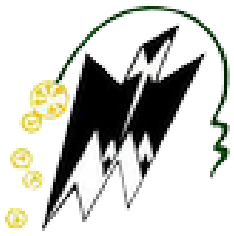
République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mouloud Mammeri de Tizi-Ouzou



Faculté De Génie Électrique et d'Informatique
Département de Télécommunications

Mémoire de Fin d'Etudes

de MASTER ACADEMIQUE
Filière :
Télécommunication
Spécialité :
Réseaux et Télécommunications

Par

Lina SAHARI
Malha MALKI

Thème

Mise en place d'une solution de sécurité pour un réseau d'entreprise

Soutenu le : 26/06/2024

Devant le jury :

Président :	Mme. Tassadit BECHA	Univ. UMMTO
Promoteur :	Mme. Dihia BELKACEMI	Univ. UMMTO
Examinateur :	Mme. Ouiza BOUSSOUM	Univ. UMMTO

Remerciements

Nous remercions d'abord "le bon Dieu" de nous avoir donné le courage et la patience pour réaliser ce modeste travail.

Ensuite, nous tenons à exprimer notre gratitude à notre promotrice, Madame ***Dihia Belkacemi****, pour sa disponibilité, son soutien et ses précieux conseils tout au long de ce travail.*

Nos remerciements s'adressent également aux membres du jury qui ont eu l'amabilité d'évaluer notre travail et de participer au jury de soutenance.

Un hommage éternel à tous les enseignants qui nous ont encadrés depuis nos premières années d'études jusqu'à aujourd'hui.

Nous adressons un grand merci à nos familles pour leur soutien durant cette recherche et toutes ces longues années, ainsi qu'à nos amis et à tous ceux qui nous ont aidés de près ou de loin.

…

Dédicace

A*vec tout honneur et fierté, je dédie ce modeste travail :*

À *moi-même, et je voudrais remercier la personne que je suis devenue. À cette petite fille que j'étais, qui a toujours rêvé de briller, qui s'est fixé des objectifs et a persévéré malgré les obstacles. Merci à moi-même pour la détermination et le courage d'affronter les difficultés, qui m'ont permis d'arriver là où je suis aujourd'hui.*

À *mon côté fidèle, à celle dont les prières ont été la raison de ma réussite et la baume de mes blessures, à mon ange dans la vie,****ma maman Saadi Lila****.*

À *celui dont je porte le nom,****mon papa Sahari Mouhend ou Idir****, merci pour tout ce que tu m'as donné.*

À *mon petit frère bien-aimé* ***Sahari Yanis****, à mon petit soutien, je te souhaite prospérité et réussite dans ta vie.*

Que nulle dédicace ne puisse exprimer mes sincères sentiments, pour votre patience illimitée, votre encouragement continue, votre aide, en témoignage de mon profond amour et respect pour vos grands sacrifices.

À *ma binôme et chère amie* ***Malki Malha*** *, qui a été à mes côtés tout au long de mon cursus universitaire. Dans les moments difficiles comme dans les moments de joie. Ta patience, ton sérieux ont été des piliers sur lesquels j'ai pu m'appuyer. Merci pour ta volonté de travailler et pour ton soutien tout au long de notre recherche et réalisation de ce travail.*

À *mes chers amis* ***Cirta, Naouel, Assia, Amel, Celia, Safia, Mélissa, Lala, Zazo.***

À *tous mes amis sans exception.*

À *toute ma grande famille, à mes chères cousines* ***Hasni Nesrine*** *et* ***Hasni Hayet****.*

À *toutes les personnes qui m'aiment et que j'aime.*

…

Sahari Lina*.*

Dédicace

A*vec tout mon respect et mes sentiments de joie et de fierté, je dédie ce modeste travail :*

À *la plus belle mère* ***Zarif Jedjiga****, celle qui m'a donné la vie, ma source d'amour et de joie. Elle a toujours été là à mes côtés pour guider chacun de mes pas, sa patience et sa gentillesse n'ont pas de limites.*

À *mon très cher père,* ***Malki Hocine****, mon héros, mon exemple de force et de sagesse. Merci pour tes précieux conseils et les leçons de vie qui ont marqué mon chemin. Je suis honorée d'être ta fille.*

À *Ma chère petite sœur,* ***Malki Sabrina*** *, ma confidente et ma complice de vie, cette réussite est aussi la vôtre.*

Cette simple dédicace pour vous remercier pour tout ce que vous avez fait et continuer de faire pour moi, votre confiance et encouragement ont façonné la personne que je suis devenue. Vous êtes mon modèle de vie, je suis reconnaissante chaque jour de vous avoir comme parents, que Dieu vous protège.

À *Ma chère binôme, ma meilleure amie* ***Sahari Lina*** *, ma compagne de mon cursus universitaire qui était toujours à mes côtés dans le pire avant le bien, merci pour ta patience, ton soutien et tout ce que tu as apporté à notre travail. Je te souhaite le meilleur dans la suite de ton parcours.*

À *Mes chers amis* ***Hocine, Naouel, Cirta, Assia, Amel, Celia, Safia, Tina.***

À *Tous les membres de ma grande famille et mes chers cousins et cousines.*

. . .

Malki Malha*.*

Abstract

Computer networks have become vital resources, essential to the smooth running of businesses. However, connecting them to the Internet poses major security risks. Malicious users can exploit network and system vulnerabilities to carry out attacks with potentially serious consequences. For this reason, corporate network security is not just a necessity, but an obligation. The aim of our work is to deploy effective security solutions to protect the corporate network against these threats, while guaranteeing the three essential attributes of IT security : confidentiality, integrity and availability. To achieve this, we began by studying Algérie Télécom's initial network architecture to identify any weaknesses. We then proposed a new network architecture incorporating various security solutions. Finally, we simulated these solutions using Packet Tracer to test and ensure the proper functioning of the proposed solutions.

Keywords :IT security, Firewalls, VPN, ACLs, Computer networks, Enterprise, Attacks.

Résumé

Les réseaux informatiques sont devenus des ressources vitales et essentielles pour le bon fonctionnement des entreprises. Cependant, leur connexion à Internet présente des risques importants en termes de sécurité informatique. Les utilisateurs malintentionnés peuvent exploiter les vulnérabilités des réseaux et des systèmes pour mener des attaques dont les conséquences peuvent être graves. Pour cette raison, la sécurité d'un réseau d'entreprise n'est pas seulement une nécessité, mais une obligation. L'objectif de notre travail est de déployer des solutions de sécurité efficaces afin de protéger le réseau de l'entreprise contre ces menaces, tout en garantissant les trois attributs essentiels de la sécurité informatique, à savoir la confidentialité, l'intégrité et la disponibilité. Pour ce faire, nous avons commencé par étudier l'architecture du réseau initiale de l'entreprise Algérie Télécom afin d'identifier ses éventuelles failles. Ensuite, nous avons proposé une nouvelle architecture réseau intégrant diverses solutions de sécurité. Enfin, nous avons simulé ces solutions à l'aide de Packet Tracer pour effectuer des tests et assurer le bon fonctionnement des solutions proposées.

Les mots clés : Sécurité informatique, Pare-feu, VPN, ACLs, Réseaux informatiques, Entreprises, Attaques.

Table des matières

Table des figures

Liste des tableaux

LISTE DES ABRÉVIATIONS

AAA **A**uthentication **A**uthorization **A**ccounting
ACE **A**ccess **C**ontrol **E**ntry
ACL **A**ccess **C**ontrol **L**ist
AH **H**eader **A**utenfication
AP **A**ccess **P**oint
BNC **B**ayonet **N**eill **C**oncelman
CLNS **C**onnectioneless **N**etwork **S**ervice
CPU **C**entral **P**ocessing **U**nit
DDOS **D**istributed **D**enial **O**f **S**ervice
DHCP **D**ynamic **H**ost **C**onfiguration **P**rotocol
DMZ **Z**one **D**emilitarized
DNS **D**omain **N**ame **S**ystem
DOS **D**enial **O**f **S**ervice
ESP **E**ncapsulating **S**ecurity **P**ayload
FTP **F**ile **T**ransfer **P**rotocol
FTTH **F**ibre **T**o **T**he **H**ome
HIDS **H**ost-based IDS
HTTP **H**yper **T**text **T**ransfer
ICMP **I**nternet **C**ontrol **M**essage **P**rotocol
IDS **I**ntrusion **D**etection **S**ystem
IP **I**nternet **P**rotocol
IPS **I**ntrusion **P**revention **S**ystem
IPsec **I**nternet **P**rotocol Security
LAN **L**ocal **A**rea **N**etwork
LC **L**ucent **C**onnector
L2TP **L**ayer 2 **T**unneling **P**rotocol
LSDB **L**inK **S**tate **D**ata **B**ase
MAC **M**edia **A**ccess **C**ontrol
MAN **M**etropolitan **A**rea **N**etwork
NAT **N**etwork **A**ddress **T**ranslation
NIDS **N**etwork-based IDS

OSI **O**pen **S**ystems **I**nterconnection
PAN **P**ersonal **A**rea **N**etwork
POP **P**ost **O**ffice **P**rotocol
PPTP **P**oint To **P**oint **T**unneling **P**rotocol
QOS **Q**uality **O**f **S**evice
RFC **R**eques **F**or **C**omments
SC **S**ubscriber **C**onnector
SMTP **S**imple **M**ail **T**ransfer **P**rotocol
ST **S**traight **T**ip
STP **S**hilded **T**wisted **P**air
SSH **S**ecure **S**hell
SSL **S**ecure **S**oket **L**ayer
SVI **S**witched **V**irtual **I**nterface
TCP **T**ransmission **C**ontrol **P**rotocol
UDP **U**ser **D**atagram **P**rotocol
UPS **U**ninterruptible **P**ower **S**upply
UTP **U**nshilded **T**wisted **P**air
VLAN **V**irtual **L**ocal **A**rea **N**etwork
VOIP **V**oice **O**ver **I**nternet **P**rotocol
VPN **V**irtual **P**rivate **N**etwork
WAN **W**ide **A**rea **N**etwork
WLAN **W**ireless **L**ocal **A**rea **N**etwork

Introduction Générale

L'informatique occupe une place centrale dans la société moderne, où les réseaux informatiques sont devenus indispensables. Aujourd'hui, une multitude d'appareils sont constamment connectés, permettant aux individus, aux entreprises et aux gouvernements de partager des informations, de collaborer et de mener des activités à une échelle sans précédent. Les simples connexions locales ont évolué à grande vitesse, entrainant l'utilisation d'infrastructures interconnectées complexes mais efficace. Cela permet une communication instantanée à l'échelle nationale et mondiale. Ainsi, les réseaux informatiques ont profondément modifié les modes de communication modernes grâce à la technologie et aux ressources numériques. Ils représentent désormais l'ossature des entreprises qui investissent des sommes considérables dans le matériel et les logiciels nécessaires [1]. Cependant, l'accès à ces technologies n'est pas sans risques [18].

Les risques liés à l'utilisation d'ordinateurs et d'autres moyens d'échanges de données représentent une menace pour le bon fonctionnement des entreprises. Avec la croissance sans précédent de la connectivité, de nouveaux défis sont apparus, notamment la menace croissante des cyberattaques. Cela met en lumière l'importance cruciale de la sécurité des réseaux informatiques, particulièrement ceux des entreprises [20].

La sécurité informatique, dans une perspective globale, consiste en un ensemble de mesures visant à contrer à ces cybermenaces de plus en plus sérieuses qui peuvent compromettre les réseaux des entreprises. Conscients de l'importance cruciale des réseaux informatiques et de leur sécurité, nous sommes profondément motivés à approfondir nos connaissances dans ce domaine. C'est pourquoi nous avons choisi de le traiter dans le cadre de notre projet de fin d'études, tout en mettant l'accent sur la sécurité des réseaux d'entreprises [18].

Pour ce faire, nous avons effectué un stage au sein de l'entreprise Algérie Télécom, plus précisément au centre ERSTC de Tizi-Ouzou, une entreprise publique chargée principalement de la mise en œuvre d'initiatives de télécommunications à grande échelle à travers le pays. Le réseau informatique de cette entreprise est particulièrement exposé aux attaques informatiques. Une perturbation de son fonctionnement pourrait entraîner la défaillance totale du système de communication, causant ainsi importantes pertes financières. Cela nécessite la mise en place d'une sécurité efficace afin d'assurer son bon fonctionnement. Dans ce contexte, notre objectif est de répondre à la question suivante : Comment élaborer une politique de sécurité pour leur architecture réseau afin de réduire le risque d'incidents causés par des actes malveillants ?

Organisation du mémoire

Notre mémoire est organisé en 4 chapitres :

— **Chapitre 1 : Généralités sur les réseaux informatiques.** Ce chapitre introduit les notions fondamentales des réseaux informatiques, couvrant les principes de base et les concepts essentiels.

— **Chapitre 2 : Généralité sur la sécurité informatique.** Ce chapitre explore la sécurité informatique et ses différents aspects. Il inclut également les mesures nécessaires pour assurer la sécurité des systèmes d'information.

— **Chapitre 3 : Conception.** Ce chapitre présente l'organisme d'accueil, analyse les failles de son réseau initial et propose des solutions pour renforcer sa sécurité.

— **Chapitre 4 : Réalisation et tests.** Ce dernier chapitre est consacré à la mise en œuvre des solutions proposées dans le chapitre précédent et à leur validation à travers des tests.

Nous terminerons notre mémoire avec une conclusion générale et perspectives.

Chapitre I

Généralités sur les réseaux informatiques

Introduction

Dans ce premier chapitre, nous aborderons les concepts de base des réseaux informatiques, les caractéristiques des différents réseaux, les supports de transmission, le modèle OSI, le protocole TCP/IP ainsi que quelques notions sur l'adressage.

I.1 Fondements des Réseaux Informatiques

I.1.1 Définition des réseaux informatiques

La notion de réseau informatique désigne un ensemble de dispositifs électroniques connectés les uns aux autres, tels que les ordinateurs, les imprimantes, les serveurs, les smartphones, etc., afin de communiquer et de partager des ressources [1]. Les premières révolutions des réseaux consistaient à transporter des données informatiques, tandis que les révolutions plus récentes offrent la possibilité d'acheminer des contenus multimédia [8].

I.1.2 Historique de l'évolution des réseaux

Les réseaux informatiques ont évolué de manière progressive, passant par différentes étapes au cours des années. On peut les résumer en ces étapes clés [39] :

- **1950-1960 :** l'avènement de la micro-informatique et l'apparition des cartes réseaux.
- **1969 :** après l'introduction de la commutation de paquets, le lancement de l'ARPANET (Advanced Research Projects Agency Network).
- **1970-1980** : l'invention de l'Ethernet, suivie du développement des protocoles TCP/IP et de la création des premiers réseaux d'entreprises.
- **1990-2000 :** la Commercialisation de l'Internet et révolution des communications avec le World Wide Web.
- **2000-2010 :** l'expansion des réseaux sociaux et popularisation de la technologie Wi-Fi a eu lieu au fil des années.
- **2010-Aujourd'hui :** émergence du cloud computing, développement de l'internet des objets (IoT) et déploiement de la technologie.

Il faut noter que cette révolution technologique dans le domaine des réseaux informatiques a profondément influencé les systèmes et les différents réseaux de communications et de connectivité dans l'ère contemporaine [39].

I.1.3 Type des réseaux

On peut distinguer différents types de réseaux informatiques, regroupés en quatre catégories principales (voir la Figure I.1) [1] :

- **Réseaux PAN (Personal Area Network, IEEE 802.15) :** Les réseaux PAN sont conçus pour connecter des appareils personnels d'un seul utilisateur ou de plusieurs

utilisateurs. Ils sont également appelés réseaux individuels ou réseaux domestiques [1][8].
Les réseaux PAN se caractérisent par :

- **Une portée limitée :** Les réseaux PAN ont une portée restreinte, généralement de quelques dizaines de mètres.
- **Une connexion sans fil :** Les connexions au sein d'un réseau PAN sont généralement sans fil, en utilisant des technologies telles que le Bluetooth et le Zigbee.
- **Une faible consommation d'énergie :** Les protocoles utilisés dans ce type de réseau sont optimisés pour consommer moins d'énergie, étant donné que les appareils utilisés sont souvent alimentés par des batteries.
- **Un haut débit :** Les réseaux PAN peuvent offrir une transmission fiable et rapide des données avec des hauts débits.
- **Une interopérabilité :** Les normes de communication des réseaux PAN garantissent l'interopérabilité entre différents types d'appareils et de fabricants.

- **Réseaux LAN (local area network, IEEE 802.11) :** Les réseaux LAN sont des réseaux informatiques qui couvrent une zone limitée. À la différence des réseaux PAN, ils permettent la communication entre différents terminaux au sein d'une même zone, telle qu'une maison, un bâtiment, un campus ou une entreprise [1]. Les réseaux LAN se caractérisent par :
  - **Une portée limitée :** Les réseaux LAN ont une portée relativement courte, allant de quelques dizaines à quelques centaines de mètres.
  - **Une haute vitesse de transmission :** Ils offrent des débits de transmission élevés, permettant une communication rapide entre les appareils connectés.
  - **Topologie variée :** Les réseaux LAN peuvent adopter différentes topologies, selon les besoins spécifiques du réseau.
  - **Une administration centralisée :** Un administrateur réseau est responsable de la configuration, de la surveillance et de la maintenance du réseau.
  - **Une connectivité filaire et sans fil :** La connectivité filaire est courante dans les réseaux LAN, mais les technologies sans fil, telles que le Wifi, sont de plus en plus répandues dans ce type de réseaux pour plus de flexibilité.
  - **L'évolutivité :** Les réseaux LAN sont généralement évolutifs, permettant l'ajout d'autres équipements si nécessaire.
  - **L'accès rapide aux ressources :** : La communication au sein des réseaux LAN assure une transmission rapide des données en raison de la proximité des équipements.

- **Réseaux MAN (Metropolitan Area Network, IEEE 802.16) :** On utilise un réseau MAN afin d'interconnecter des équipements dans une zone métropolitaine. Un réseau MAN permet de relier plusieurs réseaux LAN et offre un débit élevé ainsi qu'une portée étendue sur plusieurs dizaines de kilomètres, avec une gestion centralisée.
- **Réseaux WAN (wide Area Network) :** Les réseaux WAN couvrent de vastes zones géographiques, permettent de connecter des sites distants situés à des milliers de kilomètres, engendrant des villes, des pays voir des continents. Le réseau public

Internet est le plus célèbre exemple de ce type de réseau [1].

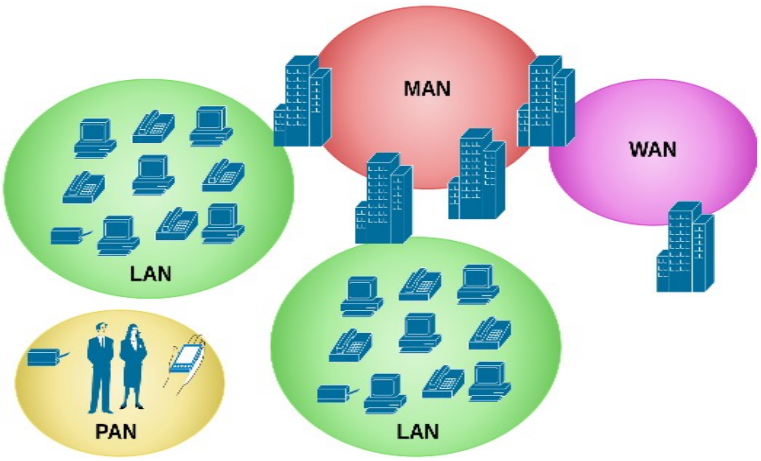


FIGURE I.1 – catégories de réseaux informatiques [6].

I.2 Composants et Topologies de Réseaux

I.2.1 Matériels d'un réseau informatique

Un réseau informatique est constitué de plusieurs périphériques qui interagissent entre eux pour la fourniture de services de haute qualité. Ces périphériques peuvent être classés comme suit :

- **Les périphériques finaux :** également appelés hôtes, sont des dispositifs qui initient une communication et fournissent des services aux utilisateurs, tels que :
  - Ordinateurs (stations de travail, ordinateurs portables, serveurs de fichiers, serveurs Web,etc.).
  - Imprimantes réseau.
  - Téléphones VoIP.
  - Caméras de surveillance.
  - Appareils portatifs (smartphones, tablettes, etc.).

