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
EPARTEMENT D'INFORMATIQUE

Mémoire de fin d'études

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

Option : Réseaux Mobilité &Système Embarqué.

Thème :

Mise en place d'une solution de Sécurité d'un réseau informatique. Cas d'une Banque

Proposé et dirigé par :

Mr : A.Dib

Mr : M.Kibouh

Réalisé par :

Mlle: DIBOUN Terkouia

Mlle :DAHMANE Hakima

Promotion: 2013/2014

Remerciements

Nous tenons à exprimer notre profonde gratitude à notrepromoteur MrA. DIB et notre encadreur MrM.KIBOUH de l'école 2INT Partners, pour leurs suivis et leurs conseils précieux tout au long de l'élaboration de notremémoire.

Notre parfaite considération à l'ensemble des enseignantsqui ontcontribué à notre formation.

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

Enfin, nous tenons à remercier toutes les personnes quiont contribué de près ou de loin à la réalisation de ce modeste travail.

Dédicace

Avec un énorme plaisir, un cœur ouvert et une immense joie, que je dédie mon travail à mes très chers, respectueux et magnifique parents qui m'ont soutenus tout au long de ma vie ainsi à mes sœurs et mes frères

Et en particulier a ma binôme Diboun Terkouia et toute la promo RMSE 2013/2014

A toute personnes qui m'ont encouragé ou aidé au long de mes études

Hakima

Dédicaces

Je dédie ce modeste travail à :

Mes très chers parents, qui m'ont soutenu tout au long de mes études.

Mes frères.

Mon fiancé ainsi que sa famille.

Toute ma famille.

Mes chers amis(e)

Et toute notre promotion Master II RMSE 2014.

terkouia

Sommaire

Table des figures

Table des figures

Table des figures

Table des figures

Glossaire

AAA	Authentication Authorization Accounting
ACE	Access Control Entries
ACL	Access Control List
AH	Authentication Heade
AIM	Adaptive Identification and Mitigation
AIP SSM	Advanced Inspection and Prevention Security Services Module
API	Application Programming Interface
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
DHCP	Dynamique Host Configuration Protocol
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
ID	Identify
IT	Information Technology
IDS	Intrusion Detection Services
IETF	Internet Engineering Task Force
IIS	Internet Information Services
IMAP	Internet Message Access Protocol
IOS	Inter-network Operating System
IP	Internet Protocol
IPsec	Internet Protocol Security
IPS	Intrusion Prevention Services

Glossaire

ISA	Internet Security and Acceleration
ISO	International Organization for Standardization
KIPS	Kernel Intrusion Prevention System
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
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
PAN	Personal Area Network
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
RFC	Request for Comments
RPV	Réseau privé virtuel
RPF	Reverse Path Forwarding
SSH	Secure Shell
SSL	Secure Socket Layer
SNMP	Simple Network Management Protocol

Glossaire

SMTP	Simple Mail Transfer Protocol
Spof	Single Point Of Failure
SQL	Structured Query Language
TCP	Transfer Control Protocol
Telnet	TELecommunication NETwork
TMG	Threat Management Gateway
UDP	User Datagram Protocol
URL	Uniform Resource Locator
URPF	Unicast Reverse Path Forwarding
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

L'informatique est la science du traitement rationnel de l'information, notamment par machines automatiques, considérée comme support des connaissances et des communications, dans les domaines technique, économique et social. La principale caractéristique de l'informatique c'est qu'elle est communicante par réseau.

Cependant, les réseaux informatiques des entreprises sont devenus indispensable dans la gestion, l'organisation, la production et la communication. Ils mettent en œuvre des données sensibles, les stockent, les partagent en interne et en externe. Cette ouverture vers l'extérieur permet aux entreprises d'augmenter leurs gains de productivité et de compétitivité mais d'un autre côté elle les conditionne.
Il est donc impossible de renoncer aux bénéfices de l'informatisation, d'isoler le réseau de l'extérieur, de retirer aux données leur caractère électronique et confidentiel. Les données sensibles de l'entreprise sont donc exposées aux actes de malveillance dont la nature et la méthode d'intrusion sont sans cesse changeantes.

Toutes pertes mènent à une catastrophe informatique qui a toujours des conséquences fâcheuses pour une entreprise.C'est pourquoi on doit mettre en place une politique de sécurité.

Notre travaille a pour but d'étudier les failles d'un réseau d'une banque et proposer des solutions aptes à les corriger afin d'augmenté sa sécurité.

Dans notre démarche, il sera donc question pour nous, de présenter dans le chapitre I l'étude théorique des conceptions générales d'une sécurité réseaux en définissant les différents réseaux , politique de sécurité, les attaques courantes et les solutions de ces dernières(logiciel et matérielles).Dans le chapitre II nous présenterons notre architecture existante et étudierons les différentes failles de celle-ci. Dans le chapitre III nous proposerons une solution permettant d'augmenter le niveau de sécurité du réseau. Dans le dernier chapitre nous effectuerons un cas pratique de l'implémentation d'une architecture réseau sécurisée.

Introduction

Les réseaux jouent un rôle croissant dans notre société de l'information. La nécessité de donner accès aux informations et aux ressources à de nombreux utilisateurs sur de nombreux ordinateurs rend une mise en réseau pratiquement indispensable dans la plupart des environnements professionnels.

De nos jours, les réseaux permettent une intégration entre fonctions associées et entreprises plus poussée qu'autrefois.

Cependant, les attaques informatiques ne cessent d'être dirigées contre les entreprises. Pour cela, il faut mettre en place une bonne politique de sécurité.

Dans ce chapitre, nous définirons et présenterons les différents type des réseaux informatiques, nous aborderons aussi les différents aspects liés à la sécurité de ces derniers en étudiant les types d'attaques, leurs mécanismes de détection et de protection.

Ainsi, nous expliquerons la vision de Cisco qui a introduit le self-defending Network, la notion de découpage en zone, 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.

I.1. Les réseaux informatiques :

a. Définition :

Un réseau est un groupe de périphériques interconnectés capables de transporter différents types de communication, y compris des données informatiques traditionnelles, de la voix interactive, de la vidéo et des produits de divertissement. Un réseau numérique permet l'échange entre machines distantes de données qui sont nécessaire, relayées de liaison en liaison par les machines intermédiaires. Généralement ils sont composés de 4 éléments essentiels :

- Les périphériques
- Les messages
- Les protocoles
- Les supports

Comme le montre la figure suivante :

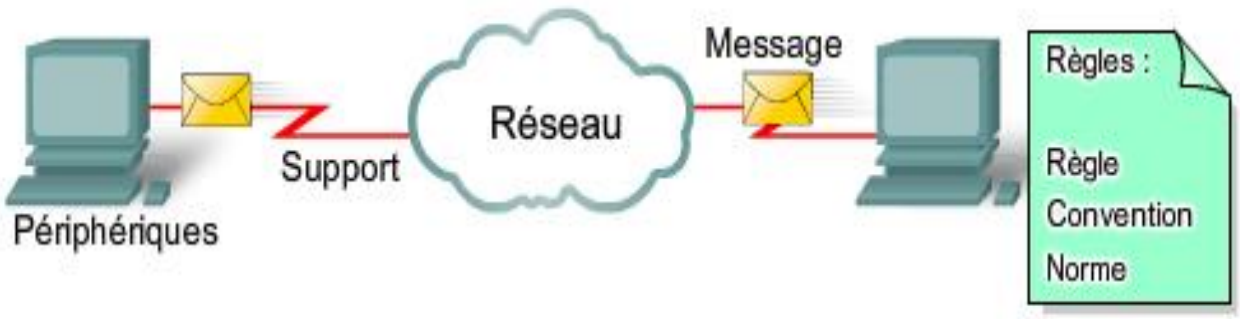


Figure I.1 : réseau informatique

b. Objectifs des réseaux :

- ü Permettre le partage des ressources.
- ü Accroître la résistance aux pannes.
- ü Diminuer les coûts.

c. Applications :

- ü Accès à des services à distance : bases de données, programmes...
- ü Communication : Mail, News, Talk, Téléconférence etc....

d. Critère de qualité d'un réseau :

Les réseaux doivent prendre en considération quatre critères pour répondre aux attentes des utilisateurs :

- Ø **Tolérance aux pannes** : Le réseau doit être constamment disponible même en cas de pannes du matériel et des logiciels.

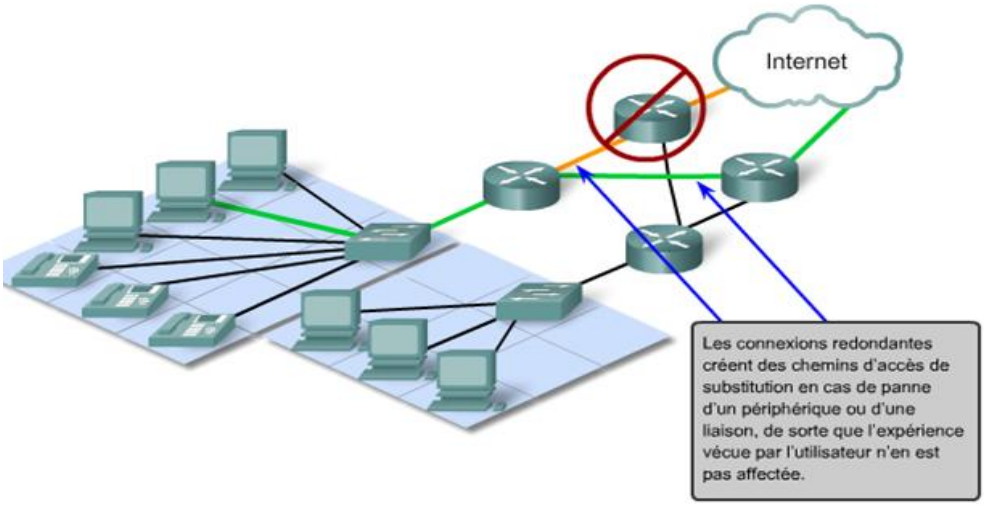


Figure I.2 : Tolérance aux pannes

Ø **Evolutivité** : Le réseau doit être en mesure de s'étendre rapidement afin de prendre en charge de nouveaux changements.

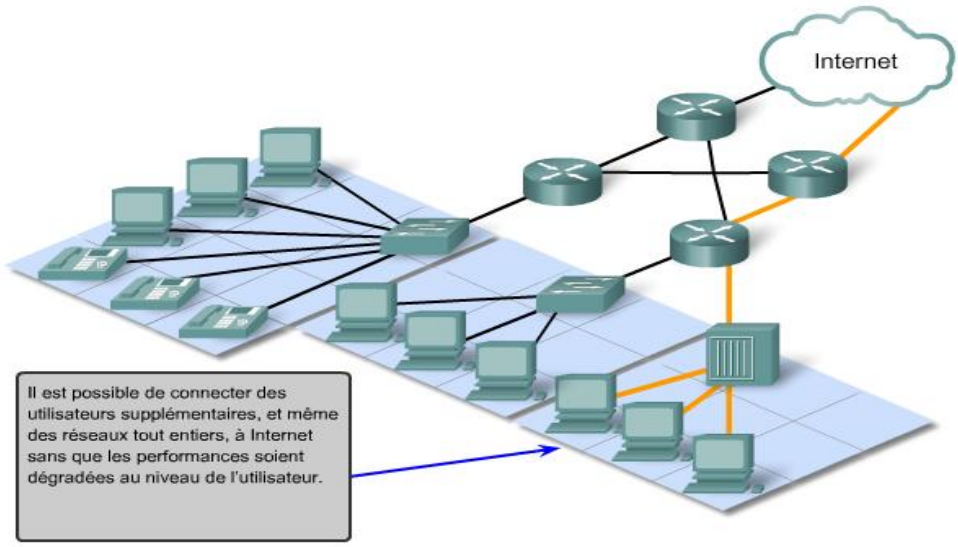


Figure I.3 : Evolutivité

Ø **Qualité de service (QoS):** Vise le niveau de performance des services offerts dans le réseau. Elle établit les priorités de livraison des différents messages transmis sur un réseau. Elle assure un transfert homogène et ininterrompu des données pour faire face aux besoins des utilisateurs.

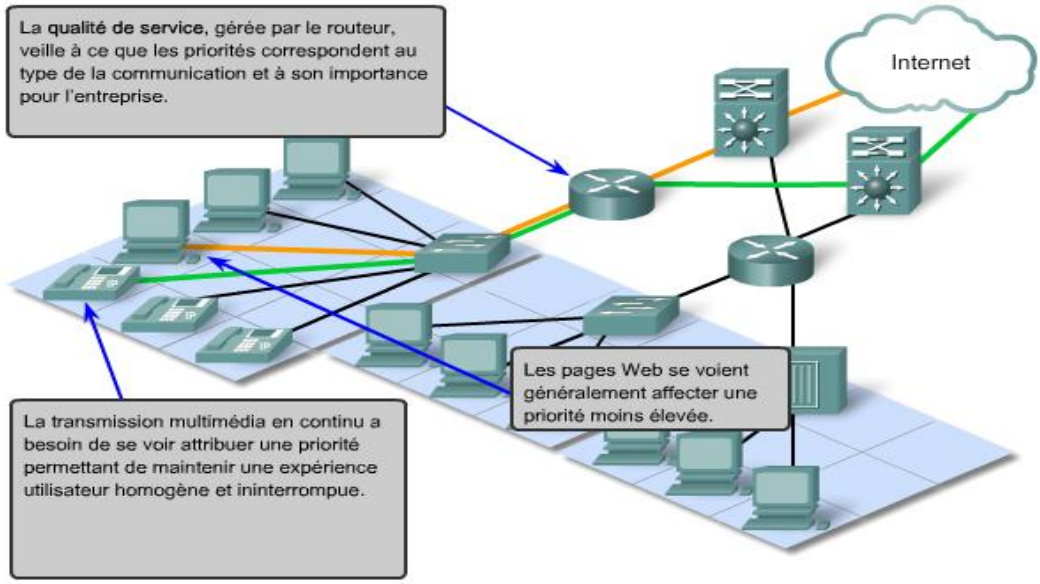


Figure I.4 : Qualité de service

Ø **Sécurité:** Protège les informations confidentielles et stratégiques contre le vol, la destruction ou la falsification.

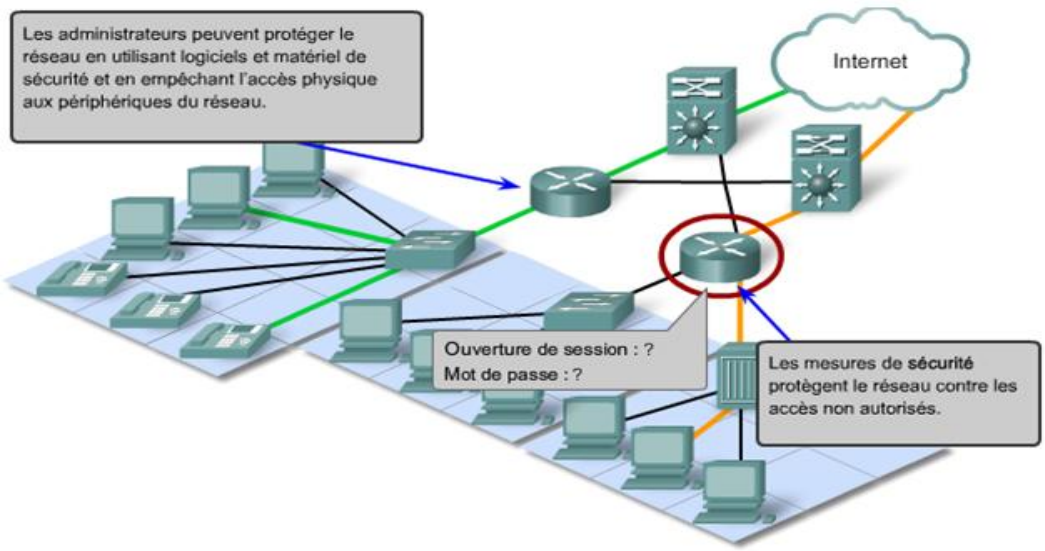


Figure I.5 : Sécurité

e. Catégories des réseaux :

Ø **Selon la distance**

- Réseaux personnels (PANs) **è** jusqu'à 10 m
- Réseaux locaux (LANs) **è** entre 10m et 1km
- Réseaux métropolitains (MANs) **è** ≈10 km
- Réseaux étendus (WANs) **è** Echelle de la terrec

- **Selon la topologie :**
  - Réseaux en Bus
  - Réseaux en Anneau
  - Réseaux en étoile
  - Réseaux Maillés
  - Réseau en arbre
- **Selon Le support**
  - Réseaux filaires
  - Réseaux sans fils

f. Les modèles réseaux :

- **Le modèle OSI (Open Systems Interconnection) :** Les systèmes de communication en réseau sont souvent décrits grâce au modèle de référence Open Systems Interconnection (OSI). Ce modèle a été développé par l'ISO (International Organization for Standardization). Le modèle OSI est constitué de 7 couches remplissant chacune une fonctionnalité particulière, de la couche application à la couche de transmission chacune des différentes couches ne représente pas nécessairement un protocole spécifique. L'illustration ci-après présente la structure de ce modèle :

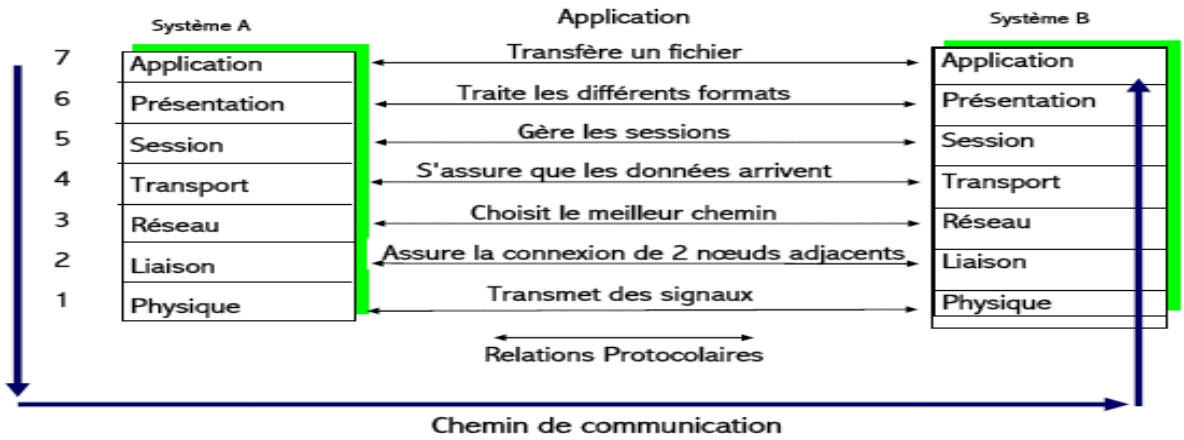


Figure I.6 : Modèle OSI

- **Le modèle TCP-IP (Transmission Control Protocol – Internet Protocol) :** La famille des protocoles TCP/IP est particulièrement adaptée pour la mise en œuvre de réseaux de grande ampleur (WAN). TCP/IP est aujourd'hui, parmi les protocoles standardisés et routables, le protocole le plus complet et le plus diffusé pour les réseaux d'entreprise. Les protocoles de la suite TCP/IP sont généralement définis par des documents RFC (Request for Comments). L'IETF (Internet Engineering Task Force) est responsable de la maintenance des normes de la suite TCP/IP.

Les protocoles de couche application TCP/IP les plus connus :

- Le protocole DNS (Domain Name Service) est utilisé pour traduire les adresses Internet en adresses IP.
- Le protocole HTTP (Hypertext Transfer Protocol) est utilisé pour transférer les fichiers qui constituent les pages du Web.
- Le protocole SMTP (Simple Mail Transfer Protocol) est utilisé pour transférer les courriels et les pièces jointes.
- Le protocole Telnet, protocole d'émulation de terminal, est utilisé pour permettre un accès distant aux serveurs et aux périphériques réseau.
- Le protocole FTP (File Transfer Protocol) est utilisé pour le transfert interactif de fichiers entre les systèmes.
- La figure si après montre la différence entre les modèles OSI et TCP/IP

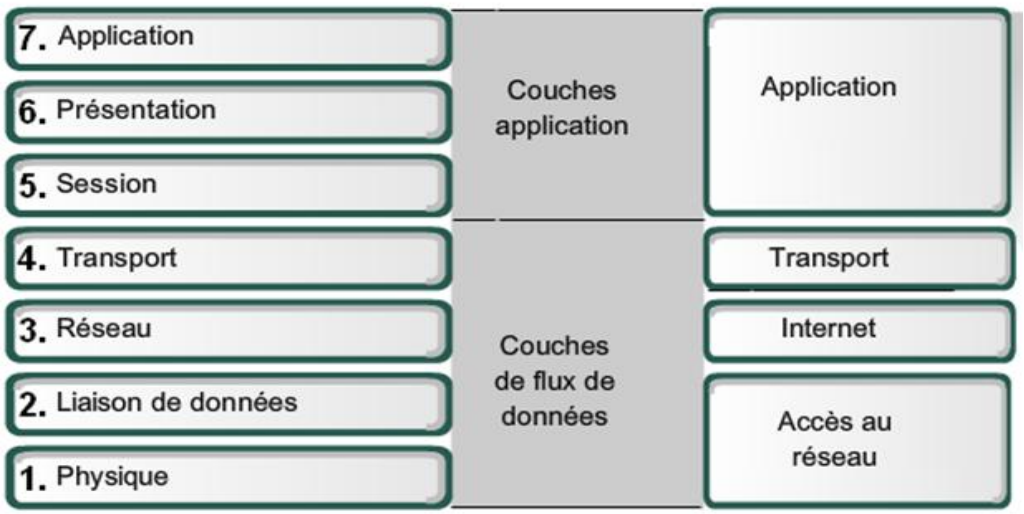


Figure I.7 : Différences entre OSI et TCP/IP

I.2. Sécurité des réseaux informatique

1. Récapitulatif des plus récentes attaques

ü 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.

ü 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.

2. 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, elle consiste à assurer que les ressources d'une organisation sont uniquement utilisées dans le cadre prévu.

La sécurité informatique vise généralement cinq principaux objectifs :

- **L'intégrité** : garantir que les données sont bien celles que l'on croit être.
- **La confidentialité** : assurer que seules les personnes autorisées aient accès aux ressources échangées.
- **La disponibilité** : permet de maintenir le bon fonctionnement du système d'information.

3. Politique de sécurité

a. Définition : Une politique de sécurité informatique est un plan d'actions définies pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme.

Cependant, Une politique de sécurité réseau est un document générique qui définit des règles à suivre pour les accès au réseau informatique et pour les flux autorisés ou non, détermine comment les politiques sont appliquées et présente une partie de l'architecture de base de l'environnement de sécurité du réseau.

b. Les types de politique de sécurité

- **Politique réglementaire (Regulatory) :** Se basant sur la réglementation d'une entreprise.
- **Politique-conseil (Advisory) :** Définissant les comportements et activités permis aux employés au sein de l'entreprise ainsi que les sanctions possibles.
- **Politique informationnelle (Informative):** Jouant un rôle éducationnel auprès des employés sur des sujets pointus.

4. Terminologies de la sécurité informatique :

- **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
- **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:** Une menace est un signe qui laisse prévoir un danger comme elle peut être une personne, un objet, ou un événement qui peut créer un danger en termes de disponibilité, d'intégrité ou de confidentialité

5. 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:** une menace intensionnelle est une action exécutée 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** :

Les détournements des données (l'écoute sur le réseau à l'aide des sniffeurs, les indiscrétions) : c'est le cas de l'espionnage industriel, l'espionnage commercial, les violations déontologiques ;

Les détournements de logiciels : les copies illicites par exemple.

- **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 aux menaces actives, nous pouvons citer :

- La destruction, la modification, la fabrication, l'interruption ou l'interception de données.
- Une divulgation de l'information (violation de la confidentialité de l'objet),
- Une modification des objets (violation de l'intégrité de l'objet)
- Un déni de service (violation de la disponibilité).

5.1. Les attaques informatiques :

a. Les différentes étapes d'une attaque

La plupart des attaques, de la plus simple à la plus complexe fonctionnent comme suite :

- **Identification de la cible :** cette étape est indispensable à toutes attaques organisées, elle permet de récolter un maximum de renseignements sur la cible en utilisant des informations publiques et sans engager d'actions hostiles. On peut citer par exemple l'utilisation des bases Whois, l'interrogation des serveurs DNS…
- **Le scanning :** l'objectif est de compléter les informations réunies sur une cible visées. Il est ainsi possible d'obtenir les adresses IP utilisées, les services accessibles de même qu'un grand nombre d'informations de topologie détaillée (OS, versions des services, subnet, règles de firewall….). Il faut

noter que certaines techniques de scans particulièrement agressives sont susceptibles de mettre à mal un réseau et entraîner la défaillance de certains systèmes.

- **L'exploitation :** Cette étape permet à partir des informations recueillies d'exploiter les failles identifiées sur les éléments de la cible, que ce soit au niveau protocolaire, des services et applications ou des systèmes d'exploitation présents sur le réseau.
- **La progression :** Il est temps au pirate de réaliser son attaque. Le but ultime étant d'élever ses droits vers root (ou system) sur un système afin de pouvoir y faire tout ce qu'il souhaite (inspection de la machine, récupération d'informations, installation de backdoors, nettoyage des traces,…).

b. Les types d'attaques

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

ü Les attaques directes

Le pirate 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.

ü Les attaques indirectes par rebord

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

->Masquer l'identité (l'adresse IP) du pirate.

->Utiliser éventuellement les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU,a 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 rebord.

ü Les attaques indirectes par réponse

Cette attaque est une dérivée de l'attaque par rebord. Elle offre les mêmes avantages, du point de vue du pirate, 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.

c. Les techniques d'attaques

c.1. 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.

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 ses identifiants 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 l'hameçonnage (dans le cas du DNS) ou comme vecteur de virus et autres applications malveillantes.

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.

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 (désynchronisation) :

Est une technique consistant à intercepter une session TCP initiée entre deux machines afin de la détourner. Dans la mesure où le contrôle d'authentification s'effectue uniquement à l'ouverture de la session, un pirate réussissant cette attaque parvient à prendre possession de la connexion pendant toute la durée de la session.

5. Port scanning

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

c.2. Les attaques applicatives

Les attaques applicatives se basent sur des failles dans les programmes utilisés, ou encor 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 server peut entraîner l'accès à des fichiers importants ou mettre en jeux l'intégrité de système d'exploitation.

2. Les scripts

Les scripts s'exécutent sur un serveur et renvoient un résultat 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.

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 dans une requête de base de données. Ainsi, il est possible de récupérer des informations se trouvant dans la base (exemple : mot de passe) ou encore de détruire des données.

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.

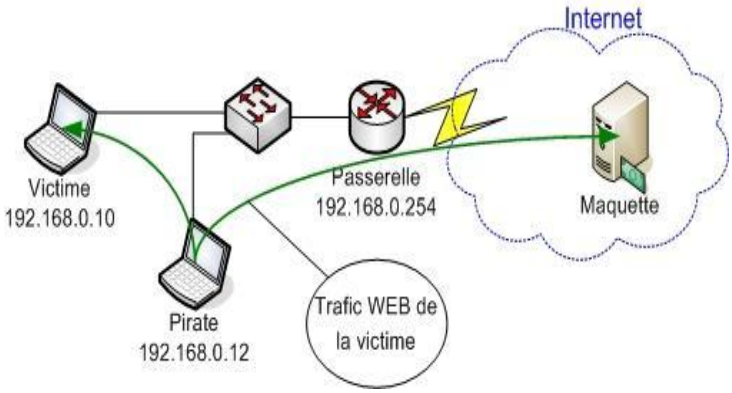


Figure I.8: Man in the middle

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.

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.

c. Packet Fragment

Cette attaque utilise une mauvaise gestion de la défragmentation au niveau ICMP. Exemple: ping of death. La quantité des données est supérieure à la taille maximum d'un paquet IP.

d. 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.

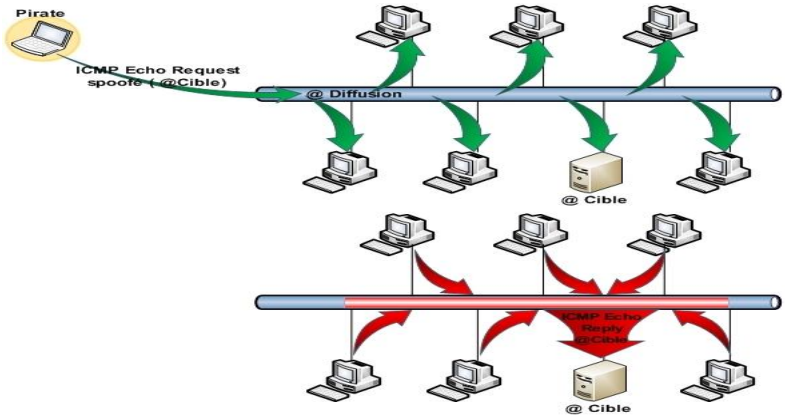


Figure I.9: Smurfling

e. Déni de service distribué (DDOS)

Le but est ici 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.

6. 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.

7. 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...).

8. Le cheval de Troie

Initialement un cheval de Troie désignait un programme se présentant comme un programme normal destiné à remplir une tâche donnée, ayant parfois un nom connu (en quelque sorte déguisé sous une fausse apparence), une fois installé il exerce 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.

9. 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.

10. 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. Cette technique est une forme d'attaque informatique reposant 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.

11. 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.

5.2. 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 plus efficaces. Les risques de failles applicatives sont, de ce fait, très grands et peuvent s'avérer dangereux pour des applications largement répandues.

a. Les systèmes de prévention d'intrusion :

Un système de prévention d'intrusion (ou IPS, Intrusion Prévention 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.

b. Les systèmes de détection d'intrusion :

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 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.

6. Les mécanismes de sécurité

6.1. 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.

1. a .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.

1. b. 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 privée 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.

1. c .Le cryptage à clé mixte

Il combine la cryptographie symétrique et asymétrique. La cryptographie asymétrique est 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.

6.2. 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 d'un message.

2. a. La Signature numérique

La signature numérique permet d'assurer à la fois l'origine et l'intégrité du message. De manière semblable au chiffrement, il existe deux classes de signatures, l'une symétrique (utilisation d'une clé partagée entre la source et la destination d'un message), l'autre asymétrique (utilisation d'une paire de clés par entité).

2. b .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.

2. c .Les Anti-virus

Un antivirus est un logiciel informatique destiné à identifier et à effacer des logiciels malveillants (malwares), également appelés virus, Cheval de Troie ou vers selon les formes.

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 :

- **à** Reconnaissance d'un code déjà connu (appelé signature) et mémorisé dans une base de données.
- **à** Analyse du comportement d'un logiciel.
- **à** Reconnaissance d'un code typique d'un virus.

7. Les protocoles de sécurité :

7.1. 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.

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 envoyer des paquets capturés lors d'une communication réseau légale.
- Encapsulating Security Payload (ESP) qui ajoute la fonction de confidentialité.

7.2 .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.

7.3. 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.

7.4. 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.

7.5. Le protocole SSH

Le SSH (Secure Shell) permet de répondre à la principale problématique posée par la sécurité des informations, 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.

7.6. 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.

7.7. 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. Les Serveurs et les clients doivent être enregistrés auprès des serveurs Kerberos. Celui-ci stocke dans sa base de données des informations relatives à leur identification, 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.

8. 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.

- **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.

9. 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.

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.

9.1. 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.

10. 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.

10.1. 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 (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.

11. Le NAT

Dans les grandes entreprises, 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.

12. 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.

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.3.Sécurisation des interconnexions réseaux

3. 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.

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 est un réseau interne devisé en trois zones
- les filiales,
- WAN (réseaux longue distance).
- la zone DMZ.

- Zone applicative (Datacenter) qui comprend les aires de stockage, les centres applicatifs et les services de téléphonie sur IP.

3.1.1. Découpage en zones de sécurité :

Le découpage en zones fonctionnelles facilite 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.

a. La zone infrastructure :

La zone infrastructure est au centre du système d'information, il existe trois zones de base :

- **La zone d'accès** : comprend les commutateurs sur lesquels sont connectés les postes de travail.

  C'est dans cette zone qu'intervient l'authentification obligatoire avant toute possibilité de communiquer. Elle permet 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 de fortes mesures de sécurité car, étant au centre de la zone d'infrastructure. 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.

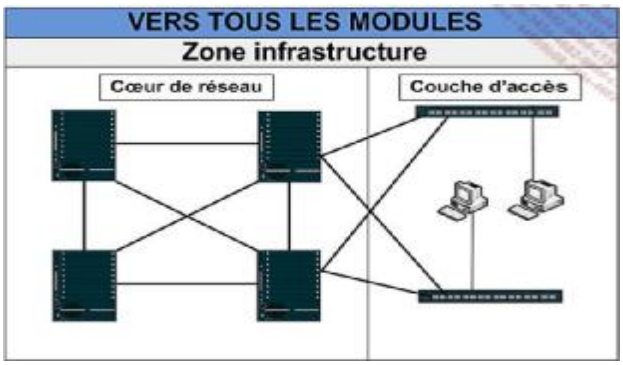


Figure I.10: Zone infrastructure.

b. Les filiales

Une filiale est une zone à part entière de l'entreprise et dispose de moyens limités pour assurer sa propre sécurité. Elle est généralement traitée comme une extension du réseau local et à ce titre bénéficie de tous les services applicatifs.

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.

La suite IPSec est indiquée pour accomplir cette tâche entre deux équipements de ces deux derniers.

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

Figure I.11: Zone filiale.

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.

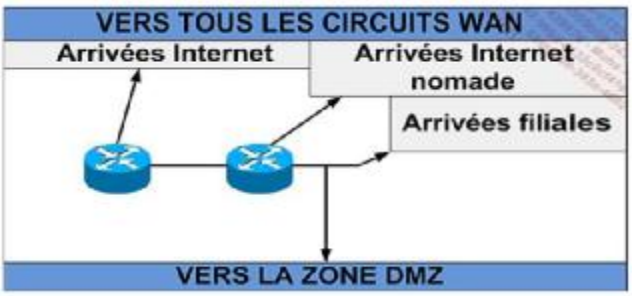


Figure I.12: Zone WAN.

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, 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.

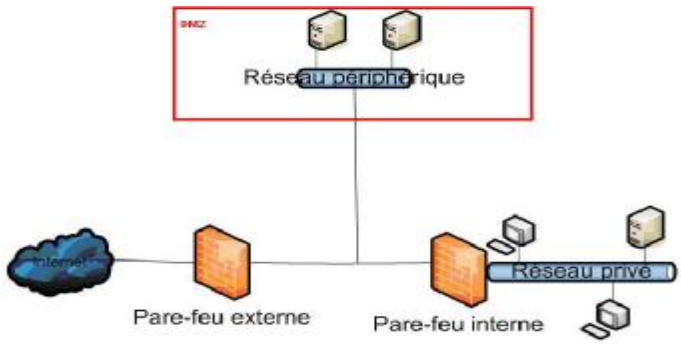


Figure I.13: Zone DMZ.

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. 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.

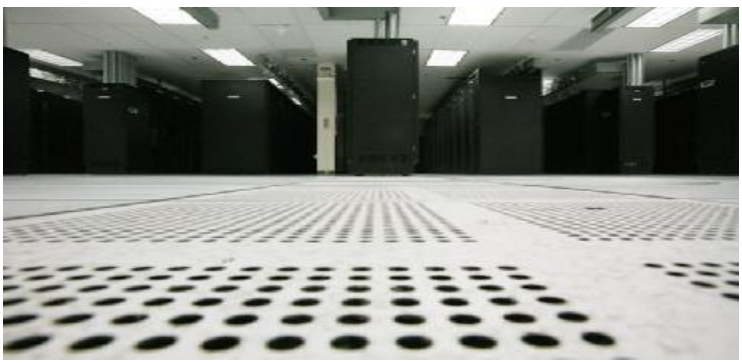


Figure I.14: Zone Datacenter.

3.2. Les Firewalls

2.1. Définition :

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:

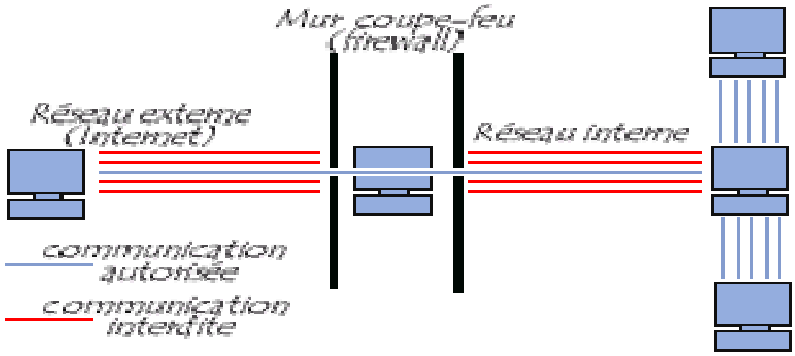


Figure I.15 : Exemple de firewall.

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.

2.2. Les fonctions d'un firewall

Un firewall dispose de plusieurs fonctions dont :

- Autoriser/ Bloquer la connexion (allow/ 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.

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.

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 basiques (filtrage sur adresse IP, port, le plus souvent en Stateless).

b. Les firewalls matériels

Ils sont intégrés directement dans la machine, 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. Ils sont aussi peu vulnérables aux attaques.

- **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. 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 fonctionnement que les firewalls matériels des routeurs, à ceci près qu'ils sont configurables à la main.

2.4. Les types de filtrage des paquets :

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 et réceptrice.
- Le type de paquet (TCP, UDP...).
- Le numéro de port .

b. Le filtrage dynamique de paquets

Le filtrage de paquets avec état (Stateful Packet Filtering) 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 niveaux 3 ou 4 du modèle OSI.

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.

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.

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 :

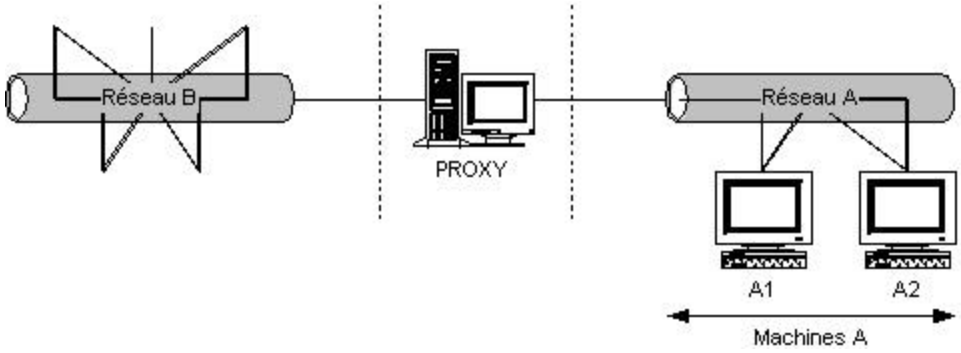


Figure I.16 : Proxy.

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 car 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.

Dans le deuxième chapitre nous étudierons les différents points de l'infrastructure de la Banque Algérie, qui a été mise à jour en 2007.

Introduction

Les attaques réseau sont aujourd'hui si nombreuses qu'il serait illusoire de prétendre les décrire toutes.

Il est cependant primordial de dresser une typologie des faiblesses de sécurité a fin de mieux appréhender ces attaques, qui ont pour point commun d'exploiter des faiblesses de sécurité. Par conséquent les entreprises ne peuvent plus ignorer ces risques et se croire à l'abri de telles épreuves.

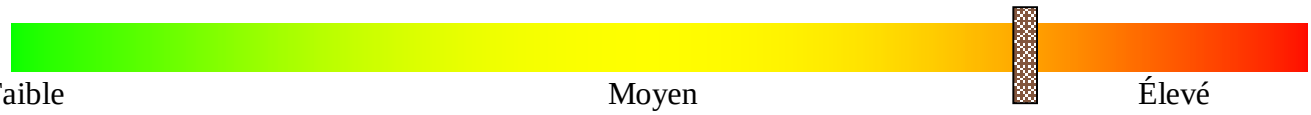
C'est pour cela que nous nous sommes penchées sur la sécurité d'une banque. Nous allons, pour lever toute ambiguïté, découvrir son architecture réseau et ses différents sites.

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.

Dans le cadre du projet de politique et stratégie de sécurité du réseau de télécommunication de la Banque d'Algérie, ont a effectués une analyse technique de l'environnement qui inclut le réseau, des routeurs, des commutateurs, des serveurs critiques, et des postes clients dans les sites A et B.

La revue de l'architecture du réseau a été exécutée en coopération étroite avec le consultant réseau de la Banque D'Algérie

Suite à l'analyse réalisée, on a constaté un niveau plutôt élevé de vulnérabilité dû à l'existence de beaucoup de vulnérabilité exploitable à distance sur les divers systèmes, comme l'existence des failles dans l'architecture du réseau et dans l'approche de gestion du réseau.



II.1. Présentation de l'architecture existante :

Notre infrastructure existante est constituée de deux sites:

Le **site A** est constitué de :

- 9 serveurs protégés par des firewalls PIX 506E.
- 1 Base de données.
- 7 zones :
  - Zone réseau externe constituée de:
    - 1 Zone SI
    - 1 Zone service bureau
  - Zone réseau interne constituée de :
    - Zone Back-end
    - Zone Front-end
    - Zone service d'administration
- 3 types de VLAN
  - VLAN Private
  - VLAN Participant
  - VLAN CPI
- 4 firewalls :
    - 2 SideWinder.

- 2 PIX.

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

Le **site B** est constitué de :

- 18 serveurs dont 10 protégés par le firewall PIX.
- 1 base de données.
- 8 zones devisées comme suite :
  - Zone réseau externe constituée de :
    - Zone SI
    - Zone service bureau
    - Zone supervision réseau
  - Zone réseau interne constituée de :
    - Zone Back-end
    - Zone Front-end
    - Zone service d'administration
- 3 types de VLAN
  - VLAN Private
  - VLAN Participant
  - VLAN CPI
- 6 Firewalls :
  - 2 SideWinder.
  - 1 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.

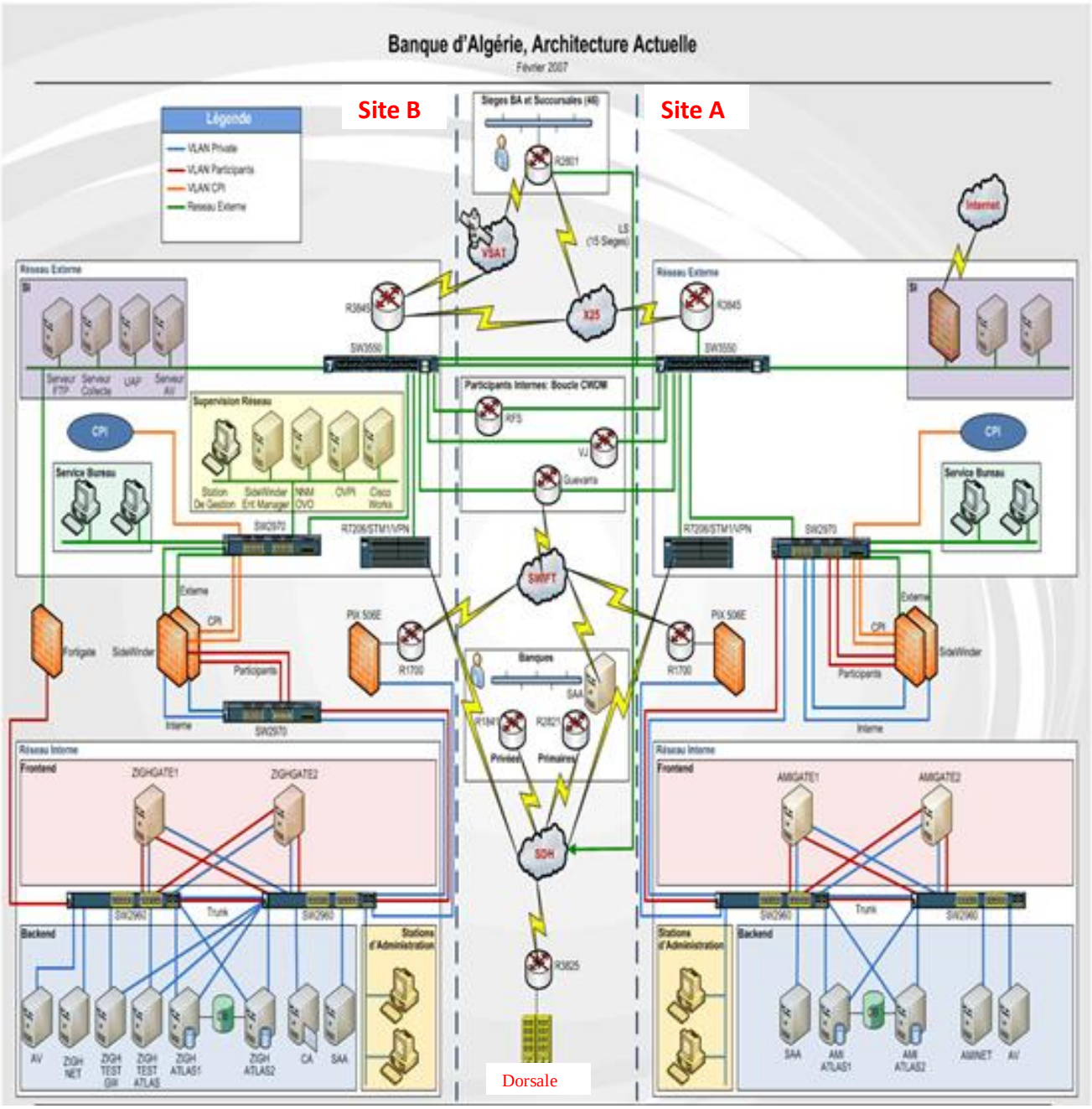


Figure II.1: L'architecture actuelle de la banque.

