République **A**lgérienne **D**émocratique et **P**opulaire

Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**ouloud **M**AMMERI DE **T**IZI- **O**UZOU

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

DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etudes

De MASTER ACADEMIQUE

Filière : Electronique

Spécialité : Instrumentation

Présenté par :

M^{r} ATBANE Ramdane

Thème

Proposition et implémentation d'une solution sécurité pour un réseau LAN

Encadré par :

M^{r} F. OUALLOUCHE, Maitre de conférences, UMMTO

2017/2018

Dédicaces

Je dédie ce modeste travail à ma chère mère

A mon cher père

A mes chères sœurs

A mes chers grands parents

Ainsi qu'à mes tantes et mes oncles

Mes cher(e)s ami(e)s

Remerciements

Avant tout, Je tiens à exprimer ma profonde gratitude à mon promoteur Mr Ouallouche Fethi pour la confiance qu'il ma a accordé en acceptant de m'encadrer dans ce mémoire. Je le remercie pour son implication, ses conseils et l'intérêt qu'il a porté à mon travail.

J'adresse mes vifs remerciements aux membres des jurys pour avoir accepté d'examiner et juger ce travail.

Je tiens aussi à remercier ma chère famille pour son soutient, encouragements et ma bienveillance pour mon bien-être et mon succès.

Je tiens à remercier mes amis(e)s pour leur sincère amitié et confiance.
Je leur dois toute ma reconnaissance et mon attachement.

A tous ces intervenants, je présente mes sincères remerciements, mon respect et ma gratitude.

ATBANE.R

Sommaire

Chapitre 2 : Les firewalls

Chapitre3 : Optimisation de la sécurité d'un réseau LAN

Liste des figures

Liste des Acronymes :

ARP : Address Resolution Protocol.

ACL : Access Control List

CERT : Computer Emergency Readiness (ou Response) Team

DES : Data Encryption Standard

DNS : Domain Name System.

DOS : Denial Of Service

DMZ : DeMilitarized Zone

FTP : File Transfer Protocol

GNS3 : Graphical Network Simulator03

HTTP : Hyper Text Transfer protocol

HMAC : Keyed-Hashing for Message AuthentiCation

H-IDS : Host Based Intrusion Detection System

IP : Internet Protocol

ICMP : Internet Control Message Protocol

IPS : Intrusion Prévention System

IMAP : Internet Message Access Protocol

IDS : Intrusion Détection System

IPSec : Internet Protocol Security

L2TP : Layer 2 Tunneling Protocol

L2F : Layer 2 Forwarding

LAN : Local Area Network

MAC : Message AuthentiCation

N-IDS : Network Based Intrusion Detection System

OSI : Open Système Interconnexion

PPTP : Point-to-point tunneling protocol

POP : Post Office Protocol

SSL : Secure Sockets Layers

SMTP : Simple Message Transfert Protocol

SNMP : Simple Network Management Protocol

TCP : Transmission Control Protocol

UDP : User Data Protocol

Introduction

L'information a toujours été 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, en filtrant le trafic entrant et sortant du réseau local. 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 est consacré aux généralités sur les réseaux, la sécurité informatique et la nécessité de la mise en œuvre d'une sécurité au sein d'un réseau informatique. Le deuxième est focalisé sur les firewalls, leurs principes et fonctionnement, ses différents types et architectures et ainsi que leurs place dans les DMZs (Zone démilitarisée). Pour finir 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.

Chapitre 1

Sécurité des réseaux

1.1.Préambule

L'informatique et en particulier l'Internet joue un rôle crucial dans le domaine des réseaux. Un grand nombre d'applications critiques d'un point de vue de leur sécurité sont déployées dans divers domaines comme le domaine militaire, la santé, le commerce électronique, etc...

La sécurité des réseaux devient alors une problématique essentielle tant pour les individus que pour les entreprises ou les Etats. Il est donc important de définir une politique de sécurité pour ces réseaux et de veiller à son respect. Néanmoins les mécanismes de sécurité préventifs mis en place ne sont pas incontournables. Il est nécessaire, de mettre en œuvre des outils permettant de détecter toute violation de la politique de sécurité, c'est-à-dire toute intrusion. Tout au long de ce chapitre, notre intérêt se porte sur les principales menaces pesant sur la sécurité des réseaux ainsi que les mécanismes de défense.

1.2.Sécurité des réseaux

1.2.1. Définition

La sécurité d'un réseau est un ensemble de moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir sa sécurité.

En général, la sécurité d'un réseau englobe celle du système informatique sur lequel il s'appuie. [1]

1.2.2. Évaluation de la sécurité d'un réseau

La sécurité d'un réseau peut s'évaluer sur la base d'un certain nombre de critères de sécurité. On distingue généralement cinq principaux critères de sécurité [1]:

a) L'identification (*identification*)

L'utilisateur d'un système ou de ressources diverses possède une identité (une sorte de clé primaire d'une base de données) qui détermine ses lettres de crédits (*credential*) et ses autorisations d'usage. Cette dernière peut être déclinée de multiples manières, compte utilisateur (login) d'un système d'exploitation ou techniques biométriques empreinte digitale, empreinte vocale, schéma rétinien…

b) L'authentification (*authentication*)

Cette opération consiste à faire la preuve de son identité. Par exemple on peut utiliser un mot de passe, ou une méthode de défi basée sur une fonction cryptographique et un secret partagé. L'authentification est simple ou mutuelle, selon les contraintes de l'environnement.

c) La confidentialité (*privacy*)

C'est la garantie que les données échangées ne sont compréhensibles que pour les deux entités qui partagent un même secret souvent appelé *association de sécurité* (SA). Cette propriété implique la mise en œuvre d'algorithmes de chiffrements soit en mode flux (octet par octet, comme par exemple dans RC4) soit en mode bloc (par exemple une série de 8 octets dans le cas du DES).

d) L'intégrité *(integrity)*

L'intégrité des données (MAC, Message AuthentiCation). Le chiffrement évite les écoutes indiscrètes, mais il ne protège pas contre la modification des informations par un intervenant mal intentionné. Des fonctions à sens unique (encore dénommées empreintes) telles que MD5 (16 octets) ou SHA1 (20 octets) réalisent ce service. Le MAC peut être associé à une clé secrète, telle la procédure HMAC (Clé, Message), *Keyed-Hashing for Message AuthentiCation.*

e) La non-répudiation *(unrepudiation)*

Elle consiste à prouver l'origine des données. Généralement cette opération utilise une signature asymétrique en chiffrant l'empreinte du message avec la clé RSA privée de son auteur (RSA (Empreinte (Message)).

On cite fréquemment un sixième attribut relatif aux notions de sûreté de fonctionnement**,** disponibilité et résilience du système.

L'évaluation de la sécurité d'un système informatique est un processus très complexe basé, en général sur une méthodologie. Cette évaluation passe par une analyse de risques. Cette dernière pesant sur un système informatique, elle même s'appuie sur un ensemble de métriques définies au préalable [1].

1.3.Les causes pour sécuriser les réseaux

1.3.1. Les enjeux

a) Enjeux économiques

Les organismes ou entreprises à but lucratif ont presque toujours la même finalité : c'est de réaliser des bénéfices sur l'ensemble de leurs activités. Cette réalisation est rendue possible grâce à son système d'information considéré comme moteur de développement de l'entreprise. D'où la nécessité de garantir la sécurité de ce dernier. La concurrence fait que des entreprises investissent, de plus en plus dans la sécurisation de leurs systèmes d'information et dans la qualité de service fourni aux clients [1].

b) Enjeux politiques

La plupart des entreprises ou organisations se réfèrent aux documents officiels de sécurité élaborés et recommandés par l'État. Ces documents contiennent généralement des directives qui doivent être appliquées par toute structure engagée dans un processus de sécurisation du réseau. Dans le cadre du chiffrement des données par exemple, chaque État définit des cadres et mesures d'utilisation des algorithmes de chiffrement et les recommande aux entreprises exerçant sur son territoire. Le non respect de ces mesures et recommandations peut avoir des conséquences graves sur l'entreprise. A ce niveau, l'enjeu est plus politique parce que chaque État souhaite être capable de décrypter toutes les informations circulant dans son espace [1].

c) Enjeux juridiques

Dans un réseau, on retrouve de l'information multiforme (numérique, papier, etc.). Le traitement de celle ci doit se faire dans un cadre bien défini et dans le strict respect des lois en vigueur. En matière de juridiction, le non respect des lois et exigences relatives à la manipulation des informations dans un système d'information peut avoir des conséquences graves sur l'entreprise. [1]

1.3.2. Les vulnérabilités

Tous les systèmes informatiques sont vulnérables. Peu importe, le niveau de vulnérabilité de ceux ci. Une vulnérabilité est une faille ou une faiblesse pouvant être exploitée par une personne mal intentionnée pour nuire.

Les vulnérabilités des systèmes peuvent être classées en catégorie (humaine, technologique, organisationnelle, mise en œuvre). [1]

a) Vulnérabilités humaines

L'être humain de par sa nature est vulnérable. La plupart des vulnérabilités humaines proviennent des erreurs (négligence, manque de compétences, surexploitation, etc.), car ne dit-on pas souvent que l'erreur est humaine? Un SI étant composé des humains, il convient d'assurer leur sécurité si l'on veut garantir un maximum de sécurité dans le SI. [1]

b) Vulnérabilités technologiques

Avec la progression exponentielle des outils informatiques, les vulnérabilités technologiques sont découvertes tous les jours.

Ces vulnérabilités sont à la base dues à une négligence humaine lors de la conception et la réalisation. Pour être informé régulièrement des vulnérabilités technologiques découvertes, il suffit de s'inscrire sur une liste ou des listes de diffusion mises en place par les CERT (Computer Emergency Readiness ou Response Team). [1]

c) Vulnérabilités organisationnelles

Les vulnérabilités d'ordre organisationnel sont dues à l'absence des documents cadres et formels, des procédures (de travail, de validation) suffisamment détaillées pour faire face aux problèmes de sécurité du système. Quand bien même ces documents et procédures existent, leur vérification et mises à jour ne sont pas toujours bien assurées. [1]

d) Vulnérabilités mise en œuvre

Les vulnérabilités au niveau mise en œuvre peuvent être dues à la non prise en compte des certains aspects lors de la réalisation d'un projet. [1]

1.3.3. Les menaces

On peut également classer les menaces en deux catégories selon qu'elles ne changent rien (menaces *passives*) ou qu'elles perturbent effectivement le réseau (menaces *actives*). [2]

a) Les menaces passives

Consistent essentiellement à copier ou à écouter l'information sur le réseau, elles nuisent à la confidentialité des données. Néanmoins, celui qui prélève une copie n'altère pas l'information elle même. [2]

b) Les menaces actives

Sont de nature à modifier l'état du réseau. [2]

1.3.4. Les attaques réseaux

Les attaques réseaux sont très nombreuses, il est donc très difficile de les recenser. Il est cependant possible de dresser une typologie des faiblesses de sécurité afin de mieux appréhender ces attaques, qui ont pour point commun d'exploiter des faiblesses de sécurité. Ces dernières peuvent être classifiées par catégories comme suit :

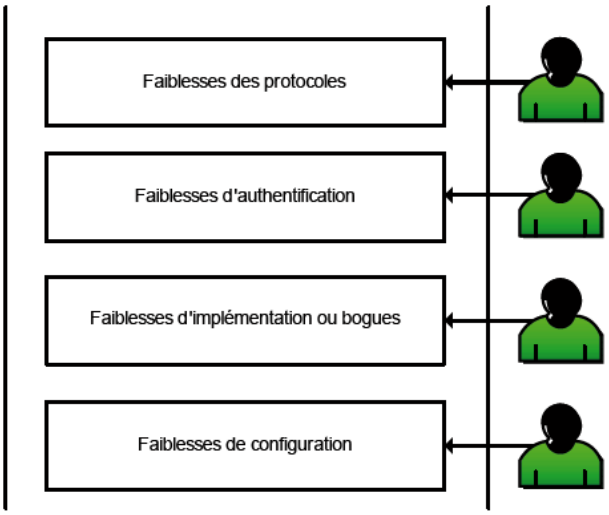

Figure 1.1 : Catégories des faiblesses

a) Faiblesse des protocoles

Quelques protocoles réseaux n'ont pas été conçus pour tenir compte des problèmes de sécurité.

Les principales attaques qui se propagent dans ce type de faiblesse sont :

- **Attaque par fragmentation** : une attaque par fragmentation est une attaque réseau par saturation exploitant le principe de fragmentation du protocole IP. En effet, le protocole IP est prévu pour fragmenter les paquets de taille importantes en plusieurs paquets IP possédant chacun un numéro de séquence et un numéro d'identification

commun. A la réception des données, le destinataire rassemble les paquets grâce aux valeurs de décalages qu'ils contiennent [8].

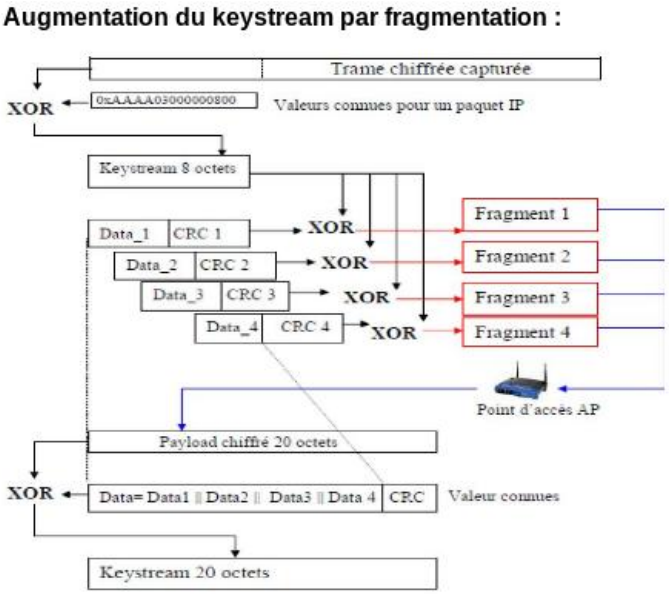

Figure 1.2 : Attaque par fragmentation

- **Attaque par dénis de service** : le déni de service consiste à empêcher les utilisateurs légitimes d'accéder aux informations ou d'obtenir les services auxquels ils ont droit, c'est une attaque contre la disponibilité. C'est souvent le type d'attaque le plus facile, puisqu'il suffit d'émettre des requêtes valide ou non, en très grand nombre (on parle alors d'inondation ou flooding, de façon à saturer les ressources disponible pour un service donné [13].

