الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'enseignement Supérieur et de la Recherche scientifique

Université Mohamed Khider Biskra
Faculté des Sciences et de la Technologie
Département de Génie Electrique
Filière : Télécommunication
Option : Réseaux Télécom

Réf:.....

Mémoire de Fin d'Etudes
En vue de l'obtention du diplôme:

MASTER

Thème

La sécurité des réseaux informatiques

Présenté par :
Derbali Ali
Soutenu le : 25 Juin 2018

Devant le jury composé de :

Mr. Ayad Soheyb	**MCB**	**Président**
Mr. Guesbaya Tahar	**MCB**	**Encadreur**
Mr. Terressa Saddek Labib	**MCA**	**Examinateur**

Année universitaire : 2017 / 2018

الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'enseignement Supérieur et de la recherche scientifique

Université Mohamed Khider Biskra
Faculté des Sciences et de la Technologie
Département de Génie Electrique
Filière : Electronique
Option : Réseaux et Télécom

Mémoire de Fin d'Etudes
En vue de l'obtention du diplôme:

MASTER

Thème

La sécurité des réseaux informatiques

Présenté par :

Derbali Ali

Avis favorable de l'encadreur :

Nom Prénom ***signature***

Avis favorable du Président du Jury

Nom Prénom ***Signature***

Cachet et signature

الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'enseignement Supérieur et de la Recherche scientifique

Université Mohamed Khider Biskra
Faculté des Sciences et de la Technologie
Département de Génie Electrique
Filière : Electronique
Option : Réseaux et Télécom

Thème :

La sécurité des réseaux informatiques

Proposé par : Derbali Ali
Dirigé par : Guesbaya Tahar

RESUMES

La sécurité des réseaux informatique est un domaine large est très importants il conserve aux données ses caractères de confidentialité de contrôler leurs accès et d'identifier les utilisateurs. Ce projet de fin d'étude master présente les outils des réseaux informatiques et une politique de sécurité des réseaux avec leurs configurations.
En pratique ce projet propose de mettre en place une politique de sécurité sur les réseaux confiants tout en réalisant une simulation d'une sécurité par le firewall.

ملخص
يعتبر أمان شبكات الكمبيوتر مجا الً واس اعا من الأهمية بمكان أن يحتفظ البيانات بأحرف السرية الخاصة بها للتحكم في الوصول إليها ولتحديد المستخدمين.
يعرض هذا المشروع أدوات شبكات الكمبيوتر وسياسة أمان الشبكة مع اعداد اجهزة الخاصة بامن الشبكة وتكويناتها.
من الناحية العملية ، يقترح هذا المشروع إعداد سياسة أمنية على الشبكات واثقة أثناء إجراء محاكاة للأمن بواسطة جدار الحماية

Dédicaces

Je vous dédie ce travail avec tous mes vœux de bonheur, santé et de réussite.

D’abord à mon cher père Ahmed Derbali ta détermination, ta force et ton honnêteté m’a permis d’avancer.

Ma Mére dans ta bonté, ta patience et ton dévouement j’ai trouvé la force et le courage d’aboutir enfin mes objectifs.

C’est à vous que je dois cette réussite. Et je suis fière de vous l’offrir.

Merci pour tous vos sacrifices

Je t’exprime à travers ce travail mes sentiments de fraternité et d’amour à tout mes proches et mes amis, vous avez toujours été présents pour les bons conseils.

Je vous souhaite une vie pleine de santé et de bonheur.

Remerciement

En préambule à ce mémoire nous remerciant ALLAH qui nous aide et nous donne la patience et le courage durant ces longues années d'études.

Je souhaite adresser mes remerciements les plus sincères aux personnes qui m'ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire ainsi qu'à la réussite de cette formidable année universitaire.

Ces remerciements vont tout d'abord à mon professeur guesbaya Tahar qui m'aidé à ce travaille et donnera le temps pour me suivre.

On n'oublie pas nos parents pour leur contribution, leur soutien et leur patience.

Enfin, j'adresse mes plus sincères remerciements à tous mes proche et mes amis, qui m'ont toujours encouragée au cours de la réalisation de ce mémoire.

Merci à tous et à toutes.

SOMMAIRE

Introduction générale

CHAPITRE 1

1.1 Introduction 1

1.2 Définition des réseaux informatiques 2

1.3 Les deux types des risques majeurs 2

1.3.1 Le risque hardware 2

1.3.2 Le risque software 2

1.4 Les moyens de protection 2

1.4.1 La protection du hardware 2

1.4.2 La protection du software 2

1.5 Qu'est-ce que la sécurité ? 3

1.6 L'importance de la sécurité 3

1.6.1 Pour gagner un avantage concurrentiel 3

1.6.2 Pour se conformer aux exigences réglementaires et aux responsabilités jiduciaire 3

1.6.3 Pour garder votre emploi 4

1.7 Les domaines de la sécurité 4

1.7.1 Sécurité physique 4

1.7.2 Sécurité de l'exploitation 4

1.7.3 La sécurité logique 5

1.7.4 La sécurité applicative 5

1.8 La sécurité Trinity 5

1.8.1 La prévention 5

1.8.2 Détection 6

1.8.3 Réponse 6

1.9 Sécurité de l'information....6
1.9.1 Confidentialité....6
1.9.2 Intégrité....7
1.9.3 Disponibilité....7
1.10 Autres concepts de sécurité....7
1.10.1 Intimité....7
1.10.2 Identification....7
1.10.3 Authentification....7
1.10.4 Autorisation....8
1.10.5 Audit....9
1.10.6 Responsabilité....9
1.10.7 Non-répudiation....9
1.11 Les causes pour sécuriser les réseaux....9
1.11.1 Enjeux économiques....9
1.11.2 Enjeux politiques....10
1.11.3 Enjeux juridiques....10
1.12 Modèles de sécurité....10
1.12.1 Sécurité par Obscurité....10
1.12.2 La défense du périmètre....10
1.12.3 La défense en profondeur....11
1.13 Les Terminologie de base des risques de réseaux:....11
1.13.1 Vulnérabilité....11
1.13.1.1 Vulnérabilités humaines....12
1.13.1.2 Vulnérabilités technologiques....12
1.13.1.3 Vulnérabilités organisationnelle....12
1.13.1.4 Vulnérabilités mise en œuvre....12
1.13.2 Menace 13

1.13.3 Catégories de menaces de sécurité. …..……..13
1.13.3.1 Menaces non structurées…….……....13
1.13.3.2 Menaces structurées.....13
1.13.3.3 Menaces externes.....14
1.13.3.4 Menaces internes 14
1.13.4 Les Risques 14
1.13.5 Les ennemis.....14
1.13.5.1 Pirates informatiques (hackers) 14
1.13.5.2 Personnel non avisé 14
1.13.5.3 Employés mécontents 15
1.14 Conclusion ……..…15

CHAPITRE 2

2. Introduction …….……17

2.2 Attaques permettant de dévoiler le réseau 18
2.2.1 Attaque par cartographie du réseau.....18
2.2.2 Attaques par Identification des Systèmes Réseau 19
2.2.2.1 Attaque par Balayage ICMP 19
2.2.2.2 Attaque par balayage TCP.....20
2.2.3 Attaque par sniffing (Renifleurs) 20
2.2.3.1 Types de Sniffing 20
2.2.4 Attaque ARP spoofing 21
2.2.5 Attaque IP spoofing.....22
2.2.6 Attaque man-in-the-middle 22
2.3 DOS ATTAQUE.....23
2.3.1 DoS cibles 23
2.3.2 Types d'attaques (DOS).....24
2.4 Comprendre le DDoS.....26

2.5 Spamming attaque 26
2.6 TROJAN 27
2.6.1 Fonctionnement 27
2.7 Virus et vers 27
2.8 Ingénierie sociale 28
2.8.1 Types d'ingénierie sociale 29
2.8.1.1 Ingénierie sociale basée sur l'humain 29
2.8.1.2 Ingénierie sociale informatisée 29
2.9 La politique de sécurité 30
2.9.1 Règles de sécurité génériques 30
2.9.2 La sécurité de réseaux 31
2.9.2.1 Les antivirus 31
2.9.2.1.1 Composants d'un antivirus 31
2.9.2.2 Accès sécurisé 32
2.9.2.3 VPN 32
2.9.2.3.1 Type de VPN 33
2.9.2.3.2 Les deux grandes catégories de VPN 33
2.9.2.4 Cryptographie 34
2.9.2.4.1 Chiffrements 34
2.9.2.4.2 Chiffrement Bloc et flux 34
2.9.2.4.3 Chiffrement symétrique et asymétrique 35
2.9.2.4.4 Hachage 36
2.9.2.4.5 Signatures numériques 36
2.9.2.4.6 Protocoles de cryptage de nouvelle génération 37
2.9.2.5 VLAN 38
2.9.2.6 Firewall 38
2.9.2.7 Zone Based Firewalls 39

2.9.2.8 IPS/IDS.....39
2.10 Conclusion.....40
CHAPITRE 3
3.1 Introduction……..……..41
3.2 Conception ……...……..…..…...42
3.2.1 Les éléments utilisés pour l'étude se traduit comme suit……42
3.2.2 Le réseau se comporte de 3 zones 42
3.2.3 Les composants de réseaux……..43
3.3 Définition de Firewall…….……43
3.4 Objectifs d'un bon pare-feu……44
3.5 LES AVANTAGES DE PARE-FEU……..44
3.5.1 Exposition de systèmes sensibles à des individus non-fiables 44
3.5.2 Exploitation des failles de protocole 44
3.5.3 Utilisateurs non autorisés.....45
3.5.4 Données malveillantes.....45
3.6 Limitations potentielles du pare-feu…….……45
3.6.1 Les erreurs de configuration ont des conséquences graves 45
3.6.2 Latence ajoutée par le pare-feu.....45
3.7 Caractéristiques de pare-feu.……46
3.7.1 Filtrage de paquets statique (stateless) 46
3.7.2 Filtrage par paquets avec état (stateful).....47
3.7.3 Inspection d'application.....48
3.7.4 Pare-feu transparents 48
3.7.5 Firewalls de nouvelle génération.....48
3.8 Network Address Translation…….....48
3.8.1 Les différents concepts de NAT……49
3.8.2 Terminologie du NAT……49

3.9 Contrôle d'accès……..…49
3.10 Etude d'un cas…….…….……..50
3.10.1 Outils utilisés……..50
3.10.2 Cisco ASA firewall…….……...51
3.10.2.1 Cisco ASA Caractéristiques…….....51
3.10.2.2 Modèle Cisco ASA……..……..……...52
3.10.2.3 Modes de base pour configurer Cisco ASA……..……56
3.10.3 Le routeur 58
3.10.4 Switch (commutateur) 58
3.10.5 GNS3.....59
3.10.6 Vmware 59
3.10.7 Securecrt.....60
3.10.8 Wireshark 61
3.11 Implémentation..……62
3.11.1 Introduction 62
3.11.2 Le processus se fait en plusieurs étapes 62
3.11.2.1 ETAPE 01...…….……..……..……62
3.11.2.2 ETAPE 02……...……..……..…….62
3.11.2.2.1 Réalisation schéma lab……..62
3.11.2.3 Etape 03…….……..63
3.11.2.3.1 Configuration des interfaces.....63
3.11.2.3.2 Configuration des interfaces g0/0, g0/1, g0/2 avec leurs adresses et le niveau de sécurité et nom de chaque l'interface.....63
3.11.2.3.3 Configuration les interfaces g2/0, F0/0, F1/1avec leur adresses et le mask. 64
3.11.2.3.4 Tester la connectivité des interfaces de routeur 01 par le Ping avec (internet, firewall, pc)……..……..……64
3.11.2.3.5 Testez la connectivité de pc kali linux vers l'internet 65
3.11.2.3.6 Configure les interfaces G2/0, F0/0 de routeur 02 dans la zone DMZ.....65

3.11.2.3.7 Test la connectivité des interfaces de routeur 02 66
3.11.2.3.8 Configure les interfaces g2/0, f0/0, f1/1 de routeur 03 dans la zone Inside . 66
3.11.2.3.9 Tester la connectivité par Ping 67
3.11.2.3.10 Configure le Protocol de routage ospf dans tous les routeurs et le firewall . 68
3.11.2.3.11 Tester la connexion entre le firewall avec tous les éléments de réseaux 68
3.11.2.3.12 Niveau de sécurité (Security Levels) 69
3.11.2.3.12.1 Tester la connectivité entre les déférant réseaux 69
3.11.2.3.13 Sécurisation de consol, aux, vty et mode enable pour les routeurs 70
3.11.2.3.14 Pour accéder aux autres réseaux en configurons le Access liste 70
3.11.2.3.15 Configure le Nat et DHCP pour connecter à l'internet 71
3.11.2.3.16 Configuration pour permise quelque trafic ou bloquer 71
3.11.2.3.17 Autre exemple bloqué l'accès à distant ssh et Telnet 73
3.11.2.3.18 Installer le mode ASDM (graphical interface) 74
3.11.2.3.19 La face graphique de ASDM 75
3.11.2.3.20 Capture par wireshark qui identifier le traffic qui roule entre le PC et serveur d'université de Biskra et serveur DNS de Google 75
Conclusion générale

Liste des figures

Figure 1.1 : si quoi la sécurité 3
Figure 1:2 : Authentification..... 8
Figure 1.3 : autorisation de donnée..... 8
Figure 1.4 : l'Audit..... 9
Figure 1.5 : Sécurité par périmètre..... 11
Figure 1.6 : Sécurité en profondeur 11
Figure 1.7 : la vulnérabilité 12
Figure 1.8 : Les menaces..... 13
Figure 1.9 : le hacker..... 14
Figure 1.10 : Employés mécontents..... 15
Figure 2.1 : Fonctionnement d'outil trace route. 18
Figure 2.2 : les différents types de balayage..... 18
Figure 2.3 : fonctionnement de la command Ping. 19
Figure 2.4 : Le balayage TCP. 19
Figure 2.5 : Écoute sur un réseau local. 20
Figure 2.6 : L'attaque ARP spoofing. 21
Figure 2.7 L'attaque IP spoofing..... 21
Figure 2.8 : Machine du pirate en tant que relais transparent..... 22
Figure 2.9 : Machine du pirate en tant que relais applicatif. 22
Figure 2.10 : Ping de la mort..... 24
Figure 2.11 : smurf attaque. 25
Figure 2.12 : DDOS attaque..... 25
Figure 2.13 : spamming attaque..... 26
Figure 2.14 : Trojan..... 27
Figure 2.15 : virus 27
Figure 2.16 : le ver 28
Figure 2.17 : ingénierie social..... 28
Figure 2 .18 : Création d'un groupe de périphériques réseau..... 32

Figure 2.19 : Exemple de VPN à accès distant et de site à site. 33
Figure 2.20 : cryptage symétrique..... 35
Figure 2.21 : cryptage asymétrique..... 35
Figure 2.22 : crypto avec IP sec..... 36
Figure 2.23 : le Protocol SSL..... 37
Figure 2.24 : les vlans. 37
Figure 2.25 : Le Firewall..... 38
Figure 2.26 : IPS/IDS..... 38
Figure 3.1 : lab. de projet. 42
Figure 3.2 : Lab de projet..... 50
Figure 3.3 : Cisco ASA 5505. 52
Figure 3.4 : Cisco ASA 5510. 53
Figure 3.5 : Cisco ASA 5550. 54
Figure 3.6 : Cisco ASA 5580. 54
Figure 3.7 : Module Cisco ASA..... 55
Figure 3.8 : Cisco ASA 5585 X. 56
Figure 3.9 : fenêtre de ASDM..... 58
Figure 3.10 : Routeur Cisco. 58
Figure 3.11 : Switch Cisco. 59
Figure 3.12 : Logiciel GNS3. 59
Figure 3.13 : Logiciel VMware Workstation..... 60
Figure 3.14 : Le terminal Securecrt. 60
Figure 3.15 : logiciel Wireshark..... 61
Figure 3.16 : Réalisation de lab..... 62
Figure 3.17 : Configuration des interfaces de ASA. 63
Figure 3.18 : Configuration des interfaces de routeur. 64
Figure 3.19 : Testez la connectivité des interfaces de routeur. 64
Figure 3.20 : Test la connectivité d'hôte..... 65
Figure 3.21 : Configurer les interfaces de routeur 2. 65
Figure 3.22 : test la connectivité de routeur 2..... 66

Figure 3.23 : Configure les interfaces de routeur 3..... 66
Figure 3.24 : Test la connectivité de routeur 3. 67
Figure 3.25 : Configure le Protocol de routage dans ASA. 68
Figure 3.26 : Test la connectivité de firewall avec les réseaux. 68
Figure 3.27 : Tester la connectivité R1 et R2. 69
Figure 3.28 Sécurisé les ports de routeur. 70
Figure 3.29 : Configuration de ACL dans ASA. 70
Figure 3.30 : Configuration NAT et DHCP dans ASA. 71
Figure 3.31 : Teste le Ping avant la configuration. 71
Figure 3.32 : Configuration pour filtré le traffic (ICMP). 72
Figure 3.33 : Test le Ping après la configuration. 72
Figure 3.34 : Accès a distant par SSH. 73
Figure 3.35 : Filtré le traffic par le blocage de SSH. 73
Figure 3.36 : Test l'accès a distant par SSH après la configuration. 74
Figure 3.37 : Activer l'interface graphique ASDM. 74
Figure 3.38 : Asdm luncher..... 75
Figure 3.39 : Capture par wireshark..... 75

Abbreviation

DMZ: Demilitarized zone

NAT: Network address translation

ACL: access list control

IDS: Intrusion Detection system

VPN: Virtual private network.

IP : Internet protocol.

ASA: Appliance Security Adaptive

DHCP: Dynamic Host Configuration Protocol.

OSPF: Open Shortest Path First.

IPS: Intrusion Prevention System.

TTL: Time to Live.

ICMP: Internet Control Message Protocol.

TCP: Transmission Control Protocol.

LAN: Local Area Network.

ARP: Address Resolution Protocol.

MAC: Media Access Control.

DOS: Denial of Service.

DDOS: Distributed Denial of Service.

ISP: Internet Service Provider.

ACS: Access Control System

IP sec: Internet Protocol Security.

UDP: User Datagram Protocol.

NGFW: Next Generation firewall.

URL: Uniform Resource Locator.

VM: Virtual Machine.

SNAT: Static NAT.

DNAT: Dynamic NAT.

ASDM: Adaptive Security Device Module.

PPPOE: Point to Point Protocol over Ethernet

SSM: Security Service Module.

AIP: Advanced Inspection Prevention.

SSP: Security Service Processor.

CLI: Command Line Interface.

SSH: Secure Shell.

FTP: File Transfer Protocol.

SMTP: Simple Mail Transfer Protocol.

POP3: Post Office Protocol v3.

SSL: Secure Sockets Layer.

MPLS: Multi-Protocol Label Switching.

AES: Advanced Encryptions Standard.

DES: Data Encryptions Standard

RSA: Rivest Shamir Adleman.

AAA: Authentication Authorization, Accounting.

DH : Diffie-Hellman.

MD5 : Message-Digest Algorithme 5.

HMAC: Hashed Message Authentication Code.

OSI: Open Systems Interconnection.

SHA: Secure Hash Algorithm.

GNS3: Global Network Solutions.

HTTP: Hypertext Transfer Protocol.

HTTPS: Hypertext Transfer Protocol Secure.

VLAN: Virtual Local Area Network

ZBF: Zone Based Firewall

IOS: Internet Operating System

INTRODUCTION GENERALE

Introduction général

Les réseaux et les systèmes d'information sont devenus des outils indispensables pour le fonctionnement des administrations et des entreprises. Ils sont aujourd'hui déployés dans tous les secteurs professionnels, les entreprises de communication, les banques, les assurances, la médecine ou encore le domaine militaire, initialement isolés les uns des autres. Ces réseaux sont dans le présent interconnectés et le nombre de points d'accès ne cesse de croitre.

Ce développement phénoménal s'accompagne naturellement de l'augmentation du nombre d'utilisateurs. Ces utilisateurs connus ou non ne sont pas forcément pleins de bonnes intentions vis à vis de ces réseaux. Ils peuvent exploiter les vulnérabilités des réseaux et systèmes pour essayer d'accéder à des informations sensibles dans le but de les lire, les modifier ou les détruire.

Des lors que ces réseaux sont apparus comme des cibles d'attaques potentielles leur sécurisation est devenue un enjeu incontournable. Cette sécurisation va garantir la confidentialité, l'intégrité, la disponibilité et la non-répudiation. Et pour cela de nombreux outils et moyens sont disponibles tels que les solutions matérielles, logiciels d'audits ou les systèmes de détection d'intrusion (IDS), les antivirus, les réseaux privés (VPN) ou encore les firewalls.

Le firewall (pare-feu) qui est un élément matériel ou logiciel permettant de filtrer les paquets de données qui traversent un réseau en bloquant certains et autorisant d'autres. Ce mécanisme de sécurité offre plusieurs fonctionnalités qui aide à mettre en place une politique de sécurité efficace tels que : (Le filetage des paquets, translation d'adresse IP (NAT) et le contrôle d'accès).

Dans ce projet de fin d'étude on va voir comment mettre une politique de sécurité des éléments d'un réseau par une configuration de base. Il s'agit de réaliser un zonage, une zone représentant le réseau local, une zone représentant les serveur dite DMZ et une zone représentant le milieu extérieur permettant l'accès à internet. Pour sécuriser le réseau local vis-à-vis du réseau extérieur non confiant on interface entre eux un firewall (Cisco ASA : en administrant le NAT et l'ACL).

Dans le réseau local on procède à la sécurisation des routeurs qui consiste à contrôler les ports (port consol, port auxiliaire et port vty cas d'accès par ssh et Telnet).

Pour réaliser cette démarche, partageons notre projet en trois chapitres.

Le premier chapitre comporte une présentation globale de la sécurité du réseau, ses éléments d'importance, model de sécurité ainsi que la terminologie de base des risques.

Le deuxième chapitre montre les différentes attaques qui peuvent atteindre un système d'information d'une entreprise. Ces attaques qui peuvent être d'une source humaine ou technique. La politique de sécurité ayant plusieurs aspects définit plusieurs mesures pour faire

face au divers attaques réseaux et pour mettre le système d'information d'une entreprise en haute sécurité.

Le troisième chapitre inclus la conception et l'implémentation du projet. La conception nous a permis d'identifier les éléments de chaque zone de notre réseau a sécurisé de même les politiques de sécurisation. Le réseau local composé de trois PC reliés au switch qui est connecté au routeur aussi d'un serveur placé dans DMZ. Le réseau local est connecté au réseau extérieur (non-confiant) par un Firewall (Cisco ASA).

L'implémentation comporte la configuration de Cisco ASA Firewall et les routeurs. Configurer le firewall s'agit de placer le NAT, de filtrer le trafic entrant et sortant par ACL, de fixer les niveaux des priorités, d'activer le serveur DHCP et choisir le Protocol OSPF pour le routage.

Configurer les routeurs par sécurisation de ses ports (aux, cons, vty), cryptage des mots de passe d'accès distant.

CHAPITRE 01

Sécurité Fondamental

1.1Introduction

Dans le monde d'aujourd'hui, la plupart des entreprises quelles que soient leurs tailles et leurs fonctionnalités ont besoin d'un système d'information qu'est un ensemble de méthodes et de moyens pour traiter et stocker les informations nécessaires. Mais le problème qui se pose comment faire échangé l'information entre les différents services, de même avec ses partenaires distants.

Un réseau informatique locale reliant les différents services de l'entreprise assure l'échange d'informations. Ce réseaux une fois interconnecté avec l'extérieur permet d'envoyer les données vers ses partenaires distants.

La sécurité des réseaux électroniques et des systèmes d'information suscite de plus en plus des préoccupations parallèlement à l'augmentation rapide du nombre d'utilisateurs. Maintenant La sécurité atteint un point critique où elle représente une nécessité pour la croissance du commerce électronique et le fonctionnement de toute l'économie d'état.

Les gouvernements se sont rendu compte de la mesure dans laquelle leur économie et leurs citoyens sont dépendants d'un fonctionnement efficace des réseaux de communication et plusieurs d'entre eux ont commencé à revoir leurs dispositions en matière de sécurité.

L'internet a créé une connectivité mondiale permettant de relier entre eux des millions de réseaux petits et grands et des centaines de millions d'ordinateurs individuels et de plus en plus d'autres appareils incluant les téléphones portables. Ceci a grandement facilité l'accès illégal et à distance aux informations.

Ce premier chapitre comporte une présentation des différents risques et vulnérabilités, de la sécurité et des stratégies de sécurité des réseaux informatiques.

1.2 Définition des réseaux informatiques

Un réseau informatique est un ensemble d'équipements reliés entre eux pour échanger des informations.

Ces informations sont très importantes pour le déroulement des activités organisationnelles. Il est donc essentiel de les protéger contre les intrusions et les accès non autorisés. Dans cette perspective se munir d'un système de sécurité informatique qui est devenu une composante essentielle de l'infrastructure des entreprises.

Cependant l'évolution de l'utilisation d'internet oblige beaucoup d'organisations à mettre en place un système d'information très développé et fiable. Desservir ainsi leurs employés de toutes les informations et outils technologiques nécessaires qui répondent à ces besoins de fiabilité et de pérennité qui passent aux travers d'une communication régulière et accrue avec leurs partenaires fournisseurs et clients.

Mais avant toutes définissons certains aspects de ces types des risques qui affectent le réseau.

1.3 Les deux types des risques majeurs

1.3.1 Le risque hardware

Sont tous les risques qui touchent les équipements réels dans une entreprise tels que (vols, incendie, fuite d'eau, poussière…)

1.3.2 Le risque software

Sont tous les risques qui touchent les programmes, les logiciels d'équipements informatiques tels que : (les virus, Worms, cheval de Troie…etc.)

