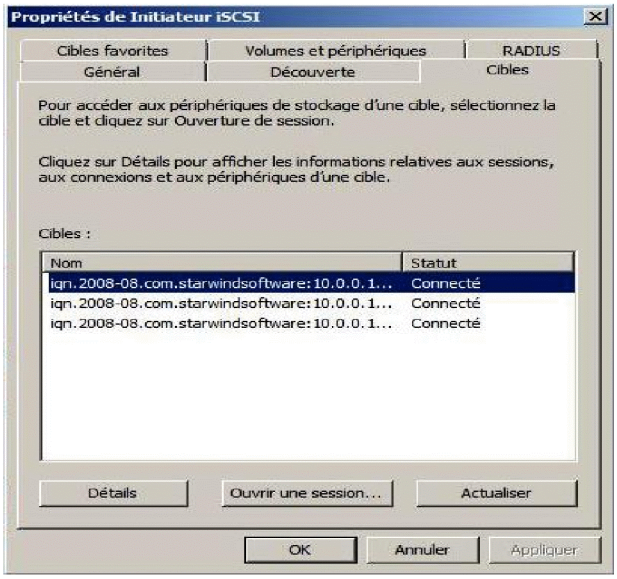

Figure V.82: Connexion des disques.

Après avoir configuré l'iSCSI Initiateur, cliquons sur Gestionnaire de serveur-> Gestion de Disque, où nous trouvons les disques créés. Pour construire un volume RAID5, il faut tout d'abord les convertir en disques dynamiques, sélectionnons les disques et convertissons les en disque dynamique.

Maintenant commençons le processus RAID 5, sur l'un des disques non alloués choisissons Nouveau volume RAID **5.**

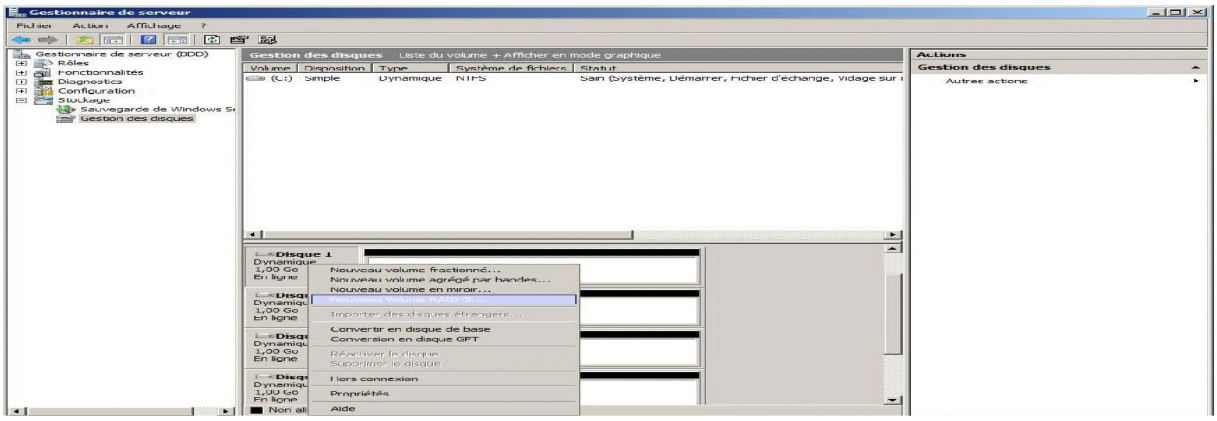

Figure V.83: Création de volume RAID 5.

Ensuite, l'assistant de création de volume de RAID5 démarre. Dans l'étape suivante ajoutons les disques qui vont être membre du volume RAID 5, les trois créé.

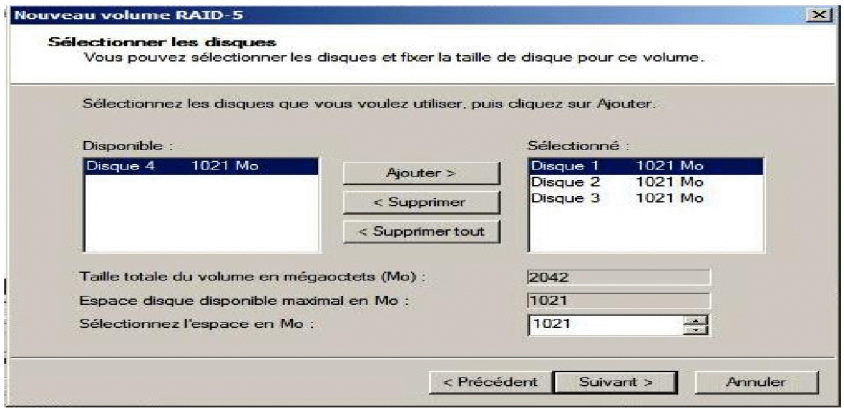

Figure V.84: Sélection des disques RAID **5**.

Après création du volume RAID **5**, nous pouvons le voir dans Gestion de disque avec une étiquette bleue.

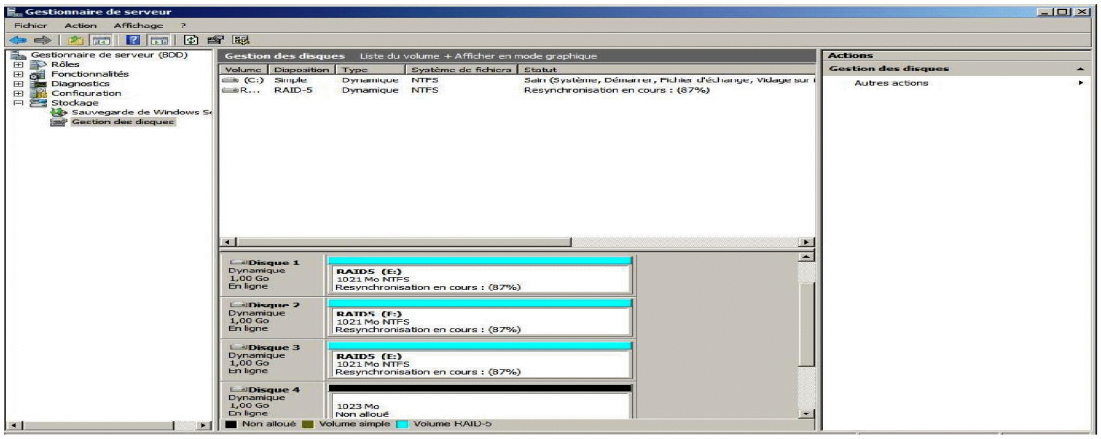

Figure V.85 : Le RAID 5.

2. Configuration des clusters de serveurs

Dans ce titre nous configurons les deux types de cluster, le cluster avec répartition de la charge réseau (NLB pour Network Load Balancing) qui est un groupe de serveurs utilisés pour

fournir un équilibrage de charge et augmenter l'extensibilité et le cluster de basculement qui permet d'accroitre la disponibilité d'une application ou d'un service dans le cas d'une défaillance du serveur.

2. 1. Cluster du basculement

2. 1.1.L'ajout de rôle de cluster du basculement

Afin d'implémenter cette solution, nous avons préparé deux nœuds (Windows Server 2008) membres du domaine **banque.com**, puis nous avons installé, sur les deux, la fonctionnalité cluster avec basculement via le gestionnaire de serveur.

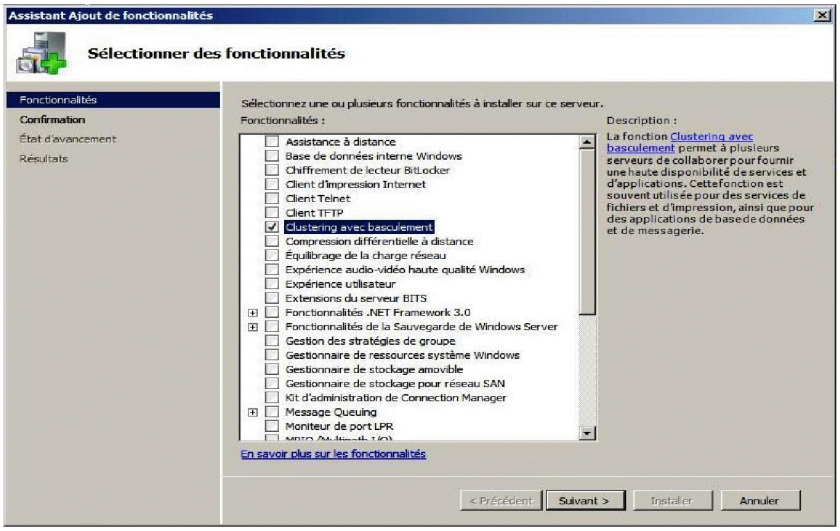

Figure V.86: L'ajout de Cluster avec basculement.

Après avoir configuré le stockage, nous connectons ces deux nœuds au stockage grâce à l'iSCSI. Une fois cela fait nous validons la configuration matérielle et logicielle. Nous lançons alors la page gestion de cluster de basculement.

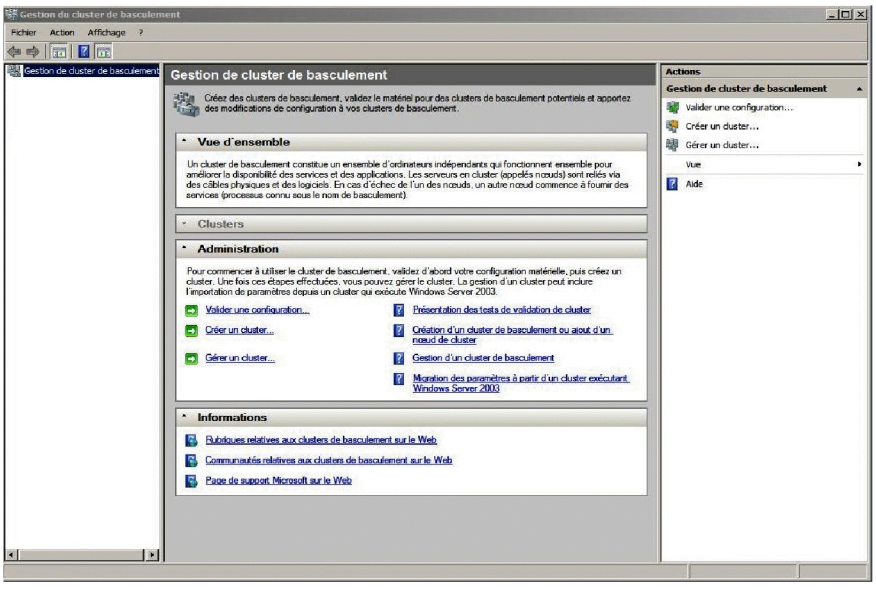

Figure V.87: Gestion de cluster de basculement.

2. 1.2. Validation de la configuration du cluster

Avant de créer un nouveau cluster, nous validons la configuration via la gestion de cluster en cliquant sur valider une configuration afin d'assurer que les nœuds respectent les pré-requis matériels et logiciels d'un cluster de basculement. Une fois la configuration validée, nous pouvons créer le cluster.

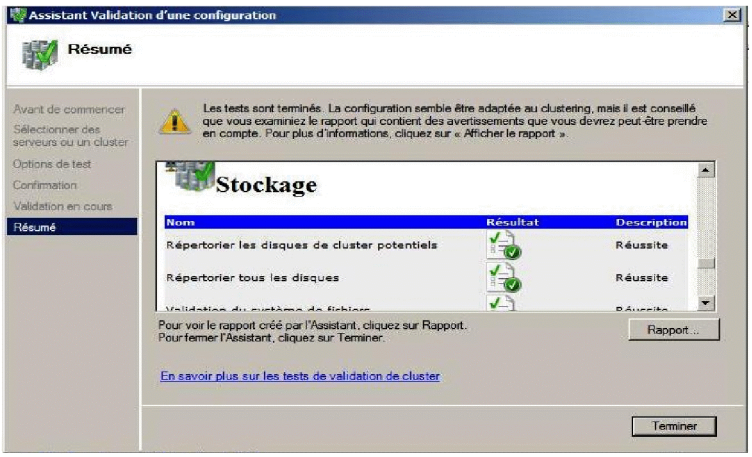

Figure V.88: Validation de la configuration.

2. 1.3. Exécution de l'assistant de création d'un cluster

Cette étape consiste à créer le cluster en exécutant l'assistant de création de cluster, ce dernier installe les bases logicielles du cluster, convertit le stockage associé en disques de cluster et créé un compte d'ordinateur Active Directory pour le cluster. En ouvrant l'assistant, nous saisissons les noms des nœuds du cluster, le nom du cluster (failover) et son adresse IP.

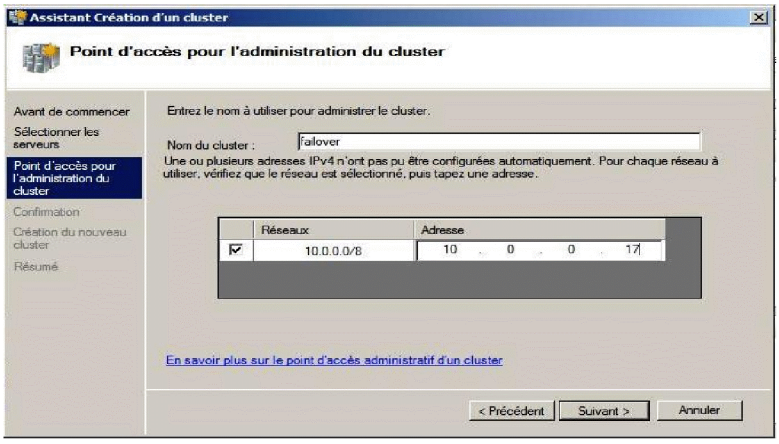

Figure V.89: L'attribution des paramètres de cluster.

La fenêtre suivante nous montre le paramétrage du cluster failover, nous pouvons continuer pour valider ou retourner en arrière pour effectuer des modifications.

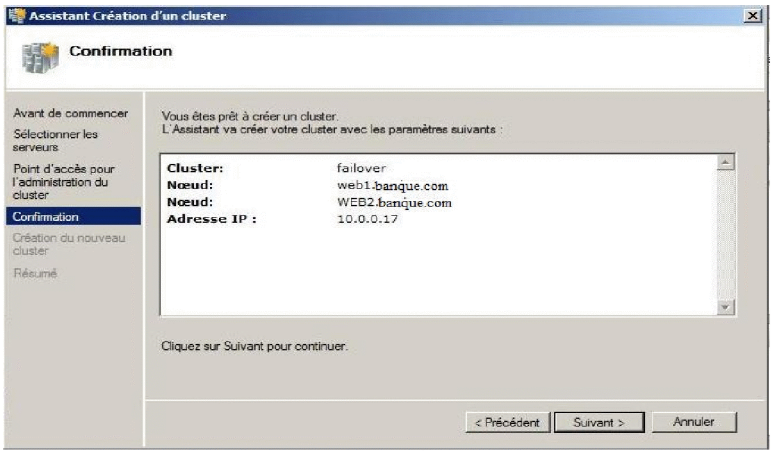

Figure V. 90: Confirmation de création de cluster.

A la fin de l'assistant, nous configurons les services ou applications pour lesquels nous proposons le basculement. Pour effectuer cette configuration, nous exécutons l'assistant Haute disponibilité.

2. 1.4. Exécution de l'assistant Haute disponibilité

Cet assistant configure le service de basculement pour un service ou une application donné. Nous le lançons en cliquant sur configurer un service ou une application dans la zone Configuration.

Dans notre cas, nous avons choisi le service Distributed Transaction Coordinator (MSDTC) qui est un composant des versions récentes de Microsoft Windows permet de coordonner des opérations qui s'étendent sur plusieurs gestionnaires de ressources, tels que les bases de données, les files d'attentes de messages et les systèmes de fichiers.

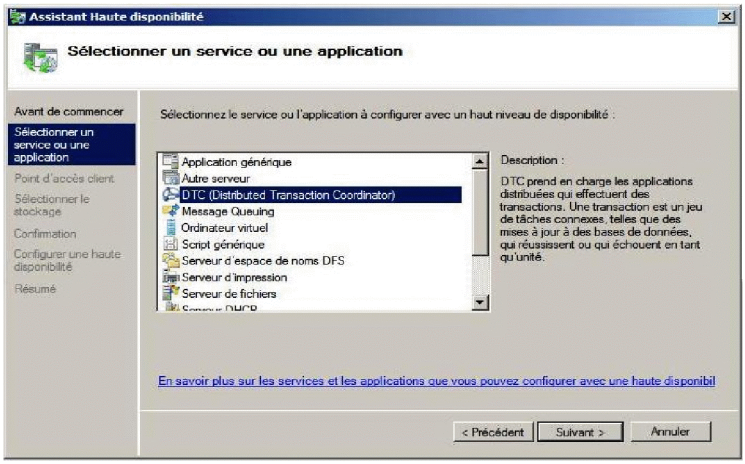

Figure V.91 : Sélection de service DTC.

Dans l'assistant suivant nous saisissons le nom et l'adresse du service pour que les clients puissent y accéder.

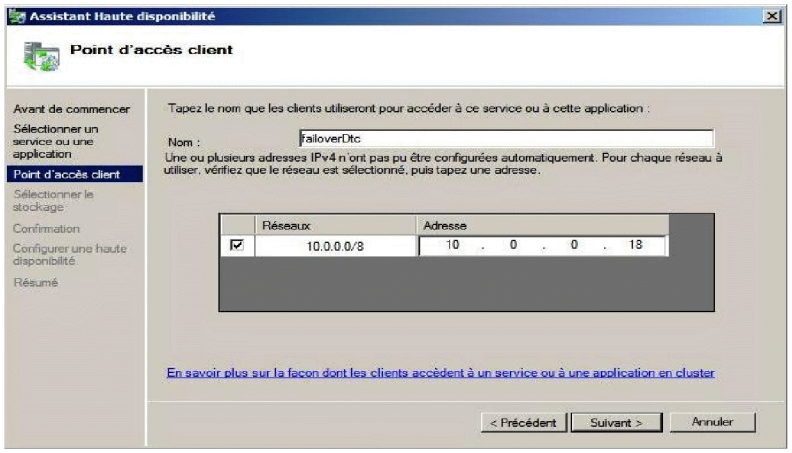

Figure V.92: Paramétrage de point d'accès client.

2. 1.5. Tester le cluster de basculement

Après avoir complété l'assistant, nous testons le failover dans l'outil de gestion du cluster de basculement. Dans l'arborescence de la console, sélectionnons le service que nous venons de créer DTC, cliquons avec le bouton droit sur le service en cluster, déplacer ce service vers un autre nœud et cliquons sur l'autre nœud .Nous observons les changements d'états dans le volet central du composant logiciel enfichable pendant le déplacement du service en cluster.

2. 2 .Cluster avec répartition de charge

2. 1.1. Création d'un cluster NLB

Afin de pouvoir créer un NLB, nous avons préparé deux nœuds machines Windows Server 2008 membres du domaine (server1 et server2) et configuré le service IIS à fournir aux clients en assurant une configuration identique pour les deux nœuds.

La prochaine étape consiste à installer la fonctionnalité de répartition de charge réseau sur tous les serveurs à joindre au cluster NLB. Pour ce faire nous ouvrons le gestionnaire de serveur, ajoutons des fonctionnalités et choisissons la fonctionnalité d'équilibrage de la charge réseau.

Après avoir installé la fonctionnalité, dans le premier nœud, lançons le Gestionnaire d'équilibrage de la charge réseau depuis Outils d'administration, dans l'arborescence, choisissons nouveau cluster, dans l'hôte, tapons le nom de la machine qui doit faire partie du nouveau cluster et cliquons sur connexion.

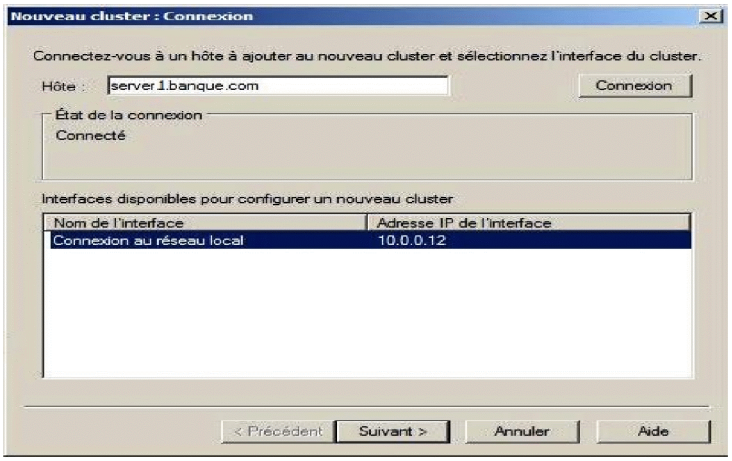

Figure V.93 : Nouveau cluster.

En suite, saisissons le nom et l'adresse IP virtuelle employés par le cluster pour répartir la charge.

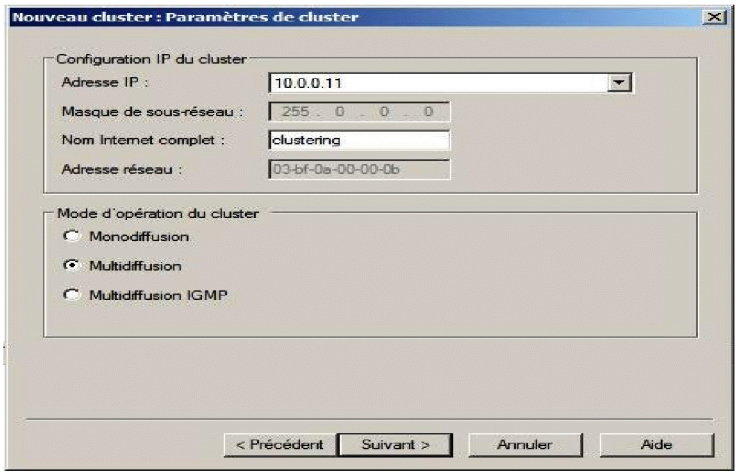

Figure V.94: Paramétrage de cluster.

Sur la fenêtre des paramètres de l'hôte, sélectionnons une valeur de priorité dans la liste déroulante. Ce paramètre spécifie un ID unique pour chaque hôte. L'hôte ayant la priorité la plus haute parmi les membres actuels du cluster pourra gérer tout le trafic réseau du cluster.

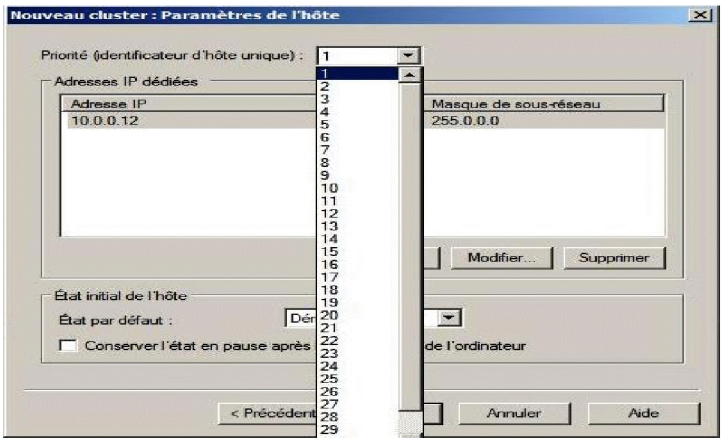

Figure V.95: Le paramétrage de l'hôte.

Sur la page adresse IP du cluster, cliquons sur ajouter pour saisir l'adresse IP du cluster partagé par chaque hôte du cluster. Pour ajouter le deuxième nœud accédons au server2, puis lançons le gestionnaire d'équilibrage de la charge réseau et sélectionnons connecter à un cluster existant après avoir cliqué sur Cluster.

Après ajout des nœuds de cluster NLB, nous les trouvons listés dans le gestionnaire d'équilibrage de la charge réseau.

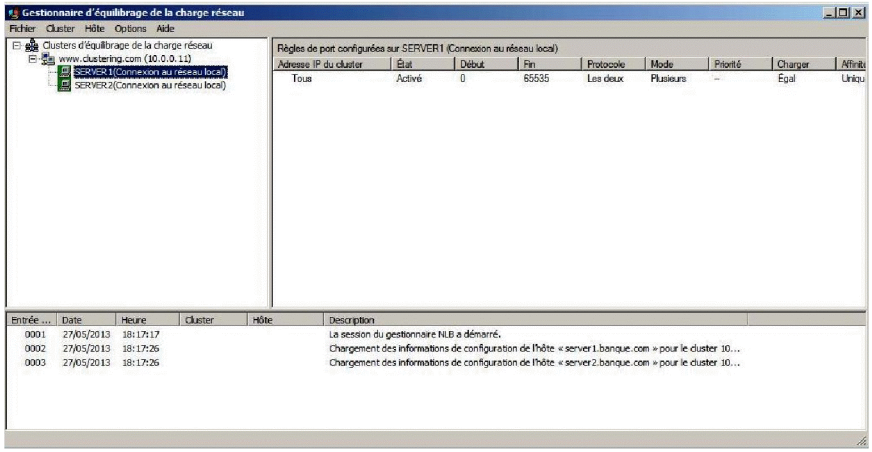

Figure V.96: Gestionnaire d'équilibrage de la charge réseau.

2. 1.2. Tester le NLB

Afin de tester le NLB, nous avons créé un site dans server1 que nous avons nommé **site_banque** et l'avons exporté vers server2.

Pour exporter **site_banque**, nous accédons à configuration du partage, sélectionnons le site puis cliquons sur exporter la configuration, dans l'assistant d'exportation de la configuration, nous précisons le chemin physique de la configuration, les informations d'identification en cliquons sur **Se connecter en**, saisissons la clé de chiffrement. Et pour finir validons**.**

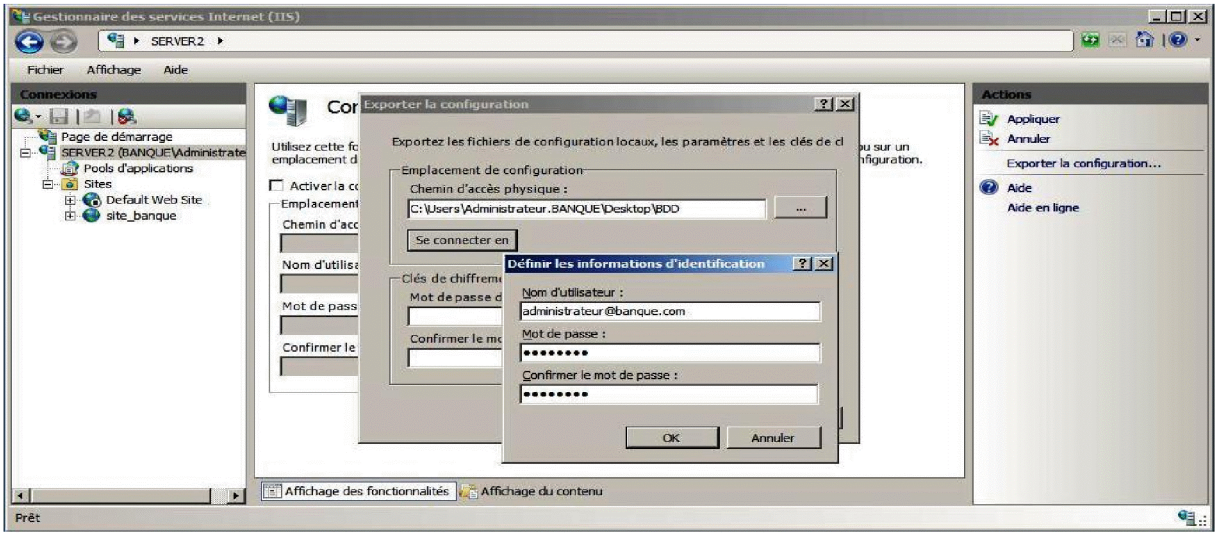

Figure V.97: Exportation de la configuration du site_banque.

L'étape suivante consiste à partager le fichier de configuration et l'importer de l'autre nœud (server2), puis accéder au server IIS, configuration de partage, cocher activer la configuration partagé et saisissons les informations demandées et la clé de chiffrement donné lors de l'exportation de la configuration du site_banque.

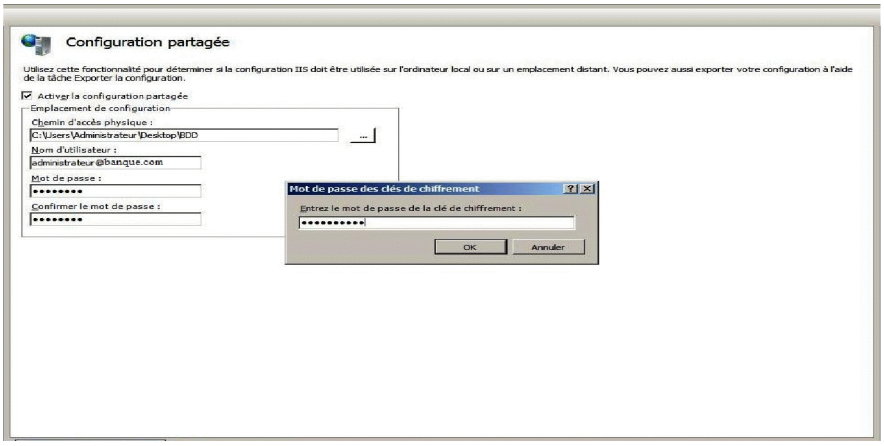

Figure V.98 : Activation de la configuration partagée.

Après avoir exporté le site, on ping avec l'adresse et le nom du cluster depuis le PDC, comme nous voyons c'est réussi.

