République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique
UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DE **G**ENIE **E**LECTRIQUE ET D'**I**NFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etudes

de MASTER ACADEMIQUE

Spécialité : Réseaux et télécommunication

Filière : Génie électrique

Présenté par

MIHOUBI MOHAMED
MEDJANI NACER

Mémoire encadré par LAHDIR.M et co-dirigé par KIBOUH.M

Thème

Sécurisation d'une infrastructure LAN/WAN A base d'équipement Cisco

Laboratoire et/ou entreprise où le travail a été réalisé : 2INTPartners

Promotion: 2015

Remerciements

Au terme de ce travail, nous tenons à exprimer notre profonde gratitude et nos sincères remerciements à notre encadreur MR LAHDIR.M pour sa patience, sa disponibilité et surtout ses judicieux conseils.

Nos plus sincères remerciements vont à tous les membres de jury qui nous ont fait l'honneur de juger notre travail.

Nos remerciements vont enfin à toute personne qui a contribué de près ou de loin à l'élaboration de ce travail.

Dédicace

Je dédie ce modeste travail à :

Mes très chers parents à qui je doits tout, je profite de les remercier pour leur encouragement, leur aide, le soutien qu'ils m'ont apporté et le sacrifice qu'ils ont fait pour moi, que Dieu les protège et les entoure de sa bénédiction.

*A la mémoire de ma Grand-Mère **HEDJILA LHADJ**.*

*Mes chères sœurs **WARDA et LILIA**.*

*Ma chère fiancée **ELYASMINE** et a toute sa famille.*

*A mon ancle **AMAR** et à toute sa famille.*

Tous mes ami(e)s ainsi qu'à tous ce qui me sont chers.

Et à toute personne m'ayant fait part de son savoir.

Mihoubi mohamed

Dédicace

Je dédie ce modeste travail à :

A la mémoire de mes chers grands parents.

A mes chers parents qui ont toujours étaient présents pour moi,

et à qui je souhaite une bonne santé et une

longue vie pleine de bonheur.

*A mes chers frères: **SAMUEL**, **MIDI** et **YOUCEF**.*

*A ma chère sœur : **NADIA** et son mari **MOHAND**.*

*Et ma nièce adorée : **DELINA**.*

A toute ma famille et mes ami(e)s.

Je remercie tous ceux et celles qui m'ont aidé à réaliser ce travail.

Medjani Nacer

Chapitre I: La sécurité des réseaux informatiques

Chapitre II : Sécurisation des interconnexions

Chapitre III : Sécurisation d'une infrastructure LAN/WAN

Chapitre IV : Application

Introduction

Introduction

Les trois derniers siècles ont chacun été marqué, par des progrès technologiques spectaculaires ; le 18 è siècles a été celui de grands systèmes mécaniques de la révolution industrielle, le 19 è siècles nous a apporté la première locomotive à vapeur. Et le 20 è siècles était l'ère de la collecte, du traitement et de la distribution des informations. Cette dernière période a aussi connu d'autres développements majeurs, comme le déploiement de réseau téléphonique à l'échelle mondiale, l'explosion de l'industrie informatique et le lancement de satellites de télécommunication.

L'informatique est devenue un outil incontournable de gestion, d'organisation, de production et de communication. Le réseau informatique de l'entreprise met en œuvre des données sensibles, les stocke, les partage en interne, les communique parfois à d'autres entreprises. Cette ouverture vers l'extérieur conditionne des gains de productivité et de compétitivité.

Il est donc impossible de renoncer aux bénéfices de l'informatisation, d'isoler le réseau de l'extérieur, de retirer aux données leurs caractères électroniques et confidentiels. Les données sensibles du système d'information d'une entreprise sont exposées aux actes de malveillance telle que l'augmentation des nombres de hacker, cyber crime. Il est donc capital de veiller à la sécurité des données aussi bien en interne qu'à l'extérieur.

La banque prise comme exemple dans notre mémoire, dispose d'un réseau informatique qui lui permet de faire des échanges d'informations avec ses partenaires. Par conséquent elle doit gérer et sécuriser son système d'information très important. Outre cette ouverture de l'extérieur, elle est menacée à l'intérieur de son réseau local par des virus informatiques et quelques disfonctionnements de son système informatique.

C'est pour palier à ces problèmes précités et dans le souci de rendre le système d'information évolutif, extensible, disponible et sécurisant, notre choix est porté à auditer et sécuriser le réseau informatique et les données de la banque et à établir une politique de sécurité.

Notre mémoire est réparti en quatre chapitres, dans le premier chapitre nous allons présenter les généralités sur la sécurité des réseaux informatiques. Dans le deuxième chapitre nous expliquerons la sécurité des différentes interconnexions. Le troisième chapitre sera consacré à la sécurisation de l'infrastructure de la banque, nous exposerons les vulnérabilités de l'architecture réseaux et les solutions proposées. Le dernier chapitre, se focalisera sur le développement de notre application ou on présentera la solution mise en place avec l'explication de la configuration et l'installation des nouveaux matériels choisis dans les solutions. Et enfin, nous terminerons notre mémoire par une conclusion ainsi que des perspectives ouvertes.

Chapitre I:
La sécurité des réseaux informatiques

I.1.Préambule

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

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

Dans ce chapitre, nous aborderons les différents aspects liés à la sécurité, les types d'attaques et leurs mécanismes de détection et la protection des réseaux informatiques

I.2.Définition d'un réseau informatique

Un réseau informatique est un ensemble d'équipement informatiques (ordinateur et périphériques) reliés entre eux grâce à des supports de communication (câble : réseau câblé, ou onde : réseau sans fil..) permettant la **communication** (transfert des informations électroniques) et le **partage de ressources** (matérielles et logicielles).

I.3.Architecture des réseaux

Les réseaux sont structurés du point de vue fonctionnel en deux catégories :

- Réseaux poste a poste (peer to peer)
- Réseaux à serveur dédié (client/serveur).

I.4.Classification des réseaux informatiques

On peut classer les réseaux selon plusieurs critères, par exemple la distance entre entité communicantes, la topologie, et le types d'accès

- Classification selon la taille

  - ✓ Les réseaux locaux LAN (Local Area Network)
  - ✓ Les réseaux MAN (Métropolitain Area Network)
  - ✓ Les réseaux étendus WAN (Wide Area Network)

- Classification selon la topologie

  - ✓ Topologie en bus
  - ✓ Topologie en anneau
  - ✓ Topologie en étoile

- Classification selon la méthode d'accès

  - ✓ Méthode d'accès CSMA/CD
  - ✓ Méthode d'accès par Token ring
  - ✓ Méthode d'accès par Standard FDDI

- Classification selon le mode de connexion

  - ✓ Modes avec connexion
  - ✓ Mode sans connexion

I.5.Les protocoles réseaux

- **Protocole DNS (Domaine Name Service)** : Est une base de données utilisée sur les réseaux IP pour transposer les noms d'ordinateurs en adresse IP
- **Protocole TCP (Transmission contrôle Protocol) :** Est un protocole fiable, orienté connexion qui permet l'acheminement sans erreur de paquets issues d'une station a une autre.
- **Protocole ICMP (Internet Control Message Protocol) :** Est un protocole qui permet le contrôle des erreurs de transmission .En effet, comme le protocole IP ne gère que le transport des paquets et ne permet pas l'envoie de message d'erreur, c'est grâce a ce protocole qu'une machine émettrice peut savoir qu'il y a eu un incident de réseau.
- **Protocole DHCP (Dynamic Host Configuration Protocol) :** Est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous -réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut.

- **FTP (File Transfert Protocol) :** Permet de transférer des fichiers d'une machine à une autre. L'utilisation de FTP depuis un poste client pour aller chercher ou déposer un fichier sur un serveur nécessite de la part de l'utilisateur de se connecter avec un nom et un mot de passe. Donc si l'utilisateur n'est pas reconnu la connexion ne sera pas établie.
- **http (Hyper Text Transfer Protocol) :** Est le protocole de communication du web permettant d'échanger des documents hyper textes contenant des données sous la forme de texte, d'image fixes ou animées et de sons. Tout client web communique avec le port **80** d'un serveur http.
- **TFTP (Trivial File Transfer Protocol ou Protocole simplifié de transfert de fichiers) :** Est un protocole simplifié de transfert de fichiers. Il fonctionne en UDP sur le port **69,** au contraire du FTP qui utilise lui TCP. TFTP reste très utilisé pour la mise à jour des logiciels embarqués sur les équipements réseaux (routeurs, pare-feu, etc.) ou pour démarrer un PC à partir d'une carte réseau.

I.6. La sécurité informatique

I.6.1.Définition

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité [01].

I.6.2.Les critères de la sécurité

La figure I.1 montre les différents critères de la sécurité.

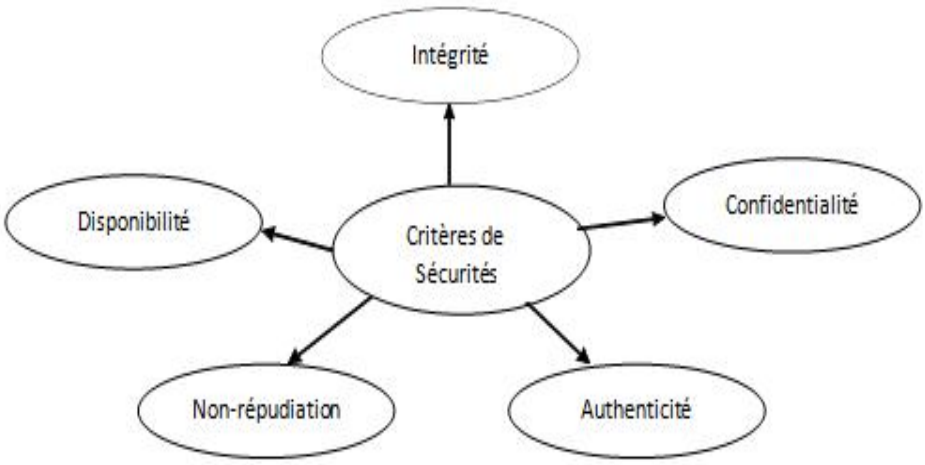


Figure I.1 : Critères de sécurité.

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

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

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

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

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

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

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

I.6.3.Politique de sécurité

I.6.3.1.Définition

la politique de sécurité définit un certain nombre de règles, de procédures et une bonne pratique permettant d'assurer un niveau de sécurité conforme au besoin de l'organisation. Elle a pour objectif:

- ✓ D'identifier les besoins en temps de sécurité, les risques informatiques et leurs éventuelles conséquences
- ✓ D'élaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiées
- ✓ De surveiller et détecter les vulnérabilités du système d'information et se tenir informer des failles sur les applications et matériels utilisés.
- ✓ De définir les actions à entreprendre et les personnes à contacter on cas de détection d'une menace.

I.6.3.2.Les types de politique de sécurité

- ✓ **La politique qui interdit tout par défaut** : dans cette approche, tout ce qui n'est pas explicitement permis est interdit. Elle consiste à définir les services à autoriser (SMTP pour l'hôte serveur de courrier, http pour l'hôte devant accéder au web) et définir les droits de chaque utilisateur.
- ✓ **La politique qui autorise tout par défaut** : dans cette approche, tout est permis sauf ce qui est considéré comme dangereux donc tout ce qui n'est pas explicitement interdit est autorisé. Elle consiste à analyser les différents risques d'application qui doivent s'exécuter, en déduire les interdictions à appliquer et autoriser tout les reste [03].

I.7. Terminologies de la sécurité informatique

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

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

I.8.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 menaces passives sont celles qui, si elles se concrétisent, ne produiraient aucune modification d'informations contenues dans le(s) système(s) et avec lesquelles ni le fonctionnement, ni l'état du système ne change. Il est très difficile de détecter ce type de menaces car elles sont inoffensives par rapport aux fonctions normales du système. L'utilisation de branchements clandestins passifs pour observer des informations transmises via une ligne de communication (surveillance de réseau) est une concrétisation d'une menace passive.
- ✓ **Menaces actives**: les menaces actives ou attaques envers un système comprennent l'altération d'informations contenues dans ce système, ou des modifications de l'état ou le fonctionnement du système. Les menaces actives sont, contrairement aux menaces passives, plus faciles à détecter si des précautions appropriées ont été prises au préalable.

  Les exemples d'attaques sont la destruction, la modification, la fabrication, l'interruption ou l'interception de données. Le résultat d'une attaque est soit une divulgation de l'information (violation de l'intégrité de l'objet) ou un déni de service (violation de la disponibilité) [04].

I.8.1.Les attaques informatiques

I.8.1.1. Les types d'attaques

Les personnes malveillantes utilisent plusieurs techniques d'attaques qui peuvent être regroupées en trois familles différentes [05] :

a. Les attaques directes

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

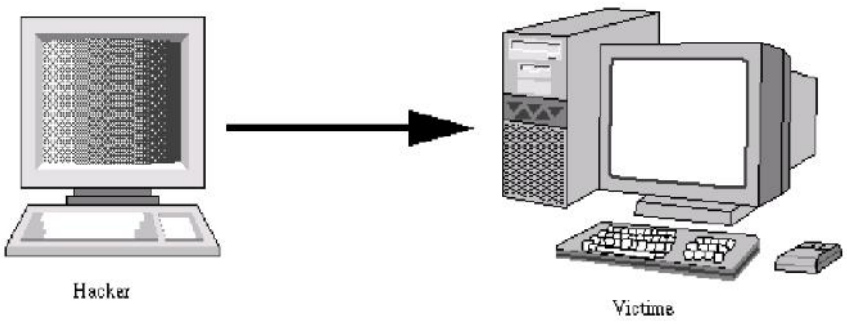


Figure I.2 : Attaque directe.

b. Les attaques indirectes par rebond

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

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

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

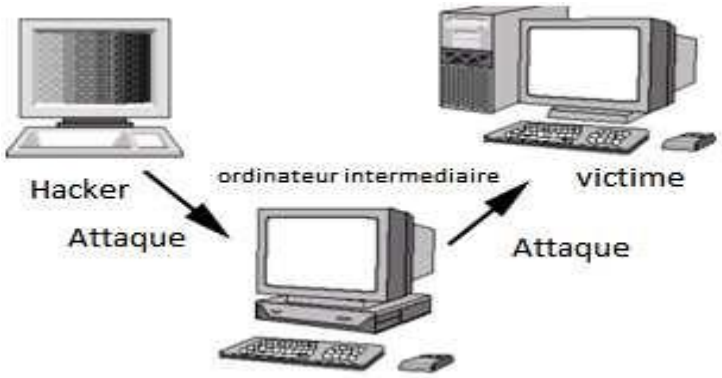


Figure I.3 : Attaque indirecte par rebond.

c. Les attaques indirectes par réponse

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

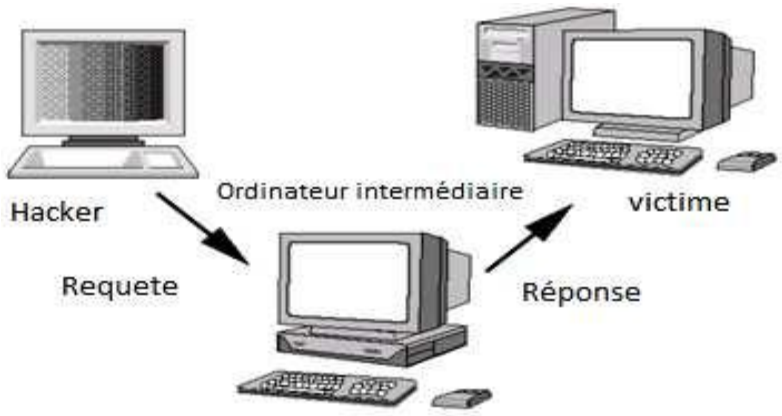


Figure I.4 : Attaque indirecte par réponse.

I.8.1.2.Les techniques d'attaques

a. Les attaques réseaux

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

1. Usurpation d'adresse IP

L'usurpation d'adresse IP (IP spoofing) est une technique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui n'a pas été attribuée à l'ordinateur qui les émet. Le but peut être de masquer sa propre identité lors d'une attaque d'un serveur, ou d'usurper en quelque sorte l'identité d'un autre équipement du réseau pour bénéficier des services auxquels il a accès [06].

2. DNS Spoofing

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

- **Empoisonnement du cache DNS**

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

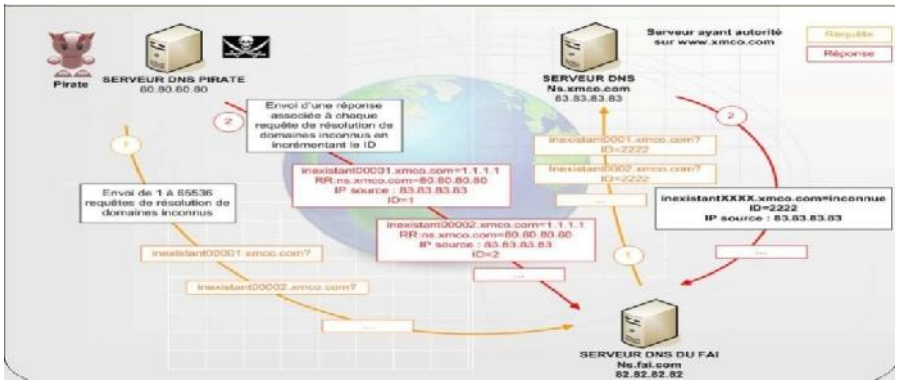


Figure I.5 : Le fonctionnement de DNS cache poisoning

- **DNS ID Spoofing**

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

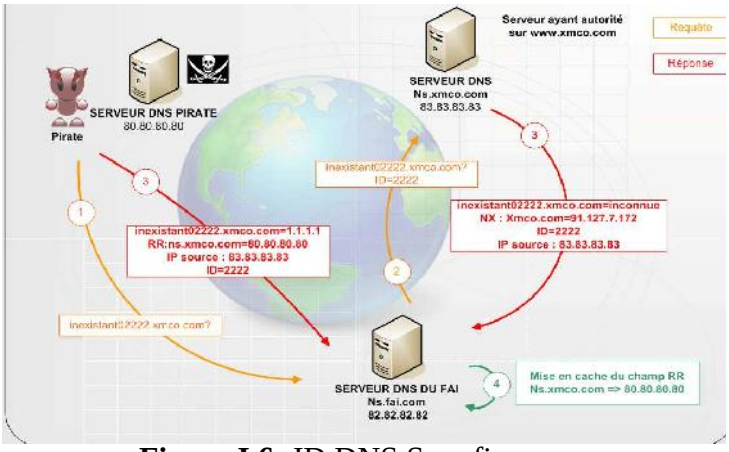


Figure I.6: ID DNS Spoofing.

3. ARP Spoofing

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

4. TCP Session Hijacking

Cette attaque consiste à rediriger un flux TCP afin de pouvoir outrepasser une protection par mot de passe. Ainsi le contrôle d'authentification s'effectuant uniquement à l'ouverture de la session, un pirate réussissant cette attaque parviendra à prendre possession de la connexion pendant toute la durée de la session. Dans un premier temps, le pirate doit écouter le réseau, puis lorsqu'il estime que l'authentification a pu se produire (délai de n secondes par exemple), il désynchronisera la session entre l'utilisateur et le serveur. Pour ce faire, il construit un paquet avec, comme adresse IP source, celle de la machine de l'utilisateur et le numéro d'acquittement TCP attendu par le serveur. En plus de désynchroniser la connexion TCP, ce paquet permettra au pirate d'injecter une commande via la session préalablement établie [07].

5. Port scanning

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

b. Les attaques applicatives :

Les attaques applicatives se basent sur des failles dans le programme utilisées, ou encore sur des erreurs de configuration. Toutes fois, il est possible de classifier ces attaques selon leur provenance :

1. les problèmes de configurations

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

Figure I.7 : Attaque par script.

3. Les injections SQL

Tout comme les attaques de scripts, les injections SQL profitent de paramètres d'entrée non vérifiés. Le but des injections SQL est d'injecter du code SQL dans une requête de base de données. Ainsi, il est possible de récupérer des informations se trouvant dans la base (exemple : des mots de passe) ou encore de détruire des données [08].

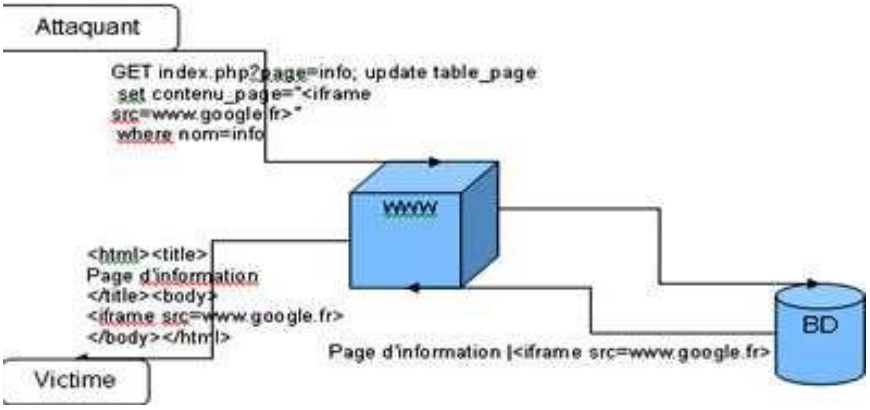


Figure1.8: Injection SQL.

4. Man in the middle

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

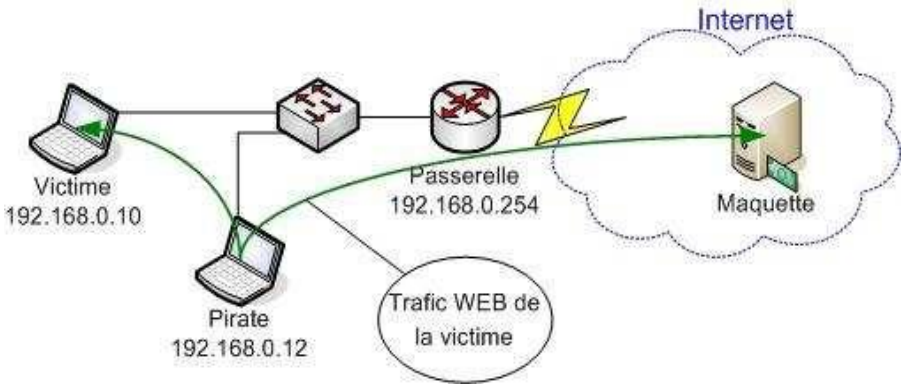


Figure I.9: Attaque Man in the middle.

5. Le Déni de service

Le déni de service est une attaque visant à rendre indisponible un service. Ceci peut s'effectuer de plusieurs manières, par le biais d'une surcharge réseau rendant ainsi la machine totalement injoignable,

ou bien de manière applicative en crashant l'application à distance. Grâce à quelques instructions malicieuses et suite à une erreur de programmation, une personne mal intentionnée peut rendre indisponible un service (serveur web, serveur de messagerie) voire un système complet. Voici quelques attaques réseaux permettant de rendre indisponible un service :

A. SYN Flooding

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

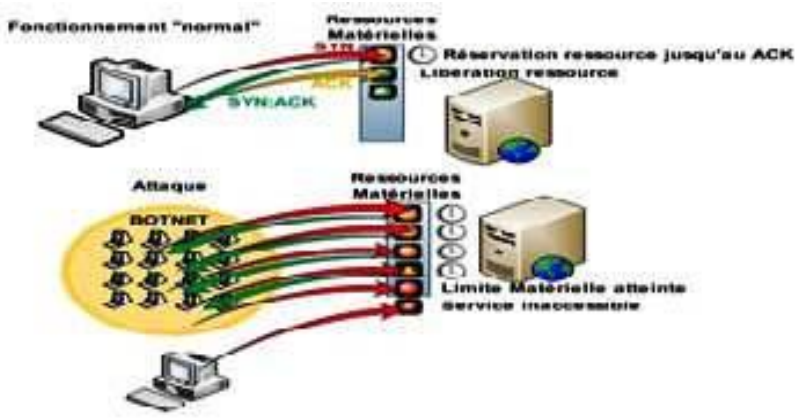


Figure I.10: SYN flooding.

B. UDP Flooding

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

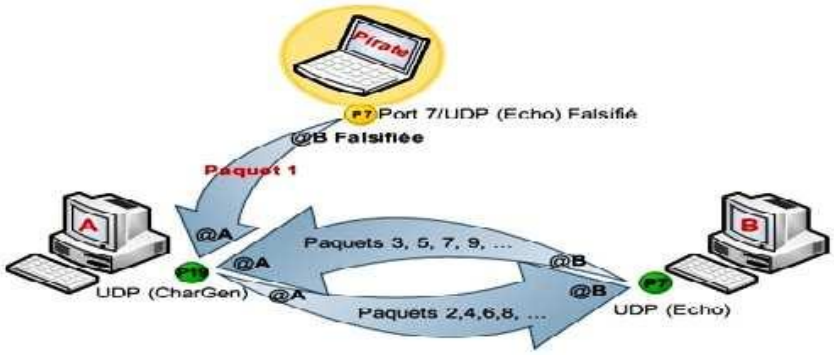


Figure I.11: UDP flooding.

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 [07].

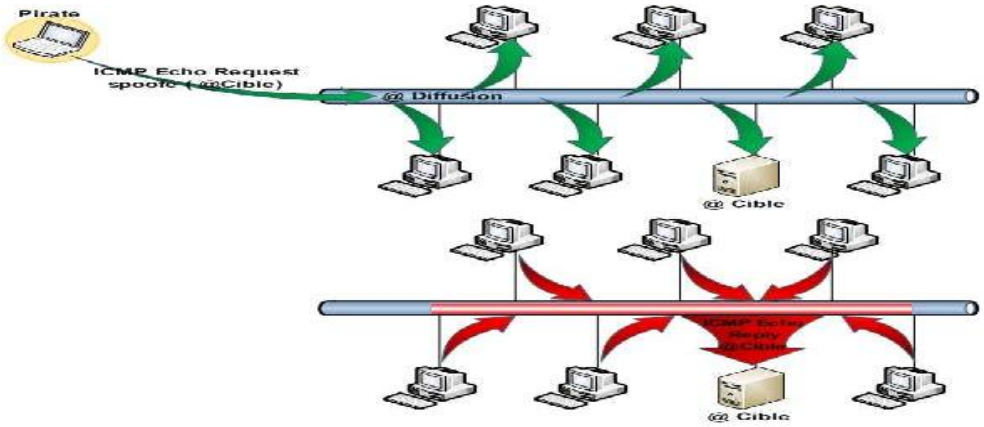


Figure I.12: Smurfling.

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...) [06].

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, voire ayant parfois un nom connu (en quelque sorte déguisé sous une fausse apparence) mais qui, une fois installé exerçait une action nocive totalement différente de sa fonction officielle. Actuellement le terme désigne à peu près tout programme qui s'installe de façon frauduleuse (souvent par le biais d'un mail ou d'une page web piégés) pour remplir une tâche hostile à l'insu de l'utilisateur. Les fonctions nocives peuvent être l'espionnage de l'ordinateur, l'envoi massif de spams, l'ouverture d'un accès pour un pirate [06].

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.

I.8.2.Les mécanismes de prévention et détections d'attaques :

La sécurité contre les attaques distantes se renforce, notamment par le biais d'équipements réseaux plus puissants, mais les attaques locales restent toutefois encore fort efficaces. Les risques de failles applicatives sont, de ce fait, très grands et peuvent s'avérer dangereux pour des applications largement répandues [09].

I.8.2.1. Les systèmes de prévention d'intrusion

Un système de prévention d'intrusion (ou IPS, Intrusion Prevention System) est un ensemble de composants logiciels et matériels dont la fonction principale est d'empêcher toute activité suspecte détectée au sein d'un système. Les IPS sont des outils aux fonctions actives, qui en plus de détecter une intrusion, tentent de la bloquer. Parmi les types d'IPS :

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

I.8.2.2. Les systèmes de détection d'intrusion

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

- **Les systèmes de détection d'intrusions :** c'est l'ensemble de composants logiciels et matériels dont la fonction principale est de détecter et analyser toute tentative d'effraction (volontaire ou non).Son fonctionnement consiste à la détection des techniques de port scanning, des tentatives de compromission de systèmes, d'activités suspectes internes ou encore des activités virales. Certains termes sont souvent utilisés quand on parle d'IDS :
- **Faux positif** : une alerte provenant d'un IDS mais qui ne correspond pas à une attaque réelle.
- **Faux négatif :** une intrusion réelle qui n'a pas été détectée par l'IDS.
- **Les systèmes de détection d'intrusions réseaux (NIDS) :** écoute tout le trafic réseau, puis l'analyse et génère des alertes si des paquets semblent dangereux. Le but des NIDS est d'analyser de manière passive les flux transitant sur le réseau et détecter les intrusions en temps réel.
- **Les systèmes de détection d'intrusions de type hôte (HIDS) :** se base sur une unique machine, n'analysant cette fois plus le trafic réseau mais l'activité se passant sur celle-ci. Il analyse en temps réel les flux relatifs à une machine ainsi que les fichiers journaux.
- **Les systèmes de détection d'intrusions hybrides :** généralement utilisés dans un environnement décentralisé, ils permettent de réunir les informations de diverses sondes placées sur le réseau. Leur appellation « hybride » provient du fait qu'ils sont capables de réunir aussi bien des informations provenant d'un système HIDS qu'un NIDS.

