République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Bejaïa
Faculté des Sciences Exactes
Département d'Informatique

MEMOIRE DE FIN DE CYCLE

En vue de l'obtention du diplôme de master professionnel

Option Administration et sécurité des réseaux

Thème

Proposition d'une solution sécurisée de réseau intranet d'Air Algérie

Réaliser par :

FERROUDJ Nadjat

GOUDJIL Nabila

Devant le jury composé de:

***Encadrant** : M r TOUAZI Djoudi*

Président: Mr AMROUN Kamal

Examinatrice: Mme ELBOUHISSI Houda

Année universitaire *2020/2021*

Remerciements

Avant tout nous tenons nos remerciements à notre dieu tout puissant de nous avoir donné le courage, la volonté, la force, la patience et la chance de suivre le chemin de la science, de mener à bien ce modeste travail, qui n'aurait jamais été réalisé sans sa bénédiction.

Nous tenons à remercier notre promoteur Mr TOUAZI Djoudi, d'avoir accepté de diriger ce travail, et pour ses précieux conseils et encouragements

Nous exprimons également notre gratitude aux membres du jury, qui nous ont honorés en acceptant de juger ce modeste travail.

Nous tenons à remercier tous les enseignants qui ont assurés notre formation Durant notre cycle universitaire. Ainsi, que tout le personnel du département informatique.

Dédicaces

Je rends grâce au bon Dieu de m'avoir donné la force, la volonté et la sagesse afin de parvenir à cette conclusion de mon cycle.

Je souhaite dédier ce travail à mes très chers parents qui n'ont pas cessé de m'encourager et de se Sacrifier afin que je puisse réussir

Que Dieu leur accorde santé, amour, bonheur et longue vie ; Aucune dédicace ne pourra compenser leurs sacrifices

À mes adorables frères, sœur: Moukrane, Siham et Fares pour tous leurs encouragements

A mon cher ami et meilleur soutenu Mustapha

À ma binôme Nabila avec qui j'ai partagé de belles années d'études

A toute ma famille et mes proches sans exception

Et toute personne que je connais et qui me sont chers et tous ceux qui m'aiment…

Nadjat

Dédicaces

Je dédie ce modeste travail à :

A mes chers parents qui m'ont soutenu durant mon existence et ma scolarité.

A mes frères et sœurs

A mes belles sœurs

A tous mes amis

A tous ceux qui ont une relation de proche ou de loin Avec la réalisation du présent mémoire.

Nabila

Table des matières

Chapitre 1 : Généralités sur les réseaux informatiques

Chapitre 2: Introduction à la sécurité informatique

Chapitre 3 : Présentation de l'architecture du réseau d'AIR Algérie

Chapitre 4 : Réalisation

Liste des tableaux

Liste des figures

Liste des abreviations

A

AAA **A**uthentication **A**uthorization **A**ccounting
ACL **A**ccess **C**ontrol **L**ist
AH **A**uthentication **H**eader
ARP **A**ddress **R**esolution **P**rotocol
ASA **A**daptive **S**ecurity **A**ppliance

B

BPDU **B**ridge **P**rotocol **D**ata **U**nit

C

CA **C**ertification **A**uthority
CD **C**ompact **D**isc
CIDR **C**lassless **I**nter **D**omain **R**outing
CISCO **C**ommercial **I**ndustrial **S**ecurity **C**orporation
CLI **C**ommand **L**ine **I**nterface
CSMA/CD **C**arrier **S**ense **M**ultiple **A**ccess / **C**ollision **D**etection

D

DVD **D**igital **V**ersatile **D**isc
DCE **D**ata **C**ircuit **E**quipment
DHCP **D**ynamic **H**ost **C**onfiguration **P**rotocol
DMZ **D**e**M**ilitarized **Z**one
DNS **D**omain **N**ame **S**ystem
DOS **D**enial **O**f **S**ervice
DTE **D**ata **T**erminating **E**quipment

E

ESP **E**ncapsulation **S**ecurity **P**ayload

F

FTP **F**ile **T**ransfer **P**rotocol

H

H-IDS **H**ost-Based **I**ntrusions **D**etection **S**ystem
HTTP **H**yperText **T**ransfer **P**rotocol
HTTPS **H**yperText **T**ransfer **P**rotocol **S**ecure

I

ICMP Internet Control Message Protocol
IDS International Data Corporation
IEEE Institute of Electrical and Electronic Engineers
IETF Internet Engineering Task Force
IMAP Internet Mail Access Protocol
IOS Internetwork Operating System
IPS Intrusion Prevention System
IPsec Internet Protocol Security
IPX Internetwork Packet Exchange
IP Internet Protocol
IPv4 Internet Protocol Version 4
IPv6 Internet Protocol Version 6

L

LAN Local Area Network
LLC Logical Link Control
L2F Layer Two Forwarding
L2TP Layer 2 Tunneling Protocol

M

MAN Metropolitan Area Network
MAC Mandatory Access Control
MAU Multistation Access Unit
MD5 Message Digest 5
MPF Modular Policy Frame-work

N

NAT Network Address Translation
N-IDS Network-Based Intrusions Detection System
NAS Network Access Server

O

OSI Open Systems Interconnection

P

PAN Personal Area Network
PAT Port Address Translation

PC	**P**ersonal **C**omputer
PPTP	**P**oint-to-**P**oint **T**unneling **P**rotocol
PPP	**P**oint to **P**oint **P**rotocol

R

RADIUS	**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice
RARP	**R**everse **A**ddress **R**esolution **P**rotocol
RFC	**R**equests **F**or **C**omments
RSA	**R**ivest, **S**hamir & **A**dleman

S

SHA_1	**S**ecure **H**ash **A**lgorithm-**1**
SMTP	**S**imple **N**etwork **M**anagement **P**rotocol
SSH	**S**ecure **S**hell
SSL	**S**ecure **S**ockets **L**ayer
STP	**S**panning **T**ree **P**rotocol

T

TACACS	**T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem
TCP	**T**ransmission **C**ontrol **P**rotocol
TCP/IP	**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol
Telnet	**T**elecommunication **N**etwork
TLS	**T**ransport **L**ayer **S**ecurity
TFTP	**T**rivial **F**ile **T**ransfer **P**rotocol

V

VLAN	**V**irtual **L**ocal **A**rea **N**etwork
VPN	**Vi**rtual **P**rivate **N**etwork
VTP	**V**LAN **T**runk **P**rotocol

W

Web WAN	**W**ide **A**rea **N**etwork

X

XSS	Cross-**S**ite **S**cripting

Introduction Générale

Avec l'évolution rapide de l'informatique et les systèmes de communication, nombre de systèmes informatiques et réseaux d'entreprises sont de plus en plus exposés aux multiples menaces, notamment les méthodes d'intrusion.

Une entreprise étant appelée à offrir non seulement à ses employés internes des services mais aussi les clients inconnus et partenaire, se voit accessible par des acteurs inconnus on leur offrant la possibilité d'accéder aux réseaux d'entreprise pour des finis des besoins. Ce qui offre la possibilité aux étrangers une porte ouverte d'accès à l'entreprise. Cette porte peut-être utilisée pour des actions non contrôlées capable de nuire à l'entreprise (piratage et destruction des données).

La sécurité se place actuellement au premier plan de la mise en œuvre et de l'administration des réseaux Informatiques. De plus, elle est devenue l'un des éléments-clés de la continuité des systèmes informatique de l'entreprise quelque soit son activité. La protection de ces informations contre une utilisation non autorisée est donc devenue un problème majeur, vu qu'actuellement, de plus en plus d'ordinateurs et des réseaux sont reliés entres eux ou à Internet. Cette connectivité a facilité, certes, l'échange entre ces composants, mais elle a augmenté en même temps les risques d'attaques contre ces réseaux.

Pour parer à ces attaques, une architecture de réseau sécurisée est nécessaire. L'architecture devant être mise en place doit comporter un composant essentiel qui est sont les mécanismes de sécurité. Ces mécanismes ont pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux possible. Cela permet de rendre le réseau ouvert sur Internet beaucoup plus sûr.

L'objectif de notre mémoire de fin de cycle est de renforcer la politique de sécurité du réseau local au sein de l'entreprise Air Algérie avec l'implémentation d'une solution basée sur plusieurs mécanisme de sécurité comme le pare-feu, VPN…ect. Pour mener à bien notre travail, nous le répartissons en quatre chapitres organisés comme suit :

Le premier chapitre sera consacré à « Généralités sur les réseaux», en décrivant les types de réseau ainsi que leurs caractéristiques.

Le deuxième chapitre « Généralités sur la sécurité informatique » est consacré à la présentation des différentes techniques de protection des réseaux informatiques contre les attaques, en expliquant en détaille les solutions de sécurité (mécanismes de sécurité).

Dans le troisième chapitre, nous étudions l'architecture physique existante du réseau Intranet de AIR Algérie.

Le dernier chapitre : nous allons passer à la « Réalisation ». Cette phase est décomposée en deux parties: dans la première nous introduirons l'outil Packet Tracer, nous passerons ensuite à la deuxième partie qui sera principalement consacrée à l'implémentation des solutions et on fini par une conclusion générale

Chapitre 1

Généralités sur les réseaux informatiques

I.1 Introduction

Le besoin de communication et le partage de ressource entre les différentes entités a poussé les entreprises à s'orienter vers les réseaux informatiques qui sont devenus indispensables pratiquement dans tous les domaines de la vie.

Alors pour bien mener à notre projet, à travers ce chapitre nous allons aborder quelques concepts de bases sur les réseaux informatiques, pour bien aider à mieux assimiler le fonctionnement des réseaux.

I.2 Définition d'un réseau informatique

Un réseau informatique, est un ensemble d'´equipements matériels et logiciels interconnectés les uns avec les autres, il permet de faire circuler les éléments ou l'échanger des informations, tel que le transfert des fichiers, le partage de ressources (imprimantes et données), la messagerie ou l'exécution de programmes à distance. [1]

I.3 Classification des réseaux

I.3.1 Classification selon l'étendue

Les réseaux informatiques sont classés en différents types selon trois critères principaux(les distances, les débits, et les type de câbles utilisés), dans ce contexte nous pouvons trouvez les types de réseaux suivants :

Réseau local, **réseau métropolitain (MAN), réseau étendu (WAN) et les réseaux PAN** (Voir l'annexe A)

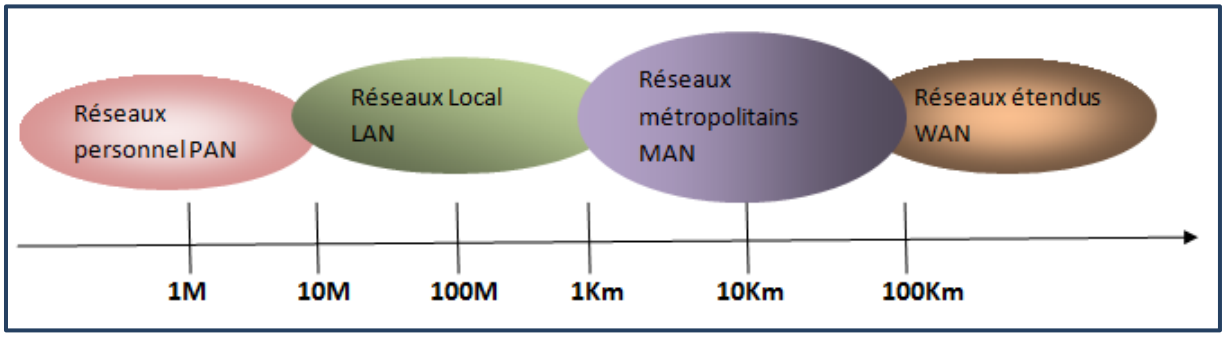


Figure I. 1: Type des réseaux informatiques

I.3.2 Classification selon la topologie

Il existe deux types de topologie : les topologies physiques et logiques.

I.3.2.1 Les topologies physiques

Elles décrivent la façon dont les machines sont connectées physiquement les uns aux autres, il existe deux mode : mode de diffusion (Un émetteur ➔Plusieurs récepteurs) et point à point (Un émetteur➔Un récepteur).

I.3.2.1.1 Mode diffusion

I.3.2.1.1.1 La topologie en bus (voir l'annexe A)

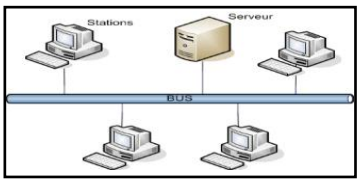


Figure I. 2: Topologie en bus

I.3.2.1.1.2 La topologie en anneau (voir l'annexe A)

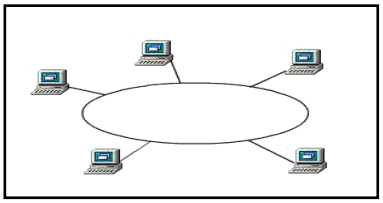


Figure I. 3: Topologie en anneau

I.3.2.1.2 Mode point à point

I.3.2.1.2.1 La topologie en étoile (voir l'annexe A)

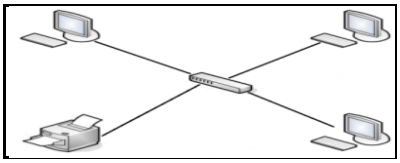


Figure I. 4: Topologie en étoile

I.3.2.1.2.2 Topologie maillée (voir l'annexe A)

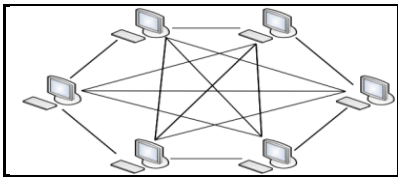


Figure I. 5: Topologie maillée

I.3.2.2 Les topologies logiques (*Topologie d'accès*) (voir l'annexe A)

I.3.2.2.1 Topologie Ethernet

I.3.2.2.2 Topologie Token ring

I.4 Les équipements des réseaux informatiques

I.4.1 Les équipements d'interconnexion (voir l'annexe A)

Répéteur, Concentrateur (hub), Pont(Bridge), Commutateur(Switch), Passerelle(Gateway), Routeur,

I.4.2 Les équipements matériels (voir l'annexe A)

I.4.2.1 Carte réseau

I.4.2.2 La fibre optique

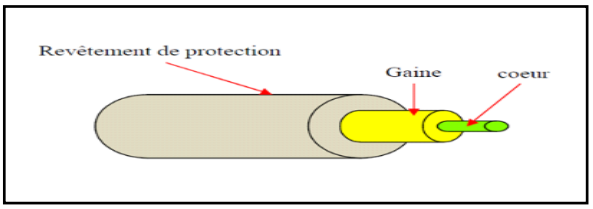


Figure I. 6: La fibre optique

I.4.2.3 La paire torsadée

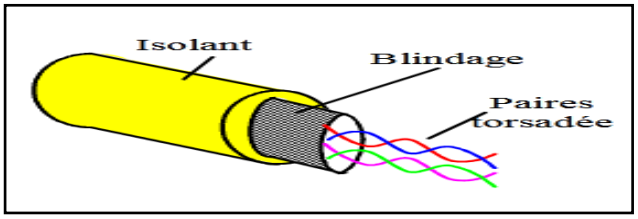


Figure I. 7: La paire torsadée

I.4.2.4 Le câble coaxial

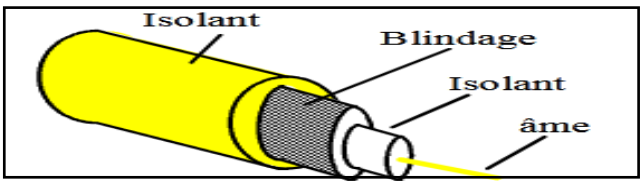


Figure I. 8: Le câble coaxial

I.4.3 Les connecteurs réseaux

- **Connecteur BNC :** adapter pour les câbles coaxiaux.
- **Connecteur RJ45 :** adapter aux câbles à paires torsadées.
- **Connecteur fibre optique:** utiliser pour les fibres optiques.

I.5 Mode de transmission

Selon le sens des échanges, on distingue trois modes de transmission : (voir l'annexe A)

I.6 Les modèles de référence

La transmission d'information entre deux programmes informatiques sur deux machines différentes passe par deux modèles : le modèle OSI ou le modèle TCP/IP. Chaque modèle inclut plusieurs couches.

I.6.1 Le modèle OSI

OSI (*Open System Interconnexion*), est un modèle de base qui été défini par l'ISO (*International Standard Interconnexions*). Cette organisation revient régulièrement pour mettre en place un standard de communications entre les ordinateurs d'un réseau [2]. Qui est adopté pour faciliter l'échange des données provenant des matériels des différents constructeurs.

I.6.1.1 Les couches du modèle OSI (Voir l'annexe B)

I.6.1.2 Processus de transmission/réception

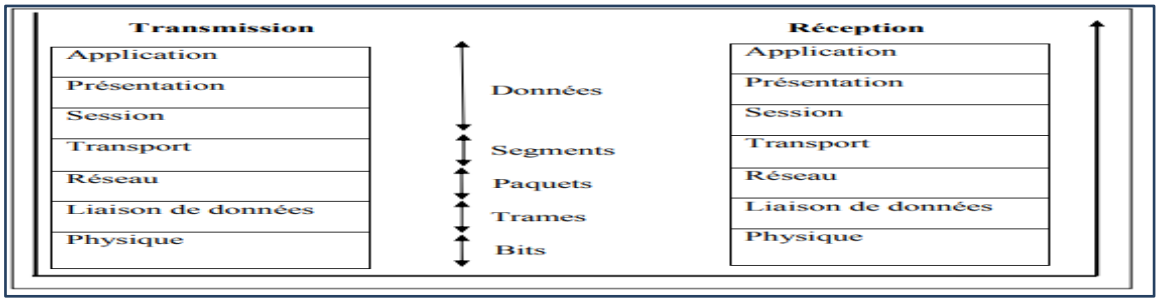


Figure I. 9: Processus de transmission/réception

I.6.2 Le modèle TCP/IP

TCP/IP (*Transmission Control Protocol/ Internet Protocol*) est le protocole le plus utilisé actuellement pour le transfert des données sur **internet,** il se base sur la notion d'adresse IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données. C'est en fait une architecteur réseau en 4 couches qui ont des taches beaucoup plus diverses était donné qu'elles correspondent à plusieurs couche du modèle OSI

TCP (*Transfert Contrôle Protocole*) se charge du transport de bout en bout pour toute application et IP (Internet Protocole) est responsable du routage à travers le réseau.

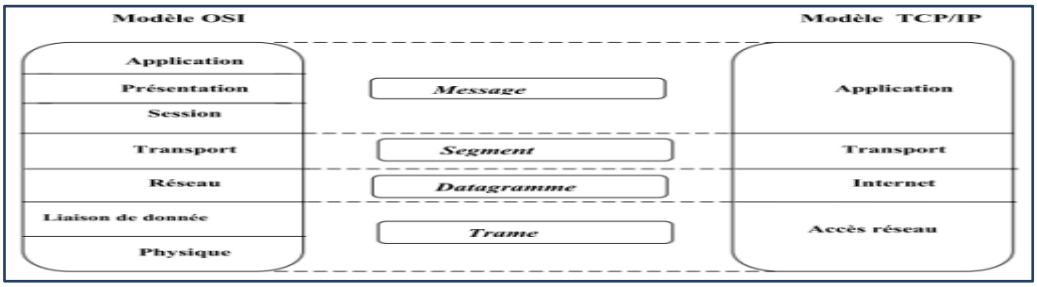


Figure I. 10: L'architecture en couche de modèle TCP/IP et les unités d'échanges

I.6.2.1 Les couches du modèle TCP/IP (Voir l'annexe B)

I.7 Les adresses internet sur le réseau

Nous distinguons deux types de réseaux adressables en IP : Le réseau public Internet où chaque équipement connecté doit posséder une adresse unique et enregistré au niveau mondial. Les réseaux privés, dans ce cas le choix des adresses est libre et ne doivent être uniques que dans ce réseau.

I.7.1 Présentation générale de l'adresse IP

Une adresse IP (*avec IP pour Internet Protocol*) est un numéro d'identification relative au réseau qui est attribué de façon permanente ou provisoire à chaque périphérique relié à un réseau informatique qui utilise l'Internet Protocol. L'adresse IP est à la base du système d'acheminement (le routage) des paquets de données sur Internet [3]. Il existe deux types de version d'adresse IP (IPV4 et IPV6) (voir l'annexe C)

Le masque d'un réseau

- Pour décomposer une adresse IP (c'est-à-dire séparer le NetID du HostID), il faut utiliser un masque (NetMask).
- définit la taille d'un réseau IP : c'est-à-dire la plage d'adresses assignables aux machines du réseau.

I.7.2 Les classes d'adresses IP

Une machine (*appelée aussi hôte ou host*) est identifiée dans l'Internet par son adresse. L'adresse IP d'une machine correspond à un numéro qui est unique dans le monde. Il existe actuellement cinq classes d'adresses IP pour les ranger de façon logique, ordonnées et différencier entres les tailles de réseau (La classe A, B, C, D et E). Voir la plage d'adressage dans l'annexe C

I.7.3 L'adressage sans classes CIDR (*Classless Inter-Domain Routing*) Voir l'annexe C

I.7.4 Les adresses particulières (Voir l'annexe C)

L'Adresse de bouclage (*Loopback*), l'adresse 0.0.0.0 et l'adresse MAC

Les adresses interdites

- L'adresse de diffusion
- L'adresse de réseau

I.7.4.1 Les adresses IP Privées

l'ICANN[1] a réservé une poignée d'adresses dans chaque classe pour permettre d'affecter une adresse IP aux ordinateur d'un réseau interne privé (Réseau local LAN) relié à internet sans risque d'enter en conflit avec une adresse IP publique.

Tableau I. 1: La plage d'adressage pour les réseaux privés

Classes	Plage d'adressage	Nombre d'adresses
A	10.0.0.0➔10.255.255.255	2^{32-8} =16777216
B	172.16.0.0➔172.31.255.255	2^{32-12}= 1048576
C	192.168.0.0➔192.168.255.255	2^{32-16} =65536

I.7.5 Les sous-réseaux

Un sous-réseau est une subdivision logique d'un réseau de taille plus importante pour optimiser les échanges entre les machines, il devient une partie d'un réseau dans lequel toutes les adresses IP des machines utilisent la même adresse réseau.

I.7.5.1 Le masque d'un sous-réseau (Voir l'annexe C)

I.8 Intranet

Le mot « intranet » est composé du latin « intra » (intérieur) et de l'anglais « net ». L'ensemble signifie donc « **réseau interne** » [4], qui est un réseau informatique privé et invisibles de l'extérieur, utilise les mêmes protocoles qu'Internet (TCP, IP, HTTP[2], SMTP, IMAP[3], etc.), fonctionne au sein d'une entreprise ou de toute autre entité organisationnelle pour but de transporter et traiter les flux d'informations internes d'un groupe d'utilisateurs identifiés [5].

L'intranet va permettre donc à l'entreprise de mettre en œuvre l'ensemble de possibilités d'Internet, mais en interne (c'est-à-dire il suffit simplement d'une connexion internet et d'un

[1] Une organisation internationale de droit qui alloue l'espace des adresses de protocole Internet et administre les noms de domaines.

[2] HTTP est la langue dans laquelle votre navigateur Web parle au serveur Web afin de lui communiquer

[3] IMAP est un protocole qui vous permet, depuis un programme (logiciel ou application) installé sur votre ordinateur ou votre smartphone, d'accéder aux messages de votre boîte aux lettres électronique de manière **synchronisé**

compte utilisateur pour accéder à toutes les ressources et fonctionnalités disponible sur l'intranet).

I.9 Extranet

Un extranet est un réseau privé de type intranet, accessible de l'extérieur et doit être sécurisé dans la mesure où cela offre un accès au système d'information à des personnes situées en dehors de l'entreprise.

Nous distinguons deux types d'authentification, à savoir :

- Authentification simple (nom d'utilisateur et mot de passe)
- Authentification forte (authentification à l'aide d'un certificat).

I.10 L'internet

Ensemble de réseaux mondiaux interconnectés qui permet à des ordinateurs et à des serveurs de communiquer efficacement au moyen d'un protocole de communication commun (IP) [6]. Elle rend accessible au public des services comme le courrier électronique (e-mail), le World Wide Web et l'échange de fichiers par FTP (*File Transfer Protocol*) …etc.

I.11 Le routage

Le routage est l'une des opérations les plus importantes du réseau informatique dans lequel le paquet de données est déplacé de la source à la destination en utilisant un chemin optimisé avec un délai faible, il existe deux modes de routages bien distincts lorsque nous souhaitons aborder la mise en place d'un protocole de routage, il s'agit du **routage statique** et du **routage dynamique** (Voir l'annexe D)

I.12 Conclusion

Ce chapitre nous a permis de découvrir et de mieux comprendre les notions et les aspects élémentaires des réseaux informatiques, où nous avons défini les réseaux informatiques et cité les différents types de réseaux ainsi que les différentes topologies et les équipement d'interconnexion réseau et d'avoir une idée sur la notion des couches dans le modèle OSI et le modèle TCP / IP et donné une description globale sur l'adressages IP et le routage.

Dans le prochain chapitre, nous aborderons la sécurité des réseaux informatiques qui compte actuellement parmi les sujets les plus importants et que la majorité des entreprises ne peuvent plus ignorer.

Chapitre 2

Introduction à la sécurité informatique

II.1 Introduction

Avec l'arrivée de l'internet dans les réseaux, La sécurité informatique est devenue un problème majeur dans la gestion des réseaux d'entreprises ainsi que pour les particuliers car le système d'information est vulnérable et qu'il peut subir des piratages, des attaques (virus, hackers…), des pertes de données...etc. Il est donc indispensable pour les entreprises de savoir définir la sécurité de ses ressources informatiques et de garantir la confidentialité, l'intégrité et la disponibilité des services. C'est pour cela Il faut mettre en place des mécanismes pour s'assurer que seules les personnes autorisées ont accès à l'information et que le service est rendu correctement.

Nous entamerons ce chapitre par une définition et une exposition des objectifs de la sécurité informatique, nous parlerons ensuite des différentes menaces, vulnérabilités et attaques qui pèsent sur les réseaux, et enfin, nous bouclerons ce chapitre par une présentation des différents mécanismes de sécurité tels que le pare-feu, la DMZ et les VPNs …etc.

II.2 Sécurité informatique

C'est la protection des données et des ressources matérielles ou logicielles (ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données), contre les attaques malveillantes en mettant en place des mécanismes de contrôle qui permettant d'assurer le bon fonctionnement du système.

Il peut s'agir :

- D'empêcher des personnes non autorisées d'agir sur le système de façon malveillante.
- D'empêcher les utilisateurs d'effectuer des opérations involontaires capables de nuire au système.
- De sécuriser les données pour éviter la perturbation ou des pannes.
- De garantir la non-interruption d'un service. [7]

II.3 Les objectifs de la sécurité

La sécurité des systèmes d'information vise à assurer les propriétés suivantes

La confidentialité : empêcher la divulgation d'informations à des entités non habilitées à les connaitre.