- **Les périphériques réseaux :** Ils permettent l'interconnexion des équipements finaux en tant qu'intermédiaires. Parmi eux, on peut citer :

  - **Les concentrateurs (hubs) :** Il s'agit d'un équipement de niveau 1 qui relie les hôtes d'un réseau local.Lorsqu'ils reçoivent une trame, les hubs diffusent cette dernière sur l'ensemble du réseau, même aux périphériques qui ne sont pas destinataires. Ils disposent généralement de plusieurs ports (habituellement 4, 8, 16 ou 32) pour connecter diverses machines entre elles [1][8].

- **Les commutateurs (switchs) :** Sont une version plus intelligente que les hubs, équipés de nombreux ports pour relier les hôtes. Lorsqu'ils reçoivent la trame, ils la dirigent spécifiquement vers le périphérique destinataire en se basant sur l'adresse MAC de destination [1]. On distingue deux types principaux de commutateurs (switches) :
  * Commutateur de niveau 2 du modèle OSI : Il opère au sein de la couche de liaison de données.
  * Commutateur de niveau 3 : Il opère au sein de la couche réseau (niveau 3) du modèle OSI.
- **Les routeurs :** Sont des dispositifs qui permettent de relier les différents réseaux. Ils sont munis des interfaces séries (serial) pour la connexion avec d'autres routeurs et des interfaces Fast Ethernet pour la connexion aux réseaux locaux [1]. Les routeurs assurent assure le bon acheminement des paquets en utilisant leur table de routage.

I.2.2 Les supports de transmission

Dans un réseau, le support de transmission est une structure physique utilisée pour acheminer l'information d'un point à un autre. On distingue les supports limités des supports non limités [1].

I.2.2.1 Les supports limités

Ce sont des supports tangibles, comme les câbles en cuivres qui conduisent l'électricité ou les câbles à fibre optique qui conduisent de la lumière.

— **Câbles en cuivre :** les informations acheminées à l'aide de ce type de câble sont sous forme de variations d'impulsion électriques [1].Par exemple :

- **Câble coaxial :** Le câble coaxial, tel qu'illustré dans la figure I.2,est constitué d'un conducteur central en cuivre entouré d'un isolant, puis d'un deuxième conducteur sous forme de métal tressé pour le blindage. L'ensemble est ensuite enveloppé dans une gaine plastique, et est compatible avec les connecteurs BNC [1]. Ces câbles sont classés selon leur impédance caractéristique et sont spécialement conçus pour les applications sans fil, reliant les antennes aux périphériques sans fil, ainsi que pour les connexions internet via câble [1][5].

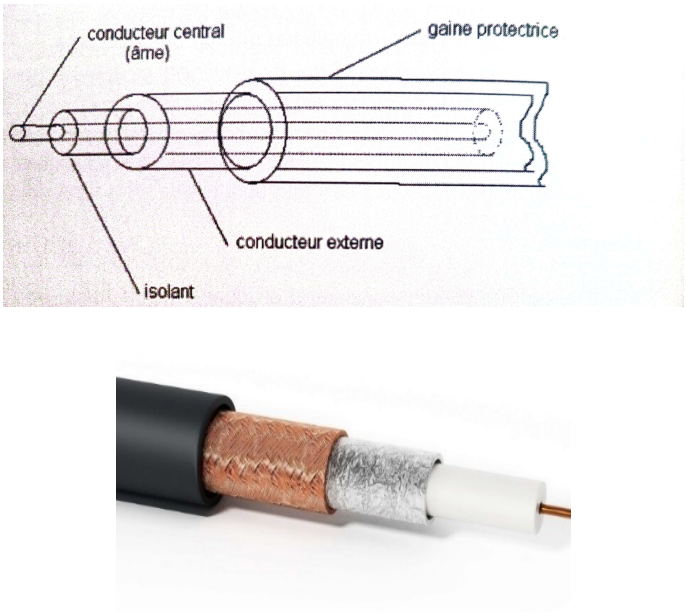


FIGURE I.2 – Câble coaxial [1][7].

- **Paire torsadée :** Une paire torsadée, dans sa forme simple, est constituée de deux brins de cuivre torsadés, chacun protégé par une enveloppe isolante, et est compatible avec les connecteurs RJ-45. On distingue deux types : la paire torsadée non blindée (UTP) et la paire torsadée blindée (STP) [1].

  - **Paire torsadée non blindée :** C'est la plus adoptée dans les réseaux locaux. La gaine externe assure la protection du fil de cuivre, des dommages physiques et les fils sont isolés électriquement par une isolation en plastique à code couleur, ce qui permet d'identifier chaque paire de fils (voir la Figure I.3) [1][2].

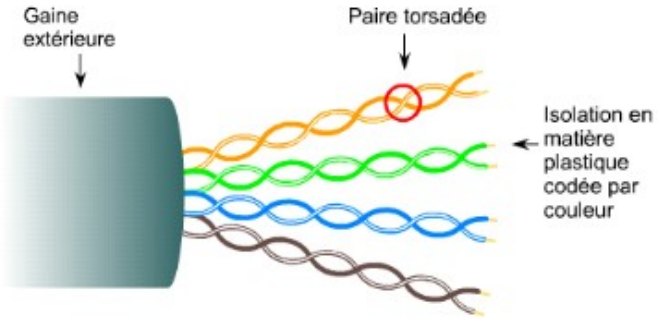


FIGURE I.3 – Paire torsadée non blindée [3].

  - **Paire torsadée blindée :** Tout comme la paire torsadée classique, elle est constituée de deux conducteurs en cuivre jointifs. Toutefois, elle inclut aussi une couche de protection métallique autour des conducteurs (voir la Figure I.4). Elle offre plus de protection que la paire torsadée non blindée et elle est plus chère et difficile à installer [2].

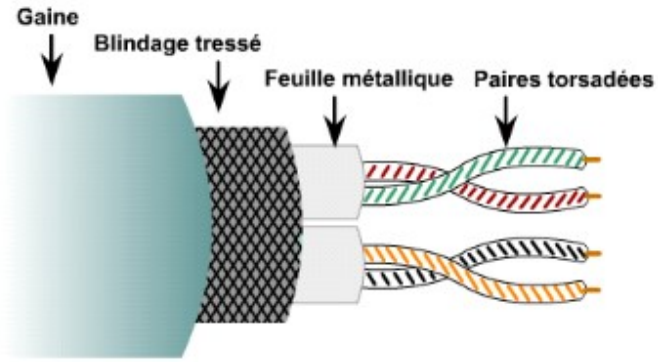


FIGURE I.4 – Paire torsadée blindée [3].

— **Câble à fibre optique :** Le câble à fibre optique est composé d'une fibre conductrice de lumière extrêmement fine (voir la Figure I.5), il transmet des données numériques sous forme des impulsions lumineuses modulées, et est compatible avec les connecteurs SC, LC, ST [1][2].

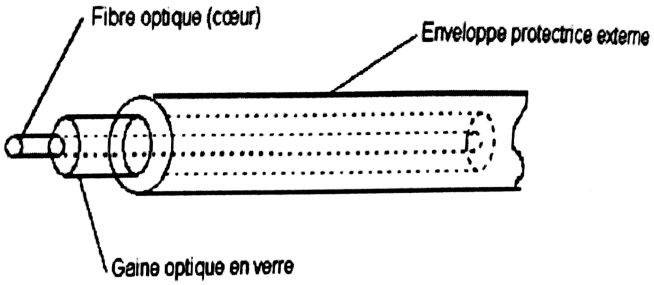


FIGURE I.5 – Fibre optique [1].

I.2.2.2 Les supports non limités

Ce sont des ondes hyperfréquences telles que l'infrarouge et les ondes radio qui sont utilisées par la technologie des réseaux sans fil et mobiles [1] [2]. Les technologies de communication de données sans fil ont également leurs limites en termes de :

- **Zone de couverture :** Bien que les supports non limités soient efficaces dans les environnements ouverts, la couverture réelle est souvent restreinte par certains matériaux de construction utilisés dans les bâtiments et structures, ainsi que par le terrain local.
- **Interférences :** La transmission sans fil est sensible aux interférences, ce qui peut perturber la communication [2].

- **Sécurité :** Contrairement à la connexion physique à un point d'accès, l'accès à un réseau sans fil ne requiert pas de connexion physique, cela permet aux périphériques et aux utilisateurs non autorisés de se connecter au réseau. Il est donc crucial de garantir la sécurité du réseau lors de la gestion des réseaux sans fil.

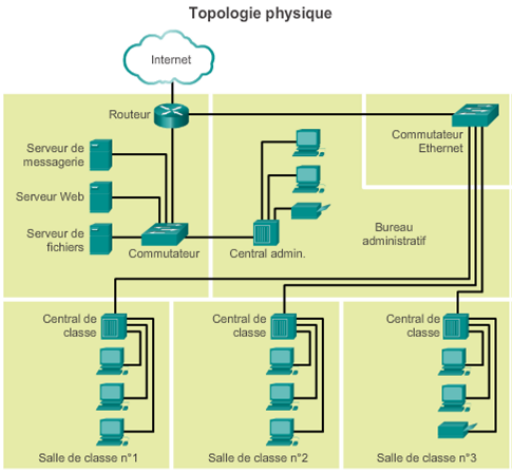
Le choix des supports de transmission se fait selon plusieurs critères, notamment [8] :

- La distance à couvrir.
- L'environnement dans lequel le support sera utilisé.
- La quantité d'information et la vitesse de transmission.
- Le coût du support et de son installation.

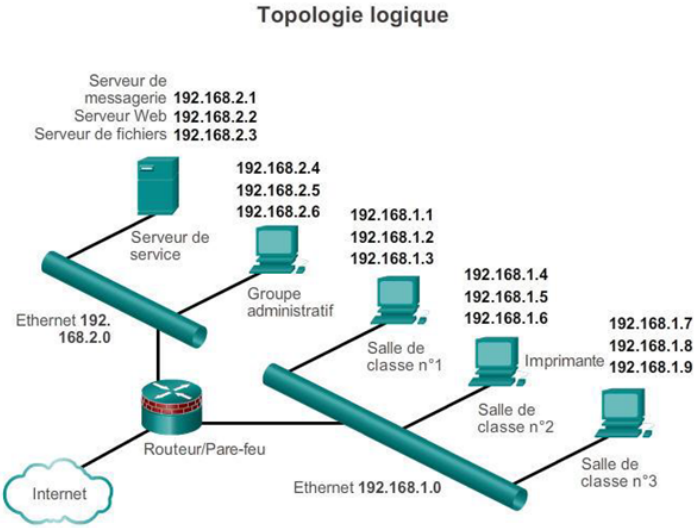
I.2.3 Topologies réseau

I.2.3.1 Diagrammes de topologie

Comme le montre la Figure I.6, Un réseau est caractérisé par un diagramme topologique, physiques et logiques. Le diagramme logique illustre le schéma d'adressage IP, les périphériques et les ports et le diagramme physique décrit la structure physique de réseau [8].



(a) Diagramme de topologie physique [8].



(b) Diagramme de topologie logique [8].

FIGURE I.6 – Diagrammes topologiques.

I.2.3.2 types de topologie

Cette classification est établie en fonction de la manière dont les équipements sont interconnectés :

- **Topologie en étoile :** Les équipements sont reliés à un nœud central (contrôleur) qui renvoie les données reçues par les différents équipements de réseau à leurs destinations (voir la Figure I.7).

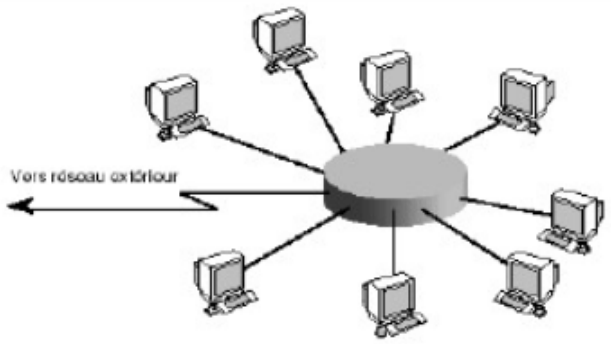


FIGURE I.7 – Topologie en étoile [17].

- **Avantages**

  Résilience aux pannes.

  Facilité de modification des équipements (ajout ou suppression).

- **Inconvénients**

  Coût plus élevé.

  Une panne du nœud central entraîne l'arrêt du réseau.

  Plus de câbles.

- **Topologie en bus :** La communication dans ce type de réseau est réalisée à travers un seul support de transmission appelé « bus », qui est partagé par tous les utilisateurs (voir la Figure I.8).

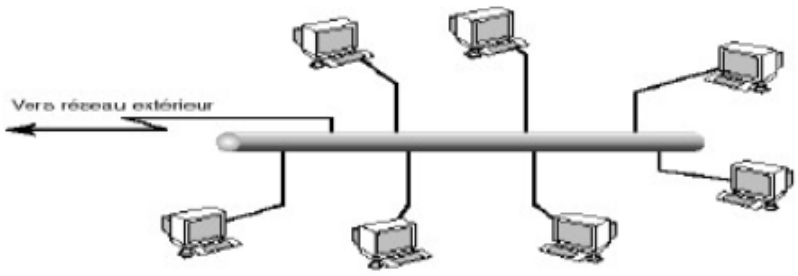


FIGURE I.8 – Topologie en bus [17].

- **Avantages**

  Peu coûteux.

  Facile à mettre en place et à étendre

  Moins de câbles.

- **Inconvénients**

  Limites en termes de longueur du câble et de nombre de stations.

  Bande passante partagée.

  Panne du bus entraînant une interruption du réseau.

- **Topologie en anneau :** Chaque poste est lié au nœud suivant formant ainsi une boucle. La communication est unidirectionnelle, chaque station transmettant à tour de rôle (voir la Figure I.9).

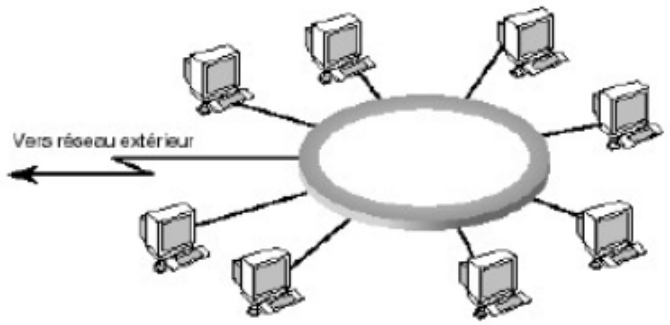


FIGURE I.9 – Topologie en anneau [17].

- **Avantages**
  - Utilisation efficace de la bande passante.
  - Absence de collisions
- **Inconvénients**
  - Risque élevé de blocage du réseau en cas de panne.
  - Complexité de mise en œuvre et de maintenance.

- **Topologie en arbre :** Aussi appelée topologie hiérarchique, elle est structurée en niveaux, formant une arborescence comme illustré dans la Figure I.10).

FIGURE I.10 – Topologie en arbre[17].

- **Avantages**
  - — Idéale pour les grands réseaux.
  - — Possibilité de connexion point à point.
  - — Extensibilité du réseau.
- — **Inconvénients**
  - — Gestion et maintenance complexes.
  - — Performance limitée en cas de grand nombre de nœuds.

- **Topologie maillée :** Toutes les stations de cette topologie peuvent établir une connexion point à point entre elles (voir la Figure I.11).

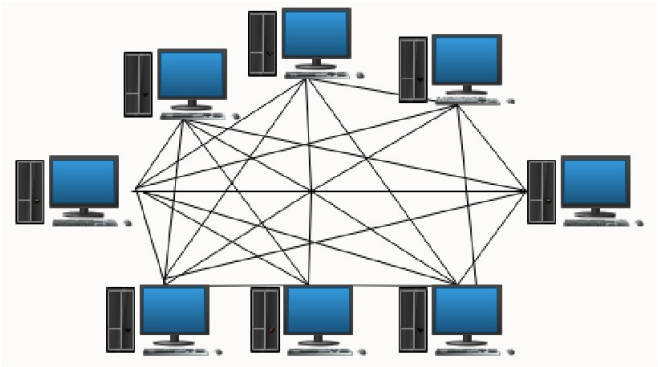


FIGURE I.11 – Topologie maillée [17].

- **Avantages**
  - — Hautes performances et fiabilité.
  - — Tolérance aux pannes.
- **Inconvénients**
  - — Coût élevé de l'installation.
  - — Gestion et maintenance complexes.

I.3 Les modèles réseaux et les protocoles utilisés

I.3.1 Les modèles réseaux

Les systèmes informatiques nécessitent une base de transmission standardisée pour garantir les fonctionnalités requises pour la communication. C'est pour répondre à ce besoin que les modèles de référence OSI (Open Systems Interconnection) et TCP/IP ont été développés [1].

I.3.1.1 Le modèle OSI

Le modèle OSI définit la manière dont les terminaux et les appareils d'un réseau doivent communiquer. Créé dans les années 1980, ce modèle est divisé en sept couches [6] [1] [8].

- **Couche application :** Cette couche est le point de contact entre l'utilisateur et le réseau, elle fournit aux utilisateurs les services de base offerts par le réseau aux utilisateurs.

- **Couche de présentation :** Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises. Elle traite les informations de manière à les rendre compatibles Entre les applications de communication, assurant ainsi l'indépendance entre les utilisateurs et la transmission des données.

- **Couche session :** Cette couche gère l'organisation des échanges en permettant l'ouverture et la fermeture de sessions entre les machines (utilisateurs).

- **Couche transport :** Cette couche assure le contrôle du transfert d'informations de bout en bout entre les deux extrémités. Elle corrige les erreurs qui pourraient survenir et garantit que les messages sont livrés dans le bon ordre.

- **Couche réseau :** Cette couche permet le routage des paquets sur le réseau entre les appareils finaux. Elle facilite également l'interconnexion des réseaux entre eux.

- **Couche liaison de données :** Cette couche a pour objectif de faciliter l'échange de données entre les nœuds sur un support commun, En se basant sur les adresses MAC. Elle assure l'envoi des données vers la destination appropriée.

- **Couche physique :**Cette couche est chargée de transmettre les bits directement sur le canal de transmission sans effectuer de traitement supplémentaire.

I.3.1.2 Le modèle TCP/IP

Il s'agit d'une version simplifiée du modèle OSI, basée sur quatre couches, comme illustré dans la la FigureI.12.

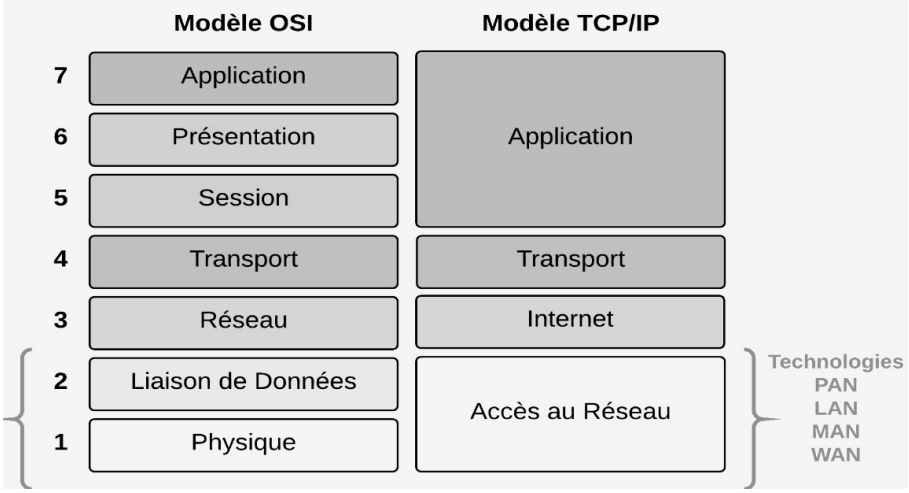


FIGURE I.12 – Modèle OSI vs TCP/IP [6].

I.3.2 Les protocoles utilisés

I.3.2.1 Définition d'un protocole

Dans le domaine des réseaux informatiques, un protocole représente un ensemble de règles et de conventions dictant comment les données circulent entre les différents nœuds d'un réseau. Il spécifie le format, l'ordre et la vérification des messages échangés, ainsi que les procédures à suivre en cas d'erreurs ou de conflits [1]. Les protocoles assurent une communication fiable et cohérente entre les appareils connectés en s'assurant que les données sont transmises et reçues correctement et de manière sécurisée. Ils sont fondamentaux pour le fonctionnement des réseaux informatiques en garantissant l'interopérabilité entre les équipements et systèmes variés [1].