Cette infrastructure est constituée de deux sites, qui contiennent une architecture identique (les seules différences résident dans le nombre de serveur et la connexion internet). Dans notre étude nous identifierons les différentes failles du site B et la faille qui réside dans la zone SI du réseau externe du site A.

La dorsale qui sépare les deux sites est prise en charge par **Algérie Télécom**, pour cela nous n'allons pas la prendre en considération dans notre étude.

II.2. Vulnérabilités De L'Architecture Du Réseau

-> Point De Défaillance Unique (Single Point of Failure - SPOF)

« Single Point of Failure » est un point unique à travers lequel passent tous les traitements, et qui paralyse un système en cas de panne.

1. L'utilisation d'un Commutateur (Switch) Interne Cisco 2970

Ce commutateur met à risque l'architecture de haute disponibilité du site de production du RTGS. Il relie le cluster de SideWinder aux commutateurs redondants Cisco 2960 auxquels se connectent les serveurs Cluster et les serveurs Gateway.

Cependant, la faillite d'un des commutateurs 2970 causera une perte complète de connectivité entre les participants et l'infrastructure du RTGS. Seuls les participants connectés à travers SWIFT pourront accéder au système.

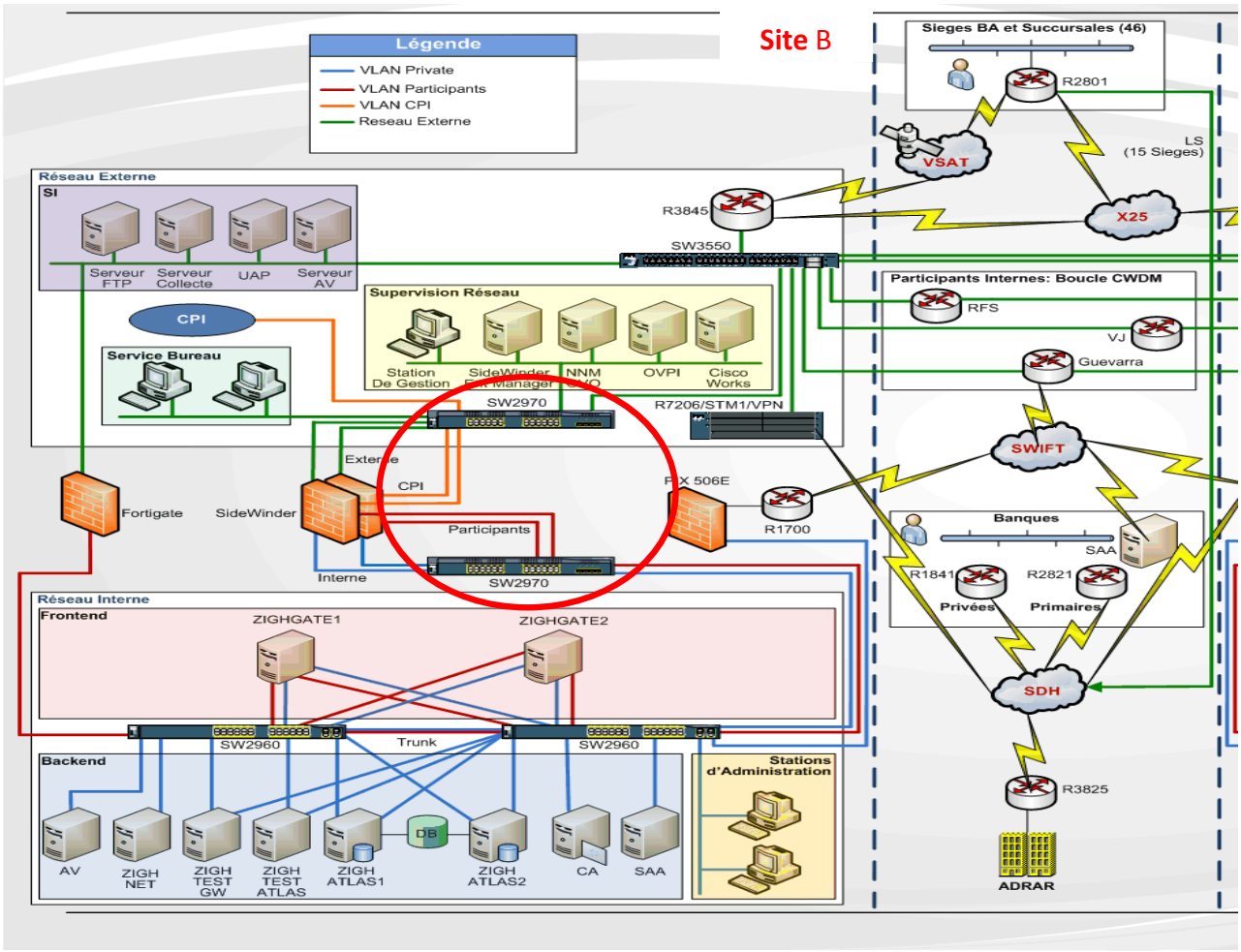


Figure II.2: Faille Commutateur (Switch) Interne Cisco 2970

2. L'utilisation d'un Commutateur (Switch) Interne Cisco 2960

Le commutateur (Switch) interne Cisco 2960, cerclé dans le schéma ci-dessous, peut mettre en danger la disponibilité du réseau. Bien qu'il existe un autre commutateur (Switch) redondant Cisco 2960 pour assurer la disponibilité de service de RTGS, Les composants ci-dessous sont connectés à un seul commutateur uniquement et donc une intervention manuelle est nécessaire au cas où un de ces commutateurs tombe en panne.

1. Le pare-feu du réseau Swift, Cisco PIX, est seulement connecté à ce commutateur et non pas a l'autre commutateur redondant. Cependant ce lien de communication avec le réseau Swift est un lien secondaire comme la Banque d'Algérie a expliquée. La connexion primaire au réseau Swift est effectuée à travers une LS au niveau du site de Guevara.

2. Le serveur Swift SAA est seulement connecté à ce commutateur.

3. Le serveur CA est seulement connecté à ce commutateur. Bien que les besoins de haute disponibilité du serveur CA ne soient pas très élevés puisqu'il est connecté une fois par semaine uniquement, il est préférable qu'il soit connecté au second commutateur aussi pour éviter une intervention manuelle au niveau du câblage réseau.

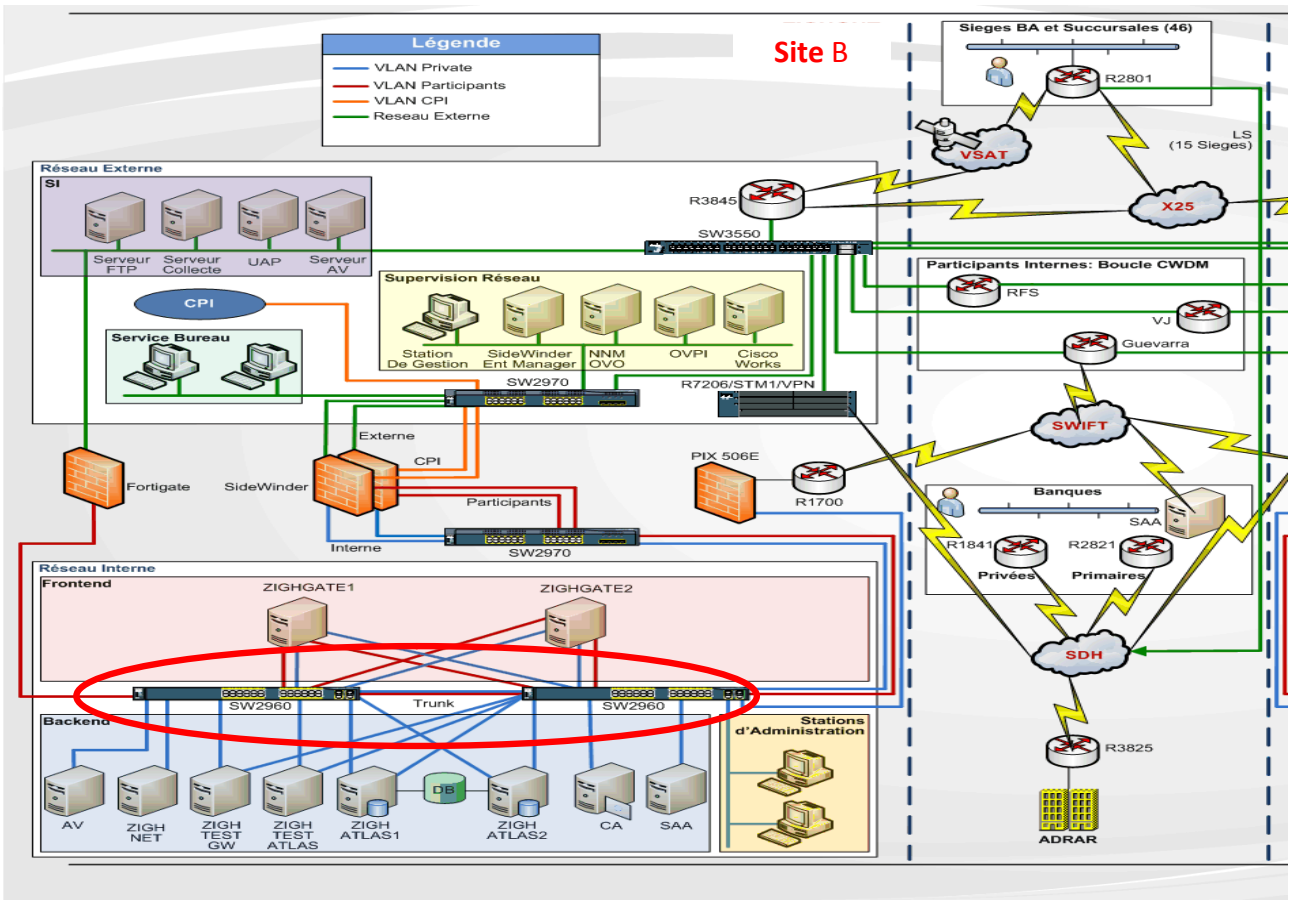


Figure II.3: Faille Commutateur (Switch) Interne Cisco 2960

3. Le commutateur SW3550

Il représente un point de défaillance comme toute l'infrastructure RTGS est connectée directement ou indirectement à ce commutateur. La faillite de ce commutateur causera donc la déconnexion de tous les utilisateurs sauf ceux connectés à travers le réseau SWIFT puisqu'il ya une connexion secondaire à travers le PIX 506 E.

De même, ce commutateur connecte le système RTGS au réseau SI. En cas de faillite du commutateur, il n'y aura aucune connectivité avec le réseau SI.

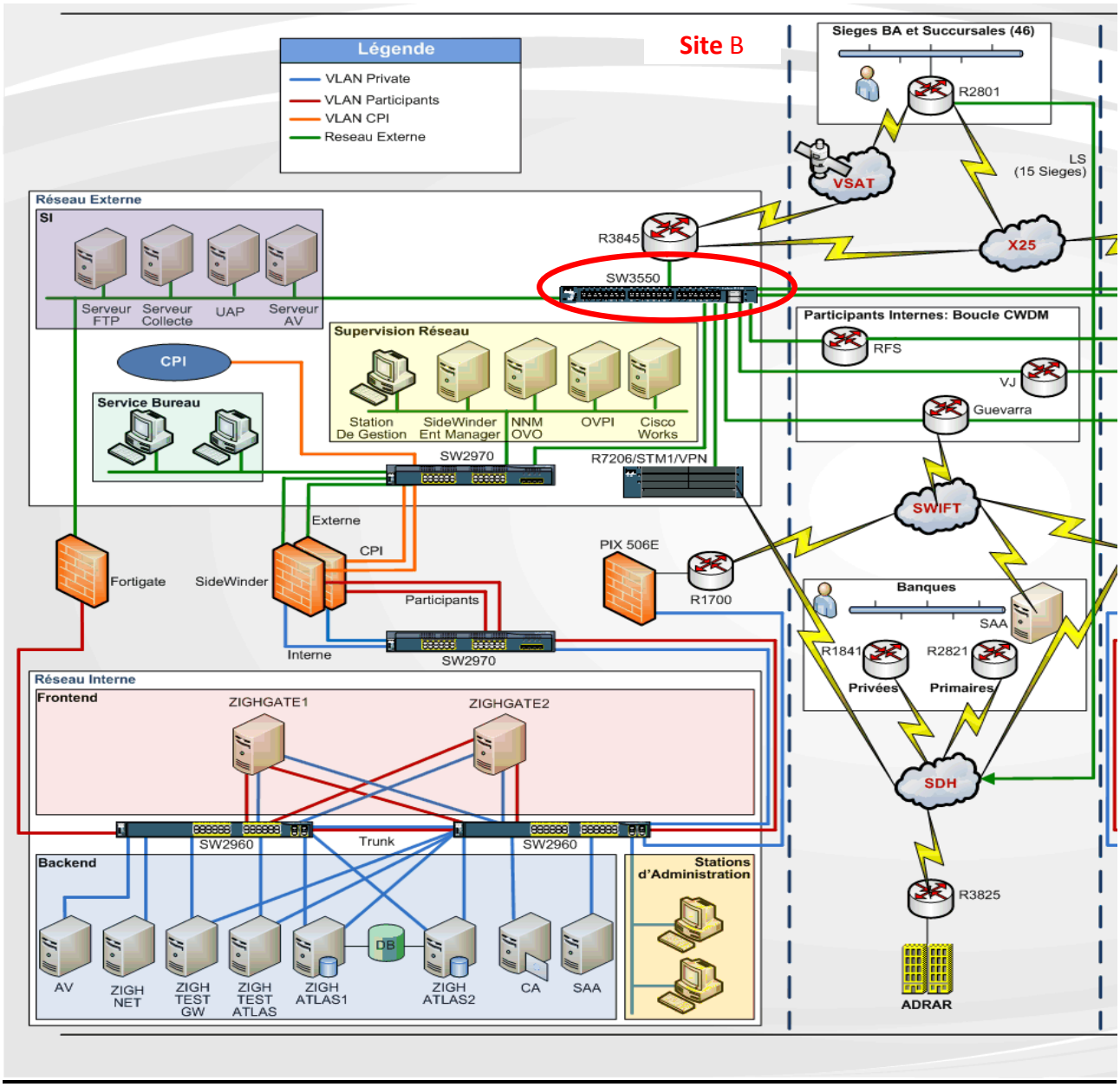


Figure II.4: La vulnérabilité du commutateur SW3550.

4. Serveur Swift SAA et Pare-feu Cisco PIX du Réseau Swift

Contrairement aux autres composants de l'infrastructure RTGS, il n'existe pas une redondance au niveau du serveur Swift SAA et du pare-feu Cisco PIX de ce réseau, sachant que la connexion à ce dernier est une connexion secondaire. La connexion primaire est effectuée à travers une ligne spécialisée au niveau du site de Guevarra. Ainsi ce risque peut être considéré tolérable par la Banque d'Algérie.

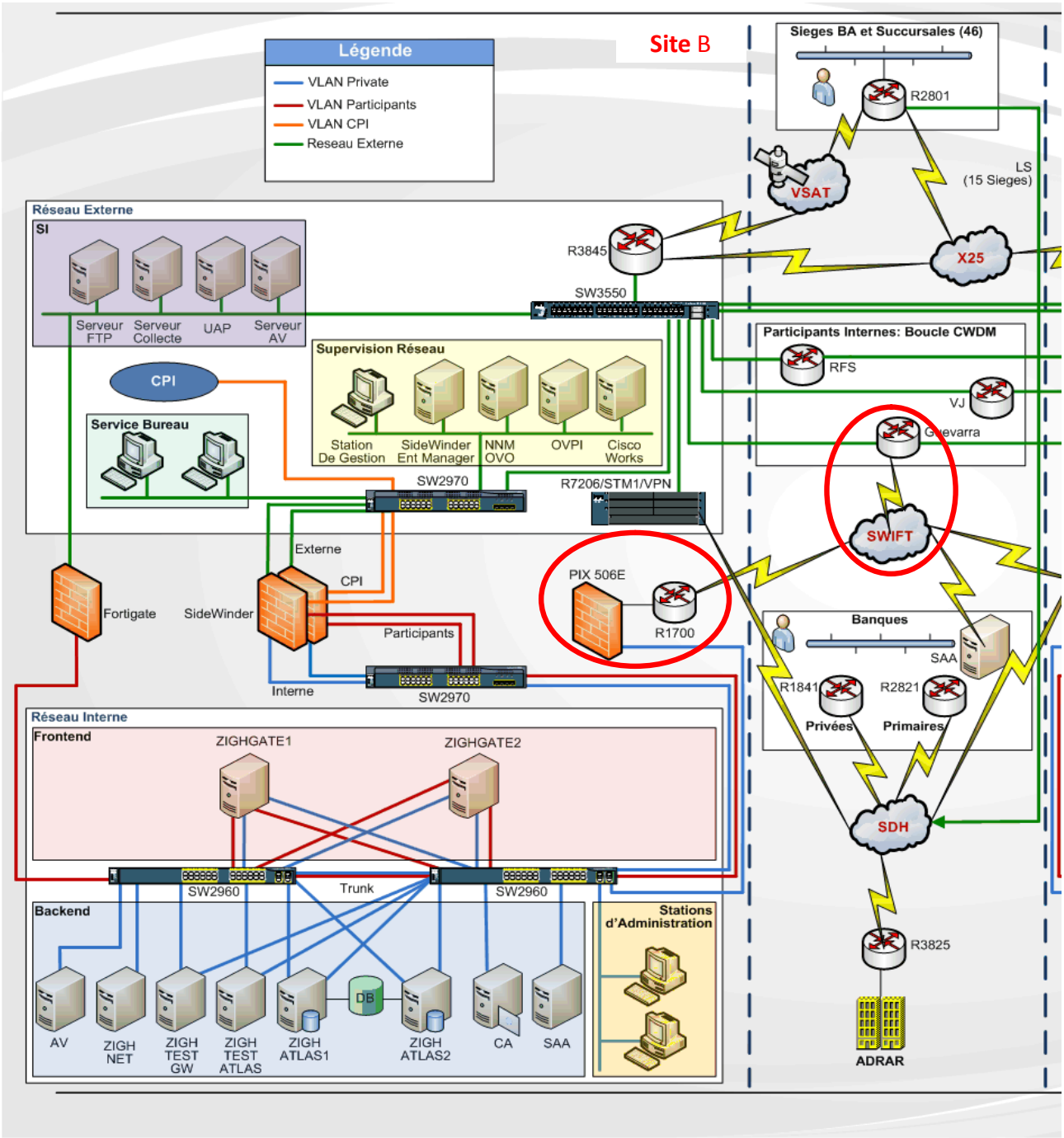


Figure II.5: Faille Serveur Swift SAA et Pare-feu Cisco PIX du Réseau Swift

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 au commutateur sw2960 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 commutateur Cisco Catalyst 3550 qui fournit la connexion vers le site A, aux participants internes, et aussi au réseau Swift puisque la connexion primaire du réseau Swift se trouve au niveau de Guevarra.
- La connexion internet, qui se trouve au niveau du réseau SI dans le site A .

  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.

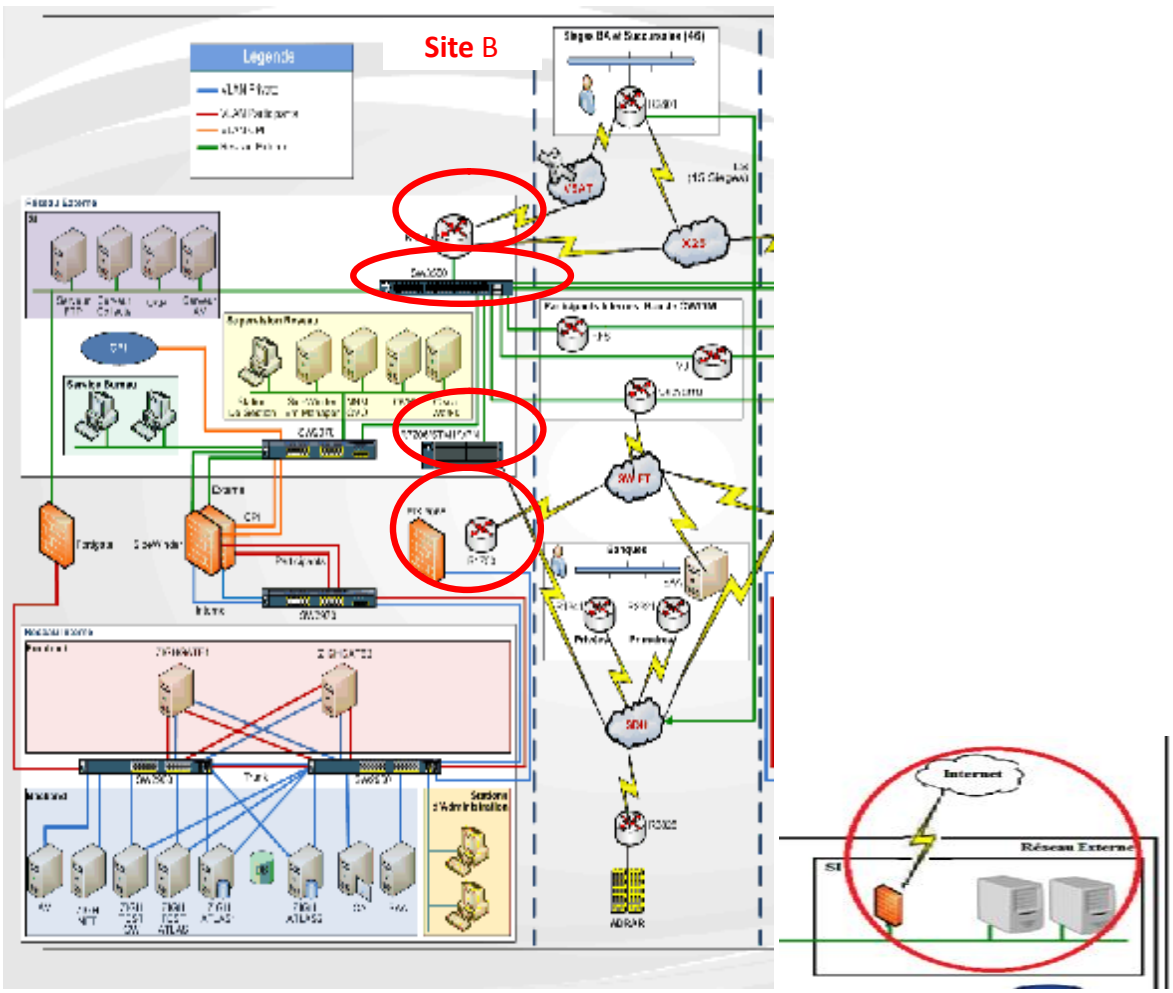


Figure II.6: Les multiple points d'entrée du réseau.

6. 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 le site B est due à la non optimisation de la sécurité. Même si ce firewall est performant .

Mettre deux firewalls Sidewinder dans la même zone constitue un risque car ces deux firewalls fonctionnent au niveau d'une 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.

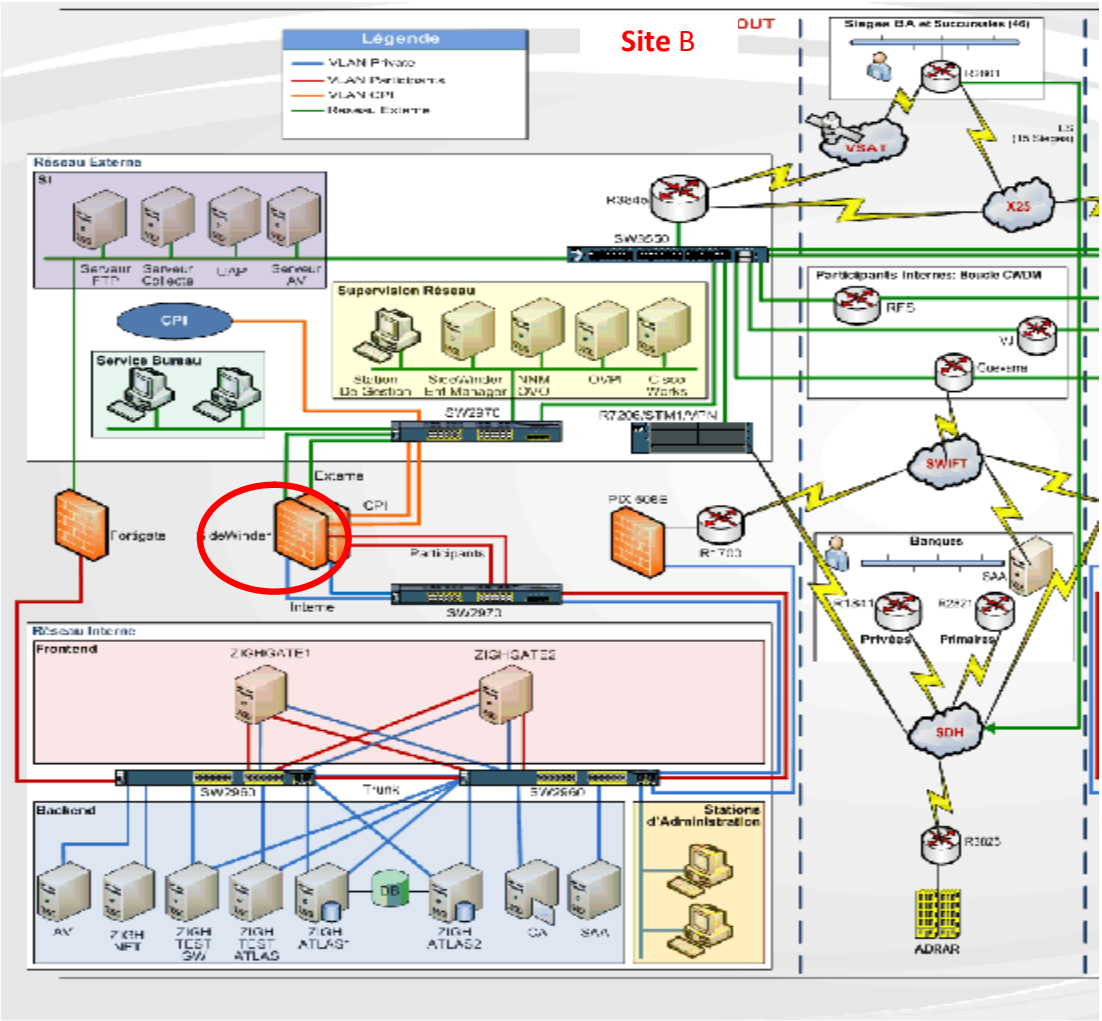


Figure II.7 : La vulnérabilité de type identique de firewalls.

II.3. 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 son protégés par des mots de passe faibles comme « cisco » et « rtgs ». Les intrus auront ainsi de 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.

II.4. 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.

II.5. 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 RTGS 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.

Conclusion

La complexité des attaques, la facilité de se renseigner sur les logiciels et les moyens d'intrusions via le web, 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.

Dans le chapitre suivant nous proposerons des solutions possibles aux vulnérabilités du réseau.

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 d'obtenir un degré de sécurité satisfaisant pour les entreprises.

Tout au long de ce chapitre, nous proposerons une nouvelle structure de l'architecture réseaux de la banque avec les solutions à mettre en place pour avoir une meilleure sécurité et à la fin nous présenterons les firewalls, ASA, TMG, FortiGate et SideWinder.

Apres avoir étudié l'infrastructure réseaux de la Banque Algérie on a pu constater que son niveau de sécurité est très bas, pour y remédier on a remplacé des composants anciens par d'autres plus récents comme Firewall PIX par un Firewall ASA aussi on a changé l'emplacement des firewalls de sorte qu'il y'aura une redondance en cas de panne de l'un de ces derniers, on a ajouté des systèmes de détection et de prévention d'intrusions (IDS, IPS) pour minimiser le taux d'intrusions , pour assurer la disponibilité du réseaux on a ajout é des failover, et on a aussi créer quelque zones pour une meilleur organisation et une sécurité plus optimale.

III.1. Présentation de l'architecture proposée :

Le Site A est constitué de :

- 10 serveurs protégés par firewall ASA
- 1 base de données
- 11 zones
  - Zone réseau externe constituée de:
    - 1 Zone SI
    - 1 Zone service bureau
  - Zone réseau interne constituée de :
    - Zone périmètre RTGS
    - Zone DMZ
    - Zone par_feu
    - Zone Front end
    - Zone administration
    - Zone gestion de sécurité
    - Zone IPS-IDS
    - Zone back end
- 5 types de VLAN
  - VLAN Private
  - VLAN Participant
  - VLAN CPI
  - Station d'administration
  - Gestion de service
- 7 firewalls :
  - 2 SideWinder.
  - 2 Fortigate.

- 2 ASA.
- 1 TMG

.

- 2 Routeurs.
- 10 Commutateurs dont l'un est un commutateur VPN.
- 4 postes :
  - 2 postes de stations d'administration.
  - 2 postes pour le service réseau.
- 6 IPS
- 6 IDS

Le Site B est constitué de :

- 21serveurs protégés par firewall ASA
- 1 base de données
- 12 zones
  - Zone réseau externe constituée de:
    - 1 Zone SI
    - 1 Zone service bureau
  - Zone réseau interne constituée de :
    - Zone périmètre RTGS
    - Zone DMZ
    - Zone par_feu
    - Zone Front end
    - Zone administration
    - Zone gestion de sécurité
    - Zone IPS-IDS
    - Zone back end
- 5 types de VLAN
  - VLAN Private
  - VLAN Participant
  - VLAN CPI
  - Station d'administration
  - Gestion de service
- 7 firewalls :
  - 2 SideWinder.
  - 2 Fortigate.
  - 1 ASA.
  - 1 TMG

.

- 2 Routeurs.

- 10 Commutateurs dont l'un est un commutateur VPN.
- 4 postes :
  - 2 postes de stations d'administration.
  - 2 postes pour le service réseau.
- 5 IPS
- 5 IDS

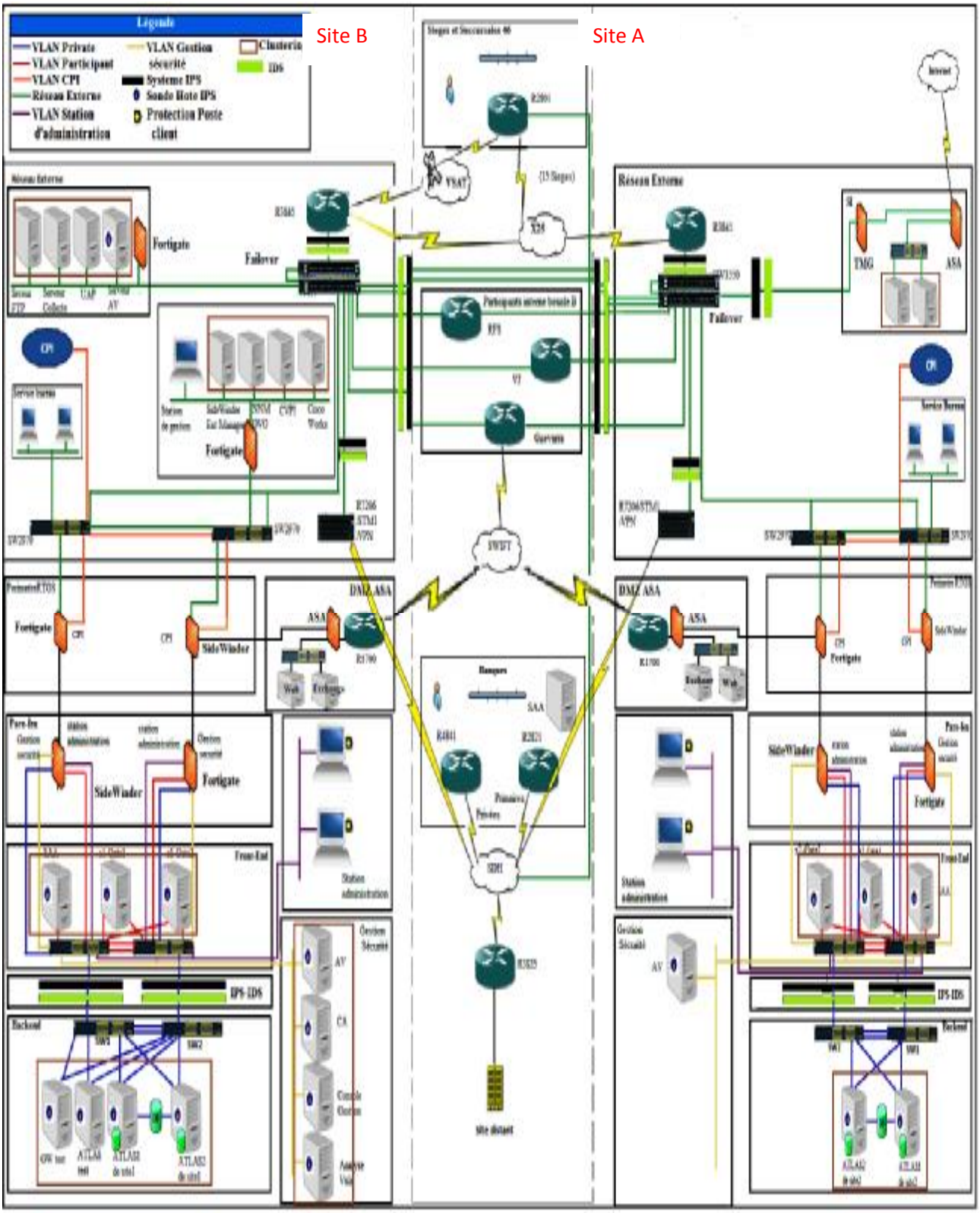


Figure III.1:L'architecture proposée.

III.2. Les changements de l'architecture réseau

1. Création de nouvelle zone :

1. a. Zone Back-end :

Cette zone comprend les serveurs de bases de données ATLAS1 et ATLAS2, et les serveurs test. Ces serveurs sont les composants les plus critiques du système RTGS et doivent être isolés du réseau.

Ces serveurs seront connectés aux deux commutateurs Cisco 2960 existants. Ils seront connectés au VLAN « private ».

Figure III.2: Création d'une zone back-end

1. b. Zone Front-end

Cette zone comprend les serveurs Gateway GATE1 et GATE2. Cette zone constitue le point d'accès des entités externes ; il est conseillé de séparer physiquement les serveurs Gateway et les serveurs Back-end pour éviter tout accès direct à ces derniers.

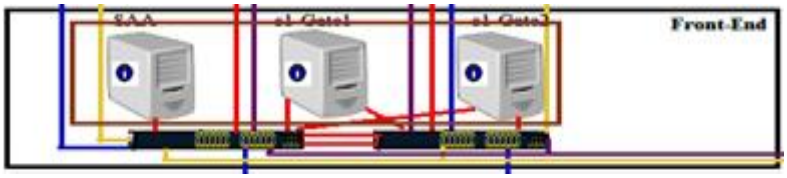


Figure III.3: Création d'une zone Front-end

1. c. Zone Station d'Administration

Cette zone comprend les stations d'administration du système RTGS. Ces stations seront connectées au VLAN « StationAdministration » au niveau des commutateurs de la zone front-end.

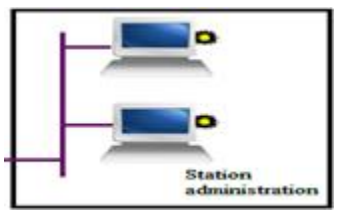


Figure III.4: Création d'une zone Station Administration

1. d. Zone Gestion de Sécurité

Cette zone comprend les systèmes relatifs à la sécurité du réseau : Le serveur anti-virus, le serveur CA, la console d'administration des produits de sécurité du système RTGS (sondes hôtes et réseau de prévention d'intrusion), et le console d'analyse de vulnérabilité du réseau.

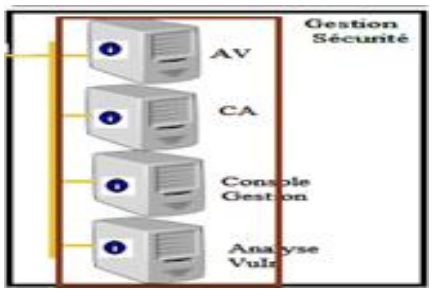


Figure III.5: Création d'une zone Gestion de Sécurité

2. Remplacement du firewall PIX par un firewall ASA :

Apres 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 SériesConcentrateur, le Cisco IPS 4000 SériesSensor 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.

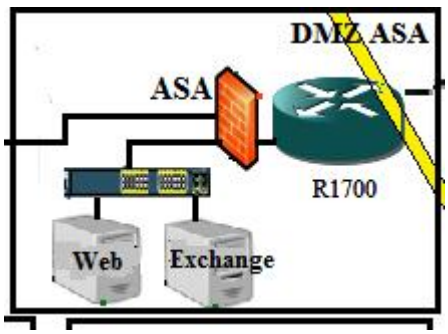


Figure III.6: Le remplacement de PIX par ASA.

3. Ajout d'un deuxième niveau de pare-feux et repositionnement des firewalls de type identique

Il est conseillé d'avoir deux niveaux de pare-feux, chaque niveau aura deux types de ce dernier, pour protéger le système RTGS. Dans ce cas si un des pare-feux est compromis l'autre luttera contre l'attaque. C'est ainsi que les consultants conseille d'introduire une zone pare-feux qui consiste de deux nouveaux pare-feux redondant. Ces pare-feux fourniront un second niveau de protection et seront utilisés pour séparer les zones Back-end, Front-end, Station d'Administration, et Gestion de Sécurité.

Ainsi :

- L'interface interne sera connecté au VLAN private
- L'accès a la zone Back-end sera seulement permit a partir de la zone Front-end, Gestion sécurité, et Stations d'administrations. Seulement les ports nécessaires seront ouverts tous les autres ports seront fermés.
- La zone Gestion de sécurité sera permise de collecter les mises a jour a partir du réseau SI. Seulement les ports nécessaires seront ouverts tous les autres ports seront fermés.

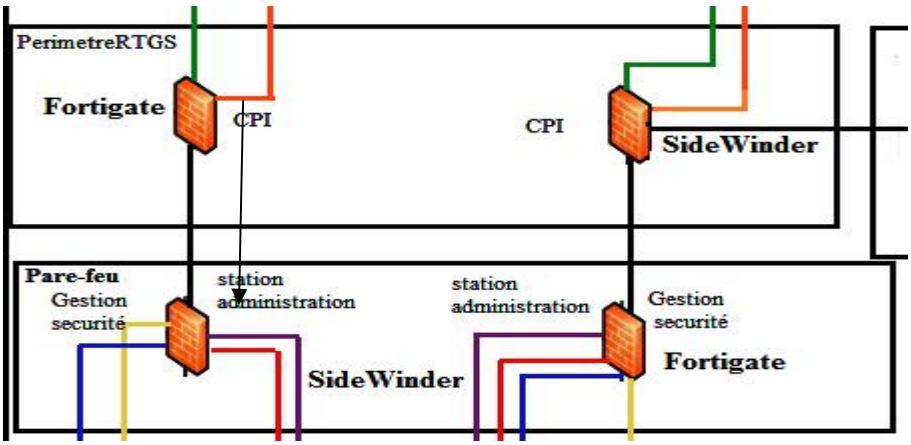


Figure III.7: L'ajout d'un niveau de firewall et permutation .

4.Séparation Des Réseaux De Gestion et Du Service Bureau

Les consultants ont noté que le réseau externe contient les postes de travail de Service Bureau et les postes de travail utilisés pour la gestion de réseau (Cisco Works, Sidewinder Enterprise Manager, console de Sidewinder) sur le même réseau virtuel (VLAN). Ces deux infrastructures ont des buts très différents et devraient avoir des procédures très différentes de contrôle d'accès.

Service Bureau est fondamentalement utilisé par des entités externes, les participants externes, qui ont des problèmes pour se connecter à RTGS de leurs lieux, alors que l'accès aux postes de travail de gestion de réseau devrait être limité seulement à quelques individus de la Banque d'Algérie.

Pour cela ; il est conseillé de séparer ces deux réseaux. Ceci peut être effectué à travers un pare-feu qui sera installé avant le réseau de gestion. Ce pare-feux permettra aussi de surveiller et protéger l'accès à partir et vers le réseau de Gestion. Le pare-feu Fortigate existant peut être utilisés pour ce but.

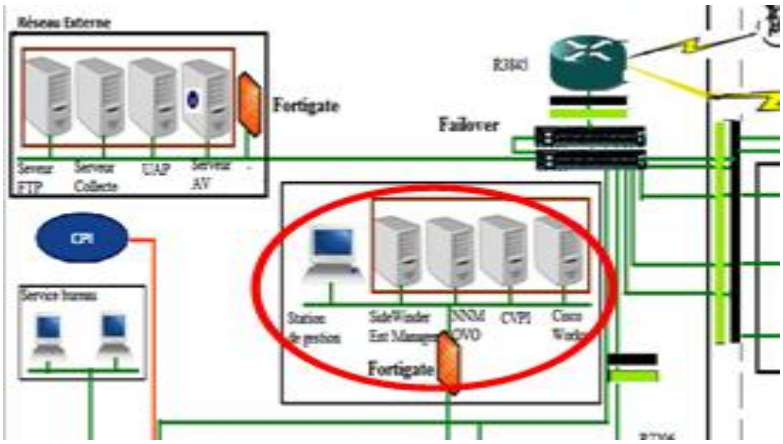


Figure III.8: Ajout d'un firewall au niveau de station de gestion

5. L'ajout des commutateurs :

5. a. 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.

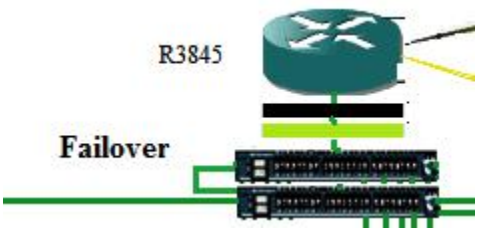


Figure III.9:L'implémentation de failover

5.b. Ajout d'un commutateur a la zone Front-end :

Pour séparer physiquement les serveurs Gateway et les serveurs Back-end et éviter tout accès direct a ces derniers ; il est conseillé d'ajouter des commutateurs a la zone Front-end identique a ceux de la zone Back-end.

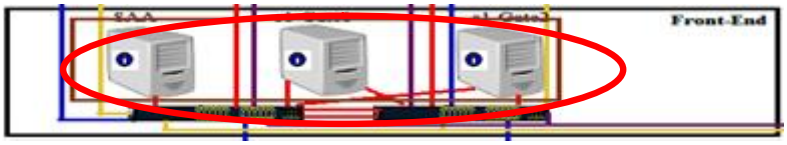


Figure III.10: Ajout d'un commutateur a la zone Front-end

5. c. Ajout d'un commutateur dans le réseau externe

Afin de ne pas mettre en danger la haute disponibilité du réseau à cause de la faillite du Cisco 2970 externe, il est conseillé d'ajouter un autre commutateur dans ce réseau. Les interfaces externes des pare-feux SideWinder seront connectées aux deux commutateurs. Similairement, les deux Switch seront connectés au Switch 3550.

Vis-à-vis de la disponibilité du Switch 3550 et du routeur 7206, la Banque d'Algérie a informé les consultants qu'elle possèdera des équipements similaires dédiés en place. Ainsi la haute disponibilité de ces équipements sera assurée.

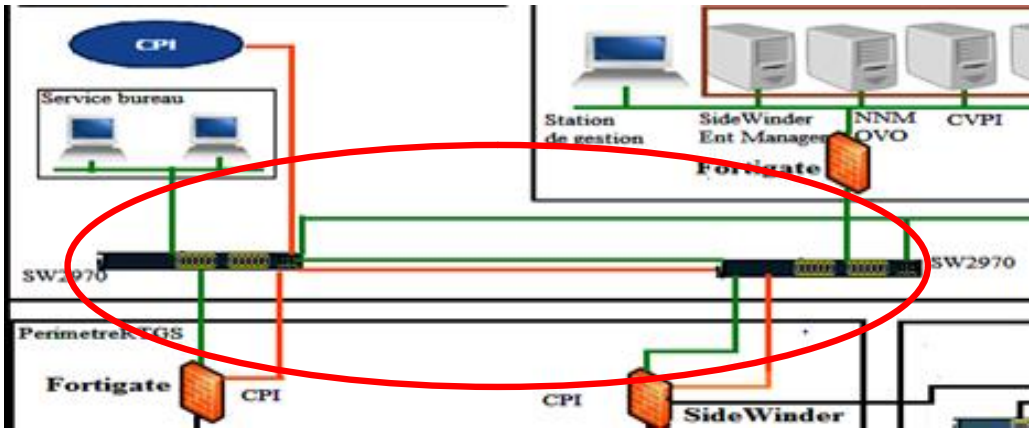


Figure III.11 : Ajout d'un commutateur dans le réseau externe

6.Ajout des IPS et des IDS :

Les systèmes de prévention d'intrusion au niveau réseau permettent de laisser passer le trafic normal tout en bloquant tout trafique malveillant. Ils complètent les pare-feux en surveillant le trafic permis par le pare-feu.