1.4 Les moyens de protection

1.4.1 La protection du hardware

Le matériel de télécommunication et très sensible pour cela il faut le protéger contre déférents accidents naturelles et humaines (immeuble adéquat, climatisation, caméra de surveillance, agent de sécurité…etc.).

1.4.2 La protection du software

Les logiciels sont des programmes qui gèrent les réseaux. Il faut les protéger contre les intrusions, les accès non autorisés qui collectent illégalement les informations et les coordonnées des clients et ensuite les modifier et les diffuser, la reprogrammation des équipements actifs. La question qu'on peut se poser est : comment sécuriser les informations?

1.5 Qu'est-ce que la sécurité ?

De nos jours la sécurité informatique est devenue un problème majeur dans la gestion des réseaux d'entreprises ainsi que pour les particuliers qui sont de plus en plus nombreux à se connecter à Internet. La transmission d'informations sensibles et le désir d'assurer la confidentialité de celles-ci est devenu un point primordial dans la mise en place des réseaux informatiques.

Il semble que nous ne pouvons pas passer une semaine entière sans savoir que des données de carte de crédit ou des informations personnelles ont été divulguées ou volés par des acteurs mal intentionnés.

La sécurité est devenue plus complexe que jamais motiver mais les capacités des Hackers continuent d'évoluer. De plus la localisation des données devient floue par les concepts de Cloud computer. Alors que nous nous efforçons d'offrir aux employés du monde entier un accès omniprésent aux données importantes. En revanche il est important de rester constamment vigilant quant à la protection des données et des entités qui les utilisent (gouvernements, entreprises, particuliers etc.). [1]

Figure 1.1 : si quoi la sécurité

1.6 L’importance de la sécurité

1.6.1 Pour gagner un avantage concurrentiel

C’est développer et maintenir une sécurité efficace car ces mesures peuvent fournir à une organisation un avantage compétitif face à la concurrence.

1.6.2 Pour se conformer aux exigences réglementaires et aux responsabilités jiduciaires

Les dirigeants de chaque entreprise ont la responsabilité d'assurer la sécurité et la solidité de l'organisation et de ses contenus. Les organisations qui dépendent des ordinateurs pour leur fonctionnement doivent élaborer des politiques et des procédures qui répondent aux exigences de sécurité de l'organisation. Ces politiques et procédures sont nécessaires non seulement pour protéger les actifs de l'entreprise mais aussi pour protéger l'organisation.

Le défaut de se conformer aux lignes directrices fédérales peut entraîner la saisie d'une institution financière par les organismes de réglementation fédéraux. Dans certains cas, les mandataires sociaux qui n'ont pas correctement rempli leurs obligations réglementaires et jiduciaires sont personnellement responsables des pertes subies par l'institution financière qui les emploie. [2]

1.6.3 Pour garder votre emploi

Enfin, pour sécuriser sa place au sein d'une organisation et pour assurer de futures perspectives de carrière, il est important de mettre en place des mesures qui protègent l’actifs organisationnels. La sécurité devrait faire partie de chaque réseau ou système. L'incapacité à fonctionner correctement peut entraîner la résiliation. [3]

1.7 Les domaines de la sécurité

Tous les domaines de l'informatique sont concernés par la sécurité d'un système d’information.

En fonction de son domaine d'application, la sécurité informatique se décline en :

1.7.1 Sécurité physique [4]

Concerne tous les aspects liés de l'environnement dans lequel les systèmes se trouvent.

La sécurité physique passe donc par :

- ✓ Des normes de sécurité.
- ✓ Protection de l'environnement (incendie, température, humidité, ...).
- ✓ Protection des accès.
- ✓ Redondance physique.
- ✓ Plan de maintenance préventive (test, ...) et corrective (pièce de rechange, ...).

1.7.2 Sécurité de l'exploitation

- ✓ En Rapport à tous ce qui touche au bon fonctionnement des systèmes, cela comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic et de mise à jour.
- ✓ La sécurité de l'exploitation dépend fortement de son degré d'industrialisation qui est qualifié par le niveau de supervision des applications et l'automatisation des tâches.
- ✓ Quelques points clés de cette sécurité :
  - o Plan de sauvegarde, secours, continuité, tests.
  - o Inventaire réguliers et si possible dynamique.
  - o Gestion du parc informatique, des configurations et des mises à jour.
  - o Contrôle et suivi de l'exploitation.

1.7.3 La sécurité logique [5]

La sécurité logique fait référence à la réalisation de mécanismes de sécurité par logiciel.

Elle repose sur la mise en œuvre d'un système de contrôle d'accès logique s'appuyant sur un service d'authentification, d'identification et d'autorisation.

Elle repose également sur :

- ✓ Les dispositifs mis en place pour garantir la confidentialité dont la cryptographie.
- ✓ Une gestion efficace des mots de passe et des procédures d'authentification.
- ✓ Des mesures antivirus et de sauvegarde des informations sensibles.

Pour déterminer le niveau de protection nécessaire aux informations manipulées, une classification des données est à réaliser pour qualifier leur degré de sensibilité (normale, confidentielle, top secret, ...).

1.7.4 La sécurité applicative

Faire un développement pertinent et l'intégrer harmonieusement dans les applications existantes.

Cette sécurité repose essentiellement sur une méthodologie de développement :

- ✓ La robustesse des applications, des contrôles programmés et des jeux de tests.
- ✓ Un plan de migration des applications critiques.
- ✓ La validation et l'audit des programmes.
- ✓ Un plan d'assurance sécurité. [5]

1.8 La sécurité Trinity [3]

Les trois étapes de la « trinité de sécurité » soient la prévention, la détection et la réponse constituent la base de la sécurité du réseau. La trinité de sécurité devrait être le fondement de toutes les politiques et mesures de sécurité d'une organisation développe et déploie.

1.8.1 La prévention

Le fondement de la trinité de sécurité est la prévention pour assurer un certain niveau de sécurité. Il est nécessaire de mettre en œuvre des mesures visant à prévenir l'exploitation des vulnérabilités de développement des systèmes de sécurité du réseau.

Rappelons qu'il est impossible de concevoir un système de sécurité qui empêchera l'exploitation de toutes les vulnérabilités mais les entreprises devraient veiller à ce que leurs mesures préventives soient suffisamment fortes pour décourager les criminels, alors ils vont à une cible plus facile.

1.8.2 Détection

Une fois les mesures préventives mises en œuvre, des procédures doivent être mises en place pour détecter les problèmes potentiels ou violations de la sécurité et dans le cas où les mesures préventives échoueraient. Il est très important que les problèmes soient détectés immédiatement. Le plus tôt possible le problème est détecté il est facile de le corriger et de le nettoyer.

1.8.3 Réponse

Les organisations doivent développer un plan qui identifie la réponse appropriée à une sécurité violée. Le plan devrait être écrit et devrait identifier qui est responsable de ces actions et produire la réponse convenable.

Avant d'entamer une discussion sérieuse sur la sécurité des ordinateurs et des réseaux, nous devons définir ce que cela implique. Premièrement, la sécurité du réseau n'est pas un problème technique c'est une affaire et problème de personnes. La technologie est la partie facile. La partie difficile est de développer une sécurité plane qui correspond aux activités de l'organisation et qui amène les gens à se conformer au plan.

1.9 Sécurité de l'information

La sécurité du réseau concerne avant tout la sécurité des informations de l'entreprise. Ces informations que nous essayons vraiment de protéger dans les ordinateurs et les réseaux qui se justifient par l'égalité suivante :

Sécurité de l'information = confidentialité + intégrité + disponibilité + authentification

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

1.9.1 Confidentialité

Il existe deux types de données:

- ✓ Les données en mouvement : Lorsqu'elles se déplacent sur le réseau.
- ✓ Les données au repos : Lorsqu'elles sont stockées sur un support de stockage (serveur, station de travail locale, dans le cloud, etc.).

La confidentialité signifie que les systèmes autorisés peuvent voir des informations sensibles ou classifiées. Cela implique également que les personnes non autorisées ne devraient avoir aucun type d'accès aux données.

En ce qui concerne les données en mouvement le principal moyen de les protégés est de les crypter avant de les envoyer sur le réseau. [4]

1.9.2 Intégrité

L’intégrité des données signifie que les modifications apportées aux données sont effectuées uniquement par des personnes ou systèmes autorisés. La corruption des données est un échec à maintenir l'intégrité des données.

1.9.3 Disponibilité

Cela s'applique aux systèmes et aux données. Si le réseau ou ses données ne sont pas disponibles pour les utilisateurs autorisés peut-être en raison d'une attaque par déni de service (DoS) ou d'une défaillance générale du réseau, l'impact peut être important pour les entreprises et les utilisateurs qui dépendent de ce réseau. [6]

1.10 Autres concepts de sécurité

1.10.1 Intimité

Le terme est utilisé fréquemment dans de nombreux contextes :

- Prévention de l'accès non autorisé.
- Absence d'accès non autorisé à des informations jugées personnelles ou confidentiels.
- Absence d'observation de surveillance ou d'examen sans consentement ou connaissance Lorsque l'on aborde la protection de la vie privée dans le domaine de l’informatique.

1.10.2 Identification

L'identification est le processus par lequel un sujet professe une identité. Un sujet doit fournir une identité à un système pour démarrer le processus d'authentification, d'autorisation et de responsabilité. Fournir une identité peut être en tapant un nom d'utilisateur, en balayant une carte à puce, en prononçant une phrase ou en positionnant nos visages, notre main ou notre doigt pour une caméra ou un appareil de numérisation.

1.10.3 Authentification

Le processus de vérification ou de test de validité de l'identité revendiquée est l'authentification. L'authentification nécessite du sujet des informations supplémentaires doit correspondre exactement à l'identité indiquée. La forme la plus commune de l'authentification utilise un mot de passe.

L'authentification vérifie l'identité du sujet en comparant un ou plusieurs facteurs par rapport à la base de données d'identités valides. Le facteur d'authentification utilisé pour vérifier l'identité est généralement étiquetés ou considérés comme des informations privées. La capacité du sujet et du système pour maintenir le secret des facteurs d'authentification pour les identités reflète directement le niveau de sécurité de ce système. [3]

Figure 1.2 : Authentification

1.10.4 Autorisation

Une fois qu'un sujet est authentifié, l'accès doit être autorisé. Le processus de l'autorisation garantit que l'activité demandée ou l'accès à un objet est possible compte tenu des droits et privilèges attribués à l'identité authentifiée.

Dans la plupart des cas, le système évalue une matrice de contrôle d'accès qui compare le sujet, l'objet et l'activité prévue. Si l'action spécifique est autorisée, le sujet est autorisé. Si l'action spécifique n'est pas autorisée, le sujet n'est pas autorisé.

L'identification et l'authentification sont des aspects de contrôle d'accès.

Figure 1.3 : autorisation de donnée

1.10.5 Audit

Le suivi ou l'audit est le moyen programmatique par lequel les sujets sont tenus responsables de leurs actes lorsqu'ils sont authentifiés sur un système. La surveillance est également le processus par lequel des activités non autorisées ou anormales sont détectés sur un système.

La surveillance est nécessaire pour détecter les actions malveillantes, des tentatives d'intrusion et des défaillances du système. [7]

Figure 1.4 : l'Audit

1.10.6 Responsabilité

La politique de sécurité d'une organisation ne peut être correctement appliquée que si la responsabilité est maintenue. En d'autres termes, la sécurité ne peut être maintenue que si les sujets sont tenus responsables de leurs actions. La reddition de comptes efficace repose sur la capacité de prouver l'identité d'un sujet et de suivre ses activités. Ainsi, la responsabilité repose sur les concepts d'identification, d'authentification, d'autorisation, contrôle d'accès et audit.

1.10.7 Non-répudiation

La non-répudiation garantit que le sujet d'une activité ou d'un événement ne peut pas nier que l'événement s'est produit. La non-répudiation empêche un sujet de revendiquer ne pas avoir envoyé de message, ne pas avoir effectué une action ou ne pas avoir été la cause d'un événement. Il est rendu possible grâce à l'identité, l'authentification, l'autorisation, la responsabilité et l'audit. La non-répudiation peut être établie à l'aide de certificats numériques. [4]

1.11 Les causes pour sécuriser les réseaux [8]

1.11.1 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 s'investissent de plus en plus dans la sécurisation de leurs systèmes d'information et dans la qualité de service fournit aux clients.

1.11.2 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 toutes structures engagées 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.

1.11.3 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 définit et dans le strict respect des lois en vigueur. En matière de juridiction le non-respect des lois relatives à la manipulation des informations dans un système d'information peut avoir des conséquences graves sur l'entreprise.

1.12 Modèles de sécurité

Trois approches de base sont utilisées pour développer un modèle de sécurité réseau. Habituellement. Les trois approches sont : la sécurité par l'obscurité, le modèle de défense du périmètre et la défense modèle de profondeur.

1.12.1 Sécurité par Obscurité

La sécurité par l'obscurité repose sur la discrétion pour la protection. Le concept derrière ce modèle est que si Personne ne sait qu'un réseau ou un système est là alors il ne sera pas sujet à l'attaque. Les bases l'espoir est que cacher un réseau ou au moins ne pas annoncer son existence servira de suffisante Sécurité. Le problème avec cette approche est qu'elle ne fonctionne jamais à long terme et une fois détecté le réseau est complètement vulnérable. [3]

1.12.2 La défense du périmètre

Le modèle de défense périmétrique est analogue à un château entouré de douves. En utilisant ce modèle dans la sécurité réseau. Les organisations durcissent ou renforcent les systèmes périmétriques et les frontières des routeurs ou une organisation peut "cacher" son réseau derrière un pare-feu qui sépare le réseau protégé d'un réseau non approuvé. L'hypothèse est que les défenses du périmètre sont suffisantes pour arrêter les intrus afin que les systèmes internes soient sécurisés. [9]

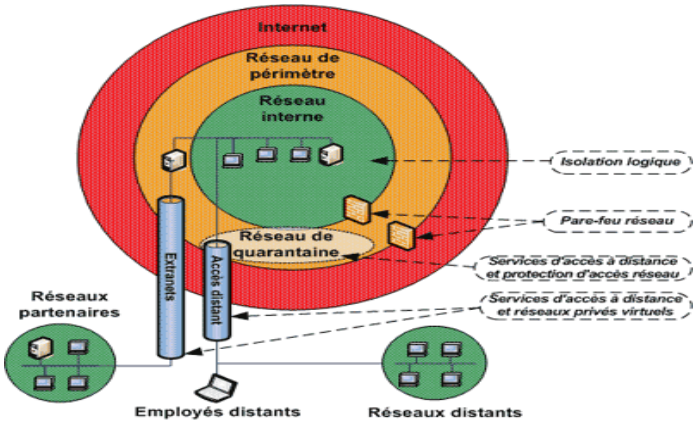

Figure 1.5 : Sécurité par périmètre

1.12.3 La défense en profondeur

La défense en profondeur s'efforce d'assurer la sécurité en renforçant et en surveillant chaque système. Des mesures supplémentaires sont encore prises sur les systèmes périmétriques mais la sécurité des réseau interne ne repose pas uniquement sur les systèmes de périmètre.

Avec l'approche de défense en profondeur le système avec le modem peut être compromis mais d'autres systèmes sur le réseau seront en mesure de se défendre. Les systèmes sur le réseau devraient également être en mesure de détecter les tentatives de hacks de système compromis.

Cette approche fournit également beaucoup plus de protection contre intrus. Les activités de l'intrus interne sont beaucoup plus susceptibles d'être détectées. [9]

Figure 1.6 : Sécurité en profondeur

1.13 Les Terminologie de base des risques de réseaux:

1.13.1 Vulnérabilité

Une vulnérabilité est une faiblesse exploitable d'un certain type. Cette l'exploitation peut résulter d'une attaque malveillante, ou peut-être accidentellement déclenchée en raison d'un échec ou d'une faiblesse de la politique d'implémentation ou d'un logiciel fonctionnant sur le réseau. La Figure 1.7 présent une vulnérabilité**.** [10]

Figure 1.7 : la vulnérabilité

1.13.1.1 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. [8]

1.13.1.2 Vulnérabilités technologiques

Avec la progression 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 Readines ou Response Team). [8]

1.13.1.3 Vulnérabilités organisationnelles

Les vulnérabilités d'ordre organisationnelles 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. [8]

1.13.1.4 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. [8]

1.13.2 Menace

Une menace est tout ce qui tente pour obtenir un accès non autorisé à compromettre, détruire ou endommager un actif.

Les menaces sont souvent réalisées via une attaque ou un exploit qui profite d’une vulnérabilité existante.

Les menaces se présentent aujourd'hui en plusieurs variétés et se propagent plus rapidement que jamais avant. Les menaces peuvent également se transformer et être modifiées au fil du temps, et vous doit être toujours diligent pour les suivre.

Figure 1.8 : Les menaces

1.13.3 Catégories de menaces de sécurité [11]

La menace de sécurité peut être classée en quatre parties et ces catégories sont les moyens ou des formulaires à travers lesquels les menaces peuvent être effectuées sur un réseau.

1.13.3.1 Menaces non structurées

Menace de sécurité non structurée est le genre de menace créée par une personne inexpérimentée essayer d'accéder à un réseau. Ils utilisent couramment des outils de piratage communs, comme scripts Shell et craqueurs de mot de passe. Une bonne solution de sécurité devrait facilement contrecarrer ce genre d'attaque.

En d'autres termes, ces types de pirates ne pouvaient pas être sous-estimé car ils peuvent causer de graves dommages au réseau.

1.13.3.2 Menaces structurées

Contrairement aux menaces non structurées, les hackers de menaces structurés sont bien expérimentés et hautement sophistiqué. Ils utilisent des outils de piratage sophistiqués pour pénétrer les réseaux et il peut percer dans les ordinateurs du gouvernement ou d'affaires pour extraire des informations. Sur certaines occasions, des menaces structurées sont perpétrées par des groupes criminels organisés ou l'industrie concurrents.

1.13.3.3 Menaces externes

Certaines personnes non autorisées à l'extérieur de l'entreprise qui n'ont pas accès au système informatique ou le réseau de l'entreprise pourrait causer une menace externe. D'habitude ils pénètrent dans le réseau de l'entreprise via Internet ou le serveur. Les deux : pirates expérimentés et pirates inexpérimentés pourraient poser des menaces externes.

1.13.3.4 Menaces internes

Ce genre de menace pourrait être un employé mécontent qui a autorisé l'accès au réseau de l'entreprise. Comme les menaces externes, les dommages qui pourraient être causés par un tel hacker dépend de l'expertise du pirate.

1.13.4 Les Risques

Les risques sont le potentiel d'accès non autorisé à compromettre la destruction ou l'endommagement d'un actif. Si une menace existe mais les contre-mesures de protections sont en place (votre objectif est de fournir cette protection), le potentiel de succès de la menace est réduit (réduisant ainsi le risque global). [22]

1.13.5 Les ennemis

1.13.5.1 Pirates informatiques (hackers)

Ce terme générique s'applique aux passionnés d'informatique s'amusant à accéder aux ordinateurs et aux réseaux d'autres personnes.

Figure 1.9 : le hacker.

1.13.5.2 Personnel non avisé

Il arrive souvent que des employés, concentrés sur leurs activités professionnelles spécifiques outrepassent les règles de base de sécurité du réseau. Ils peuvent par exemple choisir des mots de passe simples à mémoriser afin de se connecter aisément au réseau. Ces mots de passe sont alors faciles à deviner ou à forcer par les pirates, de manière logique ou à l'aide d'un utilitaire logiciel de "cracking" (logiciel permettant de découvrir les mots de passe) largement répandu. Les employés peuvent involontairement être la source de failles dans la sécurité, y compris la contamination accidentelle par des virus informatiques et leur propagation. [1]

1.13.5.3 Employés mécontents

Ce problème est bien plus troublant que l'éventualité d'une erreur humaine endommageant le réseau : un employé mécontent peut vouloir nuire à l'entreprise. Les employés mécontents souvent à la suite d'un licenciement ou d'une remontrance peuvent infecter le réseau de leur entreprise par des virus ou intentionnellement supprimer des fichiers importants ou encore en accédant à des données confidentielles afin de fournir aux concurrents des informations qu'ils n'auraient pas pu obtenir d'une autre manière. [1]

Figure 1.10 : Employés mécontents

1.14 Conclusion :

Il est vrai que le réseau informatique a aidé les entreprises de développer leurs services et garantir la communication à haut niveau entre ces différents partenaires. Mais ce réseau ne définit pas les mécanismes de sécurité pour l'échange de ces informations.

Par l'utilisation d'internet un individu de l'extérieur et qui n'a pas le droit d'accès peut modifier et voler et détruire n'importe qu'elle information peut être importante pour l'entreprise

CHAPITRE 02

Les attaques et les différentes politiques de sécurité

2.1 Introduction

Les réseaux informatiques sont devenus la principale préoccupation de la société, les informations sont stockées électroniquement et transmises à travers les réseaux et les attaques deviennent plus organisées, sophistiquées destructrices et difficiles à prévenir.

L'objectif principal de la protection des informations est d'éviter qu'une personne tierce non autorisé obtient les données de l'entreprise qui cause parfois des pertes financières. La protection donc la sécurité est un domaine très vaste et en constante évolution en cohérence avec l'évolution des technologies (réseaux, ordinateurs, programmes).

Les réseaux informatiques sont devenus le canal de la plupart des menaces. Également que la grande majorité des violations de la sécurité des organisations sont intentionnellement ou involontairement perpétrées par leurs propres employés qui peut être mécontent, insuffisamment préparé (les employés crédules, le manque d'éducation et de formation) ou motivés à exposer des informations données à des fins personnelles (des gains financiers).

Certaines attaques telles que les virus et le déni de service (DOS) sont conçues pour perturber le réseau cible et ses systèmes informatiques. Cependant la majorité des attaques visent à voler ou à fouiller des informations privées et sensibles. Il y a de nombreux méthodes d'agression représentant certaines attaques bien connues auxquelles sont confrontés les utilisateurs du système et les organisations professionnelles.

Ce chapitre explique les attaques les plus fréquentes perpétrées par des agresseurs principalement sur le réseau informatique pour atteindre divers buts et objectifs. Aussi les politiques de sécurité sont présentées.

2.2 Attaques permettant de dévoiler le réseau [13]

2.2.1 Attaque par cartographie du réseau

Les attaques visant à établir la cartographie d'un réseau ont pour but de dresser les artères de communication des futurs systèmes cibles. Elles ont recours pour cela à des outils de diagnostic tels que Trace route qui permet de visualiser le chemin suivi par un paquet IP d'un hôte à un autre.

Trace route utilise l'option durée de vie ou TTL (Time To Live) du paquet IP pour émettre un message ICMP time_exceeded (temps dépassé) pour chaque routeur qu'il traverse.

Sachant que chaque routeur qui manipule un paquet décrémente le champ TTL devient un véritable compteur de tronçon et permet de déterminer l'itinéraire précis suivi par les paquets IP vers un système cible.

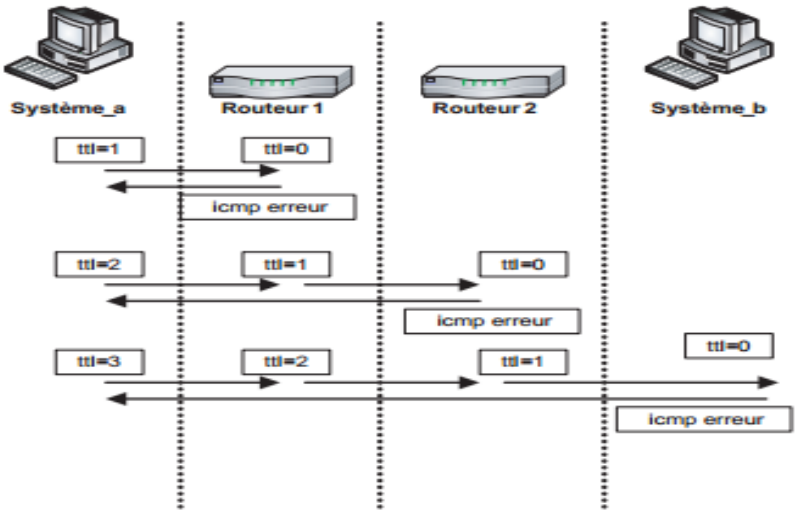

Figure 2.1 : Fonctionnement d'outil trace route.

2.2.2 Attaques par Identification des Systèmes Réseau

Certaines attaques visent à identifier tous les systèmes présents dans le but de dresser les futurs moyens de pénétration du réseau ou des systèmes qui le composent.

Il existe pour cela différentes techniques de balayage des systèmes.

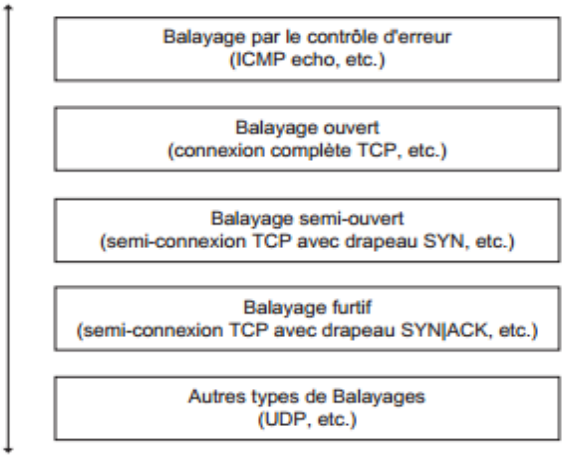

Figure 2.2 : les différents types de balayage.

2.2.2.1 Attaque par Balayage ICMP

La méthode de balayage la plus simple consiste à utiliser le protocole ICMP et sa fonction requête la plus connue sous le nom de Ping. Elle consiste à ce que le client envoie vers le serveur un paquet ICMP echo-request. Le serveur répondant (normalement) par un paquet ICMP echo-reply. Toute machine ayant une adresse IP est un serveur ICMP.