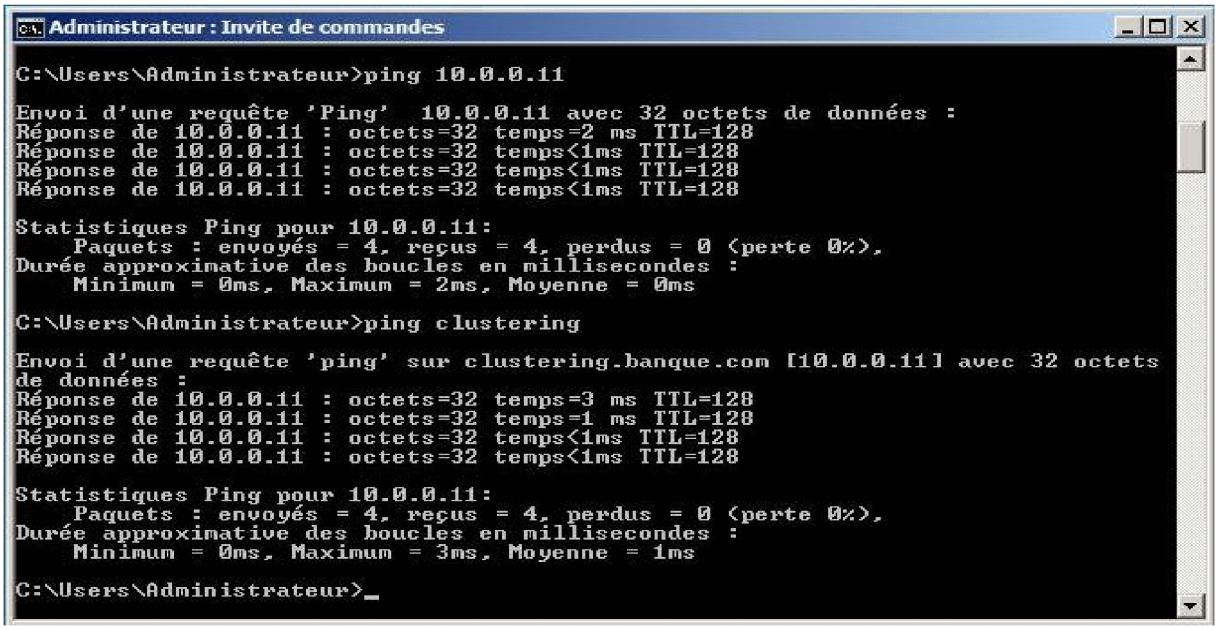

Figure V.99: Le ping avec l'adresse et le nom de cluster NLB.

La deuxième étape de test consiste à naviguer avec le nom de cluster NLB via un navigateur.

Figure V.100 : Accès au site via internet explorer.

Les deux tests réussis, nous les referons en éteignant les nœuds NLB en alternance.

Etape VI : La création de la stratégie de groupe

Une stratégie de groupe offre une infrastructure qui permet de définir de manière centralisée des paramètres de configuration et déploiement utilisateur et ordinateur dans une entreprise. Dans un environnement géré par une infrastructure de stratégie de groupe, les administrateurs n'auront pas beaucoup à intervenir car toute configuration est définie, appliquée et actualisée à l'aide des paramètres situés dans des objets de stratégie de groupe(GPO, Group Policy Object) qui affectent une portion de l'entreprise pouvant atteindre un site ou un domaine entier comme une unité d'organisation ou un groupe individuel.

1. Création d'une stratégie de groupe

Dans le PDC, nous accédons à la console Gestion de stratégie de groupe depuis outils d'administration. Pour créer un nouveau GPO, nous cliquons avec le bouton droit sur Objet de Stratégie de groupe-> nouveau.

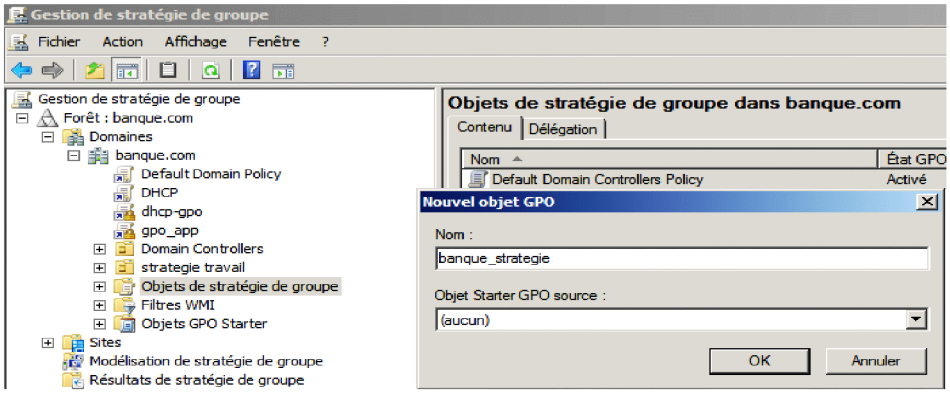

Figure V.101 : Création d'un GPO.

Dans la fenêtre qui s'ouvre saisissons le nom et l'objet de GPO.L'objet étant créé il sera affiché dans la liste des objets de stratégie de groupe dans banque.com, cliquons sur modifier.

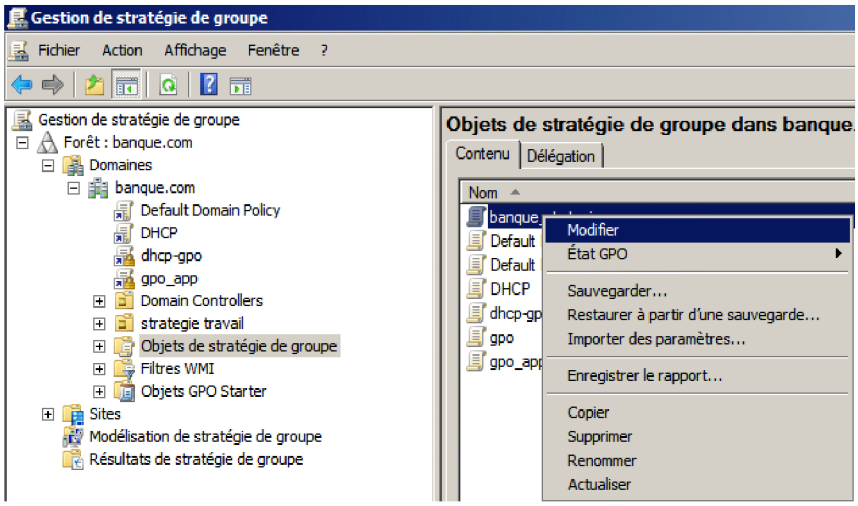

Figure V.102: Modification de GPO créé.

L'éditeur de gestion de stratégie de groupe présente des milliers de paramètres de stratégies disponibles dans un GPO au sein d'une hiérarchie structurée qui commence par une division entre les paramètres de l'ordinateur et ceux de l'utilisateur.

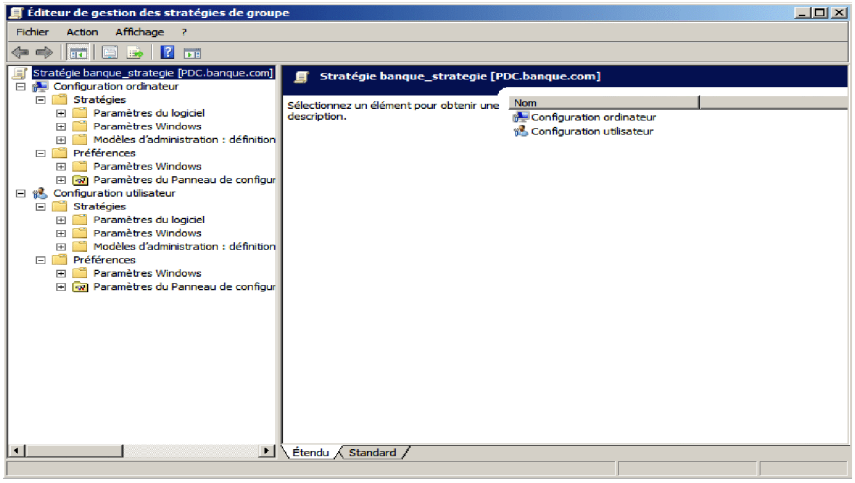

Figure V.103: Editeur de gestion de stratégie de groupe.

En se basant sur les différents paramètres de cette hiérarchie, nous allons modifier notre GPO en appliquant les paramètres suivants :

- ✓ Désactiver les ports physiques : USB, CD/DVD, Lecteur carte mémoire.
- ✓ Verrouiller des stations en dehors des horaires de travail en tenant compte de chaque utilisateur.
- ✓ Surveiller les activités des administrateurs avec l'observateur d'événement (la durée du journal de sécurité, des applications et système est de15 jours).
- ✓ Interdire la configuration avancée de TCP/IP.
- ✓ Forcer une politique de mot de passe pour les différentes stations de la banque.
- ✓ Verrouiller les comptes et définir le seuil de verrouillage des comptes (5mn).

A la fin de la modification, nous déléguons cette stratégie aux utilisateurs ou ordinateurs voulus, validons et pour finir sauvegardons.

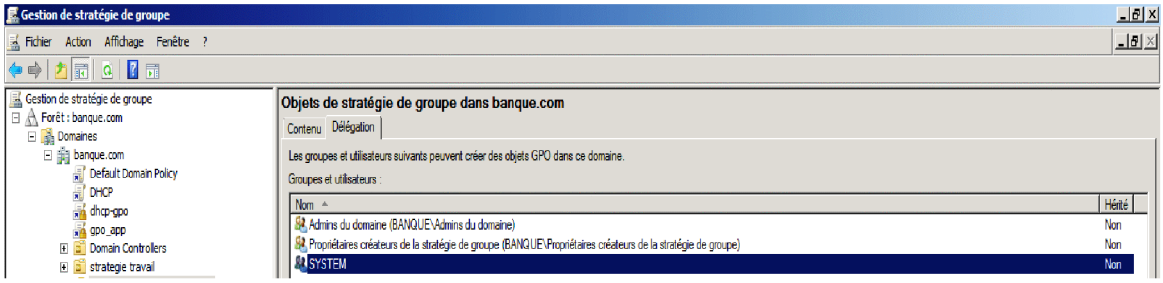

Figure V.104: Délégation de la stratégie de groupe.

Ayant configuré les paramètres il ne reste plus qu'à appliquer la stratégie sur tous les clients, avec la commande **gpupdate /force**.

Etape VII : L'implantation de la solution NAP DHCP

1.L'ajout de rôles serveur DHCP

Ayant affecté au PDC une adresse IP statique compatible avec la plage d'adresse prévue pour le sous-réseau local (10.0.0.0/8), lançons l'assistant Ajout de rôles depuis le Gestionnaire de serveur.

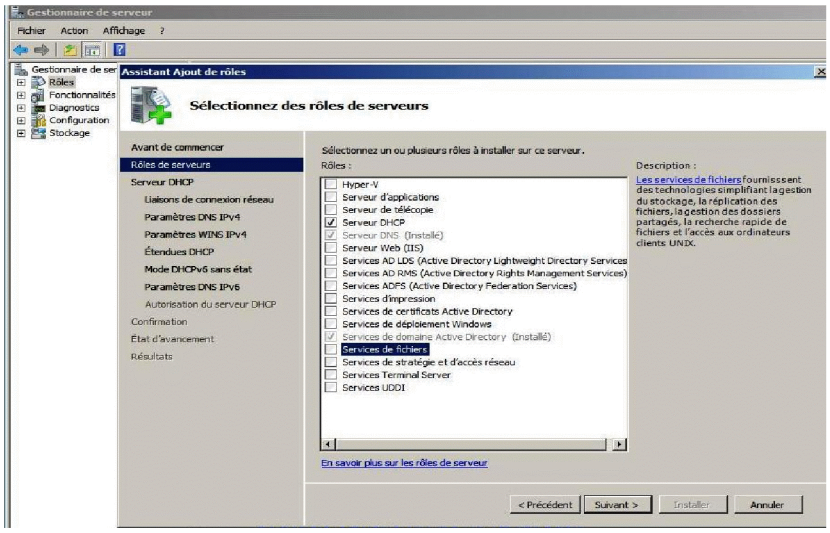

Figure V.105 : Ajout du rôle DHCP.

Sélectionnons l'adresse IP affectée manuellement, et qui sera le sous-réseau logique des adresses qui seront affectées aux clients.

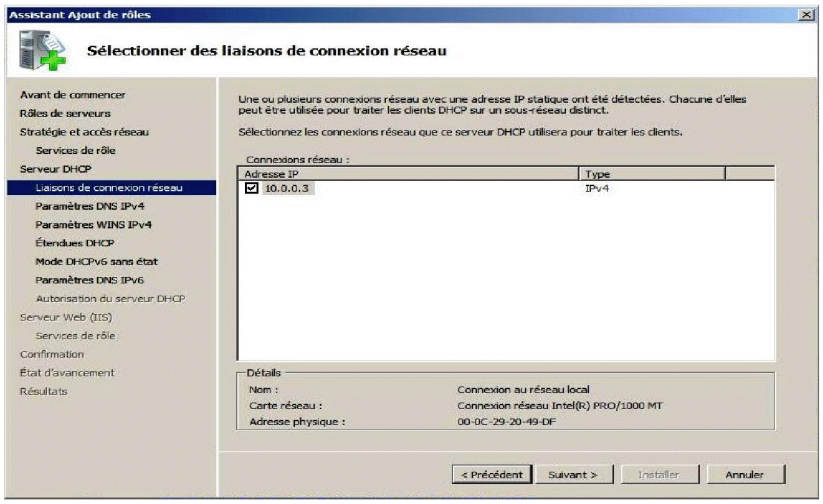

Figure V.106: Sélection des liaisons de connexion réseau.

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

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

- ✓ L'option DNS Servers Permet de configurer la liste d'adresses de serveurs DNS pour les connexions clients. Dans notre cas nous avons un seul serveur DNS qui appartient à notre domaine et dont l'adresse est **10.0.0.3**.

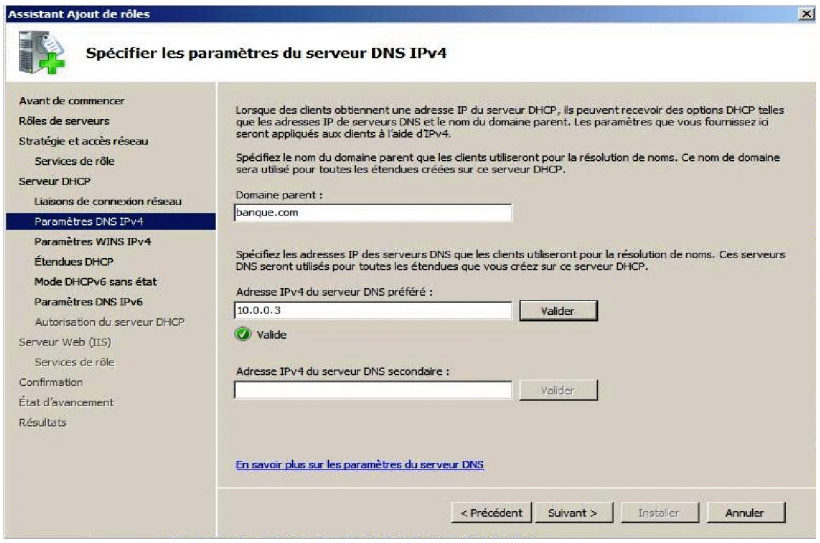

Figure V.107: Spécification des paramètres du serveur DNS IPv4.

La spécification des paramètres du serveur WINS IPv4 permet de configurer l'option WINS, grâce à la quelle nous pouvons affecter une liste de serveurs WINS aux clients. Dans notre cas n'ayant pas de serveur WINS, cette option n'a pas été validée.

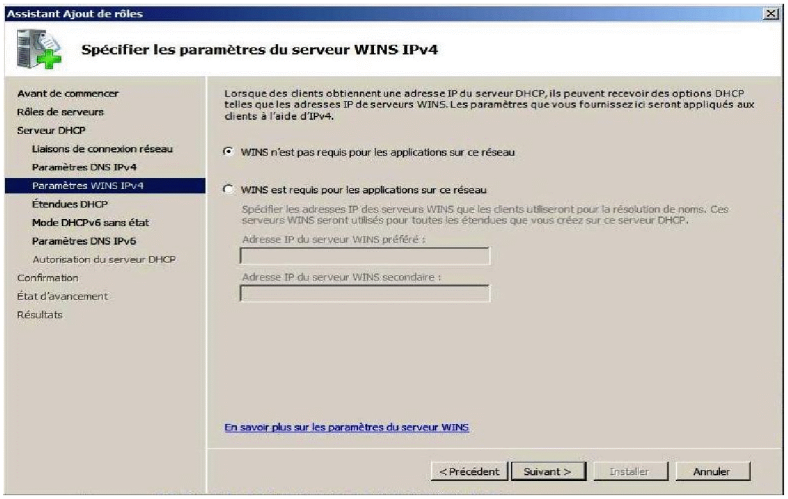

Figure V.108: Spécification des paramètres du serveur WINS IPv4.

L'ajout d'étendues DHCP permet de définir ou de modifier les étendues sur le serveur DHCP. Notre étendue d'adresses IP pour les ordinateurs du sous-réseau DHCP est 10.0.0.30-254/8.

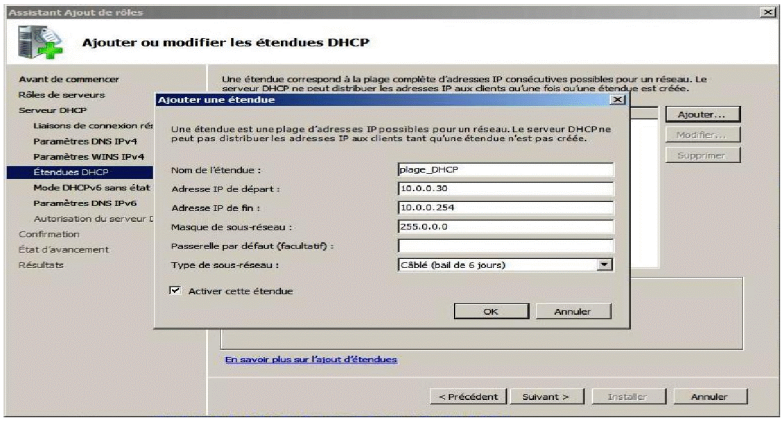

Figure V.109 : Ajouter les étendues DHCP.

N'utilisant que le mode DHCP IPv4, nous désactivons le mode IPv6.

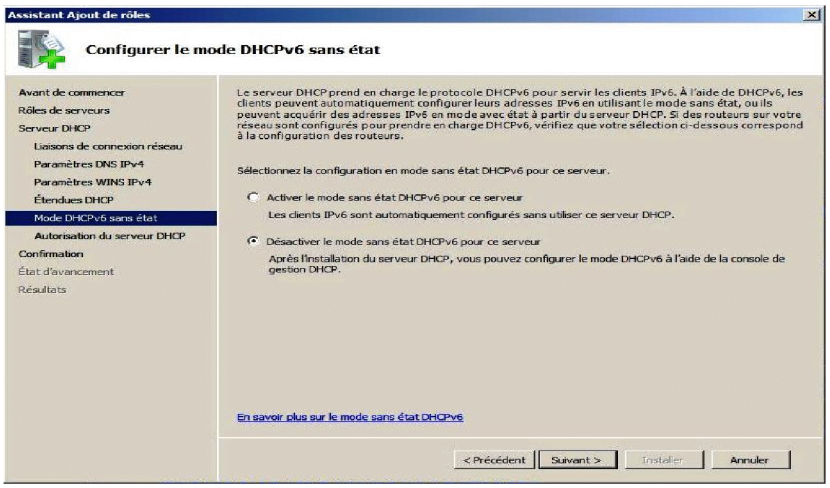

Figure V.110: Configurer le mode DHCPv6 sans état.

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

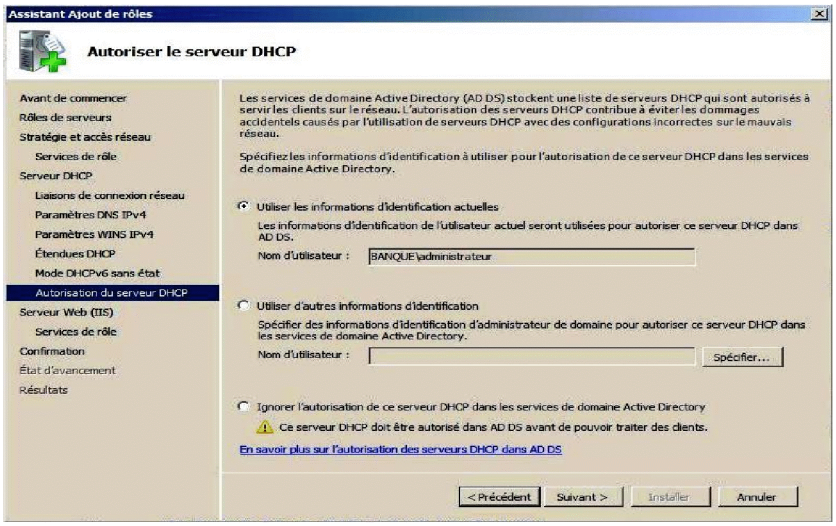

Figure V.111 : Autoriser le serveur DHCP.

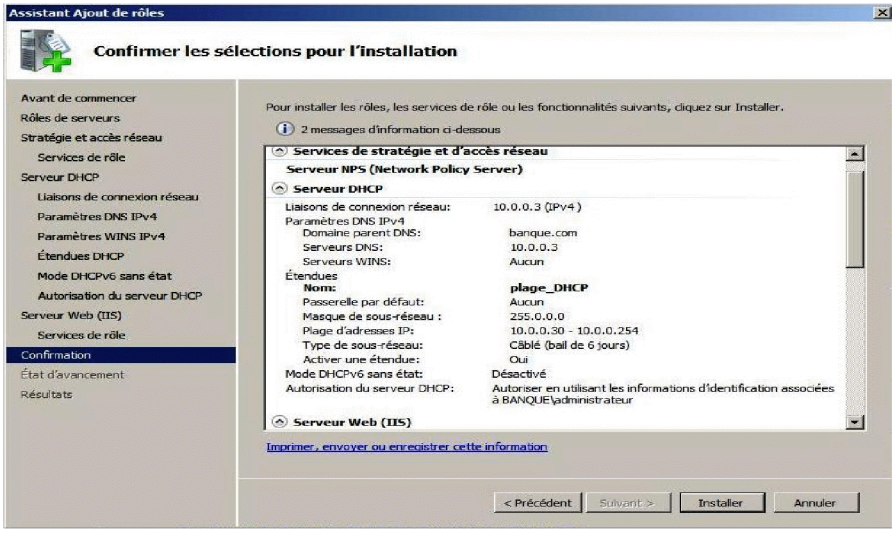

Figure V.112: Récapitulatif de l'installation.

Le NAP dépend du serveur NPS (Network Policy Server) qui agit comme serveur Radius pour évaluer l'intégrité des ordinateurs clients. Les étapes d'installation du NAP suivies sont :

- ✓ L'ajout du rôle services de stratégies et d'accès réseau via Gestionnaire.
- ✓ Lancement et l'installation du rôle NPS.

Le service NPS suffit à l'emploi d'un ordinateur Windows Serveur 2008 comme serveur RADIUS pour la mise en œuvre du DHCP.

2. Configuration de la protection d'accès réseau

Ayant installé le rôle service d'accès stratégies et d'accès réseau, passons à l'étape suivante qui est la configuration du NAP :

- ✓ Ouvrir le gestionnaire de serveur -> Protection d'accès réseau -> Configurer la protection d'accès réseau (NAP)
- ✓ Sur la page sélectionner la méthode de connexion réseau à utiliser avec NAP. (Nous avons sélectionné DHCP).
- ✓ Définir la stratégie de contrôle d'intégrité NAP, qui est l'étape la plus importante. Elle permet de refuser l'accès aux clients qui ne sont pas conformes aux règles de sécurité qui sont :
    - Un logiciel de pare-feu installé.
    - Un antivirus installé et exécuté.
    - Les mises à jour de l'antivirus à jour.
    - Les mises à jour Microsoft à jour.

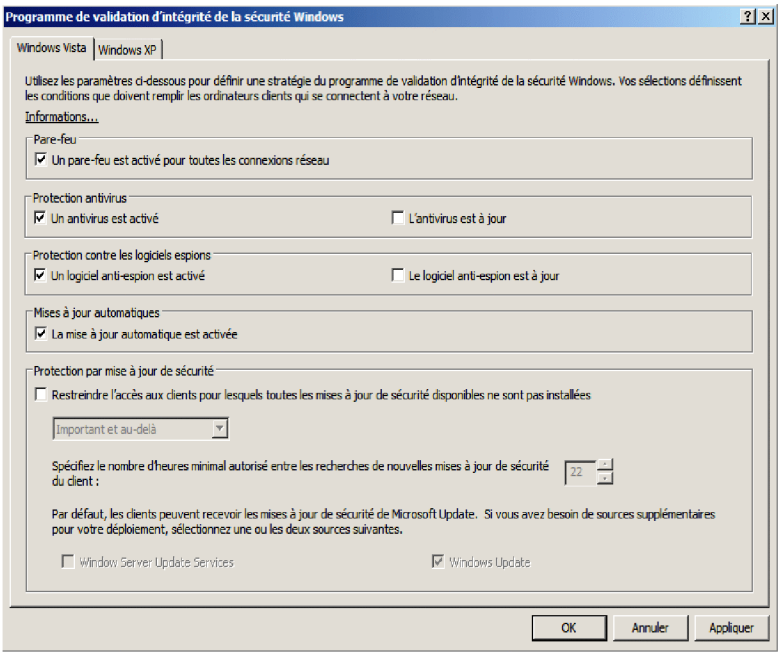

Figure V.113: Programme de validation d''integrité de la sécurité Windows.

3. La création d'une stratégie de groupe Nap DHCP

Pour appliquer la stratégie d'intégrité sur tous les clients, nous créons une stratégie de groupe pour ces derniers, en configurant les paramètres que voici :

Activation sur tous les serveurs et machines client de contrainte de quarantaine DHCP.

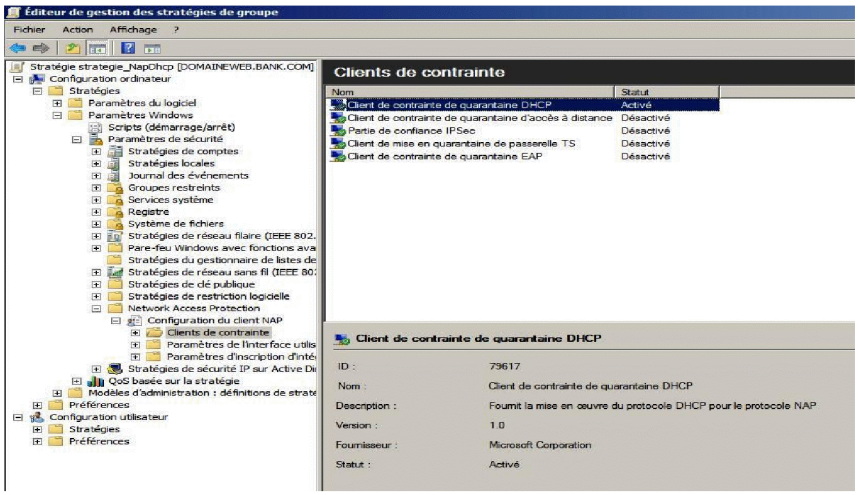

Figure V.114: Activation client de contrainte de quarantaine DHCP

Activation automatique du service système, agent de protection accès réseau.

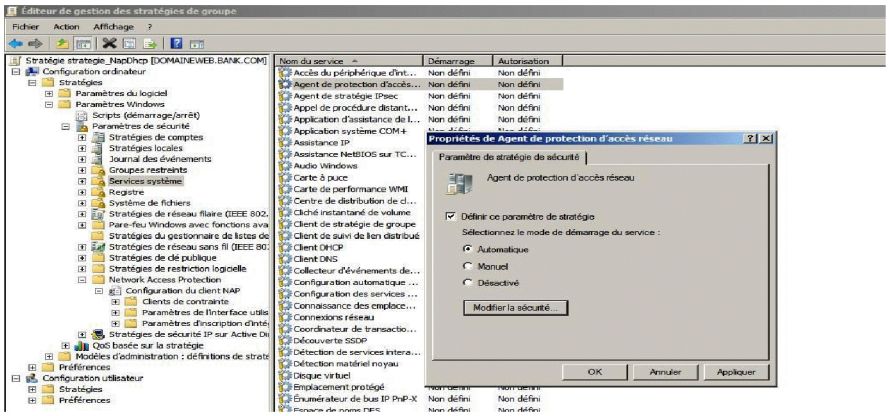

Figure V.115 : Agent de protection accès réseau.

Activation du centre de sécurité de l'ordinateur à un domaine.

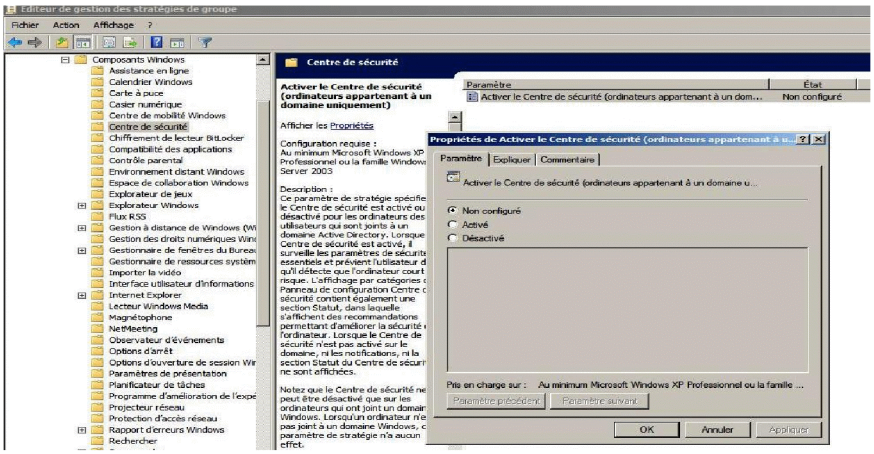

Figure V.116: Centre de sécurité de l'ordinateur à un domaine

Ayant configuré les paramètres il ne reste plus qu'à appliquer la stratégie sur tous les clients, avec la commande **gpupdate /force**. Apres cela tout ordinateur non conforme aux règles définies plus haut ne se verra pas attribuer une adresse IP.

