République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane Mira de Béjaia

Faculté des Sciences Exactes

Département d'Informatique

MÉMOIRE DE FIN DE CYCLE

En vue d'obtention d'un diplôme de Master en Informatique

Option : *Administration et Sécurité des Réseaux*

Thème

Proposition d'une solution firewall pour les réseaux locaux d'entreprise

---

Réalisé par :

M^{elle} ADOUANE Lila

M^{elle} TOUAHRI Aicha

Soutenu le 03 Juillet 2016 devant le jury composé de :

Présidente	**M^{m}**	**S. BOUKERRAM**	**Maître de conf. A**	**U. A/Mira Béjaia.**
Rapporteur	**P^{r}**	**A. BOUKERRAM**	**Professeur**	**U. A/Mira Béjaia.**
Examinateur	**M^{r}**	**M. CHELIK**	**Doctorant en LMD**	**U. A/Mira Béjaia.**

Promotion : 2015/2016

Remerciement

Tout d'abord, nous remercions Dieu, notre créateur de nous avoir donné la force, la volonté et le courage afin d'accomplir ce modeste travail .

Et nous adressons nos vifs remerciements et notre gratitude

Â :

Nos familles, surtout nos parents qui nous ont épaulés, soutenus et suivis tout au long de ce projet .

Nous tenons à adresser nos plus profonds et sincères remerciements à notre encadreur ***Pr BOUKERRAM Abdellah****, pour nous avoir encadrés et guidés tout au long de ce projet,pour tous ses conseils et ses encouragements, pour sa disponibilité et sa compréhension .*

Nous tenons également à remercier ***Mr SOUADIH*** *et* ***Mr IDIR*** *pour toutes leurs orientations, leurs aides, leur compréhensions et leurs précieux conseils .*

Aussi à tous les enseignants et employés du département Informatique à qui on doit notre avancement .

Nous tenons aussi à remercier également tous les membres de jury pour avoir accepter d'évaluer notre travail .

Enfin, nous remercions tous ceux qui nous ont soutenu et aidé dans la réalisation de ce mémoire de près ou de loin..

Dédicaces

Je tien a dédier solennellement ce modeste travail à :

A mes très chers parents, aucun hommage ne pourrait être à la hauteur de l'amour dont ils ne cessent de me combler. Que dieu leur procure bonne santé et longue vie .

A mon très cher frère Moho, son épouse Hania et leurs fils Aris .

A mes très chères sœurs :

Saida, son mari Mourad et leurs fille Aya .

Ouardia, son mari Halim et leurs fille Assia .

Zina et son fiancé Adel .

A toute ma famille et mes proches .

A ma chère amie Lila et à sa famille .

A mes amis(es) pour leur compréhension et fidélité .

Ainsi qu'à toute personne qui nous a soutenue .

Aicha

Dédicaces

Je tien a dédier solennellement ce modeste travail à :

A mes très chers parents, aucun hommage ne pourrait être à la hauteur de l'amour dont ils ne cessent de me combler. Que dieu leur procure bonne santé et longue vie .

A ma chère sœur Nassima et son marie Abdenour et leurs enfants Sylia, Kahina, Imane, Tiziri, Adam .

A mes très chères sœurs Samira, Sihem et Chahinez .

A mes chers frères Syphax et Yanis .

A mes grands parents .

A toute ma famille et mes proches .

A ma chère amie Ratiba et à sa famille.

A tous mes chers amis et mes enseignants .

Ainsi qu'à toute personne qui nous a soutenue .

Lila

Table des matières

Table des matières **i**

Liste des figures **iv**

Liste des abréviations **vi**

Introduction générale **1**

1 Généralités sur les Réseaux et la Sécurité Informatique **3**

1.1 Introduction . . . 3

1.2 Généralités sur les Réseaux . . . 3

1.2.1 Définition d'un réseau . . . 4

1.2.2 Classification des réseaux selon la taille . . . 4

1.2.3 Architecture des réseaux . . . 5

1.2.4 Topologies des réseaux . . . 6

1.2.5 Equipement d'interconnexion . . . 9

1.2.6 Modèle de référence OSI . . . 10

1.2.7 Modèle TCP/IP . . . 11

1.3 La Sécurité Informatique . . . 12

1.3.1 Terminologie de la sécurité informatique . . . 12

1.3.2 Politique de sécurité . . . 13

1.3.3 Objectifs de la sécurité informatique . . . 13

1.3.4 Mécanismes de la sécurité . . . 15

1.3.5 Attaques informatiques . . . 18

1.3.6 Mesures et techniques d'atténuation d'attaques . . . 19

1.4 Conclusion . . . 21

2 La sécurité des réseaux : Firewalls **22**
2.1 Introduction . . . 22
2.2 Définition d'un firewall . . . 22
2.2.1 De quoi protège un firewall . . . 23
2.2.2 De quoi ne protège pas un firewall . . . 24
2.3 Principe de fonctionnement . . . 25
2.3.1 Filtre de paquets . . . 25
2.3.2 Passerelle . . . 25
2.4 Différentes catégories de firewall . . . 26
2.4.1 Firewall sans états (stateless) . . . 26
2.4.2 Firewall à états (stateful) . . . 27
2.4.3 Firewall applicatif . . . 28
2.4.4 Firewall authentifiant . . . 28
2.4.5 Firewall personnel . . . 29
2.5 Types d'architectures . . . 29
2.5.1 Firewall avec routeur de filtrage . . . 29
2.5.2 Passerelle double - le réseau bastion . . . 30
2.5.3 Firewalls avec réseau de filtrage . . . 31
2.5.4 Firewall avec sous-réseau de filtrage . . . 32
2.6 Zone démilitarisée (DMZ) . . . 33
2.6.1 Firewall avec zone démilitarisée . . . 33
2.7 Choix d'un firewall pour l'entreprise . . . 34
2.8 Conclusion . . . 35

3 Contexte de travaile et Implementation **36**
3.1 Introduction . . . 36
3.2 Problématique . . . 36
3.3 Solution proposée . . . 37
3.4 Description de l'environnement du travail . . . 38
3.4.1 GNS3 . . . 38
3.4.2 IOS (Internet Work operating System) . . . 39
3.4.3 Objectif de GNS3 . . . 39
3.4.4 Description de l'interface graphique de l'émulateur GNS3 . . . 40
3.5 Implémentation de la solution . . . 41
3.5.1 Configuration de base . . . 41
3.5.2 Configuration de firewall ASA . . . 43

3.6 Conclusion 49

Conclusion générale **50**

Bibliographie **50**

A Annexe **53**

Liste des figures

1.1 Classification des réseaux informatique 5
1.2 Réseaux poste à poste 5
1.3 Réseaux client-serveur 6
1.4 Topologie linéaire 7
1.5 Topologie en bus 7
1.6 Topologie en anneau 7
1.7 Topologie en étoile 8
1.8 Topologie maillée 8
1.9 Les couches du modèle OSI et leurs protocoles 11
1.10 Comparison entre le modèle OSI et le modèle TCP/IP 12

2.1 Firewall représenté par un mur entre un ordinateur et l'Internet 23
2.2 Firewall avec routeur de filtrage 29
2.3 La passerelle double 30
2.4 Firewall avec réseau de filtrage 31
2.5 Firewall avec sous-réseau de filtrage 32
2.6 Firewall avec DMZ 34

3.1 Architecture de la solution proposée. 38
3.2 Interface graphique de l'émulateur GNS3. 40
3.3 Configuration de routeur Interent. 41
3.4 Configuration de routeur R1. 42
3.5 Configuration de routeur R2. 42
3.6 Configuration de routeur R3. 43
3.7 Configuration de firewall ASA. 44
3.8 Aperçu des interface de firewall ASA. 45
3.9 Route pour acceder à l'Internet. 45

3.10 Resultat d'une requête ICMP (ASA vers Internet). 45
3.11 Configuration du nat. 46
3.12 Configuration de class-map. 47
3.13 Configuration du ACL 1 47
3.14 Configuration du ACL 2. 48
3.15 Aperçu des ACLs configurées. 48
3.16 Configuration du Telnet. 49

Liste des abréviations

AC	**A**utorité de **C**ertification
ACL	**A**ccess **C**ontrol **L**ist
AES	**A**dvanced **E**ncryption **S**tandard
ASA	**A**daptive **S**ecurity **A**ppliance
ASDM	**A**daptive **S**ecurity **D**evice **M**anager
ATM	**A**synchronous **T**ransfer **M**ode
CCIP	**C**isco **C**ertified **I**nternetwork **P**rofessional
CCIE	**C**isco **C**ertified **I**nternetwork **E**xpert
CCNA	**C**isco **C**ertified **N**etwork **A**ssociate
CCNP	**C**isco **C**ertified **N**etwork **P**rofessional
CHAP	**C**hallenge **H**andshake **A**uthentication **P**rotocol
DEA	**D**ata **E**ncryption **A**lgorithm
DES	**D**ata **E**ncryption **S**tandard
3DES	**T**riple **D**ata **E**ncryption **S**tandard
DMZ	**D**e**M**ilitarized **Z**one
DSA	**D**igital **S**ignature **A**lgorithm
EAP	**E**xtensible **A**ositioning **P**rotocol
FTP	**F**ile **T**ransfer **P**rotocol
GNS3	**G**raphical **N**etwork **S**imulator03
GNUPG	**G**NU **P**rivacy **G**uard
ICMP	**I**nternet **C**ontrol **M**essage **P**rotocol
IDS	**I**ntrusion **D**etection **S**ysteme
IOS	**I**nternetWork **O**perating **S**ysteme
IP	**I**nternet **p**rotocole
IPS	**I**ntrusion **P**revention **S**ysteme
ISO	**I**nternational **S**tandardization **O**rganization
ISR	**I**ntegrated **S**ervices **R**outer

LAN	**L**ocal **A**rea **N**etwork
LLC	**L**ogical **L**ink **C**ontrol
MAC	**M**edia **A**ccess **C**ontrol
MAN	**M**etropolitan **A**rea **N**etwork
MD5	**M**essage **D**egest
MIPS	**M**icroprocessor without **I**nterlocked **P**ipeline **S**tages
Ms-CHAP	**M**icro**s**oft **C**hallenge **H**andshake **A**uthentication **P**rotocol
NAT	**N**etwork **A**ddress **T**ranslation
OS	**O**perating **S**ysteme
OSI	**O**pen **S**ystème **I**nterconnexion
PAN	**P**ersonal **A**rea **N**etwork
PAP	**P**assword **A**uthentication **P**rotocol
PGP	**P**retty **G**ood **P**rivacy
PIX	**P**rivate **I**nternet **E**xchange
RSA	**S**ivest **S**hamir **A**hamir
SHA	**S**tandard **H**ash **A**lgorithm
SMTP	**S**imple **M**essage **T**ransfert **P**rotocol
SNMP	**S**imple **N**etwork **M**ransfert **P**rotocol
SSH	**S**ecure **S**hell
SSL	**S**ecure **S**ocket **L**ayer
TCP	**T**ransmission **C**ontrol **P**rotocol
VPN	**V**irtual **P**rivate **N**etwork
VLAN	**V**irtual **L**ocal **A**rea **N**etwork
UDP	**U**ser **D**ata **P**rotocol
WAN	**W**ide **A**rea **N**etwork

Introduction générale

L'information était toujours un élément essentiel durant l'évolution de l'humanité, en effet une meilleure gestion de toute activité (économique, social, politique, militaire...) dépend essentiellement d'une meilleure maitrise de l'information. Le besoin d'une information fiable est en constante évolution depuis plusieurs siècles ; et cela est du à plusieurs facteurs tels que :

- L'apparition des entreprises de très grande taille ;
- La décentralisation approfondie des entreprises modernes ;
- Le volume important du trafic généré par les flux réalisés par les entreprises ;
- L'utilisation de l'information dans la sécurité et le domaine médical.

Afin de satisfaire ces besoins et autres, l'homme a fait recours à l'outil informatique, en inventant les réseaux qui sont pour but de garantir une meilleure circulation de l'information. L'univers des systèmes d'information composé de réseaux et de systèmes informatiques prend un rôle et une place chaque jour plus important dans les entreprises.

Le système d'information est vulnérable et qu'il peut subir des piratages, des attaques (virus, hackers...), des pertes de données, des sinistres. Il est donc indispensable pour les entreprises de savoir définir et de garantir la sécurité de ses ressources informatiques. La gestion de la sécurité de système et de réseau de ces entreprises implique :

- La mise en place des mécanismes de sécurité préventifs pour protéger les données et les ressources du système ou du réseau contre tout accès non autorisé ou abusif ;
- Le déploiement des outils de sécurité pour détecter les attaques qui réussiraient à porter atteinte à la sécurité du réseau ou du système malgré les mesures préventives ;
- La mise en place des mécanismes de réponse aux attaques détectées.

Pour contrer et remédier à ces problèmes de sécurité, le mécanisme de réponse mise en place est le firewall. Cet outil à pour but de sécuriser le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux possible. Cela représente une sécurité supplémentaire rendant le réseau ouvert sur Internet beaucoup plus sûr. De plus, il peut permettre de restreindre l'accès interne vers l'extérieur. En effet, des employés peuvent s'adonner à des activités que l'entreprise ne cautionne pas, le meilleur exemple étant le jeu en ligne. En plaçant un firewall limitant ou interdisant l'accès à ces services, l'entreprise peut donc avoir un contrôle sur les activités se déroulant dans son enceinte.

Notre mémoire comprend trois chapitres :

- Le premier chapitre est consacré aux généralités sur les réseaux, la sécurité informatique et les la nécessité de la mise en œuvre d'une sécurité au sein d'un réseau informatique.
- Le deuxième chapitre est focalisé sur les firewalls, leurs principes et fonctionnement, ses différents types et architectures et ainsi que leurs place dans les DMZs (Zone démilitarisée).
- Le troisième chapitre est consacré à présenter la problématique de notre travail, la solution proposée, les outils de réalisation et l'ensemble des configurations faites dans le cadre d'implémenter l'architecture de la solution proposée.

Nous allons terminer notre mémoire par une conclusion générale tirée à travers notre travail.

1

Généralités sur les Réseaux et la Sécurité Informatique

1.1 Introduction

L'utilisation de l'Internet est devenue de plus en plus indispensable dans les entreprises, cela impose l'ouverture du système d'information aux partenaires ainsi qu'aux fournisseurs. La sécurité du réseau informatique de l'entreprise représente un enjeu majeur. Il est donc essentiel de mettre en place une organisation permettant de protéger efficacement les données de l'entreprise.

Ce chapitre est scindé en deux parties : la première partie décrira quelques notions sur les réseaux informatiques, et la deuxième partie sera concentrée sur la sécurité informatique.

1.2 Généralités sur les Réseaux

D'une manière générale, un réseau n'est rien d'autre qu'un ensemble d'objets ou des personnes connectées ou maintenues en liaison, dont le but est d'échanger des informations ou des biens matériels [16].

1.2.1 Définition d'un réseau

Le réseau informatique, c'est l'ensemble des ressources de communication (matérielles et logicielles), d'ordinateurs et des clients partageable et géographiquement distribués cherchant à exploiter ces ressources.
En d'autres termes, c'est l'ensemble d'équipements interconnectés selon des règles et protocoles biens définis, partageable et géographiquement distribués [23].

1.2.2 Classification des réseaux selon la taille

Nous distinguons généralement quatre catégories de réseaux informatiques, différenciées par la distance maximale séparant les points les plus éloignés du réseau :

- **Les réseaux personnels, ou PAN (Personnel Area Network) :** interconnectent sur quelques mètres des équipements personnels (tels que les terminaux UMTS, portables, organiseurs, ...etc.) d'un même utilisateur[14].

- **Les réseaux locaux, ou LAN (Local Area Network) :** correspondent par leur taille aux réseaux intra-entreprise .Ils servent au transport de toutes les informations numériques de l'entreprise. En règle générale, les bâtiments à câbler s'étendent sur plusieurs centaines de mètres. Les débits de ces réseaux vont de quelques mégabits à quelques gigabits par seconde [14].

- **Les réseaux métropolitains, ou MAN (Metropolitan Area Network) :** permettent l'interconnexion des entreprises ou éventuellement des particuliers sur un réseau spécialisé à haut débit qui est géré à l'échelle d'une métropole. Ils doivent être capables d'interconnecter les réseaux locaux de différentes entreprises pour leur donner la possibilité de dialoguer avec l'extérieur [14].

- **Les réseaux étendus, ou WAN (Wide Area Network) :** sont destinés à transporter des données numériques sur des distances à l'échelle d'un pays, voire d'un continent ou de plusieurs continents. Le réseau est soit terrestre, et il utilise dans ce cas des infrastructures au niveau du sol, essentiellement de grands réseaux de fibre optique, soit hertzien, comme les réseaux satellite [14].

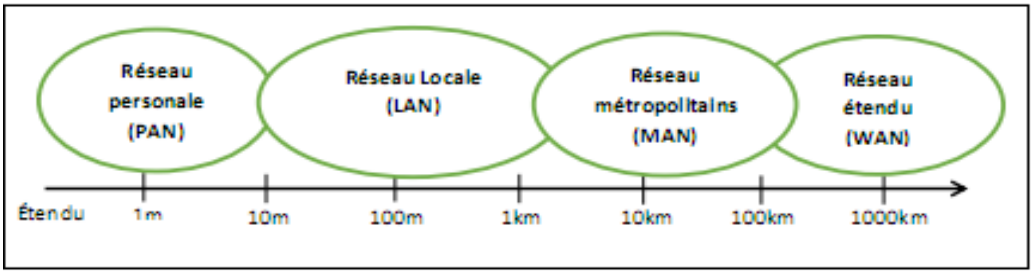


FIG. 1.1 – Classification des réseaux informatique

1.2.3 Architecture des réseaux

Pour permettre le transfert des donneés, les réseaux peuvent être organisés selon deux principes : les réseaux post à post et les réseaux client-serveur.