Il est important de noter que chaque couche des modèles réseau possède ses propres protocoles spécifiques (voir la Figure I.13) [1] [8].

- **Couche applications**
  - HTTP (Hypertext Transfer Protocol) : Utilisé pour consulter des pages web.
  - FTP (File Transfert Protocol) : Permet le transfert de fichiers.
  - SMTP (Simple Mail Transfert Protocol) : Utilisé pour l'envoi de courriels.
  - POP (Post Office Protocol) : Utilisé pour la réception de couriels.
  - DNS (Domain Name System) : Assure la correspondance entre noms de domaine et adresses IP.
  - SSH (Secure Shell) : Permet une connexion à distance sécurisée.
  - DHCP (Dynamic Host Configuration Protocol) : Permet l'attribution dynamique des configurations IP.

- **Couche transport**

— TCP (Transport Control Protocol) : Protocole orienté connexion, assurant la fiabilité de la transmission avec accusé de réception.
— UDP (User Datagram Protocol) : Protocole non orienté connexion, sans garantie de réception des données.

- **Couche réseau**

— IP (Internet Protocol) : Standard de communication incluant l'adressage et le contrôle des paquets pour guider ces derniers à travers un réseau. IPv4 attribue des adresses uniques à chaque appareil, tandis que IPv6 élargit l'espace d'adressage pour répondre à la pénurie d'adresses IPv4 en passant de 32 à 128 bits.

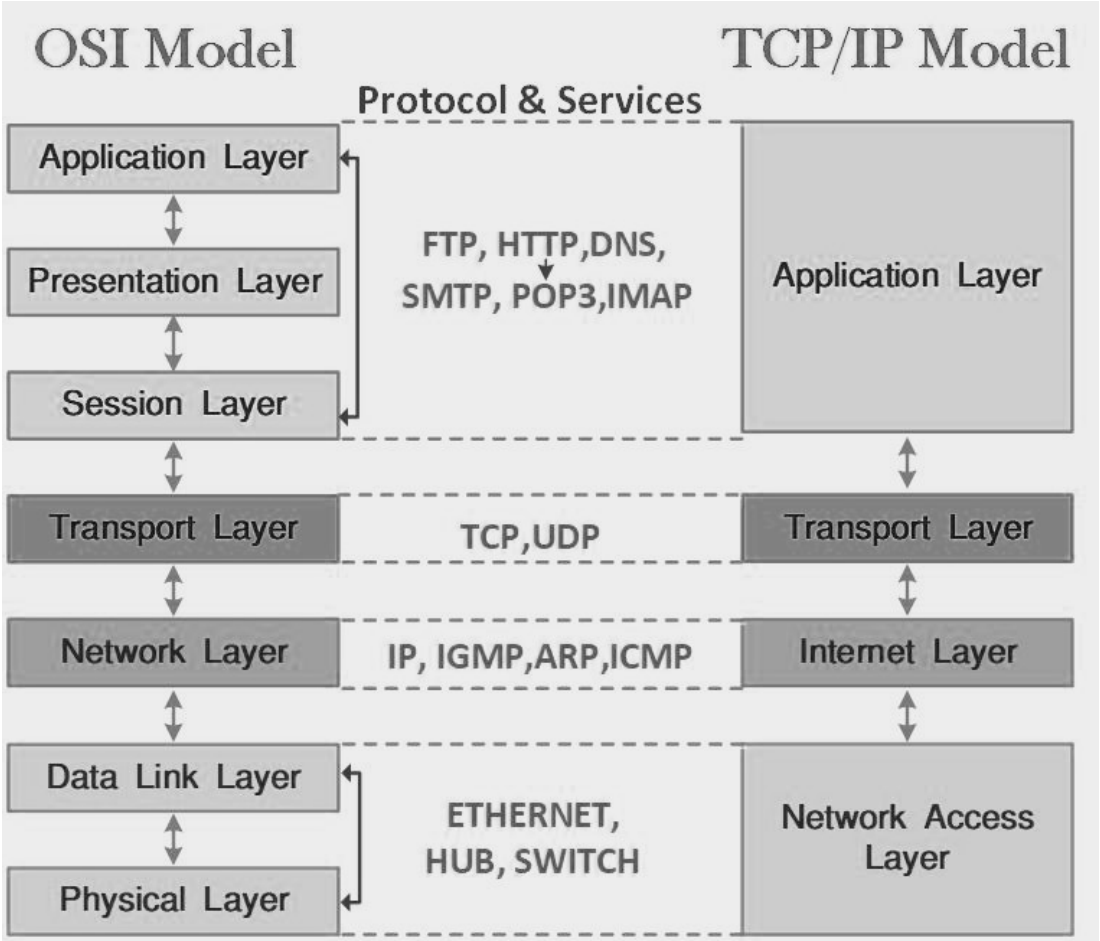


FIGURE I.13 – Protocoles des différentes couches [6].

I.4 Adressage

I.4.1 Adresse physique (MAC)

Au sein de la couche liaison de données, les nœuds établissent la communication en utilisant une adresse correspondant à l'adresse de la carte réseau, également appelée adresse physique ou adresse MAC (Media Access Control). Cette adresse est définie par l'IEEE sur 16 ou 48 bits, le format le plus courant étant sur 48 bits. Les premiers 24 bits représentent le fabricant de la carte, tandis que les 24 bits suivants correspondent au code de série spécifique à la carte. De cette manière, chaque carte possède une adresse physique unique dans le monde [9] [13].

I.4.2 Adresse logique (IP)

Dans le contexte d'internet, le système d'adressage repose sur des identifiants logiques appelés adresses IP. Chaque appareil est assigné à un nom symbolique qui se traduit par une adresse IP. Cette adresse est constituée de deux composants : l'identifiant du réseau où se situe l'appareil et l'identifiant spécifique de l'appareil. En totalité, l'adresse IP est une séquence de 32 bits, équivalant à 4 octets séparés par des points. Chaque octet est représenté par un chiffre décimal variant de 0 à 255 [13].

IPv4 : également connu sous le nom de protocole Internet version 4, utilise des adresses de 32 bits, composées de 4 groupes de 8 bits. Initialement considérées comme adéquates, ces adresses ont permis l'envoi de paquets par des chemins alternatifs en cas de problème réseau. Cependant, avec l'expansion rapide d'Internet, le nombre d'adresses disponibles est devenu insuffisant. IPv4 a rapidement atteint ses limites en termes de capacité à répondre à la demande croissante [10][11].

IPv6 : Est la nouvelle version d'IP, également appelée Protocole Internet nouvelle génération (IPng). Utilise des adresses de 128 bits mêlant chiffres et lettres. Formatées en huit groupes hexadécimaux à quatre chiffres, séparés par des deux-points. Élimine le besoin de traduction d'adresses du réseau (NAT), rétablissant la connectivité de bout en bout, facilite la mise en œuvre et le déploiement de services tels que la voix sur IP (VoIP) et la qualité de service (QoS) [10][11].

I.4.3 Adresses particulières

I.4.3.1 Adresse réseau

C'est un identifiant dédié à la représentation d'un réseau particulier, caractérisé par une partie « host id » contenant que des zéros. La validation de l'appartenance d'un périphérique a ce réseau est déterminé par trois critères spécifiques [9] [15] :

— Il partage un masque de sous-réseau identique à celui de l'adresse réseau.

— Ses bits réseau concordent avec ceux de l'adresse réseau, suivant le masque de sous-réseau.

— Il se trouve dans le même réseau de diffusion que les appareils ayant la même adresse de diffusion.

L'adresse réseau d'un hôte est calculée en combinant son adresse IPv4 avec le masque de sous-réseau par une opération AND.

I.4.3.2 Adresse de l'hôte

Les adresses hôtes sont des identifiants attribués à un dispositif. Les bits de la section hôte sont définis comme zéro dans le masque de sous-réseau. Ils peuvent prendre diverses combinaisons de bits dans leurs sections hôte, à l'exception où tous les bits sont égaux à 0 (ce qui représente une adresse réseau) ou tous les bits sont égaux à 1 (ce qui représente une adresse de diffusion) [9] [15].

I.4.3.3 Adresse de diffusion

Une adresse de diffusion est utilisée pour communiquer avec tous les appareils du réseau IPv4 lorsque la partie hot id est composée uniquement de bits à "1" [9] [15].

I.5 Les sous-réseaux

En intégrant des sous-réseaux dans un réseau plus vaste, le trafic peut parcourir des distances plus courtes sans passer par des routeurs inutiles. Cela réduit également l'utilisation des adresses IP en les attribuant à des appareils spécifiques, simplifiant ainsi la gestion du réseau pour [9][14] :

— Prévenir la perte d'adresses dans les nœuds d'un réseau.

— Réduire la congestion du réseau.

— Renforcer la sécurité.

Les adresses IP seules ne suffisent pas à déterminer à quel sous-réseau un paquet IP doit être envoyé, car elles ne spécifient que l'adresse du réseau et de l'appareil. Les routeurs utilisent un masque de sous-réseau pour classer les données en sous-réseaux au sein d'un réseau.

I.5.1 Masque de sous réseau

Le masque de sous-réseau fonctionne de manière similaire à une adresse IP, mais il est utilisé exclusivement au sein d'un réseau. Il divise partiellement l'adresse IP en deux parties : la partie réseau, identifiant le réseau spécifique, et la partie hôte, identifiant un dispositif unique dans notre réseau. Ce masque indique le nombre de bits de l'adresse IP utilisés pour l'adresse réseau et les sous-réseaux en utilisant des bits à 1. Les bits à 0 du masque correspondent aux bits de l'adresse IP indiquant l'hôte [16].

I.6 Le NAT (Network Address Translation)

Il s'agit d'une méthode qui permet de substituer l'adresse IP privée d'origine d'une machine par l'adresse IP publique du routeur dans un paquet réseau lorsqu'une machine cherche à communiquer avec un serveur situé sur Internet en utilisant une seule adresse IP publique. Et pour mieux comprendre comment il influe sur la connectivité des réseaux, explorons de plus près les divers types de NAT [12] :

— NAT statique : Le NAT statique a pour but de convertir une adresse IP privée en une adresse IP publique, en utilisant une association statique, c'est-à-dire un pour un. En d'autres termes, une adresse IP personnelle est liée à une adresse IP publique, ce qui est particulièrement bénéfique pour les serveurs Web ou les périphériques qui nécessitent des adresses statiques accessibles depuis Internet [12].

— NAT dynamique : Le NAT dynamique diffère du NAT statique par la dynamique et la temporisation des associations entre une adresse IP privée correspondante à une machine et une adresse IP publique disponible sur le routeur. Cela se fait en utilisant un pool d'adresses IP publiques qui permet de partager un ensemble restreint d'adresses IP publiques [12].

Conclusion

En conclusion, cette exploration des généralités sur les réseaux informatiques a mis en lumière leur importance fondamentale dans notre monde interconnecté. En comprenant les composants essentiels, les différents types de réseaux et les technologies émergentes, nous avons acquis une compréhension plus approfondie de l'interconnexion et de la puissance des réseaux informatiques. Cette compréhension fournit une base solide pour explorer des domaines plus spécialisés, tels que la sécurité des réseaux, qui sera détaillée dans le deuxième chapitre.

Chapitre II

Généralités sur la sécurité informatique

Introduction

Dans ce chapitre, nous commencerons par définir quelques concepts essentiels de la sécurité informatique. Ensuite, nous aborderons les thèmes des vulnérabilités, des risques, des attaques informatiques, les services de sécurités disponibles, ainsi que des mécanismes de sécurité.

II.1 Définitions

- **Sécurité informatique :** Il s'agit de l'ensemble de moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place afin de protéger le système informatique et de réduire la vulnérabilité de celui-ci contre les menaces accidentelles ou intentionnelles [18].
- **Sécurité réseau :** La sécurité réseau englobe les techniques de sécurité informatique visant à protéger un réseau informatique.
- **Sécurité de transmission :** Elle englobe les techniques de sécurité informatique visant à protéger les données transmises entre différents réseaux informatiques.

II.2 Les attributs de la sécurité

La sûreté de fonctionnement réfère à la capacité d'un système informatique à fonctionner de manière fiable, sûre et conforme à ses spécifications dans des conditions normales ou dans les situations de doutes. Elle peut être évaluée en se basant sur différentes propriétés complémentaires qui permettent de définir ses attributs principaux qui sont [19] :

- **Confidentialité :** La confidentialité vise à garantir que l'information ne soit accessible qu'aux personnes autorisées.
- **Intégrité :** L'intégrité vise à garantir que l'information ne soit ni altérée ni détruite, que ce soit par soit par accident ou par malveillance.
- **Disponibilité :** La disponibilité garantit que l'information soit Accessible et utilisable à la demande. Ce qui signifie que le système sera prêt à délivrer son service dès qu'il est nécessaire.

L'association de ces trois attributs principaux conduit à la sécurité d'un système informatique. Outre ces trois attributs, la sécurité possède des attributs dits secondaires qui sont :

- **Authentification :** L'authentification garantit la vérification de l'identité des entités qui souhaitent manipuler l'information. Ce qui permet de confirmer leur authenticité.
- **Non-répudiation :** La non-répudiation se réfère à l'impossibilité de nier avoir réalisé une action une fois celle-ci effectuée. Cette notion peut être associée à des aspects tels que :
  - L'imputabilité consiste à attribuer une action (un événement) à une entité spécifique (telle que des ressources ou des individus).

— La traçabilité offre la possibilité de conserver une trace numérique de toute action.
— L'audibilité est définie comme l'aptitude d'un système à garantir la disponibilité des informations essentielles à l'analyse future de tout événement.Cette analyse peut être un contrôle régulier ou une procédure d'audit exceptionnelle [18].

II.3 Les terminologies de la sécurité informatique

II.3.1 Les vulnérabilités

Une vulnérabilité est une faille, un bug ou une brèche pouvant être exploitée pour obtenir un accès illicite à une ressource d'information ou à des privilèges supérieurs à ceux normalement accordés pour cette ressource. On peut donc la considérer comme un indicateur de la faiblesse du système. Elle caractérise les composants du système (matériel, logiciel, les règles, les procédures, les personnels) susceptibles d'être attaqués avec succès. [18] [34].

II.3.2 Les menaces

Une menace est une éventuelle cause d'incident pouvant entraîner des dommages au système ou à l'organisation.

II.3.2.1 Les types de menaces

On peut citer deux types de menaces :

- **Les menaces accidentelles :** Elles sont catégorisées comme des risques qui surviennent de manière accidentelle sans intention préalable.
- **Les menaces intentionnelles :** Elles sont considérées comme des attaques effectuées par un individu afin de mettre en péril la sécurité informatique et accéder aux ressources sans autorisation, on peut les classer en deux catégories :
  a- **Menaces passives :** On les nomme menace passive parce que même si elles se concrétisent, ne modifient pas les informations du système et n'altèrent son fonctionnement ou son état, elles servent à collecter des informations généralement sensibles (confidentielle) d'une manière discrète. Leur détection est difficile, car elles n'affectent pas les opérations normales du système. Par exemple, l'espionnage des données transmises sur un réseau, sans altérer les communications, illustre bien une menace passive [19].
  b- **Menaces actives :** Les menaces actives, ou attaques contre un système, impliquent la manipulation des informations ainsi que des changements dans l'état ou le fonctionnement du système.Contrairement aux menaces passives, elles sont plus faciles à détecter en raison des dommages qu'elles peuvent causer, pour cela les spécialistes en réseaux mettent en place des mesures de précaution adéquates [35].

II.3.3 Les attaques

Une attaque consiste à exploiter des failles d'un système informatique ou d'un réseau informatique pour avoir un accès illicite. Les spécialistes du domaine disent que « le but d'un audit de sécurité est de se mettre dans la peau de l'attaquant. Apprendre l'attaque pour mieux se défendre » [36].

D'après cette citation, pour avoir une bonne politique de sécurité, il faut d'abord connaître tout ce qui est nécessaire sur l'attaque.

II.3.3.1 Types de hackers

Quand on parle d'une attaque, cela nous fait penser à l'attaquant, qui est souvent connu sous le nom de "hacker" ou "pirate". Ce terme a pris plusieurs significations depuis son apparition à la fin des années 50. De nos jours, ce mot est souvent utilisé pour désigner toute personne s'introduisant dans les systèmes informatiques [36] [25]. Les hackers sont catégorisés selon leur expérience et leurs motivations. On peut citer :

- **Black hat hackers :** En français, les hackers au chapeau noir. Ce type de hacker, souvent désigné comme "hacker malveillant", se révolte contre le système informatique, frôle les limites de la loi ou les dépasse carrément. Généralement, ils s'introduisent dans les systèmes dans un but nuisible. Leur intérêt est souvent personnel ou financier, et ils sont considérés comme des méchants [36].
- **Grey hat hackers :** Les hackers au chapeau gris sont un peu un hybride de hackers au chapeau noir et au chapeau blanc. Ils sont compétents et possèdent des connaissances approfondies en sécurité informatique. Ces hackers explorent souvent les systèmes sans autorisation, mais leurs intentions ne sont pas toujours malveillantes. Ils peuvent révéler des vulnérabilités pour obtenir une reconnaissance ou pour inciter les propriétaires des systèmes à les corriger, mais ils peuvent aussi franchir les limites de l'éthique [25].
- **White hat hackers :** Les hackers au chapeau blanc (éthiques), également appelés "gentils", ont pour but d'améliorer les systèmes et technologies informatiques. Ils explorent ces systèmes pour découvrir de nouvelles vulnérabilités non connues ou non publiées, afin de les signaler et de permettre leur correction. En rendant publiques ces vulnérabilités de manière responsable, ils contribuent à renforcer la sécurité informatique globale [36].
- **Scripts kiddies :** Généralement, les "script kiddies" sont des adolescents qui pénètrent par effraction dans un système après avoir acquis quelques notions de sécurité. Ils n'ont pas de réelles connaissances sur l'éthique d'un hacker. Ils réutilisent des codes et des programmes déjà utilisés et publiés, généralement par les hackers au chapeau blanc, sans comprendre les enjeux ou les risques associés. Les script kiddies ne créent pas leurs propres outils, mais se contentent d'utiliser ceux développés par d'autres, souvent sans en comprendre le fonctionnement profond. Leur motivation est souvent la curiosité, l'envie de s'amuser, ou le désir de se vanter auprès de leurs pairs, plutôt qu'un objectif malveillant ou criminel [25] [36].

II.3.3.2 Phases d'une attaque

Les pirates suivent un ensemble d'étapes pour s'introduire dans un réseau, comme le montre la Figure II.1.

