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 – **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 : Réseau Télécommunication

Présenté par :

M^{elle} BOUDIA Ghania

M^{elle} SALMI Dihya

Thème

Dirigé par :
M^{r} OUALOUCHE F.

Codirigé par :
M^{r} *KIBOUH M.*

Mise en place d'une infrastructure réseau sécurisé par Cloud Computing

Mémoire soutenu publiquement le 13/07/2015 devant le jury composé de :

MACA, UMMTO, Y.ATTAF

MACA, UMMTO, F.OUALLOUCHE

MACA, UMMTO, M.KIBOUH

MACB, UMMTO, L.AKROUR .ep LAHDIR

MACB, UMMTO, S.HAMEG

Promotion 2014/2015

Remerciement

Tout travail de recherche
n'est jamais totalement l'œuvre d'une seule personne.
À cet effet, je tiens à exprimer ma sincère reconnaissance et mes vifs remerciements à tous ceux qui ont contribué de près ou de loin à l'élaboration de ce travail ;

- *Tout d'abord à mon promoteur* ***Ouallouche F.*** *pour l'aide et le temps qu'il a bien voulu me consacrer*
  et que je ne remercierai jamais assez
  Pour son soutien et sa patience, qu'il trouve en ces lignes l'expression de ma gratitude ;
- *Je tien à remercier profondément mes encadreurs*
- *Mes sincères remerciements au DIRECTEUR DE L'ECOLE 2int*
  pour la chance qui m'ont accordé de m'accepter stagiaire au niveau de son Ecole;
- *J'adresse encore mes plus sincères remerciements à tous mes enseignants*
- *Merci à Dieu de m'avoir donné la force, la puissance et le courage de tenir jusqu'à la fin de ce travail.*

Dédicaces

J'ai l'honneur de dédier ce modeste travail à :

- *Mes chers parents ;*
- *Mes sœurs : Sabrina, fatma, Wissam ;*
- *Mes frères : Koceila et Yacine ;*
- *Mes chers amis : dihya, Lili, yasmine, lynda, Sabrina.*

Ghania

Dédicaces

J'ai l'honneur de dédier ce modeste travail à :

- *Mes très chers parents que j'aime;*
- *Ma sœur : Maya*
- *Mes frères : Ghiles, Lyes*
- *Tout le reste de ma famille que j'aime(Mouh,Belkacem,FarizaRazika ,Mahdjouba…)*
- *Mon mari que j'aime*
- *Toute ma belle famille (Ellissa, Zina …)*
- *Mes vrais amis (Ghania, Khadra, Ziri, Faroudja…)*

Dihya

Sommaire

Sommaire

Liste des Tableaux

Liste des Figures

Introduction

Le réseau informatique est un système de mise en commun de l'information entre plusieurs machines. Un réseau peut ainsi relier au moyen d'équipements de communication appropriés, des ordinateurs, des terminaux et des périphériques divers tels que des imprimantes et des serveurs.Face àl'augmentation continue des systèmes informatiques, les entreprises exploitent beaucoup d'informations, ce qui nécessite une meilleure organisation de ces dernières. L'outil informatique joue donc un rôle primordial sur ce plan pour facilité la transmission de ces données informatisée.

À une époque où communication et technologie sont les maîtres mots de notre société, on ne peut douter que l'avenir des réseaux informatiques soit de grandir et de se développer. Cet avenir est pour une bonne partie lié aux techniques et aux supports de communication utilisés dans les réseaux. De plus, la technologie actuelle permet d'accroître les volumes et les débits de transfert de données tout en diminuant les coûts. Les interconnexions des réseaux sont variéeset pratiquement tous se trouvent aujourd'hui imbriqués les uns dans les autres.

L'intégration des réseaux locaux et grande distance dans le système d'information et de communication de l'entreprise a conduit au concept de réseau d'entreprise, dans lequel l'utilisateur a accès à toutes les ressources informatiques, grâce à une réelle distribution des applications. La connexion du réseau d'entreprise au réseau Internet a rendu l'ensemble de ses ordinateurs vulnérables aux intrusions et aux risques d'attaques informatiques.

Par conséquent, l'entreprise doit adopter des procédures de sécurité qui est un sujet primordial vu l'importance des informations qui sont souvent véhiculées dans les réseaux. Cette sécurité doit identifier de manière claire et non-ambigüe les objectifs à assurer, ainsi que les règles de sécurité qui régissent la manière dont les ressources sont utilisées pour protéger le système. Une politique de sécurité repose sur l'utilisation de plusieurs techniques, telles que le firewall, IPS (IntrusionPreventionSystem)IDS (IntrusionDetection System). [1]

Dans ce mémoire nous décrivons une solution de sécurité qui est l'utilisation du Cloud Computing. Cette dernière est appliquée au réseau de l'école de formation 2INT. Ainsi, nous avons optés pour une mise en place d'une architecture réseau sécurisé pour que l'accessibilité à l'information soit immédiate à n'importe quel moment et n'importe quel endroit.

Nous avons organisés ce mémoire en quatre chapitres.

Dans Le premier nous allons présenter les généralités sur le réseau et la sécurité informatiques.

Dans le deuxième chapitre, nous expliquerons les notions fondamentales sur le Cloud Computing.

Dans le troisième chapitre, nous décrivons l'architecture réseau actuelle du l'école 2INT suivi des failles de sécurités constatées et nous proposons des solutionsà ces failles.

Le quatrième chapitre sera consacré à la mise en place d'une infrastructure Cloud Computing dans le cas de l'école 2INT.

Enfin, nous terminons notre mémoire par une conclusion et une bibliographie.

Chapitre I

Généralités sur le réseau et la sécurité informatique

1. Préambule :

Avant l'apparition des réseaux informatiques, la transmission des données entre ordinateurs était difficile. Aujourd'hui, avec l'évolution de la technologie les réseaux sont omniprésents et nous pouvons partager des applications, échanger des informations, consulter des bases de données et effectuer des transferts de fichiers entre plusieurs postes à distance. Toutes ces applications sont possibles grâces aux réseaux informatiques nées du besoin de faire communiqué des terminaux distants avec un site central, des ordinateurs entre eux et des stations de travail avec leursserveurs.

2. Généralité sur les réseaux informatique :

2.1. Définition

Un réseau est un ensemble d'objets interconnectés les uns avec les autres. Il permet de faire circuler des données entre chacun de ces objets selon des règles bien définies.

2.2. Intérêt d'un réseau :

Un ordinateur est une machine permettant de manipuler des données. L'homme, un être de communication, a vite compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre eux afin de pouvoir échanger des informations. Voici un certain nombre de raisons pour lesquelles un réseauestutile:

Un réseau permet:

- Le partage de fichiers, d'applications
- La communication entre personnes
- La communication entre processus (entre des machines industrielles)
- La garantie de l'unicité de l'information (bases de données)
- Partage de ressources [1]

2.3.Classification des réseaux informatique : On distingue deux niveaux de classification : suivant la taille et selon le type.

2.3.1.Classification selon la taille : Les réseaux sont divisés en trois grandes familles : les LAN, MAN, WAN.

a) **Le réseau LAN :Local Area Network :**Les réseaux locaux connectent plusieurs ordinateurs situés dans une zone géographique relativement restreinte, tels qu'un domicile, un bureau, un bâtiment, un campus universitaire.

   Ils permettent aussi aux entreprises de partager localement des fichiers et des imprimantes de manière efficace et rendent possible les communications interne.

b) **Le réseau MAN : Métropolitain Area Network :** le man peu couvrir une grande zonegéographique tell qu' un grand campus ou une ville.

c) **Le réseau WAN : (Wide area network):**Pour des raisons économiques et techniques, les réseaux locaux (LAN) ne sont pas adaptés aux communications couvrant de longues distances.

C'est pour toutes ces raisons que les technologies des réseaux étendus(WAN) différent de celle des réseaux locaux. Un WAN est un réseau a longue distance qui couvre une zone géographique importante (un pays, voir même un continent)

2.3.2. Classification selon le mode de communication :

On distingue généralement deux types de réseaux :

a) Réseaux organisés autour de serveurs (Client/Serveur)

b) Les réseaux poste à poste (peer to peer / égal à égal)

Ces deux types de réseau ont des capacités différentes. Le type de réseau à installer dépend des critères suivants :

- Taille de l'entreprise
- Niveau de sécurité nécessaire
- Niveau de compétence d'administration disponible
- Volume du trafic sur le réseau
- Besoins des utilisateurs du réseau

a) **Le réseau client serveur :**

Un client est un système (programme ou ordinateur) Accédant à des ressources éloignées, en se branchant via un réseau informatique sur un serveur.

Un serveur est un ordinateur détenant des ressources particulières et qu'il met à la disposition d'autres ordinateurs par l'intermédiaire d'un réseau.

L'interaction entre client et serveur conduit à l'architecture client serveur. En effet l'architecture client serveur désigne un mode de communication entre plusieurs ordinateurs d'un

réseau qui distingue un ou plusieurs postes serveur. La communication se réalise par le dialogue entre processus deux à deux. En d'autres termes c'est les clients qui demandent les informations dont ils ont besoin au serveur.

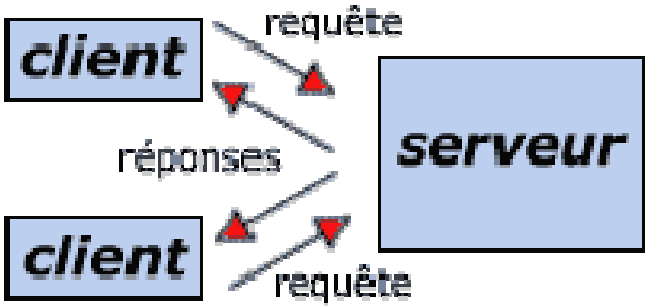


Figure 1 : réseau client serveur

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

c) Le réseau poste à poste (peer to peer) :

Dans une architecture poste à poste (peer to peer), contrairement à une architecture de réseau de type client/serveur, il n'ya pas de serveur dédié. Il est à la fois client/serveur, Cela signifie que chacun des ordinateurs du réseau est libre de partager ses ressources. [2]

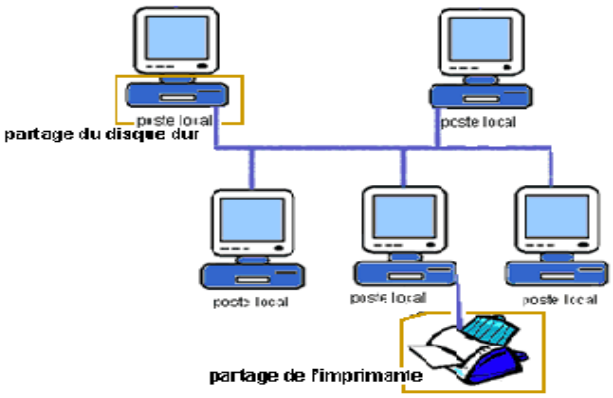


Figure 2 : réseau poste à poste

2.3.3. Classification selon la Topologie :

Un réseau informatique est constitué d'ordinateur relier entre eux grâce à des lignes de communication (câble réseau) et des éléments matériels (carte réseau), la configuration spatiale de réseau est appelé **Topologie physique**, on distingue généralement les topologies suivantes :

- topologie en bus.
- Topologie en étoile.
- Topologie en anneau.

d) Topologie en bus :

Est une variante de la liaison multipoint. Dans ce mode de liaison, l'information émise par une station est diffusée sur tout le réseau. Dans ce type de topologie, chaque station accède directement au réseau, d'où des problèmes de conflit d'accès qui nécessitent de définir une politique d'accès.

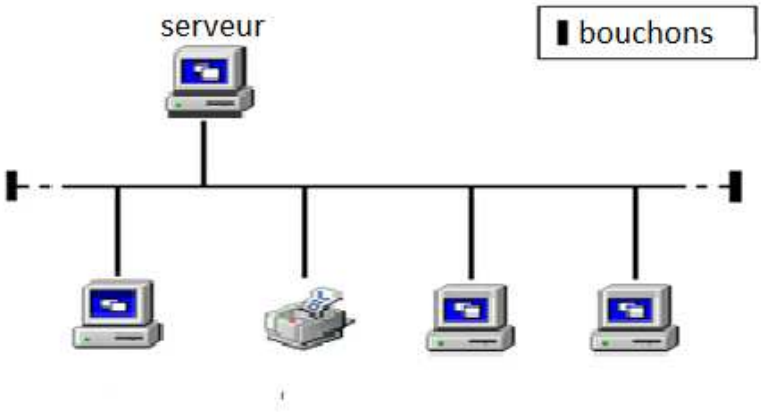


Figure 3 : topologie en bus

e) Topologie en étoile :

Est une variante de la topologie en point à point. Un nœud central émule n liaisons point à point tous les nœuds du réseau sont reliés à un nœud central commun : le concentrateur. Tous les messages transitent par ce point central. Le concentrateur est actif, il examine chaque message reçu et ne le retransmet qu'à son destinataire. Cette topologie correspond, par exemple au réseau téléphonique privé d'une entreprise. La topologie étoile autorise des dialogues entre nœuds très performants.

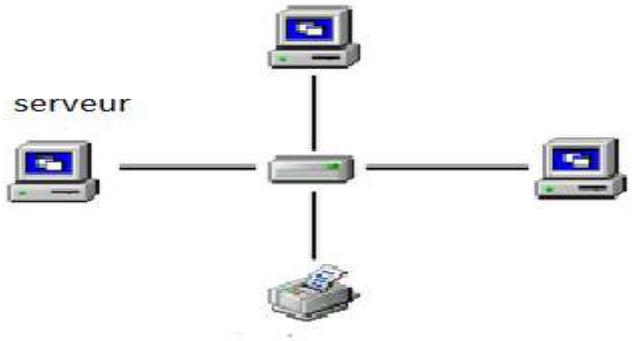


Figure 4: Topologie en étoile

f) Topologie en anneau :

Dans cette topologie chaque poste est connecté au niveau en point à point l'information circule dans un seul sens, chaque station reçoit le message et le régénére.si le message lui est destiné, la station le recopie au passage. Ce type de connexion autorise des débits élevés et convient aux grandes distances.