Authentification : C'est la propriété qui assure que seules les entités autorisées ont accès au système.

- **Authentification d'une information :** Prouver qu'une information provient de la source annoncée (émetteur).
- **Authentification d'une entité** : Prouver que l'identité est bien celle annoncée.

Intégrité : C'est assurer que les informations n'ont pas été altérées, modifiées par des personnes non autorisées.

Non-répudiation : Permettant de garantir qu'une transaction ne peut être niée.

Disponibilité : L'information sur le système doit être toujours disponible aux personnes autorisées qui permet de maintenir le bon fonctionnement du système informatique.

II.4 Terminologie de la sécurité informatique

II.4.1 Menace

Evènement, d'origine accidentel ou délibéré, capable s'il se réalise de causer un dommage à un système donné. Dans un système informatique, il peut toucher les composantes matérielles, logicielles ou informationnelles. Il existe principalement deux types de menaces :

- **Les menaces accidentelles** (non-intentionnelles): Ne supportent aucune préméditation. Dans cette catégorie sont repris les bugs logiciels et les pannes matérielles et autres défaillances incontrôlables.
- **Les menaces intentionnelles** (Attaque): Représentent l'action d'une personne désirant d'introduire dans le système et relever les informations.

II.4.2 Vulnérabilité

Une faiblesse dans le système qui peut être exploitée par une menace

II.4.3 Risque

Association d'une menace aux vulnérabilités qui permettent sa réalisation.

Vulnérabilité + Menace=Risque

II.4.4 Politique de sécurité

La politique de sécurité est l'ensemble de règles définies et destinées à contrôler les aspects de sécurité comme les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des ressources possèdent uniquement les droits qui leur ont été octroyés [8]. Elle permet de préserver la confidentialité, la disponibilité et l'intégrité des biens, des services et des informations et assurer la continuité de fonctionnement du système. Dans un premier temps une politique de sécurité, dont la mise en œuvre se fait selon

- L'analyse de la valeur des informations à protéger et l'analyse des risques ;
- L'application de règles et de procédures par les utilisateurs internes de l'organisation (définition d'une politique globale) ;
- Adoption des moyens techniques nécessaires à la réalisation de cette politique (firewall, système de détection d'intrusion,. . .) ;

II.4.5 Les attaques

Une attaque représente les moyens d'exploiter une (ou plusieurs) vulnérabilité(s) dans un système pour violer un ou plusieurs besoins de sécurité

II.5 Les scénarios d'attaques

- ***L'attaque active :*** Il s'agit d'acquérir des informations utiles sur le réseau, tel que l'attaquant intercepte la connexion et tente de modifier l'information ou crée un faux message. , ici l'intrus aura volontairement modifié les fichiers ou le système pour s'en emparer.
- ***L'attaque passive :*** L'attaquant se met en écoute non autorisée, en surveillant simplement la transmission ou la collecte d'informations. En effet ces actions ne modifient pas les fichiers et n'altèrent pas le système, il peut être empêché en utilisant des méthodes de cryptage dans lesquelles les données sont chiffrée illisibles, et donc inutilisables

.

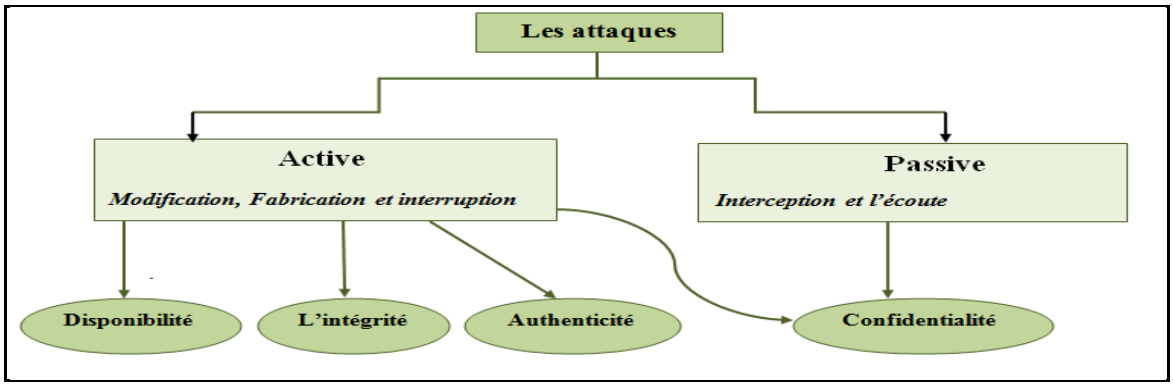


Figure II. 1: Classification des attaques

II.5.1 Objectifs des attaques

II.5.1.1 Interception

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

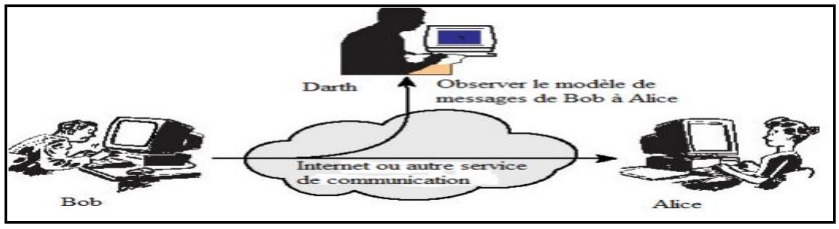


Figure II. 2: Attaque d'accès

II.5.1.2 Interruption

Dans laquelle un attaquant non autorisé essaie de se présenter comme une autre entité. Il s'agit d'une attaque sur la disponibilité des ressources.

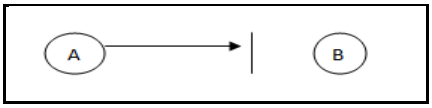


Figure II. 3: Attaque d'interruption

II.5.1.3 Modification

Implique une modification du message original, c'est-à-dire un troisième personne non autorisée intercepte des données et les altérés avant de les émettre au destinataire. Il s'agit d'une attaque sur l'intégrité de l'information. Elle peut se présentée sous forme de : virus, sflooding, XSS,…etc.

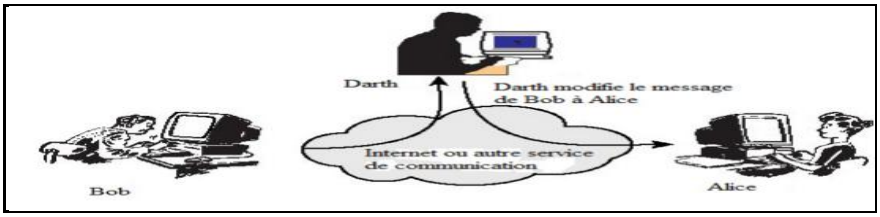


Figure II. 4: Attaque de modification

II.5.1.4 Fabrication

Il peut s'agir de l'insertion des données contrefaites dans les communications de l'application, de faux messages dans un réseau ou l'ajout d'enregistrements à un fichier. Il s'agit d'une attaque sur l'authentification.

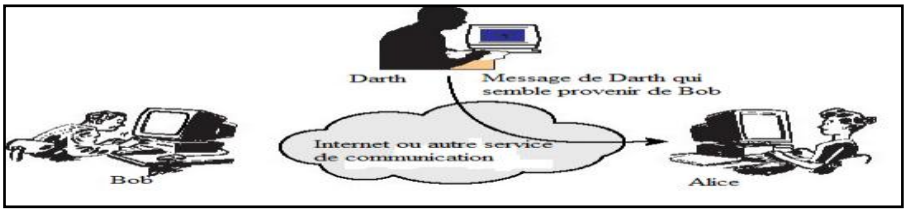


Figure II. 5: Attaque de fabrication

II.5.1.5 Rejeu

L'attaquant qui a réussi à intercepter des messages les réémet tels quels (sans aucun déchiffrement) au serveur destinataire dans le but d'obtenir des informations ou de perturber la cible de l'attaque. Nous considérons qu'il s'agit d'une attaque sur l'intégrité des messages.

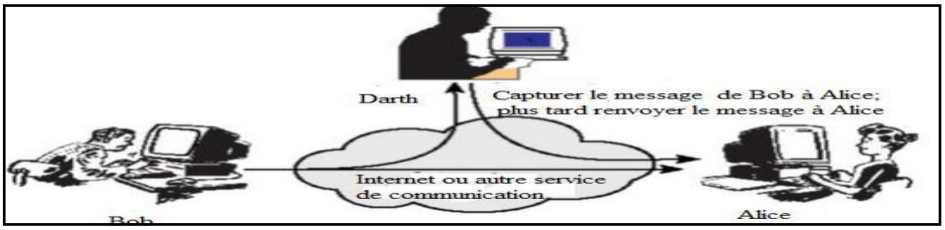


Figure II. 6: Attaque de rejeu

II.5.2 Les techniques d'attaque

II.5.2.1 Spoofing

Nous trouvons 3 attaques Spoofing principales :

II.5.2.1.1 IP spoofing

Est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par une fausse adresse IP d' une autre machine [9], le pirate commence par choisir le système qu'il veut attaquer, ensuite, après avoir obtenu le maximum de détails sur le système cible, il détermine les systèmes ou adresses IP autorisés à se connecter au se système. Grâce à cette fausse redirection, l'utilisateur peut envoyer son identifiant en toute confiance. Elle peut être classée dans les attaques de fabrication.

II.5.2.1.2 Spoofing ARP

Est une technique utilisée en informatique pour attaquer tout réseau local utilisant le protocole de résolution d'adresse ARP, il permet de modifier le cache ARP qui contient une association entre les adresses matérielles des machines et les adresses IP, les cas les plus répandus étant les réseaux Ethernet et Wifi [10] l'objectif du pirate est de conserver son adresse MAC, mais d'utiliser l'adresse IP d'un hôte approuvé. Une fois l'adresse MAC de l'attaquant connectée à une adresse IP authentique, l'attaquant commencera à recevoir toutes les données destinées à cette adresse IP.

II.5.2.1.3 Spoofing DNS

Est une cyberattaque visant le DNS[4] qui consiste à faire parvenir de fausses réponses aux requêtes DNS émises par une victime c'est-à-dire l'adresse IP correspondant à un domaine est en particulier faussée. Le terminal établit donc une connexion avec la mauvaise adresse IP et le trafic de données est redirigé vers le mauvais serveur [11]. Il existe deux types de méthode :

- ***DNS ID spoofing :*** L'attaquant essaie de répondre, avec une fausse réponse à un client avant que le serveur DNS répond.
- ***DNS Cache Poisoning :*** L'attaquant essaie d'empoisonner le cache (table de correspondance IP-NomMachine) du serveur DNS avec d'autres informations.

II.5.2.2 Man in the middle

Dite en français l'homme au milieu, c'est une attaque d'interception, consiste d'intercepter les communications entre deux entités sans que l'une ni l'autre ne puisse se douter que le canal de communication est compromis [12], l'objectif de l'attaquant est d'intercepter, de lire ou de manipuler toute communication entre la victime et sa ressource sans se faire remarquer.

II.5.2.3 XSS (Cross-Site Scripting)

Script intersites est une faille de sécurité des sites web permettant d'injecter du contenu dans une page, provoquant ainsi des actions sur les navigateurs web visitant la page [13], donc l'attaquant parvient à injecter son propre code dans l'application. Ce code sera ensuite exécuté lorsque les utilisateurs visitent la page, ce qui lui permet de voler des cookies[5] ou de consigner toutes les pressions de touche [14]. Elle peut être classée dans les attaques de modifications.

II.5.2.4 Dénis de service (DoS : Denial of Service)

C'est une attaque d'interruption visant à rendre indisponible un service (serveur web, serveur de messagerie) et donc à empêcher les utilisateurs légitimes d'un service de l'utiliser. Il exploite les faiblesses de l'architecture d'un réseau ou d'un protocole ce qui permet de bloquer les réponses système, de ce fait, les utilisateurs ne peuvent plus accéder aux ressources [15]. Il en existe plusieurs types comme le flooding…etc.

---

[44] DNS est un service permettant d'établir une correspondance entre un nom de domaine lisible par l'homme et une adresse IP lisibles par une machine.

[5] Un cookie est un fichier texte qui est déposé par votre navigateur sur votre ordinateur lorsque vous surfez sur Internet

II.5.2.5 Attaques virales

II.5.2.5.1 Virus

Désigne, dans l'univers informatique, un programme malveillant dont l'objectif principal est de perturber le bon fonctionnement d'un appareil, la plupart du temps un ordinateur sans autorisation [16], donc il contrôle des ressources de l'ordinateur pour se répliquer, se diffuser et causer toutes sortes de problèmes. Se fixe sur un programme ou un fichier à partir duquel il peut se propager d'un ordinateur à l'autre, semant des infections partout où il passe.

Presque tous les virus sont inclus dans un fichier exécutable, ce qui signifie que le virus peut être présent sur votre ordinateur mais en réalité, il ne peut pas l'infecter si vous n'exécutez pas ou n'ouvrez pas le programme. Il est important de noter qu'un virus ne peut pas se répandre sans une intervention humaine [17]

II.5.2.5.2 Les vers

Il s'agit d'un programme malveillant qui peut se reproduire[6] et se déplacer à travers des réseaux informatiques (comme l'internet) pour infecter des machines connectées sans l'aide des utilisateurs [18], donc ne nécessitent pas d'intervention humaine ni de support logique ou physique (clé USB, disque dur, programme hôte …). Ils sont dangereux car ils exploitent les vulnérabilités informatiques pour s'insérer dans une machine. Une fois qu'ils y sont parvenus, il est extrêmement difficile de les arrêter car ils se déplacent partout pour rechercher leur cible.

II.5.2.5.3 Chevaux de Troie

Est un type de programme malveillant caché dans un logiciel à l'apparence légitime qui convainc l'utilisateur et peut être téléchargé en toute confiance sur des ordinateurs, mais qui contient une fonctionnalité malveillante permet de perturber le fonctionnement d'un ordinateur ou d'en prendre le contrôle donc il donne un accès à un ordinateur en ouvrant une porte dérobée (en anglais backdoor[7]). C'est-à-dire une fois que le cheval de Troie est téléchargé et activé, les cybercriminels peuvent prendre le contrôle de l'appareil lui-même [19].

II.5.2.6 Attaque de mot de passe

Nous trouvons l'utilisation du mot de passe presque partout pour interdire l'accès (à un ordinateur, à un fichier, à un répertoire, à un programme, à un site, à une fonction...) c'est pour ça plusieurs techniques se sont développées pour les attaquer et casser ce niveau de sécurité. Nous trouvons les attaques les plus classiques suivante :

[6] C'est-à-dire au lieu d'expédier un seul ver, un ordinateur peut en expédier des centaines ou des milliers de copies

[7] Une backdoor est un moyen d'accéder à un système informatique ou à des données cryptées qui contournent les mécanismes de sécurité habituels du système

II.5.2.6.1 Attaque par force brute (recherche exhaustivité)

Est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé cryptographique, son principe consiste à essayer avec un logiciel et un simple algorithme toutes les combinaisons possibles jusqu'à trouver la bonne. C'est Une méthode efficace pour les mots de passes courts et simples, car ils sont facile à craqué. [20]

II.5.2.6.2 Attaque par dictionnaire

Est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Elle consiste à tester une série de mots de passe potentiels ayant une signification réelle, les uns à la suite des autres, en espérant que le mot de passe utilisé pour le chiffrement soit contenu dans le dictionnaire. Si ce n'est pas le cas, l'attaque échouera [21].

II.6 Mécanismes de sécurité

II.6.1 Le cryptage (chiffrement)

La cryptographie est une science basée sur les mathématiques, ce base sur la conversion des données d'un format lisible à un format codé qui peut uniquement être lu ou traité après déchiffrement par une personne ayant les moyens de le ramener à son état d'origine [22]. Le principal objectif du chiffrement consiste à garantir la confidentialité des données numériques stockées sur des systèmes informatiques ou transmises via Internet ou d'autres réseaux. Il existe deux types de chiffrement moderne :

- ***Chiffrement symétrique :*** Ou chiffrement à clé secrète, utilise la même clé pour le chiffrement et le déchiffrement des données et la clé doit être partagée secrètement avec le destinataire.

Figure II. 7: Cryptographie symétrique

- ***Chiffrement asymétrique :*** Ce chiffrement est aussi appelé chiffrement à clés publiques, utilise une paire composée d'une *clé publique* pour le chiffrement, et d'une *clé privée* pour le déchiffrement.

Figure II. 8: Cryptographie asymétrique

II.6.1.1 Fonction de hachage

C'est une fonction qui transforme une donnée quelconque en une donnée de taille fixée. Nous devons avoir les propriétés suivantes :

- Associer un et un seul condensé (haché) à un texte en clair.
- Une fonction à sens unique non-inversable (impossible de retrouver le message original à partir du condensé).
- Le haché représente en quelque sorte l'empreinte digitale du document.
- Ne reposent sur aucun secret.
- Déterministe : la même entrée fournit toujours le même hash.
- Non-continuité : un changement léger dans le message en entrée de la fonction de hachage doit produire une sortie complètement différente.
- Rapidité : la valeur de hash se calcule "très rapidement".

En particulier, en cryptographie, les algorithmes de hachage doivent montrer certaines résistances :

- Résistance à la préimage : pour une valeur *h* de hash donnée, il est très difficile de trouver un message *m* tel que *h* = hash(*m*).
- Résistance à la seconde préimage : pour un message *m* donné, il est très difficile de trouver un message *m'* tel que hash(*m*) = hash(*m'*).
- Résistance à la collision : il est très difficile que deux messages différents produisent la même sortie.

II.6.1.1.1 Les algorithmes de la fonction d'hachage

Dans le domaine de la sécurité, Il existe plusieurs algorithmes différents qui permettent d'obtenir une empreinte, le Message Digest 5 (MD5) et le Secure Hash Algorithm (SHA1) sont les deux algorithmes de hachage les plus utilisés au monde à l'heure actuelle en matière d'empreinte numérique et de cryptographie. Leur rôle est multiple, ils permettent par exemple de vérifier l'intégrité de fichiers ou messages, la vérification de mot de passe ou encore l'identification de fichiers ou données.

II.6.1.1.1.1 Le Message Digest 5 (MD5)

Est une fonction de hachage cryptographique qui permet d'obtenir pour chaque message une *empreinte numérique* (en l'occurrence généré une clef de 128 bits), développé par RSA[8]

[8] RSA est un système cryptographique, pour le chiffrement à clé publique. Il est souvent utilisé pour la sécurisation des données confidentielles, en particulier lorsqu'elles sont transmises sur un réseau peu sûr comme Internet.

[23]. Elle permet de vérifier l'intégrité des données d'un message de façon beaucoup plus sûre que le classique contrôle de parité.

Lors du transfert d'un message signé par une clé MD5, l'ordinateur émetteur génère une clé MD5, sorte d'empreinte digitale du message, puis envoie le message et la clé au destinataire.

A la réception le destinataire va de nouveau calculer la clé MD5 du message et la comparer avec celle envoyée par l'émetteur. Si les deux clés sont identiques, la transmission s'est bien passée, dans le cas contraire le destinataire sait que le message a été altéré durant la transmission et peut éventuellement demander sa réémission.

II.6.1.1.1.2 Secure Hash Algorithm (SHA_1)

Désigne une fonction de hachage cryptographique conçue par l'Agence Nationale de Sécurité américaine (NSA) [24]. Elle produisait des empreintes 160 bits qui permet d'identifier la donnée initiale et de garantir son intégrité, ce qui est utile en cryptographie.

Il est utilisé notamment dans le cadre de protocoles Internet et applications sécurisés comme TLS et SSL, SSH.

- **Protocole SSH** (ou Secure Socket Shell) : Est un protocole qui facilite les connexions sécurisées entre deux systèmes à l'aide d'une architecture client/serveur et permet aux administrateurs d'accéder à distance à un ordinateur, en toute sécurité [25].

    - De sorte que ce mécanisme **crypté** donc il assure la **confidentialité** et **l'intégrité** des données échangées (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau.
    - Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur.
    - Utilise les deux chiffrements : symétrique et asymétrique.
    - Permet aux administrateurs de contrôler, configurer, modifier leurs serveurs et d'exécution des commandes à distants sur Internet. Ainsi ils peuvent envoyer des données **confidentielles au serveur** telles que nom d'utilisateur, mot de passe et autres commandes de manière sécurisée car toutes ces données sont cryptées et ne peuvent pas être déchiffrées et lues facilement par les pirates.

II.6.1.2 Signature numérique

Est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier. Elle se

différencie de la signature écrite par le fait qu'elle n'est pas visuelle, mais correspond à une suite de caractères.

L'objectif majeur de la signature électronique est :

- Authentifier le signataire
- Garantir l'intégrité du document (garantir que le document n'a pas été altéré entre l'instant où l'auteur l'a signé et le moment où le lecteur le consulte)
- Assurer la non-répudiation, c'est-à-dire que l'émetteur du document ne peut pas nier l'avoir envoyé.

La signature d'un document utilise à la fois la cryptographie asymétrique et les fonctions de hachage. C'est en effet par l'association de ces deux techniques que nous pouvons obtenir les 5 caractéristiques d'une signature (authentique, infalsifiable, non réutilisable, inaltérable, irrévocable).

- **Authentique** : l'identité du signataire doit pouvoir être retrouvée de manière certaine
- **Infalsifiable** : une personne ne peut pas se faire passer pour un autre
- **Non réutilisable** : la signature fait partie du document signé et ne peut être déplacée sur un autre document
- **Inaltérable** : une fois que le document est signé, on ne peut plus le modifier
- **Irrévocable** : la personne qui a signé ne peut le nier [26]

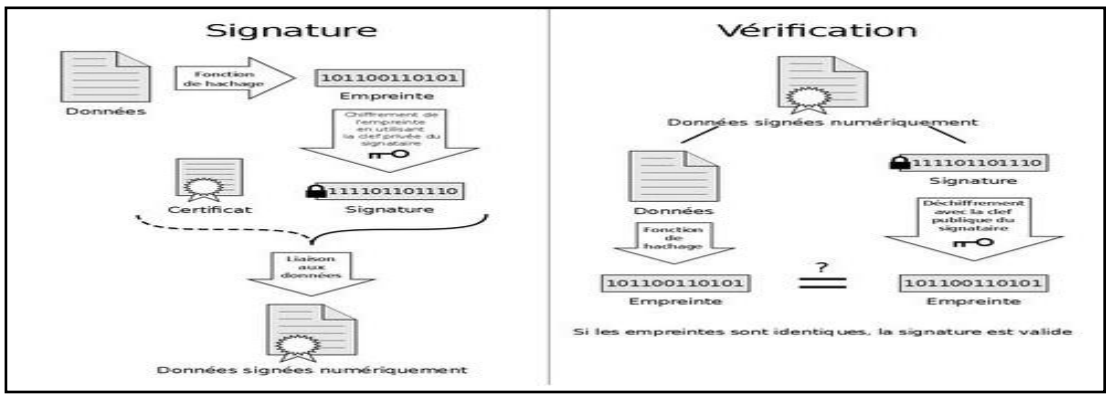


Figure II. 9: la signature et la vérification d'un document (Voir l'annexe E)

II.6.1.3 Certificat numérique

Le problème de clés publiques est qu'un pirate peut arriver à remplacer la clé publique d'un utilisateur X par la sienne, par exemple sur un annuaire, et toutes les personnes croyant encrypter pour l'utilisateur X encrypterons pour le pirate. Les systèmes à clés publiques ne garantissent donc pas que la clé est bien celle de l'utilisateur à qui elle est censée appartenir.

Les certificats électroniques servent à cela: ils permettent de lier de façon sûre une clé publique à une entité (utilisateur, serveur, etc.). Un certificat contient les informations

suivantes: un numéro de série, une clé publique, l'identifiant du propriétaire de la clé publique, la date de validité (date de début et date de fin de validité), l'identifiant de l'autorité de certification émettrice du certificat, la signature du certificat à l'aide de la clé privée de l'autorité de certification. Toutes ces informations sont signées et délivrées par un tiers de confiance appelé: autorité de certification (souvent notée CA pour Certification Authority). La clé publique ayant été préalablement largement diffusée afin de permettre aux utilisateurs de vérifier la signature avec la clé publique de l'autorité de certification.

II.6.2 L'antivirus (Voir l'annexe E)

II.6.3 La technologie AAA

Est un protocole de sécurisation des équipements réseaux dont les trois lettres signifient : Authentication, Authorization et Accounting.

- **L'authentification :** permet de contrôler l'accès à des ressources spécifique via un « Nom d'utilisateur / mot de passe » dans notre cas, elle est utilisé afin d'avoir accès à nos équipements réseaux.
- **L'Autorisation :** donne à l'utilisateur les droits de faire certaines actions ou encoure l'interdiction d'accéder à d'autre actions.
- **Traçabilité :** permet de tracer tous les faits et gestes des utilisateurs qui se sont authentifiés et qui ont été autorisés à accéder à l'équipement comme les commandes utilisé, le mode de configuration, la date et l'heure de connexion…etc. Ce qui permet alors aux administrateurs réseaux de vérifier les actions d'un utilisateur en cas de problèmes et de les résoudre rapidement et d'augmenter considérablement la sécurité réseau.

On trouve les protocoles AAA comme RADIUS, Diameter, TACACS

II.6.4 Systèmes de détection d'intrusions IDS

Est un système qui analyse et surveille le trafic réseau provenant de l'extérieur ainsi à l'intérieur, pour détecte toute activités anormales ou suspectes et toute violation de politique de sécurité, sans modifier en aucune façon les paquets réseau, [27], permet ainsi d'avoir une action de prévention sur les risques d'intrusion.

Les IDS peuvent être déployés en plusieurs endroit du réseau afin d'augmenter la sécurité, ils sont généralement de deux types :

- Les N-IDS (Network Based Intrusion Detection System), ils assurent la sécurité au niveau du réseau.
- Les H-IDS (Host Based Intrusion Detection System), ils assurent la sécurité au niveau des hôtes.

II.6.5 Systèmes de prévention d'intrusion IPS

Sont des dispositifs de sécurité réseau qui surveillent les activités du réseau ou du système pour détecter toute activité malveillante [28], comme les IDS mais celle-ci

constituent un système de contrôle qui accepte ou rejette un paquet en fonction d'un ensemble de règles, tout comme un pare-feu bloque le trafic en se basant sur l'adresse IP.

II.6.6 Les ACL

Les Access Control List (ACL) permettent notamment de faire du filtrage des paquets IP (niveau 3), c'est à dire de définir des droits d'accès aux utilisateurs du réseau donc elles permettent d'autoriser ou d'interdire la commutation des paquets, que ce soit en entrée ou en sortie vers une destination, en fonction d'un certain nombre de conditions ou de critères, tels que :

- Les adresses sources et destinations,
- Les protocoles de couches supérieures telles qu'UDP, les numéros de port
- Des paramètres dynamiques basés sur le temps : 2 heures sur une période de 24 heures. [29]

II.6.6.1 Les types d'ACL

Il existe 3 types de liste de contrôle d'accès :

II.6.6.1.1 Les ACLs standards

Qui filtrent sur l'adresse source, comparent l'adresse de la source du paquet IP aux adresses configurées dans l'ACL afin de contrôler le trafic.