4. Tester le NAP DHCP

Afin de tester notre serveur NAP DHCP, nous effectuons deux tests. Le premier, un client va essayer d'avoir une adresse IP via DHCP en gardant le pare-feu allumé, le deuxième en éteignant le pare-feu.

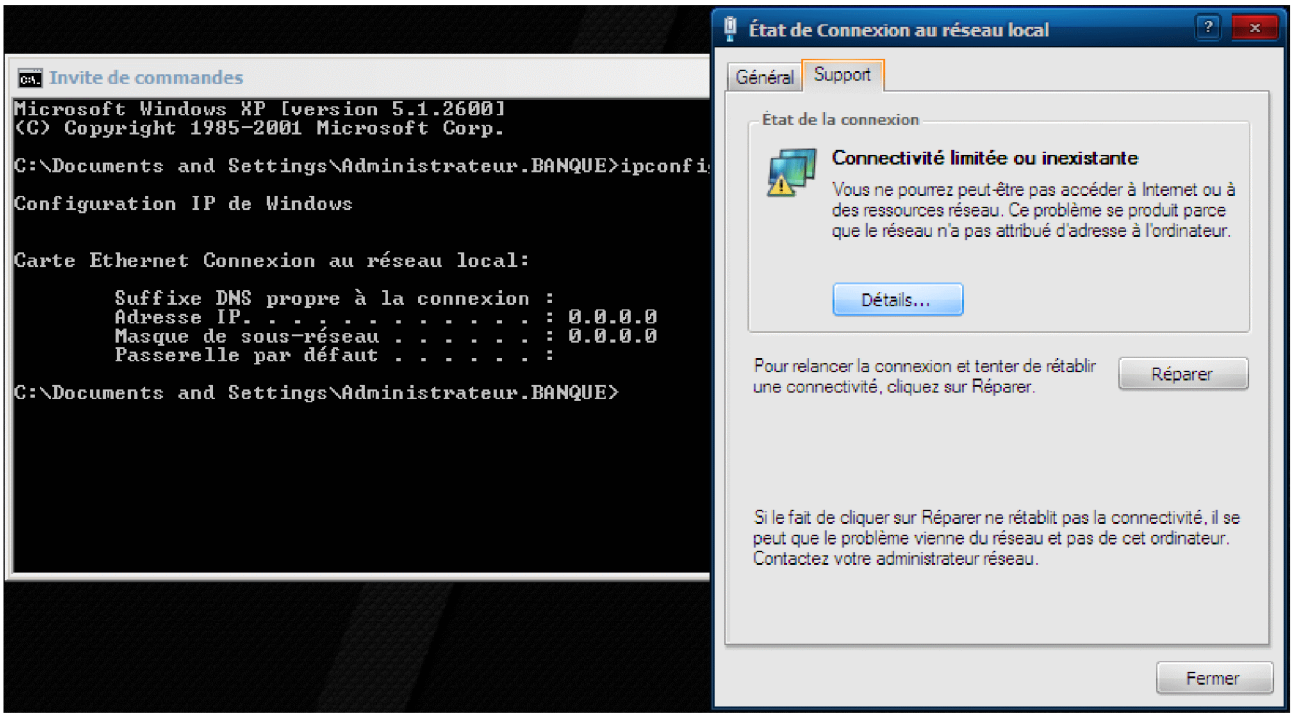

Figure V.117 : Quand le pare-feu est éteint.

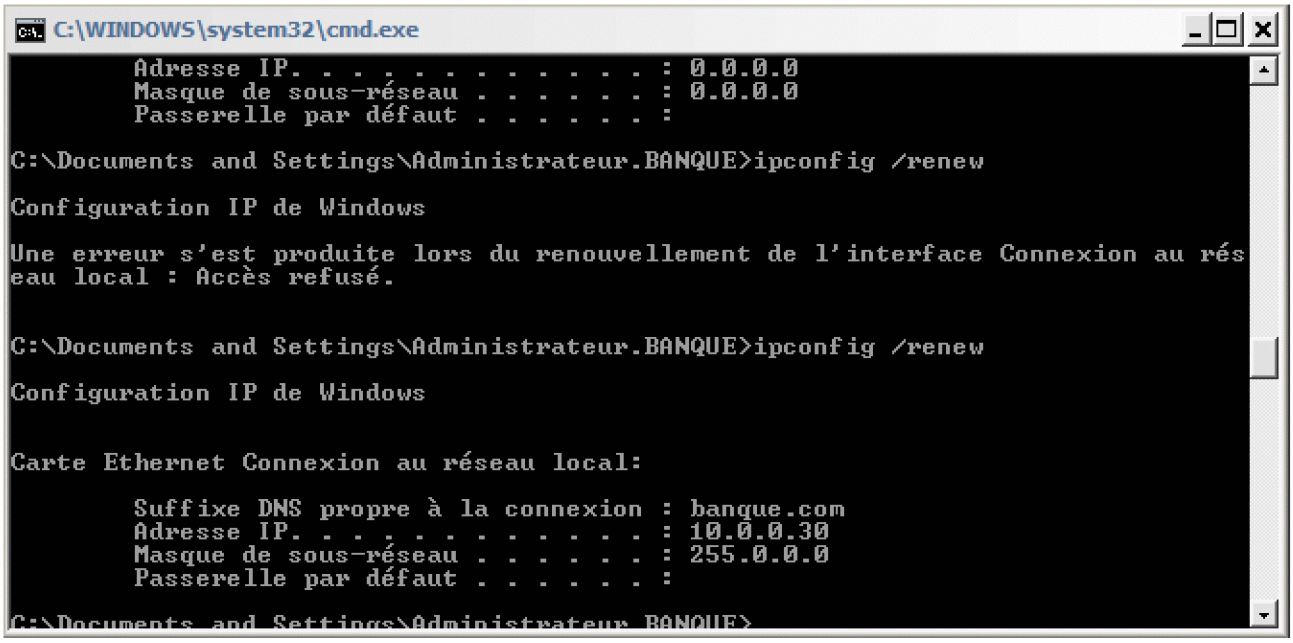

Figure V.118: Quand le pare-feu est allumé.

Nous remarquons que le client n'a pas réussi à avoir une adresse IP quant le pare-feu est éteint car il ne vérifie pas les conditions imposées par le serveur NAP, tandis que lorsque le pare-feu est allumé il a eu l'adresse en tenant compte de la plage DHCP spécifiée.

Etape VIII : Installation et déploiement de Kaspersky Administration Kit 8

Nous installons Kaspersky administration kit 8 sur le contrôleur de domaine principal PDC (l'annexe C) et nous le déployons sur l'ensemble de la forêt **banque.com.**

1. Déploiement de Kaspersky Administration Kit

Il existe plusieurs options de déploiement et de protection antivirus administrés par Kaspersky sur les ordinateurs du système réseau qui sont :

- ✓ **Installation à distance centralisée des applications sur les postes clients** : dans ce cas, l'installation des applications et la connexion au système d'administration à distance centralisé s'opère automatiquement, ne demande aucune intervention de l'administrateur et permet d'installer le logiciel antivirus sur n'import quel nombre de postes clients.
- ✓ **Installation locale des applications sur chaque poste client :** dans ce cas, l'installation des composants requis sur les postes clients et sur le poste administrateur s'opère manuellement. Les paramètres de connexion des clients au serveur seront définis lors de l'installation de l'Agent d'administration. Cette option de déploiement est utilisée dans le cas où il n'est pas possible d'exécuter une installation à distance centralisée.

Afin de faciliter le déploiement de l'anti-virus sur l'ensemble de la forêt, nous avons choisi le déploiement grâce à l'installation à distance. Nous soulignons que nous avons installé l'antivirus après l'installation du contrôleur de domaine pour profiter des avantages d'installation de kaspersky dans un domaine.

Au lancement de Kaspersky un assistant de configuration initial, nous demande de spécifier les paramètres des notifications par courrier, alors nous saisissons les informations requises.

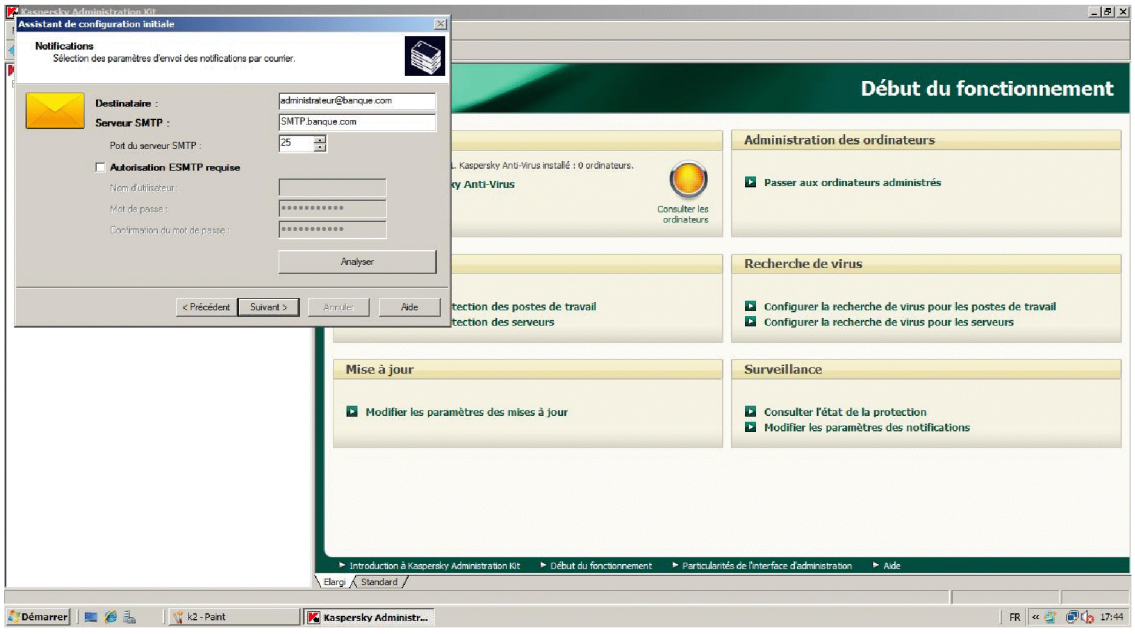

Figure V.119: Spécification des paramètres des notifications par courrier.

L'étape suivante nous donne le choix de saisir la clé maintenant ou plus tard, et lancer ou pas le processus de déploiement. Après avoir confirmé le processus de déploiement, l'assistant d'installation à distance s'ouvre.

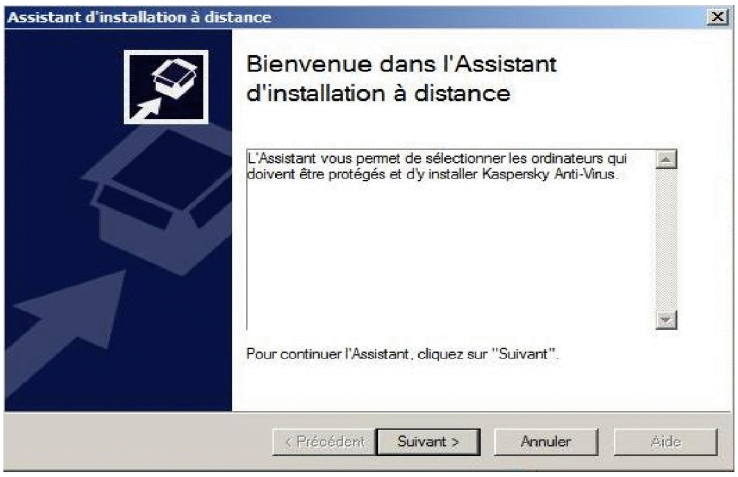

Figure V.120 : Assistant d'installation à distance.

Sélectionnons le paquet d'installation parmi la liste donnée, ou créons un autre, puis déployons l'agent d'administration (voir annexe C).

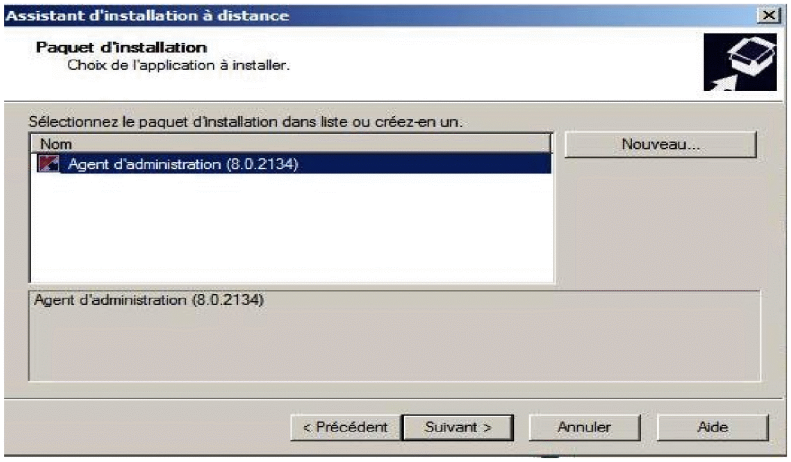

Figure V.121: La sélection de paquet d'installation.

Maintenant, sélectionnons l'ensemble de la forêt **banque.com** pour le déploiement de l'antivirus.

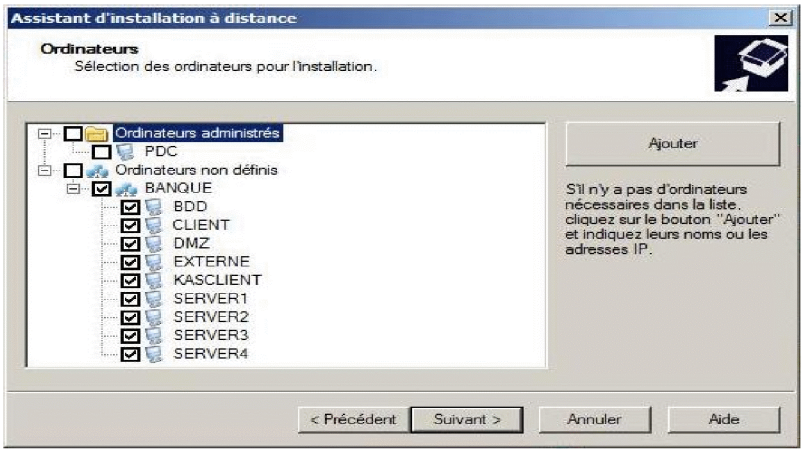

Figure V.122: La sélection des ordinateurs pour l'installation.

L'étape suivante consiste à définir les paramètres d'installation à distance.

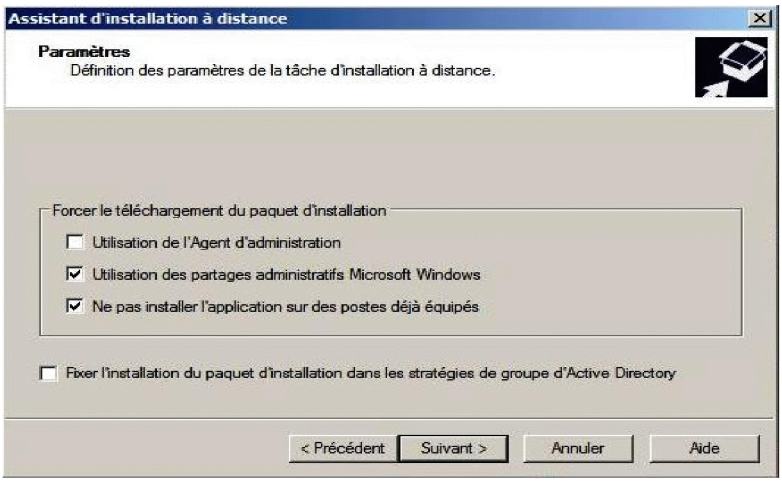

Figure V.123: La définition des paramètres d'installation à distance.

Définissons ci-après le compte avec lequel nous accédons aux ordinateurs de la forêt.

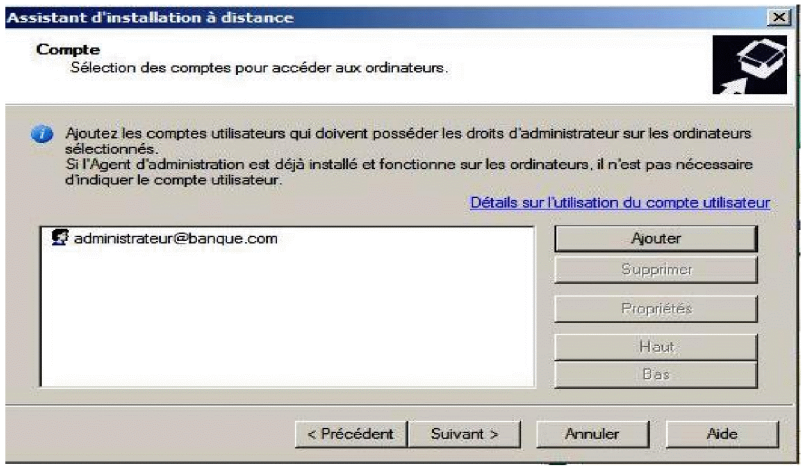

Figure V.124: Sélection du compte pour accéder aux ordinateurs.

Il nous reste plus qu'à lancer l'installation.

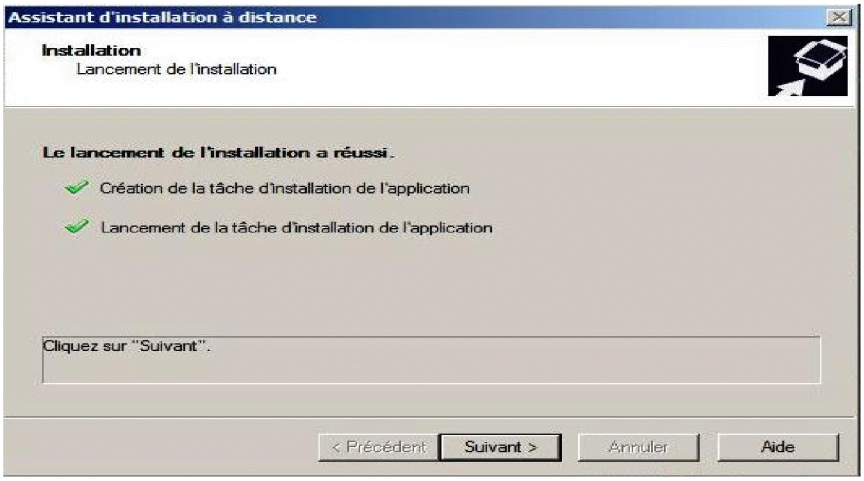

Figure V.125 : Lancement de l'installation.

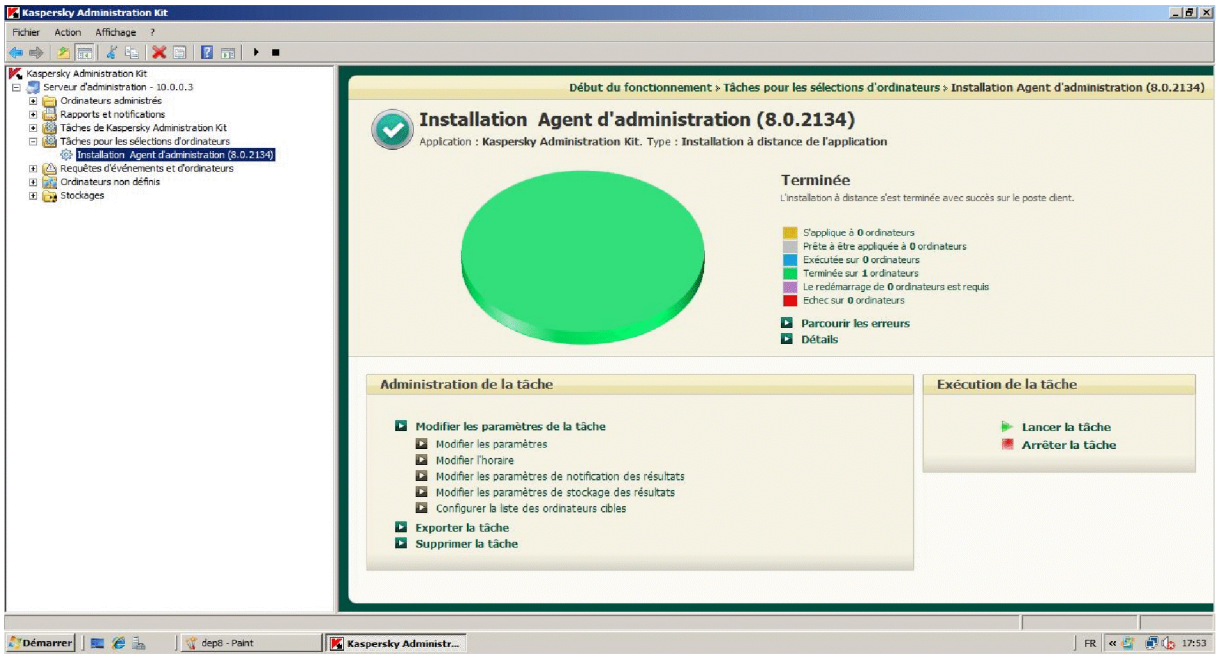

Figure V.126: Installation réussie.

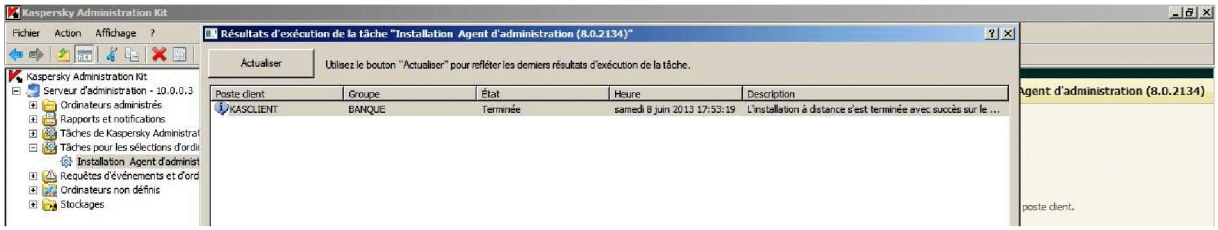

Figure V.127: Installation réussie sur la machine client.

Si nous accédons aux programmes installés sur l'une des machines clients, nous trouvons Agent d'administration.

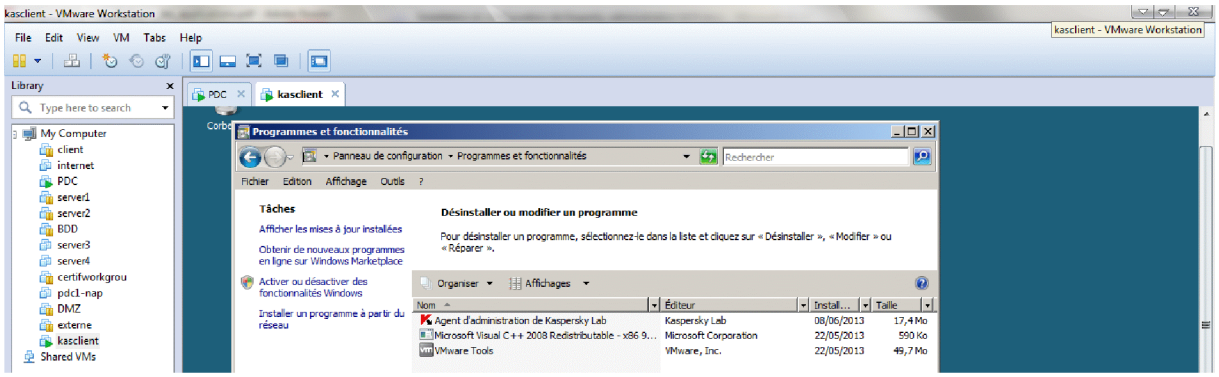

Figure V.128: Programmes installés sur la machine client.

Etape VII : La connexion des machines sous GNS3

Apres avoir implémenté les différentes solutions concernant les machines virtuelles, nous les connectons à GNS3 (le principe est expliqué dans l'annexe A). Ensuite nous relions les différents serveurs et ordinateurs au firewall ASA, après avoir configuré ses interfaces.

1. La configuration de l'ASA sous GNS3

Dans cette section nous allons configurer l'ASA sous GNS3 afin de mieux expliquer cette procédure, nous accompagnons chaque étape d'une figure.

1.1. Le chargement de l'IOS de l'ASA

Pour que l'ASA fonctionne correctement il lui faut deux images IOS, l'une **.initrd** et l'autre **.kernel** qui se chargent en deux étapes dans l'ordre suivant:

La première étape consiste à charger l'image **.initrd,** comme tout IOS, elle est expliquée dans l'annexe A.

La deuxième étape consiste à sélectionner l'ASA, dans le menu edit-> préférences -> Qemu ->ASA, en ajoutant l'image .initrd et .kernel, comme illustrée dans la figure ci-dessous, en spécifiant le nom, la RAM et d'autre critères.

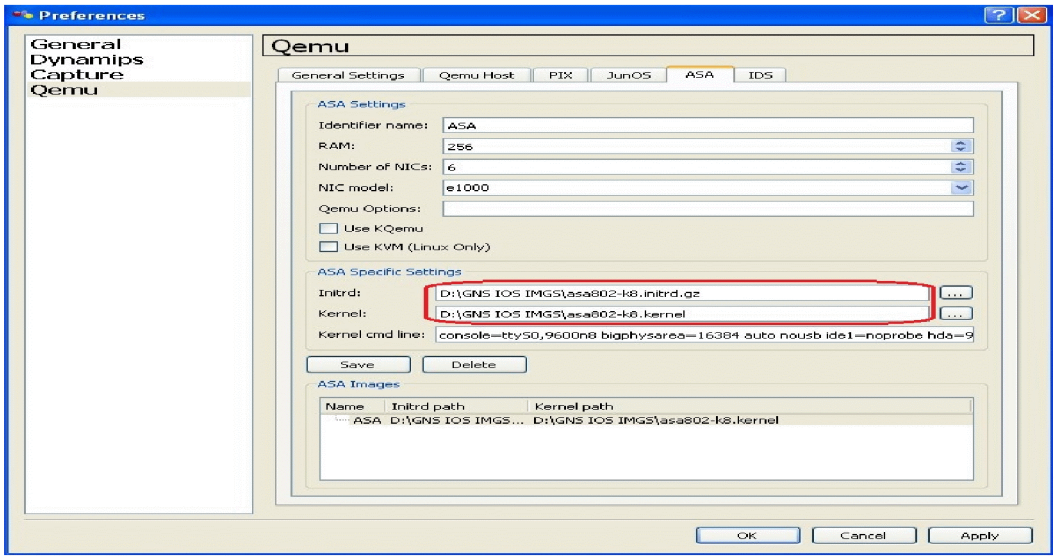

Figure V.129: L'ajout de l'IOS pour l'ASA.

Maintenant que le chargement c'est fait, l'ASA est prêt à l'utilisation. Au démarrage de l'ASA une fenêtre s'ouvre **QEMU,** afin de pouvoir lancer la console de configuration, il faut garder cette dernière ouverte pendant toute la procédure de configuration.

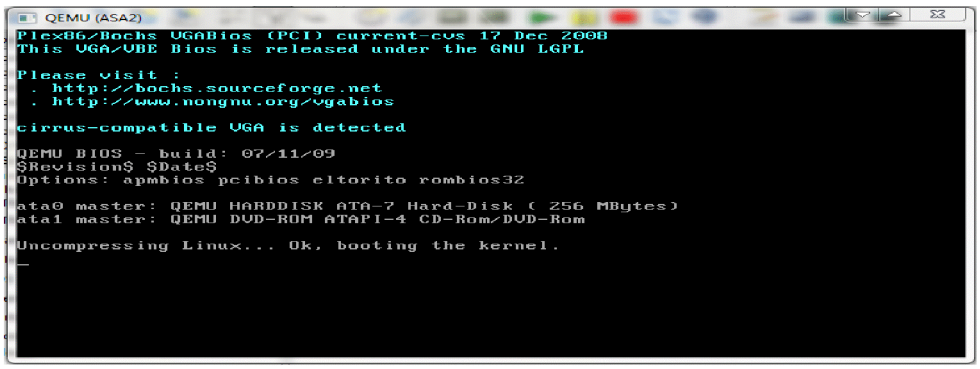

Figure V.130 : La fenêtre QEMU.

1.2. L'activation de la console

A l'ouverture de la console, un message d'activation de la console s'affiche, nous tapons les commandes suivantes comme le montre la figure ci-dessous pour activer la console.

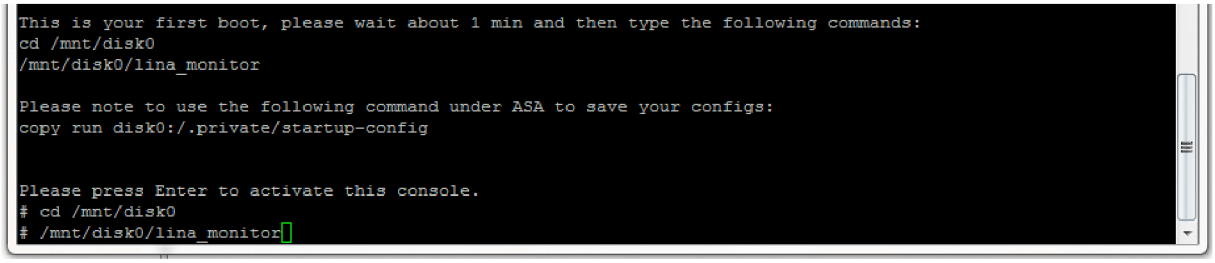

Figure V.131: Activation de la console.