L'implémentation de Système de Prévention d'intrusion offrira à la banque le temps nécessaire dont elle a en a besoin pour proprement essayer les correctifs et consulter avec CMA pour leur implémentation sans exposer les systèmes à un risque.

Du fait des besoins de sécurité croissants des entreprises et de l'évolution des technologies qui permet un fonctionnement plus efficace des systèmes de détection et de prévention d'intrusion ,il est préférable d'ajouter des IDS qui permettront d'accentuer la sécurité des IPS à tous les niveaux, que ce soit système ou réseau

Les constructeurs de systèmes de sécurité ont tendance à intégrer les IDS et IPS directement dans les firewalls, de façon à renforcer la coopération entre ceséquipements de sécurité complémentaires.

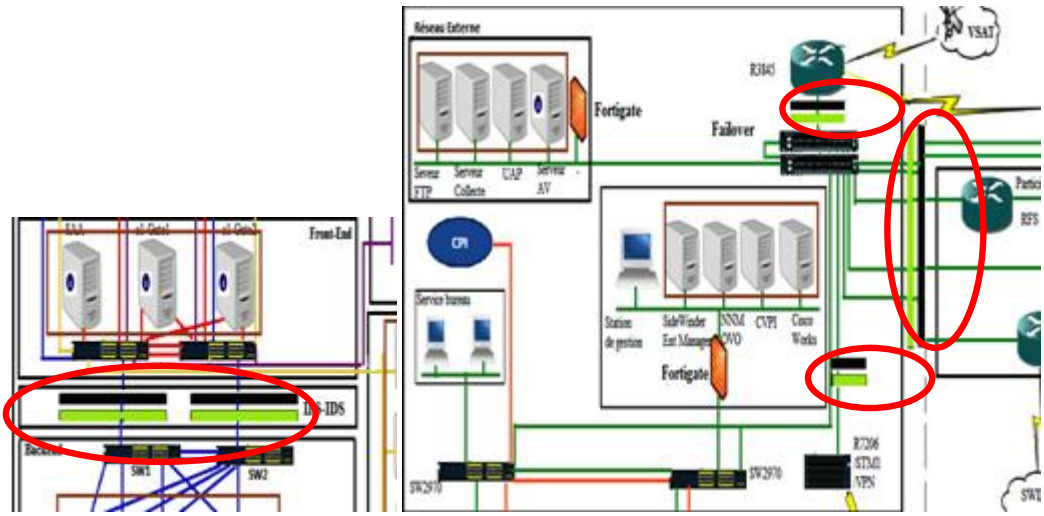


Figure III.12:l'ajout d'IPS et IDS

7. 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.

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

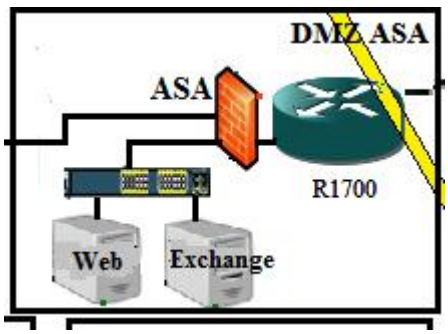


Figure III.13 : La création de la DMZ ASA.

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 et IPS comme vu plus haut.
- Pour le troisième point d'entrée, le commutateur Cisco Catalyst 3550, 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 A. 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'interne. Quant au firewall Fortigate existant, nous proposons au lieu de le supprimer du réseau, de le placer au niveau du SI du site B, afin protéger les serveurs de cette zone.

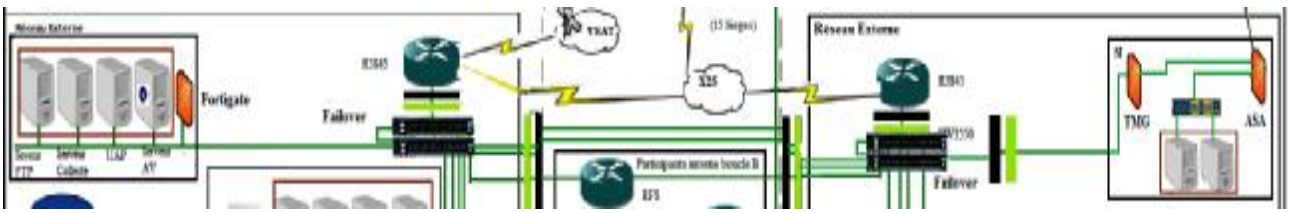


Figure III.14: La création de la DMZ SI.

II.3.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 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, cette dernière combinée avec le serveur DHCP 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.

Ensuite, 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 parmiquatre catégories :
  - Lettres minuscules (a-z)
  - Lettres majuscules (A-Z)
  - Chiffres (0-9)
  - Caractères spéciaux ($,#, %..)

II.4. 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.

II.5. 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, 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 anti-virus Kaspersky entreprise :

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 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.

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 LoadBalancing) 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.

III.6.Présentation des firewalls utilisés :

1. Le firewall ASA

1. a. Présentation

Les Serveurs de Sécurité Adaptatifs Cisco ASA 5500 combinent les meilleurs services deVPN et de sécurité, et l'architecture évolutive AIM (Adaptive Identification and Mitigation), pour constituer une solution de sécurité spécifique. Conçue comme l'élément principal de lasolution Self-Defending Network de Cisco, la gammeCisco ASA 5500 permet de mettre en place une défense proactive face aux menaces et de bloquer les attaques avant qu'elles ne se diffusent à travers le réseau, de contrôler l'activitédu réseau et le trafic applicatif et d'offrir une connectivité VPN flexible. Le résultat est unegamme de puissants serveurs de sécurité réseau multifonctions capables d'assurer enprofondeur la protection élargie des réseaux des PME/PMI et des grandes entreprises touten réduisant l'ensemble des frais de déploiement et d'exploitation et en simplifiant les tâchesgénéralement associées à un tel niveau de sécurité.Ces différentes éditions offrent uneprotection de qualité supérieure en apportant à chaque installation les services dont elle abesoin. Chaque édition de la gamme Cisco ASA 5500 regroupe un ensemble spécialisé deservices – firewall, VPN SSL et IPSec, protection contre les intrusions, services Anti-Xetc. ; qui répondent exactement aux besoins des différents environnements du réseau d'entreprise.

Et lorsque les besoins de sécurité de chaque site sont correctement assurés, c'est l'ensemblede la sécurité du réseau qui en bénéficie.

Figure III.15 : Les serveurs de sécurité adaptatifs de la gamme Cisco ASA 5500

1. b. 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):** àchaque 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 :** ilutilise 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 PathForwarding (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.

1.c.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.

2. Le firewall TMG

2. a.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 protèg0e 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.

2. b.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.

2. c.Les principaux avantages et fonctionnalités de la TMG

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

1. **Protection complète**

Figure III.16: 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.

2. **Interface de sécurité Web unifiée**

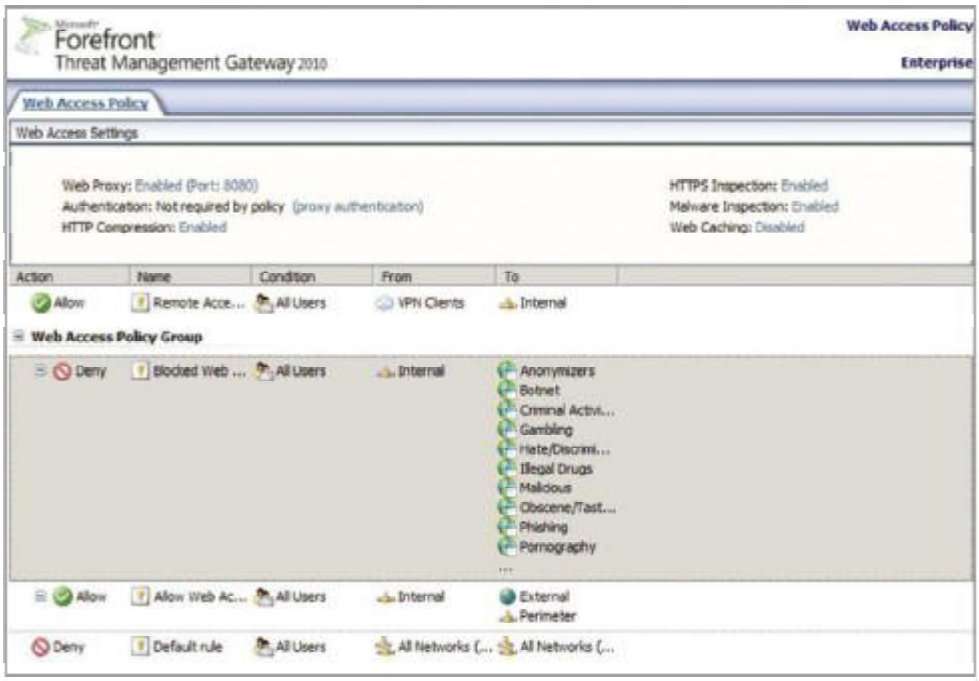


Figure III.17 La console d'administration Forefront TMG simplifie la création de stratégies.

- **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.

3. **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.

4. 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.

3. Le firewall FortiGate de Fortinet

3. a. 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 optimiser l'ensemble des fonctions de sécurité, des couches réseaux aux couches applicatives.

L'applianceFortiGate 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.

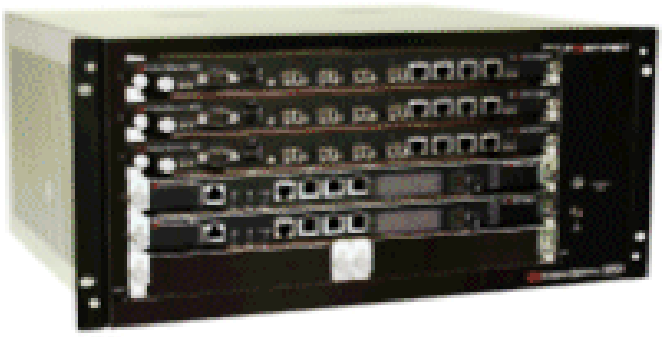


Figure III.18: Le firewall FortiGate.

3. b.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.

3. c. 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.

4. Le firewall SideWinder

4. a.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 III.19: Le firewall SideWinder.

4. b.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.

II.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.

Conclusion

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 sachant qu'on ne peut jamais atteindre 100% de sécurité.

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

Introduction

L'apparition de l'internet et des nouvelles technologies donne 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.

Cependant, il est difficile, voire impossible, d'assurer la sécurité à 100%. Et ce, quelle que soit la performance et l'efficacité des outils et techniques utilisés pour la mise en place d'une solution de sécurité.

Dans ce chapitre nous présenterons les différentes étapes suivies afin d'implémenter quelques solutions citées précédemment. 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.

1. Présentation des outils utilisés

1.1. 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 0.8.2 (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).

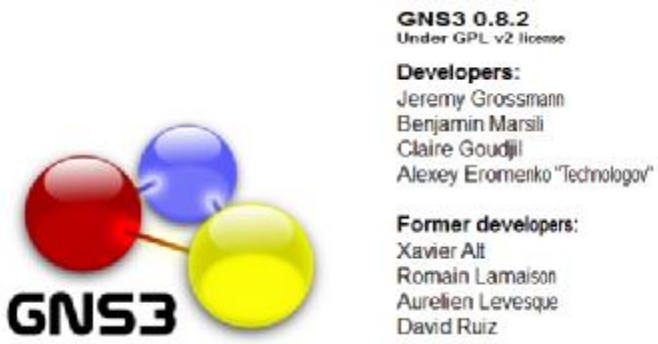


Figure IV.1 : GNS3

.

1.2. La VMware Workstation 10.0.0

Pour l'émulation de notre réseau, nous avons choisi d'utiliser la VMware Workstation 10.0.0. 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.

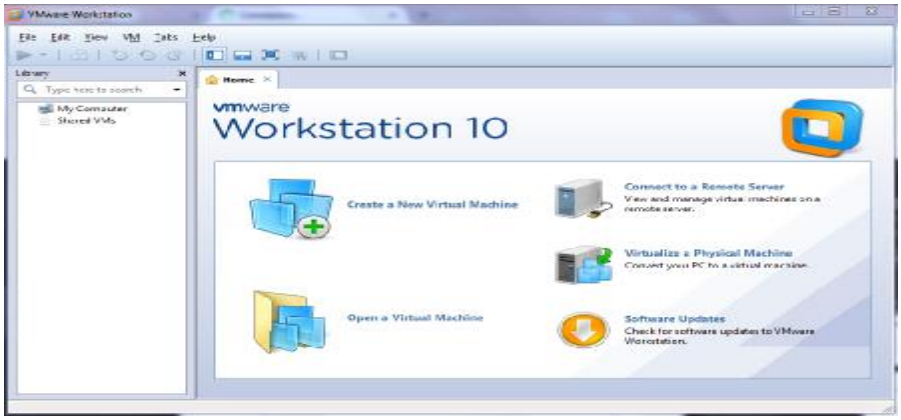


Figure IV.2: VMware Workstation 10.

1.3. 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 IV.3: Server 2008.

1.4. Microsoft Windows Server 2012

Windows Server 2012 rassemble toute l'expertise acquise par Microsoft dans la conception et la mise en œuvre de Clouds publics. C'est une plateforme idéale pour les Datacenters et Clouds privés, tout en étant hautement dynamique, disponible avec des coûts de fonctionnement optimisés.

Avec Windows Server 2012, les entreprises et les hébergeurs peuvent tirer tous les avantages d'une infrastructure Cloud qui est à la fois évolutive, dynamique et multi-tenante. Elle

assure une connexion sécurisée à vos applications dans les entreprises ou dans le Cloud et permet à l'IT de répondre aux besoins des utilisateurs de manière plus rapide et plus efficace.

Figure IV.4 : Server 2012.

1.5. 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 IV.5: Active Directory.

1.6. 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 6G
- Disque dur 500 G
- Système Windows 7 professionnel x64 bits
- Prise en charge de la virtualisation.

2. 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.

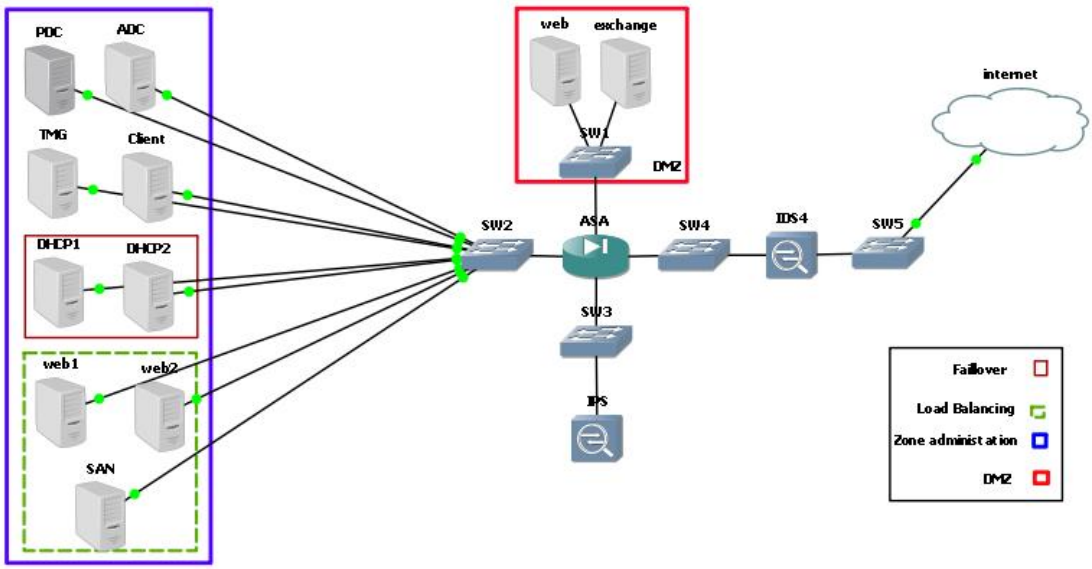


Figure IV.6 : L'infrastructure réseau mise en place sous GNS3.

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 sous Windows serveur 2012 (PDC).
- Un contrôleur de domaine secondaire sous Windows serveur 2012(ADC).
- Un serveur membre pour l'installation de la TMG sous Windows serveur 2008(TMG).
- Un serveur membre pour l'installation de Microsoft Exchange Server 2010 sous Windows serveur 2008 (exchange).
- Deux serveurs membre pour l'installation de serveur Web sous Windows serveur 2012 (web1 et web2 pour l'implémentation de la solution load balancing).
- Une machine membre client interne qui fait office de machine test. (Windows 7)
- Deux machines membres pour l'implémentation de la solution failover.
- Une machine membre pour la base de données (SAN).
- 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 2012, nous avons installé sur la première machine un contrôleur de domaine principal (PDC), **BAlgerie.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.

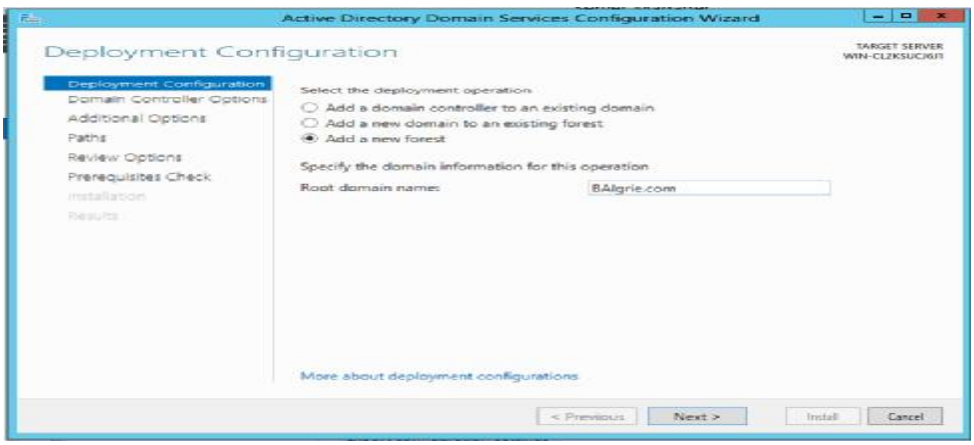


Figure IV.7: La création du domaine principal.

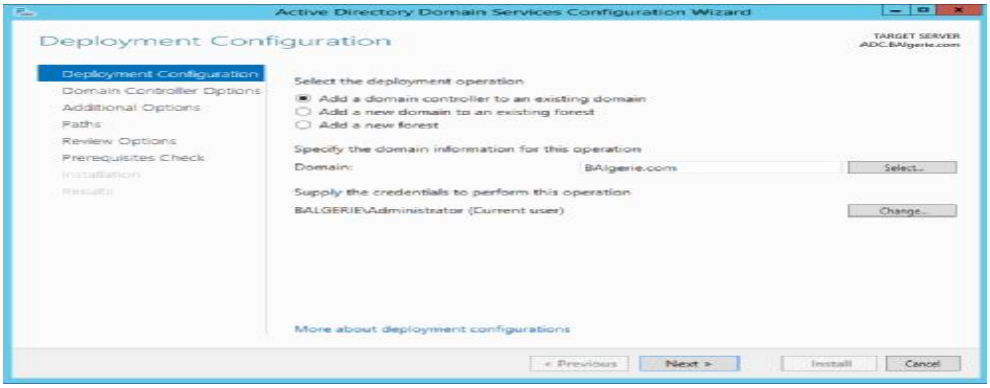


Figure IV.8: L'ajout du domaine secondaire.

Dans l'annexe B, vous trouverez l'installation et le fonctionnement de l'Active Directory sous le Windows serveur 2012.

2. Connecté un server membre au domaine principal :

Un domaine est un ensemble d'ordinateurs formant un réseau qui obéit à des règles et des procédures communes et qui est géré comme une unité. Chaque domaine possède un nom unique. Les domaines sont généralement utilisés pour les réseaux d'entreprise. Pour connecter un ordinateur à un domaine, on doit connaître le nom du domaine et posséder un compte d'utilisateur valide sur le domaine.

Pour se faire, on suit les étapes illustré si après :

- On clique sur le bouton **Démarrer**, un clic droit sur **Ordinateur**, puis sur **Propriétés** pour avoir l'onglet system par la suite on clique sur **modifier les paramètres (Change settings).**

Figure IV.9 : System

- Une fenêtre propriété system apparait, on clique sur **Modifier (Change)**

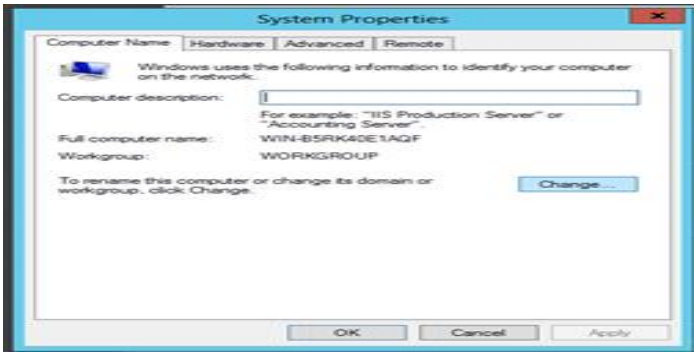


Figure IV.10 : Propriétés system

- On saisit le nom du serveur (machine) qui est dans ce cas « **Web1** »ainsi que le nom du domaine que l'en souhaite rejoindre, qui est dans notre cas « **BAlgerie.com »,** on valide les informations en cliquant sur **OK.**

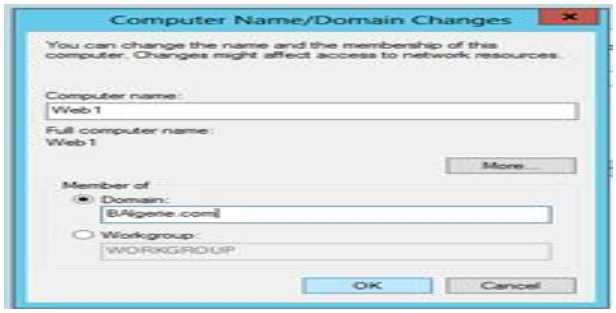


Figure IV.11: Modification du nom ou du domaine de l'ordinateur

- Dans l'onglet sécurité Windows on tape le **nom d'utilisateur** et le **mot de passe** du domaine, on clique sur OK.

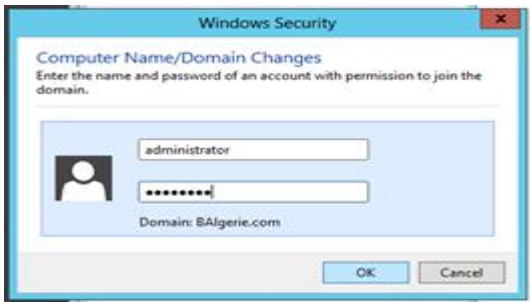


Figure IV.12 : Sécurité Windows

- Ainsi on a rejoint le domaine BAlgerie.com et une boite de confirmation apparait.

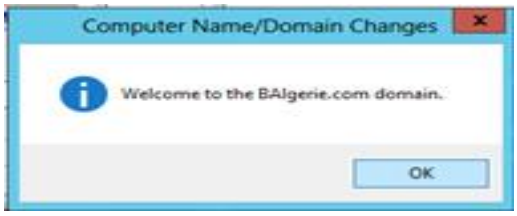


Figure IV.13 : Boite de confirmation

Il est nécessaire de redémarrer la machine pour que les modifications prennent effet.

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 cartes réseaux :

- Une interne avec l'adresse 172.16.0.250/
- Une externe avec l'adresse 192.168.2.250/
- Une pour la DMZ avec l'adresse 10.0.0.250/

3. Installation du serveur Web IIS

Le rôle du serveur Web l'IIS de Windows Server 2012 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 B).

4. Lancement de l'installation de la TMG

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

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.

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

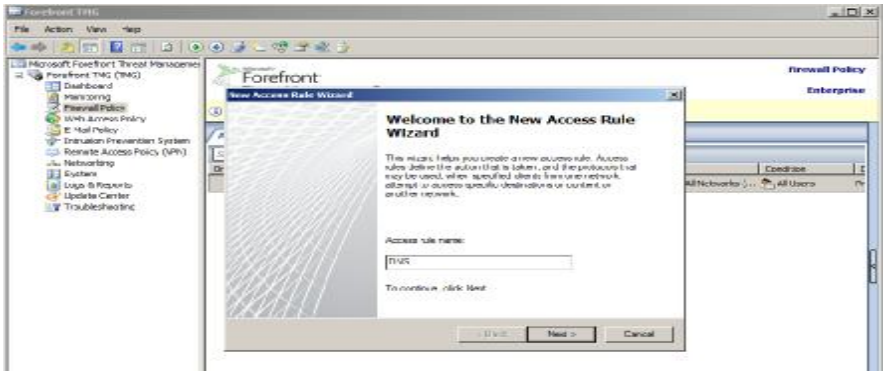


Figure IV.14: création de la règle d'accès DNS.

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

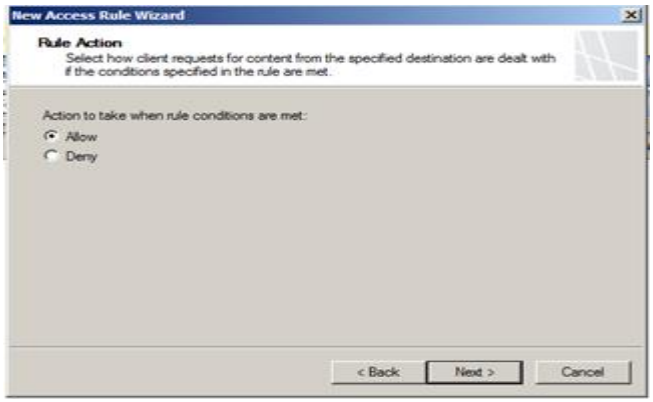


Figure IV.15: Choix de l'action de la règle.

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

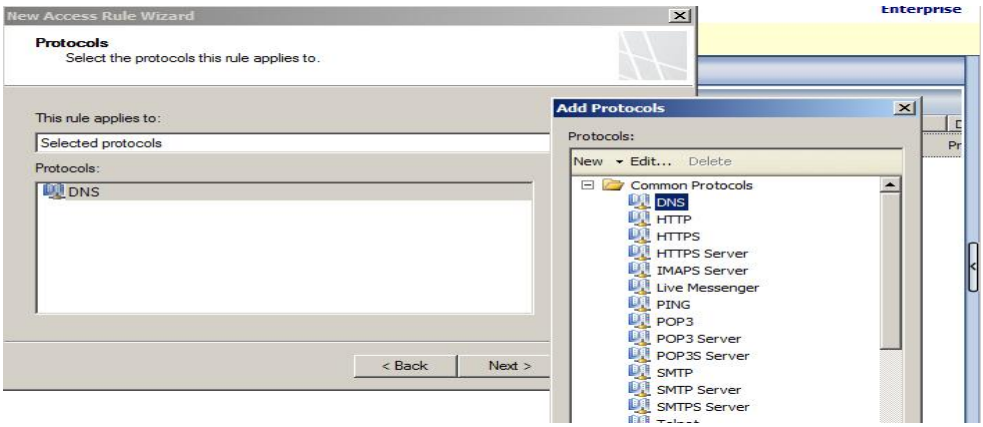


Figure IV.16 : Sélection des protocoles.

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

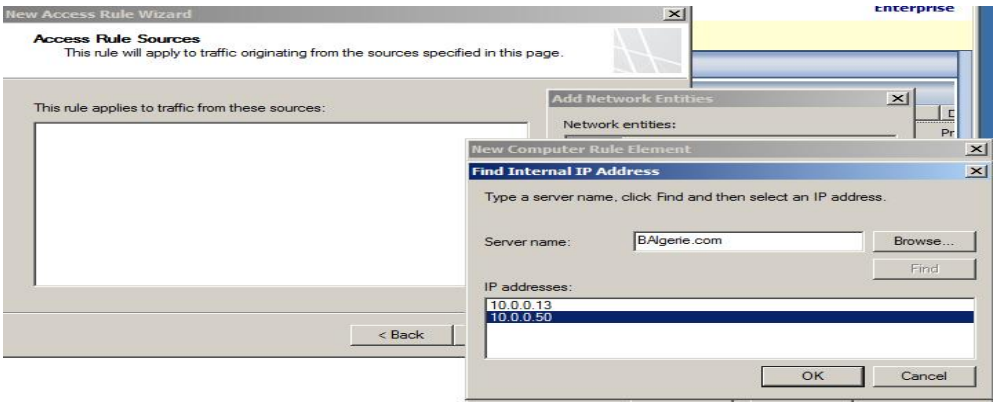


Figure IV.17 : Sélection de la source de règle d'accès.

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

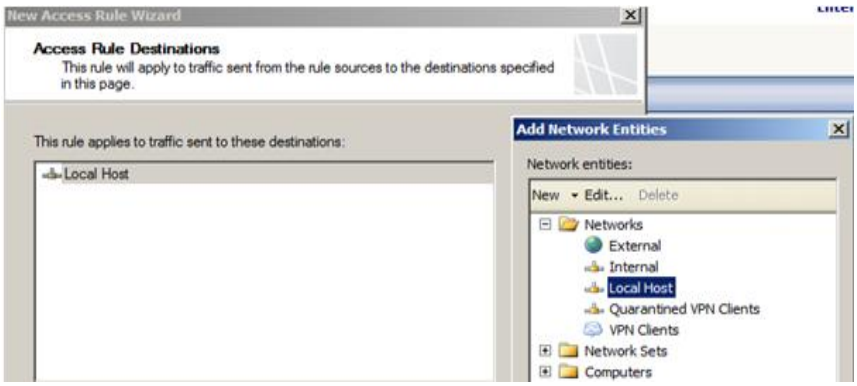


Figure IV.18 : Spécification de la destination de la règle d'accès.

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

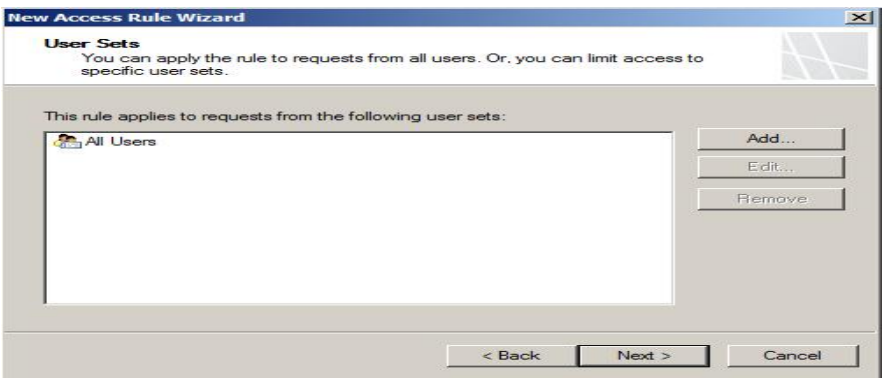


Figure IV.19: les utilisateurs concernés par la règle d'accès

Valider le récapitulatif

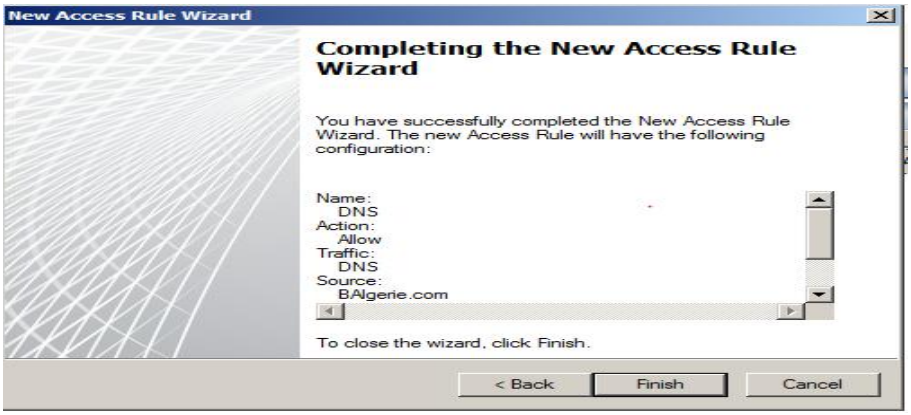


Figure IV.20 : le récapitulatif de la configuration la règle DNS

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

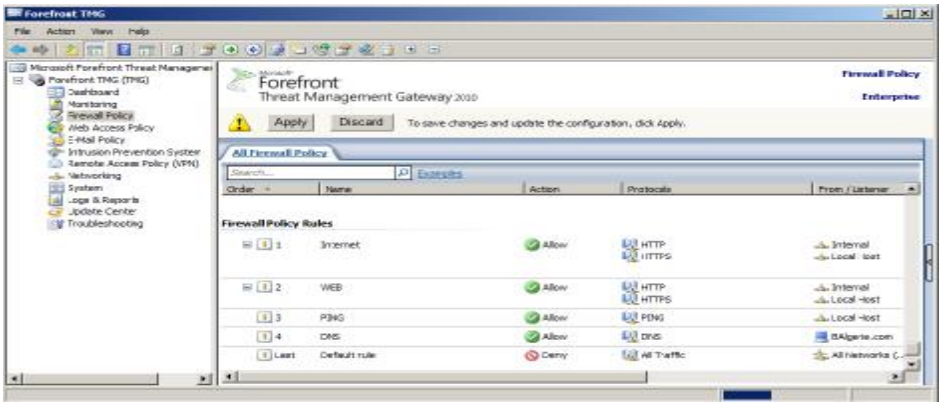


Figure IV.21: Récapitulatif des règles TMG

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 :

L'installation d'exchange 2010 nécessite un active directory de niveau fonctionnel minimum 2003, afin de 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 :

Afin d'importer les modules du gestionnaire de serveur nous avons utilisé la commande suivante : >> Import-Module ServerManager

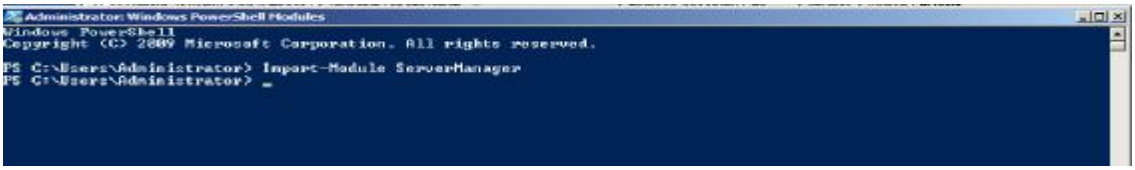


Figure IV.22: L'importation des modules de gestionnaire de serveur.

Apres que les modules sont importés, on passe à leurs ajout par la commande :

>> Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-server,Web-Basic-Auth,Web-windows-Auth,Web-Metabase,Web-Net-Ext,Web-Lgcy-Mgmt-Console,WAS-Process-Model,RSAT-Web-Server,Web-ISAPI-Ext,Web-Digest-Auth,Web-Dyn-Compression,Net-HTTP-Activation,RPC-Over-http-Proxy -Restart

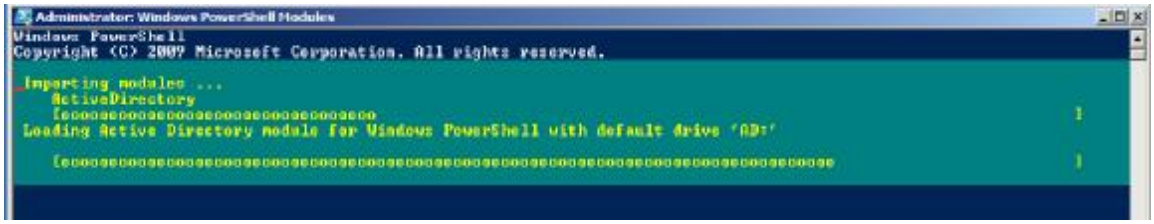


Figure IV.23 : Ajout des modules

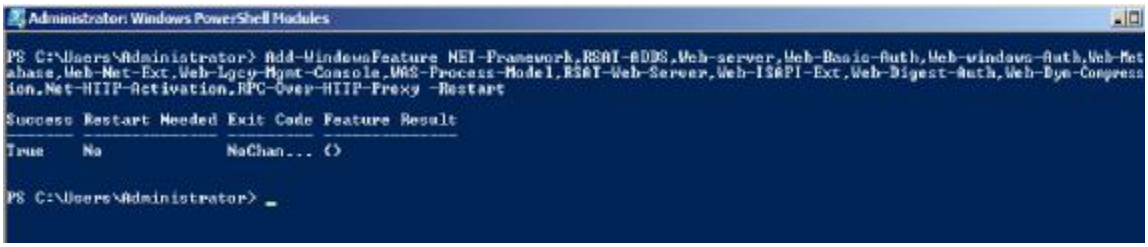


Figure IV.24: L'ajout et installation des fonctionnalités.

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 par la commande >>Set-Service Net-TcpPortSharing –StartupType .

Par la suite on a préparé l'Active Directory pour installer Exchange Server 2010. Pour ce faire nous avons ouvert 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 par la commande :
   C:\>Setup /PrepareSchema.

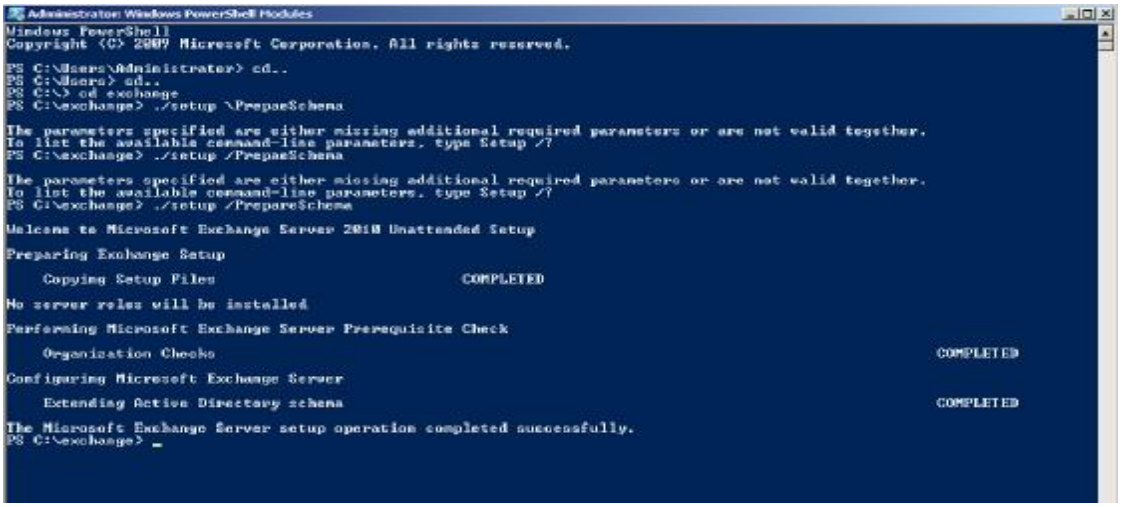


Figure IV.25 : Préparation de schéma Active Directory.

2. La seconde étape consiste à préparer la forêt BAlgerie.com

Command: C:\> Setup /PrepareAD /OrganizationName:BAlgerie

Figure IV.26 : Préparation de la forêt.

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

Commande : C:\>Setup /PrepareDomain.

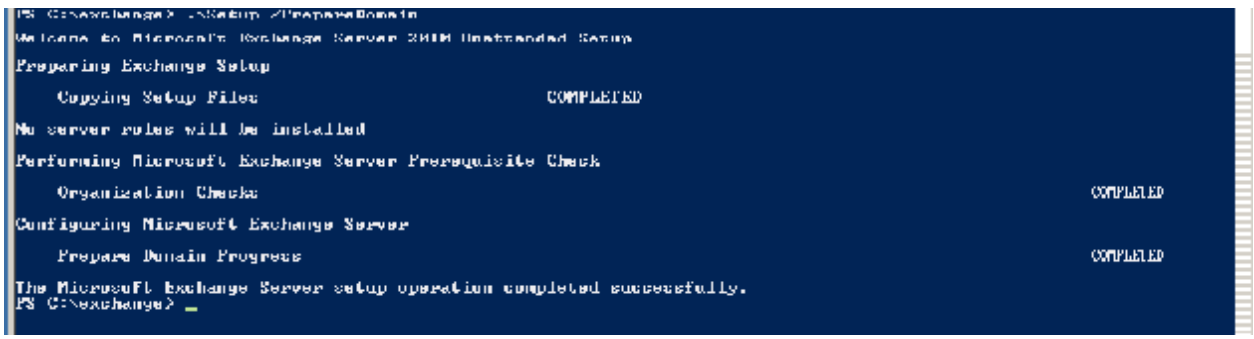


Figure IV.27 : Préparation du domaine.

2. Installation de Microsoft Exchange 2010

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

3. Configuration de Microsoft Exchange 2010

3.1 . 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.**

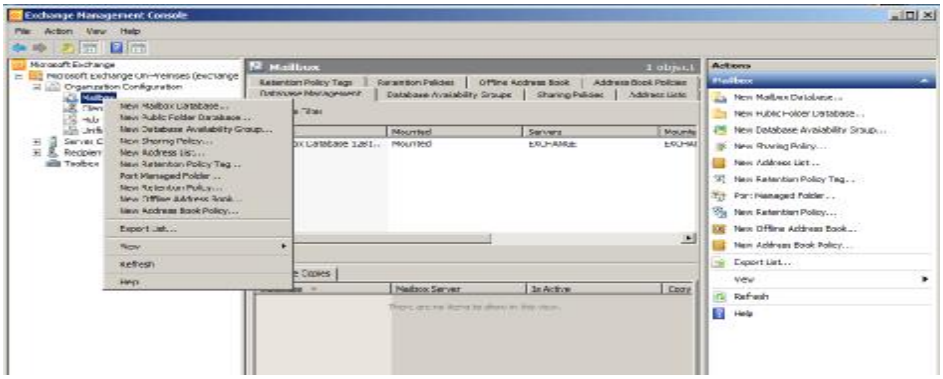


Figure IV.28: chemin de création de la base de données de boite aux lettres

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

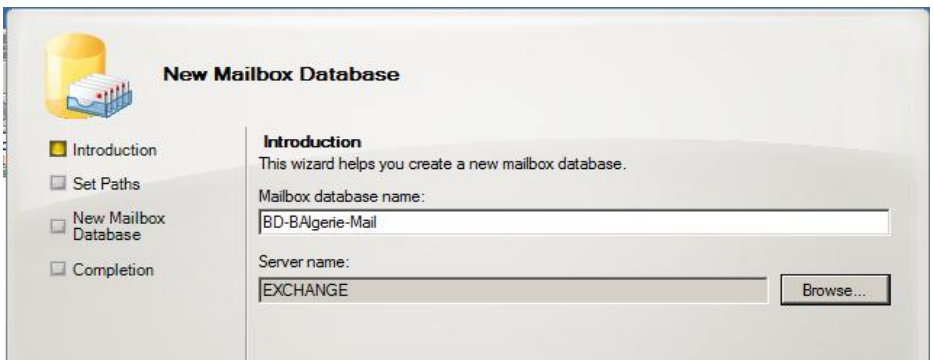


Figure IV.29 : Création de la base de données de boite aux lettres.

3.2. 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 IV.30 : Création de boite aux lettres utilisateur.

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

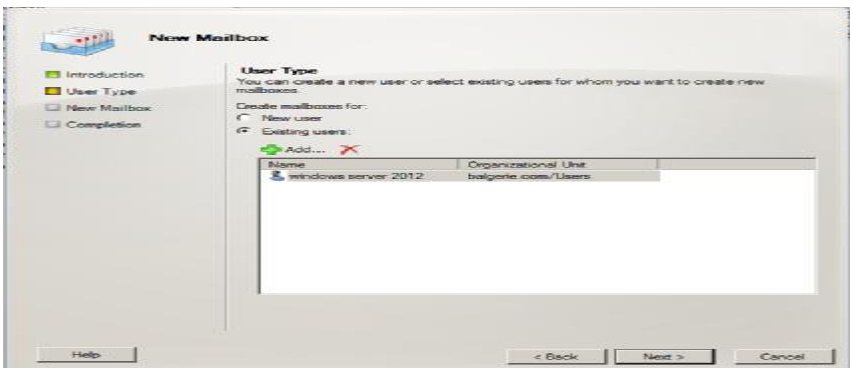


Figure IV.31: Sélection des utilisateurs.