- **Réseaux post à post :** sur un réseau post à post, les ordinateurs sont connectés directement l'un à l'autre et il n'existe pas d'ordinateur central [19].

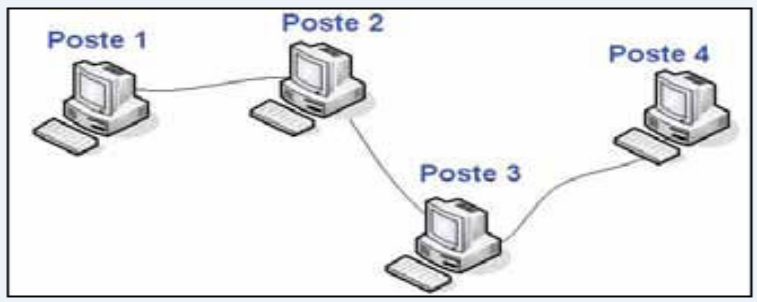


FIG. 1.2 – Réseaux poste à poste

- **Réseaux client-serveur :** sur un réseau à architecture client-serveur, tous les ordinateurs (*client*) sont connectés à un ordinateur central (*le serveur de réseau*), une machine généralement trés puissante en termes de capacité, elle est utilisée surtout pour le partage de connexion à l'Internet et pour les logiciels centralisés [19].

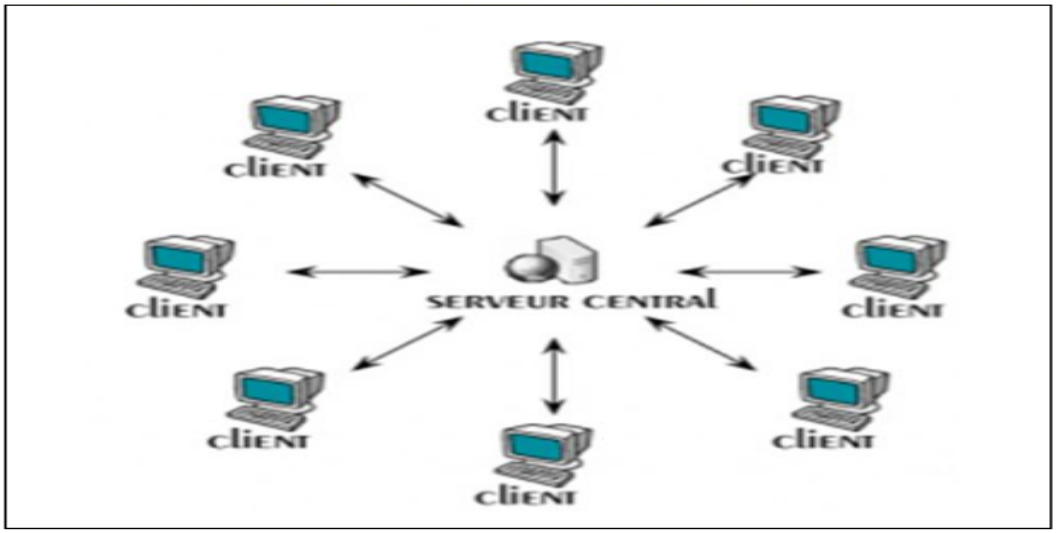


FIG. 1.3 – Réseaux client-serveur

1.2.4 Topologies des réseaux

La topologie d'un réseau recouvre tout simplement la manière dont sont reliés entre eux ses différents composants et la manière dont les interagissent. Il convient de distinguer[46] :

1. **La topologie logique** : qui représente la façon dont les données transitent dans les lignes de communication. Les tépologies logiques les plus courantes sont Ethernet, Token Ring.

2. **La topologie physique** : c'est le chemin de câblage apparent, donc ce que voit l'utilisatuer. Il existe plusieurs topologie parmi eux nous citons :

   – **La topologie linéaire :** consiste à relier les ordinateurs les uns à la suite des autres, en formant une ligne virtuelle. Offrant des avantages dans certains types d'utilisation (sécurité notamment, avec le cas des serveurs proxy), son problème principal est sa faible tolérance de panne. Un seul ordinateur qui défaille et l'ensemble du réseau (ou presque) peut se mettre à ne plus fonctionner. La réparation est alors impérative.

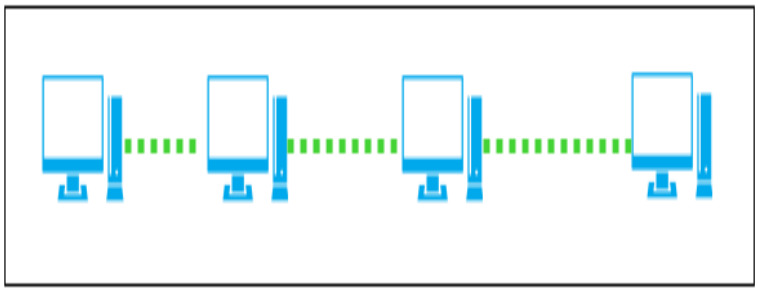


FIG. 1.4 – Topologie linéaire

– **La topologie en bus :** c'est en quelque sorte une topologie linéaire améliorée. Les hôtes sont reliés les uns à la suite des autres, mais la défaillance de l'un d'entre-eux ne perturbe pas le fonctionnement du réseau. On bouche généralement les extrémités d'un réseau utilisant la topologie en bus par des bouchons, pour éviter les réflexions du signal.

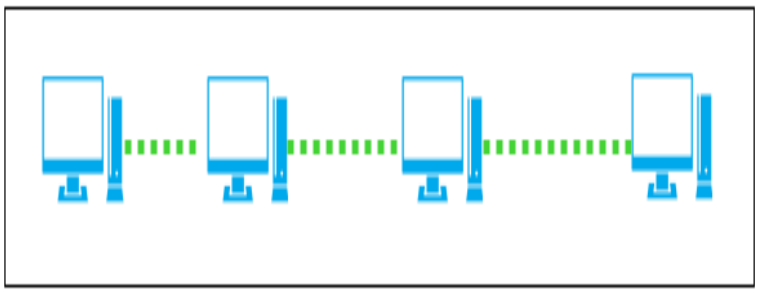


FIG. 1.5 – Topologie en bus

– **La topologie en anneau :** les ordinateurs ou périphériques sont reliés les uns aux autres, il n'y a pas d'extrémités contrairement à un réseau linéaire. La défaillance d'un élément n'entraîne pas de panne du réseau.

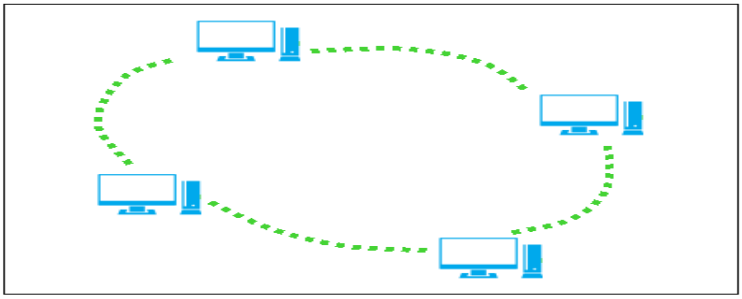


FIG. 1.6 – Topologie en anneau

– **La topologie en étoile :** c'est la plus utilisée. Un concentrateur (Hub, Switch, Routeur) représente un noeud du réseau. Les ordinateurs ou périphériques sont reliés à lui. Toute panne d'un périphérique n'entraine pas de panne du réseau. En revanche, la défaillance d'un concentrateur perturbera la communication de tous les périphériques et ordinateurs qui en dépendent.

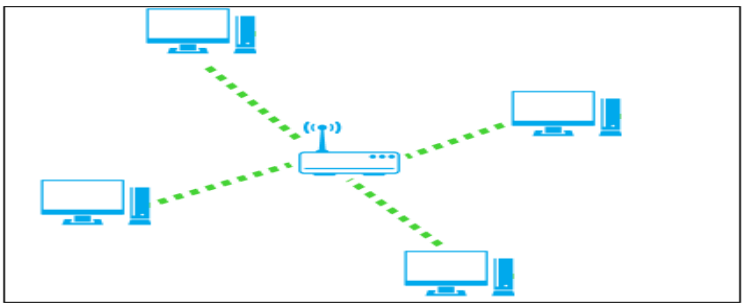


FIG. 1.7 – Topologie en étoile

– **La topologie maillée :** Internet est basé sur une topologie maillée (aussi appelée topologie mesh), qui est elle-même une amélioration de la topologie en étoile. Issue de recherches militaires, il s'agit de pouvoir relier un hôte à tous les autres, de manière directe ou indirecte. Il n'y a pas de hiérarchie centrale. L'information peut ainsi parcourir des chemins différents pour arriver au même destinataire. L'avantage principal de ce type de réseau est qu'il est très tolérant aux pannes, très évolutif, le tout simplement.

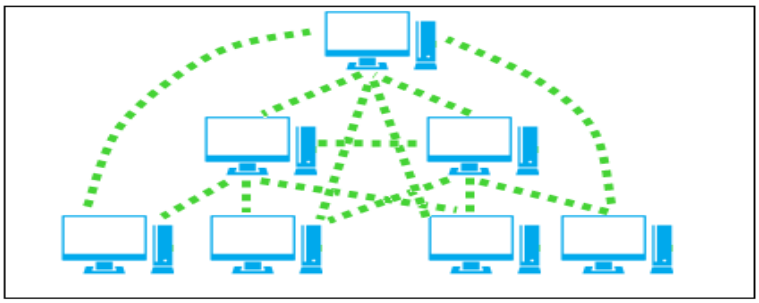


FIG. 1.8 – Topologie maillée

1.2.5 Equipement d'interconnexion

La mise en place d'un réseau soulève de nombreuses questions sur les contraintes d'utilisation. Comment faire si le réseaux a créer dépasse les distances maximaes imposées par le type de câble utilisé ? Comment faire parvenir les informations a d'autres réseaux que le sein ? Comment relier des réseaux utilisant des protocoles de communication différents ? Toutes ces questions peuvent être résolus grâce à différents types de matériels qui sont [19] :

- **Répéteur (repeater) :** c'est un équipement simple permettant de régénérer un signal entre deux nœuds du réseau, afin d'étendre la distance de câblage d'un réseau. Il travaille uniquement au niveau de la couche physique du modèle OSI, c'est-à-dire qu'il ne travaille qu'au niveau des informations binaires circulant sur la ligne de transmission et qu'il n'est pas capable d'interpréter les paquets d'informations.

- **Concentrateur (Hub) :** c'est un élément matériel tout comme le répéteur, opère au niveau de la couche physique du modèle OSI, permettant de concentrer le trafic réseau provenant de plusieurs hôtes, et de régénérer le signal. Il est ainsi une entité possédant un certain nombre de ports (il possède autant de ports qu'il peut connecter de machines entre elles, généralement 4,8 ,16 ou 32). Son unique but est de récupérer les données binaires parvenant sur un port et de les diffuser sur l'ensemble des ports, c'est pour cela il est parfois appelé répéteurs multiports.

- **Pont (bridge) :** le pont travaille au niveau logique (couche 2) de modèle OSI, c'est-à-dire qu'il est capable de filtrer les trames en ne laissant passer que celles dont l'adresse correspond à une machine située à l'opposé du pont. Ainsi le pont permet de segmenter un réseau en concevant au niveau du réseau local les trames destinées à ce dernier, et en transmettant les trames destinées aux autres réseaux. Cela permet de réduire le trafic (collision) sur chacun des réseaux et d'augmenter la confidentialité.

- **Le commutateur (switch) :** c'est un pont multiports, c'est-à-dire qu'il s'agit d'un élément actif agissant au niveau 2 du modèle OSI, il analyse les trames arrivant sur ses ports d'entrée et filtre les données afin de les aiguiller uniquement sur les ports adéquats (commutation). Le commutateur permet d'allier les propriétés du pont en matière de filtrage et du concentrateur en matière de connectivité.

- **passerelle (gateway) :** les passerelles sont des systèmes matériels et logiciels per-

mettant de faire la liaison entre deux réseaux, servant notamment à faire l'interface entre des protocoles différents.

– **Routeur :** c'est un matériel d'interconnexion qui a accès à toutes les informations des couches 1,2 et 3, notamment aux adresses logiques qui sont indépendantes de toute méthode d'accès et de topologie physique. Le routeur va donc modifier la couche physique pour changer de support la couche MAC, pour préciser les nouvelles adresses MAC, la sienne et celle du prochain périphérique intermédiaire (éventuellement un autre routeur), tout en tenant compte de la nouvelle méthode d'accès. Les adresses logiques permettent d'avoir une vision logique de l'inter-réseau, ce qui conduit un routeur à connaitre les différents chemins possibles pour atteindre un destinataire. Le routeur doit donc connaitre la liste de tous les réseaux logiques existants qu'il conserve dans une table de routage.

1.2.6 Modèle de référence OSI

Le modèle OSI (Open System Interconexion) définit une sorte de langage commun. Ce modèle a été mis au point par l'ISO (International Standardization Organization) et il est devenu le socle de référence pour tout système de traitement de communications. Il est répartit les questions relatives au domaine des communications informatique selon sept couches classées par ordre d'abstraction croissant. Son objectif est d'assurer que les protocoles spécifique utilisés dans chacune des couches coopèrent pour assurer une communication efficaces. Décrivons succinctement le rôle de chaque couche [32] :

- **Physique :** elle convertit les signaux électrique en bits de données et inversement, selon qu'elle transmet ou reçoit les informations à la couche liaison de données.

- **Liaison de données :** elle est divisée en deux sous-couches :
  – Couches LLC qui assure le transport des trames et gère l'adressage des utilisateurs.

  – Couche MAC qui structure les bits de données en trames et gère l'adressage des cartes réseaux.
- **Réseau :** elle traite la partie donnée utile contenue dans la trame. Elle connait l'adresse de tous les destination choisit par le meilleur itinéraire pour l'acheminement. Donc, elle gère l'dressage logique et le routage.

- **Transtport :** elle segmente les données de la couche session, prèpare et contrôle les tâches de la couche réseau. Elle peut multiplier les voies d'accés et corrige les erreurs de transport.

- **Session :** son unité d'information est la transaction. Elle s'occupe de la gestion et la sécurisation du dialogue entre les machines connectées, les applications et les utilisateurs.

- **Présentation :** elle convertit les données en information compréhensible par les applications et les utilisateurs : syntaxe, sémantique, conversion des caractères graphiques, format des fichiers, cryptage et compression.

- **Application :** c'est l'interface entre l'utilisateur et les applications et le réseau. Elle concerne la messagerie, les transferts et partages des fichies, l'émulationde terminaux.

La figure 1.9 illustre les couches du modèle OSI et leurs Protocoles.

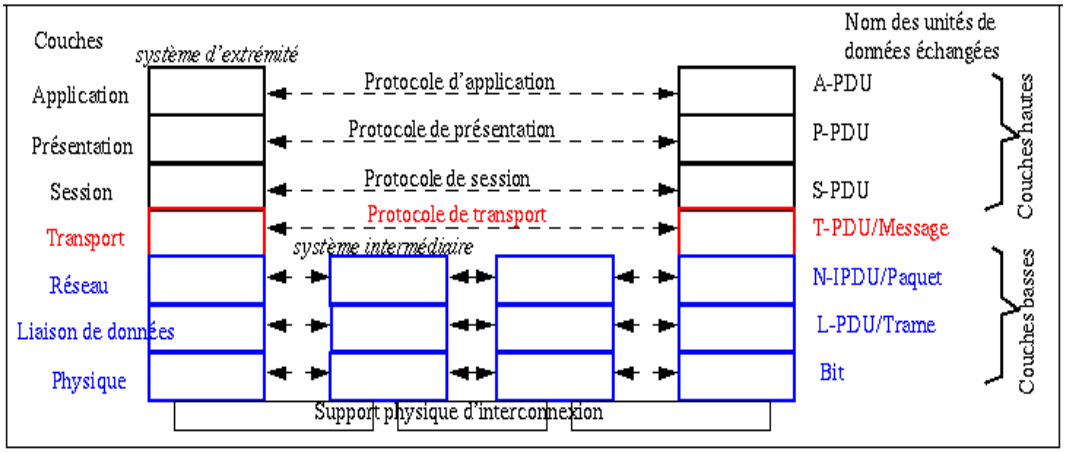


FIG. 1.9 – Les couches du modèle OSI et leurs protocoles

1.2.7 Modèle TCP/IP

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait 2 protocoles étroitement liés : un protocole de transport, TCP (Transmission Control Protocol) qu'on utilise "par-dessus" un protocole réseau, IP (Internet Protocol). Ce qu'on entend par "modèle TCP/IP", c'est en fait une architecture réseau en 4 couches dans

laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante. Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP [41].

Le schéma da la figure 1.10 nous montre la différence entre le modèle TCP/IP et le modèle OSI.

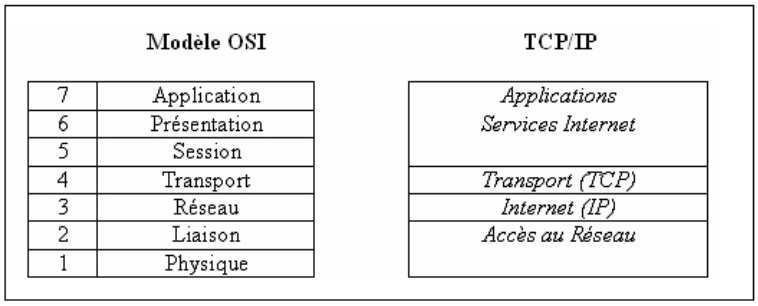


FIG. 1.10 – Comparison entre le modèle OSI et le modèle TCP/IP

1.3 La Sécurité Informatique

1.3.1 Terminologie de la sécurité informatique

Le système d'information représente un patrimoine essentiel de l'organisation qu'il convient de protéger. La sécurité informatique consiste à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu [36].