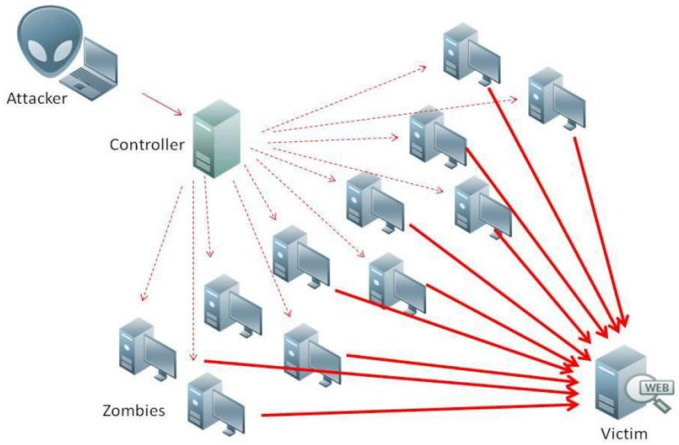

Figure 1.3 : Attaque par dénis de service

b) Faiblesse d'authentification

Les versions actuelles des protocoles IP ou ICMP, ne disposent pas de mécanisme d'authentification; de ce fait elles subissent des attaques qui s'appuient sur ces faiblesses. Parmi les principales attaques on trouve :

- **Attaque ARP :** C'est une technique d'attaque simple qui consiste à exploiter les lacunes du protocole ARP, c'est ce qu'on appelle couramment l'empoisonnement de cache ARP, elle exploite la lacune de non authentification des requêtes. En effet, rien n'indique à une machine qu'une requête provient effectivement d'une machine avec laquelle elle communique [14].

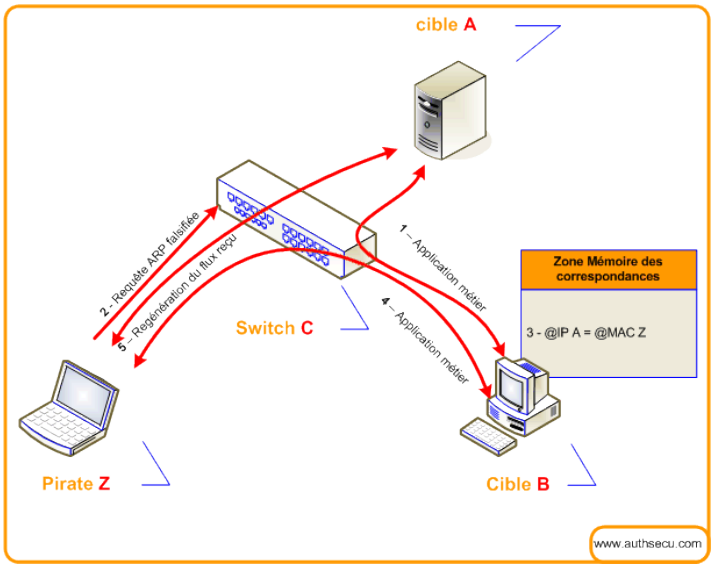

Figure 1.4 : Attaque ARP

- **Attaque man-in-the-middle :** dite en français l'homme au milieu, elle consiste à passer les échanges entre deux personnes par le biais d'une troisième, sous le contrôle de l'entité pirate, ce dernier intercepte et transforme les données, toute en masquant à chaque acteur la réalité de son interlocuteur [10].

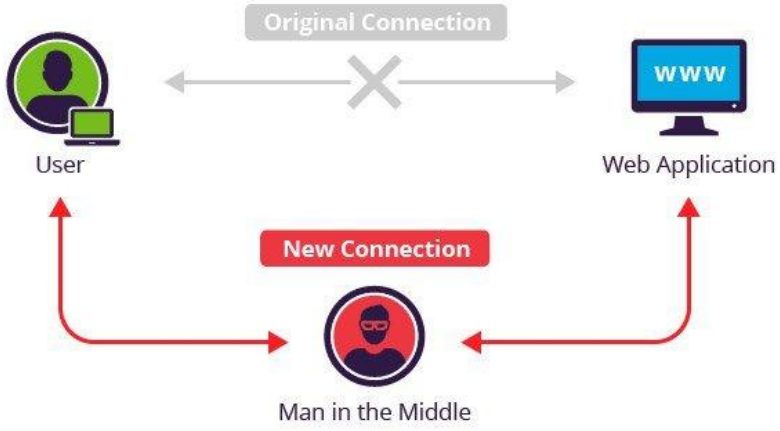

Figure 1.5: Attaque Man in the Middle

- **Attaque par réflexion :** des milliers de requêtes sont envoyées par l'attaquant au nom de la victime. Lorsque les destinataires répondent, toutes les réponses convergent vers l'émetteur officiel, dont les infrastructures se trouvent affectées [15].

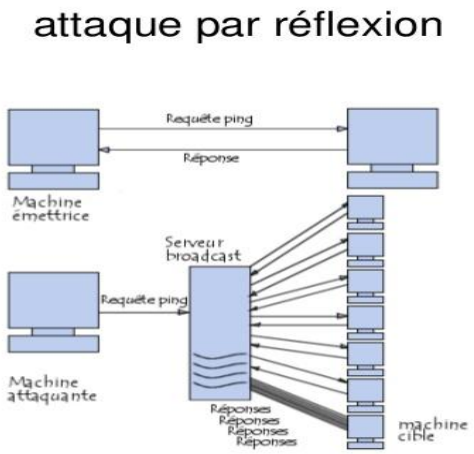

Figure 1.6 : Attaque par réflexion

- **Attaque par Rejeu de message :** Les attaques par « rejeu « (en anglais « replay attaque «) sont des attaques de type « Man in the middle « consistant à intercepter des paquets de données et à les rejouer, c'est-à-dire les retransmettre tels quels (sans aucun déchiffrement) au serveur destinataire [16].

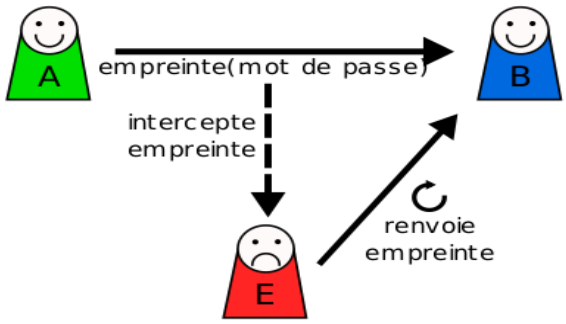

Figure 1.7 : Attaque par rejeu de message

c) Faiblesse d'implémentation

Parmi les attaques qui exploitent ce genre de faiblesse on trouve :

- **Attaque du ping de la mort :** "L'attaque du ping de la mort " est une des plus anciennes attaque réseau. Le principe consiste tout simplement à créer un datagramme IP dont la taille totale excède la taille maximum autorisée (65536 octets). Un tel paquet envoyé à un système possédant une pile TCP/IP vulnérable, provoquera un plantage [16].

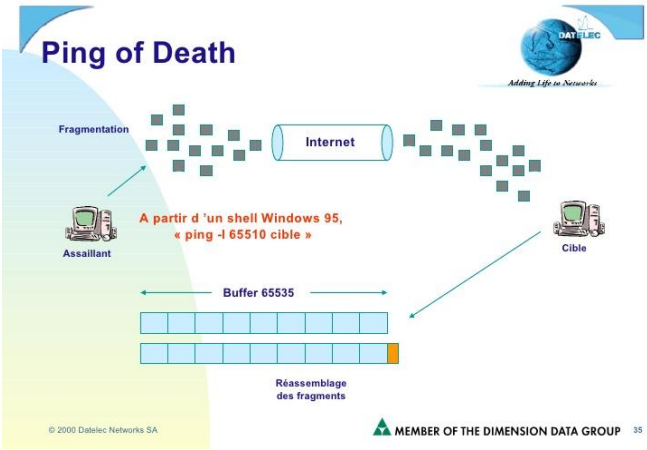

Figure 1.8 : Attaque du ping de la mort

d) Faiblesse de configuration

Une mauvaise configuration des équipements réseau, pare-feu, routeur...etc. est souvent exploitée pour mener des attaques. Les erreurs de configuration peuvent être de plusieurs natures, incluant l'erreur humaine, par conséquent les équipements réseau ne doivent accédés ou configurés que par des acteurs autorisés [17].

1.3.5. Les risques

Les risques se mesurent en fonction de deux critères principaux : la *vulnérabilité* et la *sensibilité.*

La vulnérabilité désigne le degré d'exposition à des dangers. Un des points de vulnérabilité d'un réseau est un point facile à approcher. Un élément de ce réseau peut être très vulnérable tout en présentant un niveau de sensibilité très faible : le poste de travail de l'administrateur du réseau, par exemple, dans la mesure où celui-ci peut se connecter au système d'administration en tout point du réseau. [2]

La sensibilité désigne le caractère stratégique d'un composant du réseau. Celui-ci peut être très sensible, vu son caractère stratégique mais quasi invulnérable, grâce à toutes les mesures de protection qui ont été prises pour le prémunir contre la plupart des risques. [3]

1.4.Les logiciels malveillants

Un logiciel malveillant est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur infecté. Plusieurs types de logiciels malveillants ont été proposées nous citons les plus répandus :

1.4.1. Virus

Un virus est un morceau de programme informatique malicieux, conçu et écrit pour qu'il se reproduise. Cette capacité à se répliquer, peut toucher votre ordinateur, sans votre permission et sans que vous le sachiez. En termes plus techniques, le virus classique s'attachera à un de vos programmes exécutables et se copiera systématiquement sur tout autre exécutable que vous lancez. [4]

Les virus peuvent s'avérer particulièrement dangereux et endommager plus ou moins gravement les machines infectées. Le virus peut se répandre à travers tout moyen d'échange de données numériques comme l'Internet, et notamment par l'intermédiaire des messages électroniques ou de leurs pièces attachées.

1.4.2. Vers

Un ver (ou *worm*) est un type de virus particulier qui se propage par le réseau. Le vers contrairement aux virus, une fois implantés et activés dans un ordinateur, sont des programmes capables de se propager d'un ordinateur à un autre via le réseau, sans intervention de l'utilisateur et sans exploiter le partage de fichiers.

1.4.3. Cheval de Troie

Un cheval de Troie (*Trojan horse*) est un programme qui exécute des instructions sans l'autorisation de l'utilisateur. Ces instructions sont généralement nuisibles à l'utilisateur, et qui une fois installé sur un ordinateur effectue des actions cachées et pernicieuses. [5]
Le cheval de Troie contrairement au ver ne se réplique pas.

1.4.4. Logiciel Espion

Un logiciel espion (ou spyware) est un programme, conçu dans le but de collecter des données personnelles sur ses utilisateurs et de les envoyer à son concepteur, ou à un tiers via Internet ou tout autre réseau informatique, sans avoir obtenu au préalable une autorisation explicite et éclairée desdits utilisateurs. [1]

Une variété particulièrement toxique de logiciel espion est le keylogger (espion dactylographique), qui enregistre fidèlement tout ce que l'utilisateur tape sur son clavier et le transmet à son honorable correspondant ; il capte ainsi notamment identifiants, mots de passe et codes secrets. [5]

1.4.5. Spam

Le spam est une vraie problématique. Il encombre les résultats de recherche ce qui gène l'utilisateur. Un spam peut être défini comme étant un email anonyme, non sollicité, indésirable et envoyé en grand nombre de façon automatique sans l'accord de son destinataire.

1.4.6. Cookies

Un cookie est un petit fichier très simple, en fait un texte, enregistré sur le disque dur de l'ordinateur d'un internaute à la demande du serveur gérant le site Web visité. Il contient des informations sur la navigation effectuée sur les pages de ce site. L'idée originelle est de faciliter l'utilisation ultérieure du site par la même personne.
Un cookie n'étant pas exécutable, il ne peut contenir de virus.

1.4.7. Bombe logique

Une Bombe logique est une partie d'un programme malveillant (virus, cheval de Troie, etc.) qui reste dormante dans le système hôte jusqu'à ce qu'un instant ou un événement survienne, ou encore que certaines conditions soient réunies, pour déclencher des effets dévastateurs en son sein. [6]

Les bombes logiques sont généralement utilisées dans le but de créer un déni de service en saturant les connexions réseau d'un site, d'un service en ligne ou d'une entreprise.

1.4.8. Porte dérobée

C'est un moyen de contourner les mécanismes de contrôle d'accès. Elle s'agit d'une faille du système de sécurité due à une faute de conception accidentelle ou intentionnelle.

1.5.Mécanismes de la sécurité

À cause des menaces provenant des logiciels malveillants, Il faut mettre en place des mécanismes pour s'assurer la confidentialité, l'intégrité et la disponibilité des services. Parmi ces mécanismes, on peut citer :

1.5.1. Cryptage

Le chiffrement est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement. Ce principe est généralement lié au principe d'accès conditionnel.
Bien que le chiffrement puisse rendre secret le sens d'un document, d'autres techniques cryptographiques sont nécessaires pour communiquer de façon sûre. [9]

1.5.2. Pare-feu

Un pare-feu (*firewall*, en anglais) est un dispositif matériel et/ou logiciel qui implémente la fonction de sécurité de contrôle d'accès. Un pare-feu est donc un dispositif pour filtrer les accès, les paquets IP, les flux entrant et sortant d'un système. Un pare-feu est installé en coupure sur un réseau lorsqu'il sert de passerelle filtrante pour un domaine à la frontière d'un périmètre fermé. Un pare feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit aussi d'une passerelle filtrante comportant au minimum les interfaces réseaux suivante:

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

1.5.3. Antivirus

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants. Ceux-ci peuvent se baser sur l'exploitation de failles de sécurité, mais il

peut également s'agir de programmes modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur de l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur. [7]

Un antivirus vérifie les fichiers et courriers électroniques, les secteurs de boot (pour détecter les virus de boot), mais aussi la mémoire vive de l'ordinateur, les médias amovibles (clefs USB, CD, DVD, etc.), les données qui transitent sur les éventuels réseaux (dont internet), etc.

1.5.4. Virtual Private Network *(V.P.N)*

Les entreprises et les organisations possèdent en général plusieurs sites géographiques qui travaillent conjointement en permanence. Dans chaque site géographique, les utilisateurs sont connectés ensemble grâce à un réseau local. Ces réseaux locaux sont souvent connectés via Internet. En outre, certains utilisateurs peuvent vouloir se connecter aux réseaux de l'entreprise en étant à l'extérieur chez un client ou en déplacement.
Il existait autrefois des liaisons physiques spécialisées, qui sont maintenant abandonnées au profit de liaisons logiques.