1.3. La configuration des interfaces

L'attribution des adresses se fait comme tout autre équipement Cisco, néanmoins on doit préciser la nature de l'interface inside ou outside et le niveau de sécurité de chaque interface.

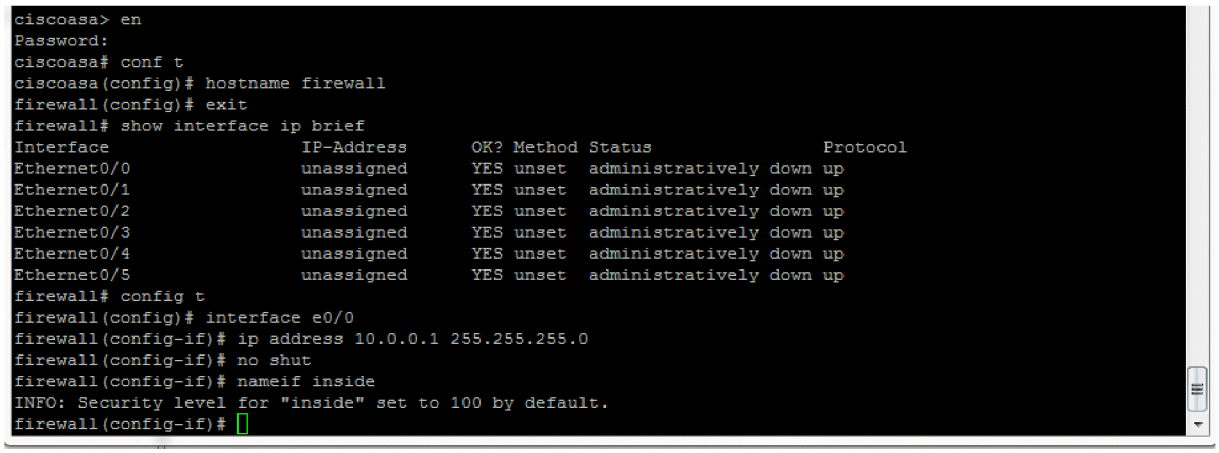

Figure V.132: La configuration des interfaces.

1.4 . La création de l'identifiant de l'utilisateur

Afin de sécuriser l'accès lors de la configuration des règles de firewall ASA, il est nécessaire d'attribuer un identifiant, un mot de passe ainsi qu'un niveau de privilèges pour l'administrateur de firewall.

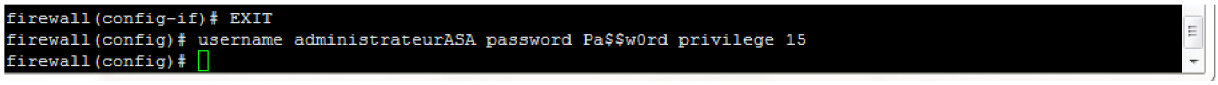

Figure V.133: L'identification de l'utilisateur.

1.5. Sécurisation par mot de passe de la console d'ASA

Pour authentifier l'accès à la console d'ASA, nous tapons les commandes suivantes, la première commande permet d'attribuer un mot de passe pour la console.

Figure V.134 : Donner le mot de passe.

La deuxième et la troisième permet de crypter le mot de passe de la console et le mot de passe de l'ASA à l'aide de protocole d'authentification SSH, ainsi que la spécification de l'algorithme de hachage et la longueur de la clé de chiffrement.

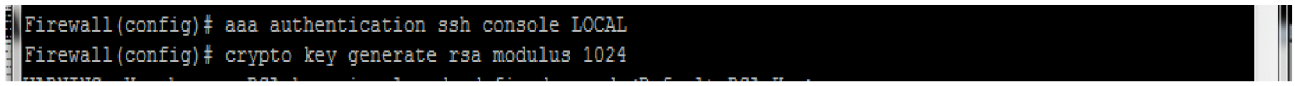

Figure V.135: Cryptage de mot de passe.

La dernière commande spécifie le sous réseau à authentifier.

firewall(config)#ssh 10.0.0.0 255.0.0.0 inside

firewall(config)#ssh 192.168.0.0 255.255.255.0 outside

firewall(config)#ssh 11.0.0.0 255.0.0.0 DMZ

Pour vérifier l'accès sécurisé à l'ASA, nous redémarrons le firewall ASA après avoir sauvegardé la configuration, et nous essayons d'accéder sans mot de passe. En utilisant la commande **show running** nous remarquons que le mot de passe est crypté.

Figure V.136 : Visualisation de la configuration.

1.6. La configuration de l'HTTP

Pour qu'une machine client puisse effectuer des requêtes HTTP, il faut le configurer au niveau de l'ASA.

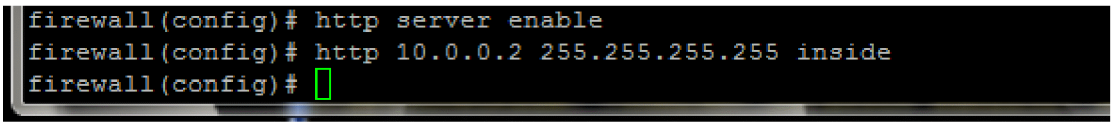

Figure V.137: La configuration de l'http.

1.7.Le chargement de l'ASDM

Pour pouvoir gérer et créer les règles de firewall ASA, il faut installer et lancer l'ASDM dans la machine distante (client).Pour cela suivons les étapes dans l'ordre que voici :

1.7.1. Installer ASDM dans le serveur TFTP

Copier le fichier TFTP et l'exécuter dans la machine client, puis ajouter l'image asdm-647.bin.

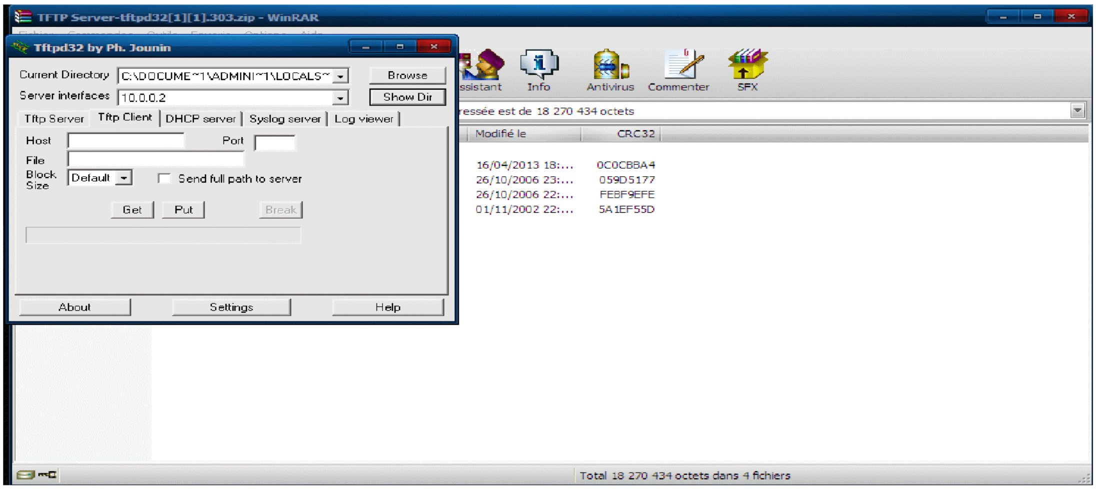

Figure V.138: Ajout de l'image ASDM à TFTP.

Maintenant, revenons à notre console ASA et chargeons l'image ASDM-647.bin en tapant les commandes suivantes :

Figure V.139: Chargement de l'image ASDM.

A la fin de chargement, si nous tapons la commande, **show flash** pour visualiser le contenu de la mémoire flash, nous voyons qu'elle contient l'image ASDM.

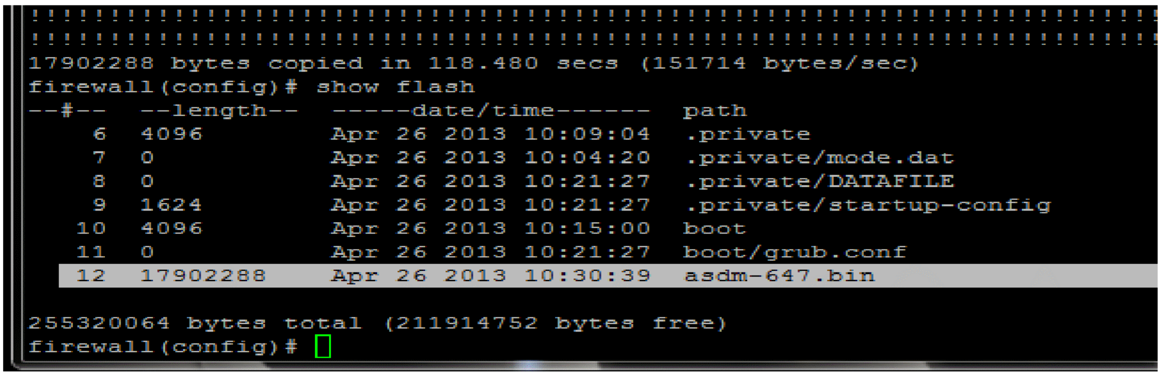

Figure V.140: Visualisation du contenu de la mémoire flash.

1.8. La sauvegarde de la configuration

Après avoir fini notre configuration nous allons la sauvegarder.

```
firewall(config)# copy run disk0:/.private/startup-config

Source filename [running-config]?

Destination filename [/.private/startup-config]?

%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
Cryptochecksum: a4502312 123e8715 285f19a8 60124074

1661 bytes copied in 2.370 secs (830 bytes/sec)open(ffsdev/2/write/41)
```

Figure V.141 : La sauvegarde de configuration.

1.9. Le lancement de l'ADSM

Avant le lancement d'ASDM, il faut s'assurer de la connexion entre l'interface de l'ASA et la machine distante en effectuant un **ping** dans les deux cotés.

```
firewall(config)# ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms
```

Figure V.142: Ping de la machine distante.

```
C:\Documents and Settings\Administrateur>ping 10.0.0.1

Envoi d'une requête 'ping' sur 10.0.0.1 avec 32 octets de données :

Réponse de 10.0.0.1 : octets=32 temps=7 ms TTL=255
Réponse de 10.0.0.1 : octets=32 temps=2 ms TTL=255
Réponse de 10.0.0.1 : octets=32 temps=2 ms TTL=255
Réponse de 10.0.0.1 : octets=32 temps=2 ms TTL=255

Statistiques Ping pour 10.0.0.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 7ms, Moyenne = 3ms

C:\Documents and Settings\Administrateur>
```

Figure V.143: Ping de l'interface ASA.

A partir de l'internet explorer de la machine distante introduisons l'adresse **https://10.0.0.1/**. Dans la page qui s'ouvre cliquons sur **poursuivre avec ce site web (non recommandé).**

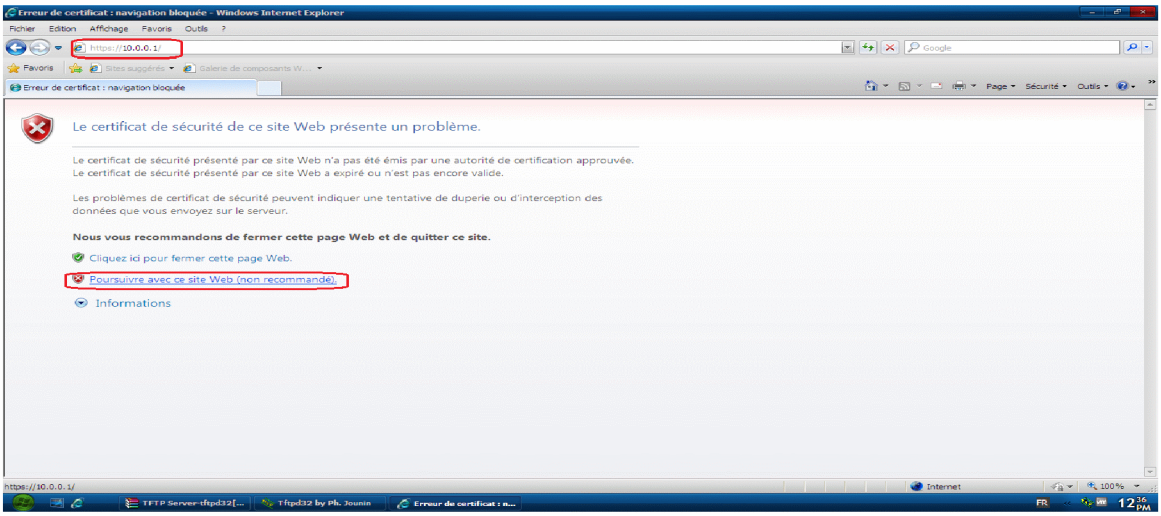

Figure V.144: Accès à l'interface d'ASA.

Cette page va nous ramener à l'interface de l'installation de l'ASDM. Cliquons sur **Install ASDM Launcher and Run ASDM**.

Une fenêtre d'authentification s'ouvre, permettant à l'administrateur du firewall d'accéder, avec le nom d'utilisateur et mot de passe à l'interface graphique ASDM.

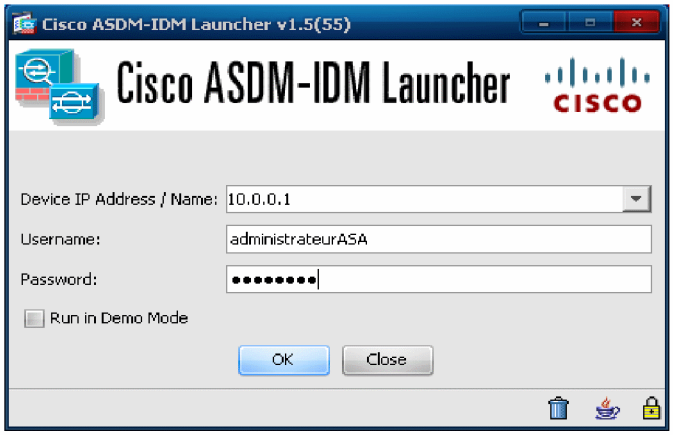

Figure V.145: L'authentification de l'utilisateur.

A la fin de l'installation, nous voyons l'interface ASDM dans le menu home.

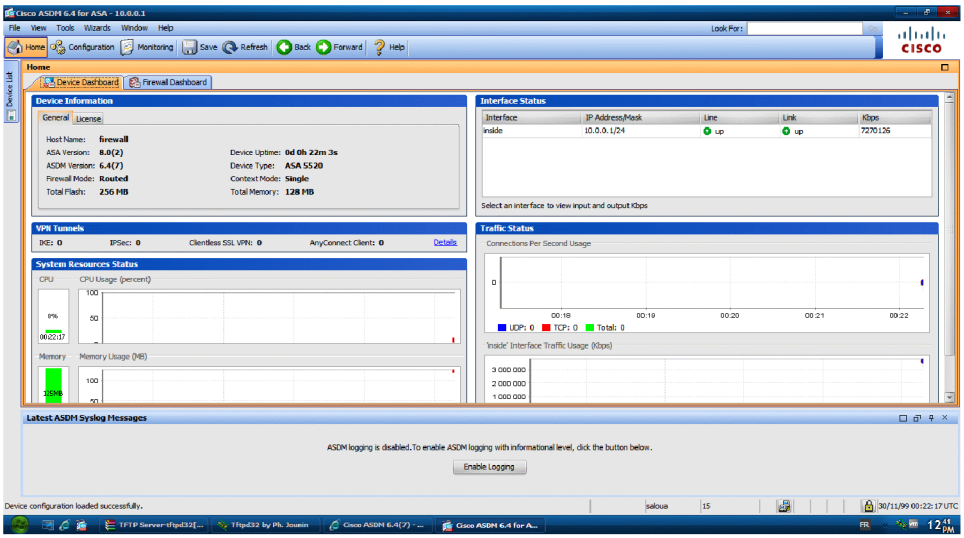

Figure V.146: Le menu Home de l'interface ASDM.

Pour ajouter des règles à ce firewall nous accédons au menu **configuration**.

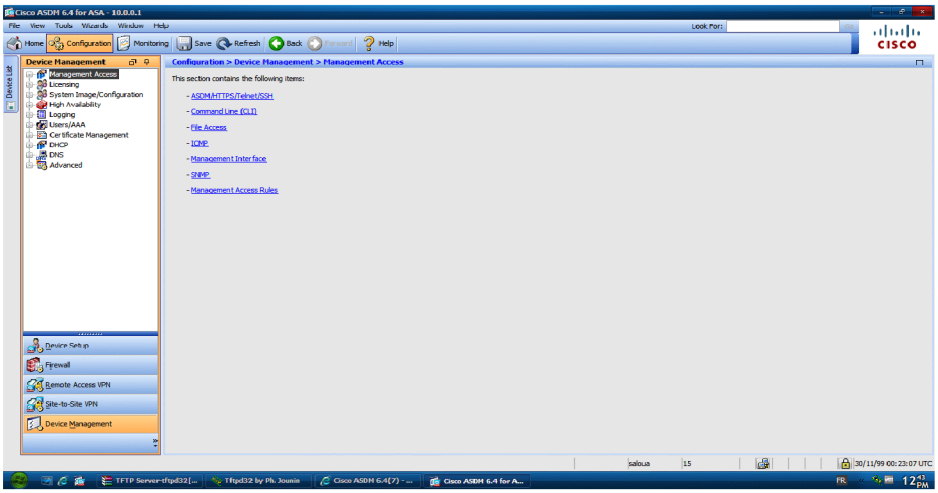

Figure V.147 : Menu configuration.

2. Création de la DMZ

Avant de créer la DMZ ASA, nous expliquons son principe de fonctionnement. Comme le montre l'architecture, l'ASA relie trois réseaux via trois interfaces.

- ✓ ASA->Intranet : L'interface **inside** avec un niveau de sécurité 100.
- ✓ ASA-> DMZ (Web et exchange) : L'interface **DMZ** avec un niveau de sécurité 50.
- ✓ ASA->internet : L'interface **ouside** avec un niveau de sécurité 0.

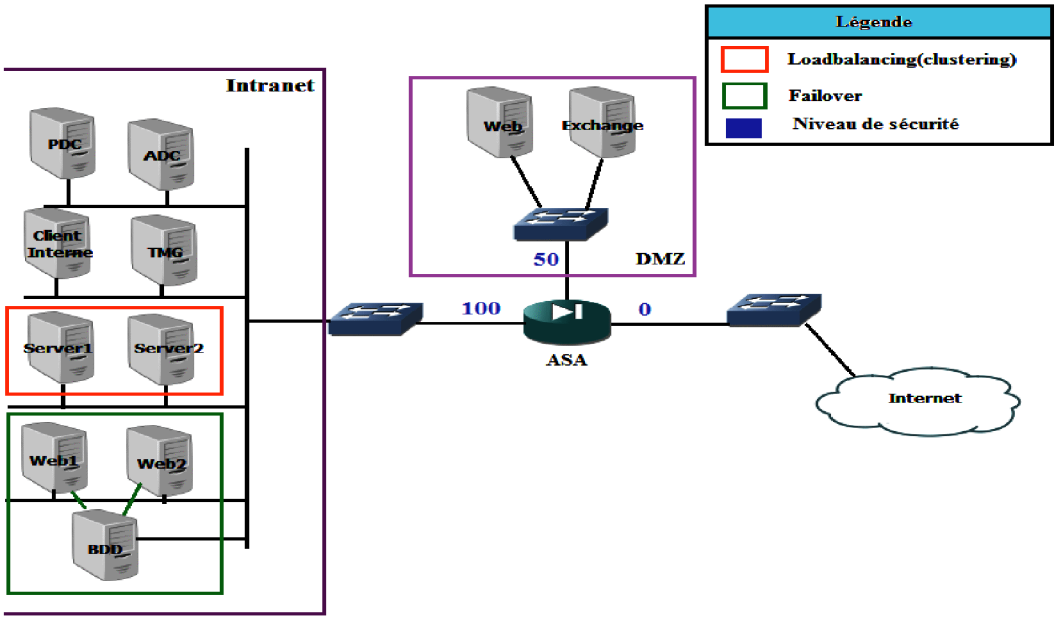

Figure V.148: La DMZ ASA.

Comme l'ASA ne permet pas le passage du trafic du niveau de sécurité supérieur à un niveau inferieur, dans cette architecture, le sens de trafic est comme suit :

- ✓ De l'intranet->DMZ c'est permis (100->50).
- ✓ De l'intranet->internet c'est permis (100->0).
- ✓ De DMZ->internet c'est permis (50->0).
- ✓ De DMZ->intranet n'est pas permis (50->100).
- ✓ De l'internet->DMZ n'est pas permis (0->50).
- ✓ De l'internet->Intranet n'est pas permis (0->100).

De cette manière, nous assurons la protection la banque de façon qu'aucun trafic ne puisse entrer. Mais pour permettre l'accès de l'extérieur vers le serveur de messagerie et le serveur web, nous allons configurer des ACL autorisant quelques protocoles TCP de l'interface outside vers l'interface DMZ.

Afin de configurer cette solution, nous accédons à l'interface graphique d'ASA, ASDM puis nous ajoutons les trois interfaces inside, outside et DMZ, en sélectionnant dans le menu configuration->interfaces->add interface.

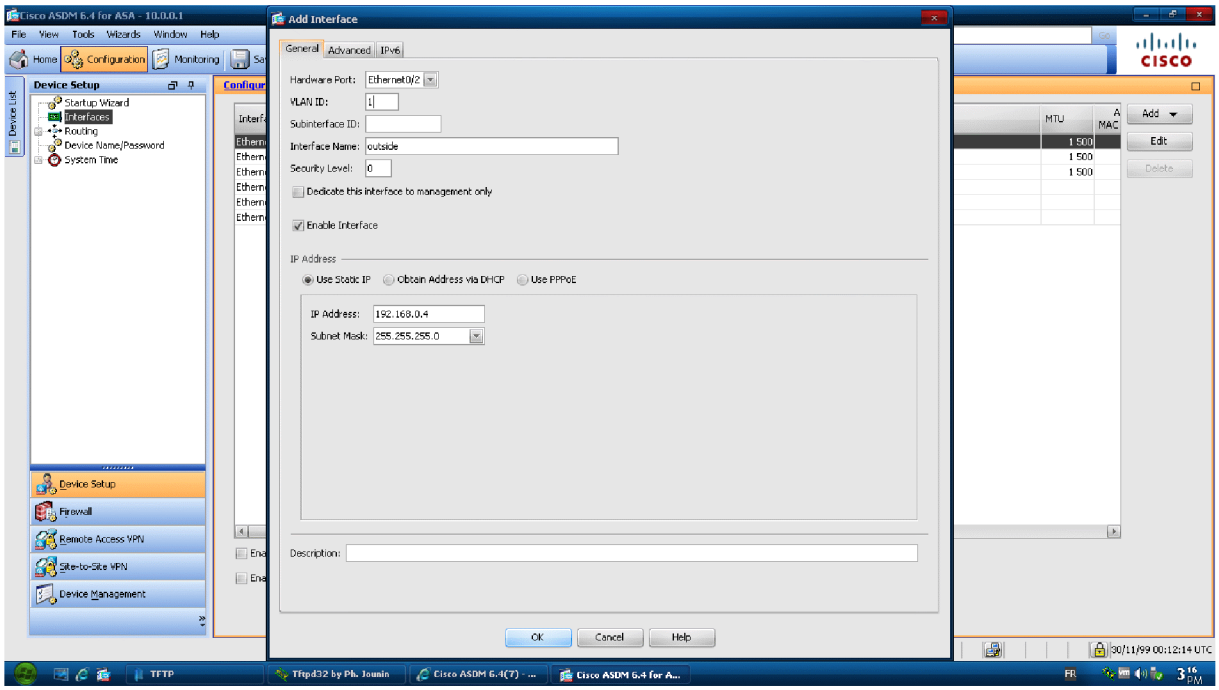

Figure V.149: Ajout d'une interface.

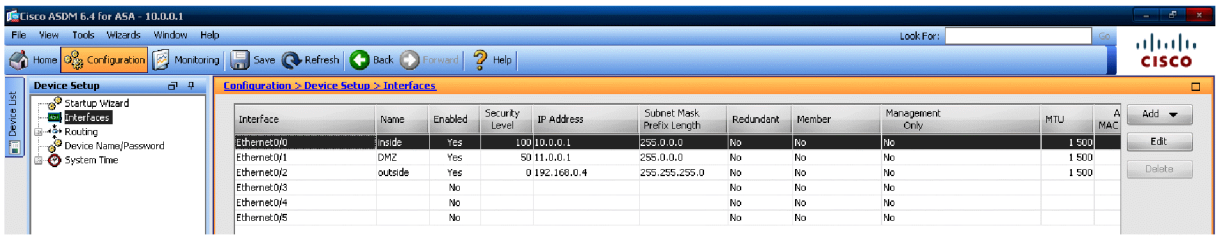

Figure V.150: L'ensemble des interfaces ajoutées.

3. Restriction du trafic

Comme nous l'avions dit, dans ASA par défaut, tout trafic de niveau supérieur à un niveau inferieur est permis, alors dans ce cas la banque n'est pas protégée des malveillants internes qui peuvent faire sortir des informations critiques de la banque.

Pour cette raison nous avons restreint le trafic sortant et entrant, de manière n'autoriser que celui autorisé par la banque. Pour ce que nous avons suggéré comme solution, et en se basant sur ce qui nous a été fournit comme informations sur les besoins de la banque. Nous avons autorisé juste les protocoles de messagerie et web : HTTPs, SMTP, POP3, IMAP4.

Et pour les autres protocoles concernant les applications et les échanges de la banque avec ses partenaires, voire des informations confidentielles, nous n'avons pas pu les déterminer et nous avons laissé le soin à la banque de les sélectionner.

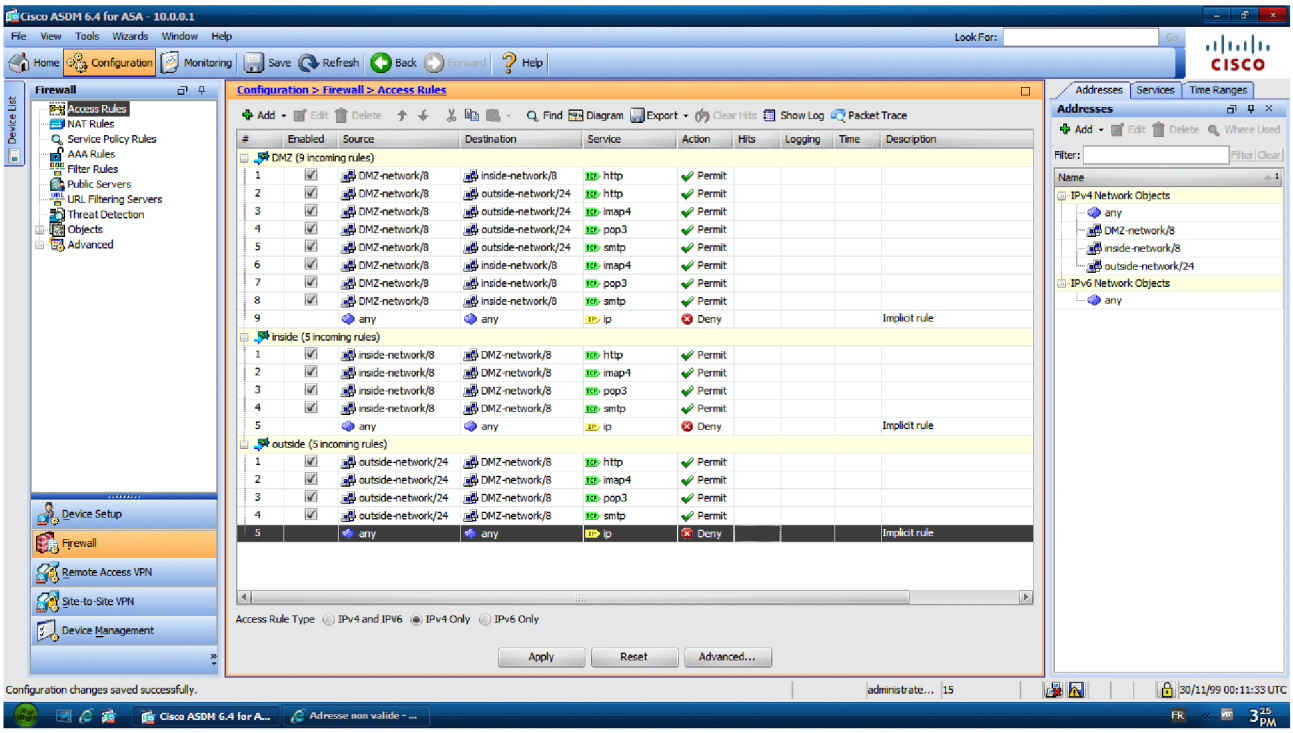

Figure V.151 : La restriction de trafic.

V.4.Conclusion

La mise en place de cette politique de sécurité, nous a permis de mettre en pratique nos acquis portant sur la sécurité réseau (les firewalls, les systèmes de prévention et détection d'intrusions, les DMZ) et la sécurité système (les protocoles chiffrés, les clusters, les certificats, le NAP et la sécurisation de la messagerie et le web).

Lors de la réalisation de cette application nous avons tout fait pour collecter le maximum d'informations et renseignements qui touchent la sécurité informatique.