La sécurité informatique est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces Nous allons brièvement évoquer quelques mots clés qui sont largement repris dans la littérature informatique lorsque la sécurité est abordée :

- **Une vulnérabilité :** est une faiblesse 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. L'expression faille de sécurité est également employée [36].

- **Une menace :** La menace désigne l'exploitation d'une faiblesse de sécurité par un attaquant, qu'il soit interne ou externe à l'entreprise. La probabilité qu'un événement exploite une faiblesse de sécurité est généralement évaluée par des études statistiques, même si ces dernières sont difficiles à réaliser [9].

- **Une attaque :** : est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel) ou bien même de l'utilisateur à des fins non autorisées par le propriétaire du système et généralement répréhensibles [9].

- **Un risque :** est le degré d'exposition des actifs informationnels aux menaces, en fonction de la valeur de ces actifs et des mesures en place pour en préserver la sécurité [36].

$$\text{Vulnérabilité} + \text{Menace} = \text{Risque}$$

1.3.2 Politique de sécurité

Une politique de sécurité est perçue comme une réglementation particulière dont l'objectif est de décrire la façon de gérer, protéger et diffuser les informations et les autres ressources sensibles au sein d'un système informatique. Une politique de sécurité sera bien souvent tout à la fois le manuel de savoir-vivre de l'utilisateur, son règlement intérieur pour l'informatique et une base solide pour assurer la sécurité du système d'information. Elle est un ensemble de règles définissant le comportement des utilisateurs, son objectif est la préservation et la sécurisation de l'intégralité du système informatique avec ses bases de données [21].

1.3.3 Objectifs de la sécurité informatique

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. Elle vise généralement aux principaux objectifs suivants :

1.3.3.1 L'authentification et identification

Le service d'authentification permet d'assurer qu'une communication est authentique (fournir une identification et de la prouver). Nous pouvons distinguer deux types d'authentification : L'authentification d'un tiers qui consiste pour ce dernier à prouver son identité et l'authentification de la source des données qui sert à prouver que les données reçues viennent bien d'un tel émetteur déclaré [17].

Sur la plupart des réseaux, le mécanisme d'authentification utilise une paire code d'identification /mot de passe. Cependant, en raison de la vulnérabilité constamment associée à l'utilisation des mots de passe, il est souvent recommandé de recourir à des mécanismes plus robustes tels que l'authentification par des certificats, des clés publiques ou à travers des centres de distribution des clés, les signatures numériques peuvent aussi servir à l'authentification. Il existe plusieurs protocoles d'authentification, nous citons quelques-uns parmi eux :PAP, SPAP, CHAP, MS-CHAP, EAP,... etc [17].

1.3.3.2 La confidentialité

La confidentialité est un service de sécurité qui consiste à assurer que seules les personnes autorisées peuvent prendre connaissance des données. Pour obtenir ce service, on utilise généralement le chiffrement des données concernées à l'aide d'un algorithme cryptographique [17].

Quelques algorithmes de chiffrements : la famille asymétrique : RSA, ELGmail, Deffie_Hellman, ...etc. Et la famille symétrique : DES, 3DES, AES, ...etc [17].

1.3.3.3 L'intégrité

L'intégrité se rapporte à la protection contre les changements et les altérations. Si les données émises sont identiques à celles reçues alors il y a une intégrité. Des différences peuvent apparaître si quelqu'un tente de modifier ces données ou tout simplement si un problème de transmission/réception intervient [17].

Les techniques utilisées pour faire face à cela sont, les bits de parité, les checksums (somme de contrôle) ou encore les fonctions de hachage à sens unique (SHA_1, MD5,...etc)

[17].

1.3.3.4 La non-répudiation

Service permettant d'assurer qu'une entité ou un processus engagé dans une communication ne pourra nier avoir reçu ou émis un message. Assurée par la signature numérique (RSA+SHA1, RSA+MD5, ...etc.) et la cryptographie à clé publique et privée [24].

1.3.3.5 La disponibilité

La disponibilité est la propriété qu'une information soit accessible lorsqu'un utilisateur autorisé en a besoin. Cela signifie que le système informatique doit fournir l'accès à l'information pour que les utilisateurs autorisés puissent la lire ou la modifier, et faire en sorte qu'aucun utilisateur ne puisse empêcher les utilisateurs autorisés d'accéder à l'information [7].

1.3.3.6 Le contrôle d'accès

Le contrôle d'accès est la faculté de limiter et de contrôler l'accès à des systèmes et des applications via des maillons de communications. Pour accomplir ce contrôle, chaque entité essayant d'obtenir un accès doit d'abord s'authentifier, de telle sorte que les droits d'accès puissent être adaptés à son cas [26].

1.3.4 Mécanismes de la sécurité

Dans ce qui suit, nous présentant les mécanismes cryptographiques les plus utilisées pour assurer : la confidentialité, l'intégrité, l'authentification et la non-répudiation.

La cryptographie demeure la technique indispensable. D'une part, protéger la confidentialité des informations transmises sur les réseaux ou stockées dans les serveurs de données et d'autre part, assurer l'intégrité d'un document ou pour prouver l'authenticité d'une opération ou d'une transaction. Elle applique des concepts mathématiques et met en place des paradigmes informatiques afin de résister aux attaques potentielles d'assaillants ou de

prouver, de manière quasi sûre, qu'une procédure est incorruptible [2].

1.3.4.1 Cryptographie symétrique

La cryptographie symétrique consiste à utiliser la même clé pour le chiffrement ainsi que pour le déchiffrement. Il est donc nécessaire que deux interlocuteurs se soient mis d'accord sur une clé privée, où ils doivent utiliser un canal sécurisé pour l'échanger [2].

Les algorithmes informatiques développés pour réaliser des opérations de cryptographie symétriques sont : DES (Data Encryption Standard), Triple DES ou DES, EA (International Data Encryption Algorithm,), AES (Advanced Encryption Standard).[6]

1.3.4.2 Cryptographie asymétrique

Pour résoudre le problème de l'échange de la clé secrète, un nouveau type de cryptographie a été inventé, il s'agit de la cryptographie asymétrique. Elle désigne une méthode cryptographique faisant intervenir une paire de clés asymétrique (publique, privée). Elle utilise cette paire de clés pour le chiffrement et le déchiffrement. La clé publique est rendue publique et distribuer librement, et la clé privée quant à elle n'est jamais distribuée et doit être garder secrète. En pratique elle est utilisé pour :

- L'´echange d'une clé symétrique.
- La signature d'un hachage d'un message.

Les trois algorithmes à clé publique suivants sont les plus fréquemment employés : RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm), Diffie_Hellman [13].

1.3.4.3 Cryptographie hybride

C'est une combinaison des meilleures fonctionnalités des deux types de cryptographie précités. La cryptographie hybride consiste à créer d'abord une clé de session qui est une clé secrète à usage unique. Pour le cryptage et le décryptage, c'est la clé de session qui est employée par un algorithme symétrique, donnant ainsi une rapidité aux deux processus [5].

Parmi les algorithmes l'utilisant, il y a PGP (Pretty Good Privacy), GnuPG (GNU PrivacyGuard) et SSL (Secure Socket Layer) qui est un protocole plus qu'un algorithme [20].

1.3.4.4 Fonction de hachage

Une fonction de hachage appelée aussi fonction de hachage à sens unique, est une fonction mathématique qui permet de transformer une chaîne de longueur variable en une chaîne de taille inférieure et fixe appelée empreinte, condensé ou haché.

La fonction de hachage assure que, si l'information était échangée en qui que ce soit, même d'un seul bit, une sortie totalement différente serait produite.

Parmi les fonctions de hachage les plus utilisées, notons : MD5 (Message Degest 5),SHA-1(Standard Hash Algorithm - 1), ...etc [13][23].

1.3.4.5 Signature numérique

L'une des utilisations de la cryptographie à clé publique est qu'elle permet l'établissement des signatures numériques. Ces dernières offrent au destinataire la possibilité de vérifier l'authenticité de l'expéditeur (origine exacte).

Ces signatures sont liées aux informations qu'elles attestent, donc, elles sont difficiles à falsifier. Elles apportent aussi l'authentification et l'identification des parties concernées et la non-répudiation en cas de désaveu de la part de l'expéditeur.

Le principe de la signature numérique est qu'elle est le résultat du cryptage du document et d'autres informations concernant l'expéditeur avec sa clé privée, affirmant ainsi son authenticité [13].

1.3.4.6 Certificat à clé publique

Un certificat, validé par une autorité de certification (AC), est l'équivalent d'une carte d'identité. Il repose sur les mêmes principes. Il permet de justifier de l'identité d'un individu (ou d'une entité) sur une présentation du certificat. Quand deux entités veulent établir une connexion sécurisée entre elle, elles échangent juste leurs certificats. Ce dernier contient

l'identité et la clé publique de cette entité.

De ce fait, les interlocuteurs auront une information qui prouve l'appartenance réelle d'une clé publique à son propriétaire supposé [27][30].

1.3.5 Attaques informatiques

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à des attaques qui peuvent être de différents types.

- **Attaques d'accès :** Une attaque d'accès ou une attaque d'interception est une tentative d'accès à l'information par une personne non autorisée. Ce type d'attaque concerne la confidentialité de l'information, et peut se produire par plusieurs techniques telles que : l'homme du milieu (Man-In-The-Middle), le sniffing, les chevaux de Troie, porte dérobée. . ..etc [12].

- **Attaques de modification :** Un tiers non autorisé intercepte des données et les modifie avant de les envoyer au destinataire.Il s'agit d'une attaque sur l'intégrité de l'information. Elle peut se présentée sous forme de : virus, sflooding, bombe logique. . .. . ..etc [3].

- **Attaques par déni de service :** Les attaques de type Denial-of-Service ont pour but de saturer un routeur ou un serveur afin de le crasher ou en préambule d'une attaque massive. Ces types d'attaque sont très faciles à mettre en place et très difficile à empêcher. Parmi les technique utilisés pour réaliser ce type d'attaque on cite : Le flooding, le débordement de tampon, le smurf . . ..etc [13].

- **Attaques de rejeu :** L'attaquant qui a réussi à intercepter des messages les réémet dans le but d'obtenir des informations ou de perturber la cible de l'attaque. Nous considérons qu'il s'agit d'une attaque sur l'intégrité des messages.

- **Attaque de fabrication :** Un tiers non autorisé insère des données contrefaites dans les communications de l'application. Il s'agit d'une attaque sur l'authentification.

- **Attaques d'interruption :** Une partie de l'application distribuée est détruite ou est

devenue inaccessible. Il s'agit d'une attaque sur la disponibilité [3].

1.3.6 Mesures et techniques d'atténuation d'attaques

En matière de gestion des risques, il est crucial que chaque entreprise prenne les mesures les plus adéquates.

1.3.6.1 Programme antivirus

Les antivirus sont des logiciels conçus pour repérer les traces d'activité des virus et les bloquer, et isoler ou supprimer les fichiers qui en sont responsables. Leur mode de fonctionnement est basé sur une veille permanente, un programme antivirus doit être installé et actif sur tout ordinateur et qui doit être tenu à jour [39].

1.3.6.2 Correctifs mise à jour de système d'exploitation

Il est essentiel de télécharger et d'activer les mises à jour automatiques de sécurité de fournisseur du système d'exploitation, d'installer et d'appliquer les correctifs (qui sont des compléments de logicielsvisant à corriger les failles de sécurité dans les systèmes d'exploitation ou les applications), pour pallier aux nouvelles failles de sécurité et rester protégé contre les menaces et les pirates [20][25].

1.3.6.3 VLAN (Virtual Local Area Network)

Un VLAN est un domaine de diffusion limité, qui se comporte comme un réseau local partagé. La différence avec un vrai réseau local provient de l'emplacement géographique des clients, qui peut être quelconque. L'idée est d'émuler un réseau local et donc de permettre à des clients parfois fortement éloignés géographiquement d'agir comme s'ils étaient sur le même réseau local. Les échanges à l'intérieur d'un VLAN sont sécurisés et les communications contrôlées [10][15].

1.3.6.4 VPN (Virtual Private Network)

Un VPN est une connexion réseau privée sécurisée construite au sommet d'infrastructures accessibles au public. Il offre une alternative à l'utilisation du serveur proxy pour

accéder à distance aux ressources ainsi qu'une méthode sécurisée pour s'authentifier sur un réseau. Grâce aux réseaux privés virtuels, ils permettent à l'administrateur l'intervention à distance sur un réseau et aux employés d'accéder au réseau à partir de n'importe quel endroit dans le monde et d'une simple connexion à Internet. Aucun obstacle ne vient empêcher le travail à domicile, ce qui permet aux entreprises d'avoir une meilleure souplesse [31].

1.3.6.5 IDS (Systèmes de détection d'intrusions)

Un système automatisé dont le rôle est la détection des intrusions dans un système informatique tout en examinant les audits de sécurité fournis par le système d'exploitation ou bien les outils de contrôle du réseau. Son but principal est la détection des utilisations non autorisées, les mauvaises utilisations et les abus dans un système informatique par les utilisateurs internes et externes [22].

1.3.6.6 IPS (Système de prévention d'intrusion)

Le fonctionnement d'un IPS est similaire à celui d'un IDS. Il capture le trafic du réseau puis l'analyse. Mais au lieu d'alerter l'utilisateur d'une intrusion ou d'une attaque, l'IPS bloque directement les intrusions en supprimant les paquets illégitimes. Pour informer l'utilisateur, l'IPS peut aussi remplir un fichier de journalisation qui contiendra la liste des paquets supprimés et éventuellement un message indiquant la raison de cette suppression [11].

1.3.6.7 Firewall (pare-feu)

Le firewall (pare-feu) est un système aux fonctions de filtrage évoluées. Indépendamment des fonctions de routage et de translation d'adresses, chaque paquet reçu est examiné, une décision de rejet ou d'acceptation est prise en fonction de nombreux critères (l'adresse destination, l'adresse source, le protocole transporté (ICMP, UDP...), le port destination, le port source, ...etc.)[23].

1.4 Conclusion

Au cours de ce chapitre, nous avons présenté quelques généralités sur les réseaux informatique. Ensuite, nous avons donné une vue globale sur la sécurité des réseaux, où nous avons énuméré quelques attaques qui peuvent perturber et corrompre le fonctionnement du réseau, et cité quelques techniques pour atténuer ces dernières.

Le chapitre suivant, sera consacré à l'une des techniques d'atténuation d'attaque citée précédemment, qui est les firewalls.

2

La sécurité des réseaux : Firewalls

2.1 Introduction

Les firewalls ont aujourd'hui pris une place très importante dans les réseaux informatiques . Dans ce chapitre, nous allons voir que veut dire un firewall, les différentes catégories existantes et les différentes architectures.

2.2 Définition d'un firewall

Un firewall, appelé aussi coupe-feu ou pare-feu à pour but de contrôler et de filtrer l'accès entre un réseau d'entreprise ou l'ordinateur d'un particulier et un autre réseau qui est ici Internet. Le firewall peut être soit un objet matériel ou un programme fonctionnant sur un ordinateur [4].

FIG. 2.1 – Firewall représenté par un mur entre un ordinateur et l'Internet

Dans les deux cas, le firewall doit se placer à la jonction entre le réseau à protéger et Internet. Le firewall examine tout le trafic entre les deux réseaux pour voir s'il correspond à certains critères définis par l'administrateur. Si cela correspond, les données accèdent au réseau, sinon elles sont stoppées. Un firewall filtre aussi bien dans le sens de l'envoi de données vers l'extérieur que dans celui de la réception.Un firewall peut ainsi empêcher un logiciel d'accéder a Internet ou une personne d'accéder a certains services comme le FTP par exemple [4].

2.2.1 De quoi protège un firewall

Certains firewalls laissent uniquement passer le courrier électronique. De cette manière ils interdisent toute autre attaque qu'une attaque basé sur le service de courrier. D'autres firewalls, moins strictes,bloque uniquement les services reconnus comme étant des services dangereux [4].

Généralement,les firewalls sont configures pour protéger contre les accès non authentifier du réseau externe. Ceci, plus qu'autre chose, empêche les vandales de se loger sur des machines de vote réseau interne, mais autorise les utilisateurs de communiquer librement avec l'extérieur [4].

Les firewalls sont également intéressant dans le sens ou ils constituent un point unique ou l'audit et la sécurité peuvent être imposes. Tous les échanges passeront par lui . Il pourra donner des résumés de trafic, des statistiques sur ce trafic, ou encoretoutes les connexions

entre les deux réseaux [4].

2.2.2 De quoi ne protège pas un firewall

Un firewall ne protège pas des attaques qui ne passe pas par lui . Certaines entreprises achètent des firewalls a des prix incroyables alors que certains de leurs employés sont parfois connectes par modem au monde exterieur. Il est important de noter qu'un firewall doit être a la mesure de politique de sécurité globale du réseau [4].

Il ne sert à rien de mettre une porte blindée sur une maison en bois. par exemple, un site contenant des documents top-secret n'a pas besoin d'un firewall : il ne devrait tout simplement pas être connecte a Internet, et devrait être isole du reste du réseau [4].

Une autre chose contre laquelle un firewall ne peut protéger est les traites qui sont a l'intérieur de l'entreprise. Si un espion industriel décide de faire sortir des données, il y arrivera, surtout sur disquette. Il faut mieux vérifier qui a accès aux informations que de mettre un firewall dans ce cas [4].

Les firewalls ne protègent pas très bien des virus. Il y a trop de manières différentes de coder des fichiers pour les transfère. En d'autres termes, un firewall ne pourra pas remplacer l'attention et la conscience des utilisateurs qui doivent respecter un certain nombre de règles pour éviter les problèmes. La première étant bien évidemment de ne jamais ouvrir un fichier attache a un mail sans être sûr de sa provenance [4].