Un réseau virtuel privé (*Virtual Private Network*, en anglais d'où l'abréviation VPN) consiste en fabrication d'un tunnel logique qui sera contracté par les communications de l'entreprise, lesquelles seront véhiculées dans cette tranchée numérique construite sur un réseau fréquenté par d'autres usagers. Dans la pratique, il s'agit d'un artifice, car les données vont utiliser un chemin ordinaire, emprunté par tout le monde, mais ces données chiffrées et tagguées seront sécurisées, à l'image du transport de containers plombés sur une route. Le caractère privé du réseau est donc complètement virtuel puisqu'il ne s'agit pas de liaison physique spécialisée. Le caractère privé est créé par un protocole cryptographique (IPSec ou PPTP). Un VPN est donc une communication sécurisée entre deux points d'un réseau public, d'où l'expression de tunnel.

Un VPN fournit un service fonctionnellement équivalent à un réseau privé, en utilisant les ressources partagées d'un réseau public. Les réseaux VPN Internet sont utilisés dans plusieurs types d'application : Intranet étendus, Extranet, accès distants. Des tunnels empruntent le réseau Internet et assurent une sécurité robuste des échanges de données :

authentification forte des équipements VPN source et destination, intégrité et confidentialité des données échangées.

VPN fournit aux utilisateurs et administrateurs du système d'information des conditions d'exploitation, d'utilisation et de sécurité à travers un réseau public identiques à celles disponibles sur le réseau privé. Parmi les protocoles VPN les plus utilisés, on peut citer :

VPN IPSec et VPN SSL

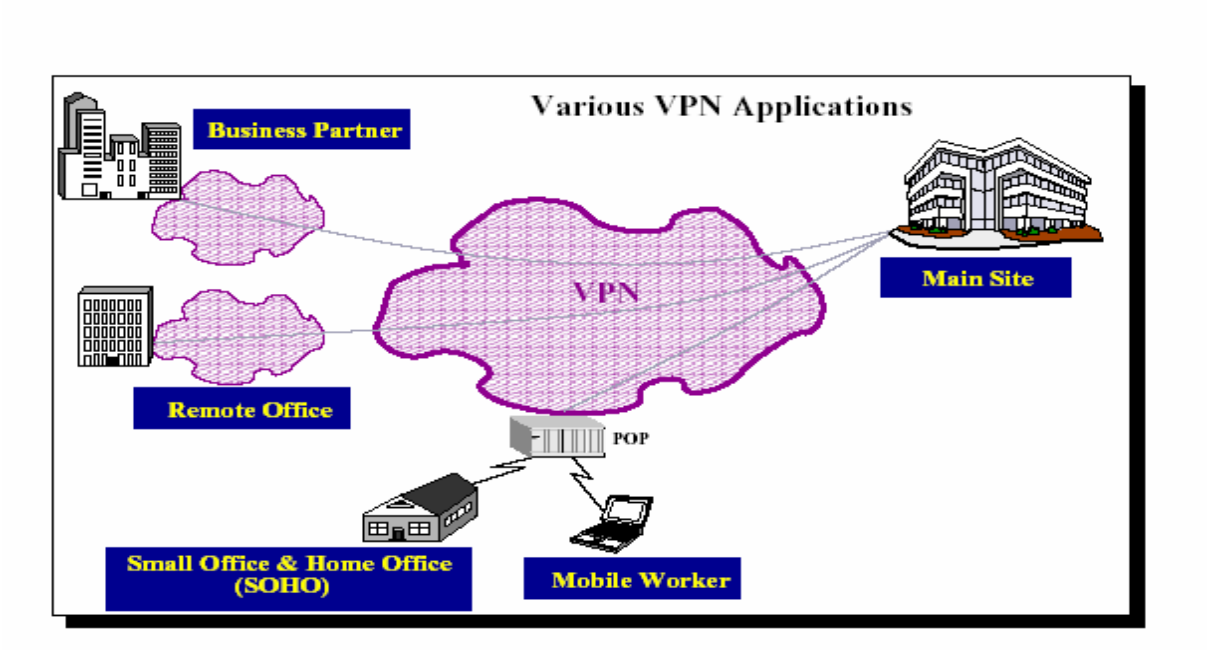

Figure 1.9 : Différentes applications VPN

a) Internet Protocol Security *(IPSec)*

IPSec est un protocole destiné à fournir différents services de sécurité. Son intérêt principal reste sans contexte son mode de tunneling, c'est-à-dire d'encapsulation d'IP qui lui permet entre autres choses de créer des réseaux privés virtuels (ou VPN en anglais).

Citons quelques propriétés générales des tunnels destinées aux VPN :

• Les données transitant sont chiffrées (confidentialité) et protégées (intégrité)

• Les 2 extrémités sont authentifiées

• Les adresses sources et destination sont chiffrées

Il ne faut pas négliger les aspects pratiques tels que la charge processeur dû au chiffrement, le débit théorique possible, l'overhead induit et donc le débit effectif…

De plus IPSec n'est pas le seul protocole permettant d'établir des tunnels, il en existe d'autres comme les « point-à-point » tel que L2TP, L2F ou encore PPTP qui peut induire un overhead non négligeable.

IPSec est un protocole au niveau de la couche réseau qui offre une :

• Intégrité des paquets : les paquets sont protégés de sorte que tous les changements pendant leur transmission peuvent être détectés

• Confidentialité des paquets : les paquets sont chiffrés avant d'être transmis sur les réseaux.

b) Secure Sockets Layers *(SSL)*

SSL (Secure Sockets Layers) est un procédé de sécurisation des transactions effectuées via Internet. Il repose sur un procédé de cryptographie par clef publique afin de garantir la sécurité de la transmission de données sur Internet. Son principe consiste à établir un canal de communication sécurisé entre deux machines (un client et un serveur) après une étape d'authentification.

Le système SSL est indépendant du protocole utilisé, ce qui signifie qu'il peut aussi bien sécuriser des transactions faites sur le Web par le protocole HTTP que des connexions via le protocole FTP, POP ou IMAP. En effet, SSL agit telle une couche supplémentaire, permettant d'assurer la sécurité des données, situées entre la couche application et la couche transport (protocole TCP par exemple).

1.5.5. Intrusion Détection System *(IDS)*

Un système de détection d'intrusion (ou IDS : Intrusion Détection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions. [11]

Un IDS réagit en cas d'anomalie, à condition que le système puisse bien identifier les intrus externes ou internes qui ont un comportement anormal, en déclenchant un avertissement, une alerte, en analysant éventuellement cette intrusion pour empêcher qu'elle ne se reproduise, ou en paralysant même l'intrusion.

Un IDS est un capteur informatique qui écoute de manière furtive le trafic sur un système, vérifie, filtre et repère les activités anormales ou suspectes, ce qui permet ultérieurement de décider d'action de prévention. Sur un réseau, l'IDS est souvent réparti dans tous les emplacements stratégiques du réseau.

Il faut distinguer deux aspects dans le fonctionnement d'un IDS : le mode de détection utilisé et la réponse apportée par l'IDS lors de la détection d'une intrusion.

Les techniques sont différentes selon que l'IDS inspecte un réseau ou que l'IDS contrôle l'activité d'une machine (hôte, serveur).

• Sur un réseau, il y a en général plusieurs sondes qui analysent de concert, les attaques en amont d'un pare-feu ou d'un serveur.

• Sur un système hôte, les IDS sont incarnés par des applications standards furtives qui analysent des fichiers de journalisation et examinent certains paquets issus du réseau.

Il existe deux grandes familles distinctes d'IDS:

• Les N-IDS (Network Based Intrusion Detection system), ils assurent la sécurité au niveau du réseau.

• Les H-IDS (Host Based Intrusion Detection system), ils assurent la sécurité au niveau des hôtes.

Un N-IDS nécessite un matériel dédié et constitue un système capable de contrôler les paquets circulant sur un ou plusieurs liens réseau dans le but de découvrir si un acte malveillant ou anormal a lieu.

Le H-IDS réside sur un hôte particulier et la gamme de ces logiciels couvre donc une grande partie des systèmes d'exploitation tels que Windows, Linux, ect...

Le H-IDS se comporte comme un démon ou un service standard sur un système hôte. Traditionnellement, le H-IDS analyse des informations particulières dans les journaux de logs (syslogs, messages, lastlogs...) et aussi capture les paquets réseaux entrant/sortant de l'hôte pour y déceler des signaux d'intrusion (Déni de services, Backdoors, chevaux de troie...).

1.5.6. Intrusion Prévention System *(IPS)*

Un système de prévention d'intrusion (ou IPS, Intrusion Prévention System) est un outil similaire aux IDS, sauf que ce système peut prendre des mesures afin de diminuer les risques d'impact d'une attaque. C'est un IDS actif, il détecte un balayage automatisé, l'IPS peut bloquer les ports automatiquement. [11]

1.6.Mise en place d'une politique de sécurité

La mise en œuvre d'une politique de sécurité globale est assez difficile, essentiellement par la diversité des aspects à considérer. Une politique de sécurité peut se définir par un certain nombre de caractéristiques : les niveaux où elle intervient, les objectifs de cette politique et enfin les outils utilisés pour assurer cette sécurité.

Chaque aspect différent doit être pris en compte, de façon à atteindre les objectifs de sécurité désirés, en utilisant de façon coordonnée les différents outils disposition. [12]

Nous allons tout d'abord parler des différents aspects d'une politique de sécurité, avant de définir les objectifs visés, puis de voir les outils disponibles pour appliquer cette politique. [12]

Une politique de sécurité s'élabore à plusieurs niveaux. [12]

- sécuriser l'accès aux données de façon logicielle (authentification, contrôle d'intégrité).
- sécuriser l'accès physique aux données : serveurs placés dans des salles blindées avec badge d'accès…
- Un aspect très important pour assurer la sécurité des données d'une entreprise est de sensibiliser les utilisateurs aux notions de sécurité, de façon à limiter les comportements à risque : si tout le monde peut accéder aux salles de serveurs, peut importe qu'elles soient sécurisées !
- De même, si les utilisateurs laissent leur mot de passe écrit à côté de leur PC, son utilité est limitée…
- Enfin, il est essentiel pour un responsable de sécurité de s'informer continuellement, des nouvelles attaques existantes, des outils disponibles…de façon à pouvoir maintenir à jour son système de sécurité et à combler les brèches de sécurité qui pourraient exister.

1.7.Discussion

Dans ce chapitre, on a présenté les principales notions et concepts de la sécurité des systèmes informatiques et des réseaux, dont on a décrit plus particulièrement les menaces provenant des logiciels malveillants et introduit une politique de sécurité.

Ainsi différentes méthodes et mécanismes connus pour sécuriser les réseaux.

A travers les différentes sections qu'on a montrées, on a conclu qu'aucun réseau n'est totalement sûr et il est impossible de garantir la sécurité totale d'un réseau.

Chapitre 2
Les firewalls

2.1.Préambule

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 a 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 [18].

Figure 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 à Internet ou une personne d'accéder à certains services comme le FTP par exemple [18].

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 basée sur le service ~~de~~ courrier. D'autres firewalls, moins stricts, bloquent uniquement les services reconnus comme étant des services dangereux [18].

Généralement, les firewalls sont configurés pour protéger contre les accès non authentifiés du réseau externe. Ceci, plus qu'autre chose, empêche les pirates de se loger sur des machines de votre réseau interne, mais autorise les utilisateurs de communiquer librement avec l'extérieur [18].

Les firewalls sont également intéressants dans le sens ou ils constituent un point unique où l'audit et la sécurité peuvent être imposés. Tous les échanges passeront par lui. Il pourra donner des résumés de trafic, des statistiques sur ce trafic, ou encore toutes les connexions entre les deux réseaux [18].

2.2.2. De quoi ne protège pas un firewall

Un firewall ne protège pas des attaques qui ne passent pas par lui. Certaines entreprises achètent des firewalls a des prix incroyables alors que certains de leurs employés sont parfois connectés par modem au monde extérieur. Il est important de noter qu'un firewall doit être à la mesure de politique de sécurité globale du réseau [18].

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 à Internet et devrait être isolé du reste du réseau [18].

Une autre chose contre laquelle un firewall ne peut protéger est la menace existante à l'intérieur de l'entreprise. Si un espion industriel décide de faire sortir des données, il y arrivera. Il vaut mieux vérifier qui a accès aux informations que de mettre un firewall dans ce cas [18].

Les firewalls ne protègent pas très bien des virus. Il y a trop de manières différentes de coder des fichiers pour les transférer. 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 attaché à un mail sans être sûr de sa provenance [18].

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 passent également très facilement. Les virus sur Internet sont bien moins important que les virus sur disquette [18].

2.3.Principe de fonctionnement

Le fonctionnement d'un firewall repose sur le filtrage des paquets 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. [19]

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 [19].

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 [19].

– Les proxys 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 [19].

• 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 [19].

– Le client établit une connexion TCP avec la passerelle en demandant de communiquer avec le serveur.

– La passerelle peut :

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

– La passerelle se connecte au serveur et relaie les données entre les deux connexions TCP. [19]

2.4.Scénarios d'attaques (Pénétrations de réseaux)

Qu'est-ce qu'une backdoor ? Une backdoor est un accès <caché> sur votre système qui permet à un pirate d'en prendre le contrôle à distance. Il existe une multitude de sortes de backdoor, et en général dans ce domaine, l'imagination des pirates rivalise avec l'incrédulité des utilisateurs. Voici quelques scénarios d'attaques [20] :

2.4.1. Premier cas (Pas de protection)

Considérons un ordinateur victime sur lequel on a installé une backdoor en exploitant une des failles du système. L'attaquant a alors la possibilité d'utiliser tous les services

présents sur cet ordinateur. Il lui suffit d'envoyer ses ordres à la backdoor et de récupérer les réponses.

2.4.2. Deuxième cas (Filtrer les flux entrants illégaux)

La sécurité du système n'étant pas infaillible, il faut installer un pare-feu avec états. Le trafic entrant est maintenant stoppé comme il se doit. Malheureusement, le pirate étant rusé et malicieux, il a pris soin de s'arranger pour que sa backdoor initie elle-même les sessions. Du coup le Firewall laisse passer les requêtes de l'attaquant qui sont considérées comme des réponses par celui-ci.

2.4.3. Troisième cas (Bloquer les flux entrants et sortants)

Dans le cas précédent, le problème était dû aux flux sortants qui permettaient au cheval de Troie d'initier les sessions avec la machine de l'attaquant. Il s'agit donc de bloquer les flux sortants. Pour cela la défense insère donc un proxy afin de contrôler ce qui sort du réseau.

Malheureusement le trojan peut encore sortir, certes avec plus de difficultés puisqu'il devra se renseigner sur les flux autorisés à sortir par le proxy, et les utiliser pour passer le proxy. Par exemple on peut en capsuler des ordres dans du HTTP, dans du SSL, DNS.