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

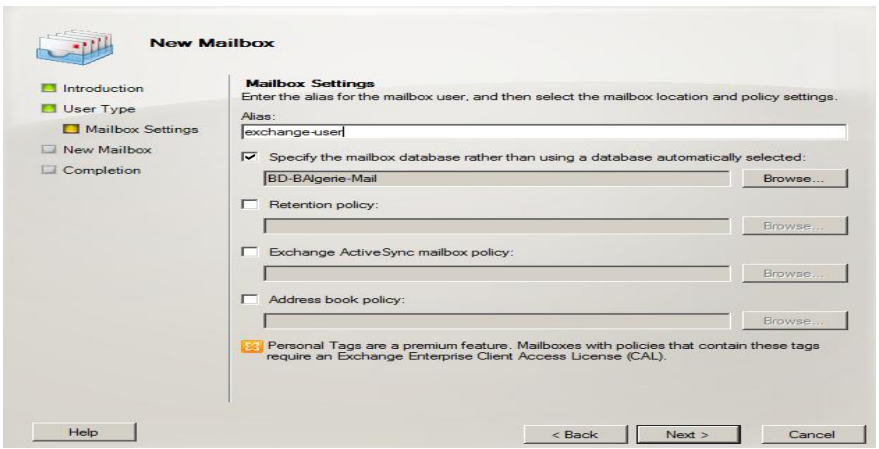


Figure IV.32 : Paramétrage de boite aux lettres

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**.

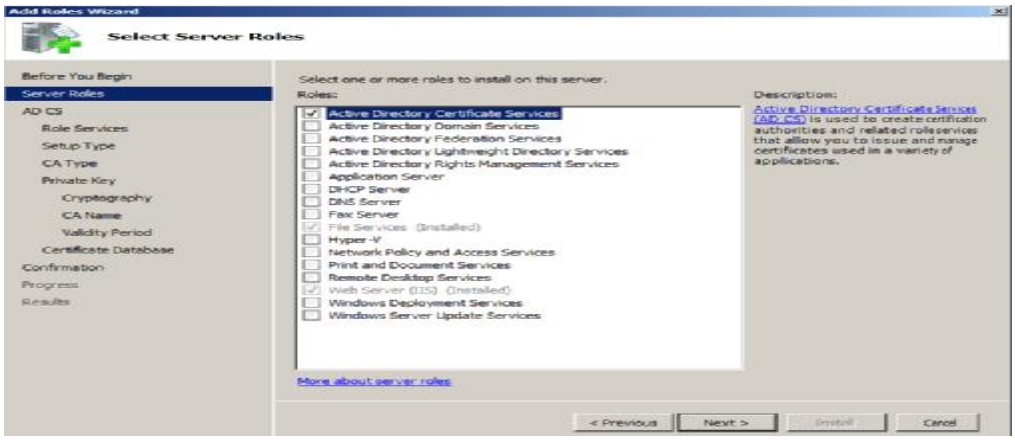


Figure IV.33: Ajout du service de certificats Active Directory.

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 IV.34 : Les services de rôle.

Lors de l'installation, il faut spécifier le type de l'installation de la CA,

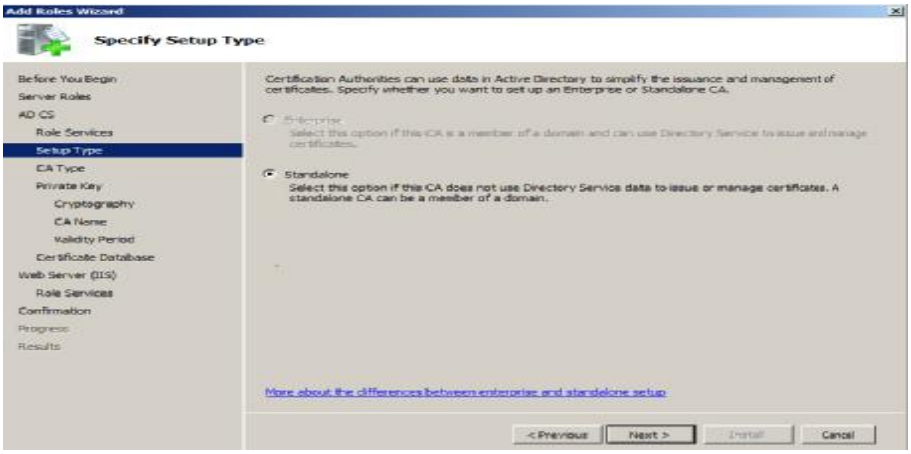


Figure IV.35 : Spécification du type d'installation.

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).

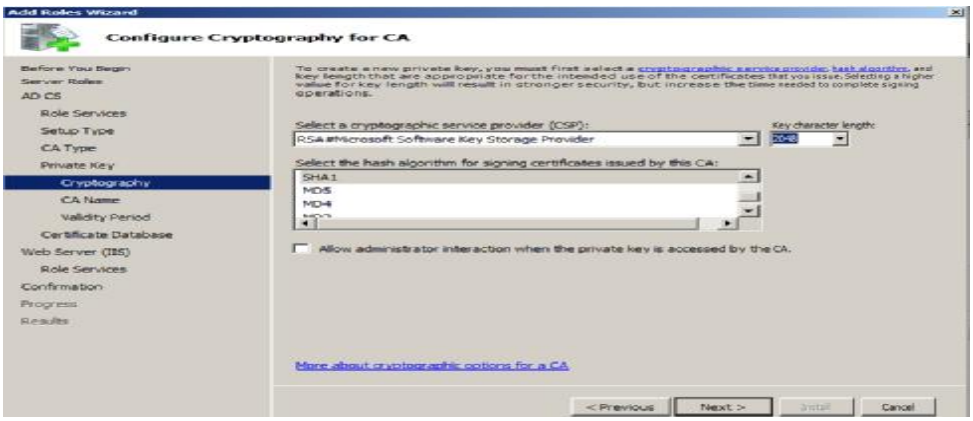


Figure IV.36 : Création d'une nouvelle clé privée.

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

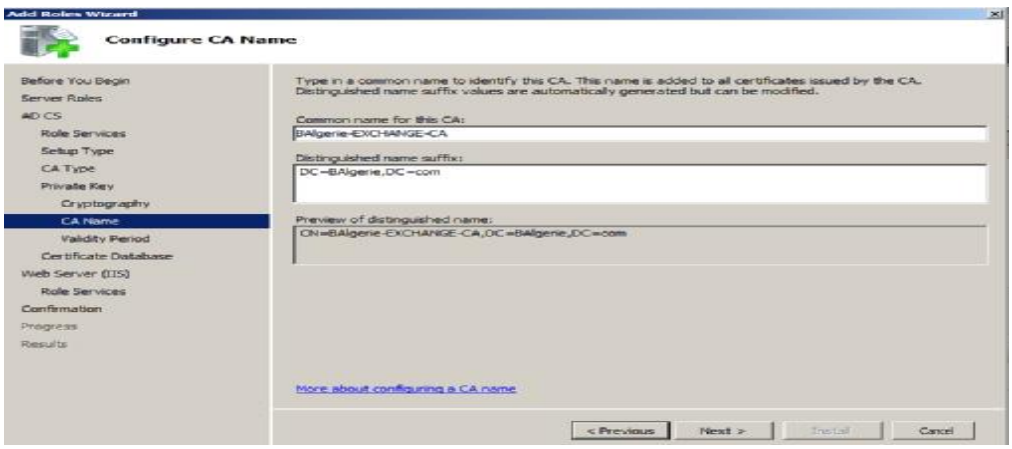


Figure IV.37: Nomination de l'Autorité de certificat.

En cliquant sur installer l'AD CS ainsi que le Web Server (IIS) seront installé, comme c'est illustré ci-dessous

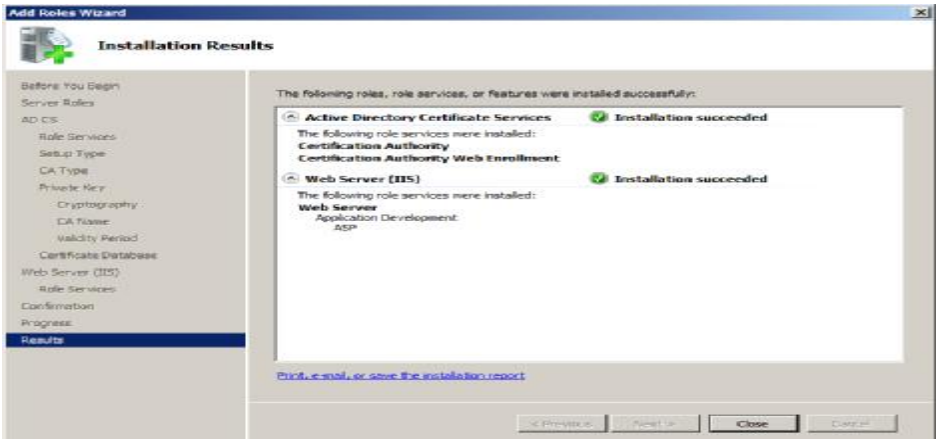


Figure IV.32 : Installation d'Autorité de Certificat

Nous remarquons qu'un certificat auto-signé d'exchange pour exchange (du nom d'hôte pour le nom d'hôte) est aussi créé automatiquement dans serveur IIS. 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 è 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.

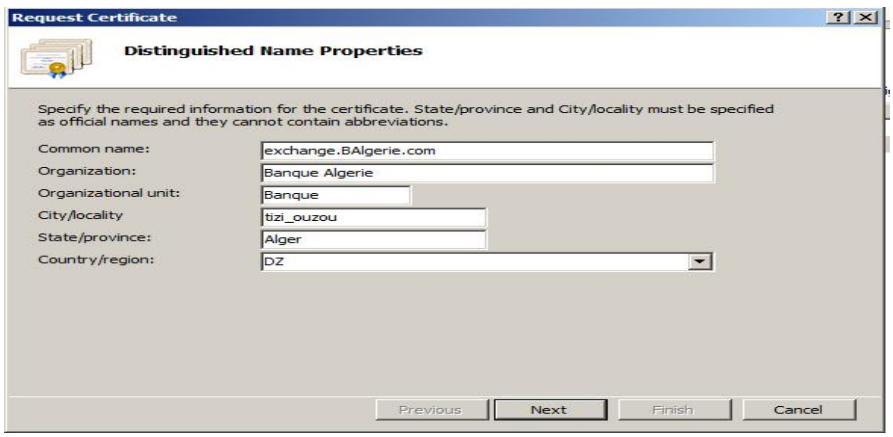


Figure IV.33: Demande de certificat.

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

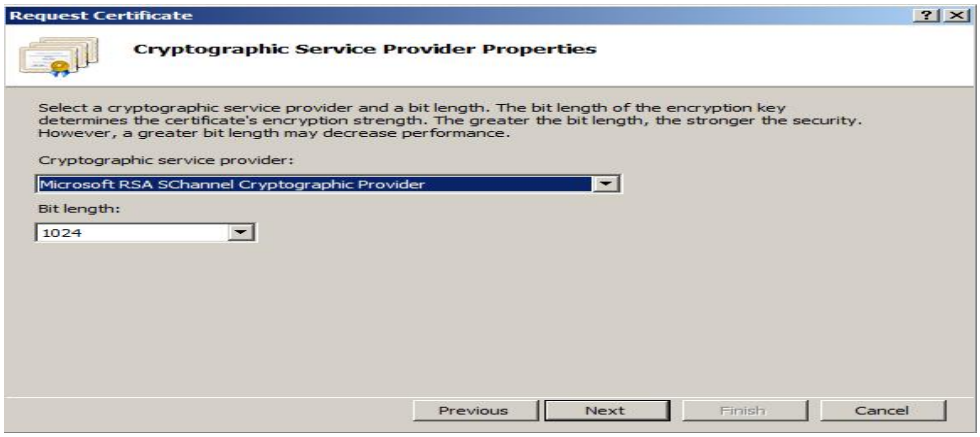


Figure IV.34: Propriétés du fournisseur de services de chiffrement

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

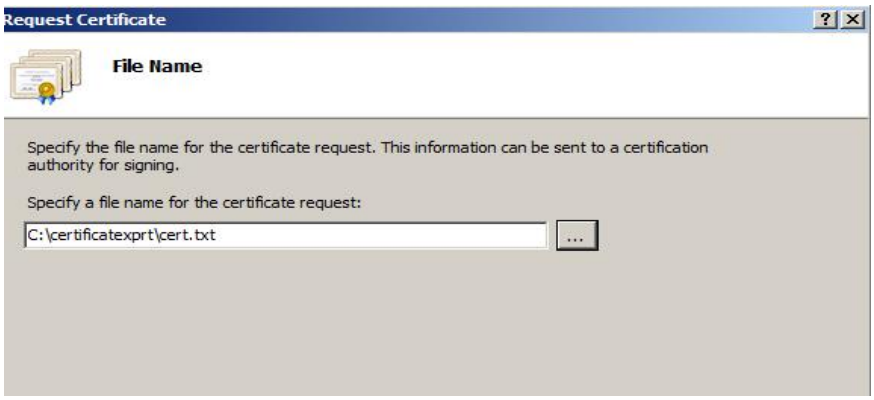


Figure IV.35 : Fichier de demande de certificat.

Pour soumettre la demande de certificat via internet explore suivant ces étapes : *https://localhost/certsrv* **è** demande de certificat **è** 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.

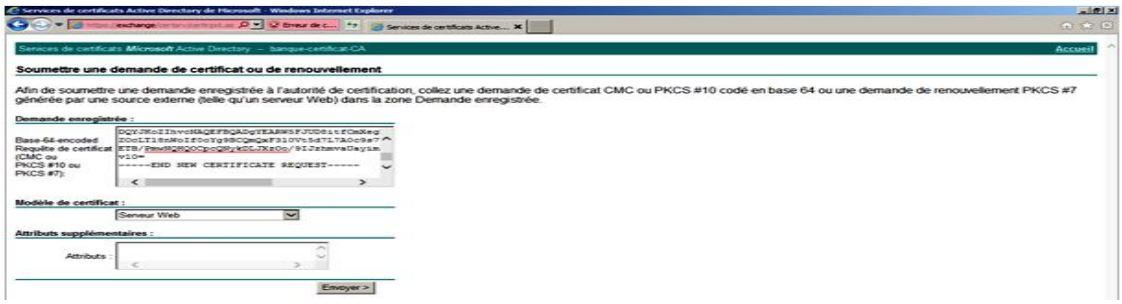


Figure IV.36 : Soumettre une demande de certificat.

Téléchargeons le certificat en spécifiant son emplacement.

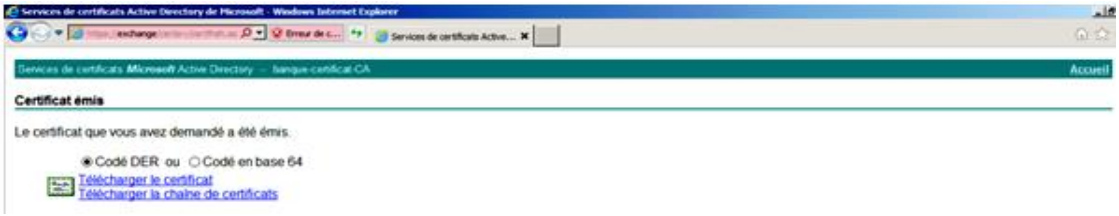


Figure IV.37 : Téléchargement de certificat.

3. Terminer la demande de certificat

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

Figure IV.38 : Terminer la demande de certificat.

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

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.

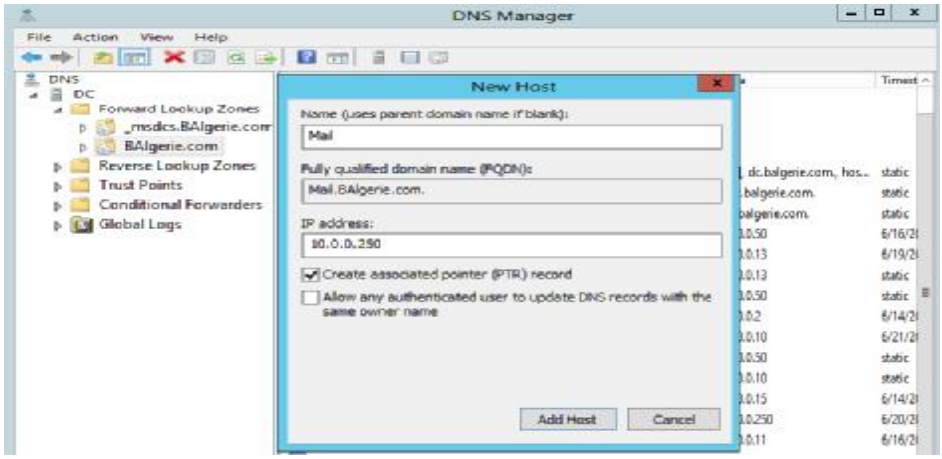


Figure IV.39: Enregistrement de serveur de messagerie Exchange.

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.BAlgerie.com**

5. La publication du serveur de messagerie via TMG

A ce stade si nous essayons d'accéder avec l'adresse https://Mail.BAlgerie.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 avons procédé comme suit :

Depuis le serveur exchange :

- Nous avons exporté l'autorité de certificat BAlgerie-certificat-CA.et le BAlgerie-exchange-CA.L'exportation se fera d'une manière sécurisée avec l'utilisation de l'administrateur et d'un mot de passe.
- Nous avons mis ces certificats exportés dans un dossier et partageons les avec, pour autoriser la lecture uniquement par l'administrateur.
- Ayant été partagé, le dossier peut être lu depuis la TMG, où il sera copié.

5.a. L'exportation du certificat

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 :

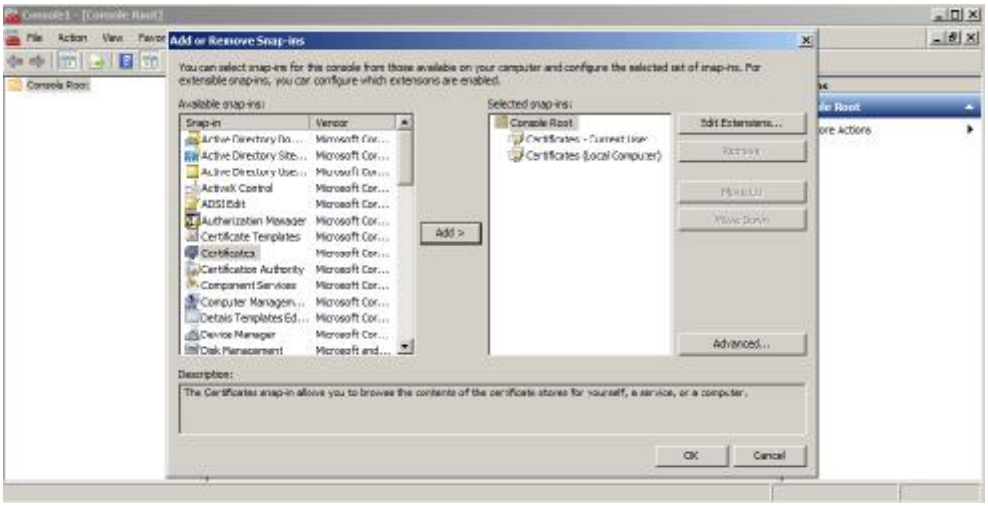


Figure IV.40: Les certificats avec la Console Microsoft

Dans certificat (ordinateur local) **è** dossier autorité de certificat **è** BAlgerie-certificat-CA **è** exportons la clé privée comme suit :

Figure IV.41: Exportation de la clé privée.

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

Figure IV.42: format du fichier d'exportation.

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

Figure IV.43 : Mot de passe.

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

Figure IV.44: Fichier à exporter.

5. b. Importation du certificat

Maintenant que la CA et le certificat exchange.BAlgerie.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 :

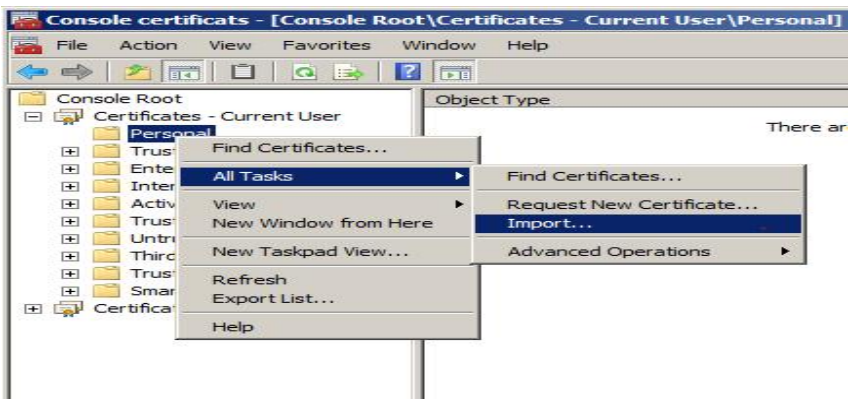


Figure IV.45: La console MMC.

Sélectionnons le fichier à importer.

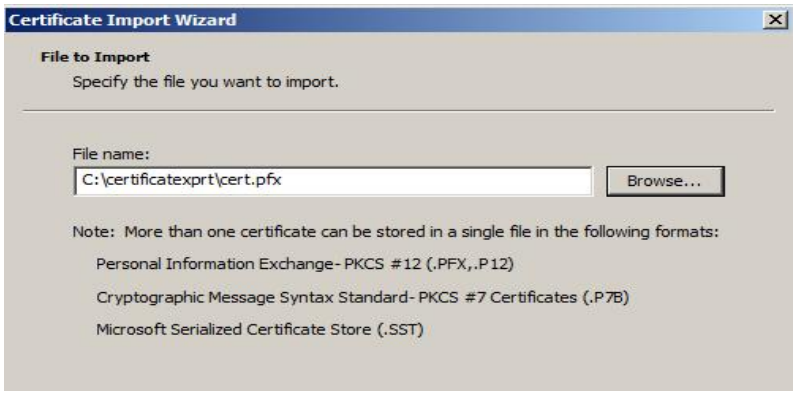


Figure IV.46: Fichier à importer.

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

Figure IV.47: Mot de passe.

6.Création du certificat Mail.BAlgerie.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.BAlgerie.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 **è** toutes les tâches **è** opérations avancées **è** gérer les stratégies d'inscription.

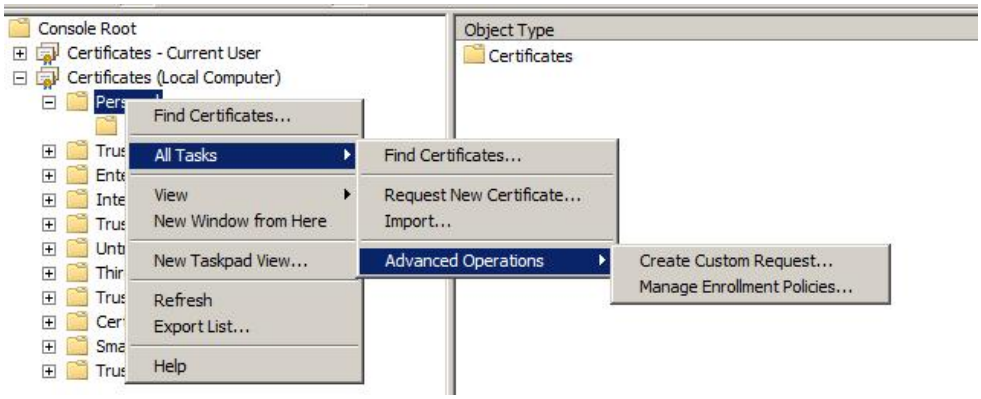


Figure IV.48 : Gestion des inscriptions.

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.

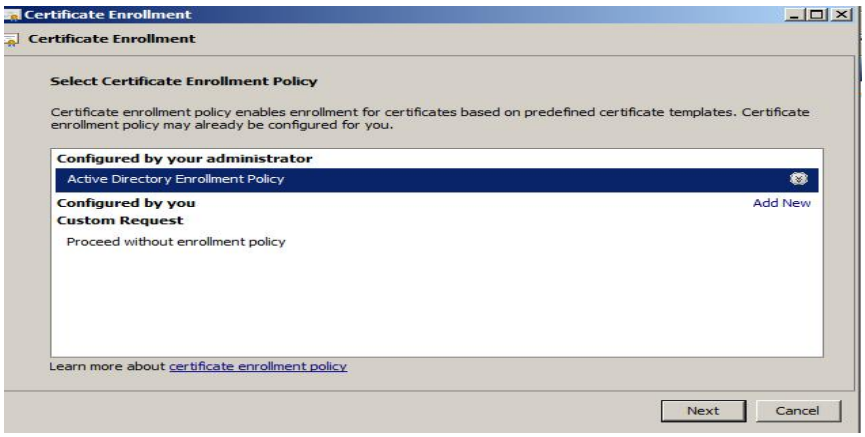


Figure IV.49: Sélection de la stratégie d'inscription de certificat

Nous avons utilisé le certificat pour l'échange de mail via le web, le modèle choisi est donc Serveur Web avec le format PKCS #10

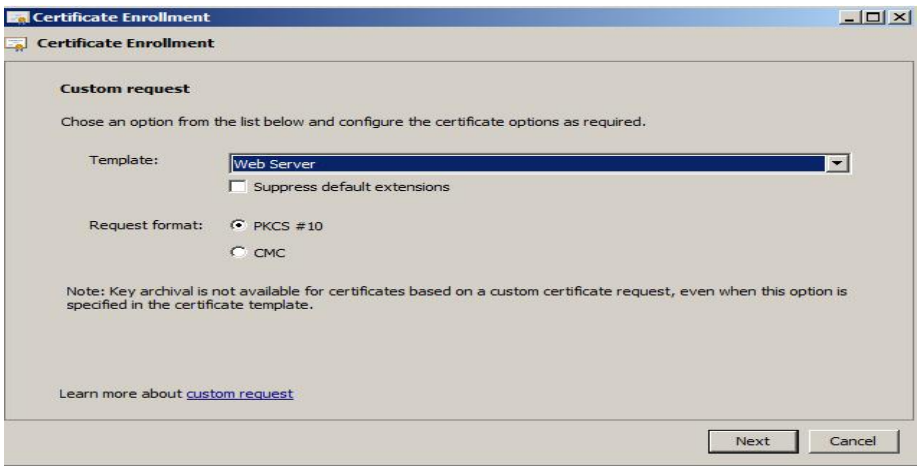


Figure IV.50: demande personnalisée.

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

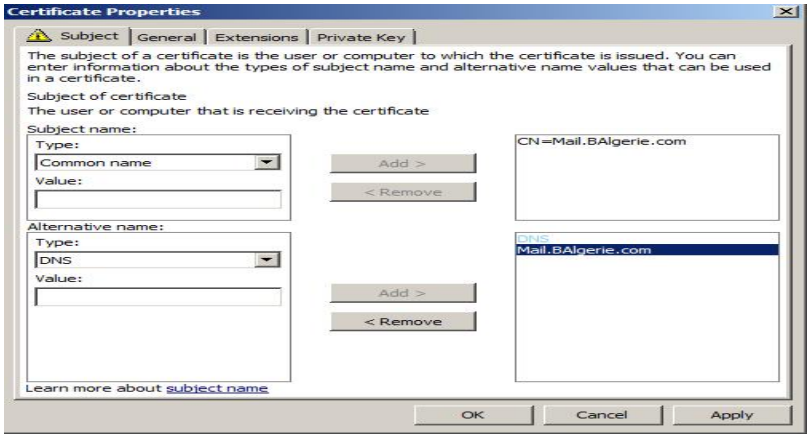


Figure IV.51: Objet de propriétés du certificat.

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.

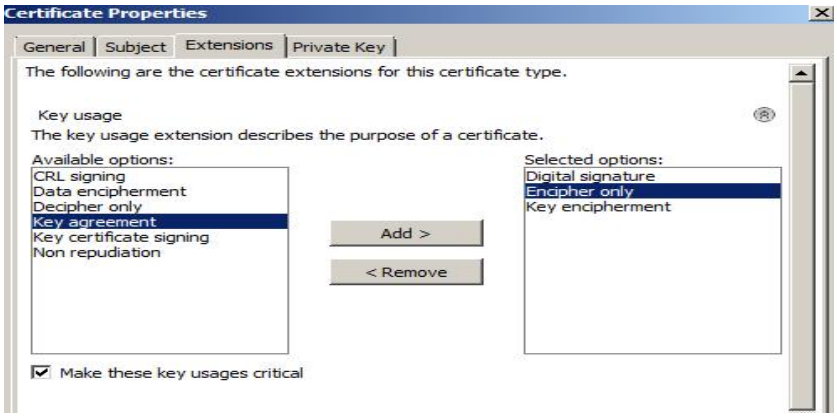


Figure IV.52: Extension de propriétés du certificat.

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

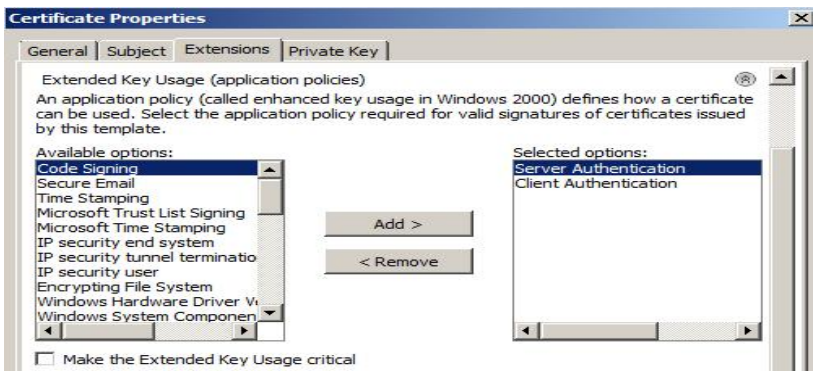


Figure IV.53: Stratégie application de propriétés du certificat.

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

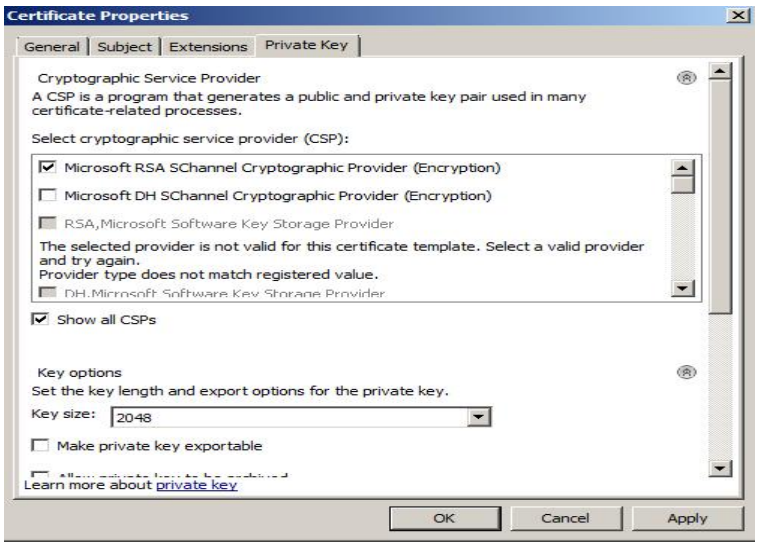


Figure IV.54: Clé privée de propriétés du certificat.

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

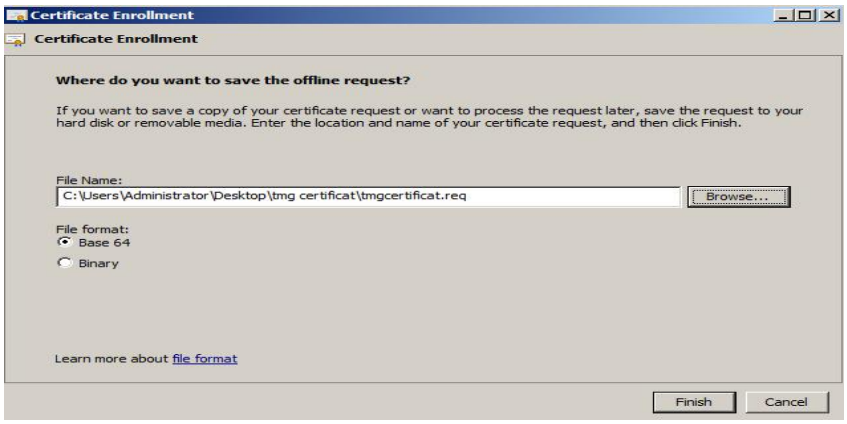


Figure IV.55 : Format fichier.

Pour finaliser la demande de certificat, nous utilisons l'Internet explorer pour télécharger et installer La CA sur TMG en suivant les mêmes étapes que sur le serveur exchange. Une fois la CA installé on ajoute la règle d'accès pour la TMG permettant un accès à OWA.

7. Ajout de règle d'accès TMG

7.1Configuration d'Exchange pour l'accès au site web de l'extérieur.

7.1.1. Configuration des connecteurs

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

7.1.1. 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.

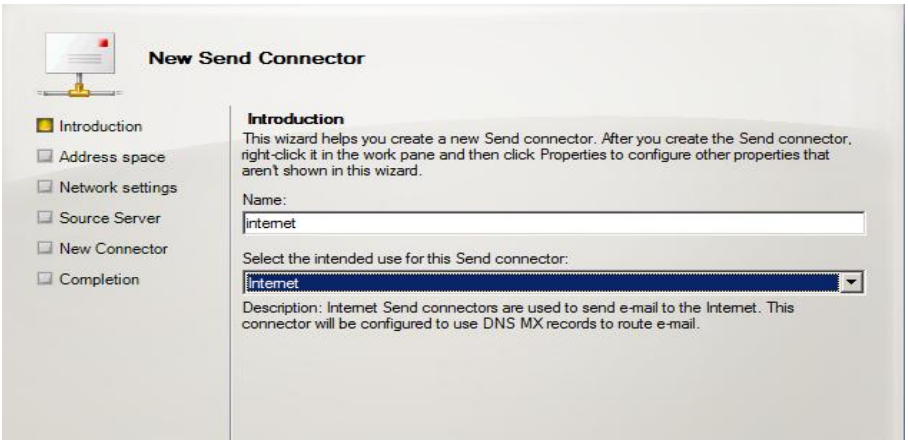


Figure IV.56 : Création d'un nouveau connecteur d'envoi.

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.

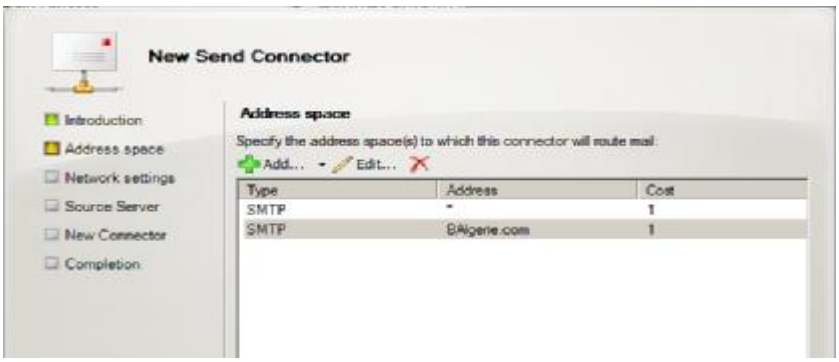


Figure IV.57 : Espace d'adressage.

- Ensuite, nous avons configuré 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.
- On termine par la spécification du serveur source qui est le HUB de transport, **Exchange.BAlgerie.com,** qui permet l'envoi de mails

Figure IV.58 : Fin de création

7.1.1.b. Connecteur de réception

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

7.2. Configuration d'Outlook Anywhere

Pour permettre à OWA d'être vu de l'extérieur nous avons activé l'Outlook Anywhere. Dans configuration du serveur **è** accès au client **è** activer Outlook Anywhere.

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.

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

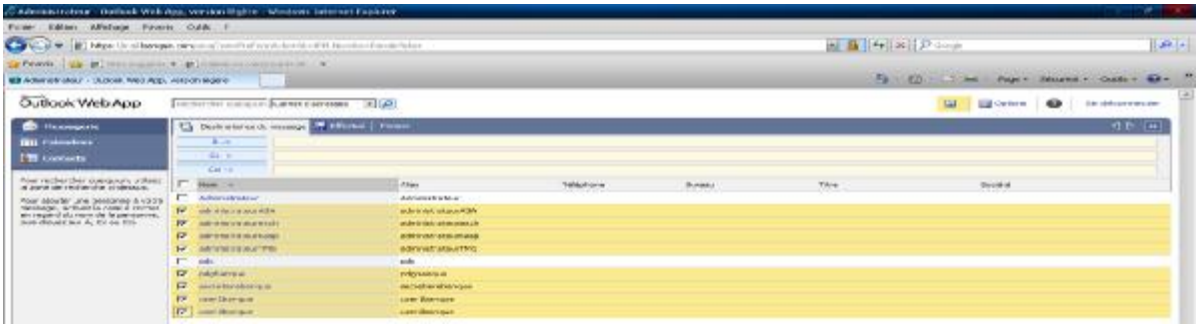


Figure IV.59: La sélection des contacts de la banque.

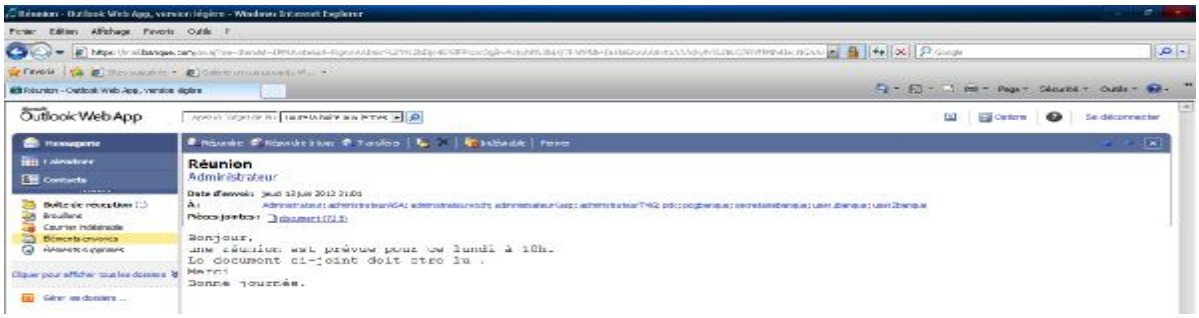


Figure IV.60: Message envoyé.

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

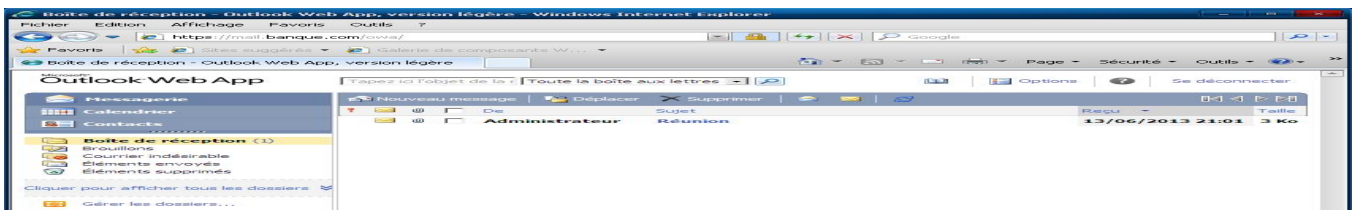


Figure IV.61 : Message reçu

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

1. Installation de SAN

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.a. Configuration de SAN

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 disque. Quand un disque est défaillant, Windows server 2012 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 disk E, F, G, H (Annexe C). Pour accéder à ces disques nous avons configuré le iSCSI Initiateur, pour le faire, dans outils d'administration choisissons iSCSI Initiateur.

2. Installation NLB (Network Load Balancing)

Nous avons configurer le cluster avec répartition de la charge réseau NLB (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 dans notre cas on a effectué le NLB pour les serveur WEB1 et WEB2.

Pour ce faire nous avons suivi les étapes suivantes :

Création de deux serveurs Web sur lesquels nous avons créé deux sites web comme illustré si dessous

3.Création de site web :

Apres avoir installé deux serveurs web IIS (annexe C), les avoir joint au domaine, nous avons aussi créé dans chacun de ses derniers un site web pour ce faire ; nous avons suivi les étapes illustré si après.

Dans gestion de services IIS

Figure IV.62: IIS manager

Nous déroulons le dossier « **Sites** » sur la gauche nous remarquons qu'il y a déjà un site par défaut appelé « **Default Web Site** » qui est créé à l'installation d'IIS et qui écoute sur le port 80.

Afin de créer un nouveau site Web, cliquons sur la colonne de gauche puis «**Ajouter un site Web**». Comme c'est montré dans la figure suivante.

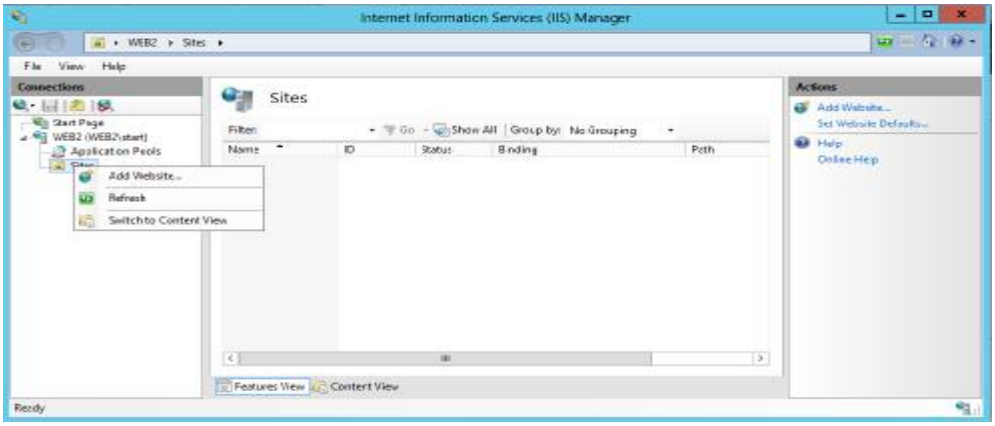


Figure IV.63 : Création de site web

L'assistant d'ajout de site Web s'exécute et quelques informations sur le site à créer sont demandées, on les a remplis comme sur la figure si après :

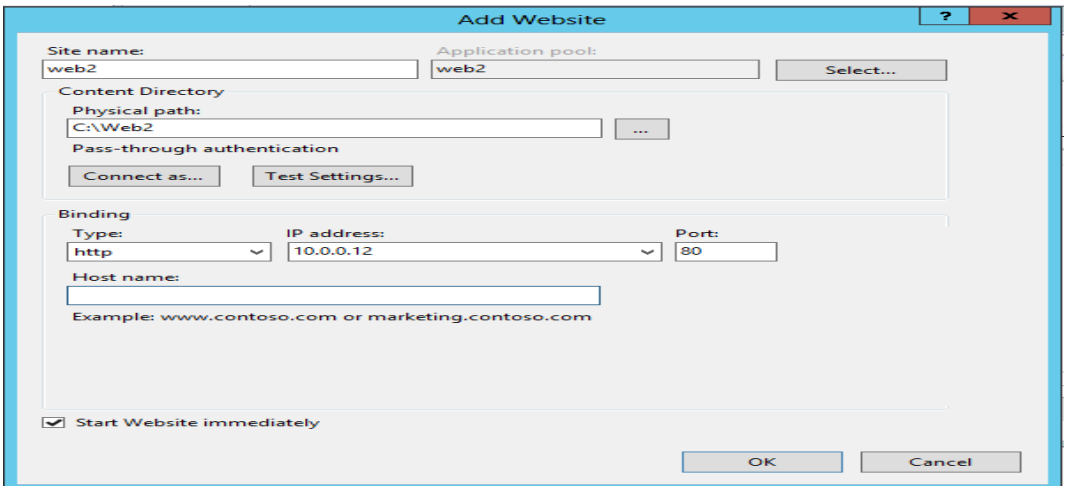


Figure IV.64 : Remplissage des informations.

Une fois les différents champs renseignés, cliquons sur « **OK** » pour validez puis on a créer une page « **.html** » dans le répertoire de notre site web pour obtenir un résultat lors d'une tentative d'accès. La figure si dessous illustre la création de ce dernier.

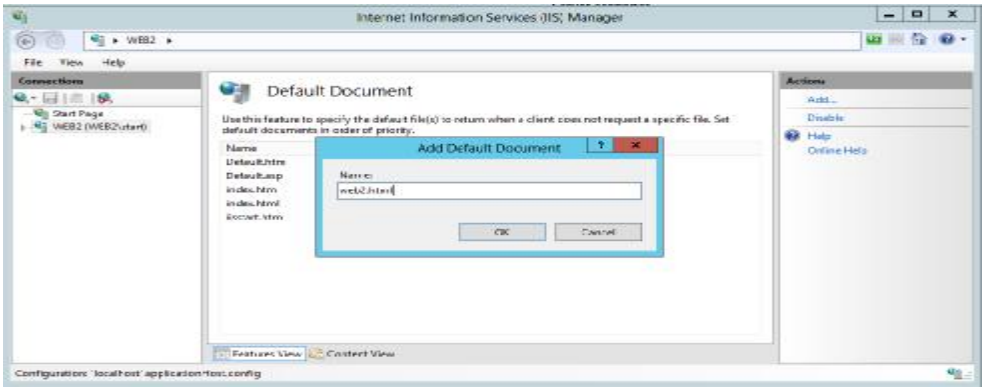


Figure IV.65 : création du document .html

De la même façon ; nous avons fait la création de deuxième site web.