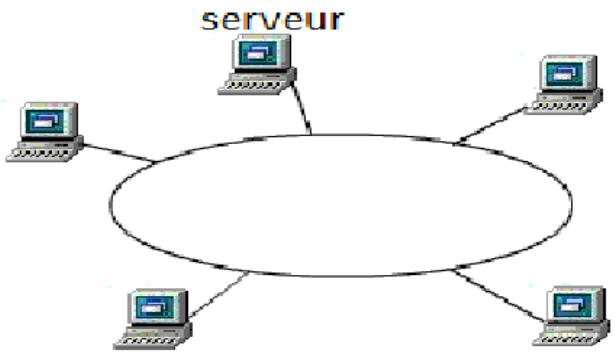


Figure 5 : Topologie en anneau

g) Topologie logique:

Par opposition à la topologie physique, représente la façon dont les données transitent dans les lignes de communication. [3]

3. La communication sur un réseau :

Définition d'un protocole :

Un protocole de communication est un ensemble de règles et de procédures permettant de définir un type de communication particulier. Les protocoles sont hiérarchisés en couches, pour décomposer et ordonner les différentes tâches. Il existe plusieurs familles de protocoles ou modèles, chaque modèle étant une suite de protocoles. Parmi ces modèles on trouve l'OSI et le TCP/IP.

3.1. Le modèle OSI (Open System Interconnections):

Le modèle de référence, également appelé modèle OSI (Open System Interconnections), est un modèle théorique conçu dans les années 1980 pour permettre l'interconnections de systèmes de communication ouverts hétérogènes. Pour faciliter cette interconnexion, un modèle dit d'interconnexion des systèmes l'informatique. Il constitue aujourd'hui le socle de référence pour tous les systèmes de traitement de l'information. Chaque couche regroupe des ouverts, appelé encore OSI (Open Systems Interconnections) a été défini par l'ISO (International Standards Organisation). Le modèle OSI répartit les protocoles utilisés selon sept couches, définissant ainsi un langage commun pour le monde des télécommunications et de dispositifs matériels (dans les couches basses) ou logiciels (dans les couches hautes). Entre couches consécutives sont définies des interfaces sous forme de primitives de service et d'unités de données rassemblant les informations à transmettre.

Modèle OSI	
Niveau	**Couche**
Niveau 7	Couche application
Niveau6	Couche présentation
Niveau5	Couche session
Niveau4	Couche transport
Niveau3	Couche réseau
Niveau2	Couche liaison de données
Niveau1	Couche physique

Tableau 1 : Modèle OSI

❖ Les rôles des différentes couches sont les suivants :

- **Couche 1 : Physique**

La couche physique rassemble les moyens électriques, mécaniques, optiques ou hertziens par lesquels les informations sont transmises. Les unités de données sont donc des bits 0 ou 1

- **Couche 2 : Liaison de données**

La couche liaison gère la fiabilité du transfert de bits d'un nœud à l'autre du réseau, comprenant entre autres les dispositifs de détection et de correction d'erreurs, ainsi que les systèmes de partage des supports. L'unité de données à ce niveau est appelée trame.

- **Couche 3 : Réseau**

La couche réseau aiguille les données à travers un réseau à commutation. L'unité de données s'appelle en général un paquet.

- **Couche 4 : transport**

La couche transport regroupe les règles de fonctionnement de bout en bout, assurant ainsi la transparence du réseau vis-à-vis des couches Supérieures. Elle traite notamment l'adressage, l'établissement des connexions et la fiabilité du transport.

- **Couche 5 : session**

La couche session réunit les procédures de dialogue entre les applications : établissement et interruption de la communication, cohérence et synchronisation des opérations.

- **Couche 6 : présentation**

La couche présentation traite les formes de représentation des données, permettant traduction entre machines différentes

- **Couche 7 : application**

Source et destination de toutes les informations à transporter, la couche application rassemble toutes les applications qui ont besoin de communiquer par le réseau : messagerie électronique, transfert de fichiers, gestionnaire de bases de données.

3.2. Le modèle TCP/IP (transfert contrôle protocole / internet protocole) :

Le modèle TCP/IP reprend l'approche modulaire du modèle OSI (utilisation de modèle ou de couche) mais ne contiens, lui, que quatre couche.ces couches ont des taches beaucoup plus diverses étant donné qu'elles correspondent à plusieurs couches du modèle OSI

❖ Les rôles des différentes couches sous les suivants :

h) La couche application : elle englobe l'application standard du réseau (Telnet, SMTP, FTP…).

i) La couche transport : elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaitre l'état de la transmission.

j) La couche internet : elle est chargée de fournir les paquets de données.

k) La couche accès réseau : spécifie la forme sous laquelle les données doivent être acheminées quelque soit le type de réseau utilisé. [4]

Niveau	Modèle TCP/IP	Modèle OSI	Protocole TCP/IP
Niveau4	Couche Application	Couche Application	Telnet
		Couche présentation	
		Couche session	
Niveau3	Couche transport (TCP/IP)	Couche transport	TCP ou UDP
Niveau2	Couche internet(IP)	Couche réseau	IP
Niveau1	Couche Accès réseau	Couche liaison	PPP,Ethernet
		Couche physique	

Tableau 2 : Modèle TCP/IP

4. Sécurité informatique :

Les attaques informatiques ne cessent d'être dirigées contre l'entreprise, petite ou grande 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.

4.1. Définition de la sécurité informatique :

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

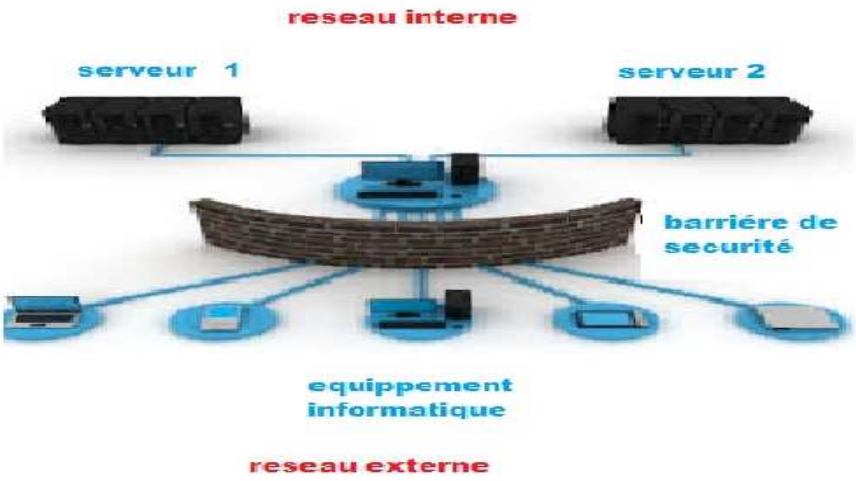


Figure 6 : Conceptde sécurité

4.2.Les critères de la sécurité.

4.2.1. 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 (altérationtotale) 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 contribuerà préserver son intégrité, permettra de la protéger plus ou moins efficacement contre une menacede corruption ou de destruction.

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

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

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

4.2.4. Authentification: doit permettre de vérifier l'identité d'une entité pour pouvoir assurer son authentification, ainsi seules les personnes autorisées auront accès aux ressources. [5]

5. Politique de sécurité

5.1. Définition

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

Une politique de sécurité est donc un document confidentiel qui en faisant abstraction des contingences matérielles et techniques fournit une collection de directives de sécurité classées parthèmes.

6. Les types de menaces :

a)Menaces accidentelles: ce sont celles qui existent sans qu'il y ait préméditation, exemples,défaillance de systèmes, bévues opérationnelles et bugs dans les logiciels.

b)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 les systèmes et avec lesquelles ni le fonctionnement, ni l'état du système ne change.

-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

.

7. Les types d'attaques

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

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.

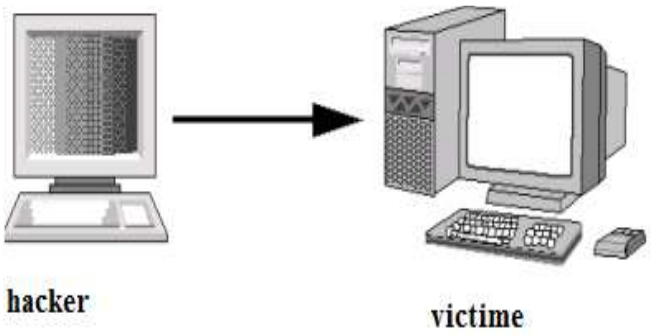


Figure 7 : Attaque directe.

b) Les attaques indirectes par rebond

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

- Masquer l'identité (l'adresse IP) du hacker.
- Utiliser éventuellement les ressources de l'ordinateur intermédiaire car il est pluspuissant 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 8 : 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 pointde vue du hacker, mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il larépercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va êtreenvoyée à l'ordinatrice victime. [6]

8. Les techniques d'attaques :

a)**Les attaque réseaux :**

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

Usurpation d'adresse IP

L'usurpation d'adresse IP (IP spoofing) est une technique qui consiste à envoyer des paquetsIP 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.

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.

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.

b) Les attaques applicatives :

Les attaques applicatives se basent sur des failles dans les programmes utilisés, ou des erreurs de configuration.

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.

Figure9: Attaque Man in the middle.

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.

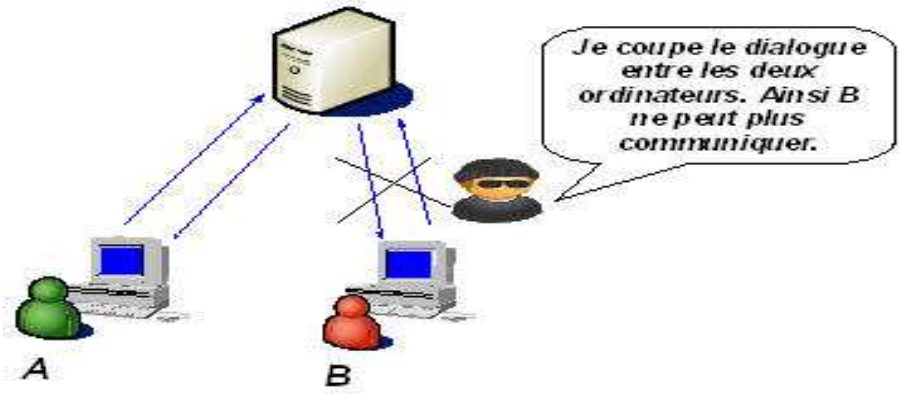


Figure 10 : Attaque Déni de service

c)Attaques de mots de passe : Il existe des moyens permettant aux pirates 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'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.

d) 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 desprogrammes et données utilisant un langage de script. Lors de l'accès à ces derniers, le code duvirus s'exécutera de façon d'abord silencieuse (phase de multiplication pendant laquelle il infecterad'autres fichiers) puis visible (activation de la fonction nocive).

e) Le cheval de Troie :le terme désigne à peu près toutprogramme qui s'installe de façon frauduleuse (souvent par le biais d'un mail ou d'une page webpiégés) pour remplir une tâche hostile à l'insu de l'utilisateur.

f) Un ver : Un ver est un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant unréseau informatique. Contrairement à un virus informatique, un ver n'a pas besoin d'un programmehôte pour se reproduire, il exploite les différentes ressources de l'ordinateur qui l'héberge pourassurer sa reproduction.

9. Les protocoles de sécurité

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 desécurité élevé. La sécurisation se faisant au niveau IP, IPSec peut être mis en œuvre sur tous leséquipements du réseau et fournir un moyen de protection unique pour les échanges de données..

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 protocole SSH

Le SSH (Secure Shell) permet de répondre à la principale problématique posée par la sécuritédes informations, la confidentialité. En effet, grâce à ce protocole, il est possible de chiffrer desdonnées par un système de clés privées et publiques. Ces données transitent dans un tunnel, unesorte de canal sécurisé où il est impossible de savoir ce qui se passe à l'intérieur. [7]

10. 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.

Chapitre II

Etude du Cloud Computing

1. Préambule :

Le Cloud Computing est un système de stockage de données. Celles-ci ne sont pas stockées physiquement sur le disque dur de l'ordinateur mais sur des serveurs distants. Ces machines sont généralement situées dans des endroits appelé « Data Center»

Au centre du système d'information, le Datacenter concentre les données et les traitements informatiques. En effet, le lieu d'hébergement des données est généralement multiple, et réparti sur plusieurs Datacenter. Il est donc un espace aménagé et sécurisé pour abriter, traiter et protéger les données.