Conclusion générale

Conclusion générale

La sécurité informatique assure la protection des ressources matérielles et logicielles d'une infrastructure. En effet, les différentes menaces et attaques sur divers systèmes nous ont amenées à nous poser des questions sur les moyens à mettre en place pour la garantir. En choisissant ce thème ouvert, nous avons pu explorer une infime partie de la sécurité.

La réalisation de ce mémoire nous a permis d'accroitre nos connaissances dans le vaste domaine de la sécurité. Cela en usant des différents outils, concepts et mécanismes de la sécurité. En découvrant le monde de la cyberattaque, les motivations des pirates, nous nous sommes rendu compte des limites de la sécurité. Par ailleurs, ce travail nous a permis de côtoyer le monde professionnel qui nous était jusqu'à lors inconnu.

Lors de l'étude et la réalisation de ce projet, nous avons appris que le choix des logiciels et équipements, récents soient-ils, ne suffisent pas à garantir une sécurité optimale. Avant d'effectuer le choix final de chaque équipement et logiciel, il est primordial de bien situer l'emplacement, de bien connaitre leurs fonctionnalités et de fixer judicieusement leurs objectifs d'utilisation.

En conclusion, nous souhaitons que cette politique de sécurité de la banque que nous avons mise en place, malgré toutes les contraintes temporelles et matérielles, soit enrichie et approfondie dans l'avenir.

Le Résumé

La sécurité informatique assure la protection des ressources matérielles et logicielles d'une infrastructure. En effet, les différentes menaces et attaques sur divers systèmes nous ont amenées à nous poser des questions sur les moyens à mettre en place pour la garantir. En choisissant ce thème ouvert, nous avons pu explorer une infime partie de la sécurité. Dans ce mémoire nous avons mis en place une politique de sécurité pour remédier aux failles de sécurités étudiées dans l'étude de l'existant.

ANNEXES

Annexe A : GNS3

A.GNS3

Pour la rédaction de cette annexe nous nous sommes basées sur le site officiel de GNS3.

A.1. Installation de GNS3

GNS3 est téléchargeable depuis le site officiel de GNS3. La version téléchargée est GNS3 v0.7.4 all-in-one. Son installation est une succession du terme suivant. Au lancement de GNS3, il existe deux possibilités de configuration qui sont :

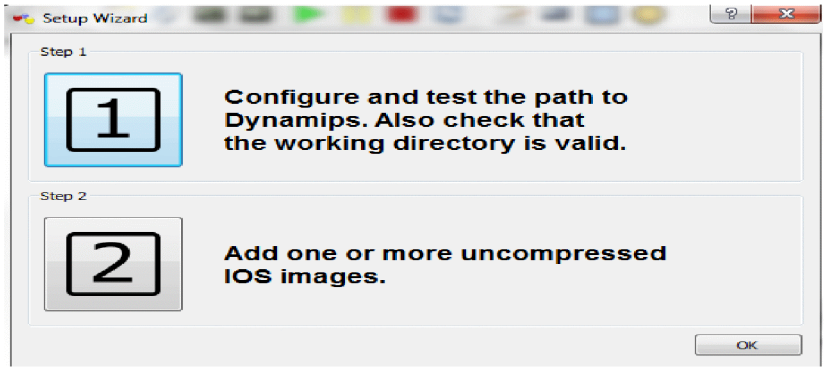

Figure A.1: Les possibilités de configuration de GNS3.

A.2. L'ajout et configuration des IOS

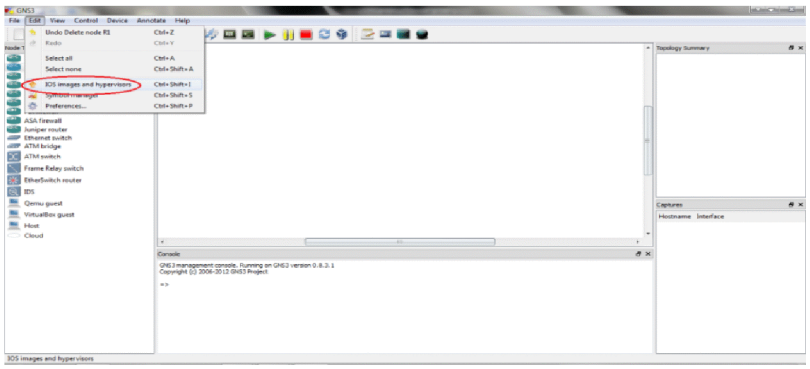

Figure A.2 : L'ajout de l'IOS.

L'IOS étant le systéme d'exploitation des équipements Cisco, il les gère en se basant sur l'architecture matérielle. Avant de configurer les IOS, il faut les télécharger. Après le téléchargement, l'étape suivante consiste à lier l'IOS à son modèle d'équipement.

Pour ajouter l'IOS aux équipements adéquats:

- ✓ Sélectionnons dans le menu Edit->IOS Images and Hypervisors
- ✓ Cliquons sur image file et sélectionnons l'IOS depuis son emplacement, puis choisissons la plate forme et le modèle de l'équipement et enfin sauvegardons.

A.3. Création d'une topologie réseaux basique

Après avoir configuré l'IOS d'un routeur 3600, faire un drag and drop sur la fenêtre principale, le routeur apparaîtra avec un nom par default R1. Pour le configurer, cliquons sur configurer.

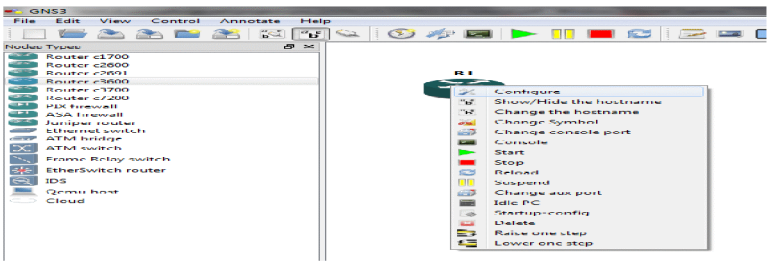

Figure A.3: La configuration d'un routeur.

Ensuite apparaît la fenêtre indiquant les propriétés du routeur (appelé node configurator). L'onglet général indique la plateforme, le modèle du routeur ainsi que son IOS. Startup config est le fichier de configuration stocké dans la NVRAM.

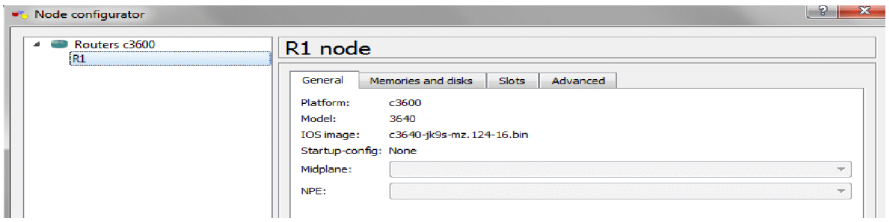

Figure A.4: Le node configurator.

Sur l'onglet Memories and Disk, la RAM et la NVRAM peuvent être configurées.

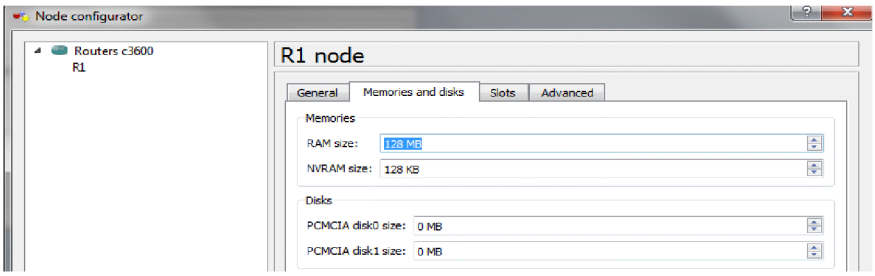

Figure A.5: Configuration de la RAM et la NVRAM.

L'onglet slot (interfaces) permet de choisir les modules à ajouter au routeur.

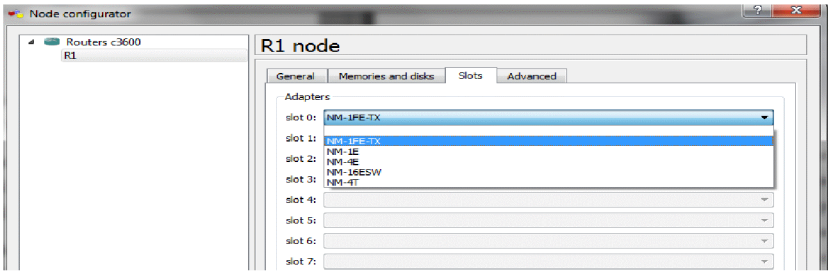

Figure A.6 : Le choix des modules des routeurs.

Apres avoir fait le choix du routeur, effectuant un clic droit sur le routeur et start, et pour avoir accès à la console, puis effectuons un clic droit et console. L'image de l'IOS apparaît décompressée et chargé en RAM.

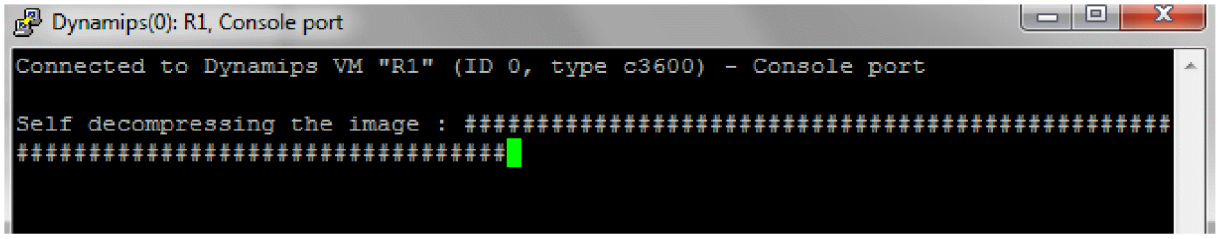

Figure A.7: La décompression de l'IOS.

A.4. Optimisation de l'utilisation des ressources CPU

GNS3 consommant les ressources matérielles, la CPU du PC utilisé peut atteindre des sommets comme ci-dessous.

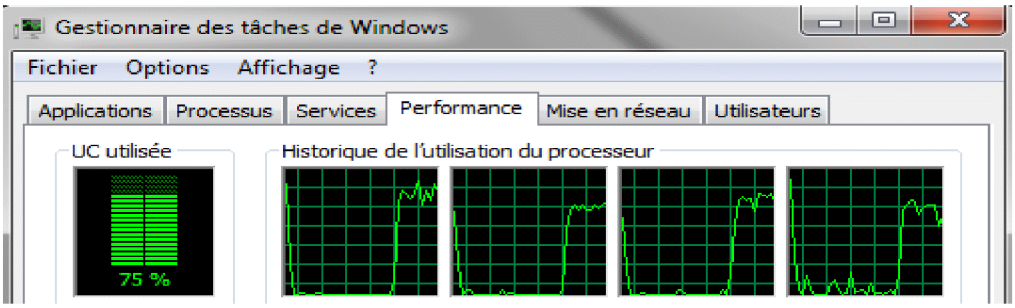

Figure A.8: Gestionnaire des taches de Windows.

Pour éviter cela, effectuons un clic droit sur le routeur et sélectionn idle PC. Une fenêtre temporaire apparaît le temps de calculer ce qui est appelé idle value, puis s'affiche un menu déroulant avec une ou plusieurs valeurs différentes de l'idle value. Il faut choisir la valeur avec un astérix. Un message de confirmation apparaitra pour indiquer que cela a été appliqué. L'utilisation de la CPU devrait revenir à un niveau raisonnable (quelques %)

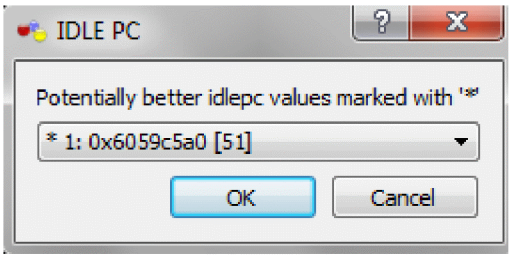

Figure A.9: IDLE PC.

A.5. Capture de paquet

GNS3 permet de capturer le trafic sur un lien donné à l'aide de **wireshark** (qui est installé avec cette version de GNS3). Prenons un exemple de deux routeurs connectés en Fastthernet, il

faut effectuer un clic droit sur le lien physique, et cliquer sur capture. Un menu déroulant apparait avec possibilité de choisir l'interface physique.

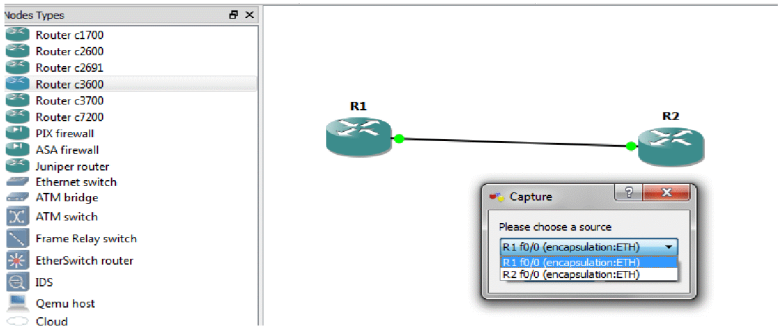

Figure A.10: La capture.

Après sélection, wireshark se charge (s'il n'a pas été installé dans le répertoire par default, il faut modifier cela dans le menu Edit-> Préférence ->Capture en sélectionnant le répertoire où il se trouve). Il permet de visualiser le ping qui sera effectué entre les deux routeurs.

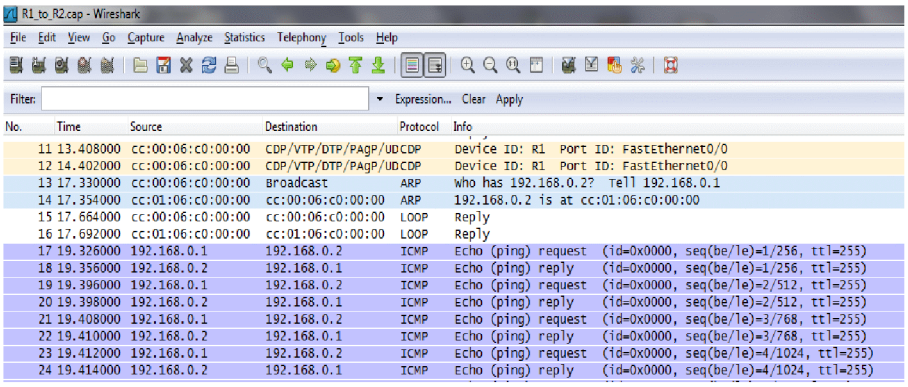

Figure 11: La capture avec Wireshark.

A.6. La connexion d'une interface routeur à la carte réseau d'une machine virtuelle

A.6.a. La procédure

Ajoutons un cloud (nuage) dans l'espace de travail en choisissant « Change Symbol », il est possible de le transformer en un autre équipement (une machine) et le connecter par un câble avec une interface du routeur. Celle-ci connectée, elle représente la carte réseau qui peut être configurée avec les paramètres IP pour une connexion logique à l'interface du routeur.

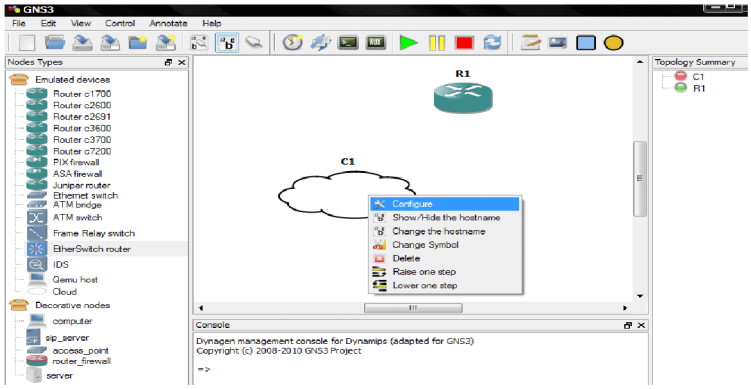

Figure A.12 : La configuration du nuage.

Lors de la configuration de la machine la fenêtre Node configurator apparaît. Elle liste les différentes cartes réseau dont dispose la machine physique. Apres sélection de la carte réseau voulue, il suffit de l'ajouter.

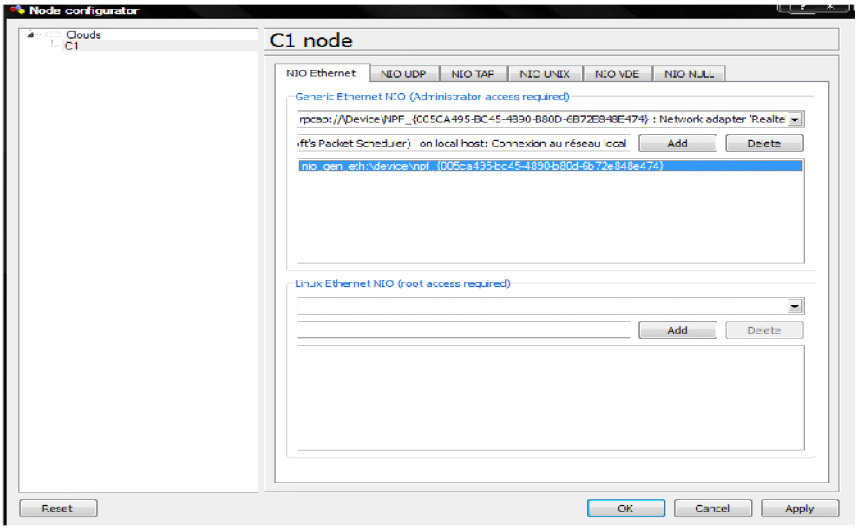

Figure A.13 : Le choix de la carte réseau.

Annexe B : Active Directory

B.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.

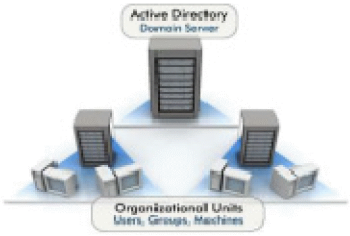

Figure B.1 : Active Directory.

B.2. La structure d'Active directory

B.2.1. Sites et domaines

Un site désigne la combinaison d'un ou plusieurs sous-réseaux IP. Bien souvent, on attribue un sous-réseau IP à un site physique d'une entreprise. Cela permet de distinguer les postes sur le réseau de l'entreprise. En créant des sites Active Directory, les ordinateurs feront qu'ils font partie de tel ou tel site. Cela est très important dans une configuration multi-sites du même domaine Active Directory. Si un contrôleur de domaine fait partie du site Agence par exemple et qu'un ordinateur du site Agence a besoin d'un accès à Active Directory, alors il n'aura pas besoin de contacter le site Siege, il ira directement voir le serveur de l'agence. Si le serveur de l'agence est en panne alors il pourra aller voir le serveur du siège en utilisant des liens WAN. Les sites sont

généralement symbolisés par des ovales. Voici la représentation des sites mentionnés précédemment.

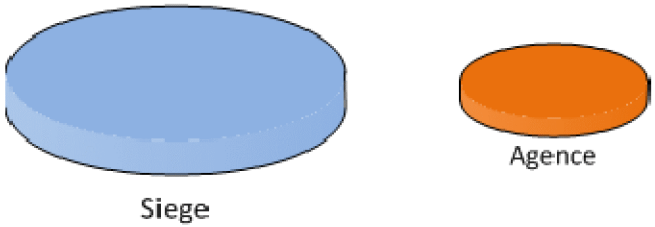

Figure B.2: Représentation des sites.

Un domaine, contrairement à un site, mappe la structure logique de l'organisation. C'est-à-dire bien souvent la hiérarchie. Le domaine n'a aucun lien avec le réseau IP, c'est un ensemble d'ordinateurs et d'utilisateurs partageant le même annuaire. Un domaine porte un nom. L'espace de nomination est réalisé grâce au système DNS. Il peut avoir plusieurs sous-domaines, on crée ainsi une arborescence. Le séparateur est le point. Si l'on souhaite créer un sous-domaine corps dans un domaine existant developpez.adds, alors le domaine se nommera corps.developpez.adds.

Bien qu'il soit possible de créer plusieurs domaines et sous-domaines, il est conseillé d'être le plus proche de la configuration idéale, une configuration mono-domaine. Il est très simple de créer des domaines à tour de bras. Cependant, créer des domaines multiplie la charge administrative par le nombre de domaines créés. La création d'un domaine supplémentaire doit être justifiée dans la mesure où elle va fortement impacter la charge de travail.

Voici des justifications possibles :

- ✓ La délégation de l'administration d'Active Directory ne convient pas dans l'organisation pour des raisons principalement politiques.
- ✓ La sécurité des données du domaine, par exemple, lors de l'utilisation de serveurs.

Un domaine est généralement représenté par un triangle.

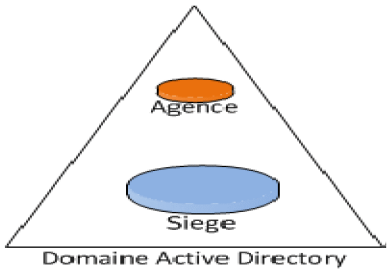

Figure B.3: Représentation d'un domaine.

Ce qu'il faut retenir, c'est qu'un domaine peut être sur plusieurs sites mais qu'un site (au sens Active Directory) ne peut pas avoir plusieurs domaines. Un site mappe la structure physique alors que le domaine mappe la structure logique de l'organisation.

B.2.2. Arborescences et forêts

Une arborescence est une notion qui découle du système DNS et des domaines Active Directory. Comme nous l'avons vu précédemment, il est possible de créer des domaines dans des domaines. Cette création se fait dans un espace de nommage contigu, Comme l'exemple précédent le sous-domaine corps fait partie du domaine developpez.adds et portera donc le nom corps.developpez.adds. Cette notion d'arborescence est différente de celle de forêt. Une forêt peut comprendre plusieurs arborescences. La forêt developpez.adds présentée ci-dessous comporte quatre arborescences :

- ✓ de developpez.adds à windows.developpez.adds.
- ✓ de developpez.adds à dev.corp.developpez.adds.
- ✓ de developpez.adds à corp.developpez.adds.
- ✓ de corp.developpez.com à dev.corp.developpez.adds.

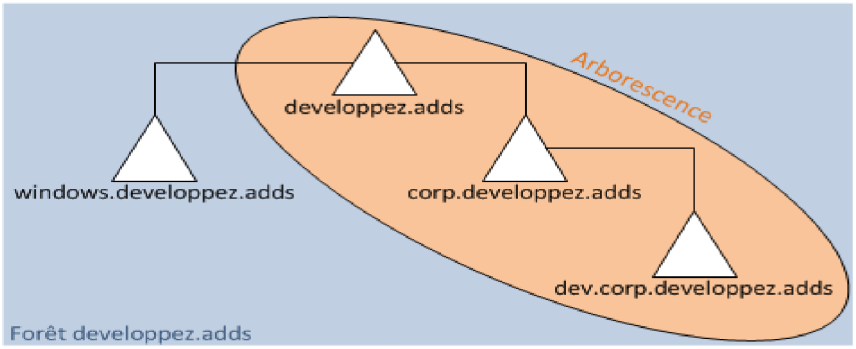

Figure B.4: Forêt et arborescence.

Les arborescences d'une même forêt peuvent partager des ressources et des fonctions administratives. Comme pour les domaines, il est conseillé d'être, le plus possible dans la configuration idéale, c'est-à-dire en mono-forêt. La configuration idéale est donc un Active Directory mono-domaine mono-forêt.

B.2.3. Niveau fonctionnel de forêt et de domaine

Active Directory est un produit en évolution depuis sa création. Afin de conserver des niveaux de compatibilité entre les différentes versions de Windows et des produits s'implantant dans Active Directory (Exchange, MOM, SCCM, etc.), il a été introduit la notion de niveau de forêt et de domaine. Actuellement il existe plusieurs niveaux:

- ✓ Windows 2000 mixte.
- ✓ Windows 2000 natif.
- ✓ Windows 2003.
- ✓ Windows 2003 R2.
- ✓ Windows 2008.
- ✓ Windows 2008 R2.

Pour augmenter le niveau fonctionnel d'une forêt, il faut que tous les domaines soient au minimum de ce niveau fonctionnel. Un niveau fonctionnel impose que tous les contrôleurs de domaine soient capables de gérer ce même niveau. Par exemple, pour avoir un niveau fonctionnel Windows 2008, il faut que tous les contrôleurs de domaine soient en Windows 2008. Il est possible d'avoir des contrôleurs de domaine de version supérieure dans un domaine de niveau inférieur : on peut avoir un niveau fonctionnel Windows 2003 avec des contrôleurs de domaine Windows 2003 et Windows 2008.

B.2.4. Utilisateurs et ordinateurs

Chaque utilisateur dans Active Directory est associé à un objet. Cet objet contient plusieurs attributs qui décrivent l'utilisateur (nom, prénoms, login, adresse e-mail, téléphone, département,...). Ces attributs peuvent permettre de trouver des utilisateurs dans le domaine. Ils peuvent par exemple être utilisés dans Exchange pour constituer des listes dynamiques de distribution d'e-mails. Ces utilisateurs peuvent se voir attribuer des autorisations sur d'autres objets d'Active Directory. Lorsqu'il y a plusieurs utilisateurs, il est possible de les gérer par groupe.

Les ordinateurs disposent également de comptes spécifiques dans Active Directory. Ces comptes existent pour gérer la sécurité pour les accès à certaines ressources comme les stratégies de groupe, les logins, l'accès au réseau avec NAP par exemple. On pourra également gérer les ordinateurs par groupe.

B.2.5. Groupes

Il existe deux types de groupes. Le premier et le plus courant est le groupe de sécurité. Ce type permet de gérer la sécurité pour l'accès et l'utilisation des ressources de réseau. Le deuxième type est le groupe de distribution. Ce type permet simplement de gérer des listes de distribution d'e-mails dans un serveur de messagerie. Pour ces groupes, il existe trois étendues :

- ✓ **Domaine local :** Il est possible d'ajouter des comptes de n'importe quel domaine et/ou des groupes "Domaine local" du même domaine et/ou des groupes universels/globaux de

n'importe quel domaine. Les autorisations portent uniquement sur le domaine auquel le groupe appartient.

- ✓ **Globale :** Il est possible d'ajouter des comptes du domaine d'appartenance et/ou des groupes globaux du domaine d'appartenance. Les autorisations peuvent être accordées dans n'importe quel domaine.
- ✓ **Universelle :** Il est possible d'ajouter des comptes de n'importe quel domaine et/ou des groupes globaux et universels de n'importe quel domaine. Les autorisations pour cette étendue portent sur tout le contenu de la forêt.

B.2.6. RODC

Il s'agit d'une nouveauté apparue avec Windows 2008. Il signifie Read-Only Domain Controller ou Contrôleur de domaine en lecture seule. Il s'agit d'un contrôleur de domaine spécialement prévu pour les architectures de type Branch Office ou réseau d'agences donc en architecture multi-sites. Un contrôleur de domaine en lecture seule sera installé dans les agences, les seules modifications possibles seront faites par le biais du contrôleur de domaine responsable de la réplication. Ce contrôleur de domaine responsable de la réplication est nommé tête de pont.

L'avantage principal du RODC est qu'il ne nécessite quasiment aucune maintenance et est plus sécurisé qu'un contrôleur de domaine classique puisqu'il est en lecture seule. Ce type de contrôleur de domaine est parfait pour les agences où il n'y a pas d'administrateur système. Cependant, cela est problématique pour les applications ayant besoin d'un accès en écriture sur Active Directory.

B.2.7. DNS

Le DNS est la base d'Active Directory. C'est grâce au DNS que les postes utilisateurs ou serveurs membres du domaine peuvent trouver le ou les serveur(s) Active Directory. Pour trouver le serveur Active Directory, les utilisateurs vont demander au DNS l'enregistrement de type SRV ayant pour nom _ldap._tcp.developpez.adds (où developpez.adds est le nom de domaine). Cet enregistrement SRV contient le nom du serveur qui possède l'annuaire ainsi que le port TCP à utiliser pour accéder à ce serveur en LDAP. Par défaut, ce port est le 389 pour les communications non cryptées. Une requête DNS supplémentaire sera effectuée pour connaitre l'IP du serveur en question. Une fois que le client saura quel serveur contacter, il pourra avoir accès (à condition d'avoir des identifiants) aux différentes ressources proposées grâce à Active Directory, comme partage de fichiers et d'imprimantes, messagerie,... Il est dont vital pour l'architecture d'avoir un service DNS qui fonctionne correctement. Généralement, on utilise le serveur DNS fourni avec Windows Server et la plupart du temps, placer le serveur DNS sur le serveur Active Directory. Il est

possible d'utiliser des serveurs différents du type Bind9 sous Linux. Cependant, cela requiert une certaine configuration, notamment pour la réplication des informations entre serveurs, celle-ci ne sera plus gérée par Active Directory mais par le serveur DNS.

B.3. L'installation d'Active Directory sous Windows 2008

B.3.1. Procédure

Dans le menu « Démarrer. Tous les Programmes. Outils d'administration. Gérer votre serveur ». Cliquer sur le lien « Ajouter ou supprimer un rôle ».