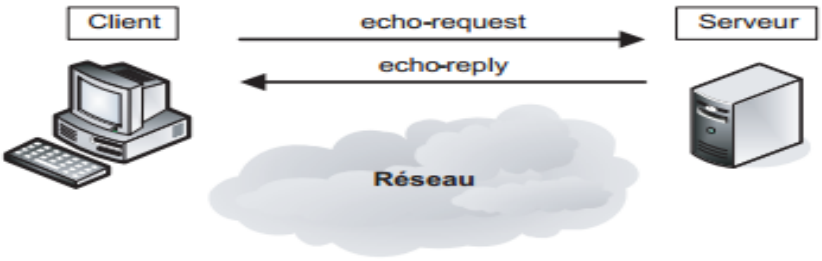

Figure 2.3 : fonctionnement de la command Ping.

2.2.2.2 Attaque par balayage TCP

L'envoie d'un paquet SYN vers un port réseau particulier de l'adresse IP du serveur. Si le port est en écoute le paquet SYN/ACK est reçu en retour. Sinon la réception d'un paquet RST signifie qu'il n'y a pas de service en écoute sur le port. L'envoie en réponse un paquet RST pour terminer la connexion.

Si aucune réponse n'est reçue en retour c'est qu'il existe un équipement filtrant entre le serveur et le client ou qu'il n'y a aucune machine derrière l'adresse IP visée.

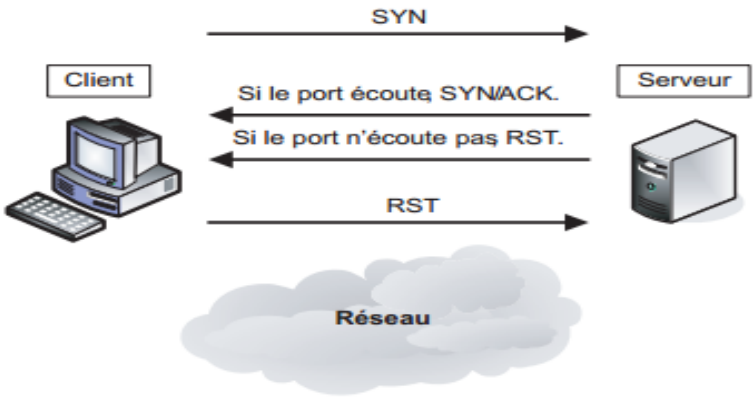

Figure 2.4 : Le balayage TCP.

2.2.3 Attaque par sniffing (Renifleurs)

Un renifleur est un programme ou un périphérique qui surveille les données circulant sur un réseau. Les renifleurs peuvent être utilisés pour des activités légitimes telles que la gestion de réseau ou pour des activités illégitimes Comme le vol d'informations trouvées sur un réseau. Une variété de différents types de renifleurs sont disponibles. [14]

2.2.3.1 Types de Sniffing

✓ **Passive Sniffing**

Reniflage passif : lorsqu'un renifleur rassemble des paquets au niveau de la couche de liaison de données, il peut potentiellement saisir tous les paquets sur le LAN de la machine exécutant le programme de renifleur.

La majorité des outils sniffer sont idéalement adaptés pour renifler des données dans un environnement de concentrateur. Ces outils sont appelés sniffers passifs car ils attendent passivement que les données soient envoyées avant de les capturer. Ces renifleurs sont efficaces pour collecter silencieusement des données du LAN. [15]

✓ **Active Sniffing**

Les renifleurs commutent, injectent activement du trafic dans le LAN pour permettre le reniflage du trafic. C'est ce qu'on appelle le reniflement actif. Certaines des méthodes utilisées dans cette attaque sont les suivantes:

- ✓ ARP spoofing.
- ✓ MAC flooding.
- ✓ MAC duplicating.

✓ **Contre-mesures**

Le cryptage est le meilleur moyen d'être protégé contre le reniflement. Cela n'empêchera pas un renifleur de fonctionner mais toutes les données lues par le renifleur seront incompréhensibles. Le renifleur ne sera pas capable de déchiffrer les données cryptées.

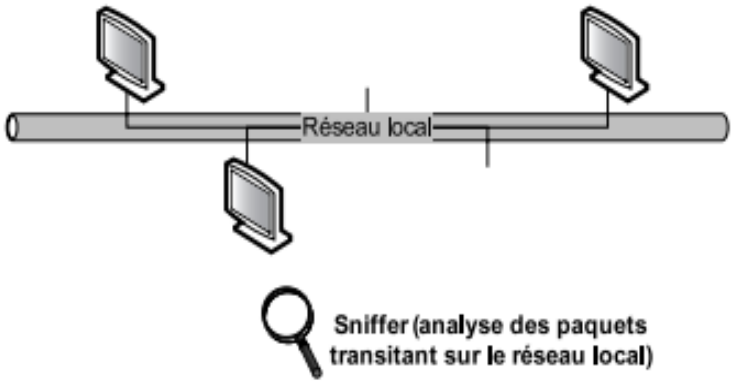

Figure 2.5 : Écoute sur un réseau local.

2.2.4 Attaque ARP spoofing

Comme son nom l'indique, l'attaque ARP spoofing s'appuie sur le protocole ARP (Adresse Résolution Protocol) qui implémente le mécanisme de résolution d'une adresse IP (32 bits) en une adresse MAC (48 bits) pour rediriger le trafic réseau d'un ou plusieurs systèmes vers le système pirate. [13]

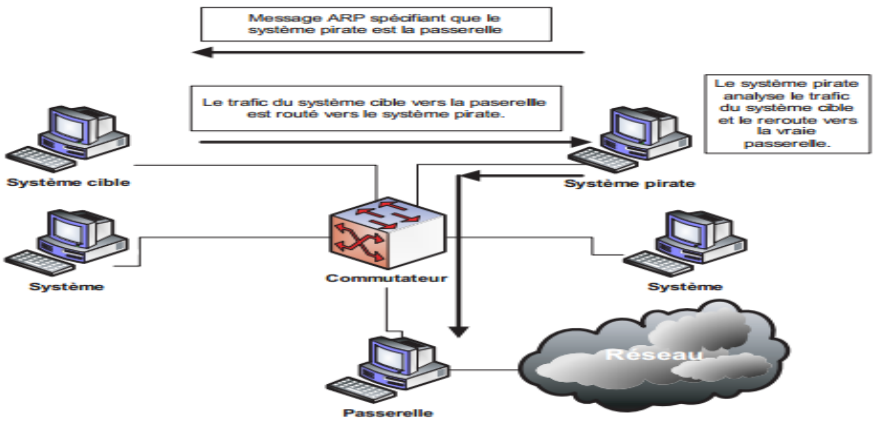

Figure 2.6 : L'attaque ARP spoofing.

2.2.5 Attaque IP spoofing

L'attaque IP spoofing consiste à se faire passer pour un autre système en falsifiant son adresse IP. Le pirate commence par choisir le système qu'il veut attaquer. Après avoir obtenu le maximum de détails sur ce système cible. Il détermine les systèmes donc les adresses IP autorisés à se connecter au système cible. Le pirate procède ensuite aux étapes illustrées pour mener à bien son attaque sur le serveur cible en utilisant l'adresse IP de la machine A. [12]

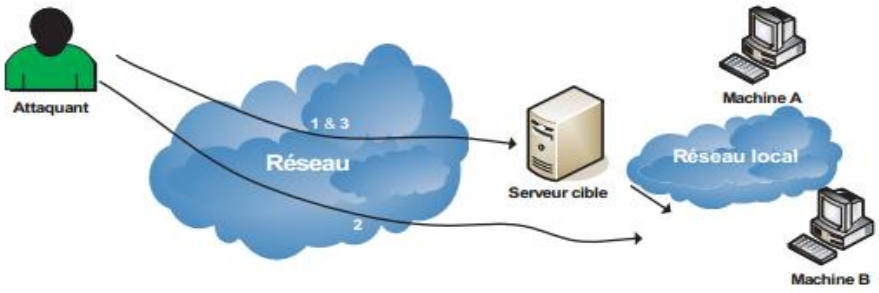

Figure 2.7 L'attaque IP spoofing

2.2.6 Attaque man-in-the-middle [13]

L'attaque man-in-the-middle consiste à faire passer les échanges réseau entre deux systèmes par le biais d'un troisième sous le contrôle du pirate. Ce dernier peut transformer à sa guise les données à la volée tout en masquant à chaque acteur de l'échange la réalité de son interlocuteur.

Au final l'échange se présente sous l'une des trois formes suivantes :

• **Relais transparent :** La machine du pirate transforme les données à la volée. Elle veut rester la plus transparente possible et se comporte comme un routeur conservant toutes les caractéristiques des paquets dont elle assure le transit à l'exception du contenu.

En termes d'adresses IP A et B sont réellement en relation l'une avec l'autre

Figure 2.8 : Machine du pirate en tant que relais transparent.

• **Relais applicatif :** La machine du pirate assure l'échange entre les deux machines A et B. A parle avec la machine du pirate laquelle parle avec B. A et B n'échangent jamais de données directement. Cette méthode est nécessaire pour les attaques vers SSL

Figure 2.9 : Machine du pirate en tant que relais applicatif.

2.3 DOS ATTAQUE

Le déni de service est une attaque visant à empêcher une communication normale en désactivant la ressource elle-même ou en désactivant un périphérique d'infrastructure qui lui fournit une connectivité. La ressource désactivée peut prendre la forme de données client, de ressources de site Web ou d'un service spécifique.

La forme la plus courante de déni de service consiste à submerger une victime avec autant de trafic que toutes les ressources disponibles du système sont submergées et incapables de traiter des demandes supplémentaires.

Les éléments qui peuvent indiquer qu'une attaque DoS peut être en vigueur tels que:

- Indisponibilité d'une ressource.
- Perte d'accès à un site Web.
- Ralentissement des performances.
- Augmentation des spams (courrier Ennuyeux). [14]

2.3.1 DoS cibles [16]

✓ **Compromission de serveur Web**

Une attaque DoS réussie et la compromission subséquente d'un serveur Web constituent l'exposition publique la plus large contre une cible spécifique. Ce que nous voyons le plus souvent est une perte de disponibilité pour une page Web d'entreprise ou une ressource Web.

✓ **Ressources back-end**

Les ressources dorsales incluent les éléments d'infrastructure qui prennent en charge une ressource publique telle qu'une page Web. Les attaques DoS qui suppriment une ressource principale telle qu'une base de données client ou une batterie de serveurs rendent toutes les ressources frontales indisponibles.

2.3.2 Types d'attaques (DOS) [15]

Les attaques DoS contiennent de nombreux concepts dont chacun est nécessaire pour comprendre la nature de la classe d'attaque dans DoS.

✓ **Inondations de demande de service**

Dans cette forme d'attaque DoS, un service tel qu'un serveur Web ou une application Web est inondé de requêtes jusqu'à ce que toutes les ressources soient épuisées.

Les demandes de service sont généralement effectuées en établissant des connexions TCP répétées à un système. Les connexions TCP répétées consomment des ressources sur le système de la victime jusqu'au point d'épuisement.

✓ **Attaque par inondation SYN**

Ce type d'attaque exploite la poignée de main à trois voies avec l'intention d'attacher un système. Pour que cette attaque se produise l'attaquant va falsifier les paquets SYN avec une adresse source fictive.

Quand le système victime répond avec un SYN-ACK il va à cette adresse fausse et puisque l'adresse n'existe pas cela amène le système victime à attendre une réponse qui ne viendra jamais. Cette période d'attente lie une connexion au système car le système ne recevra pas d'accusé de réception.

✓ **ICMP Inondation Attaque**

Une requête ICMP nécessite que le serveur traite la demande et répond, consommant les ressources de l'unité centrale. Les attaques sur le protocole ICMP incluent les attaques smurf, les inondations ICMP qui en tirent parti en inondant le serveur de requêtes ICMP sans attendre la réponse.

✓ **Ping de la mort**

Le Ping de la mort était un paquet plus grand que le 64K autorisé, Bien qu'il ne soit pas une menace importante aujourd'hui en raison du blocage du Ping des patchs du système d'exploitation et de la conscience générale, apogée le Ping of Death était un exploit DoS formidable et extrêmement facile à utiliser.

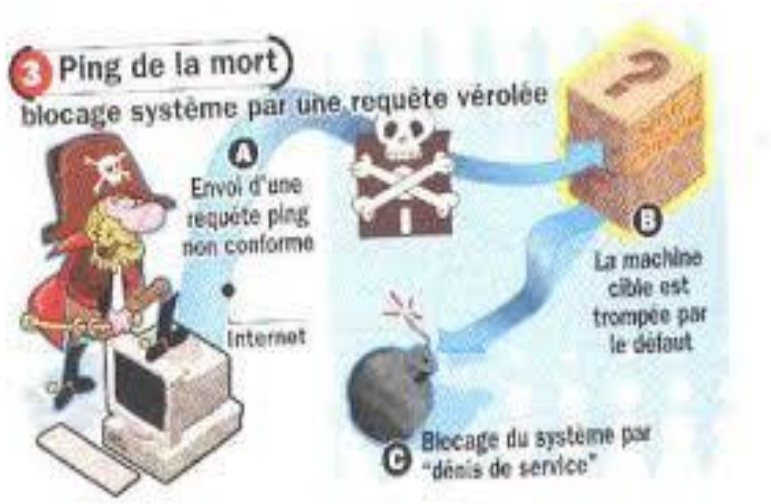

Figure 2.10 : Ping de la mort.

✓ **Larme**

L'attaque se produit sous la forme de ruptures lorsqu'un attaquant envoie des paquets fragmentés personnalisés avec des valeurs de décalage qui se chevauchent pendant la tentative de reconstruction. Cela provoque l'instabilité de la machine cible lors de la tentative de reconstruction des paquets fragmentés.

✓ **Smurf**

Une attaque smurf usurpe l'adresse IP de la machine cible et envoie de nombreux paquets de requêtes d'écho ICMP aux adresses de diffusion des sites intermédiaires. Les sites intermédiaires amplifient le trafic ICMP vers l'IP source saturant ainsi le segment réseau de la machine cible.

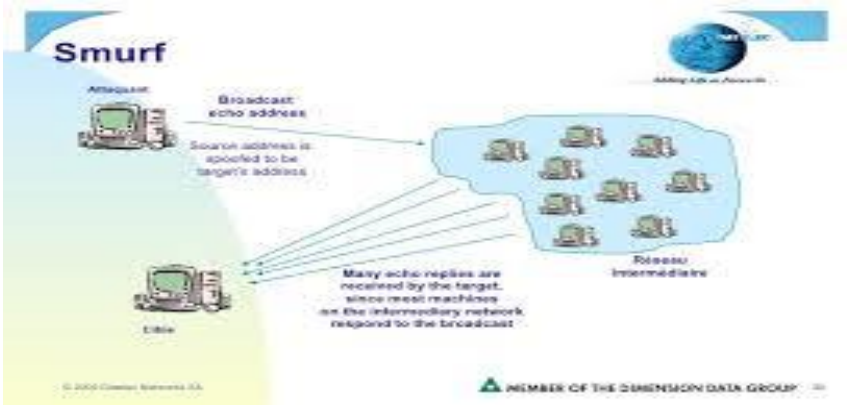

Figure 2.11 : smurf attaque.

✓ **Débordement de tampon**

Le Débordement de tampon (buffer over flow) est une technique DoS qui tire avantage d'une erreur dans le codage d'un programme en entrant plus de données que la mémoire tampon du programme ou l'espace mémoire n'a pas de place.

2.4 Comprendre le DDoS

Les attaques par déni de service distribué (DDoS) ont les mêmes objectifs de DOS mais la mise en œuvre est beaucoup plus complexe et exerce plus de pouvoir. Alors qu'une attaque DoS dépend d'un seul système ou d'un très petit nombre de systèmes pour attaquer une victime. Une attaque DDoS augmente en ayant plusieurs attaquants après une victime peut atteindre quelques centaines à quelques millions dans certains cas. [17]

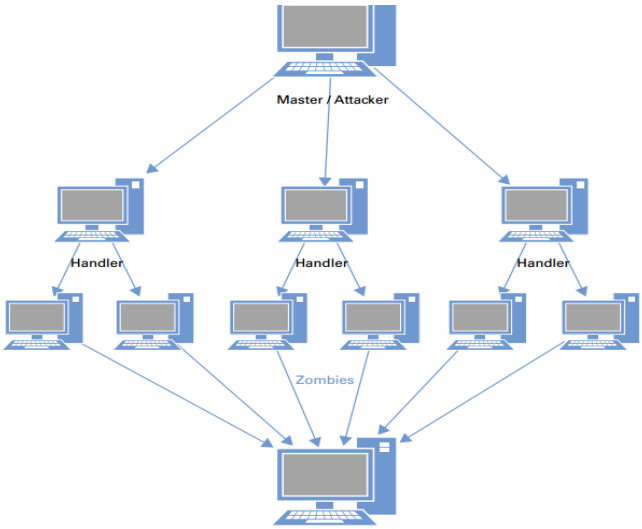

Figure 2.12 : DDOS attaque.

2.5 Spamming attaque

Le terme "spam" désigne un courrier électronique, un groupe de discussion ou une discussion indésirable. Le spam n'est généralement pas une menace pour la sécurité mais plutôt un type d'attaque par déni de service.

Les attaques de spamming sont dirigées par inondation de messages non désirés à la victime.

Boîte de réception e-mail ou autre système de messagerie. De telles attaques provoquent des problèmes de DoS pour remplir l'espace de stockage et empêcher la livraison de messages légitimes.

Dans les cas extrêmes, les attaques de spams peuvent provoquer des blocages du système ou des plantages et interrompre l'activité d'autres utilisateurs sur le même sous-réseau ou le même ISP. [14]

Figure 2.13 : spamming attaque.

2.6 TROJAN

Un cheval de Troie est défini comme un programme malveillant et destructeur de sécurité. Un cheval de Troie informatique est utilisé pour entrer sans être détecté dans l'ordinateur de la victime. Stocké sur cet ordinateur et causant d'immenses dommages à la victime. Les utilisateurs peuvent télécharger un fichier qui semble être un film mais lorsqu'il est exécuté déclenche un programme dangereux qui efface le disque dur ou envoie des numéros de carte de crédit et des mots de passe à l'attaquant. [15]

2.6.1 Fonctionnement

- Un cheval de Troie peut supprimer des fichiers, transmettre des informations, modifier des fichiers existants et installer d'autres programmes.
- Le cheval de Troie peut tenter d'exploiter une vulnérabilité pour augmenter le niveau d'accès au-delà de celui de l'utilisateur qui l'exécute.
- En cas de succès le cheval de Troie peut fonctionner avec des privilèges accrus et peut installer un autre code malveillant sur la machine de la victime.
- Un cheval de Troie en fonction des actions qu'il effectue peut fausser ou impliquer le système distant en tant que source d'une attaque par usurpation d'identité et ainsi engager la responsabilité du système distant. [15]

Figure 2.14 : Trojan.

2.7 Virus et vers

Un programme malveillant est un logiciel ou un code hostile ou intrusif. Les programmes malveillants ont le potentiel de faire des ravages sur les ordinateurs professionnels et personnels.

Dans le monde entier la plupart des entreprises ont été touchées par ces programmes à un moment donné. Bien que de nombreuses personnes se réfèrent à un programme malveillant en tant que virus, les virus ne sont techniquement que l'un des nombreux types de programmes malveillants. Ces programmes sont les suivants:

- ✓ **Virus**

Un virus est un programme auto-répliquant qui produit son propre code en attachant des copies de lui-même à d'autres codes exécutables et fonctionne sans la connaissance ou le désir de l'utilisateur. Un vrai virus informatique est contagieux et peut contaminer d'autres fichiers; Cependant, les virus peuvent infecter des machines externes uniquement avec l'aide d'utilisateurs d'ordinateurs. [12]

Figure 2.15 : virus

- ✓ **Worms (ver)**

Un ver est un programme malveillant qui peut infecter à la fois les machines locales et distantes. Les vers se propagent automatiquement en infectant le système après système dans un réseau et même en s'étendant à d'autres réseaux. Par conséquent les vers ont un plus grand potentiel de causer des dommages car ils ne dépendent pas des actions de l'utilisateur pour l'exécution. [15]

Figure 2.16 : le ver

2.8 Ingénierie sociale

L'ingénierie sociale est l'utilisation de l'influence et de la persuasion pour tromper les gens dans le but d'obtenir des informations ou d'effectuer une action. Les individus à tous les niveaux d'activité ou d'interaction communicative peuvent utiliser cette méthode. Toutes les mesures de sécurité adoptées par une organisation sont vaines lorsque les employés sont conçus par des étrangers. Certains exemples d'ingénierie sociale incluent, sans le savoir, répondre aux questions des étrangers, répondre aux courriers indésirables et se vanter auprès des collègues. [17]

2.8.1 Types d'ingénierie sociale [15]

Figure 2.17 : ingénierie social.

2.8.1.1 Ingénierie sociale basée sur l'humain

Un attaquant pourrait utiliser la technique de l'usurpation d'identité d'un employé et recourir ensuite à des méthodes déviantes pour accéder à des données privilégiées. Il ou elle peut donner une fausse identité et demander des informations sensibles.

- ✓ **Posant en tant qu'utilisateur important**

Usurpation d'identité est prise à un niveau supérieur en assumant l'identité d'un employé important afin d'ajouter un élément d'intimidation. Le facteur de réciprocité joue également un rôle dans ce scénario, où les employés de niveau inférieur peuvent faire tout leur possible pour aider un employé de plus haut niveau afin que leur faveur reçoive l'attention positive nécessaire pour les aider dans l'environnement de l'entreprise.

Une autre tendance comportementale qui aide un ingénieur social est la tendance des gens à ne pas remettre en question l'autorité. Souvent, les gens font quelque chose en dehors de leur routine pour quelqu'un qu'ils perçoivent comme étant en autorité

✓ **Posant comme support technique**

Une autre technique implique un attaquant se faisant passer pour un technicien de soutien, en particulier lorsque la victime ne maîtrise pas les domaines techniques. L'attaquant peut se faire passer pour un vendeur de matériel, un technicien ou un fournisseur informatique lors de l'approche de la victime.

2.8.1.2 Ingénierie sociale informatisée

✓ **Fenêtres contextuelles**

Dans ce type d'ingénierie sociale, une fenêtre apparaît à l'écran informant l'utilisateur qu'il a perdu sa connexion réseau et qu'il doit entrer à nouveau son nom d'utilisateur et son mot de passe. Un programme que l'intrus avait précédemment installé enverra ensuite l'information par courrier électronique à un site distant.

✓ **Pièces jointes au courrier**

Il y a une forme commune qui peut être utilisée. Il implique un code malveillant. Ce code est généralement caché dans un fichier joint à un message électronique. Ici, on s'attend à ce qu'un utilisateur non averti ouvre le fichier, permettant au code du virus de se répliquer.

✓ **Sites Internet**

Les attaquants peuvent utiliser des sites Web pour effectuer l'ingénierie sociale. Cela implique une ruse pour amener un utilisateur inconscient à divulguer des données potentiellement sensibles, telles qu'un mot de passe utilisé au travail.

De nombreux employés saisissent le même mot de passe qu'ils utilisent au travail, de sorte que l'ingénieur social dispose désormais d'un nom d'utilisateur et d'un mot de passe valides pour entrer dans le réseau d'une organisation.

2.9La politique de sécurité

Une politique de sécurité est un ensemble de règles qui fixent les actions autorisées et interdites dans le domaine de la sécurité. Chaque entreprise vaudra définir une politique de sécurité, elle va être obligée de respecter ses règles et les améliorer pour qu'elle soit bien protégée contre les différents types de menace.

2.9.1 Règles de sécurité génériques

✓ **Consistance du plan d'adressage**

Il s'agit des règles qui garantissent la consistance du plan d'adressage des équipements réseau. De manière générique, il ne doit exister de doublons dans le plan d'adressage global du réseau.

✓ **Consistance des Configurations**

Il s'agit des règles qui garantissent la consistance des configurations des équipements réseau. De manière générique, tout élément de configuration défini doit être appliqué, et tout élément de configuration appliqué doit être défini. Ces règles peuvent être complexes comme la vérification de la grammaire associée au langage de configuration.

✓ **Consistance des filtrages**

Il s'agit des règles qui garantissent la consistance des filtrages utilisés pour contrôler par exemple les flux de données ou de routage. De manière générique, les éléments constituant un filtrage ne doivent être ni redondants, ni contradictoires entre eux. Ces règles peuvent être complexes comme la vérification des règles inutiles.

✓ **Routage**

Il s'agit des règles de configuration relatives à la protection du routage réseau. Ces règles s'appliquent à la fois au routage interne du réseau ainsi qu'aux interconnexions de routage du réseau avec l'extérieur. Ces règles peuvent être complexes comme la vérification de la topologie du routage interne et externe du réseau, la consistance de la politique de routage, etc.

✓ **Service**

Il s'agit des règles de configuration relatives à la protection des services du réseau. Ces règles peuvent être complexes comme la vérification des périmètres de sécurité d'un VPN.

✓ **Partenaires**

Il s'agit des règles de configuration relatives à la protection des interconnexions avec les services réseau d'un partenaire.

✓ **Administration**

Il s'agit des règles de configuration relatives à la protection des équipements réseau.

2.9.2 La sécurité de réseaux

2.9.2.1 Les antivirus

Est un logiciel ayant pour objectif principal de protéger une machine contre différents types d'infections informatiques telles que des virus. Cependant, des différences peuvent exister entre ces types de logiciels. Elles se situent principalement dans le nombre de fonctionnalités, leur mise en place ainsi que les méthodes utilisées pour la détection d'anomalies.