I.9. Les mécanismes de sécurité

I.9.1.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 [10].

I.9.1.1. Le cryptage symétrique

Le cryptage à clé privée ou symétrique est basé sur une clé (ou algorithme) partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages.

Figure I.13 : Cryptage symétrique.

I.9.1.2.Le cryptage asymétrique

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

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

- ✓ Une première clé, visible, appelé clé publique est utilisée pour chiffrer un texte en clair.
- ✓ Une deuxième clé, secrète, appelée clé privée est connue seulement par le destinataire, qui est utilisé pour déchiffrer un texte.

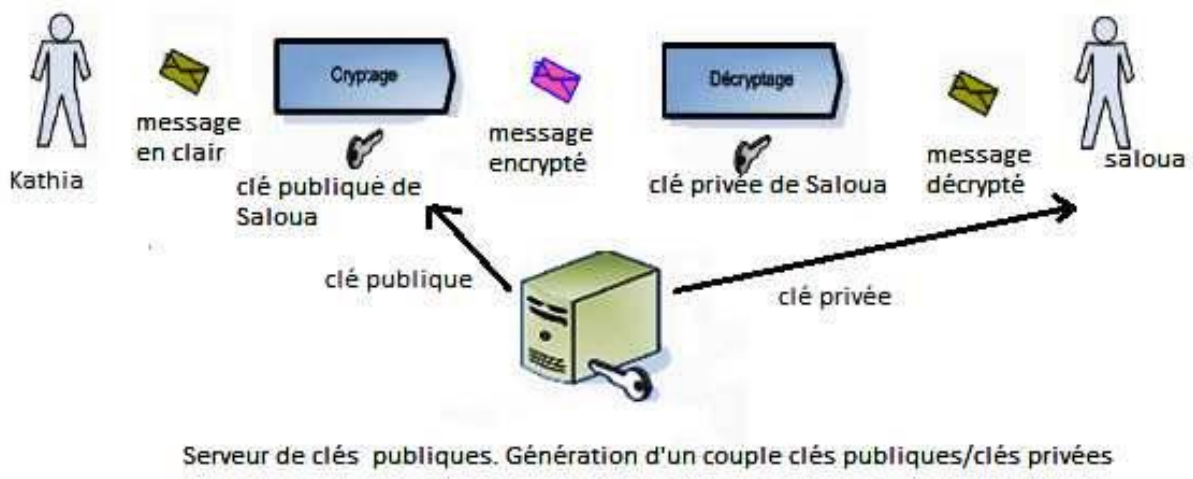


Figure I.14 : Le cryptage asymétrique.

I.9.2. la signature

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

I.9.2.1.la signature numérique

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

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

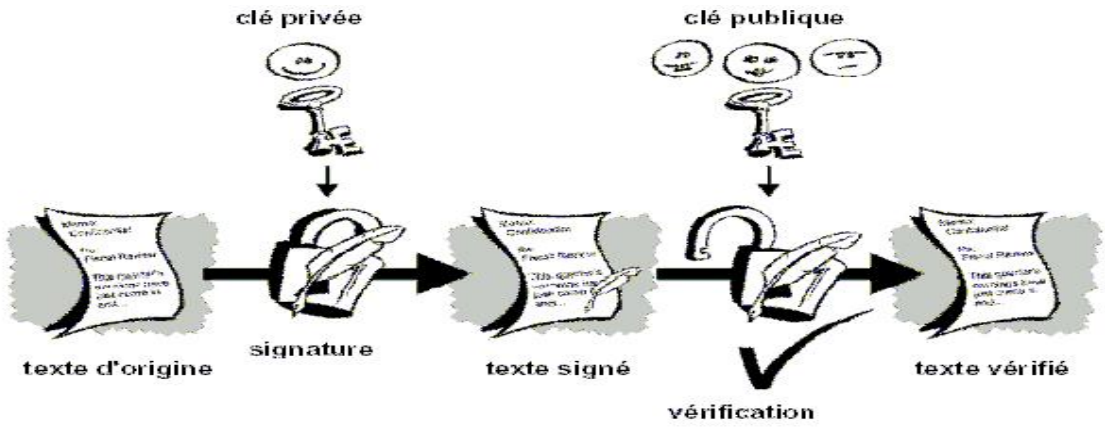


Figure I.15 : La technique de signature numérique.

I.9.2.2. les certificats

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

Si le récepteur connaît la clé publique de la CA, il peut vérifier que le certificat provient vraiment de l'autorité concernée et assurer que le certificat contient des informations viables et une clé publique valide [11].

I.9.3. Les Anti-virus

Un antivirus est un logiciel informatique destiné à identifier et à effacer des logiciels malveillants (malwares), également appelés virus, Chevaux de Troie ou vers selon les formes [08].

L'antivirus analyse les fichiers entrants (fichiers téléchargés ou courriers électroniques), la mémoire vive de l'ordinateur et les périphériques de stockage comme les disques durs, internes ou externes, les clés USB et les cartes à mémoire Flash. La détection d'un logiciel malveillant peut reposer sur trois méthodes :

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

- ✓ Reconnaissance d'un code typique d'un virus.

I.10. Les protocoles de sécurité

I.10.1.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 [08].

IPSec distingue deux niveaux de protection à travers deux protocoles :

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

I.10.2.Protocole SSL

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

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

- ✓ Le navigateur du client fait une demande de transaction sécurisée au serveur.
- ✓ Suite à la requête du client, le serveur envoie son certificat au client.
- ✓ Le serveur fournit la liste des algorithmes cryptographiques qui peuvent être utilisés pour la négociation entre le client et le serveur.
- ✓ Le client choisit l'algorithme.
- ✓ Le serveur envoie son certificat avec les clés cryptographiques correspondantes au client.
- ✓ Le navigateur vérifie que le certificat délivré est valide.
- ✓ Si la vérification est correcte alors le navigateur du client envoie au serveur une clé secrète
- ✓ chiffrée à l'aide de la clé publique du serveur qui sera donc le seul capable de déchiffrer puis D'utiliser cette clé secrète. [02].

I.10.3. Protocole HTTPs

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

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

I.10.4. 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.

I.10.5. 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 [12].

I.11.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 [13].
- ✓ **Serveur de stratégie NAP :** lorsque le serveur NPS est configuré en tant que serveur de stratégie NAP, NPS évalue les déclarations d'intégrité envoyées par les ordinateurs clients compatibles avec la protection d'accès réseau (NAP) qui tentent de se connecter au réseau en assurant l'authentification et l'autorisation des demandes de connexion. Il peut configurer des stratégies NAP et des paramètres dans le serveur NPS, y compris les programmes de validation d'intégrité système, la stratégie de contrôle d'intégrité et les groupes de serveurs de mise à jour qui permettent aux ordinateurs clients de mettre à jour leur configuration afin de se conformer à la stratégie réseau de l'organisation.
- ✓ **Proxy RADIUS :** le serveur NPS utilisé en tant que proxy RADIUS permet de configurer des stratégies de demande de connexion qui spécifient, les demandes de connexion transmises par le serveur NPS à d'autres serveurs RADIUS et les serveurs RADIUS auxquels on souhaite transmettre les demandes de connexion. Il est également possible de configurer le serveur NPS de manière à ce qu'il transmette les données de comptes à un ou plusieurs ordinateurs dans un groupe de serveurs RADIUS distants à des fins de journalisation.

I.12. 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.

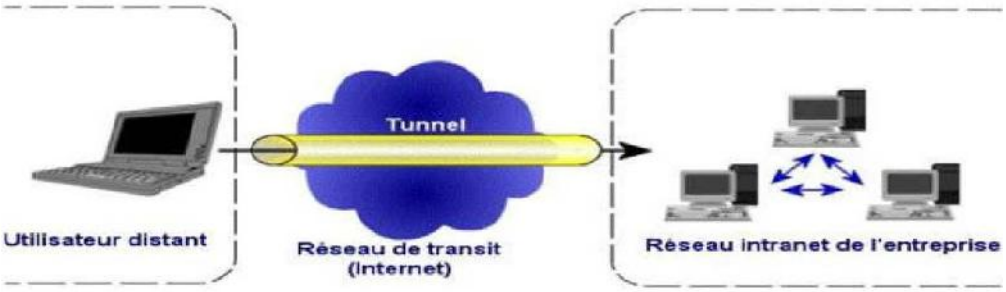


Figure I.16 : Réseau privé virtuel.

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

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets de l'entreprise, les VPN d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagé, comme Internet [06].

I.13. Les VLAN

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

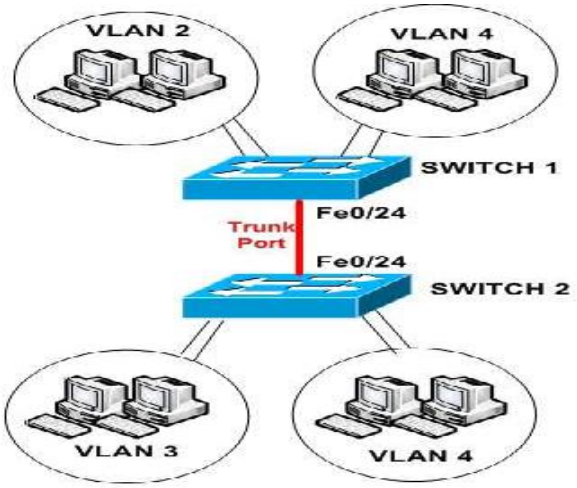


Figure I.17 : Exemple de VLAN.

I.14. Le NAT

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

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

Trois types d'adresse sont possibles :

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

I.15. Les ACL

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

Les ACL semblent avoir toujours existé sur les routeurs et rares sont les configurations où elles n'apparaissent pas. Elles servent principalement au filtrage des paquets sur les interfaces physiques.

Cependant leur mode de définition est employé pour catégoriser les réseaux en vue, entre autre, de les injecter dans un protocole de routage ou de les soumettre à une règle de qualité de service.

Il existe deux types d'ACL :

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

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

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

I.16.Discussion

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

Il devient donc urgent de mettre en place des mécanismes pour satisfaire au mieux les besoins de la sécurité. Et l'un des mécanismes incontournables, est la mise en place d'une politique de sécurité qui doit être au préalable bien réfléchit et étudiée selon l'entreprise comme le souligne Rivière, le Pdg de Lexsi (laboratoire d'expertise en sécurité informatique) : « Une politique de sécurité ne se met pas en place en fonction du nombre de postes, mais du métier de l'entreprise, de la valeur des données qui circulent et de ce que représente l'outil informatique pour sa pérennité ».

Donc une politique de sécurité comprend un ensemble de bases définissant une stratégie, des directives, des procédures, des codes de conduite, des règles organisationnelles et techniques.

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

Chapitre II : Sécurisation des interconnexions

II.1.Préambule

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

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

II.2. L'architecture réseau et sécurité

II.2.1. L'auto défense du réseau

Le concept d'auto défense du réseau (self-defending Network) est une approche de la sécurité des réseaux introduite par Cisco. Ce concept s'étend à toutes les couches du modèle OSI et offre des services sécuritaires aux équipements, utilisateurs et applications. Connecté à des systèmes de contrôle et de surveillance, il en résulte une architecture réseau sécurisée [4].

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

- ✓ Zone infrastructure qui représente le réseau interne. Ce dernier est à son tour divisé en trois zones.
  - les filiales.
  - les réseaux longue distance (WAN).
  - la zone DMZ.

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

II.2.1.1.Découpage en zones de sécurité

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

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

a. La zone infrastructure

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

Il existe trois zones de base :

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

Elle est essentiellement sécurisée. C'est la qu'intervient l'authentification obligatoire avant toute possibilité de communiquer. Elle permet aussi la protection contre les attaques par déni de service et par usurpation de session.

- ✓ **La zone d'agrégation :** elle est située immédiatement à la suite de la zone d'accès à laquelle elle peut être combinée à des fins de simplification. Ce sont donc les techniques de sécurité au niveau 3 qui prévalent comme le filtrage inter VLAN, les ACL de tous types et la protection des protocoles de routage.

- ✓ **La zone de cœur du réseau :** elle ne reçoit pas à proprement parler de fortes mesures de sécurité car, étant au centre de la zone d'infrastructure, elle bénéficie de la sécurité des zones qui l'entourent. Malgré tout, la sécurité de cette zone existe. Elle se concentre autour des principes de sécurité des

équipements, des protocoles de routage et de la sûreté de fonctionnement grâce aux multiples techniques de redondance.

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

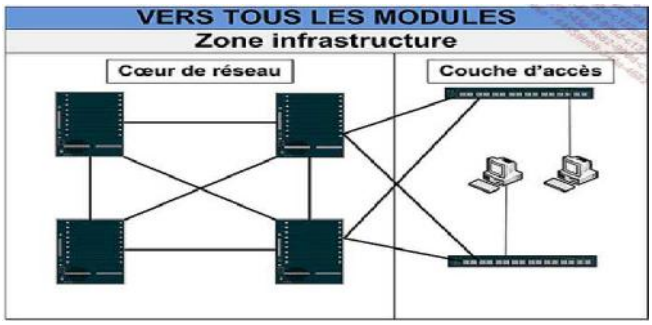


Figure II.1 : Zone infrastructure.

b. Les filiales

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

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

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

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

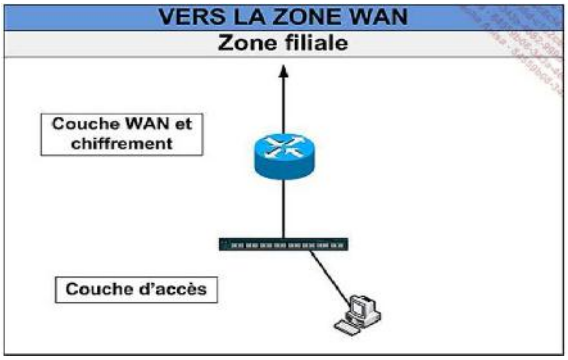


Figure II.2 : Zone filiale.

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. Il est primordial de prendre les mesures de protection visant à limiter certains types de trafic en fonction de leur débit afin de se prémunir contre les attaques par saturation.

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

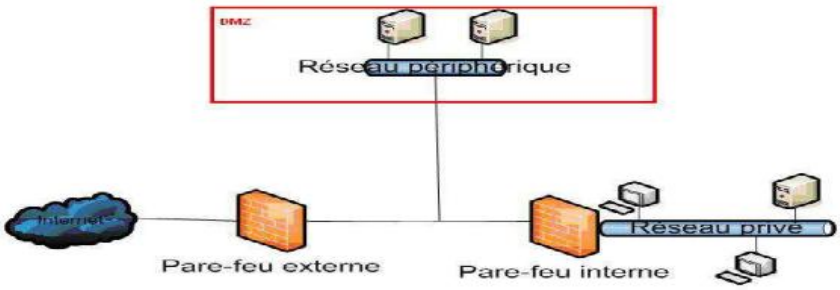


Figure II.3 : Zone WAN.

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 en prévenance de l'internet, qu'elles concernent le trafic intranet, extranet ou internet. Elle se compose d'un ou plusieurs ordinateurs formant l'infrastructure d'un système de défense du périmètre qui sécurise l'essentiel des communications [12].

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

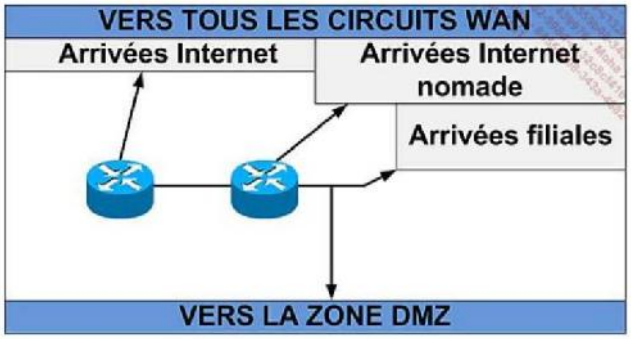


Figure II.4 : Zone DMZ.

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. Un Datacenter combine en effet toutes les composantes de la sécurité et requiert un niveau de disponibilité à la hauteur de la criticité des informations qu'il héberge. Les mesures de protections associées à ce dernier vont de la protection physique des accès, à la redondance électrique en passant par la protection contre les incendies.

La sécurité au niveau réseau du Datacenter repose principalement sur le déploiement d'ACL qui vise à garantir que le trafic entrant autorisé correspond aux services fournis par le Datacenter. Il en va de même en sens inverse en s'assurant de la correspondance du trafic sortant avec les requêtes émises de l'extérieur. Etant une zone interne, le trafic qui y transite n'est habituellement pas chiffré.

Cette disposition favorise le déploiement de dispositif d'analyse et de surveillance comme les sondes de détections d'intrusions finement ajustées sur les trafics caractéristiques de la zone. S'il est décidé de chiffrer le trafic, il conviendra de disposer de relais si la surveillance est souhaitée. La figure suivante montre un exemple d'architecture d'une zone Datacenter.

Figure II.5 : Zone Datacenter

II.2.2. Les Firewalls

II.2.2.1.Définition

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

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

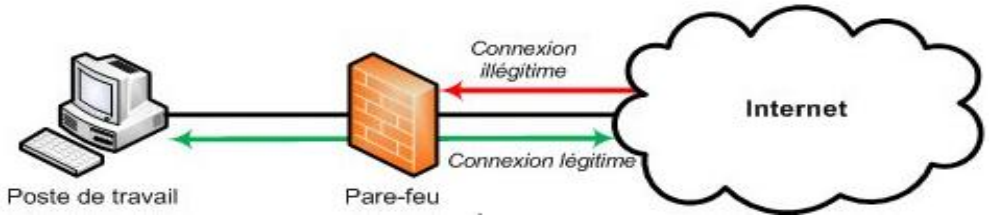


Figure II.6 : Firewall

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

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

II.2.2.2. Les fonctions d'un firewall

Un firewall dispose de plusieurs fonctions dont :

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

II.2.2.3.Les différents types de firewall

a. Les firewalls bridge

Ces derniers sont relativement répandus. Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus, d'où leur appellation de firewall. Leurs interfaces ne possèdent pas d'adresse IP, et ne font que transférer les paquets d'une interface à une autre en leur appliquant les règles prédéfinies. En effet, quand une requête ARP est émise sur le câble réseau, le firewall ne répond jamais et comme il ne fait que transmettre les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirigée directement contre le firewall, étant donné qu'aucun paquet ne sera traité par ce dernier comme étant sa propre destination. Donc, la seule façon de le contourner est de passer outre ses règles. Toute attaque devra donc faire avec ses règles, et essayer de les contourner [15].

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

Avantages

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

Inconvénients

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

b. Les firewalls matériels

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

Avantages

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

Inconvénients

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

c. Les firewalls logiciels

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

1. Les firewalls personnels

Ils ont pour but de sécuriser un ordinateur particulier, et non pas un groupe d'ordinateurs.

Souvent payants, ils peuvent être contraignants et quelque fois très peu sécurisés. En effet, ils s'orientent plus vers la simplicité d'utilisation plutôt que vers l'exhaustivité, afin de rester accessible à l'utilisateur final.

2. Les firewalls plus

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

II.2.2.4. Les type 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.
- ✓ L'adresse IP de la machine réceptrice.
- ✓ Le type de paquet (TCP, UDP...).
- ✓ Le numéro de port.

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

b. Le filtrage dynamique de paquets

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

- ✓ L'adresse IP Source/Destination.
- ✓ Le numéro de port Source/Destination.
- ✓ Le protocole de 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, il suppose une connaissance des protocoles utilisés par chaque application sur le réseau, et notamment de la manière dont elles Structure les données échangées.

Un firewall effectuant un filtrage applicatif est appelé passerelle applicative ou proxy, car il sert de relais entre deux réseaux en s'interposant et en effectuant une validation fine du contenu des paquets échangés. Le proxy représente donc un intermédiaire entre les machines du réseau interne et externe, subissant les attaques à leur place. De plus, le filtrage applicatif permet la destruction des en-têtes précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire.

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

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

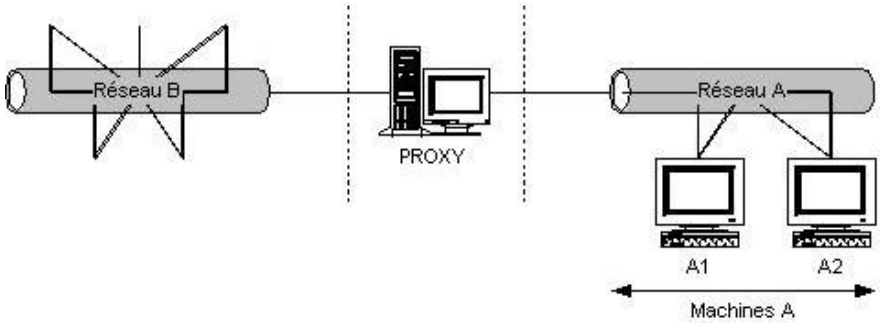


Figure II.7 : Proxy.

II.3.Discussion

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

Dans le troisième chapitre, nous présenterons et étudierons la vulnérabilité du réseau de la banque qu'on a pris comme exemple, et nous allons proposer des solutions et une nouvelle structure de l'architecture réseaux pour remédier à ces vulnérabilités.

Chapitre III : Sécurisation d'une infrastructure LAN/WA N

III.1. Préambule

Les attaques informatiques constituent aujourd'hui l'un des fléaux de notre civilisation moderne. Il ne se passe plus une semaine sans que l'on apprenne que telle entreprise ou tel institut a essuyé de lourdes pertes financières en raison d'une déficience de la sécurité de son réseau. Par conséquent, les entreprises ne peuvent plus ignorer ces risques et se croire à l'abri de telles épreuves.

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

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

III.2. Présentation de l'architecture existante

L'architecture existante dans notre cas sera le réseau d'une banque. Cette infrastructure est constituée de deux sites, qui contiennent une architecture identique comme il est illustré dans la figure III.1 (les seules différences résident dans le nombre de serveur et la connexion internet).

Notre étude va portée sur l'identification des différentes failles du site 1 et la faille qui réside dans la zone SI du réseau externe du site 2.

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

Le **site 1** est constitué de :

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

- 2 postes de stations d'administration.
- 1 poste pour le superviseur réseau.
- 2 postes pour le service réseau.

Le **site 2** est constitué de :

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

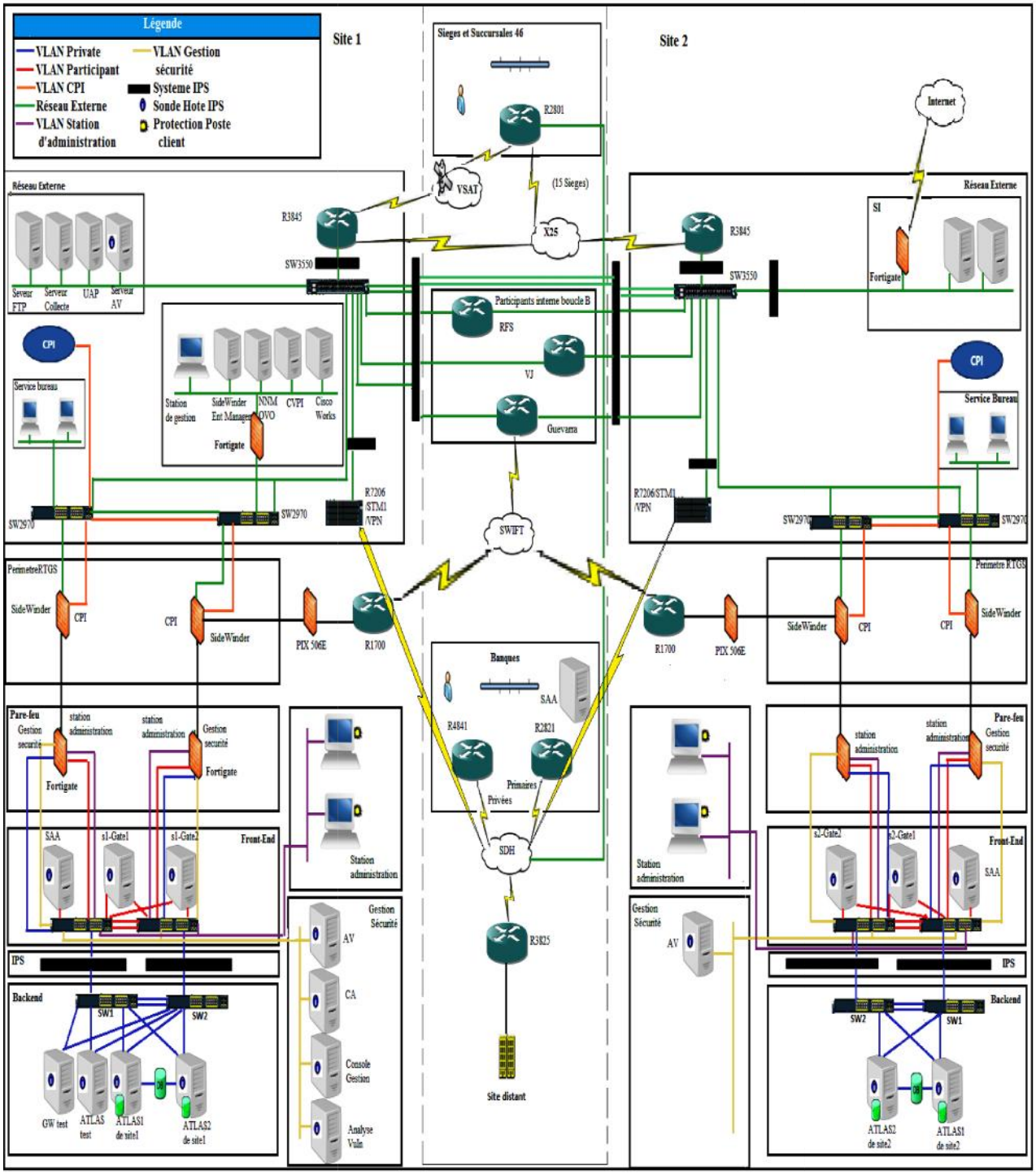


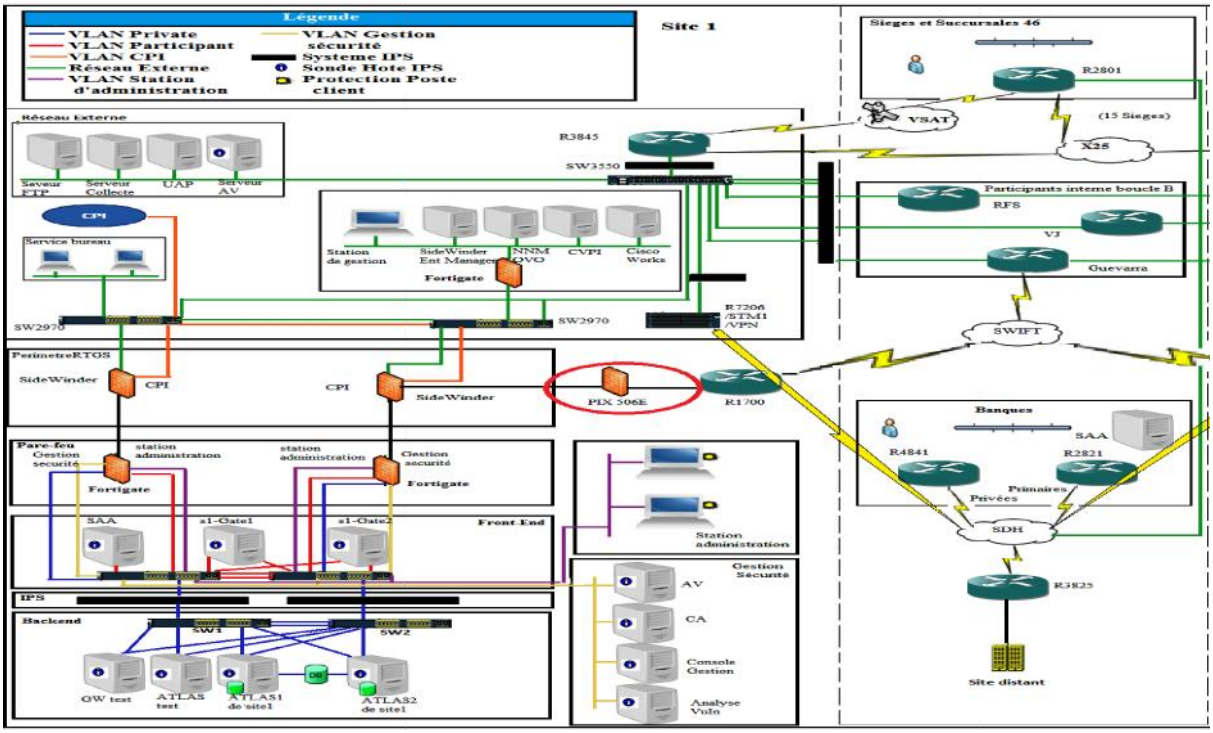
Figure III.1: L'architecture existante de la banque.