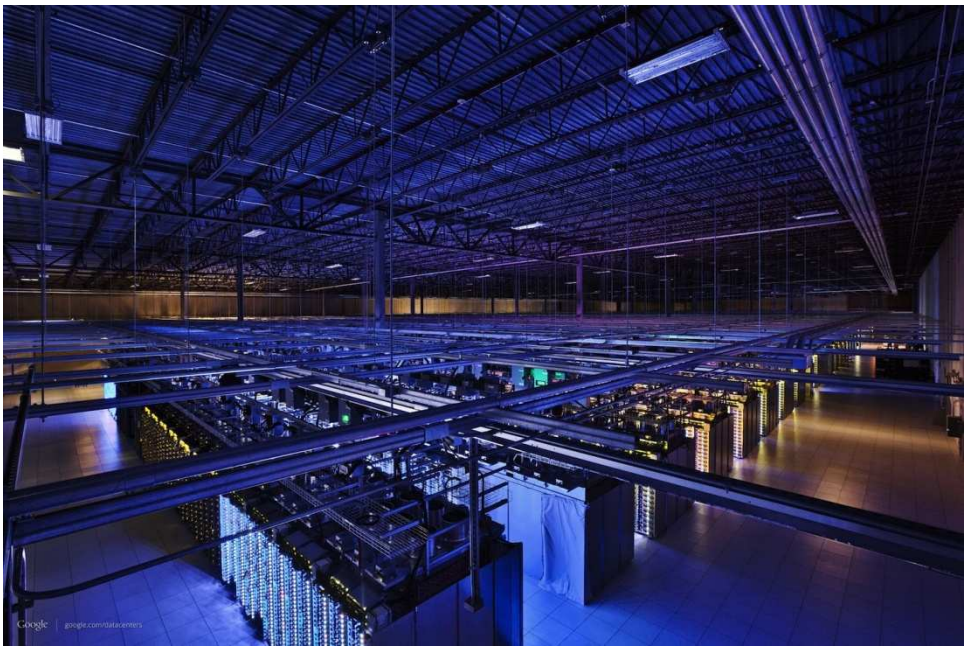


Figure 11 : Datacenter

2. LaVirtualisation :

La virtualisation est une technique qui permet de partager et d'utiliser les ressources à partird'un seul système informatique composé de plusieurs machines virtuelles. Chaque machine virtuellefournit un système informatique complet très semblable à une machine physique. Ainsi, chaque

machine virtuelle peut avoir son propre système d'exploitation, applications et services réseau. [8]

2.1. Les avantages de la virtualisation :

✓ La sécurité et la fiabilité ***:*** isoler les services sur des serveurs différents

- ✓ la réduction des coûts.
- ✓ Disponibilité **:** Si l'und'eux tombe en panne, les autres sont présents afin d'assurer une haute disponibilité.[9]

3. Définitionsdu Cloud Computing :

Il s'agit de la dématérialisation de l'informatique c'est-à-dire déporter toutes les opérations normalement effectuer sur nos ordinateurs sur des serveurs à distance autrement dit sur internet, L'ensemble de ses serveurs constituent le Cloud.

Figure 12: CloudComputing

3.1.Les différentes couches de service du Cloud :

Le CloudComputing peut être décomposé en trois couches :

a) Application (**SaaS**, Software as a Service)
b) Platform (**PaaS**, Platform as a Service)
c) Infrastructure (**IaaS**, Infrastructure as a Service)

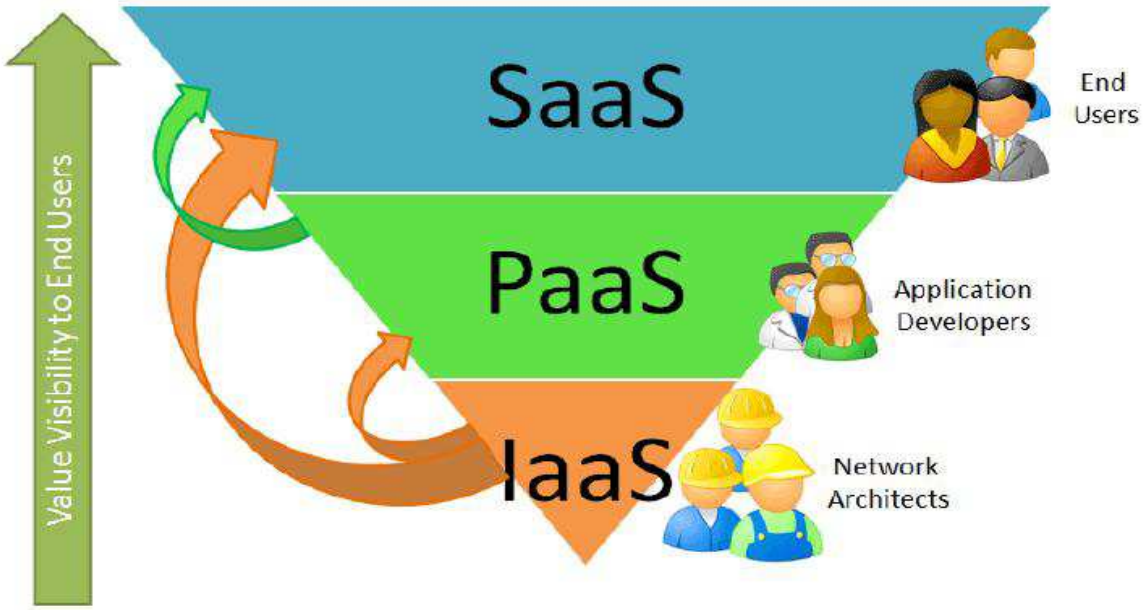


Figure 13: Les couches du Cloud Computing

a) couche Infrastructure en tant que service:« *Infrastructure as a Service* » ou «*IaaS*» :

Fournit une infrastructure qui va servir à développer des solutions Cloud Computing. Il peut s'agir d'un hébergeur de site web, une entreprise qui va se charger de faire fonctionner le site pendant que le propriétaire du site se chargera du contenu.

b) couche Plateforme en tant que service : « *Platform as a Service* » ou « *PaaS*» :

Fournit une plateforme logicielle qui va servir à développer une solution CloudComputing. Par exemple, un serveur d'application web que l'on aurait porté sur le Cloud.

c) couche Logiciel en tant que service : « *Software as a Service* » ou « *SaaS*» :

Fournit un logiciel à la demande mais ce dernier reste sur le Cloud. Par exemple, on peut mettre une suite bureautique sur le Cloud. [10]

3.2.Modèles de déploiement :

a) Cloud public : Il appartient à des prestataires de service qui loue l'utilisation de leurs serveurs ces services sont mis à la disposition du grand public par intermédiaire d'Internet.

b) Cloud Privé : Il est propre a l'entreprise,à l'aide de la virtualisation il est possible de transformer les serveurs existant au sein de l'entreprise cela crée un réseau puissant comme le Cloud public mais gérer entièrement par l'entreprise.

c)Cloud hybride : C'est un mélange des deux précédents, le public louer par des prestataires de services et le privé crée et gérer par l'entreprise. [11]

3.3.Les caractéristiques du Cloud Computing:

Le Cloud Computing permet :

- Un accès libre et ouvert au client, qui peut établir sa connexion de n'importe où et avoir accès à ses données immédiatement. (Grande flexibilité).

-Un coût qui évolue selon les besoins des utilisateurs (payer selon la consommation).

-La mémoire n'est plus limitée contrairement au disque dur physique.

-Les données du Cloud sont dupliquées automatiquement en cas de perte de ses dernières.

3.4. Sécurité dans le Cloud Computing :

Même si les avantages sont beaucoup plus importants que les inconvénients il faut prendre les mesures de sécurité suivantes :

- On élimine le risque de perte de données en ligne en sauvegardant des copies.
- On accède aux données avec des mots de passe et des identifiants.
- On réduit l'utilisation des ordinateurs publics.
- On choisit des connexions fiables et sécurisé.
- Il faut choisir un prestataire de services adéquat. [12]

Discussion :

Le Cloud permet d'améliorer la sécurité des données : fini la perte de clé USB ou de PC contenant des informations confidentielles. Tout est centralisé et sécurisé par authentification de l'utilisateur.

Chapitre III

l'étude de l'nfrastructure Existante

1. Préambule

Les types de menaces qui s'attaquent auréseau informatique sont extrêmement variés. Heureusement, différentes solutions de sécuritépermettent aux entreprises de bien se protéger.

La sécurité doit être envisagée dès la conception de la structure réseau informatique de l'entreprise. L'analyse et la mise en place de solutions sont incontournables car lacybercriminalité augmente.

Toute entreprise existante d'une certaine taille dispose en général d'un réseau informatique, même celles qui n'en sont qu'à une idée de projet viable y pense très souvent à une éventuelle mise en ouvred'un réseau informatique au sein de leur structure. Mais la plus part de ces entreprises ignorent l'importance de définir une politique de sécurité avant la mise en place de leur réseau et l'étude suivante en est la preuve.

Dans ce chapitre, nous allons effectuer une critique de l'infrastructure existante et ressortir la problématique qui nous a conduits à mener ce travail et à proposer la solution qui est la nôtre.

2.Architecture du réseau de l'école 2INT:

Dans notre démarche, il sera donc question de présenter dans un premier temps une architecture réseau existante pour laquellenousproposerons des améliorations et nous implémenterons une sécurité adéquate.

L'étude de l'existant, point clé de notre démarche, c'est une étape essentielle qui vise à représenter l'architecture de notre travail. Nous porterons une attention particulière sur le service où sera implémentée notre solution.

❖ Cette architecture illustre l'architecture de l'existant :

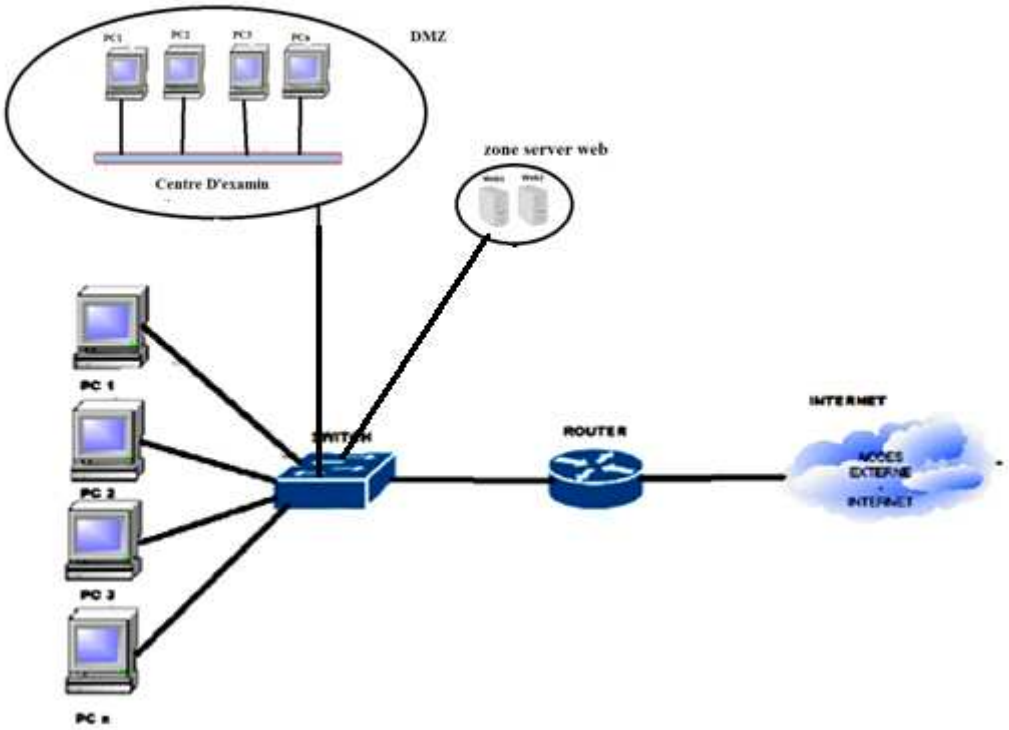


Figure 14 : Architecture réseau de l'école 2int.

Nous avons plusieurs ordinateurs interconnectés entre eux formant un réseau local, puis connecté à l'aide de routeurs à un réseau externe (internet) et des sous réseau DMZ ,serveur Web.

3. Critiques existante dans cette architecture :

Une analyse du réseau de l'entreprise, nous a permis de définir un nombre de contraintes pouvant réduire ces performance voir même sa dégradation, certaine de ces contraintes peuvent être un obstacle à la réalisation de la mission de cette entreprise.

3.1. Coté architecture réseau :

a) Pas de sécurité de firewall qui résiste à l'attaque réseau.

b) Manque d'IPS pour anti intrusion.

c) Problèmes de sauvegardes :

Si la plupart des systèmes de stockage en ligne (Cloud) proposent des sauvegardes, les données situées sur votre poste de bureau sont souvent conservées sur un seul disque.

d) Une seule ligne internet qui est insuffisante car avec un seul provider le trafic augmente et la connexion s'affaiblit se qui posera de divers problèmes a l'entreprise.

3.2. Du coté système :

- Mots de passe faibles : les routeurs son protégés par des mots de passe faibles comme « Cisco » les intrus auront ainsi de diverses options qui leur permettront de causer des dommages et d'interrompre les activités.
- Manque de disponibilité de données :Le système doit fonctionner sans faille durant les plages d'utilisation prévues, et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.

4. Solution apporté à notre architecture :

D'après l'étude faite sur l'existant dans notre entreprise on a constaté de nombreuses défaillances coté architecture et coté système qui font de l'entreprise une cible idéal pour les hackers et c'est pour cette raison que nous avons apportées quelques modifications appropriés pour optimiser la sécurité de cette dernière puis nous avons procédé comme suit :

a) Compléter l'architecture existante avec deux firewalls suivis d'IPS pour renforcer la sécurité du réseau interne.

1. Pare-feu (informatique) : Un pare-feu (coupe-feu, garde-barrière en l'anglaisfirewall), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet).

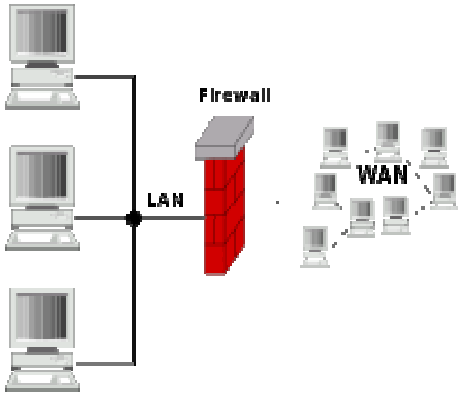


Figure 15: description de pare-feu

2.L'ajout d'IPS: Il est également plus possible de contenir les intrusions à quelques points du réseau. Prévention des intrusions est nécessaire tout au long de l'ensemble du réseau pour détecter et arrêter une attaque sur tous les points entrant et sortant.

b)Insertion d'un deuxième provider en cas d'interruption de l'autre.Tell que **« Algérie Télécom »**

c)Sécurisation des accès aux équipements réseau (Router et Switch) avec le renforcement des mots de passe

e)Récupération des données :Lorsque les entreprises commencent à s'appuyer sur les services du Cloud Computing, elles n'ont plus besoin de programmes complexes de récupération des données. Les fournisseurs de Cloud Computing se chargent de la plupart de ces tâches et ils le font plus vite.