Après avoir accéder au mode de configuration globale on applique la règle qui permet de créer l'ACL standard

Access-list ***Number*** {***permit | deny***} ***@IP source*** [***masque générique***]

1. ***Number :*** numéro de l'ACL. (1 – 99 ou 1300 - 1999).
2. ***Permit | deny :*** Choix de l'action, autoriser ou interdire le trafic.
3. ***Adresse source :*** Identifie l'adresse IP source.
4. ***Masque générique :*** Toute adresse IP vérifiée par une instruction ACL se voit appliquer le masque générique correspondant à l'instruction.

Le numéro d'ACL « Number » est attribué à chacune des instructions qui composent la liste. Chaque nouvelle instruction créée vient s'ajouter après les instructions déjà créés (c'est à dire en bas de la liste).

II.6.6.1.2 Les ACLs étendues

Qui filtrent sur l'adresse source, l'adresse destination ainsi que les ports sources et destination.

La syntaxe de la commandes permettent de créer l'ACL étendue est la suivante :

Access-list ***Number*** {***permit*** **|** ***deny***} ***Protocol*** ***@IP source*** [masque source générique] ***@IP destination*** [masque destination générique] ***Opérateur Opérande***

1. ***Number :*** numéro de l'ACL. (100 -199 ou 2000-2699)
2. ***Permit / deny :*** autoriser ou interdire le trafic.
3. ***Protocole :*** Type du protocole (IP, TCP, UDP, ICMP…).
4. ***Adresse source / destination :*** Identifie l'adresse IP source, et destination.
5. ***Opérateur :*** Opérateur à choisir parmi les opérateurs suivant :

Tableau II. 1: Tableau d'Opérateur

It	Less than	Plus petit que
Gt	Creater Than	Plus grand que
Eq	Equal	Egale à
Neq	Not equal	Différent de
Range	Range	Plage inclusive

Un opérateur placé après l'adresse source teste le port source, un opérateur placé après l'adresse destination teste le port destination.

6. ***Opérande :*** Numéro de port, optionnel, qu'il s'agisse du protocole UDP ou du protocole TCP, les champs port source et destination sont exprimés en 16 bits. Le numéro de port s'étend donc de 0 à 65535.

II.6.6.1.3 Les ACLs nommées

Il est ainsi possible de modifier le numéro qui permettait de définir le type de liste d'accès, standard ou étendue, en attribuant des noms à ces listes d'accès. La syntaxe est un peu modifiée, car on doit spécifier le type de l'ACL, la syntaxe est donc la suivante :

IP Access-list {***extended*** **|** ***standard***} ***nom_Acl***

II.6.7 Le NAT (Network Address Translation):

Les adresses IP sont classées en deux catégories: publiques et privées. Donc les adresses IP utilisées en interne (privées) sont généralement non routables, et ne sont donc pas utilisables directement sur l'Internet, c'est pour cette raison que la translation d'adresse est utilisée pour permettre aux machines du réseau privé d'accéder à Internet, de façon générale à d'autres réseaux et réduit le besoin d'adresses publiques IPv4. Le processus est généralement effectué par des routeurs ou des pare-feu.

Il existe trois types de traduction d'adresses:

1. **NAT statique** : traduit une adresse IP privée en une adresse publique. L'adresse IP publique est toujours la même.
2. **NAT dynamique** : les adresses IP privées sont mappées au pool d'adresses IP publiques (associe une seule adresse à n adresses).

3. **Traduction d'adresse de port (PAT)** : une adresse IP publique est utilisée pour tous les périphériques internes, mais un port différent est attribué à chaque adresse IP privée. Également connu sous le nom de surcharge NAT. [30]

II.6.8 Les VPN

II.6.8.1 Réseau privé

Constitué de différents appareils et machines qui travaillent ensemble (partage de ressources) dans un même organisme ou entreprise (réseau interne).

II.6.8.2 Réseau privé virtuel (VPN)

Est un système informatique destiné à vous protéger lorsque vous surfez sur internet. C'est un tunnel à l'intérieure du réseau internet qui permet d'échanger des informations de manière sécurisée et anonyme en utilisant une adresse IP différente de celle de votre ordinateur. Il isole donc les échanges du reste du trafic [31]

Ce réseau est dit virtuel car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet comme support de transmission), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent accéder aux données en clair.

Un utilisateur non autorisé, ne peut en aucun cas avoir accès aux données transmises sur le réseau et en cas d'interceptions, les informations interceptées sont cryptées, illisibles, et donc inutilisables. Le VPN permet donc d'obtenir une liaison sécurisée à moindre coût qui vise à apporter certains éléments essentiels dans la transmission de données:

- L'authentification (et donc l'identification) des interlocuteurs,
- La confidentialité des données (le chiffrement vise à les rendre inutilisables par quelqu'un d'autre que le destinataire).

II.6.8.3 Principe de fonctionnement

Un réseau privé virtuel repose sur un protocole, appelé protocole de tunneling, qui permet de faire circuler les informations de façon cryptée d'un bout à l'autre du tunnel tout se passe exactement comme si la connexion se faisait en dehors d'Internet après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel (tunnel).

Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et serveur VPN(ou plus généralement serveur d'accès distant) l'élément chiffrant et déchiffrant les données du coté de l'organisation.

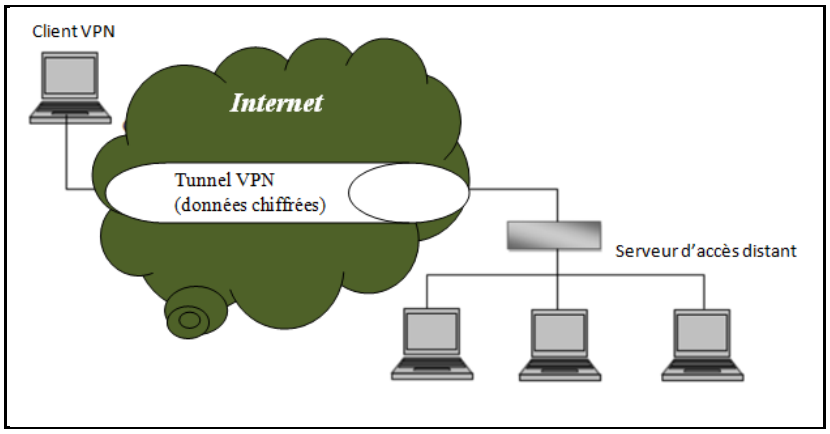


Figure II. 10: Tunnel d'un VPN

II.6.8.4 Protocoles de tunneling

Un protocole VPN constitue la base de tout service VPN. C'est le garant de la sécurité et de la transmission efficace des données acheminées entre le client et le serveur VPN. Il existe de nombreux types de protocoles VPN disponibles, chacun ayant des forces et des capacités différentes

II.6.8.4.1 PPTP (*point-to-point tunneling protocol*)

C'est un protocole de la couche liaison de données le plus ancien, le plus facile à configurer et à utilisé. Offrir une performance stable et une vitesse fiable mais ne fournit aucun cryptage de données ou aucune mesure de sécurité supplémentaire [32].

II.6.8.4.2 Protocole L2TP (*Layer 2 Tunneling Protocol*)

Est un protocole réseau de la couche liaison de données originaire du L2F de Cisco et du PPTP de Microsoft, Il n'a aucun capacité de cryptage ou de confidentialité, c'est donc pour cette raison qu'il est généralement s'appuis sur un protocole de cryptage (comme IPSec) qui passe dans le tunnel pour assurer la confidentialité [32].

II.6.8.4.3 L2F (LayerTwoFowarding)

Est un protocole niveau 2 qui implémenté dans le système d'exploitation IOS (InternetworkingOperatingSystem)

II.6.8.4.4 OpenVPN

Est un protocole populaire car il est open source, gratuit et le plus utilisé actuellement. Il offre la meilleure vitesse et une plus grande sécurité et fiabilité avec différentes options de chiffrement (comme par exemple utilisation des certificats numérique pour l'authentification)

Il peut utiliser deux protocoles de transport : TCP et UDP [33], et peut aussi fonctionner sur n'importe quel port comme le port 443 de HTTPS

II.6.8.4.5 Le protocole SSL/ TLS (Secure Sockets Layers)

SSL est un protocole de communication sécurisé de la couche session du modèle OSI basé sur le chiffrement. Il a été développé dans le but de garantir la confidentialité, l'authentification et l'intégrité des données dans les communications internet.

SSL a finalement évolue vers TLS (Transport Layer Security).

II.6.8.4.6 Protocole IPsec (Internet Protocol Security)

Est une suit de protocole normalisés par l'IETF[9], il a été conçu pour sécuriser les communications réseau à partir de la couche réseau ce qui lui permet donc de sécuriser tout type d'applications et protocoles réseau basés sur IP avec l'utilisation des services de sécurité cryptographique.

Le protocole IPSec vient complémenter le protocole IP pour cela fait appel à deux entêtes de sécurité l'en-tête d'authentification (AH, Authentication Header) et l'en-tête de confidentialité-authentification (ESP, Encapsulating Security Payload Header). Qui permet d'intégrer des notions essentielles de sécurité suivantes :

- L'authentification
- L'intégrité
- Confidentialité
- La non-répudiation
- Protection contre les écoutes et analyses de trafic
- L'anti-rejeu

Basé sur deux modes

- **Mode transport:** le mode transport est souvent utiliser pour protéger les données en provenance de couches supérieures (généralement ce sont des données). Dans ce mode, les entêtes IP ne sont pas modifiés, on chiffre ou on authentifie juste la partie data d'un paquet IP
- **Mode tunnel:** dans le mode tunnel on protège tout le paquet (y compris l'entête IP) et on l'encapsule dans un nouveau paquet avec un nouvel entête IP

[9]IETF est le premier organisme de normalisation Internet, développant des standards ouverts via des processus ouverts pour améliorer le fonctionnement d'Internet.

II.6.8.5 Typologies des VPN

Il existe deux catégories de VPN: VPN d'entreprise et VPN d'opérateur qui peuvent être utilisé simultanément ou séparément au sein d'une même entreprise.

II.6.8.5.1 VPN d'entreprise

Il existe trois types qui sont: les VPN site à site, les VPN poste à site, et les VPN poste à poste.

II.6.8.5.1.1 VPN site à site

Il s'agit de relier deux sites d'une même entreprise ou bien le site d'une entreprise et celui d'un fournisseur, ou d'un client c'est à dire se base sur l'intranet afin de relier le réseau des bureaux principaux au reste des bureaux d'une même entreprise, et se base sur extranet lorsqu'il s'agit de relier une entreprise à une autre

Généralement ce type de VPN est mis en place par l'interconnexion de deux éléments Matériels (routeurs ou pare-feu) situés entre le réseau interne et le réseau publique de chaque site et se sont ces derniers qui se chargent de l'authentification, du routage des paquets, du cryptage et du décryptage

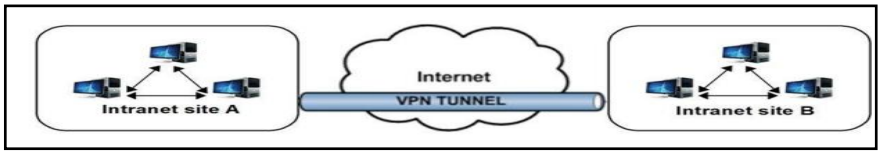


Figure II. 11: VPN site à site

II.6.8.5.1.2 VPN poste à site

Ce type de VPN est aussi fréquemment utilisé et permet aux utilisateurs distants d'accéder aux ressources de l'entreprise via un VPN Il existe deux cas :

- L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS[10] (Network Access Server) du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.
- L'utilisateur distant a simplement besoin d'un client VPN installé sur son ordinateur pour se connecter directement au site de l'entreprise de manière cryptée.

[10] NAS (**serveur de stockage en réseau)** est un serveur de fichiers autonome, relié à un réseau, dont la principale fonction est le stockage de données en un volume centralisé pour des clients réseau

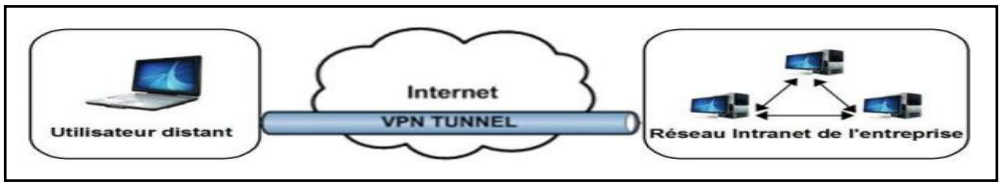


Figure II. 12: le VPN d'accès

II.6.8.5.1.3 VPN poste à poste

L'objectif de ce type d'architecture est d'établir un canal sécurisé de bout en bout entre deux postes ou, plus couramment, entre un poste et un serveur. Le poste et le serveur peuvent être situés sur le même réseau ou sur deux réseaux différents reliés eux-mêmes par un VPN site à site.

II.6.8.5.2 VPN opérateur

C'est un réseau privatif mis en place par un opérateur afin d'interconnecter plusieurs sites d'une entreprise. Ce type de réseau est plus couteux que les VPN d'entreprise mais offre de grandes performances, la disponibilité et une communication sécurisée entre les différents sites. On parle alors plus de réseaux de tunnels que de véritable réseau VPN.

II.6.9 Les VLAN

Un VLAN (Virtual Local Area Network ou Virtual LAN, en français Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique distribué sur des équipements fonctionnant au niveau deux et trois du modèle OSI [34], C'est-à-dire il segmente les réseaux commutés (utilisateurs, périphériques, etc.) en différents domaines de broadcast de manière logique sur la base des fonctions, des équipes de projet ou des applications de l'entreprise, quel que soit l'emplacement physique ou les connexions au réseau.

II.6.9.1 Les typologies d'un VLAN

Plusieurs types de VLANs sont définis, selon le critère de commutation et le niveau auquel il s'effectue, il faut tout d'abord des commutateurs spéciaux de niveau deux du model OSI qui supportent le VLAN. Il existe plusieurs méthodes de construction:

II.6.9.1.1 VLAN de niveau 1

Appelé aussi VLAN par port. Par l'administrateur chaque port d'un commutateur est attribué à un VLAN. Toutes les stations connectées à un port appartiennent au VLAN correspondant, lorsqu'une station est déplacée sur un autre port, celui-ci est également attribué au VLAN de la station. De même, si une station change de VLAN, le port auquel elle

est connectée est attribué à son nouveau VLAN. C'est une contrainte qu'il faut gérer lorsque le réseau s'agrandit

Les VLAN par ports sont facile à mettre en place et offrent une bonne flexibilité en utilisant le protocole DHCP[11] (*Dynamic Host Configuration Protocol*) cependant tout déplacement d'une station nécessite une reconfiguration des ports (Manque de souplesse).

II.6.9.1.2 VLAN de niveau 2 (*par Adresse IEEE*)

Appelé aussi VLAN MAC. L'adresse MAC d'une machine est affectée à un VLAN. En pratique, c'est encore le port qui est affecté à un VLAN, mais de manière dynamique. En effet, l'administrateur saisit dans la table du switch le couple adresse MAC/VLAN. Lorsque le switch découvre sur quel port est connecté la machine, il affecte dynamiquement le port au VLAN. Il gère donc une deuxième table, la table port/VLAN. Cette structure permet également de définir plusieurs VLAN par port à condition d'utiliser le marquage [35]

L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation géographique. Si une station est déplacée sur le réseau physique, son adresse physique ne change pas, elle continue d'appartenir au même VLAN (ce fonctionnement est bien adapté à l'utilisation des machines portables). Si on veut changer de VLAN il faut modifier l'association Mac / VLAN.

II.6.9.1.3 VLAN par protocole et par sous-réseau

Sont les VLAN de niveau 3 on distingue deux types

II.6.9.1.3.1 Le VLAN par protocole

(*En anglais Protocol-Based VLAN*) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, etc.), regroupe ainsi toutes les machines utilisant le même protocole au sein d'un même réseau [36]. Avec les réseaux VLAN basés sur les protocoles, c'est le protocole de couche 3 transporté par la trame qui permet de déterminer l'appartenance aux réseaux VLAN. Cette méthode peut fonctionner dans un environnement où figurent plusieurs protocoles

II.6.9.1.3.2 VLAN par Sous-réseau

Un VLAN par sous réseau utilise les adresses IP. Un réseau virtuel est associé à chaque sous réseau IP. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une

[11] DHCP est le protocole qui permet à un ordinateur qui se connecte sur un réseau d'obtenir *dynamiquement* sa configuration (principalement, une adresse IP et un masque de sous-réseau). Le but principal étant la simplification de l'administration d'un réseau.

station mais il souffre de lenteur par rapport aux Vlan de niveau 1 et 2. En effet, le commutateur est obligé de décapsuler le paquet jusqu'à l'adresse IP pour pouvoir détecter à quel VLAN il appartient. Il faut donc des équipements plus couteux (car ils doivent pouvoir décapsuler le niveau 3) pour une performance faible.

II.6.9.2 Les avantages d'un VLAN

- Augmentation des performances : Contrôler la taille des domaines de broadcast et de ce fait réduire le nombre de collisions sur ces domaines.
- Gérer correctement la mobilité des postes
- Les utilisateurs sont affectés par logiciel aux différents VLANs
- Une station peut appartenir à plusieurs VLAN simultanément
- La simplification de la gestion : Les domaines de broadcast sont définis administrativement donc l'ajout de nouveaux éléments ou le déplacement d'éléments existants peut être réalisé rapidement et simplement sans devoir manipuler les connexions physiques dans le local technique.
- Augmentation de la sécurité : Grâce à la notion des groupes, qui conduit à l'isolement des utilisateurs selon leurs centres d'intérêts, certaines ressources seront alors protégées, ainsi il y aura un renforcement considérable de la sécurité du réseau.
- une organisation efficace du réseau.
- Meilleures performances : La création de domaine de diffusion plus petit amène une diminution de la quantité de trafic inutile sur le réseau, qui résulte une augmentation des performances.

II.6.10 Les pare-feu

II.6.10.1 Définition

(*Appelé aussi Coupe-feu, Garde-barrière ou Firewall*) est un élément du réseau informatique, logiciel et/ou matériel) qui permet de protéger une machine ou un réseau quelconque et contrôle le trafic intérieur/extérieur qui le traverse, selon une politique d'accès aux ressources informatiques, [37] celle-ci définissant quels sont les communications autorisés ou interdits.

Il comporte au minimum deux interfaces réseau :

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

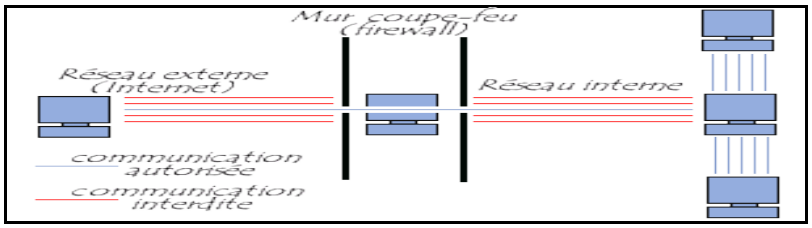


Figure II. 13: Les interfaces réseau d'un pare-feu et les type de communication

II.6.10.2 Fonctionnement d'un pare-feu

Le pare-feu est l'un des outils de sécurité informatique les plus anciens et les plus couramment déployés, Lorsqu'on est connecté à Internet, notre ordinateur peut-être à tout moment la cible d'une attaque. Donc on doit le protégé en installant la diapositif de protection (pare-feu) qui contient un ensemble de règles prédéfinies permettant :

- De filtrer et n'autoriser la connexion que sous certaines conditions (adresse IP et port), avec la commande ***[Allow]***
- De bloquer la connexion et empêcher toute intrusion dans le réseau à l'aide de [***Deny,Rejeter]***
- La demande de connexion sans avertir l'émetteur à laide de [***Drop]***
- Aussi de contrôler les sorties des utilisateurs internes.

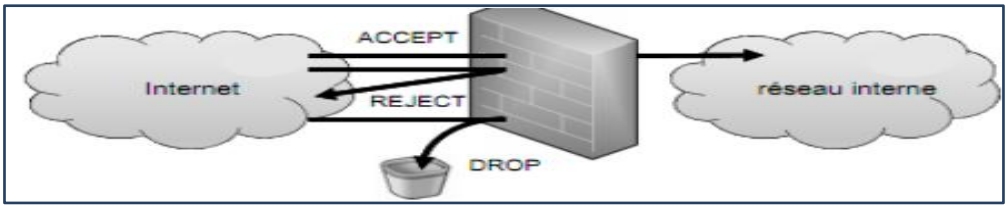


Figure II. 14: Fonctionnement d'un pare-feu

Pour réaliser cela, un pare-feu se base sur les couches 3 (IP), 4 (TCP/UDP donc les ports) et la couche 7(applicative) du modèle OSI pour contrôler les flux et de les bloquer en cas d'attaques

Pour les couches 3 et 4 permet de contrôler les adresses IP et les ports par exemple

- Bloquer SSH ou Telnet
- Créer une règle qui accepte les connexions des protocoles TCP/UDP vers le port 80 (http) c'est-à-dire n'importe quelle machine connectée au réseau Internet est autorisée à accéder au service web.

Alors qu'un pare-feu qui se base sur la couche 7 permet lui de bloquer l'utilisation d'un logiciel par exemple

L'ensemble de ces règles permettent de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. Chaque paquet traversant le pare-feu est soumis à ces règles. On distingue habituellement deux types de politiques de sécurité permettant :

- Soit d'autoriser uniquement les communications ayant été explicitement autorisées : « tout ce qui n'est pas explicitement autorisé est interdit »
- Soit d'empêcher et Bloquer les échanges qui ont été explicitement interdites.

Donc il est très important de noter qu'un pare-feu doit être à la mesure de politique de sécurité globale du réseau par ce que ne protège pas des attaques qui ne passent pas par lui ainsi les menaces existante à l'intérieur de l'entreprise , et ne protègent pas très bien des virus.

En d'autres termes, un firewall ne pourra pas remplacer l'attention et la conscience des utilisateurs qui doivent respecter un certain nombre de règles pour éviter les problèmes. La première étant bien évidemment de ne jamais ouvrir un fichier attaché à un mail sans être sûr de sa provenance .donc il faut s'assurer que chaque poste de travail dispose d'un antivirus. [38]

II.6.10.3 Les différents types de filtrages

II.6.10.3.1 Le filtrage simple de paquet (sans états)

Stateless en anglais est la méthode de filtrage la plus simple, elle opère au niveau de la couche réseau et transport du modèle OSI. Il analyse les en-têtes de chaque paquet de données (datagramme) indépendamment des autres en se basant sur les règles prédéfinies par l'administrateur (*généralement appelées ACL, Access Control List*) [39]. Cela consiste à accorder ou refuser le passage de paquet d'un réseau à un autre en se basant sur l'adresse IP Source/Destination, le numéro de port Source/destination et le protocole de niveau 3 ou 4(type de paquet TCP, UDP, ICMP … etc.).

II.6.10.3.2 Le filtrage de paquets avec état :

C'est le filtrage dynamique, est une évolution des pare-feu sans états. L'amélioration est par rapport à la conservation de la trace des sessions et des connexions dans des tables d'états internes au Firewall pour appliquer les règles de filtrage. De cette manière, L'application des règles est alors possible sans lire les ACL à chaque fois, car l'ensemble des paquets appartenant à une connexion active seront acceptés.

Par exemple à partir du moment où une machine autorisée initie une connexion à une machine située de l'autre coté du Pare-feu. L'ensemble des paquets transitant dans le cadre de cette connexion sont implicitement acceptés par le Pare-feu. Le Firewall prend alors ses décisions en fonction des états de connexions, et peut réagir dans le cas de situations protocolaires anormales

Pour conserve les états des connexions on trouve 4 types d'états

- NEW : Un client envoie sa première requête vers un serveur web.
- ESTABLISHED : Connexion déjà initiée (après un NEW).
- RELATED : Peut être une nouvelle connexion, mais elle présente un rapport direct avec une connexion déjà connue.
- INVALID : Correspond à un paquet qui n'est pas valide, c'est-à-dire un paquet associé à une connexion inconnue. [39]

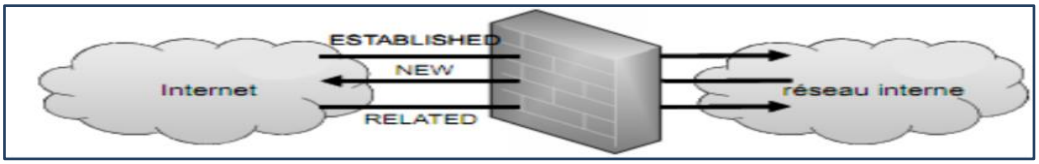


Figure II. 15: les états des connexions de filtrage des paquets

II.6.10.3.3 Le filtrage applicatif

(*Aussi nommé pare-feu de type proxy ou passerelle applicative*) fonctionne sur la couche 7 du modèle OSI et analyse le trafic échangé au niveau de cette couche. Cela suppose que le firewall connaisse l'ensemble des protocoles utilisés par chaque application. Chaque protocole dispose d'un module spécifique à celui-ci. C'est à dire que, par exemple, le protocole HTTP sera filtré par un processus proxy http [39].

Donc le pare-feu proxy est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et internet qui permet de limiter les commandes à un service plutôt que de l'interdire donc toutes les communications se feront par le serveur proxy, qui jouera en réalité le rôle d'un translateur d'adresse réseau (NAT) c'est-à-dire le destinataire ne connaitra pas l'adresse de l'émetteur car il ne communiquera qu'avec le serveur proxy qui présente juste sa propre adresse et non pas celle du l'utilisateur de réseau local.

II.6.10.4 Les différents types de pare-feu

II.6.10.4.1 Les pare-feu bridge

Agissent comme des câbles réseau avec la fonction de filtrage en plus, leurs interfaces ne possèdent pas d'adresse IP et ne font que transférer les paquets d'une interface à une autre en leur appliquant les règles prédéfinies.

Cette absence d'adresse IP est particulièrement utile, car cela signifie que le pare-feu est indétectable pour un hacker. En effet, quand une requête ARP est émise sur le câble réseau, le pare-feu ne répondra jamais. Ses adresses Mac ne circuleront jamais sur le réseau, et comme il ne fait que « transmettre » les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirigée directement contre le pare-feu. Ces types de pare-feu se trouvent typiquement sur les switchs [40].