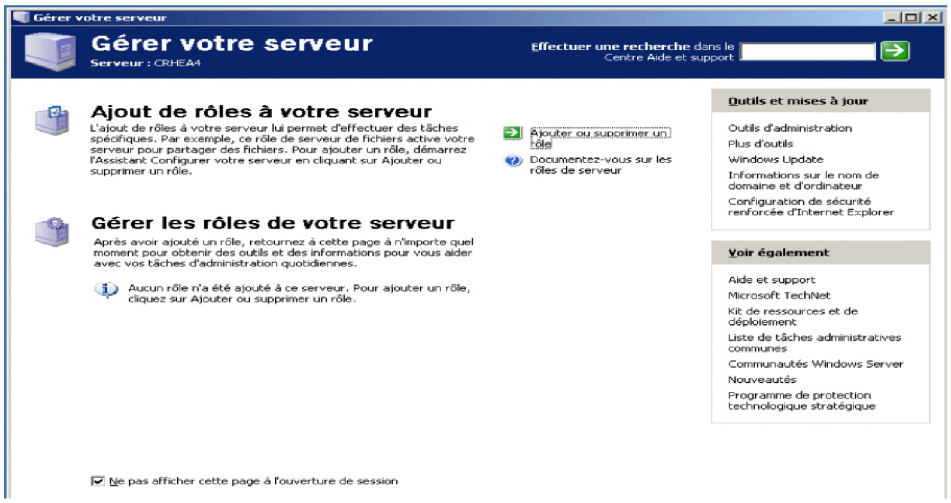

Figure B.5 : l'assistant « Gérer votre serveur ».

L'étape préliminaire (figure B.6) vous invite à effectuer les dernières vérifications avant le début de la procédure d'installation d'Active Directory. Quand tous les éléments nécessaires sont en place, cliquer sur le bouton « Suivant > » pour continuer.

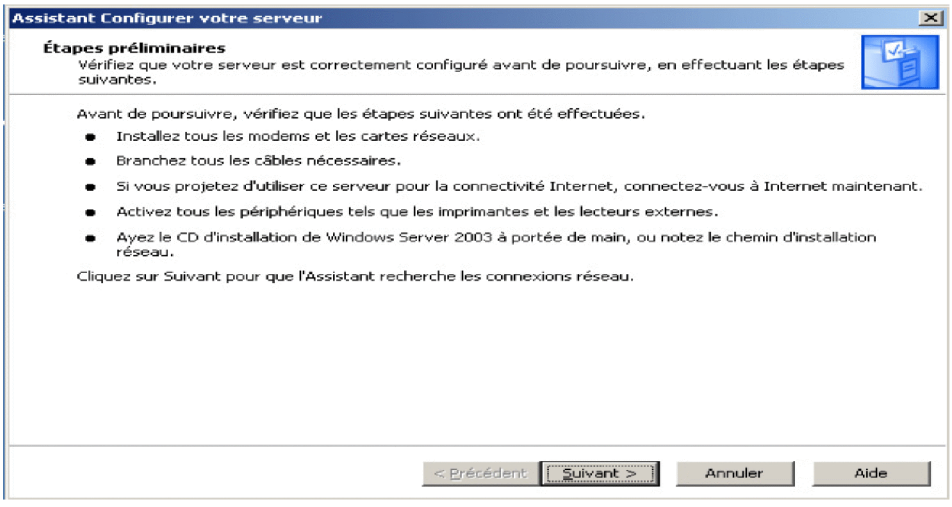

Figure B.6 : Etapes préliminaires, instant des ultimes vérifications.

Figure B.7 : Détection des paramètres réseau.

Ensuite spécifier le nouveau rôle « contrôleur du domaine » dans la liste de l'assistant «Configurer votre serveur » de la (Figure B.8)

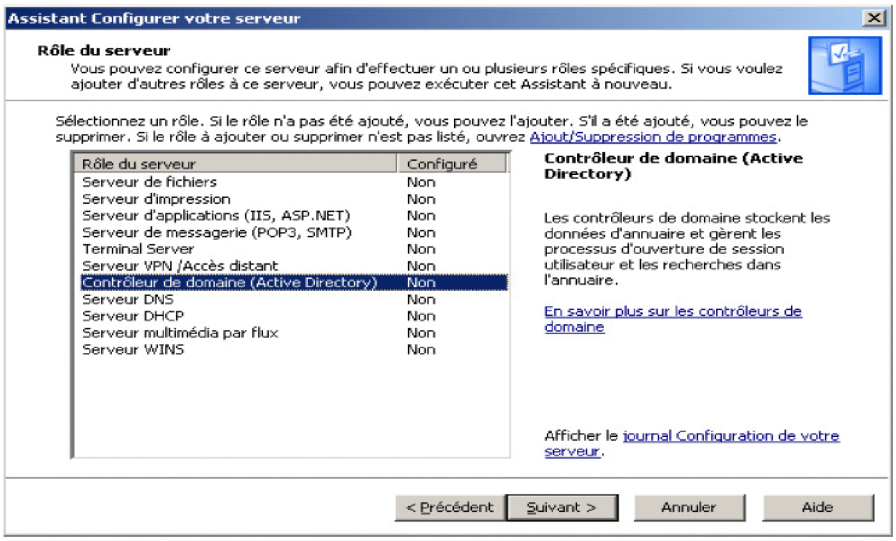

Figure B.8 : Sélection du rôle Contrôleur de domaine.

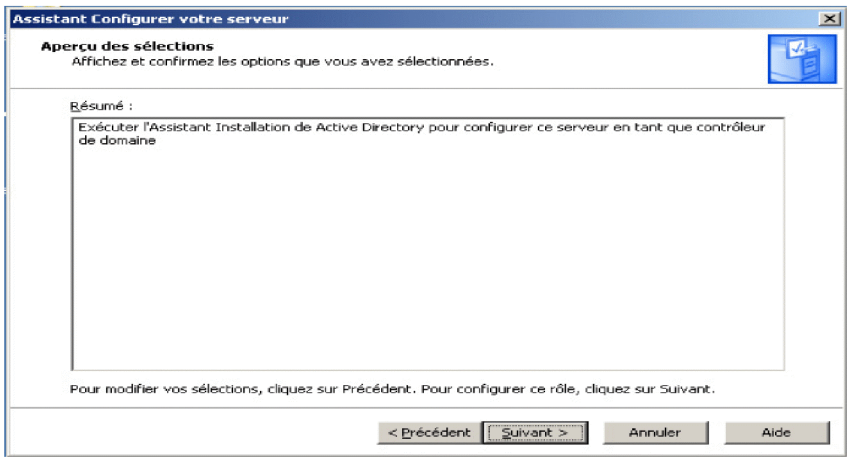

Figure B.9 : Résumé de l'installation à effectuer.

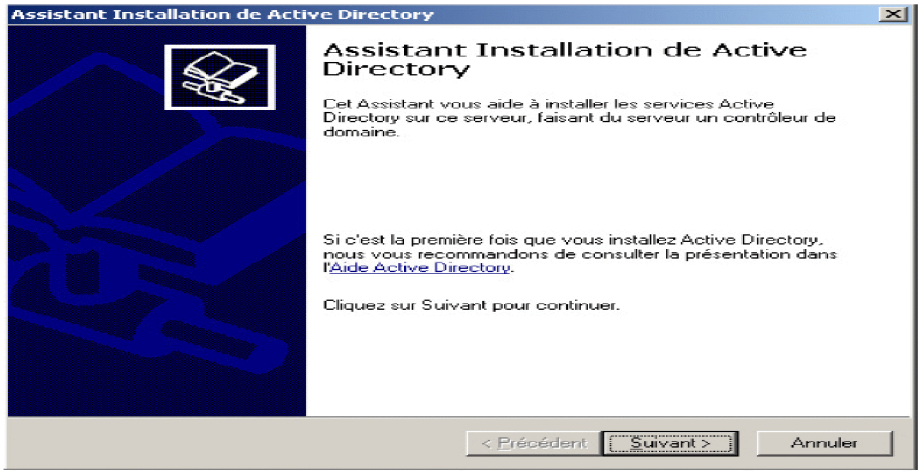

Figure B.10 : Lancement de l‟.assistant d'installation d'Active Directory.

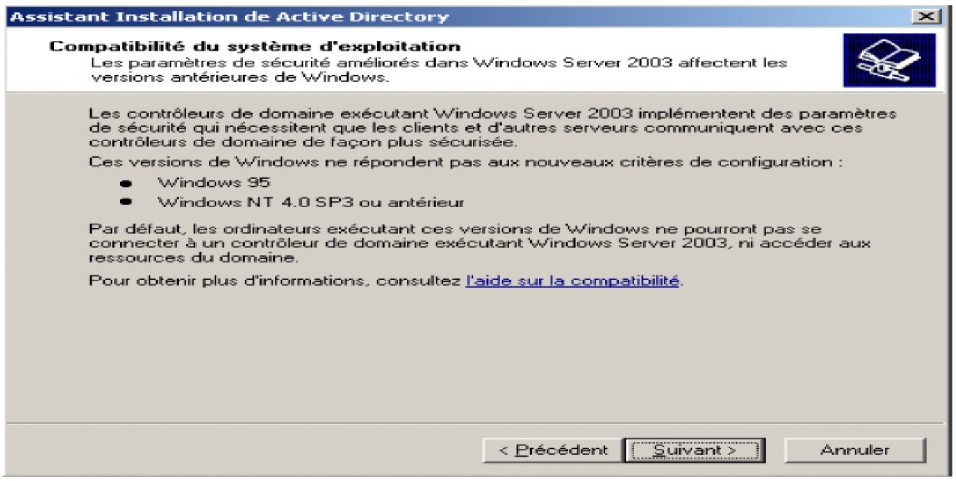

Figure B.11 : Compatibilité des systèmes d'exploitation clients.

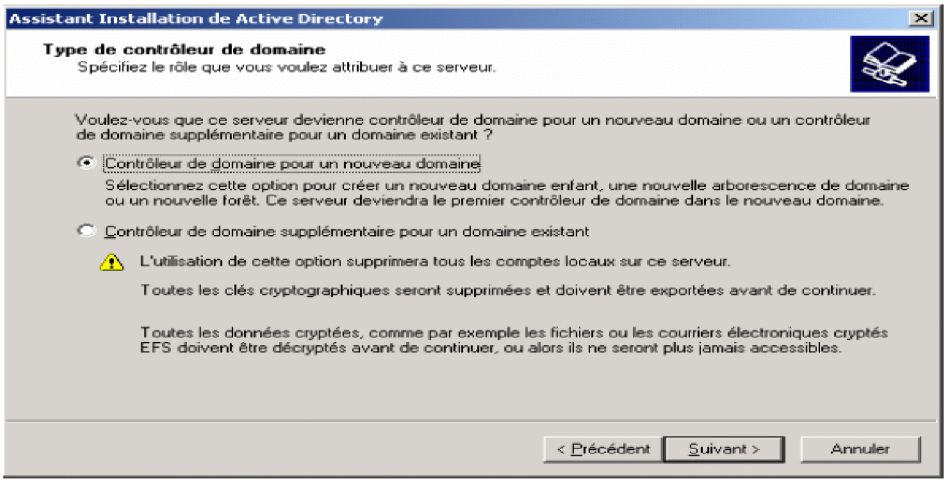

Figure B.12 : Installation du contrôleur principal du domaine.

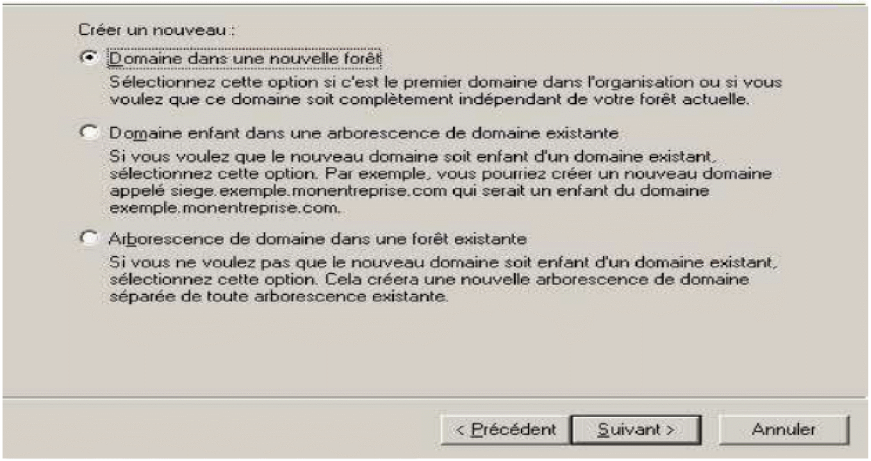

Figure B.13 : Nouveau nom dans nouvelle forêt.

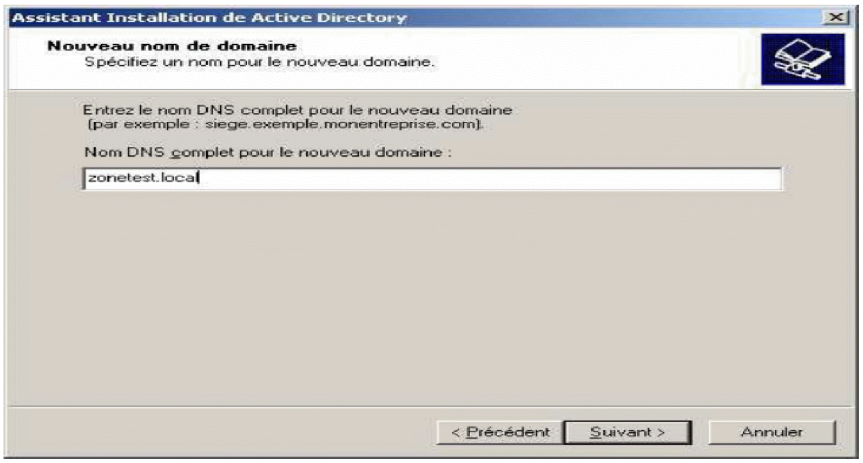

Figure B.14 : Nom DNS du domaine.

Ensuite donner le chemin de la base de données et du journal Active Directory. Microsoft préconise des disques durs différents pour des raisons de performances et de meilleure récupération (figure B.15).

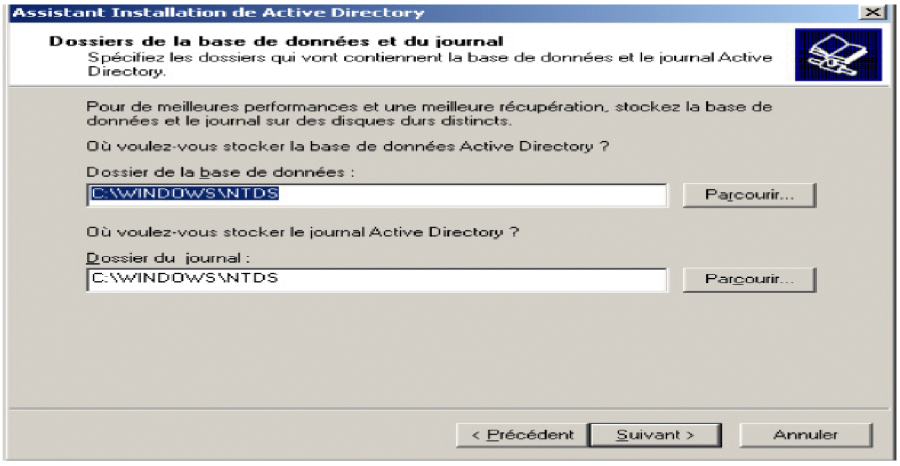

Figure B.15 : Emplacement des données et du journal AD.

On Indique ensuite „emplacement du dossier Sysvol selon Figure B.16.

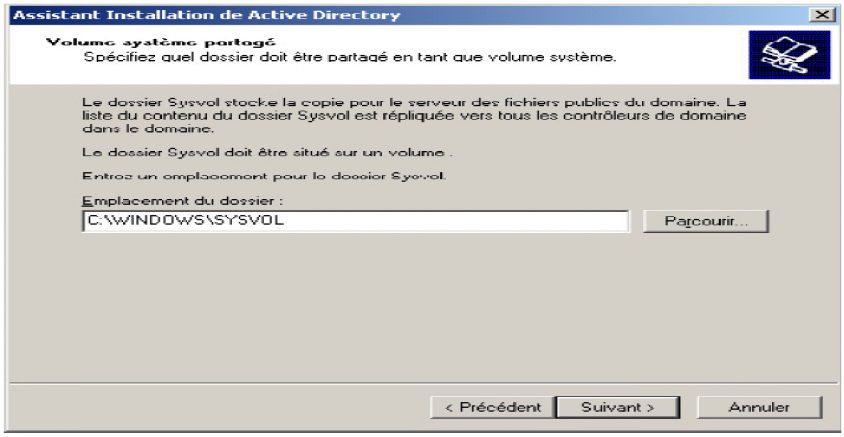

Figure B.16 : Emplacement du dossier Sysvol.

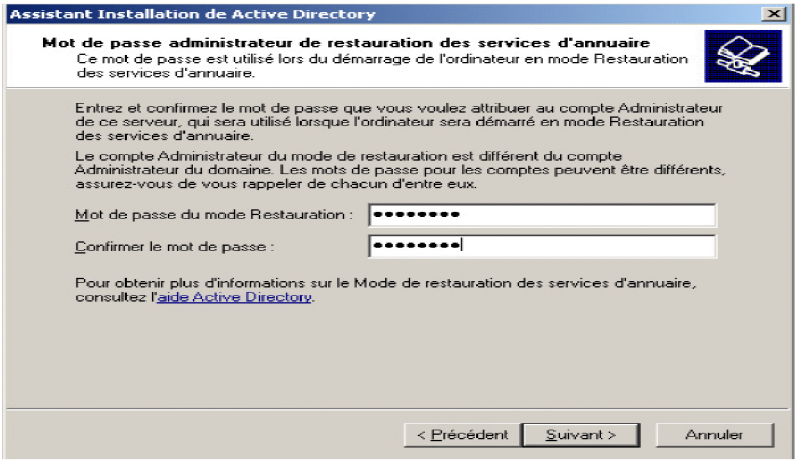

Figure B.17 : Saisie du mot de passe administrateur.

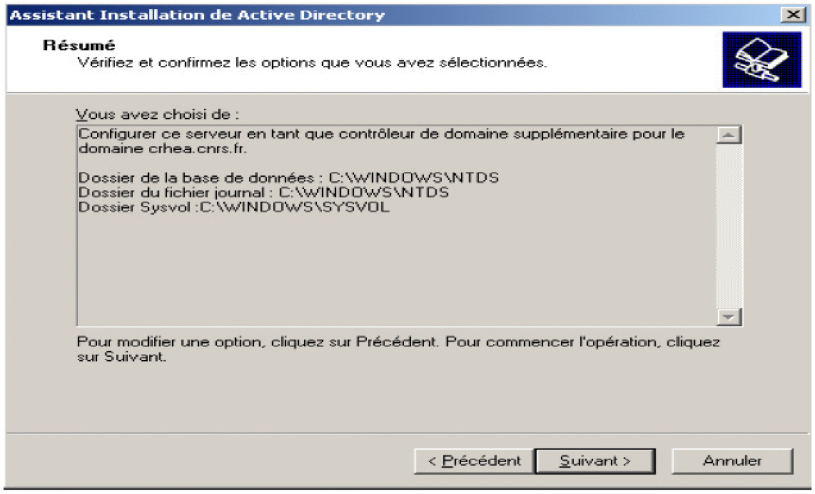

Figure B.18 : Affichage du résumé.

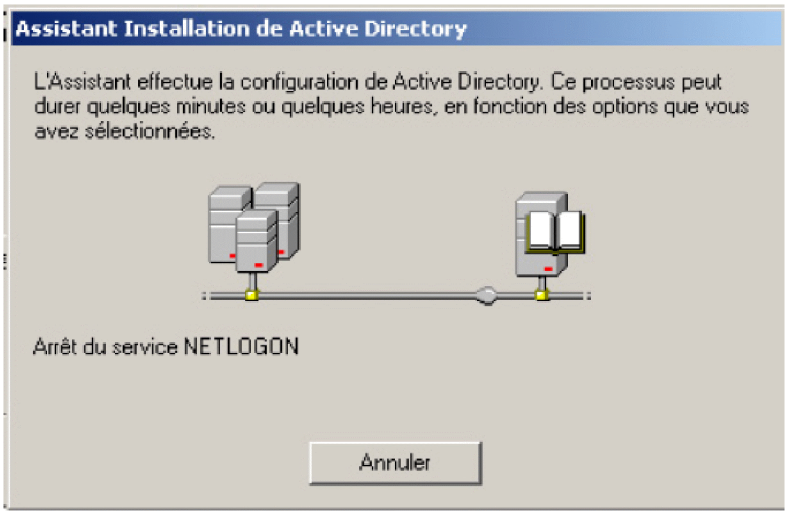

Figure B.19 : Configuration d'Active Directory.

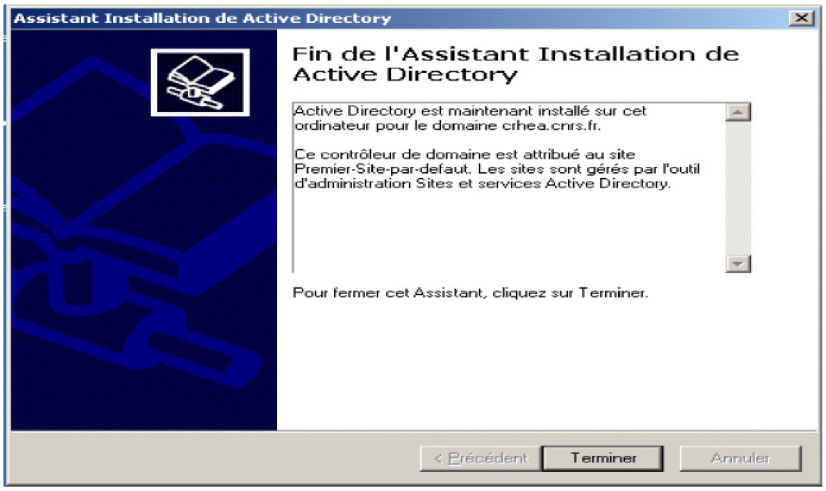

Figure B.20 : Fin de l'installation d'Active Directory.

Annexe C : Installations

C.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.

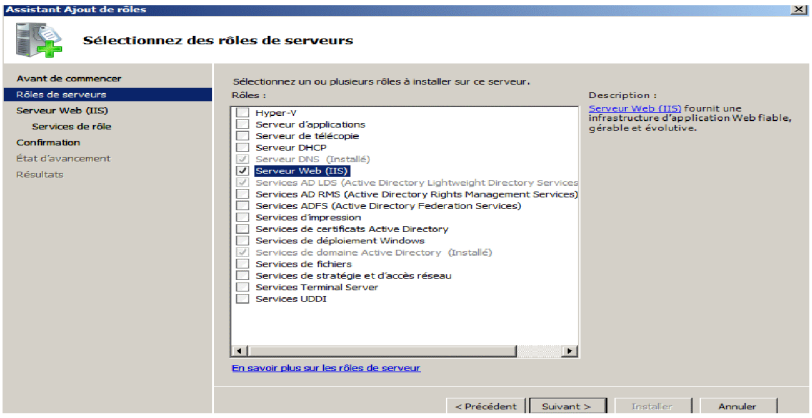

Figure C.01: Illustration 1.

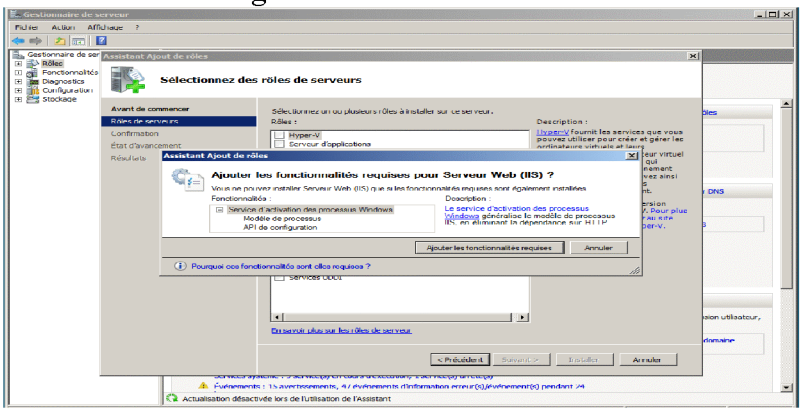

Figure C.02: Illustration 2.

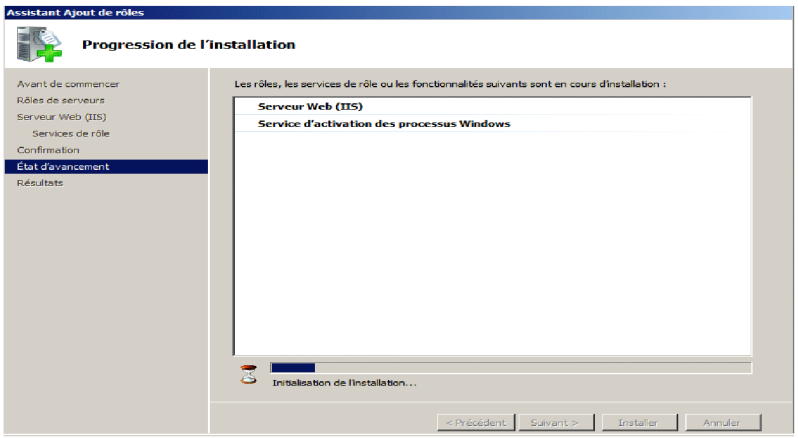

Figure C.03: Illustration 3.

C.2. Installation de la TMG

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

Figure C.04 : 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 :

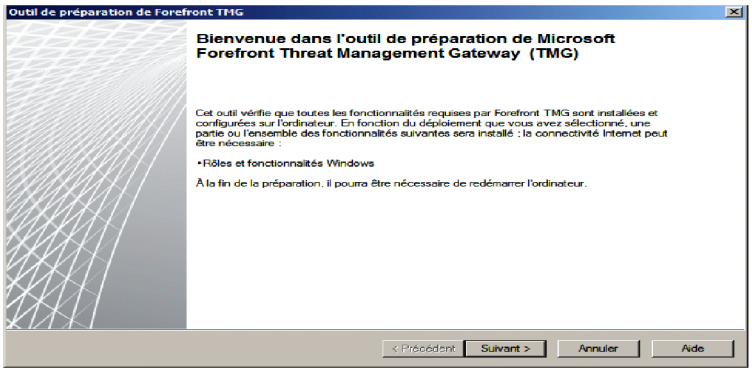

Figure C.05 : Lancement de l'exécution des outils de préparation.

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

Figure C.06: Le choix des fonctionnalités de la TMG.

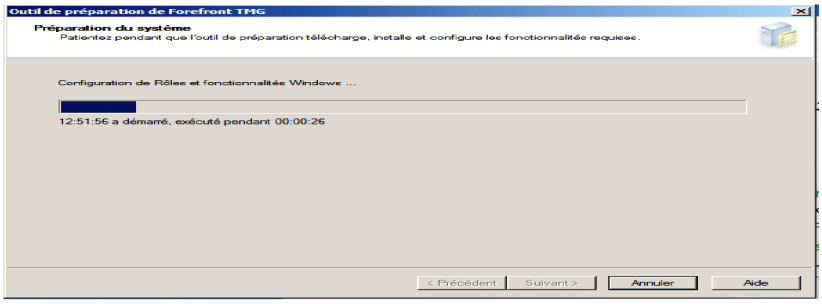

Figure C.07 : Préparation des outils.

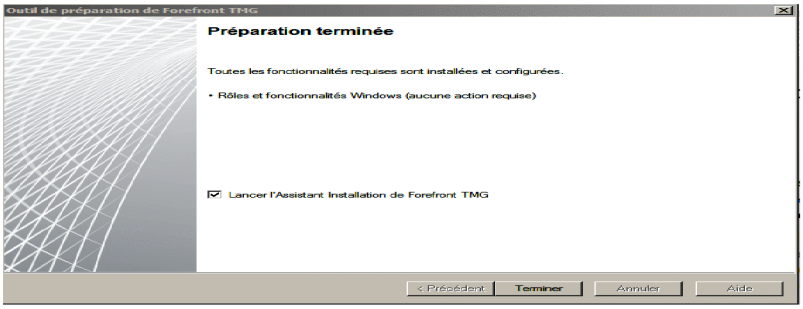

Figure C.08 : Fin de préparation des outils et lancement d'assistant d'installation de la TMG.

Voici la liste des rôles et fonctionnalités TMG qui seront activés après l'exécution de la deuxième étape :

- Network Policy Server.
- Routing and Remote Access Services.
- Active Directory Lightweight Directory Service Tools.
- Network Load Balancing Tools.
- Windows PowerShell.
- Microsoft .NET Framework 3.5 SP1.
- Windows Web Services API.
- Microsoft Windows Installer 4.5.
- Microsoft Chart Controls for Microsoft .NET Framework 3.5 and 3.5 SP1.

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

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

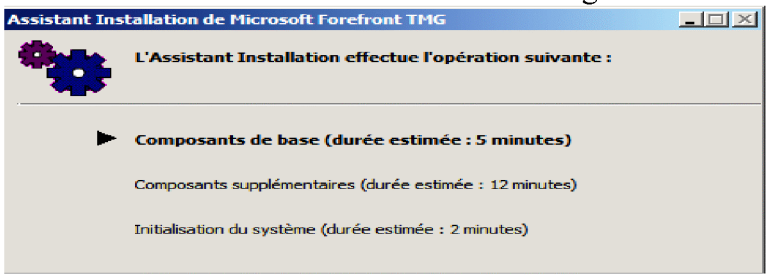

Figure C.09 : Assistant d'installation de la TMG.

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

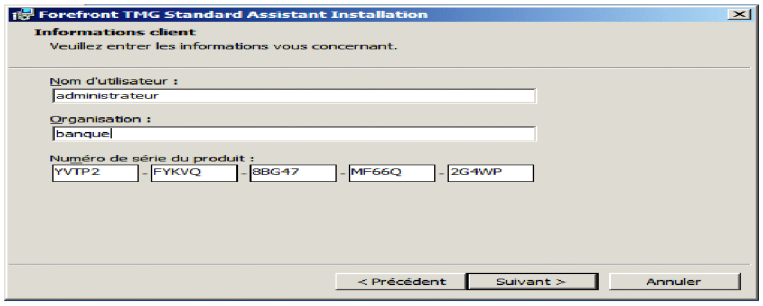

Figure C.10 : Validation de la licence.