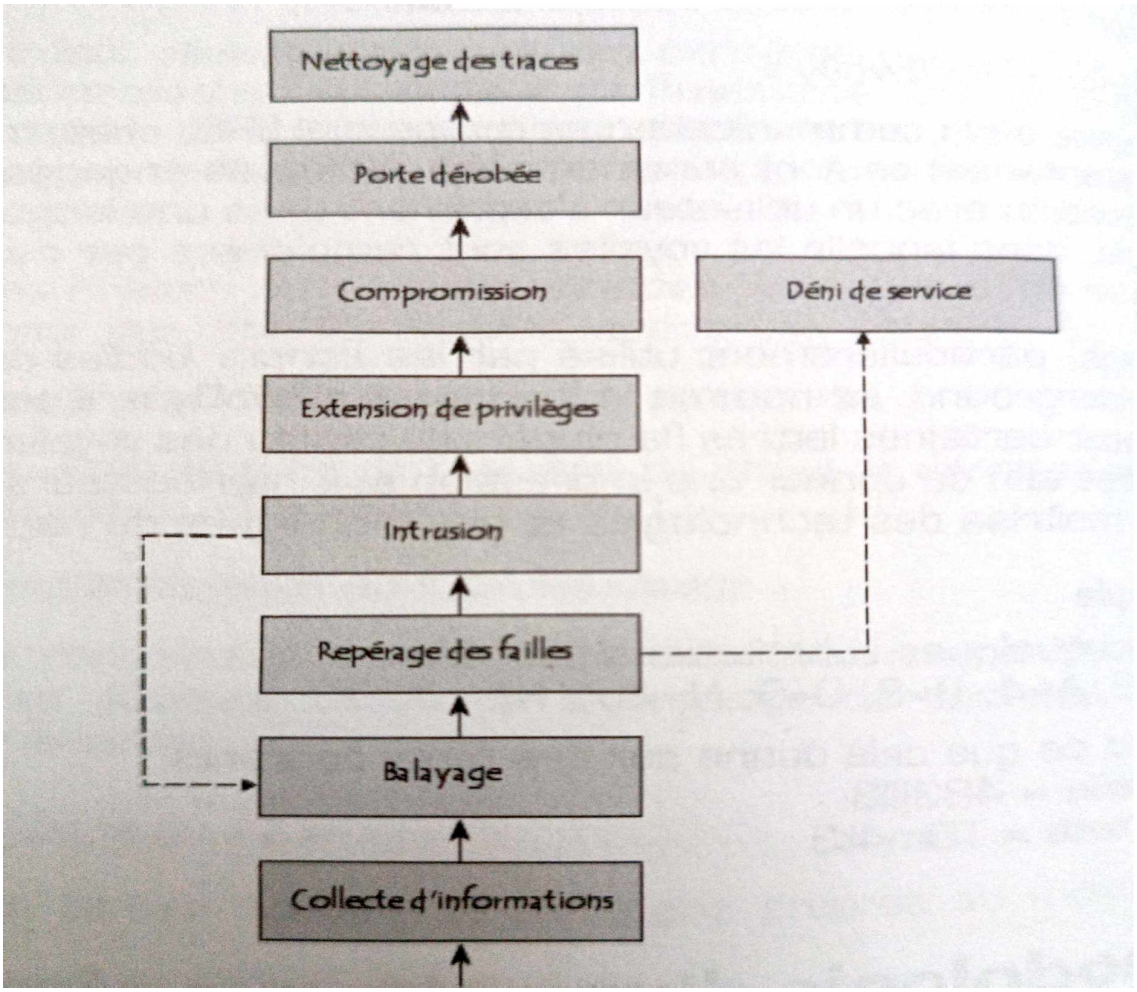


FIGURE II.1 – Les phases d'une attaque [25].

- **Collecte d'informations :** C'est la phase essentielle d'une attaque. À ce stade, l'attaquant essaye d'obtenir le maximum d'informations sur l'infrastructure de communication du réseau cible, comme :
  - — Adresse IP.
  - — Nom de domaine.
  - — Protocoles réseau.
  - — Services activés.
  - — Architecture des serveurs,etc.
- **Balayage du réseau :** Le pirate, après avoir acquis des connaissances sur la topologie du réseau, aura la possibilité de scanner le réseau à l'aide d'un logiciel qui lui permet de connaître les adresses IP actives et les ports ouverts correspondant aux services accessibles, ainsi que les systèmes d'exploitation utilisés par les serveurs [25].
- **Repérage des failles :** Lorsque l'attaquant arrive à cette étape, il dispose déjà des informations nécessaires sur le réseau, côté logiciel et matériel. Il détermine alors les failles existantes au sein du réseau cible [25].

- **Intrusion :** Dans cette étape, le pirate essaye d'accéder à des comptes valides sur les machines et utilise plusieurs méthodes pour ce faire, comme l'ingénierie sociale, les attaques par force brute, etc [25].
- **Exploit :** L'exploit représente un programme informatique conçu pour exploiter une vulnérabilité. Son objectif est de permettre à l'attaquant de tirer parti de cette vulnérabilité pour obtenir des privilèges non autorisés ou provoquer des erreurs système [25].
- **Extension des privilèges :** L'attaquant, après avoir obtenu plusieurs accès au réseau en se connectant à un ou plusieurs comptes peu protégés, va essayer d'augmenter ses privilèges (super utilisateur/super administrateur) [25].
- **Compromission :** Grâce aux phases précédentes, l'attaquant disposera d'une carte détaillée du réseau, ce qui lui permettra d'étendre encore son action en exploitant les relations de confiance existante entre les différentes machines.
- **Nettoyage des traces :** À ce stade, le hacker a atteint un niveau de maîtrise suffisant du réseau. D'abord, il va laisser une porte dérobée pour lui permettre d'accéder facilement au réseau une autre fois. Ensuite, il va supprimer tous les fichiers prouvant son accès, comme les journaux d'activités et les fichiers créés, ce qui signifie la suppression des lignes d'activités concernant ses actions [25].

II.3.3.3 Techniques d'attaque

Chaque attaque peut être classée dans un groupe spécifique en fonction de son objectif et de sa méthode :

a- **Attaques d'accès :** Les attaques d'accès visant la confidentialité consistent à écouter le réseau pour obtenir des informations sensibles.

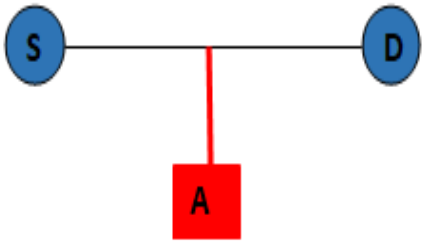


FIGURE II.2 – Attaques d'accès.

- **Ingénierie sociale :** L'attaquant établit des relations avec le personnel pour obtenir des informations sur le système informatique en général. Ce type d'attaque utilise fréquemment les réseaux sociaux pour obtenir des noms d'utilisateur et des mots de passe. En se faisant passer pour des collègues, des supérieurs ou des amis, les attaquants peuvent manipuler les employés pour qu'ils divulguent des informations sensibles, des identifiants d'accès ou des informations confidentielles sur l'entreprise [36] [25]. L'attaquant attire la victime

avec des courriels, des messages texte, des offres d'emploi alléchantes, des promotions spéciales ou d'autres appâts attrayants, incitant ainsi la victime à fournir involontairement des informations ou à cliquer sur des liens malveillants.

- **Porte Dérobée :** Une fois que l'attaquant a réussi à accéder à un réseau, il laisse souvent une porte dérobée pour faciliter un accès ultérieur. Cette porte dérobée peut prendre la forme d'un code malveillant injecté dans le système cible, permettant à l'attaquant de l'exploiter à volonté. De plus, l'attaquant peut également modifier les règles du pare-feu pour contourner les mesures de sécurité et maintenir l'accès non autorisé au réseau.
- **Sniffing :** L'attaquant se met à l'écoute sur le réseau pour obtenir des informations en utilisant un renifleur de paquets tel que "Wireshark". Ce type d'outil lui permet d'intercepter et d'analyser le trafic réseau, lui donnant ainsi accès à des données sensibles telles que les identifiants de connexion, les communications non chiffrées et d'autres informations confidentielles échangées entre les périphériques du réseau.

b- **Attaques de modification :** Les attaques de modification visent à compromettre l'intégrité du système. L'objectif de ce type d'attaque est d'altérer le système ou les données de manière non autorisée.

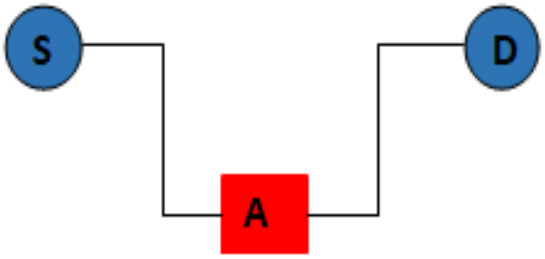


FIGURE II.3 – Attaques de modification.

- **Virus :** Un virus informatique est un programme caché dans un autre, qui peut s'exécuter et se reproduire en infectant d'autres ordinateurs. Lors de l'ouverture d'un fichier infecté, le virus se propage en insérant des copies de lui-même dans d'autres programmes ou fichiers, ce qui provoque des dommages sur le système, comme la corruption des données ou la prise de contrôle totale du système [25] [37].
- **Vers :** On le trouve aussi sous le nom de 'ver réseau'. Il se reproduit et se déplace de manière autonome grâce à ses propres mécanismes. Contrairement aux virus, les vers n'ont pas besoin de se cacher dans d'autres programmes pour s'exécuter. En exploitant les vulnérabilités des réseaux, ils se propagent rapidement d'un ordinateur à l'autre, sans intervention humaine [36].
- **Cheval de troie :** c'est Un code nuisible placé dans un programme apparemment sain, accomplissant une fonction illicite tout en donnant l'apparence d'une fonction légitime. L'appellation de cette attaque provient de la légende de l'Odyssée d'Homère, où les Grecs ont introduit un énorme cheval de bois dans la cité de Troie, cachant ainsi les soldats à l'intérieur [37] [25].

- **Bombe logique :** Une bombe logique est un programme malveillant qui se déclenche à une date ou un instant précis, capable de s'activer simultanément sur un grand nombre de machines.

1. **Attaques par saturation :** Cette forme d'attaque, axée sur la disponibilité, implique l'envoi massif de fichiers depuis une machine dans le but de saturer le système, connue sous le nom de DoS (Déni de Service), ou bien à partir de plusieurs machines, appelée DDoS (Déni de Service Distribué).

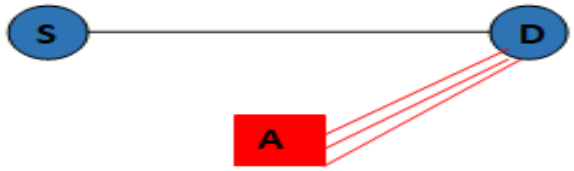


FIGURE II.4 – Attaques par saturation.

- **Ping of death :** Le 'ping de la mort' consiste à envoyer des paquets ICMP mal formés ou surdimensionnés dans le but de provoquer un dysfonctionnement du système cible.
- **Flooding :** Consiste à envoyer de nombreux paquets TCP SYN à la machine cible en utilisant une fausse adresse de retour pour ne pas recevoir d'ACK de la part de la cible. La machine cible met les demandes dans une file d'attente en attendant l'ACK jusqu'à ce que la file soit saturée.
- **smurf :** C'est une technique dite "attaque par réflexion". Elle est basée sur l'utilisation d'un serveur broadcast capable de dupliquer un message et de l'envoyer à toutes les machines du réseau. L'attaquant, en falsifiant l'adresse IP source (adresse à laquelle le serveur doit théoriquement répondre), envoie une requête ping à un ou plusieurs serveurs broadcast, puis dirige plusieurs réponses vers la machine cible [36].

2. **Attaques par Répudiation :** Les attaques visant la non-répudiation, où l'attaquant ne laisse aucune trace de son attaque en passant par d'autres machines.

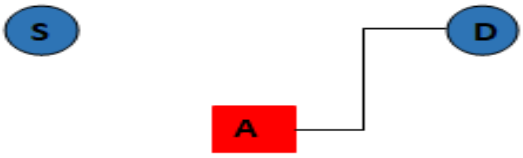


FIGURE II.5 – Attaque par répudiation.

- **IP spoofing :** L'usurpation d'adresse IP est une technique qui consiste à remplacer l'adresse IP de la source par une autre. Elle est utilisée par les attaquants pour éviter que leurs paquets soient filtrés par les systèmes de filtrage du réseau [25].
- **DNS spoofing :** Son principe est de donner des réponses incorrectes aux requêtes DNS, ce qui signifie associer une adresse IP incorrecte à un nom de domaine. Cela permet de rediriger les internautes, à leur insu, vers des sites pirates. Grâce à cette fausse redirection, l'utilisateur peut transmettre son identifiant en toute confiance [18].

II.4 Établissement d'une politique de sécurité

La politique de sécurité établit les règles, les procédures et les meilleures pratiques à mettre en place par toute organisation afin d'assurer un niveau de sécurité adéquat, renforçant ainsi sa structure face à différents risques [28].

II.4.1 Les mécanismes de sécurité informatique

II.4.1.1 La cryptographie

La cryptographie repose fondamentalement sur l'application de principes mathématiques pour garantir la sécurité des données. Elle autorise la sauvegarde sécurisée d'informations sensibles ainsi que la transmission sécurisée à travers des réseaux peu fiables, afin de prévenir toute tentative de piratage, de falsification ou d'interception [20].
Ce domaine comporte une multitude de termes spécifiques souvent utilisés, chacun correspondant à une facette particulière de la cryptographie [20] :

- **Cryptographie Symétrique :** La cryptographie symétrique, aussi appelée chiffrement à clé symétrique, désigne une catégorie d'algorithmes cryptographiques qui emploient une seule et même clé pour chiffrer le texte original et déchiffrer le texte chiffré.

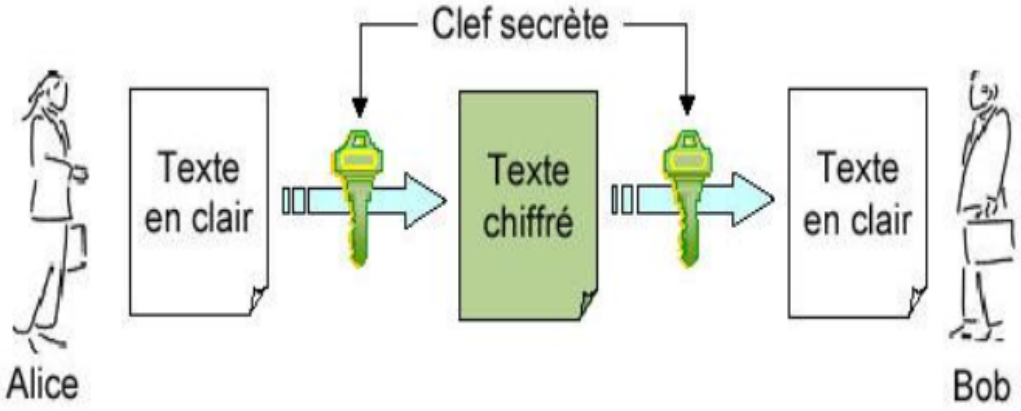


FIGURE II.6 – La cryptographie Symétrique [20].

- **Cryptographie Asymétrique :** La cryptographie asymétrique fait référence à un algorithme cryptographique qui requiert deux clés différentes, l'une étant publique pour crypter des données, tandis que l'autre est privée ou secrète pour le décryptage.

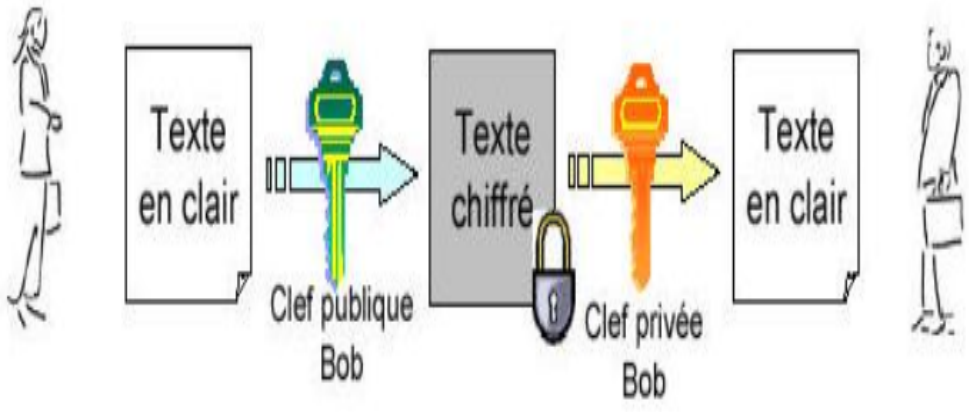


FIGURE II.7 – La cryptographie Asymétrique [20].

- **Signature numérique :** C'est une méthode permettant de vérifier l'identité de l'expéditeur d'un message ou du signataire d'un document, tout en assurant que le contenu original du message ou du document envoyé n'a pas été modifié depuis son envoi initial. En général, les signatures numériques sont faciles à transporter, car elles peuvent être facilement transférées entre divers supports numériques. Grâce à leur caractère unique et complexe, il est presque impossible de les reproduire par quelqu'un d'autre et elles peuvent être datées automatiquement.
- **La fonction de hachage :** Il s'agit d'un outil mathématique qui transforme une valeur numérique d'entrée en une valeur de hachage unique et compressée. Cette valeur de hachage est utilisée pour détecter toute altération des données. Bien que l'entrée de la fonction de hachage puisse être de longueur variable, la sortie est toujours une chaîne de longueur fixe.

II.4.1.2 L'authentification

C'est le processus qui vérifie si les informations d'identification fournies par un utilisateur correspondent à celles enregistrées dans une base de données autorisée. Elle permet aux organisations de sécuriser leurs réseaux en restreint uniquement les utilisateurs ou les processus authentifiés à accéder à leurs ressources protégées telles que les systèmes informatiques, de réseaux, de bases de données sensibles, de sites Web et d'autres applications ou services en ligne [21].
Une fois qu'un utilisateur ou un processus est authentifié, il est généralement soumis à une étape d'autorisation où il est déterminé si cette entité authentifiée a le droit d'accéder à une ressource spécifique ou à un système protégé [21].

II.4.1.3 Serveur Proxy

Également appelé serveur mandataire. Le terme « proxy » désigne l'action au nom d'un autre, et c'est justement le rôle d'un serveur proxy. Offre la possibilité de dissimuler une adresse IP et d'accéder à du contenu en ligne. Il agit en tant que client ou serveur Web afin de recevoir et de transmettre les informations. Les données Internet circulent via le serveur proxy pour atteindre l'adresse requise, puis la demande passe à nouveau par ce serveur proxy avant de recevoir les informations demandées [23].

II.4.1.4 Les anti-virus

Sont des logiciels informatiques spécialement développés pour détecter, neutraliser et supprimer les logiciels malveillants qui ont la capacité d'exploiter des vulnérabilités de sécurité ou de modifier et de supprimer des fichiers, qu'ils soient personnels ou indispensables au bon fonctionnement du système. Afin d'y parvenir, les antivirus analysent divers éléments tels que les fichiers, les e-mails, les secteurs de démarrage, la mémoire vive, les supports amovibles tels que les clés USB, les CD et les DVD, ainsi que les données qui circulent sur les réseaux, dont Internet [22].

II.4.2 Les protocoles de sécurité

Un protocole est une méthode conventionnelle qui facilite la communication entre les processus, c'est-à-dire un ensemble de règles et de procédures à suivre définies pour l'émission et la réception de données à travers un réseau [25]. Il en existe différentes formes de protocoles de sécurité en fonction des attentes de la communication [25] :

- **Protocole SSL** (Secure Socket Layer) : ou couche de sockets sécurisée, est un mécanisme de sécurisation des transactions sur Internet. En utilisant la cryptographie à clé publique, il permet ainsi d'établir un canal de communication sécurisé entre deux machines une fois l'authentification effectuée.
- **Protocole SSH** (Secure Shell) : C'est une technique établie qui permet aux utilisateurs d'accéder à distance à une machine de manière sécurisée via un canal de communication protégé appelé tunnel. Les informations échangées entre le serveur et le client sont cryptées, ce qui empêche toute interception du réseau par le biais d'un analyseur de trames.
- **Protocole HTTPs** (Hypertext Transfer Protocol Secure) : Aussi appelé HTTP sécurisé, renforce la sécurité des transactions effectuées via le protocole HTTP en incorporant des mesures de sécurité supplémentaires. Il s'assure de l'authentification et du chiffrement des informations transmises entre les sites web et les navigateurs, ce qui porte une protection accrue pour les échanges confidentiels. À la différence de SSL, qui fonctionne sur la couche de transport, HTTPS garantit la sécurité des communications directement au niveau du protocole HTTP.
- **Protocole IPsec** (Internet Protocol Security) : Il s'agit d'une technique de sécurité couramment employée afin de garantir des échanges sécurisés au sein d'un réseau informatique. Ce protocole propose différentes options de protection, comme la confidentialité, l'authentification et la sécurité des données en cours de transmission. Il est inclus dans le protocole IP et sert à garantir la sécurité des échanges sur les réseaux publics tels qu'Internet ou les réseaux privés d'entreprises. Il est principalement constitué de deux protocoles : le protocole AH (Header Authentication)

pour l'authentification des données et le protocole ESP (Encapsulating Security Payload) pour la confidentialité, l'authenticité et l'intégrité des données. IPsec peut être mis en œuvre de deux manières : le mode transport, où seul le contenu du datagramme IP est crypté, et le mode tunnel, où le datagramme IP entier est encapsulé dans un autre datagramme IP, ce qui offre une protection supplétive [24].

II.4.3 VPN (réseau privé virtuel)

Il s'agit d'un tunnel sécurisé au sein d'un réseau, tel qu'internet. Il permet un échange sécurisé et anonyme d'informations en utilisant une adresse IP différente de celle de l'appareil. Ce système permet de se connecter à Internet tout en masquant localisation réelle. Ce réseau est qualifié de virtuel, car il connecte deux réseaux physiques (réseaux locaux) par une connexion non fiable (internet). De plus, il est privé, parce que seuls les ordinateurs des réseaux locaux reliés par le VPN peuvent accéder aux données échangées en clair [26] [27].