4. L'ajout de rôle de cluster du basculement

Afin d'implémenter cette solution, nous avons préparé les deux nœuds (web1 et web2) membres du domaine BAalgerie.com comme nous l'avons expliqué précédemment, puis nous avons installé, sur ces deux nœuds , la fonctionnalité cluster avec basculement via le gestionnaire de serveur.

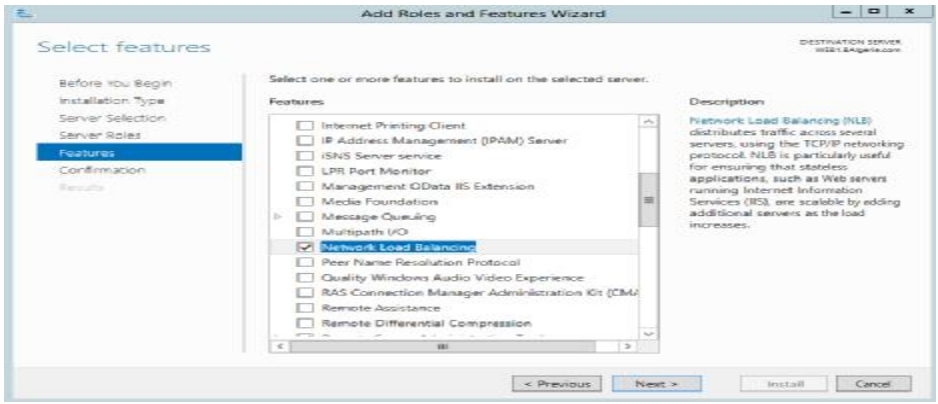


Figure IV.66 : L'ajout de Cluster avec basculement.

Après avoir configuré le stockage, nous connectons ces deux sites 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.

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. On clique droit sur NLB (network load balancing) **è** nouveau cluster

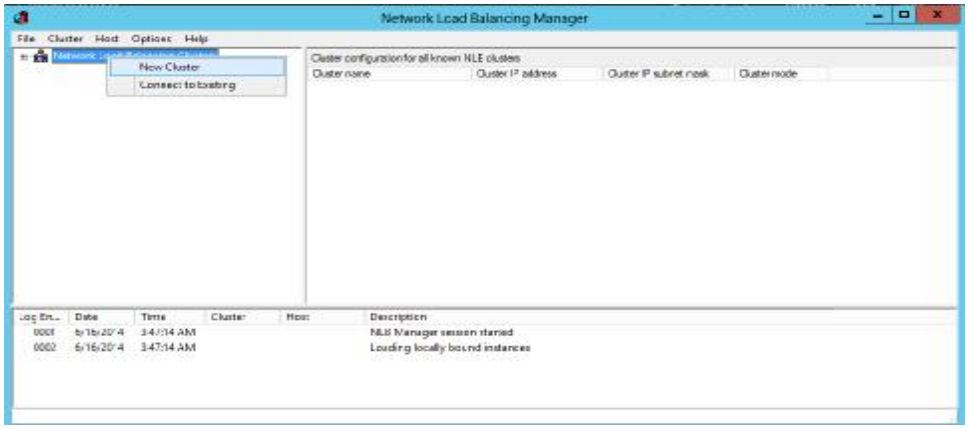


Figure IV.67 : Gestion de cluster de basculement.

Dans la fenêtre qui apparait on saisit les informations des deux sites web1 et web2 comme le montre la figure suivante :

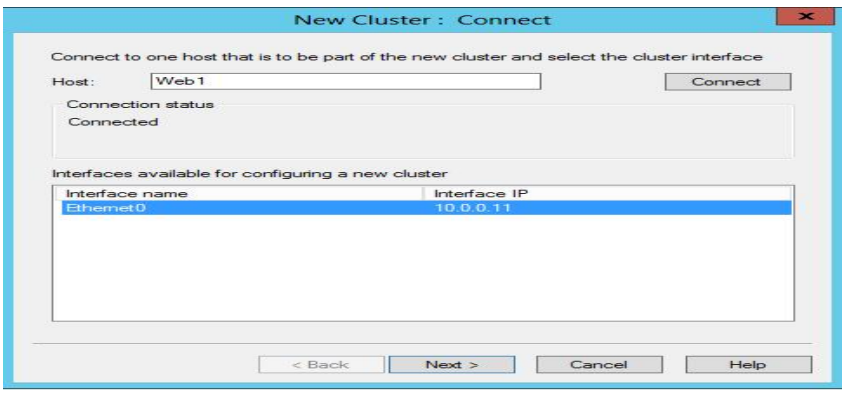


Figure IV.68 : Nouveau cluster avec le web1

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.

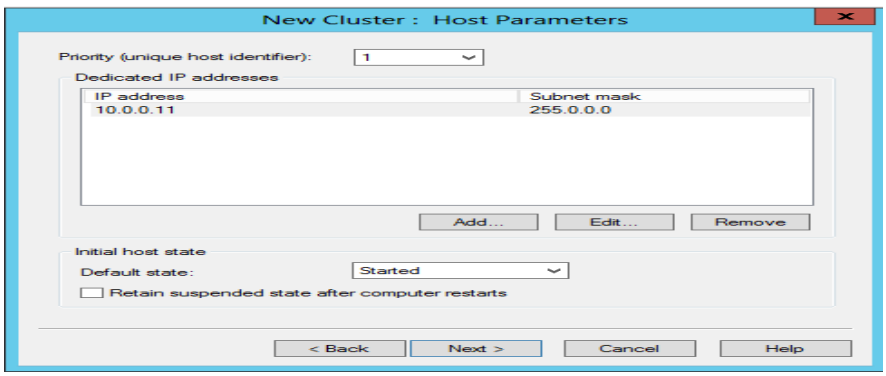


Figure IV.69 : Paramètre de l'hôte

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.

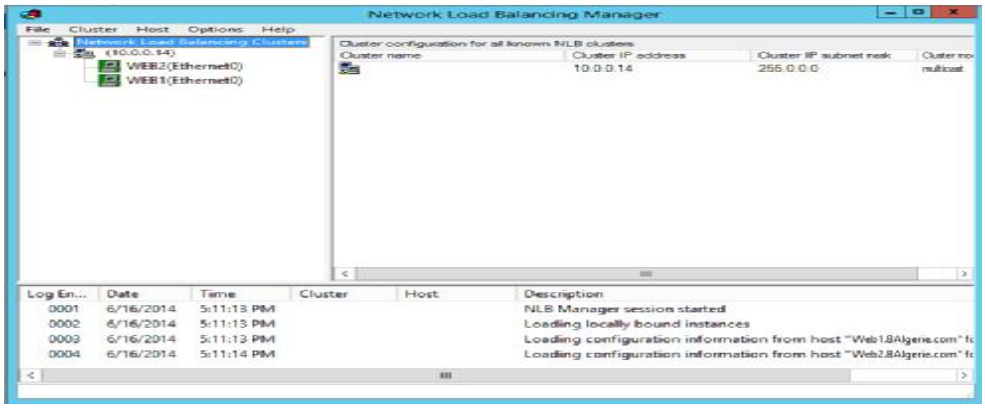


Figure IV.70 : Gestionnaire d'équilibrage de la charge réseau.

On a associe l'adresse IP du cluster aux IIS des deux serveurs :

Server Manager **è** Outils **è** Gestionnaire IIS

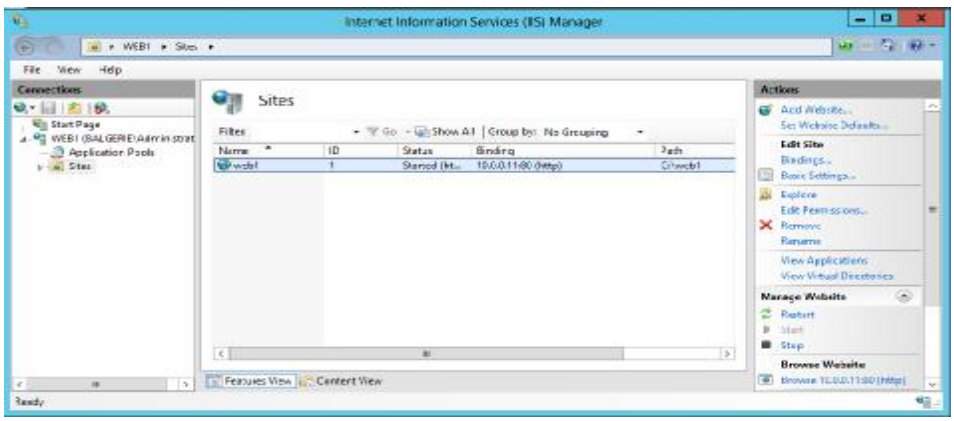


Figure IV.71 : Gestionnaire IIS.

Cliquons sur le dossier Site **è** liaison **è** on ajoute nos deux sites puis on leurs associera l'adresse du cluster comme montré si après :

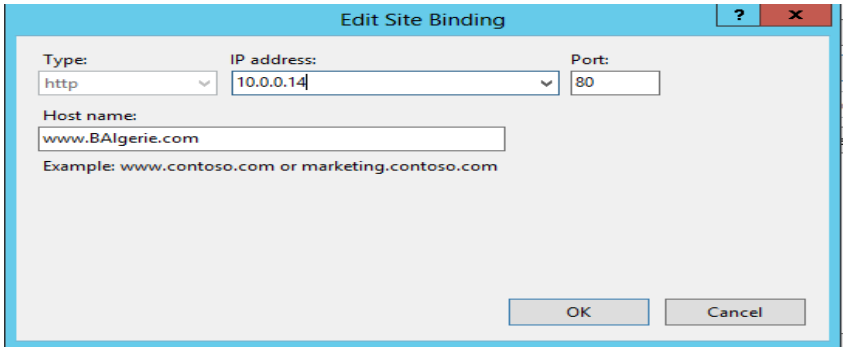


Figure IV.72: Liaison de Site

5.Création d'un DNS dans le serveur principal :

Une fois que le cluster a été bien créer, nous l'avons par la suite ajoutés au DNS du serveur principale PDC, pour ce faire nous avons procédé comme suite : Gestion de Serveur **è** outils **è** DNS **è** BAlgerie.com comme c'est montré sur la figure suivante :

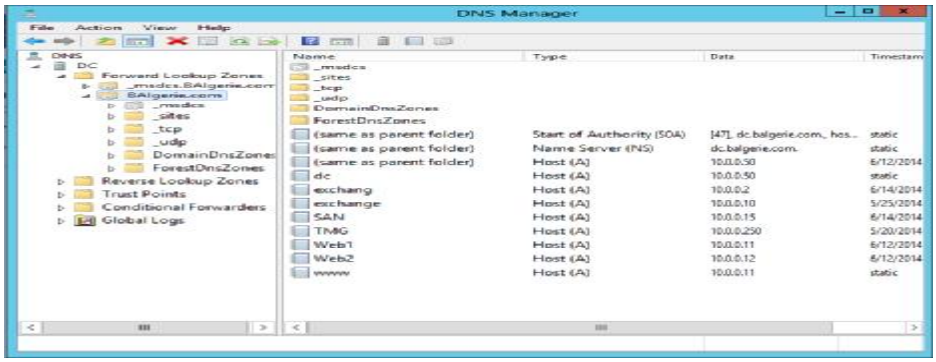


Figure IV.73 : Gestionnaire DNS

On clique droit sur BAlgerie.com **è** Nouvel hôte (A ou AAA)

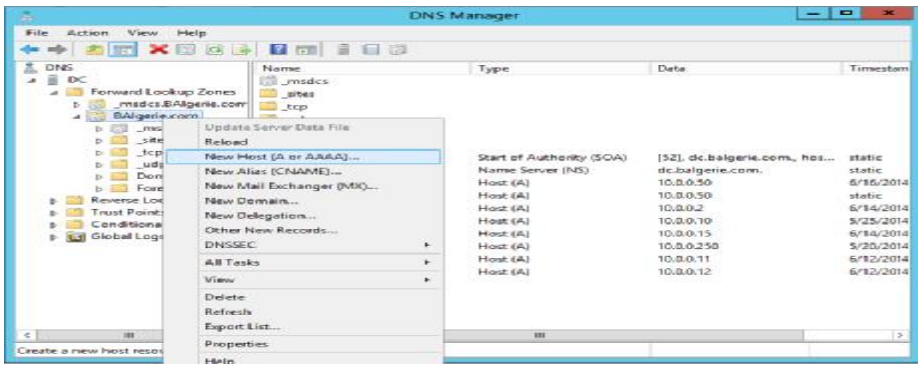


Figure IV.74 : Création nouvel hôte

On saisit les informations du cluster, ainsi le cluster sera raccordé au DNS

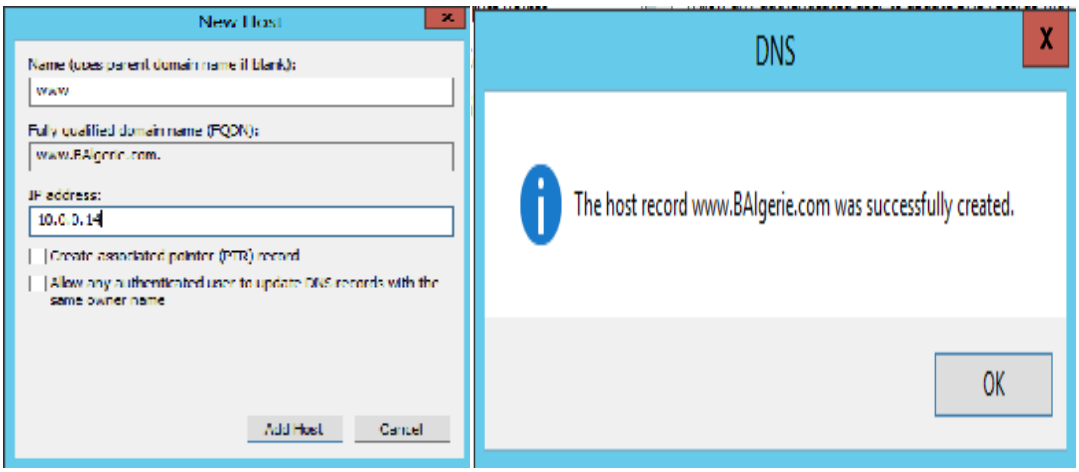


Figure IV.75 : Fin création de l'hôte

6. Tester le NLB

Pour tester et s'assurer du bon fonctionnement du load balnacing on a effectué un test de connexion,

Dans les 1er temps nous nous somme connectés en laissant les deux serveurs actifs comme illustré si dessous

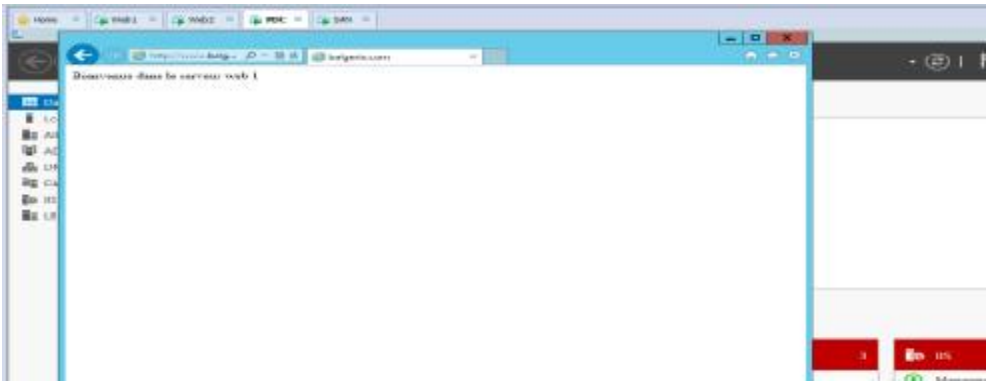


Figure IV. 76: Premier teste réussis.

On a vu que dans le teste 1 c'est le serveur 1 qui a répondu, car il est prioritaire.

Fermons le serveur 2 et puis nous effectuons une deuxième connexion et dans ce cas le serveur 2 réponds a la requête comme montré si après

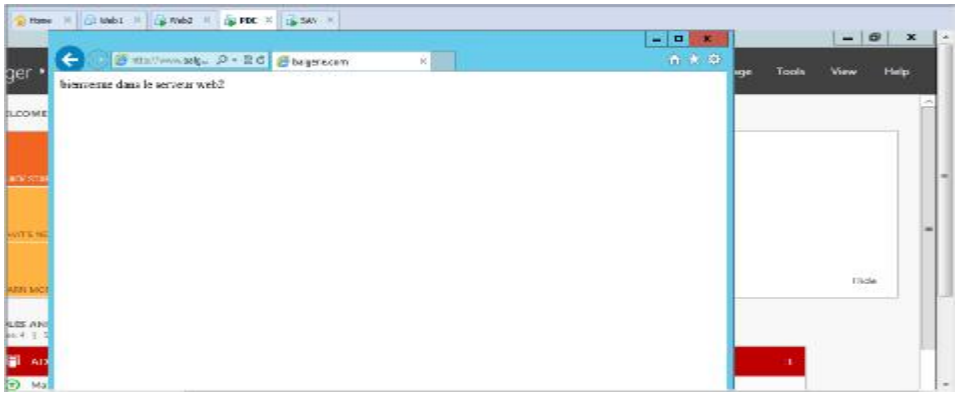


Figure IV.78 : Deuxième teste réussis

Etape VI : 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.

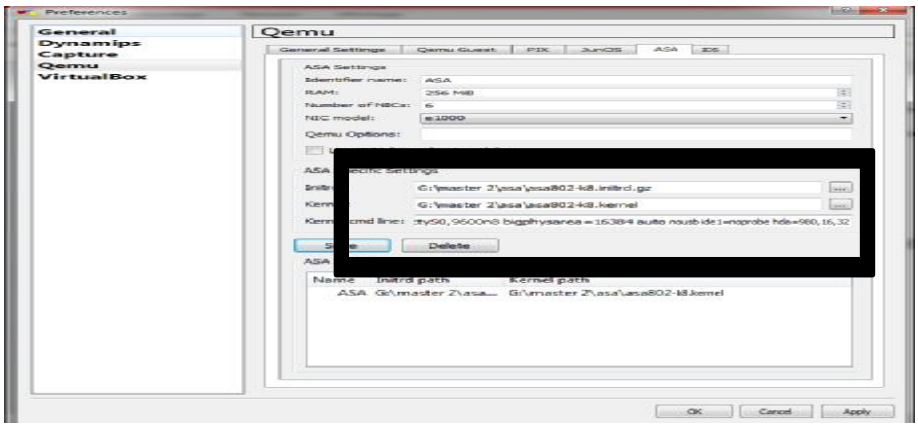


Figure IV.79 : L'ajout de l'IOS pour l'ASA.

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.

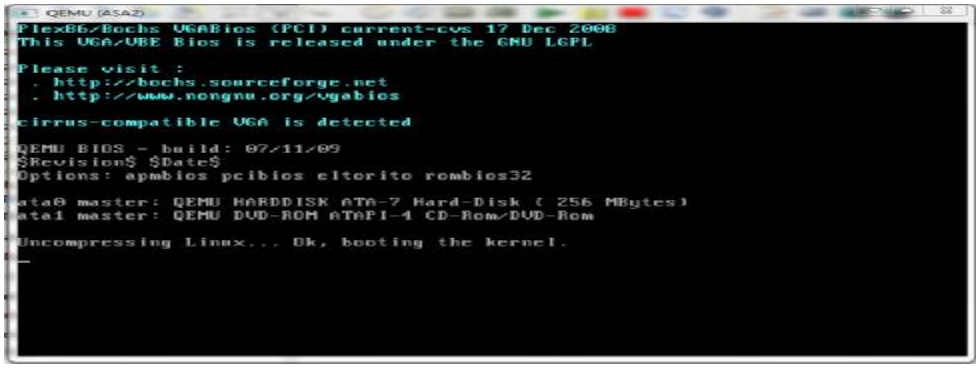


Figure IV.80: La fenêtre QEMU.

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.

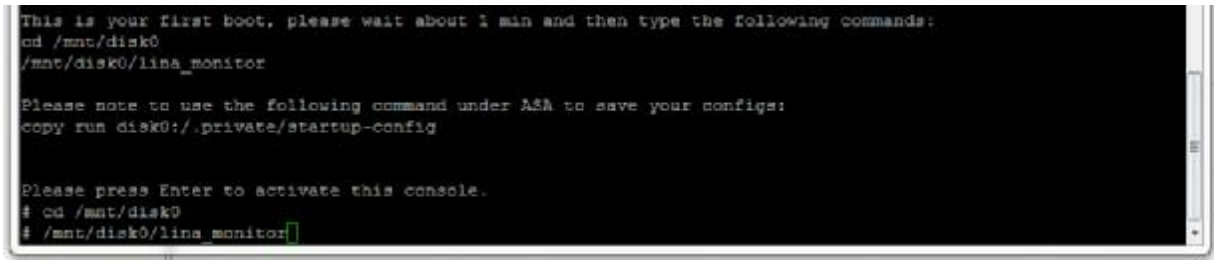


Figure IV.81 : Activation de la console

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.

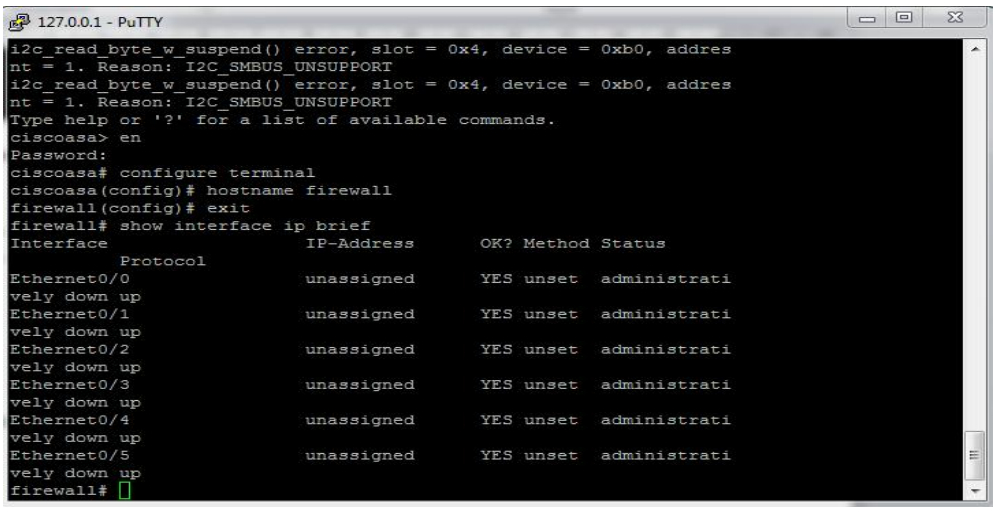


Figure IV.82: Passer au mode privilège

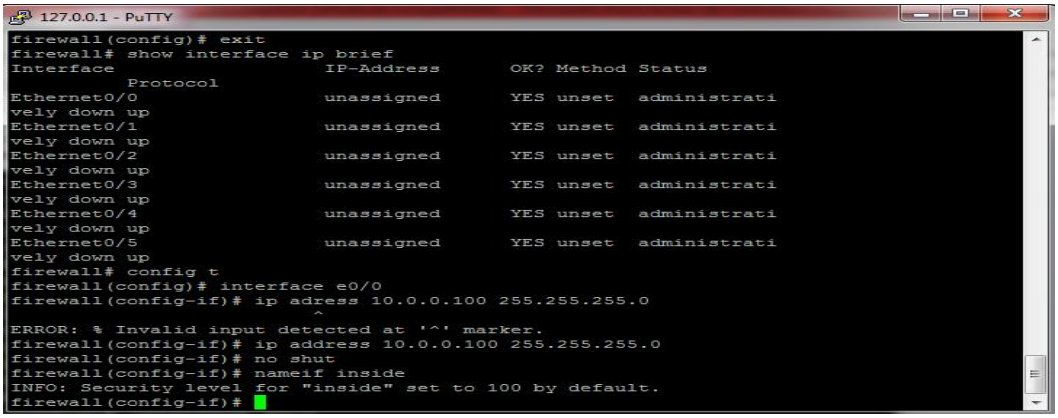


Figure IV.83: La configuration des interfaces.

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.

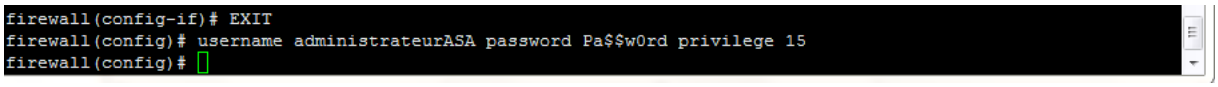


Figure IV.84: L'identification de l'utilisateur.

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 IV.85 : 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.

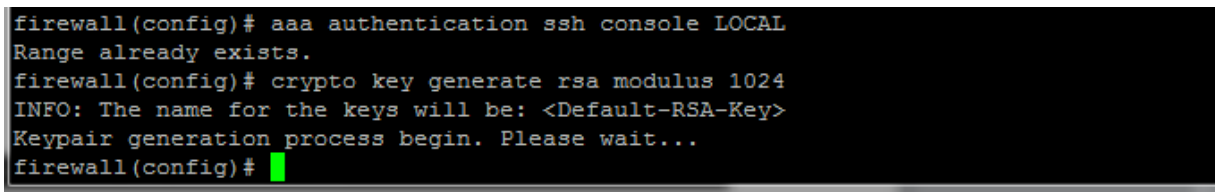


Figure IV.86: Cryptage de mot de passe.

La dernière commande spécifie le sous réseau à authentifier.

firewall(config)#ssh 10.0.0.100 255.0.0.0

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.

```
firewall(config)# show run
: Saved
:
ASA Version 8.0(2)
!
hostname firewall
enable password /yB/dTCJeUBCqR7U encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.0.0.100 255.255.255.0
!
interface Ethernet0/1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
```

Figure IV.87 : 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.

```
firewall(config)# http server enable
firewall(config)# http 10.0.0.1 255.255.255.255 inside
firewall(config)#
```

Figure IV.88: 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.

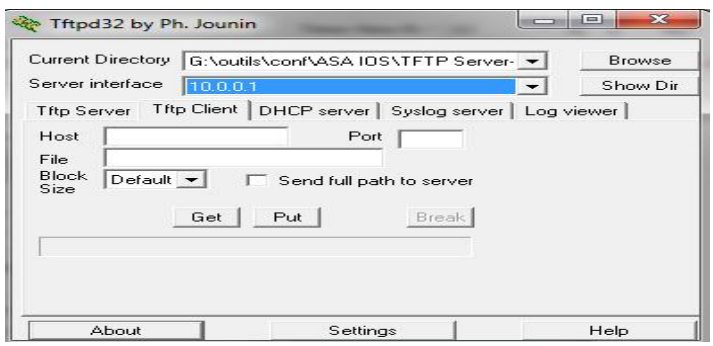


Figure IV.89: Ajout de l'image ASDM à TFTP.

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

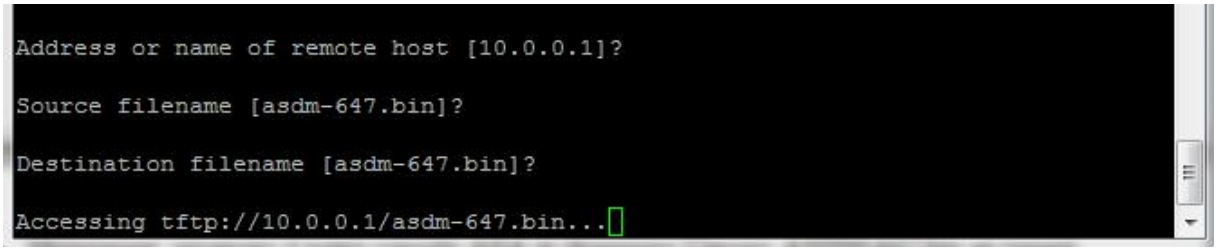


Figure IV.90 : Chargement de l'image ASDM.

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.

1.8. La sauvegarde de la configuration

Après avoir fini notre configuration nous allons la sauvegarder.

Figure IV.91: La sauvegarde de configuration.

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) 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.

La sécurité informatique est un domaine qui relie diverses techniques, applications et dispositifs en charge d'assurer l'intégrité et la confidentialité de l'information d'un système informatique et de ses utilisateurs. 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 garantie d'une bonne sécurité.

Nous nous sommes intéressés à la sécurité du réseau informatique de la Banque Algérie. Ceci nous a permis, grâce aux outils libres utilisés, d'augmenter le niveau de sécurité sur ce réseau.

Toutefois, la sécurité d'un réseau informatique étant un secteur très sensible, nous n'avons travaillé que dans la limite des possibilités qui nous ont offertes. Nous avons la conviction qu'une approche similaire, utilisée par le personnel spécialisé de la banque, peut permettre non seulement de finaliser cette étude mais aussi de l'étendre sur d'autres agences dans le cadre d'une politique de sécurité réseau globale.

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 cette dernière. 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 jusque-là 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 solution 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.

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 v0.8.2 all-in-one. Son installation est une succession du terme suivant. Au lancement de GNS3, il existe deux possibilités de configuration qui sont :

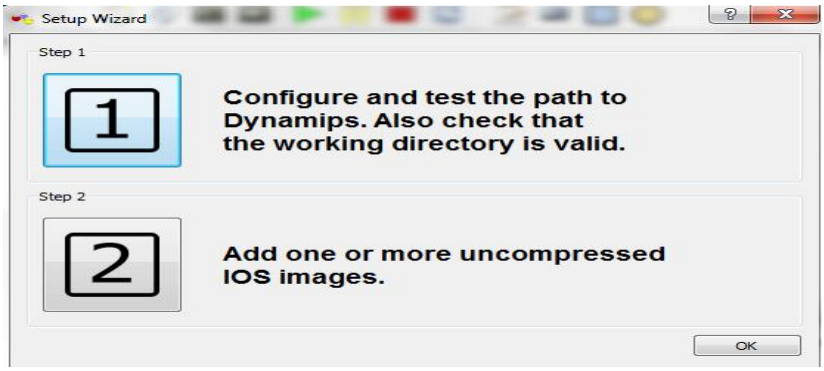


Figure A.1: Les possibilités de configuration de GNS3.

A.2. L'ajout et configuration des IOS

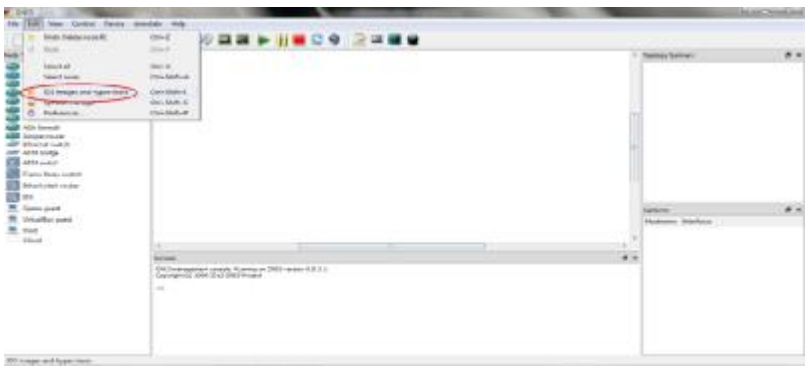


Figure A.2 : L'ajout de l'IOS.

L'IOS étant le système 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.

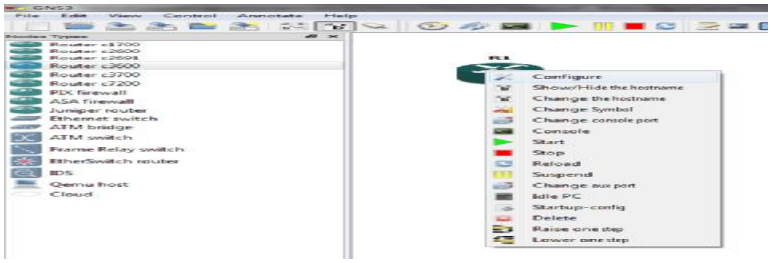


Figure A.3: La configuration d'un routeur.

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.

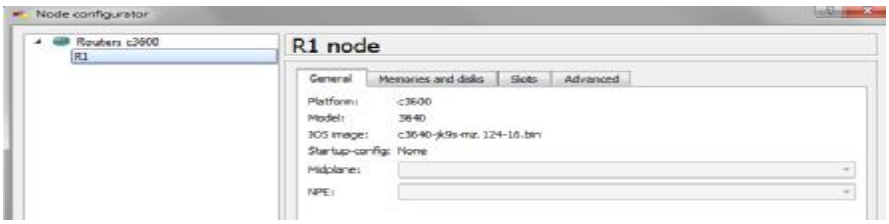


Figure A.4: Le node configurator.

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

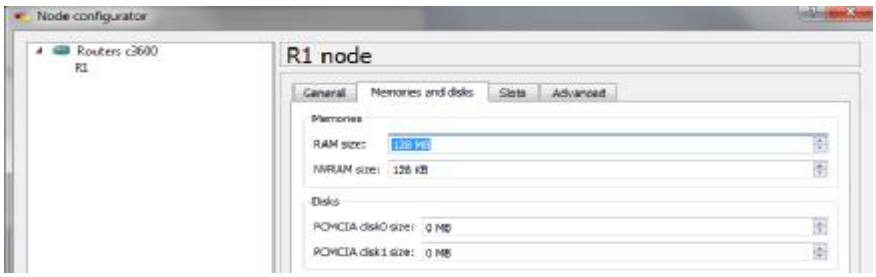


Figure A.5: Configuration de la RAM et la NVRAM.

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

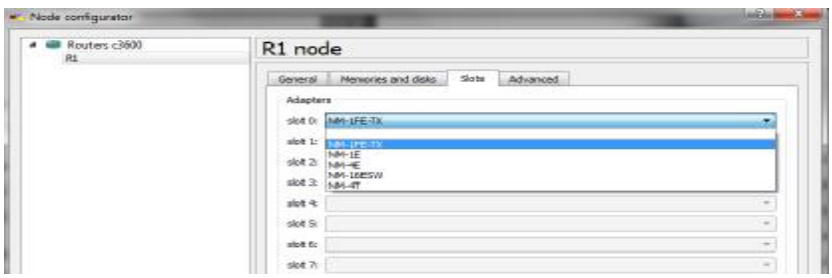


Figure A.6 : Le choix des modules des routeurs.

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.

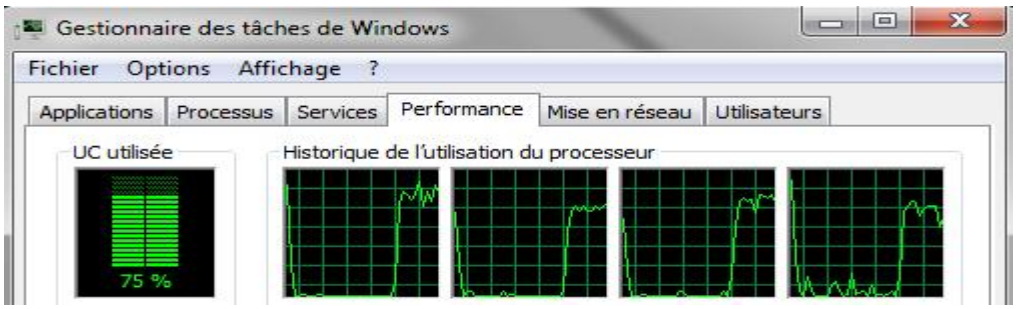


Figure A.8: Gestionnaire des taches de Windows.

Pour éviter cela, effectuons un clic droit sur le routeur et sélection 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 %)

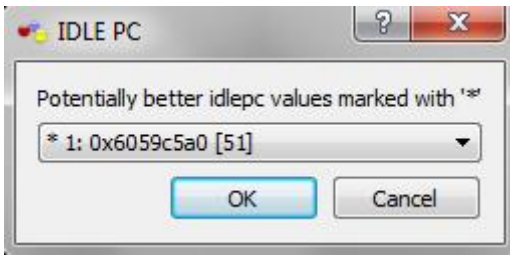


Figure A.9: IDLE PC.

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 Fast ethernet, 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.

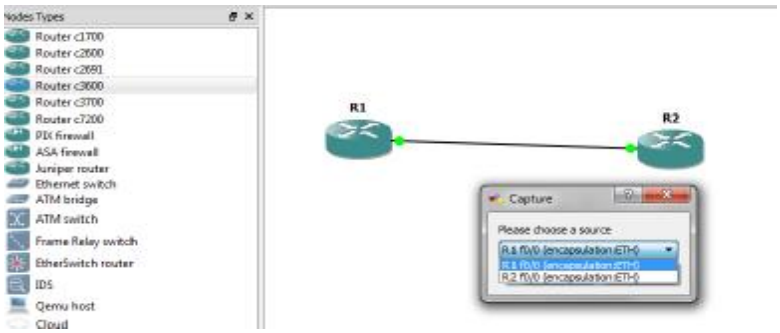


Figure A.10: La capture.

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.

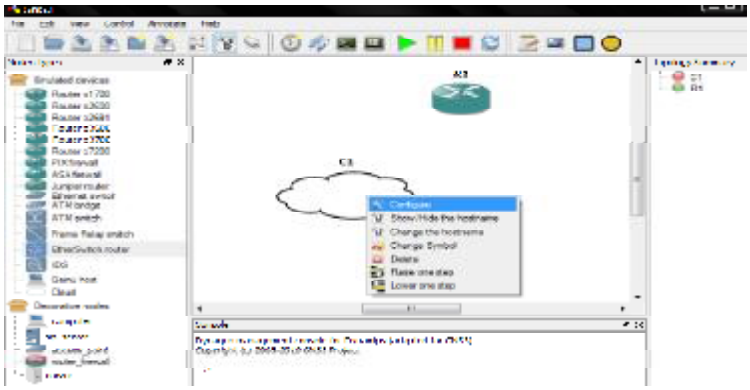


Figure A.12 : La configuration du nuage.

A.7. configuration IPS et IDS :

Un clique sur IDS -> ajouter l'image de IPS et IDS comme illustrée dans la figure ci-dessous, en spécifiant le nom, la RAM et d'autre critères.

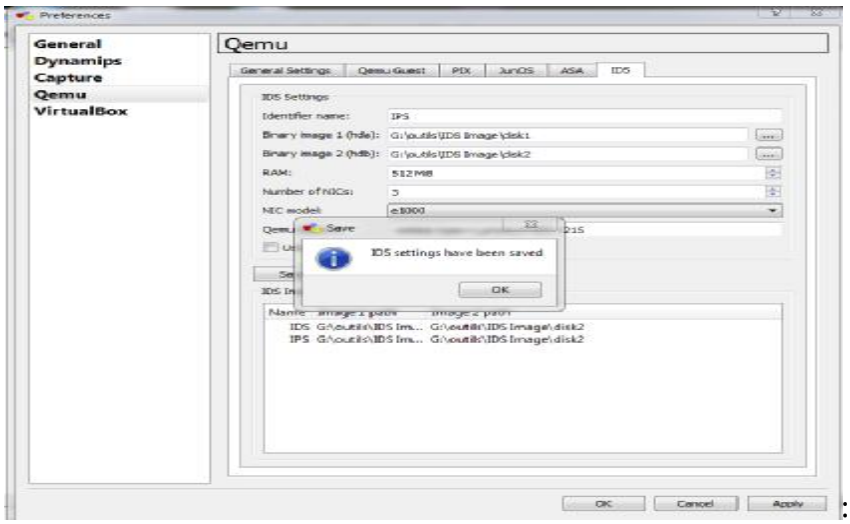


Figure A.13: L'ajout de l'image d'IPS et IDS

Cliquant sur OK le chargement sera fait.

1. Démarrage d'IDS

A l'ouverture de la console, un message vérification s'affiche, nous tapons les le nom et le mot de passe comme le montre la figure ci-dessous pour accéder.

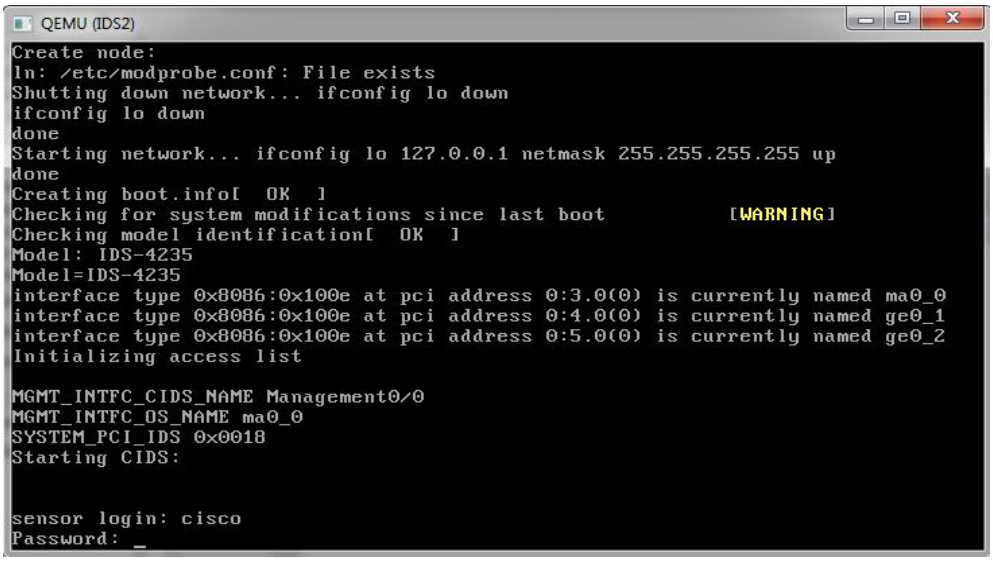


Figure A.14: Accès aux IPS

2. La configuration

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.

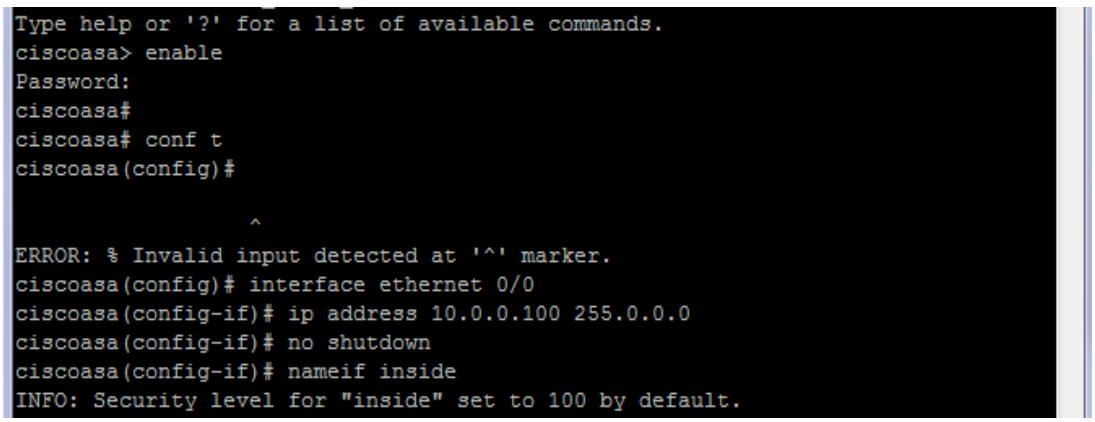


Figure A.15: La configuration des interfaces.