III.2.1. Les vulnérabilités de l'architecture réseau :

1. Le firewall PIX506^{E}

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

Comme illustré dans la figure III.2 le firewall Cisco PIX506^{E} qui lie le réseau Swift et le périmètre RTGS même si cette liaison est secondaire, (la liaison primaire est effectuée à travers une ligne spécialisée au niveau du site de Guevarra), le PIX constitue un point critique qui ne peut être négligé.



FigureIII.2 :La vulnérabilité de PIX506E.

2. L'utilisation de type identique de firewalls

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

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

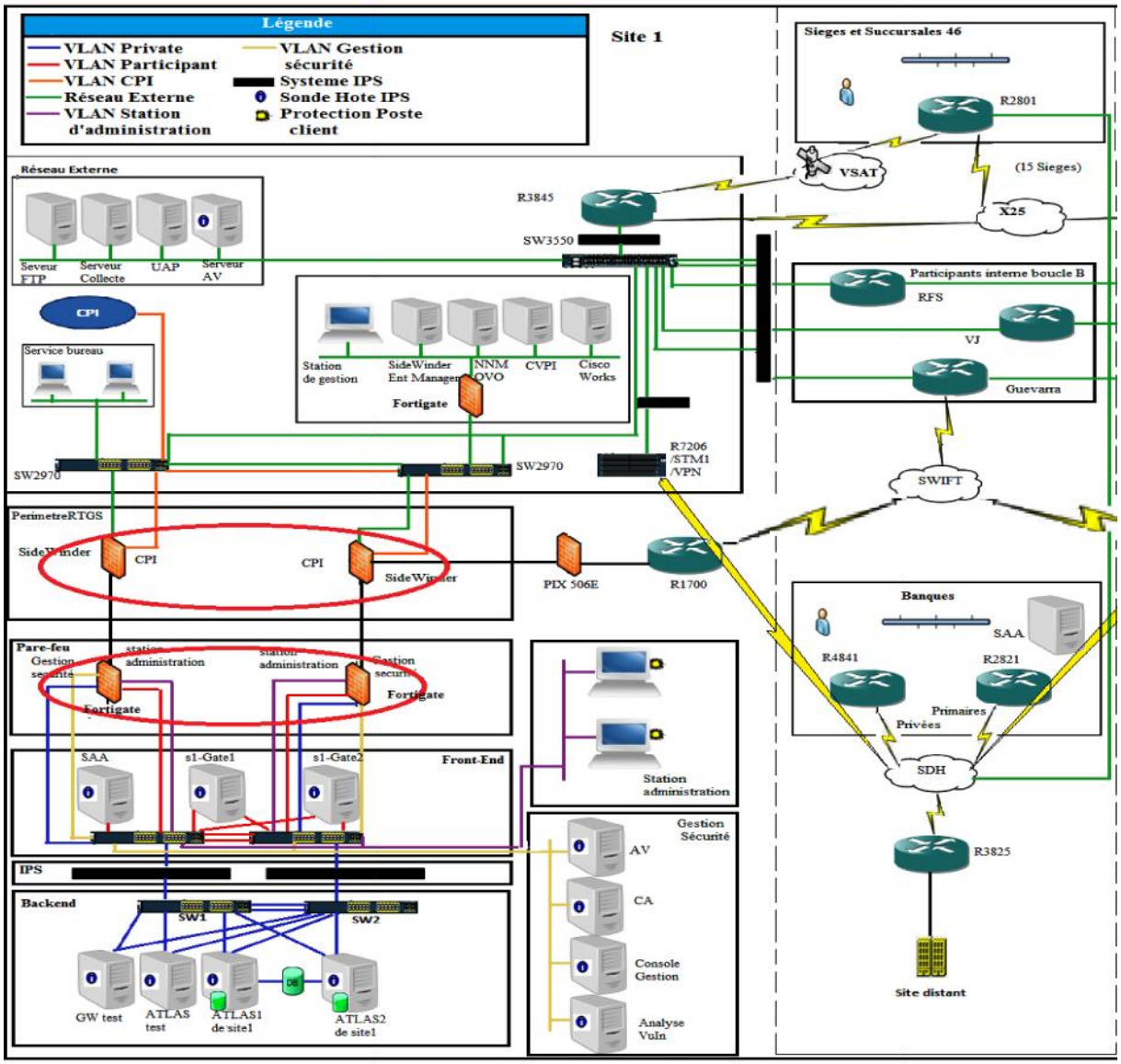


Figure III.3: La vulnérabilité de type identique de firewalls.

3. Le system de prévention d'intrusion IPS

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

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

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

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

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

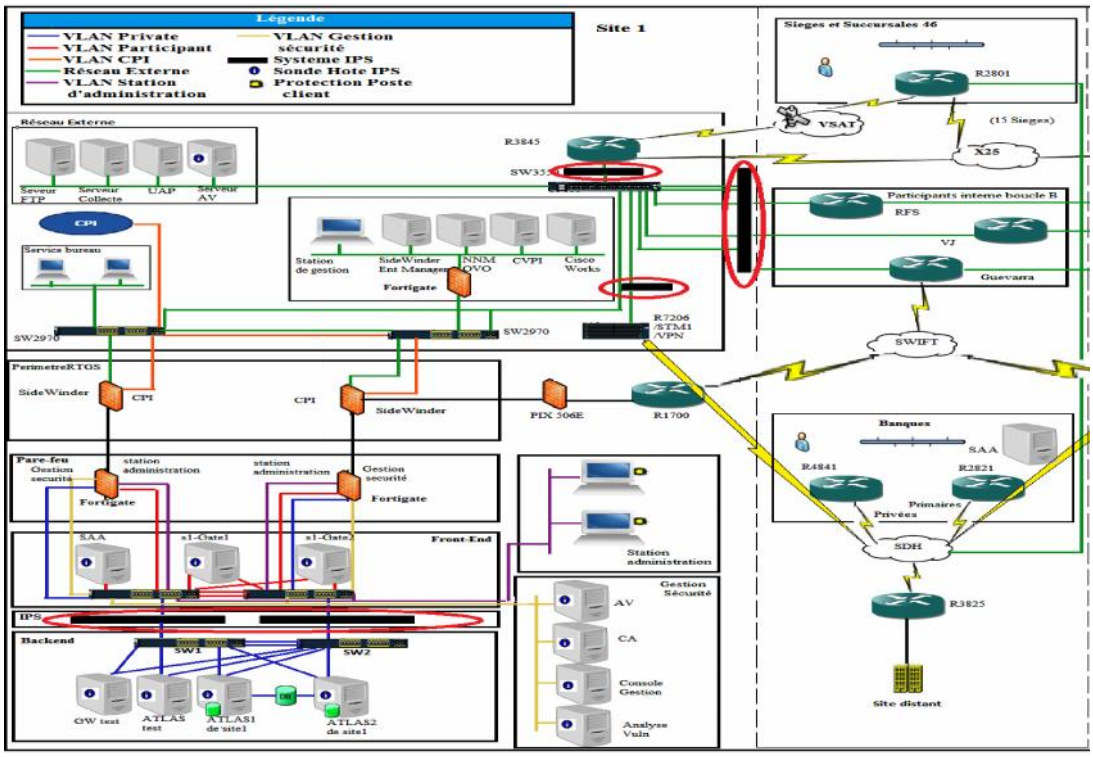


Figure III.4 : La vulnérabilité IPS.

4. Le commutateur SW3550

Comme illustré dans la figure III.5, le commutateur SW3550 représente un point de défaillance, vu que toute l'infrastructure RTGS est connectée directement ou indirectement à ce seul commutateur. La panne de ce commutateur causera la déconnexion de tous les utilisateurs sauf ceux connectés à travers le réseau SWIFT puisqu'il y a une liaison secondaire à travers le PIX 506^{E}. Sans oublier aussi, que 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.

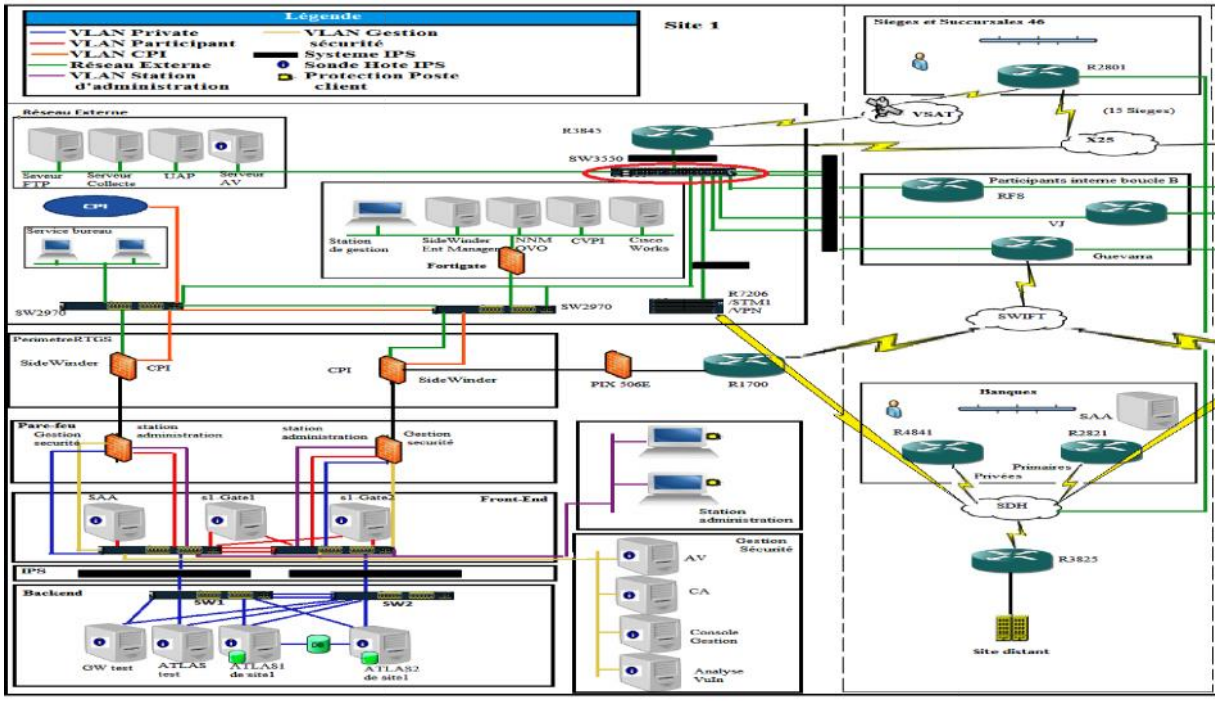


Figure III.5 : La vulnérabilité du commutateur SW3550.

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

Dans le réseau de télécommunication de la banque, il existe plusieurs points d'entrée du réseau avec les entités externes, comme le montre la figure III.6:

- ✓ Le pare-feu Cisco PIX 506^{E} qui connecte les participants externes directement à la zone Périmètre RTGS 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.
- ✓ La connexion internet, qui se trouve au niveau du réseau SI dans le site 2.

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

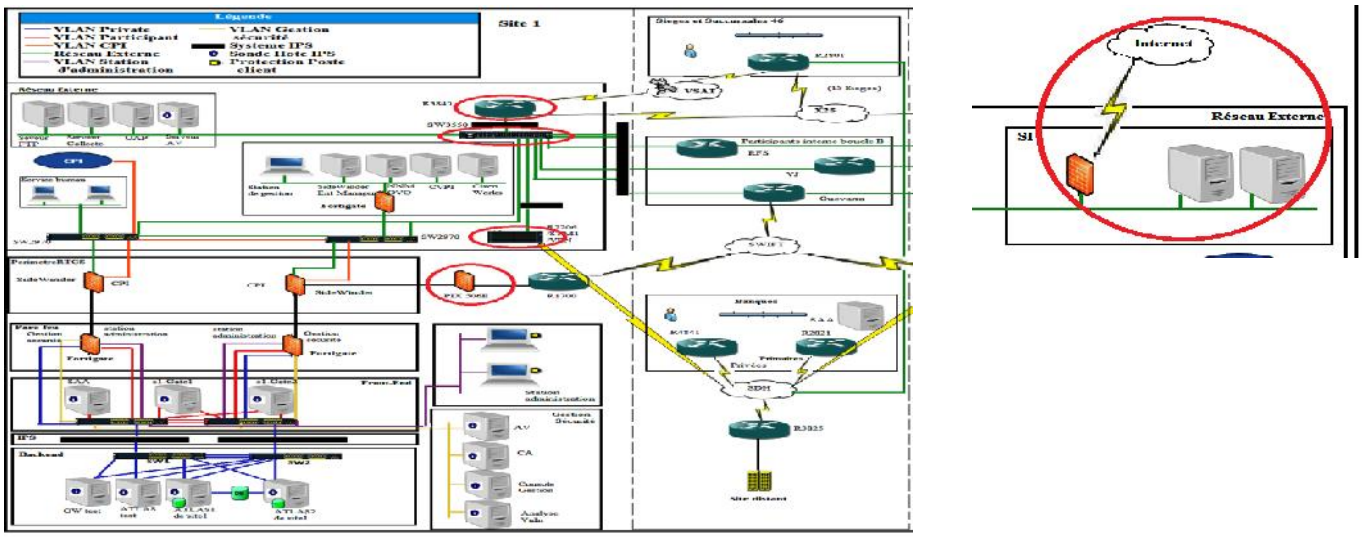


Figure III.6: Les multiple points d'entrée du réseau.

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

1. Utilisation de protocoles à texte clair (ClearText)

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

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

La deuxième version SNMPV2 a introduit quelques nouveaux types, mais sa nouveauté majeure est l'opération GETBULK, qui permet à une plateforme 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 des diverses options qui leur permettront de causer des dommages et d'interrompre les activités métier. Cette vulnérabilité existe à cause du manque de lignes directrices de sécurité de mot de passe, et la mauvaise appréciation des conséquences de l'utilisation de mots de passe faibles.

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

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

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

2. Trafic sortant non restreint

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

3. Compte partagé pour la gestion du firewall

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

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

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

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

2. 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 rendla 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.

3. 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.

4. 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.

III.3. Les solutions proposées :

III.3.1. L'architecture proposée

Après avoir identifié les différentes failles et vulnérabilités de l'infrastructure de la banque, nous avons proposé une nouvelle architecture du réseau qui contient les différentes solutions proposées comme le montre la figure III.7.

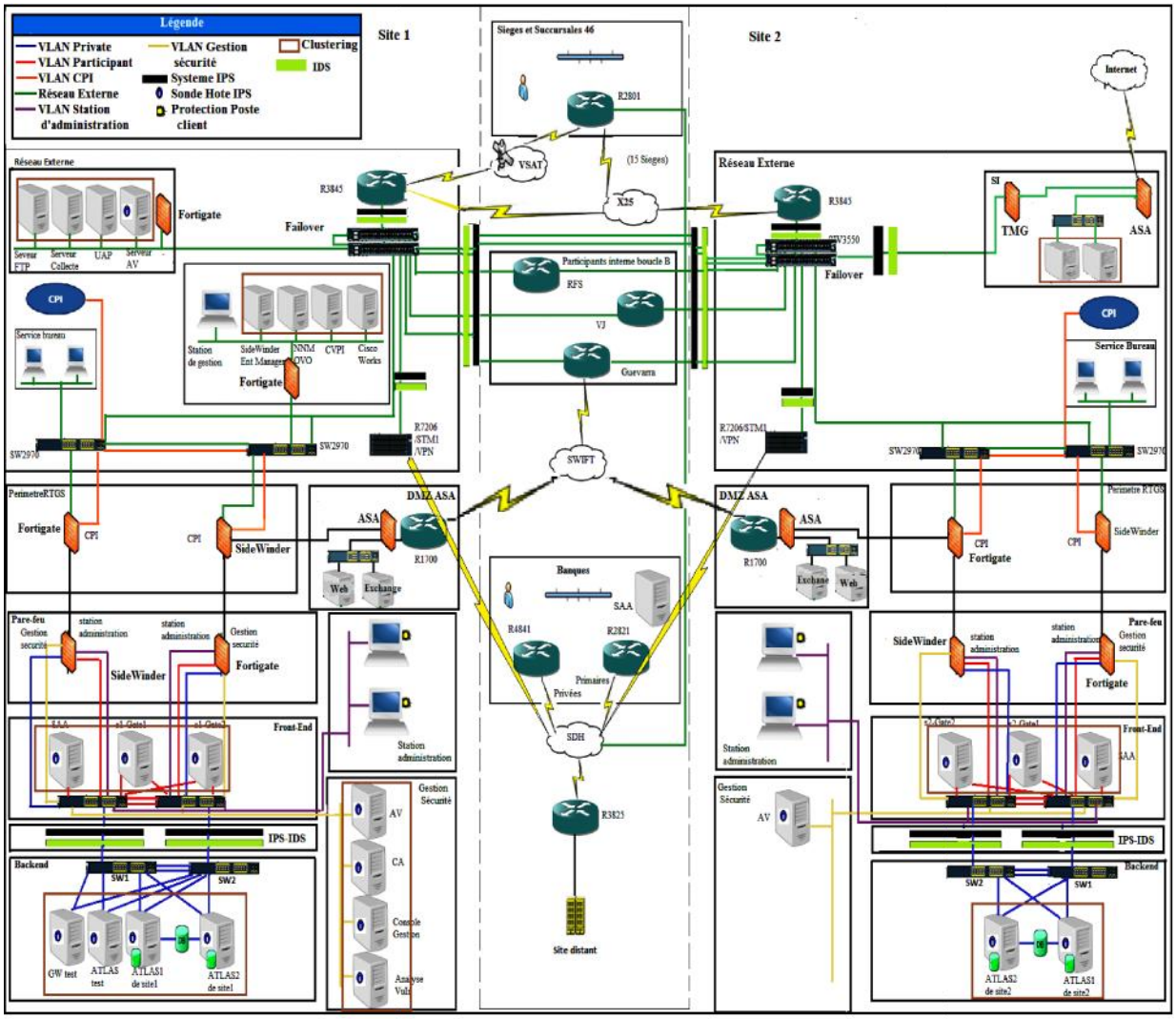


Figure III.7 :L'architecture proposée.

III.3.2. Les changements de l'architecture réseau

1. Remplacer le PIX par 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 SeriesConcentrator, le Cisco IPS 4000 SeriesSensor 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 des IPS assez limitées.

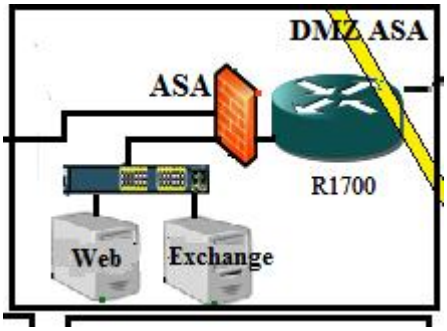


Figure III.8 : Le remplacement de PIX par ASA.

2. Repositionnement des firewalls de type identique

Pour remédier aux vulnérabilités de l'utilisation de firewalls de type identique et mieux exploiter les fonctionnalités des firewalls disponibles, nous proposons de permuter les firewalls comme la montre la figure III.9 pour une meilleure sécurité.

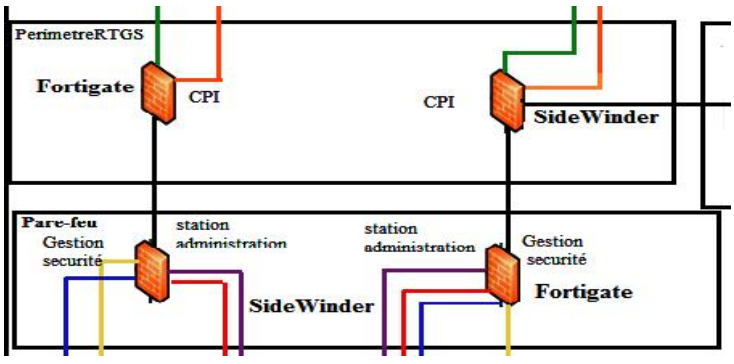


Figure III.9 : La permutation des firewalls

3. L'ajout des IDS

Malgré les inconvénients des IPS, on peut retenir que ces derniers sont actifs, pour cette raison nous proposons d'utiliser en plus des IPS existants des IDS qui permettront d'accentuer la sécurité des IPS à tous les niveaux, que ce soit système ou réseau. (L'emplacement des IPS et IDS est montré dans la figure III.10).

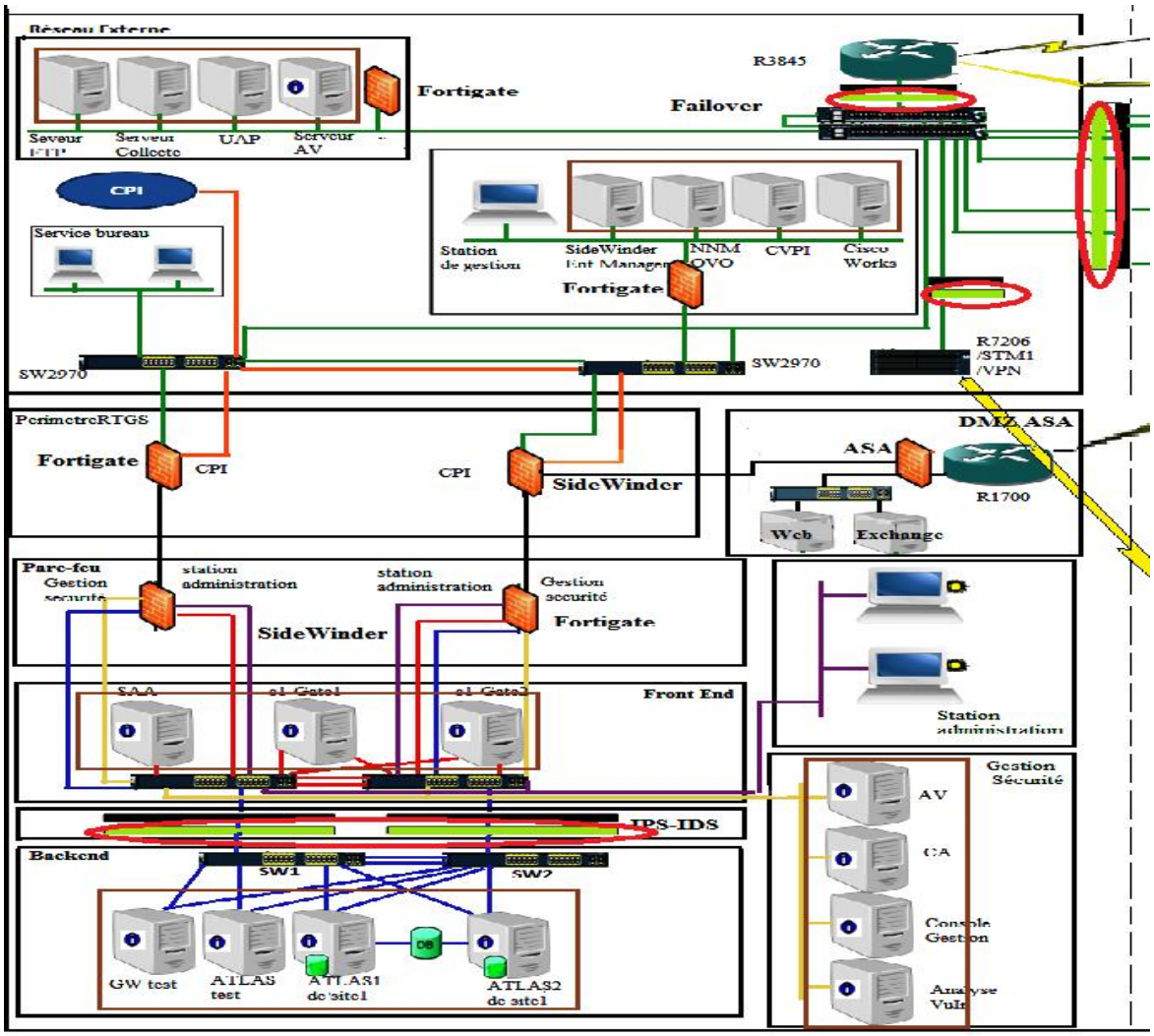


Figure III.10:L'ajout des IDS.

4. L'implémentation du Failover

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

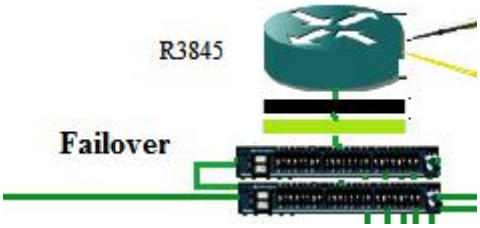


Figure III.11 :L'implémentation de failover**.**

5. La sécurisation des points d'entrées réseau

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

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

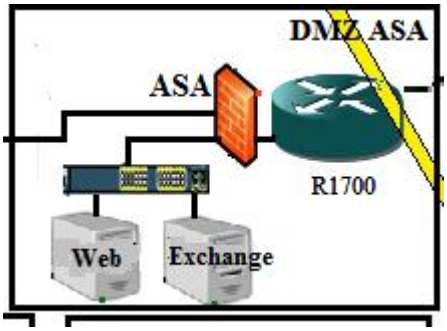


Figure III.12 : La création de la DMZ ASA.

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

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

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

- ✓ Pour le deuxième point d'entrée que constitue le routeur Cisco 3845, nous avons proposé l'ajout de l'IDS comme vu plus haut.
- ✓ Pour le quatrième point d'entrée, la connexion internet qui se trouve au niveau du réseau SI dans le site 2.Nous proposons de créer une DMZ qui contiendra les serveurs existants dans SI raccordés par un commutateur à un firewall ASA et un firewall TMG. L'ASA gère le trafic entrant et sortant de la banque et la protège de l'extérieur. La TMG définit et contrôle tout le trafic interne. Ces derniers comme nous l'avions dit, offrent une meilleure protection pour l'internet. Quant au firewall Fortigate

existant, nous proposons au lieu de le supprimer du réseau, de le placer au niveau du SI du site 1, afin protéger les serveurs de cette zone.

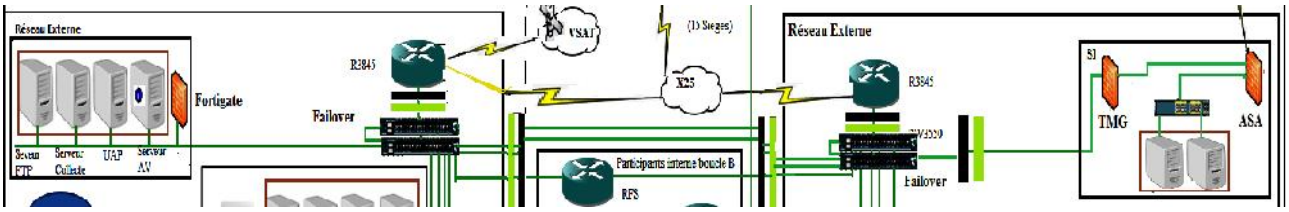


Figure III.13 : La création de la DMZ SI.

III.3.3. 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 l'internet, le moyen trouvé pour sécuriser les transactions de la banque est le cryptage. Dans le cas où un pirate récupère le mot de passe crypté il ne peut rien faire avec. La solution consiste à utiliser pour gérer le réseau les protocoles chiffrés, HTTPS, SSL et IPSec.

- ✓ Utiliser le protocole HTTPs pour sécuriser des transactions HTTP adopté pour permettre une navigation sécurisée sur le web.
- ✓ Afin d'assurer la sécurité des échanges indépendamment du protocole applicatif utilisé. Nous proposons l'utilisation du protocole SSL pour chiffrer les communications entre les différents points entités à l'intérieur et l'extérieur de la banque et protéger les données.
- ✓ Pour vérifier l'intégrité des ordinateurs avant de leurs accorder un accès au réseau interne de la banque, nous proposons d'implémenter la protection d'accès réseau (Network Access Protection), cette dernière combinée avec le serveur DHCP (Dynamique Host Configuration Protocol) attribue dynamiquement les adresses IP aux clients internes conformes. Parmi les règles de conformité qui peuvent être spécifiées par l'utilisateur nous trouvons, l'activation du pare-feu, l'installation d'un anti-virus et les mises à jour. Si le client n'est pas conforme il ne se verra pas attribuer une adresse IP interne jusqu'à ce qu'il soit conforme. Et s'il contient une adresse IP et qu'entre temps il n'est plus conforme il se verra retirer l'adresse IP interne au prochain bail. Donc pour des questions de sécurité le bail doit être au maximum valable 8 jours.