2.9.2.1.1 Composants d'un antivirus

✓ **Scanner**

Il examine (scan) l'ordinateur à la demande : un fichier, un dossier ou tous les fichiers de votre disque. Un scan complet consomme beaucoup de ressources matérielles et de temps, mais il est conseillé de le faire de temps en temps.

✓ **Moniteur**

Il analyse en temps réel les fichiers auxquels vous accédez au cours de votre utilisation normale et stoppe immédiatement une exécution virale. Il est composé de plusieurs modules dont le nom change suivant les logiciels. Par exemple McAfee VirusScan en a quatre, chacun dédié à une tâche : email, Web, téléchargement, système.

En fonction de sa configuration et de la puissance de votre ordinateur, il ralentit plus ou moins vos applications.

✓ **Base de signatures de virus**

Une signature est un bout de code permettant d'identifier un virus, un peu comme une empreinte digitale humaine. La base de signatures référence des dizaines de milliers de virus, troyens et variantes. Elle doit être mise à jour fréquemment pour reconnaître les nouveaux spécimens.

2.9.2.2 Accès sécurisé

✓ **AAA**

L'utilisation de l'authentification, de l'autorisation et de la comptabilité (AAA) pour vérifier l'identité d'un utilisateur et ce que cet utilisateur est autorisé à faire est un excellent moyen de sécuriser le plan de gestion sur un routeur ou un commutateur. Le défi cependant est que la plupart des entreprises ont de nombreux périphériques réseau.

C'est un processus en deux parties. La première partie consiste à configurer sur le serveur ACS des informations sur les utilisateurs et leurs mots de passe et sur ce que ces utilisateurs sont autorisés à faire. La deuxième partie consiste à indiquer au routeur qu'il doit renvoyer l'une de ses décisions concernant l'authentification ou l'autorisation au serveur ACS. [18]

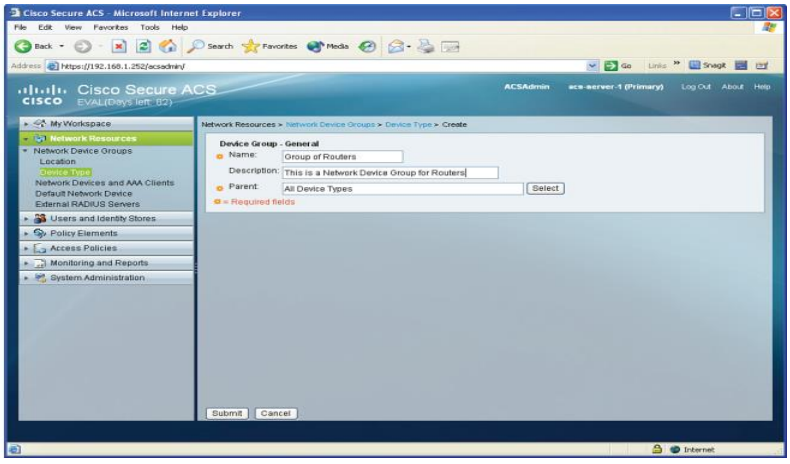

Figure 2 .18 : Création d'un groupe de périphériques réseau

2.9.2.3 VPN

VPN (Virtual Private Network) est un terme générique utilisé pour décrire une communication réseau qui utilise une combinaison de technologies pour sécuriser une connexion tunnellisée via un réseau autrement non sécurisé.

Les protocoles de tunnellisation sont exploités à la couche deux (2) de modèle OSI ou à la couche trois (3). Les protocoles de tunnellisation les plus couramment utilisés sont IP sec, L2TP, PPTP et SSL. Un paquet avec une adresse IP privée non routable peut être envoyé à l'intérieur d'un paquet avec une adresse IP globalement unique, étendant ainsi un réseau privé sur Internet.

2.9.2.3.1Type de VPN

Sur la base de la définition d'un réseau privé virtuel, les éléments suivants pourraient être considérés comme des technologies VPN.

2.9.2.3.2Les deux grandes catégories de VPN

- ✓ **VPN à accès distant**

Certains utilisateurs peuvent avoir besoin de créer une connexion VPN entre leur ordinateur individuel et le siège social de l'entreprise. C'est ce qu'on appelle une connexion VPN d'accès distant. Les VPN à accès distant peuvent utiliser les technologies IP sec ou Secure Shell (SSL) pour leur VPN.

De nombreux clients Cisco utilise le client Cisco AnyConnect pour les VPN SSL à accès distant. L'utilisation de VPN SSL est plus répandue, même si le client Cisco AnyConnect prend également en charge IP sec (IKEv2). [18]

- ✓ **VPN d'un site à site**

L'implémentation VPN est celle des entreprises qui souhaitent connecter deux sites ou plus en toute sécurité (probablement via Internet) afin que chaque site puisse communiquer avec l'autre site ou les autres sites. Cette implémentation est appelée un VPN de site à site. Les VPN de site à site utilisent traditionnellement une collection de technologies VPN appelées IP sec. [3]

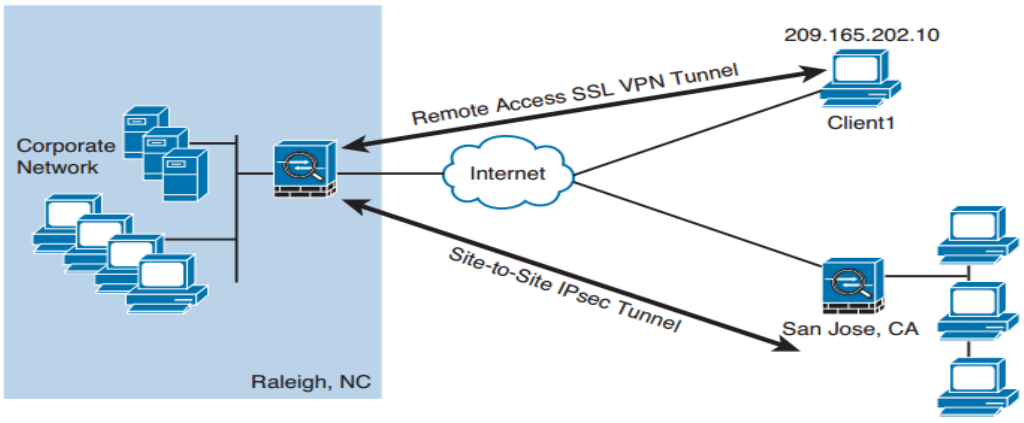

Figure 2.19 : Exemple de VPN à accès distant et de site à site.

2.9.2.4 Cryptographie

2.9.2.4.1 Chiffrements

Un chiffrement est un ensemble de règles, que l'on peut aussi appeler un algorithme, sur la façon d'effectuer cryptage ou décryptage. Littéralement des centaines d'algorithmes de cryptage sont disponibles, et il y a probablement beaucoup d'autres qui sont exclusifs et utilisés à des fins spéciales telles que le gouvernement et la sécurité nationale.

Les méthodes courantes utilisées par les chiffrements sont les suivantes:

✓ **Substitution**

Ce type de chiffrement remplace un caractère par un autre.

Pour rendre plus difficile, ont déplacé plus d'un seul caractère et seulement choisi certaines lettres à substituer. La méthode exacte de substitution pourrait être appelée la clé. Si les deux parties impliquées dans le VPN comprennent la clé, elles peuvent à la fois chiffrer et déchiffrer les données.

✓ **Poly alphabétique**

Ceci est similaire à la substitution, mais au lieu d'utiliser un seul alphabet, il pourrait utiliser plusieurs alphabets et basculer entre eux par un caractère de déclenchement dans le message codé.

✓ **Transposition**

Cela utilise de nombreuses options différentes, y compris le réarrangement des lettres.

2.9.2.4.2 Chiffrement Bloc et flux

✓ **Chiffrement par bloc**

Un chiffrement de bloc est une clé symétrique (même clé pour chiffrer et déchiffrer) un chiffrement qui fonctionne sur un groupe de bits appelé un bloc. Un algorithme de chiffrement par bloc peut prendre un bloc de 64 bits de texte brut et générer un bloc de 64 bits de texte chiffré. Avec ce type de chiffrement, la même clé à chiffrer est également utilisée pour déchiffrer.

Des exemples d'algorithmes de chiffrement par blocs symétriques comprennent les suivants :

- ✓ Advanced Encryptions Standard (AES).
- ✓ Triple Digital Encryptions Standard (3DES).
- ✓ Blowfish.
- ✓ Digital Encryptions Standard (DES).
- ✓ International Data Encryptions Algorithmes (IDEA). [18]

✓ **Chiffrement par flux**

Un chiffrement de flux est un chiffrement de clé symétrique (même clé à chiffrer que déchiffrer), où chaque bit de données en clair à chiffrer est fait 1 bit à la fois contre les bits du flux de clé, également appelé flux chiffré.

La sortie résultante est un flux de texte chiffré. Parce qu'un flux de chiffrement ne doit pas tenir dans une taille de bloc donnée, il peut y avoir légèrement moins de tête qu'un chiffrement de bloc qui nécessite un remplissage pour compléter une taille de bloc. [18]

2.9.2.4.3 Chiffrement symétrique et asymétrique

✓ **Symétrique**

Un algorithme appelé chiffrement symétrique utilise la même clé pour chiffrer les données et décrypter les données.

Des algorithmes de chiffrement symétriques sont utilisés pour la plupart des données de protéger dans les VPN. La raison pour laquelle nous utilisons symétrique pour chiffrer la majeure partie de nos données est parce qu'il est beaucoup plus rapide d'utiliser un algorithme de chiffrement symétrique et prend moins de CPU pour le même algorithme de chiffrement symétrique que pour un algorithme asymétrique.

La longueur minimale de la clé doit être d'au moins 128 bits pour que les algorithmes de chiffrement symétrique soient considérés comme relativement sûrs. Exemple pour chiffrement symétrique

DES, 3DES, AES, Idée, RC2, RC4, RC5, RC6, Blowfish. [16]

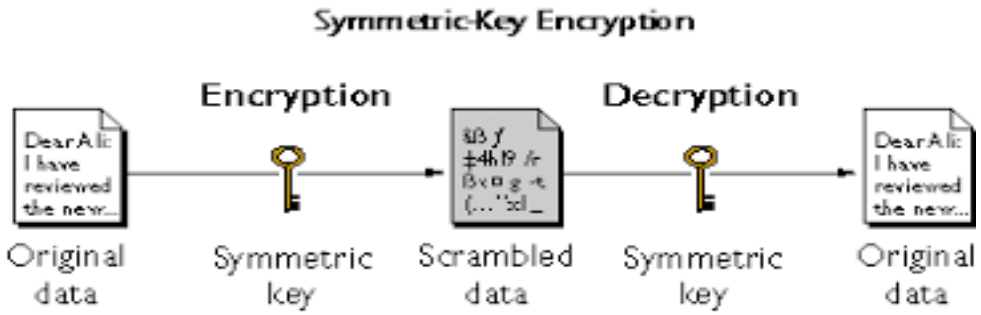

Figure 2.20 : cryptage symétrique

✓ **Asymétrique**

Un algorithme asymétrique est un algorithme à clé publique. Au lieu d'utiliser la même clé pour crypter et décrypter, nous utilisons deux clés différentes qui fonctionnent mathématiquement ensemble comme une paire. Appelons ces clés la clé publique et la clé privée.

Des exemples d'algorithmes asymétriques sont les suivants:

RSA, DH, ELGAMAL, DSA, ECC. [7]

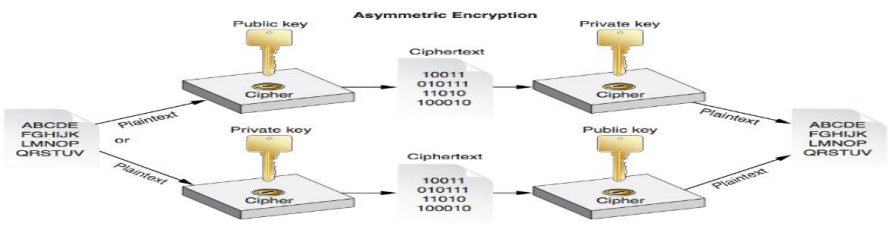

Figure 2.21 : cryptage asymétrique

2.9.2.4.4Hachage

Le hachage est une méthode utilisée pour vérifier l'intégrité des données.

Une fonction de hachage cryptographique est un processus qui prend un bloc de données et crée une petite valeur de hachage de taille fixe. C'est une fonction unidirectionnelle, ce qui signifie que si deux ordinateurs différents prennent les mêmes données et exécutent la même fonction de hachage, ils doivent obtenir la même valeur de hachage de taille fixe (par exemple, un hachage de 12 bits). (L'algorithme de résumé de message 5 [MD5])

C'est ce qu'on appelle la résistance aux collisions. Le résultat du hachage est une petite chaîne de données de longueur fixe, parfois appelée digest, digestion de message ou simplement hachage. [17]

2.9.2.4.5Signatures numériques

Lorsque vous signez quelque chose, cela représente souvent un engagement à suivre, ou du moins à prouver que vous êtes ce que vous dites être. Dans le monde de la cryptographie, une signature numérique offre trois avantages principaux:

*Authentification .

*Intégrité des données.

*Non-répudiation.

2.9.2.4.6Protocoles de cryptage de nouvelle génération [23]

L'industrie est toujours à la recherche de nouveaux algorithmes de chiffrement, d'authentification, de signature numérique et d'échange de clés pour répondre aux exigences de sécurité et de performance croissantes.

- ✓ La cryptographie à courbe elliptique (ECC, Elliptic Curve Cryptography) remplace la signatures RSA par l'algorithme ECDSA et remplace l'échange de clés DH par ECDH. ECDSA est une variante de la courbe elliptique de l'algorithme DSA, qui est une norme depuis 1994. Le nouvel échange de clés utilise DH avec des courbes P-256 et P-384.
- ✓ AES en mode Galois / Counter (GCM) de fonctionnement.
- ✓ Algorithme de signature numérique ECC.

✓ IPSEC

IP sec est un ensemble de protocoles et d'algorithmes utilisés pour protéger les paquets IP au niveau de la couche 3. IP sec offre les principaux avantages de la confidentialité grâce au chiffrement, à l'intégrité des données via le hachage et le HMAC, et à l'authentification à l'aide de signatures numériques ou à l'aide d'une clé pré-partagée (PSK). IP sec fournit également un support antireplay.

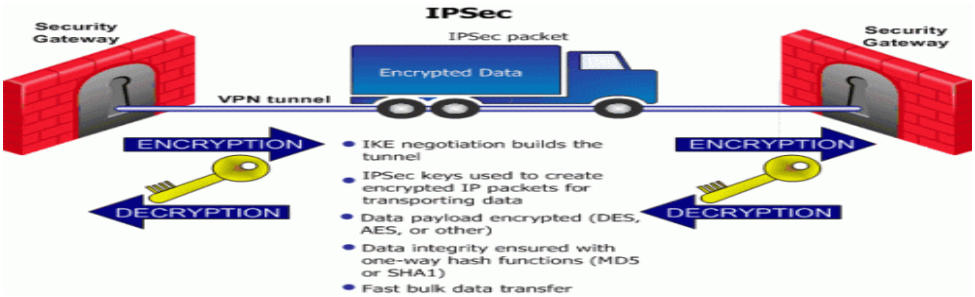

Figure 2.22 : crypto avec IP sec

✓ **SSL**

La transmission d'informations sur un réseau public doit être sécurisée par chiffrement pour empêcher tout accès non autorisé à ces données.

Pour utiliser SSL l'utilisateur se connecte à un serveur SSL ce qui est une façon élégante de dire un serveur Web qui prend en charge SSL en utilisant HTTPS plutôt que HTTP. Un moyen facile de se rappeler est que le S signifie sécurisé.

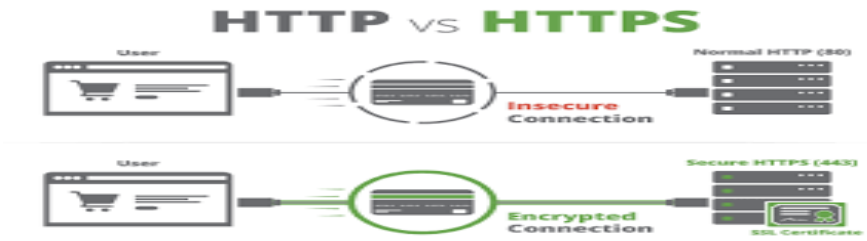

Figure 2.23 : le Protocol SSL.

2.9.2.5 VLAN

Un réseau local virtuel (VLAN) est un autre nom pour un domaine de diffusion de couche 2. Les VLAN sont contrôlés par le commutateur. Le commutateur contrôle également les ports

associés aux VLAN. Si les commutateurs sont dans leur configuration par défaut tous les ports par défaut sont affectés au VLAN 1, ce qui signifie que tous les périphériques y compris les deux utilisateurs et le routeur, se trouvent tous dans le même domaine de diffusion ou VLAN.

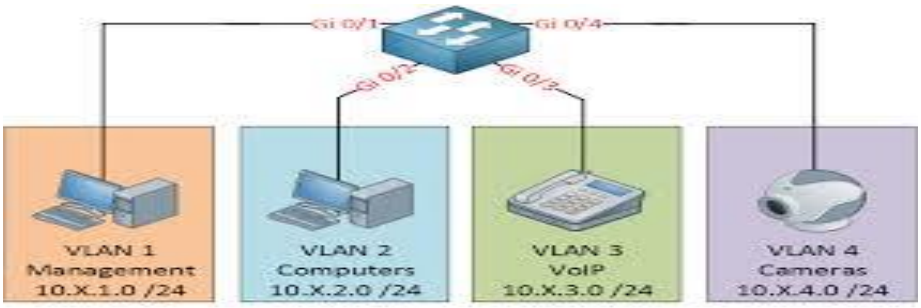

Figure 2.24 : les vlans.

2.9.2.6 Firewall

Un firewall ou pare-feu est un dispositif physique (matériel) ou logique (logiciel) servant de système de protection pour les ordinateurs domestiques. Il peut également servir d'interface entre un ou plusieurs réseaux d'entreprise afin de contrôler et éventuellement bloquer la circulation des données en analysant les informations contenues dans les flux de données (cloisonnement réseau). C'est –à-dire il interdit ou il autorise divers flux rentrants et sortants.

Figure 2.25 : Le Firewall.

2.9.2.7 Zone Based Firewalls

Cisco a implémenté un ensemble de fonctions de pare-feu avec état dans le logiciel Cisco IOS appelé pare-feu à zone (ZBF). ZBF a un prédécesseur appelé le contrôle d'accès basé sur le contexte (CBAC), qui a fourni des fonctionnalités de pare-feu de base dans le logiciel Cisco IOS. ZBF permet à l'administrateur de configurer des stratégies de pare-feu plus granulaires et introduit une stratégie de refus par défaut qui interdit le trafic entre les zones de sécurité du pare-feu jusqu'à ce qu'une stratégie explicite soit configurée.

2.9.2.8 IPS/IDS

Les systèmes de détection d'intrusion (IDS) et de prévention des intrusions (IPS) font partie de nombreux systèmes utilisés dans le cadre d'une approche de défense en profondeur pour protéger le réseau contre le trafic malveillant.

Un capteur est un périphérique qui examine le trafic sur le réseau puis prend une décision basée sur un ensemble de règles pour indiquer si ce trafic est correct ou s'il est malveillant d'une manière ou d'une autre. Parce que ce sont des systèmes agissant sur la base de règles configurées, aucun système n'est jamais parfait à 100%. Cependant, l'objectif est le même: réduire le risque de trafic malveillant, même s'il ne peut être complètement éliminé. [19]

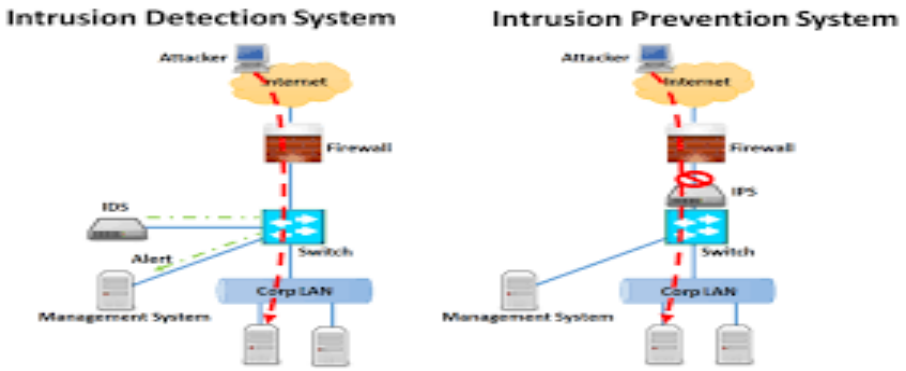

Figure 2.26 : IPS/IDS

2.10Conclusion

Ces menaces ont pris l'ampleur dans le monde d'aujourd'hui. Si une entreprise n'adapte pas une politique de sécurité pour protéger ces informations à l'intérieur et à l'extérieure et réduire les risques qu'elle peut atteindre son système d'information. Celle-ci ne sera pas une entreprise fiable et de confiance, elle peut perdre ces clients facilement.

L'établissement d'une politique de sécurité par les entreprises qui offrent des services de système d'information. Elles leurs obligent d'être à l'épanouissement des nouvelles mécanismes et mesures de sécurité qui nécessitent une amélioration et un renouvellement a sa politique de sécurité toutes en respectant certaines normes mondiales dans le domaine de sécurité des systèmes d'informations afin d'obtenir un certificat par laquelle l'entreprise est identifier comme entreprise de confiance.

Chapitre 3

Conception
Et
Implémentation

3.1 Introduction

De nos jours toutes les entreprises possèdent un réseau local accès à Internet afin d'accéder à des informations disponibles sur le réseau pour communiquer avec l'extérieur. Cette ouverture vers l'extérieur est indispensable et dangereuse en même temps. Ouvrir l'entreprise vers le monde signifie aussi laisser place ouverte aux étrangers pour essayer de pénétrer le réseau local de l'entreprise.

Et pour parer à ces attaques une architecture sécurisée est nécessaire. Pour cela le cœur d'une telle architecture est basée sur un firewall et de mieux un firewall matériel qui propose un véritable contrôle sur le trafic réseau de l'entreprise.

Il permet d'analyser, sécuriser et de gérer le trafic réseau et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu et sans l'encombrer avec des activités inutiles et d'empêcher une personne sans autorisation d'accéder à ce réseau de données.

Dans ce chapitre définissons la conception du projet pour donner un bon architecteur de sécurisation. Elle se compose de trois parties.

Partie confiante, partie non confiante et partie des serveurs dans les zones DMZ (Zone Démilitarisée) tout en plaçant le firewall au milieu.

La première étape présente le firewall et ces principales caractéristiques.

Le travail de l'implémentation basant sur un firewall matériel dans un réseau d'entreprise est de configurer (firewall). Afin de montrer l'importance de ces éléments dans l'étude d'un cas pour autoriser ou bloquer un trafic ou plusieurs trafics aux utilisateurs par ACL et défini le niveau de sécurité (Security Levels) afin de connecter à l'internet.

3.2Conception

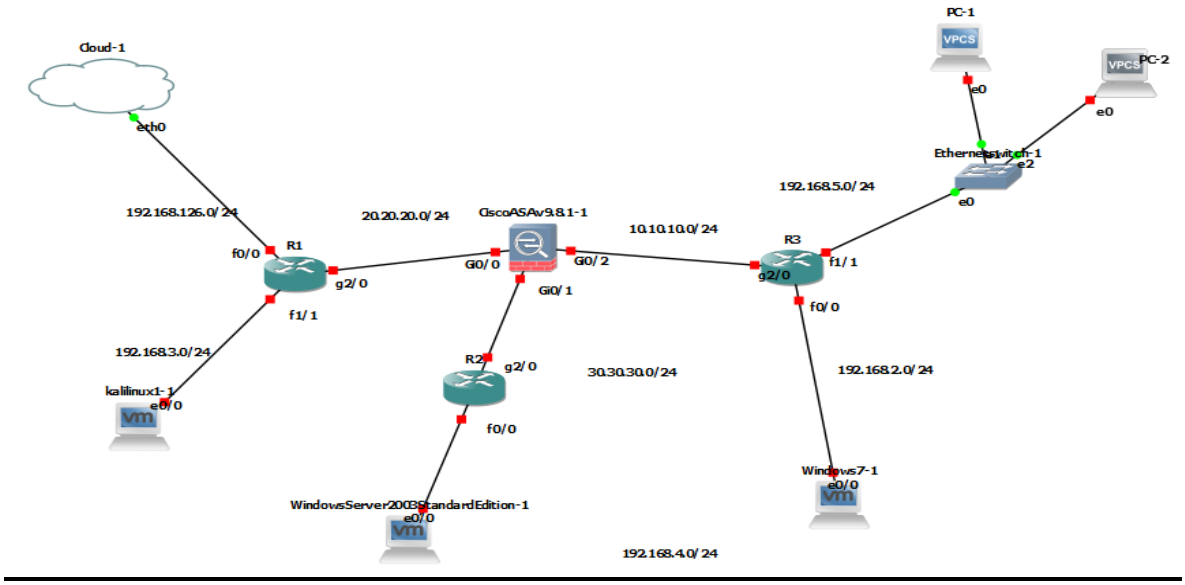

Figure 3.1 : lab. de projet.

Le but ce projet est d'identifier les différents éléments pour une bonne sécurisation du réseau.

3.2.1 Les éléments utilisés pour l'étude se traduit comme suit

- Un système d'exploitation Windows 7.
- Installation logiciel GNS3 possède une forte capacité et apte à recevoir plusieurs éléments de réseau (routeur, switch, firewall, etc.) est qui communique avec le monde extérieur.
- VMware Workstation fonctionne avec Virtual et relie avec la carte réseau physique.

3.2.2 Le réseau se comporte de 3 zones

1-zone 01 confiante : présente le réseau interne de l'entreprise ainsi que son matériel et les fichiers importants.