II.6.10.4.2 Les pare-feu matériels

Est un périphérique physique installé entre un réseau informatique et Internet ou à la périphérie du réseau pour surveiller les paquets de données, possédant, au minium deux interfaces réseau, qui va analyser les données qui transitent par lui *(tout trafic entrant et sortant par réseau passe à travers celui-ci avant d'atteindre des ordinateurs individuels)* [41], et vérifier si elles correspondent aux règles de politique de sécurité ou bien non comme par exemple de rejeter systématiquement toutes les requêtes provenant d'un domaine précis, ou

bien toutes les requêtes utilisant un protocole spécifique, ou bien encore toutes celles relatives à tel ou tel numéro de port. Il est d'habitude intégré dans un router/modem.

II.6.10.4.3 Le pare-feu logiciel

Est un programme qui peut être installés sur un ordinateur en le téléchargé directement à partir d'un site Web ou les charger à partir d'un CD ou d'un DVD [42]. Il s'exécute sur un ordinateur local**,** et répondre aux besoins d'un utilisateur individuel (Hardware Firewall), mais en principe, il accomplit les mêmes tâches qu'un pare-feu matériel. Les pare-feu logiciel surveillent les paquets de données entrant et sortant par réseau et décident, selon des règles, s'il faut les bloquer ou autoriser. Nous pouvons les classer en deux catégories : les pare-feu personnels et les pare-feu plus sûr.

II.6.10.4.3.1 Personnels

Ils sont assez souvent commerciaux et ont pour sécuriser un ordinateur particulier, et non pas un groupe d'ordinateurs. Souvent payants, ils peuvent être contraignants et quelque fois très peu sécurisé. En effet, ils s'orientent plus vers la simplicité d'utilisation plutôt que vers l'exhaustivité, afin de rester accessible à l'utilisateur final.

II.6.10.4.3.2 Les Firewalls plus ''Sérieux''

Tournant généralement sous linux, car cet OS offre une sécurité réseau plus élevée et un contrôle plus adéquat, ils ont généralement pour but d'avoir le même comportement que les firewalls matériels des routeurs, à ceci prêt qu'ils sont configurables à la main. Toute fonctionnalité des firewalls de routeurs est potentiellement réalisable sur une telle plateforme. [43]

II.6.11 Zone démilitarisée

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, un serveur FTP public, DNS ou de proxy etc.), fournissent aux hackers une importante surface d'attaque. Si ces derniers sont directement liés au réseau local. Une solution à ce problème est de créer une zone démilitarisée (notée **DMZ** pour *DeMilitarized Zone*) [44], qui est une interface située entre un réseau connu (réseau interne) et un réseau externe (internet). Cette séparation physique permet d'autoriser les accès internet à destination des serveurs placés dans la DMZ et non à ceux destinés au réseau privé (interne) [45], pour éviter toute connexion directe avec le réseau interne et de prévenir celui-ci de toute attaque extérieure depuis le Web.

La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

- Trafic du réseau externe vers la DMZ autorisé.
- Trafic du réseau externe vers le réseau interne interdit.
- Trafic du réseau interne vers la DMZ autorisé.

- Trafic du réseau interne vers le réseau externe autorisé.
- Trafic de la DMZ vers le réseau interne interdit.
- Trafic de la DMZ vers le réseau externe refusé.

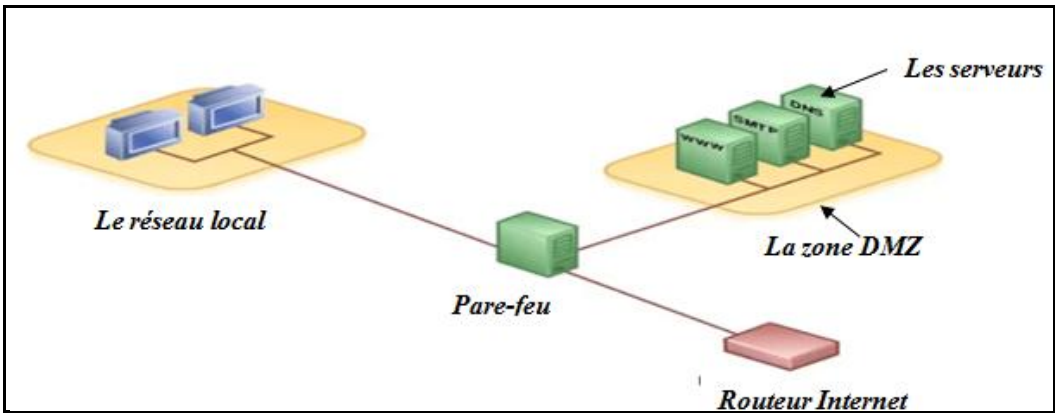


Figure II. 16: La zone DMZ dans un réseau

II.7 Conclusion

Nous avons vu à travers ce chapitre l'impacte de la sécurité informatique sur les réseaux, en exposant l'objectifs de la sécurité et quelques attaques qui peuvent infectées un réseau local et l'importance d'une politique de sécurité qui devra prendre en compte les besoins des utilisateurs, ainsi que les risques encourus dans le but d'´eriger une vraie stratégie de sécurité.

Chapitre 3

Présentation de l'architecture du réseau d'AIR Algérie

III.1 Introduction

Avant de se lancer dans la configuration de réseau intranet d'Aire Algérie. Nous allons présenter :

- ✓ L'architecture de réseau et sa structure hiérarchique.
- ✓ Les équipements utilisés pour constituer le réseau et les dispositifs de sécurité.

Pour donné des suggestions afin d'amélioré la sécurité de réseau Air Algérie et de rendre le trafic plus efficace.

III.2 Présentation globale du réseau intranet d'AIR Algérie

Le réseau informatique d'Air Algérie est constitué de quatre zones (voir la figure III.1), chaque zone à l'architecture d'un arbre, et qui est connectée à la direction générale et avec la zone voisin pour en cas de panne d'une ligne relier le site central à un site quelconque, la communication entre les concernés passe par un site intermédiaire qui n'est autre qu'un voisin du site secondaire

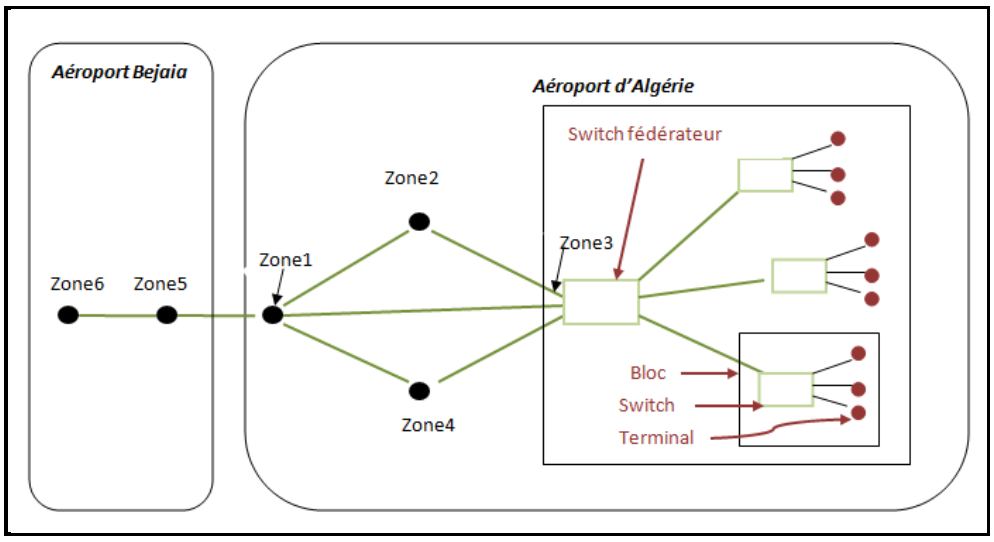


Figure III. 1: La topologie physique du réseau local

III.3 Description détaillé de chaque zone

Chaque zone est composée de blocs, il consiste donc un nœud et une feuille de la structure arborescente du réseau. Le regroupement des blocs se fait sur la base de la proximité géographique des blocs sur le site,

Voici le schéma général d'Air Algérie dont chaque direction a pour but d'assurer le bon fonctionnement de chaque partie du groupe comme le montre la Figure III.2

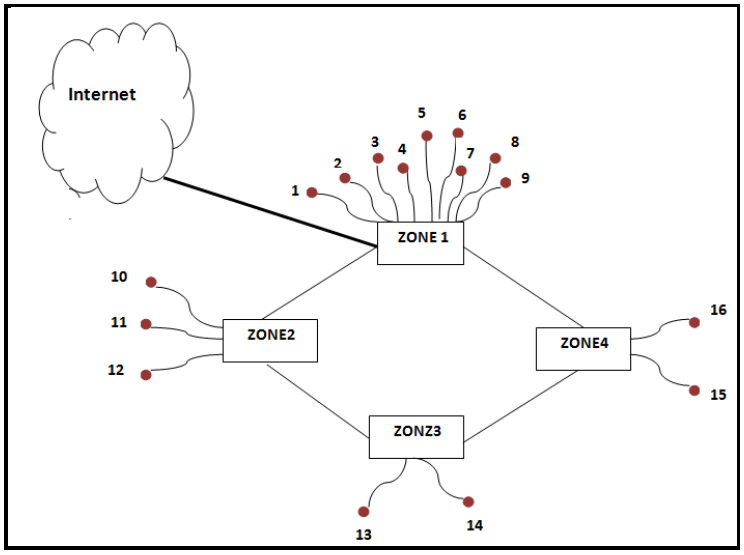


Figure III. 2: Schéma Synoptique de distribution inter-bâtiment du réseau d'AIR Algérie

Tableau III. 1: Description détaillé des zones

Zone 1 : direction générale	Secrétaire générale **1**	Cellule communication **2**	Inspection générale **3**	Bureau d'étude **4**	Direction qualité **5**	Direction financière **6**	Direction des ressources humaines 7	Direction des affaires **8**	Direction promotion œuvre social **9**
Zone 2 : division exploitation	Direction des opérations aériennes **10**				Direction de transport **11**				
Zone 3 : division système	Direction informatique télécom **12**				Direction planification et STRL de gestion **13**				
Zone 4 : division maintenance	Direction technique **14**				Direction logistique **15**				

III.4 **Principes d'un modèle de conception** (Voir l'annexe G)

III.4.1 Modèle hiérarchique de conception

La conception d'un réseau hiérarchique implique la division du réseau en couches distinctes. Chaque couche fournit des fonctions spécifiques qui définissent son rôle dans le réseau global. **Le modèle hiérarchique à trois couches (***couche d'accès, couche de distribution et couche cœur de réseau***) proposé par Cisco Systems est celui que nous implémentons tel que** chaque zone dispose d'un Switch fédérateur, relié à d'autres Switchs chargés de la commutation de paquets jusqu'aux blocs.

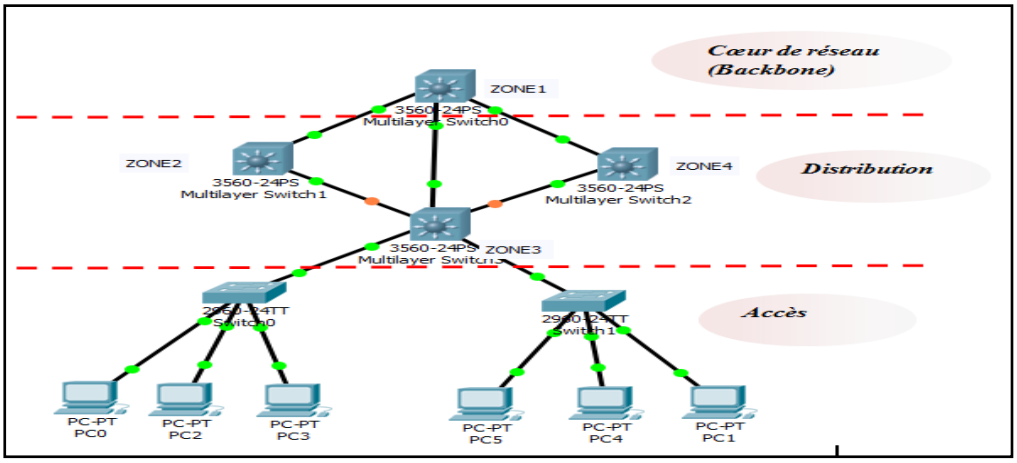


Figure III. 3: Le modèle hiérarchique à trois couches d'AIR Algérie

III.4.1.1 La couche cœur (zone 1) *:*

C'est la couche supérieure dont le rôle consiste à relier les différentes directions qui compose l'Air Algérie: *les sites distants, les réseaux locaux (LANs) ou les étages.* Les objectifs à ce niveau sont les performances, la stabilité et le moins de complexité possible Cette couche est aussi appelée Backbone.

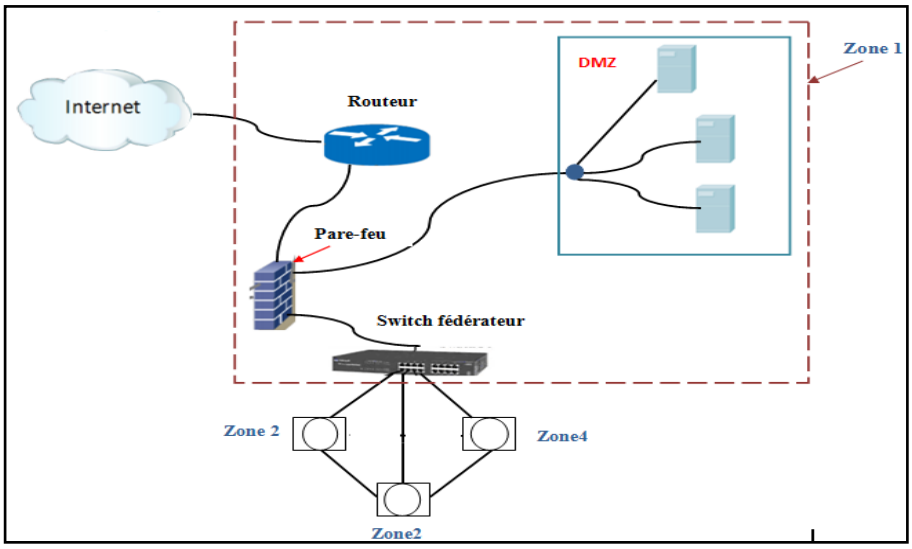


Figure III. 4: Présentation de la Zone 1 (Backbone)

III.4.1.2 La couche de distribution *(Zone2 ,3 et 4)*

A pour rôle de filtrer, de router, d'autoriser ou non les paquets. Elle regroupe les données reçues à partir des commutateurs de la couche d'accès, avant qu'elles ne soient transmises vers la couche cœur de réseau, c'est-à-dire entre la partie « liaison » et la partie « utilisateur ».

III.4.1.3 La couche d'accès

Cette couche qui est la dernière du modèle hiérarchique Permet aux utilisateurs d'accéder aux périphériques du réseau. A ce niveau, on utilise des switches de niveau 2 car la configuration de ce type de switches pose moins de contraintes, Son rôle principal est de fournir un moyen de connecter et de contrôler les périphériques qui sont autorisés à communiquer sur le réseau.

III.5 Proposition d'une configuration sécurisée

Objectif de notre travail est de configurer les équipements CISCO d'Aire Algérie d'une manière sécurisée et assure le bon fonctionnement de système, on a illustré les propositions citées ci-dessous :

- La configuration de l'accès à la console des équipements : pour protéger les équipements contre tout accès non autorisé. Des mots de passe sont configurés pour l'accès à la console.
- Sécurisé l'administration des équipements Cisco
- La configuration de pare-feu
    1) Segmentation des interfaces de pare-feu en VLAN
    2) Configuration des ACL au niveau du pare-feu pour pouvoir autoriser ou refuser l'accès aux ressources disponibles dans le réseau

3) Configuration des VPN au niveau du pare-feu
4) Configuration de la zone DMZ pour les serveurs interne qui ont besoin d'être accessibles de l'extérieur
5) Configuration de NAT

- Configuration sécurisé pour des accès administratifs à distance aux périphériques (l'utilisation de protocole SSH)
- Configuration des protocoles d'administration et de gestion des VLANs
  A. Configuration de protocole VTP sur les switchs
  B. Configuration de protocole spanning Tree sur les switchs

III.6 Conclusion :

Ce chapitre présente une étude sur le plan sécuritaire du réseau intranet d'Aire Algérie, qui permet de rendre notre réseau plus rigide et plus fort devant les attaques.

Les solutions citées ci-dessus sont mises en œuvre sous CISCO Packet Tracer dans le Chapitre qui suit.

Chapitre 4

Réalisation

IV.1 Introduction

Dans ce chapitre, nous allons passer à la dernière étape qui est la réalisation avec un outil CISCO appelé Packet Tracer que nous allons décrire dans l'annexe F

Nous allons intéresser à la sécurité de réseau d'entreprise Air Algérie. Nous proposerons des solutions pour améliorer la sécurité de ce réseau.

IV.2 Réalisation de l'architectures LAN d'AIR Algérie

Compose de deux sites l'une se situe a Alger et l'autre à Bejaïa.

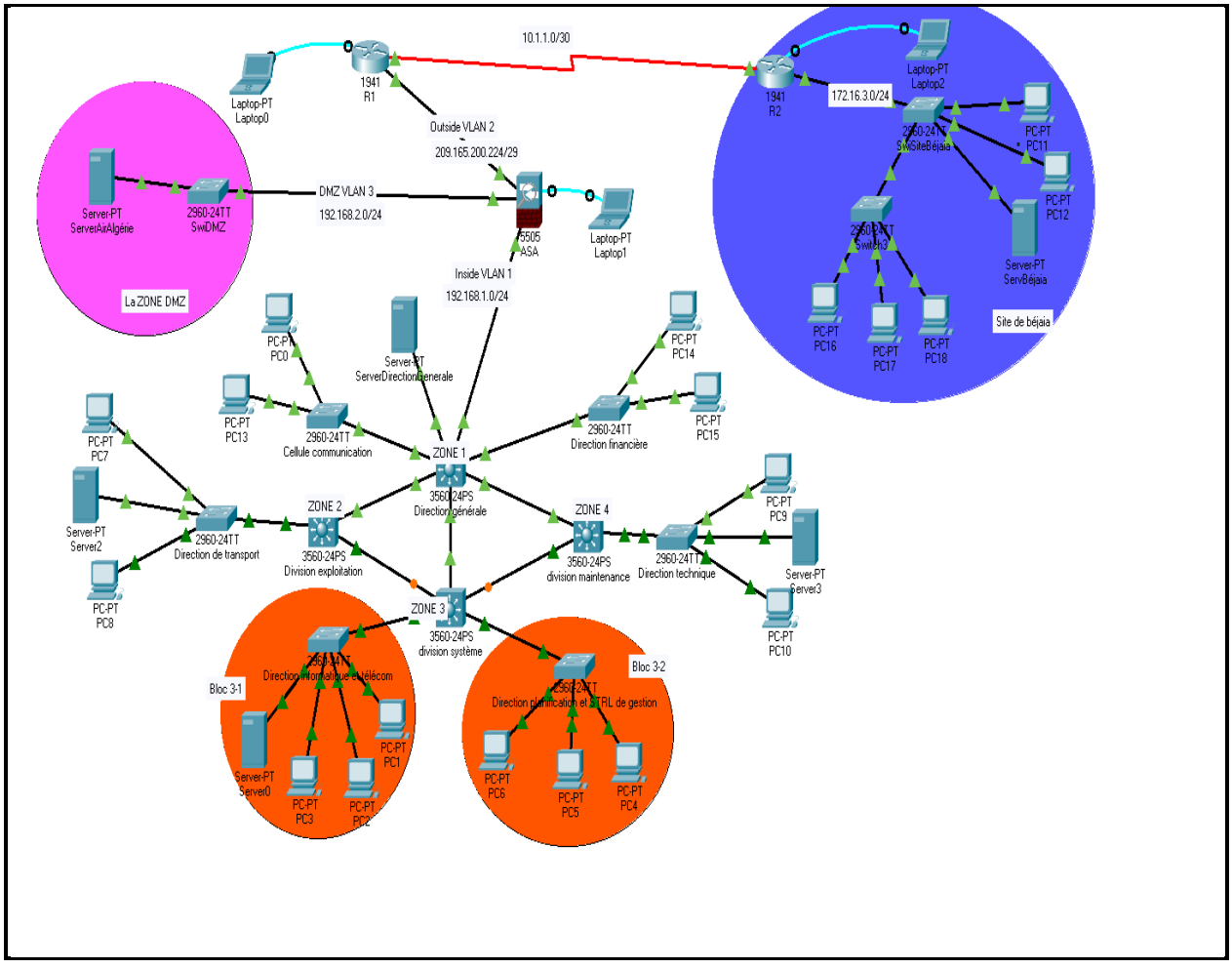


Figure IV. 1: L'architecteur de réseau AIR Algérie

Les interfaces des équipements sont indiquées dans le tableau IV.1 suivant

Tableau IV. 1: Table d'adressage du réseau ASA et du pare-feu avec la sécurité de la couche 2

Equipement	*Interface*	*Adresse IP*	*Masque*	*Default geteway*
R1	Fa0/0	209.165.200.225	255.255.255.248	N/A
	S0/1/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	Fa0/0	172.16.3.1	255.255.255.0	N/A
	S0/1/0	10.1.1.2	255.255.255.252	N/A
ASA	Vlan 1 E0/1	192.168.1.1	255.255.255.0	N/A
	Vlan 2 E0/0	209.165.200.226	255.255.255.248	N/A
	Vlan 3 E0/2	192.168.2.1	255.255.255.0	N/A
DMZ Serveur	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-1…PC-10	NIC	192.168.1.5-192.168.1.14	255.255.255.0	192.168.1.1
PC-11 /PC-12	NIC	172.16.3.2-172.16.3.3	255.255.255.0	172.16.3.1

IV.3 Configuration de bases des équipements

Tous les équipements Cisco disposent d'un port console, permet un accès simple et rapide à l'interface de configuration en ligne de commande (CLI) depuis votre PC d'une manière physique et via le terminal.

La console est le mode de connexion qui est à utiliser quand vous configurez votre équipement pour la première fois, et qu'il ne dispose pas encore d'une adresse IP. Une fois que le PC est physiquement connecté au port console, on pourra commencer la configuration (voir la figure IV.5).

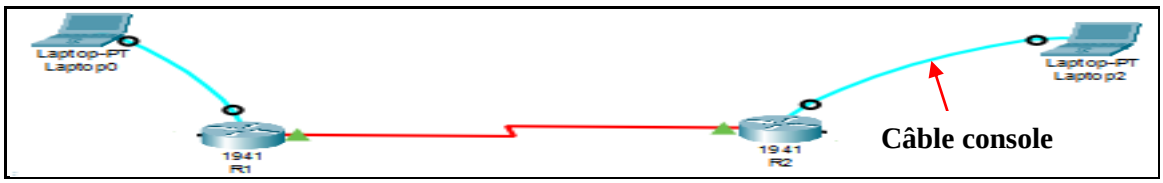


Figure IV. 2: L'utilisation de câble console

IV.4 Sécuriser l'accès aux périphériques

ISO utilise des modes organisés hiérarchiquement pour faciliter la protection des périphériques, dans le cadre de ces dispositifs de sécurité, ISO peut accepter plusieurs mots de passe, ce qui nous permet d'établir différents privilèges d'accès au périphérique

Au début d'une configuration de base du chaque routeur et switch, on commence par l'attribution d'un nom aux équipements avec la commande suivante hostname, le but de cette

configuration est de renommer les équipements avec des noms significatifs, ensuite on passe à la configuration des mots de passe

- Sécuriser l'accès au mode privilégié avec un mot de passe chiffré (cisco comme mot de passe)
- Sécuriser l'accès à la ligne de console (ciscoCon comme mot de passe)
- Sécuriser l'accès à la ligne d'accès à distance avec le protocole SSH (cisco comme mot de passe et admin comme nom d'utilisateur)
- Chiffrer les mots de passe en clair

La figure (IV.6) montre les commandes mise en place.

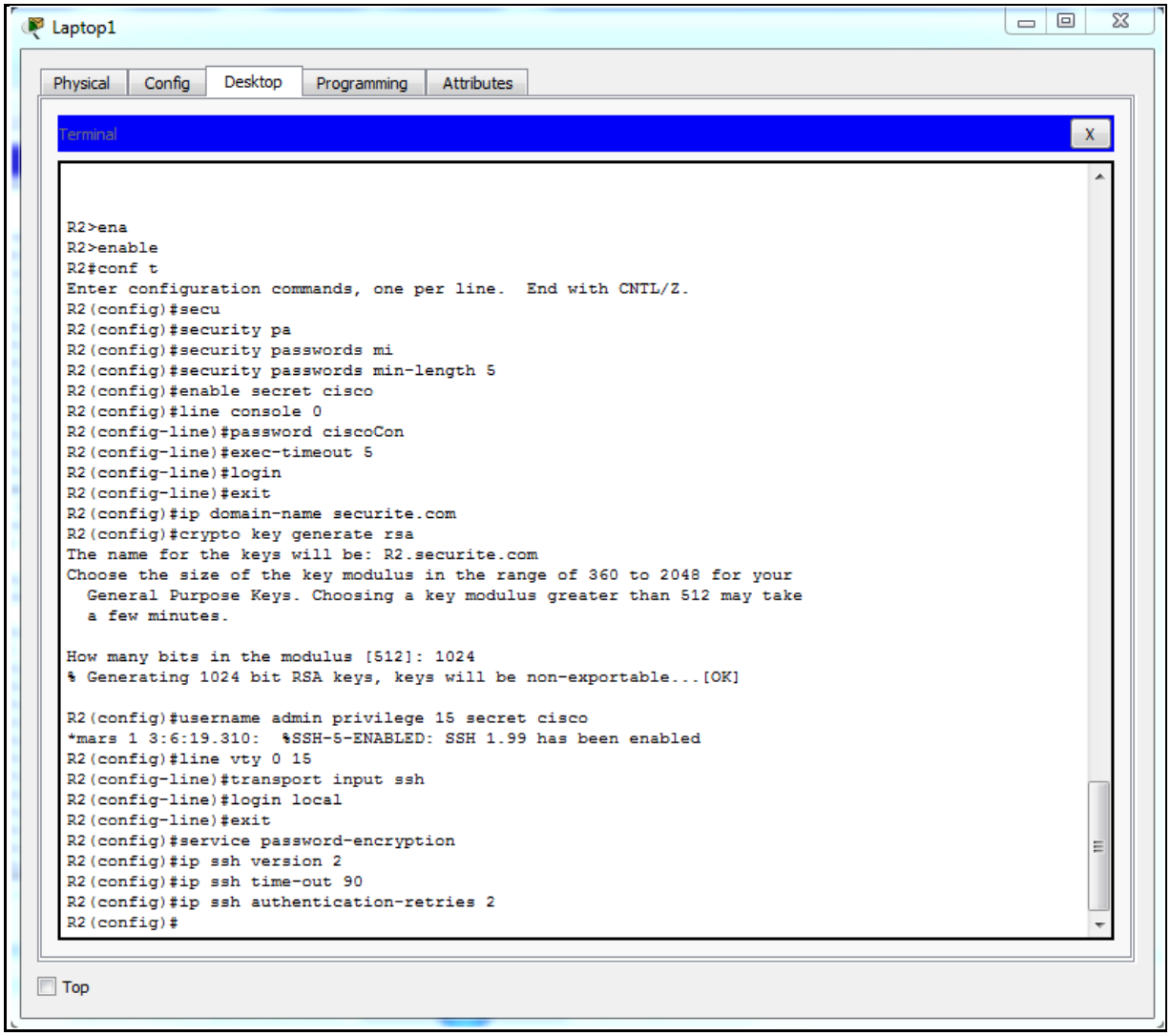


Figure IV. 3: Attribution des mots de passe et la configuration de SSH pour le Routeur

Remarque :

La même chose pour les switchs juste on va attribuer des adresses IP pour VLAN 1 de chaque switchs pour l'accès à distance avec le protocole SSH

Il est recommandé d'utiliser des mots de passe différents pour chacun de ces niveaux d'accès. En effet, bien que l'utilisation de plusieurs mots de passe différents ne facilite pas l'ouverture d'une session, cette précaution est nécessaire pour protéger convenablement l'infrastructure réseau contre l'accès non autorisé.