2 .Utilisation de mots de passe fort

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

- ✓ Avant toute chose souligner l'importance de changer les mots de passe par défaut.

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

III.3.4. 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.

III.3.5. 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 2008, prend en charge toutes les exigences citées plus haut pour mettre en place une bonne politique de sécurité. Il permet aussi de spécifier la durée de validité de mot de passe, s'il doit être changé à la première utilisation ou non.

2. L'utilisation anti-virus Kaspersky

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

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

Ces fonctionnalités facilitent la mise en place d'un responsable de sécurité chargé d'administrer, surveiller, déployer et mettre à jour régulièrement Kaspersky Admin Kit [16].

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.

III.4. Discussion

La complexité des attaques, la facilité de se renseigner sur les logiciels et les moyens d'intrusions via le net, font que n'importe qu'elle architecture aussi sécurisée soit-elle peut être confrontée à d'innombrables défaillances. C'est le cas de notre architecture, qui doit être protégée des attaques informatiques pouvant nuire à son bon fonctionnement. Mais comme nous l'avons vu, en nous basant uniquement sur les documents fournis sur l'infrastructure de la banque, il existe diverses vulnérabilités que nous avons découvertes et expliquées dans ce chapitre. Nous tenons à souligner que cette liste de failles n'est pas exhaustive car nous nous sommes limitées aux données qui ont été mises à notre disposition.

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

Dans le chapitre suivant, nous allons mettre en pratique quelques solutions mentionnées dans celui-ci.

Chapitre IV : Application

IV.1.Préambule

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

Dans cette application nous essaierons de minimiser au maximum les risques d'attaques et les points vulnérables de la banque en accordant aux différents administrateurs la responsabilité de sensibiliser les membres de l'entreprise au secret professionnel.

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

IV.2. Présentation des outils utilisés

IV.2.1. Le simulateur graphique de réseaux

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

Figure IV.1: GNS3.

IV.2.2. La VMware Workstation 10

Pour l'émulation de notre réseau, nous avons choisi d'utiliser la VMware Workstation 10. 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.

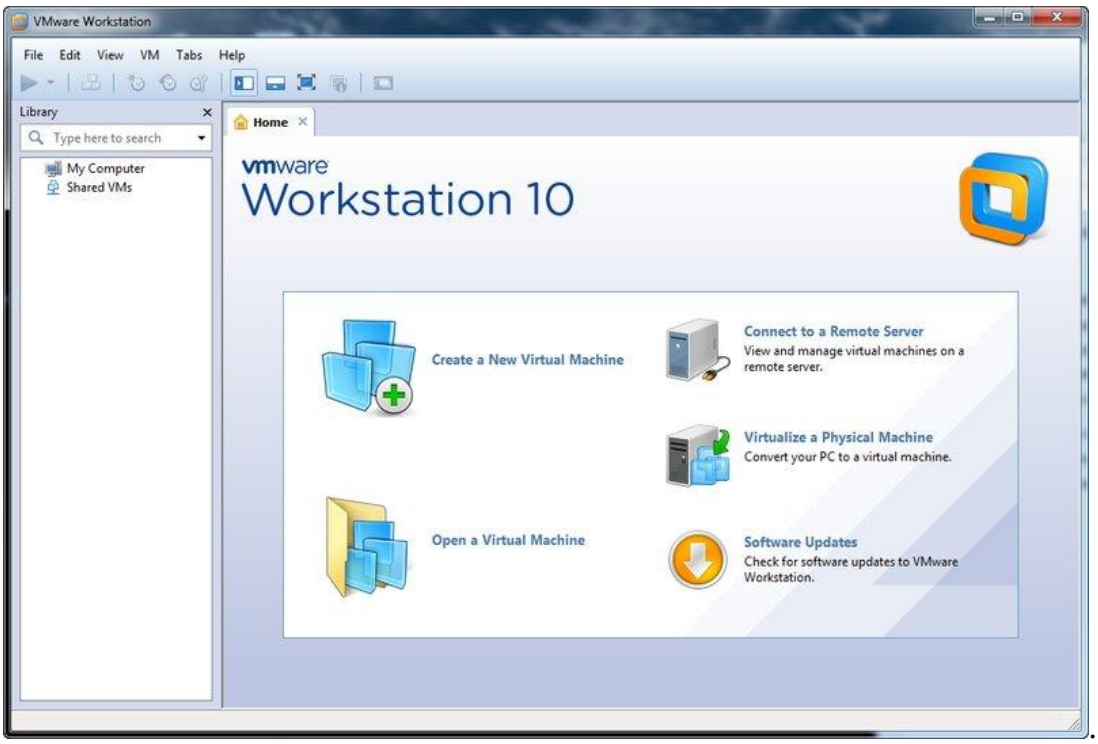


Figure IV.2: VMware Workstation 10.

IV.2.3. Microsoft Windows Server 2012

Microsoft Windows Server 2012 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 : Windows Server 2012.

IV.2.4. Active Directory

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

Figure IV.4: Active Directory.

IV.2.5. Les caractéristiques du PC utilisé

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

- ✓ Processeur I5 x64 bits
- ✓ RAM 5GO

- ✓ Disque dur 560 GO
- ✓ Système Windows 7 professionnel x64 bits Prise en charge de la virtualisation.

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

Vu qu'il est impossible d'implémenter toute l'infrastructure réseau de la banque avec les solutions réseaux et systèmes proposées. Nous avons simplifié l'architecture de sorte à permettre la mise en place de notre politique de sécurité. L'architecture simplifié comporte deux zone (zone station de travail et zone DMZ), comme le montre La figure IV.5.

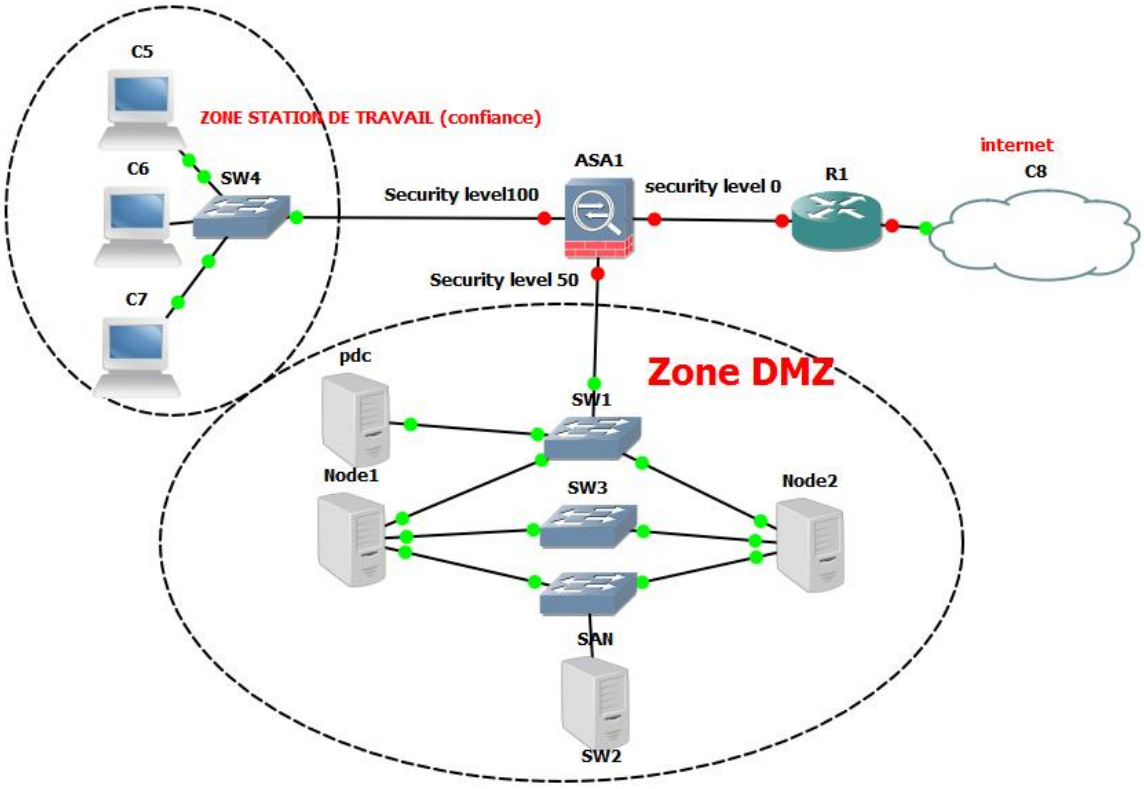


Figure IV.5 : L'infrastructure réseau mise en place sous GNS3.

Nous allons sécuriser les deux zones grâce à un firewall ASA, qui va sécuriser le trafic entrant et sortant.

Dans la zone DMZ nous implémenterons le faillover pour la disponibilité des données.

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

Etape I : la préparation des machines

Nous avons préparé les machines suivantes :

- Un contrôleur de domaine principal.
- Un contrôleur de domaine secondaire.
- Une machine membre client interne qui fait office de machine test.
- Deux machines membres pour l'implémentation de la solution failover.
- Une machine membre pour le SAN (storage area network).
- 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), banque.com. Sur la deuxième machine nous avons effectué le déploiement du contrôleur de domaine pour avoir un contrôleur de domaine secondaire (ADC). Ce dernier sert à la réplication du PDC.

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

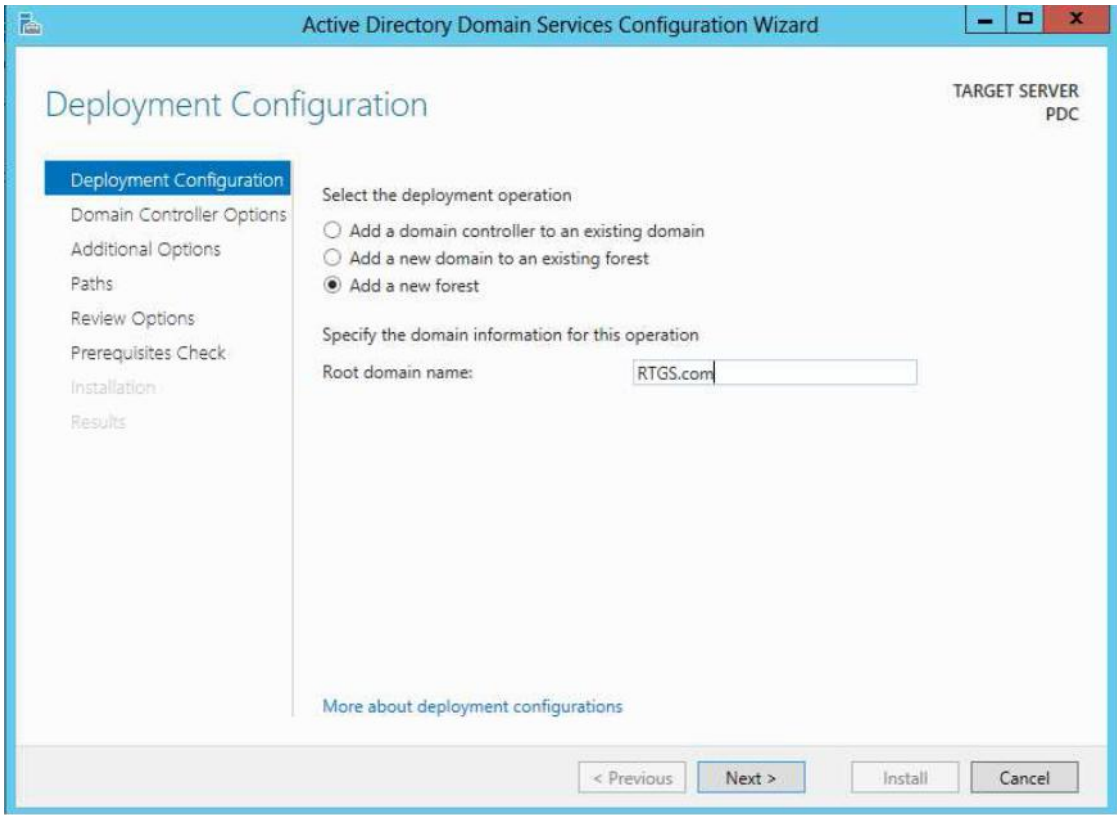


Figure IV.6 : La création du domaine principal.

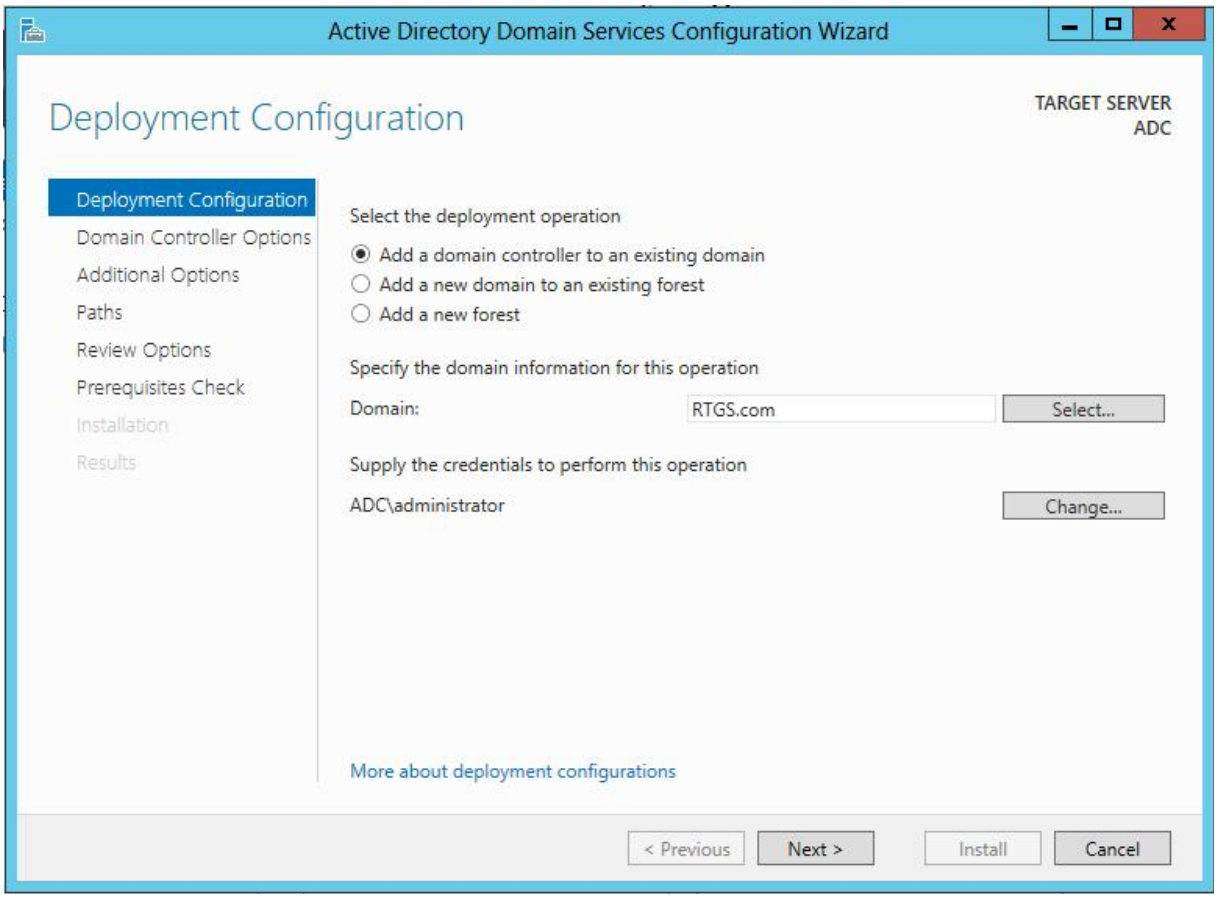


Figure IV.7 : L'ajout du domaine secondaire.

2. L'ajout d'un serveur ou machine membre

Un serveur ou une machine membre ne sont pas des contrôleurs de domaine mais seulement des membres du domaine. Pour ajouter un membre, il faut accéder aux propriétés systèmes et modifier le domaine de l'ordinateur comme le montre la figure IV.8.

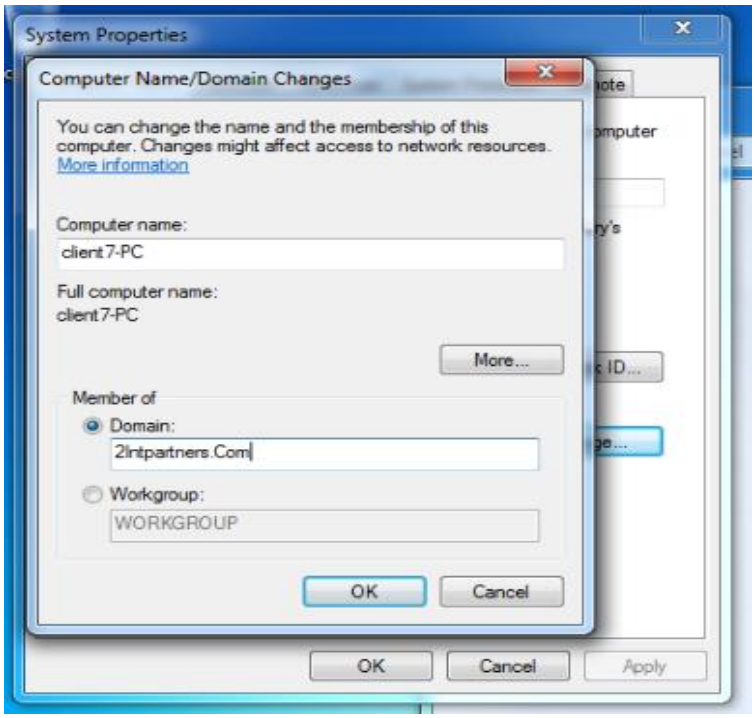


Figure IV.8 : Ajout de la machine client au domaine banque.com.

Etape II : Installation et configuration du stockage

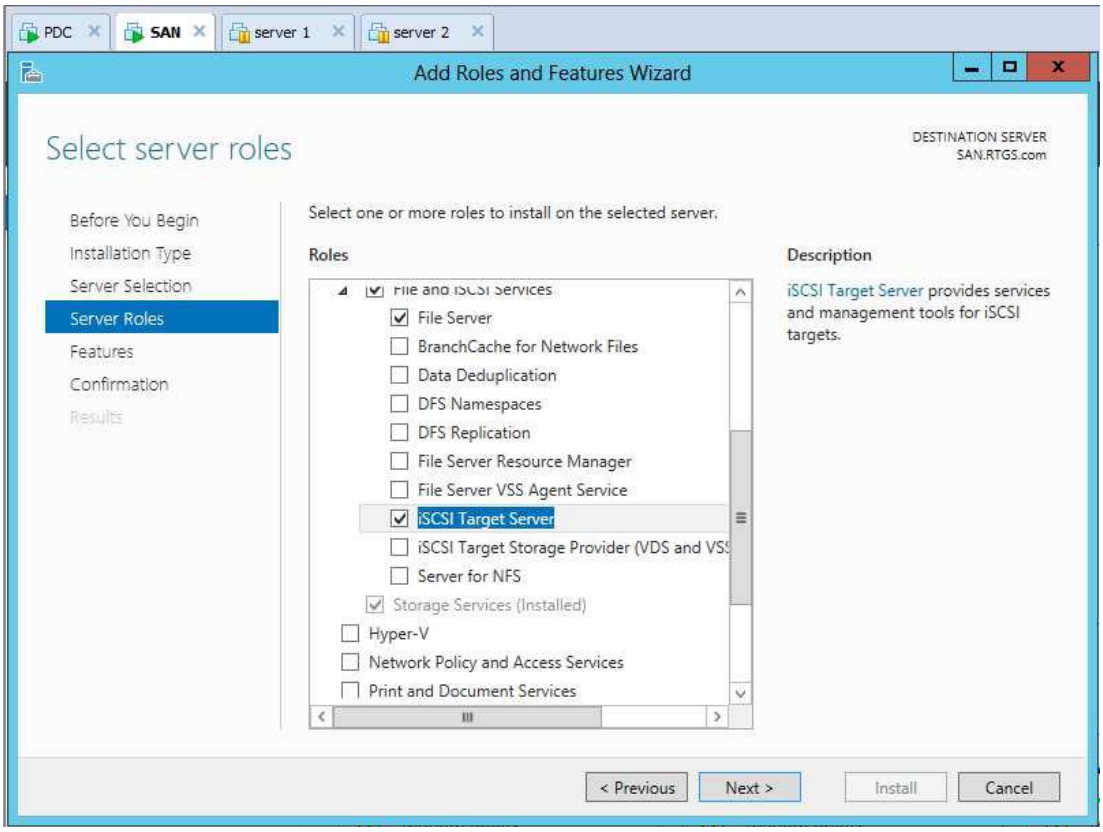
1. **Installation de SAN**

Dans une 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).

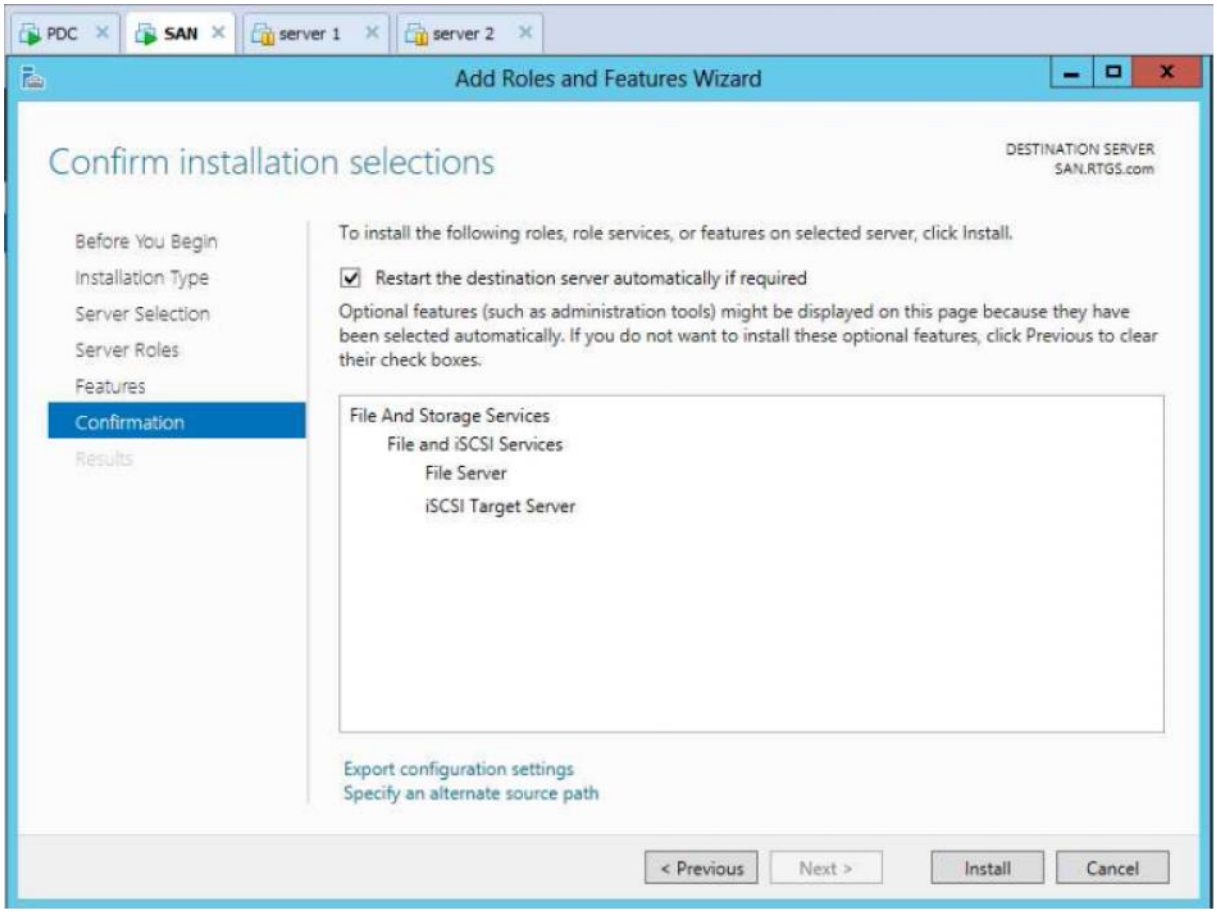
2. Les réseaux iSCSI SAN

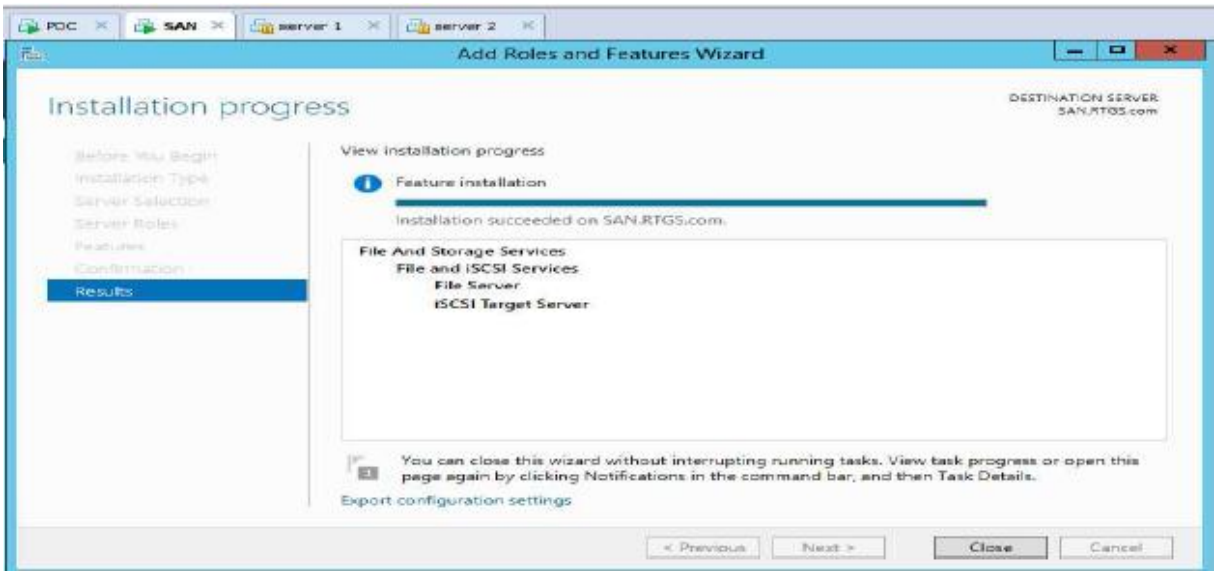
iSCSI (Internet SCSI) est un standard industriel développé pour permettre une transmission de commande via un réseau Ethernet en utilisant le protocole TCP/IP. Les serveurs communiquent avec les périphériques iSCSI grâce à un agent logiciel installé localement appelé initiateur iSCSI. Ce dernier exécute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

Dans cette section nous présenterons les différentes étapes d'installation du service iSCSI SAN sur un serveur membre de RTGS.com que nous avons nommé SAN



On clique sur Install pour installer le rôle iSCSI :





Une fois l'ajout de rôle de iSCSI, nous allons à Server Manager > Fichier et services de stockage > iSCSI. On clique sur Créer un disque virtuel iSCSI, démarrer l'Assistant disque virtuel iSCSI Nouvelle.