Il faut prendre des mesures globales et importantes contre les virus. Avant de traquer les virus a l'entrée du réseau, il faut s'assurer que chaque poste de travail dispose d'un antivirus. Les virus passe également tres facilement par disquette. Les virus sur Internet sont bien moins important que les virus sur disquette [4].

Quoiqu'il en soit, de plus en plus de vendeurs de firewall vous offrent des firewalls qui détectent les virus. Ils permettent probablement d'arrêter les virus simple. Ne comptez pas sur leur protection [4].

2.3 Principe de fonctionnement

Le fonctionnement d'un firewall repose sur le filtrage des packets cela peut se faire de différentes manières. Il existe deux types de firewall qui sont les filtres de paquet et les passerelles.

2.3.1 Filtre de paquets

Le filtrage du trafic de données se fait au niveau des couches 3 et 4 du modèle OSI. Certains firewalls sont en fait des routeurs possédant des fonctions de filtrage de paquets. Avec des règles appropriées, l'administrateur réseau peut interdire ou autoriser un certain nombre de services ainsi que bloquer les accès aux équipements de son site, tout en permettant à ses machines l'accès aux services de l'Internet. Le routeur doit être configuré avec une liste d'accès.[47]

Une liste d'accès définit les conditions pour qu'un paquet puisse franchir un routeur. Les informations contenues dans ces listes portent :

- Sur le numéro du protocole de niveau 3, les adresses IP, les numéros de ports...
- D'autres informations dans le paquet comme les drapeaux TCP
- Le type de la règle, c'est-à-dire soit une autorisation soit un refus de faire traverser le paquet [47].

2.3.2 Passerelle

Il existe deux types de passerelles :

- **Passerelles de niveau applicatif (proxy)**

  Les passerelles applicatives sont des serveurs effectuant un filtrage plus ou moins fin sur les données échangées entre deux réseaux pour un service TCP/IP particulier. Ces passerelles sont situées entre un client du réseau interne et un serveur du réseau externe. Pour chaque communication, deux connexions sont donc à considérer : client/passerelle et passerelle/serveur [47]

  .

  – Les proxies filtrent en fonction du service demandé : Telnet, FTP, SMTP, HTTP...

- Le client se connecte au serveur proxy et demande l'accès au serveur distant.
- Le serveur proxy vérifie l'adresse du client, authentifie le client à l'aide d'un serveur d'authentification (type RADIUS) et l'autorise à se connecter sur le serveur.
- Le serveur proxy se connecte sur le serveur distant et relaie les données entre les deux connexions [47].

- **Passerelles de niveau circuit**

Les passerelles de niveau circuit filtrent au niveau transport. L'avantage est qu'elles sont communes à toutes les applications TCP/IP [47].

- Le client établit une connexion TCP avec la passerelle en demandant de communiquer avec le serveur.
- La passerelle peut :

  1. vérifier l'adresse IP du client.
  2. autoriser une connexion sur un port pour une durée maximale fixée.
  3. n'autoriser la réutilisation d'un même port qu'après un certain délai.
  4. authentifier un terminal

- La passerelle se connecte au serveur et relaie les données entre les deux connexions TCP.[47]

2.4 Différentes catégories de firewall

Depuis leur création, les firewalls ont grandement évolué. Ils sont effectivement la première solution technologique utilisée pour la sécurisation des réseaux. De ce fait, il existe maintenant différentes catégories de firewall. Chacune d'entre-elles disposent d'avantages et d'inconvénients qui lui sont propre.

2.4.1 Firewall sans états (stateless)

Ce sont les firewalls les plus anciens mais surtout les plus basiques qui existent. Ils font un contrôle de chaque paquets indépendamment des autres en se basant sur les règles pré-

définies par l'administrateur (généralement appelées ACL, Access Control List) [28].

Ces firewalls interviennent sur les couches réseau et transport. Les règles de filtrages s'appliquentalors par rapport à une d'adresses IP sources ou destination, mais aussi par rapport à un port source ou destination [28].

2.4.2 Firewall à états (stateful)

Les firewalls à états sont une évolution des firewalls sans états. La différence entre ces deux types de firewall réside dans la manière dont les paquets sont contrôlés. Les firewalls à états prennent encompte la validité des paquets qui transitent par rapport aux paquets précédemment reçus. Ils gardent alors en mémoire les différents attributs de chaque connexion, de leur commencement jusqu'à leur fin, c'est le mécanisme de stateful inspection.

De ce fait, ils seront capables de traiter les paquets non plus uniquement suivant les règles définies par l'administrateur, mais également par rapport à l'état de la session :

- NEW : Un client envoie sa première requête.
- ESTABLISHED : Connexion déjà initiée. Elle suit une connexion NEW.
- RELATED : Peut être une nouvelle connexion, mais elle présente un rapport direct avec uneconnexion déjà connue.
- INVALID : Correspond à un paquet qui n'est pas valide [28].

Les attributs gardés en mémoires sont les adresses IP, numéros de port et numéros de séquence des paquets qui ont traversé le firewall. Les firewalls à états sont alors capables de déceler une anomalie protocolaire de TCP. De plus, les connexions actives sont sauvegardées dans une table des états de connexions. L'application des règles est alors possible sans lire les ACL à chaque fois, car l'ensemble des paquets appartenant à une connexion active seront acceptés [28].

Un autre avantage de ce type de firewall, se trouve au niveau de la protection contre certaines attaques DoS comme par exemple le Syn Flood. Cette attaque très courante consiste à envoyer en masse des paquets de demande de connexion (SYN) sans en attendre la réponse (c'est ce que l'onappel flood). Ceci provoque la surcharge de la table des connexions des serveurs ce qui les rendincapable d'accepter de nouvelles connexions. Les firewalls stateful étant capables de vérifier l'étatdes sessions, ils sont capables de détecter les tentatives

excessives de demande de connexion. Il estpossible, en autre, ne pas accepter plus d'une demande de connexion par seconde pour un clientdonné [28].

Un autre atout de ces firewalls est l'acceptation d'établissement de connexions à la demande. C'est à dire qu'il n'est plus nécessaire d'ouvrir l'ensemble des ports supérieurs à 1024. Pour cette fonctionnalité, il existe un comportement différent suivant si le protocole utilisé est de type orienté connexion ou non. Pour les protocoles sans connexion (comme par exemple UDP), les paquets de réponses légitimes aux paquets envoyés sont acceptés pendant un temps donné. Par contre, pour les protocoles fonctionnant de manière similaire à FTP, il faut gérer l'état de deux connexions (donnée et contrôle). Ceci implique donc que le firewall connaisse le fonctionnement du protocole FTP (et des protocoles analogues), afin qu'il laisse passé le flux de données établi par le serveur [28].

2.4.3 Firewall applicatif

Les firewalls applicatif (aussi nommé pare-feu de type proxy ou passerelle applicative) fonctionnesur la couche 7 du modèle OSI. Cela suppose que le firewall connaisse l'ensemble des protocoles utilisés par chaque application. Chaque protocole dispose d'un module spécifique à celui-ci. C'est à dire que, par exemple, le protocole HTTP sera filtré par un processus proxy HTTP [28].

Ce type de firewall permet alors d'effectuer une analyse beaucoup plus fine des informations qu'ils font transiter. Ils peuvent ainsi rejeter toutes les requêtes non conformes aux spécifications du protocole. Ils sont alors capables de vérifier, par exemple, que seul le protocole HTTP transite à travers le port 80. Il est également possible d'interdire l'utilisation de tunnels TCP permettant de contourner le filtrage par ports. De ce fait, il est possible d'interdire, par exemple, aux utilisateurs d'utiliser certains services, même s'ils changeant le numéro de port d'utilisation du service (comme par exemple les protocoles de peer to peer)[28].

2.4.4 Firewall authentifiant

Les firewalls authentifiant permettent de mettre en place des règles de filtrage suivant les utilisateurs et non plus uniquement suivant des machines à travers le filtre IP. Il est alors possible de suivre l'activité réseau par utilisateur [28].

Pour que le filtrage puisse être possible, il y a une association entre l'utilisateur connecté et l'adresse IP de la machine qu'il utilise [28] .

2.4.5 Firewall personnel

Les firewalls personnels sont installés directement sur les postes de travail. Leur principal but est de contrer les virus informatiques et logiciels espions (spyware) [28].

Leur principal atout est qu'ils permettent de contrôler les accès aux réseaux des applicationsinstallés sur la machines. Ils sont capables en effet de repérer et d'empêcher l'ouverture de ports par des applications non autorisées à utiliser le réseau [28].

2.5 Types d'architectures

Pour assurer une meilleure sécurité du réseau, il est important de mettre en place plusieurs filtres de différents niveaux, mais il s'accompagne d'un cout plus élevé.

2.5.1 Firewall avec routeur de filtrage

La solution firewall la plus simple, mais aussi la moins sure, se borne au réseau. On l'obtient en configurant le routeur qui assure la connexion avec l'Internet. La figure suivante illustre cette solution appelée Firewall avec routeur de filtrage [39] :

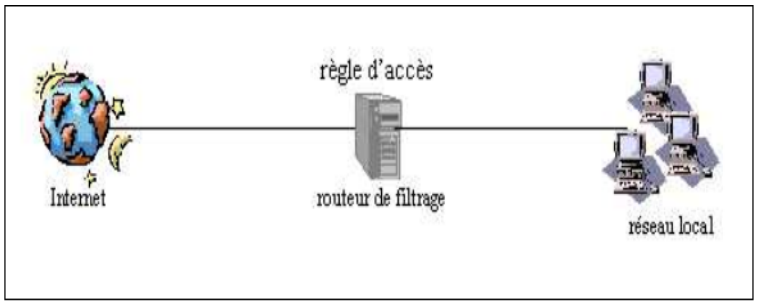


FIG. 2.2 – Firewall avec routeur de filtrage

Cette solution permet de réaliser les différents serveurs d'un Intranet sur plusieurs systèmes. Le routeur de filtrage contient les autorisations d'accès basées exclusivement sur les

adresses IP et les numéros de port.[39]

Avantages : facilité de configuration, bon marché, de plus il fournit des traces exploitables avec la possibilité d'alarmes pour [39] :

- Une vérification du bon fonctionnement des filtres du routeur,
- Il y ait encore un peu de temps pour réagir si le routeur est compromis.

Inconvénient : lorsque le routeur est contourné ou paralysé, le réseau entier est ouvert [39].

2.5.2 Passerelle double - le réseau bastion

Il existe une autre possibilité permettant de réaliser un firewall d'application à peu de frais : La passerelle double. Comme son nom l'indique, il s'agit d'un ordinateur inclus à la fois dans les deux réseaux Internet et Intranet. Cette machine doit être équipée de deux cartes réseau. Comme elle est la seule soupape de sécurité entre les deux réseaux, elle doit être configurée avec le plus grand soin [39].

La passerelle double n'autorise aucun trafic IP entre les réseaux. On l'appelle également réseau bastion, car il contrôle tous les services accessibles de l'extérieur comme de l'intérieur du réseau interne tels que les serveurs Web, FTP et Mail. Un " serveur Proxy " supplémentaire est également configuré pour permettre aux utilisateurs du réseau interne d'accéder à Internet. Le nom "réseau bastion" découle des mesures particulières de protection qui sont prises en prévision de possibles intrusions [39].

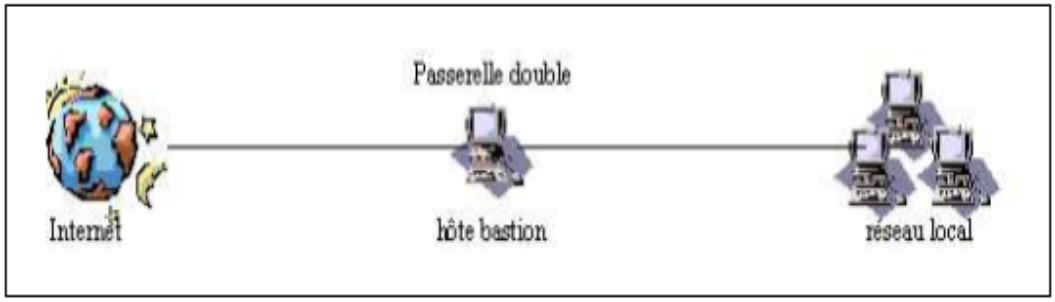


FIG. 2.3 – La passerelle double

La passerelle double est la possibilité la plus simple pour réaliser un firewall d'application n'autorisant aucun trafic IP entre les réseaux [39].

Avantage : bon marché[39].

Inconvénient : du fait de tout ce qu'elle doit faire (routage et application), une telle configuration pourrait rencontrer des problèmes de performance.

2.5.3 Firewalls avec réseau de filtrage

La combinaison des deux méthodes est ici plus sûre et efficace. Au niveau du réseau, un routeur sous écran est configuré de façon à n'autoriser les accès de l'extérieur et de l'intérieur que par l'intermédiaire du réseau bastion sur lequel fonctionnent tous les serveurs assurant les serveurs Internet. Cette possibilité est appelée Firewall avec réseau de filtrage. La figure suivante illustre cette solution [39] :

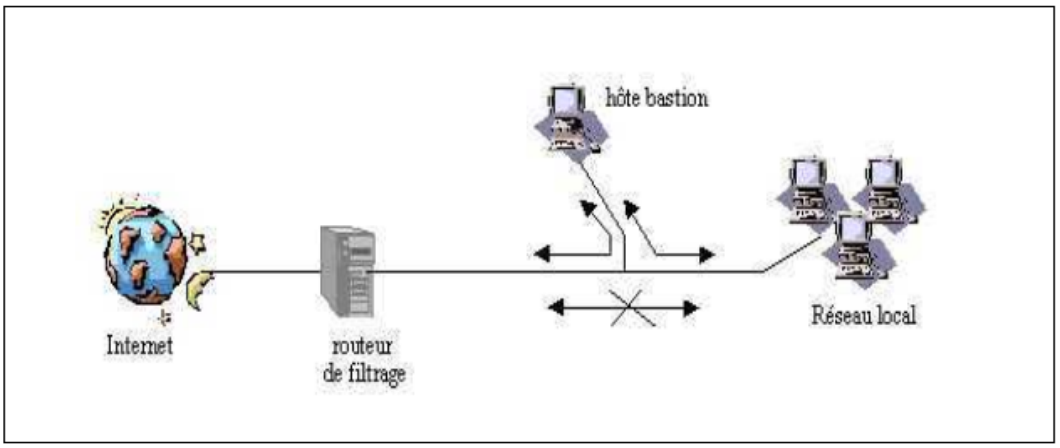


FIG. 2.4 – Firewall avec réseau de filtrage

Firewall avec réseau de filtrage dans lequel seuls les accès au réseau bastion sont autorisés. Pour la grande majorité des entreprises, cette solution est sûre et abordable, car les prestataires Internet assurent la seconde partie de la protection à l'autre bout de la ligne. En effet, votre entreprise y est également connectée à un routeur, et le trafic de données est réglé par un serveur Proxy au niveau de la couche application. Les pirates doivent par conséquent franchir deux obstacles [39].

Avantage : bon marché et sûr lorsque le prestataire est équipé en conséquence.

Inconvénient : le système comporte deux sécurités distinctes, le routeur et le réseau bastion, Si l'une des deux est paralysée, le réseau est menacé dans son intégralité [39].

2.5.4 Firewall avec sous-réseau de filtrage

Cette solution est de loin la plus sûre, mais également la plus onéreuse. Un Firewall avec sous-réseau de filtrage se compose de deux routeurs sous écran. L'un est connecté à Internet, et l'autre à l'intrant/LAN. Plusieurs réseaux bastions peuvent s'intercaler pour former entre ces deux routeurs, en quelque sorte, leur propre réseau constituant une zone tampon entre un Intranet et l'Internet appelée zone démilitarisée [39].

De l'extérieur, seul l'accès aux réseaux bastions est autorisé. Le trafic IP n'est pas directement transmis au réseau interne. De même, seuls les réseaux bastions, sur lesquels des serveurs Proxy doivent être en service pour permettre l'accès à différents services Internet, sont accessibles à partir du réseau interne. La figure suivante illustre cette variante.

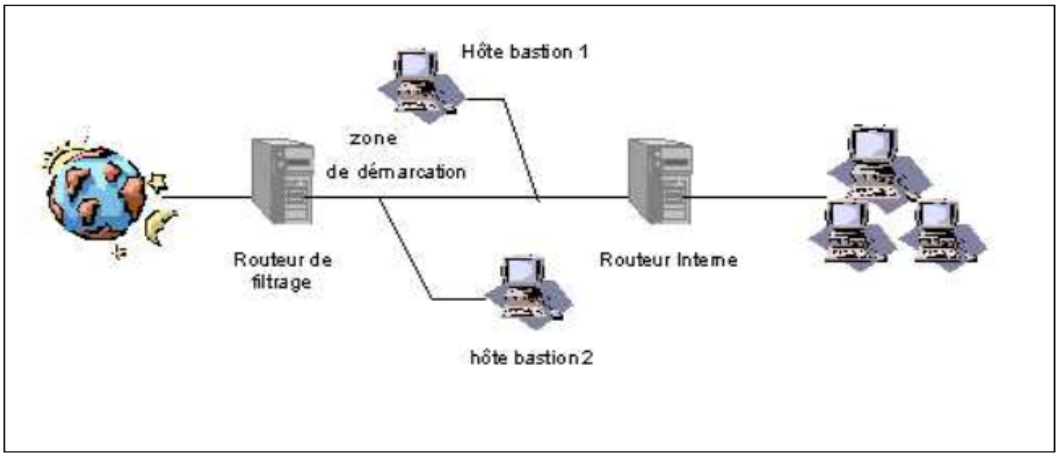


FIG. 2.5 – Firewall avec sous-réseau de filtrage

Pour s'introduire sur le réseau d'entreprise à travers ce firewall, il faut franchir les deux routeurs, ainsi que les réseaux bastions intercalés. [39]

- Le routeur interne :
  - Autoriser le trafic entre le bastion 1 et les machines internes et inversement.