II.4.3.1 Types de VPNs [26] [27]

- **VPN d'accès à distance :** Le VPN d'accès à distance offre aux utilisateurs la possibilité de se connecter à un autre réseau en utilisant un tunnel privé et chiffré, que ce soit Internet où le système interne de leur entreprise.
- **VPN site à site :** Aussi connu sous le nom de VPN de routeur à routeur. Ce type est principalement employé dans le domaine du travail, notamment lorsqu'une entreprise dispose de bureaux à différents endroits. Le VPN site-à-site permet la création d'un réseau interne sécurisé où les divers sites peuvent se connecter entre eux.

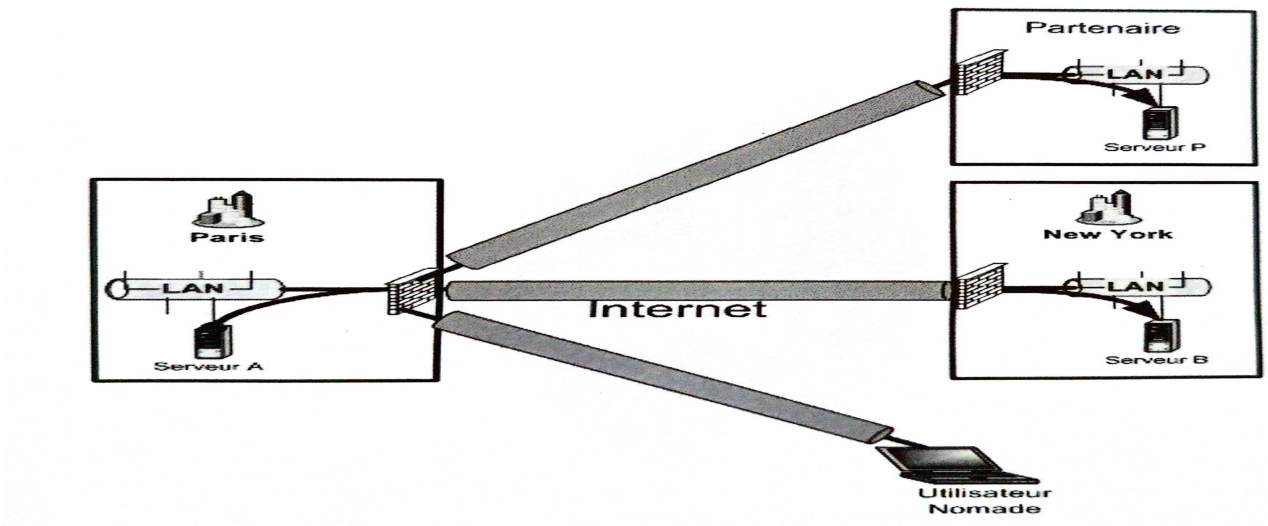


FIGURE II.8 – Types de VPNs [27].

II.4.3.2 Fonctionnement d'un VPN

Un réseau privé virtuel utilise des protocoles connus sous le nom de "protocoles de tunnelisation" qui garantissent la sécurité des données qui transitent d'une extrémité du VPN à l'autre grâce à des algorithmes de cryptographie. Perçu comme un tunnel sécurisé en raison de sa capacité à chiffrer les informations entre son point d'entrée et son point de sortie, les rendant ainsi illisibles pour toute personne qui les intercepte en continu. Le client VPN est l'outil ou le logiciel utilisé par l'utilisateur pour crypter et décrypter les données, tandis que le serveur VPN est l'outil ou le logiciel utilisé par l'organisation pour ces mêmes fonctions [25].

— **Les protocoles de tunnelisation [25]**

- PPTP (Point to Point Tunneling Protocol) : Il permet de générer des trames sous le protocole PPP (utilisé pour relier un système informatique à un autre par une connexion point-à-point) et de les comprimer dans un message IP.
- Le protocole L2TP (Layer Two Tunneling Protocol) : C'est un protocole classique qui combine les caractéristiques de PPTP. Il encapsule des trames PPP, qui peuvent elles-mêmes intégrer d'autres protocoles tels que l'IP.
- IPSEC : Ce protocole garantit la sécurité des communications au niveau de la couche réseau en utilisant deux modules principaux :

a) AH (Authentification Header) : garantit l'intégrité, l'authentification et prévient la relecture des paquets à encapsuler.

b) ESP (Encapsulating Security Payload) : Il établit le chiffrement des paquets tout en garantissant des services similaires à ceux offerts par AH.

II.4.4 Pare-feu

En anglais (Firewall) est un système qui se présente sous forme d'un logiciel installé sur une machine ou d'un dispositif physique. Il joue un rôle essentiel dans la protection des réseaux par :

— La création d'une barrière protectrice entre les réseaux internes sécurisés.

— Le contrôle des réseaux externes non sécurisés.

— L'assurance de la sécurité de l'ensemble du trafic et permettant de repérer et d'interdire l'accès au trafic indésirable.

Il est donc faisable de mettre en place une politique d'accès aux ressources du réseau en déterminant les types de trafic autorisés ou non sur le réseau internet. Il agit également comme une passerelle filtrante en filtrant les flux de données qui y circulent en fonction de diverses caractéristiques telles que l'origine et la destination des paquets, ainsi que les options présentes dans les données [25] [29].

Les pare-feux diffèrent selon le type de trafic à filtrer, avec une variété de fonctionnalités et de niveaux de maturité. En peut distinguer de nombreux types de pare-feu [29] :

— **Pare-feu sans état :** Ce type de pare- feu fonctionne au niveau réseau et transport du modèle OSI. Il examine chaque paquet et permet son passage s'il respecte les règles préétablies, qui sont basées sur des critères tels que l'adresse IP, les ports d'entrée et de sortie, ainsi que les protocoles de couche 3 et 4. Il est cependant complexe dans sa configuration et ne permet pas un filtrage approfondi.

— **Pare-feu avec état :** Les pare-feux équipés d'un état sont plus stricts que ceux qui ne l'ont pas. Ils veillent à la cohérence des paquets en utilisant une connexion établie, assurant ainsi que chaque paquet suit de manière logique le précédent. Ces pare-feux sont capables de filtrer les paquets et ont également une mémoire pour détecter les problèmes de manière plus efficace. Ils ont donc la capacité de faire face aux attaques de type DoS, une caractéristique qui n'est pas présente dans les pare-feux classiques.

— **Pare-feux applicatifs :** Il s'agir de la nouvelle génération de pare-feu qui interviennent au niveau de la couche d'application. Un proxy HTTP, par exemple, filtre toute demande HTTP. Malgré leur plus grande fiabilité par rapport aux pare-feux avec état, ils demandent plus de temps de calcul lorsqu'ils sont exposés à un débit élevé.

— **Pare-feu personnel :** Il est utilisé lorsque la zone protégée se restreint à l'ordinateur sur lequel le pare-feu est installé. Il assure la surveillance de l'accès au réseau des applications installées sur la machine, en particulier en empêchant les attaques de type programme nuisible (cheval de trois) qui ouvrent une brèche dans le système afin de permettre au pirate de prendre en main la machine à distance [25].

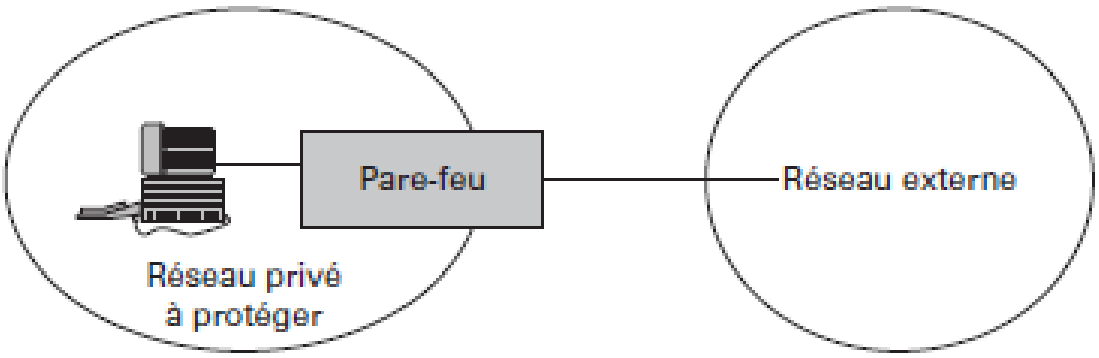


FIGURE II.9 – Pare-feu [29]

II.4.5 La zone démilitarisée (DMZ)

La DMZ utilisée lorsque l'on doit accéder à certaines machines du réseau interne depuis l'extérieur, telles que des serveurs, sans mettre en péril la sécurité de l'entreprise. Cela nécessite la mise en place d'une architectures réseau qui cloisonnent les différents segments. La DMZ est spécialement conçue pour héberger des applications ouvertes au public, tout en évitant les connexions directes avec le réseau interne. Elle joue donc le rôle d'une zone de tampon entre le réseau à protéger et les éventuelles menaces extérieures [25] [28].

En général, on applique la politique de sécurité suivante sur la DMZ [25].

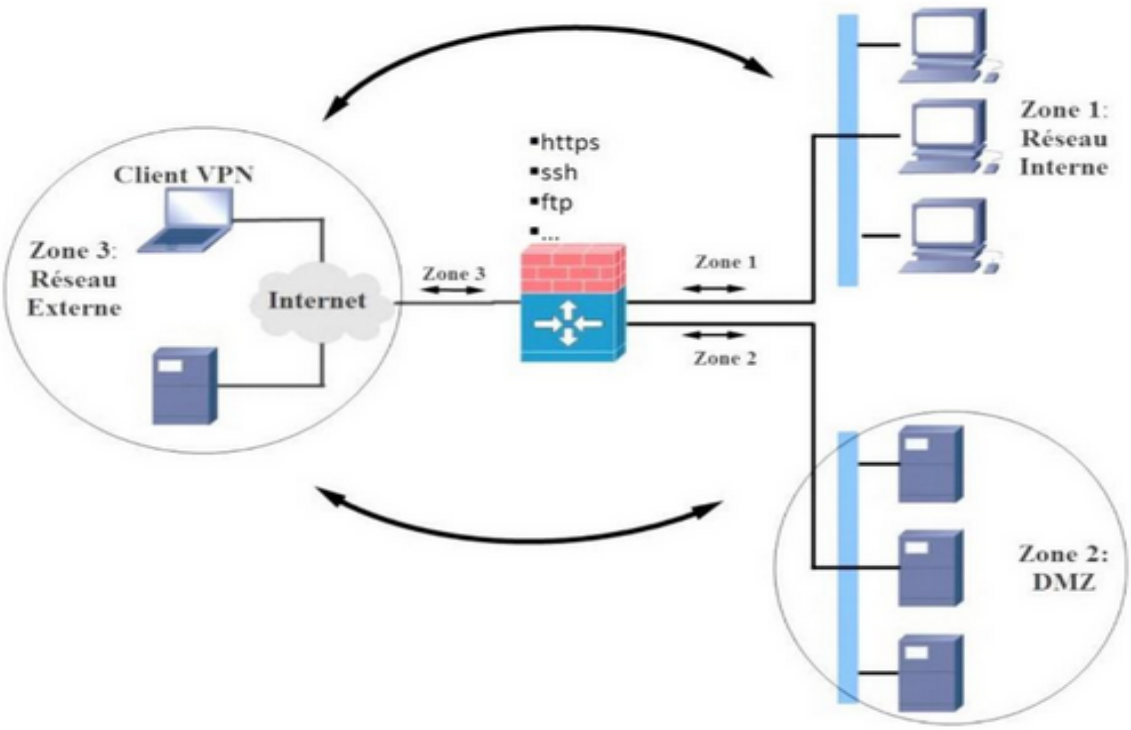


FIGURE II.10 – La DMZ [28].

— Permettre le trafic du réseau externe vers la DMZ.
— Interdire le trafic du réseau externe vers le réseau interne.
— Permettre le trafic du réseau interne vers la DMZ.
— Permettre le trafic du réseau interne vers le réseau externe.
— Interdire le trafic de la DMZ vers le réseau interne.
— Interdire le trafic de la DMZ vers le réseau externe.

II.4.6 Liste de contrôle d'accès

Access Control List (ACL), en français, liste de contrôle d'accès, est une série structurée de filtres connus sous le nom d'entrées de contrôle d'accès (ACE). Elles sont mises en œuvre pour le trafic entrant ou sortant des interfaces LAN/WAN pour un routeur [30].

- Adresse IP source.
- Adresse IP destination.
- Port source.
- Port destination.
- Protocole de destination (IP, TCP, UDP, ICMP, etc.).

Les ACL permettent d'indiquer quel genre de trafic doit être examiné, transmis ou géré en se basant sur les critères suivants [30] :

II.4.6.1 ACL standard

Vise le trafic en se basant sur les adresses IP source, sans tenir compte des ports spécifiques employés [30].

II.4.6.2 ACL étendue

Offre une filtrabilité plus précise en intégrant une large gamme de champs dans les en-têtes IP, TCP et UDP [30]. Sous Cisco, les numéros d'ACL permettent de déterminer le type d'ACL, comme indiqué ci-dessous :

- 1-99, 1300-1999 : Les ACL standard.
- 100-199, 2000-2699 : Les ACL étendues.

II.4.7 Les Systèmes de Détection et de Prévention des Intrusions IDS/IPS

II.4.7.1 Système du détection d'intrusion (IDS)

L'IDS est un dispositif logiciel et/ou de matériel qui permet de surveiller tous les paquets qui circulent sur un réseau afin de repérer les tentatives d'intrusion. En fonction du type de trafic et de sa configuration, il peut déclencher diverses alertes. En raison de son fonctionnement en temps réel, un IDS nécessite une quantité considérable de ressources, comme la puissance de calcul et la bande passante. Il est recommandé de l'installer sur une machine spécialement conçue pour cela [31]. Il existe deux grandes familles d'IDS [31] :

— Les NIDS : NIDS (système de détection d'intrusion dans le réseau) est un outil qui observe passivement et en temps réel tous les flux qui traversent un réseau afin de détecter des intrusions. Il capture l'ensemble du trafic réseau, l'analyse et déclenche des alertes lorsqu'il repère des paquets indésirables. Ainsi, un NIDS nécessite une capacité de bande passante suffisante pour gérer l'ensemble du trafic réseau et un matériel performant pour analyser ce trafic en mouvement.

— Les HIDS : HIDS est principalement destiné à surveiller une machine individuelle et analyser le trafic entrant et sortant ainsi que les journaux (logs) de cette machine spécifique. Par conséquent, un HIDS requiert une bande passante et une puissance CPU bien inférieure à celle d'un NIDS. Toutefois, afin de garantir un fonctionnement optimal, il est essentiel d'installer le HIDS sur un système propre, car il utilise l'état du système lors de son installation pour repérer les activités suspectes. En outre, lorsque plusieurs postes doivent être surveillés, il est indispensable d'implémenter un HIDS sur chaque poste, ce qui pose un problème logistique. Cependant, l'avantage des HIDS réside dans leur capacité à minimiser les alertes erronées (faux positifs).

II.4.7.2 Systèmes de prévention des intrusions

Les IPS regroupent à la fois du matériel et des logiciels visant à prévenir les intrusions ou toute autre activité suspecte détectée. Ils agissent de manière proactive pour stopper ces activités, tandis que les IDS se limitent à les détecter sans intervenir pour les arrêter [31]. Les IPS interviennent à différents niveaux [31] :

— Au niveau applicatif : l'IPS surveille tous les processus d'un système et les interrompt dès qu'ils adoptent un comportement non conforme.

— Au niveau Transport/Session : lorsque l'IPS détecte une session suspecte, il peut la mettre fin en envoyant un TCP Reset (Flag RST).

— Au niveau réseau : l'IPS est utilisé comme un routeur et peut entraver le trafic ou collaborer avec d'autres équipements réseau.

Ce système a une grande efficacité, mais il présente plusieurs inconvénients [31].

- Par erreur, les IPS peuvent empêcher le trafic légitime sans l'intervention humaine (faux positifs). Par exemple, pendant des périodes dans lesquelles le réseau est très utilisé, un IPS intégré peut interpréter ce trafic comme une attaque de déni de service et bloquer des connexions légitimes.
- Les attaquants ont la possibilité d'exploiter les IPS afin de mener des attaques de déni de service. En ajustant leur adresse IP dans le but de correspondre à celle d'un équipement essentiel du réseau, peut provoquer une détection par l'IPS, ce qui peut entraîner le blocage de l'attaquant et éventuellement de l'équipement réseau touché.
- Les attaquants repèrent fréquemment les IPS, car ils ont la capacité d'identifier et de bloquer rapidement les attaques en cours. Lorsque l'IPS est détecté, l'attaquant cherche à trouver une faille dans son fonctionnement afin de la contourner.

II.4.8 Le réseau local virtuel

Les VLANs rassemblent différents périphériques au sein d'un réseau local, les faisant fonctionner comme s'ils étaient reliés par le même câble. En employant des connexions logiques plutôt que physiques, ils renforcent l'efficacité du système en segmentant de vastes domaines de diffusion en unités plus petits. De cette manière, lorsqu'un membre d'un VLAN envoie une trame de diffusion, elle est reçue par tous les membres de ce VLAN, mais pas par ceux des autres VLANs [32].

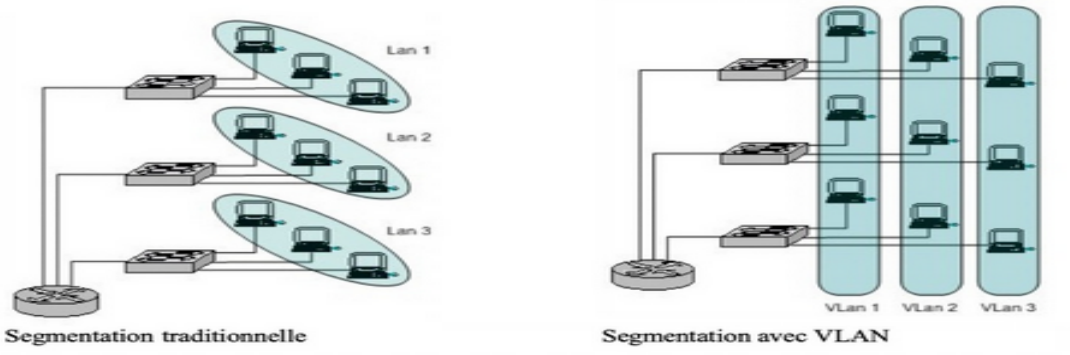


FIGURE II.11 – Segmentation avec VLANs [32].

II.4.8.1 Les avantages des VLANs [32]

- Sécurité.
- Optimiser les coûts.
- Des performances améliorées.
- La diminution des domaines de diffusion.
- Facilitent la gestion du réseau.

II.4.8.2 Attribution des VLANs [32]

— Le VLAN de niveau 1 (VLAN par port) : consiste à attribuer un VLAN à chaque port du commutateur, ce qui signifie que chaque carte réseau est associée à un VLAN selon le port auquel elle est connectée.

— Le VLAN de niveau 2 (VLAN basé sur l'adresse MAC) : chaque adresse MAC est associée à un VLAN particulier, ce qui permet une affectation dynamique des ports du commutateur à un VLAN selon l'adresse MAC de la carte réseau connectée.

— Le VLAN de niveau 3 (VLAN basés sur les adresses IP) attribue chaque carte réseau à un VLAN en fonction de son adresse IP.

II.4.8.3 Types des VLANs [32]

— VLAN par défaut : La mise en marche initiale d'un commutateur entraîne l'intégration de tous les ports dans le VLAN par défaut, ce qui permet la communication entre tous les périphériques du réseau.

— VLAN de données : Le VLAN de données est un réseau local virtuel spécifiquement conçu pour acheminer le trafic des utilisateurs. Il est impossible d'inclure des VLAN destinés à la voix ou à la gestion dans un VLAN de données.

— VLAN de gestion : Ce VLAN est spécifiquement conçu pour administrer les caractéristiques d'un Switch.

— VLAN natif : attribué à un port " trunk 802.1 Q", qui assure la liaison entre les commutateurs afin de transmettre le trafic de plusieurs VLAN.