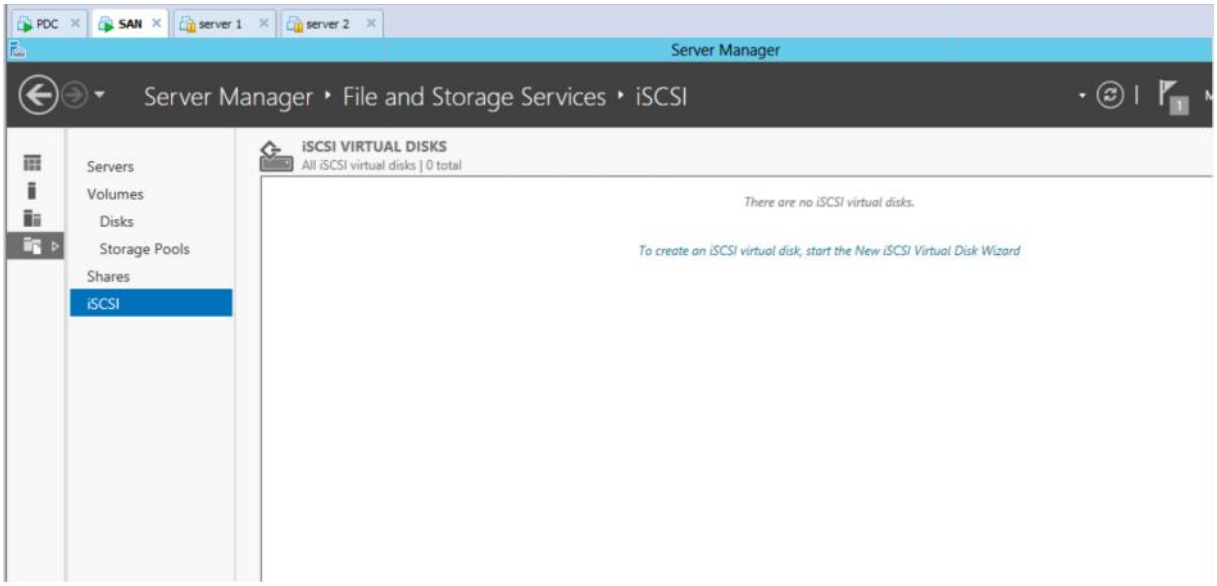
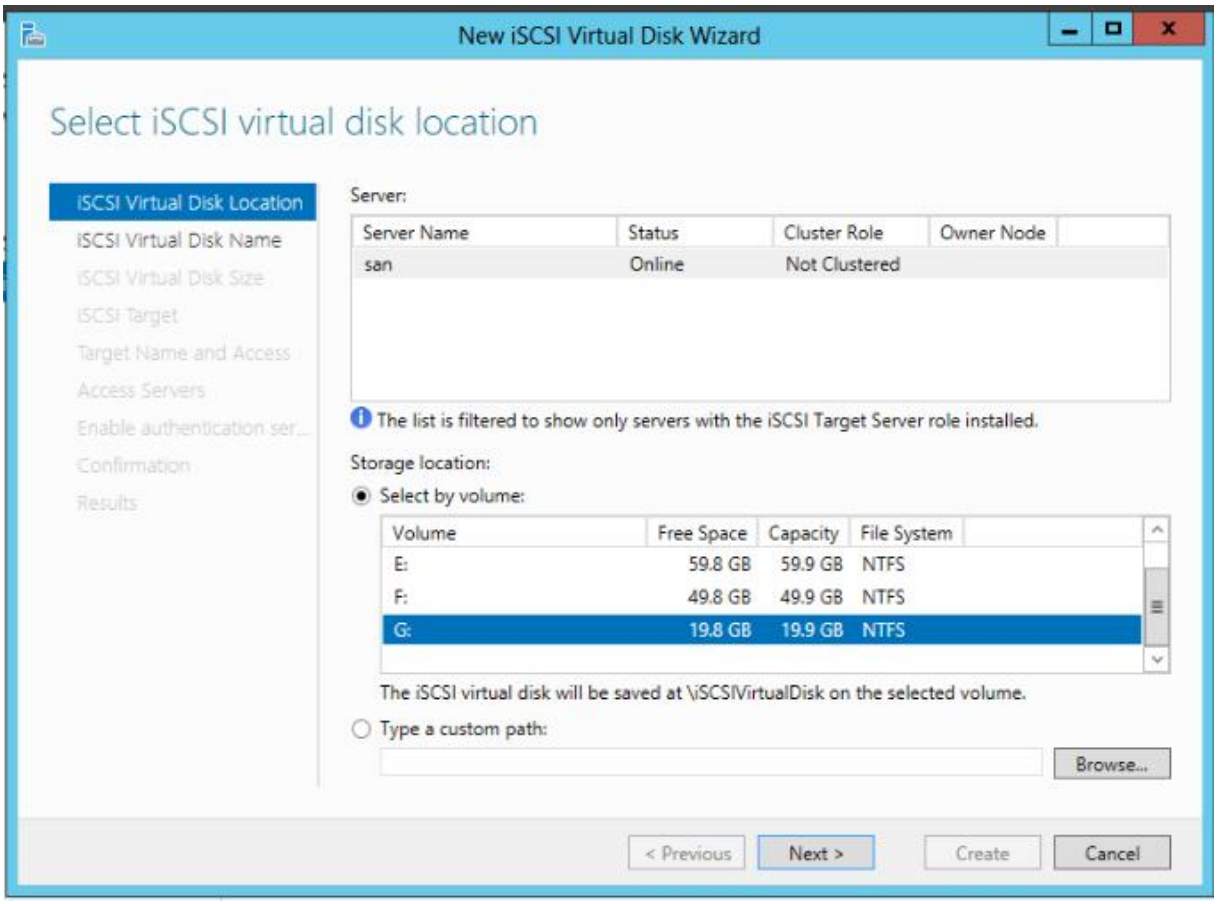
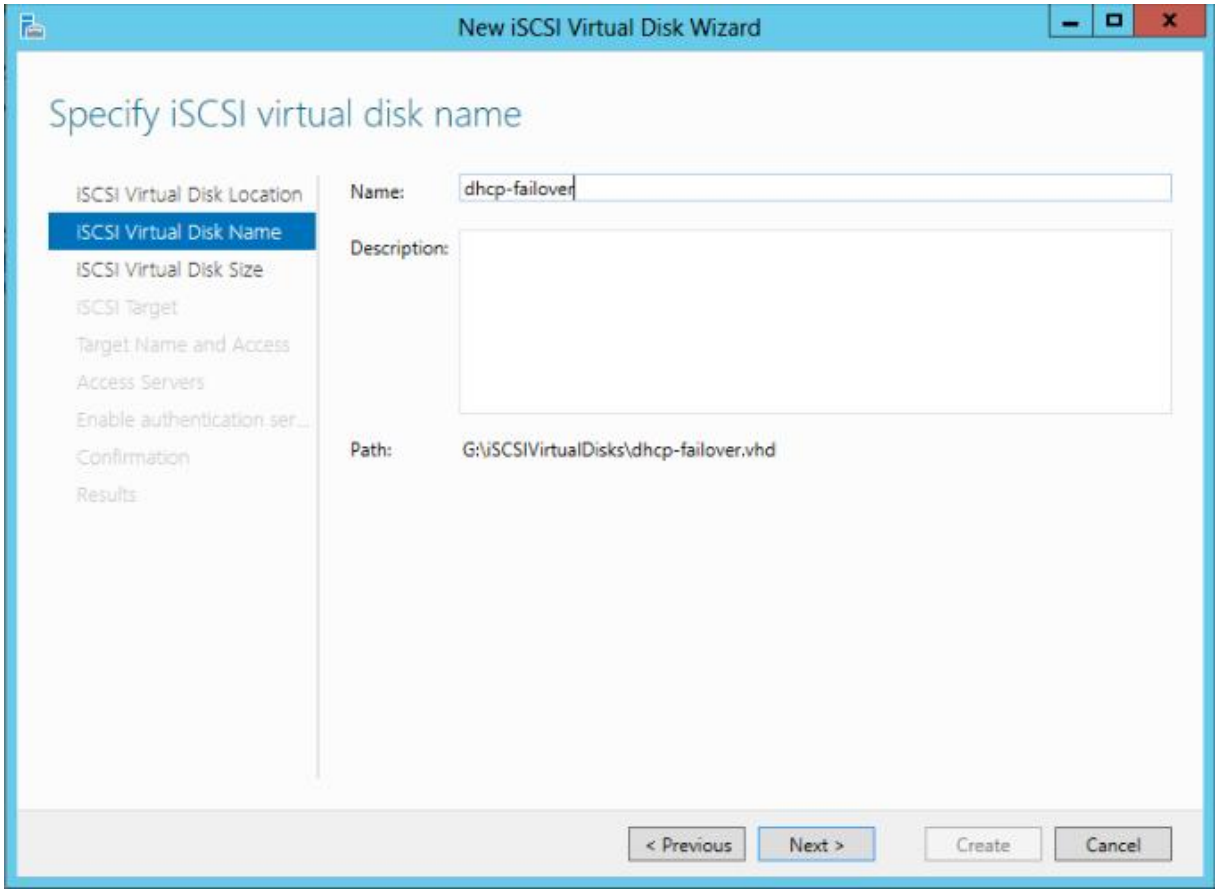


Figure IV.9 : Création d'un disque virtuel iSCSI.

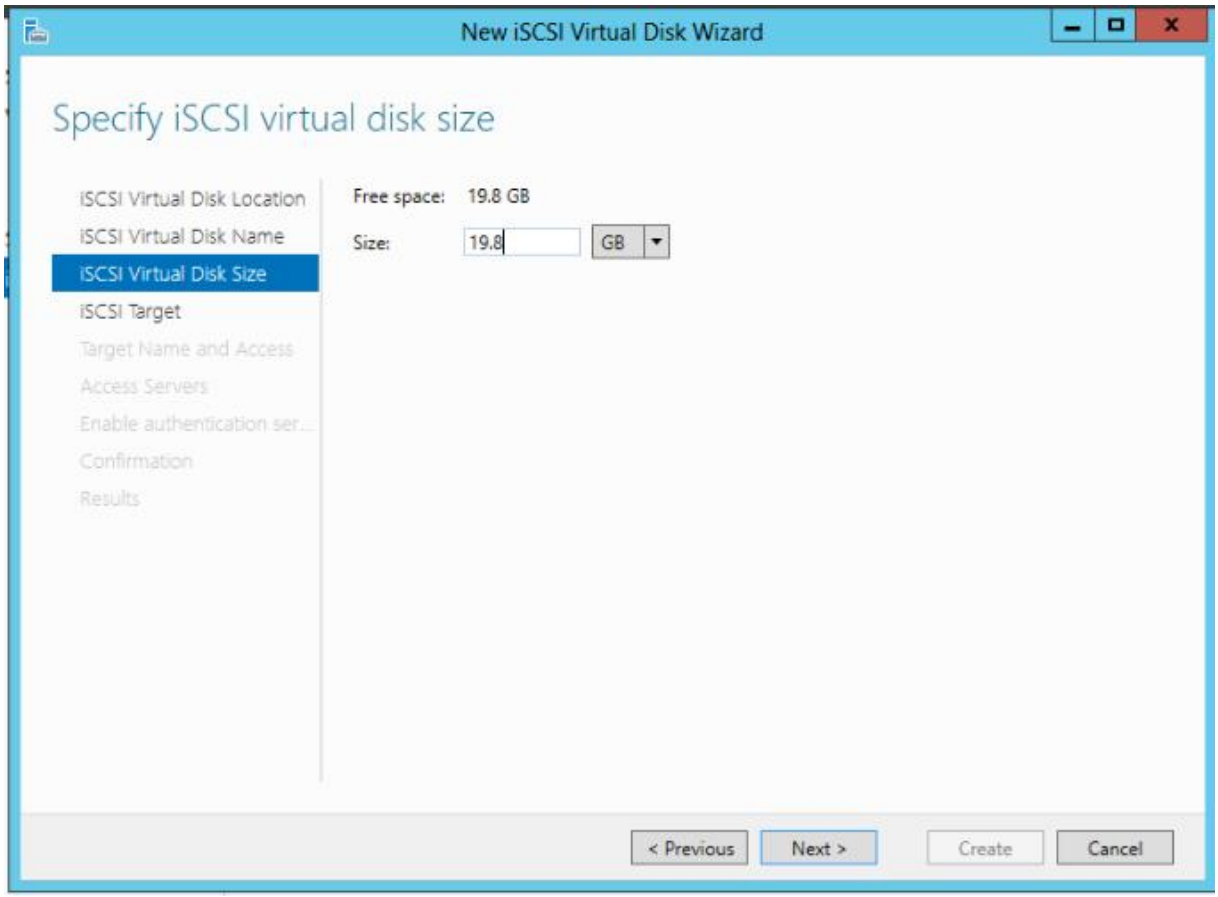
Nous avons choisis où nous souhaitons créer le disque virtuel, puis on a cliqué sur Suivant. Pour nous, nous avons choisis de le placer dans le G.



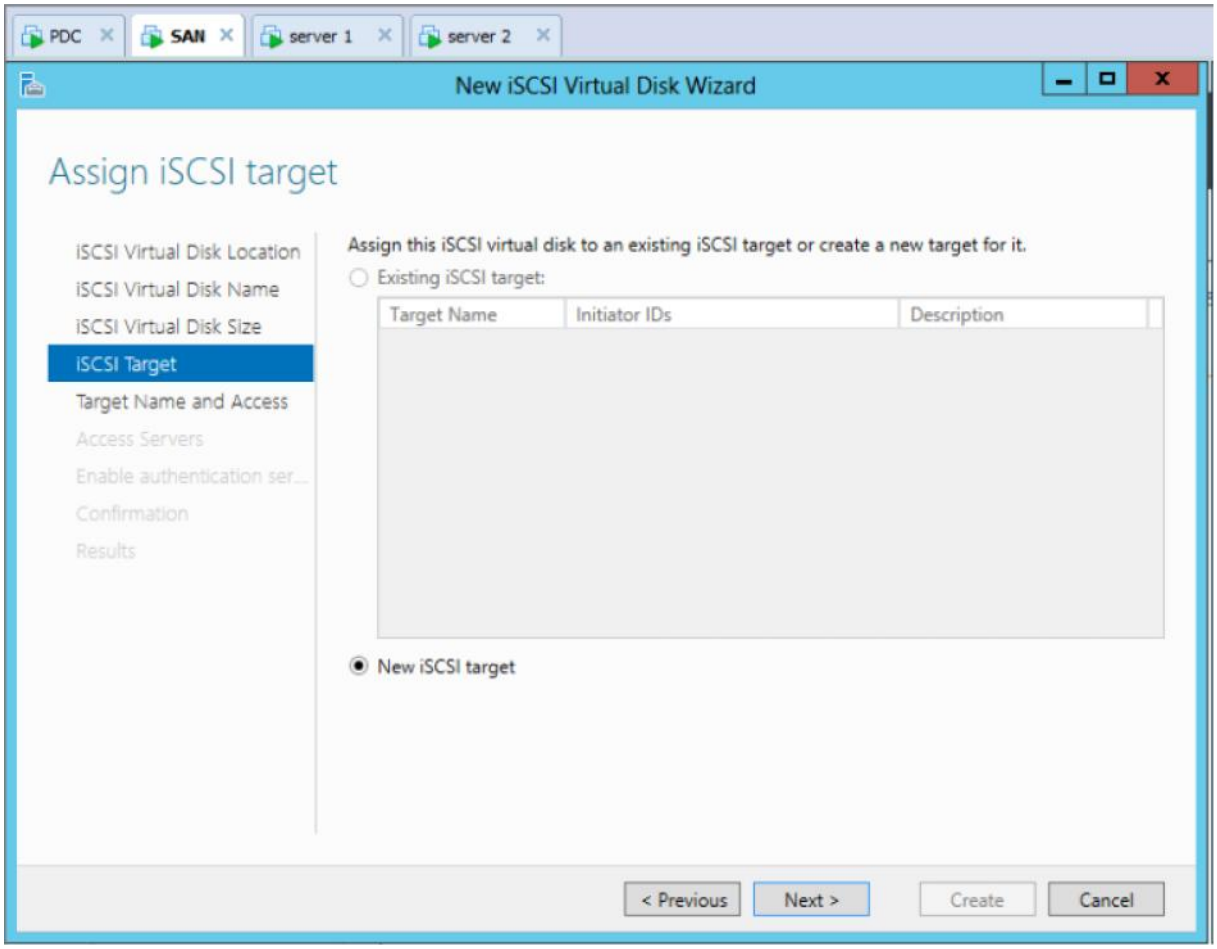
On lui a Donné un nom.



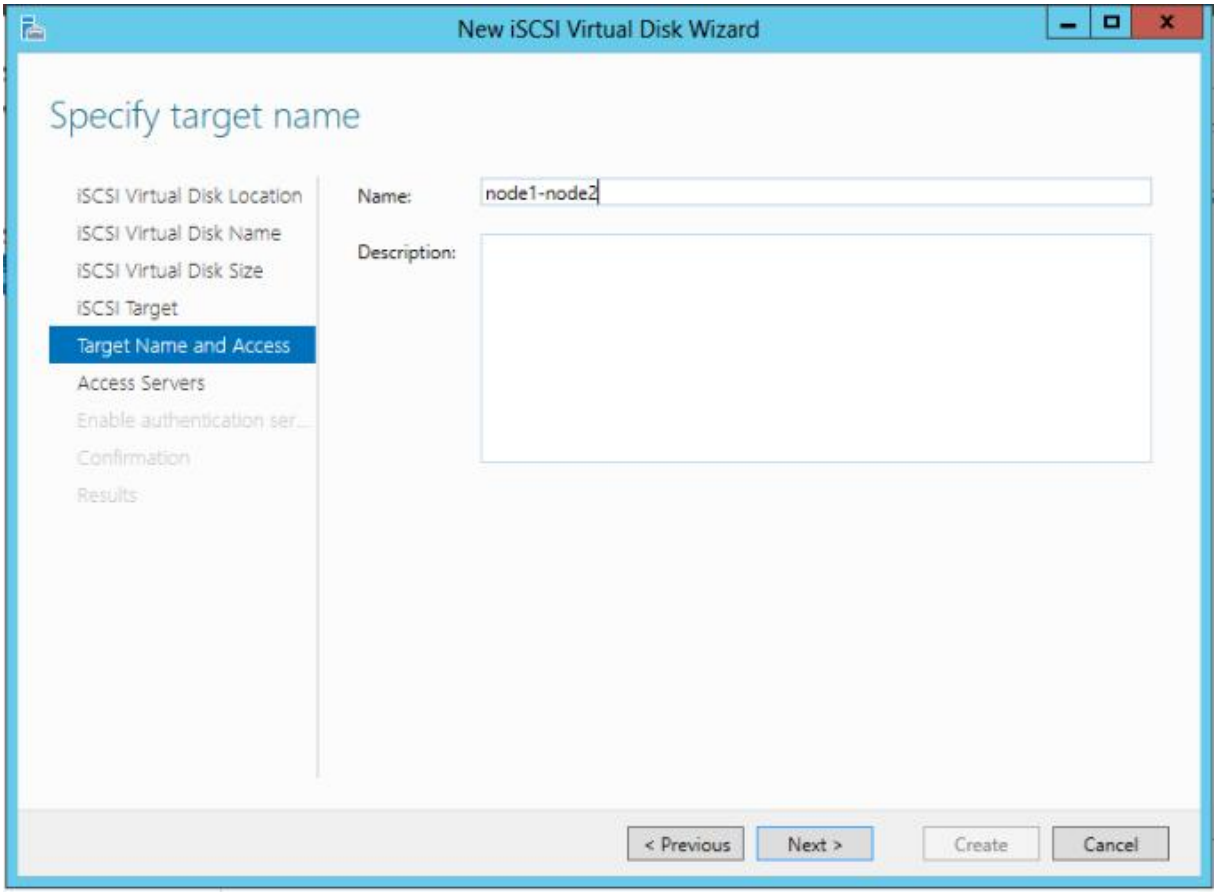
On a donné 19.8 Go sur l'espace de disque.



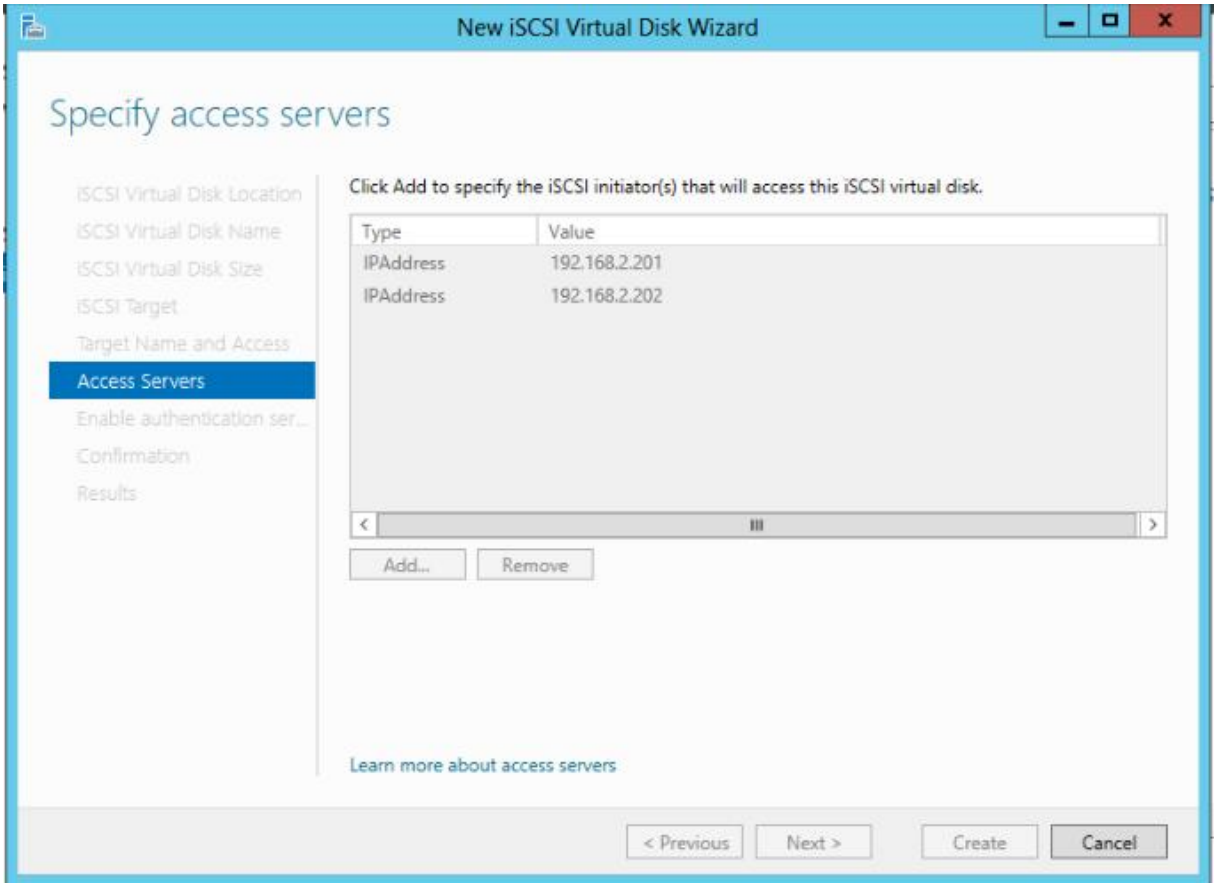
On crée une nouvelle cible iSCSI, On clique sur Suivant.



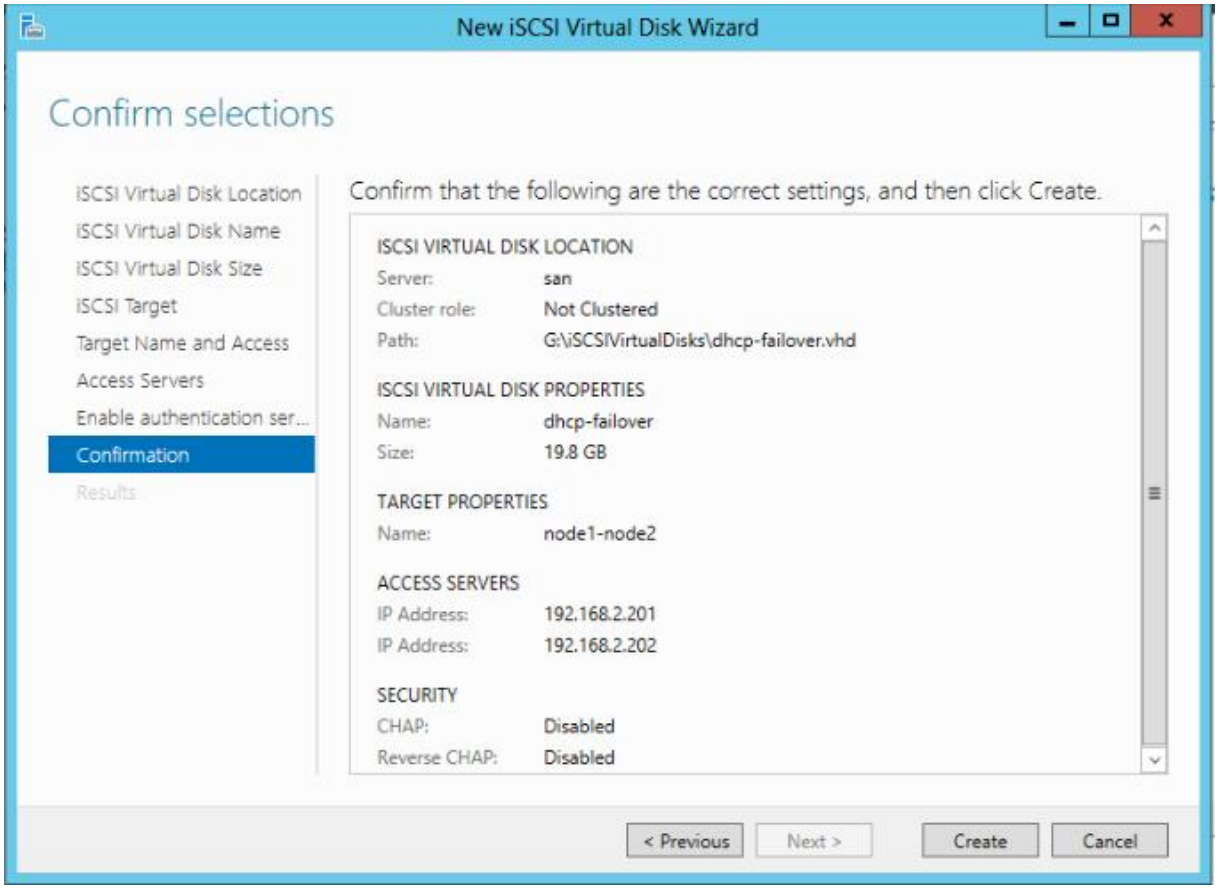
On donne un nom à notre cible puis on clique sur Suivant.

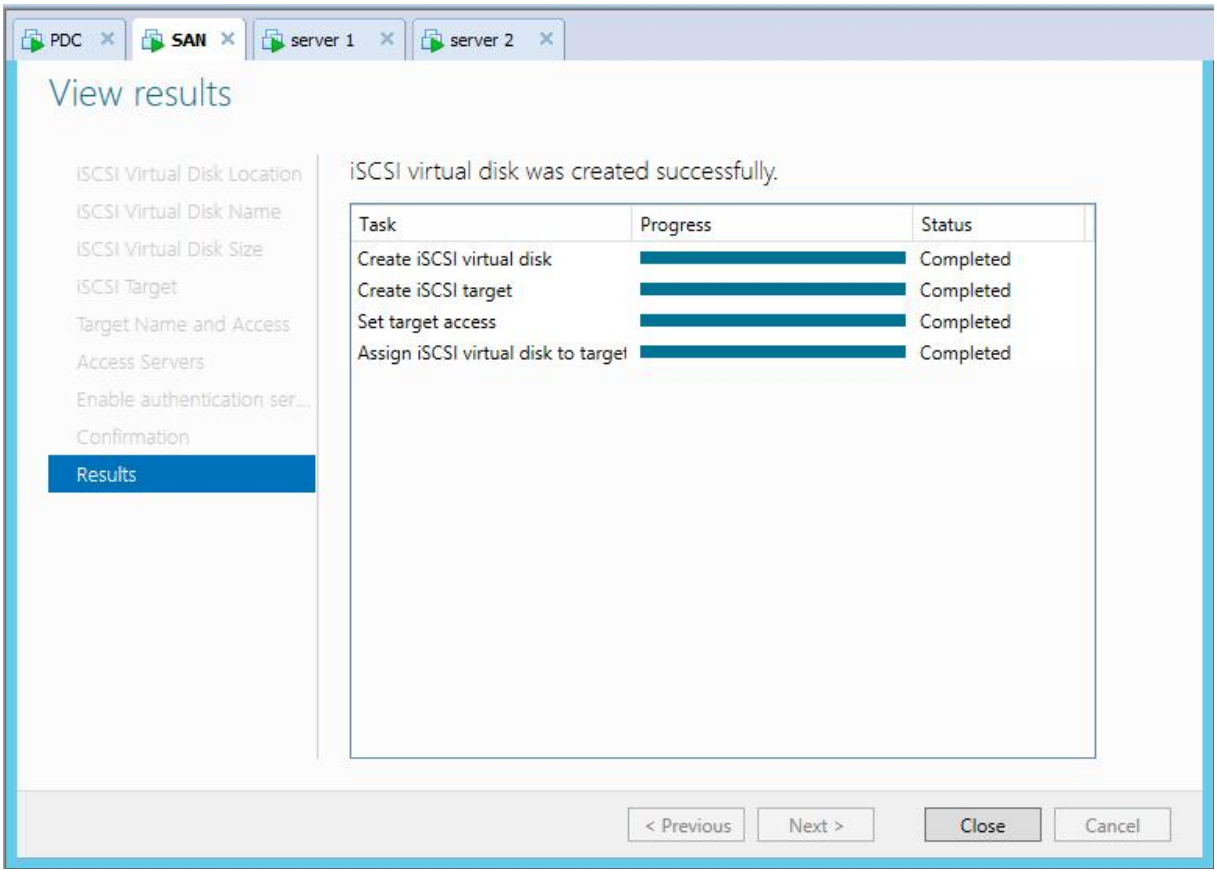


On clique sur Ajouter pour ajouter les serveurs qui se connecteront à notre SAN iSCSI.