Les mots de passe doivent aussi être changés suivant une périodicité. Ils doivent être fort c'est-à-dire composé de chiffres, caractères spéciaux (@§!&#), majuscules et minuscules. Ceci permet d'éviter les attaques par dictionnaire ou par force brute.

Dans notre exemple on a pris des mots de passe simple pour tous les niveaux de sécurité, juste a fin de faciliter la tâche.

IV.5 Configuration des routeurs

IV.5.1 Configuration des interfaces

Chaque interface possède un type (Serial, FastEthernet), dans cette étape nous allons attribuer les adresses IP et des masques aux interfaces des routeurs et les activer ainsi on va déterminer le taux de transmission : clock rate Dans le cas des liaisons série (entre les routeurs), l'horloge doit être activée en spécifiant sa fréquence

A. Pour le routeur 1 :

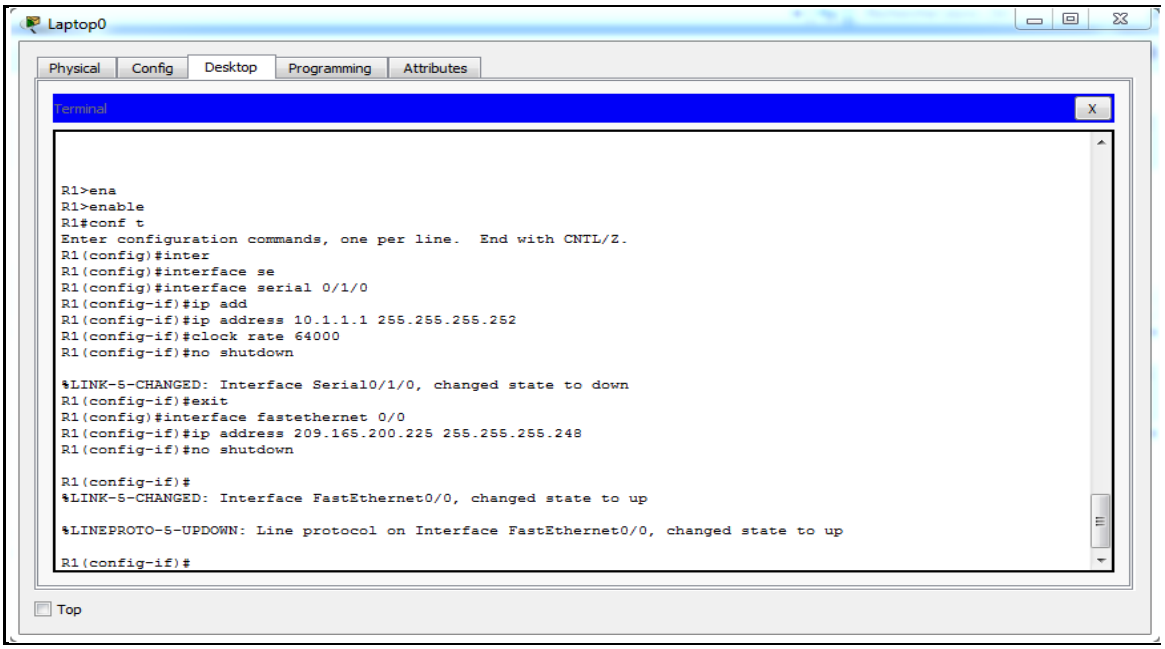


Figure IV. 4: Configuration des interfaces de R1

B. Pour le routeur 2 :

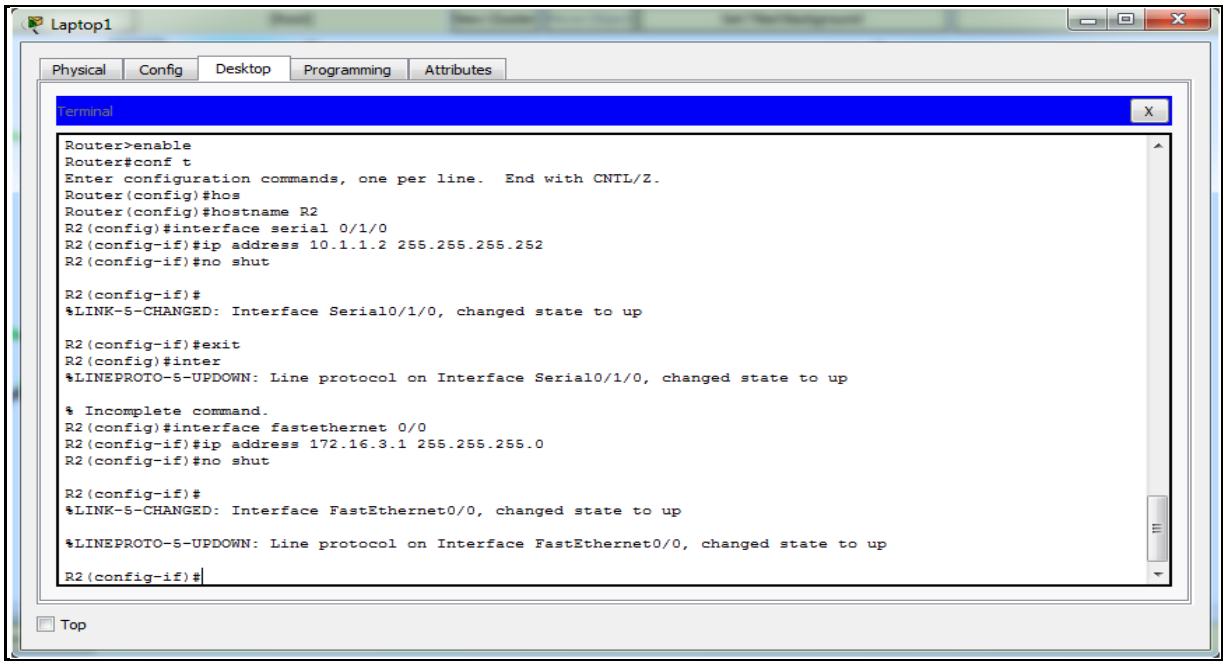


Figure IV. 5: Configuration des interfaces de R2

IV.5.2 Configuration du routage

Nous allons appliquer sur chaque routeur la fonction de routage, avec le protocole de routage Statique. Ce qui donne aux périphériques l'accès vers tous les autres emplacements. La commande permettant de configurer le routage Statique sur un routeur est montrée sur les figures suivantes :

A. Routeur 1 :

```
R1(config)#ip route 192.168.1.0 255.255.255.0 209.165.200.226
R1(config)#ip route 172.16.3.0 255.255.255.0 10.1.1.2
```

Figure IV. 6: Le routage statique de routeur R1

B. Routeur 2 :

```
R2(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.1
```

Figure IV. 7: Le routage statique de routeur R2

Commande d'enregistrement de la configuration courante Après avoir configuré les interfaces de chaque routeur et fonction de routage, on doit sauvegarder la configuration actuelle pour la réappliquer automatiquement en cas de redémarrage du routeur. La commande qui nous permet la sauvegarde s'exécute en mode Privilégié : copy running-config startup-config

IV.6 Configuration de firewall ASA

IV.6.1 Réglages des paramètres ASA et de la sécurité d'interface

Nous allons tout d'abord configurer le nom de pare-feu comme « ASA » et le nom de domaine en tant que « securite.com », ensuite, à l'aide de la commande « enable password » nous allons configurer un mot de passe « cisco » pour le mode d'activation et au final, nous allons régler l'horloge pour régler manuellement la date et l'heure (Voir la Figure IV.11).

```
ciscoasa>enable
Password:
ciscoasa#conf t
ciscoasa(config)#hostname ASA
ASA(config)#domain-name securite.com
ASA(config)#enable password cisco
ASA(config)#clock set 23:11:30 12 july 2021
```

Figure IV. 8: Configuration du nom d'hôte, nom de domaine, mot de passe et l'horloge

IV.6.2 La configuration des interfaces du l'ASA

Ce pare-feu est composé de 3 interfaces, la première sera reliée au réseau interne (LAN), la deuxième au réseau externe (WAN) et la troisième sera pour la DMZ. Chacune d'elle est associée à un niveau de sécurité.

Pour le moment, nous allons configurer que les interfaces VLAN 1 (Inside) et VLAN 2 (Outside). L'interface VLAN 3 (DMZ) sera configurée dans la prochaine partie.

Commençons par le configuration de l' interface logique VLAN 1 pour le réseau intérieur (192.168.1.0/24) et définir le niveau de sécurité sur le paramètre le plus élevé de 100.Ensuite, créer une interface logique VLAN 2 pour le réseau extérieur (209.165.200.224/29) et définir le niveau de sécurité sur le paramètre le plus bas de 0 et activer l'interface VLAN 2.

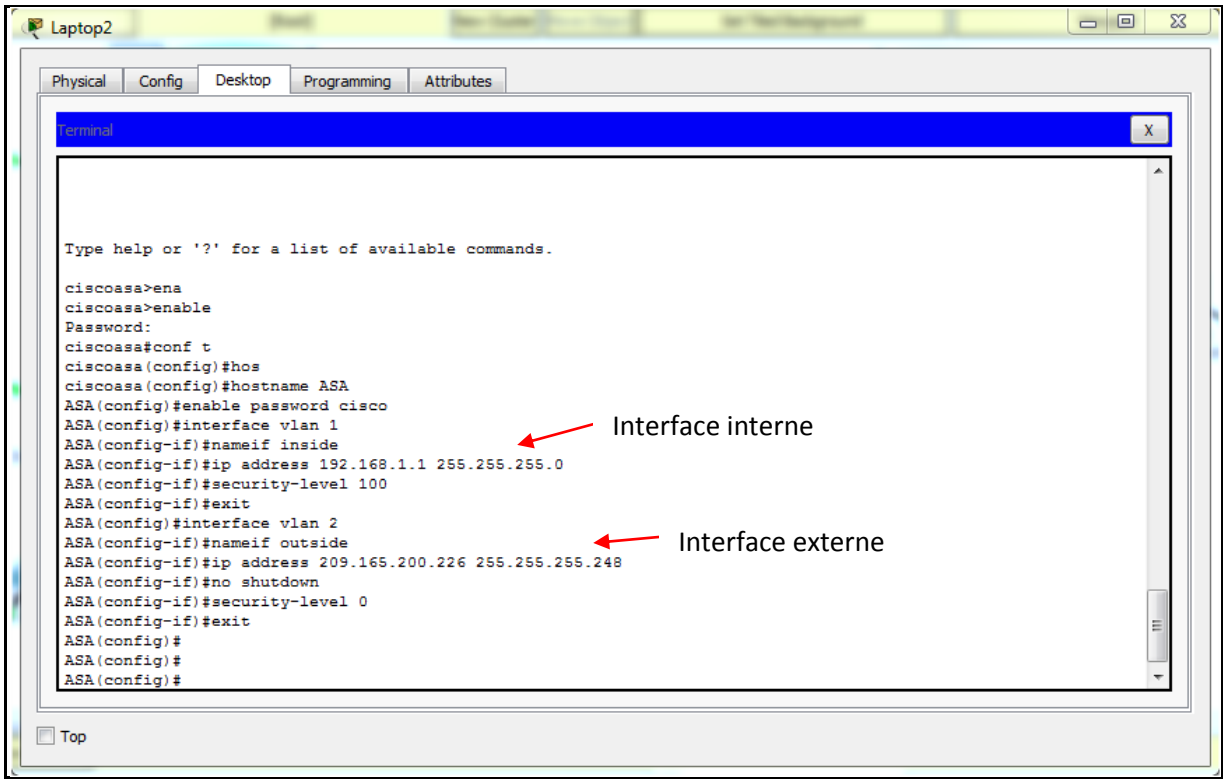


Figure IV. 9: Liste des commandes pour la configuration de l'interface interne et externe de l'ASA

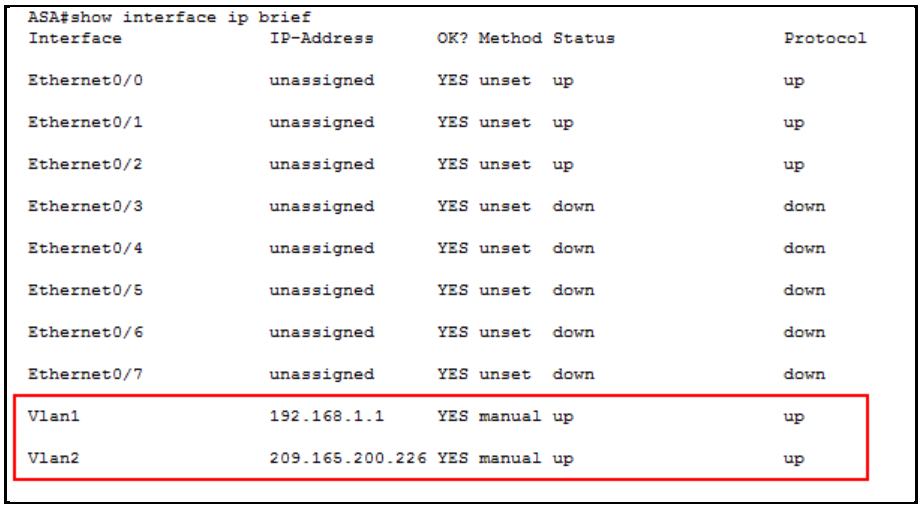
Les interfaces physiques du pare-feu sont au final raccordées aux divers VLAN en utilisant la commande switchport access vlan suivie d'un numéro de VLAN. La figure (IV.13) montre la configuration des interfaces de pare-feu.

```
ASA(config)#interface ethernet 0/1
ASA(config-if)#switchport access vlan 1
ASA(config-if)#no shut
ASA(config-if)#exit
ASA(config)#interface ethernet 0/0
ASA(config-if)#switchport access vlan 2
ASA(config-if)#no shutdown
ASA(config-if)#exit
```

Figure IV. 10: Raccorder les interfaces aux VLANs

IV.6.3 Vérification de notre configuration :

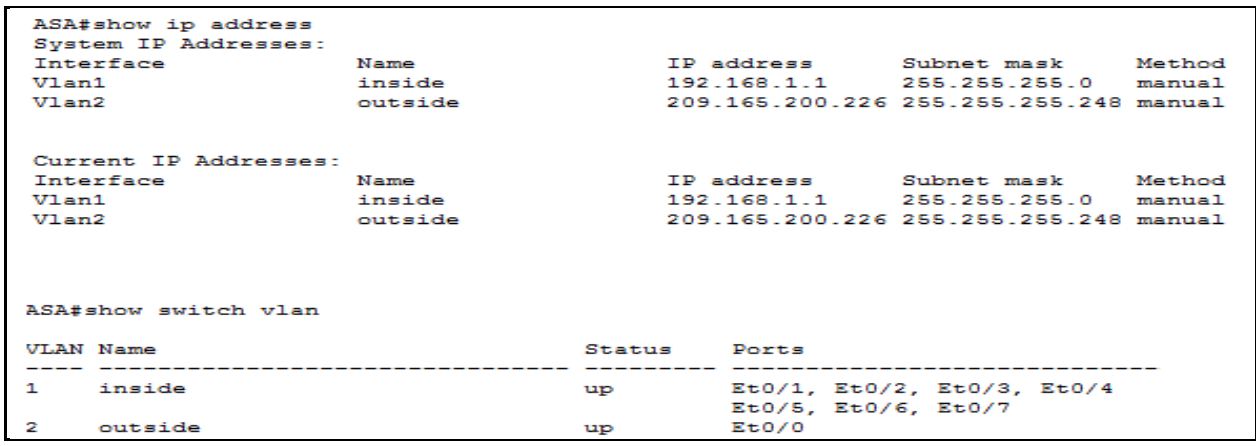
Maintenant, nous utilisons la commande « show interface ip brief » pour afficher l'état de toutes les interfaces ASA.



```
ASA#show interface ip brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  down                  down
Ethernet0/4            unassigned      YES unset  down                  down
Ethernet0/5            unassigned      YES unset  down                  down
Ethernet0/6            unassigned      YES unset  down                  down
Ethernet0/7            unassigned      YES unset  down                  down
Vlan1                  192.168.1.1     YES manual up                    up
Vlan2                  209.165.200.226 YES manual up                    up
```

Figure IV. 11: Affichage d'état des interfaces ASA

Ensuite, nous voulons afficher les informations des interfaces VLAN de la couche 3 en tapant la commande « show ip address ». Et pour l'affichage des VLAN intérieurs et extérieurs configurés sur l'ASA et les ports attribués on tape la commande « show switch vlan »



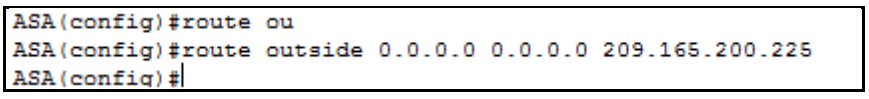
```
ASA#show ip address
System IP Addresses:
Interface              Name                IP address      Subnet mask      Method
Vlan1                  inside              192.168.1.1     255.255.255.0    manual
Vlan2                  outside             209.165.200.226 255.255.255.248  manual

Current IP Addresses:
Interface              Name                IP address      Subnet mask      Method
Vlan1                  inside              192.168.1.1     255.255.255.0    manual
Vlan2                  outside             209.165.200.226 255.255.255.248  manual


ASA#show switch vlan

VLAN Name                             Status     Ports
---- -------------------------------- ---------- -------------------------------
1    inside                           up         Et0/1, Et0/2, Et0/3, Et0/4
                                                 Et0/5, Et0/6, Et0/7
2    outside                          up         Et0/0
```

Figure IV. 12: Vérification des informations des interfaces VLAN

IV.6.4 Configuration de la stratégie de routage, de traduction d'adresses et d'inspection

IV.6.4.1 Configuration d'une route par défaut statique pour l'ASA :

Après avoir configuré les interfaces da ASA, nous ajoutons une route statique par défaut pour tout le trafic sortant vers internet. Nous allons par la suite émettre la commande « show route » pour vérifier que la route par défaut statique est dans la table de routage ASA.



```
ASA(config)#route ou
ASA(config)#route outside 0.0.0.0 0.0.0.0 209.165.200.225
ASA(config)#
```

Figure IV. 13: Configuration d'une route par défaut statique pour l'ASA

```
ASA#show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.200.225 to network 0.0.0.0

C    192.168.1.0 255.255.255.0 is directly connected, inside
C    192.168.2.0 255.255.255.0 is directly connected, DMZ
     209.165.200.0/29 is subnetted, 2 subnets
C       209.165.200.0 255.255.255.248 is directly connected, outside
C       209.165.200.224 255.255.255.248 is directly connected, outside
S*   0.0.0.0/0 [1/0] via 209.165.200.225
```

Figure IV. 14: L'affichage d'une route par défaut statique pour l'ASA

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	ASA1	R1	ICMP		0.000	N	0	(e...
	Successful	R1	ASA1	ICMP		0.000	N	1	(e...
	Successful	PC3	ASA1	ICMP		0.000	N	2	(e...
	Failed	PC3	R1	ICMP		0.000	N	3	(e...

Figure IV. 15: Test de connectivité

IV.6.4.2 Configuration de la traduction d'adresses à l'aide des objets NAT et réseau :

Le réseau LAN dispose d'une plage d'adresse privée alors pour que les postes du réseau LAN puissent se connecter à internet il leur faut une adresse IP routable. Pour résoudre se problème nous avons configuré le NAT : Depuis l'intérieur vers l'extérieur de façon dynamique pour traduire les adresses réseau internes (192.168.1.0/24) en adresse globale de l'interface extérieure de l'ASA. Nous allons par la suite émettre la commande « show nat »

```
ASA(config)#object network inside-net
ASA(config-network-object)#subnet 192.168.1.0 255.255.255.0
ASA(config-network-object)#nat
ASA(config-network-object)#nat (inside,outside) dynamic interface
ASA(config-network-object)#exit

ASA#show nat
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic inside-net interface
    translate_hits = 0, untranslate_hits = 0
```

Figure IV. 16: Configuration de la traduction d'adresses

IV.6.4.3 Modification de la stratégie globale de service d'inspection d'application MPF par défaut :

Dans cette étape nous allons modifier la politique par défaut MPF inspection d'application de service globale pour permettre aux hôtes du réseau interne d'accéder aux serveurs web sur Internet. Lorsqu'il est correctement configuré, seul le trafic initié de l'intérieur est autorisé à revenir vers l'interface externe. On va d'abord créer une classe inspection-default qui correspond à défaut d'inspection du trafic. Ensuite, créer une politique-carte global-policy et l'inspecter avec ICMP. Enfin, on fixe la carte politique globalement à toutes les interfaces. La figure ci-dessous montre les commandes nécessaires pour cette opération.

```
ASA#conf t
ASA(config)#class
ASA(config)#class-map inspection_default
ASA(config-cmap)#match de
ASA(config-cmap)#match default-inspection-traffic
ASA(config-cmap)#exit
ASA(config)#polic
ASA(config)#policy-map global_policy
ASA(config-pmap)#class inspection_default
ASA(config-pmap-c)#inspect icmp
ASA(config-pmap-c)#exit
ASA(config)#service
ASA(config)#service-policy glabal_policy global
ERROR: Policy map glabal_policy does not exist
ASA(config)#service-policy global_policy global
ASA(config)#end
ASA#cop
ASA#copy ru
ASA#copy running-config sta
ASA#copy running-config startup-config
Source filename [running-config]?
Cryptochecksum: 0c185bea 6cc9613d 1b131727 60736544

1127 bytes copied in 2.268 secs (496 bytes/sec)
```

Figure IV. 17: Modification de la stratégie globale de service d'inspection d'application par défaut MPF

A partir de PC3, nous envoyons une requête Ping à l'interface R1 Fa0/0 à l'adresse IP (209.165.200.225/29). Cette fois le test est réussi car le trafic ICMP est maintenant inspecté et le trafic de retour légitime est autorisé.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC3	R1	ICMP		0.000	N	0	(e...	(delete)

Figure IV. 18: Test de vérification

IV.6.5 Configuration du DHCP, AAA et SSH

IV.6.5.1 Configuration d'ASA en tant que serveur DHCP :

Au cours de cette partie, nous allons configurer un pool d'adresses DHCP, l'activer sur l'interface intérieure ASA et spécifier l'adresse IP du serveur DNS à donner aux clients. Ensuite, nous allons activer le démon DHCP dans l'ASA pour écouter les demandes de client DHCP sur l'interface activée (à l'intérieur).

```
ASA#conf t
ASA(config)#dhcpd address 192.168.1.5-192.168.1.36 inside
ASA(config)#dhcpd dns 209.165.201.2

ASA(config)#dhcpd dns 209.165.201.2 interface inside
ASA(config)#dhcp ena
ASA(config)#dhcp enable inside
```

Figure IV. 19: Configuration d'ASA en tant que serveur DHCP

A la fin, nous allons remplacer le PC2 d'une adresse IP statique par un client DHCP et vérifier qu'il reçoit les informations d'adressage IP.

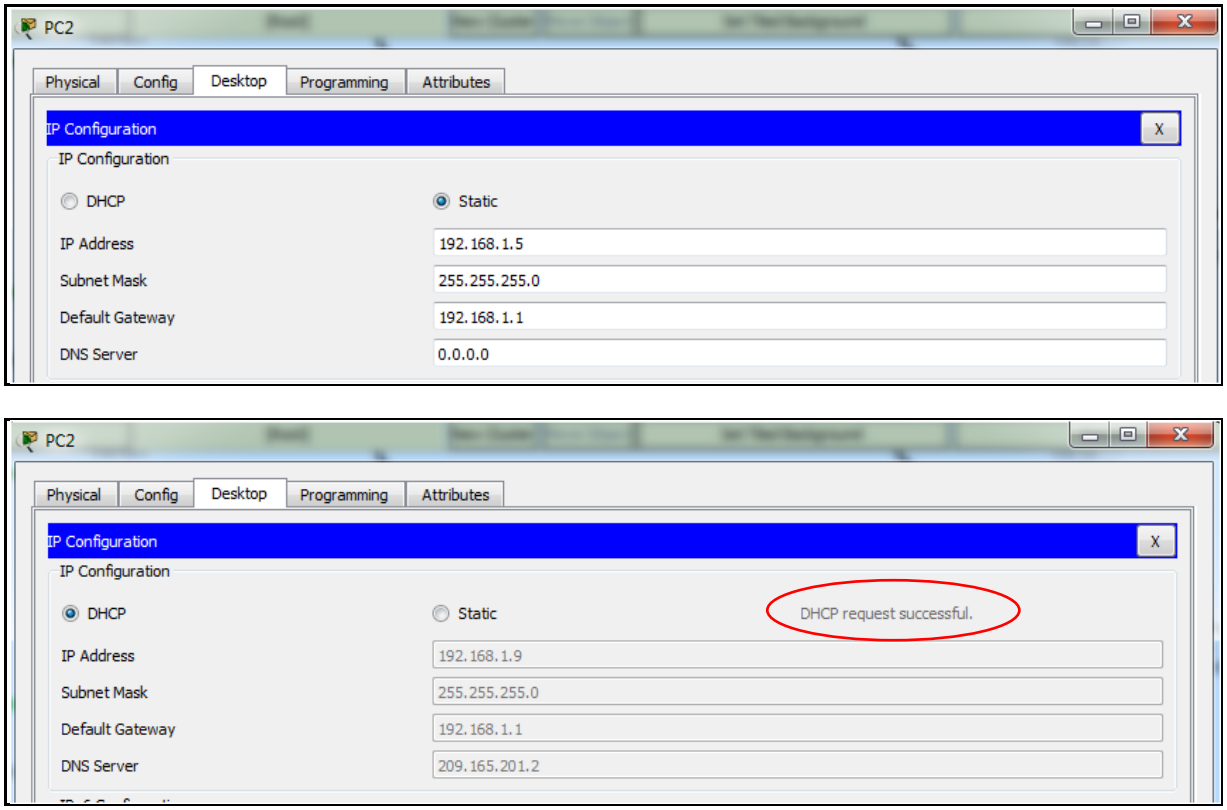


Figure IV. 20: Vérification d'une adresse IP statique par une adresse DHCP

IV.6.5.2 Configuration de l'AAA pour utiliser la base de données locale pour l'authentification

Maintenant, nous allons définir un utilisateur local nommé « admin » en entrant la commande « username », nous allons spécifions un mot de passe « cisco» et nous configurons le protocole AAA pour utiliser la base de données ASA locale et authentifier les utilisateurs ssh

```
ASA(config)#username admin password cisco
ASA(config)#aaa authentication ssh console LOCAL
```

Figure IV. 21: Configuration de l'AAA la base de données locale pour l'authentification

IV.6.5.3 Configuration de l'accès à distance à l'ASA :

Le serveur ASA peut être configuré pour accepter les connexions d'un hôte unique ou d'une gamme d'hôtes sur le réseau intérieur ou extérieur.