Les VLANs sont implémentés de deux façons sur un commutateur réseau à travers [35] :

— Un port d'accès : configuré afin de transmettre le trafic d'un VLAN spécifique assigné à ce port.

— Un port trunk fait partie d'abord de tous les VLAN et transmet le trafic de plusieurs VLAN en même temps.

Conclusion

En conclusion, la sécurité informatique joue un rôle essentiel dans notre environnement numérique, où les menaces sont omniprésentes. Ce chapitre met en lumière la nécessité fondamentale de préserver la sécurité des systèmes et des données contre toute attaque éventuelle.Il est crucial de comprendre les différents types d'attaques et d'examiner les mécanismes de défense pour garantir une sécurité optimale. Le prochain chapitre

se consacrera à la mise en pratique de ces connaissances en développant des solutions de sécurité solides.

Chapitre III

Conception

Introduction

Dans ce chapitre, nous allons d'abord donner un aperçu général de l'organisme d'accueil, à savoir Algérie Télécom, en abordant ses activités et ses objectifs. Par la suite, nous décrirons la structure d'accueil et préciserons le cadre de notre travail. Ensuite, nous évaluerons l'architecture actuelle et identifierons ses faiblesses. Enfin, nous proposerons des solutions pour remédier à ces faiblesses et renforcer la sécurité de notre réseau.

III.1 Présentation d'Algérie Télécom

III.1.1 Historique d'Algérie Télécom

Algérie Télécom est une entreprise publique spécialisée dans les réseaux et les services de communication électronique. Créée en vertu de la loi 2000/03 du 5 août 2000, cette législation a réorganisé le secteur des postes et des télécommunications en séparant les activités postales de celles des télécommunications. Ainsi, établie en tant que société par actions (SPA) et entreprise publique économique, Algérie Télécom a commencé ses activités le 1er janvier 2003. Elle affirme son rôle crucial dans la mise en œuvre des programmes de développement de la société de l'information en Algérie. En prenant en compte les besoins variés de sa clientèle à travers les différents segments des services de télécommunications, elle s'engage à répondre de manière proactive aux exigences et aux attentes du marché [38].

FIGURE III.1 – L'entreprise Algérie Télécom [38].

III.1.2 Les activités d'Algérie Télécom

— La création, l'utilisation et la supervision des liaisons avec tous les opérateurs des réseaux de télécommunications [38].

— La conception, l'utilisation et l'administration des réseaux de télécommunications, qu'ils soient publics ou privés [38].

— La proposition de services de télécommunication pour le déplacement et la transmission de la voix, des textes, des données numériques et d'informations audiovisuelles [38].

— La mise à disposition de lignes téléphoniques fixes [38].

— Mise en place des solutions technologiques modernes permettant aux entreprises de communiquer de manière plus efficiente en interne et en externe [38].

— L'attribution de divers services tels que l'accès à internet haut débit et des connexions sans fil (4G LTE) [38].

— Développement et hébergement de solutions web [38].

III.1.3 Les principaux objectifs d'Algérie Télécom

— L'augmentation de la densité de la connectivité [38].

— L'expansion de l'accès à Internet à large bande [38].

— L'intégration de nouvelles technologies dans les multiples secteurs des télécommunications et des technologies de l'information et de la communication [38].

— Améliorer l'accessibilité des services téléphoniques et faciliter leur utilisation par un large éventail d'utilisateurs, notamment dans les zones rurales [38].

— Une alliance qui s'ouvre à toutes les compétences en matière de services et d'équipements de télécommunications, peu importe leur origine nationale [38].

— Mise en place d'une infrastructure réseau capable de supporter les besoins des clients en termes de qualité des produits, de sécurité et de services fournis [38].

— Une relation client forte, basée sur la transparence et la proximité [38].

— Prise en charge rapide des réclamations des clients [38].

— Mise en place de solutions facilitant la communication entre les entreprises [38].

— Mise en place d'un système d'information facilitant l'accès aux informations [38].

III.1.4 L'organigramme général d'Algérie Télécom

L'organigramme présenté dans (la Figure III.2) illustre la structure organisationnelle d'Algérie Télécom. Il met en évidence les différentes divisions et départements, ainsi que les relations hiérarchiques entre eux.

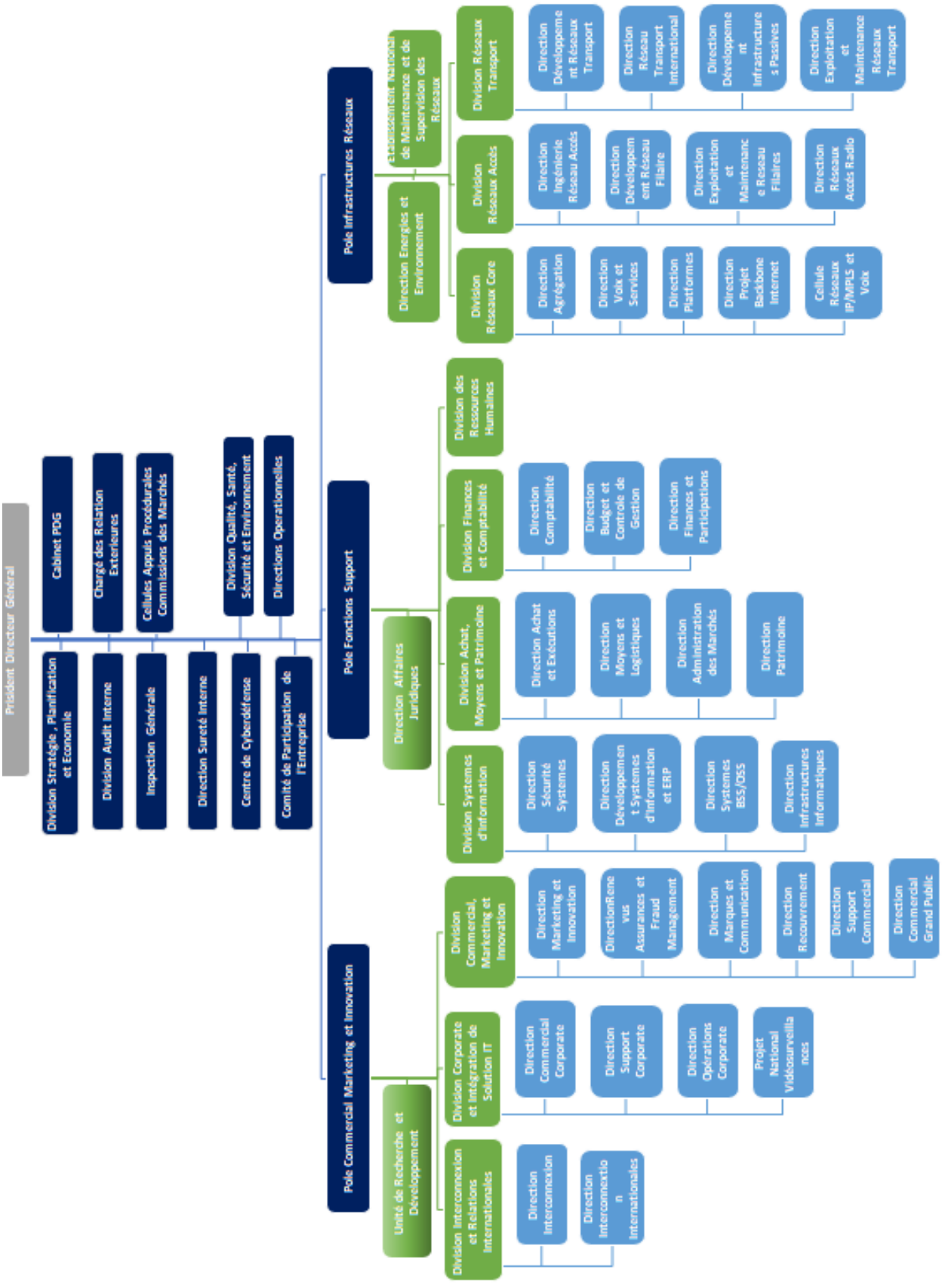


FIGURE III.2 – organigramme général d'Algérie Télécom.

Le schéma ci-dessous montre l'organisation de la direction opérationnelle (la Figure III.3)

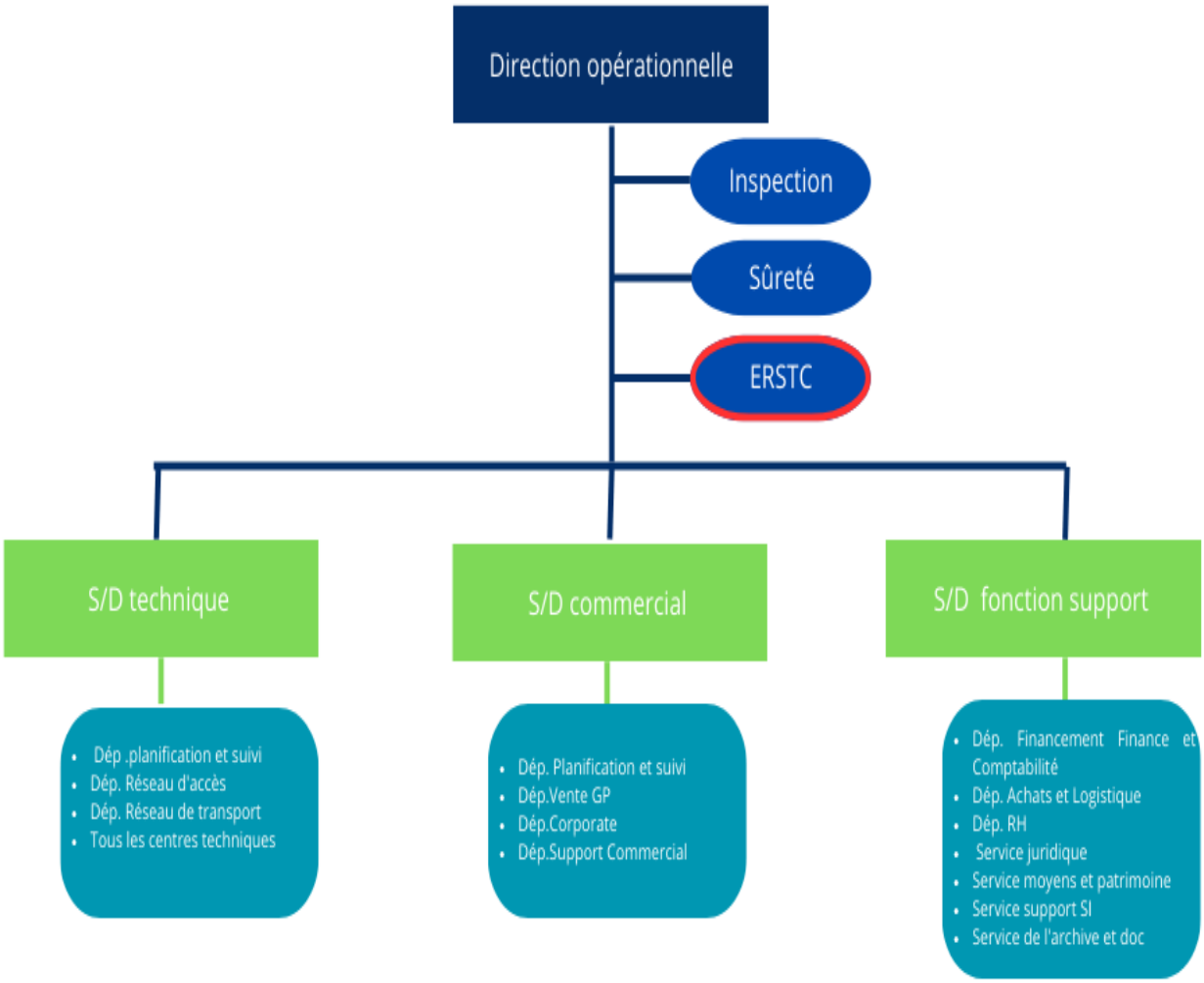


FIGURE III.3 – Organisation de la direction opérationnelle.

III.2 Contexte de notre travail

Nous avons effectué notre stage pratique au sein du département ERSTC (Établissement Régional du Support Technique et Commercial). L'ERSTC est un service rattaché administrativement à la Direction Opérationnelle des Télécommunications (DOT), tandis que tous les projets à mener et les décisions sont prises par la Direction Générale (DG).

III.2.1 Description et rôles de l'ERSTC

Cet établissement régional, fondé en 2009, dans le but spécifique de répondre aux besoins des clients d'Algérie Télécom en matière de construction et de maintenance des réseaux d'entreprises. Son équipe est constituée d'un responsable du centre, d'ingénieurs et de techniciens qualifiés. Sa mission principale est de couvrir les trois wilayas suivantes : Tizi-Ouzou, Boumerdès et Bouira. Les principales tâches qu'il se fixe incluent :

- Résolution des problèmes signalés par les clients (NAFTAL, CASNOS, Banques, etc.).
- Élaboration et entretien d'équipements informatiques, bureautiques et télécommunications de l'entreprise Algérie Télécom (ACTL, CMT, DOT, DRT, etc.).
- Mise en place de diverses connexions (XDSL, LS/RMS, X25, FO, etc.).
- Analyse et mise en place des réseaux LAN (filaire et WIFI).
- Accompagnement des stagiaires tout au long de leur apprentissage.
- Configuration de divers dispositifs de réseau et de transmission (Modem, Routeur, Firewall, Point d'accès, etc.).

III.2.2 Organigramme de l'Établissement Régional du Support Technique et Commercial (ERSTC)

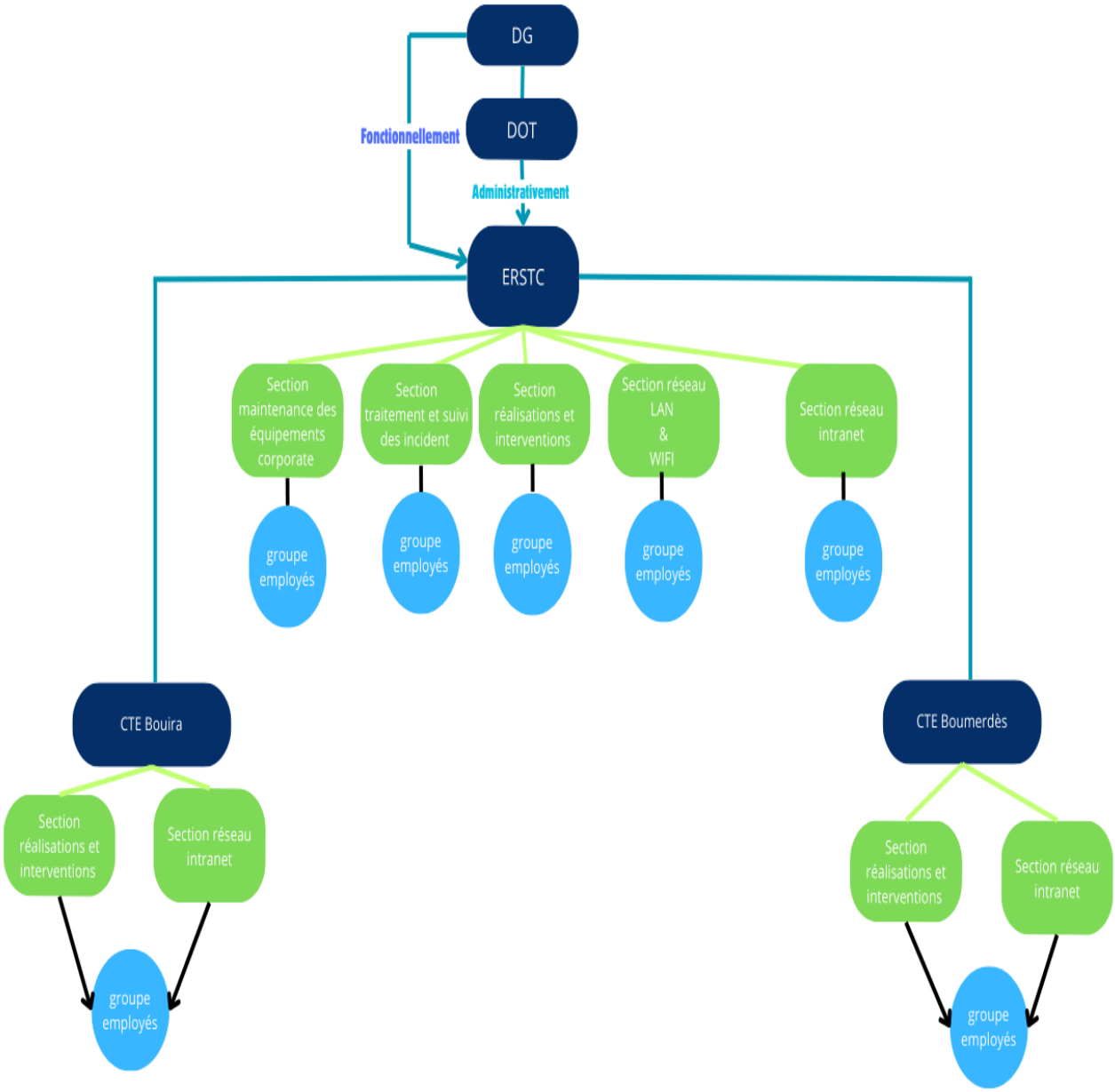


FIGURE III.4 – Organigramme de l'ERSTC.

Selon la Figure III.4, l'ERSTC est repartie en plusieurs sections. Chaque section a pour but d'accomplir des tâches prédéfinies pour assurer le bon fonctionnement de cet établissement. Ces sections sont définies comme suit :

III.2.2.1 Section réalisations et interventions

Cette section a pour but d'assurer le bon déroulement des opérations de déploiement des liaisons spécialisées et de la gestion des dérangements affectant ces derniers.

III.2.2.2 Section réseaux LAN et WIFI

Cette section a pour but d'assurer l'installation et la maintenance des réseaux LAN et Wi-Fi déployés dans le cadre des projets Corporate.

III.2.2.3 Section réseau intranet

Cette section a pour but d'assurer une prise en charge optimale des réclamations relatives au réseau intranet d'AT.

III.2.2.4 Section traitement et suivi des incidents

Cette section a pour but d'assurer la bonne prise en charge des incidents signalés.

III.2.2.5 Section maintenance des équipements Corporate

Cette section a pour but d'assurer le diagnostic et le rétablissement des pannes affectant les équipements Corporate.

Au niveau des DOT de Bouira et Boumerdès, des CTE (Centre Technique d'Entreprise) ont récemment été créés et sont reliés à l'ERSTC. Ils regroupent deux sections : réalisation et intervention, ainsi qu'un réseau intranet chargé des mêmes missions et activités dans les deux Wilayas. L'équipe de L'ERSTC peut se déplacer pour intervenir au niveau de ces deux Wilayas lorsque les CTE ne peuvent pas gérer certaines situations.

III.3 Objectif de notre travail

Notre travail consiste à analyser et à améliorer la sécurité du réseau informatique du service ERSTC (Établissement Régional du Support Technique et Commercial). Pour ce faire, nous allons mener une évaluation critique de l'architecture actuelle du réseau, identifier ses vulnérabilités et ses faiblesses potentielles, puis proposer des solutions pour renforcer la sécurité globale du système.

III.3.1 Présentation de l'architecture du réseau initial

Comme le montre la Figure III.5, l'architecture de l'entreprise Algérie Télécom regroupe trois sites reliés au site principal situé à Alger, passant par deux RMS (Réseau Multiservices) : l'un à Tizi-Ouzou et l'autre à Alger.