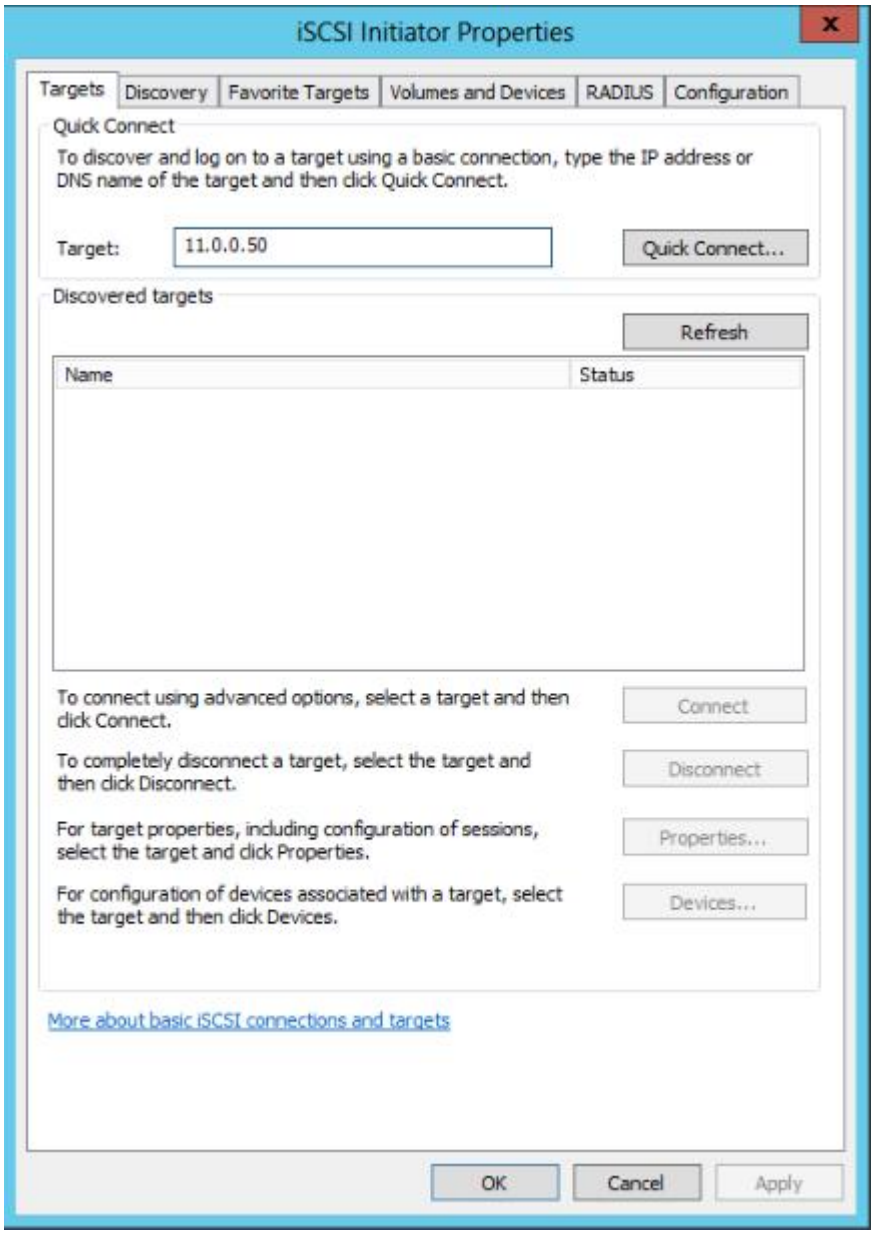


On clique sur Créer.

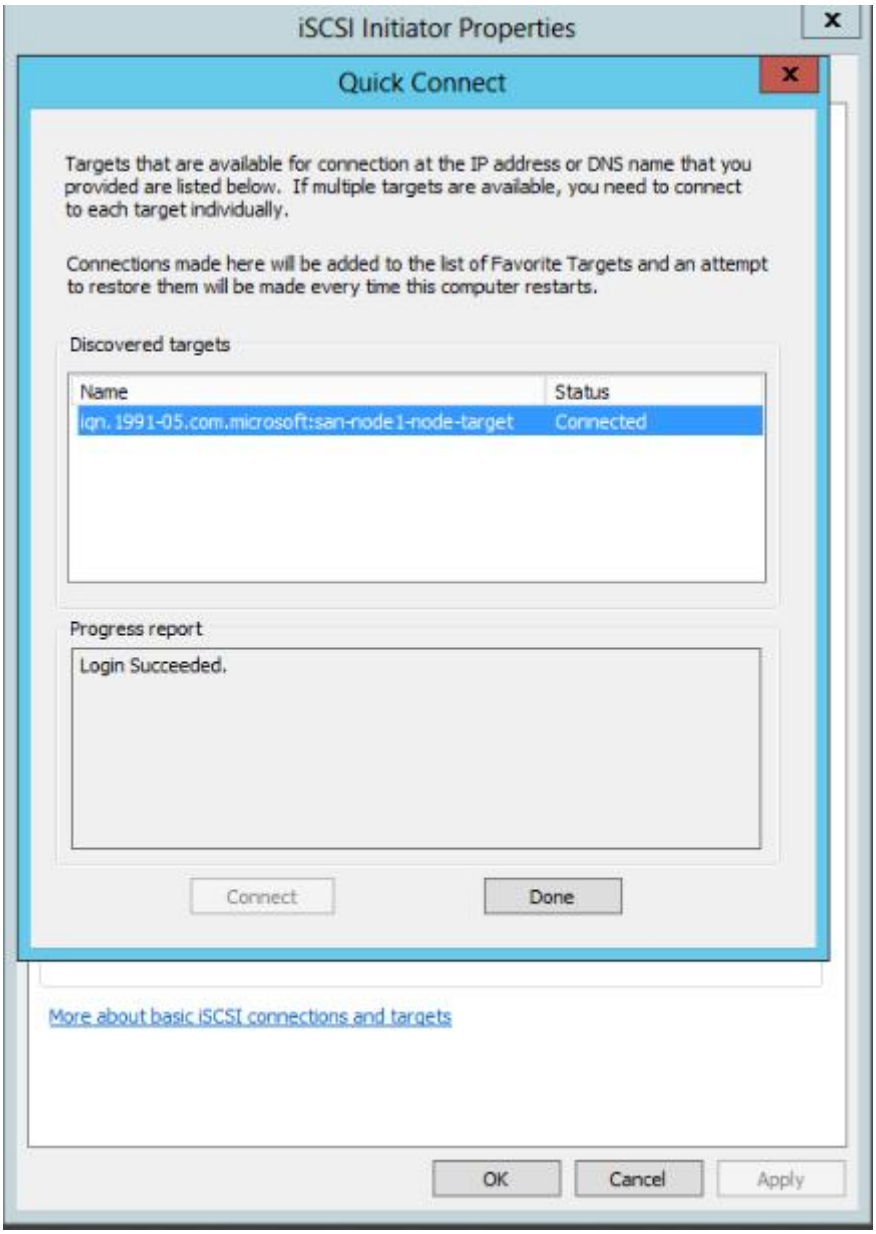




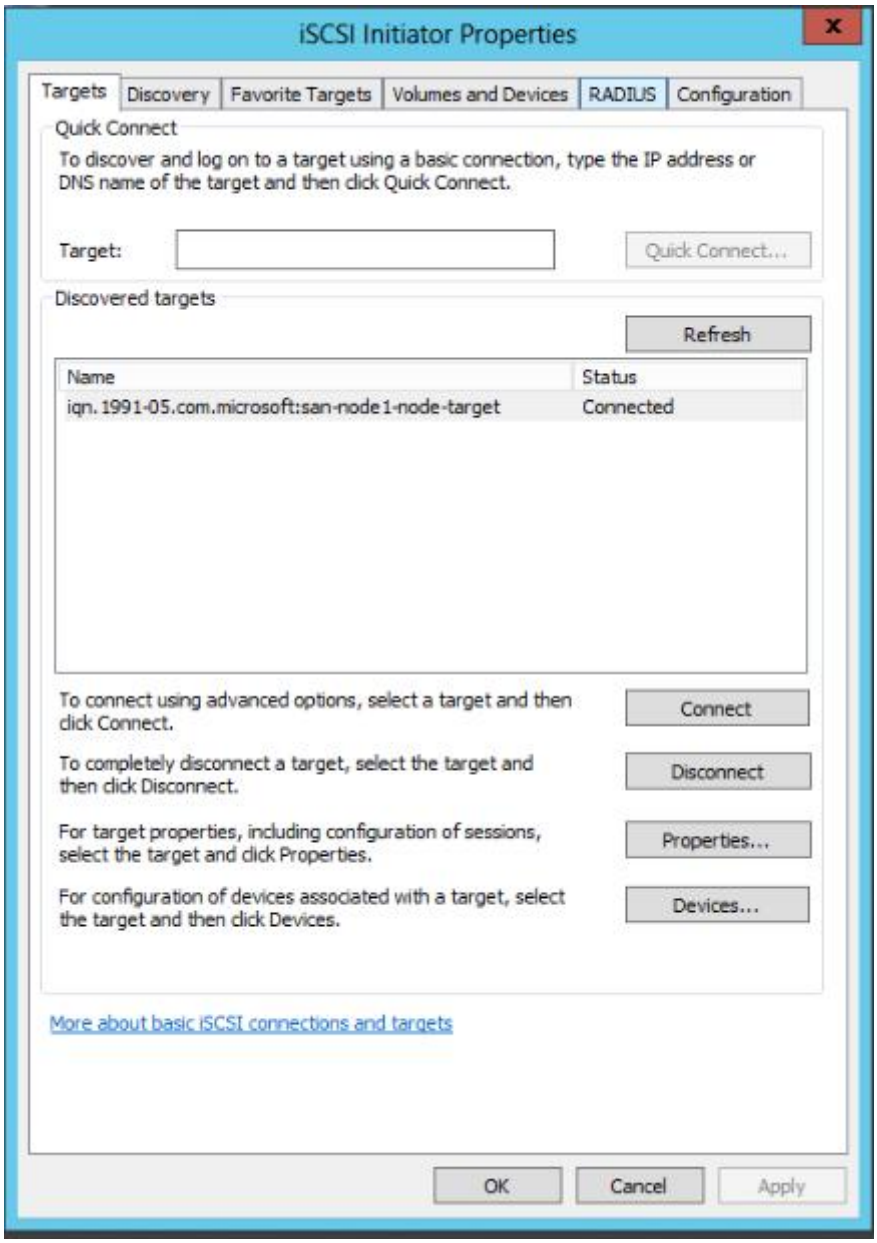
Maintenant, c'est prêt pour le serveur 2, pour s'y connecter. On sélectionne tools > initiateur iSCSI. On entre l'adresse IP de notre réseau SAN iSCSI qu'on vient de configurer, puis on clique sur Connexion rapide ...



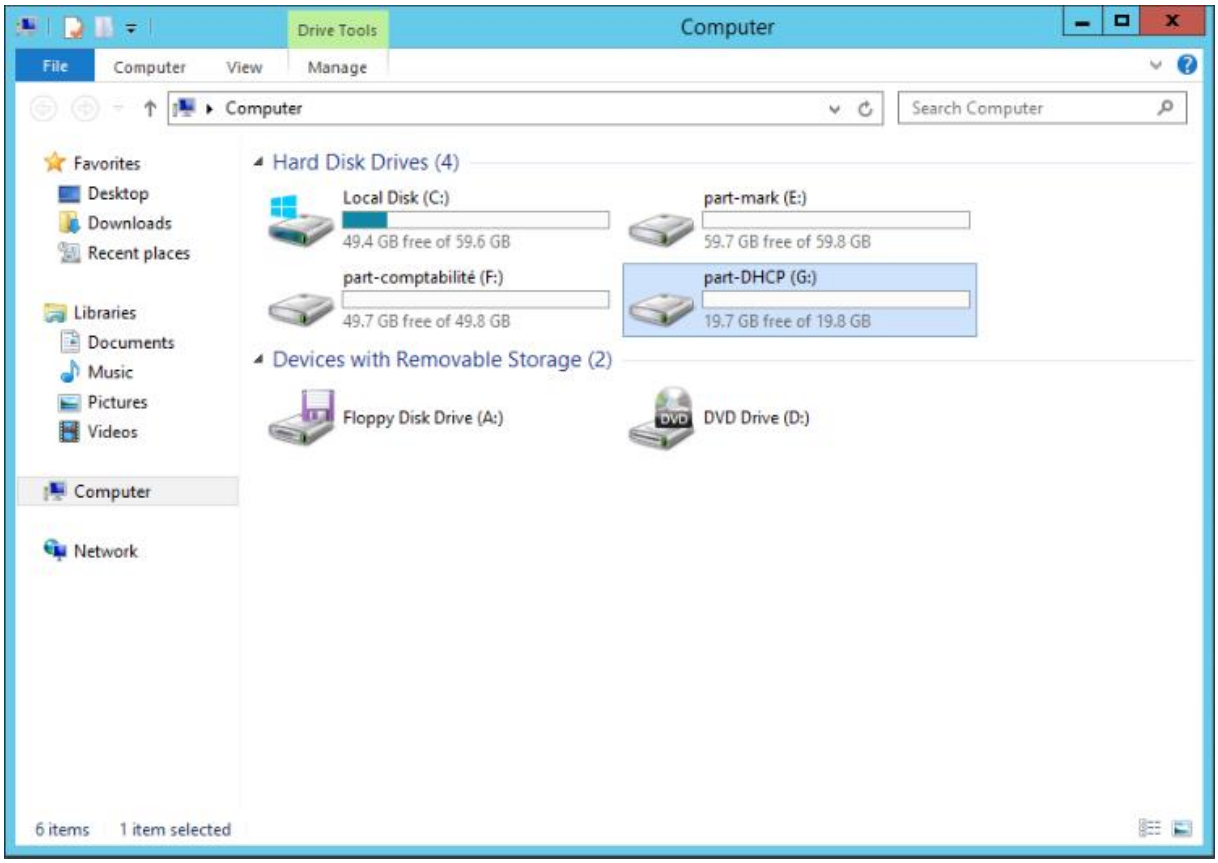
On remarque qu'il est connecté.



Maintenant qu'on est connecté au SAN.



Nous allons à notre Espace disque qui montre en effet que nous avons maintenant un nouveau Lecteur.



IV.4. Cluster du basculement (Failover cluster)

Afin d'implémenter cette solution, nous avons préparé deux noeuds (Windows Server 2012) membres du domaine(RTGS.com), puis nous avons installé, sur les deux, la fonctionnalité cluster avec basculement via le gestionnaire de serveur.

1. Configuration des cartes réseaux

On a besoin de 3 cartes réseaux dans node1 et node 2

Node 1 :

Interne 10.0.0.201

Passerelle 192.168.2.201

SAN 11.0.0.201

Node 2 :

Interne 10.0.0.202

Passerelle 192.168.2.202

SAN 11.0.0.202

Une cartes réseaux sure SAN

SAN 10.0.0.10 et deux cartes réseaux PDC de domaine avec DNS

Interne 10.0.0.200

SAN 192.168.2.200

2. L'ajout de rôle de cluster du basculement

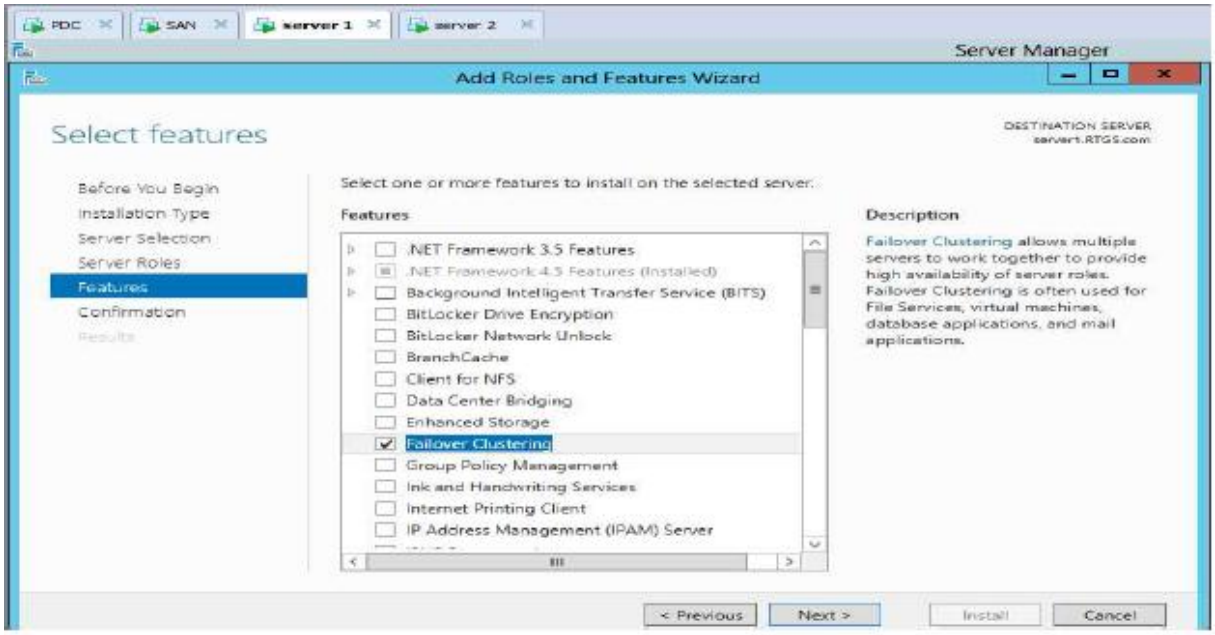
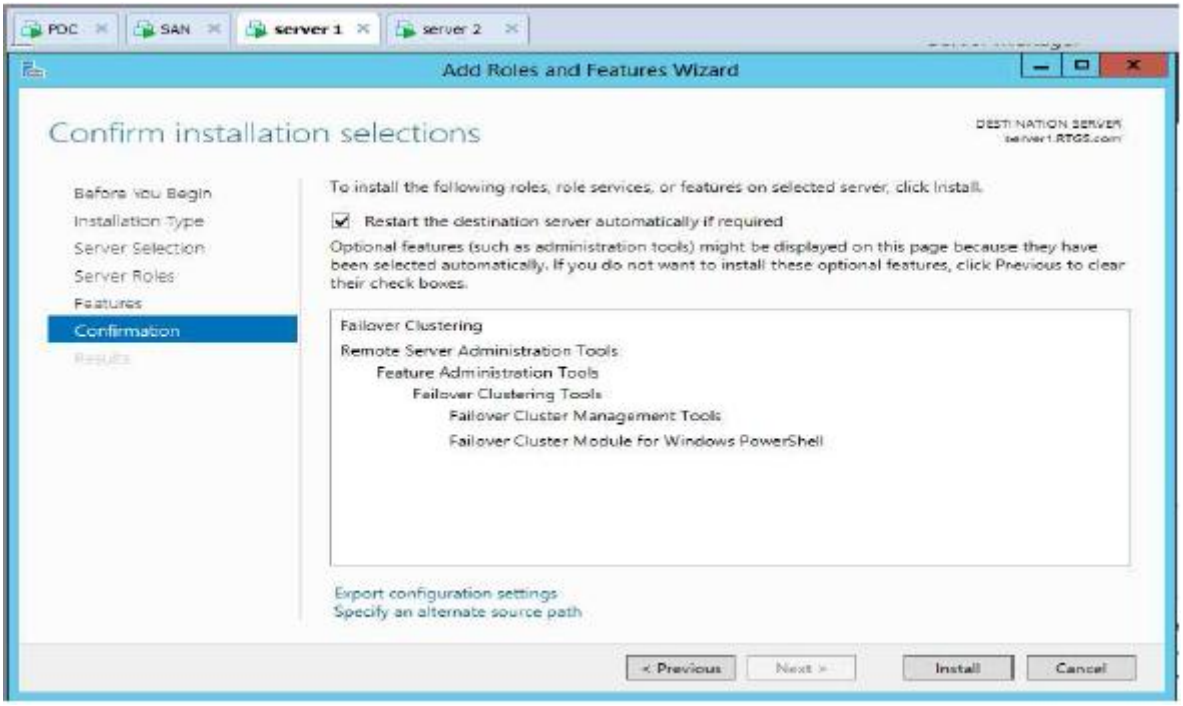
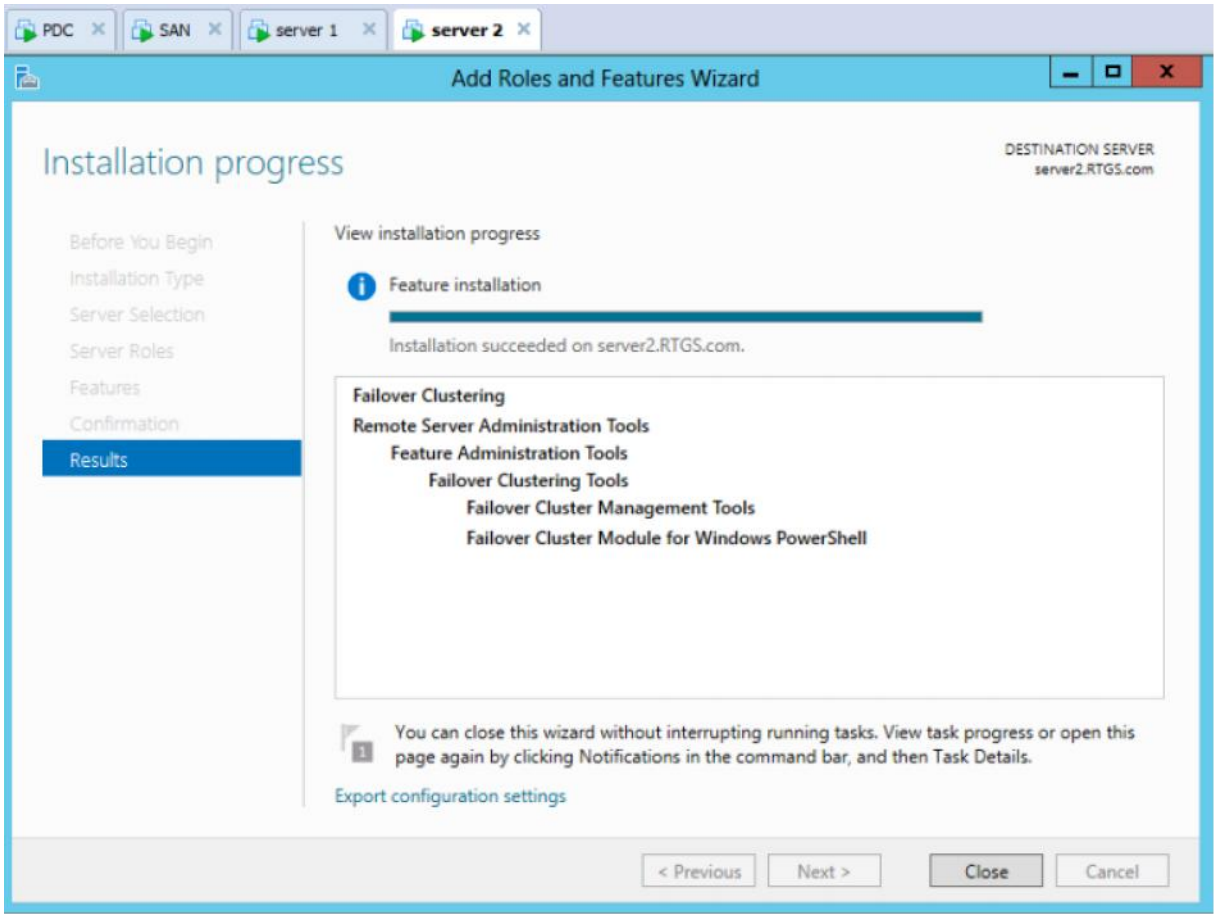


Figure IV.10 : Ajout de rôle de Cluster de Basculement.

On clique sur Next après sur Install





Le rôle failover cluster est installé.