- Cette figure illustre la nouvelle architecture :

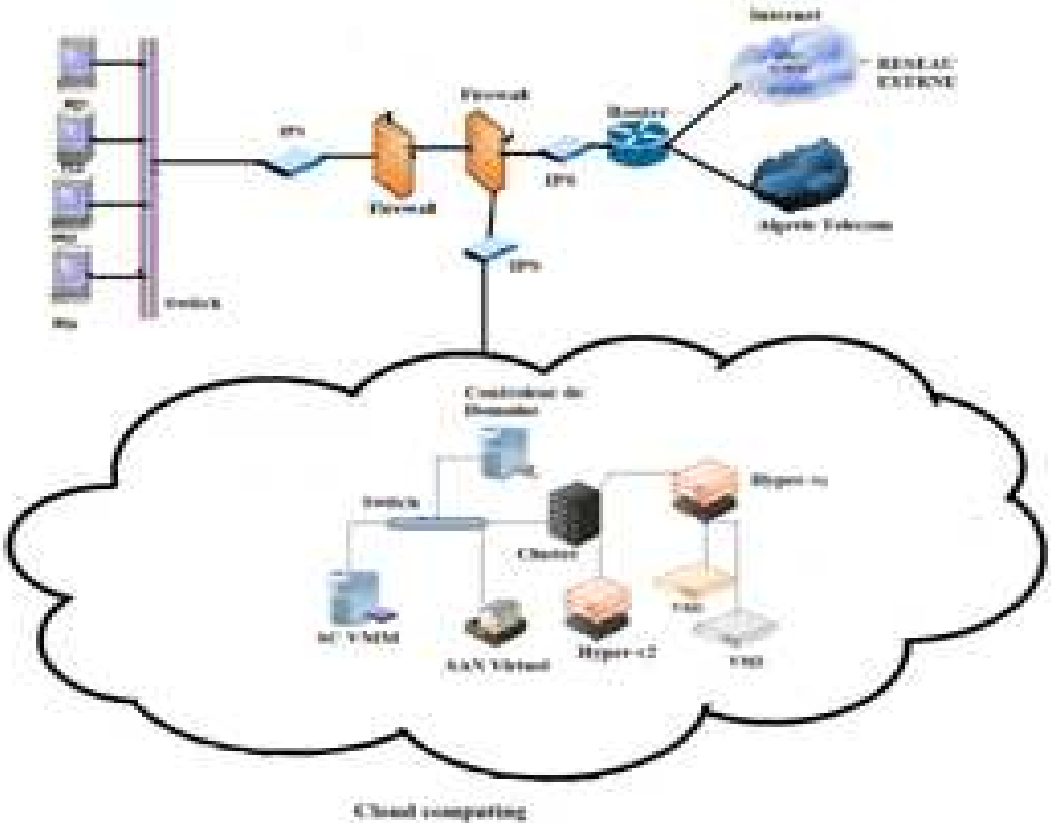


Figure 16 : Nouvelle architecture de l'existant

- **Définition des éléments du Cloud :**

1**)VM :** En informatique, une machine virtuelle (anglais virtual machine) est une illusion d'un appareil informatique créée par un logiciel d'émulation. Le logiciel d'émulation simule la présence de ressources matérielles et logicielles telles que la mémoire, le processeur, le disque dur, voire le système d'exploitation et les pilotes, permettant d'exécuter des programmes dans les mêmes conditions que celles de la machine simulée. Les machines virtuelles sont également utilisées pour isoler des applications pour des raisons de sécurité, pour augmenter la robustesse d'un serveur en limitant l'impact des erreurs système ou pour émuler plusieurs machines sur une seule machine physique (virtualisation).

2)**SCVMM** (system center Virtuel machine manager):est utilisé Pour la gestion centralisé des machines Virtuel

3)**Hyper V1 :** outil de vitalisation des machines Virtuel (pour crée plusieurs machines virtuel)

4)**HyperV2 :** L'ajout de HyperV2 supplémentaires permet de fournir une tolérance aux pannes.

5**)Cluster :** est aussi utilisé pour la tolérance aux pannes.

6**)SAN Virtuel** :en informatique, un réseau de stockage, ou SAN (de l'anglaisstorageareanetwork), est un réseau spécialisé permettant de mutualiser des ressources de stockage(pour la gestion centralisé de stockage).

7)**Contrôleur de domaine :** c'est une machine sur la qu'il on a installé le nom de domaine, Les contrôleurs de domaine stockent les données et gèrent les interactions entre l'utilisateur et le domaine, y compris les processus d'ouverture de session, l'authentification et les recherches dans l'annuaire. Si vous envisagez d'utiliser ce serveur pour fournir le service d'annuaire Active Directory aux utilisateurs et aux ordinateurs du réseau, Créez des contrôleurs de domaine supplémentaires lorsque vous voulez améliorer la disponibilité et la fiabilité des services réseau. L'ajout de contrôleurs de domaine supplémentaires permet de fournir une tolérance de pannes, d'équilibrer la charge des contrôleurs de domaine existants, de fournir une prise en charge supplémentaire de l'infrastructure aux sites et d'améliorer les performances en simplifiant la connexion des clients à un contrôleur de domaine lorsqu'ils ouvrent une session sur le réseau.

Discussion :

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

Donc nous avons proposé des solutions qui permettront depallier ces différentes vulnérabilités.

Chapitre VI

Mise en oeuvre de la solution proposéé

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 par fun ou pour usurper des données et informations confidentielles.

Dans cette solution nous essaierons de minimiser au maximum les risques d'attaques et les points vulnérables de l'école 2int en accordant aux différents administrateurs la responsabilité de sensibiliser les membres de l'entreprise au secret professionnel.

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

2. Les étapes suivies pour la mise en place de notre application :

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

Les étapes : la préparation des machines

Nous avons préparé les machines suivantes :

- Un contrôleur de domaine principal.
- Un serveur membre pour l'installation de la TMG.
- Deux machine pour l'installation hyperv1 et hyper v2
- Deux machines membres pour l'implémentation de la solution failover.
- Une machine membre pour l'installation system center Virtual machine manager

Microsoft Windows Server 2012

Microsoft Windows Server 2012, anciennement connu sous le nom de code Windows Server 8, est la dernière version du système d'exploitation réseau Windows Server.

Il s'agit de la version serveur de Windows 8 et du successeur de Windows Server 2008 R2.

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.

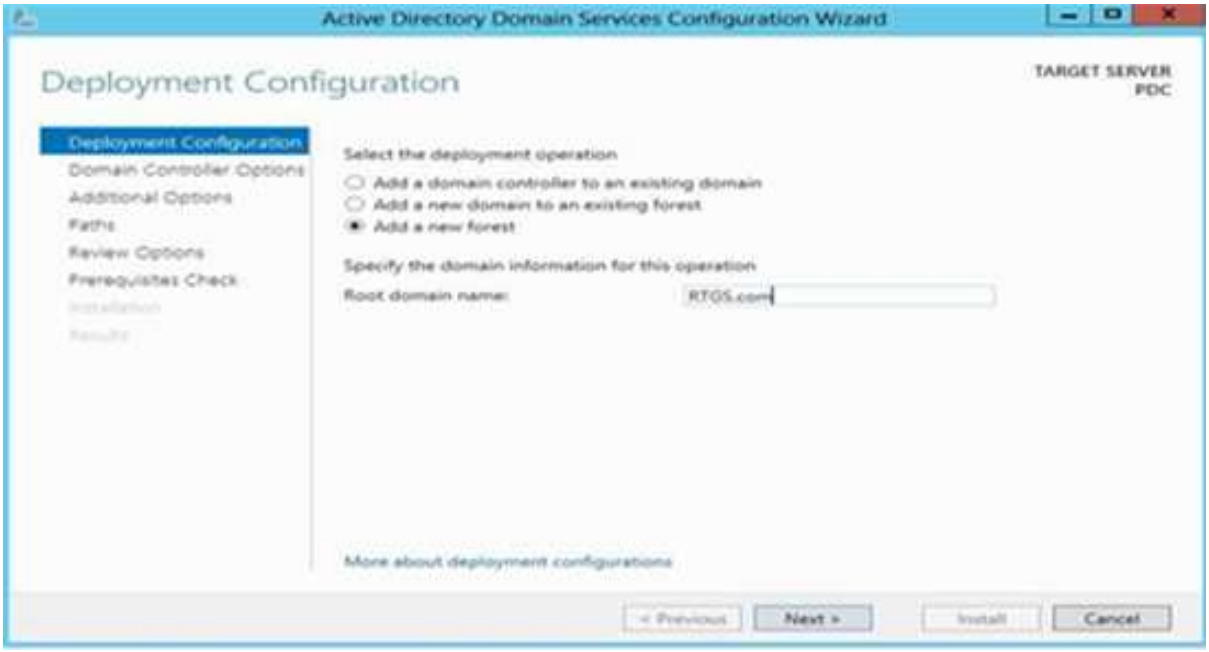
3. L'installation du contrôleur de domaine principale et secondaire

Windows Server 2012: Active Directory Domain Services

Active Directory est la base d'un réseau Microsoft. Il permet la gestion des ressources : utilisateurs et périphériques, l'authentification et la sécurisation des accès.

Après préparation de deux machines virtuelles Windows Server 2012, nous avons installé sur la première machine un contrôleur de domaine principal (PDC), 2int.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.

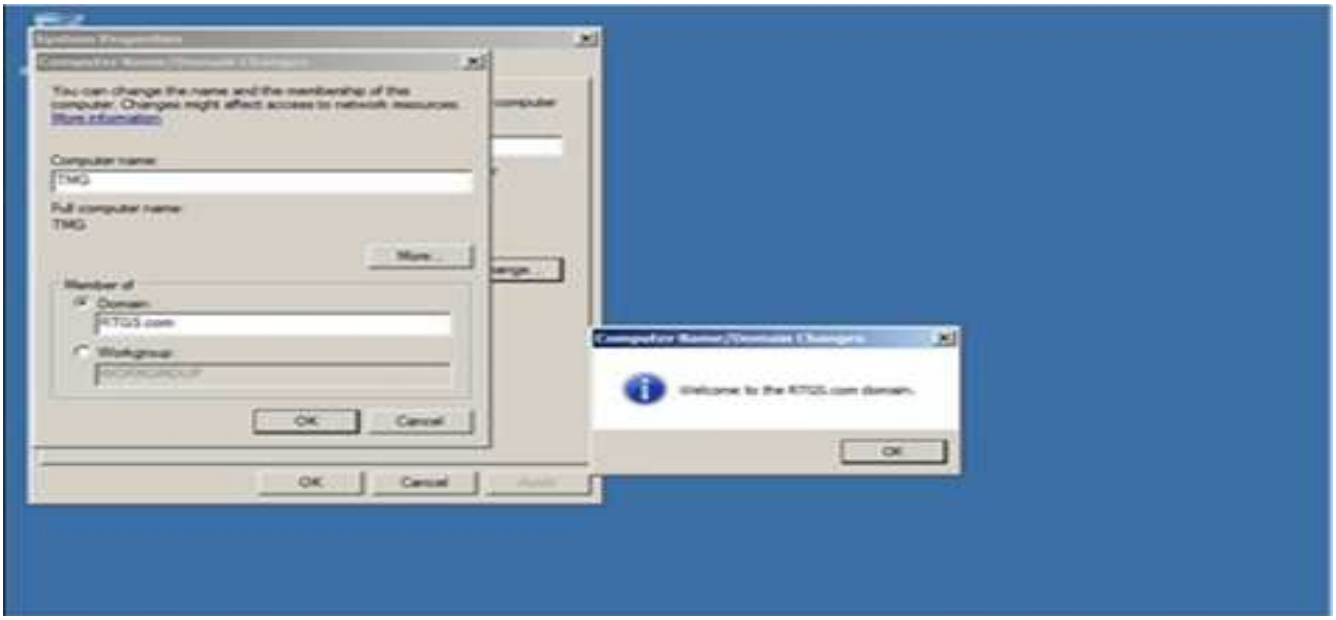
L'installation des deux contrôleurs est la même à la différence du choix de l'étape montrée ci-dessous. La première figure montre le choix de la création d'un nouveau domaine principal et la deuxième l'installation d'un contrôleur de domaine secondaire.



La création du domaine principal.

L'ajout d'un serveur ou machine membre

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



Ajout de la TMG au domaine 2int.com.

4. L'installation et configuration de la TMG :

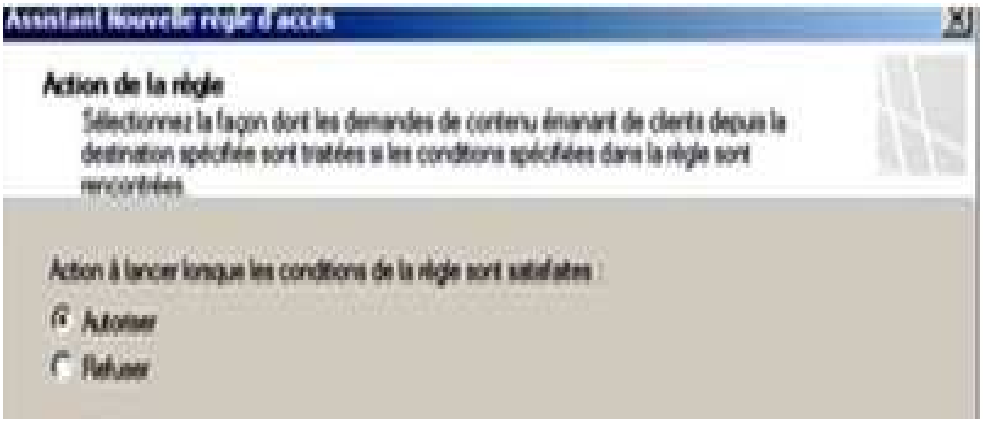
Pour éviter tout problème pendant l'installation de Forefront TMG 2010, avant de commencer,nous avons pris en compte les conditions suivantes :

La console de gestion de la TMG.