2.5.Les techniques et outils de découvertes de pare-feu

Il existe beaucoup d'outils et beaucoup de techniques permettant d'identifier un pare-feu. Il est évident que la plupart des outils utilisés par les pirates pour découvrir les pare-feu sont utilisables pour une activité tout aussi louable telle que la vérification du bon fonctionnement du firewall et de la robustesse du réseau.

Dans un premier temps il convient de localiser le ou les pare-feu, ensuite l'attaquant cherchera à identifier le pare-feu, soit en espérant exploiter une faille même du pare-feu, soit il cherchera à identifier les règles du pare-feu afin d'y détecter une faille dans le filtrage de paquet.

Pour identifier les règles d'un pare-feu, il faut utiliser un scanner de port. Il existe de nombreux scanner de ports, les plus connus sont Firewalk, Nmap et Hping2 [20].

2.6. Configuration théorique des défenses

Il existe deux politiques de configurations différentes en ce qui concerne le pare-feu ; la première consiste à tout autoriser sauf ce qui est dangereux : cette méthode est beaucoup trop laxiste.

En effet, cela laisse toute latitude à l'imagination des intrus de s'exprimer. Et à moins d'avoir tout prévu de façon exhaustive, on laissera forcément des portes ouvertes, des failles béantes dans notre système. A éviter absolument.

La deuxième consiste à tout interdire sauf ce dont on a besoin et ce en quoi on a confiance : cette politique est beaucoup plus sécuritaire.

En effet, les services sont examinés avant d'être autorisés à passer le firewall, et sont donc tous soumis à un examen plus ou moins approfondi.

Ainsi, pas de mauvaise surprise sur un service que l'on pensait ne pas avoir installé, plus d'oubli : tout service autorisé est explicitement déclaré dans le firewall.

Cette politique s'accompagne de la création de deux zones : une zone interne et l'extérieur.

On peut considérer que tout ce qui est dans notre réseau local est autorisé, sans prendre de trop gros risques : le firewall est là pour nous protéger des attaques extérieures [20]

2.7. 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.

2.7.1. 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 prédéfinies par l'administrateur (généralement appelées ACL, Access Control List) [21].

Ces firewalls interviennent sur les couches réseau et transport. Les règles de filtrages s'appliquent alors par rapport à une d'adresses IP sources ou destination, mais aussi par rapport à un port source ou destination [21].

2.7.2. 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 en compte 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 une connexion déjà connue.

• INVALID : Correspond à un paquet qui n'est pas valide [21].

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 [21].

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'on appel flood).

Ceci provoque la surcharge de la table des connexions des serveurs ce qui les rend incapable d'accepter de nouvelles connexions.

Les firewalls stateful étant capables de vérifier l'état des sessions, ils sont capables de détecter les tentatives excessives de demande de connexion. Il est possible, en autre, ne pas accepter plus d'une demande de connexion par seconde pour un client donné [21].

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 [21].

2.7.3. Firewall applicatif

Les firewalls applicatif (aussi nommé pare-feu de type proxy ou passerelle applicative) fonctionne sur 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 [21].

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) [21].

2.7.4. 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 [21].

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 [21].

2.7.5. 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) [21].

Leur principal atout est qu'ils permettent de contrôler les accès aux réseaux des applications installés 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 [21].

2.8.Les différents types de pare-feu

Il existe trois types de pare-feu qui sont les suivants :

2.8.1. Les pare-feu bridge

Les pare-feu bridge agissent comme des câbles réseau avec la fonction de filtrage en plus, leurs interfaces ne possèdent pas d'adresse IP et ne font que transférer les paquets d'une interface à une autre. Cette absence d'adresse IP est particulièrement utile, car cela signifie que le pare-feu est indétectable pour un hacker lambda.

En effet, quand une requête est émise sur la câble réseau, le pare-feu bridge ne répondra jamais, car ses adresses MAC ne circuleront jamais sur le réseau, et comme il ne fait que transmettre les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirigé contre le pare-feu.

Parmi ses avantages on trouve qu'il est impossible de l'éviter puisque les paquets passeront par ses interfaces et il est peu coûteux, par contre sa configuration est souvent contraignante [20].

2.8.2. Les pare-feu matériels

Les pare-feu matériels se trouvent souvent sur des routeurs achetés dans le commerce par de grands constructeurs comme Cisco. Intégrés directement dans la machine.

Leur configuration est souvent relativement ardue, mais leur avantage est que leur interaction avec les autres fonctionnalités du routeur est simplifiée de par leur présence sur le même équipement réseau, ils sont intégrés au matériel réseau avec une administration relativement simple et ils ont un bon niveau de sécurité mais ils dépendent du constructeur pour les mises à jour [20].

2.8.3. Les pare-feu logiciels

Les pare-feu logiciels sont présents à la fois dans les serveurs et les routeurs, nous pouvons les classer en deux catégories ; les pare-feu personnels et les pare-feu plus sûr.
Les pare-feu personnels sont assez souvent commerciaux et ont pour but de sécuriser un ordinateur particulier, et non pas un groupe d'ordinateurs.

Souvent payants, ils peuvent être contraignants et quelque fois très peu sécurisés.

2.9. 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.

2.9.1. 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 [22] :

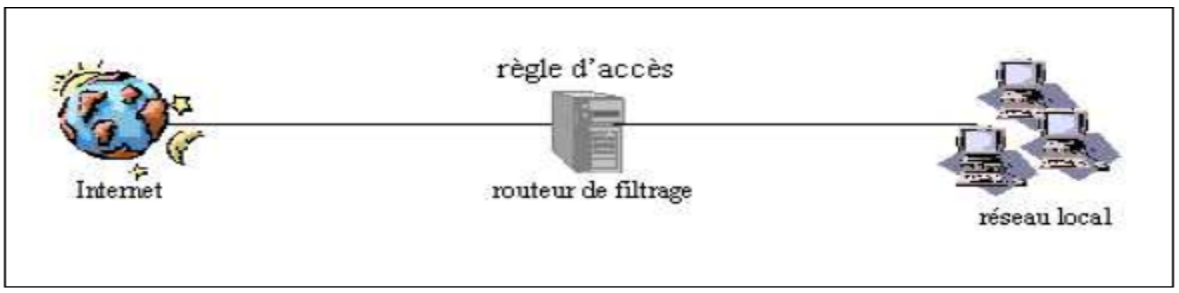

Figure 2.2 : Firewall avec routeur de filtrage

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. [22]

- **Avantages :** facilité de configuration, peu coûteux, de plus il fournit des traces exploitables avec la possibilité d'alarmes pour [22] :

• 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 [22].

2.9.2. 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, est 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 [22].

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 [22].

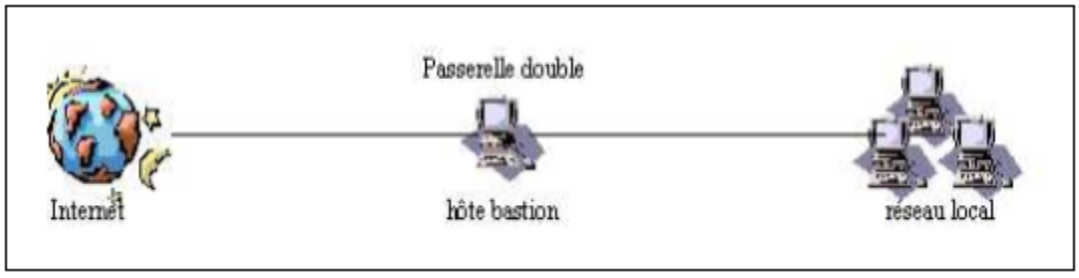

Figure 2.3 : La passerelle double

La passerelle double est la possibilité la plus simple pour réaliser un firewall d'application n'autorisant aucun trafic IP entre les réseaux [22].

- **Avantage :** bon, peu coûteux, accessible [22].
- **Inconvénient :** du fait de tout ce qu'elle doit faire (routage et application), une telle configuration pourrait rencontrer des problèmes de performance.

2.9.3. 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 [22] :

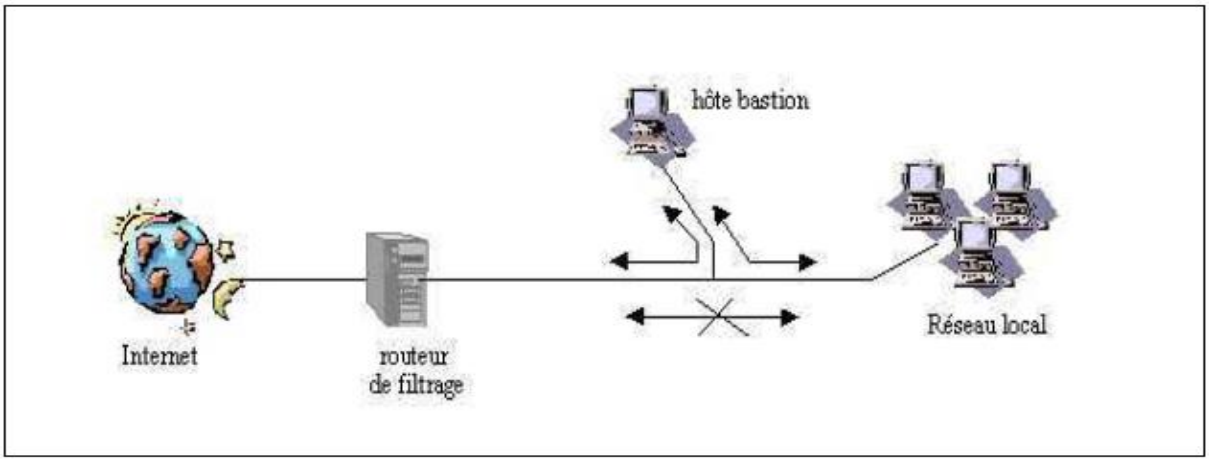

Figure 2.4 : Firewall avec réseau de filtrage

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, l'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 [22].

- **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 [22].

2.9.4. 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 [22].

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.

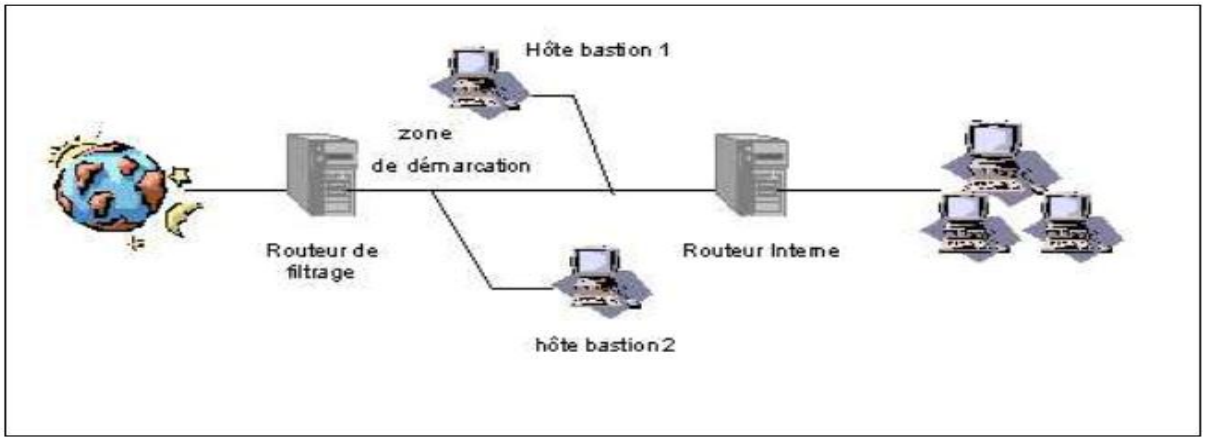

Figure 2.5 : Firewall avec sous-réseau de filtrage

Pour s'introduire sur le réseau d'entreprise à travers ce firewall, il faut franchir les deux routeurs, ainsi que les réseaux bastions intercalés. [22]

• 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. [22]

- **Avantage :** système Firewall très sûr [22].
- **Inconvénients :** coût d'investissement élevé, effort administratif important [22].

2.10. Zone démilitarisée (DMZ)

2.10.1. 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 [23].

La configuration la plus répandue 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 [23] :

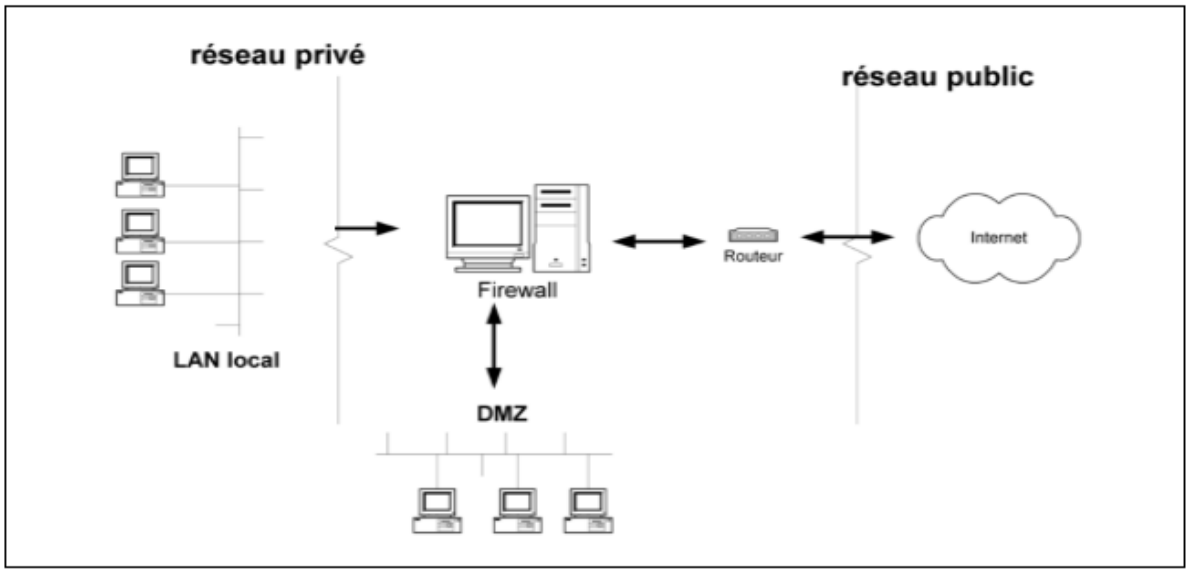

Figure 2.6 : Firewall avec DMZ

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.

2.11. 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 capacité à 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 [24] [25].

2.12. Discussion

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.

Chapitre 3
Optimisation de la sécurité d'un réseau LAN

3.1.Préambule :

Dans ce chapitre nous allons nous intéresser à la sécurité d'un réseau d'entreprise, en commençant par trouver les failles de celui-ci. A partir de là nous proposerons des solutions pour améliorer la sécurité de ce réseau.