- Interdire tout autre trafic.

- Le routeur externe
  - Filtre le trafic entre le monde extérieur et le bastion2.
  - Interdit tout autre trafic direct (donc pas de trafic entre le réseau interne et l'extérieur).
- Les deux bastions peuvent discuter sans aucune règle (zone démilitarisée " DMZ ").
- Le bastion interne :
  - Assure les fonctions de DNS vis-à-vis du réseau interne en envoyant ses requêtes au bastion externe.
  - Assure les fonctions de proxy avec authentification pour les applications distantes (Telnet, FTP, etc.).
  - Assure le relais du Mail sortant (SMTP).
- Le bastion externe :
  - Filtre au niveau applicatif les paquets en direction du réseau interne.
  - Assure le relais du mail entrant.
  - Assure les fonctions de DNS vis-à-vis du réseau externe.[39]

Avantage : système Firewall très sûr [39].

Inconvénients : coût d'investissement élevé, effort administratif important [39].

2.6 Zone démilitarisée (DMZ)

2.6.1 Firewall avec zone démilitarisée

Le firewall a pour fonction de surveiller les trames passant sur le réseau et de les bloquer ou de les laisser passer. Le firewall décide de laisser passer ou non une trame en fonction de sa source, de sa destination, et des règles d'approbation définies dans sa table de règles [44].

La configuration la plus rependue pour un réseau connecté à Internet est une configuration avec firewall et zone démilitarisée (DMZ). Un firewall est placé entre Internet, le réseau local LAN, et une zone spéciale appelée DMZ, qui contient serveurs Web, Extranets, FTP, etc. . ., qui doit pouvoir être accédée d'Internet et du LAN local. La DMZ est une sorte de zone tampon entre l'extérieur et le réseau interne. La figure suivante illustre cette solution [44] :

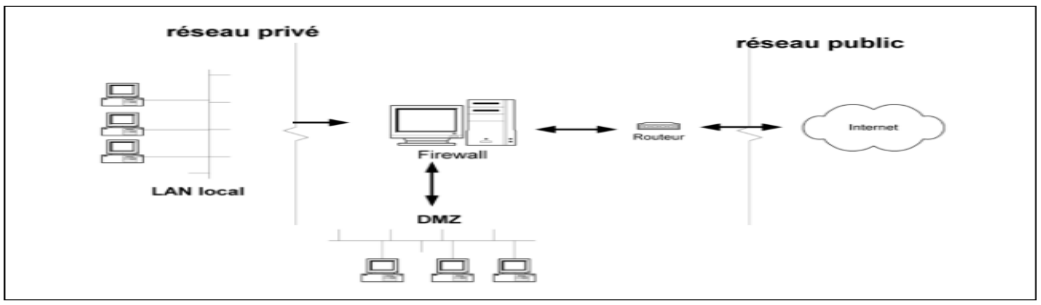


FIG. 2.6 – Firewall avec DMZ

Le firewall permet alors de filtrer les trames et de les diriger vers telle ou telle zone en fonction des règles internes définies par les administrateurs.

2.7 Choix d'un firewall pour l'entreprise

La façon de configurer un firewall et de le gérer est tout aussi importante que les capacités intrinsèques qu'il possède. Toutefois, lorsque le choix s'impose, nous prenons en considération les critères suivants :

- La nature, le nombre des applications appréhendées (FTP, messagerie, HTTP, SNMP, vidéo conférence, etc.),
- Type de filtres, niveau de filtrage (niveau applicatif, niveau TCP, niveau IP, possibilité de combiner ces niveaux),
- Facilites d'enregistrement des actions et des événements pour audits future.
- Les outils et facilites d'administration (interface graphique ou lignes de commandes, administration distante après authentification de gestionnaire, etc.),
- Simplicité de configuration et de mise en ouvre.
- Sa capacitéà supporter un tunnel chiffre permettant éventuellement de réaliser un réseau prive virtuel (VPN pour virtuel private network).
- La disponibilité d'outils de surveillance, d'alarmes, d'audit actif.
- Possibilité d'équilibrage de charges et de gestion de la bande passante de réseau.
- L'existence dans l'entreprise de compétences en matière d'administration du système d'exploitation du firewall [18] [34].

2.8 Conclusion

Ce chapitre a porté sur les firewalls, ou nous avons brossé de façon claire les notions, le principe et le fonctionnement. Ainsi que la combinaison des firewalls avec les zones dématérialisées.
Le prochain chapitre sera porté sur le contexte du travail et l'implémentation de notre solution.

3

Contexte de travaile et Implementation

3.1 Introduction

Dans ce chapitre, nous allons vous présenter les problèmes rencontrer par les entreprises, ainsi que la solution proposée pour remédier a ces problèmes.

A fin de mettre en évidence la solution pare feu (firewall) nous allons en premier lieu, définir l'environnement du travail à utiliser qui l'émulateur GNS3 (version0.8.6). En second lieu, nous décrirons la procédure de configuration et illustrons les différents tests d'évaluations garantissant le succès de l'implémentation réalisée.

3.2 Problématique

L'informatique est aujourd'hui un composant critique de l'entreprise. La sécurité du système d'information est au cœur de la préoccupation des responsables informatiques. Ils se doivent de garantir la protection du réseau et l'intégrité des données face aux menaces qui évoluent en permanence. Il est important pour l'entreprise de faire face à l'évolution des menaces et de savoir répondre aux réglementations imposées.

Parmi ces attaques quelle connait n'importe quelle entreprise sont :

- Attaques de type déni de service, attaques applicatives.
- Intrusion, vols de donnée.
- Virus, spyware, keylogger.
- Spam, phishing.
- Usurpation d'identité.

En complément des solutions traditionnelles de sécurité, il est maintenant nécessaire pour les entreprises de se protéger contre les nouvelles générations de cyberattaque. Ces attaques sont très ciblées et très dangereuses mais restent paradoxalement très discrètes ce qui les rend difficiles à détecter. Leur objectif est d'exfiltrer des informations sensibles sans être remarquées.

3.3 Solution proposée

Le firewall est une réponse a la mise en place d'une solution de sécurité sur le réseau d'entreprise. Il propose un véritable contrôle sur le trafic. La connaissance et la maitrise de ce type de matériel est important et est une notion a connaitre.

Une entreprise qui dispose d'un réseau interne (privé), il préférable d'opter pour un firewall réseau plutôt qu'un firewall personnel.

L'objectif de notre travail est de configurer un firewall matériel et de le mettre en place dans un réseau d'entreprise et nous allons traiter la mise en place des règles de filtrage.

Notre solution est consituée de 3 réseau telque nous avons configuré un firewall ASA situé entre une réseau LAN, réseau DMZ et réseau WAN. L'architecture choisie est représentée dans la figure suivante :

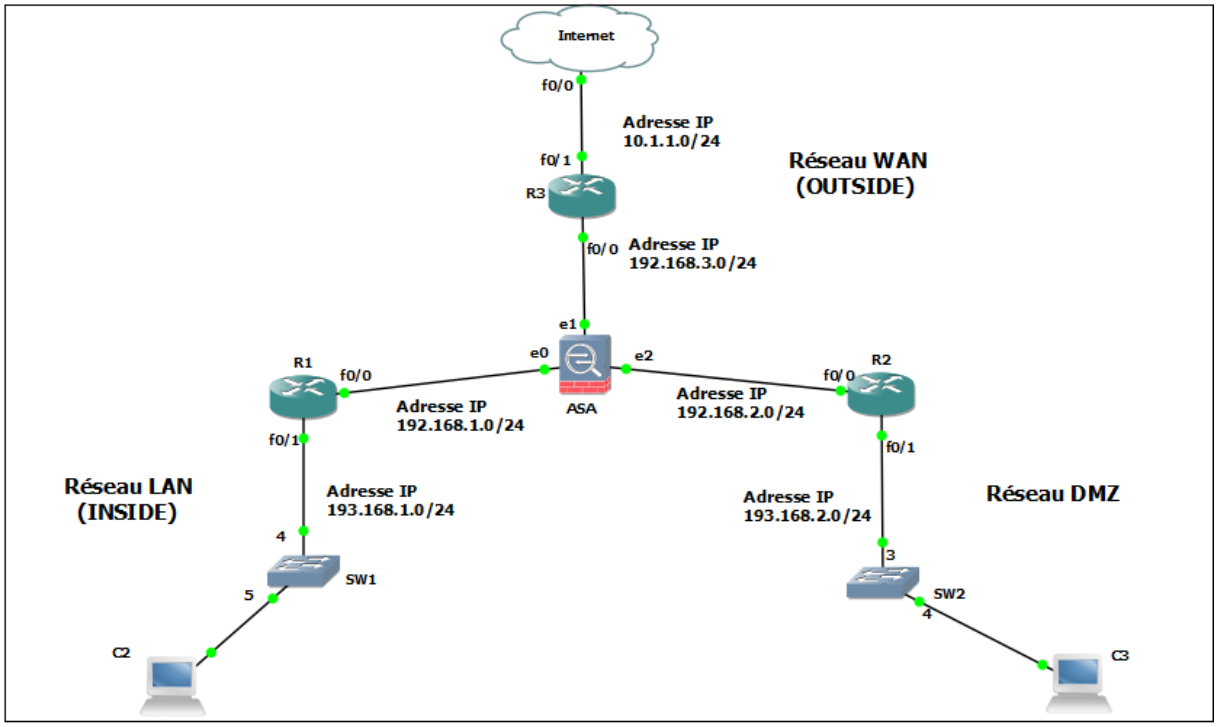


FIG. 3.1 – Architecture de la solution proposée.

3.4 Description de l'environnement du travail

3.4.1 GNS3

GNS 3(Graphical Network Simulator),est un logiciel libre qui permet la simulation d'un réseau informatique , c'est un emulateur qui est proche de la réalité ,il est parfait pour se préparer aux certifications Cisco CCNA ,CCNP,CCIP,CCIE [42].

GNS3 permet d'avoir un routeur Cisco virtuel sur un ordinateur. a savoir qu'il ne fournit pas D'IOS il faut se les procurer a l'aide d'un compte Cisco ou a partir de Google, au plus il fonctionne sur de multiples plateformes, incluant Windows, linux, et Mac OS X... etc[42]. Pour fournir des simulations complètes et précises, GNS3 est fortement lié à :

- **Dynamips :** est un émulateur de matériel Cisco (en rapport avec les processeurs Mips utilisés)[38].

- **Dynagen :** est un produit complémentaire écrit en Python, s'interfaçant avec Dynamips grâce au mode hyper viseur. Dynagen facilite la création et la gestion de maquettes grâce à un fichier de configuration simple décrivant la topologie du réseau à simuler et une interface texte interactive [43].

- **Qemu :**est une machine source de l'émulateur et de virtualisation générique et ouverte. Il est utilisé par GNS3 pour exécuter Cisco ASA, PIX et IDS ainsi que tout Système d'exploitation classique [43].

- **Virtual Box ou machine virtuelle :** est un logiciel de virtualisation de système d'exploitation qui permet de créer un ou plusieurs ordinateurs virtuels dans lesquels s'installent d'autres systèmes d'exploitation (systèmes invités), et de faire fonctionner Plus d'un système d'exploitation en même temps en toute sécurité [35].

3.4.2 IOS (Internet Work operating System)

La fonction de base de Cisco IOS est de permettre la communication de données entre les nœuds du réseau. En plus de routage et de commutation, Cisco IOS propose des dizaines de services supplémentaires qu'un administrateur peut utiliser pour améliorer la performance et la sécurité du trafic réseau. Ces services incluent le cryptage, l'authentification, les capacités de pare-feu, l'application de la politique, l'inspection approfondie des paquets, qualité de service, le routage intelligent et la capacité proxy. Dans Integrated Services Routers de Cisco (ISR), IOS peut également soutenir le traitement des appels et des services de communications unifiées [45].

- **Image IOS :**GNS3 est un logiciel de simulation qui utilise les IOS des routeurs Cisco, alors avant toute implémentation il faut intégrer les IOS Cisco dans le logiciel [37].

3.4.3 Objectif de GNS3

L'objectif de GNS3 est d'apporter aux étudiants et professionnels des nouvelles technologies de communication travaillant dans le domaine de l'administration systèmes et réseaux une solution pour virtualiser et modéliser fidèlement des réseaux.

Le principal avantage de GNS3 réside dans l'émulation matérielle, en lieu et place de l'utilisation de simulateurs qui souvent est une manière limitée de virtualiser du matériel. Grâce à GNS3, les utilisateurs peuvent tester et estimer, dans des conditions quasi réelles et sans avoir à financer le matériel, leurs configurations et réseaux avant de les mettre en place physiquement.GNS3 nous permet :

- Le design de topologies réseaux de haute qualité et complexes.[38]
- Emulation de plusieurs plate-forme de routeurs Cisco IOS, ou encore IPS, PIX et firewalls ASA.[38]
- Simulation de switches Ethernet, ATM et Frame Relay. [38]
- Connexion de réseaux simulés au monde réel. [38]
- Capture de paquets grâce à Wireshark. [38]

3.4.4 Description de l'interface graphique de l'émulateur GNS3

Le simulateur et l'émulateur GNS3 met à notre disposition tous les éléments nécessaires pour sa manipulation, il contient différentes parties et interfaces que nous pouvons utiliser, et la liste des éléments actifs et matériels disponibles que nous pouvons ajouter dans otre topologie réseau, les principaux éléments sont énumérés dans la figure suivante :

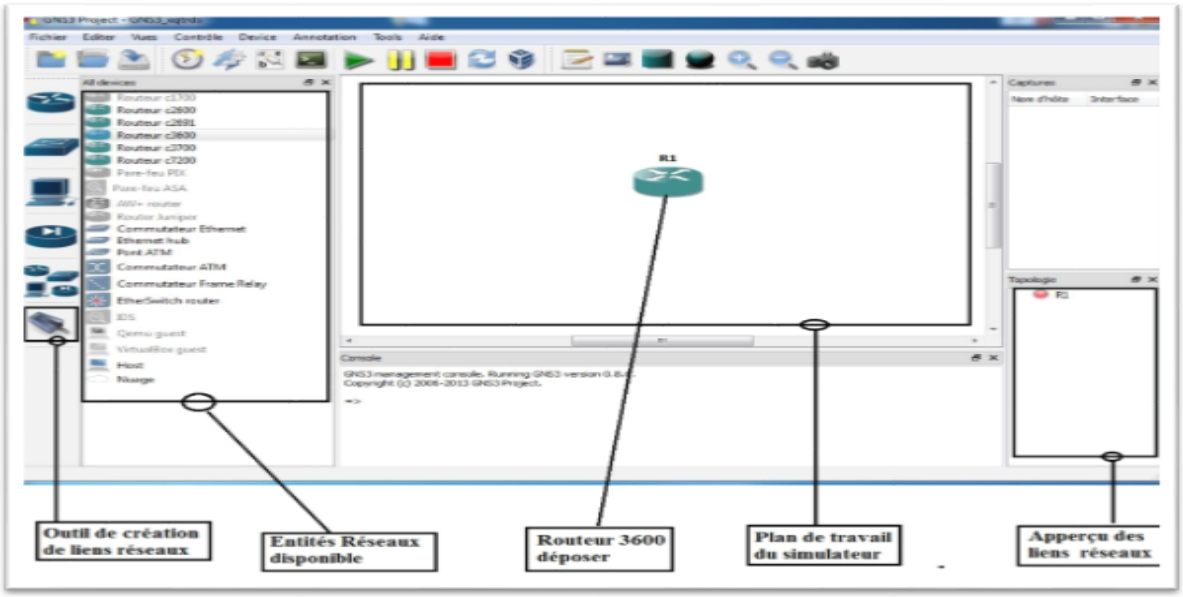


FIG. 3.2 – Interface graphique de l'émulateur GNS3.

3.5 Implémentation de la solution

3.5.1 Configuration de base

Nous allons commencer par l'attribution des configurations de base réseau des différents routeurs. D'abord, nous allons configurer et activer leurs différentes interfaces et le routage par défaut, comme c'est présenté ci-dessous :

- **Routeur Internet**

Commandes	Explication
Internet>	Mode EXEC utilisateur
Internet *>enable*	Mode EXEC privilégié
Internet *#configure terminal*	Mode de configuration globale
Internet (config)*# interface FastEthernet0/0*	Accès à la configuration de l'interface F0/0
Internet (config)*#ip addr 10.1.1.1 255.255.255.0*	Adresse IP et masque de sous réseau de F0/0
Internet (config)*#no shutdown*	Activation de l'interface F0/0
Internet (config)*#exit*	Routeur au mode EXEC privilégié
Internet *#ip route 0.0.0.0 0.0.0.0 10.1.1.2*	Routage static par défaut
Internet (config)*#exit*	Routeur au mode EXEC privilégié
Internet *#write*	Sauvegarder la configuration

FIG. 3.3 – Configuration de routeur Interent.

- **Routeur R1**

Commandes	Explication
R1>	Mode EXEC utilisateur
R1>*enable*	Mode EXEC privilégié
R1#*configure terminal*	Mode de configuration globale
R1(config)# *interface FastEthernet0/0*	Accès à la configuration de l'interface F0/0
R1(config)#*ip addr 192.168.1.1 255.255.255.0*	Adresse IP et masque de sous réseau de F0/0
R1 (config)#*no shutdown*	Activation de l'interface F0/0
R1 (config)#*exit*	Routeur au mode EXEC privilégié
R1 (config)# *interface FastEthernet0/1*	Accès à la configuration de l'interface F0/1
R1 (config)#*ip addr 193.168.1.1 255.255.255.0*	Adresse IP et masque de sous réseau de F0/1
R1 (config)#*no shutdown*	Activation de l'interface F0/1
R1 (config)#*exit*	Routeur au mode EXEC privilégié
R1 #*ip route 0.0.0.0 0.0.0.0 192.168.1.2*	Routage static par défaut
R1 (config)#*exit*	Routeur au mode EXEC privilégié
R1 #*write*	Sauvegarder la configuration

FIG. 3.4 – Configuration de routeur R1.