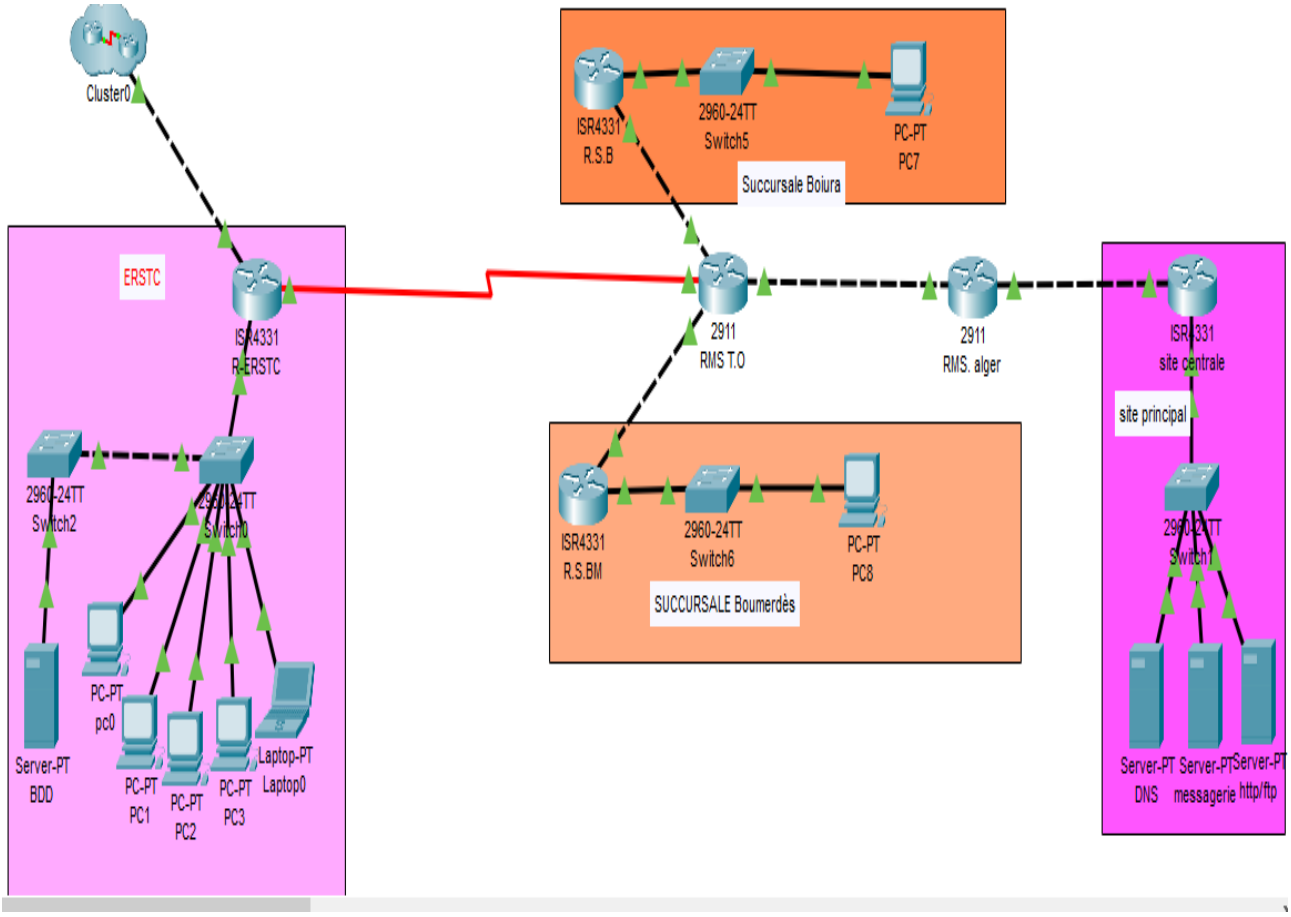


FIGURE III.5 – Architecture du réseau existant.

L'architecture du réseau initial est composée de :

- **Site (ERSTC) structuré comme suit :**
  - Un routeur : pour diriger le trafic de données entre différents réseaux en utilisant des tables de routage pour déterminer le chemin le plus efficace vers la destination souhaitée.
  - Deux Switch : pour connecter plusieurs équipements au sein d'un même réseau local, leur permettant ainsi de communiquer entre eux en transférant les données.
  - Des ordinateurs : pour traiter, stocker et manipuler des données, afin d'effectuer diverses tâches.
  - La plupart des serveurs d'Algérie Télécom sont centralisés à Alger. Toutefois, dans notre situation, l'ERSTC envisage de déployer un serveur de bases de données dans le but de stocker les informations de manière sécurisée et de les rendre accessibles aux utilisateurs autorisés.
- **Un site principal d'Alger.**
- **Une succursale à Boumerdès.**
- **Une succursale à Bouira.**

III.3.2 Étude critique

- **Critique 1 :** Inexistence d'une politique de sécurité précisant quel trafic est autorisé en entrée et en sortie, ainsi que d'une solution de sécurité permettant de gérer ce trafic.
- **Critique 2 :** Une communication entre les sites distants non sécurisée, ce qui signifie que les données transmises ne sont pas cryptées. Cette absence de cryptage peut entraîner différents types d'attaques, car les données non protégées peuvent être facilement lues en clair ou interceptées par des tiers malveillants.
- **Critique 3 :** Le déploiement d'un serveur de base de données sans la mise en place d'une architecture sécurisée pourra constituer une vulnérabilité pour le réseau de l'entreprise.
- **Critique 4 :** L'absence de redondance des équipements importants peut entraîner divers problèmes opérationnels, tels que des interruptions de service et des pertes de données, compromettant ainsi la productivité et la satisfaction des utilisateurs.
- **Critique 5 :** L'utilisation d'équipements obsolètes et de logiciels non mis à jour peut exposer le réseau à des risques de sécurité considérables. En effet, ces appareils et logiciels peuvent contenir des failles de sécurité connues et non corrigées, qui constituent des points d'entrée potentiels pour les attaquants. De plus, l'utilisation de mots de passe non robustes ou connus et communs à plusieurs utilisateurs accroît encore ces risques. Les attaquants peuvent alors recourir à des techniques telles que l'attaque par force brute pour déchiffrer ces mots de passe et avoir accès.

III.3.3 Solutions proposées

Après avoir effectué une étude critique sur le réseau initial du service ERSTC, nous proposons une nouvelle architecture qui intègre les différentes solutions proposées pour répondre aux critiques formulées.

Comme le montre la Figure III.6, l'architecture proposée est composée des éléments suivants :

- Un site ERSTC divisé en deux sous réseaux :
  - Un réseau interne.
  - Une DMZ (zone démilitarisée).
- Un site principal d'Alger.
- Une succursale à Boumerdès.
- Une succursale à Bouira.

- **Solution 1 :** Pour répondre à la première critique, nous proposons :

- La mise en place d'un pare-feu ASA pour gérer le trafic entrant et sortant. Ce pare-feu, de type matériel et évolutif, peut être ajusté en fonction des exigences de sécurité.
- La mise en place d'une charte de sécurité indiquant quel trafic est autorisée en entrée et en sortie.

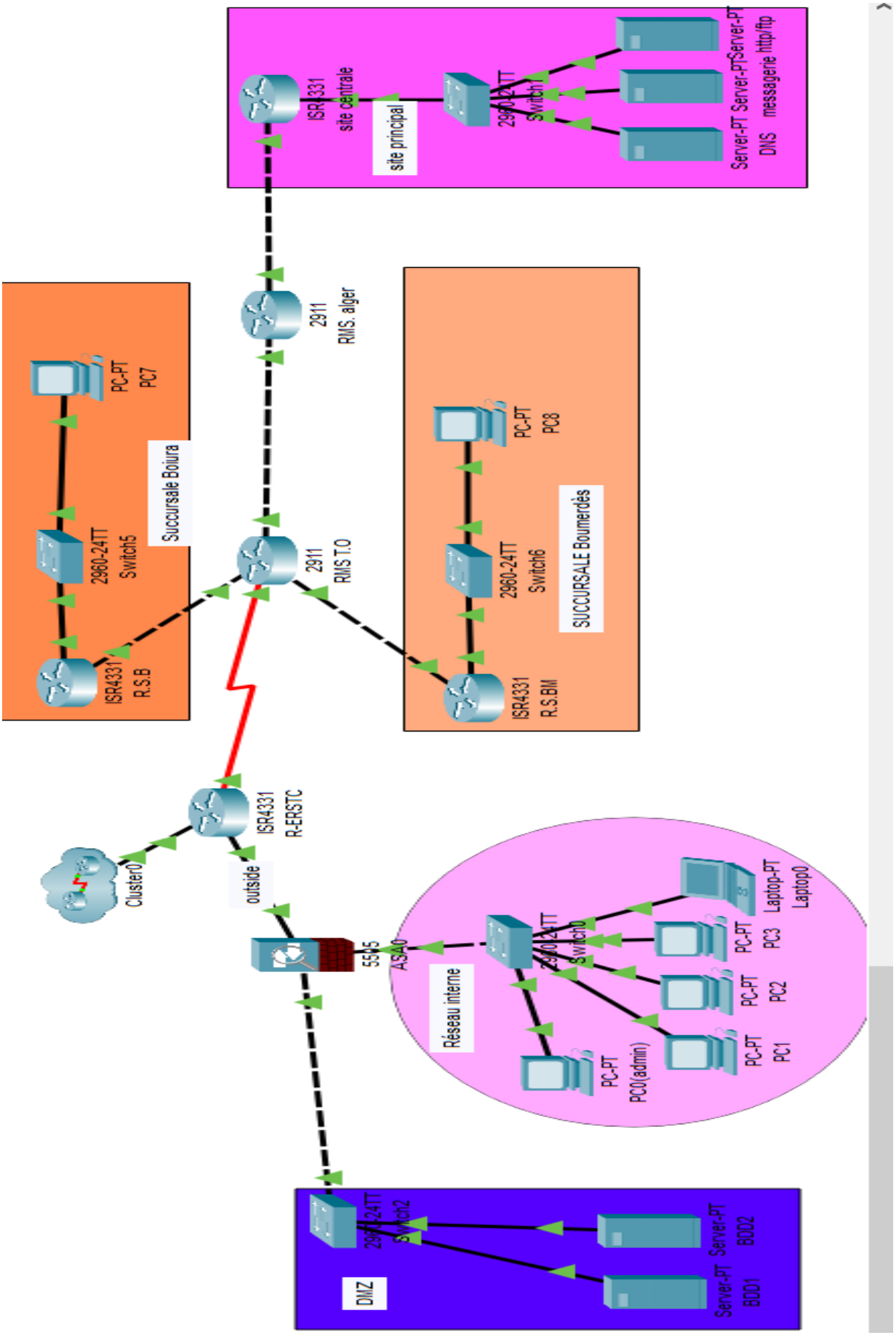


FIGURE III.6 – La nouvelle architecture réseau proposée.

- **Solution 2 :** Pour répondre à la deuxième critique, nous envisageons de mettre en place un VPN site-to-site pour sécuriser la communication entre le site ERSTC et les deux succursales de Bouira et Boumerdès.
- **Solution 3 :** Pour répondre à la troisième critique, nous proposons de mettre en place une DMZ qui offre une isolation contrôlée entre le réseau interne et Internet, permettant ainsi de garantir la sécurité des données et des ressources sensibles (serveur bases de données).
- **Solution 4 :** Pour répondre à la quatrième critique, nous proposons de dupliquer le serveur de base de données afin de partager la charge entre eux, car il est indispensable à notre infrastructure réseau en raison de sa gestion d'informations sensibles et essentielles. Pour garantir la disponibilité continue de ses services, on propose aux responsables de l'ERSTC de le dupliquer dans un autre site distant, qui sera le site principal d'Alger.
- **Solution 5 :** Pour répondre à la cinquième critique, nous suggérons au responsable du service ERSTC de créer une charte de sécurité. Ce document contiendra des instructions visant à sensibiliser les employés sur l'importance de la sécurité informatique, notamment en ce qui concerne la présence et la mise à jour des antivirus. Les antivirus sont essentiels pour détecter et éliminer les logiciels malveillants et les menaces potentielles. Il est important de les maintenir à jour pour bénéficier des dernières signatures de virus et des correctifs de sécurité. De plus, la charte encouragera la création de mots de passe robustes et forts, renforçant ainsi la sécurité des systèmes et des données de l'entreprise. En combinant cette proposition avec les autres pratiques de sécurité, ce service peut renforcer sa posture de sécurité.

Conclusion

Dans ce chapitre, nous avons étudié attentivement l'architecture de service ERSTC, en analysant de manière critique les vulnérabilités principales à éviter dans son réseau. En réponse à ces failles, nous avons élaboré des solutions visant à renforcer la sécurité du réseau initial. Dans le chapitre suivant, nous aborderons la phase de réalisation et de tests, où nous montrons en pratique ces solutions afin d'assurer une protection efficace.

Chapitre IV

Mise en place et tests

Introduction

Dans ce dernier chapitre, nous allons mettre en pratique l'architecture réseau sécurisée développée dans le chapitre 3, en utilisant le simulateur Cisco Packet Tracer. Nous avons présenté diverses configurations appliquées tout au long de notre projet, y compris les mécanismes de défense intégrés. Nous montrerons ensuite les résultats obtenus à travers les tests réalisés afin de résoudre les problèmes identifiés au début de notre étude.

IV.1 La présentation du simulateur Cisco Packet tracer

Packet Tracer, un logiciel développé par CISCO, offre la possibilité de créer un réseau virtuel physique et de simuler le fonctionnement des protocoles réseaux sur ce réseau. L'utilisateur peut constituer son réseau en utilisant différents équipements tels que des routeurs, des commutateurs, etc. Ces dispositifs doivent ensuite être connectés à travers divers types de câbles ou de fibre optique. Une fois que tous les équipements connectés il devient envisageable de configurer les adresses IP, les services disponibles et d'autres paramètres pour chacun d'entre eux. La Figure IV.1 montre le logo du simulateur Cisco Packet Tracer.

FIGURE IV.1 – Logo du simulateur Cisco Packet Tracer.

Une fois le simulateur est ouvert, la fenêtre montrée en Figure IV.2 va apparaître :

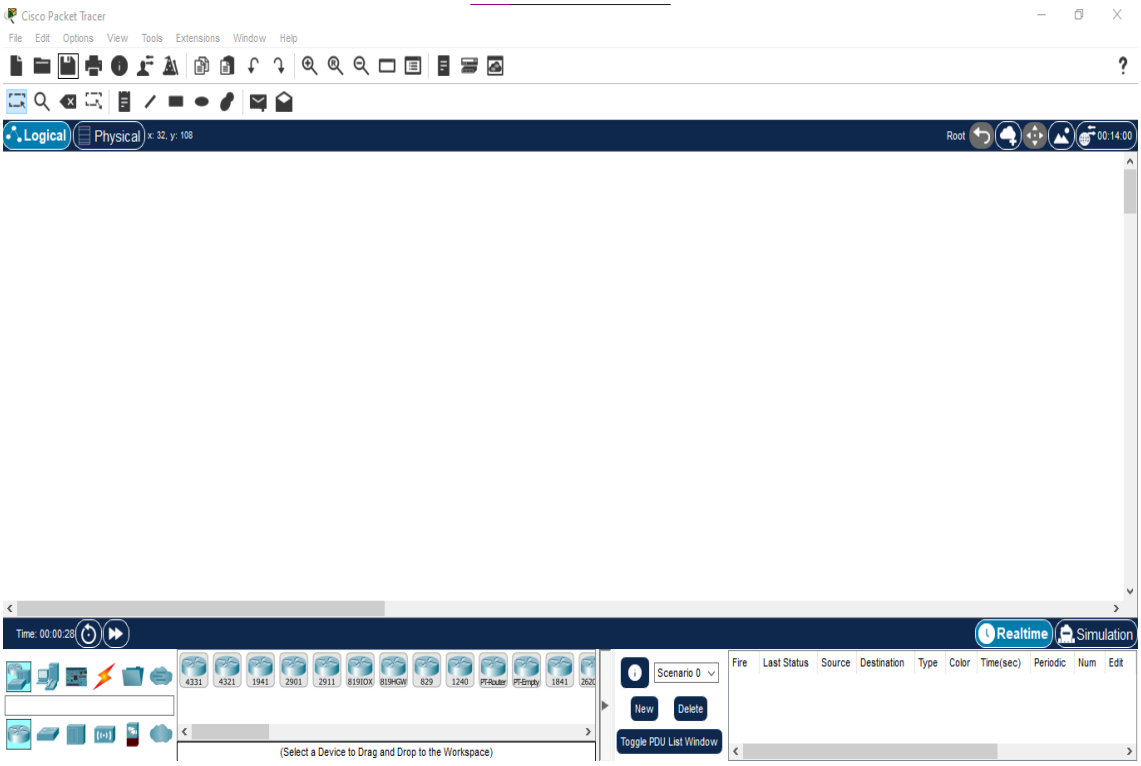


FIGURE IV.2 – Lancement du simulateur Cisco Packet Tracer.

IV.2 Configuration des solutions proposées

Avant de commencer la réalisation des solutions proposées, nous allons définir le plan d'adressage IP de chaque site.

IV.2.1 Le plan d'adressage IP pour le réseau initial

IV.2.1.1 Le plan d'adressage IP pour le site ERSTC

Le tableau IV.1 représente le plan d'adressage IP pour le site ERSTC.

Équipements	Interface	Adresse IP	MSR	Passerelle
R-ERSTC	S0/1/0	11.1.1.9	255.255.255.252	/
	G0/0/0	192.168.10.1	255.255.255.0	/
	G0/0/1	1.1.1.1	255.255.0.0	/
PC0 (admin)	Fa0	192.168.10.4	255.255.255.0	192.168.10.1
PC2	Fa0	192.168.10.5	255.255.255.0	192.168.10.1
PC3	Fa0	192.168.10.6	255.255.255.0	192.168.10.1
LAPTOP 0	Fa0	192.168.10.8	255.255.255.0	192.168.10.1
SERVEUR BDD	Fa0	192.168.10.9	255.255.255.0	192.168.10.1

TABLE IV.1 – Tableau de plan d'adressage IP pour le site ERSTC.

IV.2.1.2 Le plan d'adressage IP pour la succursale à Bouira

Le tableau IV.2 représente le plan d'adressage IP pour la succursale à Bouira.

Équipements	Interface	Adresse IP	MSR	Passerelle
R-SUCCURSALE	G0/0/0	192.168.12.1	255.255.255.0	/
	G0/0/1	11.1.1.1	255.255.255.252	/
PC7	Fa0	192.168.12.5	255.255.255.0	192.168.12.1

TABLE IV.2 – Tableau de plan d'adressage IP pour la succursale à Bouira.

IV.2.1.3 Le plan d'adressage IP pour la succursale à Boumerdès

Le tableau IV.3 représente le plan d'adressage IP pour la succursale Boumerdès.

Équipements	Interface	Adresse IP	MSR	Passerelle
R-SUCCURSALE	G0/0/1	192.168.11.1	255.255.255.0	/
	G0/0/0	11.1.1.5	255.255.255.252	/
PC8	Fa0	192.168.11.7	255.255.255.0	192.168.11.1

TABLE IV.3 – Tableau de plan d'adressage IP pour la succursale à Boumerdès.

IV.2.1.4 Le plan d'adressage IP pour site principal

Le tableau IV.4 représente le plan d'adressage IP pour le site principal.

Équipements	Interface	Adresse IP	MSR	Passerelle
R-SITE PRINCIPAL	G0/0/1	192.168.13.1	255.255.255.0	/
	G0/0/0	11.1.1.18	255.255.255.252	/
SERVEUR DNS	Fa0	192.168.13.4	255.255.255.0	192.168.13.1
SERVEUR MESSAGERIE	Fa0	192.168.13.5	255.255.255.0	192.168.13.1
SERVEUR HTTP/FTP	Fa0	192.168.13.6	255.255.255.0	192.168.13.1

TABLE IV.4 – Le plan d'adressage IP pour le site principal.

IV.2.2 Le plan d'adressage IP pour le réseau sécurisé

IV.2.2.1 Le plan d'adressage IP pour le site ERSTC

Le tableau IV.5 représente le plan d'adressage IP pour le site ERSTC.

Équipements	Interface	Adresse IP	MSR	Passerelle
R-ERSTC	S0/1/0	11.1.1.9	255.255.255.252	/
	G0/0/0	209.165.200.225	255.255.255.248	/
	G0/0/1	1.1.1.1	255.255.0.0	/
ASA	Et0/0	209.165.200.226 (vlan 2)	255.255.255.248	/
	Et0/1	192.168.10.1 (vlan 1)	255.255.255.0	/
	Et0/2	192.168.20.1 (vlan 3)	255.255.255.0	/
PC0 (admin)	Fa0	192.168.10.5	255.255.255.0	192.168.10.1
PC1	Fa0	192.168.10.6	255.255.255.0	192.168.10.1
PC2	Fa0	192.168.10.7	255.255.255.0	192.168.10.1
PC3	Fa0	192.168.10.8	255.255.255.0	192.168.10.1
LAPTOP 0	Fa0	192.168.10.9	255.255.255.0	192.168.10.1
SERVEUR BDD 1	Fa0	192.168.20.3	255.255.255.0	192.168.20.1
SERVEUR BDD 2	Fa0	192.168.20.4	255.255.255.0	192.168.20.1
PC0 (admin)	Fa0	NAT : dynamique	/	/
PC1	Fa0	NAT : dynamique	/	/
PC2	Fa0	NAT : dynamique	/	/
PC3	Fa0	NAT : dynamique	/	/
LAPTOP 0	Fa0	NAT : dynamique	/	/
SERVEUR BDD 1	Fa0	NAT : 209.165.200.227 (stat)	/	/
SERVEUR BDD 2	Fa0	NAT : 209.165.200.228 (stat)	/	/

TABLE IV.5 – Tableau de plan d'adressage IP pour le site ERSTC.