2-zone 02 non confiante : présente le réseau externe qui contient des éléments dangereux pouvant défecter le réseau interne de l'entreprise par (virus, malware…etc.)

3-zone 03 dmz : présente le réseau qui contient quelques serveurs de l'entreprise pouvant laisser le monde extérieur à accéder au niveau des mêmes serveurs.

3.2.3 Les composants de réseaux

- Réseau interne se compose :
  - ✓ D'un routeur qui route le trafic à autres réseaux.
  - ✓ Un switch pour relier les hots.
  - ✓ PC pour la connexion.
- Réseau externe se compose : (routeur, réseaux internet et pc).
- Réseau dmz se compose : (routeur, serveur).

Pour assurer la sécurité du réseau et le filtrage des données un pare-feu doit être configuré avec une bonne politique de configuration pour la gestion et la protection du réseau. Pour cela nous définissons le fonctionnement de base d'un firewall et ses principales caractéristiques.

3.3 Définition de Firewall

Un pare-feu est un concept qui peut être implémenté par un seul périphérique, un groupe de périphériques ou même simplement un logiciel s'exécutant sur un périphérique tel qu'un hôte ou un serveur.

La fonction d'un pare-feu est principalement de refuser aux trafic indésirable de traverser la frontière du pare-feu pour le trafic réseau.

Cela signifie qu'un pare-feu dans sa forme de base pourrait être implémenté par ce qui suit:

- **Un routeur**

Ou un autre périphérique de transfert de couche 3 disposant d'une liste d'accès ou d'une autre méthode utilisée pour filtrer le trafic qui tente de passer entre deux de ses interfaces. C'est la principale méthode implémentée par un routeur IOS (utilisant des fonctions de pare-feu) ou par le pare-feu de l'Appliance de sécurité adaptative (ASA).

- **Un commutateur**

Qui a deux LAN virtuels (VLAN) sans aucun routage entre eux, ce qui permettrait de garder le trafic séparé des deux réseaux différents (en ne pouvant pas avoir de communications inter-VLAN) .

- **Hôtes ou serveurs**

Qui exécutent un logiciel qui empêche le traitement de certains types de trafic reçu et qui contrôle le trafic pouvant être envoyé. Ceci est un exemple de pare-feu logiciel.

3.4 Objectifs d'un bon pare-feu

- **Il doit résister aux attaques**

Si un pare-feu peut être abattu ou compromis le point où il permet l'accès non désiré, il échoue donc à mettre en œuvre la politique correctement. Si le pare-feu est victime d'une attaque par déni de service (DoS), au point où il ne peut pas fournir un accès normal aux utilisateurs c'est également un problème. S'il existe une vulnérabilité qu'un attaquant peut exploiter avec un exploit permettant ainsi à l'attaquant de modifier la configuration du pare-feu cela est également un problème. [20]

- **Le trafic entre les réseaux doit être forcé à travers le pare-feu**

Si plusieurs chemins existent entre le réseau A et le réseau B et un pare-feu contrôle le trafic pour ces connexions mais s'il existe des chemins alternatifs le trafic malveillant a le potentiel d'éviter le pare-feu.

Donc s'il y a plusieurs chemins chacun de ces chemins devrait avoir la même politique de pare-feu et très probablement aura la même méthodologie de pare-feu à chaque point.[20]

3.5 Les avantages de pare-feu

Les entreprises font souvent un investissement important dans la sécurité y compris les fonds qu'elles dépensent pour les pare-feu.

Certains des éléments qu'un pare-feu peut aider à protéger contre :

3.5.1 Exposition de systèmes sensibles à des individus non-fiables

En masquant la plupart des fonctionnalités d'un hôte ou d'un périphérique réseau et en ne permettant que la connectivité minimale requise pour ce système donné le pare-feu réduit l'exposition de ce système. Un exemple permet uniquement le trafic Web à une adresse IP spécifique d'un serveur Web sur la zone démilitarisée (DMZ).

Même si ce serveur web a d'autres services sont en cours d'exécution. Ces services ne seront pas accessibles aux utilisateurs qui tentent d'accéder à ces services via le pare-feu.[21]

3.5.2 Exploitation des failles de protocole

Le pare-feu configure et inspecte les protocoles afin d'assurer la conformité aux normes de ce protocole sur plusieurs couches de la pile de protocoles.

Peut également contrôler le temps qu'il faudra pour une séquence de connexion normale avant de dire que c'est suffisant.

3.5.3 Utilisateurs non autorisés

En utilisant des méthodes d'authentification un pare-feu peut contrôler le trafic de l'utilisateur autorisé via le pare-feu et être configuré pour bloquer tout autre trafic en fonction de la stratégie. Par exemple un pare-feu pourrait tirer parti des services d'authentification, d'autorisation et de comptabilité (AAA) en utilisant sa configuration locale ou un contrôle d'accès Serveur (ACS).[18]

3.5.4 Données malveillantes

Un pare-feu peut détecter et bloquer les données malveillantes ce qui arrêterait le trafic d'atteindre la destination prévue. Cette fonction pourrait également être fourni par un système de prévention des intrusions (IPS).

3.6Limitations potentielles du pare-feu

Pourrions espérer qu'en achetant un pare-feu et en le mettant en place tous nos problèmes de sécurité pourraient être enrayés. Il doit être compris que le fait d'avoir un pare-feu et de mettre en œuvre correctement les politiques pour une organisation sont des mesures d'atténuation pour réduire le risque mais n'éliminent pas complètement le risque. En outre les pare-feu ont certaines limites:

3.6.1 Les erreurs de configuration ont des conséquences graves

Le travail du pare-feu consiste à implémenter une politique en fonction d'un pare-feu spécifiques il Dispose de moyens spécifiques pour implémenter des fonctionnalités telles que les listes de contrôle d'accès (ACL), l'inspection des paquets, la traduction d'adresses réseau (NAT), l'authentification etc….

Si les règles de pare-feu ne sont pas correctement implémentées il se peut que l'implémentation de la stratégie ne soit pas exécutée comme prévu. Il faut un bon équipement technique et une bonne configuration technique pour pouvoir mettre en place une politique efficace

3.6.2 Latence ajoutée par le pare-feu

Si un pare-feu est soumis à un énorme travail d'analyse de tout le trafic, l'analyse peut prendre quelques millisecondes ou plus par paquet et par conséquent un léger retard peut être ajouté au temps de livraison du trafic réseau global.

3.7Caractéristiques de pare-feu

Les pare-feu basés sur le réseau fournissent des fonctionnalités clés utilisées pour la sécurité du périmètre. La tâche principale d'un pare-feu réseau est de refuser ou d'autoriser le trafic qui tente d'entrer ou de quitter le réseau sur la base de règles et de règles explicites préconfigurées.

Les processus utilisés pour autoriser ou bloquer le trafic peuvent inclure les éléments suivants :

- Des techniques simples de filtrage de paquets
- Serveurs proxy (également connus sous le nom de passerelle de couche d'application
- NAT
- Pare-feu d'inspection stateful
- Pare-feu transparent
- Contexte de nouvelle génération et pare-feu sensibles aux applications

3.7.1 Filtrage de paquets statique (stateless)

Le filtrage de paquets statiques est basé sur les couches 3 et 4 du modèle OSI. L'un des défis du filtrage statique des paquets est que l'administrateur doit savoir exactement quel trafic doit être autorisé via le pare-feu. Ce qui peut être difficile si de nombreux utilisateurs ont besoin d'accéder à de nombreux serveurs.

- **Avantages et inconvénients des filtres de paquets**
- **Les avantages**
  - ✓ Basé sur des ensembles simples d'autorisations ou de refus d'entrées
  - ✓ Avoir un impact minimal sur les performances du réseau

- ✓ Sont simples à mettre en œuvre
- ✓ Configurable sur la plupart des routeurs
- ✓ Peut effectuer de nombreux besoins de filtrage de base sans avoir à payer le coût d'un pare-feu haut de gamme.

- **Les inconvénients**
  - ✓ Sensible à l'usurpation IP. Si la liste de contrôle d'accès autorise le trafic à partir d'une adresse IP spécifique et si quelqu'un usurpe l'adresse IP source l'ACL autorise ce paquet individuel.
  - ✓ Ne filtre pas les paquets fragmentés avec la même précision que les paquets non fragmentés.
  - ✓ Les ACL extrêmement longs sont difficiles à maintenir.
  - ✓ Stateless (ne conserve pas les informations de session pour les flux de trafic actuels passant par le routeur).
  - ✓ Certaines applications sautent et utilisent de nombreux ports dont certains sont dynamiques. Une ACL statique peut être nécessaire pour ouvrir une très large gamme de ports afin de prendre en charge une application qui peut n'utiliser que quelques-uns d'entre eux.

3.7.2 Filtrage par paquets avec état (stateful)

Avec un dispositif de filtrage de paquets avec état, pour les clients situés à l'intérieur du réseau d'entreprise alors qu'ils tentent d'accéder aux ressources sur les réseaux publics externes. Les pare-feu examinent l'adresse IP source, l'adresse IP de destination, les ports utilisés et d'autres couches d'informations et se souviennent de cette information dans une base de données avec état sur le pare-feu. Il est appelé stateful parce que le pare-feu se souvient de l'état de la session.[21]

- **Avantages et inconvénients du filtrage de paquets avec état**

- **Les avantages**
  - ✓ Peut être utilisé comme principal moyen de défense en filtrant le trafic indésirable ou inattendu.
  - ✓ Peut-être implémenté sur les routeurs et les firewalls dédiés.
  - ✓ Dynamique par rapport au filtrage de paquets statique.
  - ✓ Fournit une défense contre l'usurpation d'identité et les attaques par déni de service (DoS). [21]

- **Les inconvénients**
  - ✓ Peut ne pas être en mesure d'identifier ou d'empêcher une attaque de couche application.
  - ✓ Tous les protocoles ne contiennent pas d'informations d'état étroitement contrôlées, telles que le protocole UDP (User Datagramme Protocol) et le protocole ICMP (Internet Control Message Protocol).
  - ✓ Certaines applications peuvent ouvrir dynamiquement de nouveaux ports à partir du serveur.
  - ✓ La technologie Stateful, en elle-même ne prend pas en charge l'authentification de l'utilisateur.

3.7.3 Inspection d'application

Un pare-feu d'inspection des applications peut analyser et vérifier les protocoles jusqu'au niveau 7 du modèle de référence OSI mais n'agit pas en tant que proxy entre le client et le serveur auquel le client accède.

3.7.4 Pare-feu transparents

Un pare-feu transparent est plus sur la façon dont nous injectons le pare-feu dans le réseau. Par opposition aux technologies qu'il utilise pour le filtrage Un pare-feu transparent peut utiliser le filtrage basé sur les paquets, le filtrage avec état, l'inspection des applications comme nous l'avons vu plus haut mais la grande différence avec les pare-feu transparents est qu'ils sont implémentés au niveau 2.

3.7.5 Firewalls de nouvelle génération

Les firewalls de prochaine génération (NGFW) offrent des services de sécurité axés sur les menaces permettant une protection plus complète contre les menaces connues et avancées y compris la protection contre les attaques de logiciels malveillants ciblées et persistantes. Un exemple d'un NGFW est le Cisco ASA avec les services de FirePOWER. Il combine le pare-feu ASA classique avec la prévention des menaces Sourcefire et la protection avancée contre les logiciels malveillants dans un seul appareil.

L'objectif de NGFW est de maintenir une visibilité complète sur les utilisateurs. Les appareils mobiles, les applications côté client, les communications machine virtuelle (VM) à VM, les vulnérabilités, les menaces et les localisateurs de ressources uniformes (URL).

3.8 Network Address Translation

NAT (Translation d'adresse réseau) est un mécanisme permettant de conserver les adresses IP enregistrées dans des réseaux de grande taille et de simplifier la gestion de l'adressage IP.

L'adresse IP privée (réseau interne) est traduite en une adresse IP publique routable. Cela permet de transporter le paquet sur des réseaux externes publics tels qu'Internet. Donc le NAT permet de masquer les adresses privées des réseaux locaux derrière une adresse publique. [5]

3.8.1 Les différents concepts de NAT [5]

- **NAT statique (SNAT)**

SNAT (Static Network Address Translation) est l'association d'une adresse IP interne. Cette association est effectuée par le pare-feu en remplaçant dans les paquets l'adresse IP interne par l'adresse externe. Ainsi le pare-feu va faire cette modification dans l'entête IP du paquet.

- **NAT dynamique (DNAT)**

Le NAT dynamique est l'association d'une adresse publique à plusieurs adresses IP privé. Cette stratégie souvent appelée en anglais "IP masquerading" permet à plusieurs ordinateurs d'un réseau local d'accéder à Internet via une seule adresse IP publique.

3.8.2 Terminologie du NAT [5]

Distinction entre interne et externe :

- **Adresses internes :** Sont celles qui sont maîtrisées par l'administrateur du réseau d'extrémité.
- **Adresses externes :** Sont celles dont on n'a pas la maîtrise et qui font partie d'un réseau public tel que l'Internet.

Distinction entre adresses locales et globales :

- **Adresses locales :** Sont celles qui ne sont pas nécessairement des adresses légitimes.
- **Adresses globales :** Sont celles qui sont routables et qui ont une signification à portée globale.

3.9 Contrôle d'accès [21]

Le firewall défini un contrôle d'accès par une liste qui contienne des adresses IP ou des numéros de ports autorisés ou interdits par le dispositif de filtrage. Les ACL (Access Control List, ou en français liste de contrôle d'accès) sont divisés en deux grandes catégories :

- **ACL standard**

Ne peut contrôler que deux ensembles :

- ✓ L'adresse IP source avec le masque.
- ✓ Une partie de l'adresse IP destination avec le masque.

- **ACL étendue**

Peut contrôler l'adresse IP de source et destination autoriser ou bloquer avec type de protocole (TCP, UDP, ICMP, IP) et les numéros de port de l'application choisi.

3.10 Etude d'un cas

Pour définir dans ce Lab la conception de projet par la configuration de base d'un firewall dans un réseau d'entreprise et pour cela la première étape présente le Cisco firewall ASA et ces principales caractéristiques.

Faire une politique de sécurité par les ACLs, niveau de sécurité (sécurité Levels), le NAT, sécurité de routeur par psydoname et mot de passe.

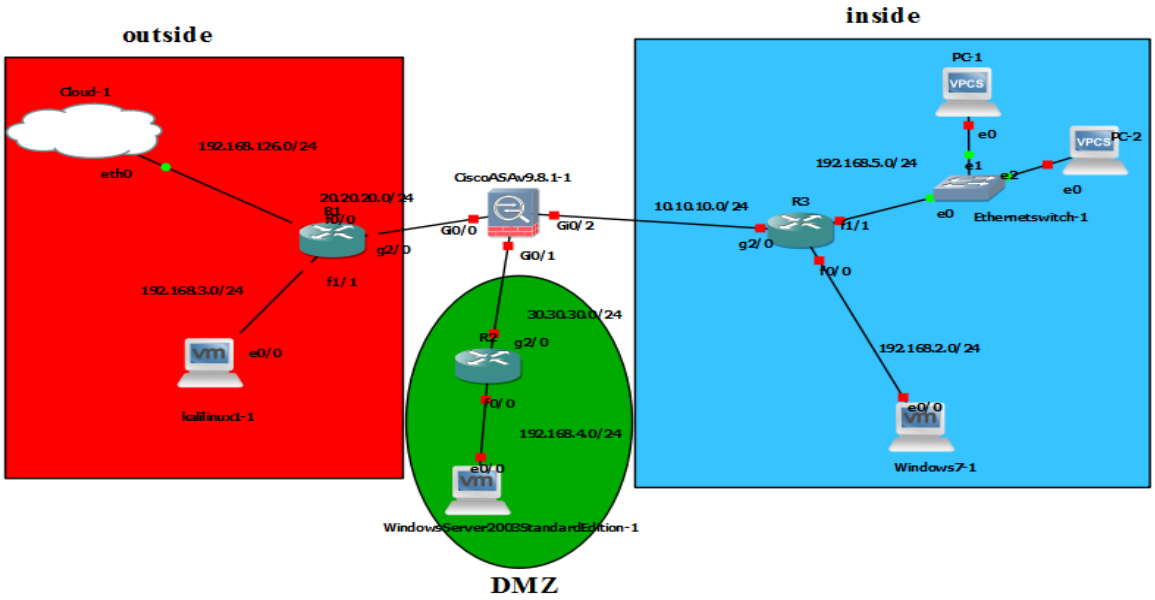

Figure 3.2 : Lab de projet.

3.10.1 Outils utilisés

- ✓ Firewall ASA.
- ✓ (03) les routeurs pour le routage.
- ✓ Cloud pour partager l'internet.
- ✓ Switch pour relier plusieurs hôtes.
- ✓ (04) PC Virtual avec des système exploitation déférant.
- ✓ GNS3 logiciel de réseaux pour exécuté l'étude.
- ✓ VMware pour communiquer avec carte réseaux physiques.
- ✓ ASDM pour configurer le firewall ASA par interface graphique.
- ✓ Securecrt pour transfert la configuration au matériel.
- ✓ Wireshark pour faire des captures sur l'interface.

3.10.2 Cisco ASA firewall

Le Cisco ASA (Appareils de Sécurité Adaptative) est un Serveur de sécurité multifonctions de nouvelle génération fais partie de la Gamme Cisco ASA 5500. Il protège les réseaux de grands tailles contre les attaques de réseau, les menaces applicatives et sécurise les échanges inter-sites et nomade-à-site. La très haute performance de l'ASA est particulièrement indiquée pour les réseaux qui transportent de la voix et de la vidéo. [18]

3.10.2.1 Cisco ASA Caractéristiques

- ✓ Moteur de filtrage de paquets avec état.
- ✓ Inspection et contrôle des applications.
- ✓ Contrôle d'accès basé sur l'utilisateur.
- ✓ Audit de session.
- ✓ Modules de services de sécurité.
- ✓ Filtrage du trafic Botnet basé sur la réputation.
- ✓ Filtrage d'URL par catégorie.
- ✓ Proxy de communications unifiées cryptographiques (UC).
- ✓ Prévention du déni de service.
- ✓ Corrélation de trafic.
- ✓ VPN d'accès à distance.
- ✓ VPN de site à site.
- ✓ Interfaces redondantes.
- ✓ La virtualisation du trafic et des règles.
- ✓ Fonctionnalité de routage IP riche.
- ✓ Puissante traduction d'adresses réseau (NAT).
- ✓ Opération transparente (pontée).
- ✓ DHCP intégré, DDNS et PPPoE.
- ✓ Prise en charge d'IPv6.
- ✓ Prise en charge de la multidiffusion IP.
- ✓ Contrôle de gestion et protocoles.
- ✓ Gestion de logiciel simple.
- ✓ Flexibilité de la configuration et évolutivité.
- ✓ Cisco Security Management Suite. [19]

3.10.2.2 Modèle Cisco ASA

- **ASA 5505**

L'ASA 5505 est le plus petit modèle de la gamme ASA tant en termes de taille physique que de performance. Il est conçu pour les petits bureaux et les bureaux à domicile (SOHO). Pour une entreprise plus importante l'ASA 5505 est fréquemment utilisé pour prendre en charge les télétravailleurs dans des endroits éloignés.

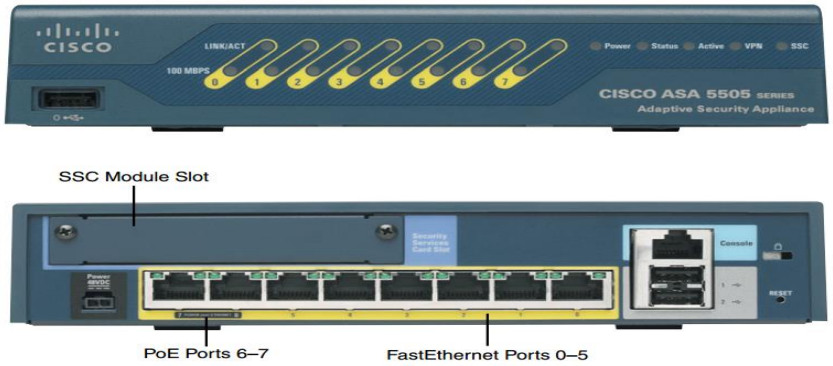

Figure 3.3 : Cisco ASA 5505.

- **ASA 5510,5520 et 5540**

Les modèles ASA 5510, 5520 et 5540 utilisent tous un châssis commun et ont des indicateurs identiques sur le panneau avant et des connexions matérielles. Les modèles différents toutefois par leurs performances de sécurité.

L'ASA 5510 est conçu pour les petites et moyennes entreprises (PME) et les bureaux distants pour les grandes entreprises.

L'ASA 5520 convient aux moyennes entreprises. Tandis que l'ASA 5540 est plus adapté aux moyennes et grandes entreprises et aux réseaux de fournisseurs de services.

Les modèles ASA 5510, 5520 et 5540 ont un port AUX qui peut être utilisé pour la gestion hors bande via une connexion série asynchrone ou un modem. Ils ont également un port FastEthernet qui est désigné pour le trafic de gestion mais peut être reconfiguré pour le trafic de données normal si nécessaire.

Les châssis ASA 5510, 5520 et 5540 ont un emplacement SSM pouvant être rempli avec l'un des éléments suivants:

- ✓ SSM Gigabit Ethernet à quatre ports

- ✓ SSM avancé d'inspection et de prévention (AIP)
- ✓ SSM de sécurité et de contrôle du contenu (CSC). [20]

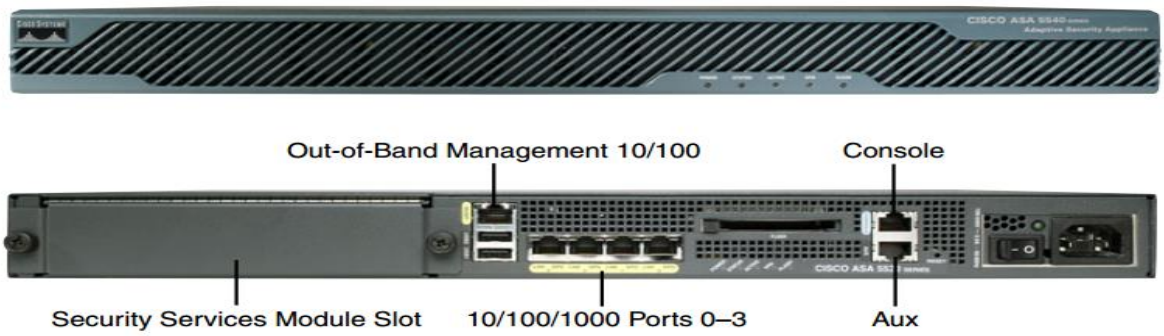

Figure 3.4 : Cisco ASA 5510.

- **ASA 5550**

L'ASA 5550 est conçu pour prendre en charge les grandes entreprises et les réseaux de fournisseurs de services.

L'ASA 5550 est identique aux modèles ASA 5510, 5520 et 5540. La différence la plus notable est que l'ASA 5550 dispose d'un module Gigabit Ethernet 4 ports fixe (4GE-SSM) dans l'emplacement SSM qui ne peut pas être supprimé ou modifié.

L'architecture ASA 5550 comporte deux groupes d'interfaces physiques qui se connectent à deux bus internes distincts. Les groupes d'interfaces sont appelés slot 0 et slot 1, correspondant au bus 0 et au bus 1. Le slot 0 est constitué de quatre ports Ethernet Gigabit Ethernet intégrés.

L'emplacement 1 se compose de quatre ports cuivre intégrés et de quatre ports Gigabit Ethernet SFP intégrés bien que seulement quatre des huit ports puissent être utilisés à tout moment. [19]

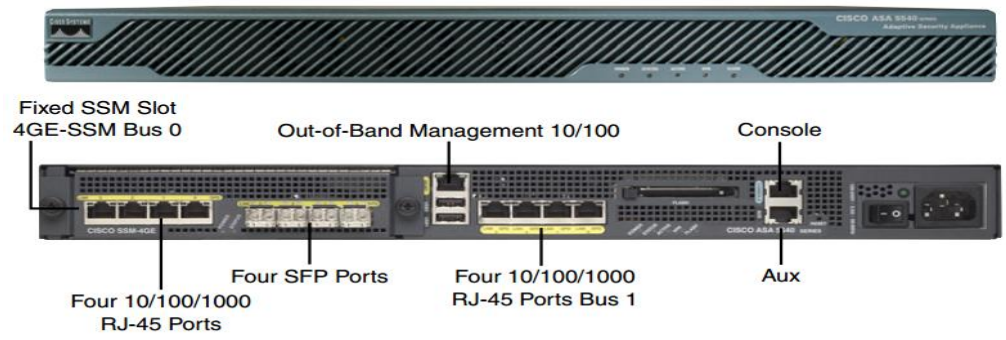

Figure 3.5 : Cisco ASA 5550.

- **ASA 5580**

L'ASA 5580 est un modèle performant de la famille conçu pour les grandes entreprises, les centres de données et les grands fournisseurs de services. Il peut prendre en charge jusqu'à 24 interfaces Ethernet Gigabit ou jusqu'à 12 interfaces Ethernet 10Gigabit. C'est l'un des deux modèles qui a un châssis plus grand qu'une unité de rack standard (RU).

L'ASA 5580 est disponible en deux modèles de performance: l'ASA 5580-20 (débit de 5 Gbit / s) et l'ASA 5580-40 (débit de 10 Gbit / s). Le châssis comprend deux ports Gigabit Ethernet 10/100/1000 intégrés normalement utilisés pour le trafic de gestion hors bande. Le système utilisé également deux alimentations redondantes.