- **Routeur R2**

Commandes	Explication
R2>	Mode EXEC utilisateur
R2>*enable*	Mode EXEC privilégié
R2 #*configure terminal*	Mode de configuration globale
R2 (config)# *interface FastEthernet0/0*	Accès à la configuration de l'interface F0/0
R2(config)#*ip addr 192.168.2.1 255.255.255.0*	Adresse IP et masque de sous réseau de F0/0
R2 (config)#*no shutdown*	Activation de l'interface F0/0
R2 (config)#*exit*	Routeur au mode EXEC privilégié
R2 (config)# *interface FastEthernet0/1*	Accès à la configuration de l'interface F0/1
R2 (config)#*ip addr 193.168.2.1 255.255.255.0*	Adresse IP et masque de sous réseau de F0/1
R2 (config)#*no shutdown*	Activation de l'interface F0/1
R2 (config)#*exit*	Routeur au mode EXEC privilégié
R2 #*ip route 0.0.0.0 0.0.0.0 192.168.2.2*	Routage static par défaut
R2 (config)#*exit*	Routeur au mode EXEC privilégié
R2 #*write*	Sauvegarder la configuration

FIG. 3.5 – Configuration de routeur R2.

- **Routeur R3**

Commandes	Explication
R3>	Mode EXEC utilisateur
R3>*enable*	Mode EXEC privilégié
R3 *#configure terminal*	Mode de configuration globale
R3 (config)# *interface FastEthernet0/0*	Accès à la configuration de l'interface F0/0
R3(config)#*ip addr 192.168.3.1 255.255.255.0*	Adresse IP et masque de sous réseau de F0/0
R3 (config)#*no shutdown*	Activation de l'interface F0/0
R3 (config)#*exit*	Routeur au mode EXEC privilégié
R3 (config)# *interface FastEthernet0/1*	Accès à la configuration de l'interface F0/1
R3 (config)#*ip addr 10.1.1.2. 255.255.255.0*	Adresse IP et masque de sous réseau de F0/1
R3 (config)#*no shutdown*	Activation de l'interface F0/1
R3 (config)#*exit*	Routeur au mode EXEC privilégié
R3 *#write*	Sauvegarder la configuration

FIG. 3.6 – Configuration de routeur R3.

3.5.2 Configuration de firewall ASA

3.5.2.1 Configuration des interfaces

Après avoir configuré les routeurs, nous allons entamer la configuration du firewall ASA. Ce firewall est composé de 3 interfaces, la première sera reliée au reseau interne (LAN), la deuxième au réseau externe (WAN) et la troisième sera pour la DMZ. Les figures suivantes représente les interfaces configurées de firewall ASA :

Commandes	Explication
ciscoasa>	Mode EXEC utilisateur
ciscoasa >*enable*	Mode EXEC privilégié
ciscoasa #*configure terminal*	Mode de configuration globale
ciscoasa (config)#*hostname ASA*	Définir le nom de firewall
ASA (config)# *interface Ethernet0/0*	Accès à la configuration de l'interface E0/0
ASA (config-if)# *nameif inside*	Définir le nom de l'interface E0/0
ASA (config-if)# *security-level 100*	Niveau de sécurité de l'interface E0/0
ASA(config)#*ip addr 192.168.1.1 255.255.255.0*	Adresse IP et masque de sous réseau de E0/0
ASA (config)#*no shutdown*	Activation de l'interface E0/0
ASA (config)#*exit*	Routeur au mode EXEC privilégié
ASA (config)# *interface Ethernet0/1*	Accès à la configuration de l'interface E0/1
ASA (config-if)# *nameif outside*	Définir le nom de l'interface E0/1
ASA (config-if)# *security-level 0*	Niveau de sécurité de l'interface E0/1
ASA(config)#*ip addr 192.168.3.2 255.255.255.0*	Adresse IP et masque de sous réseau de E0/1
ASA (config)#*no shutdown*	Activation de l'interface E0/1
ASA (config)#*exit*	Routeur au mode EXEC privilégié
ASA (config)# *interface Ethernet0/2*	Accès à la configuration de l'interface E0/2
ASA (config-if)# *nameif dmz*	Définir le nom de l'interface E0/2
ASA (config-if)# *security-level 50*	Niveau de sécurité de l'interface E0/2
ASA(config)#*ip addr 192.168.2.2 255.255.255.0*	Adresse IP et masque de sous réseau de E0/2
ASA (config)#*no shutdown*	Activation de l'interface E0/2
ASA (config)#*exit*	Routeur au mode EXEC privilégié

FIG. 3.7 – Configuration de firewall ASA.

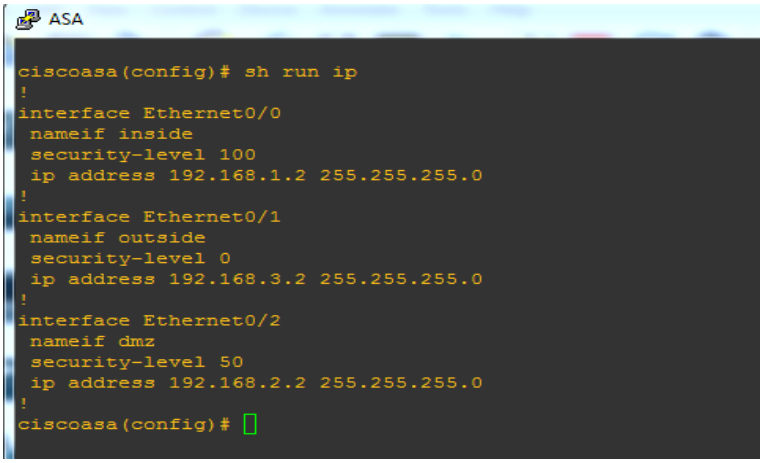


FIG. 3.8 – Aperçu des interface de firewall ASA.

Aprés avoir configurer les interfaces da ASA, nous ajoutons une route par défaut pour tout le trafic sortant vers internet.

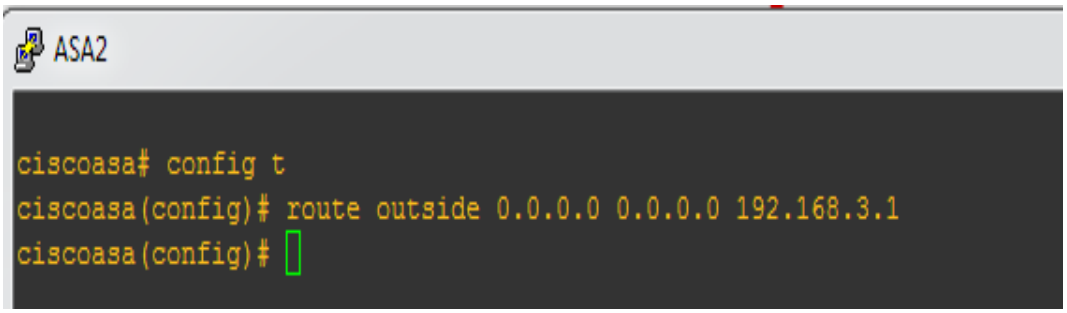


FIG. 3.9 – Route pour acceder à l'Internet.

Nous envoyons une requête pour vérifier si la communication n'est pas coupée. La figure suivante représente la réussite de test :

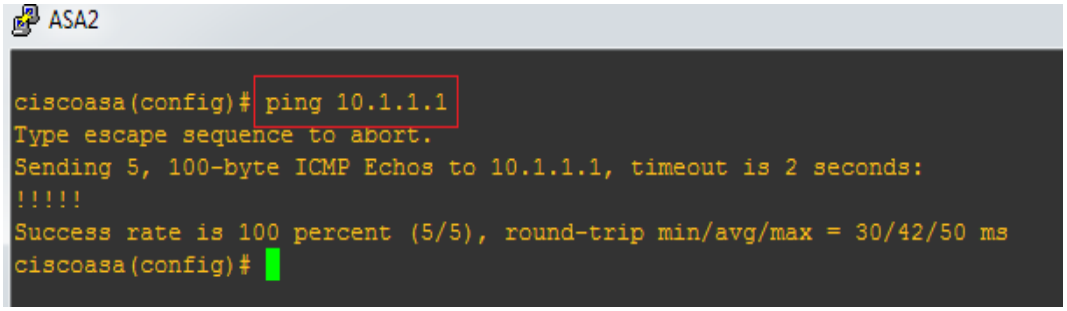


FIG. 3.10 – Resultat d'une requête ICMP (ASA vers Internet).

3.5.2.2 Configuration de nat et de class-map

- **Nat (Network Address Translation) :** permet d'utiliser des adresses n'ayant pas de signification globale pour se connecter à travers l'Internet en traduisant celles-ci en adresses globales routables

  Nous allons créer la règle de nat pour que LAN puisse accéder au WAN. Pour ce faire, nous allons préciser l'adresse du LAN, la direction du nat ainsi que l'interface de sortie de façon dynamique (Figure 3.11).

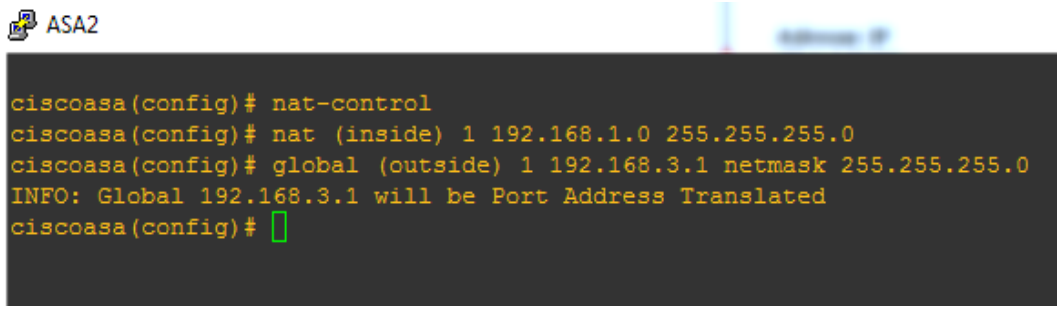


FIG. 3.11 – Configuration du nat.

- **Class-map :** nous permettent de créer et de configurer une carte de couche 3 et 4 classe pour classifier le trafic réseau

  Nous allons définir une class-map pour indiquer le trafic à analyser et autorisé. Le trafic à analyser sera le flux (protocole) ICMP (Figure 3.12).

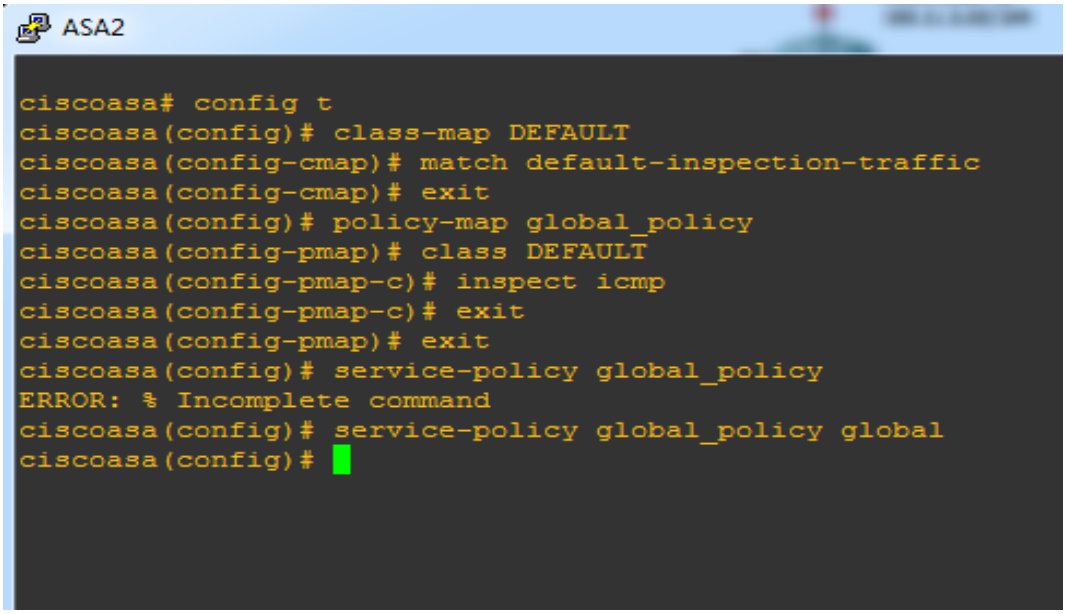


FIG. 3.12 – Configuration de class-map.

3.5.2.3 Configuration des ACL

Les ACL (Access Control Lists) permettent de filtrer des packets suivant des critères définis par l'utilisateur.

- **ACL 1 :** autoriser le WAN à accéder à R2 en DMZ, l'ACL a crée sera de ce sens :

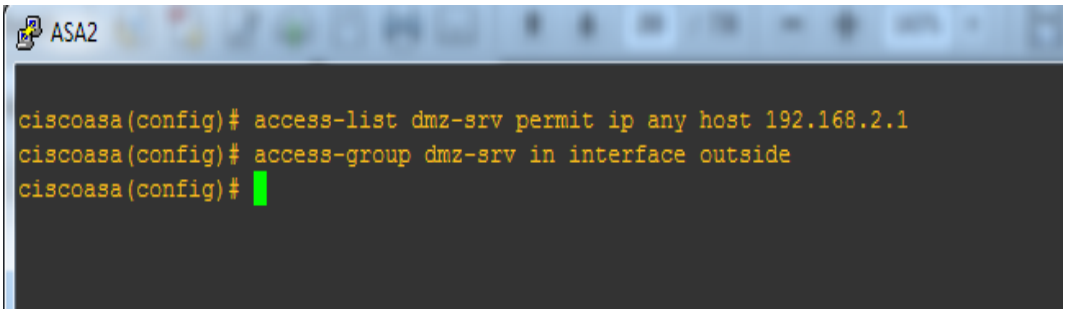


FIG. 3.13 – Configuration du ACL 1

- **ACL 2 :** autoriser R1(LAN) à pinger R2(DMZ), l'ACL a crée sera de ce sens :

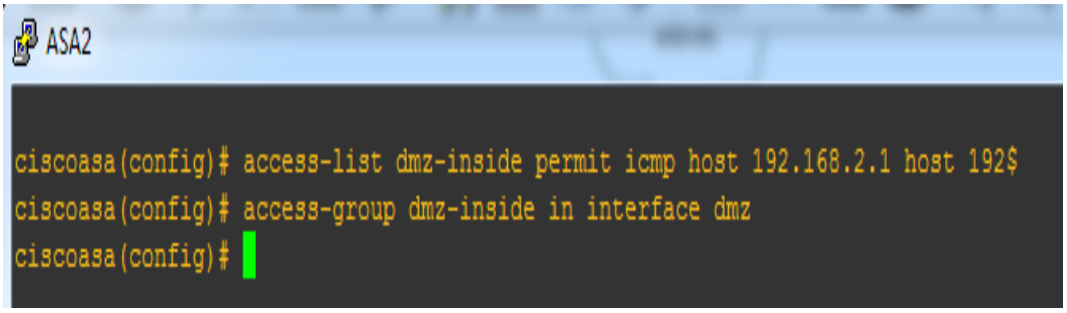


FIG. 3.14 – Configuration du ACL 2.

La figure suivante représente l'ensemble des ACLs configurées.

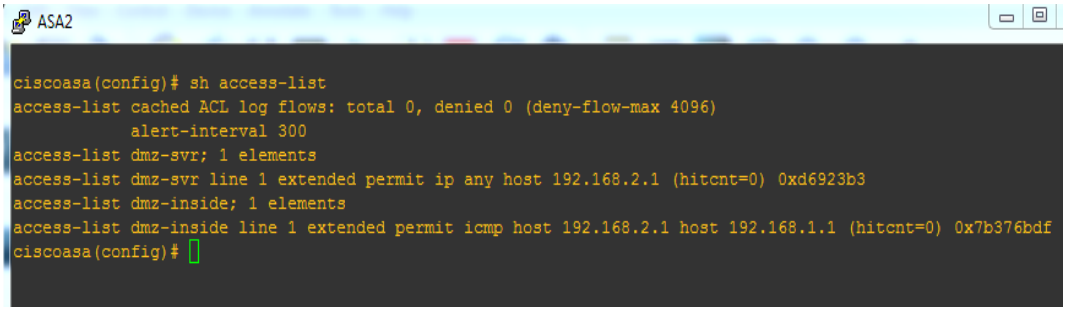


FIG. 3.15 – Aperçu des ACLs configurées.

3.5.2.4 Outil Telnet

- **Telnet :** utilitaire permettant de se connecter sur un serveur distant à partir de n'importe quel ordinateur sur le réseau TCP/IP en mode terminale

Par défaut, le firewall ASA refusera les connections remote d'un hôte dans un de ses réseaux, comme le réseau LAN ne peut pas prendre la main sur lui.

Pour y remédier, nous devons autoriser le réseau LAN 192.168.1.0/24 à se connecter en telnet sur l'interface inside du firewall ASA.