3. Validation de la configuration du cluster

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

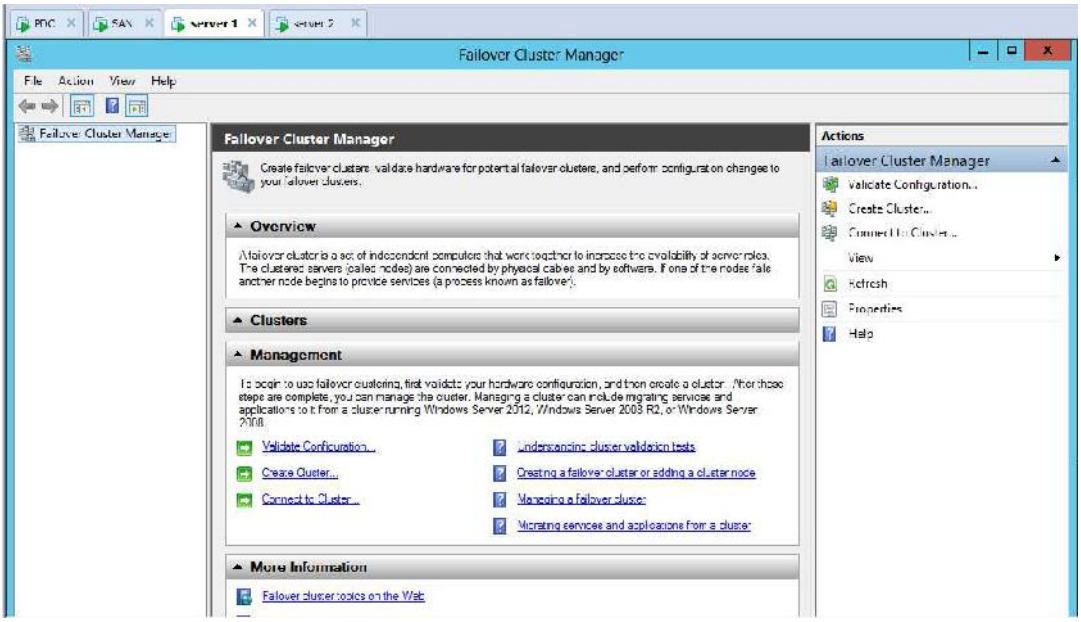
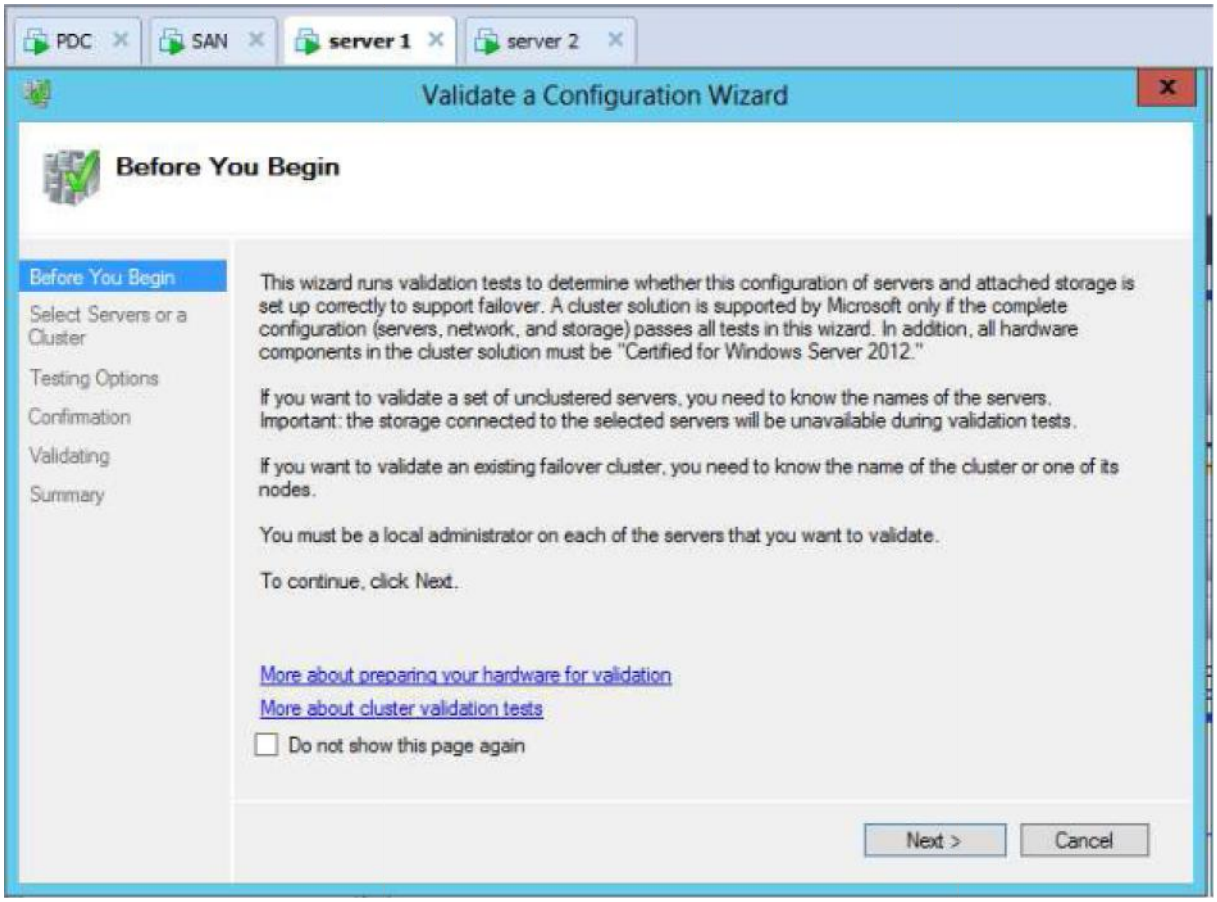
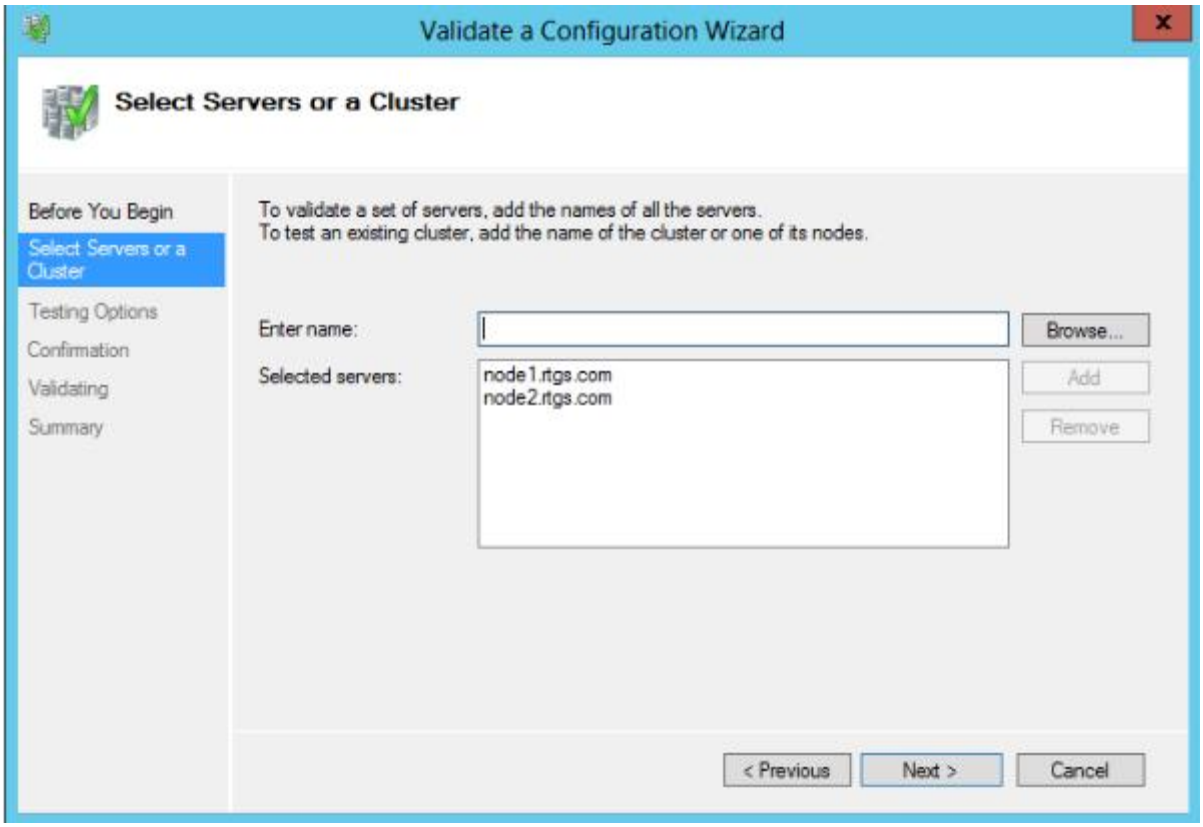


Figure IV.11 : Gestion de cluster de basculement.

L'assistant affiche d'abord une page d'accueil. On clique sur Suivant pour aller à la page Sélectionner des serveurs ou une page de cluster. Sur cette page, on entre les noms des nœuds de cluster que nous souhaitons valider





On clique sur Suivant pour accéder à la page de confirmation, qui porte sur les tests qui seront exécutés, ensuite on clique sur Suivant pour démarrer le processus de test de validation de cluster.

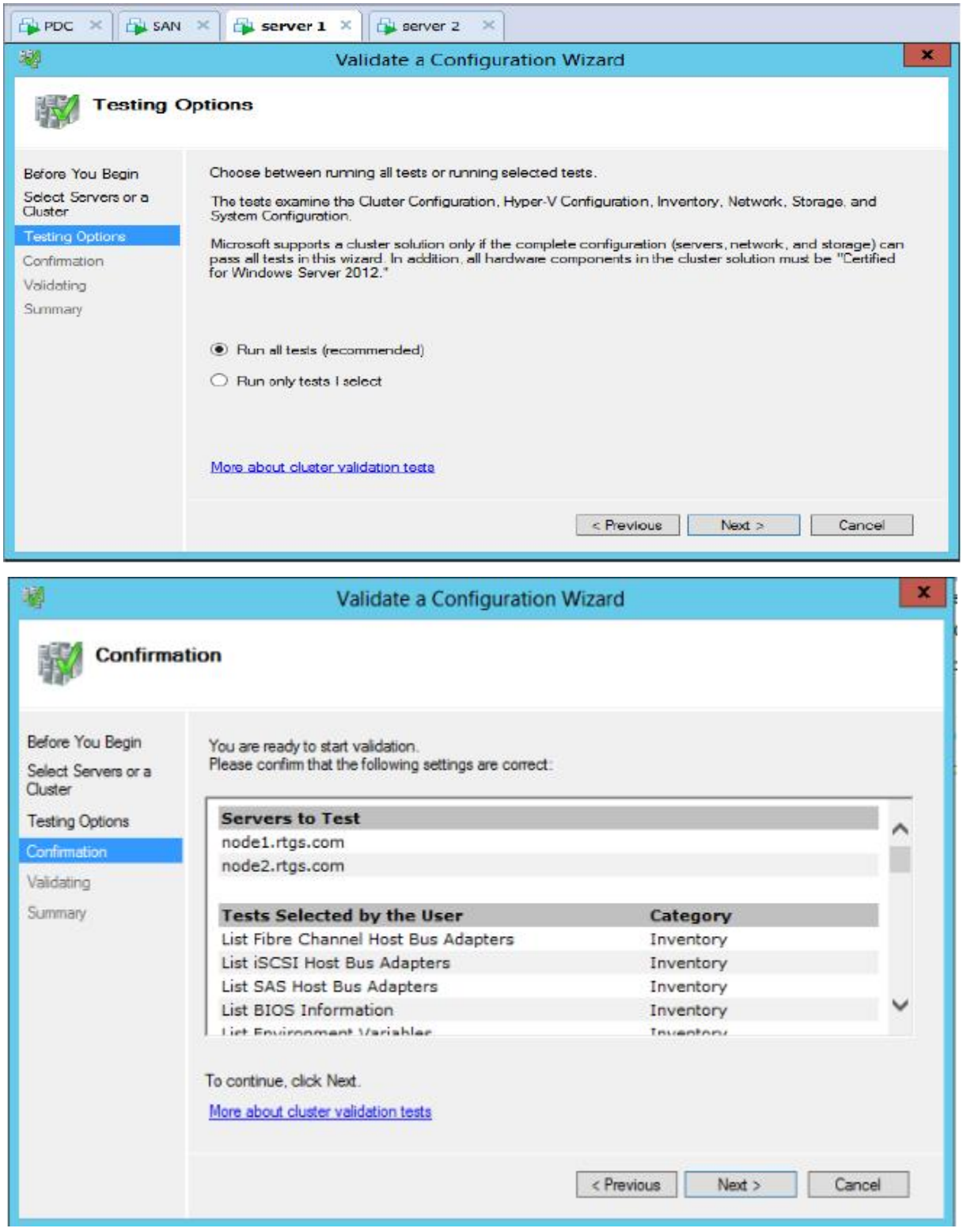


Figure IV.12: Validation de la configuration.

Une fois les tests de validation réussissent, nous pouvons créer le cluster.

Sur le point d'accès pour l'administration la page de cluster, vous devez spécifier le nom de votre groupe et l'adresse IP, à la fois de ce qui doit être unique dans le réseau.

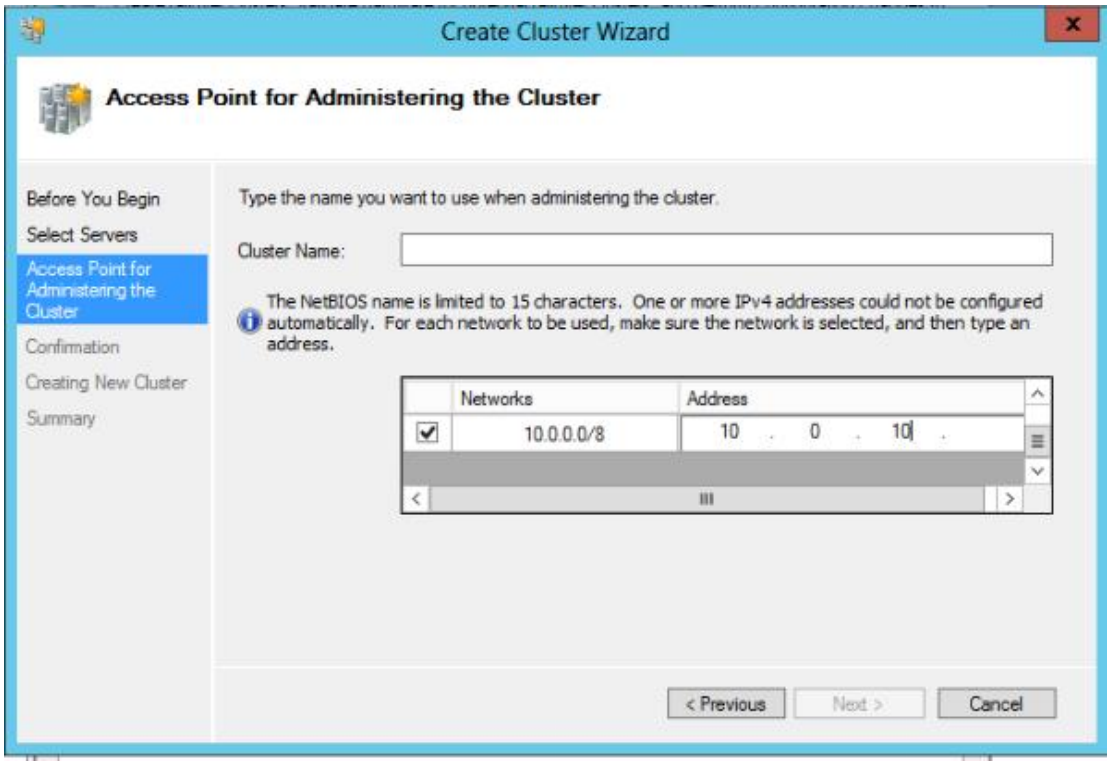


Figure IV.13: L'attribution des paramètres de cluster.

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

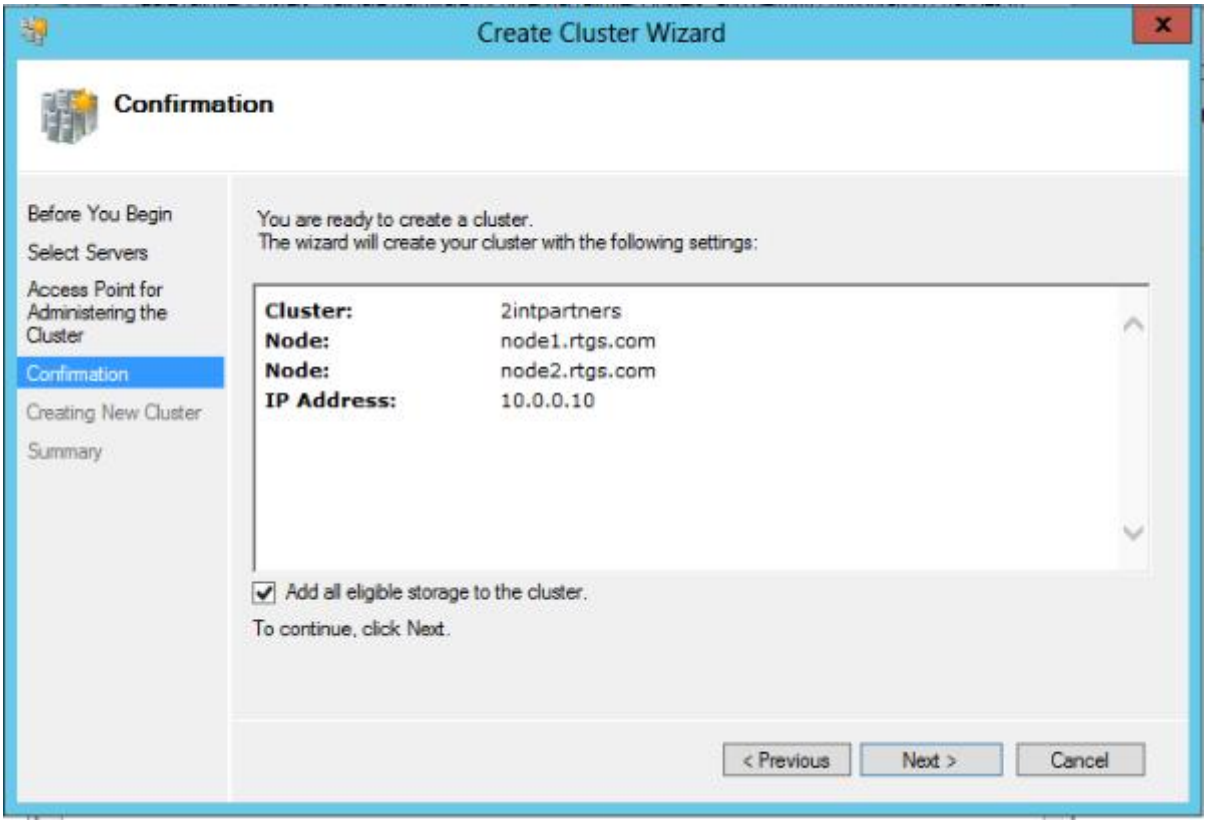


Figure IV. 14: Confirmation de création de cluster.

Etape III : La connexion des machines sous GNS3

Apres avoir implémenté les différentes solutions concernant les machines virtuelles, nous les connectons à GNS3. 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
- 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.

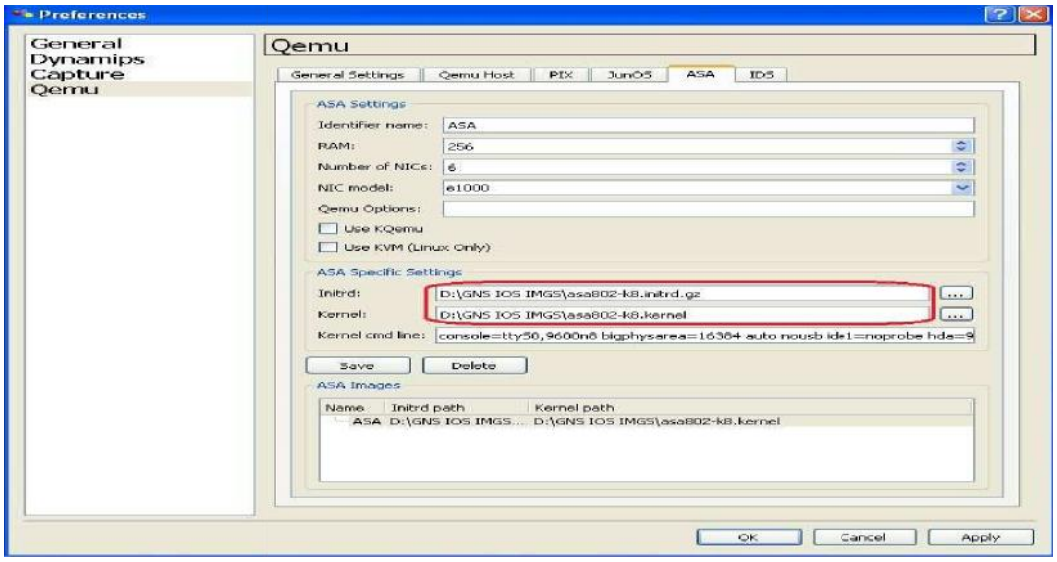
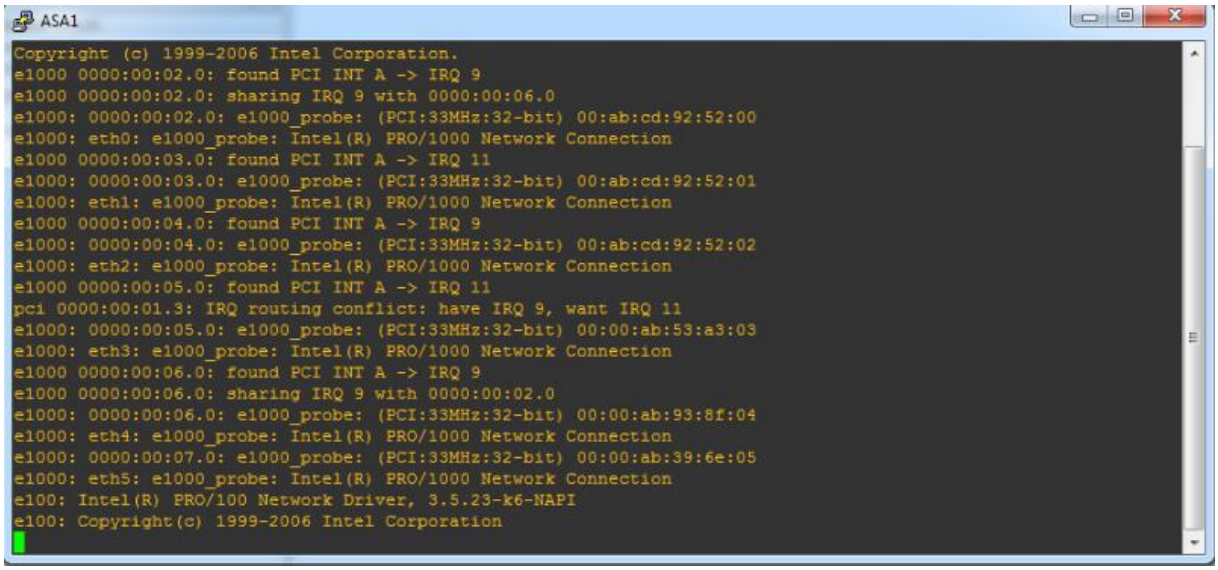


Figure IV.15: L'ajout de l'IOS pour l'ASA.

Maintenant que le chargement 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.



Pour activer la console de l'ASA, on introduit les deux clés d'activation comme illustré dans la figure IV.16.

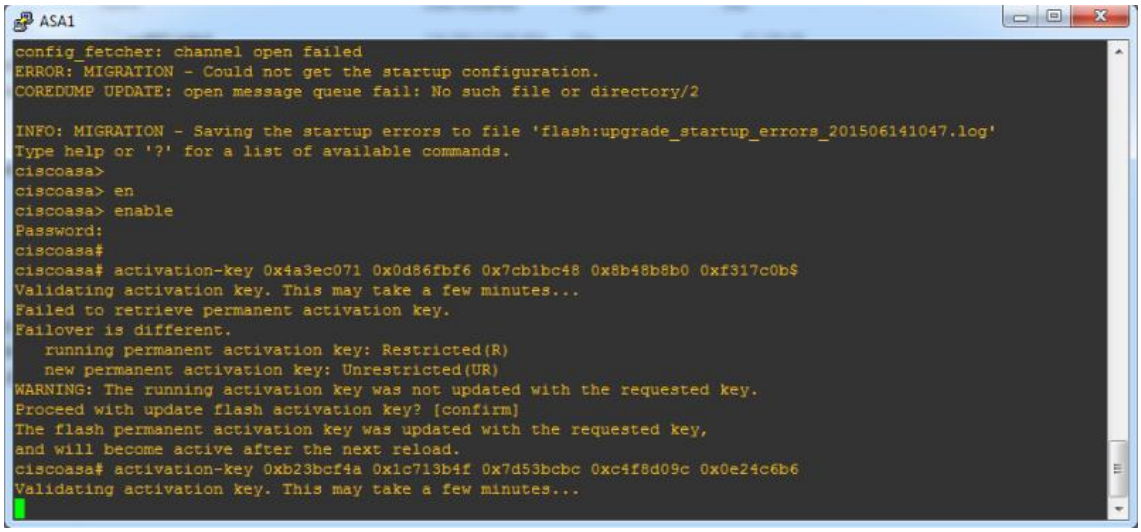


Figure IV.16 : activation de la console.

1.2. Configuration des interfaces de l'ASA

Nous tapons les commandes suivantes pour vérifier les interfaces de l'ASA, comme le montre la figure IV.17.

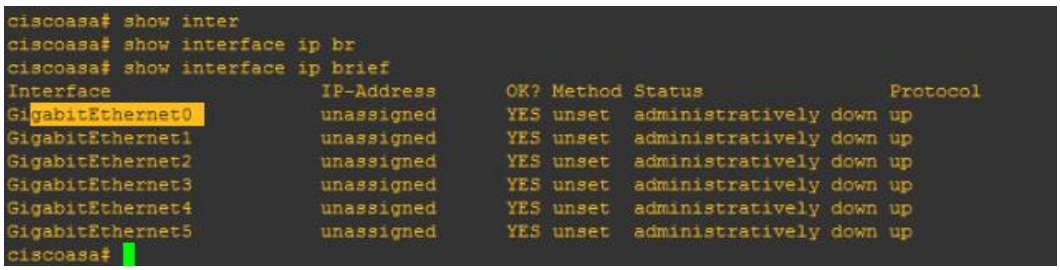


Figure IV.17 : interfaces de l'ASA.

Nous allons configurer l'interface e0 qui relie le réseau interne à l'ASA, comme le montre la figure IV.18.

```
ciscoasa(config)# interface gigabitEthernet 0
ciscoasa(config-if)# ip add
ciscoasa(config-if)# ip address 10.0.0.2 255.0.0.0
ciscoasa(config-if)# no shut
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nam
ciscoasa(config-if)# namei
ciscoasa(config-if)# nameif management
INFO: Security level for "management" set to 0 by default.
```

Figure IV.18 : configuration de l'interface.

Ensuite on donne le niveau de sécurité pour le réseau interne qui est de 100, comme le montre la figure IV.19.

```
ciscoasa(config-if)# security-level 100
```

Figure IV.19 : niveau de sécurité.

1.3. La configuration de l'HTTP

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

```
ASAcisco(config)# http server en
ASAcisco(config)# http server enable
ASAcisco(config)# htt
ASAcisco(config)# http 10.0.0.222 255.255.255.255 management
```

Figure IV.20: La configuration de l'http.

1.4. 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 :

1.4.1. Installer ASDM dans le serveur TFTP

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

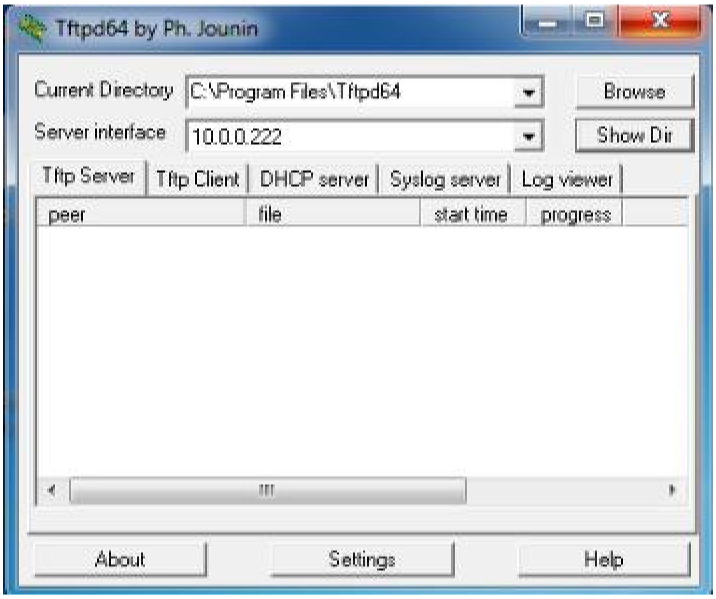
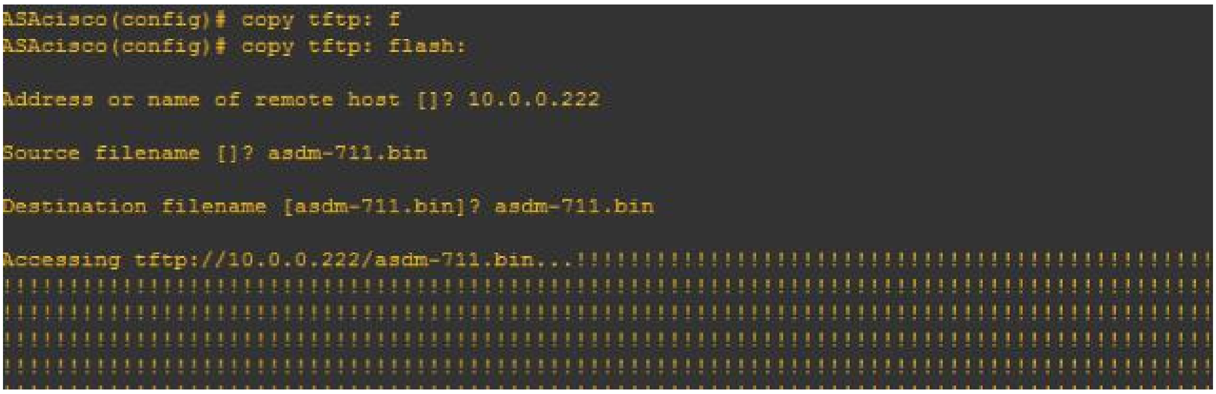


Figure IV.21: Ajout de l'image ASDM à TFTP.

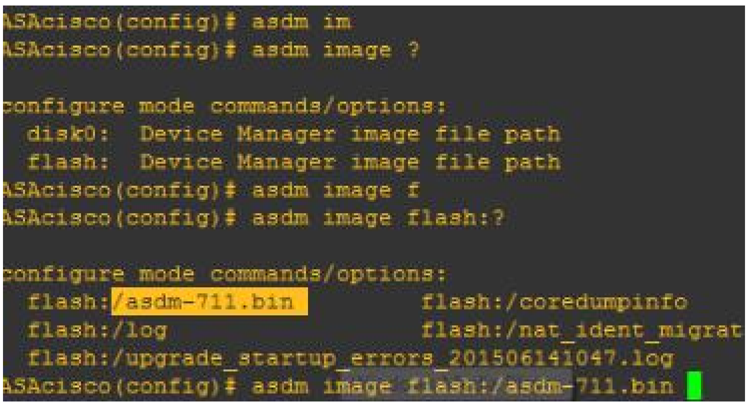
Maintenant, revenons à notre console ASA et chargeons l'image ASDM-647.bin en tapant les commandes suivantes :



```
ASAcisco(config)# copy tftp: f
ASAcisco(config)# copy tftp: flash:

Address or name of remote host []? 10.0.0.222

Source filename []? asdm-711.bin

Destination filename [asdm-711.bin]? asdm-711.bin

Accessing tftp://10.0.0.222/asdm-711.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Figure IV.22: 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.