Notre solution consistera en un remaniement des différentes configurations, et l'implémentation d'un pare-feu matériel dans l'architecture, qui sera configuré par le biais de l'interface graphique ASDM.

3.2.Description de l'environnement de travail

3.2.1. GNS3

GNS3 (Graphical Network Simulator),est un logiciel libre qui permet la simulation d'un réseau informatique , c'est un émulateur qui est proche de la réalité ,il est parfait pour se préparer aux certifications Cisco CCNA ,CCNP,CCIP,CCIE [26].

GNS3 permet d'avoir un routeur Cisco virtuel sur un ordinateur. à savoir qu'il ne fournit pas d'IOS il faut se les procurer à 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 [26].

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). [27]
- **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 [28].

- **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 [28].

- **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 [29].

3.2.2. 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 [30].

- **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 [31].

3.2.3. 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. [27]

• Emulation de plusieurs plate-forme de routeurs Cisco IOS, ou encore IPS, PIX et firewalls ASA. [27]

• Simulation de switches Ethernet, ATM et Frame Relay. [27]

• Connexion de réseaux simulés au monde réel. [27]

• Capture de paquets grâce à Wireshark. [27]

3.2.4. 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 notre topologie réseau.

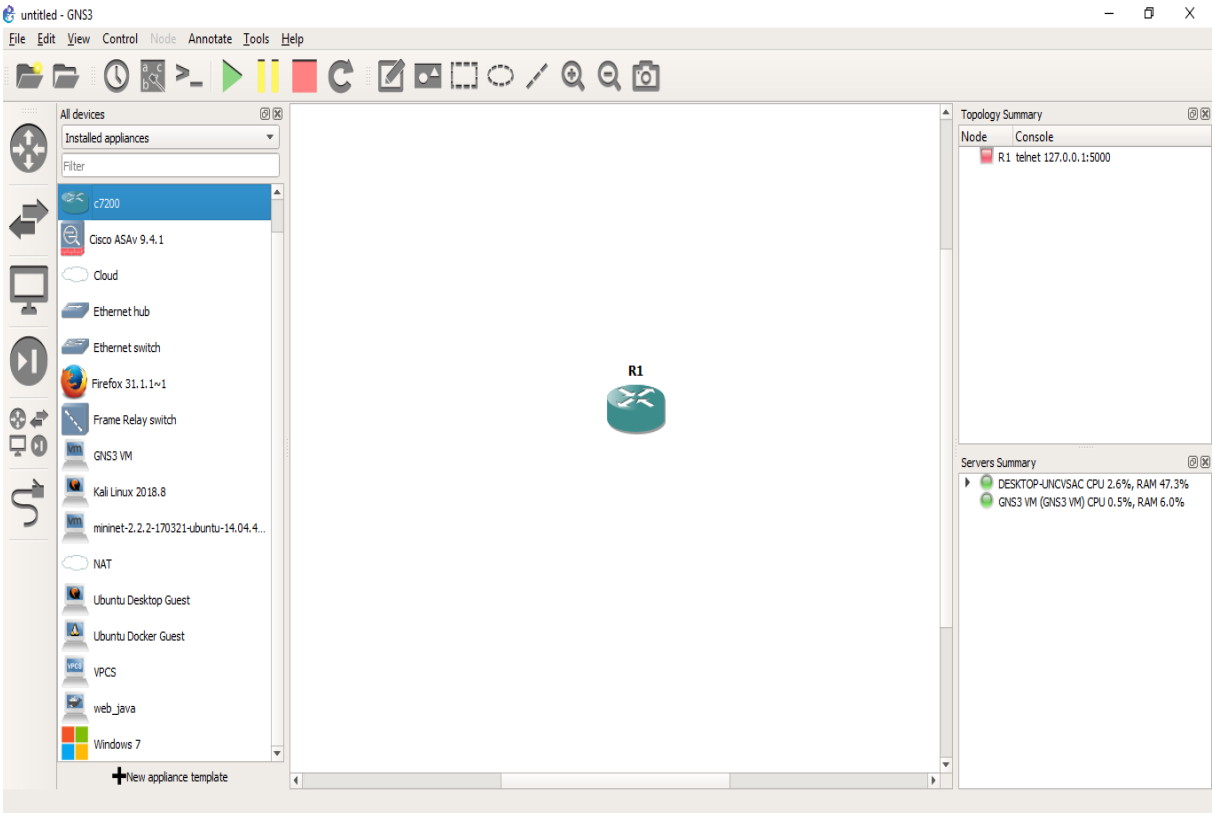

Figure 3.1 : Interface graphique de l'émulateur GNS3

3.3. Scénario étudié

En complément des solutions traditionnelles de sécurité, il est maintenant nécessaire pour les entreprises de se protéger contre les nouvelles générations de cyber attaque. 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.

La stratégie utilisée pour sécuriser le réseau sera d'abord de scanner le réseau existant pour trouver ses vulnérabilités et pour justifier le besoin de rajouter des éléments à l'architecture ou de changer la configuration de certaines entités.

La sécurité du réseau sera ainsi jaugée par un nombre tests de pénétration, exécutés par le biais du système d'exploitation Kali Linux qui comporte un très grand nombre d'outils permettant de scanner le réseau pour détecter ses failles et les exploiter pour savoir à quel point notre réseau est sécurisé.

3.3.1. Topologie existante

La structure de notre topologie est celle d'un réseau d'entreprise, elle est constituée de :

- Un routeur connecté au fournisseur de service (ISP), alimentant ainsi le réseau local d'une connexion internet.
- 2 switchs Ethernet d'accès sur les quelles sont connectés les différents hôtes.
- 2 serveurs (FTP et HTTP)
- Des clients de différents OS.

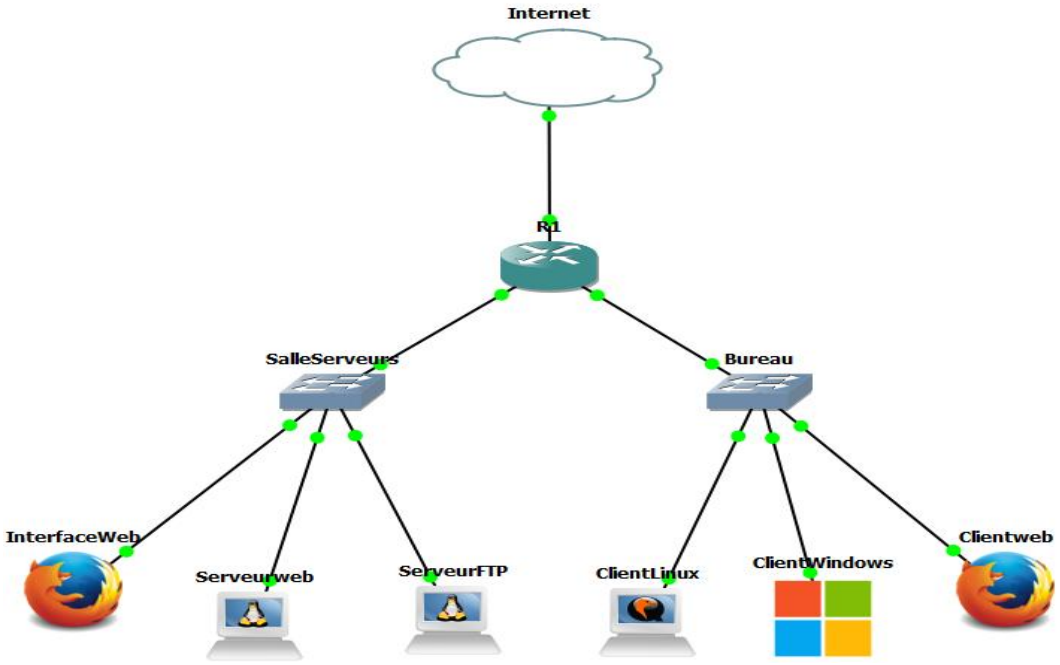

Figure 3.2 : Architecture du réseau existant

3.3.2. Présentation du matériel

a) Les Routeurs Cisco

Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, au mieux, selon un ensemble de règles. [32]

La fonction principale d'un routeur Cisco consiste diriger des paquets destinés à des réseaux locaux et distant en :

- ✓ Déterminant le meilleur chemin pour l'envoie des paquets.
- ✓ Transférant les paquets vers leurs destinations.

Figure 3.3 : Routeur Cisco

b) Les Switches Cisco

Les commutateurs Cisco Catalyst, nouvelle famille de périphérique autonomies à configuration fixe, apportent aux postes de travail une connectivité Fast Ethernet et Gigabit Ethernet optimisent les services de LAN sur les réseaux d'entreprise. [32]

➢ **Caractéristiques :**

- Fonctionnalités intelligentes à la périphérie du réseau.
- Un commutateur est également l'un des éléments fondamentaux utilisés lors de la création d'un petit réseau.
- Un commutateur peut être connecté sans être configuré

Figure 3.4 : Switch cisco

3.3.3. Failles de sécurité du réseau existant

Les différents types d'attaques menés sur le réseau nous ont permis de découvrir certaines vulnérabilités que ce soit dans la configuration ou dans l'architecture du réseau. Dans ce qui suit nous allons décrire les failles les plus sensibles de la structure.

a) Failles dans l'architecture

- **Serveur WEB**

Celui-ci pouvant être accessible de l'extérieur du réseau, son emplacement dans l'architecture peut représenter un danger considérable. En effet on peut le considérer comme porte d'entrée vers le réseau LAN et les données sensibles contenues dans les différentes bases de données. La figure suivante illustre le résultat d'un test Nmap qui montre que le port 80 est ouvert, ce qui représente une faille potentiellement exploitable par des personnes malintentionnées.

Port	Protocol	State	Name	Version
80	tcp	open	http	Apache httpd 2.4.18 ((Ubuntu))

Figure 3.5 : Scan Nmap sur le serveur Web

- **Point unique de défaillance**

L'architecture est composée d'un seul routeur dont dépend tout le réseau. Une simple panne de celui-ci engendrerait la coupure de communication entre les clients et les serveurs à l'échelle LAN, et la perte de connexion Internet sur tout le réseau.

- **Absence de système de défense**

L'inexistence d'un firewall, ou d'un proxy pour restreindre le trafic entrant et sortant du réseau peut causer l'infiltration d'un paquet malveillant, ou une attaque de type « reverse tunnel » qui permettrait de dévier les permissions d'accès au routeur.

b) Failles dans la configuration et la gestion du réseau

- **Mots de passe faibles**

Les interfaces de gestion des switchs et routeurs sont très mal protégés, les mots de passes utilisés sont des mots standards qui se trouvent dans toutes les listes de mots de passes que les hackers utilisent pour brute force un système. Une intrusion dans l'administration du réseau causerait des dommages à l'exploitation, et pourrait faire perdre beaucoup de ressources à l'entreprise.

- **Serveur FTP**

La faille du serveur réside dans ses lignes de transmission. Celles-ci ne sont pas cryptés, ce qui permet de les voir en clair rien qu'en écoutant avec un sniffer.

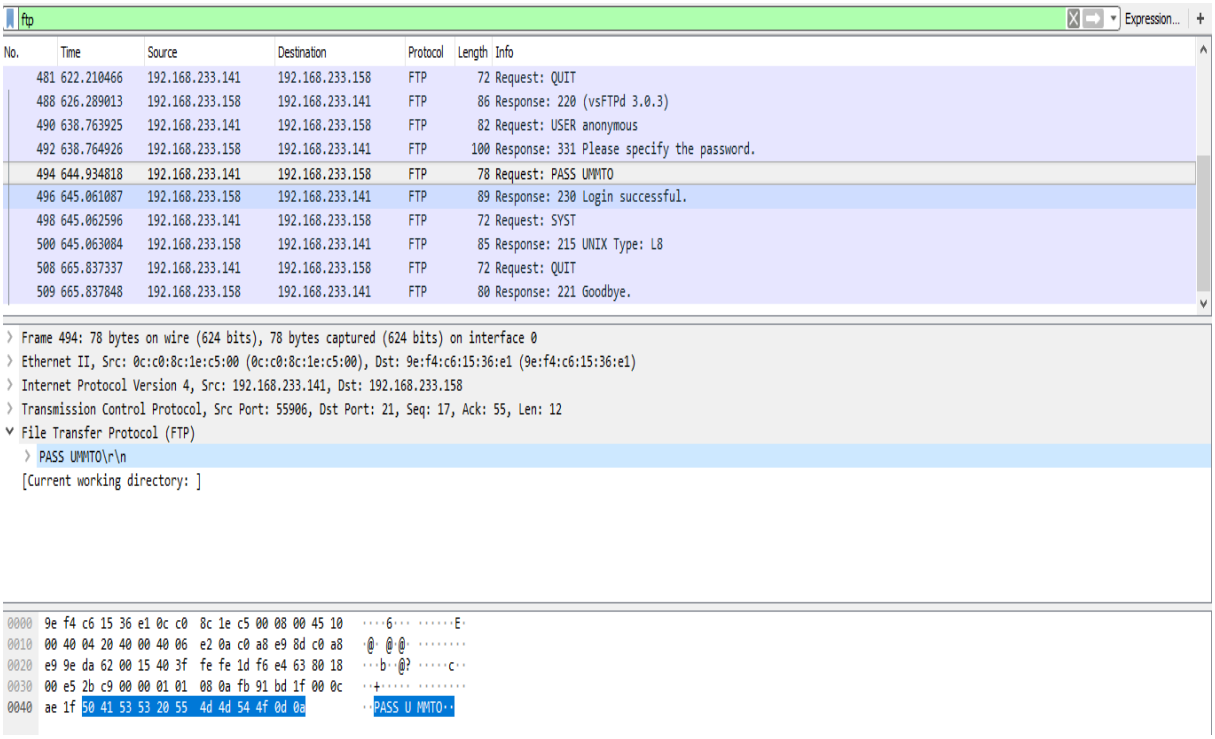

Figure 3.6 : Capture wireshark du mot de passe FTP

Cette faille pourrait s'avérer très compromettante si jamais les informations contenues dans le serveur étaient sensibles.

Une autre faille dans la configuration du FTP; l'option anonymous enable qui permet aux utilisateurs anonymes de se connecter au serveur. Celle-ci étant activée, il a suffit d'une seconde pour infiltrer le serveur.

```
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-09-07 13:23:05
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries, ~1 try per task
[DATA] attacking ftp://192.168.233.147:21/
[21][ftp] host: 192.168.233.147   login: anonymous   password: sp@rta.com
[STATUS] attack finished for 192.168.233.147 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-09-07 13:23:06
```

Figure 3.7 : Attaque brute sur le serveur FTP

- **Postes Clients :**

Le client Windows est sous une session Administrateur, ceci représente une vulnérabilité majeure, pour le poste et pour le réseau. Les droits administrateurs offrent aux malwares et autres logiciels malveillants la possibilité d'altérer les fichiers système de Windows, jusqu'à rendre l'OS inutilisable. Aussi, des permissions non contrôlées peuvent conférer un accès libre à des personnes mal intentionnées.