Continuant les configurations, entrer **yes** ; puis saisissant le nom

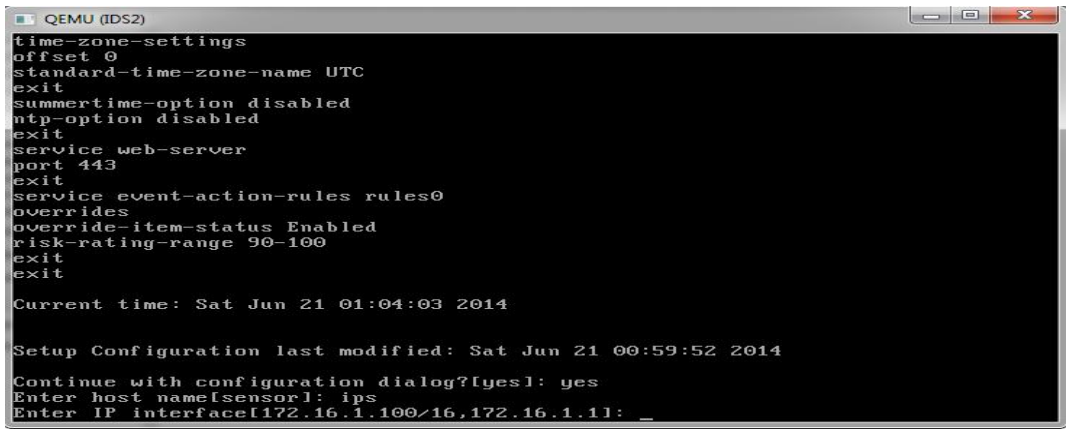


Figure A.16 : création du nom

Pour sauvegarder les configurations ; faut choisir la sélection 2 :

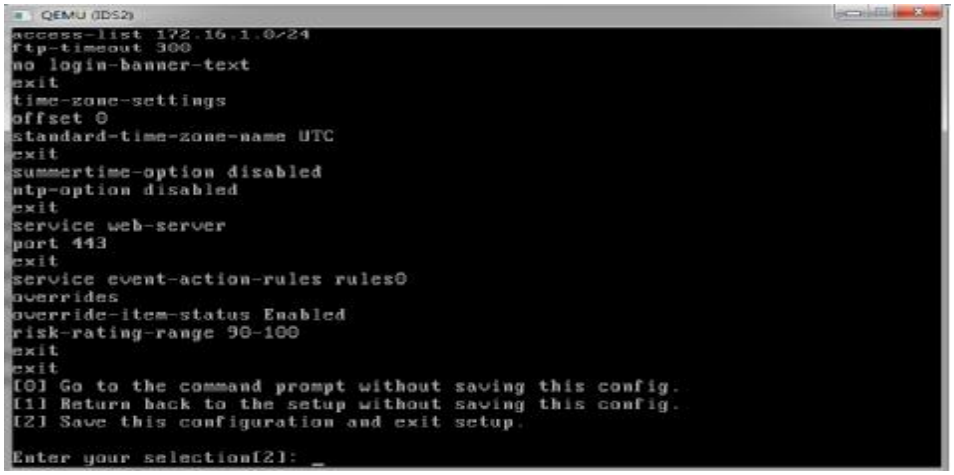


Figure A.18. : Sauvegarde des figurations

Annexe B

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. L'installation d'Active Directory sous Windows 2012

Dans le menu «Server manager ».Lancer « l'Assistant Ajout de rôle et de fonctionnalités » Ensuite spécifier le nouveau rôle « Active Directory Domain Services » dans la liste de «Rôle de serveurs »

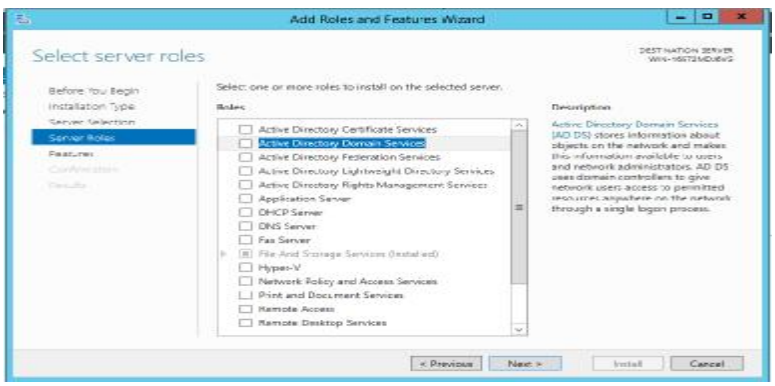


Figure B.2: Sélection du rôle « Active Directory Domain Services »

Active Directory Domain Services a besoin de fonctionnalités annexes :

- La console de gestion des stratégies (GPO Management),
- Les outils d'administration de RSAT

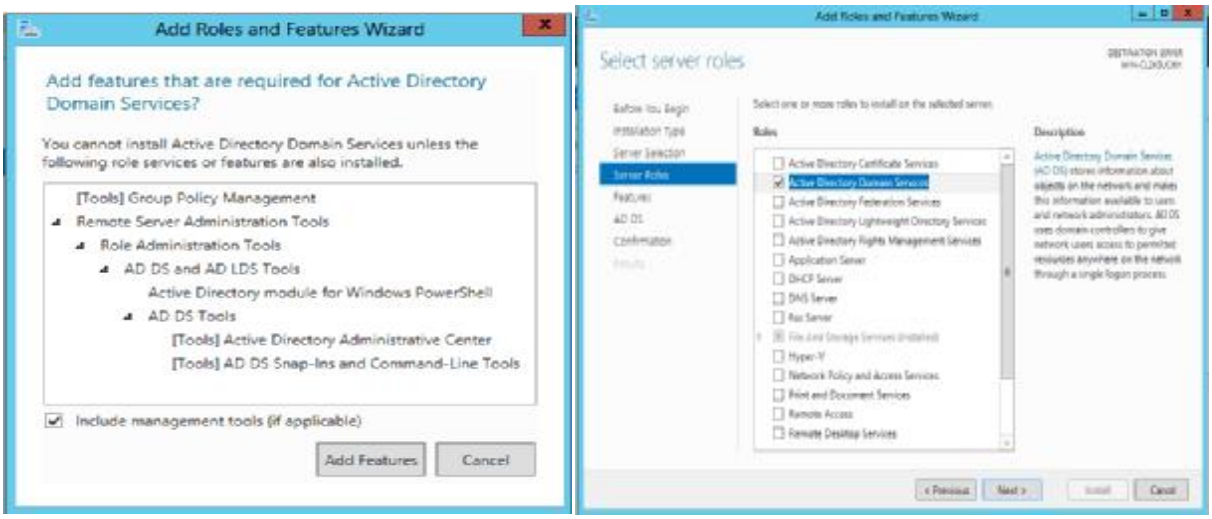


Figure B.3: Ajout les outils de gestion

On clique sur Ajouter des fonctionnalités, puis continuant l'assistant en cliquant sur Suivant. Les fonctionnalités obligatoires ont été pré cochées, cliquant sur Suivant.

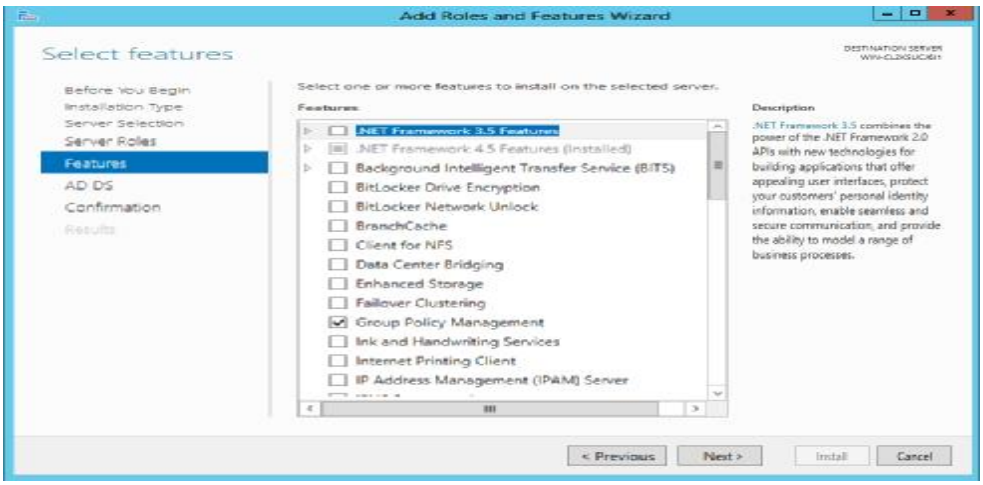


Figure B.4: Les fonctionnalités qui ont été pré cochées

Un message d'avertissement est affiché, il rappelle les bases d'active Directory : redondance des contrôleurs de domaine, nécessité de DNS, …

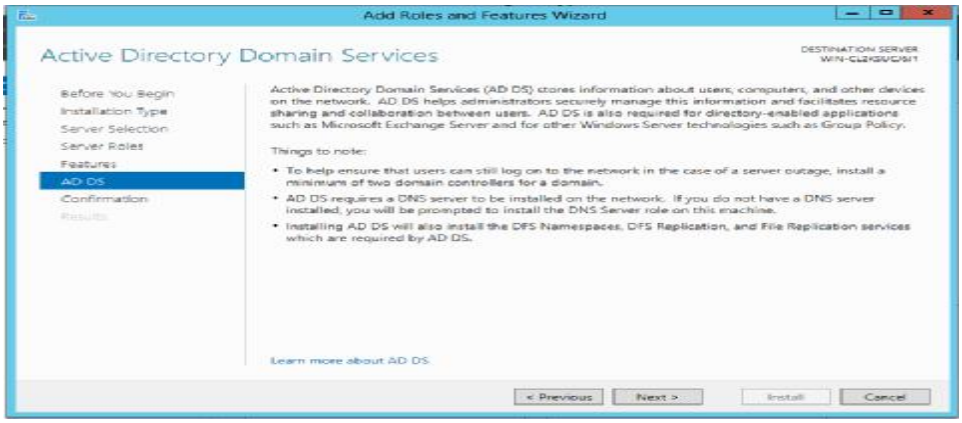


Figure B.5: message de rappelle les base d'active Directory

Enfin un dernier récapitulatif s'affiche puis on clique sur Installer :

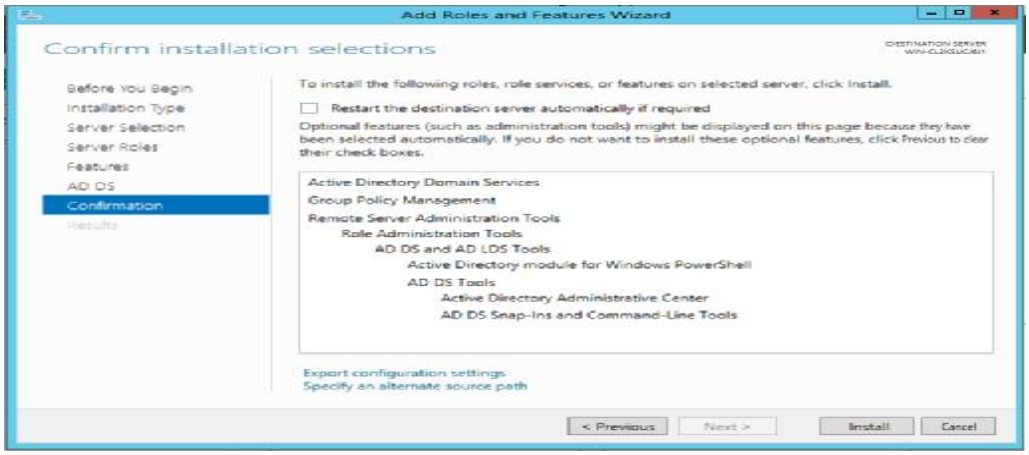


Figure B.6 : confirmer l'installation Active Directory Domain Services

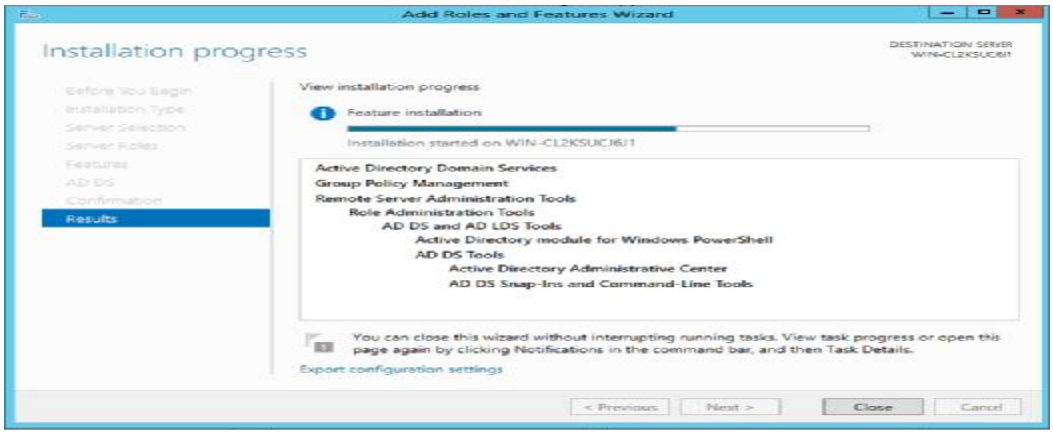


Figure B.7: Progression de l'installation Active Directory Domain Services

Puis le message suivant est affiché :

« Des étapes supplémentaires sont requises pour faire de cet ordinateur un contrôleur de domaine. Cliquez donc sur Promouvoir ce serveur en contrôleur de domaine. »

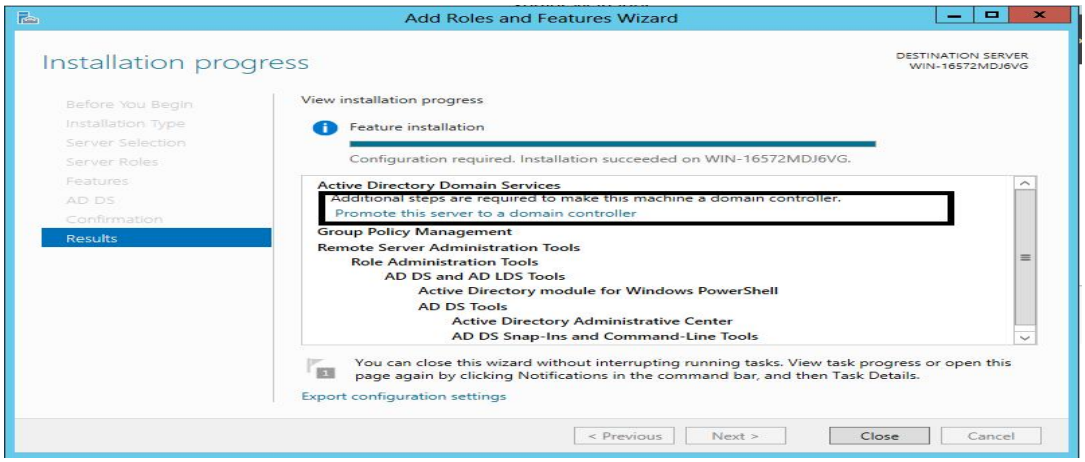


Figure B.8 : fenêtre message

L'assistant de Configuration des services de domaine Active Directory se lance.

S'il s'agit du premier contrôleur ; il est nécessaire de créer une forêt :

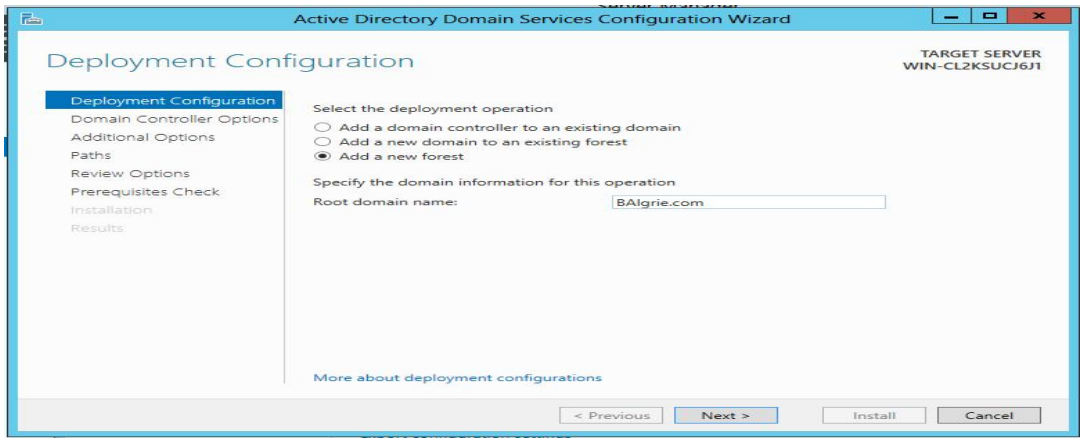


Figure B.9: Ajout d'une nouvelle forêt

Puis définir le niveau fonctionnel de la forêt et du domaine et définir le mot de passe de restauration

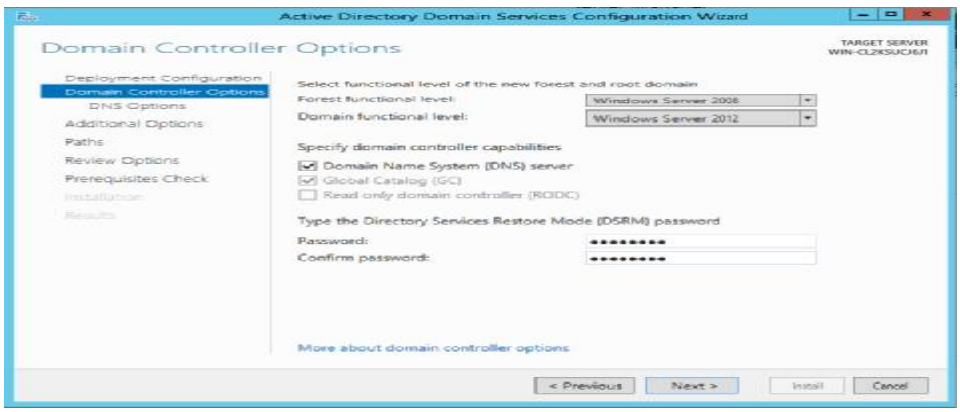


Figure B.**10**: l'Ajout de server DNS

Si le premier domaine dans une infrastructure n'ayant pas de DNS, le message d'erreur suivant est normal : la zone de nom de domaine sera créée automatiquement par la suite.

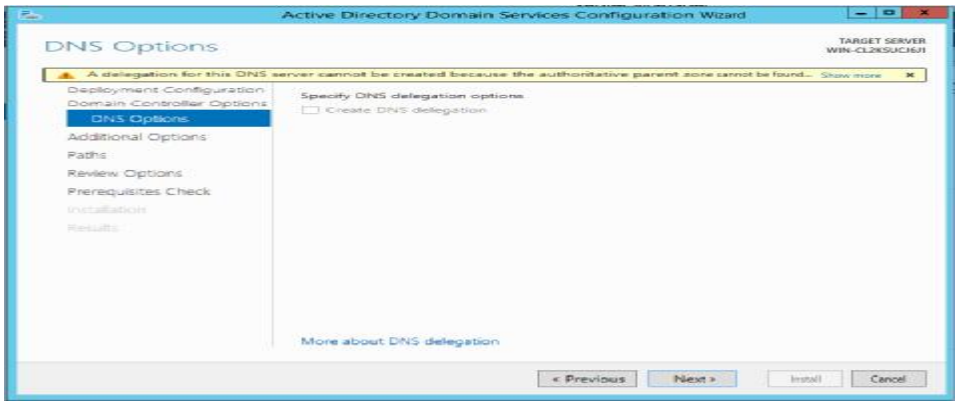


Figure B.11: Option de DNS

Le nom NETBIOS de domaine est ensuite déterminé, peut éventuellement l'échanger;

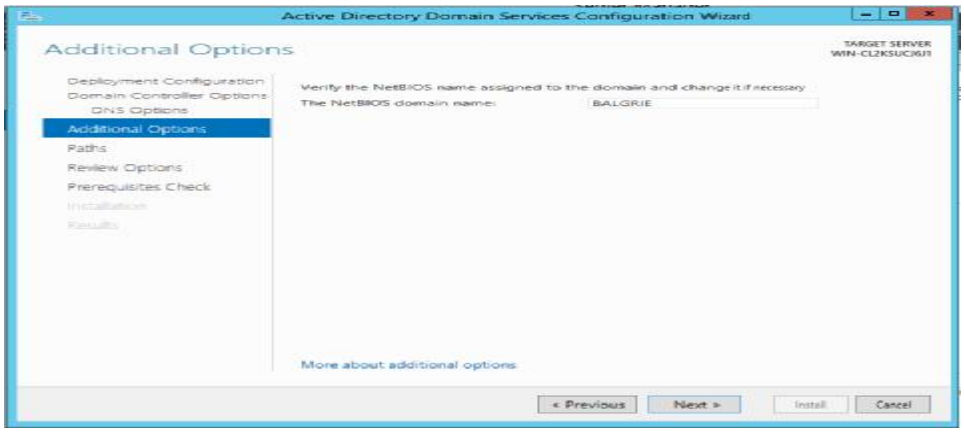


Figure B.12 : confirmer le nom du domaine

cliquant « suivant ». Ensuite précisant les chemins de stockage de l'AD :

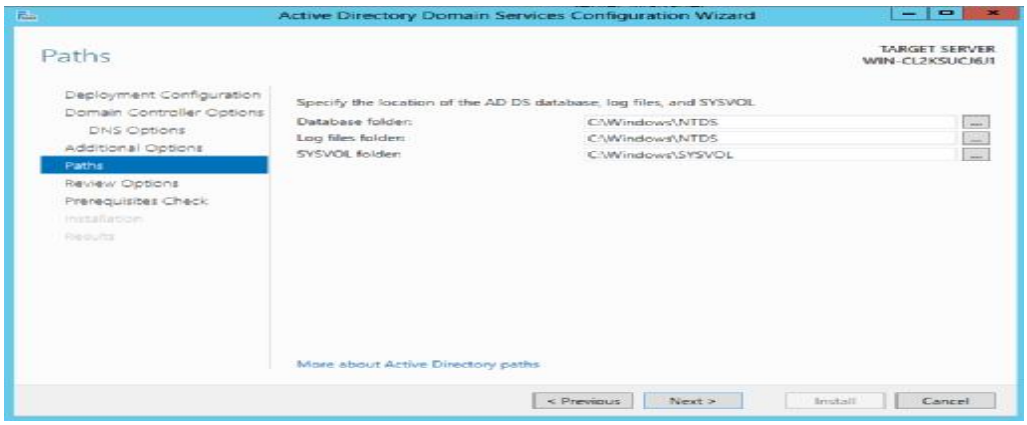


Figure B.13 : chemin de stockage de l'AD

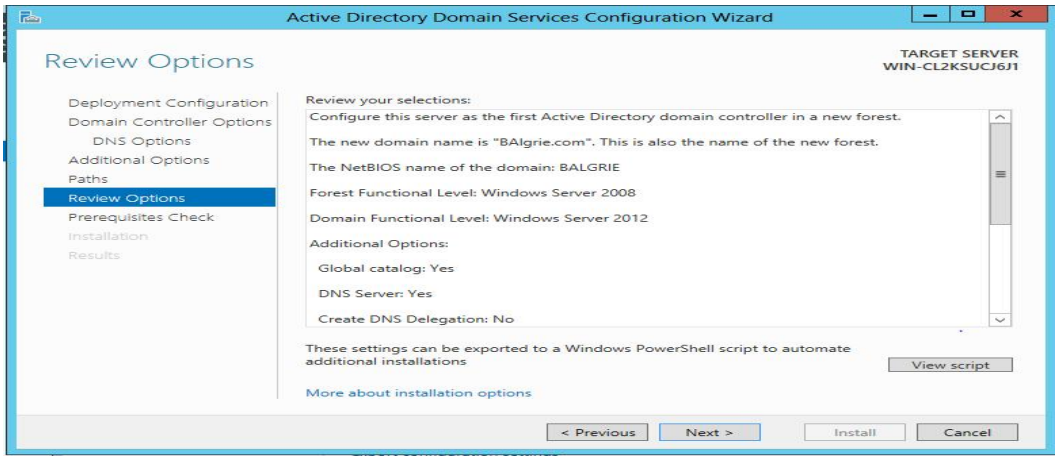


Figure B.14 : Tableau vérification de paramétrage

Après vérification, un rapport affiche tous les points importants :

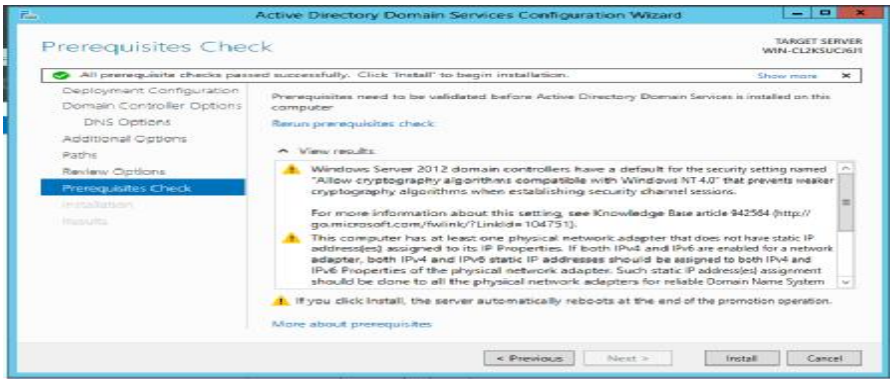


Figure B.15 : Résumé de tous les points importants

Si plus rien ne s'y oppose, vous pouvez cliquer sur Installer.

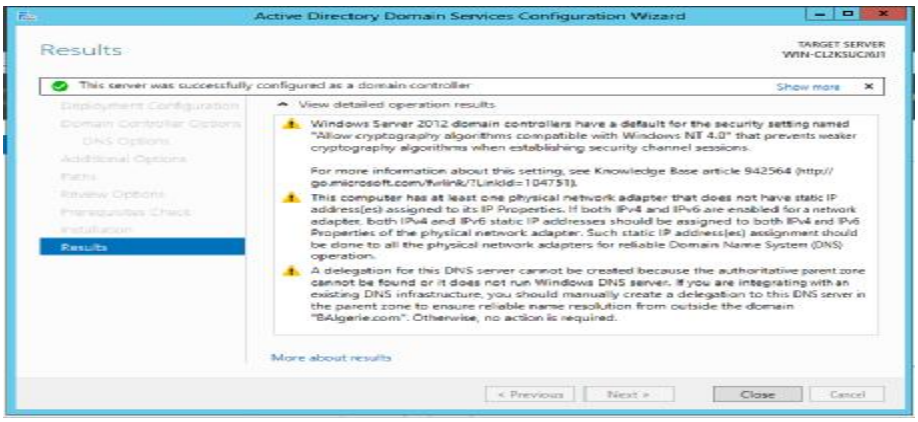


Figure B.16: Démarrage d'installation AD

B.3. Installation de la TMG

B.3.1.Au premier lieu on doit faire l'installation d'un Windows Server 2008 R2 (Forefront TMG 2010 ne s'installe que sur Windows Server 2008 édition 64 bit ou Windows Server 2008 R2 qui lui n'est disponible qu'en 64 bit)

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

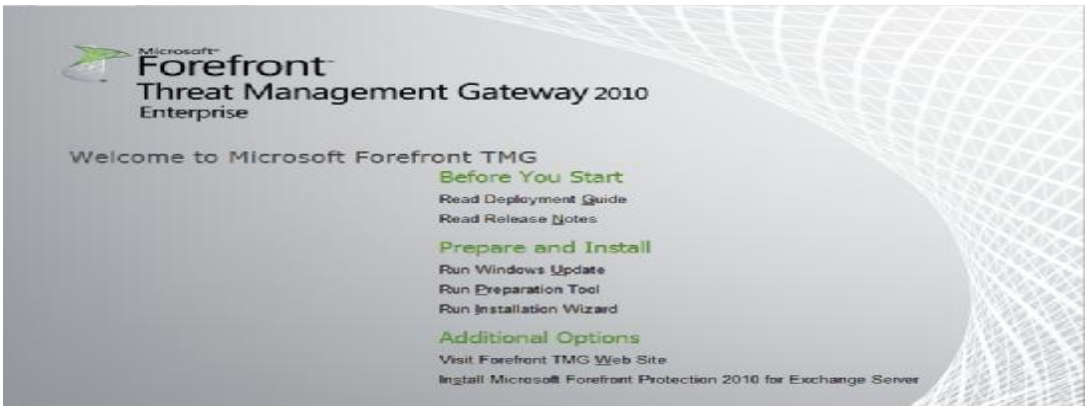


Figure B.17 : Lancement de l'installation de la TMG.

Comme il apparait, 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 :

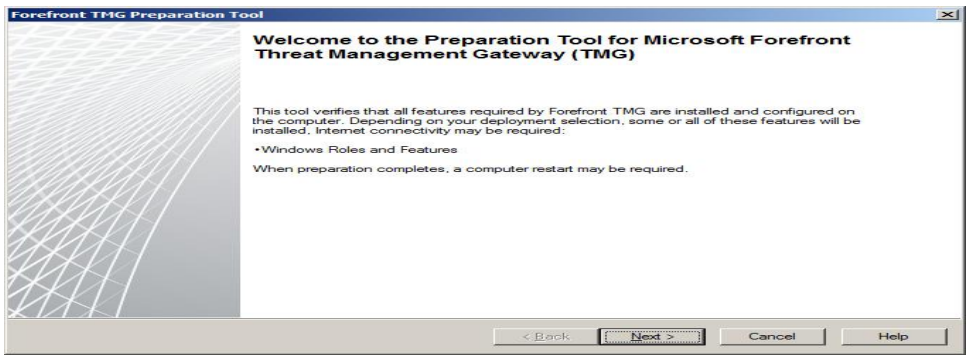


Figure B.18 : Lancement de l'exécution des outils de préparation.

Apres avoir cliqué sur suivant et coché « accepter les conditions licence »puis suivant ; nous choisissons d'installer les services et fonctionnalités de TMG et la console de gestion Dans notre cas on laisse le choix par défaut :

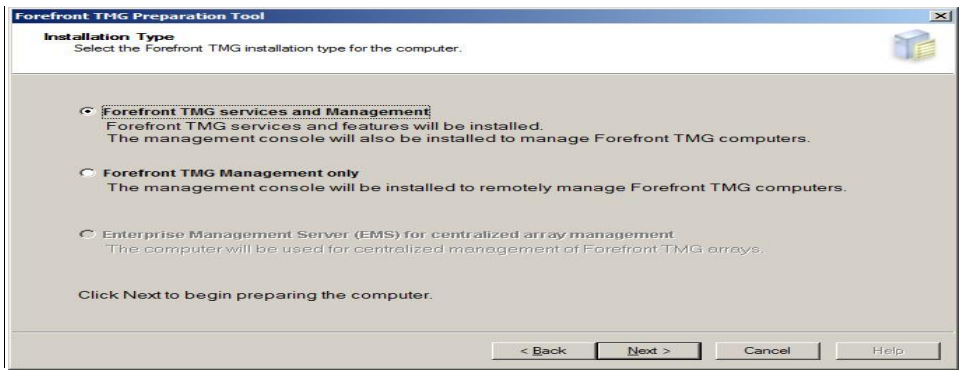


Figure B.19 : Le choix des fonctionnalités de la TMG.

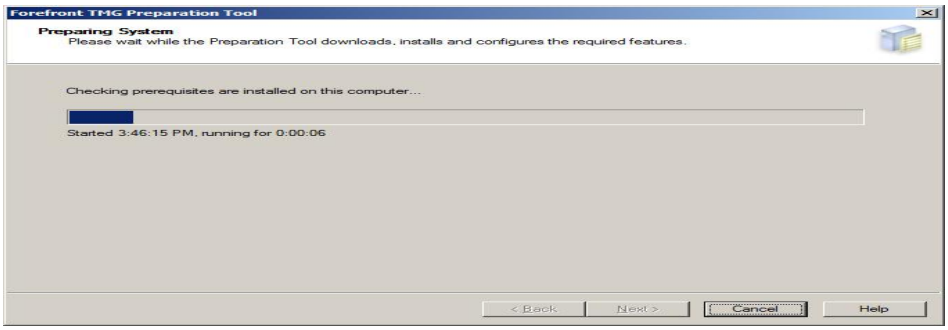


Figure B.20 : Préparation des outils.

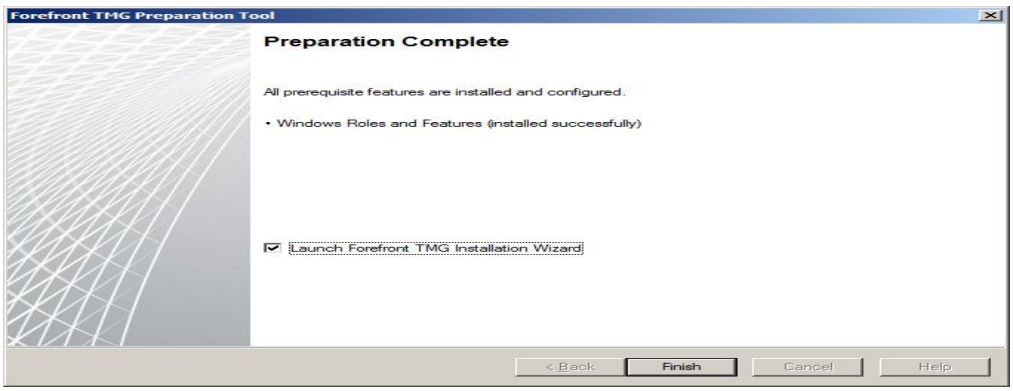


Figure B.21 : Ajout des outils d'installation

Figure 4: Fin de préparation des outils et lancement d'assistant d'installation de la TMG.

Etape 3 : Exécuter l'assistant d'installation.

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

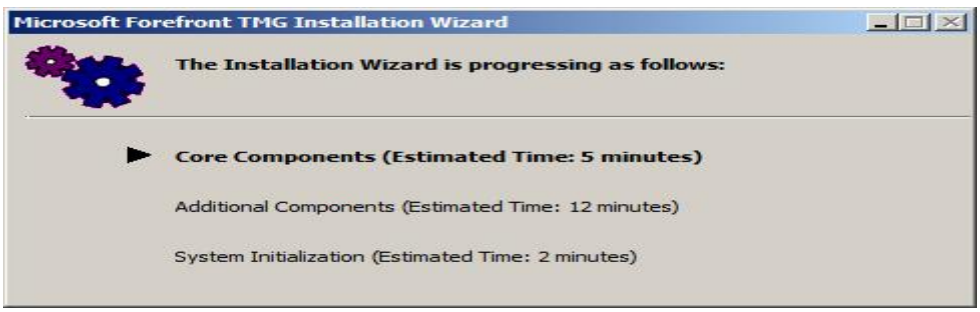


Figure B.22: Assistant d'installation de la TMG

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

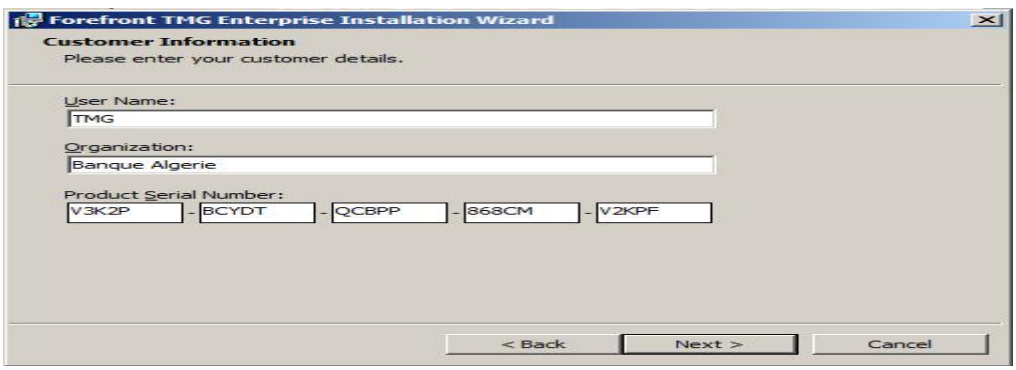


Figure B.23: Validation de la licence

On continu avec une succession de suivant **:**

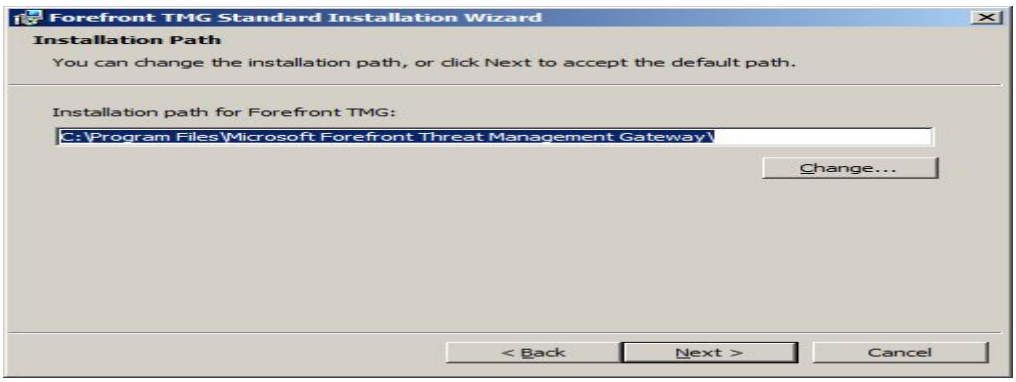


Figure B.24: le chemin d'installation de Forefront TMG 2010

Dans cette étape est demandé d'ajouter les cartes réseau configuré auparavant, dans notre cas ; nous sélectionnons 3 interfaces réseaux :

- **Internal** : carte réseau interne.
- **External** : carte réseau externe .
- **DMZ** : Carte réseau de notre domaine.

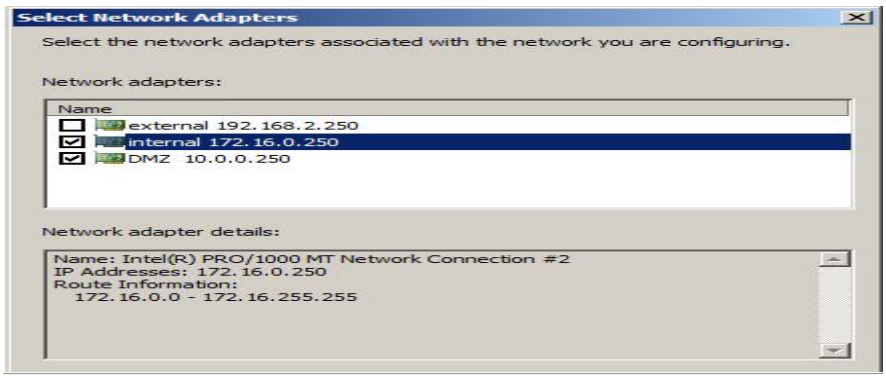


Figure B.25: Sélection des cartes réseau.

Cliquer sur **OK**

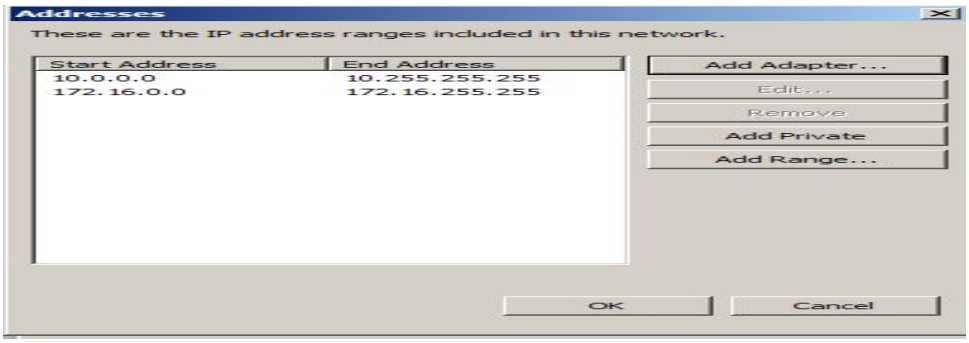


Figure B.26 : Liste de la plage des valeurs.

La table des adresses locales a été construite automatiquement. Cliquer sur OK jusqu'à la fin d'assistant d'installation**.**

B.4. 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 **è** outil d'administration **è** gestionnaire de serveur, et l'ajouter comme rôle, les figures suivantes illustrent la procédure à suivre .

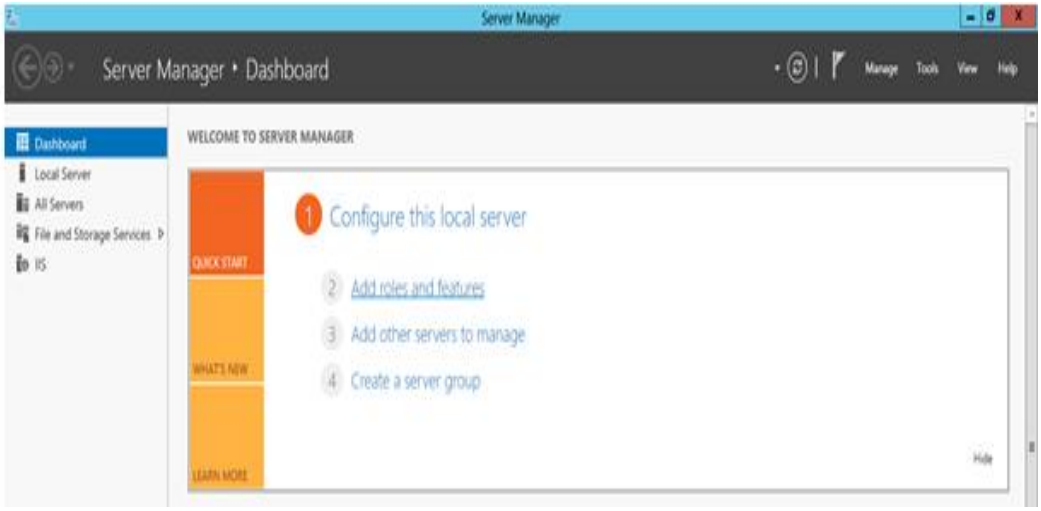


Figure B.27: Gestionnaire de serveur.

Dans l'onglet **d'ajout de rôles et de fonctionnalités**, on clique **sur serveur sélectionné** (server selection) puis sur **suivant**,

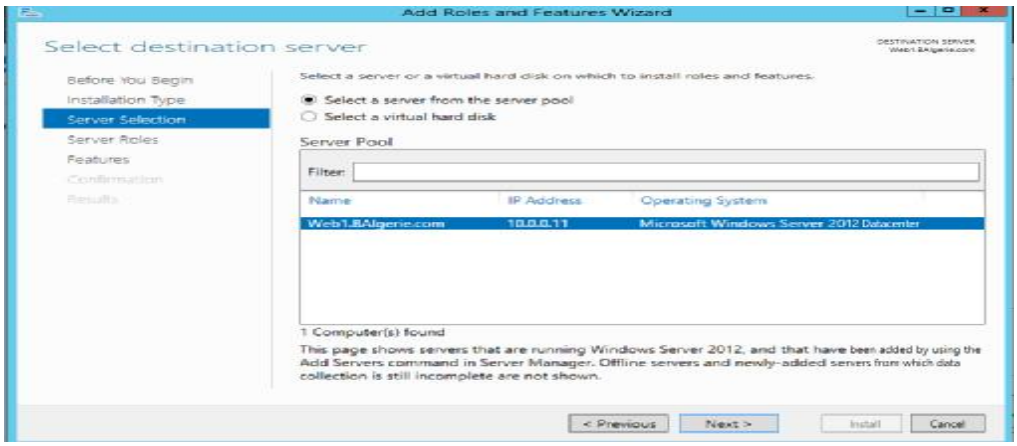


Figure B.28: server selection.