```
ASAcisco(config)# asdm im
ASAcisco(config)# asdm image ?

configure mode commands/options:
  disk0:  Device Manager image file path
  flash:  Device Manager image file path
ASAcisco(config)# asdm image f
ASAcisco(config)# asdm image flash:?

configure mode commands/options:
  flash:/asdm-711.bin                flash:/coredumpinfo
  flash:/log                         flash:/nat_ident_migrat
  flash:/upgrade_startup_errors_201506141047.log
ASAcisco(config)# asdm image flash:/asdm-711.bin
```

1.5. Le lancement de l'ADSM

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

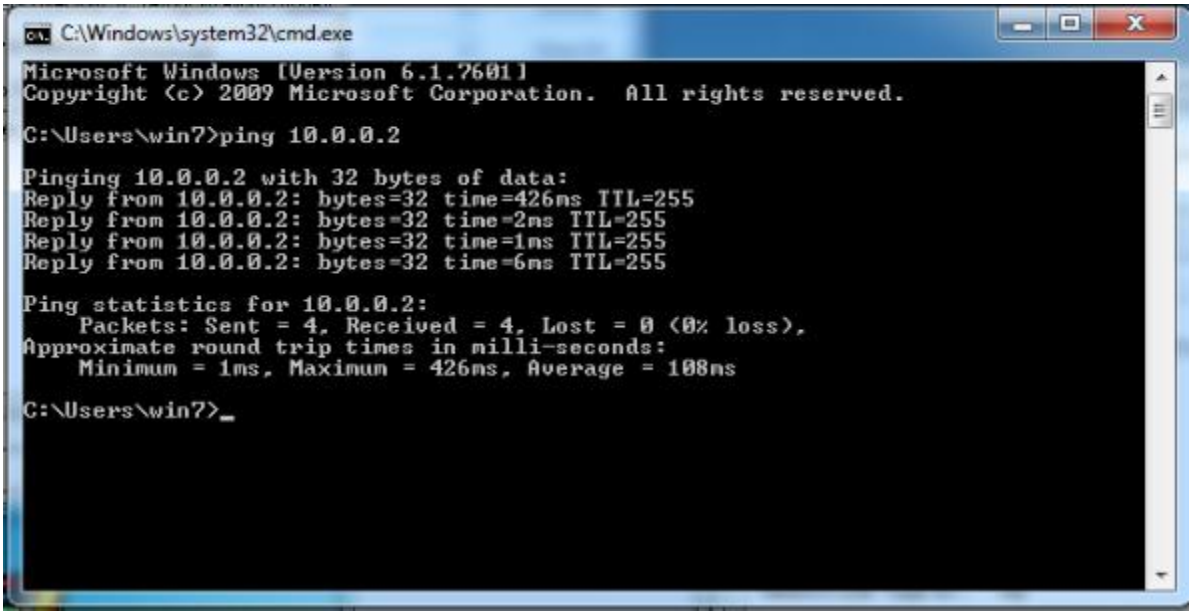


Figure IV.23: Ping de la machine distante

A partir de l'internet explorer de la machine distante introduisons l'adresse https://10.0.0.2/.

Dans la page qui s'ouvre cliquons sur poursuivre avec ce site web (non recommandé).

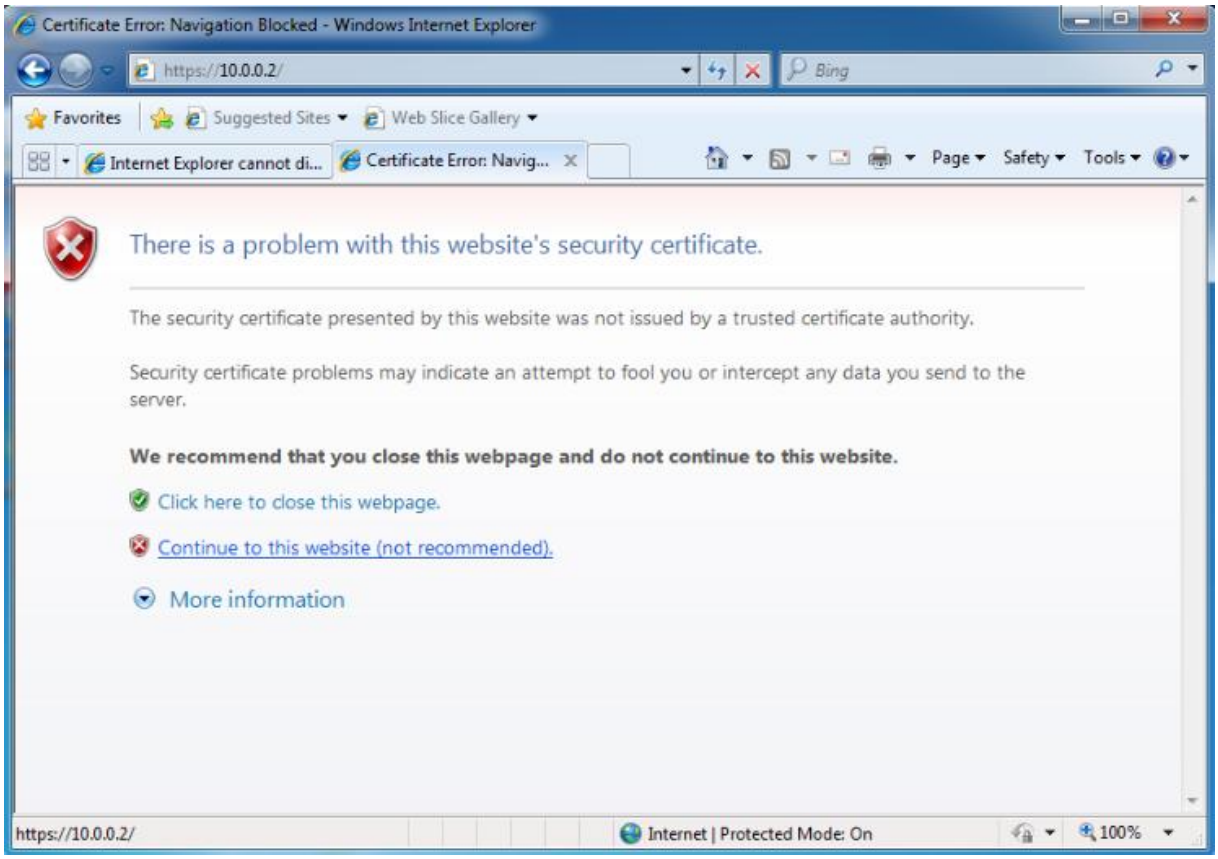


Figure IV.24: Accès à l'interface d'ASA.

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

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

Figure IV.25: L'authentification de l'utilisateur.

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

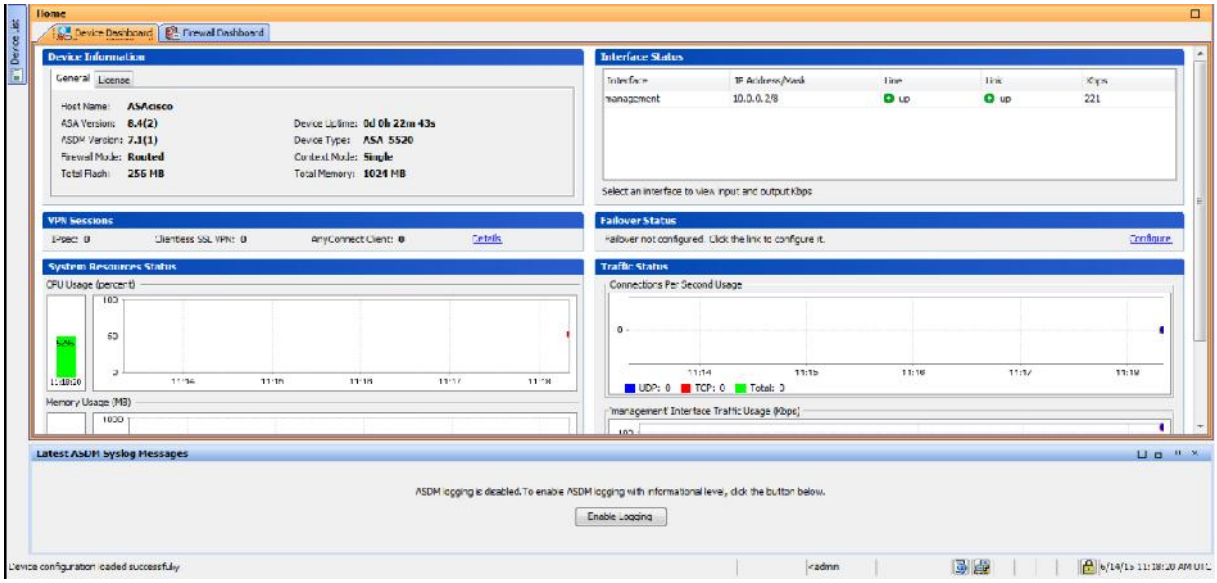


Figure IV.26: Le menu Home de l'interface ASDM.

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

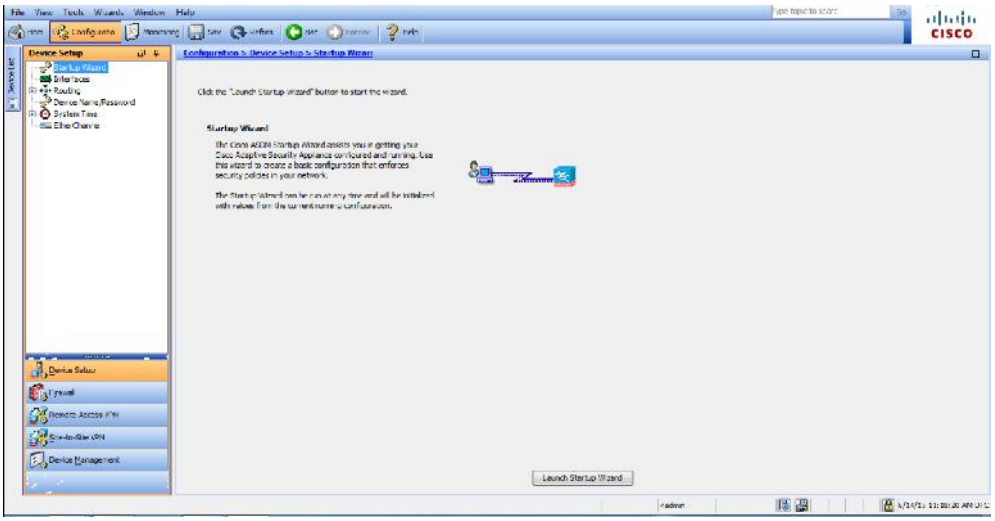
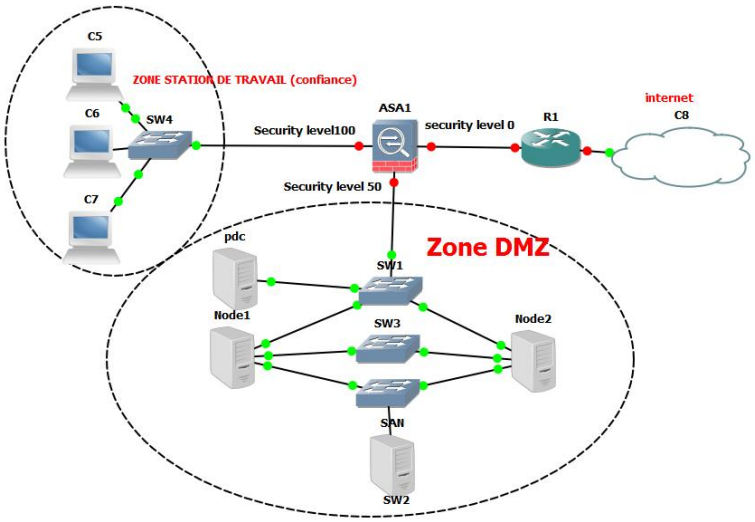


Figure IV.27: Menu configuration.

2. Création de la DMZ

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



ASA->Intranet : L'interface inside avec un niveau de sécurité 100.

ASA-> DMZ : L'interface DMZ avec un niveau de sécurité 50.

ASA->internet : L'interface outside avec un niveau de sécurité 0.

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

De l'intranet->DMZ c'est permis (100->50).

De l'intranet->internet c'est permis (100->0).

De DMZ->internet c'est permis (50->0).

De DMZ->intranet n'est pas permis (50->100).

De l'internet->DMZ n'est pas permis (0->50).

De l'internet->Intranet n'est pas permis (0->100).

De cette manière, nous assurons la protection la banque de façon qu'aucun trafic ne puisse entrer.

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

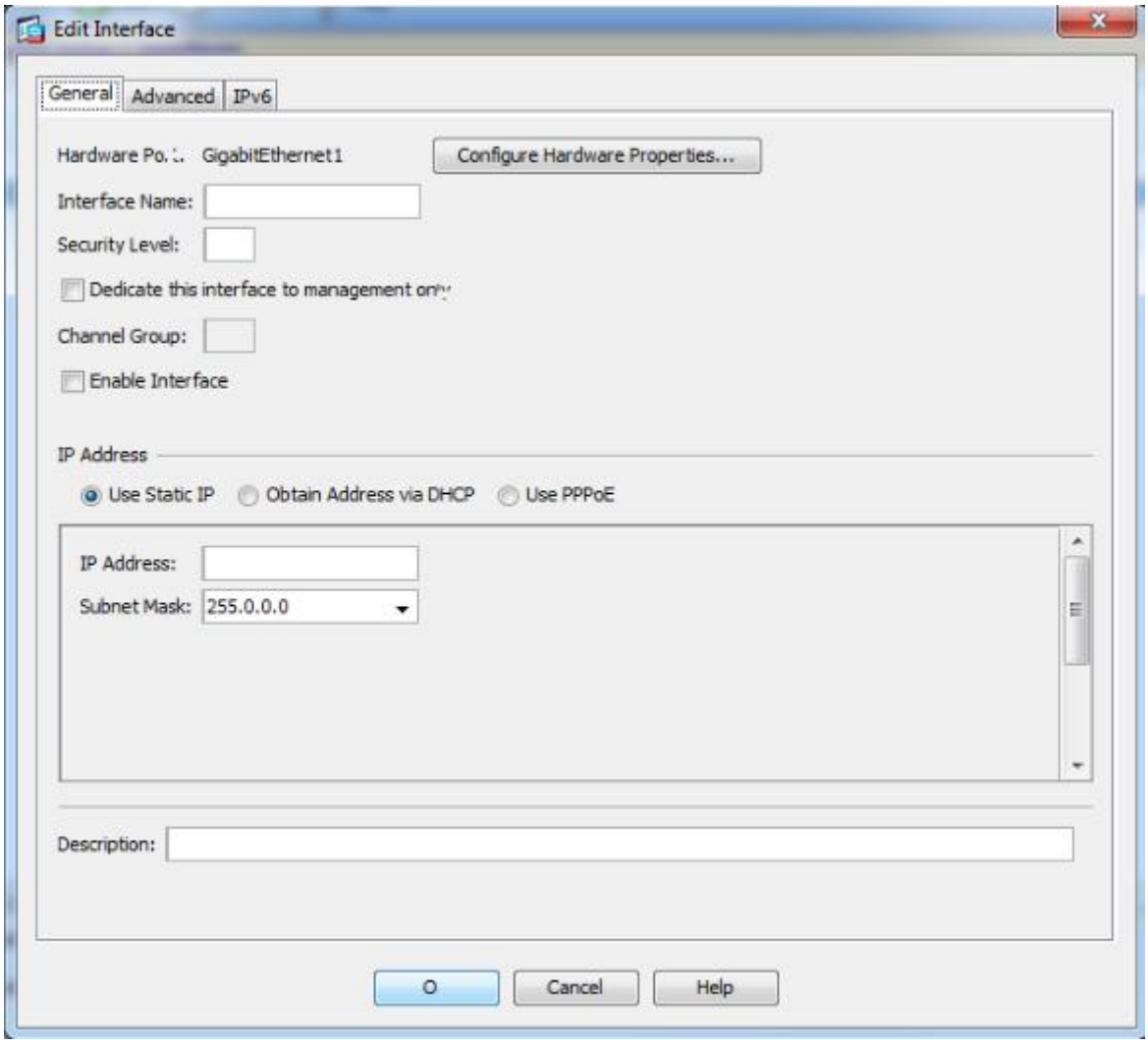


Figure IV.28: Ajout d'une interface.

Si on vérifie dans la console d'ASA on trouve que l'interface de la DMZ a été ajoutée avec un niveau de sécurité de 50, comme le montre la figure IV.29.

```
ASAcisco# show nameif
Interface                  Name                       Security
GigabitEthernet0           management                 100
GigabitEthernet1           DMZ                         50
ASAcisco# show inter
ASAcisco# show interface ip ip b
ASAcisco# show interface ip ip br
ASAcisco# show interface ip ip bri
ASAcisco# show interface ip br
ASAcisco# show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0           10.0.0.2        YES manual up                    up
GigabitEthernet1           11.0.0.2        YES manual administratively down up
GigabitEthernet2           unassigned      YES unset  administratively down up
GigabitEthernet3           unassigned      YES unset  administratively down up
GigabitEthernet4           unassigned      YES unset  administratively down up
GigabitEthernet5           unassigned      YES unset  administratively down up
ASAcisco#
```

Figure IV.29 : interface de la DMZ.

Pour l'interface qui relie l'ASA au réseau externe, en procède à sa configuration comme le montre la figure IV.30.

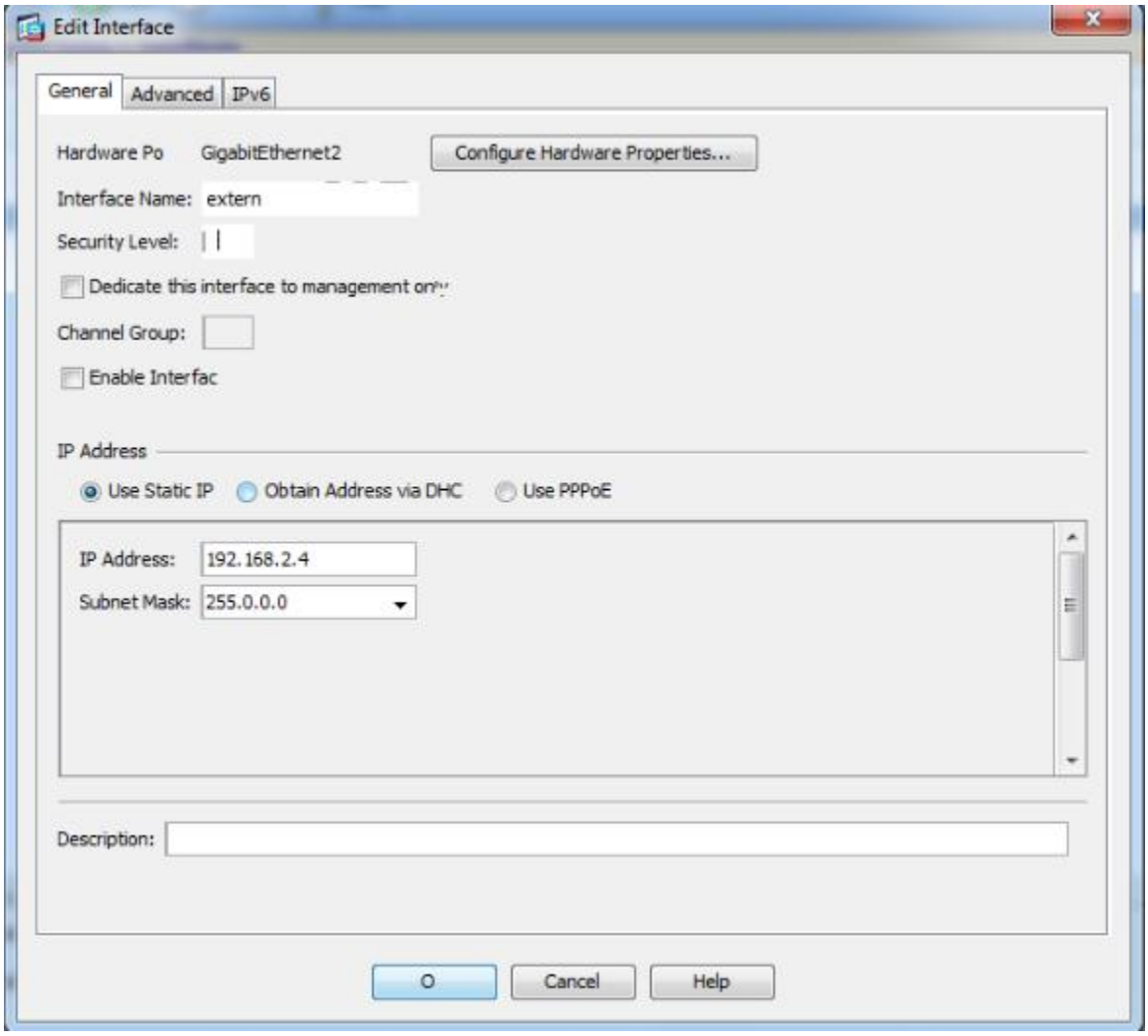


Figure IV.30: Ajout de l'interface du réseau externe.

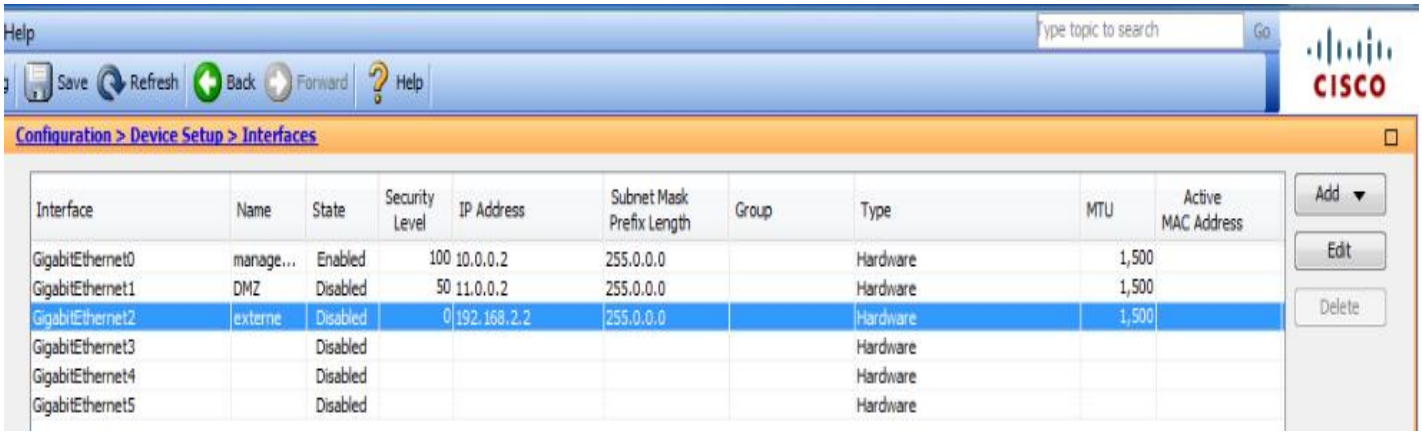


Figure IV.31 : L'ensemble des interfaces ajoutées.

IV.5.Discussion

Durant ce chapitre, nous avons présenté l'implémentation et la mise en œuvre de notre politique de sécurité qui consiste à implémenter et configurer le firewall ASA et la DMZ qui contient le faillover pour assurer à tout moment la disponibilité des données.

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

Conclusion

Conclusion

La base de notre projet est la sécurisation du réseau de la banque. En effet, nous nous sommes intéressés dans le premier chapitre sur la sécurité des réseaux informatiques et dans le deuxième chapitre sur la sécurisation des interconnexions.

Dans le troisième chapitre, nous avons étudié le réseau existant de la banque qui nous a permis d'avoir des idées sur tout le réseau informatique et de pouvoir donner quelques approches de solutions relatives aux problèmes trouvés.

Ensuite, nous avons procédé à l'étude détaillée des solutions proposées. Ceci nous a permis de confirmer les défaillances dans le réseau, et grâce aux outils libres, d'évaluer le niveau de vulnérabilité sur ce réseau.

La sécurité des systèmes d'information prend tout son sens dans un contexte tel que celui dans lequel nous avons travaillé et représente aujourd'hui une tâche de fond à prendre en compte par toute entreprise qui désire disposer d'un ensemble d'outils et de méthodes qui lui permettent et assurent la gouvernance de son système d'information. Ainsi après la définition d'une politique de sécurité et la connaissance des principes de base de la sécurité, l'implémentation d'un processus de sécurité s'avère indispensable afin d'instaurer un réseau sécurisé.

Bien évidement la sécurité à 100% reste un idéal à atteindre, surtout devant le large éventail des menaces qui mettent en danger l'exploitation d'un système d'information dans une banque. Ainsi il est important de bien formaliser une politique de sécurité en prenant en compte les risques réels qu'encourt un système informatique et en évaluant les coûts que peuvent engendrer les problèmes résultants de ces risques par rapport au coût nécessaire à la mise en place des solutions palliative à ces problèmes.

Enfin, l'élaboration d'une charte d'utilisation du réseau informatique et surtout une sensibilisation des utilisateurs du réseau sur le bien fondé de ces mesures de sécurité ainsi que leurs importance.

Perspective :

Il semble que, quelque soit les démarches suivies pour aborder un problème, on ne pourra atteindre complètement les objectifs initiaux, qui sont très variés et qu'ils ne peuvent être tous satisfaits dans notre travail. C'est pourquoi nous proposons d'élaborer une solution pour le stockage des données de la banque comme le Cloud computing.

[1] ACISSI, sécurité informatique Ethical Hacking apprendre l'attaque pour mieux se défendre, (3ème édition) Broché – 12 septembre 2012

[2] Solange Ghernouatu-Hélie, sécurité informatique et réseaux, Dunod, 2008.

[3] Jérôme Delduca, la sécurité informatique en mode projet-organisez la sécurité du SI de votre entreprise, ENI, 2010.

[4] Bruno M, la sécurité informatique CERAM, << Fondamentaux des sciences de l'information >>.

[5] Université de Nice, le livre sécuritéinfo.com, 2010.

[6] Eric Filiol, les virus informatiques, Springer Verlag, 2009.

[7] laurent Bloch, Cristoph Wolfhugel, Sécurité informatique principes et méthodes, Eyrolles, 2007.

[8] Guy Pujolle, Les réseaux locaux, Eyrolles, 2003.

[9] David Burgermeister, Les systémes de détéction d'intrusion, 2006.

[10] Guillaume Desgeorge, La sécurité des réseaux, 2000.

[11] Gary Hallen, CCNP security IPS 642-627 quick referencen Cisco presse Library of Bolvon Calin Borgdan, 2011.

[12] Pierre Jaquet, Lavoisier, Les réseaux et l'informatique de l'entreprise, 2003.

[13] FreeRadius, Serge Bonderes, Authentification réseau avec RADIUS 802.1X, EAP, Eyrolles, 2007.

[14] Roger Sanchez, Les réseaux locaux virtuels, 2006.

[15] Amakou M'BATA, Olivier PERSENT, Firewall ,pare-feux, Mur de feu, 2006.

http://www.memoireonline.com/recherche3.html

AAA	Authentification Authorization Accounting
ACE	Access Control Entry
ACL	Access Control List
AH	Authentification Heade
AIP SSM	Advanced Inspection and Prevention Security Services Module
ARP	Adress resolution protocol
ASA	Adaptive Security Appliance
ASDM	Adaptive Security Device Manager
CA	Certificate Authority
CD/DVD	Compact Disc / Digital Versatile Disc
CSC SSM	Content Security and Control Security Services Module
DDoS	Distributed Denial-of-Service a
DMZ	Demilitarized zone
DNS	Domain Name System
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GNS3	Graphical Network Simulateur
HIDS	Host Intrusion Detection System
HTTPS	Hypertext Transfer Protocol secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection Services
IIS	Internet Information Services
IOS	Inter-network Operating System
IP	Internet Protocol
IPsec	Internet Protocol Security
IPS	Intrusion Prevention Services
ISA	Internet Security and Acceleration
iSCSI	internet Small Computer System Interface

internet Small Computer System Interface

KIPS Kernel Intrusion Prevention System

LAN Local Area Network

MAC Media Access Control

MIB Management information base

NAS Network Attached Storage

NAP Network Access Protection

NAT Network Address Translation

NIDS Network Intrusion Detection System

NLB Network Load Balancing

NPS Network Policy Server

NTFS New Technology File System

OS Operating System

OSI Open Systems Interconnection

PAT Port Address Translation

PGP Pretty Good Privacy

PIX Private Internet Exchange

PKI Public-key infrastructure

PKCS Public-key Cryptography Standars

POP3 Post office Protocol version 3

PPP Protocol Point-To- Point

QOS Quality Of Service

RADIUS Remote Authentification Dial In User Service

RAID Rendundant Array of Independent Disks

RPV Réseau privé virtuel

RPF Reverse Path Forwarding

RTGS Real Time Gross System

SSH	Secure Shell
SSL	Secure Socket Layer
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
TCP	Transfer Control Protocol
Telnet	TELecommunication NETwork
TFTP	Trivial File Transfert Protocol
TMG	Threat Management Gateway
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
USM	User-based Security Module
VPN	Virtual Private Network
VLAN	Virtual Local Area Network
VACM	View Access Control Model
WAN	Wide Area Network