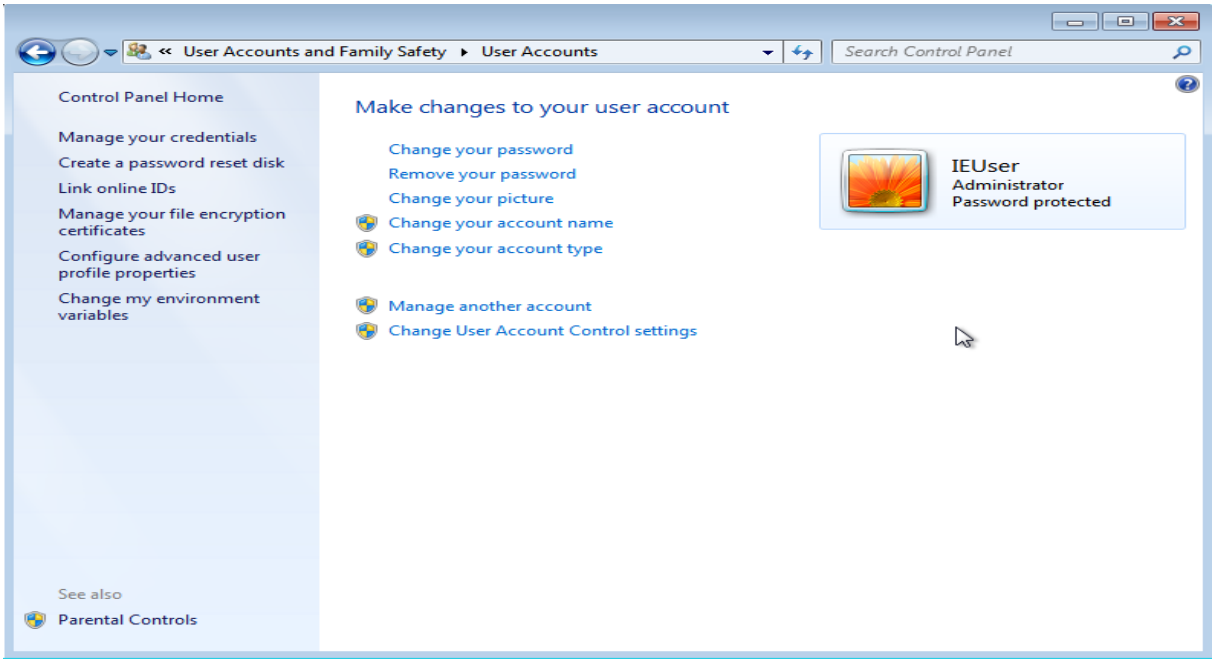

Figure 3.8 : Configuration comptes utilisateurs sous windows 7

- **Manque de restrictions dans le réseau LAN**

La communication entre les différents composants du réseau est libre et non restreinte. Ceci pourrait mener des employés ou autre, à accéder aux informations de services ou départements ne les concernant pas, causant ainsi de potentiels dommages internes.

3.4.Solutions proposées :

Pour pallier aux manques flagrants de notre réseau en termes de sécurité nous avons pensé à un certain nombre de solutions. L'objectif en est de réduire autant que possible les risques de fuite ou d'infiltration. Pour commencer l'architecture du réseau a été revue.

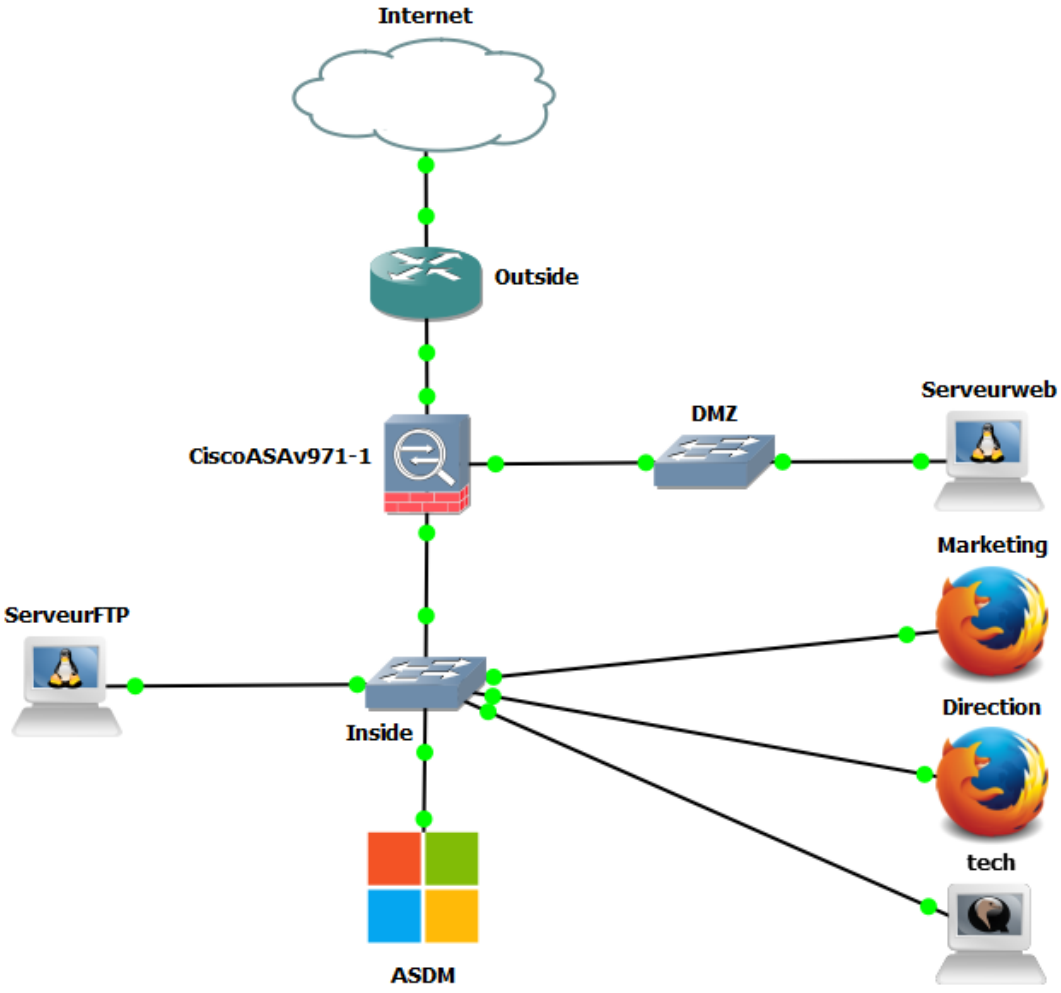

Figure 3.9 : Architecture proposée

3.4.1. Modification de l'architecture réseau

a) Ajout Pare-feu ASA

Le pare-feu permettra le filtrage des ports, et la restriction des communications pour plus de contrôle sur le trafic interne et externe.

Nous avons opté pour une version virtuelle de la gamme ASA, qui a été installée comme QEMU sur la machine virtuelle de l'émulateur. Celle-ci est plus compatible avec l'environnement de travail et offre une plateforme plus stable que l'image.

b) Ajout Interface ASDM

Cisco Adaptative Security Device Manager (ASDM), est une interface graphique qui permet de gérer le firewall ASA, il offre la possibilité de superviser l'activité du réseau par le biais du trafic qui traverse le pare-feu et d'avoir une meilleure visibilité sur les différentes configurations instaurées dans le firewall. Cet outil simplifie l'implémentation des stratégies de sécurité et la gestion des ACL.

c) Création Zone démilitarisée (DMZ)

L'architecture du réseau a été totalement revue, en vue d'optimiser sa sécurité. Nous avons ajouté une DMZ qui fera office de tampon entre l'extérieur et le réseau LAN. Celle-ci consistera du réseau web qui doit être accessible de l'extérieur. Le trafic internet allant vers le réseau LAN devra d'abord passer par la zone démilitarisée.

3.4.2. Implémentation du réseau

a) Serveur VSFTPD

Les mots de passes de ce serveur étant envoyés en clair par défaut, la solution que nous proposerons pour améliorer la sécurité du serveur de fichiers sera de crypter la ligne de transmission en utilisant le protocole SSL/TLS.

Nous allons tout d'abord générer un certificat SSL en utilisant une clé RSA de 2048bits. La commande utilisée est la suivante.

```
root@Serveurftp:/etc/init.d# openssl req -x509 -nodes -days 365 -newkey rsa:2048
 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem
```

Figure 3.10 : Création d'un certificat SSL

Nous devons ensuite configurer le serveur FTP pour qu'il applique le certificat et la clé privé RSA, à ses lignes de transmission, et qu'il adopte le protocole SSL/TLS. La configuration pour laquelle nous avons opté est illustrée dans la figure ci-dessous, celle-ci est ajoutée dans le bas du fichier /etc/vsftpd.conf.

```
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
require_ssl_reuse=NO
ssl_ciphers=HIGH
```

Figure 3.11 : Configuration SSL du serveur FTP

La dernière ligne de configuration permet de renforcer les suites cryptographiques.

La commande require_ssl_reuse confère une protection contre l'attaque Man In The Middle mais nous avons choisi de ne pas l'adopter car elle n'est pas compatible avec certaines versions de clients FTP.

Nous tacherons aussi de décommenter la ligne chroot_local_users=YES, pour que les utilisateurs locaux ne puissent accéder qu'aux répertoires qui leur sont assignés.

La connexion à partir d'un client devra afficher le résultat suivant.

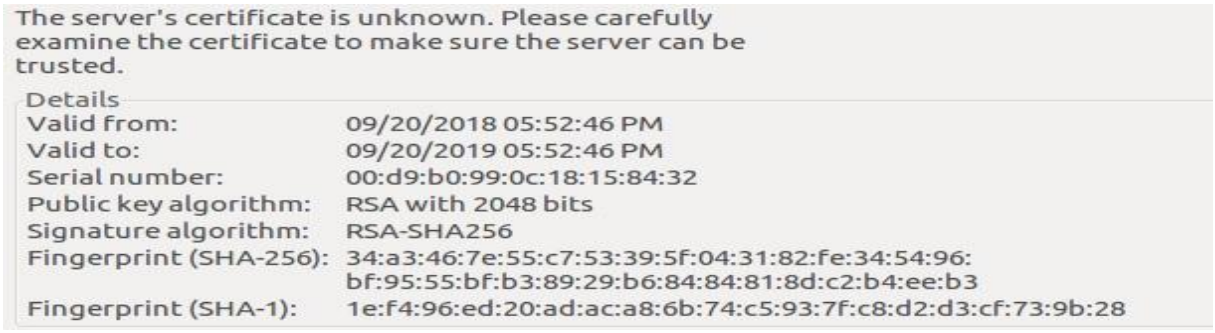

Figure 3.12 : Détails du Certificat et de la clé RSA

b) Configuration du firewall par ASDM

Cette alternative à la ligne de commande du firewall ASA, offre une interface graphique assez confortable pour configurer toutes les facettes du pare-feu.

Pour commencer, un assistant de configuration nous permettra de mettre en place les paramètres de base de filtrage de notre réseau.

La première étape qui s'affiche à nous est le nom de l'équipement, comme illustré dans la figure ci-dessous.

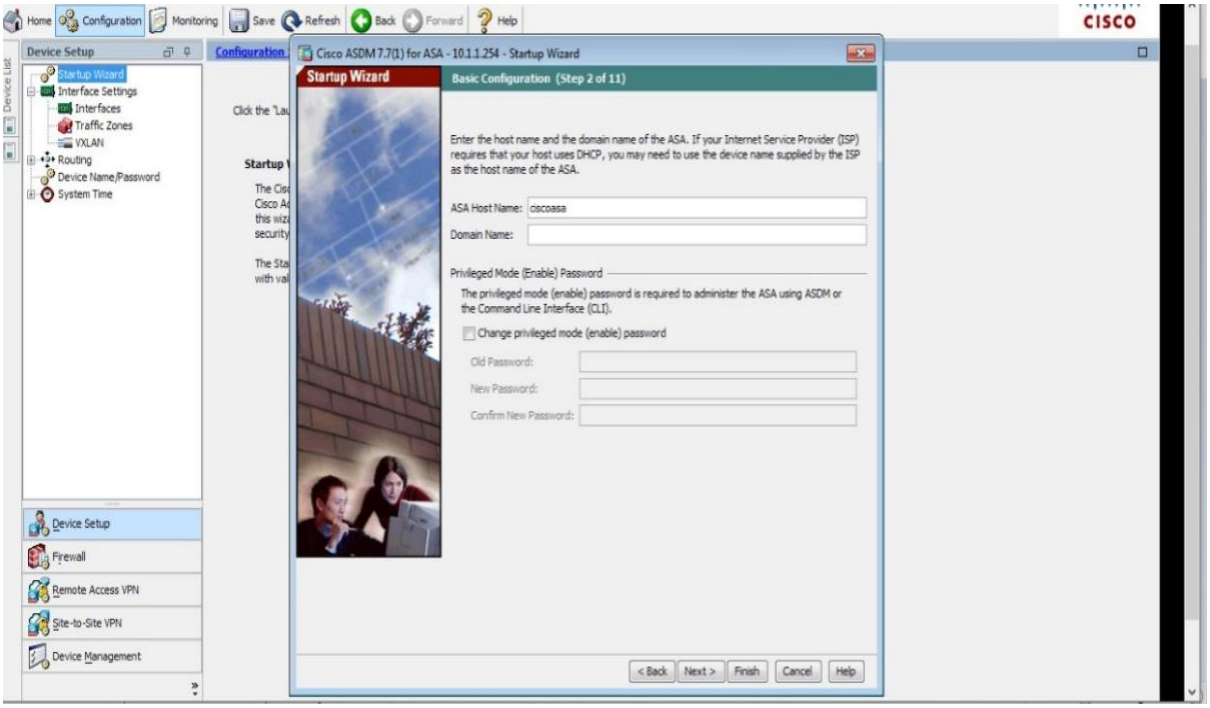

Figure 3.13 : Assistant de configuration ASDM

Ensuite, nous devons configurer l'interface Outside (extérieure) du réseau, l'identifier et lui allouer une adresse IP comme suit.