Dans cette étape, les hôtes du réseau extérieur peuvent uniquement utiliser SSH pour communiquer avec l'ASA. Les sessions SSH peuvent être utilisées pour accéder à l'ASA depuis le réseau intérieur.

Premièrement, nous allons générer une paire de clés RSA, qui est requise pour prendre en charge les connexions SSH. Deuxièmement, nous allons configurer l'ASA pour permettre des connexions SSH d'hôte sur le réseau intérieur (192.168.1.5/24) et de l'hôte de gestion à distance à la succursale (172.16.3.3/24) sur le réseau extérieur. En définissant le délai d'expiration SSH sur 10 minutes.

```
ASA(config)#username admin password cisco
ASA(config)#aaa authentication ssh console LOCAL
ASA(config)#crypt
ASA(config)#crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: no
ERROR: Failed to create new RSA keys named <Default-RSA-Key>
ASA(config)#ssh 192.168.1.5 255.255.255.255 inside
ASA(config)#
ASA(config)#ssh timeout 10
```

Figure IV. 22: Configuration de l'accès à distance à l'ASA

Finalement, nous allons établir une session SSH du PC-1 à l'ASA (192.168.1.1/24).

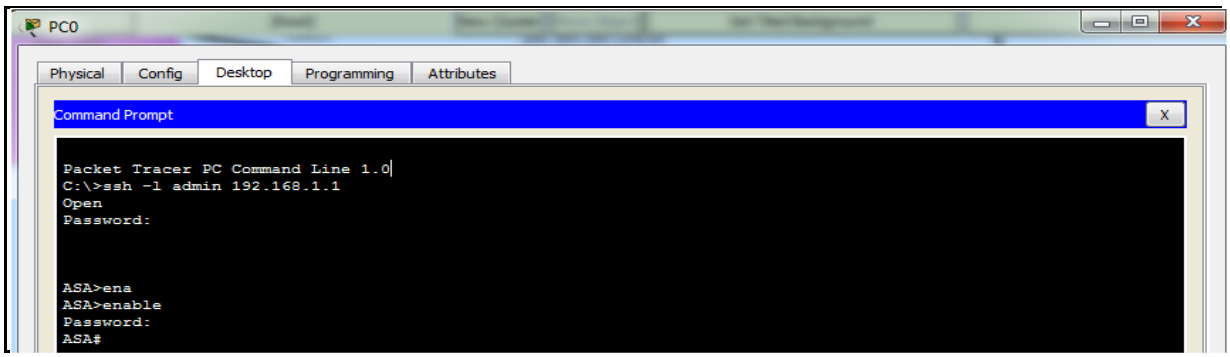


Figure IV. 23: Test de vérification SSH

IV.6.6 Configuration d'une DMZ, d'un NAT statique et des ACLs

IV.6.6.1 Configuration de l'interface DMZ VLAN 3 sur l'ASA :

Nous allons configurer DMZ VLAN 3, où résidera le serveur Web d'accès public, l'attribuer l'adresse IP (192.168.2.1/24), le nommer DMZ et l'attribuer un niveau de sécurité de 70.

Étant donné que le serveur n'a pas besoin d'initier la communication avec les utilisateurs internes, nous désactivons le transfert vers l'interface VLAN 1. Par la suite, nous allons assigner l'interface physique ASA E0/2 au DMZ VLAN 3 et activer l'interface. La configuration de la zone DMZ illustré dans la figure (IV.24).

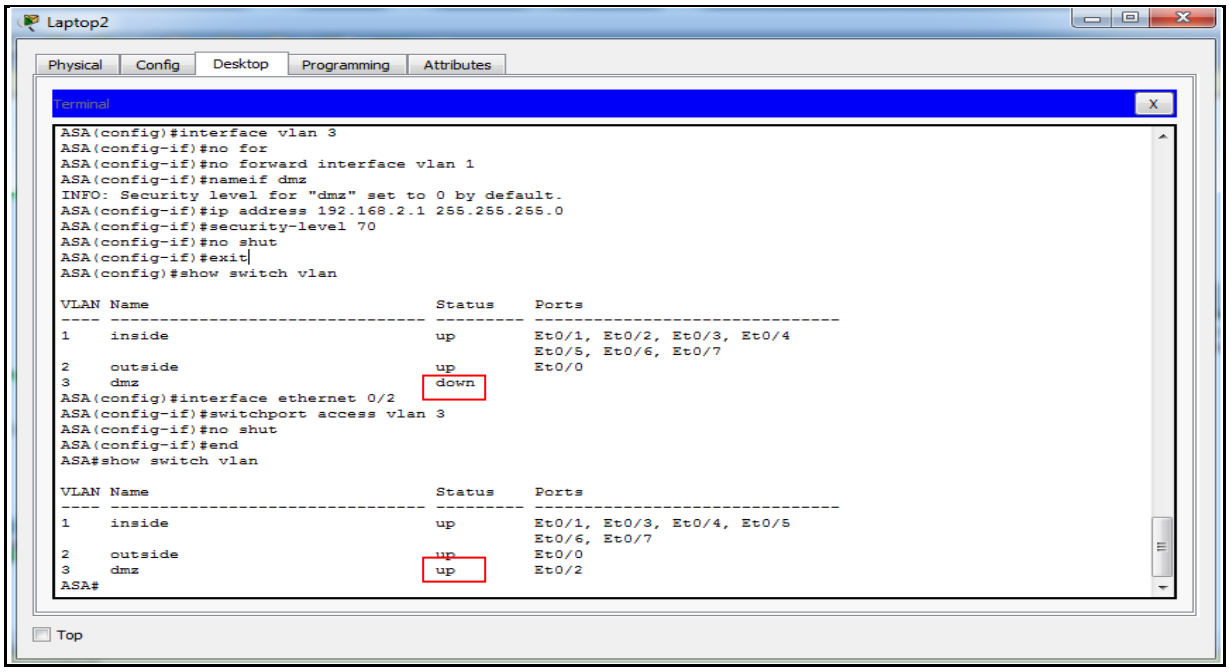


Figure IV. 24: Configuration de l'interface DMZ VLAN 3 sur l'ASA

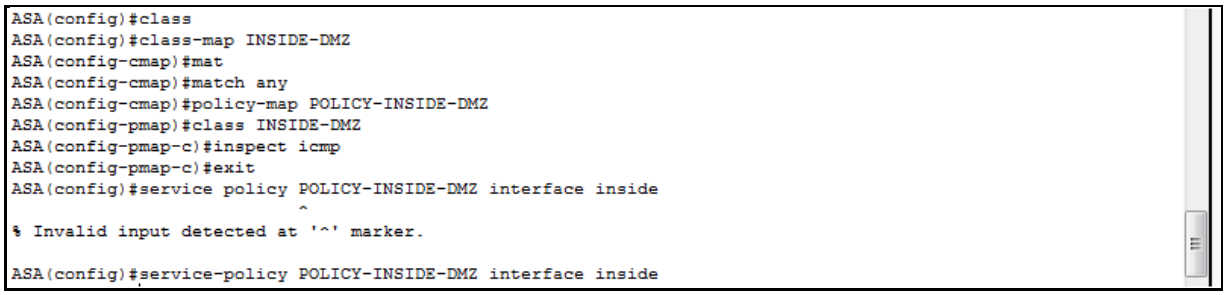


Figure IV. 25: Modification de la stratégie globale de service d'inspection pour la zone DMZ

IV.6.6.2 Configuration du NAT statique et dynamique sur le serveur DMZ à l'aide d'un objet réseau :

Dans cette étape, nous avons configuré le NAT depuis l'intérieur vers l'extérieur de façon dynamique. Par la suite nous configurons un objet réseau nommé « dmz-server » et l'attribuer l'adresse IP statique du serveur DMZ (192.168.2.3/24). En mode de définition d'objet, nous allons utiliser la commande « nat » pour spécifier que cet objet est utilisé pour traduire une adresse DMZ en une adresse externe à l'aide d'un NAT statique et spécifier une adresse publique traduite de (209.165.200.227/29).

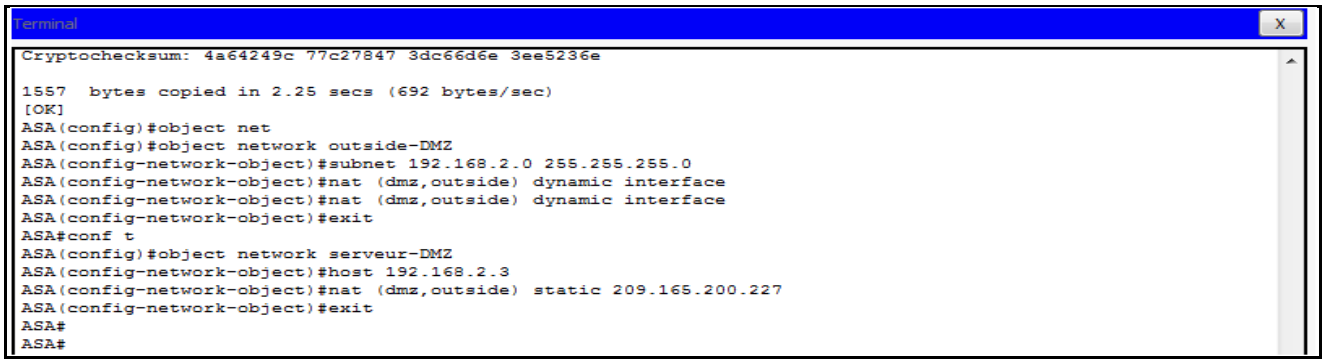


Figure IV. 26: Configuration du NAT statique et dynamique sur le serveur DMZ à l'aide d'un objet réseau

IV.6.6.3 Configuration des ACLs

Configuration d'une ACL pour autoriser l'accès au serveur DMZ depuis Internet : Nous allons configurer une liste d'accès nommée « ENTRANET » qui autorise le protocole ICMP, TCP (www, FTP pour transfère de fichier, SMTP pour le l'envoi d'email et POP3) depuis n'importe quel hôte externe vers l'adresse IP interne du serveur DMZ et appliquer la liste d'accès à l'interface extérieure ASA dans la direction « IN ».

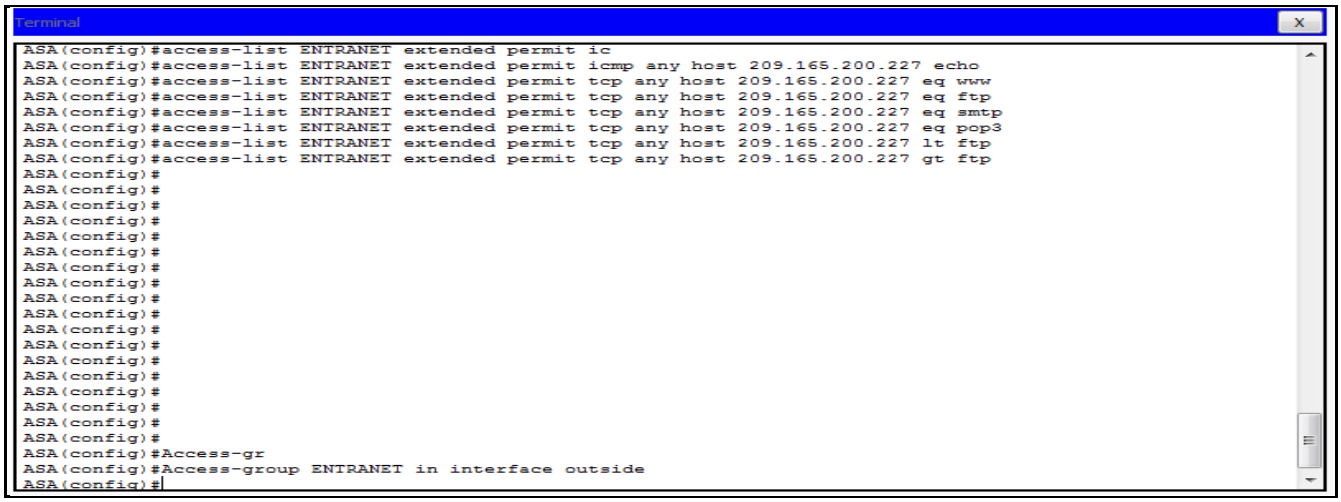


Figure IV. 27: Configuration des ACLs de la zone DMZ

Configuration d'une ACL pour autoriser l'accès au serveur DMZ depuis Internet

IV.6.6.4 Test d'accès au serveur DMZ :

Dans cette simulation, la possibilité de tester avec succès l'accès extérieur et intérieur au serveur Web DMZ

Figure IV. 28: Test d'accès au serveur DMZ à l'intérieure de réseau Inside

Figure IV. 29: Test d'accès au serveur DMZ à l'extérieure de réseau Outside

IV.7 Mise en place d'un IPsec VPN de site à site

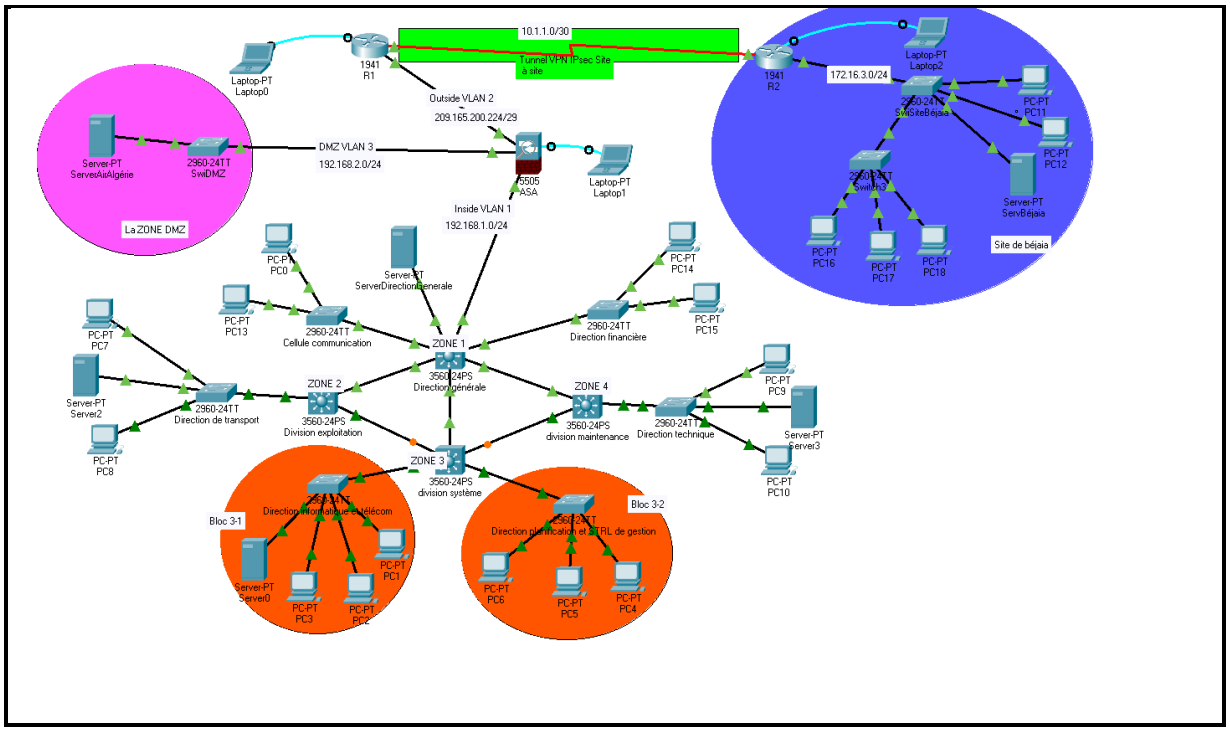


Figure IV. 30: Mise en place d'un IPsec VPN de site à site sur l'architecture réseau d'AIR Algérie

L'architecture proposée dans la figure (IV.33) dispose de deux sites, notre topologie illustre leurs interconnexions via un tunnel VPN. Pour cela, il faudrait définir une clef partagée, une association de sécurité, une fonction de hachage …etc. Ainsi, cette solution permettra aux sites AIR Algérie et Bejaïa d'échanger des données en passant par Internet d'une façon sécurisée en utilisant le tunnel VPN.

Nous choisirons pour les deux sites les même clefs de chiffrement, le type de hachage, la taille de police, la longueur des clés, la durée de vie de clé avant renégociation, la méthode de cryptage des données, la durée de vie de la clé de cryptage, une ACL permettant d'identifier le trafic à traiter par le tunnel et enfin la création d'une cryptomap.

Tableau IV. 2: Paramètres de stratégie ISAKMP

Paramètre		**R1**	**R2**
Méthode de distribution des clés	Manuel ou **ISAKMP**	ISAKMP	ISAKMP
Algorithme de chiffrement	DES, 3DES,ou **AES**	AES	AES
Algorithme de hachage	MD5 ou **SHA-1**	SHA-1	SHA-1
Méthode d'authentification	**Clés Pre-share ou** RSA	Pre-share	Pre-share
Algorithme d'échange de clés	**Groupe DH(Diffie-Hellman) 1, 2 , ou 5**	DH 5	DH 5
Durée de vie de IKE SA	**86400 secondes ou moins**	86400	86400
Clé ISAKMP	/	Cisco	Cisco

Objectifs de la configuration simulée Cette réalisation a pour le but de :

- L'objectif de cette configuration simulé est de bloquer les attaques Dos, man in the middle et les craques des mots passes.

IV.7.1 Configuration et vérification d'IPsec VPN site à site à l'aide de la CLI

IV.7.1.1 Configuration des paramètres IPsec sur le routeur R1

1. Activer le module sécurité securityk9 sur le routeur :
   Exécution de la commande show version pour vérifier que la licence de pack est active si ce n'est pas le cas voir la figure IV.32

```
-----------------------------------------------------------------
Technology     Technology-package          Technology-package
               Current         Type        Next reboot
-----------------------------------------------------------------
ipbase         ipbasek9        Permanent   ipbasek9
security       None            None        None
data           None            None        None

Configuration register is 0x2102
```

Figure IV. 31: la commande show version pour le routeur 1

2. Activation de module pour autoriser la configuration de VPN

```
R2(config)#license boot module c1900 technology-package securityk9
```

Figure IV. 32: Activation de module au niveau de R1

3. Après l'enregistrement et redémarrage de routeur, on refaites un show version, le module est activé en version d'évaluation

```
-----------------------------------------------------------------
Technology     Technology-package          Technology-package
               Current       Type          Next reboot
-----------------------------------------------------------------
ipbase         ipbasek9      Permanent     ipbasek9
security       securityk9    Evaluation    securityk9
data           disable       None          None

Configuration register is 0x2102
```

Figure IV. 33: la commande show version après l'activation de module

4. Identification du trafic intéressant :

Au cours de cette partie, nous allons configurer une liste ACL 110 pour identifier le trafic du LAN sur R1 au LAN sur R2 comme intéressant. Ce trafic intéressant déclenchera la mise en œuvre du VPN IPsec chaque fois qu'il y a du trafic entre les réseaux locaux R1 et R2. Tout autre trafic provenant des réseaux locaux ne sera pas chiffré. (Voir la figure IV.34)

5. Configuration des propriétés ISAKMP :

Maintenant, à l'aide du tableau des paramètres de stratégie ISAKMP « Tableau IV.2 » nous allons configurer les propriétés de la politique 10 de cryptage ISAKMP sur R1 avec la clé de cryptage partagée « cisco ». Les valeurs par défaut ne doivent pas être configurées, par conséquent, seuls le chiffrement, la méthode d'échange de clés et la méthode DH doivent être configurés.

```
R1(config)#access-list 110 permit ip 209.165.200.224 0.0.0.255
172.16.3.0 0.0.0.255
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#crypto isakmp key cisco address 10.1.1.2
```

Figure IV. 34: Configuration des paramètres IPsec et des propriétés ISAKMP du R1

6. Configuration des propriétés ISAKMP :

Nous allons créer le jeu de transformations « VPN-SET » pour utiliser « esp-aes » et « esp-sha-hmac » et créer par la suite la carte cryptographique « VPN-MAP » qui lie tous les paramètres de la phase 2 ensembles. Nous allons utiliser le numéro de séquence 10 et l'identifier comme une carte « ipsec-isakmp ». (Voir la figure IV.35)

7. Configuration de la carte cryptographique sur l'interface sortante :

Enfin, il suffit d'appliquer la crypto map pour lier la carte de chiffrement « VPN-MAP » à l'interface S0/1/0 de sortie de routeur et dès que nous appliquons cette étape, nous recevons un message de routeur qui confirme ISAKMP : ISAKMP is ON. (Voir la figure IV.36)

```
R1(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R1(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#set peer 10.1.1.2
R1(config-crypto-map)#set transform-set VPN-SET
R1(config-crypto-map)#match address 110
R1(config-crypto-map)#
```

Figure IV. 35: Configuration des propriétés ISAKMP sur R1

```
R1(config-crypto-map)#int ser 0/1/0
R1(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Figure IV. 36: Configuration de la carte cryptographique sur l'interface sortante du R1

IV.7.1.2 Configuration des paramètres IPsec sur le routeur R2

Remarque : Les paramètres pour R2 sont identiques, la seule différence étant les adresses IP attribuées et les listes d'accès (Voir la figure IV.37).

```
R2(config)#access-list 110 permit ip 172.16.3.0 0.0.0.255 209.165.200.224 0.0.0.255
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#encryption aes 256
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 5
R2(config-isakmp)#exit
R2(config)#crypto isakmp key cisco address 10.1.1.1

R2(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R2(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R2(config-crypto-map)#set peer 10.1.1.1
R2(config-crypto-map)#set transform-set VPN-SET
R2(config-crypto-map)#match address 110

R2(config-crypto-map)#int ser 0/1/0
R2(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Figure IV. 37: Les commandes de configuration du VPN IPsec sur le routeur R2

IV.7.1.3 Vérification du VPN IPsec

IV.7.1.3.1 Vérification du tunnel avant le trafic intéressant :

Sur le routeur R1, nous tapons la commande « show crypto ipsec sa » et nous remarquons que le nombre de paquets encapsulés, cryptés, décapsulés et décryptés sont tous définis sur 0.

```
R1#show crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (209.165.200.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (172.16.3.0/255.255.255.0/0/0)
   current_peer 10.1.1.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0
```

Figure IV. 38: Vérification du tunnel avant le trafic intéressant

IV.7.1.3.2 Création d'un trafic intéressant :

Depuis PC-1 de réseau LAN, nous envoyons une requête Ping à PC-11 de l'agence de Bejaïa. (Voir la figure IV.39).

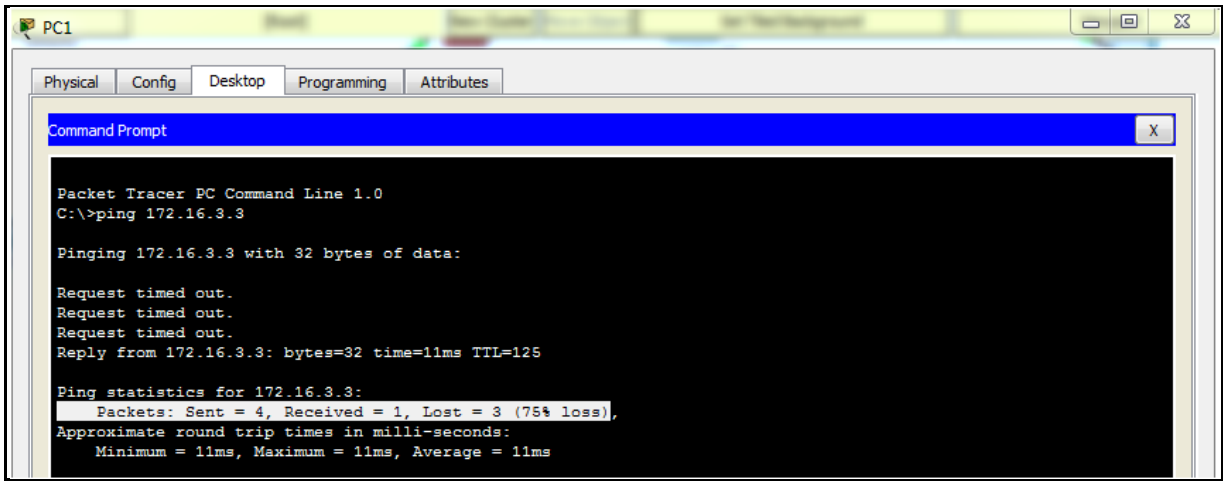


Figure IV. 39: Vérification du tunnel avant le trafic intéressant

IV.7.1.3.3 Vérification du tunnel après un trafic intéressant :

Sur le routeur R1, nous lançons la commande « show crypto ipsec sa » et nous remarquons bien que le nombre de paquets est supérieur à 0, ce qui indique que le tunnel VPN IPsec fonctionne. (Voir la figure IV.40)

```
R1#show crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (209.165.200.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (172.16.3.0/255.255.255.0/0/0)
   current_peer 10.1.1.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 0
   #pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0
```

Figure IV. 40: Vérification du tunnel après le trafic intéressant

IV.7.1.3.4 Création du trafic non intéressant :

Depuis PC-1, nous envoyons une requête Ping à PC-10.