Le châssis ASA 5580 dispose de neuf emplacements d'extension PCI Express au total. L'emplacement 1 est réservé à un module accélérateur cryptographique pour prendre en charge les opérations VPN hautes performances. [20]

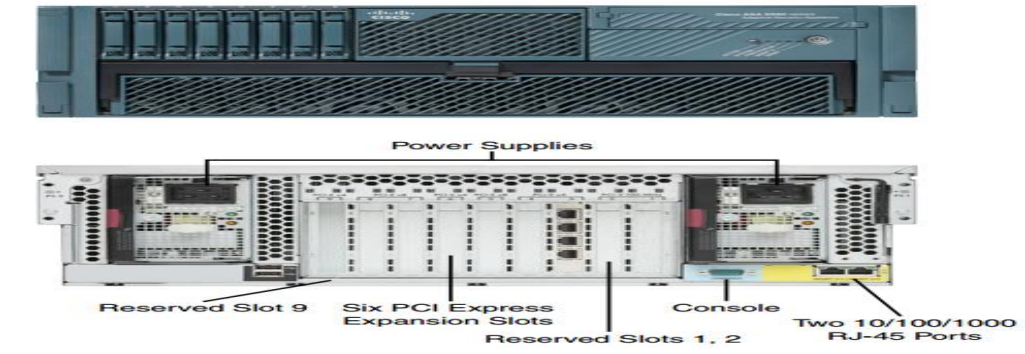

Figure 3.6 : Cisco ASA 5580.

- **Modules de services de sécurité [19]**

La plupart des modèles ASA peuvent accepter un module SSM (Security Services Module). Le SSM contient un matériel dédié pouvant décharger des fonctions spécialisées ou gourmandes en ressources processeur.

Cisco propose le SSM AIP (Advanced Inspection and Prévention), le SSM Content Security and Control (CSC) et le SSM Gigabit Ethernet (4GE) à 4 ports

- **SSM avancé d'inspection et de prévention (AIP)**

L'AIP-SSM exécute l'image du logiciel Cisco IPS et effectue des fonctions de prévention d'intrusion réseau en conjonction avec l'ASA. L'ASA peut mettre l'AIP-SSM en ligne où le trafic est redirigé en interne vers le module pour inspection et traitement avant d'être transmis. Sinon l'AIP-SSM peut fonctionner en mode espion où l'ASA copie le trafic vers le module au cours du transfert.

- **SSM de sécurité et de contrôle du contenu (CSC)**

Le CSC-SSM exécute un antivirus, un antispyware, un antispam, un antiphishing, un blocage de fichiers, un blocage et un filtrage d'URL complets ainsi qu'un filtrage de contenu en conjonction avec l'ASA. L'ASA redirige en interne le trafic via le CSC-SSM, qui exécute l'image logicielle Trend Micro InterScan pour Cisco CSC-SSM. Etant donné que de nombreuses fonctions du CSC-SSM atténuent une telle variété d'approches malveillantes il est communément appelé le module "Anti-X". Les trafics HTTP, FTP, SMTP et POP3 sont protégés par le CSC-SSM.

- **Port Gigabit Ethernet (4GE) SSM**

Le 4GE-SSM fournit quatre ports Ethernet Gigabit supplémentaires à un modèle ASA 5510, 5520 ou 5540. Bien que le module dispose de quatre ports RJ-45 cuivre 10/100/1000 et de quatre ports fibre optique SFP seuls quatre ports de tous types peuvent être utilisés à tout moment.

Figure 3.7 : Module Cisco ASA.

- **ASA 5585-X**

L'ASA 5585-X est le modèle le plus performant de la famille est conçu pour les grandes entreprises et les centres de données critiques. Il peut supporter jusqu'à 12 interfaces 10/100/1000 et 8 interfaces Ethernet 10Gigabit.

L'ASA 5585-X est disponible en quatre modèles de performance selon le processeur SSP (Security Services Processor) suivant: SSP-10 (débit de 3 Gbit / s), SSP-20 (débit de 7 Gbit / s), SSP -40 (débit de 12 Gbit / s), et le SSP-60 (débit de 20 Gbit / s). Chaque modèle nécessite 2 RU et utilise deux sources d'alimentation pour la redondance. [21]

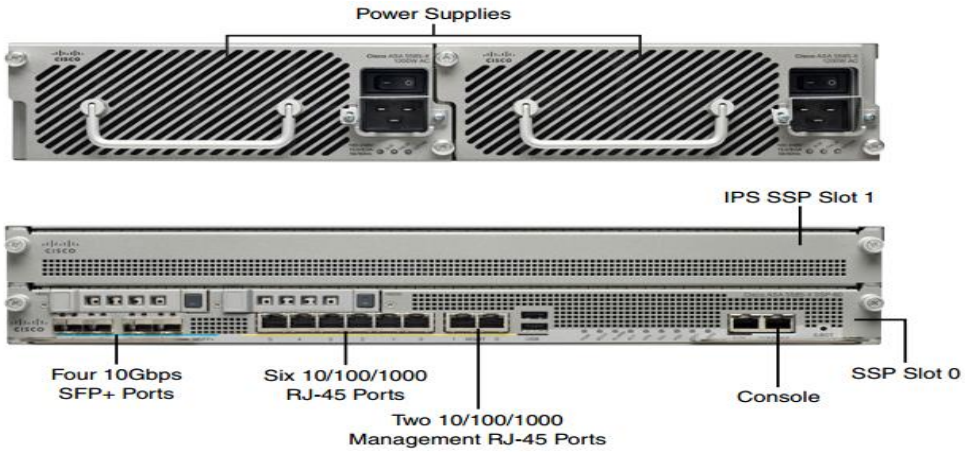

Figure 3.8 : Cisco ASA 5585 X.

3.10.2.3 Modes de base pour configurer Cisco ASA

- **Pour configurer les Appareils de Sécurité Adaptative Cisco a défini deux modes de base**

* le premier c'est le mode graphique appelé ASDM (Adaptive Security Device Manager)

* le deuxième par invite de commande CLI (Commande-Line Interface).

- **Le mode CLI**

Un interpréteur de commande c'est un programme généralement fait partie des composantes de base d'un système d'exploitation. Son rôle est de traiter les commandes tapées au clavier par l'utilisateur.

Ces commandes une fois interprétée auront pour effet de réaliser telles ou telles tâches d'administration ou bien de lancer l'exécution d'un logiciel.

- ✓ CLI par une connexion de console asynchrone.
- ✓ CLI par une session Telnet.
- ✓ CLI par Secure Shell (SSH) version 1.x ou 2.

- **Les types de mode configuration dans CLI**

Mode utilisateur-EXEC

Ciscoasa>

Mode Privileged-EXEC

ciscoasa> enable

Mot de passe: password

Ciscoasa #

Mode de configuration globale

Ciscoasa # configure terminal

Ciscoasa (config) #

Mode de configuration spécifique

Ciscoasa (config-if) #

- **Le mode interface graphique ASDM**

Les Cisco ASA Firewall sont livrés avec un logiciel d'administration graphique ASDM. Il est chargé de l'Appliance de sécurité puis utilisé pour configurer, surveiller et gérer l'appareil. Il permet de récupérer, modifier et administrer les politiques de sécurité ainsi que de faire du monitoring.

Figure 3.9 : fenêtre de ASDM.

3.10.3 Le routeur

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. Selon un ensemble de règles il y a habituellement confusion entre routeur et relais car dans les réseaux Ethernet les routeurs opèrent au niveau de la couche 3 du modèle OSI.

Figure 3.10 : Routeur Cisco.

3.10.4 Switch (commutateur)

Est un type de concentrateur réseau utilisé dans les topologies en étoile. La différence avec un HUB vient de la méthode de renvoi des données vers le destinataire. Dans le cas d'un hub les données sont transmises sur tous les ports. Le Switch garde en mémoire dans une table l'adresse du destinataire. Il décode au préalable le message pour l'envoyer uniquement sur ordinateur associé.

Figure 3.11 : Switch Cisco.

3.10.5 GNS3

GNS3 (Graphical Network Simulator) est un logiciel libre permettant l'émulation ou la simulation de réseaux informatiques.

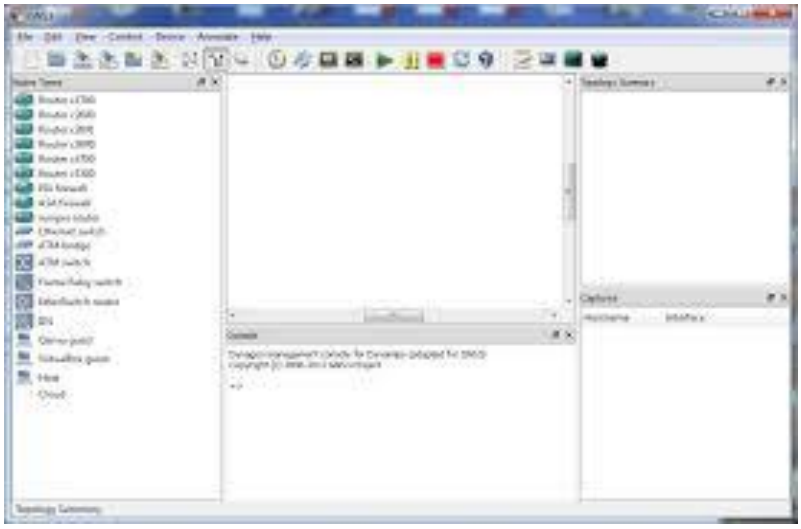

Figure 3.12 : Logiciel GNS3.

3.10.6 Vmware

C'est la version station de travail du logiciel. Elle permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux). Ceux-ci pouvant être reliés au réseau local avec une adresse IP différente tout en étant sur la même machine physique (machine existant réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps. La limite correspondant aux performances de l'ordinateur hôte, La version Linux présente l'avantage de pouvoir sauvegarder les fichiers de la machine virtuelle (* .vmsd) pendant son fonctionnement.

Figure 3.13 : Logiciel VMware Workstation.

3.10.7 Securecrt

SecureCRT combine une émulation de terminal à toute épreuve avec les options de chiffrement fort d'intégrité des données et d'authentification du protocole Secure Shell. SecureCRT fournit un accès distant sécurisé, un transfert de fichiers et un tunneling de données pour tous les membres de votre organisation.

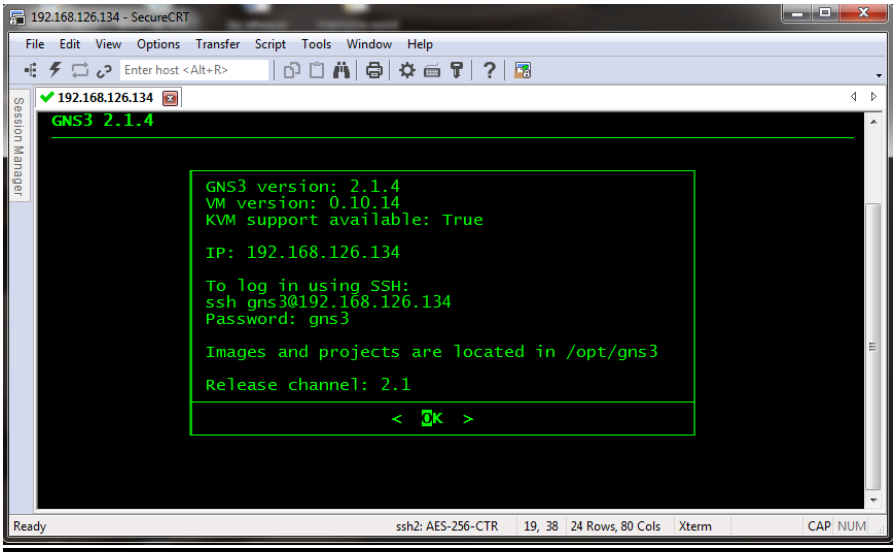

Figure 3.14 : Le terminal Securecrt.

3.10.8 Wireshark

Est un analyseur de paquets libre et gratuit. Il est utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie.

Wireshark utilise la bibliothèque logicielle GTK+ pour l'implémentation de son interface utilisateur et pcap pour la capture des paquets ; il fonctionne sur de nombreux environnements compatibles UNIX comme GNU/Linux, FreeBSD, NetBSD, OpenBSD ou Mac OSX, mais également sur Microsoft Windows. Il existe aussi entre autre une version en ligne de commande nommé TShark. Ces programmes sont distribués gratuitement sous la licence GNU General Public License.

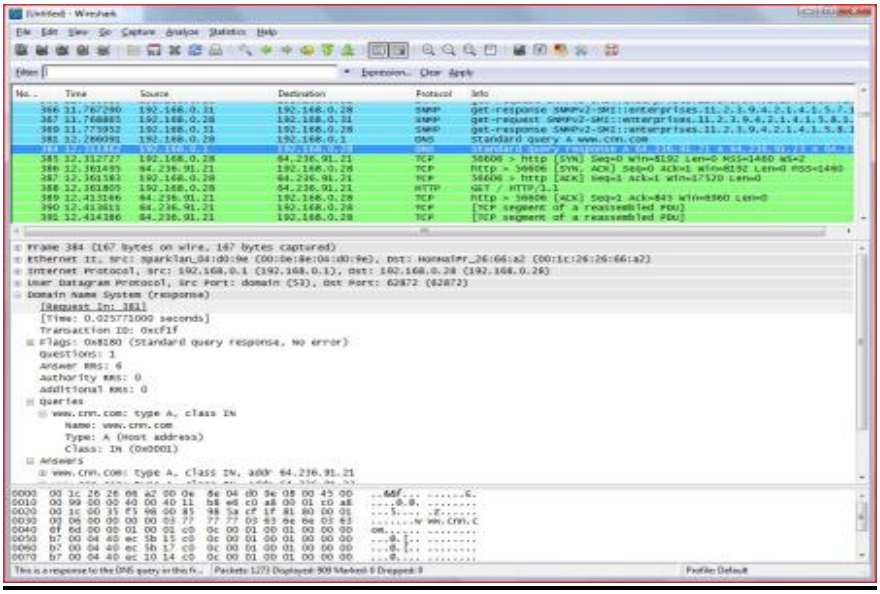

Figure 3.15 : logiciel Wireshark.

3.11 Implémentation

3.11.1 Introduction

Le travail de l'implémentation basant sur un firewall matériel dans un réseau d'entreprise est de configurer (firewall, routeurs) afin de montrer l'importance de ces éléments pour la sécurisation de réseau.

L'étude d'un cas : pour autoriser ou bloquer un trafic ou plusieurs trafics aux utilisateurs par ACL et défini le niveau de sécurité (Security Levels) afin de connecter à l'internet. Dans cette implémentation nous distinguons différents contextes de configuration Cisco ASA.

Notre approche de notre solution en fournissant toutes les étapes nécessaires pour contrôler le réseau interne et le filtrage des données permises ou interdites à travers le développement d'une liste spéciale d'utilisateurs.

3.11.2 Le processus se fait en plusieurs étapes

3.11.2.1 ETAPE 01

- ✓ Installation de logiciel GNS3 avec leur GNS3VM.
- ✓ Installation VMware Workstation.
- ✓ Installation le terminal Securecrt.

Relier entre eux.

3.11.2.2 ETAPE 02

3.11.2.2.1 Réalisation schéma lab.

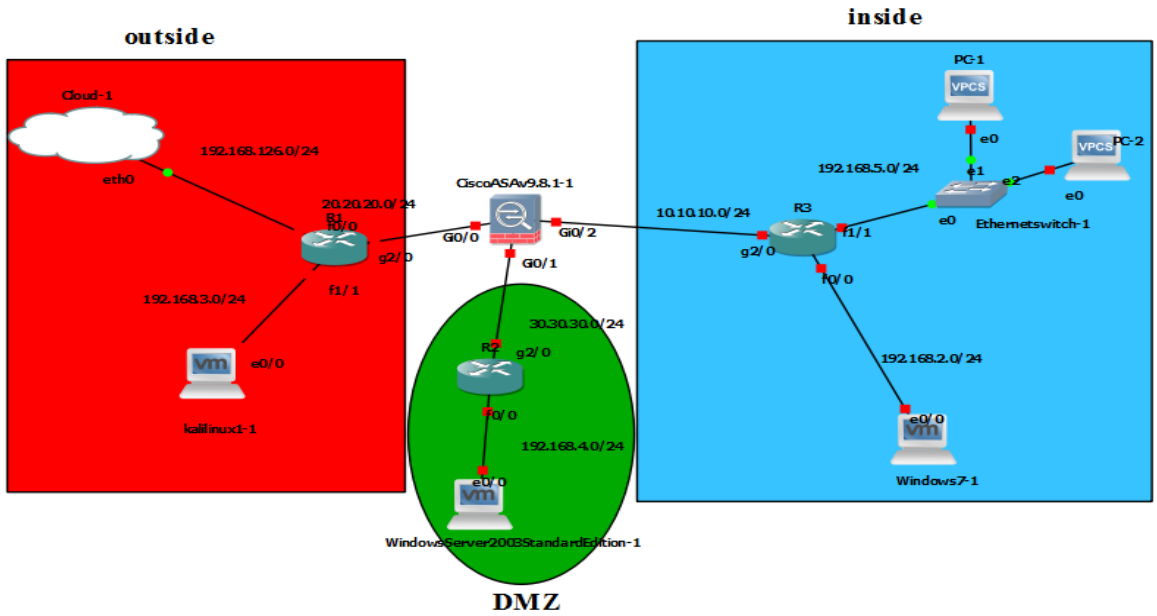

Figure 3.16 : Réalisation de lab

3.11.2.3 Etape 03

3.11.2.3.1 Configuration des interfaces

- **Configure Cisco ASAv**

Le branchement des routeurs avec le firewall ASAv configure les interfaces par consol en mode CLI avec l'ouverture de terminal Securecrt.

Le port console est un port de gestion qui fournit un accès hors bande ASAv. Il est utilisé pour la configuration initiale d'un firewall pour la surveillance et pour les procédures de reprise après sinistre.

3.11.2.3.2 Configuration des interfaces g0/0, g0/1, g0/2 avec leurs adresses et le niveau de sécurité et nom de chaque l'interface.

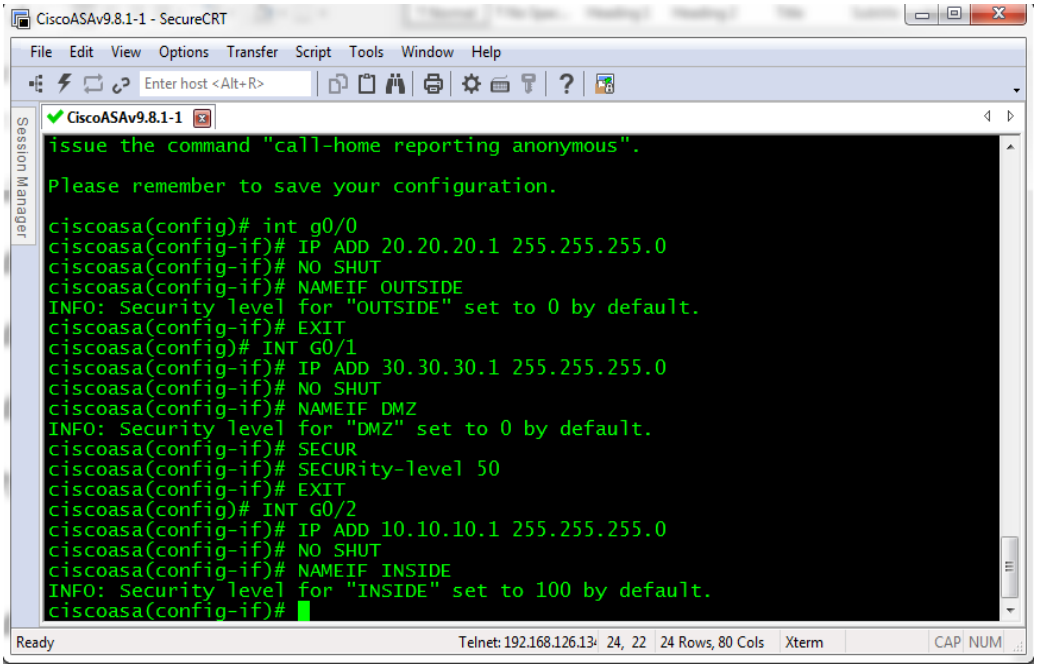

Figure 3.17 : Configuration des interfaces de ASA.

- **Configuration des interfaces de routeur 01dans la zone outside**

Après le branchement avec le firewall, le cloud et pc Configure les interfaces par le consol avec le terminale securecrt.

3.11.2.3.3 Configuration les interfaces g2/0, F0/0, F1/1avec leur adresses et le mask.

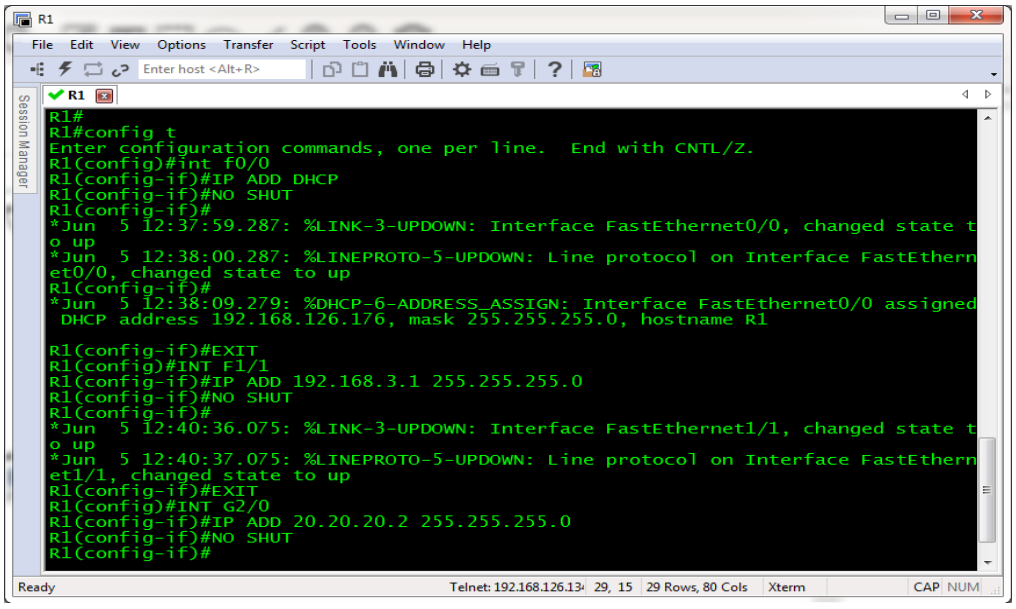

Figure 3.18 : Configuration des interfaces de routeur.

3.11.2.3.4 Tester la connectivité des interfaces de routeur 01 par le Ping avec (internet, firewall, pc).

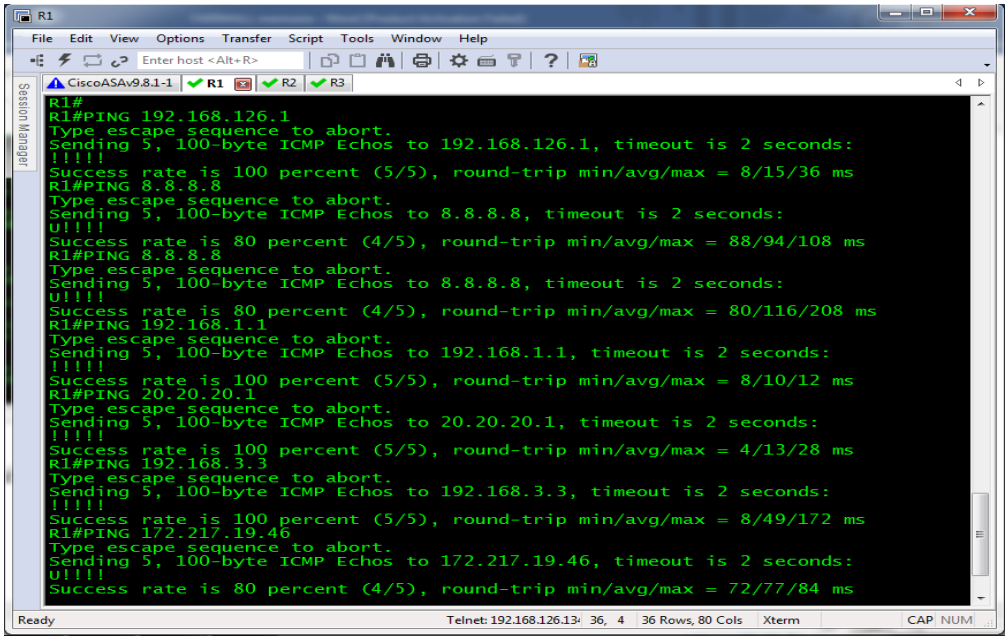

Figure 3.19 : Testez la connectivité des interfaces de routeur.