4.1 La création des règles de la TMG :

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

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



Le trafic destinataire étant le réseau local sélectionnons l'hôte local.

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

5. Server system center Virtual machine manager:

Permet de gérer le parc des serveurs Virtual au sein d'une entreprise, cette application prend un sens lorsque le parc de serveurs hôtes est supérieur à 25 machines pour des raisons de coût et de mise en place. Grâce à SCVMM il est bien plus simple d'administrer cet ensemble de serveurs en y installant un simple agent sur l'ensemble des serveurs. Celui-ci assure un lien entre l'hôte et SCVMM en passant par l'intermédiaire du contrôleur de domaine.

Il est possible d'administrer SCVMM par la console d'administration locale ou distante, qui nécessite une installation en dur sur la machine et qui prend comme paramètre de connexion le nom du serveur SCVMM ou son adresse IP. On peut aussi passer directement par une interface web, qui impose la mise en place d'un serveur IIS.Pour finir nous porterons un regard sur les développements futurs qui pourront compléter les solutions que nous avons pu voir dans ce chapitre.

Une fois votre serveur configuré (adresse IP fixe définie, serveur correctement nommé et joint au domaine, nous allons installer les deux logiciels indispensables à l'installation et au fonctionnement de SCVMM.

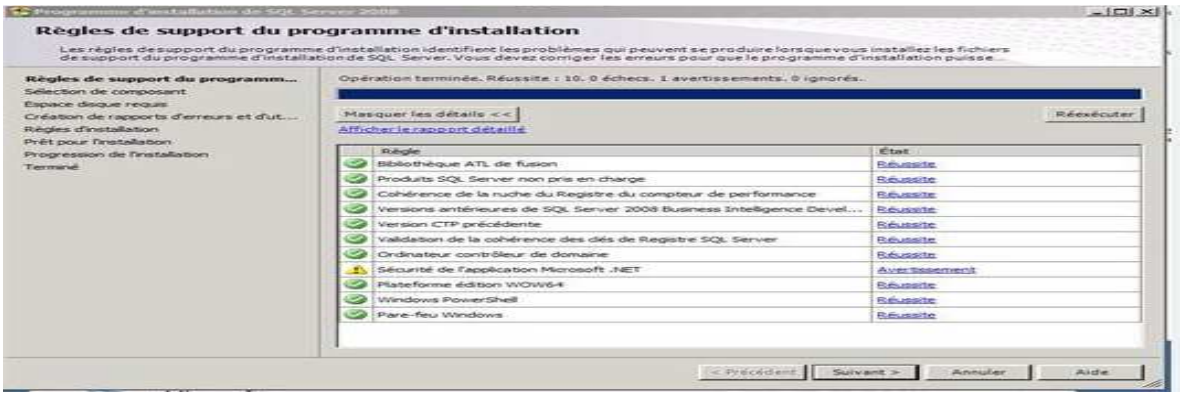
En commence par l'installation de Windows AIK. Il s'agit d'un logiciel qui fournit une aide à la configuration, à la personnalisation et au déploiement de Windows 7 et Server 2008R2.

Après avoir lu les termes du contrat de licence, cochez « J'accepte » et ensuite cliquez sur suivant :

Sélectionnez le chemin d'installation puis cliquez sur Suivant :

Une fois l'installation terminée, nous allons passer au deuxième prérequis : l'installation de Microsoft SQL Server.

Une Allez dans le panneau Installation puis en clique sur « Nouvelle installation autonome SQL server ou ajout de fonctionnalités à une installation existante ». Puis cliquez sur Suivant. Lisez les termes du contrat de licence et ensuite en coche « J'accepte les termes du contrat de licence » puis en clique sur Suivant. L'assistant va vérifier que tous les pré requis sont bien respectés. Voici la fenêtre qui apparait une fois toutes les vérifications effectuées :



5.1. Installation de SCVMM

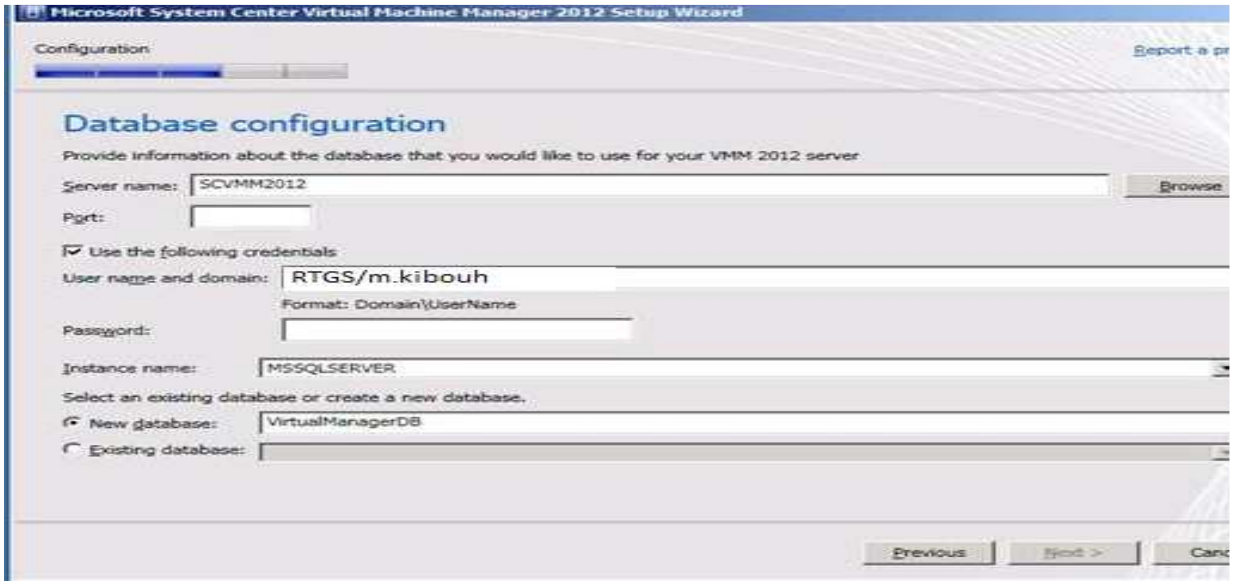
Nous allons enfin rentrer dans le vif du sujet, l'installation de System Center Virtual Machine Manager 2012. Pour lancer la procédure d'installation cliquez sur Installer :

Lisez les termes de la licence, cochez la case « J'ai lu, compris et accepte les termes du contrat de licence », puis cliquez sur Suivant :

Sélectionnez les fonctionnalités à installer « VMM server ». Vous pouvez remarquer que la console d'administration est implicitement installée, puis cliquez sur Suivant :

Nous passons dans la partie de configuration, définissez le nom du serveur de base de données, ainsi que son port (uniquement si vous avez changé celui d'origine).

Sélectionnez l'utilisateur ayant les droits adéquats (dans notre cas le compte administrateur de domaine est aussi l'administrateur SQL), ainsi que son mot de passe, ensuite le nom de l'instance SQL, et enfin le nom de la base de données, puis cliquez sur Suivan



Sélectionnez le compte de service adéquat (dans notre cas, s'agissant d'un environnement de test, on utilise le compte administrateur de domaine), saisissez le mot de passe de ce compte, puis cliquez sur Suivant :

5.2. Ajout d'un Hôte (joint au domaine)

Nous allons voir comment ajouter un hôte qui est membre du même domaine que le serveurVMM.

Le début de la procédure d'installation est identique à celle de la partie précédente.

Dans l'onglet fabrique, puis faire un clic droit sur serveur et sélectionnez « Ajoutez un hôte ou cluster Hyper-V

L'assistant se lance, sélectionnez « ***Ordinateur Windows dans un domaine Active Directory*** **»**, puis cliquez sur **Suivant**

Dans cette fenêtre, sélectionnez un compte disposant des droits d'administration sur les machines distantes à ajouter ainsi que son mot de passe, puis cliquez sur **Suivant** :

Dans cette fenêtre nous allons ajouter les machines en les désignant soit par leur nom, soit par leur adresse IPV4 ou IPV6. Dans notre cas nous utiliserons l'adresse IPV4, une fois l'adresse saisie, puis cliquez sur **Suivant**

Sélectionnez le groupe de serveurs auquel vous souhaitez ajouter les machines. Dans notre cas, ils sont directement mis à la racine « **Tous les hôtes** ». Il est possible de réassigner des hôtes utilisant déjà un agent SCVMM. Cliquez sur **Suivant**

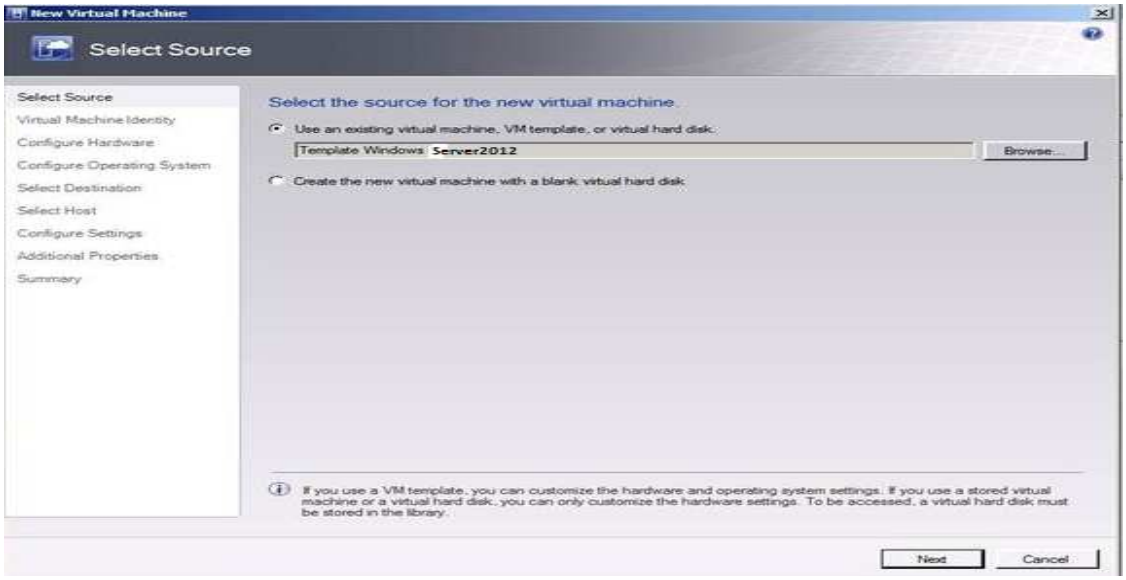
Voici un récapitulatif de tous les paramétrages sélectionnés précédemment. Après avoir vérifié que tout correspond à vos choix, cliquez sur **Terminer** :

5.3. Création de Machine Virtuelle par Modèle

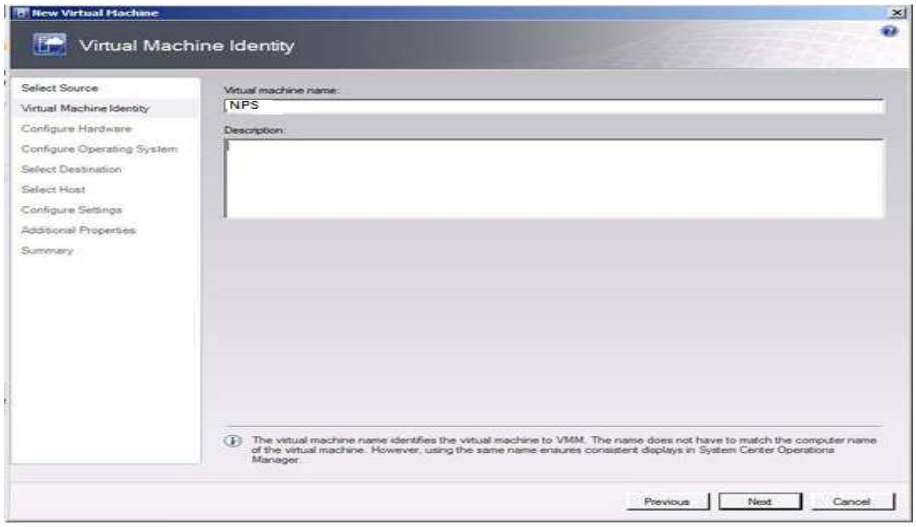
Nous allons déployer une machine virtuelle à partir d'un modèle qui se trouve dans la librairie.

Pour cela allez dans l'onglet VM puis cliquez sur « ***Créer une nouvelle machine virtuelle*** ».