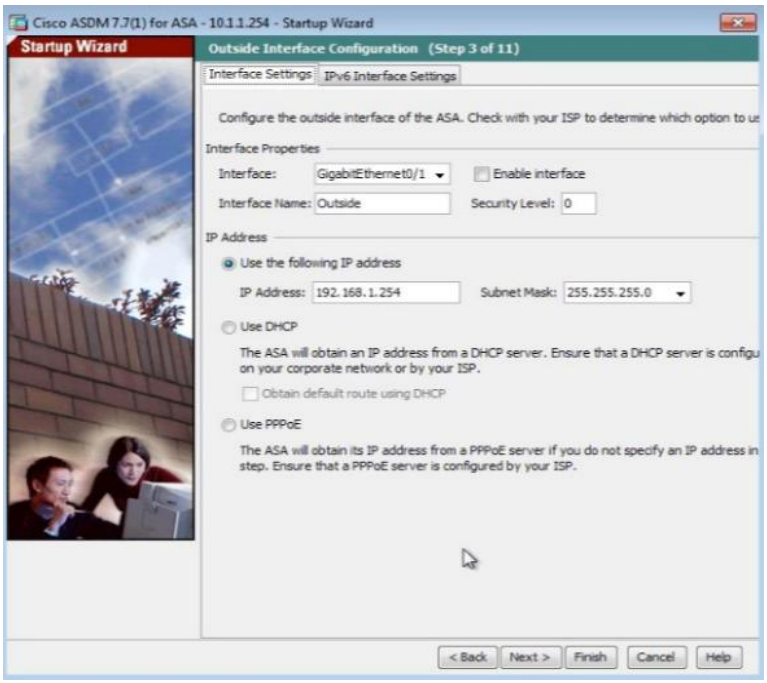

Figure 3.14 : Interface Outside du pare-feu

En ce qui concerne l'étape 4 qui consiste en la configuration des autres interfaces du pare-feu nous ferons celà manuellement, en dehors de l'assistant de configuration.

L'étape suivante sera de déclarer une passerelle par défaut pour l'interface extérieure, comme suit.

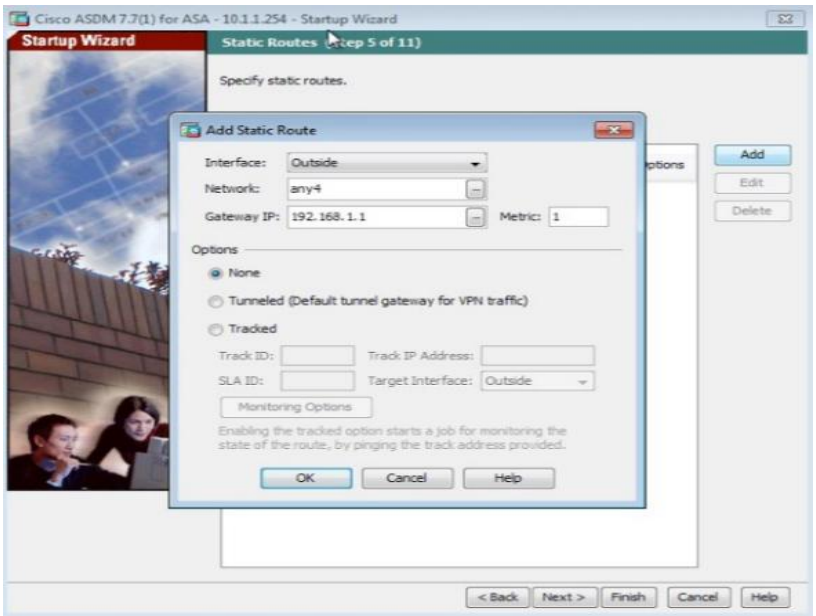

Figure 3.15 : Déclaration statique des routes

Et pour finir la procédure, nous allons activer le PAT (Port Address Translation), ce qui traduira l'adresse externe (publique) transportant les données internet, en plusieurs adresses privées et permettra aux appareils du réseau d'accéder à internet.

Figure 3.16 : Utilisation du PAT

Nous appuierons sur finish pour terminer l'assistant de configuration.

Nous devrons ensuite, ajouter un serveur DNS, pour la résolution des noms et la possibilité d'accéder au web. Il suffira d'aller dans Device Management > DNS >DNS client, comme illustré dans la figure ci-dessous.

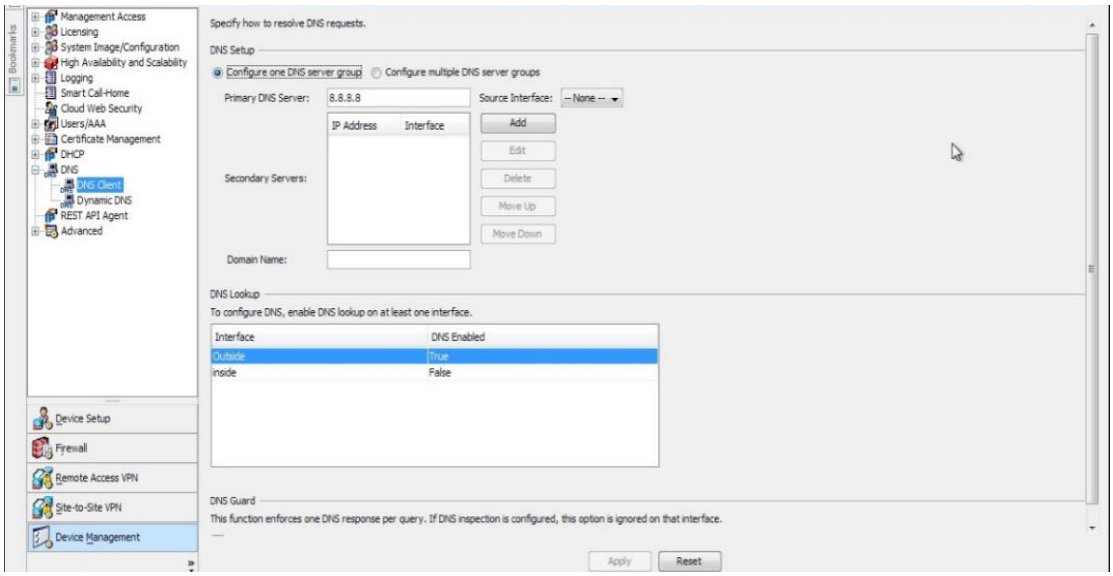

Figure 3.17 : Ajout d'un DNS

Notre appareil étant dorénavant fonctionnel, Nous ajouterons l'interface DMZ avec un niveau de sécurité 50 ce qui permettra au serveur web de communiquer avec l'extérieur mais pas avec l'interface INSIDE.

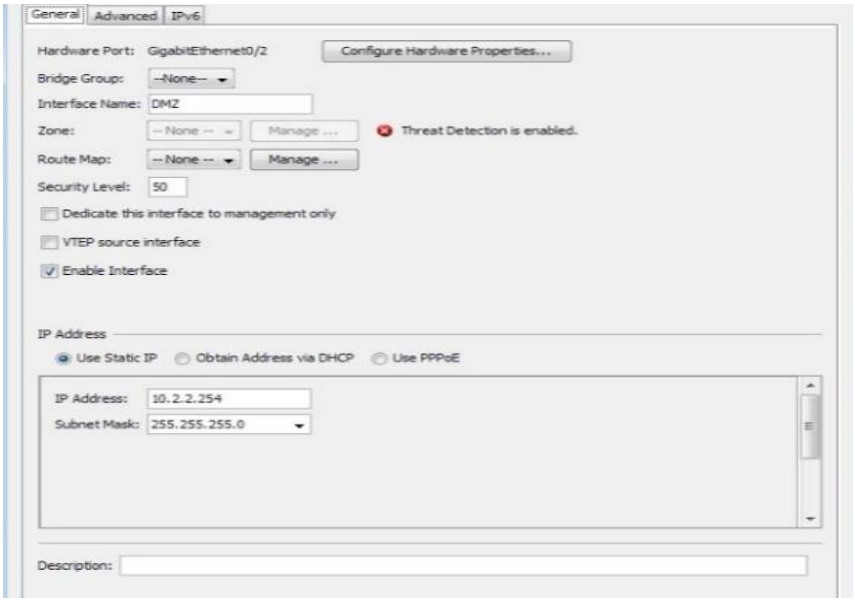

Figure 3.18 : Interface DMZ

Pour que la DMZ puisse communiquer avec le réseau LAN, nous devons utiliser les listes d'accès (ACL) et permettre à une adresse, à un protocole ou à un numéro de port de transmettre des données à l'interface INSIDE.

Ceci se fait de la même façon que l'exemple suivant qui empêche une adresse interne, en l'occurrence le serveur FTP d'accéder au réseau externe.

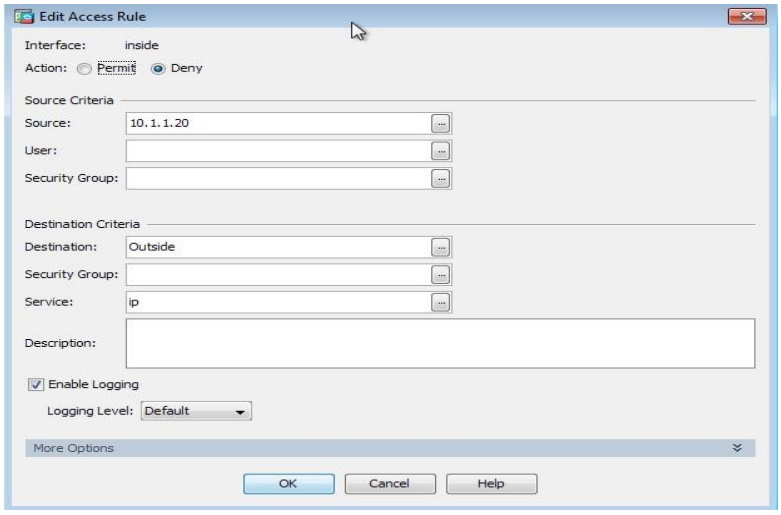

Figure 3.19 : Ajout ACL

Nous pouvons aussi filtrer les pages web utilisant des protocoles obsolètes, provoquant des failles de sécurité, comme le cas d'ActiveX.

Figure 3.20 : Activation filtre ActiveX

Après avoir configuré tout les aspects du firewall, nous pouvons aussi activer des options de supervision à partir de l'ASDM. Celui-ci offre la possibilité de détecter certains types d'activités pouvant se rapporter à une menace. Pour ce faire, il suffit d'aller dans la section firewall > Threat detection.

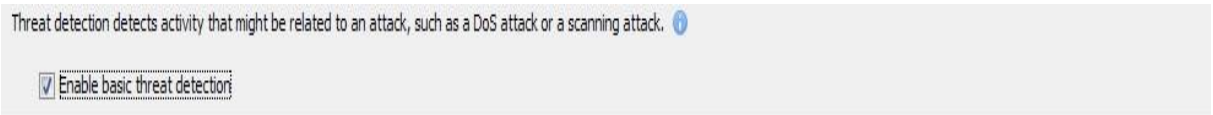

Figure 3.21 : Threat detection

Et pour avoir un œil sur ce qui se passe réellement dans le réseau, et la nature du trafic traversant ou pas le pare-feu, on peut générer des graphs de différentes variables et étudier le comportement de l'équipement en fonction des flux de données. La figure suivante est celle d'un graphe qui montre le nombre de paquets bloqués par le pare-feu en temps réel.

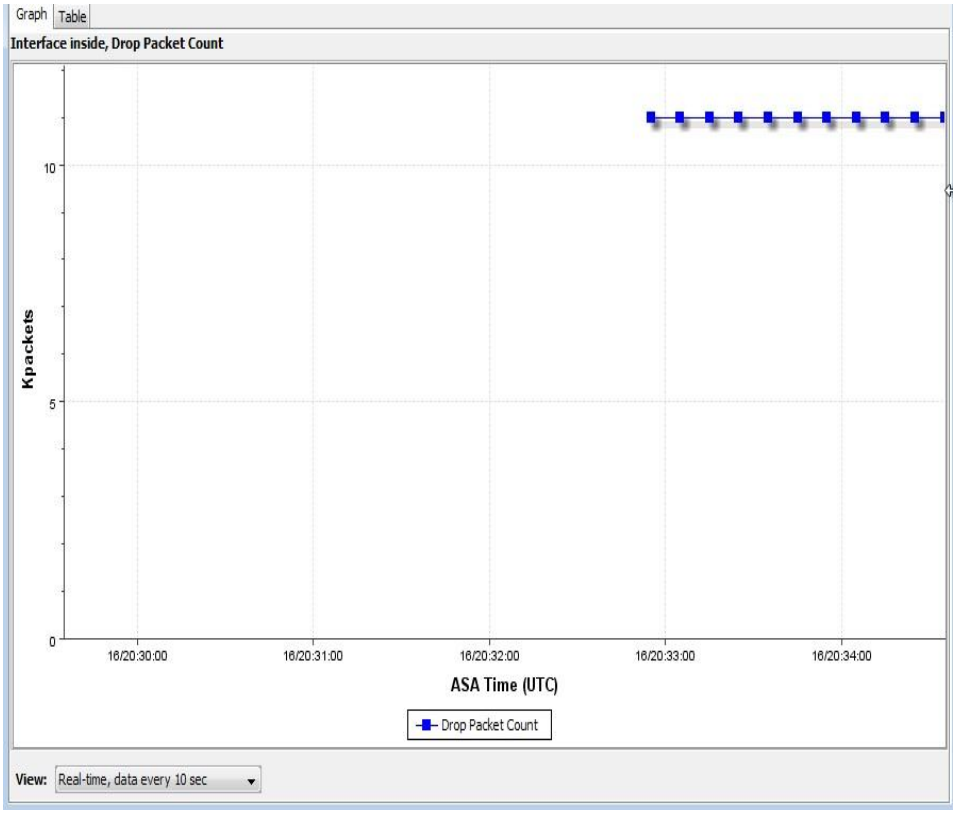

Figure 3.22 : Monitoring du firewall

3.5.Résultats

3.5.1. Tests d'accessibilité

a) Clients Firefox

Les postes clients Marketing et direction, sont des postes web que nous avons générés sur une machine virtuelle Mozilla Firefox dont le système d'exploitation est un linux tinycore.

Ceux-ci sont sensés se connecter à internet et au serveur http pour pouvoir faire fonctionner leurs applications.

Après configuration du réseau, la figure suivante montre le résultat du test de connectivité de ces clients.