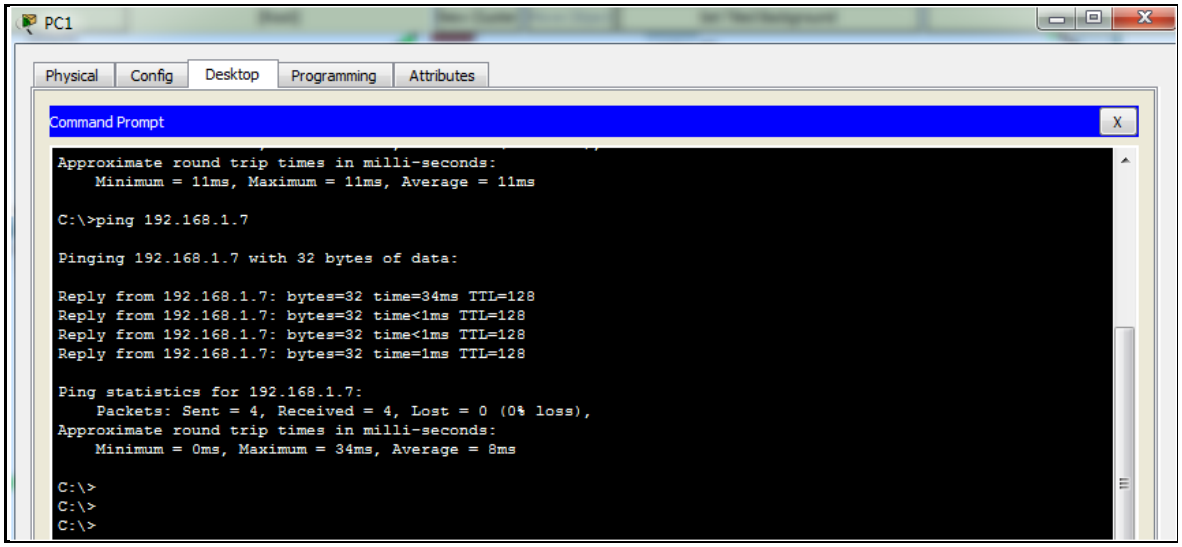


Figure IV. 41: Création du trafic non intéressant

IV.7.1.3.5 Vérification du tunnel après un trafic non intéressant:

Sur le routeur R1, nous allons relancer la commande « show crypto ipsec sa », nous remarquons que le nombre de paquets n'a pas changé, ce qui vérifie que le trafic non intéressant n'est pas chiffré. (Voir la figure IV.42)

```
R1#show crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port):
(209.165.200.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port):
(172.16.3.0/255.255.255.0/0/0)
   current_peer 10.1.1.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 0
   #pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0
```

Figure IV. 42: Vérification du tunnel après un trafic non intéressant

IV.7.1.3.6 Vérifions les informations retournées par le VPN sur R1

```
R1#show crypto ipsec transform-set
Transform set VPN-SET: {    { esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },
Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

Figure IV. 43: Les informations retournées par le VPN sur R1

La commande crypto IPSec transform-set nous a permis de savoir quel mode utilisé, dans notre cas c'est le mode tunnel. La vérification de la MAP VPN

IV.7.1.3.7 La vérification de la MAP VPN

```
R1#show crypto map
Crypto Map VPN-MAP 10 ipsec-isakmp
        Peer = 10.1.1.2
        Extended IP access list 110
            access-list 110 permit ip 209.165.200.0 0.0.0.255 172.16.3.0 0.0.0.255
        Current peer: 10.1.1.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                VPN-SET,
        }
        Interfaces using crypto map VPN-MAP:
                Serial0/1/0
```

Figure IV. 44: La vérification de la MAP VPN

L'exécution de la commande crypto map permet d'afficher l'adresse IP de destination et l'interface de sortie qui est activée.

IV.8 Mettre en œuvre la sécurité de la couche 2

IV.8.1 Configuration du pont racine avec le protocole STP[12]

Depuis la direction générale, nous allons exécuter la commande « spanning-tree vlan 1 root primary » pour affecter le commutateur central (direction générale) comme un pont racine.

Assignation du commutateur Division_Exploitaion et Divion_maintenance comme pont racine secondaire à l'aide de la commande « spanning-tree vlan 1 root secondary ».

```
Direction_Generale(config)#spanning-tree vlan 1 root pr
Direction_Generale(config)#spanning-tree vlan 1 root primary
Direction_Generale(config)#
```

Figure IV. 45: Configuration du pont racine principal sur la direction générale

```
Division_Exploitation(config)#spanning-tree vlan 1 root se
Division_Exploitation(config)#spanning-tree vlan 1 root secondary
Division_Exploitation(config)#
```

Figure IV. 46: Configuration du pont secondaire sur le switch Division Exploitation

Remarque : la même chose pour le commutateur Divion_maintenance.

IV.8.2 Configuration du protocole VTP et le mode TRUNK

IV.8.2.1 C'est quoi VTP :

C'est un protocole propriétaire Cisco de niveau 2. Il sert à la propagation de création/suppression/modification de VLAN sur tous les switchs de réseau à partir d'un seul switch cœur. C'est-à-dire le serveur VTP diffuse ses configurations VLAN, tandis que le client VTP met à jour sa configuration VLAN en fonction des informations reçues du serveur.

IV.8.2.2 VTP serveur :

Le Switch cœur du LAN AIR Algérie (direction générale), sera configuré comme un Server-VTP. Donc, c'est lui qui gère l'administration de l'ensemble des VLANs et évitant au même temps à l'administrateur de faire des erreurs, en se trompant par exemple de nom de VLAN.

En suite, on va créer un lien « TRUNK » entre les Switchs, afin de faire circuler les trames d'un Switch à l'autre. La figure suivante représente la Configuration du VTP et de port en mode TRUNK du Switch Direction_générale

[12] STP est un protocole réseau de niveau 2 qui permet de créer un chemin logique unique pour éviter les boucles dans les réseaux commutés

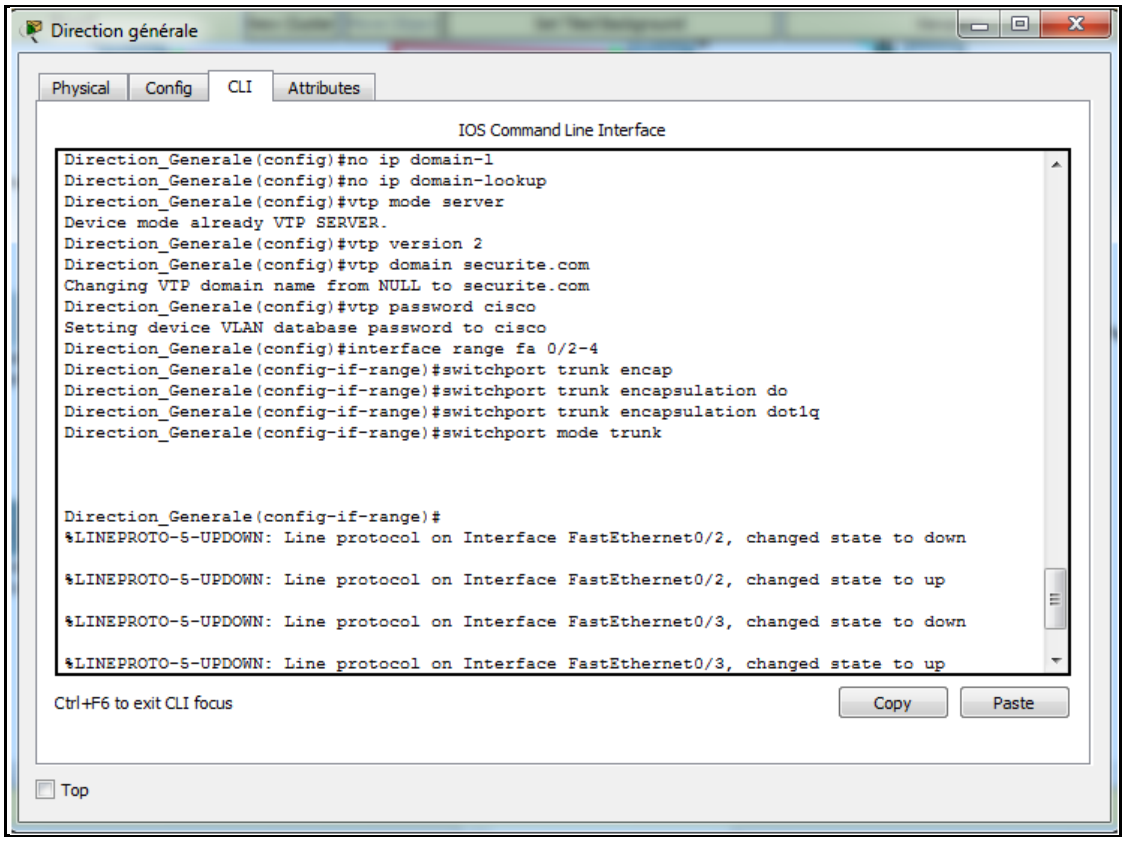


Figure IV. 47: VTP serveur et l'activation des liens trunk

IV.8.2.3 VTP client :

Par ailleurs, la configuration des Client-VTP sera au niveau de tous les commutateurs de Distribution et d'Accès du LAN en respectant le même nom du domaine et mot de passe, comme le montre la Figure IV.45 ainsi il **ne permet pas** à l'administrateur de faire des modifications sur les VLAN.

Remarque : La configuration des ports "TRUNK " pour toutes les interfaces des Switchs fédérateurs (Division_exploitation, Division_maintenance et Division_système).

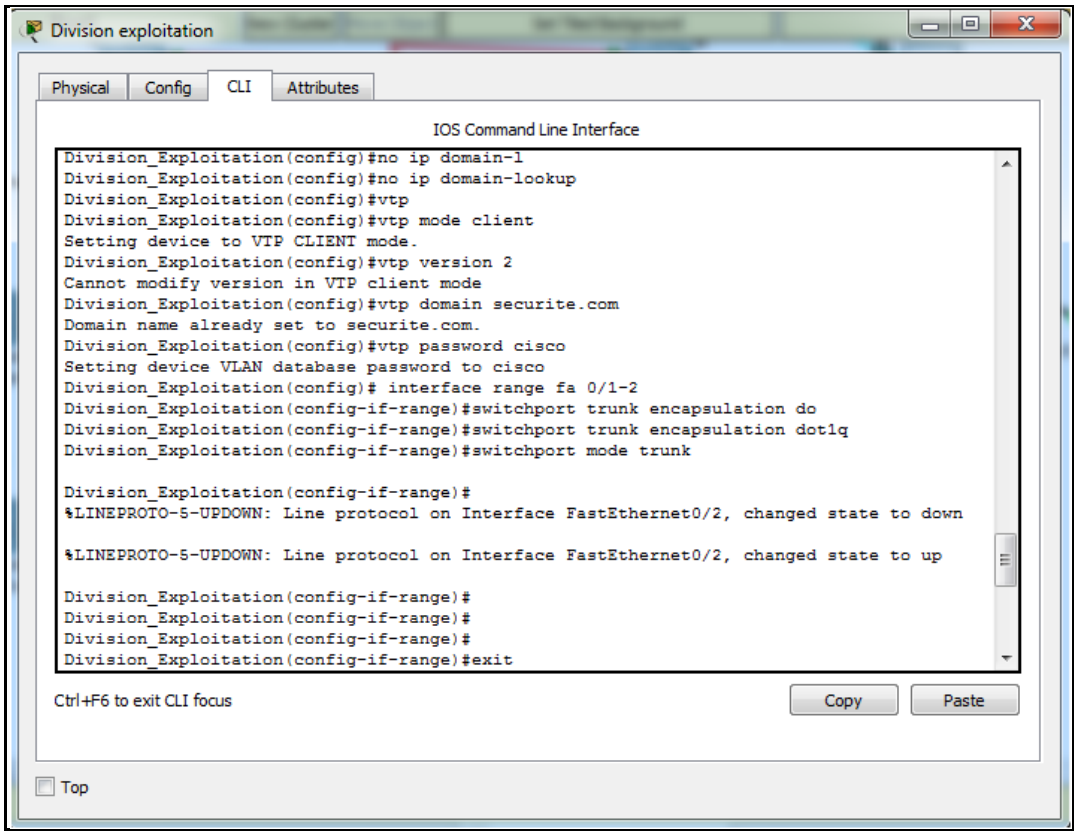


Figure IV. 48: VTP client et l'activation des liens trunk

Une fois que les VTP-Clients sont configurés, la configuration des VLANs effectuée sur le Switch cœur (VTP-Server) sera propagée à l'ensemble des autres commutateurs du réseau (clients), En effet, l'ensemble des VLANs vont être créés automatiquement.

IV.8.3 Protection contre les attaques STP

Au cours de cette partie, nous allons sécuriser les paramètres STP pour empêcher les attaques de manipulation STP.

IV.8.3.1 Activation du PortFast sur tous les ports d'accès :

PortFast est configuré sur les ports d'accès qui se connectent à un seul poste de travail ou serveur pour leur permettre de devenir actif plus rapidement. Sur les ports d'accès connectés des commutateurs dirctio_info_télecom, nous utilisons la commande « spanning-tree portfast ».

```
Direction Info Telecom(config-if-range)#spanning-tree portfast
```

Figure IV. 49: Activation du PortFast sur le switch Direction_Info_Télécom

IV.8.3.2 Activation de la protection BPDU sur tous les ports d'accès »

La protection BPDU est une fonctionnalité qui peut aider à empêcher les commutateurs non autorisés et l'usurpation d'identité sur les ports d'accès. Pour cela, nous allons activer la protection BPDU sur les ports d'accès direction_info_télecom.

```
Direction_Info_Telecom(config-if-range)#spanning-tree bpduguard enable
```

Figure IV. 50: Activation du de la protection BPDU sur le switch Direction_Info_Télécom

IV.8.4 Configuration de la sécurité des ports et de la désactivation des ports inutilisés

IV.8.4.1 Activation de la sécurité des ports de base sur tous les ports connectés aux machines :

Cette procédure doit être effectuée sur tous les ports d'accès sur le commutateur. Nous allons définir le nombre maximum d'appris l'adresse MAC à 2, permettre à l'adresse MAC d'être apprise dynamiquement et définir la violation à l'arrêt. NB : Un port de commutateur doit être configuré en tant que port d'accès pour activer la sécurité du port.

```
Direction_Info_Telecom(config)#interface range fastEthernet 0/2-4
Direction_Info_Telecom(config-if-range)#swi
Direction_Info_Telecom(config-if-range)#switchport mode access
Direction_Info_Telecom(config-if-range)#switchport access vlan 1
Direction_Info_Telecom(config-if-range)#switchport po
Direction_Info_Telecom(config-if-range)#switchport port-security
Direction_Info_Telecom(config-if-range)#switchport port-security ma
Direction_Info_Telecom(config-if-range)#switchport port-security maximum 2
Direction_Info_Telecom(config-if-range)#switchport port-security mac
Direction_Info_Telecom(config-if-range)#switchport port-security mac-address sticky
Direction_Info_Telecom(config-if-range)#switchport port-security violation shutdown
```

Figure IV. 51: Configuration de la sécurité des ports de base

Nous allons émettre la commande « show port-security » sur l'interface Fa0/2 pour vérifier que la sécurité du port a été configurée.

```
Direction_Info_Telecom#show port-security interface fastEthernet 0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Figure IV. 52: Vérification de la sécurité du port

IV.8.4.2 Désactivation des ports inutilisés :

Dans la première tache, on commence par la configuration de mode accès avec la commande « switchport mode access » et placer les interfaces dans le vlan 10 qu'on a créé avec la commande « switchport access vlan »

Dans cette dernière tache, nous désactivons tous les ports actuellement inutilisés pour des raisons d'efficacité.

```
Direction_Info_Telecom(config-if-range)#interface range fastEthernet 0/5-24 , gigabitEthernet
0/1, gigabitEthernet 0/2
Direction_Info_Telecom(config-if-range)#swi
Direction_Info_Telecom(config-if-range)#switchport mo
Direction_Info_Telecom(config-if-range)#switchport acc
Direction_Info_Telecom(config-if-range)#switchport access vl
Direction_Info_Telecom(config-if-range)#switchport access vlan 10
Direction_Info_Telecom(config-if-range)#exit
```

```
Direction_Info_Telecom(config)#interface range fastEthernet 0/5-24 , gigabitEthernet 0/1, gigabitEthernet 0/2
Direction_Info_Telecom(config-if-range)#shu
Direction_Info_Telecom(config-if-range)#shutdown
```

Figure IV. 53: Désactivation des ports inutilisés

IV.9 Conclusion

Au cours de ce dernier chapitre, nous avons mis en place les solutions de sécurité (mécanismes et protocoles) décrits et présentés dans les chapitres précédents pour montrer et prouver la nécessité de la mise en œuvre de politiques de sécurité dans les réseaux Cisco.

Notre but de cette simulation générale qui englobe tous les différents mécanismes et protocoles est d'implémenter une stratégie basée sur un fort plan de sécurité pour la protection contre les menaces et la lutte contre les attaques qui engendrent les réseaux Cisco.

Après nous avons pu décrire la procédure de configuration concernant la mise en place de politiques de sécurité sur les réseaux locaux et les réseaux Internet de l'entreprise ainsi que les résultats de ces configurations. Notre but était d'améliorer et assurer le fonctionnement sécurisé des réseaux configurés donc nous avons atteint notre objectif comme nous avons pu le constatés grâce aux captures ci-haut

La conclusion générale

Ce mémoire s'inscrit dans le cadre d'un projet de fin d'étude. Il aboutie a l'implémentation d'une solution pour sécuriser le réseau informatique d'Air Algérie, Il est difficile de mettre en œuvre une solution qui répond parfaitement aux besoins ressentis dans une entreprise, ce qui oblige les administrateurs réseau de travailler sans cesse afin d'arriver à une solution permettant d'améliorer la sécurité qui est quasi-indispensable pour le bon fonctionnement d'un réseau.

En effet, nous avons présenté un travail divisé en deux grandes parties, à savoir l'approche théorique qui subdivisé en deux chapitre : le premier a porté sur les concepts fondamentaux des réseaux locaux, dans lequel nous avons fait un petit aperçu sur les différentes typologies et les équipements d'interconnexion des réseaux locaux, ensuite dans le second chapitre, nous parlerons de l'impacte de la sécurité informatique sur les réseaux en exposant les objectifs ainsi que les stratégies de sécurité.

La deuxième partie a été consacrée à la finalisation du projet, laquelle est aussi subdivisé en deux chapitres dont le premier a porté sur l'architecture physique existante du réseau intranet d'Air Algérie, nous avons proposé de diviser ce réseau en deux sites indépendants pour une meilleure fluidité du trafic, qui devient de plus en plus important et de moins surcharger le firewall, ces deux sites seront ensuite reliés par un tunnel sécurisé. Dans chaque site nous avons proposé la mise en place :

- D'un Vlan avec le protocole VTP.
- D'un VPN site à site pour relié les deux sites tout en assurant les propriétés de sécurité, de confidentialité et d'authentification.
- D'un ACL afin de filtrer le trafic réseau.

Le dernier chapitre a été consacré à la réalisation du projet, où nous avons présenté l'outil de simulation « Packet tracer » ayant servi à l'élaboration du projet, tout en expliquant les configurations des différents équipements, nous avons également procédé à une série de tests en envoyant des requêtes "ping" pour évaluer l'efficacité de notre solution.

Ce travail nous a permis d'acquérir une expérience personnelle et professionnelle très bénéfique. Ce fut une occasion pour notre groupe de se familiariser avec l'environnement du travail et de la vie professionnelle, d'élargir et d'approfondir nos connaissances sur l'administration des réseaux informatiques.

Bibliographie

[1] : Guy PUJOLLE, les réseaux, livre de l'édition EYROLLES, (2008).

[2] : Laurent BLOCH et Christophe WOLFHUGEL, 2ème édition de Sécurité Informatique, de l'édition EYROLLES, (2009).

[3] : https://fr.wikipedia.org/wiki/Adresse_IP

[4] : https://www.ionos.fr/startupguide/productivite/intranet/

[5] : https://dumas.ccsd.cnrs.fr/dumas-01618811/document

[6] : https://www.insee.fr/fr/metadonnees/definition/c1864

[7] : https://www.devantis-evolution.ch/Securite.htm

[8] : https://web.maths.unsw.edu.au/~lafaye/CCM/secu/secuintro.htm

[9] : https://web.maths.unsw.edu.au/~lafaye/CCM/attaques/usurpation-ip-spoofing.htm

[10] : https://fr.wikipedia.org/wiki/ARP_poisoning

[11] : https://www.ionos.fr/digitalguide/serveur/securite/dns-spoofing/

[12] : https://fr.wikipedia.org/wiki/Attaque_de_l%27homme_du_milieu

[13] : https://fr.wikipedia.org/wiki/Cross-site_scripting

[14] :https://blog.arcoptimizer.com/sur-la-strategie-de-script-intersite-et-de-securite-du-contenu

[15] : https://fr.wikipedia.org/wiki/Attaque_par_d%C3%A9ni_de_service

[16] : https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203493-virus-definition-traduction-et-acteurs/

17] : https://www.websecurity.digicert.com/fr/ca/security-topics/difference-between-virus-worm-and-trojan-horse#

[18] : https://www.kaspersky.fr/resource-center/threats/computer-viruses-and-malware-facts-and-faqs

[19] : https://www.citypassenger.com

[20] : https://fr.wikipedia.org/wiki/Attaque_par_force_brute

[21] : https://fr.wikipedia.org/wiki/Attaque_par_dictionnaire

[22] : https://www.kaspersky.fr/resource-center/definitions/encryption

[23] : https://fr.wikipedia.org/wiki/MD5

[24] : https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203471-sha-secure-hash-algorithm-definition-traduction/

[25] : http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-fr-4/ch-ssh.html

[26] : https://www.francenum.gouv.fr/comprendre-le-numerique/la-signature-electronique-un-outil-devenu-incontournable

[27] : https://blog.varonis.fr/ids-et-ips-en-quoi-sont-ils-differents/

[28] : https://cisco.goffinet.org/ccna/filtrage/concept-ids-ips/

[29] : https://www.connecthostproject.com/acl.html

[30] : https://www.manageengine.com/fr/network-configuration-manager/configlets/what-is-nat.html

[31] : https://idealogeek.fr/vpn-reseau-prive-virtuel/

[32] : www.le-vpn.com

[33] : https://www.opportunites-digitales.com/protocoles-vpn

[34] : https://www.commentcamarche.net/contents/543-vlanreseaux-virtuels

[35] : http://projet.eu.org/pedago/sin/ISN/8-VLAN.pdf

[36] : https://www.commentcamarche.net/contents/543-vlan-reseaux-virtuels

[37] : http://deptinfo.cnam.fr/Enseignement/CycleProbatoire/SECURITE/cours_parefeux.pdf

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

[39] : http://www-igm.univ-mlv.fr/~duris/NTREZO/20052006/MasquelierMottierPronzato-Firewall-rapport.pdf

[40] : https://wikimemoires.net/2012/08/quest-ce-quun-firewall-fonctionnement-et-types-de-firewall/

[41] : https://geekflare.com/fr/hardware-vs-software-cloud-firewall/

[42] : http://www.ordinateur.cc/Logiciel/antivirus-Software/101169.html

[43] : https://wikimemoires.net/2012/08/quest-ce-quun-firewall-fonctionnement-et-types-de-firewall/

[44] : https://www.ionos.fr/digitalguide/serveur/securite/quest-ce-quune-zone-demilitarisee-dmz/

[45] : Jabou Chaouki, Schillings Michaël et Hantach Anis, " TER Détection d'anomalies sur le réseau ", Rapport de projet, Université Paris Descartes, 2009.

Annexe A

Classification des réseaux

Classification selon l'étendue

1. **Réseau local (LAN : Local Area Network) :** Lorsque le réseau s'étend sur un périmètre local **(<1 Km)** et un débit de données de 10 à 1000 Mbit/s
2. **Réseau métropolitain (MAN :Metropolitan Area Network)** : lorsque le réseau s'étend sur un périmètre**(<100 Km)** et un débit de données de 1 à 100 Mbit/s.
3. **Réseau étendu (WAN :Wide Area Network) :** Lorsque le réseau s'étend sur longue distance**(>100 Km)** et un débit de données de 1 à 100 Mbits/s c'est le réseau public internet.
4. **Réseau PAN (Personal Area Network) :** c'est un réseau personnels, souvent de faible portée, on l'utilise surtout pour les liaisons sans fil : souris, clavier, imprimante etc. il s'étend sur 1 mètre carré environ.

Classification selon la topologie

La topologie en bus

Est l'organisation la plus simple d'un réseau où tous les nœuds sont connectés sur le même support de transmission (qui est un câble de backbone unique terminé aux deux extrémités par un bouchon de terminaison). C'est un réseau à diffusion qui désigne le fait que lors de l'émission de données sur le bus par une station de travail, les données circulent sur toute la longueur du bus et seule la station de travail destinatrice peut la récupérer. Un seul ordinateur peut émettre à la fois.

L'avantage de cette topologie est qu'un ordinateur en panne ne perturbe pas le reste du réseau. Par contre, en cas de rupture de câble, le réseau devient inutilisable

La topologie en anneau

C'est un réseau où toutes les entités sont reliées entre elles dans une boucle fermée. Les données circulent dans une direction unique, d'une entité à la suivante et n'accepte une donnée en circulation sur l'anneau que, si elle correspond bien à son adresse. Dans le cas contraire, l'entité en question fait passer la donnée à l'entité suivante. Ce qui permet d'éviter le problème majeur de la topologie en bus : la collision des données.

L'inconvénient de cette topologie est que le retrait ou la panne d'une entité active paralyse le trafic du réseau et il est également difficile d'insérer une nouvelle station.

La topologie en étoile

C’est la topologie la plus courante. Toutes les machines sont reliées à un appareil comme un Hub, un Switch ou un routeur qui est au centre du réseau pour communiquer à une autre machine, le message envoyé par l’ordinateur est obligé de passer par ce point central ce qui permet d’éviter les collisions entre les paquets, ce type de réseau est facile à mettre en place et à surveiller mais il faut plus de câbles que pour les autres topologies, Le risque est que si l’appareil central n’est plus en état de marche, le réseau ne fonctionne plus.

Topologie maillée

Est une topologie réseau hybride de type étoile correspond à plusieurs liaisons point à point entre les différents ordinateurs (c'est-à-dire Chaque terminal est relié à tous les autres).

Le principal avantage de ce type de topologie est l’adaptabilité : une ligne coupée ne perturbe pas les communications.

Topologie Ethernet

(Aussi connu sous le nom de *norme IEEE 802.3*). Elle est aujourd’hui l’un des technologies les plus utilisés en local. Il repose sur une topologie physique de type bus linéaire, c’est-à-dire tous les ordinateurs sont reliés à une même ligne de transmission. La communication se faite à l’aide d’un protocole appelé CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*). Chaque station veut émettre doit vérifier si le canal est libre parce que, au moment ou deux stations émettent en même temps, il y a alors une collision, les machines vont interrompre leur envoi de message et attendre aléatoirement un temps avant de réessayer d’envoyer leur données.

Topologie Token ring

Token Ring repose sur une topologie en anneau (ring). Il utilise la méthode d’accès par jeton (token). Dans cette technologie, seul le poste ayant le jeton a le droit de transmettre (pendant un temps déterminé). Si un poste veut émettre, il doit attendre jusqu’à ce qu’il ait le jeton. Dans un réseau Token Ring, chaque nœud du réseau comprend un MAU (Multi station Access Unit) qui va donner successivement "un temps de parole" à chaque poste et permit ainsi de régénérer le signal.