Un assistant se lance, sélectionnez le modèle adapté puis cliquez sur **Suivant** :



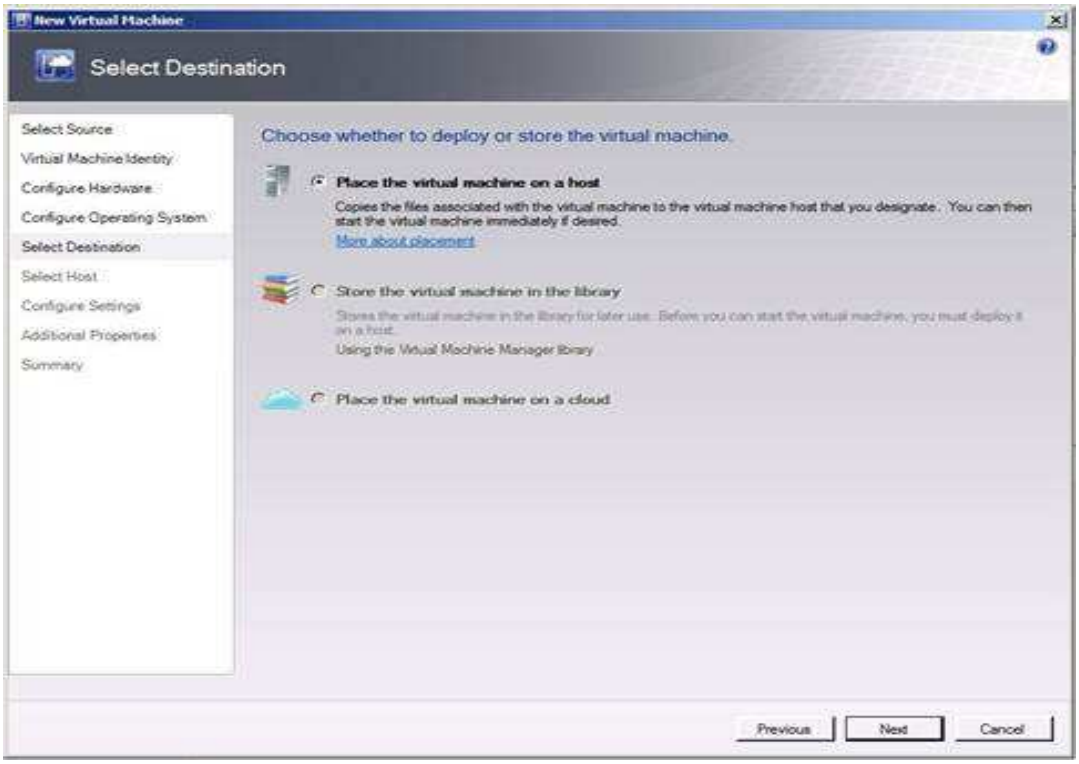
Sélectionnez le nom de votre machine virtuelle ainsi que sa description puis cliquez sur **Suivant** :



Dans cette fenêtre vous trouverez la configuration hardware. Comme nous partons du modèle précédemment construit, vous n'avez rien à modifier ici, cliquez donc sur **Suivant** :

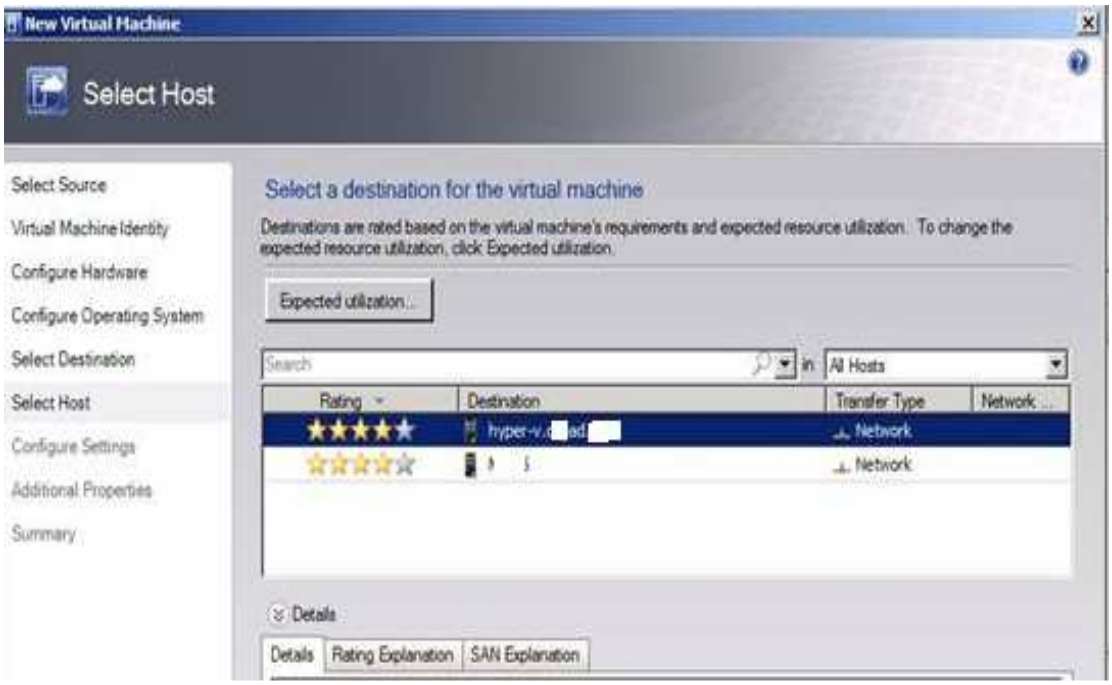
Vous avez la possibilité de choisir l'emplacement où sera déployée votre machine virtuelle (sur un serveur HyperV, dans une librairie ou dans un Cloud). Dans notre cas sélectionnez

Serveur hôte puis cliquez sur **Suivant** :



Dans cette page vous devez définir le serveur hôte sur lequel vous souhaitez déployer votre VM. Privilégiez le serveur hyperayant le plus grand nombre d'étoiles (plus il y a d'étoiles, plus le serveur est adapté).

Sélectionnez le serveur hôte qui vous convient, puis cliquez sur **Suivant** :
Vérifiez que la machine est correctement nommée, qu'elle est bien attachée au disque dur et que la configuration de la carte réseau est bonne, puis cliquez sur **Suivant** :



Une fois votre choix effectué, cliquez sur **Suivant** :

Apparait alors le récapitulatif de vos choix. Si vous voulez éviter que la VM démarre automatiquement dès qu'elle sera déployée, décochez la case « ***Démarrer la machine virtuelle, à la fin de son déploiement sur le serveur hôte*** ».

5.4.Création d'un cluster

Sur vos serveurs Hyper V2 activer la fonctionnalité de clustering avec basculement

Dans l'onglet fabrique, cliquez en haut à gauche sur **Créer** puis sélectionnez « ***Hyper-V Cluster*** » :

L'assistant se lance, sélectionnez le nom de votre cluster, ainsi que le nom et le mot de passe d'un compte administrateur, puis cliquez sur **Suivant**

Sélectionnez ensuite les nœuds qui seront rattachés à ce cluster (dans notre cas le cluster est composé de deux nœuds hyperv1-hayperv2) puis cliquez sur **Suivant** :

Sélectionnez l'adresse IP que vous souhaitez donner à votre cluster, et ce pour chaque carte réseau (dans notre cas nous n'utiliserons qu'une seule carte réseau en IPV4 192.168.3.200), cliquez ensuite sur **Suivant**

Sélectionnez les disques durs (virtuels) dans le SAN de cluster, puis cliquez sur **Suivant**

Voici un récapitulatif des différents paramètres déjà saisis. Une fois que vous avez tout vérifié, cliquez sur **Terminer**

Discussion :

Dans ce chapitre, nous avons mis en place une infrastructure Cloud au sein de 2int, à travers cette réalisation nous avons pu dégager l'intérêt de Cloud, et ce que peut nous apporte comme bénéfices et augmentation de performances pour 2int.

Conclusion

Conclusion

De nos jours, la sécurité informatique est quasi-indispensable pour le bon fonctionnement d'un réseau, aucune entreprise ne peut prétendre vouloir mettre en place une infrastructure réseau, quel que soit sa taille, sans envisager une politique de sécurité.

Dans ce mémoire nous avons étudiés le réseau de l'école de formation 2int, nous avons relevé quelques failles puis apporté une solution convenable qui est l'utilisation du Cloud Computing.

Notre objectif est de mettre à disposition de l'école 2int des espaces de stockages pour la sauvegarde de ses données, cette technologie lui permettra d'avoir une sécurité accrue et qui sera bien moins exposées aux risques de perte et une disponibilité maximale des données. Mais aussi faire la location des services aux publics pour avoir des bénéfices supplémentaires.
Mais tout travail est loin d'être parfait donc nous le laissons avec des perspectives ouvertes.

Annexes

A.1. GNS3

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

Figure A.1: GNS3.

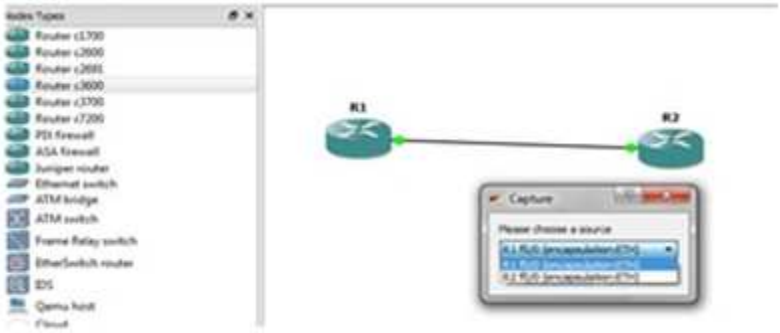
A.1.1. Installation de GNS3

GNS3 est téléchargeable depuis le site officiel de GNS3. La version téléchargée est GNS3

v0.7.4 all-in-one. Son installation est une succession du terme suivant. Au lancement de GNS3, ilexiste deux possibilités de configuration qui sont :

A.1.5. Capture de paquet

GNS3 permet de capturer le trafic sur un lien donné à l'aide de wireshark (qui est installé avec cette version de GNS3). Prenons un exemple de deux routeurs connectés en Fastethernet, il faut effectuer un clic droit sur le lien physique, et cliquer sur capture. Un menu déroulant apparait avec possibilité de choisir l'interface physique



Après sélection, wireshark se charge (s'il n'a pas été installé dans le répertoire par default, il faut modifier cela dans le menu Edit-> Préférence ->Capture en sélectionnant le répertoire où il se trouve).

Il permet de visualiser le Ping qui sera effectué entre les deux routeurs

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

A.1.6. La connexion d'une interface routeur à la carte réseau d'une machine virtuelle

La procédure

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

A.2. Packet Tracer

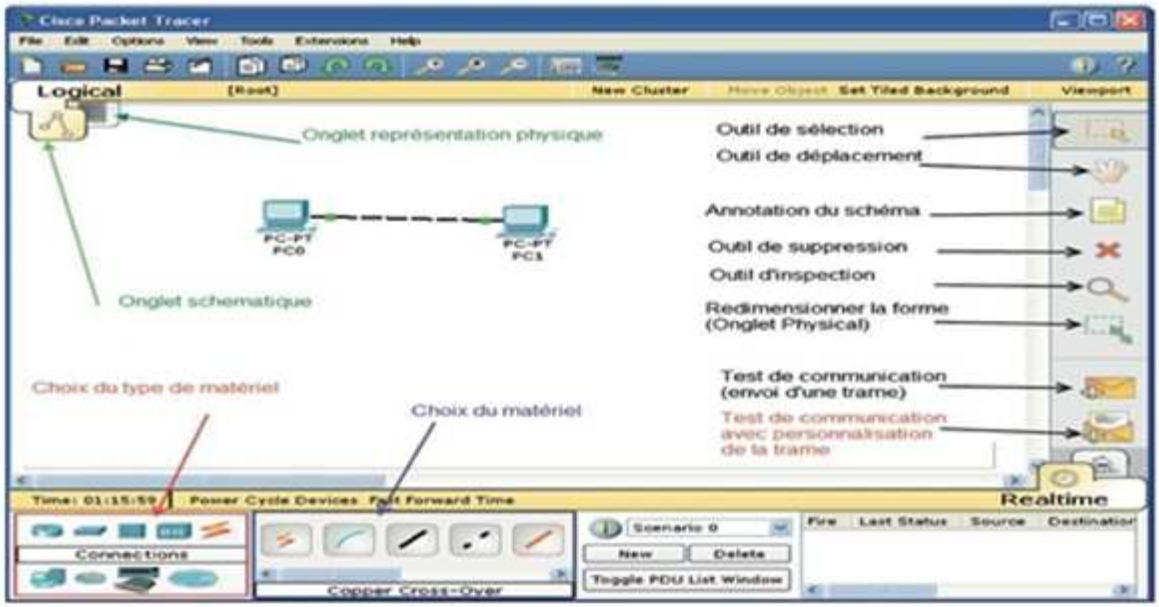
Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc. . .

A.2.1. **Présentation de l'écran principal** :

- Une barre de menu classique.
- Une barre d'outils principale avec les fonctionnalités de base de gestion de fichier,d'impression, etc.….

Pour créer votre schéma :

On suppose qu'il n'y a pas de schéma au départ sinon cliquer sur File/New. Se placer dans l'onglet LOGICAL sous la barre d'outils principale.

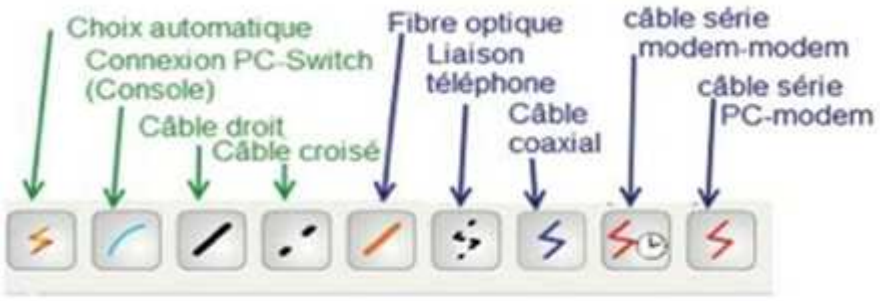


A.2.2. Placement du matériel

- Choisir le Type de matériel
- Selon le type, la liste du matériel change de manière dynamique
- Placer tout le matériel souhaité pour créer votre architecture.

A.2.3. Interconnecter vos équipements

- Choisir l'outil câblage.
- Choisir le type de connexion.
- Cliquer sur le premier équipement.
- Choisir le connecteur désiré.
- Cliquer ensuite sur le deuxième équipement et choisir le connecteur désiré.
- La connexion doit être visible sur le schéma.
- Les points de couler aux extrémités de la connexion informe de l'état de la liaison. Ils peuvent être rouges, orange ou vert.
- Il est possible de modifier le nom des éléments en double cliquant sur leur nom.
- Il est souhaitable également d'annoter le schéma (adresse IP, adresse du réseau, etc.…) avec l'outil Note.