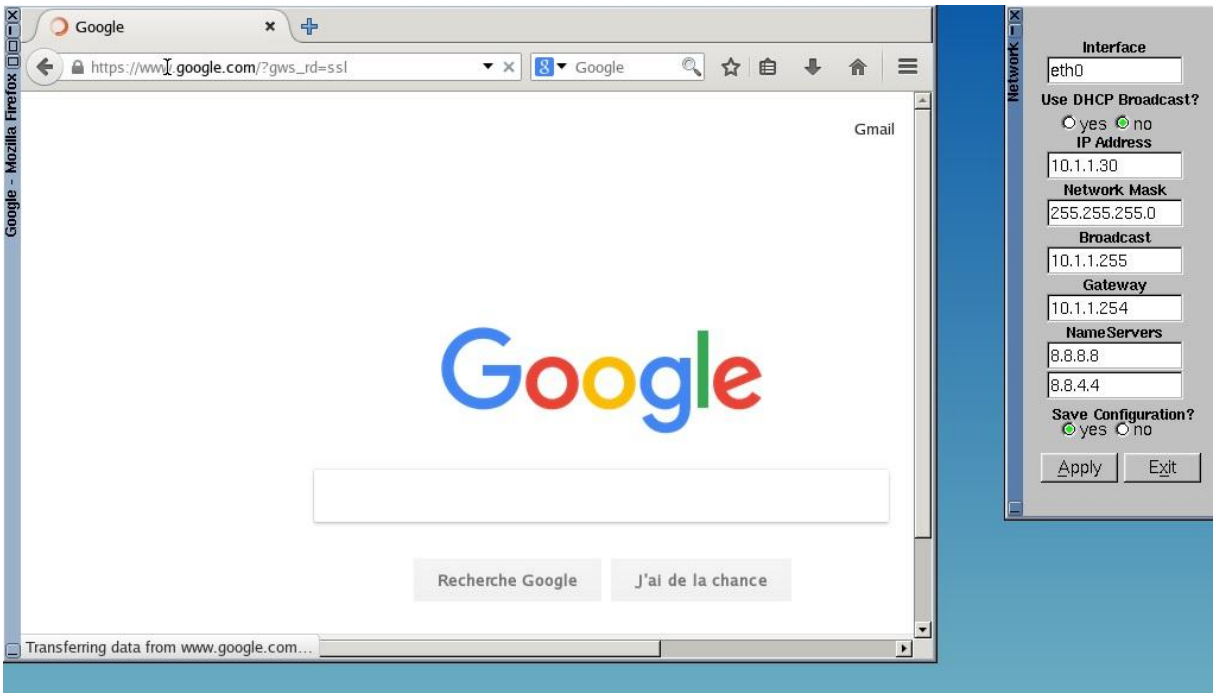

Figure 3.23 : Test de connectivité machine Firefox

Ce résultat confirme la stratégie planifiée, selon laquelle les machines Marketing et Direction ont accès à internet.

b) Serveur FTP

Le serveur FTP donne l'accès à la base de données de l'entreprise et de ce fait aux informations sensibles. C'est pour des raisons de confidentialités et de préservation de la sécurité ; la connectivité externe de cette machine a été bloquée.

Figure 3.24 : Test serveur FTP

Le test d'accessibilité confirme que notre serveur de fichiers est bel et bien isolé du réseau externe.

3.5.2. Tests de vulnérabilité

Dans cette section nous allons reproduire le même type d'attaques utilisés pour trouver les failles du réseau, et observer la différence dans le comportement de notre structure.

Les tests ont été faits pour toutes les parties de l'architecture, mais pour éviter les répétitions nous allons ici nous intéresser au serveur FTP, l'organe le plus sensible de la topologie.

Les attaques initiées sont de deux types : Scan de ports derrière le pare-feu avec NMAP et une attaque interne avec Wireshark ou nous allons Analyser le trafic allant et venant du serveur FTP.

a) Scan de ports

Pour commencer nous avons lancé une attaque NMAP basique sur l'adresse IP du serveur en question. Avant l'application de notre solution, nous avons trouvé le port FTP (21) ouvert ce qui constituait une possible porte d'entrée, si exploitée correctement par le hacker.

La figure ci-dessous montre le résultat de l'attaque après configuration du firewall.

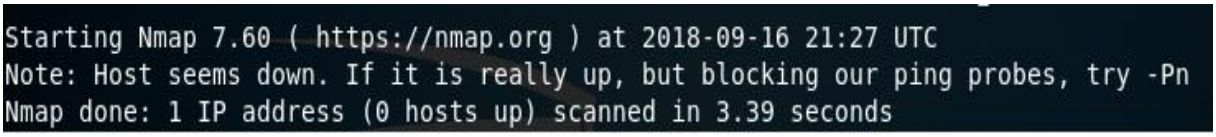

Figure 3.25 : Scan Nmap basique

Le résultat du scan affiche la machine cible (serveur FTP) comme étant éteint. Ceci peut être expliqué par un blocage des paquets de la part du pare-feu.

Pour correctement jauger le niveau de sécurité du réseau, nous avons lancé un scan plus avancé, sensé contourner le pare-feu et débloquer le passage des paquets envoyés par l'attaque. Pour des raisons d'éthique nous n'allons pas nous étaler sur le sujet.

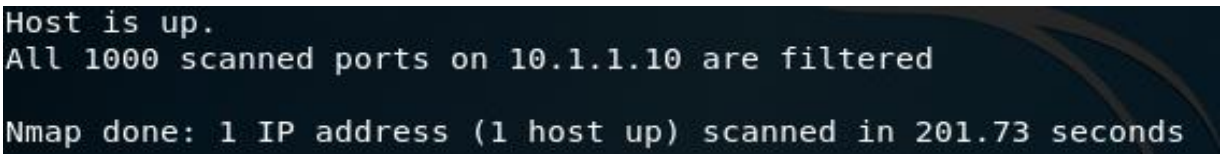

Figure 3.26: Scan NMAP Avancé

Après un scan de près de 4 minutes, comme affiché par la figure ci-dessus, l'attaque a réussi à atteindre la cible et la détecter, mais tout les ports de notre serveur sont filtrés par le pare-feu, ce qui démontre la validité de notre solution.

b) Analyse wireshark

Lors du test de l'architecture initiale, le mot de passe de connexion au serveur FTP s'est affiché en clair sur la capture wireshark. Nous allons maintenant reproduire le même scénario et comparer les résultats. La capture finale est affichée dans la figure ci-dessous.

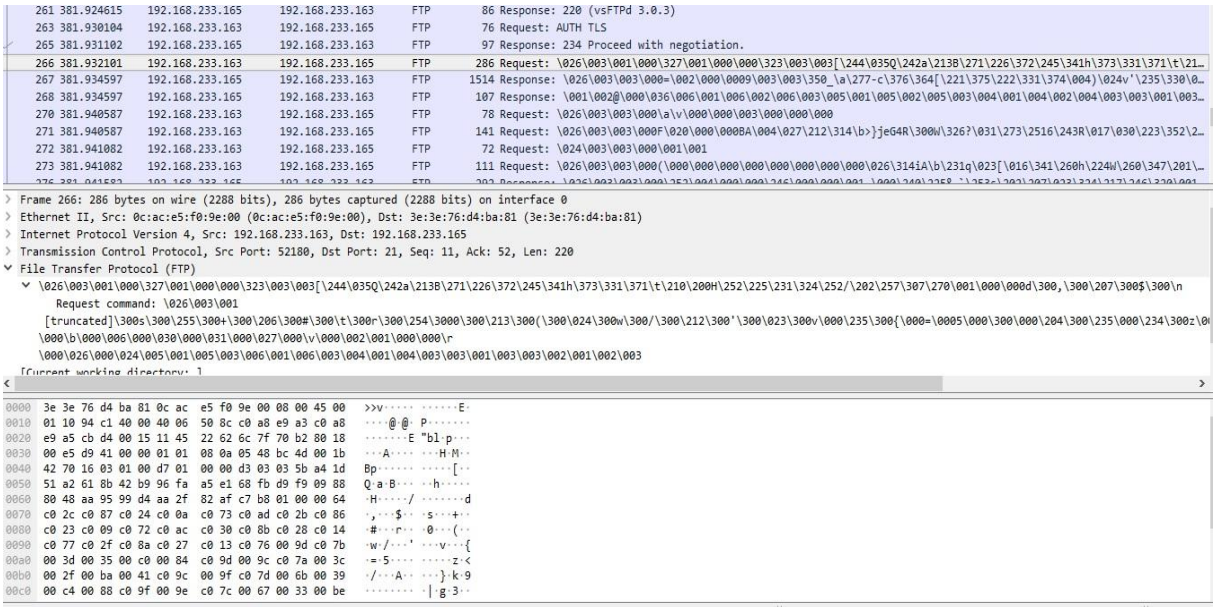

Figure 3.27 : Capture Wireshark de la ligne FTP cryptée

Comme nous pouvons le constater, le chiffrement RSA a été appliqué à toutes les transactions de données entrant et sortant du serveur FTP, le hacker pourra difficilement prélevé une information utile de cette capture, et la clé RSA de 2048 bits n'étant pas cassable par force brute, la sécurité des fichiers locaux en est grandement augmentée.

3.6.Discussion :

L'objectif de ce chapitre était d'améliorer la sécurité d'un réseau d'entreprise.

Pour ce faire, nous avons étudié ses failles et jaugé sa vulnérabilité. Pour palier à ses manques sécuritaires, nous avons modifié l'architecture du réseau en ajoutant un pare-feu asa configuré et supervisé par l'interface ASDM et en isolant le serveur web du LAN créant ainsi une DMZ. Nous avons ensuite instauré un chiffrement RSA grâce au protocole SSL/TLS, pour crypter les données transitant dans le réseau.

Des tests pour valider notre procédure ont ensuite été effectués, et les résultats étaient satisfaisants.

Conclusion

L'objectif de ce travail était d'améliorer la sécurité d'un réseau d'entreprise, de sorte à éviter les cas d'attaques ou d'infiltration les plus évidents, et avoir un meilleur contrôle sur le comportement du réseau en terme de restrictions et de permissions.

Une étude bibliographique a d'abord été effectuée, dans le but d'avoir une meilleure compréhension des différentes attaques et les meilleures façons d'y faire face. Ayant choisis le pare-feu comme dispositif de défense, nous nous sommes étalées sur ses différentes fonctions et les façons dont il peut être déployé.

Pour implémenter notre stratégie de sécurité, l'idée était d'abord de se mettre à la place du hacker. Nous avons simulé un nombre d'attaques, à partir d'une machine virtuelle du système d'exploitation Kali Linux sous GNS3, dans le cadre du Ethical Hacking. Les tests d'intrusion ont dévoilé plusieurs failles que ce soit dans l'architecture ou dans la configuration des différents éléments. Les données récupérées durant cette procédure, nous ont ensuite servis de base pour planifier la défense de notre réseau.

Dans le souci de combler les failles critiques de la topologie, nous avons implémenté un pare-feu ASA combiné à son interface de gestion ASDM, aussi nous avons modifié l'architecture de sorte à créer une zone démilitarisée qui constituera le seul point accessible à partir de l'extérieur. Du point de vue configuration, un chiffrement RSA sur base du protocole SSL/TLS a été adopté pour les lignes de transmission.

Après déploiement de la solution proposée, les mêmes tests d'intrusion appliqués précédemment, et d'autres plus poussés, ont été reproduits dans le réseau. Les résultats ont démontrés que la nouvelle architecture offrait une protection assez consistante, réussissant à repousser les différentes attaques, internes ou externes.

Cette solution n'est toutefois pas infaillible, et ne résous pas tous les soucis de sécurité. La détection de menaces restantes limitées, et les restrictions web de l'intérieur vers l'extérieur quasiment inexistants. Une recherche plus approfondies des vulnérabilités du réseau pourrait dévoiler d'autres failles non résolues.

Pour aller plus loin dans la sécurité réseau, nous envisageons d'étudier les NGFW ou Pare-feu de nouvelle génération, comme le pack Firepower de Cisco qui combine les propriétés d'un firewall traditionnel, un IPS de nouvelle génération et une protection malware.

Bibliographie

[1]: Elie MABO, La sécurité des systèmes informatiques (Théorie), support de cours, 2010.

[2]: La sécurité des réseaux, support de cours, Mercredi, 8. novembre 2006.

[3]: Dominique SERET, Ahmed MEHAOUA et Neilze DORTA, « RESEUX ET TELECOMMUNICATIONS », support de cours, Université René Descartes – Paris, 2006.

[4]: Laurence Monaco, « Quelques définitions », 2010.

[5]: Laurent Bloch et Christophe Wolfhugel, « Sécurité Informatique-principes et méthodes », livre vol.276, P.57, 2007.

[6]: Laurent Poinsot «Introduction à la sécurité informatique», support de cours, Université Paris 13.

[7]: Vincent Erceau & Romain Colombier, « GMSI Informatique », Projet SAS, 2011.

[8]: PILLOU jean-François BAY jean philippe. Tous sur la sécurité informatique. dunod, 2005.

[9]: Rabehi Sidi Mohamed El Amine, « Mise en place d'un serveur radius sous linux pour la sécurisation d'un réseau 802.11 », Projet de fin d'étude, Université Abou Bakr Belkaid, Tlemcen-Algérie, 2011.

[10]: LORENS Cedric LEVIER laurent. Tableaux de bord de la sécurité réseau. Edition eyrolles, 2003.

[11]: Elies Jebri, « Introduction à la sécurité», support de cours, 2008 disponible sur url : https://www.google.fr/search?newwindow=1&q=ddata.overblog.com%2F...%2F0%2F...%2FIntroduction_a_la_securite_2008_elies.pdf , consulté le : Mai 2013.

[12]: Nicolas Baudoin et Marion Karle, « NT Réseaux –IDS et IPS », 2000, support de cours, Enseignant Etienne Duris en 2003-2004.

[13]: DESWARTE Ludovic ME Yves. Sécurité des réseaux et système repartis. Lavoisier, février 2002.

[14]: EVENGELISTA Thierry. Les IDS (intrusion detection system). dunod, 2004.

[15]: DNS, types d'attaques et techniques de sécurisation,p4. AFNIC, 2009.

[16]: CHAIKHI DOUAS Youssef. Les types d'attaques informatiques, module veille et technologie. 2010.

[17]: DENIS Valois BENJAMIN Morin CEDRIC Liorens, LAURENT Levier. Tableaux de bord de la sécurité réseau. 3eme édition, Edition eyrolles, 2010.

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

[19] :https://wapiti.telecom.lille.fr/commun/ens/peda/options/st/rio/pub/exposes/exposesrio2000/ Blick 20Lammari/site/firewall/fontionnement.html.52

[20] : A.JAQUEMIN, A.MERCIER, Les firewalls.

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

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

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

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

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

[26] : www.gns3.net

[27] : www.gns3.net.qemu

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

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

[30] : 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.

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

[32] : VINCENT REMASEILLES, (La sécurité des réseaux avec Cisco), 2008, ENI Edition.