Dans la liste des **rôles** on coche **Web Server (IIS)**

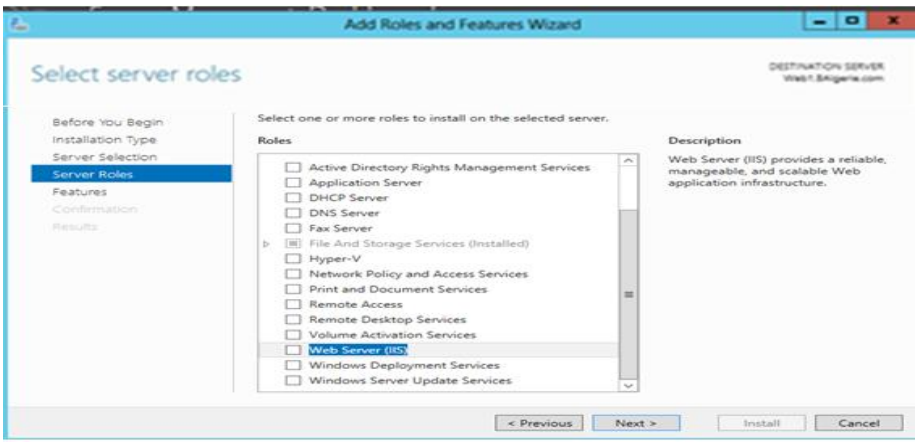


Figure B.29: choix du server rôle Web Server IIS

Sur cette dernière on clique sur **ajouter les fonctionnalités**

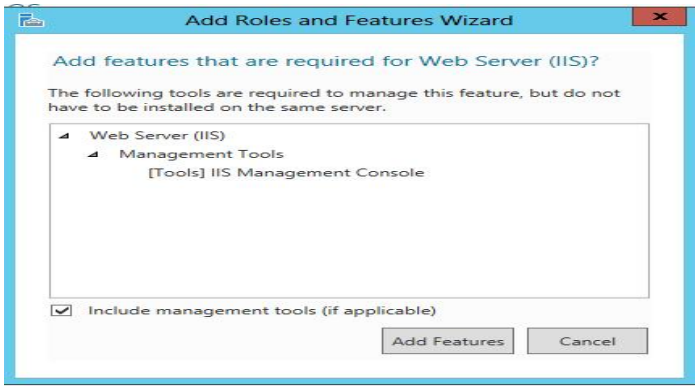


Figure B.30: Ajout les outils de gestion

- Ainsi le serveur web IIS sera activé comme le montre la figure suivante :

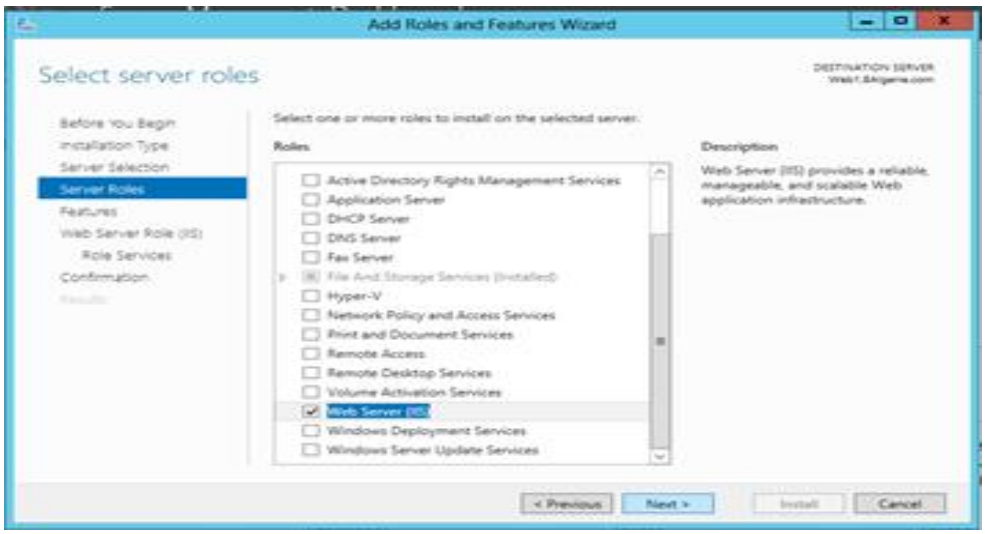


Figure B.31 : activation du web server IIS

- On poursuit l'installation en cliquant sur **suivant è suivant è suivant** puis dans l'onglet confirmation on vérifie que les composants de serveur Web sont activés puis on clique sur

installer (Install) et une fenêtre d'avancement de l'installation sera affiché comme le montrent les illustrations suivantes

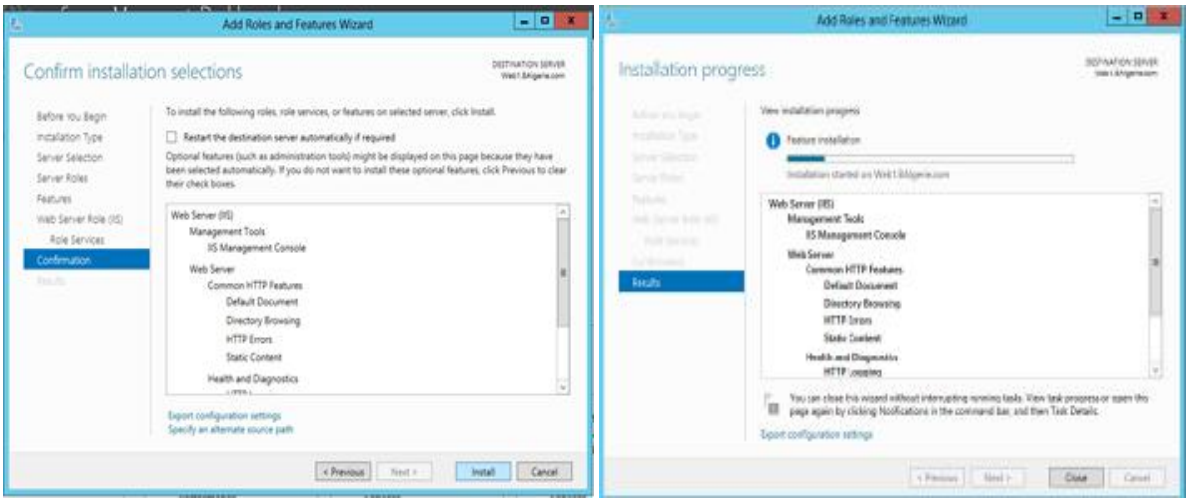


Figure B.32: confirmation et l'avancement de l'installation.

Remarque :

Les composants Web Server (IIS) suivants doivent être installés lors d'une installation sous Windows Server 2012. Si ces services de rôle ne sont pas ajoutés, l'installation s'interrompra jusqu'à leur installation :

- Serveur Web
  - Fonctionnalités HTTP communes
    - Document par défaut
    - Contenu statique
  - Sécurité
    - Filtrage des demandes
    - Authentification de base
    - Authentification Windows
  - Développement d'applicationss
    - .NET Extensibility 3.5
    - ASP.NET 3.5
    - Extensions ISAPI
    - Filtres ISAPI
- Outils de gestion
  - Console de gestion IIS
  - Compatibilité avec la gestion IIS 6

- Compatibilité avec la métabase IIS 6

§ Scripts et outils de gestion IIS

§ Service de gestion

C.1. 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.

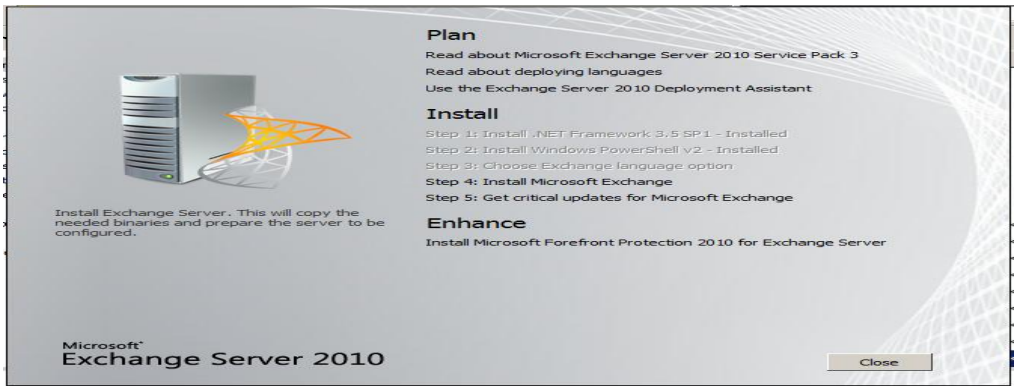


Figure C.1: Lancement d'installation de l'Exchange.

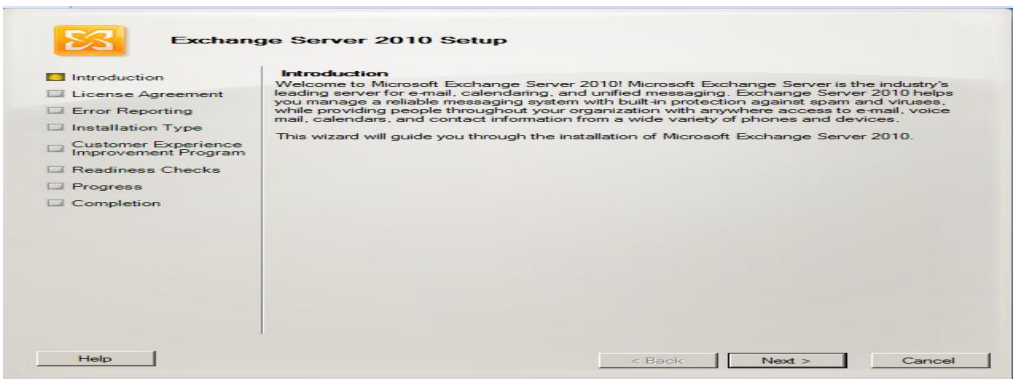


Figure C.2: Introduction

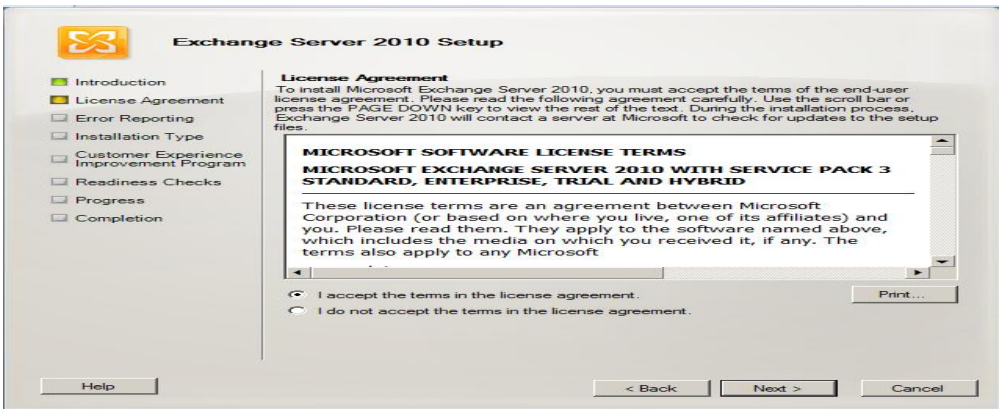


Figure C.3: Accepter de la licence.

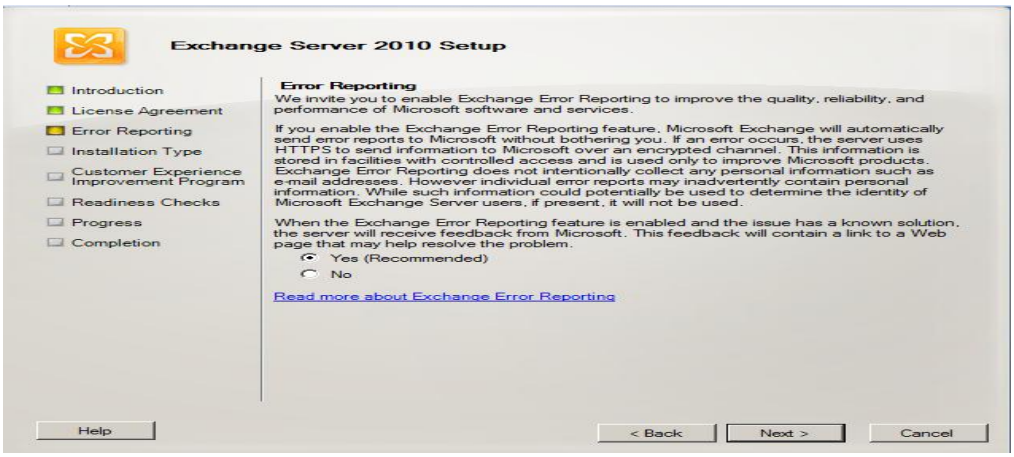


Figure C.4: Le choix de rapport d'erreur.

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.

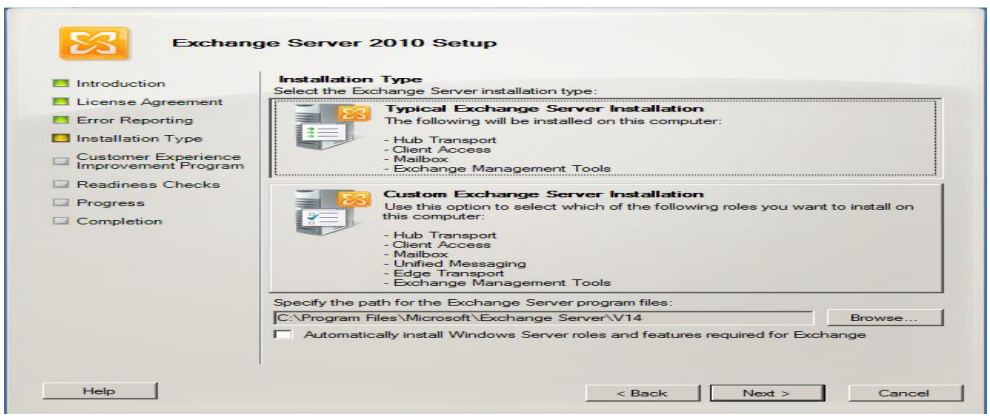


Figure C.5: Le choix de type d'installation.

Figure C.6: 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.

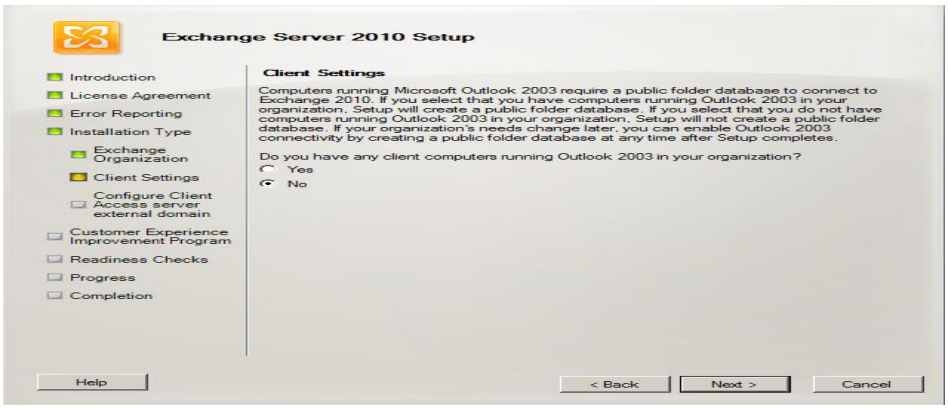


Figure C.7: Paramètre client.

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

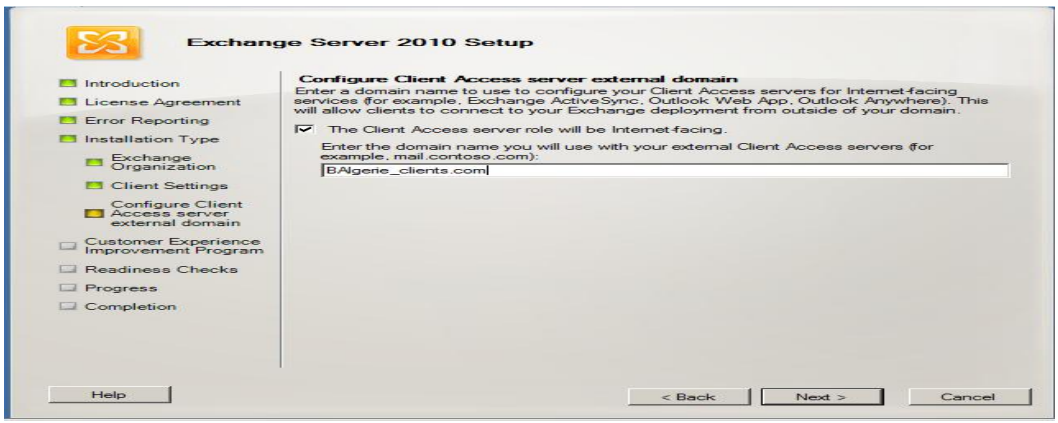


Figure C.8: Configuration de domaine externe du serveur d'accès client.

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

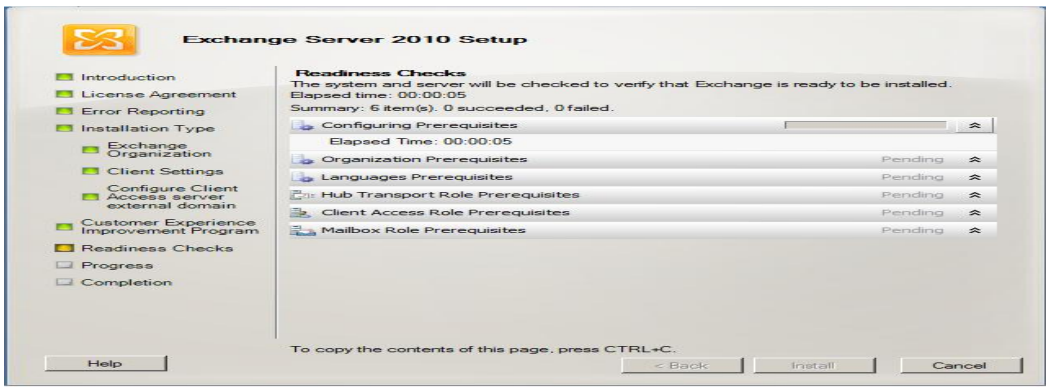


Figure C.9: Les tests de préparation.

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.

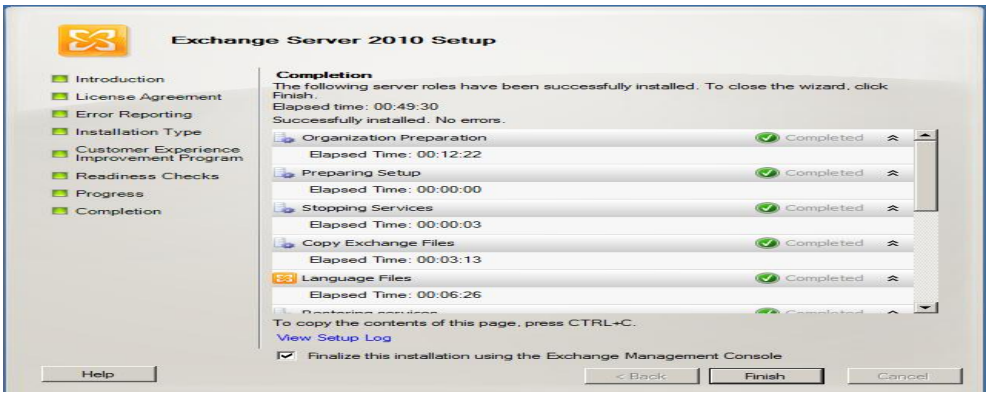


Figure C.10: Achèvement de l'installation.

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.

C.2. 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.2.1 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 être le périphérique de stockage final ou un périphérique intermédiaire comme un commutateur.

a. Installation d'iSCSI SAN :

Apres avoir joint le domaine principale, on configure le server SAN en ajoutant le rôle ISCSI SAN en suivant les étapes illustrés si après

- Démarrer (Start) **è** Gestionnaire de Serveur (Server Manager) **è** Ajout de rôles et de fonctionnalités (add roles and features)
- Dans l'onglet **d'ajout de rôles et de fonctionnalités**, on clique **sur serveur sélectionné** (server selection) puis sur **suivant**, dans la liste des **rôles** on clique sur **File and iSCSI services** puis on coche **iSCSI Target server** **è** **ajouter les fonctionnalités (add features)** ainsi le service **iSCSI** sera ajouté comme le montre la figure suivante

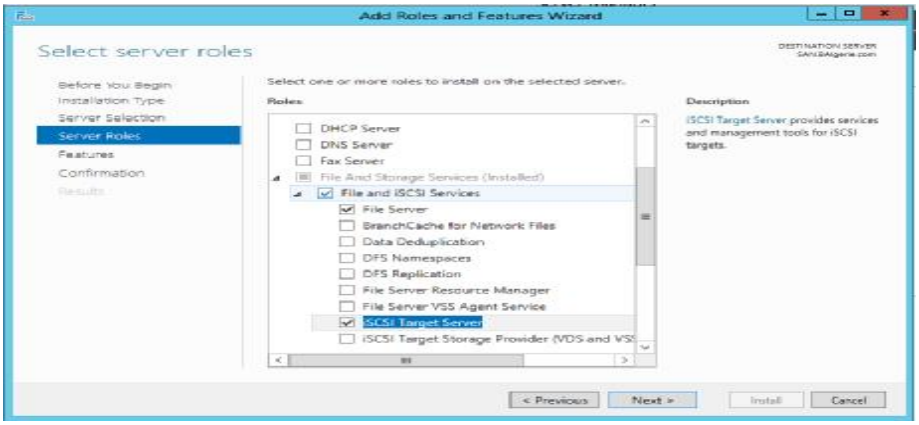


Figure C.11: Ajout de l'iSCSI Target server.

On clique sur **suivant** **è** **suivant** une fenêtre de vérification s'affiche et on confirme l'installation en cliquant sur **installer** si les composants désirées sont vérifiés

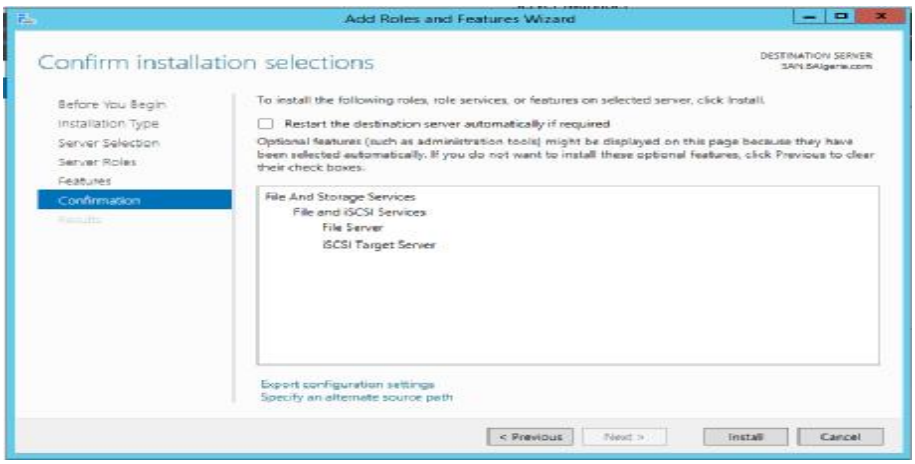


Figure C.12: confirmation et installation.

Puis une fenêtre de progression nous sera affichée comme sur la figure suivante

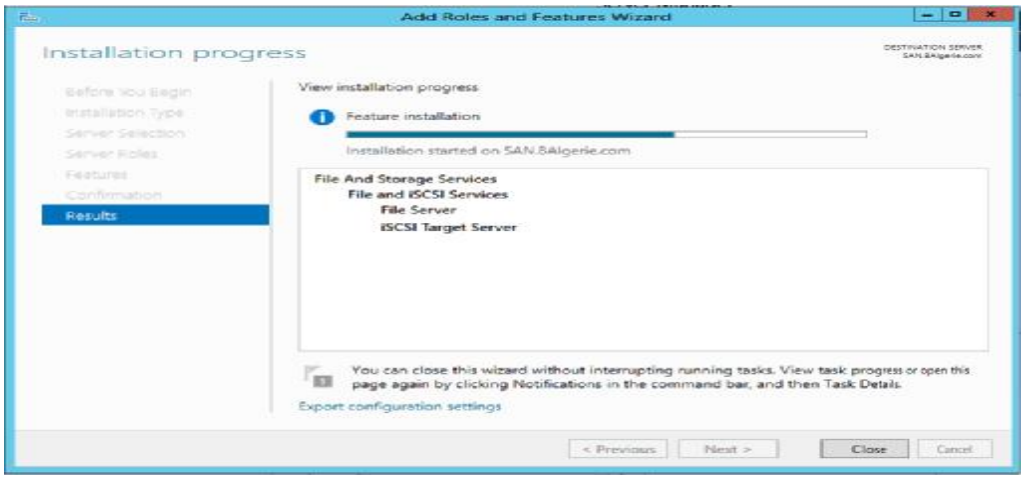


Figure C.13 : progression de l'installation

Ainsi l'iSCSI est bien installé avec ses différents composants.

b. Création de disque virtuel

Pour créer un disque virtuel, ouvrir le **Gestionnaire de serveur** puis cliquer sur **Services de fichiers et de stockage** Puis cliquer sur **Pools de stockage**.

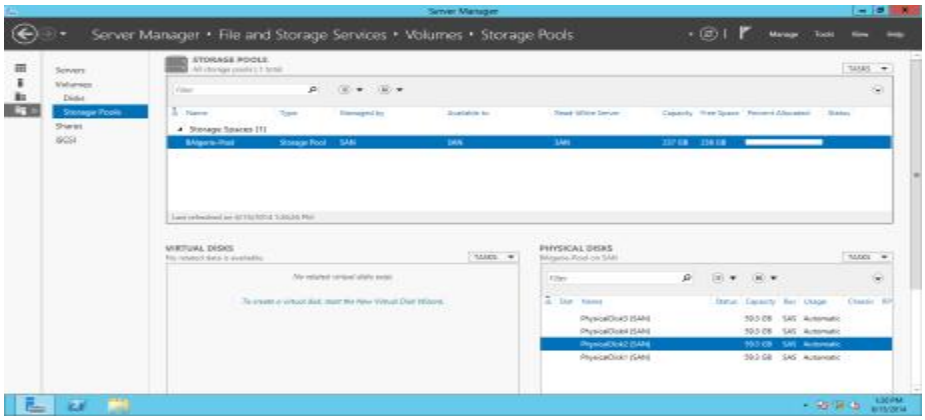


Figure C.14 : pools stockage

Au niveau du panneau **Disques Virtuels** cliquer sur **Tâches** puis sur **Nouveau disque Virtuel**.

La fenêtre suivante s'affiche.

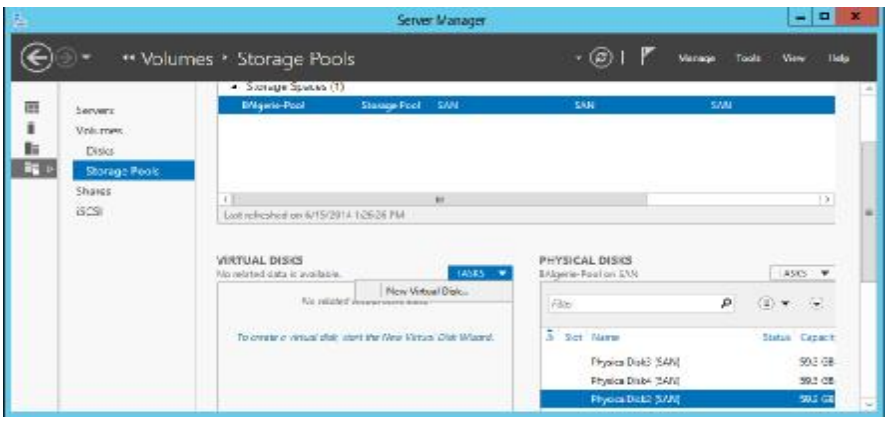


Figure C.15 : création de disque

Cliquer sur **Suivant** puis choisir le **Pool de stockage** au sein duquel le disque virtuel doit être créé puis cliquer sur **Suivant**.

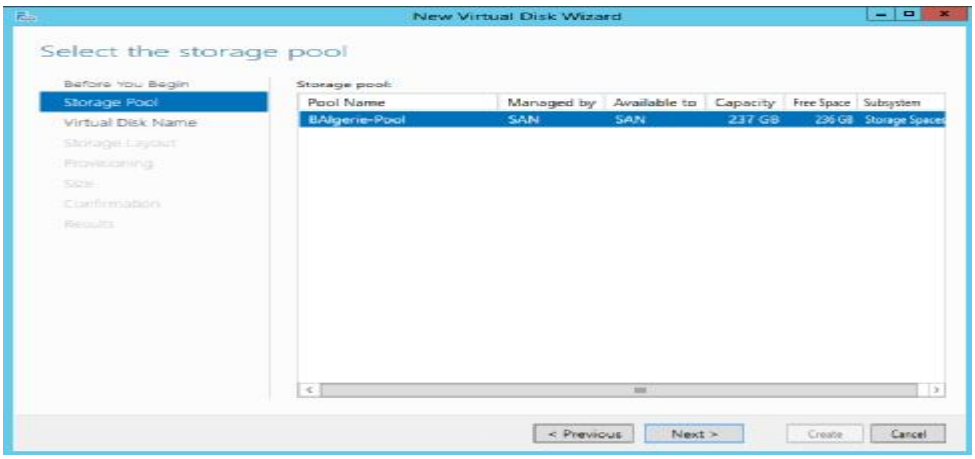


Figure C.16 : Sélection l'emplacement de création

Renseigner le nom du disque virtuel à créer puis cliquer sur suivant.

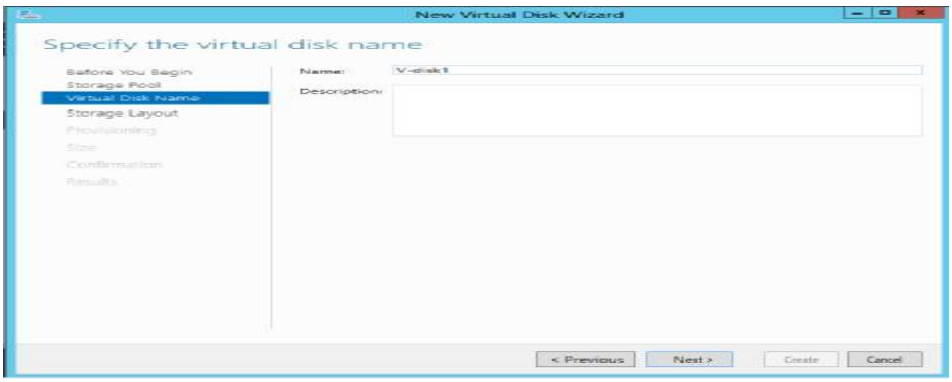


Figure C.17 :Entrer le nom du disque

Choisir le type de stockage à créer :

- **Simple** (volume de type RAID 0).
- **Mirror** (volume de type RAID 1).
- **Parity** (volume de type RAID 5).

Puis cliquer sur **Suivant**.

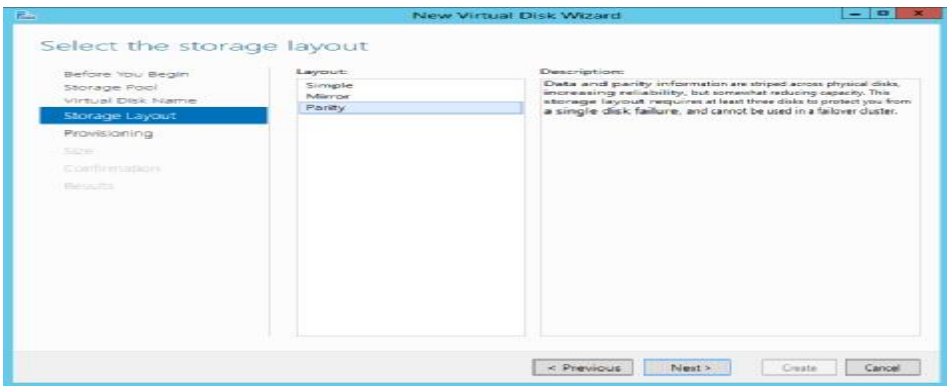


Figure C.18 : Type de stockage

Choisir le type de disque (thin ou thick) puis cliquer sur **Suivant**.

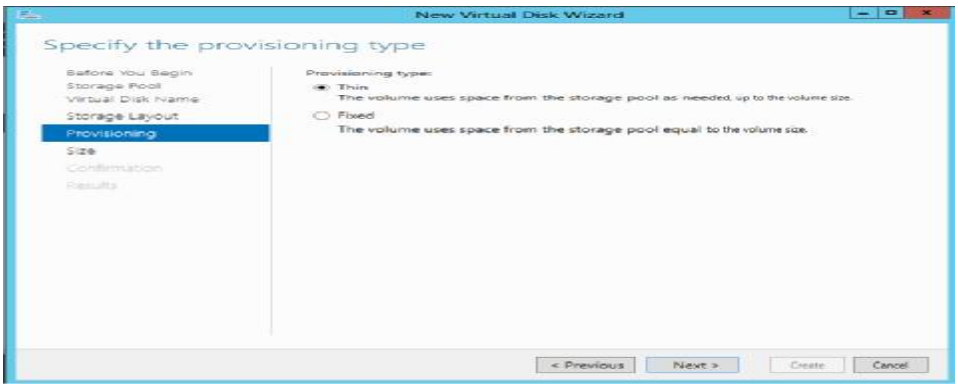


Figure C.19 : Type de disque

Renseigner la taille maximale allouée au disque virtuel puis cliquer sur **Suivant**.

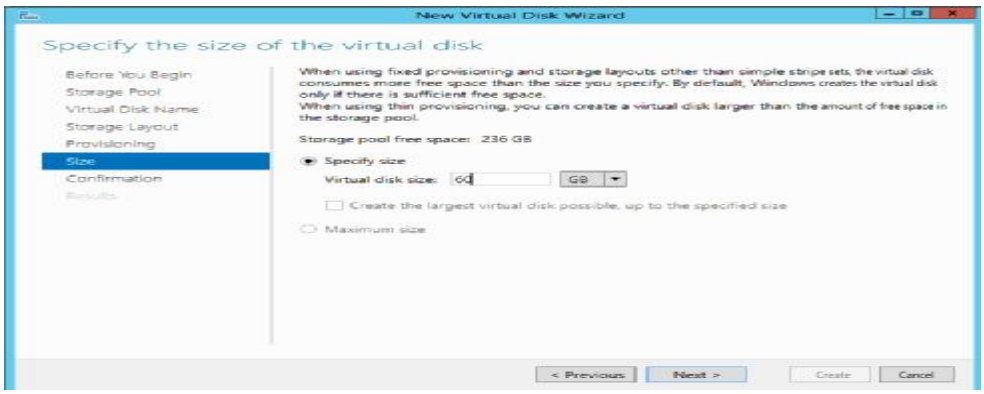


Figure C.20 : Taille de disque

Puis cliquer sur **Suivant**.

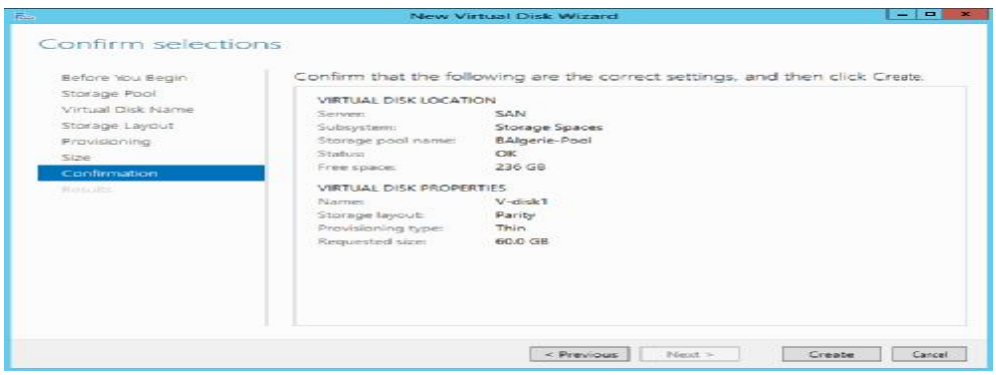


Figure C.21 :Confirmation des configurations

Puis cliquer sur **Créer**. Le disque virtuel sera créé

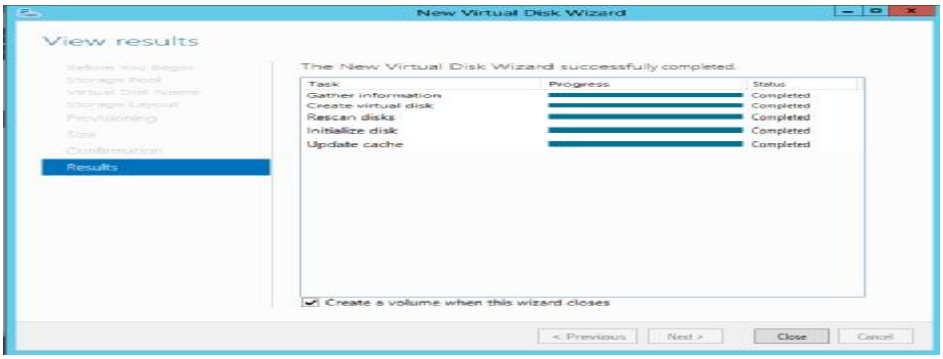


Figure C.22 : Confirmation de création

c. Créer un volume sur un disque virtuel

Pour créer un volume sur un disque virtuel, ouvrir le **Gestionnaire de serveur**.

Puis cliquer sur **Services de fichiers et de stockage** puis cliquer sur **Pools de stockage**.

Effectuer un clic droit sur le disque virtuel à initialiser puis cliquer sur **Nouveau Volume**

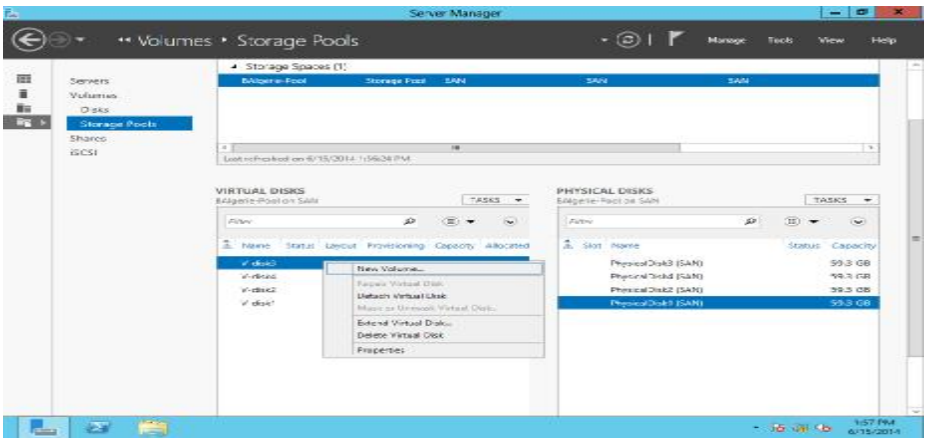


Figure C.23 : Création de volume

Cliquer sur **Suivant ->**

Choisir le serveur auquel le volume sera présenté puis cliquer sur **Suivant**.

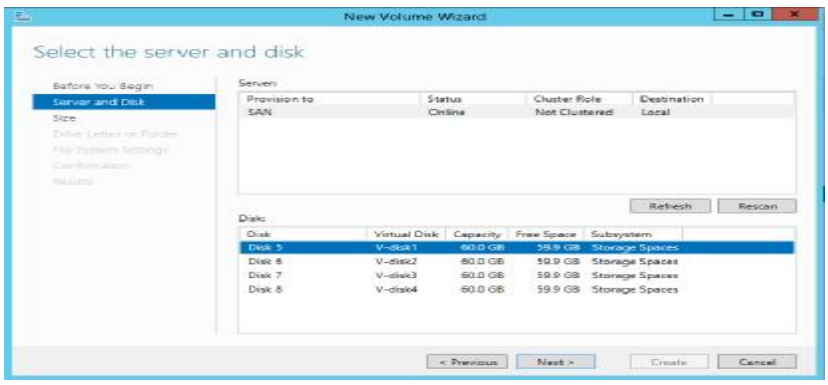


Figure C.24 : Server où le volume sera présenté

Renseigner la taille du volume à créer. Puis cliquer sur **Suivant**.

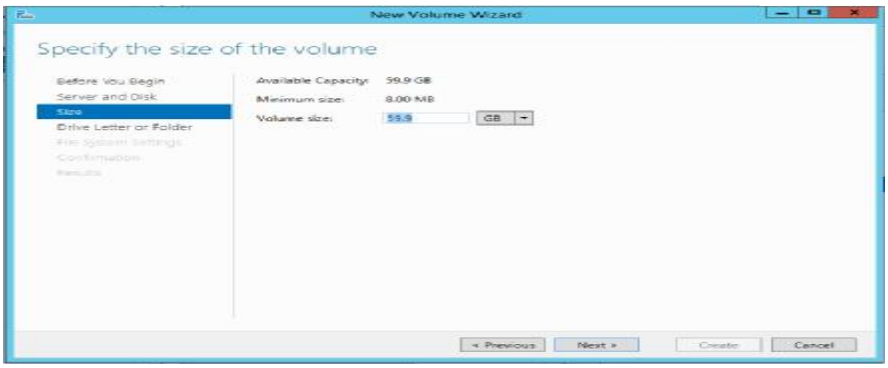


Figure C.25 : La taille du volume à créer

Choisir la lettre de lecteur ou le dossier assigné au volume puis cliquer sur **Suivant**.

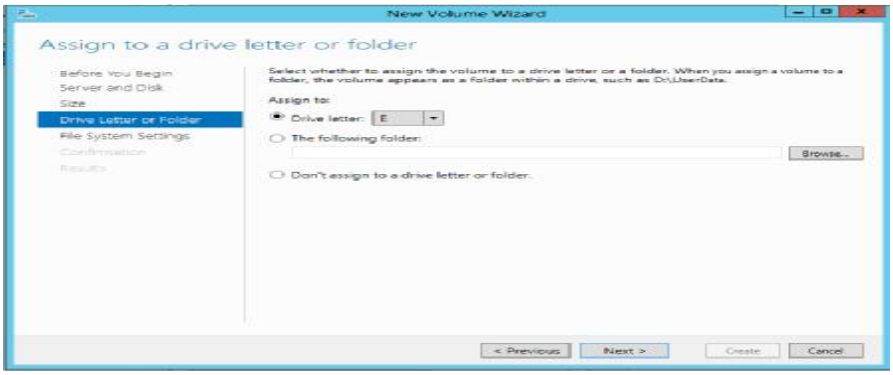


Figure C.26 : Lettre assigné au volume

Choisir le système de fichiers et le nom du volume puis cliquer sur **Suivant**

Cliquer sur **Créer**.

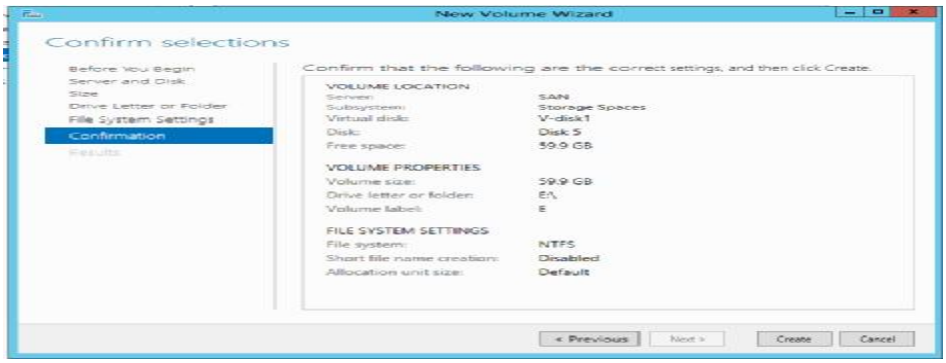


Figure C.28 : Confirmation des paramètres

Cliquer sur **Fermer**

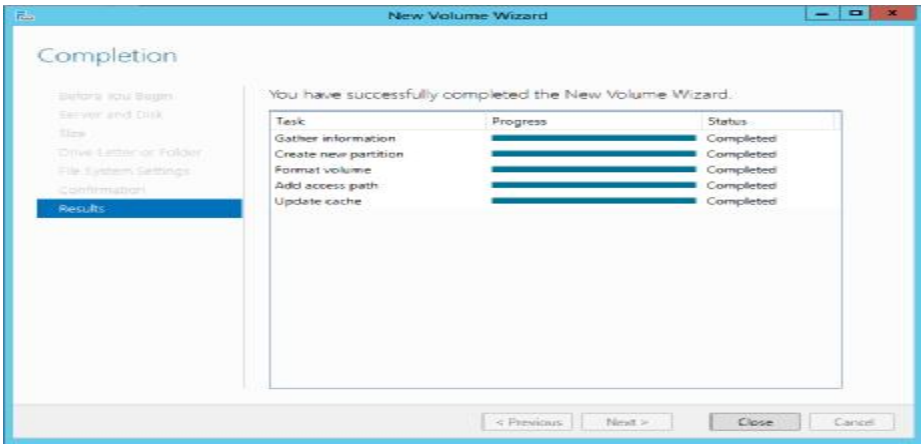


Figure C.29 : Confirmation de création

d. Création de disques iSCSI

Pour créer des disques iSCSI, ouvrir le gestionnaire de serveur, puis dans la partie **Services de Fichiers et de Stockage**, cliquer sur **iSCSI**.

Figure C.30 : sélection iSCSI

Cliquer sur **Tâches**. Puis **Nouveau disque virtuel iSCSI**

Figure C.31 : Nouveau disque virtuel iSCSI

Choisir le **serveur hôte** du **disque virtuel** et le **volume** sur lequel le disque sera créé puis cliquer sur **Suivant**.

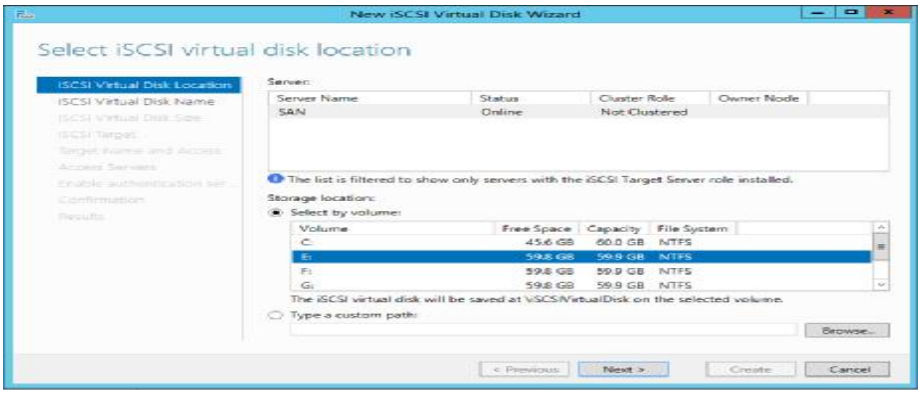


Figure C.32 : Volume dont le disque sera créé

Renseigner un **nom** et éventuellement une **description** puis cliquer sur **Suivant**.