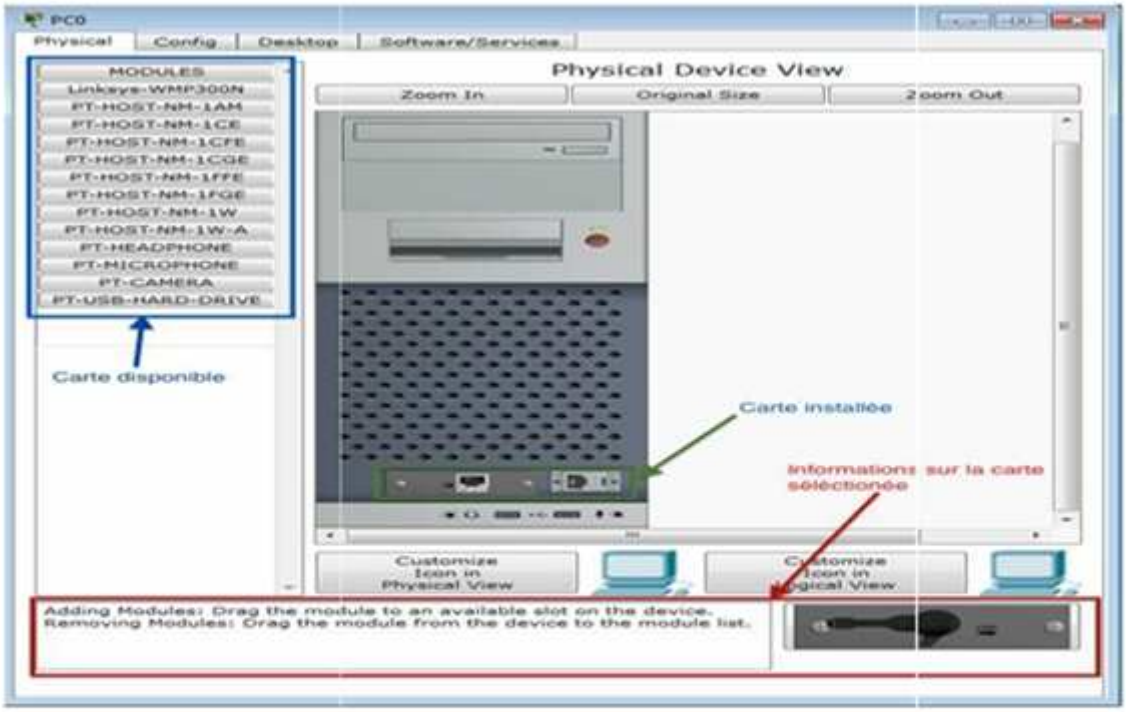


A.2.4. Paramétrage des appareils :

Pour accéder au paramétrage d'un appareil, il faut cliquer sur la représentation de l'appareil.

Deux à quatre onglets sont accessibles avec cette fenêtre en fonction de type de l'équipement. Paramétrage physique (Physical). Le paramétrage physique consiste à placer

les bonnes cartes dans l'appareil. Les cartes disponibles se trouvent à gauche de l'écran. Pour le placer, commencer par éteindre l'appareil avec le bouton Marche/Arrêt (M/A). Si besoin retirer la carte en place, par glisser déplacer de l'appareil vers la liste des cartes. Glisser la nouvelle carte sélectionnée de la liste des modules à l'emplacement vide. Appuyer à nouveau sur le bouton M/A.



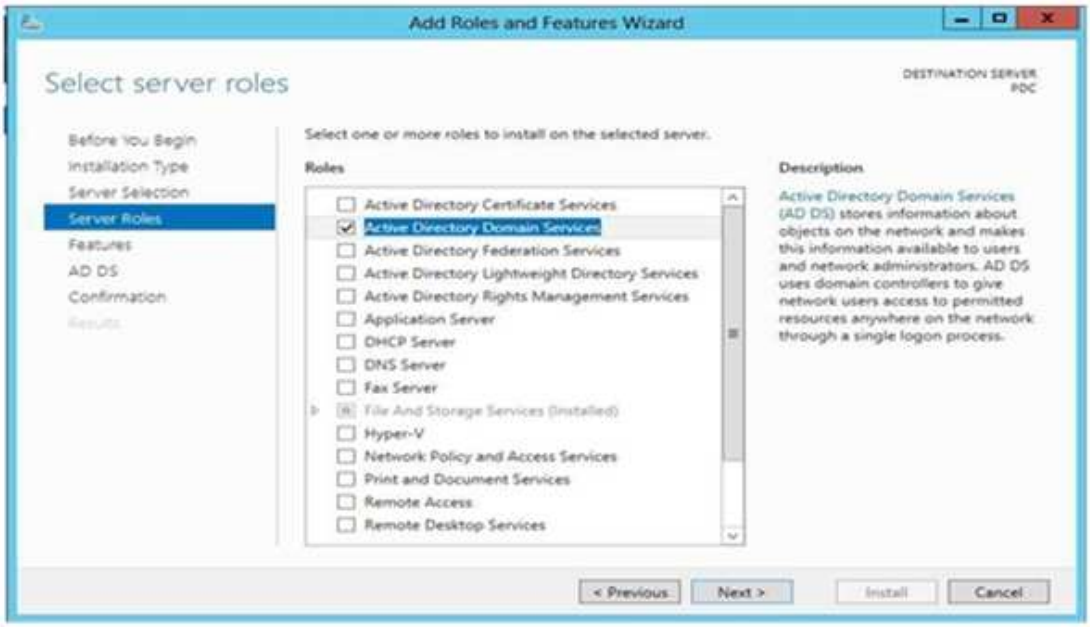
A.3. Windows Server 20 12: Active Directory Domain Services

Figure A.3 : Windows Server 2012 et Active Directory.

Active Directory est la base d'un réseau Microsoft.

Il permet la gestion des ressources : utilisateurs et périphériques, l'authentification et lasécurisation des accès. Mais c'est aussi la base de nombreux autres services comme DNS, WINS,DHCP, …..

Pour ajouter Active Directory, vous devez passez par l'assistant de gestion des Rôles :



Auparavant, il était possible de lancer l'assistant Active Directory avec la commande dcpromo, mais celle ci a été supprimée.

On clique donc sur Ajouter des fonctionnalités, puis continuez l'assistant en cliquant sur « Suivant ».

Les fonctionnalités obligatoires ont été pré cochées, cliquez sur Suivant.

A.4. Installation de Forefront TMG 2010

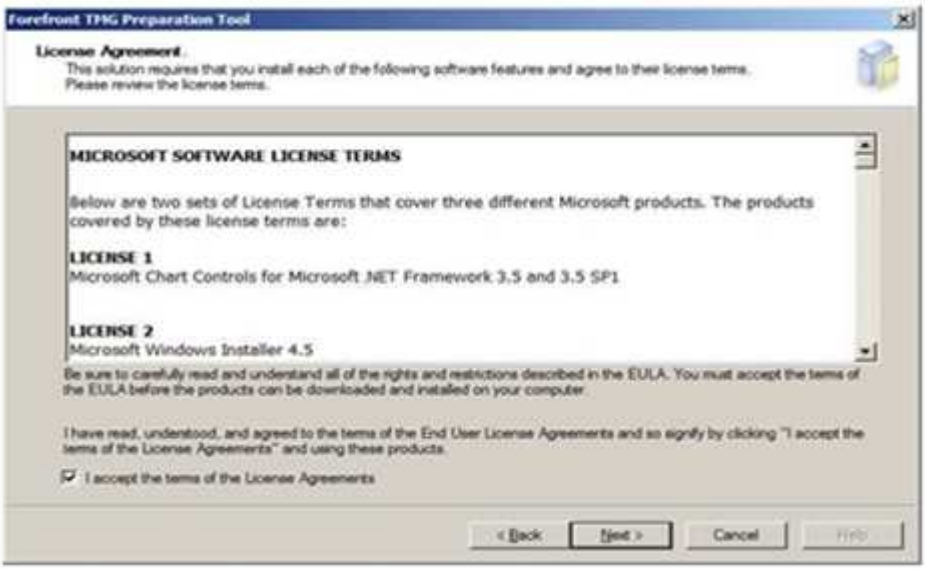
Installation d'un serveur mono-carte (rôle proxy Web ou reverse proxy)

- Etape 1 - Installation d'un Windows Server 2008 R2 Forefront TMG 2010 ne s'installe que sur Windows Server 2008 édition 64 bit ou Windows Server 2008 R2 qui lui n'est disponible qu'en 64 bit.
- Etape 2 - Mise à jour du système via Microsoft Update
- Etape 3 - Préparation à l'installation de Forefront TMG 2010

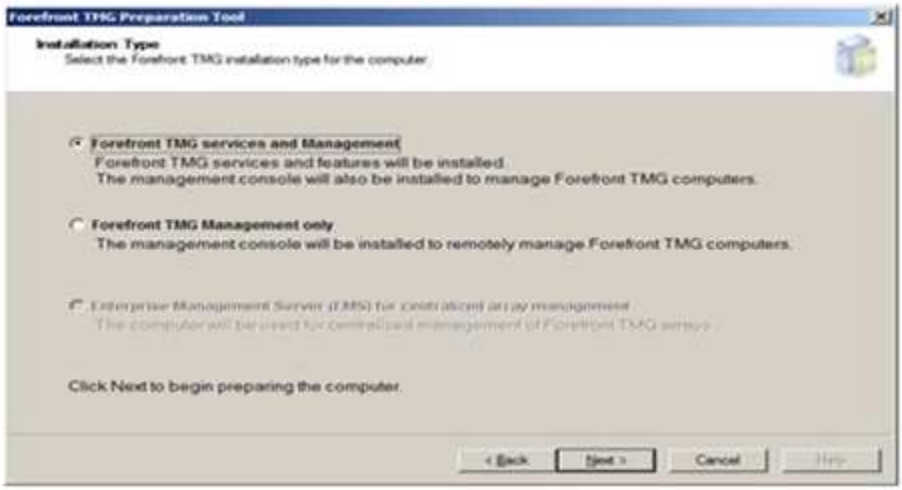
Figure A.4: Forefront, Threat Management Gateway.

Sélectionner RunPreparationTool

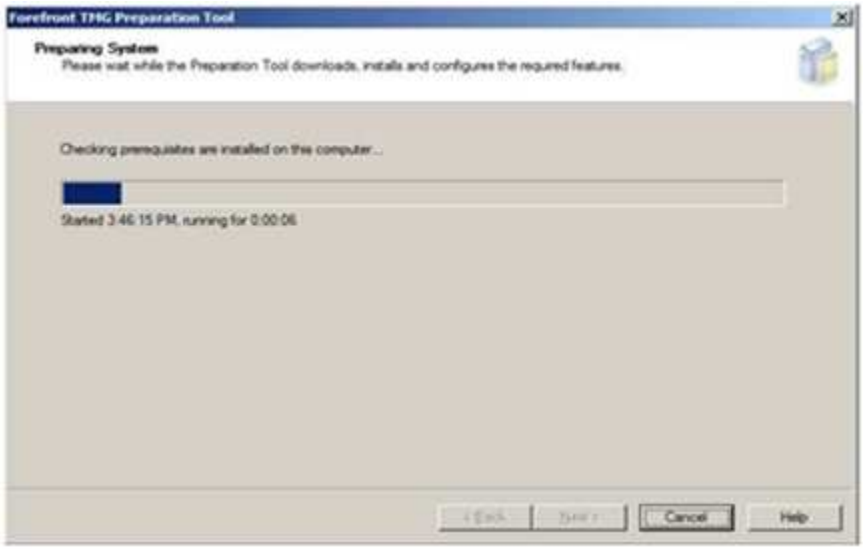
Cliquer sur Next

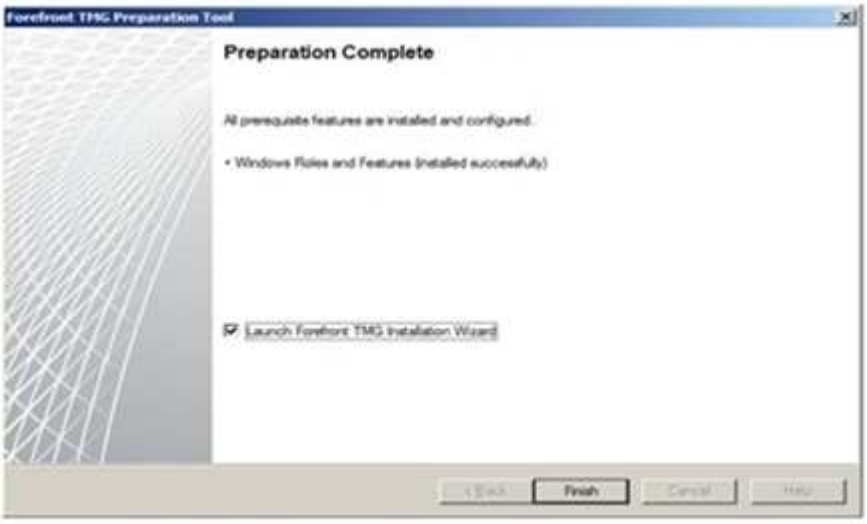


Accepter la licence et cliquer sur Next



Ici la machine va être le serveur Forefront TMG donc on garde la sélection proposée (si c'était juste un poste d'administration, il faudrait sélectionner la seconde option). Cliquer sur Next.