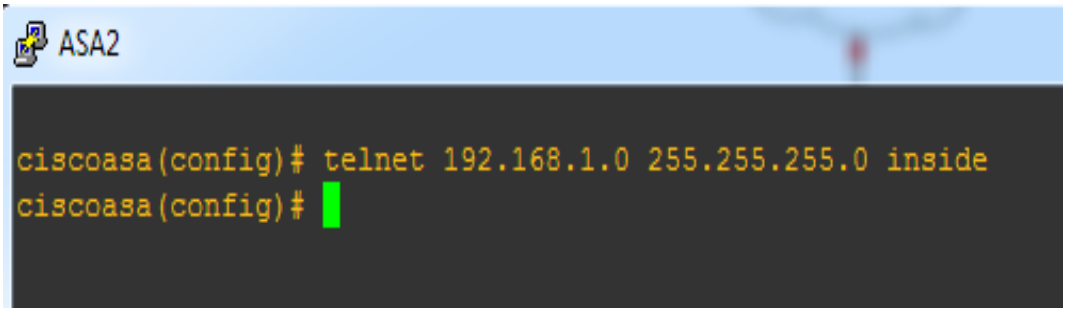


FIG. 3.16 – Configuration du Telnet.

3.6 Conclusion

Au cours de ce chapitre, nous avons cite les problèmes rencontrer par les entreprises et nous avons proposé une solution afin de répondre a quelque problèmes ensuite nous avons décrit l'environnement de travaille GNS3, enfin nous avons présenter les différentes étapes de l'implémentation de notre solution firewall, ainsi que les résultats des différentes tests effectué a fin de vérifier le bon fonctionnement.

Conclusion générale

La sécurité des réseaux informatique et particulièrement celle des réseaux locaux d'une entreprise est en évolution, ceci est du a l'ouverture des systèmes informatiques sur internet. Cette interconnexion à Internet les a directement exposés à des attaques informatiques complexes. De ce fait les entreprises doivent protéger leurs réseaux en mettant en place des solutions efficaces de protection contre ces attaques afin de garantir un niveau élevé de sécurité. Une protection vigilante contribue à garantir la continuité de l'activité de l'entreprise et minimise les conséquences désactreuses.

Dans notre cas, nous avons opté pour la mise en place d'une solution firewall. Cette outil a pour but de sécurisé au maximum le réseau local de l'entreprise. Dans notre travail, nous avons proposé une architecture sécurisée où le cœur de cette architecture est basé sur un firewall.

Pour répondre à quelques problèmes de sécurité rencontrée par les entreprises nous avons configuré le boitier ASA firewall entre trois réseaux LAN/DMZ/WAN.

Les différentes configurations qui sont réalisés sur le ASA sont le Nat dynamique afin que LAN puisse accéder au WAN d'une manière sécurisé et définir une class-map pour indiquer le trafic à analyser et autorisé, créer des ACL pour autorise et bloquer un trafic et la connexion en Telnet pour un membre qui fait partait de l'entreprise puisse accéder a distance d'une manière sécurisé.

Ce travail a fait l'objet d'une expérience intéressante, et a eu énormément d'apport sur nos connaissances et nos compétences en termes de configuration dans un environnement GNS3. De plus nous avons aussi enrichi nos connaissances dans le domaine de la sécurité d'un réseau d'entreprise grâce à l'implémentation d'une architecture réseau sécurisé base sur un firewall. Par contrainte de temps nous avons seulement implémenté quelque configu-

ration.

Bibliographie

[1] A. ABOU EL KALAM, " Modèles et politiques de sécurité pour les domaines de la santé et des affaires sociales ", Thèse de Doctorat,Institut National Polytechnique de Toulouse, 2003.

[2] A. ALTUNAIJI, " Mise en place d'un réseau sécurisé sous linux", Université Claude Bernard, Lyon 1, France, novembre 2002.

[3] A. CONTES, " Une Architecture De Sécurité Hiérarchique, Adaptable Et Dynamique Pour La Grille ", thèse doctorat, Université de Nice - Sophia Antipolis, Septembre 2005.

[4] A. MARACON, B. FABREJON " Les Firewalls - La sécurité des réseaux ", Eyrol, 1999

[5] A. MOKHTARI, " La Sécurité dans les Échanges et la Sauvegarde des Données ", DEA M.I.S.I. Université de Versailles. 2000 - 2001.

[6] A. PEREZ, " Architecture des réseaux de télécommunications ", Hermes Siences publications, 2002

[7] A. SAIDANE, " Conception et réalisation d'une architecture tolérant les intrusions pour des serveurs Internet ", thèse doctorat, Institut National des Sciences Appliquées de Toulouse, janvier 2005.

[8] A. THIERY, J. CLAVEL, " Les Plans de Sécurité Informatique ", édition Dunod, Paris, mars 2013

[9] C. LLORENS, L. LEVIER, D. VALOIS, " Tableaux de bord de la sécurité réseau ", 2ème édition, Eyrolles, paris, 2006.

[10] D. DROMARD, D. SERET, " Architecture des réseaux ", Pearson France, 2009.

[11] D. FERNANDES, P. A. SARR, " La protection des contre les attaques DOS ", Université de Paris Descarte, Mai 2010.

[12] D.ROUMANET, " Architectures Réseaux Télécoms : Analyseur réseau Wireshark ", 2007, IN : http ://www.prism.uvsq.fr/ mogue/INI1/TD-TP/TP7/Manuel_WireShark.pdf

[13] E. TEME, B. TIGANA, " Proposition d'une Architecture Sécurisée du Réseau Intranet de L'Université A. Mira de Bejaïa ", Mémoire ingéniorat, Université A. Mira-Bejaia, 2007.

[14] G. PUJOLLE, " Initiation-aux-réseaux ", Eyrolles, Edition 2000.

[15] G. PUJOLLE, " Les réseaux ", 6ème édition, Eyrolles, 2008.

[16] G. PUJOLLE, " Les réseaux ", Paris, Edition 2014.

[17] I. HAJJEH, " Conception et validation d'un nouveau protocole pour la sécurisation des échanges. ", thèse doctorat, Ecole Nationale Supérieure des Télécommunications, Paris, décembre 2004.

[18] J. F. CARPENTIER, " La sécurité informatique dans la petite entreprise ", 2ème édition, copyright-Edition ENI -Décembre 2012

[19] J. F. PILLOU, " Tous sur les réseaux et Internet ", édition Dunod, Paris, 2006

[20] J. HRUSKA et P. LAMMER, " Les menaces à la sécurité des systèmes et des données de A à Z ", Edition Sophos, 2013.

[21] J. ILLAND, N. DAUSQUE, K. KORTCHINSKY, " Sécurité Informatique ", CNRS, février 2005.

[22] J. Kim, " Integrating Artificial Immune Algorithms for Intrusion Detection ", thèse doctorat, University College London, 2002.

[23] J. P. ARNAUD, C. SERVIN, " réseaux et télécoms" 2ème édition, Dunod, 2006.

[24] J. PETIT, " Surcoût de l'authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires ", thèse doctorat, Université de Toulouse, Juillet 2011.

[25] L. BLOCH, C. WOLFHUGEL, " Sécurité informatique Principes et méthodes ", édition Eyrolles, paris, 2007.

[26] L. POINSOT, " Cours " Sécrypt ", Introduction à la sécurité informatique ", UMR 7030 - Université Paris 13 - Institut Galilée, 2012.

[27] M. BADRA, " Le transport et la sécurisation des échanges sur les réseaux sans fil ", Thèse de doctorat, l'Ecole Nationale Supérieure des Télécommunications, 2004.

[28] M. M. PRONZATO, " Les Firewalls ", 3ème année ingénieurs en Informatique et Réseaux, 2000, IN : www.igm.univ-mlv.fr

[29] M. SUTER, " Sécurité informatique dans les entreprises suisses", Center for Security Studies (CSS), ETH, Zurich, août 2006.

[30] M. RIGUIDEL, " La sécurité des réseaux et des systèmes ", ENST Paris, 2006-2007.

[31] O. A. BENCHCHAOUI, " SSL VPN ", projet technique, Université Paris Est, Septembre 2011.

[32] P. ATELIN, " Réseaux Informatiques Notions fondamentales (Normes, Architecture, Mod7le OSI, TCP/IP, Ethernet, Wi-Fi,...) ", Editions ENI, 2009

[33] P. F. BONNEFOI, " Cours de Sécurité Informatique ", Université de Limoges, 2012.

[34] S. GHERNAOUTI, " Sécurité Internet, Stratégie et Technologie ", Dunod, Paris, 2000.

[35] T. NEJIBA, S. DJEBBI, " Sécurisation des routeurs Cisco ", Rapport de stage de perfectionnement, université virtuelle de Tunis, 2010-2011.

[36] V. REMAZEILLES, " La sécurité des réseaux avec CISCO ", Edition ENI, 2009.

[37] W. L. SIME SIME, " Mise en place d'une architecture VPN MPLS avec gestion du temps de connexion et de la bande passante utilisateur ", Master Européen en Informatique, Institut d'Ingénierie d'Informatique de Limoge, 2009.

[38] http ://eip.epitech.eu/2013/gns3/fr/project.html.

[39] http ://firewalls.chez.com/chapitre2.html : le firewall, une technique de protection.

[40] https ://framasoft.org/article1857.html

[41] http ://www.frameip.com/tcpip/

[42] www.gns3.net

[43] www.gns3.net.qemu

[44] http ://www.mnfauvel.com/Kb/html/fonctio4.htm.

[45] http ://searchnetworking.techtarget.com/definition/Cisco-IOS-Cisco-Internetwork-Operating-System

[46] http ://www.vulgarisation-informatique.com/topologie-reseau.php

[47] https ://wapiti.telecom.lille.fr/commun/ens/peda/options/st/rio/pub/exposes/exposesrio2000/Blick 20Lammari/site/firewall/fontionnement.html.

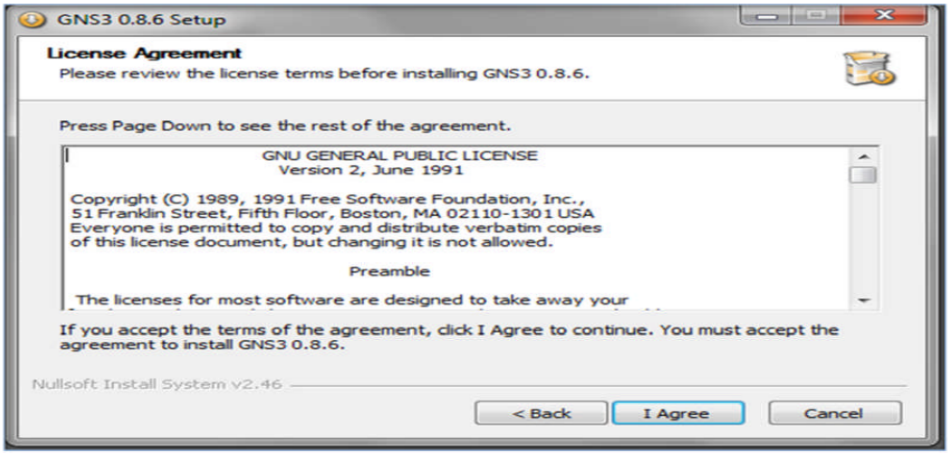
A

Annexe

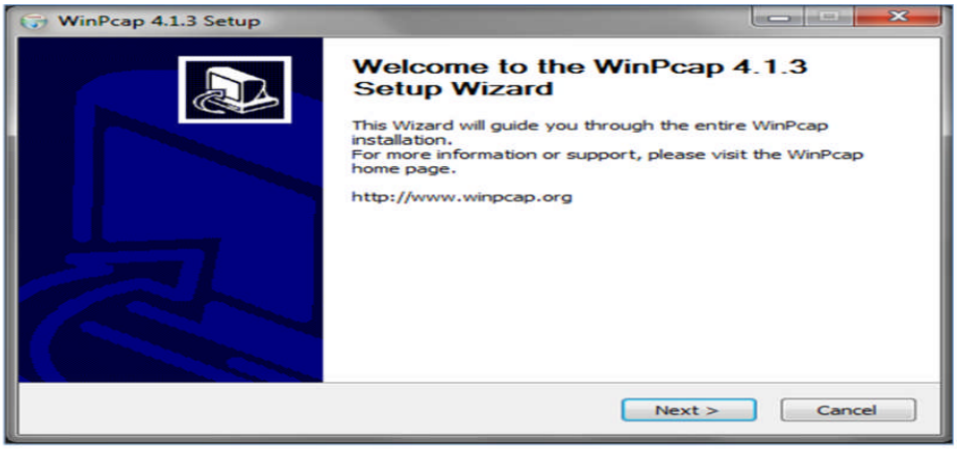
A.1 L'installation de GNS3

Après avoir téléchargé le logiciel GNS3 version 0.8.6, nous lancerons son installation, une fenêtre va apparaitre sur laquelle nous devons cliquer sur le bouton next pour continuer l'installation comme suit :

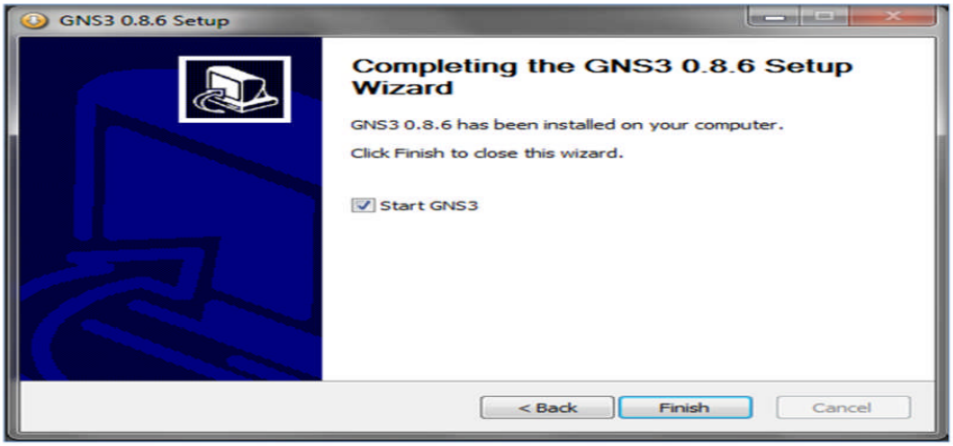
Ensuite la fenêtre suivante s'affiche, nous devons accepter la License et continuer l'installation.



GNS3 dispose de plusieurs logiciels intégrés pour assurer son fonctionnement, parmi eux le logiciel winpcap et le logiciel wireshark que nous deverons installer. Nous allons suivre les différentes instructions pour terminer l'intallation des deux logiciels comme le montres les figures suivante :

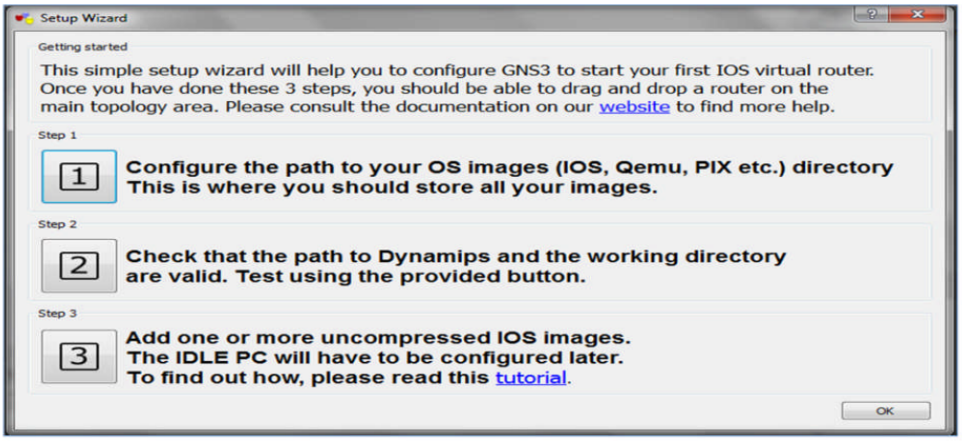


Après avoir suivi les différentes instructions, nous terminerons enfin l'installation du gns3 en cliquant sur le bouton finish.



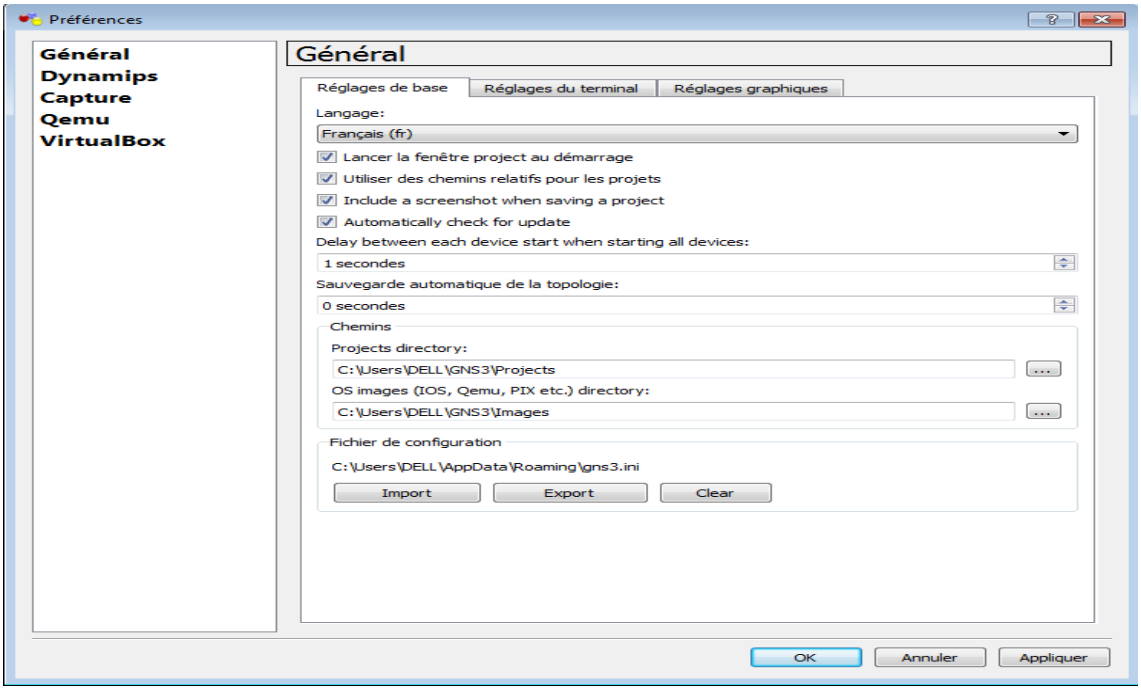
A.2 La configuration de GNS3

L'installation est terminée. Nous pouvons maintenant lancer GNS3. Tout d'abord, il faudra configurer et tester le fonctionnement du Dynamips et ajouter des images IOS pour travailler sur GNS3.