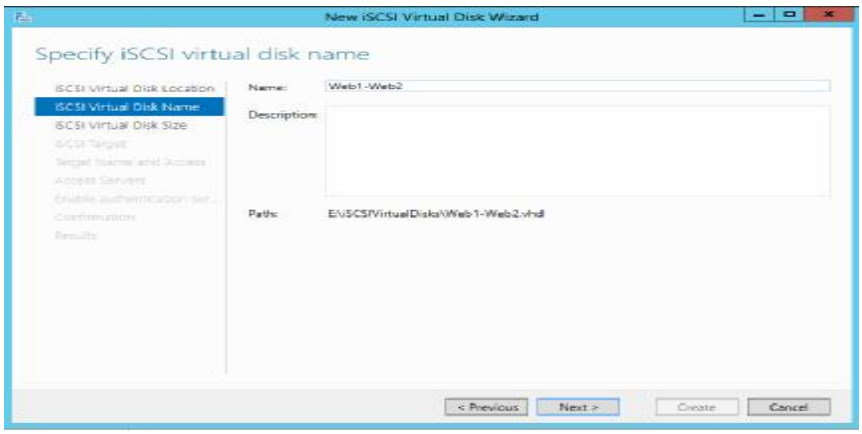


Figure C.33 :le nom de disque

Renseigner la taille du disque virtuel à créer puis cliquer sur **Suivant**.

Figure C.34 : la taille du disque virtuel à créer

Cliquer sur **Nouvelle cible iSCSI** puis cliquer sur **Suivant**.

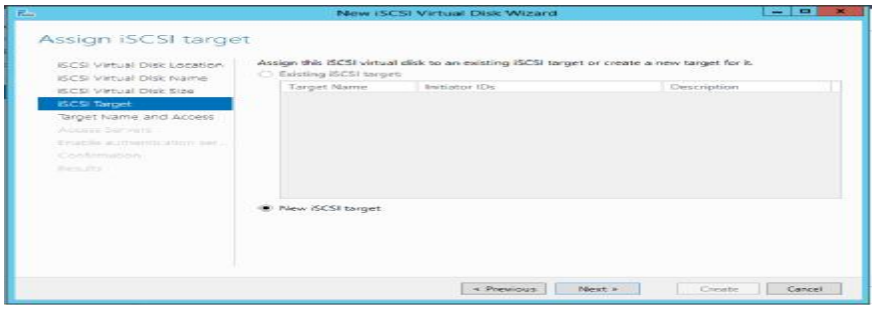


Figure C.35 : Nouvelle cible iSCSI

Cliquer sur **Next**.

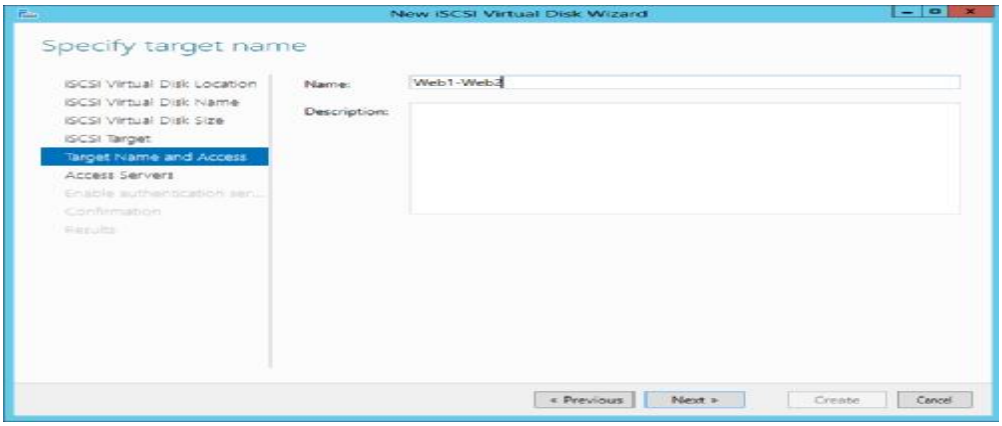


Figure C.36 : le nom de disque

Cliquer sur **Ajouter**.

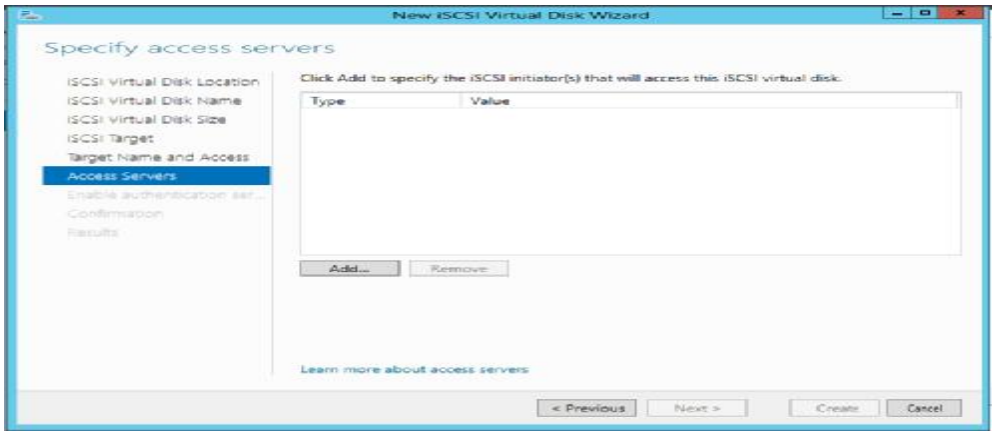


Figure C.37 : Ajout de disque

Ajouter les adresses IP :

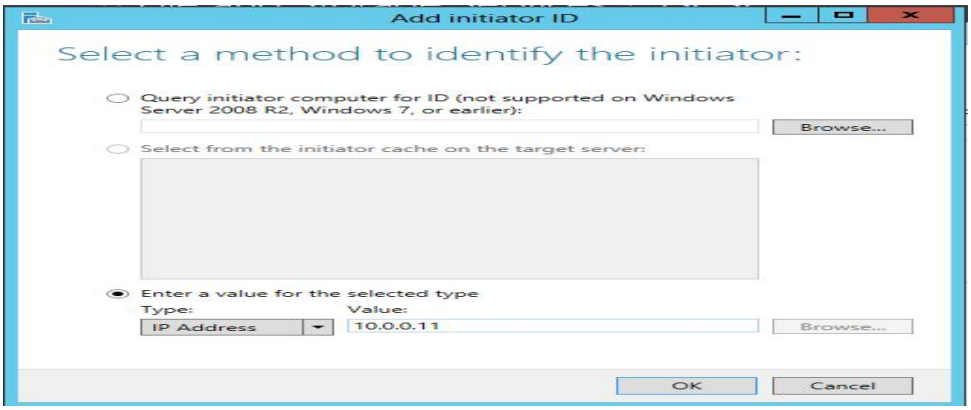


Figure C.38 : Association d'adresse IP

Une fois les adresses ajoutés cliquer sur **Suivant**.

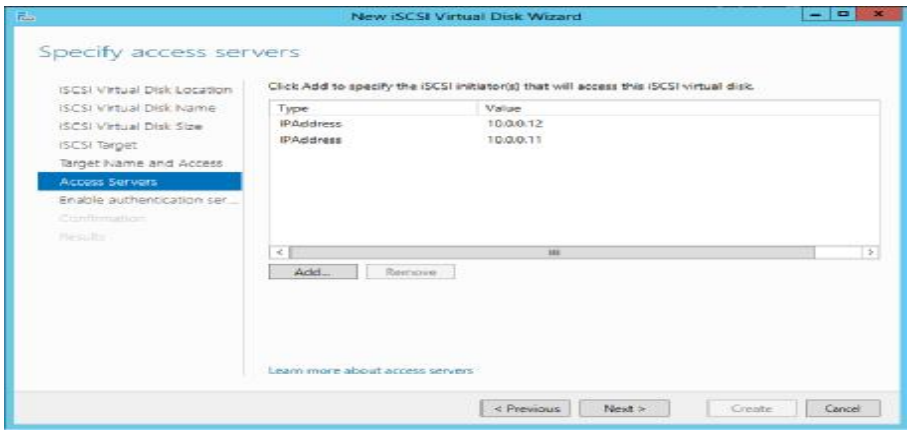


Figure C.39 :Les adresses IP ajoutés

Activer ou non le protocole CHAP ou CHAP inversé. Puis cliquer sur **Suivant**.

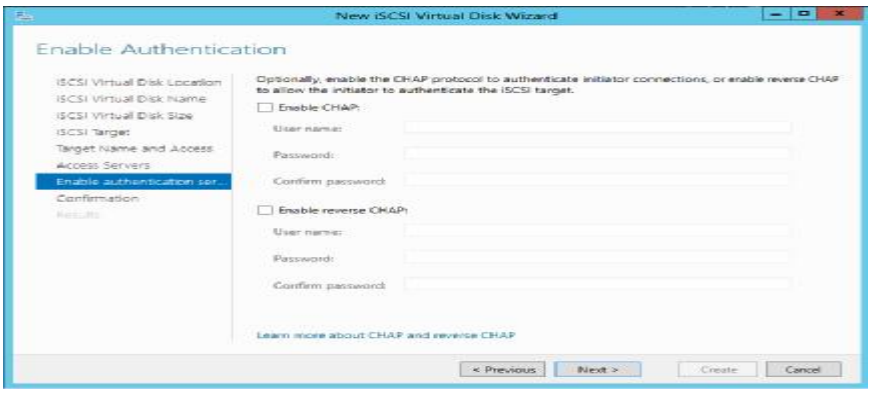


Figure C.40 : Activation ou non des protocoles

Cliquer sur **Créer**

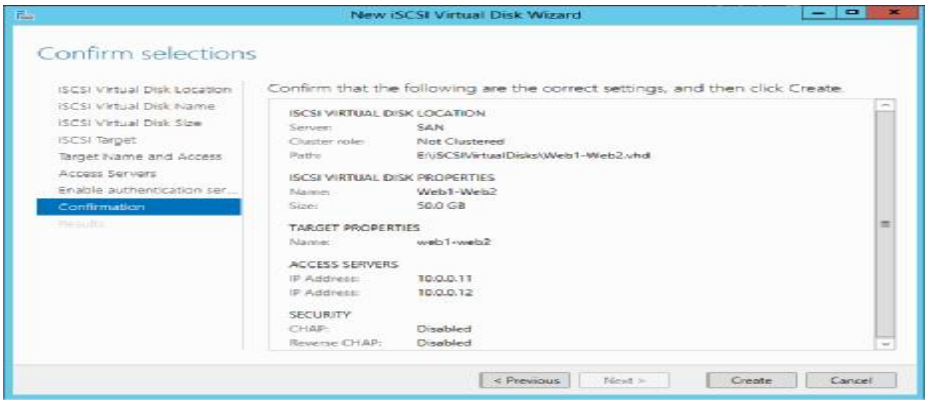


Figure C.41 : confirmation des paramètres

Le disque est maintenant créé.

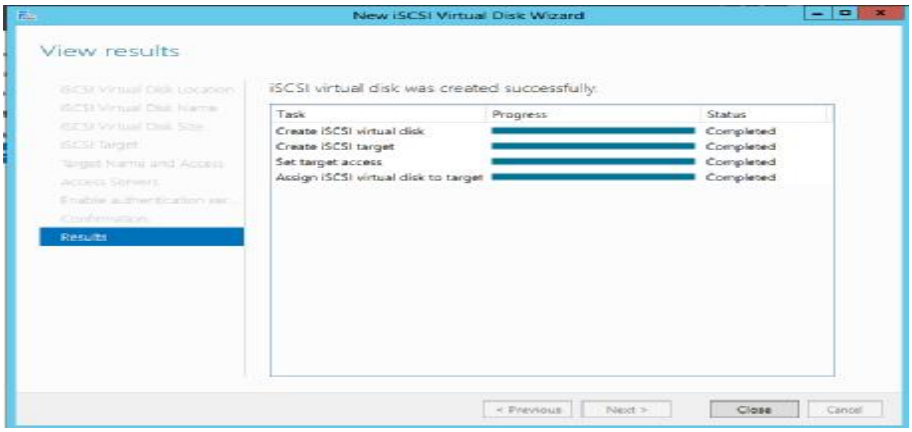


Figure C.42 : création réussite

e. Création d'un Pool de Stockage

La liste des disques physiques apparait -> Cliquer sur **Pools de stockage**.

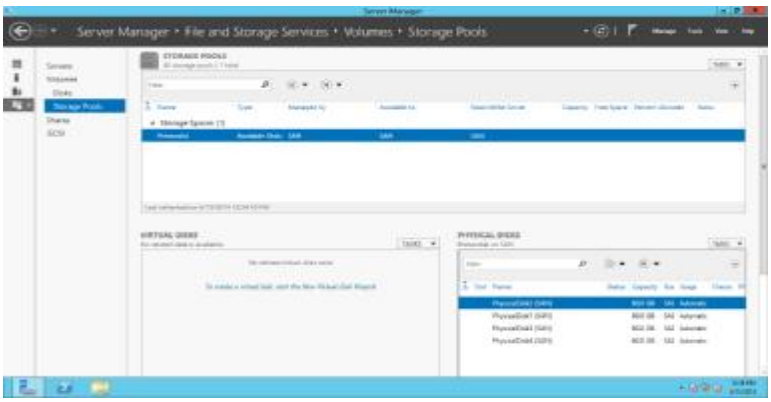


Figure C.43 : Accès au pools de stockage

Puis cliquer sur **Tâches** puis **Nouveau Pool de stockage**

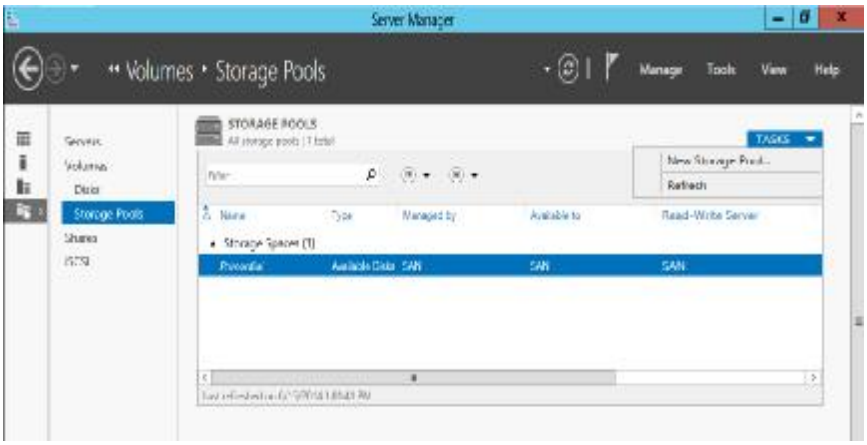


Figure C.44 : Nouveau pool de stockage

L'assistant de création d'un **Pool de stockage** s'affiche. Cliquer sur **Suivant**.

Entrer un **Nom de Pool** et éventuellement une **description**.

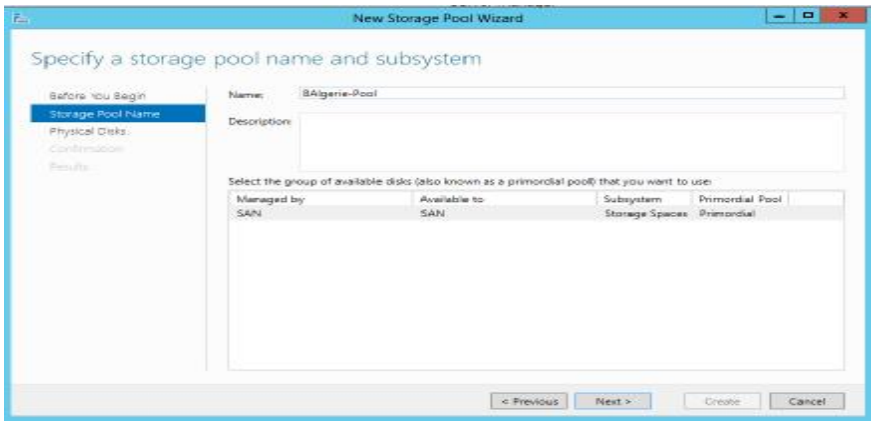


Figure C.45 : le nom de pool de stockage

Cliquer sur **Suivant**.

Choisir le /les disques physiques associés au **Pool** puis cliquer sur **Suivant**.

NOTE : La partie **affectation** permet de paramétrer un /des disques en hot spare.

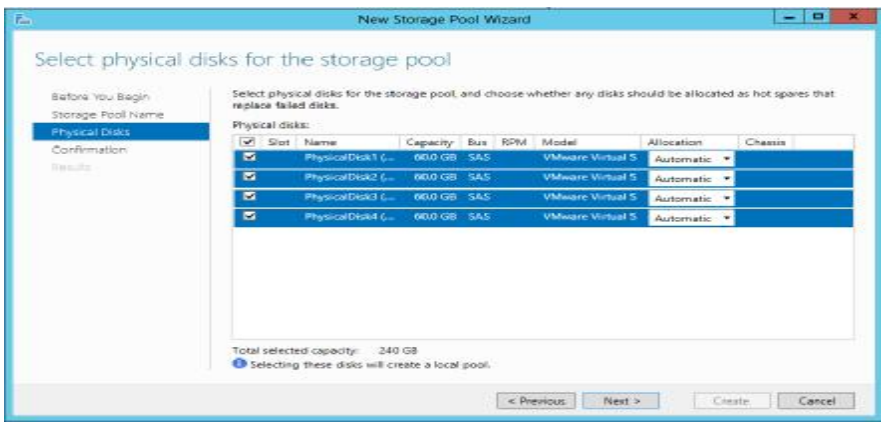


Figure C.46 : choix de disque physiques associés au Pool

Puis cliquer sur créer.

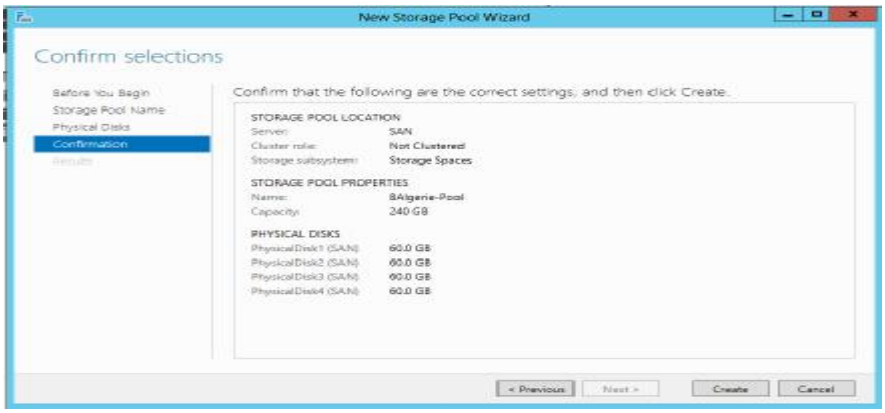


Figure C.47 : confirmations des paramètres

Attendre la fin du processus de création puis cliquer sur **Fermer**.

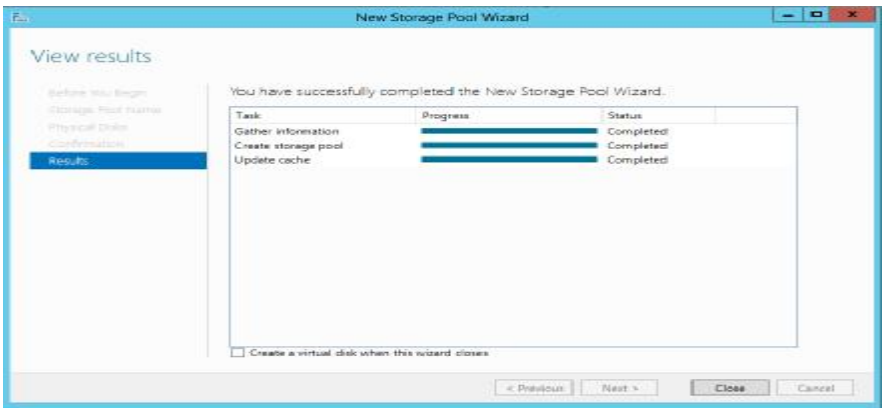


Figure C.48 : fin de création

f.Installation rôle de server cible iSCSI

Pour installer le rôle de fournisseur de stockage iSCSI, ouvrir le gestionnaire de serveur, puis dans la partie **Services de Fichiers et de Stockage**, cliquer sur **iSCSI ->Suivant** ; Choisir le type d'installation puis cliquer sur **Suivant ;**

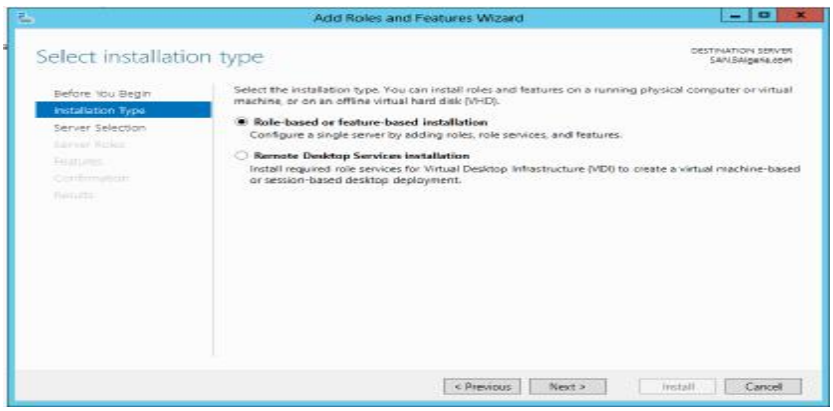


Figure C.49 : Type d'installation

Choisir le serveur sur lequel installer le rôle puis cliquer sur **Suivant**.

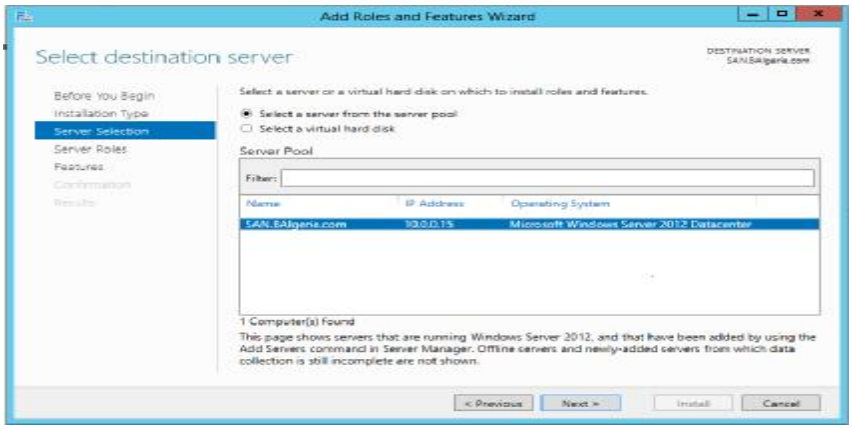


Figure C.50 : sélection de server

Sélectionner le rôle **de server cible iSCSI**. Cliquer sur **Suivant**.

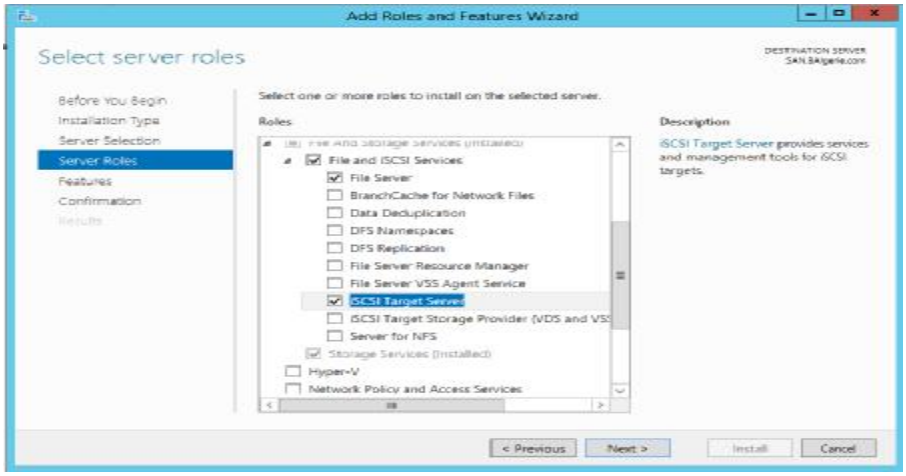


Figure C.51 : Ajout d'iSCSI

Cliquer sur **Suivant** -> **Installer**.

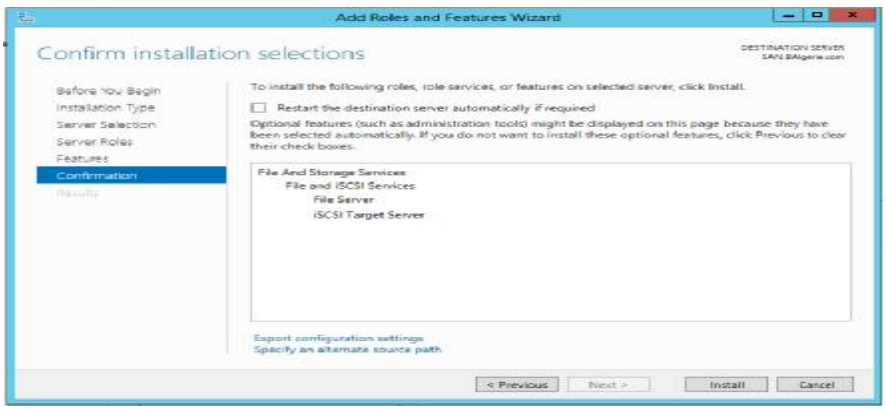


Figure C.52 : confirmer l'installation

Cliquer sur **Fermer**.

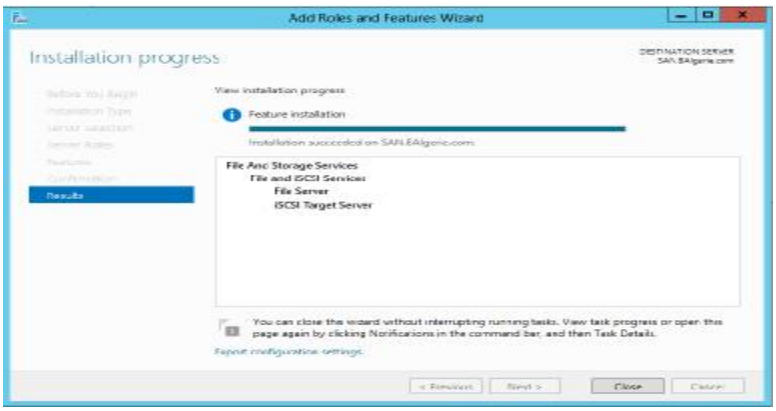


Figure C.53 : progression d'installation

Apres avoir joint le serveur au domaine, on clique sur **ajouter les fonctionnalités**

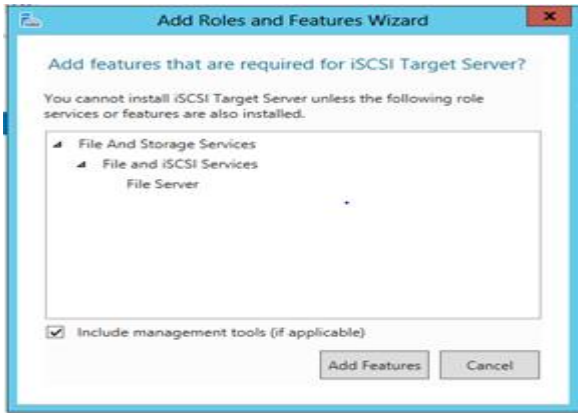


Figure C.54 : Ajout des outils

g.Création d'un disque Virtuel

Aller « virtuelle machine and setting » puis « hardware » pour ajouter un disque :

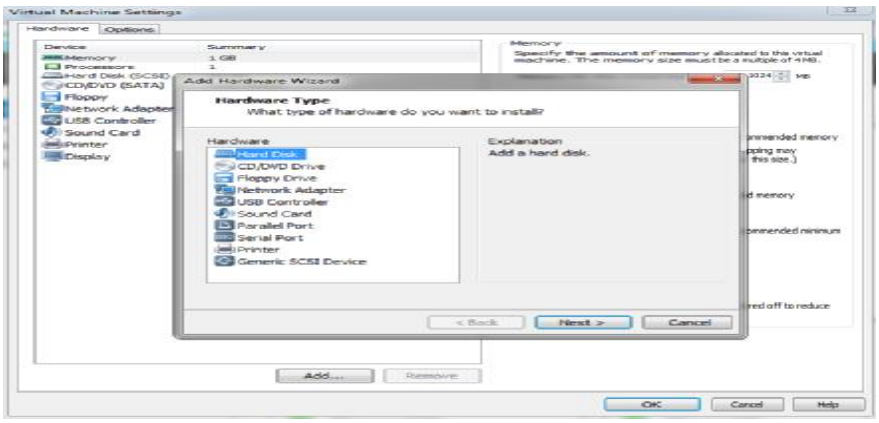


Figure C.55 : l'ajout de disque

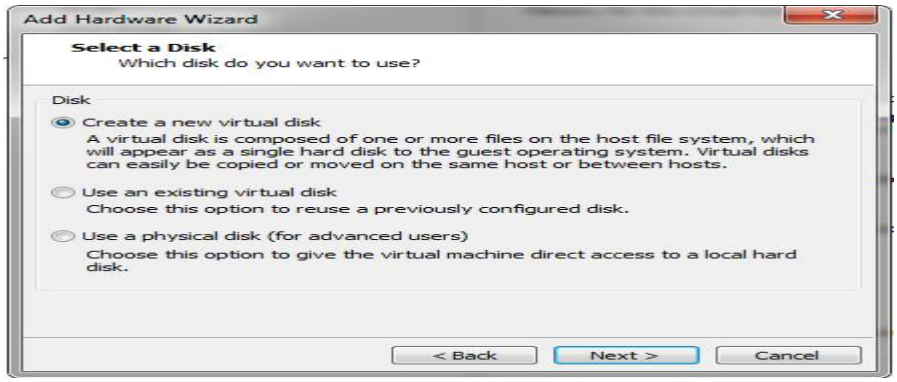


Figure C.56 : sélectionné ‘ virtuel disk’

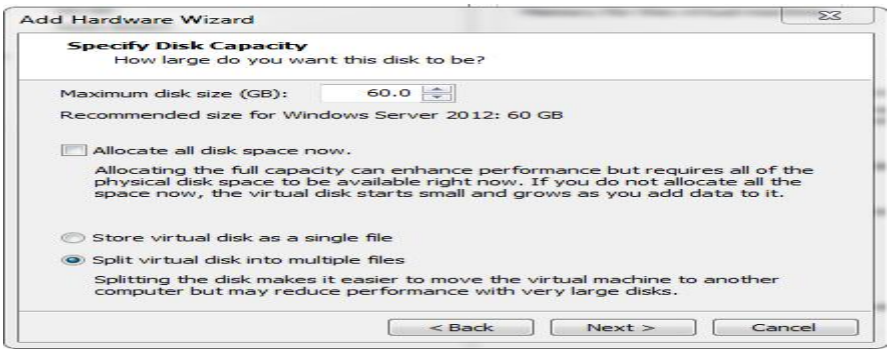


Figure C.57 :

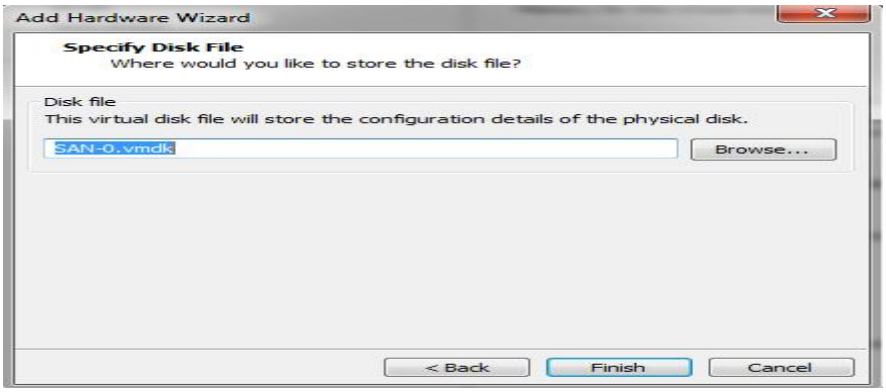


Figure C.58 : Spécifions le fichier de disque virtuel

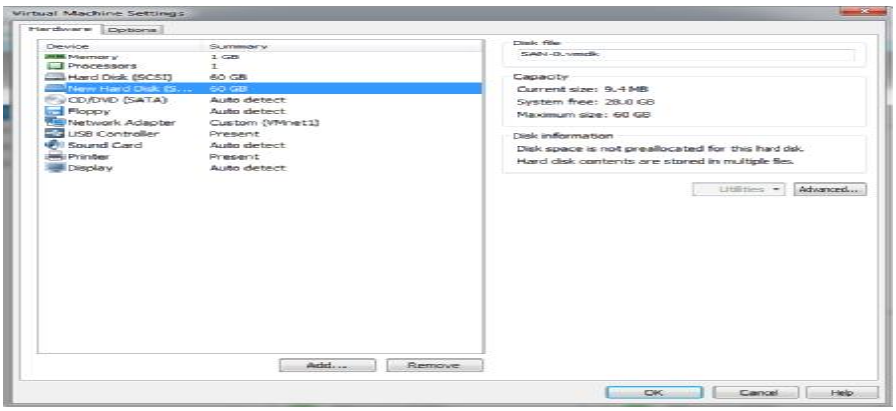


Figure C.59 : Fin de création de disque

h.Créer un volume sur un disque virtuel

Pour créer un volume sur un disque virtuel, ouvrir le **Gestionnaire de serveur**.

Puis cliquer sur **Services de fichiers et de stockage**

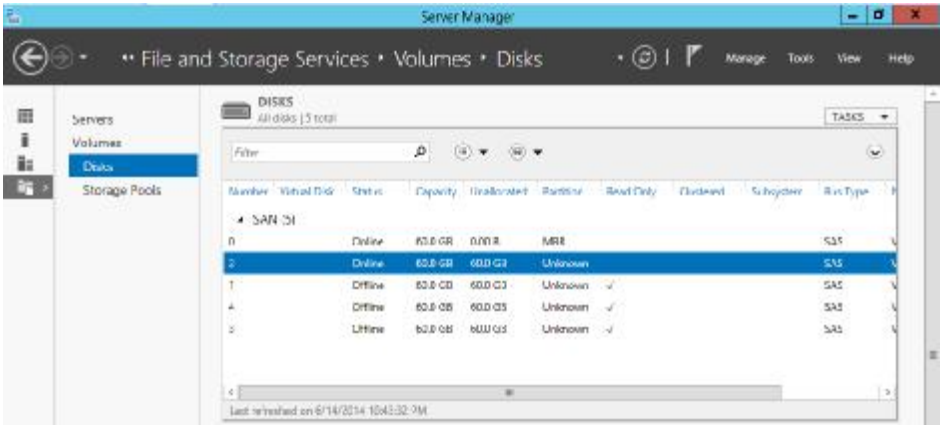


Figure C.60 : Services de fichiers et de stockage

Choisir le serveur auquel le volume sera présenté puis cliquer sur **Suivant**.

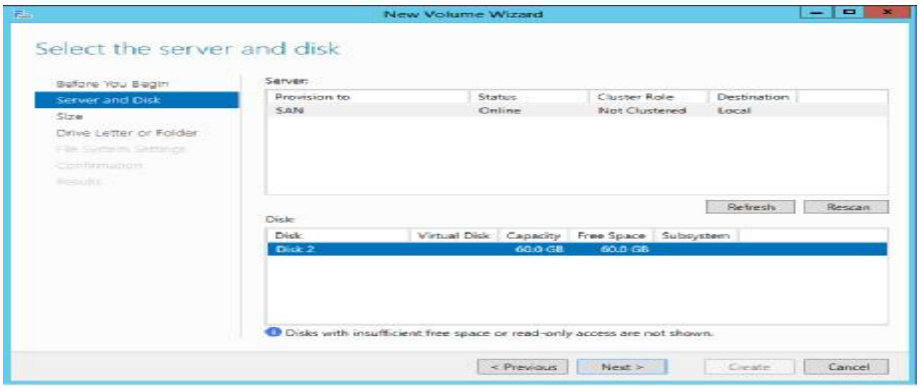


Figure C.61 : Sélection serveur auquel le volume sera présenté

Renseigner la taille du volume à créer. Puis cliquer sur **Suivant**.

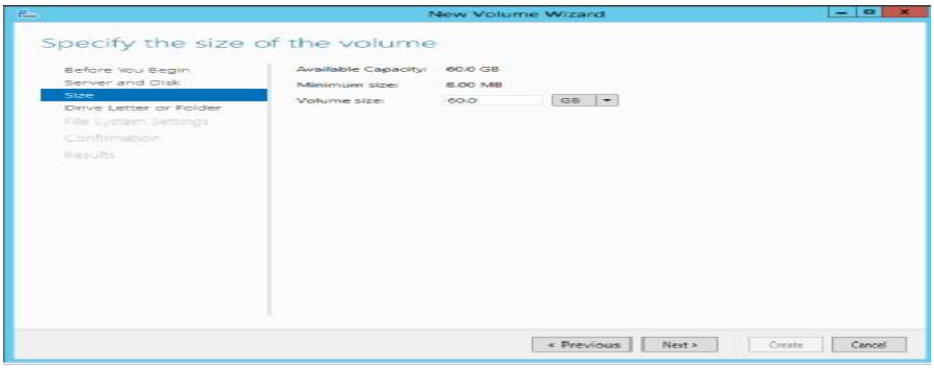


Figure C.62 : la taille du volume à créer

Choisir la lettre de lecteur ou le dossier assigné au volume puis cliquer sur **Suivant**.

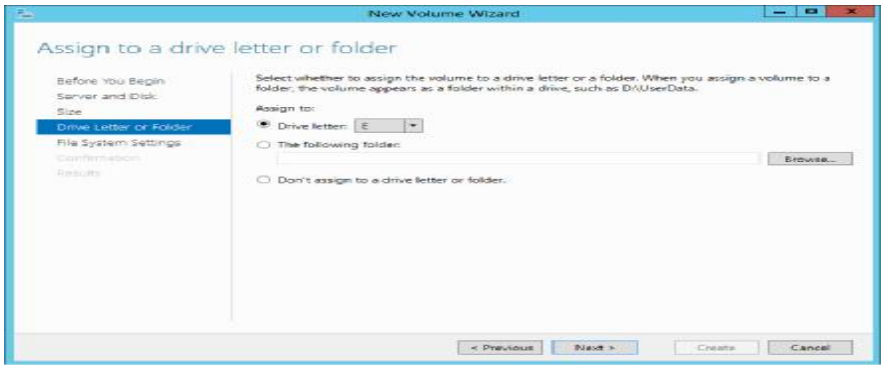


Figure C.63 : la lettre de lecteur assigné au volume

Choisir le système de fichiers et le nom du volume puis cliquer sur **Suivant**.

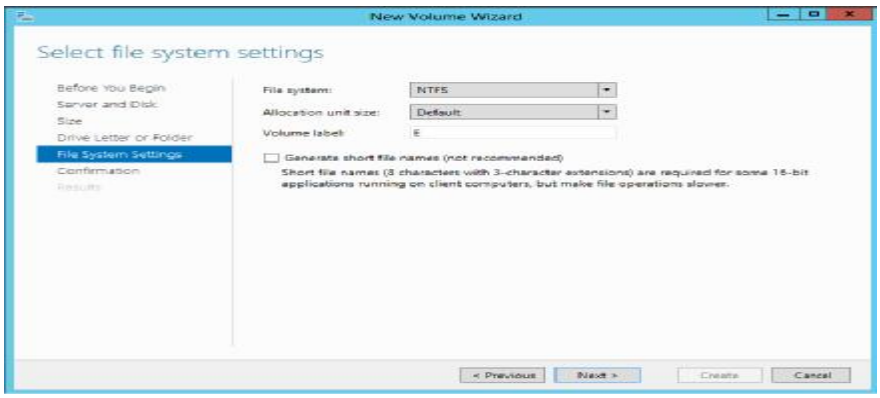


Figure C.64 : le système de fichiers

Cliquer sur **Créer**.

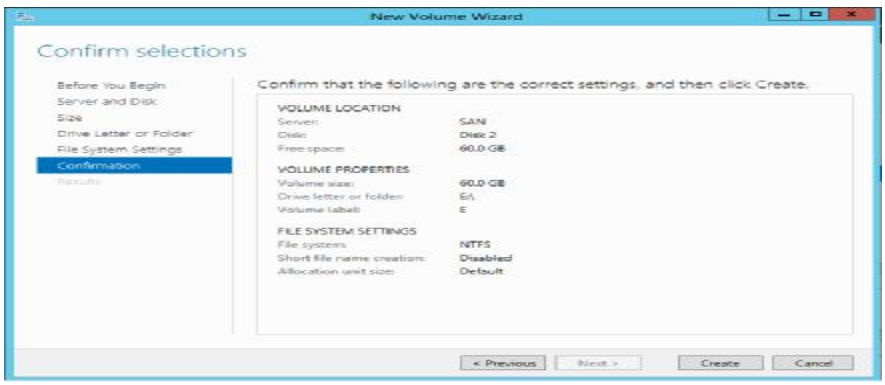


Figure C.65 : confirmer les paramètres

Cliquer sur **Fermer**.

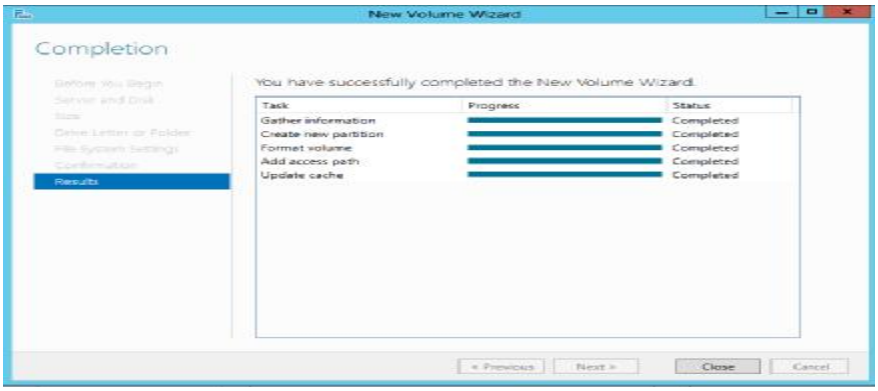


Figure C.65 : création complète

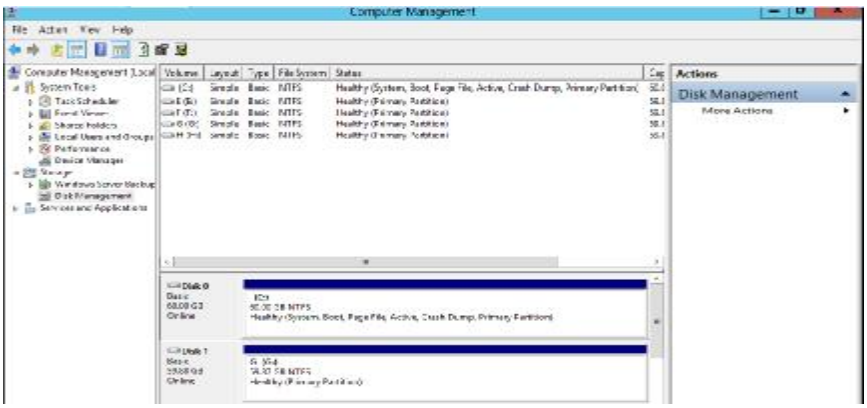


Figure C.66 : résultat de création

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 informatiqueCERAM, « 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 BolovanCalinBorgdan, 2011

[12] Laurent Bloch, CristophWolfhugel, 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 détectiond'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] AvoledoMickaël, 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.

[25Nicolas Baudoin Ingénieurs2000Marion Karle 2003-2004**NT Réseaux**IDS et IPS Enseignant : Etienne Duris 2003/2004 IR32

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

[28]Laurent LEVIER Certified Information Systems Security Professional (CISSP) Certified Information Security Manager (CISM) Officier de sécurité du réseau interne, Equant Télécommunications

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.clustersec.com/dhcp-failover-sur-windows-server-2012/

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

http://popravak.wordpress.com/2012/02/15/cisco-ips-sensor-scenario-two-inline-interface-pairs/

http://free4arab.com/?cat=17

http://fr.scribd.com/doc/77060306/Configuration-et-gestion-d-Exchange-2010-tuto-de-A-a-Z

http://blogs.technet.com/b/stanislas/archive/2010/12/10/forefront-tmg-2010-guide-d-installation-d-un-serveur-mono-carte-role-proxy-web-ou-reverse-proxy-en-pas-224-pas.aspx