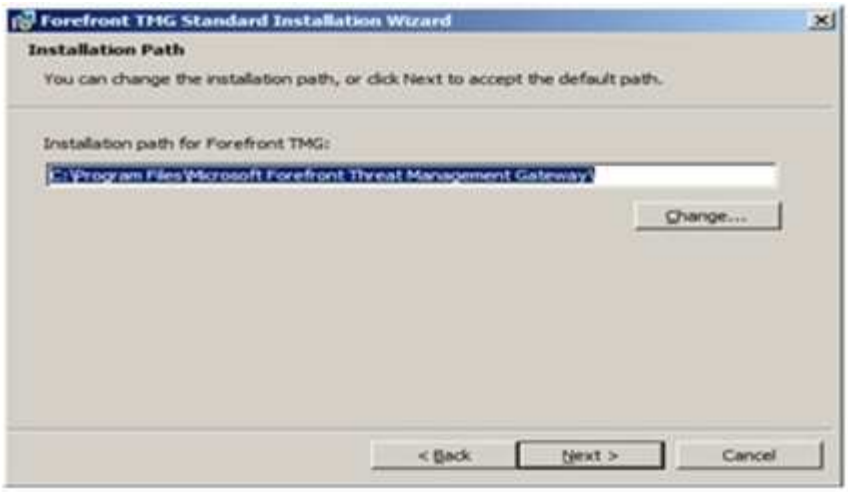
Fin de la préparation. Cliquer sur Finish pour démarrer l'installation de Forefront TMG 2010.

Etape 4- Installation de Forefront TMG 2010

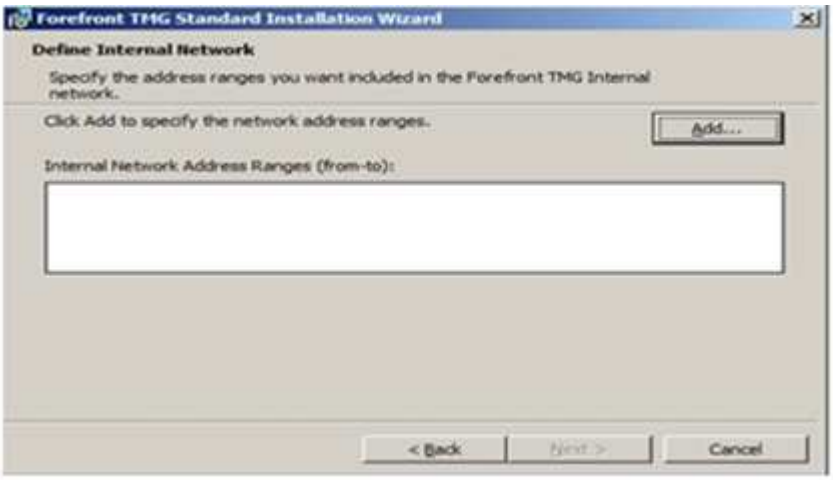
Cliquer sur Next

Accepter la licence et cliquer sur Next

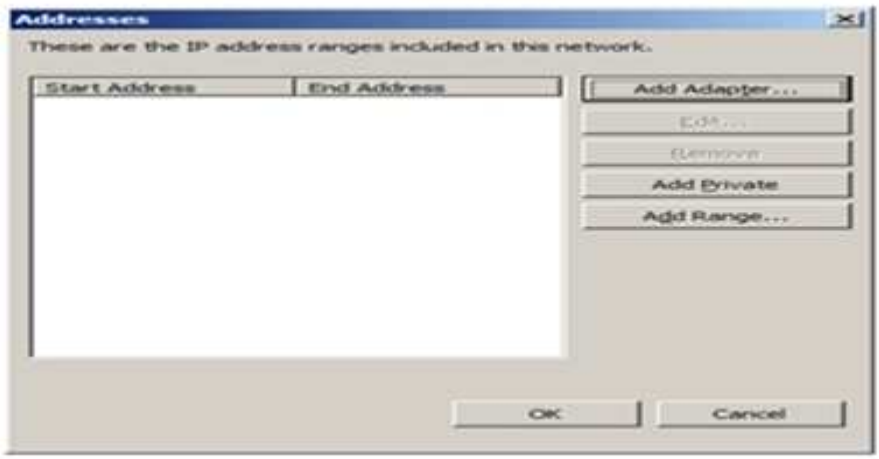
Saisir les informations de licence et cliquer sur Next



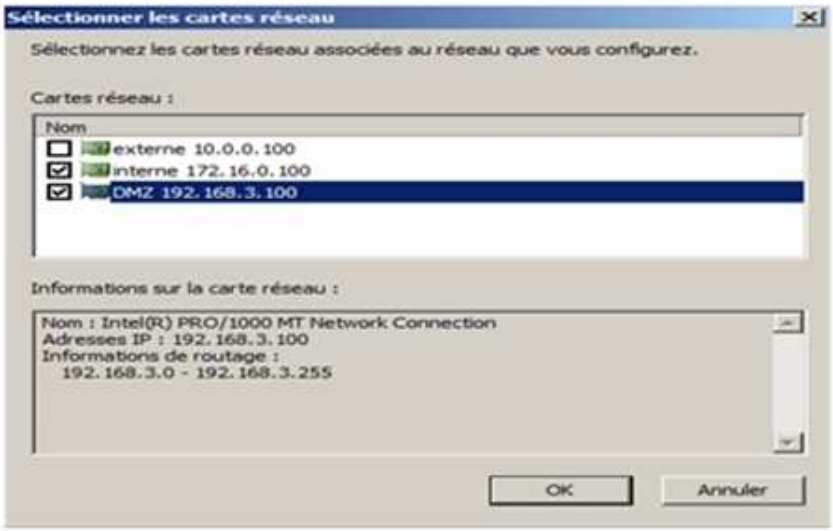
Choisir le chemin d'installation de Forefront TMG 2010. Cliquer sur Next

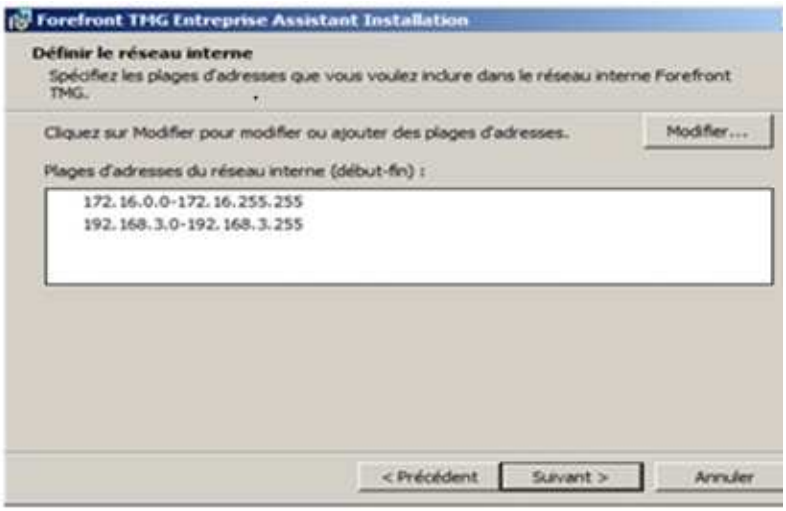


Dans cette étape sont déclarés les réseaux internes qui est inclut au domaine RTGS.dz externe et DMZ (ce qui dans le cas d'une configuration mono-carte est un peu particulier à la différence d'une configuration multi cartes réseau). Cliquer sur Add.



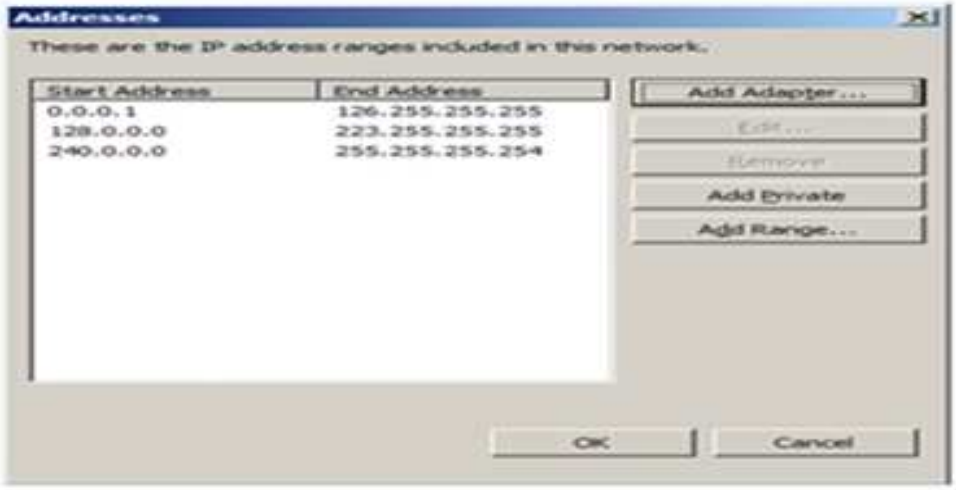
Cliquer sur Add Adapter et on ajoute les 2 carte réseaux internal et DMZ.



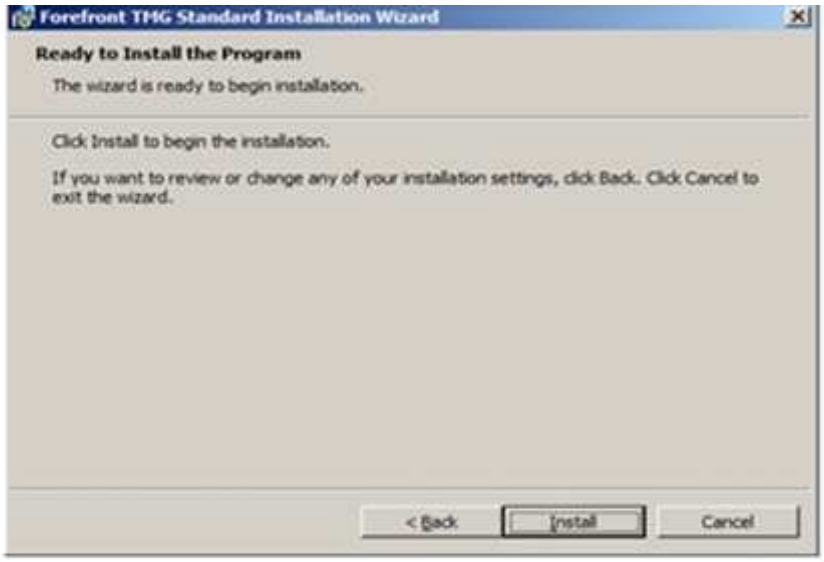


Cliquer sur OK

La table des adresses locales a été construite automatiquement. Cliquer sur OK.

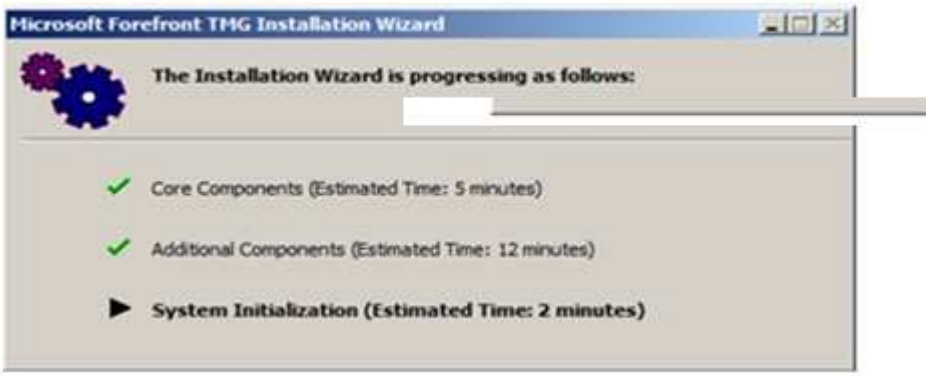


Cliquer sur Next



Cliquer sur Install. A partir de cet instant,


Microsoft Forefront TMG Installation Wizard
The Installation Wizard is progressing as follows:
Core Components (Estimated Time: 5 minutes)
Additional Components (Estimated Time: 12 minutes)
System Initialization (Estimated Time: 2 minutes)


Microsoft Forefront TMG Installation Wizard
The Installation Wizard is progressing as follows:
Core Components (Estimated Time: 5 minutes)
Additional Components (Estimated Time: 12 minutes)
System Initialization (Estimated Time: 2 minutes)


Microsoft Forefront TMG Installation Wizard
Installation Wizard Completed
The Installation Wizard completed successfully.
Launch Forefront TMG Management when the wizard closes
Click Finish to exit the wizard.
Finish

Sommaire

[1] : Jean-Françoispillou, tout sur les réseaux et internet,2007

[2] : jacques Philippe,réseau intranet et internet, ellipses 2010

[3] : Jean-Françoispillou,tout sur les réseaux et internet,2007

[4] :Claudeservin, réseau et télécoms,2eme édition, préface de jean-pierre arnand,2003 /2006

[5] : Williamstallings sécurité des réseaux application et standard, 2003

[6] Jean-Françoispillou, jean Philippebay, tout sur la sécurité informatique 2eme édition ,2009

[7] : JoséDordoigne, réseauinformatiques notion fondamentales, 2011

[8] :David GELIBERT, Farid SMILI la sécurité et la virtualisation, 2012

[9] : FloreLafargue, stefane pagnon le Cloud Computing une nouvelle filière fortement structurante, 2012

[10] : pascalSauliere, CloudComputing et sécurité ,2010

[11]www.commentcamarche.net/faq/37890-des-solutions-cloud-pour-avoir-ses-donnees-partout.

[12] :http://www.contenus-en-ligne.com/lancement-de-www-je-me-forme-com-la-formation-en-ligne-pour-tous.

[13] : Baptiste Lacroix, livre blanc comment le Cloud peut-il booster votre entreprise ?,2013.

ARP : Address Resolution Control

ASA: Adaptive Security Appliance

CSA: Cloud security alliance

DMZ: Demilitarized zone

DHCP: dynamic host configuration protocol

Dos: Deny of Service

IPS: Intrusion Prevention System

IDS: Intrusion Detection System

IIS: Internet Information Services

IP: Internet Protocol

MAN: Metropolitan Area Network

MAC: Medium Access Control

OSI Open System Interconnection**s**

PPP:Point to Point Protocol

PaaS: Platform-as-a-Services

SMTP: Simple Mail Transport Protocol

SSH: Secure Socket Shell

SSL: Secure Sockets Layers

SaaS: Software-as-a-Service

TMG: Threat Management Gateway

TCP: transfer control protocol

VPN: virtual private network

WAN: Word Area Network