3.11.2.3.5 Testez la connectivité de pc kali linux vers l'internet

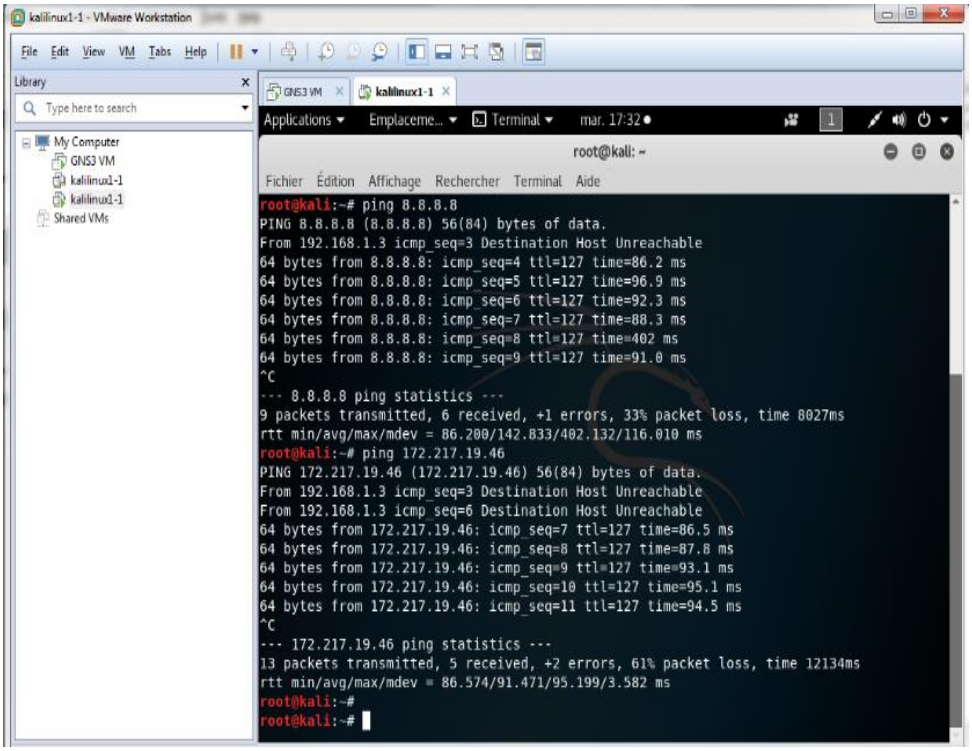

Figure 3.20 : Test la connectivité d'hôte.

3.11.2.3.6 Configuration les interfaces G2/0, F0/0 de routeur 02 dans la zone DMZ

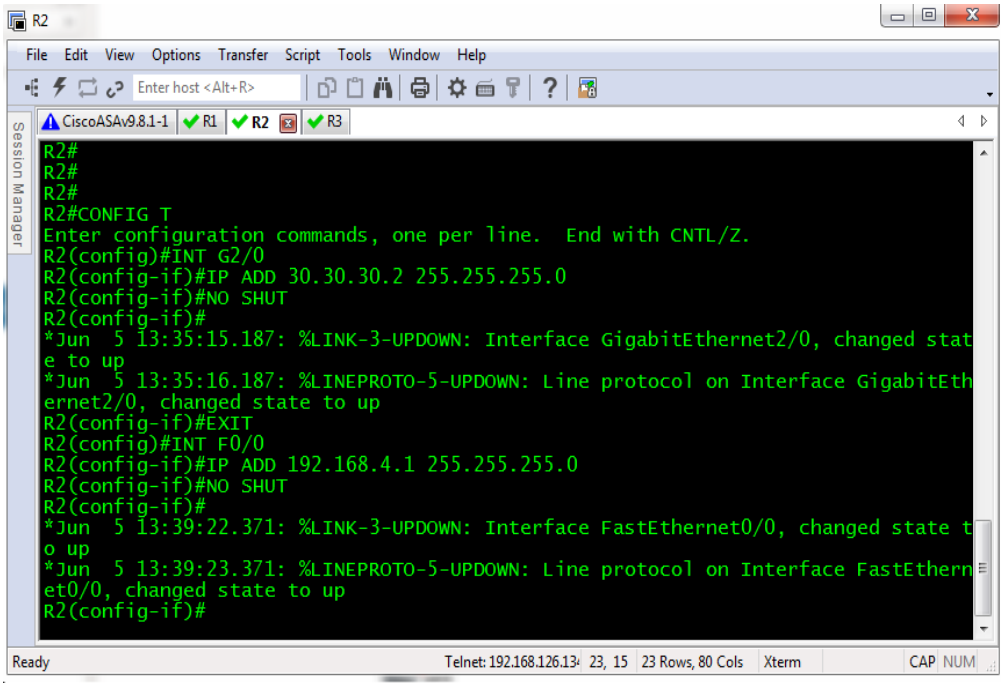

Figure 3.21 : Configurer les interfaces de routeur 2.

3.11.2.3.7 Test la connectivité des interfaces de routeur 02

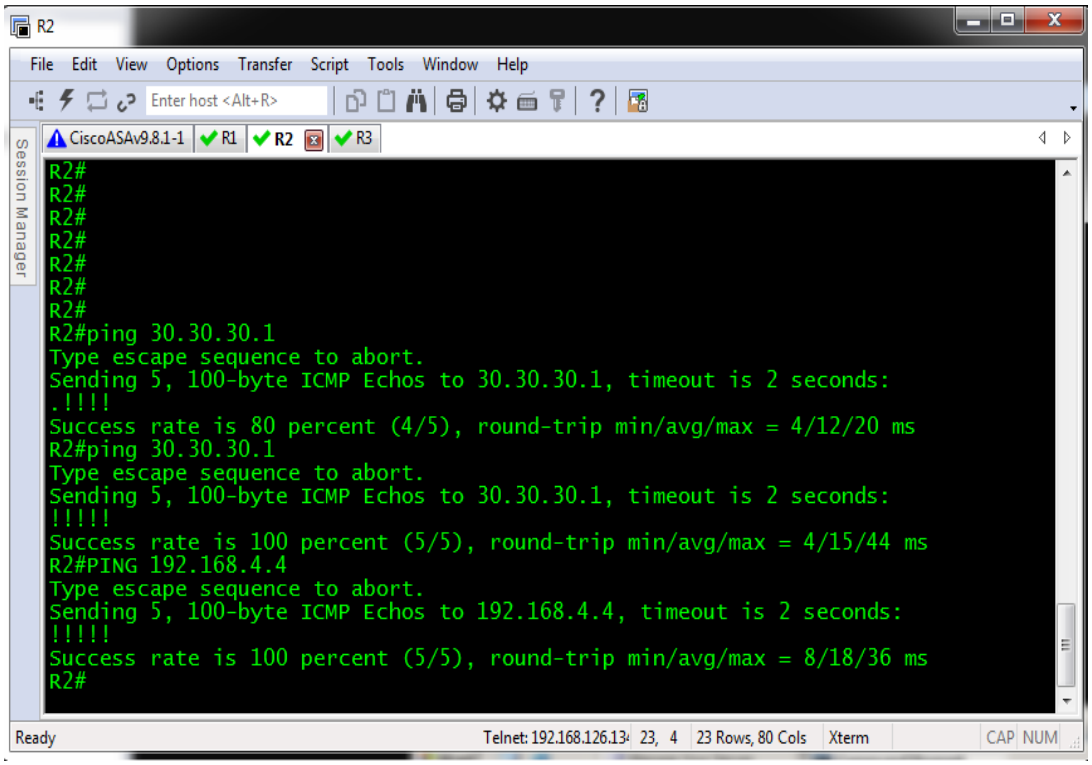

Figure 3.22 : test la connectivité de routeur 2.

3.11.2.3.8 Configuration les interfaces g2/0, f0/0, f1/1 de routeur 03 dans la zone Inside

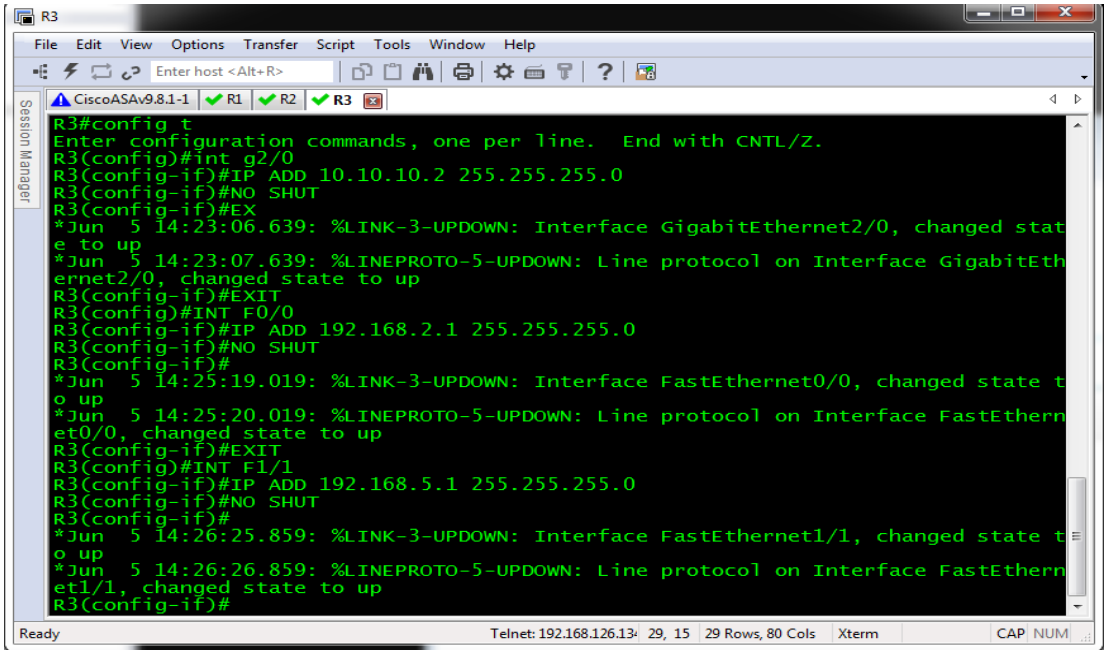

Figure 3.23 : Configure les interfaces de routeur 3

3.11.2.3.9 Tester la connectivité par Ping

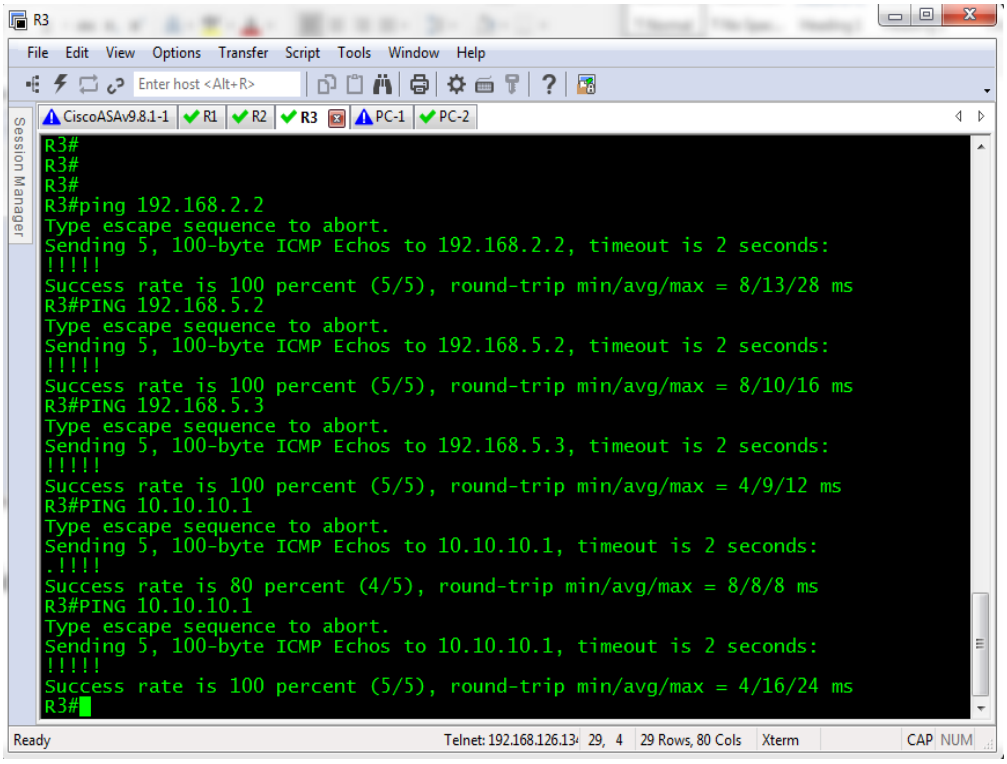

Figure 3.24 : Test la connectivité de routeur 3.

Pour identifier les réseaux au routeur et le firewall il faut choisir un Protocol de routage pour connecter aux autres réseaux, choisissons le Protocol ospf.

- **Le Protocol de routage OSPF**

OSPF est un protocole de routage dynamique défini par l'IETF à la fin des années 80. Il a fait l'objet d'un historique relativement complexe de RFC. Ce protocole a deux caractéristiques essentielles :

- ✓ Il est ouvert : c'est le sens du terme Open de OSPF. Son fonctionnement est connu de tous.
- ✓ Il utilise l'algorithme SPF pour Shortest Path First plus connu sous le nom d'algorithme de Dijkstra afin d'élire la meilleure route vers une destination donnée

3.11.2.3.10 Configure le Protocol de routage ospf dans tous les routeurs et le firewall

- **Configure a ASAv**

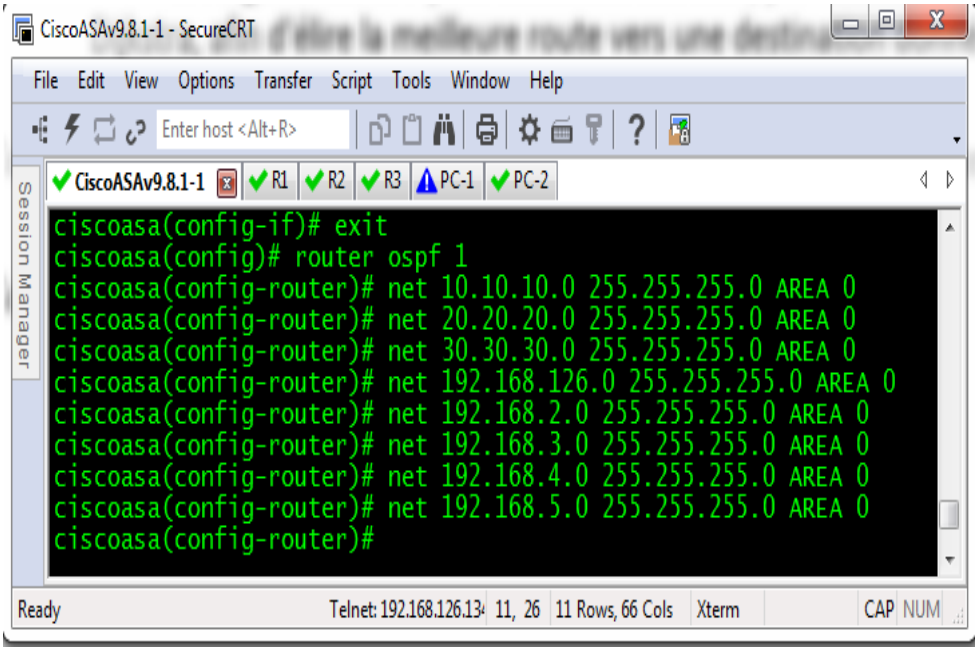

Figure 3.25 : Configure le Protocol de routage dans ASA.

Le même processus avec les routeurs.

3.11.2.3.11 Tester la connexion entre le firewall avec tous les éléments de réseaux

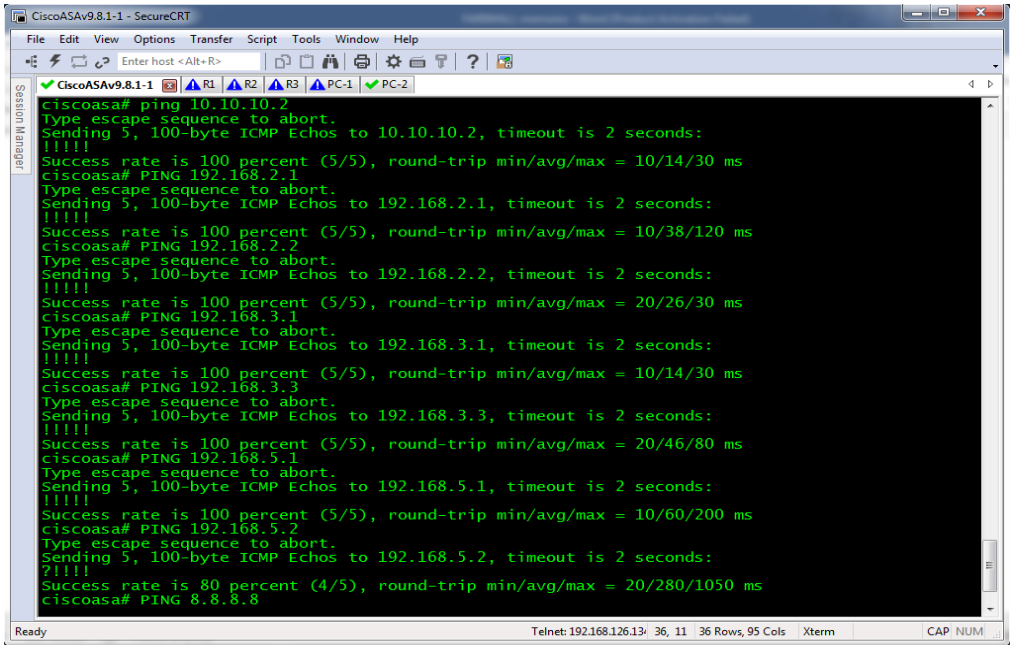

Figure 3.26 : Test la connectivité de firewall avec les réseaux.

La connexion entre les réseaux est nulle.

Parce que tous les trafics passent à travers le firewall qui possède une configuration par défaut bloquant la connexion et représente le niveau de sécurité (Security Levels).

Politique de sécurité dans les routeurs et le firewall

3.11.2.3.12 Niveau de sécurité (Security Levels)

Chaque interface doit avoir un niveau de sécurité compris entre 0 et 100 (du plus bas au plus élevé). Par exemple nous devons affecter notre réseau le plus sécurisé tel que le réseau d'entreprise interne au niveau 100. Le réseau externe connecté à Internet peut être de niveau 0. D'autres réseaux tels qu'un réseau domestique peut être intermédiaire. Nous pouvons affecter des interfaces au même niveau de sécurité.

Le firewall permet à un réseau de niveau haut de passer vers un réseau de niveau bas et vice versa.

3.11.2.3.12.1 Tester la connectivité entre les déférant réseaux

Routeur 02 vs Routeur 01

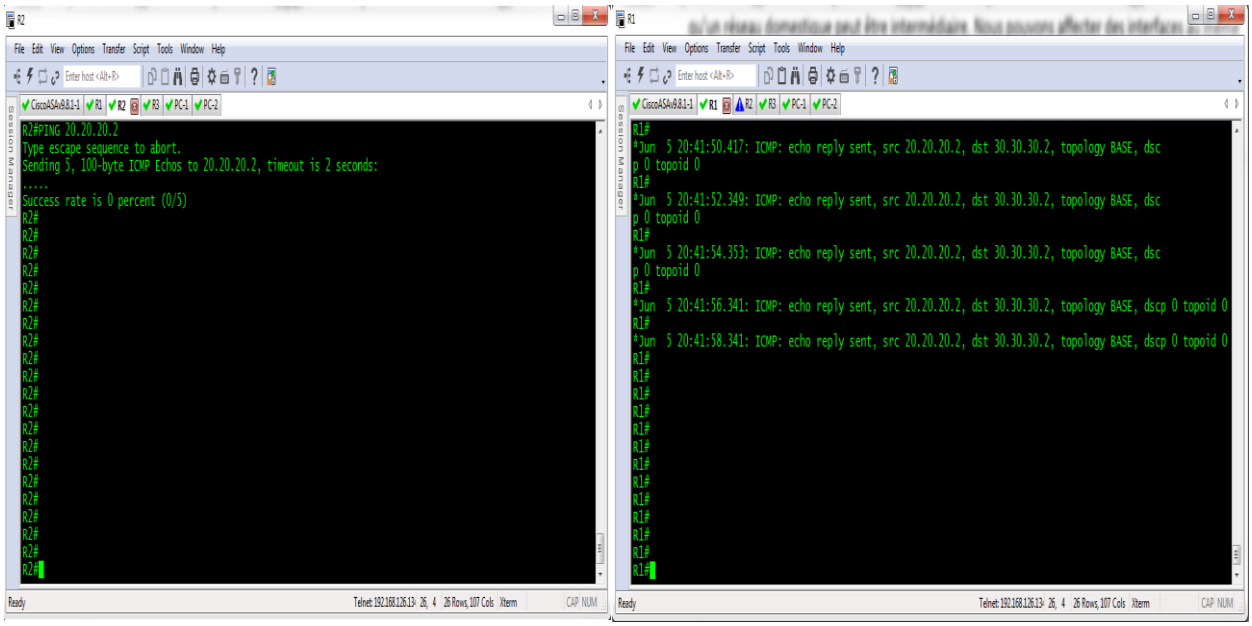

Figure 3.27 : Tester la connectivité R1 et R2.

3.11.2.3.13 Sécurisation de consol, aux, vty et mode enable pour les routeurs

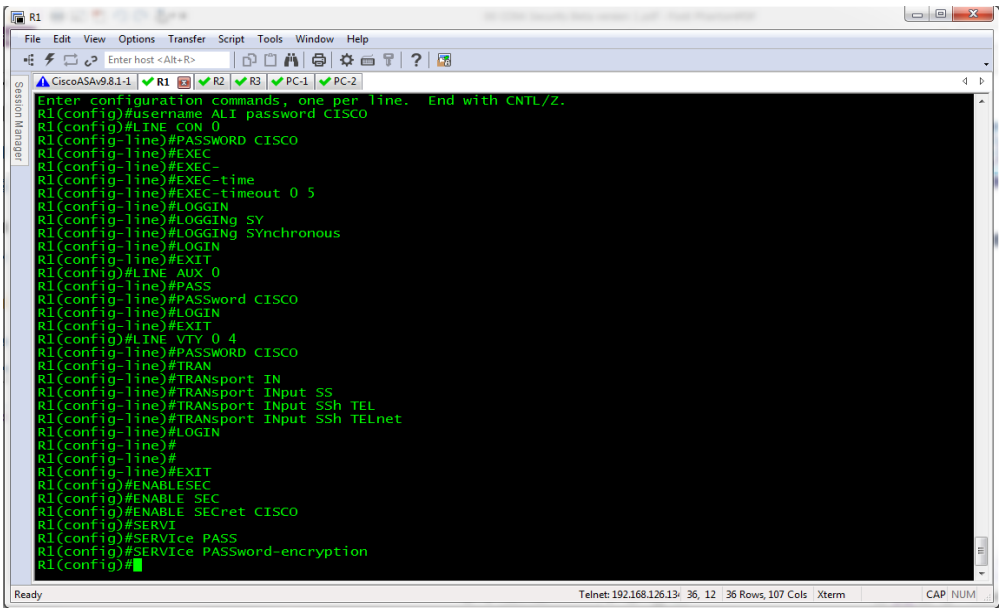

Figure 3.28 Sécurisé les ports de routeur.

3.11.2.3.14 Pour accéder aux autres réseaux en configurons le Access liste

Configuration de Access liste au ASAv pour permettre la connexion libre

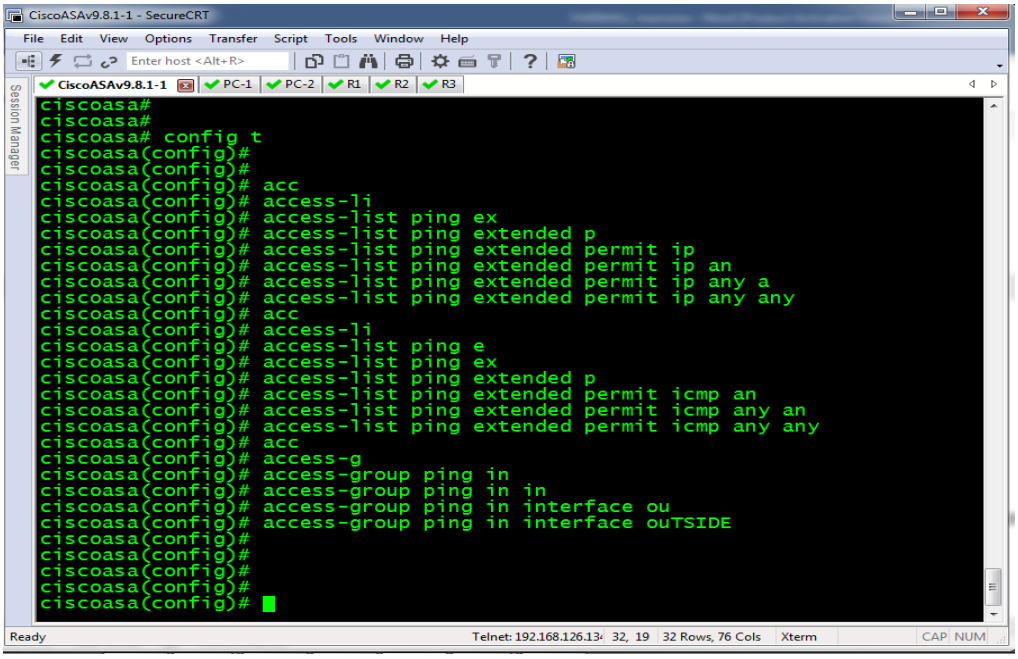

Figure 3.29 : Configuration de ACL dans ASA.

Les réseaux sans connecté entre eux mais les réseaux ont même niveau de sécurité ne peut pas connecter sois Inside ou outside.

Mettez une commande au firewall est :

- ✓ Inside: same security traffic permit inter-interface.
- ✓ Outside: same security traffic permit intra-interface.