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.

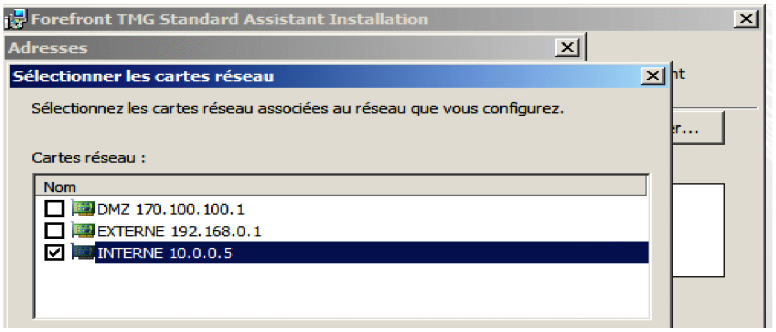

Figure C.11 : Sélection des cartes réseau.

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.

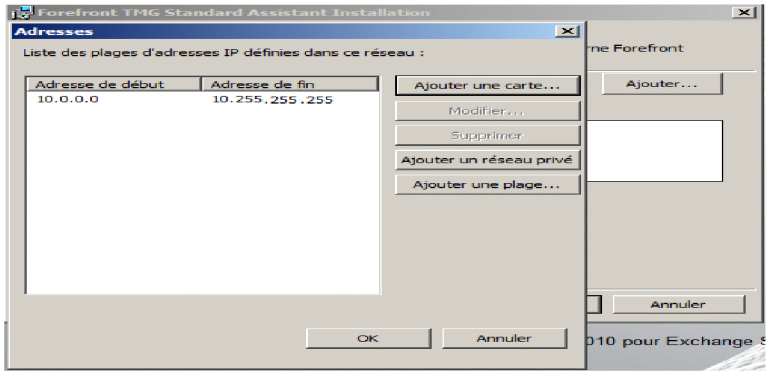

Figure C.12 : Liste de la plage des valeurs.

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

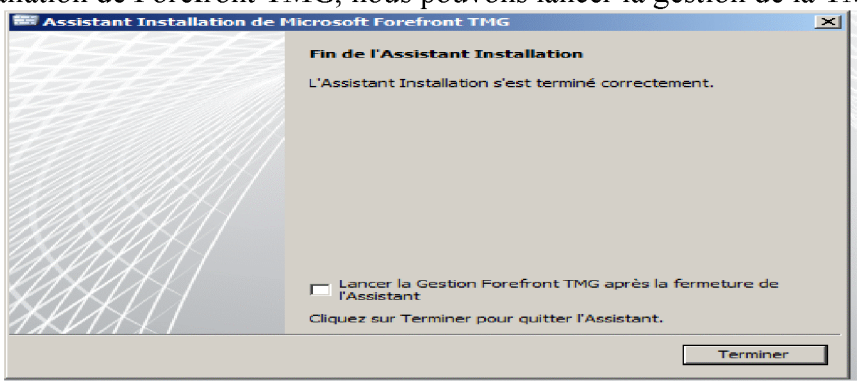

Figure C.13 : Fin d'assistant d'installation.

C.3. 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 C.14: Lancement d'installation de l'Exchange.

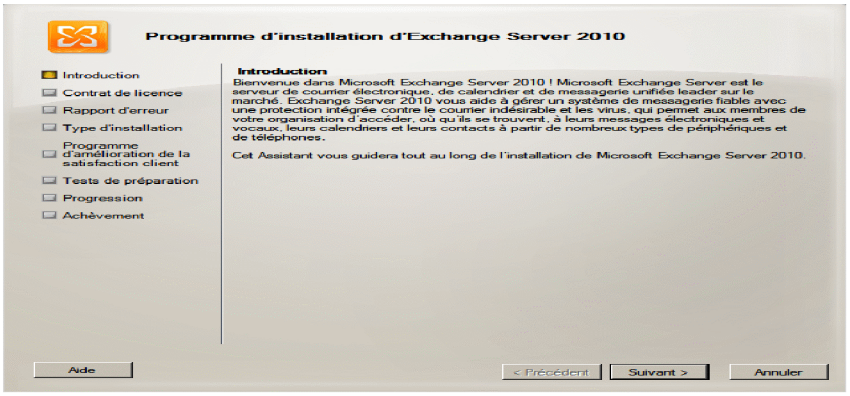

Figure C.15: Introduction.

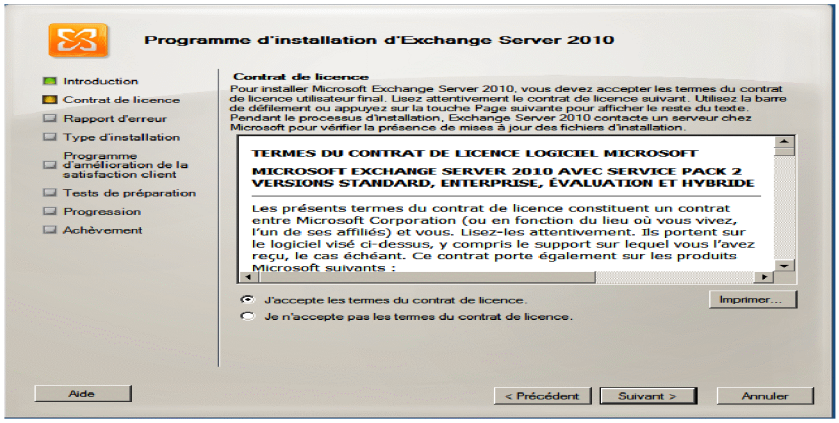

Figure C.16: Acceptation de la licence.

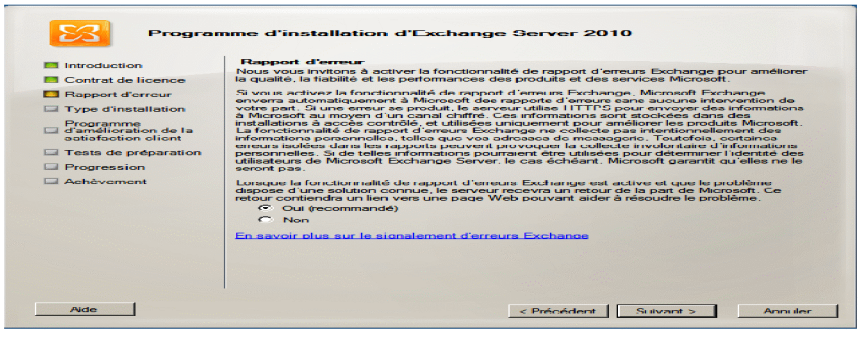

Figure C.17: Le choix de rapport d'erreur.

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.

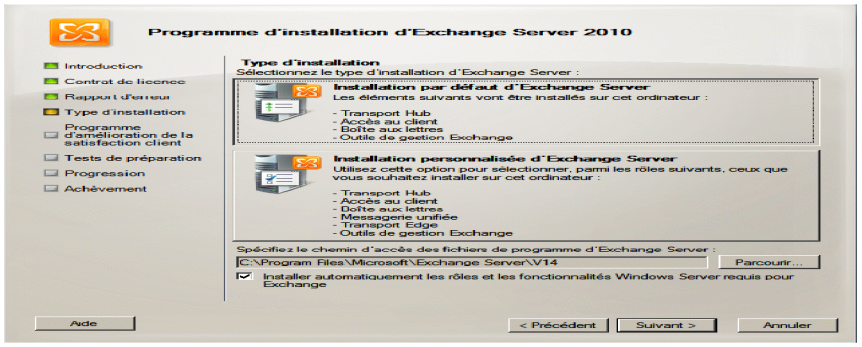

Figure C.18: Le choix de type d'installation.

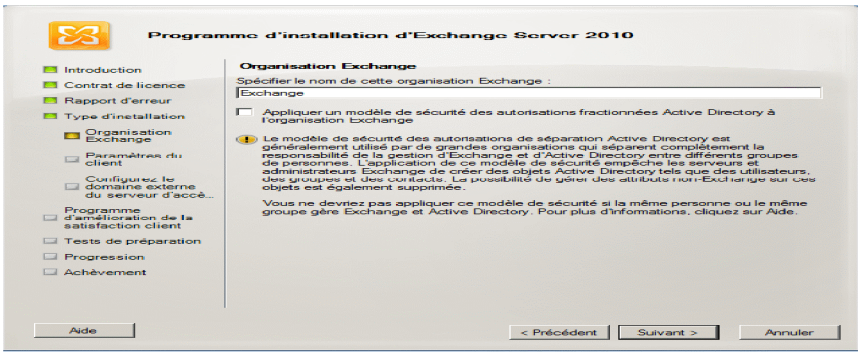

Figure C.19 : Spécification de nom de l'organisation.

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 la banque n'a pas ce genre de clients donc nous avons fait le choix correspondant.

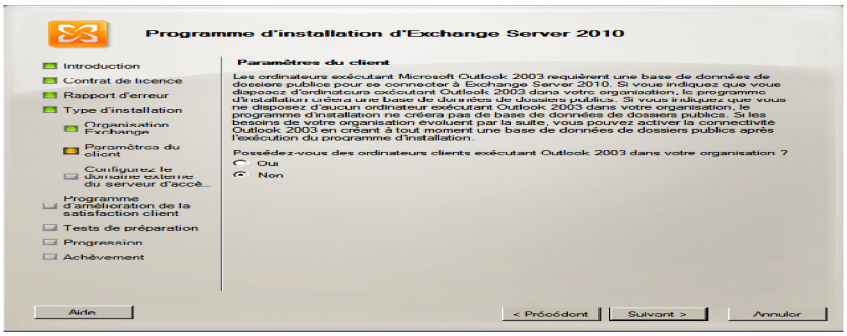

Figure C.20 : Paramètre client.

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

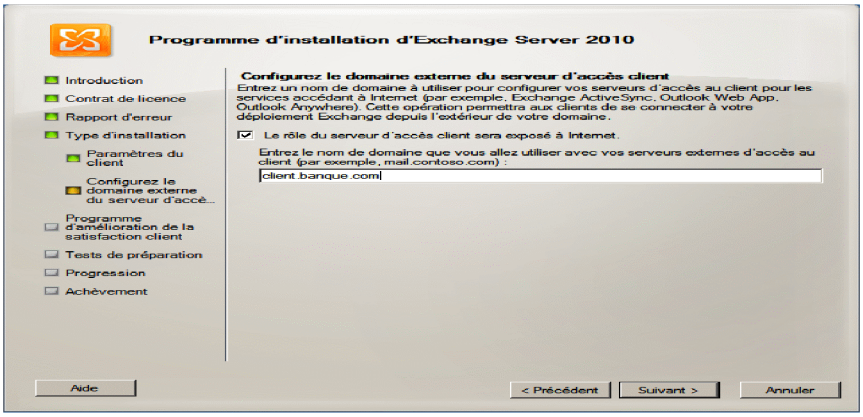

Figure C.21: Configuration de domaine externe du serveur d'accès client.

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

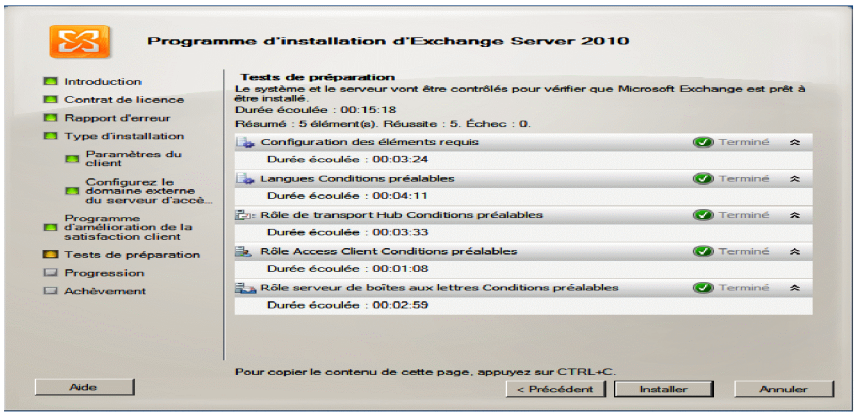

Figure C.22: Les tests de préparation.

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 1h09mn04s à s'installer.

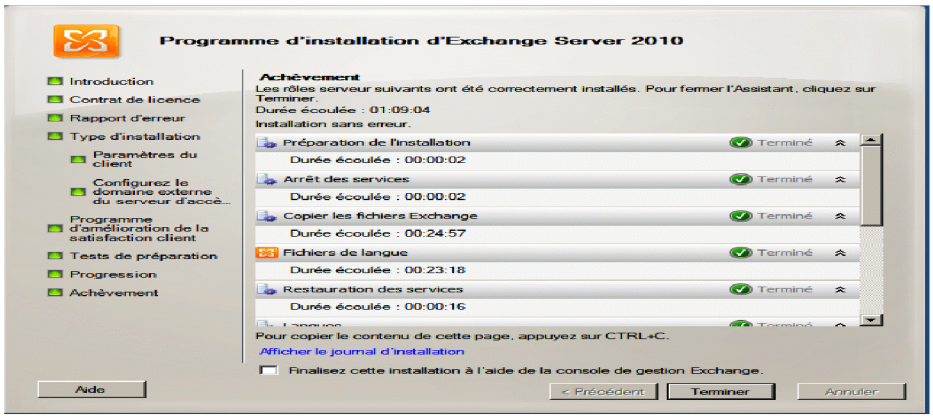

Figure C.23 : Achèvement.

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.

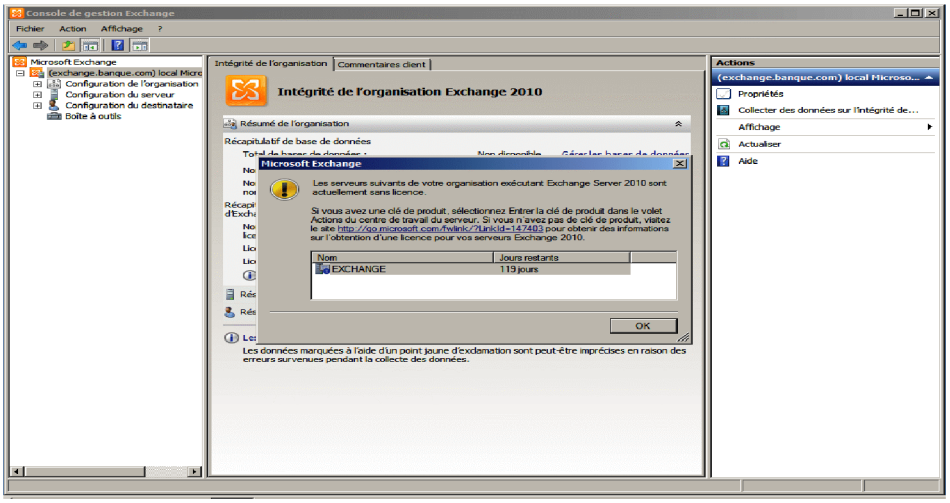

Figure C.24: La console de gestion Exchange.

C.4. Les réseaux locaux de stockage (SAN)

Les réseaux SAN sont des réseaux de haute performance destinés à livrer des blocs de données entre des serveurs et des sous-systèmes de stockage. Du point de vue du système d'exploitation, le stockage SAN semble être installé localement. La caractéristique la plus importante est que le stockage SAN ne se limite pas à un seul serveur, mais est disponible pour tous les serveurs. Ainsi le stockage peut être déplacé d'un serveur à un autre, mais en dehors des systèmes de fichier cluster, il n'est pas accessible par plusieurs serveurs en même temps. Les SAN sont généralement de deux types Fibre Channel et iSCSI.

Et comme notre objectif est de sécuriser l'architecture réseau nous avons préféré d'implémenter l'iSCSI qui possède une connectivité à grande distances et une sécurité intégrée.

C.4.1. Les réseaux iSCSI SAN

iSCSI(Internet SCSI) est un standard industriel développé pour permettre une transmission de commande via un réseau Ethernet en utilisant le protocole TCP/IP. Les serveurs communiquent avec les périphériques iSCSI grâce à un agent logiciel installé localement appelé initiateur iSCSI. Ce dernier exécute des demandes et reçoit des réponses d'une cible iSCSI, qui peut elle-même être le périphérique de stockage final ou un périphérique intermédiaire comme un commutateur.

a. Installation de Starwind iSCSI SAN

Dans cette section nous présenterons les différentes étapes d'installation du logiciel StarWind iSCSI SAN sur un serveur membre de **banque.com** que nous avons nommé **BDD**, conçu pour le stockage partagé sous l'environnement WMware.

Au lancement du fichier d'installation de StarWind, l'assistant d'installation apparaît.

Figure C.25: Lancement d'installation du Starwind iSCSI SAN.

Cliquer sur suivant et accepter la licence

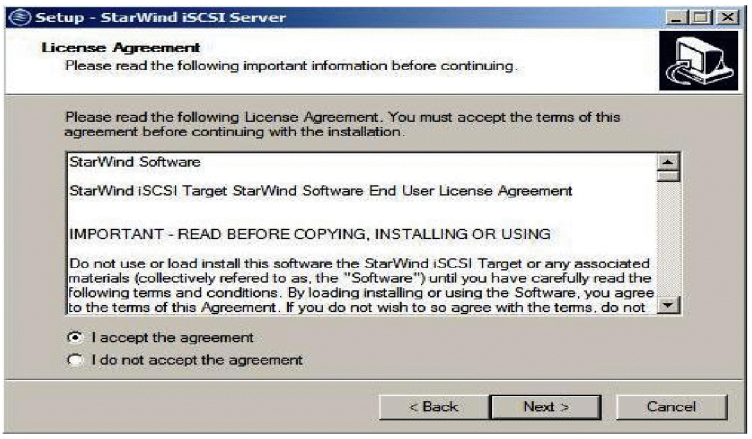

Figure C.26: Acceptation de licence.

La fenêtre qui suit montre les différentes caractéristiques et avantages proposée par le StarWind. Ensuite nous choisissons l'emplacement d'installation.

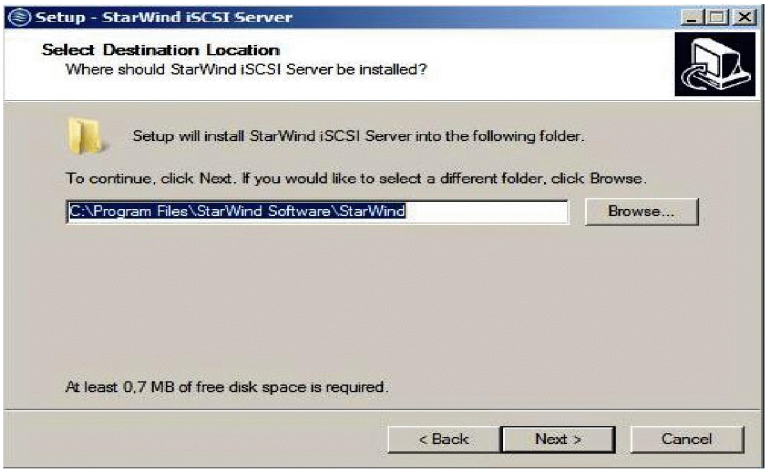

Figure C.27 : Sélection de l'emplacement d'installation.

Ensuite nous spécifions le type d'installation, **StarWind iSCSI Service** pour l'accès distant aux serveurs ou **StarWind Management Console** qui fournit une interface graphique pour la

gestion et le contrôle de stockage. Nous avons alors choisi **Full installation** qui combine ces deux types d'installation.

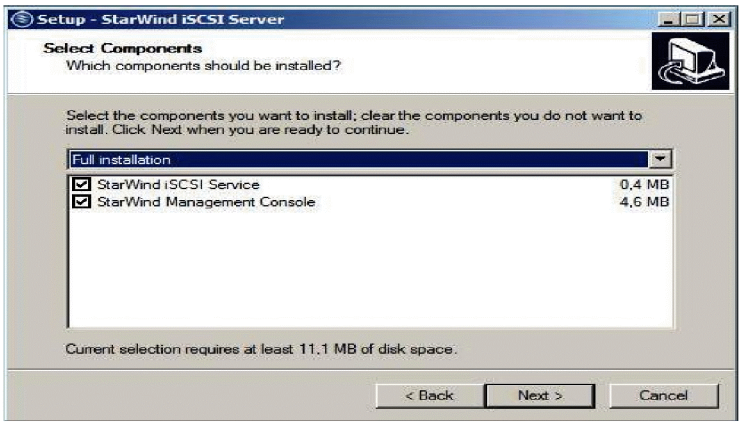

Figure C.28 : Sélection de type d'installation.

Après avoir complété le processus d'installation, nous précisons le type de clé à utiliser, dans notre cas c'est la free. .

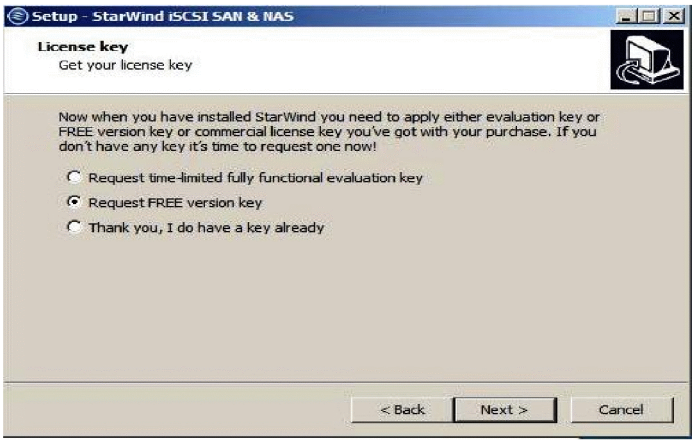

Figure C.29: Le choix de la clé de la licence.

Le choix suivant consiste à sélectionner la solution StarWind dont on a besoin, donc nous spécifions Starwind iSCSI SAN & NAS.

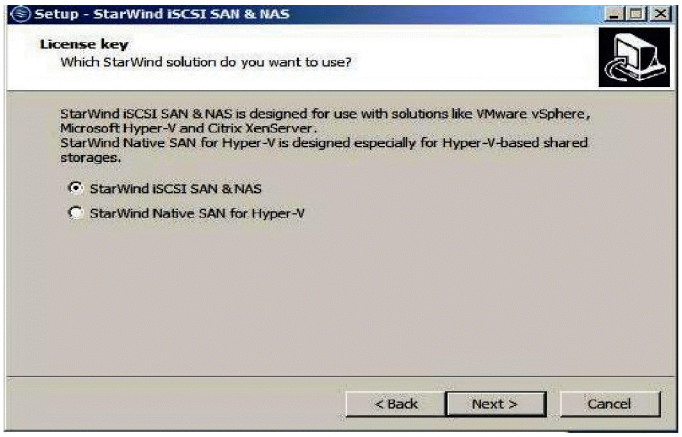

Figure C.30 : Le choix de solution à implémenter.

Apres avoir téléchargé le fichier de la clé gratuite, nous indiquons son emplacement à l'assistant d'installation.

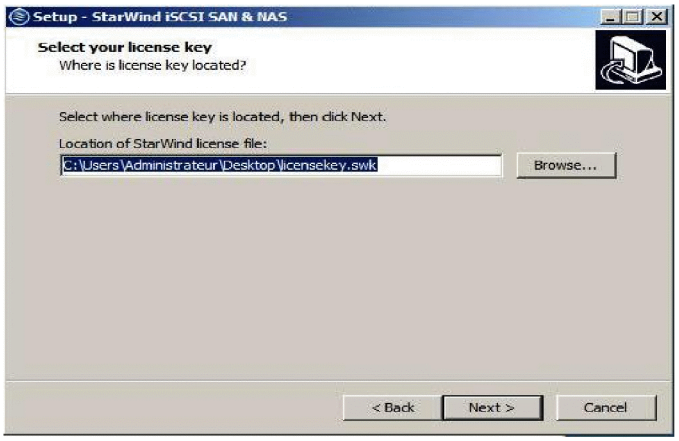

Figure C.31 : Spécification de l'emplacement de fichier de la clé.

L'étape suivante nous résume les informations sur le fichier de la licence.

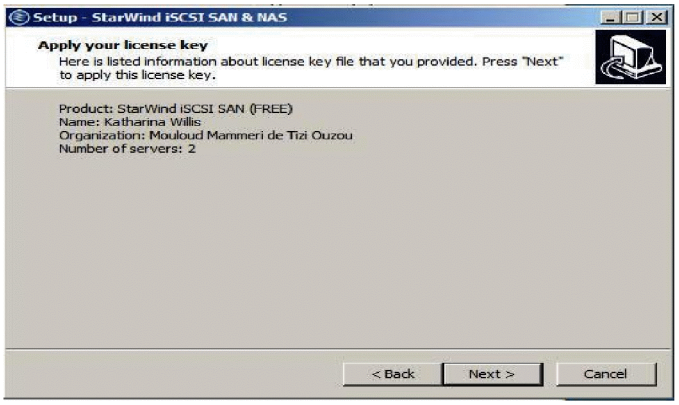

Figure C.32: Le résumé de fichier de licence.

Ensuite nous vérifions nos paramètres, nous pouvons les changer en cliquant sur Back ou bien les confirmer en cliquant sur Install.

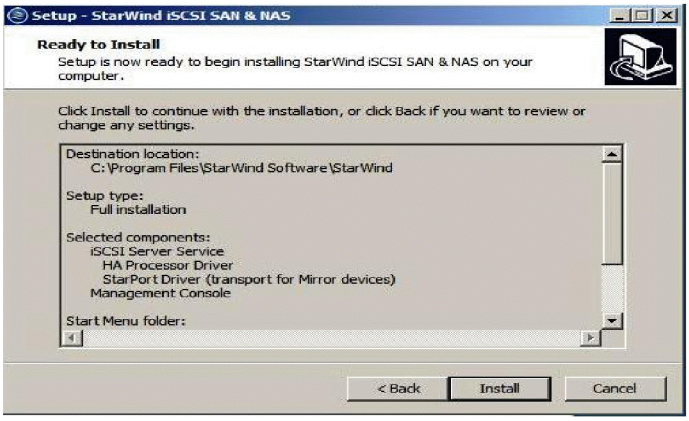

Figure C.33 : Vérification des paramètres.

Et pour compléter l'installation nous cliquons sur finish.

b. Création de disque virtuel

A son lancement Starwind contient par défaut un login **root** et un mot de passe **starwind,** une fois entrées avec ces paramètres, nous les avons modifié pour des raisons de sécurité.

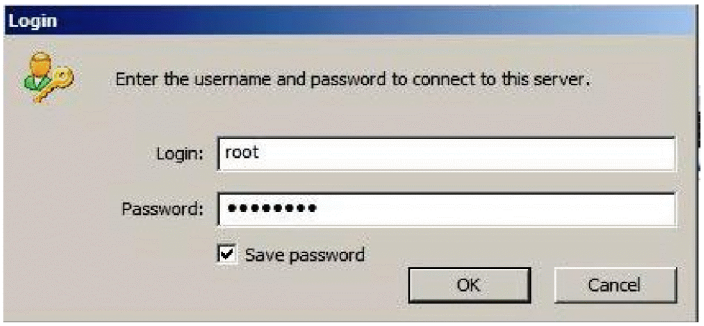

Figure C.34: Authentification de Starwind par défaut.

Pour créer des disques virtuels, dans le menu de la console Starwind nous cliquons sur **Add Device**. Une fenêtre apparaît avec la liste des équipements pour choisir celui dont en a besoin, alors nous avons choisi **Virtuel Hard Disk**.

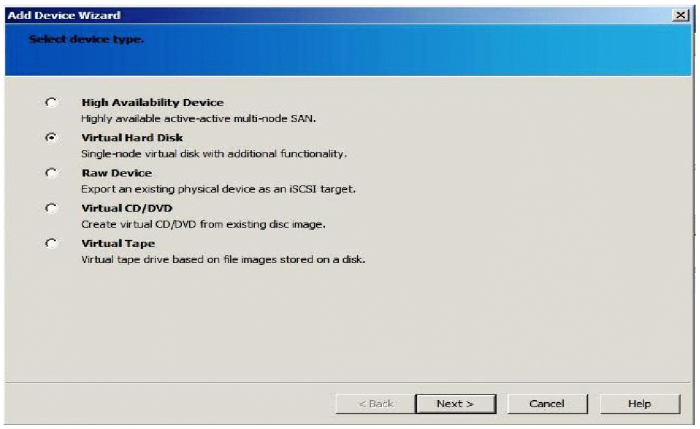

Figure C.35 : La sélection de type de l'équipement à créer.

Ensuit image file qui nous permet d'utiliser des fichiers disque comme un moyen de stockage.

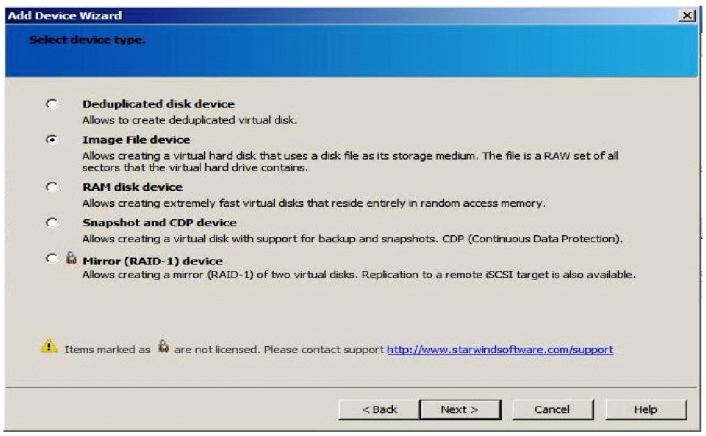

Figure C.36: Le choix du l'image file.