Les équipements d'interconnexion

Répéteur

C'est un élément qui régénère et augmente le signal pour le transmettre d'un réseau à un autre. Il agit au niveau 1(physique) du modèle OSI. Est conçu pour remédier au problème d'affaiblissement des signaux.

Concentrateur (hub)

Est un dispositif qui joue le rôle d'un répéteur multiport donc lorsqu'un paquet est reçu sur un port, celui-ci est envoyé aux autres ports afin que tous les segments du réseau local pissent accéder à tous les paquets, travail sur la 1 ère couche de modèle OSI et utilise la topologie étoile avec une communication Half Duplex.

Pont (Bridge)

Les ponts sont des équipements permettant de relier des réseaux travaillant avec le même protocole au niveau de la couche 2 de modèle OSI.

Commutateur (*Switch*)

Est un hub intelligent qui peut relier un segment de réseau à un ou plusieurs autres segments selon leurs adresses physiques de la couche liaison de données. Il possède une mémoire interne qui contient les informations sur le réseau commuté stocké dans une table appelé « table de commutation ».

Passerelle (*Gateway*)

Est un système matériel et logiciel permettant de passer des informations d'un réseau à un autre (relier deux réseaux informatiques de types différents) en adaptant les différent couche de modèle OSI.

Routeur

Opèrent au niveau de la couche réseau du modèle OSI (*Open System Interconnexion*), capable d'interconnecter plusieurs réseaux utilisant différents protocoles entre eux. Il permettant d'assurer le routage des paquets afin de déterminer le chemin qu'un paquet de données va emprunter

Les équipements matériels

Carte réseau

La carte réseau est l'interface entre l'ordinateur et le réseau. Elle assure donc les échanges et les transferts des données avec les autres appareils présents sur le réseau tels que des serveurs, des imprimantes ou même des PCs. Elle est identifiée avec une adresse physique (***l'adresse Mac***).

La fibre optique

Est un support physique de transmission de données IP à très haut débit et sur une grande distance, se compose d'une fibre d'émission et une fibre de réception .Il permet de propager des ondes lumineuses entre deux lieux avec une transmission très rapide sans perte la vitesse (Exemple: câbles Sous-marins).

La paire torsadée

Décrit un modèle de câblages où une ligne de transmission est formée de deux conducteurs enroulés en hélice l'un autour de l'autre sert à la protection contre les interférences. Il existe deux type : la paire torsadée blindée et non blindées

- La paire torsadée blindée est entourée d'une couche conductrice de blindage, cela permet une meilleur protection contre les interférences (exemple : réseau Token ring).
- La paire torsadée non blindée n'est pas entourée d'un blindage protecteur. C'est le type e câble fréquemment utilisé pour les téléphones et certains réseaux informatiques domestiques.

Le câble coaxial

C'est un câble électrique constitué d'une carte centrale appelée âme généralement en cuivre (c'est-à-dire un fil de cuivre enveloppé dans un isolant, puis un blindage métallique tressé enfin une gaine extérieur), Il est utilisé pour la transmission de signaux numérique ou analogique par une fréquence haute ou basse entre différents appareils audio et vidéo

Mode de transmission

Selon le sens des échanges, on distingue trois modes de transmission :

- La liaison simplex (c'est le mode de communication unidirectionnel).
- La liaison half-duplex (deux systèmes interconnectés sont capable d'émettre et de recevoir chacun leur tour).
- La liaison full-duplex (deux systèmes interconnectés sont capable d'émettre et de recevoir simultanément).

Annexe B

Les modèles de référence

Les couches du modèle OSI

Tableau B. 1: Différentes couches du modèle OSI

Niveau	Couches	Description	Exemple
7	**Application**	assure l'interface avec les applications, il s'agit donc du niveau le plus proche des utilisateurs géré directement par les logiciels. Plusieurs protocoles sont utilisé FTP, Telnet et SSH, SMTP, http et SSL	navigateurs Web messagerie électronique transfert de fichiers connexion distante
6	**Présentation**	s'occupe de la mise en forme des données, pour le rôle d'adapter toutes les données à émettre à un format standard épuré de tous les aspects liés à l'environnement de travail et en particulier au système d'exploitation.	Encryptant et compression des données mise en forme des textes, images et vidé
5	**Session**	Cette couche permet à deux applications de créer une connexion qui est permanente. Donc la couche session ouvre, gère et ferme les sessions entre deux systèmes hôte en communication. C'est à ce niveau que l'on décide du mode de transmission : simplexe, semi-duplex ou duplex.	Ouverture de session Windows Authentification
4	**Transport**	C'est une couche de bout en bout : elle permet l'´etablissement, le maintien et la rupture de connexions de transport. Selon les fonctionnalités offertes par le réseau (les couches inférieures), Elle est responsable du bon acheminement des messages complets au destinataire.	UDP TCP FireWall
3	**Réseau**	Cette couche assure la connectivité et l'acheminement de paquets d'une extrémité à une autre et le routage des paquets de données entre les nœuds du réseau. Elle gère donc l'adressage logique et le routage	Routeur ICMP[13]
2	**Liaison de données**	C'est à ce niveau que les données numériques sont traduites en signal. elle a pour rôle d'assurer la transmission des trames entre les systèmes d'une manière correcte. Elle est divisée en deux sous-couches : Mac[14] et LLC[15]	HDLC CSMA /CD l'interface avec la carte réseau(Switch) Ethernet, PPP
1	**Physique**	S'occupe de la transmission des bits représentés par des signaux électriques (numérique ou analogique), il décrit aussi les équipements de transmission en respectant certains protocoles bien définis	Hub Câble réseau Carte réseau

[13] Pour les messages de contrôle et d'erreur
[14] Sous-couche d'accès au médium
[15] Le contrôle logique de la liaison permet d'établir un lien logique entre la couche MAC et la couche de niveau 3 du modèle OSI et fiabiliser le protocole MAC par un contrôle d'erreur et un contrôle de flux

Les couches du modèle TCP/IP

Tableau B. 2: Différentes couches du modèle TCP/IP

Couche	Description	Protocole
Application	Elle prend en charge les protocoles de haut niveau comme protocole d'adressage et l'administration réseau…, qui assurant le transfert de fichiers, le courrier électronique et la connexion à distance.	SMTP[16] La téléphonie IP et la VoIP (SIP) La connexion à distance (TELNET, SSH) Le Web (HTTP) L'administration réseau (PING) La sécurité (SSL), DNS, DHCP, TFTP
Transport	Assure une communication de bout en bout en faisant abstraction des machines intermédiaires entre l'´emetteur et le destinataire Assure le transfert des données et les contrôles de flux qui permettent de vérifier l'état de la transmission.	**TCP :** transport fiable (données transmises sans erreur et reçus dans l'ordre de leur émission) orienté connexion. **UDP :** transport non fiable de données et sans connexion.
Internet	traite le format des paquets envoyés à travers l'Internet, ainsi que des mécanismes qui permettent de propager les paquets échangées, elle assurer que les données envoyées arrivent correctement à destination.	**IP** (transport des datagrammes IP) **ICMP** **ARP[17]** **RARP[18]**
Accès réseau	Assure l'interface physique avec le réseau elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé.	Ethernet,Token Ring X.25[19]

[16] SMTP est le protocole de communication utilise pour transférer le courrier électronique (mails) vers les serveurs messagerie.
[17] ARP traduire l'adresse IPv4➔adresse Mac.
[18] RARP Le protocole inverse d'ARP.
[19] X.25 est le protocole normalisé pour la communication des paquets qui ne précise pas comment sont acheminés au sein du réseau mais définit seulement les procédures d'échange

Annexe C

Présentation générale de l'adresse IP

IPv4 (*Internet Protocol version 4*) **:** C'est la version 4 sur 32 bits qui est actuellement la plus utilisée, et décrite par la norme RFC[20] 791. Elle est généralement représentée en notation décimale avec quatre nombres compris entre 0 et 255, séparés par des points ce qui donne par exemple
« 192.168.1.1 » [24]

IPv6 (*Internet Protocol version 6*) **:** C'est la version 6 sur 16 octets qui permettre de connecter un plus grand nombre d'hôtes sur un réseau car les plages d'adresses IPv4 étant proches de la saturation, les opérateurs incitent à la transition d'IPv4 vers IPv6. C'est le protocole réseau sans connexion de la couche 3 du modèle OSI (Open Systems Interconnection). Sa norme est la RFC 2460 [25]

Chaque adresse IP d'une machine est appelée l'adresse logique peuvent être divisé en deux partie, la partie réseau et la partie hôte à l'aide d'un masque de réseau.

Le Net ID : correspond à l'adresse réseau, permet d'identifier les systèmes qui sont situés sur le même réseau physique.

Le Host ID : correspond à l'adresse de la machine sur le réseau, elle identifie un poste de travail, un serveur, un routeur etc.

Les classes d'adresses IP

Tableau C. 1: Les classes d'adresses IP

Classes	Plages d'adressage	Spécification
A	0.0.0.1➔126.255.255.254	Cette classe est destinée pour les très grands réseaux. Seul le premier octet est utilisé pour la partie réseau, ce qui laisse donc 3 octets pour la partie hôte
B	128.0.0.1➔ 191.255.255.254	Une @ IP de classe B dispose de deux octets pour identifier le réseau et de deux octets pour identifier les machines sur ce réseau
C	192.0.0.1➔ 223.255.255.254	Une @ IP de classe C dispose de trois octets pour identifier le réseau et d'un seul octet pour identifier les machines sur ce réseau.
D	224.0.0.0➔239.255.255.255.	La classe D permet de gérer une communication multipoint est destinée à faire de la diffusion d'information sur plusieurs hôtes simultanément. Elle n'a donc pas de NetID ni de HostID.
E	240.0.0.0➔247.255.255.255	La classe E est réservée s à un usage spécifique

[20] RFC (*Request For Comments*) est un ensemble de documents qui décrivent, spécifient, aident à l'implémentation et standardisent la majorité des normes, standards, technologies et protocoles liés à Internet et aux réseaux en général. Établies par un organisme qui s'appelle l'*IETF* (Internet Engineering Tasking Force)

L'adressage sans classes CIDR (*Classless Inter-Domain Routing*)

Comme son nom l'indique, l'adressage par classes est abandonné ici, (Il n'y a donc plus de masque fixé par référence à une classe), c'est le système de gestion et d'allocation d'adresses IP le plus utilisé aujourd'hui. Ce système, qui est régi par les RFC 1518 et 1519, a été conçu pour remplacer l'adressage par classes pour les raisons de fiabilité et de performance. Elle est notamment utilisée sur le réseau public Internet.

Par exemple 192.168.10.0/23 applique un masque de 255.255.254.0 au réseau 192.168.10.0

Le but de ce nouveau système s'articule autour de deux points :

- Économiser les adresses IP.
- Faciliter le routage.

Les adresses particulières

L'Adresse de bouclage (*Loopback*)

C'est l'interface réseau réservée utilisée par le système local pour permettre les communications entre processus. L'hôte utilise cette adresse pour s'envoyer des paquets à lui-même sans passer par le réseau. Par exemple le système du réseau TCP/IP doit utiliser l'adresse IP 127.0.0.1 pour le loopback IPv4 sur l'hôte locale. Elle sert à travailler en mode client/serveur[21] sur la même machine

Exemple : ping 127.0.0.1 « un ping vers votre ordinateur ».

L'adresse 0.0.0.0

Est une méta-adresse non-routable utilisée pour désigner une destination inconnue ou non-atteignable. Donner un sens particulier à un datagramme invalide. Cette adresse est l'adresse par défaut qui veut dire pour aller n'importe où (quand on ne trouve pas d'entrée correspondant à une adresse réseau de destination), on emprunte l'adresse (ou le port ou l'interface) de sortie indiquée dans la table de routage. C'est la destination par défaut qui correspond à l'adresse 0.0.0.0 dans la table de routage.

L'adresse MAC

Relative à la carte réseau est un identifiant unique attribué à chaque carte réseau. C'est une adresse physique. Concrètement, c'est un numéro d'identification composé de 12 chiffres hexadécimaux. Par convention, on place un symbole deux-points (:) tous les 2 chiffres. Une adresse MAC ressemble donc à cela : 01:23:45:67:89:AB.

[21] Représente l'environnement dans lequel des applications de machines clientes communiquent avec des applications de machines de type serveurs qui leur fournit des services

Les adresses interdites

Dans les plages d'adresses assignables à des machines d'un réseau, il y aura toujours deux adresses interdites : l'adresse de broadcast (diffusion) et l'adresse du réseau.

L'adresse de diffusion

Lorsque on met tous les bits à 1 dans le Hostid, on obtient la dernière adresse dans un réseau qui est l'adresse de broadcast : c'est une adresse de diffusion générale à toutes les machines du réseau (Exemple : 192.168.52.255 avec un masque 255.255.255.0).

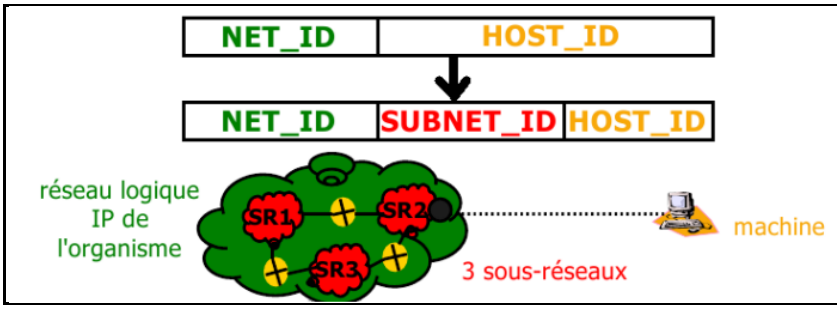
L'adresse de réseau

On remarque que l'adresse d'un réseau est composée du NetID et d'un HostID où tous les bits sont à 0. On en déduit qu'une adresse de réseau ne peut être assignée à une machine pour éviter tout risque de confusion.

Le masque d'un sous-réseau

Un masque de sous-réseau (désigné par subnet mask) est un masque indiquant le nombre de bits utilisés pour identifier le sous-réseau et le nombre de bits caractérisant les hôtes

Pour segmenter un réseau en sous-réseaux, il faut alors décomposer la partie hostid de l'adresse IP en deux parties : une adresse de sous-réseau (subnetid) et une adresse machine (hostid).



Par exemple, pour créer 3 sous-réseaux, il faudra prendre 2 bits dans la partie HostID et on créera 22 donc 4 sous-réseaux :

1. 0 0 pour le sous-réseau n°0
2. 0 1 pour le sous-réseau n°1
3. 1 0 pour le sous-réseau n°2
4. 1 1 pour le sous-réseau n°3

Évidemment, le masque de départ change et doit maintenant englober la partie netid et la partie subnetid. Ce nouveau masque se nomme masque de sous-réseaux. Le nombre de machines adressables dans chaque sous-réseau est:

$2^{(nb\ bits\ hostid)}$ – 2 adresses interdites

Exemple : pour le réseau 192.168.1.0/24 découpé en 4 sous-réseaux (2^2 sous-réseaux)

Net_ID=24 bits Subnet= 2 bits Host_ID=32-24-2=6 bits

- Le masque de sous-réseau sera : 24 + 2 = 26 bits soit 255.255.255.192
- Le nombre de machines adressables dans chaque sous-réseau est : $2^6 - 2 = 62\ adresses$

Tableau C. 2: Les adresses principales pour chaque sous-réseau

Numéro de sous-réseau	**Adresse de sous-réseau**	**L'adresse de 1 ère machine**	**L'adresse de dernière machine**	**L'adresse de diffusion**
sous-réseaux n°0	192.168.1.0/26	192.168.1.1	192.168.1.62	192.168.1.63
sous-réseaux n°1	192.168.1.64/26	192.168.1.65	192.168.1.126	192.168.1.127
sous-réseaux n°2	192.168.1.128/26	192.168.1.129	192.168.1.190	192.168.1.191
sous-réseaux n°3	192.168.1.192/26	192.168.1.193	192.168.1.254	192.168.1.255

Annexe D

Le routage

Tableau D. 1: Tableau comparative entre le routage statique et routage dynamique

	Routage Statique	***Routage dynamique***
Mise en œuvre dans	Les petits réseaux	Grands réseaux
Configuration	Manuel	Automatique
Les routes	Défini par l'utilisateur	Les itinéraires sont mis à jour en fonction du changement de topologie
La construction de la table de routage	Les routes sont remplies à la main	Les routes sont remplies dynamiquement dans la table
Algorithme de routage	N'utilise pas d'algorithmes de routage	Utilise des algorithmes de routage complexes pour effectuer des opérations de routage (court chemin)
La sécurité	Fournit une haute sécurité	Moins sécurisé en raison de l'envoi de diffusions et de multidiffusion
Échec du lien	L'échec de liaison bloque le routage	L'échec de liaison n'affecte pas le routage
Modifications apportées à la topologie	Intervention de l'administrateur requise	S'adapte automatiquement aux modifications apportées à la topologie
Prévisibilité	La route dépend de la topologie actuelle	La route menant à la destination est toujours la même
Les protocoles	Ne nécessite pas de protocole	Utilise des protocoles tels que RIP
Les ressources	N'a pas besoin de ressources supplémentaires	Nécessite des ressources supplémentaires telles que la mémoire la bande passante…etc.

Annexe E

Exemple de la signature et vérification d'un document

Si Alice souhaite envoyer un document signé à Bob.

- Tout d'abord, elle génère l'empreinte du document au moyen d'une fonction de hachage.
- Puis, elle crypte cette empreinte avec sa clé privée.

Elle obtient ainsi la signature de son document. Elle envoie donc ces deux éléments à Bob

- Pour vérifier la validité du document, Bob doit tout d'abord déchiffrer la signature en utilisant la clé publique d'Alice. Si cela ne fonctionne pas, c'est que le document n'a pas été envoyé par Alice.
- Ensuite, Bob génère l'empreinte du document qu'il a reçu, en utilisant la même fonction de hachage qu'Alice (On supposera qu'ils suivent un protocole établi au préalable).
- Puis, il compare l'empreinte générée et celle issue de la signature.
- Si les deux empreintes sont identiques, la signature est validée. Nous sommes donc sûr que :

    1. C'est Alice qui a envoyé le document,
    2. Le document n'a pas été modifié depuis qu'Alice l'a signé.

- Dans le cas contraire, cela peut signifier que :
    1. Le document a été modifié depuis sa signature par Alice,

Ce n'est pas ce document qu'Alice a signé

L'antivirus

Est l'un des principaux dispositifs de sécurité pour garantir la protection des données de l'utilisateur et une navigation optimale sur le web contre d'autres logiciels malveillants. Ce logiciel élimine ou réduit le cyber attaques. Il possède deux propriétés principales, la première est une protection constante qui vous permet notamment de naviguer en toute tranquillité sur le Web. La seconde il offre la possibilité d'effectuer une analyse des supports de stockage (disque dur, CD-Rom, clé USB…)

Annexe F

Présentation du simulateur Packet Tracer:

Packet Tracer est un simulateur de matériel réseau développé par Cisco Systems, permettant d''elaborer des représentations virtuelles de réseaux et de simuler le comportement des protocoles réseaux. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs, les serveurs, des ordinateurs…etc. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique, wifi…etc.). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les Switchs ...etc.

Exploration de l'interface de Packet Tracer

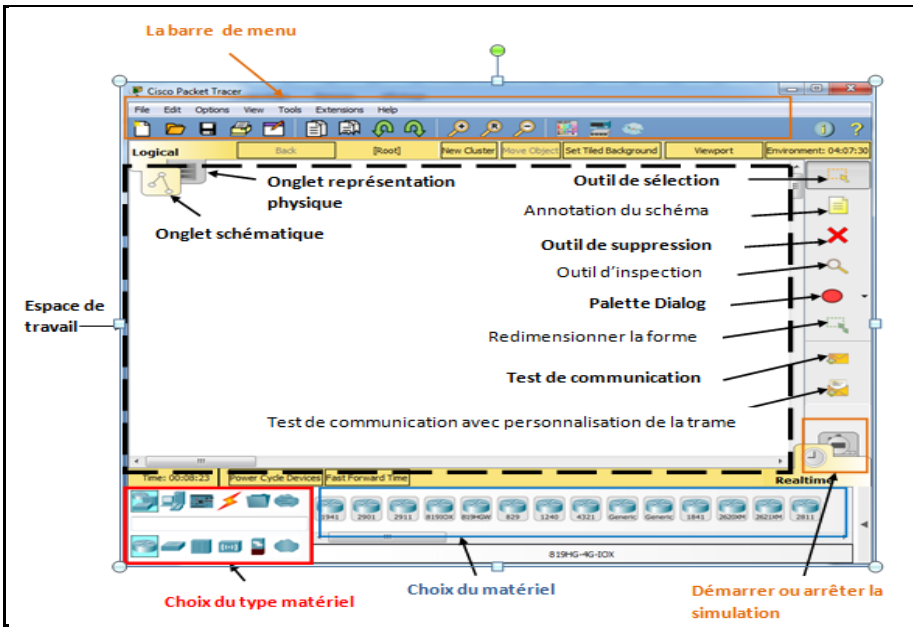


Figure F. 1: Interface Cisco Packet Tracer

Eléments de base du Packet Tracer:

Pour construire un réseau, l'utilisateur doit choisir parmi les catégories proposées par Packet Tracer qui sont représentés sur la figure (IV.2). Lorsqu'une catégorie est sélectionnée, l'utilisateur a alors le choix entre plusieurs équipements différents. Pour ajouter un équipement, il suffit de cliquer dessus puis de cliquer à l'endroit choisi. La figure suivante correspond à la zone décrite.

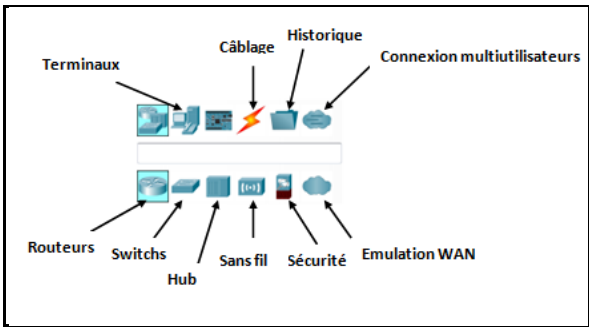


Figure F. 2: Type matériels

Création d'une connexion :

Pour relier deux équipements, il faut choisir la catégorie "Connections" puis cliquer sur la connexion désirée. Dans nos travaux pratiques, nous n'utiliserons que 3 sortes de connexions : les câbles droits, les câbles console et câble serial (Voir la figure IV.3).

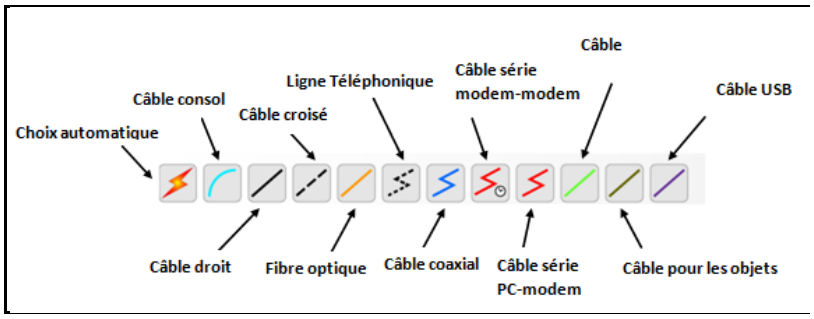


Figure F. 3: Les différents supports de transmission

Tableau F. 1: Utilisation des différents supports de transmission

Désignation	***Utilisation***
Câble console	Utilisé pour la configuration des routeurs ou Switchs en local
Câble droit	Utilisé pour relier deux éléments de différent type (Pc-Switch par exemple)
Câble croisé	Utilisé pour relier deux éléments de même type (Pc-Pc par exemple)
Câble série	Utilisé pour relier deux routeurs distants **(Câbles DCE[22] et DTE[23])**
Câble Coaxial	Pour la ligne téléphonique, sauf (ports utilisés sont des ports coaxiales)
Fibre optique	pour les équipements possèdent les ports fibre adéquates.
Ligne téléphonique	Pour connexions téléphoniques entre les équipements possédant des ports modem.

[22] DCE utilisé pour des équipements intermédiaires utilisés sur des liaisons (modems,...)
[23] DTE utilisé pour des équipements terminaux (PC, imprimante,...etc.).

Annexe G

Principes d'un modèle de conception

Un modèle de conception sert à construire des réseaux en respectant certaines règles d'architecture qui leur permettent de répondre aux besoins actuels et futurs des entreprises et de leurs utilisateurs.

Voici les principes de se modèle :

- **Hiérarchie** : le modèle offre des niveaux fonctionnels : Core/Distribution/Access
- **Modularité** : il supporte facilement la croissance et les changements; faire évoluer le réseau est facilité par l'ajout de nouveaux modules au lieu redessiner entièrement l'architecture du réseau.
- **Flexibilité** : les changements dans l'entreprise peuvent être adaptés au réseau rapidement selon les besoins
- **Sécurité** : la sécurité est intégrée au niveau de chaque couche

Résumé

Suite à notre étude sur la sécurité des réseaux informatiques ainsi que les différentes menaces auxquelles les réseaux d'entreprises sont exposés, nous nous rendons compte qu'il n'est pas évident d'assurer une sécurité optimale à un réseau informatique et de le protéger contre d'éventuelles intrusions et menaces. Avoir un réseau complètement sécurisé est pratiquement irréalisable. Par conséquent, il est nécessaire de pouvoir détecter les intrusions lorsqu'elles se produisent. Cela est rendu possible grâce aux mécanismes de sécurité. Ces mécanismes consistent à détecter, prévenir et lutter contre les attaques.

Dans ce travail, nous nous intéressons à l'implémentation purement software sur une plateforme configurable basée sur CISCO dans laquelle nous allons configurer les différentes solutions de sécurité et nous testons la fiabilité de chaque solution.

Mots-clés : Sécurité informatique, politique de sécurité, mécanismes de sécurité, attaques, ACL, Cryptographie, par-feu, IDS, VPN, IPsec, ISAKMP, SSH et antivirus.

Abstract

Following our study on the security of computer networks as well as the various threats to which business networks are exposed, we realize that it is not easy to ensure optimal security for a computer network and to protect it. against possible intrusions and threats. Having a completely secure network is practically impossible. Therefore, it is necessary to be able to detect intrusions when they occur. This is made possible by the security mechanisms. These mechanisms consist of detecting, preventing and combating attacks.

In this work, we are interested in the pure software implementation on a configurable platform based on CISCO. In which the various security solutions are configured and the reliability of each solution is tested.

Keywords: Computer security, security policy, security mechanisms, attacks, ACL, Cryptography, firewall, IDS, VPN, SSH and antivirus.