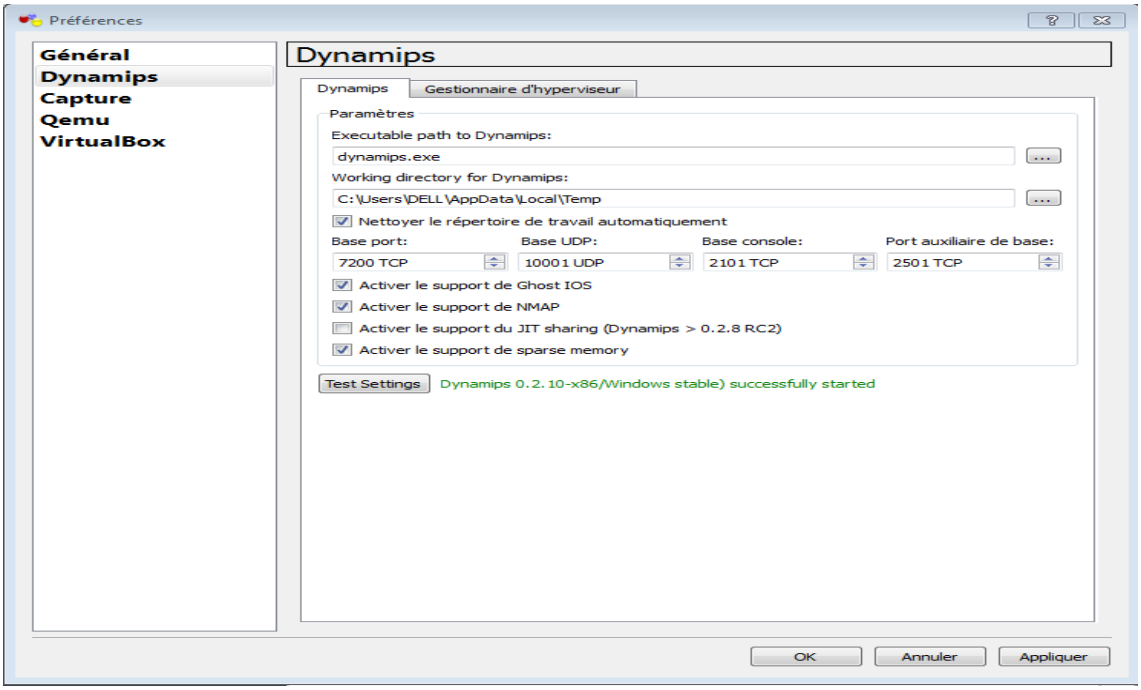


Pour cela, Nous avons trois étapes à suivre :

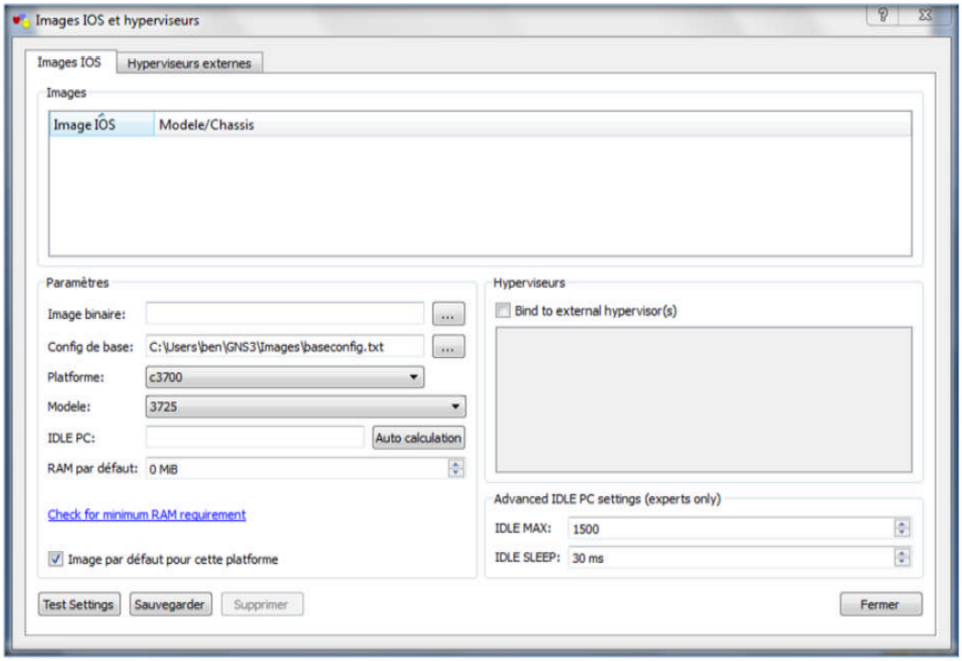
La première consiste à cliquer sur le bouton 1 affiché dans la figure précédente, où une fenêtre apparait comportant les paramètres généraux du logiciel tel que : la langue, les emplacements et les noms des projets et d'images. . .etc.

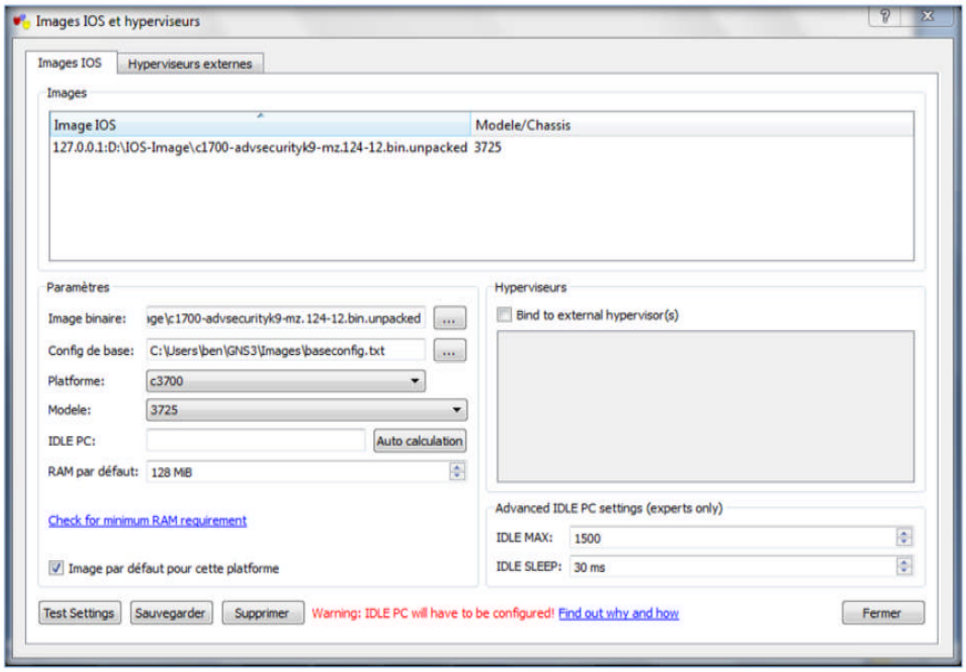


La deuxième étape consiste à tester le bon fonctionnement du dynamips, en cliquant sur le bouton test setting, un message sera afficher pour nous informer sur l'état du dynamyms comme illustré ci-dessous.



Enfin, il nous reste à ajouter les images IOS pour pouvoir utiliser les routeurs souhaités. Pour cela, nous entamerons la troisième étape de configuration, dans l'interface images IOS et hyperviseurs, nous cliquerons sur le bouton parcourir devant fichier image dans les paramètres, puis nous allons spécifier l'image depuis le répertoire dans le quel elle se trouve, enfin nous sauvegardons, comme l'illustre les figures suivantes.





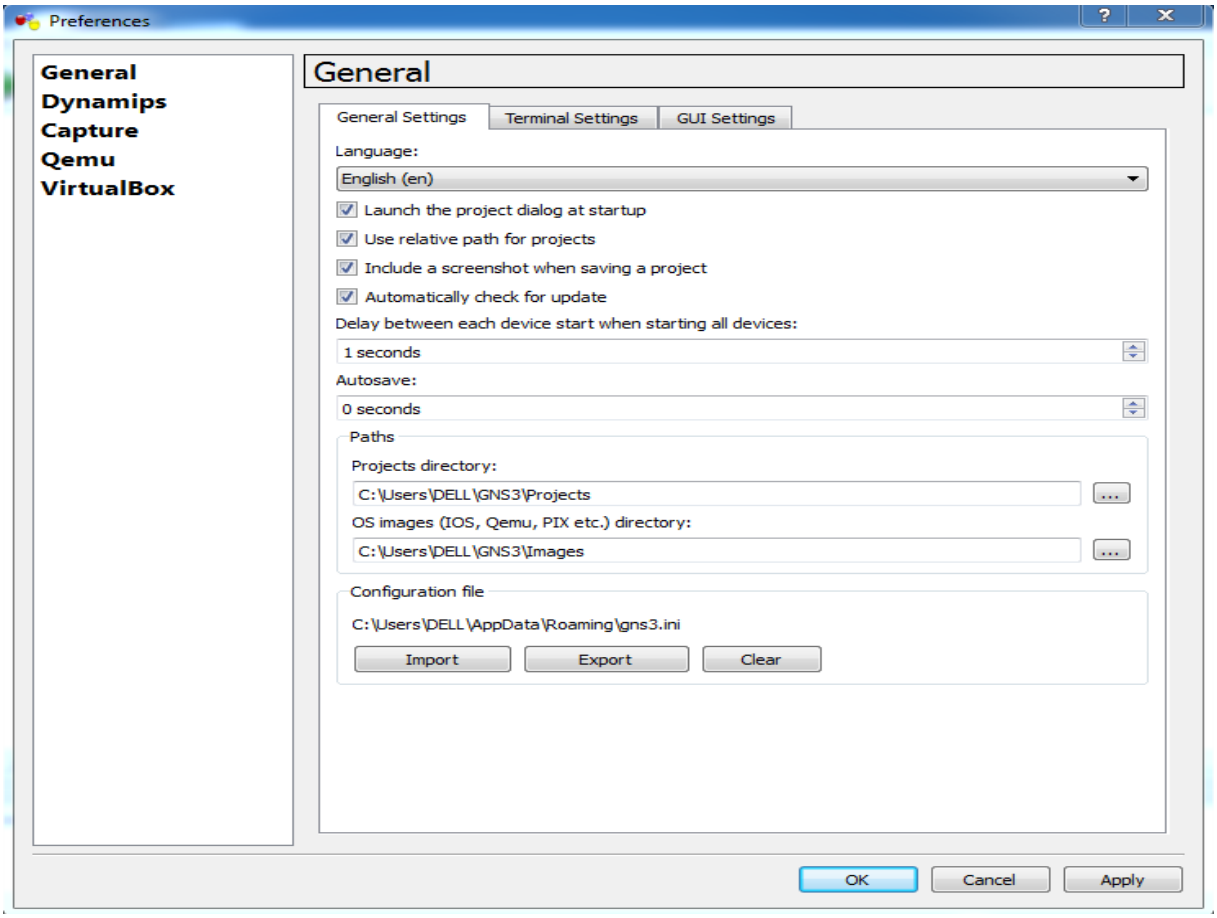
A.3 Mise en place d'un pare-feu ASA sur GNS3

Pour mettre en place un réseau virtuel comportant un pare-feu ASA, il nous faut les éléments suivants :

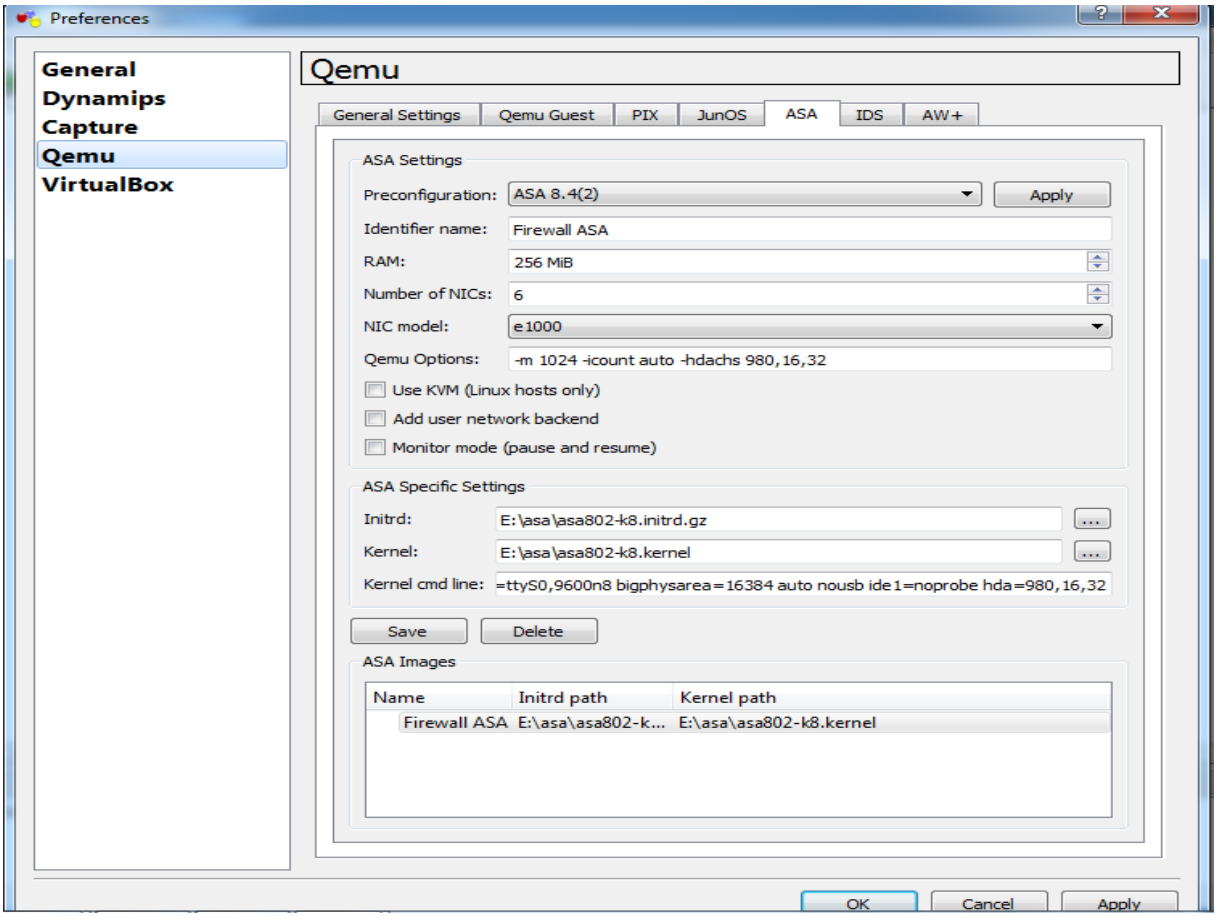
- Un ordinateur fonctionnant de préférence sous un système 64bits.
- Le fichier de boot de l'ASA appelé "initrd.gz".
- Une image d'un IOS d'un Firewall ASA appelé "kernel".
- La configuration pour Qemu : -m 1024 -icount auto -hdachs 980,16,32 .
- La commande noyau : -append ide_generic.probe_mask=0x01 ide_core.chs=0.0 :980, 16, 32 auto nousb console=ttyS0,9600 bigphysarea=65536.

A.4 La configuration de pare-feu ASA dans GNS3

Nous avons toutes les élements concernant le pare-feu ASA, il nous reste juste son configuration. Pour cela, nous ouvrons GNS3. Dans la barre de menu, nous cliquons sur le bouton Edit puis nous sélectionner Préférence, comme illustrer dans la figure suivante :



Ensuite, nous cliquons sur l'onglet Qemu (à gauche), puis dans l'onglet ASA (à droit), une fenêtre apparait ou nous allons remplit les champs vides par les parametres concernant le pare-feu ASA, comme illustré dans la figure suivante.



RÉSUMÉ

L'ouverture des systèmes informatiques des entreprises engendre plusieurs problèmes de sécurité, de ce fait la présence d'une politique qui protège les données de réseau local contre les menaces qui provient soit de l'intérieur soit de l'extérieur est devenue indispensable.

Notre travail consiste à proposer une architecture réseau sécuriser contre ces menaces dont nous avons exploité la technique de sécurité le pare-feu (firewall) où nous avons réalisé les différentes configurations sur le ASA firewall entre trois réseaux LAN/DMZ/WAN qui permet de répondre à quelque problème de sécurité d'une entreprise. Pour mettre notre solution en pratique nous avons utilisé le simulateur GNS3 qui offre la possibilité d'implémenter des architectures de réseau physique.

Mots clés : Pare-feu, DMZ, GNS3, LAN, WAN, Technique de sécurité.

ABSTRACT

The opening of business computer systems creates several security issues, thus the presence of a policy that protects the local network against data threats is either from within or from outside has become indispensable.

Our job is to provide network architecture secure against these threats which we have operated safety technology firewall firewall) and we realized the different configurations on the ASA firewall between three LAN / DMZ / WAN networks that meets some of an enterprise security issue. To put into practice our solution we used the GNS3 simulator that provides the ability to implement physical network architectures.

Key words : Firewall, DMZ, GNS3, LAN, WAN, Security technology.