Après nous choisissons la méthode de création du disque.

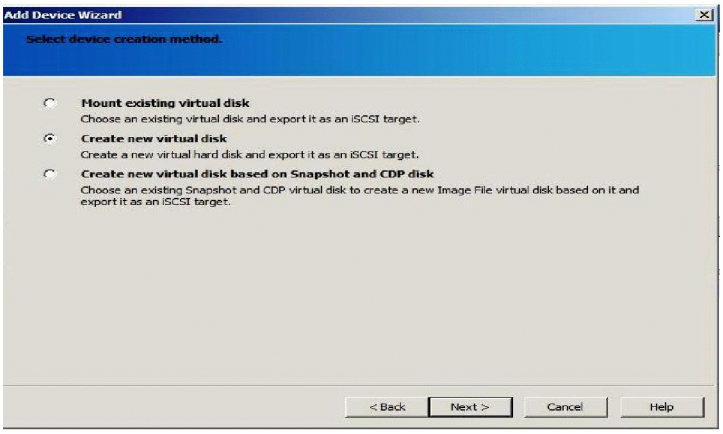

Figure C.37: La méthode de création de disque virtuel.

Dans l'étape qui suit, nous spécifions l'emplacement, le nom et la taille du disque virtuel.

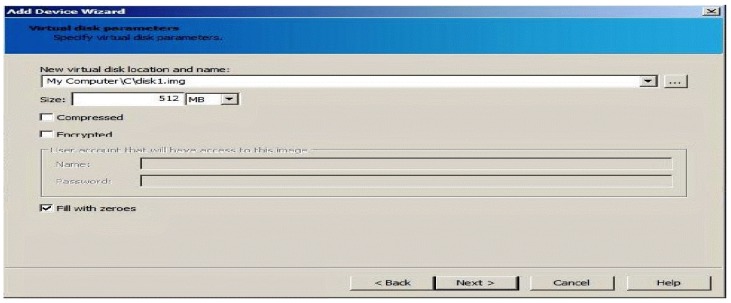

Figure C.38: Spécification des paramètres de disque virtuel.

Le quatrième paramètre nous donne le choix entre trois options, **Compressed** permet de compresser le disque virtuel, **Encrypted** pour authentifier l'accès au disque virtuel et **Full with zeroes** utilisé pour la sécurité. Cette derniére détecte quand les clients non confiés se connectent au disque virtuel.

Maintenant nous spécifions les paramètres du disque virtuel, nous sélectionnons le mode Asynchronous car il est recommandé pour le RAID 5. Pour avoir plus d'informations sur le paramétrage de disque cliquer sur help.

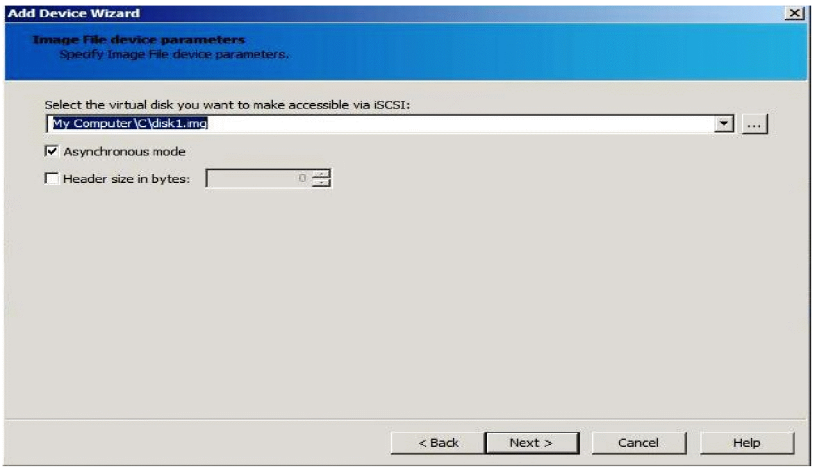

Figure C.39 : Le paramétrage de l'image file.

L'étape suivante consiste à paramétrer le cache pour stocker les données en mémoire.

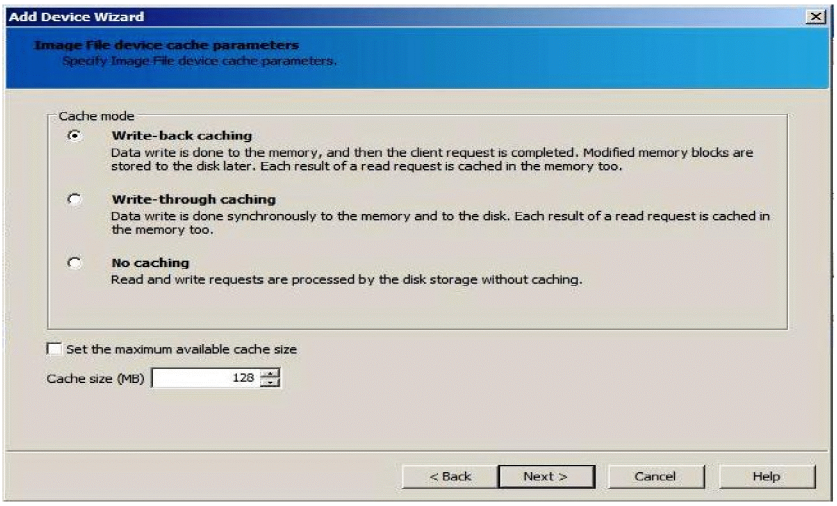

Figure C.40 : Le paramétrage de cache.

Ensuite, nous déterminons les paramètres de la cible et cochons la permission de clustering.

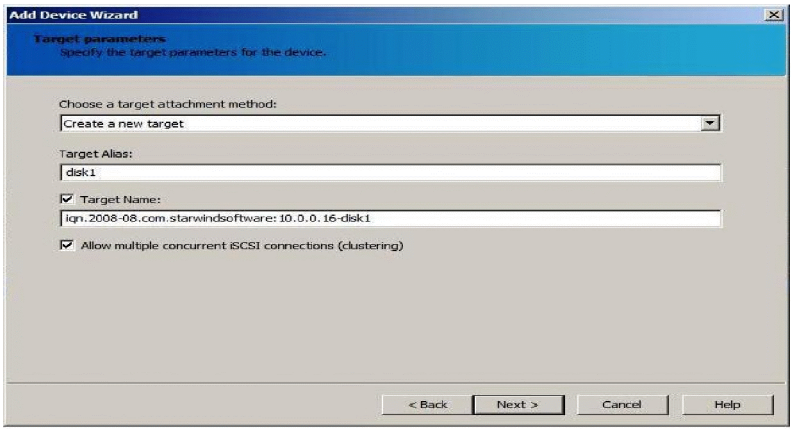

Figure C.41 : Spécification des paramètres de la cible.

Puis nous vérifions l'ensemble de nos paramètres et revenons en arrière en cas de modification à faire sinon continuons pour valider notre création en cliquant sur finish.

C.5. Installation et configuration de Kaspersky administration kit 8

Kaspersky Administration Kit 8 est une application développée pour exécuter, de manière centralisée, les principales tâches d'administration de la sécurité des ordinateurs du réseau d'une entreprise. Il repose sur les applications faisant partie de la suite Kaspersky Business Optimal et Kaspersky Corporate Suite. Il est compatible avec toutes les configurations de réseaux qui utilisent le protocole TCP/IP. Il est aussi un outil pour administrateurs de réseaux d'entreprise et pour les responsables de sécurité antivirale.

Figure C.42: Kaspersky Administration Kit.

L'application Kaspersky Administration Kit se présente sous forme des composants principaux :

- ✓ **Serveur d'administration**: c'est un entrepôt centralisé d'informations sur les applications Kaspersky Lab installées sur le réseau local de la société et un outil efficace de gestion de ces applications.
- ✓ **Agent d'administration**: coordonne les interactions entre le Serveur d'administration et les applications Kaspersky Lab installées sur un poste spécifique du réseau (lui-même un poste de travail ou un serveur). Ce composant est unique pour toutes les applications Windows de la gamme des produits Kaspersky Open Space Security.
- ✓ **Console d'administration**: fournit l'interface utilisateur nécessaire pour les services administratifs du Serveur et de l'Agent. Le module gestionnaire est conçu comme une extension MMC (Microsoft Management Console).

L'installation de Kaspersky requière la configuration logicielle suivante :

C.5.1. Configuration logicielle

- ✓ Microsoft Data Access Components (MDAC) de version 2.8 ou supérieure ou Windows DAC 6.0.
- ✓ Système de gestion des bases de données : Microsoft SQL Express 2005, Microsoft SQL Express 2008 R2, Microsoft SQL Express 2008 R2 ; Microsoft SQL Server 2005, Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2 ou MySQL Enterprise.
- ✓ Microsoft Windows Server 2003 et supérieur ; Microsoft Windows Server 2003 x64 et supérieur ; Microsoft Windows Server 2008 ; Microsoft Windows Server 2008 déployé en mode Server Core ; Microsoft Windows Server 2008 x64 avec Service Pack 1et tous les SP actuels (pour Microsoft Windows Server 2008 x64 Microsoft Windows Installer 4.5 doit être installé) ; Microsoft Windows Server 2008 R2 ; Microsoft Windows Server 2008 R2 déployé en mode Server Core ; Microsoft Windows XP Professional avec Service Pack 2 et

supérieur ; Microsoft Windows XP Professional x64 et supérieur ; Microsoft Windows Vista x64 avec Service Pack 1 et supérieur, Microsoft Windows Vista x64 avec Service Pack 1et tous les SP actuels (pour Microsoft Windows Server 2008 x64 Microsoft Windows Installer 4.5 doit être installé) ; Microsoft Windows 7.

Après avoir effectué cette configuration, nous lançons l'exécutable Kasperky administration kit 8.

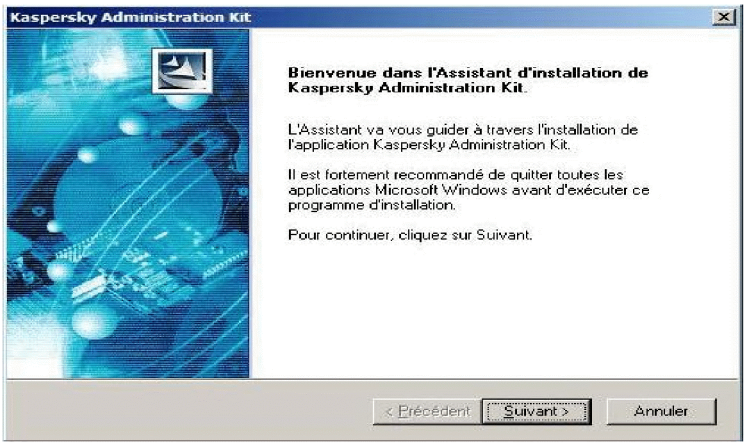

Figure C.43 : L'assistant d'installation de Kaspersky Administration kit.

Nous indiquons le répertoire d'installation des composants. Il s'agit par défaut de **<Disque>:\Program Files\Kaspersky Lab\Kaspersky Administration Kit**. Si ce répertoire n'existe pas, il sera créé automatiquement. Cliquons sur **Parcourir** pour sélectionner un autre répertoire. Sélectionnons ensuite les composants de Kaspersky Administration Kit que nous désirons installer :

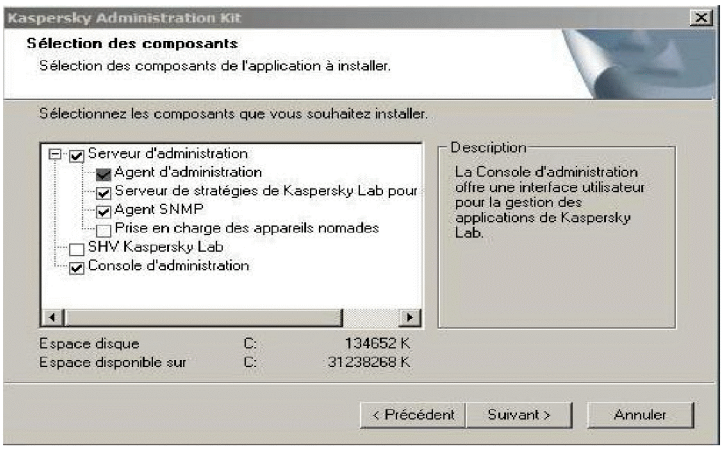

Figure C.44 : Sélection des composants.

Notons qu'il est interdit d'annuler l'installation de l'Agent d'administration, il s'installe toujours. Définissons ensuite la taille du réseau, cela permettra de configurer l'interface de l'application et les paramètres de fonctionnement de manière optimale.

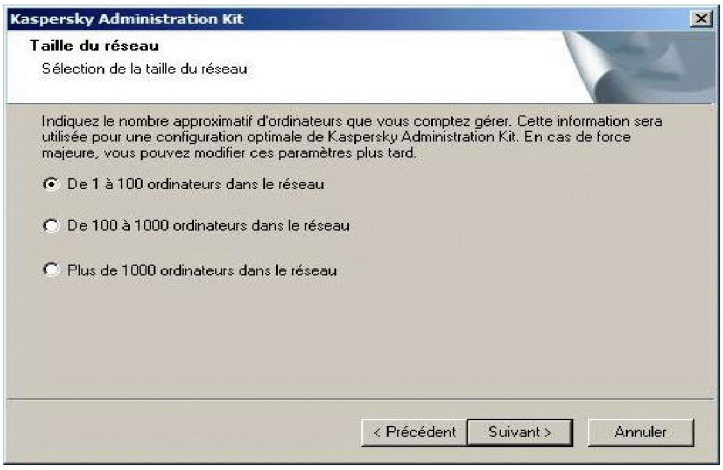

Figure C.45 : Spécification de la taille du réseau.

Définissons le compte utilisé pour lancer le Serveur d'administration en tant que service sur l'ordinateur

- ✓ **Compte du système local** : le Serveur d'administration est en cours d'exécution avec les privilèges Compte du système local.
- ✓ **Compte d'utilisateur** : le Serveur d'administration sera lancé sous un compte utilisateur inclus dans le domaine. Dans ce cas, le Serveur d'administration initiera toutes les opérations avec les privilèges de ce compte. A l'aide du bouton Parcourir définissons l'utilisateur, dont le compte sera utilisé, et saisissons le mot de passe.

Comme nous voulons déployer cet anti-virus sur l'ensemble de notre foret, nous choisissons Compte utilisateur.

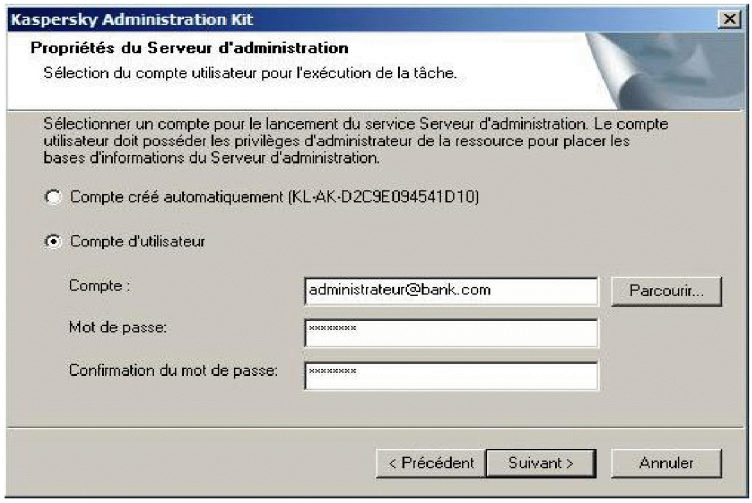

Figure C.45: Propriété de serveur d'administration.

Dans l'étape suivante nous définissons la ressource **Microsoft SQL Server (SQL Express)** ou **MySQL**, qui sera utilisée pour le placement de la base de données du Serveur d'administration.

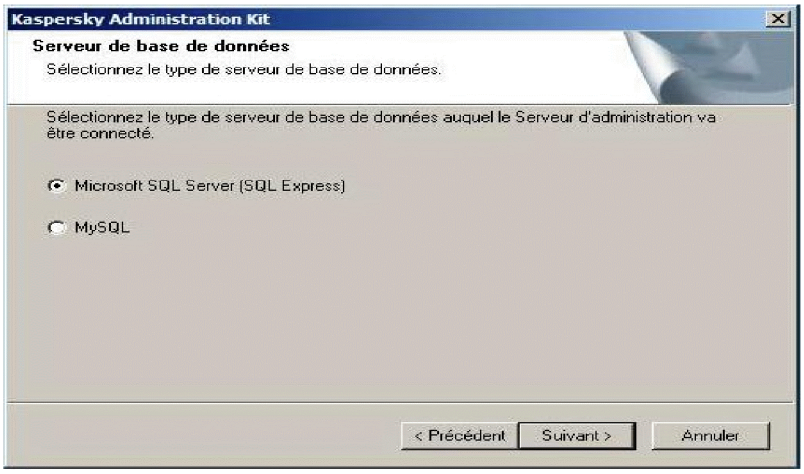

Figure C.46: La sélection du type de la base de données.

Comme nous avons sélectionné Microsoft SQL Server, nous saisissons le nom du serveur **SQL**, le nom de la base de données qui sera crée pour le placement de l'information du Serveur d'administration.

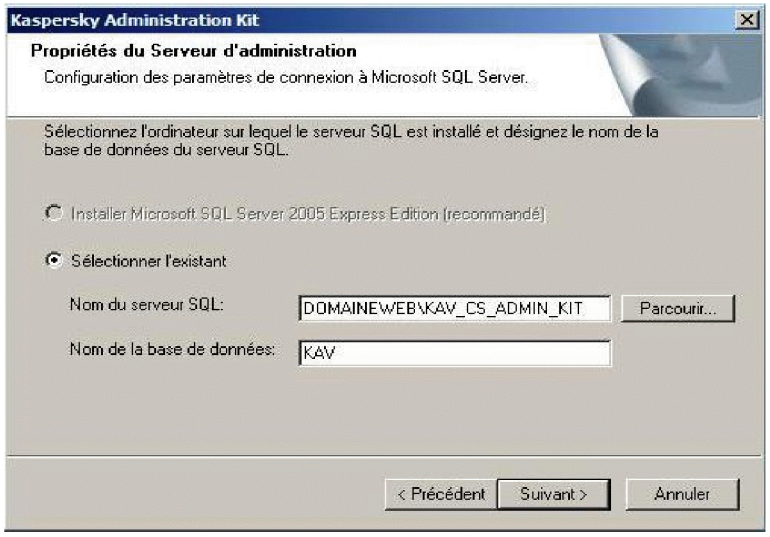

Figure C.47: Propriétés du serveur d'administration.

Définissons ensuite la méthode d'authentification à utiliser lors de la connexion du Serveur d'administration au serveur SQL.

Pour SQL Express ou Microsoft SQL Server nous pouvons sélectionner une de deux options :

- ✓ **Mode d'authentification Microsoft Windows** : dans ce cas lors de la vérification des privilèges le compte sera utilisé pour le lancement du Serveur d'administration.
- ✓ **Mode d'authentification du serveur SQL** : le compte indiqué ci-après sera utilisé dans le cas de sélection de ce mode.

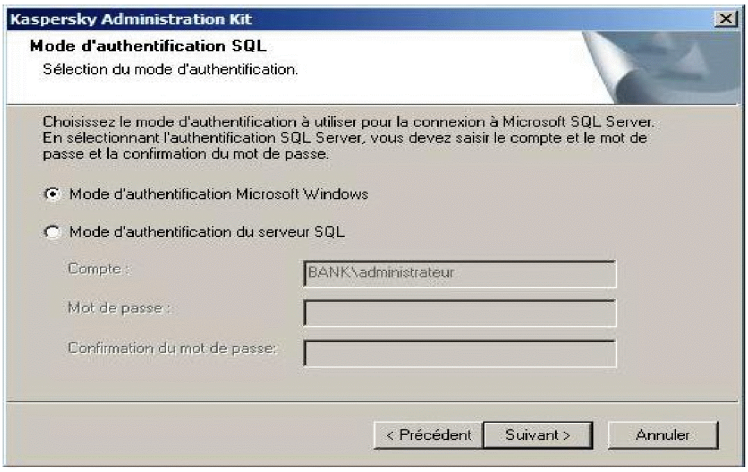

Figure C.48: Sélection de mode d'authentification SQL.

Puis nous déterminons l'emplacement et le nom du dossier public qui sera utilisé pour :

- ✓ La sauvegarde des fichiers pour l'installation à distance des applications (les fichiers sont copiés sur le Serveur d'administration lors de la création des paquets d'installation).
- ✓ Le stockage des mises à jour copiées depuis la source sur le Serveur d'administration.

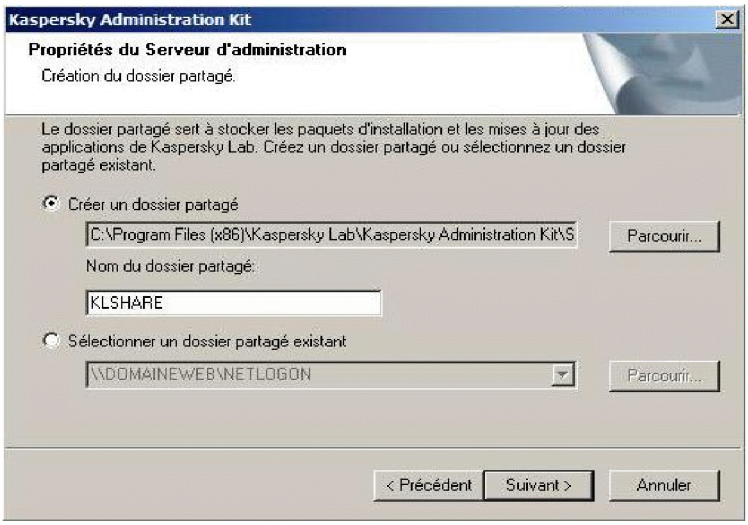

Figure C.49: Création du dossier partagé.

Définissons ensuite les paramètres de connexion au Serveur d'administration:

- ✓ Numéro de port pour la connexion au Serveur d'administration. Par défaut, il s'agit du port 14000.
- ✓ Numéro du port SSL, utilisé pour établir une connexion sécurisée avec le Serveur d'administration, en utilisant le protocole SSL. Par défaut, il s'agit du port 13000.

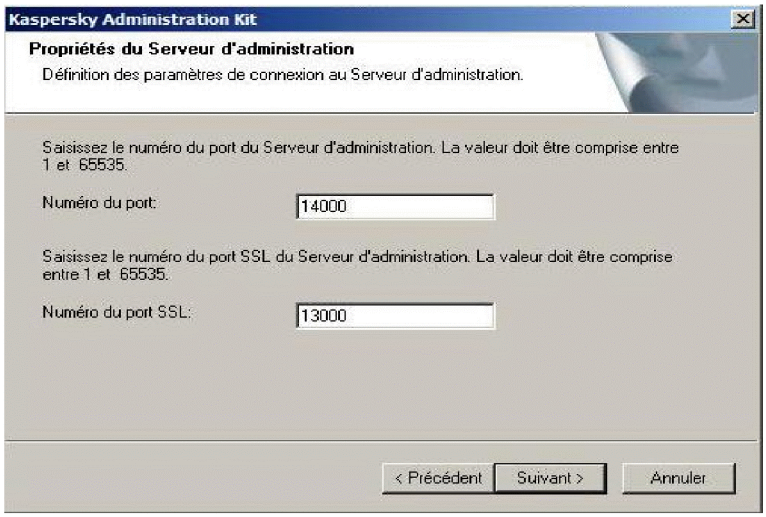

Figure C.50 : Paramétrage de la connexion du serveur d'administration.

Puis nous spécifions l'adresse du Serveur d'administration, en choisissant l'une des trois options :

- ✓ **Nom DNS** : Cette option est utilisée dans le cas où le serveur DNS est présent dans le réseau, et les postes clients peuvent l'obtenir à l'aide de l'adresse du Serveur d'administration.
- ✓ **Nom NETBIOS** : Il est utilisé si les postes clients obtiennent l'adresse du Serveur d'administration via le protocole NetBIOS, ou si un serveur WINS est présent dans le réseau.
- ✓ **Adresse IP** : Cette option est utilisée uniquement si le serveur a une adresse IP fixe qui ne sera pas modifiée par la suite.

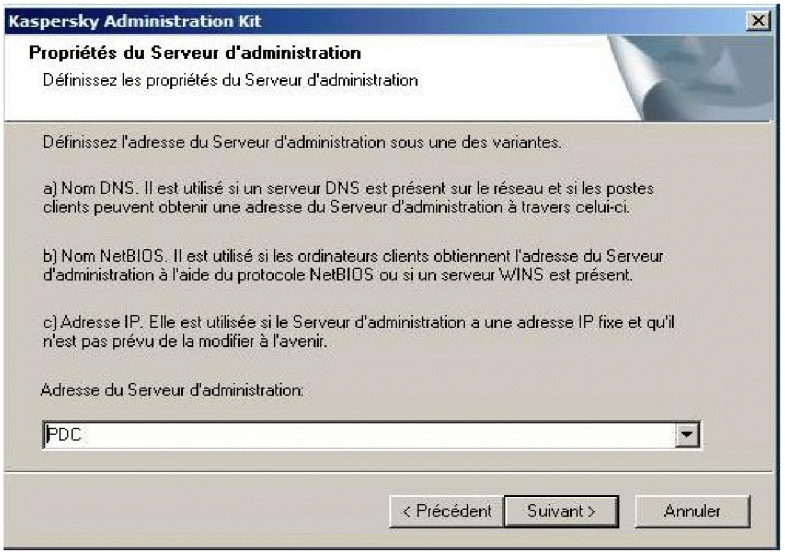

Figure C.51: Définition des propriétés de serveur d'administration.

Puis nous validons la fin de l'installation.

Bibliographie

Bibliographie

[01] ACISSI, Sécurité informatique Ethical Hacking apprendre l'attaque pour mieux se défendre, ENI, 2012.
[02] Solange Ghernouatu-Hélie, Sécurité informatique et réseaux, Dunod, 2008.
[03] Robert-Lingeon, Guide de la sécurité des systèmes d'information, Centre national de la recherche scientifique, 1999.
[04] Vincent Remazeilles, La sécurité des réseaux avec CISCO, Eni, 2009.
[05] Jérôme Delduca, La sécurité informatique en mode projet - Organisez la sécurité du SI de votre entreprise, ENI, 2010.
[06] Bruno M, La sécurité informatique CERAM, « Fondamentaux des sciences de l'information ».
[07] Université de Nice, Le livre sécuritéinfo.com, 2010.
[08] Thierry Evangelista, Les systèmes de détection d'intrusions informatiques, Dunod, 2004.
[09] Guillaume Desgeorge, La sécurité des réseaux, 2000.
[10] Eric Filiol, Les virus informatiques, Springer Verlag, 2009.
[11] Gary Hallen, CCNP security IPS 642-627 quick reference, Cisco Presse Library of Bolovan Calin Borgdan, 2011
[12] Laurent Bloch, Cristoph Wolfhugel, Sécurité informatique principes et méthodes, Eyrolles, 2007.
[13] Guy Pujolle, Les réseaux, Eyrolles, 2003.
[14] Roger Sanchez , Les réseaux locaux virtuels, 2006.
[15] José Dordoigne, Réseaux informatique, notions fondamentales, 2011.
[16] Guy Pujolle, Les réseaux, Eyrolles, 2008
[17] David Burgermeister, Les systèmes de détection d'intrusions, 2006.
[18] Pierre Jaquet, Lavoisier, Les réseaux et l'informatique de l'entreprise, 2003.
[19] FreeRaduis, Serge Bonderes, Authentification réseau avec RADIUS 802.1X, EAP, Eyrolles 2007.
[20] Amakou M'BATA, Olivier PERSENT, Firewall, Pare-feux, Mur de feu, 2006
[21] Joseph Steinberg, SSL VPN accès web et extranets sécurisés, Eyrolles, 2006.
[22] Avoledo Mickaël, Pare-feu Cisco PIX 515^{E}, 2009.
[23] Cisco Systém, Description des Serveurs de Sécurité Adaptatifs dela gamme Cisco ASA 5500 fiche technique, INC, 2007
[24] Vladimir Holostov, Forefront TMG 2010 Common Criteria Evaluation Guidance Documentation Addendum Microsoft Forefront Threat Management Gateway Team, Microsoft Corp, 2010.
[25] Yuri Diogenes, Dr Tom Shinder, Forefront Threat Management Gateway (TMG), Micrsoft Forefront TMG Team, Administrator's Companion, 2010
[26] Fortinet, Guide d'installation des FortiGate-100A Version 3.0MR1,Fortinet, 2006
[27] Kaspersky Lab ZAO, Kaspersky Administration Kit 8 Administrator's Guide, Kaspersky Lab, 2009

Webographie

http://quebec.huffingtonpost.ca/2013/02/20/apple-pirate-hackers-facebook-qui-sera-le-prochain_n_2724599.html

http://fr.wikipedia.org/wiki/Chronologie_des_%C3%A9v%C3%A9nements_impliquant_Anonymous

http://www.micropaiement-sms.com/google-apple-yahoo-paypal-microsoft-pirates/

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

www.fortinet.com

www.cisco.com/go/security

www.cisco.com/go/evpn

www.Technet.com

http://www.cisco.com/en/US/docs/security/pix/pix62/quick/guide/501quick.html

http://www.securecomputing.com/

http://www.mcafee.com/us/products/firewall-enterprise.aspx

http://www.fortinet.com/products/fortigate/index.html

http://technet.microsoft.com/library/ff355324.aspx

http://www.kaspersky.com/fr/administration_kit