3.11.2.3.15 Configuration le Nat et DHCP pour connecter à l'internet

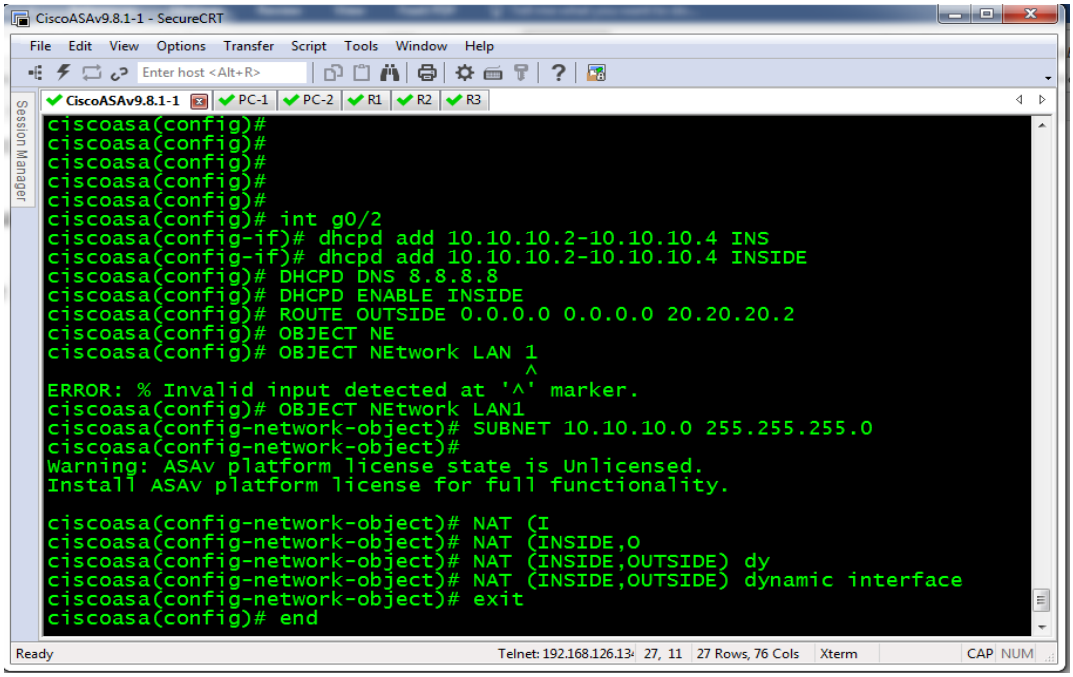

Figure 3.30 : Configuration NAT et DHCP dans ASA.

3.11.2.3.16 Configuration pour permise quelque trafic ou bloquer

Avant la configuration

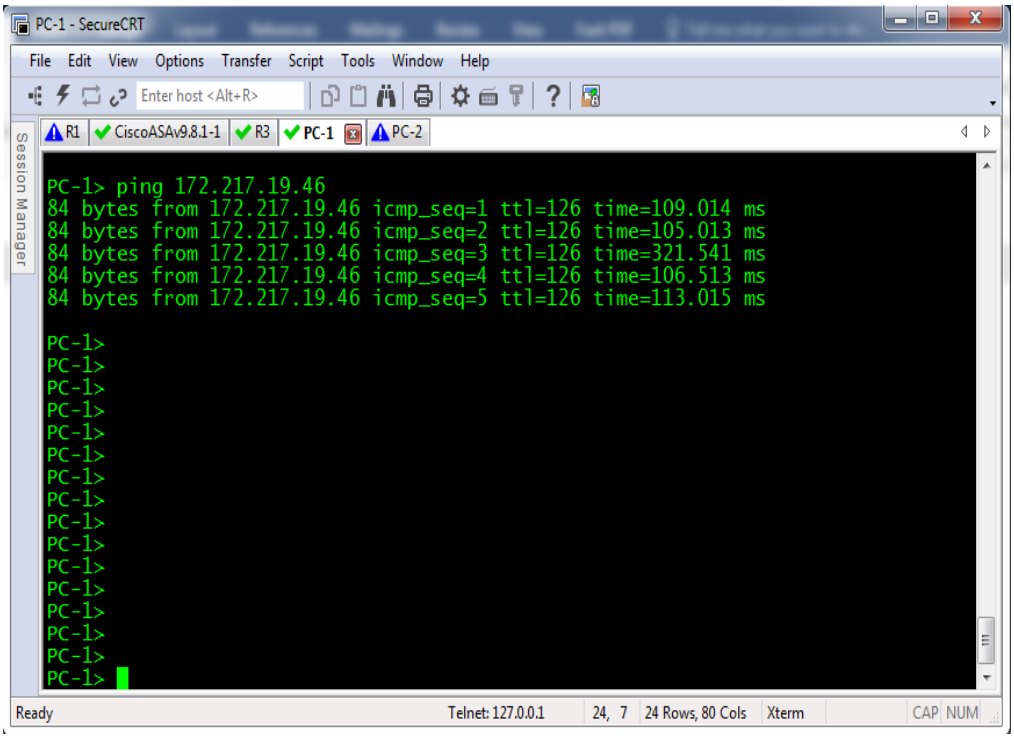

Figure 3.31 : Teste le Ping avant la configuration.

La configuration

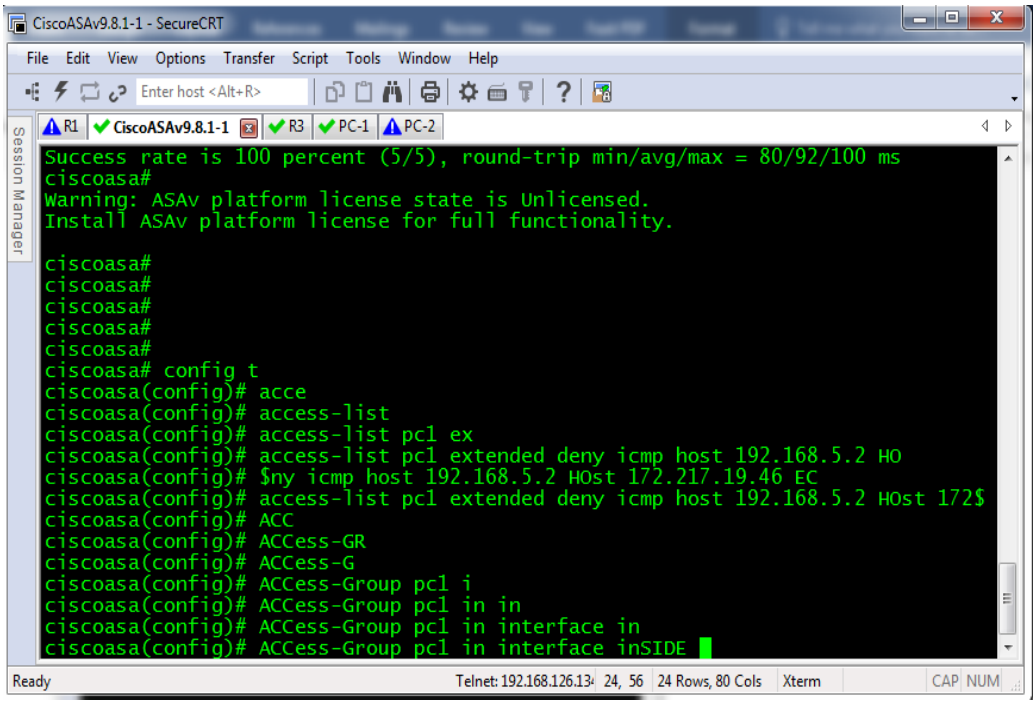

Figure 3.32 : Configuration pour filtré le traffic (ICMP).

Après la configuration

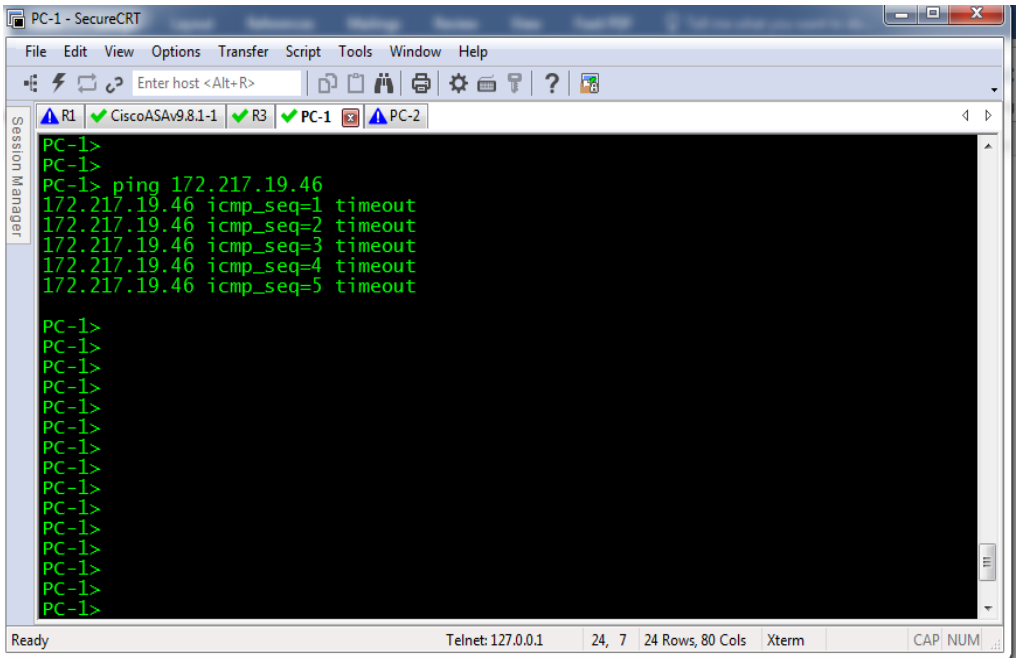

Figure 3.33 : Test le Ping après la configuration.

3.11.2.3.17 Autre exemple bloqué l'accès à distant ssh et Telnet

Avant la configuration

```
R3#
R3#
R3#
R3#
R3#
R3#
R3#SSH -l ALI 20.20.20.2
Password:

Password:
R1>
R1>
R1>
R1>
R1>
R1>
R1>
R1>
R1>
R1>
R1>
```

Figure 3.34 : Accès à distant par SSH.

La configuration

```
ciscoasa>
ciscoasa>
ciscoasa>
ciscoasa> ena
Password:
ciscoasa# config t
ciscoasa(config)#
ciscoasa(config)# acc
ciscoasa(config)# access-list
ciscoasa(config)# access-list SSH EX
ciscoasa(config)# access-list SSH EXtended DEN
ciscoasa(config)# access-list SSH EXtended DENy TCP H
ciscoasa(config)# access-list SSH EXtended DENy TCP Host 10.10.10.2 H
ciscoasa(config)# $Ny TCP Host 10.10.10.2 Host 20.20.20.2 E
ciscoasa(config)# $Ny TCP Host 10.10.10.2 Host 20.20.20.2 Eq S
ciscoasa(config)# $Ny TCP Host 10.10.10.2 Host 20.20.20.2 Eq SS
ciscoasa(config)# access-list SSH EXtended DENy TCP Host 10.10.10.2 Host 20.20$
ciscoasa(config)# ACC
ciscoasa(config)# ACCess-G
ciscoasa(config)# ACCess-Group ALI
ciscoasa(config)# ACCess-Group SSH
ciscoasa(config)# ACCess-Group SSH IN
ciscoasa(config)# ACCess-Group SSH IN IN
ciscoasa(config)# ACCess-Group SSH IN INterface IN
ciscoasa(config)# ACCess-Group SSH IN INterface INSIDE
ciscoasa(config)#
```

Figure 3.35 : Filtré le traffic par le blocage de SSH.

Après la configuration

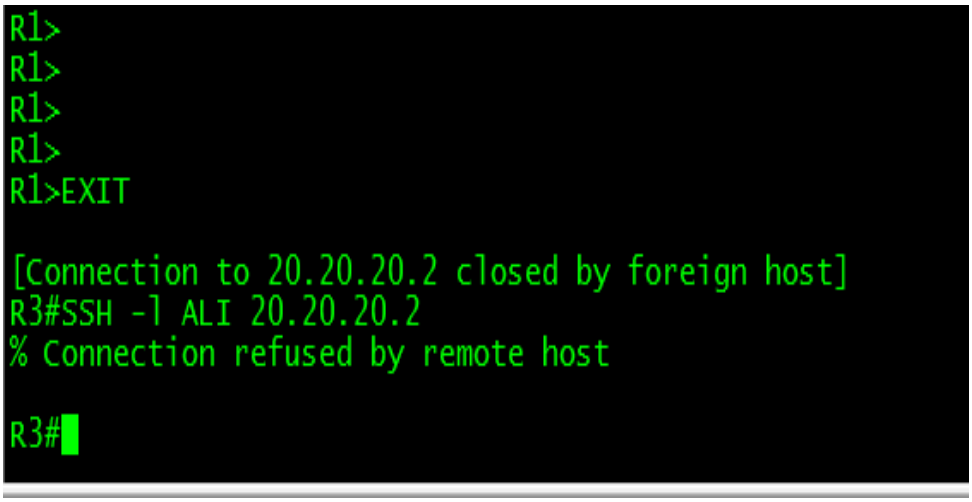

Figure 3.36 : Test l'accès a distant par SSH après la configuration.

3.11.2.3.18 Installer le mode ASDM (graphical interface)

- **La configuration pour accéder par ASDM**

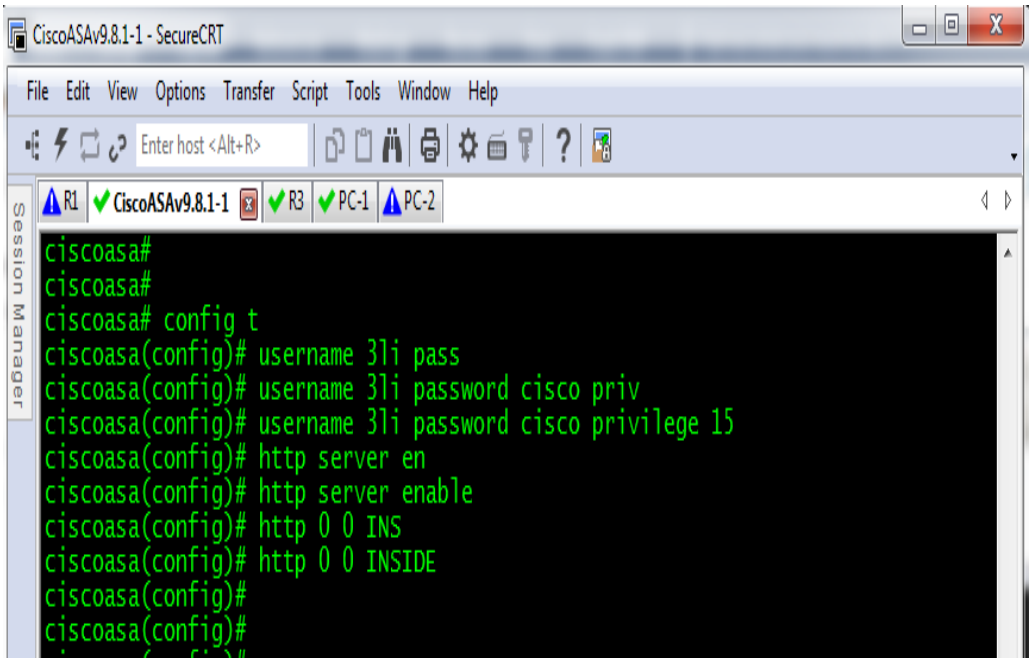

Figure 3.37 : Activer l'interface graphique ASDM.

3.11.2.3.19 La face graphique de ASDM

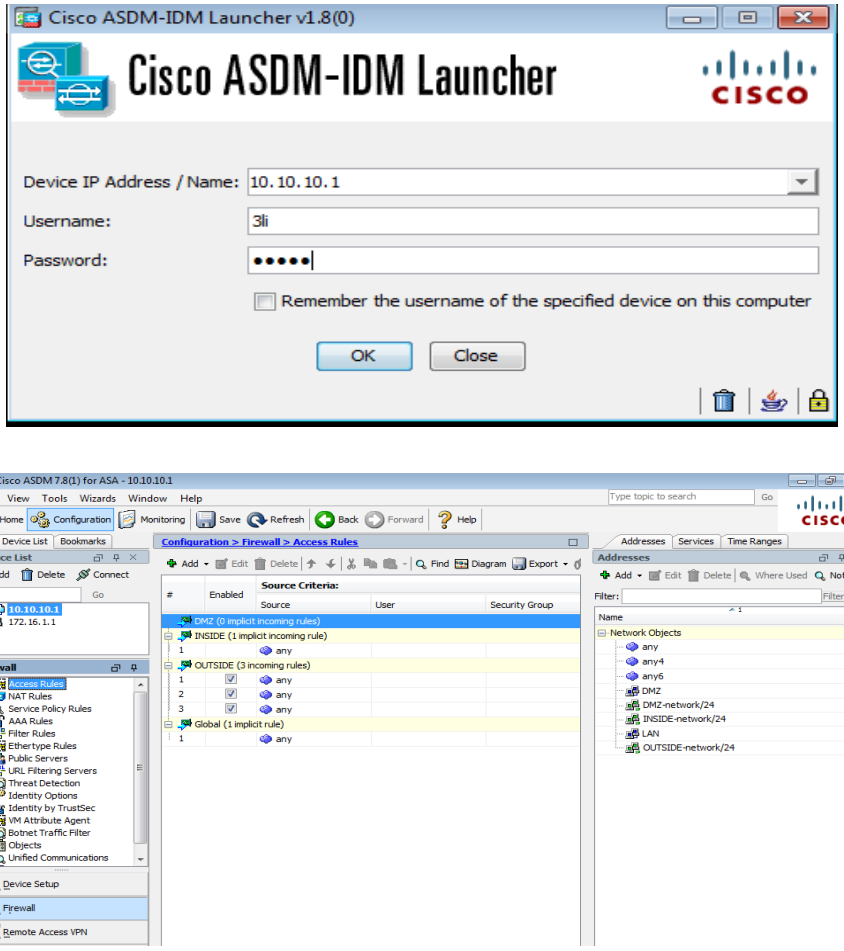

Figure 3.38 : Asdm luncher

3.11.2.3.20 Capture par wireshark qui identifier le traffic qui roule entre le PC et serveur d'université de Biskra et serveur DNS de Google

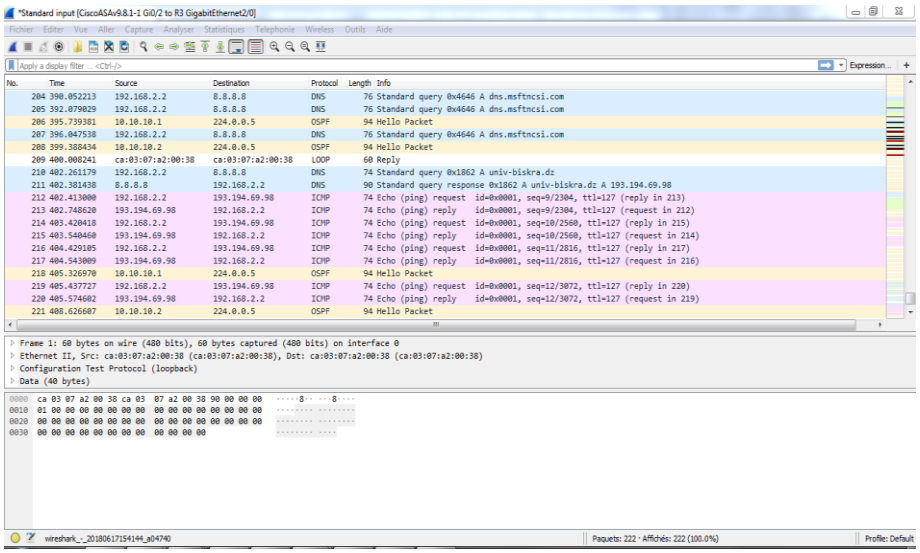

Figure 3.39 : Capture par wireshark

Conclusion

Cisco ASA est un équipement qui peut fournir plusieurs mécanismes de sécurité dans une seule plate-forme, le firewall un des ces mécanismes qui offre plusieurs fonctionnalité non seulement la translation des adresses réseau, le filtrage de trafic réseau d'après ou vers le réseau interne d'entreprise est la principale fonction pour un firewall, car il offre une inspection pour tous les paquets transite sur le réseau, mais la NAT elle ne fait que convertir les adresses privés par d'autre publique ou le contraire. Maitriser les outils de sécurisation des réseaux locaux n'est pas chose aisée, surtout que le nombre de failles ne cesse d'augmenter et les intrusions nombreuses. Protéger sa vie privée, ses données ou l'accès à son réseau est une nécessité à notre époque.

Dans ce chapitre, on a monté un réseau test qui nous a permis d'expérimenter le degré de sécurité qu'apporte un firewall à un réseau local ou même à un PC personnel. En résume, les résultats observés nous permettent de dire que nous avons réussi à sécuriser notre réseau contre certaines attaques connues, car les méfaits des virus et autres programmes espions ne sont nullement arrêtés par le firewall.

Ce point faible du firewall n'a pas trouvé de solutions, car il n'est pas envisageable à ce jour de faire rechercher les virus par le firewall, sinon on ralentirait dramatiquement le réseau, chose qui est exclue à moins d'avoir des avancées concernant la rapidité de traitements dans un proche avenir. On a procédé à plusieurs essais pour connecter des utilisateurs non autorisés, sans succès. Le firewall fonctionne correctement sans être parfait à 100 pourcent.

CONCLUSION GENERALE

Conclusion général

Dans cette mémoire on a étudié un mécanisme de sécurité pour élaborer une politique de sécurité au sein d'un réseau, il s'agit de Firewall qui offre plusieurs solutions pour faire face au menace qui peut atteindre un réseau d'entreprise depuis l'extérieur, ou on a parlé sur les principaux fonctionnements comme le filtrage des paquets et aussi sur la translation des adresses IP (NAT).

Cette dernière elle peut cacher le réseau d'entreprise derrière un réseau public cela il accompagnera de protéger son réseau de plusieurs attaques qui ont d'une source externe. Cependant ces menaces qui peut atteindre un réseau est aussi de source interne, un employé ou un utilisateur de réseau depuis l'intérieur de l'entreprise peut exploiter les failles de la politique de sécurité, par une simple connaissance de réseau il peut accéder à n'importe quelle source d'information dans des domaines et des taches qu'elle ne concerne pas, il peut voler, détruire, et aussi modifier ces information. Et pour ces raisons la mise en place des mesures de sécurité qui peuvent réduire les risques internes est très nécessaire, une solution telle que les VLAN (Virtuel Local Area Network) est très répandu pour faire séparer les différent tache d'une entreprise.

On s'est proposé de nous intéresser à la sécurité des réseaux informatiques et en particulier à la mise en place d'un firewall, qui filtrera tout ce qui rentre et sort du réseau privé vers INTERNET. Pour cela, on s'est d'abord intéressé aux attaques existantes et aux techniques de sécurité utilisées jusqu'à ce jour. Entre autre, l'authentification, le contrôle d'accès, la confidentialité et l'intégrité des données, le non répudiation etc. Il existe un moyen pour effectuer plusieurs actions sécuritaires en même temps et à un endroit névralgique, qui pourrait être l'entrée du réseau privé, par l'intermédiaire d'un firewall, d'où notre intérêt pour ce moyen efficace de sécuriser un réseau LAN.

C'est ce qui a motivé ce travail, et donc on a installé et configuré un firewall, en établissant des règles de filtrage précises, selon nos besoins et on a ensuite effectué des tests de bon fonctionnement, en utilisant un réseau test constitué du firewall au milieu de réseau LAN privé et le net. Les résultats obtenus nous confortent dans l'idée que pour sécuriser les données névralgiques ou tout bêtement sa vie privée, un firewall s'impose comme une solution très efficace et peu coûteuse.

Bibliographie

[1] : Cisco« GUIDE SÉCURITÉ CISCO», Cisco System,2004 w w w . c i s c o . c o m / g o / offices

[2] : Aman Vladimir Gnuan « Concevoir la Sécurité Informatique en Entreprise » publié sous licence creative commons en 2014

[3]: John E. Canavan« Fundamentals of Network Security» Boston • London.2001

[4]: Solange Ghernaouti « Sécurité informatique et réseaux » Dunod, Paris. 2013

[5]: Bouchouika Nadjet, Belkadi Sihem « La configuration de base d'un Firewall Cisco ASA 5550 », Mémoire Fin D'étude, Promoteur Zeraoulia Khaled, Zerrouk Radia. C.F.C de Bab Ezzouar 2009.

[6] : Michel Riguidel « Cours de Sécurité », télécom paris 2007-2008.

[7]: Ronald L. Krutz, Russell Dean Vines «The CISSP Prep Guide», Wiley Publishing, Indiana 2003.

[8]: Bendella Zineb « Gestion de la sécurité d'une application Web à l'aide d'un IDS comportemental optimisé par l'algorithme des K-means » Master en Informatique, Encadreur BENMAMMAR Badr. Université Abou Bekr Belkaid– Tlemcen .2013

[9]: Laurent Bloch, Christophe Wolfhugel «Sécurité informatique »,Groupe Eyrolles, 2007, 2009, 2011

[10]:https://www.couresehero.com/file/13280047/Network –security-basics/ 10/03/2018

[11]: Sulaimon Adeniji Adebayo «network security », bachelor's thesis, Turku University of applied sciences 2012

[12]: LESCOP Yves«LA SÉCURITÉ INFORMATIQUE » Post BTS ,2002

[13]: Cédric Liorens, Laurent Levier, Denis Valois « Tableaux de bord de la sécurité réseau », EYROLLES, Paris Cedex 05 2003, 2006

[14]: Dave Kleiman« The Official CHFI Study Guide», Syngress Publishing, Burlington 2007

[15]: Stephen Helba«Certified Ethical Hacker », EC-Council 2010

[16]: Sean-Philip Oriyano, « Certified Ethical Hacker Version 8 Study Guide » sybex, Indiana 2014

[17]: Sean-Philip Oriyano« Certified Ethical Hacker Version 9 Study Guide » sybex, Indiana 2016

[18]: Omar Santos, John stuppi « CCNA Security » Cisco Press, Indianapolis 2015

[19]: David Hucaby, Dave Garneau, Anthony Sequeira « CCNP Security FIREWALL Official Cert Guide», Cisco Press 2011

[20]: Alexandre Matos « Cisco Firewalls », Cisco Press, Indianapolis 2011

[21]: Kwok T. Fung, « Network SecurityTechnologies » CRC Press2005