IV.2.2.2 Le plan d'adressage IP pour la succursale à Bouira

Le tableau IV.6 représente le plan d'adressage IP pourla succursale à Bouira.

Équipements	Interface	Adresse IP	MSR	Passerelle
R-SUCCURSALE	G0/0/0	192.168.12.1	255.255.255.0	/
	G0/0/1	11.1.1.1	255.255.255.252	/
PC7	Fa0	192.168.12.5	255.255.255.0	192.168.12.1

TABLE IV.6 – Tableau plan d'adressage IP pour la succursale à Bouira.

IV.2.2.3 Le plan d'dressage IP de la succursale à Boumerdès

Le tableau IV.7 représente le plan d'adressage IP pour la succursale Boumerdès.

Équipements	Interface	Adresse IP	MSR	Passerelle
R-SUCCURSALE	G0/0/1	192.168.11.1	255.255.255.0	/
	G0/0/0	11.1.1.5	255.255.255.252	/
PC8	Fa0	192.168.11.7	255.255.255.0	192.168.11.1

TABLE IV.7 – Tableau de plan d'adressage IP pour la succursale à Boumerdès.

IV.2.2.4 Le plan d'dressage IP pour le site principal

Le tableau IV.8 représente le plan d'adressage IP pour le site principal.

Équipements	Interface	Adresse IP	MSR	Passerelle
R-SITE PRINCIPAL	G0/0/1	192.168.13.1	255.255.255.0	/
	G0/0/0	11.1.1.18	255.255.255.252	/
SERVEUR DNS	Fa0	192.168.13.4	255.255.255.0	192.168.13.1
SERVER MESSAGERIE	Fa0	192.168.13.5	255.255.255.0	192.168.13.1
SERVEUR HTTP/FTP	Fa0	192.168.13.6	255.255.255.0	192.168.13.1

TABLE IV.8 – Tableau de plan d'adressage IP pour le site principal.

IV.2.3 Configuration de la politique de sécurité sur le pare-feu" CISCO ASA-5505"

IV.2.3.1 Configuration de base du pare-feu

- Commençons par configurer le nom de pare-feu, le nom de domaine, et le mot de passe (voir la Figure IV.3).

— La commande **"hostename"**permet de définir le nom de pare-feu.
— La commande **"domain-name"** permet de définir le nom de domaine.
— La commande **"enable password"** permet de configurer un mot de passe pour protéger le mode privilégié (enable mode).

```
ciscoasa>en
Password:
ciscoasa#conf t
ciscoasa(config)#hostname CISCOASA
CISCOASA(config)#domain-name ciscosecurity.com
CISCOASA(config)#enable password cisco55
```

FIGURE IV.3 – La configuration de base du pare-feu.

IV.2.3.2 Configuration des zones du pare-feu

Elle consiste à segmenter le réseau en différentes zones de sécurité, chacune avec des niveaux de protection spécifiques.

- **Configuration de la zone interne :** création d'une interface VLAN 1 avec les paramètres indiqués en Figure IV.4.

```
CISCOASA(config)#interface vlan 1
CISCOASA(config-if)#nameif INSIDE
CISCOASA(config-if)#ip address 192.168.10.1 255.255.255.0
CISCOASA(config-if)#security-level 100
CISCOASA(config-if)#exit
```

FIGURE IV.4 – La création de l'interface VLAN 1.

D'après la Figure IV.4.

— Le nom de la zone est "INSIDE".
— L'adresse IP de l'interface VLAN 1 est "192.168.10.1".
— Le niveau de la sécurité est 100, ce qui signifie qu'aucun utilisateur de niveau inférieur ne peut y accéder.

- Affectation de l'interface Ethernet 0/1 au VLAN 1(voir la Figure IV.5).

```
ciscoasa(config)#interface e0/1
ciscoasa(config-if)#switchport access vlan 1
```

FIGURE IV.5 – Affectation de l'interface Ethernet 0/1 au VLAN 1.

- **Configuration de la zone externe :** : création d'une interface VLAN 2 avec les paramètres indiqués en Figure IV.6

```
ciscoasa(config)#interface vlan 2
ciscoasa(config-if)#nameif OUTSIDE
ciscoasa(config-if)#ip address 209.165.200.226 255.255.255.248
ciscoasa(config-if)#security level 0
```

FIGURE IV.6 – La création de l'interface VLAN 2.

D'après la Figure IV.6.

— Le nom de la zone est "OUTSIDE".
— L'adresse IP de l'interface VLAN 2 est "209.165.200.226".
— Le niveau de la sécurité est 0, ce qui signifie qu'il s'agit d'une zone non sécurisée.

- Affectation de l'interface Ethernet 0/0 au VLAN 2(voir la Figure IV.7).

```
ciscoasa(config)#interface e0/0
ciscoasa(config-if)#switchport access vlan 2
```

FIGURE IV.7 – Affectation de l'interface Ethernet 0/0 au VLAN 2.

- **Configuration de la zone démilitarisée (DMZ) :** création d'une interface VLAN 3 avec les paramètres indiqués en Figure IV.8).

```
CISCOASA(config)#interface vlan 3
CISCOASA(config-if)#no forward interface vlan 1
CISCOASA(config-if)#nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
CISCOASA(config-if)#security-level 70
CISCOASA(config-if)#ip address 192.168.20.1 255.255.255.0
CISCOASA(config-if)#exit
```

FIGURE IV.8 – La création de l'interface VLAN 3.

D'après la Figure IV.8

— Le nom de la zone est "DMZ".
— Interdire l'accès au réseau interne.
— L'adresse IP de l'interface VLAN 3 est "192.168.20.1".
— Le niveau de la sécurité est 70, un compromis entre les niveaux de sécurité 0 et 100. Cela permet de limiter l'accès direct aux ressources internes tout en autorisant un certain accès depuis et vers l'extérieur à l'aide de listes de contrôle d'accès (ACL).

- Affectation de l'interface Ethernet 0/2 au VLAN 3(voir la Figure IV.9).

```
ciscoasa(config)#interface e0/2
ciscoasa(config-if)#switchport access vlan 3
```

FIGURE IV.9 – Affectation de l'interface Ethernet 0/2 au VLAN 3.

IV.2.3.3 Configuration du NAT statique et des ACL pour la DMZ

- Les règles NAT configurées possèdent les caractéristiques suivantes (voir la Figure IV.10).

```
ciscoasa(config)#object network DMZ-SERVER
ciscoasa(config-network-object)#host 192.168.20.3
ciscoasa(config-network-object)#nat ( DMZ,OUTSIDE ) static 209.165.200.227
ciscoasa(config-network-object)#host 192.168.20.4
ciscoasa(config-network-object)#nat ( DMZ,OUTSIDE ) static 209.165.200.228
```

FIGURE IV.10 – Configuration du NAT statique.

— Création d'un objet réseau nommé **"DMZ SERVER".**
— Attribuer au serveur BDD 1 une adresse publique (209.165.200.227).
— Attribuer au serveur BDD 2 une adresse publique (209.165.200.228).

- Ajout d'une liste de contrôle d'accès (ACL) afin d'autoriser l'accès aux serveurs de la DMZ depuis les succursales (voir la Figure IV.11).

```
ciscoasa(config)#access-list OUTSIDE-DMZ extended permit icmp any host 192.168.20.3
ciscoasa(config)#access-list OUTSIDE-DMZ extended permit icmp any host 192.168.20.4
ciscoasa(config)#access-group OUTSIDE-DMZ  in interface outside
```

FIGURE IV.11 – Configuration d'ACL sur le pare-feu.

— La commande **"access-list OUTSIDE-DMZ extended permit ICMP any host 192.168.20.4"** permet d'autoriser le trafic ICMP vers le serveur BDD2.
— La commande **"access-list OUTSIDE-DMZ extended permit ICMP any host 192.168.20.3"** permet d'autoriser le trafic ICMP vers le serveur BDD1.
— La commande **"access-group OUTSIDE-DMZ in interface outside "** permet d'appliquer les ACL au niveau de l'interface externe (outside).

IV.2.3.4 Configuration du Routage statique, du NAT dynamique et des Politiques d'Inspection

- **Configuration du routage statique :** pour permettre à l'ASA de se connecter à des réseaux externes, nous allons configurer une route statique par défaut sur son interface externe (voir la Figure IV.12).

```
ciscoasa(config)#route OUTSIDE 0.0.0.0 0.0.0.0 209.165.200.225
```

FIGURE IV.12 – Configuration du routage statique.

- **Configuration du NAT dynamique :** créer Un objet réseau, nommé **INSIDE-NETWORK** pour la configuration du NAT. Cet objet**INSIDE-NETWORK** permet de traduire les adresses du réseau interne (192.168.1.0/24) en une adresse publique globale sur l'interface externe de l'ASA (voir la Figure IV.13).

```
CISCOASA(config)#object network INSIDE-NETWORK
CISCOASA(config-network-object)#subnet 192.168.10.0 255.255.255.0
CISCOASA(config-network-object)#nat ( INSIDE,OUTSIDE ) dynamic interface
CISCOASA(config-network-object)#exit
```

FIGURE IV.13 – Configuration du NAT dynamique.

- **Création et configuration d'une politique d'inspection :** pour mettre en place une politique d'inspection, il est nécessaire de créer d'abord une 'class-map', une' policy-map 'et un' service-policy'(voir la Figure IV.14).

```
CISCOASA(config)#class-map insepction_default
CISCOASA(config-cmap)#match default-inspection-traffic
CISCOASA(config-cmap)#exit
CISCOASA(config)#policy-map global-policy
CISCOASA(config-pmap)#class insepction_default
CISCOASA(config-pmap-c)#inspect icmp
CISCOASA(config-pmap-c)#exit
CISCOASA(config)#service-policy global-policy global
```

FIGURE IV.14 – Création et configuration d'une politique d'inspection.

— La commande **"class-map inspection-default"** permet de créer une class-map nommée inspection-default.

— La commande **"match default-inspection-traffic"** permet d'appliquer l'inspection du trafic par défaut.

— La commande **"policy-map global-policy"** permet de créer une policy-map nommée global-policy.

— La commande **"class inspection-default"** permet d'appliquer la class-map déjà créée au niveau de la policy-map.

— La commande **"inspect icmp"** permet d'ajouter l'inspection du trafic ICMP à la liste de mappage (inspection-default).

— La commande **"service-policy global-policy global"** permet de créer une politique de service nommée global-policy et d'activer un mappage de stratégies globales (ce qui signifie qu'elle est active sur chaque interface de l'ASA).

IV.2.3.5 Configuration des protocoles DHCP, AAA, SSH

- **Configuration du DHCP :** Nous allons configurer le pare-feu en tant qu'un serveur DHCP pour attribuer la configuration dynamique aux machines de la zone interne (voir la Figure IV.15).

```
CISCOASA(config)#
CISCOASA(config)#
CISCOASA(config)#dhcpd add 192.168.10.5-192.168.10.36 inside
CISCOASA(config)#dhcpd dns 209.165.201.2 interface inside
CISCOASA(config)#dhcpd enable inside
CISCOASA(config)#
```

FIGURE IV.15 – Configuration du DHCP.

- **Configuration de AAA :** Cela permet d'utiliser les données locales pour l'authentification (voir la Figure IV.16).

```
CISCOASA(config)#
CISCOASA(config)#username admin password cisasa12
CISCOASA(config)#aaa authentication ssh console LOCAL
CISCOASA(config)#
```

FIGURE IV.16 – Configuration du AAA.

— La commande **"username admin password cisasa12"** permet de créer un compte utilisateur avec un nom d'utilisateur"admin" et mot de passe "cisasa12".

— La commande **"aaa authentication ssh console LOCAL"** permet d'autoriser les connexions ssh et consoles et vérifier les informations de l'authentification localement.

- **Configuration de l'accès à distance SSH au pare-feu :** Permet aux administrateurs de configurer et de gérer le pare-feu à distance (voir la Figure IV.17).

```
CISCOASA(config)#
CISCOASA(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]: yes
Keypair generation process begin. Please wait...
CISCOASA(config)#
CISCOASA(config)#
CISCOASA(config)#ssh 192.168.10.5 255.255.255.255 inside
CISCOASA(config)#ssh timeout 10
CISCOASA(config)#
```

FIGURE IV.17 – Configuration du SSH.

— La commande **"crypto key generate rsa modulus 1024 "** permet de créer une clé de chiffrement rsa d'une taille de 1024 bits.

— La commande **"ssh 192.168.10.5 255.255.255.255 inside"** permet d'autoriser l'accès que pour la machine qui porte l'adresse"192.168.10.5" du réseau interne.

IV.2.4 La mise en place du VPN site à site

A- VPN entre l'ERSTC et la succursale bouira.

Pour configurer un VPN site-à-site, nous avons suivi ces étapes :

— Configuration de la première phase ISAKMP : Cette phase permet la création d'une policy isakmp et la définition de ses paramètres.

— Configuration de la deuxième phase IPSEC : Cette phase permet la création d'une transform-set et la définition de ses paramètres.

IV.2.4.1 Configuration du VPN sur le routeur du ERSTC

- Création d'une politique ISAKMP (phase1) et configuration de ses propriétés (voir la Figure IV.18).

  — La commande **"crypto isakmp policy 10"** permet la création de la stratégie ISKMP avec le numéro de séquence 10, ce numéro indique le niveau de priorité.

  — La commande **"encryption aes 256"** signifie l'algorithme de cryptage utilisé(aes), l'attribut 256 signifie que les clés générées sont codées sur 256 bits.

  — La commande **"hash sha"** signifie l'algorithme de hachage utilisé (sha).

— La commande **"encryption pre-share"** signifie la méthode d'authentification utilisée (authentification à clé partagée).

— La commande **"group 5"** correspond à la méthode utilisée pour la génération de la clé symétrique pour le chiffrement des données échangées. L'attribut 5, Signifie que la clé générée est sur 1536 bits.

```
R-ERSTC(config)#crypto isakmp policy 10
R-ERSTC(config-isakmp)#encryption aes 256
R-ERSTC(config-isakmp)#hash sha
R-ERSTC(config-isakmp)#authentication pre-share
R-ERSTC(config-isakmp)#group 5
R-ERSTC(config-isakmp)#lifetime 86400
R-ERSTC(config-isakmp)#exit
```

FIGURE IV.18 – La création d'une politique ISAKMP sur le routeur ERSTC.

- Création de la clé partagée (voir la Figure IV.19).

```
R-ERSTC(config)#crypto isakmp key vpnpa55 address 11.1.1.1
```

FIGURE IV.19 – La création de la clé partagée sur le routeur ERSTC.

— La commande **"crypto isakmp key vpnpa55 address 11.1.1.1"** définit la clé partagée. Dans notre cas, nous avons utilisé la clé 'vpnpa55'.

- Création d'une transform-set et la configuration de ses paramètres (phase 2) (voir la Figure IV.20)

```
R-ERSTC(config)#crypto ipsec transform-set esp-aes esp-sha-hmac
```

FIGURE IV.20 – La création d'une transform-set sur le routeur ERSTC.

— Dans la configuration présentée en Figure IV.20, nous avons utilisé le protocole de sécurité 'ESP' avec deux paramètres : 'AES' pour l'algorithme de cryptage utilisé et "SHA" pour l'algorithme de hachage utilisé.

- Création d'une liste d'accès afin d'autoriser le trafic entrant depuis la succursale vers le ERSTC (voir la Figure IV.21).

```
R-ERSTC(config)#access-list 110 permit ip 209.165.200.224 0.0.0.7 192.168.12.0 0.0.0.255
```

FIGURE IV.21 – La création d'une liste d'accès sur le routeur ERSTC.

— La commande **"access-list 110 permit ip 209.165.200.224 0.0.0.7 192.168.12.0 0.0.0.255"** permet d'autoriser le trafic entrant depuis la succursale vers ERSTC.

- Création de la crypto map pour définir le flux de données qui doit subir un traitement de sécurité et le chemin qu'il doit emprunter. (voir la Figure IV.22).

```
R-ERSTC(config)#CRYpto map VPN-MAP 10 ipsec-isakmp
R-ERSTC(config-crypto-map)#set peer 11.1.1.1
R-ERSTC(config-crypto-map)#set pfs group5
R-ERSTC(config-crypto-map)#set security-association lifetime seconds 86400
R-ERSTC(config-crypto-map)#match address 110
R-ERSTC(config-crypto-map)#set transform-set VPN-SET
R-ERSTC(config-crypto-map)#exit
```

FIGURE IV.22 – La création de la crypto map sur le routeur ERSTC.

— La commande **"crypto map VPN-MAP 10 ipsec-isakmp"** permet la création d'une carte de chiffrement avec un numéro de séquence est 10. Il est à noter que nous pouvons également utiliser un numéro entre 1-65535 à condition qu'il soit le même pour les deux réseaux.
— La commande **" Set peer 11.1.1.1"** détermine l'adresse de l'interface de la succursale Bouira.
— La commande **"set security-association liftime seconds 86400"** définit la durée de vie de la clé de cryptage.
— La commande **" Set transform-set VPN-SET "** relie les deux configurations VPN-MAP et transform-set.
— La commande **"match address 110 "** correspond l'ACL 110 déjà créé à la crypto map.

- Application de la crypto map sur l'interface de sortie du routeur (voir la FigureIV.23).

```
R-ESRSTC(config)#interface s0/1/0
R-ESRSTC(config-if)#CRYPTO MAP VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

FIGURE IV.23 – Application de la crypto map sur l'interface de sortie du routeur ERSTC.

Le message" ISAKMP is ON " signifie que la crypto map est activée.

IV.2.4.2 La configuration du VPN sur le routeur de la succursale à Bouira

- Création d'une politique ISAKMP (phase1) et configuration de ses propriétés (voir la Figure IV.24).

```
R-SUCCURSALE-B(config)#crypto isakmp policy 10
R-SUCCURSALE-B(config-isakmp)#encryption aes 256
R-SUCCURSALE-B(config-isakmp)#authentication pre-share
R-SUCCURSALE-B(config-isakmp)#group 5
R-SUCCURSALE-B(config-isakmp)#lifetime 86400
R-SUCCURSALE-B(config-isakmp)#exit
```

FIGURE IV.24 – La création d'une politique ISAKMP (phase1) sur le routeur de succursale à Bouira.

— La commande **"crypto isakmp policy 10"** permet la création de la stratégie ISAKMP avec le numéro de séquence 10, ce numéro indique le niveau de priorité.
— La commande **"encryption aes 256"** signifie l'algorithme de cryptage utilisé(aes), l'attribut 256 signifie que les clés générées sont codées sur 256 bits.
— La commande **"hash sha"** signifie l'algorithme de hachage utilisé (sha).
— La commande **"encryption pre-share"** signifie la méthode d'authentification utilisée (authentification à clé partagée).
— La commande **"group 5"** correspond à la méthode utilisée pour la génération de la clé symétrique pour le chiffrement des données échangées.L'attribut 5,signifie que la clé générée est sur 1536 bits.

- Création de la clé partagée (voir la Figure IV.25).

```
R-SUCCURSALE-B(config)#crypto isakmp key vpnpa55 address 11.1.1.9
```

FIGURE IV.25 – La création de la clé partagée sur le routeur de la succursale à Bouira.

— La commande **"crypto isakmp key vpnpa55 address 11.1.1.9"** définit la clé partagée. Dans notre cas, nous avons utilisé la clé ‘vpnpa55’.

- Création d’une transform-set et la configuration de ses paramètres.(phase 2) (voir la Figure IV.26)

```
R-SUCCURSALE-B(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```

FIGURE IV.26 – La création d’une transform-set sur le routeur de la succursale à Bouira.

— Dans la configuration montrée en Figure IV.26, nous avons utilisé le protocole de sécurité ‘ESP’avec deux paramètres : ‘AES’ pour l’algorithme de cryptage utilisé et "SHA" pour l’algorithme de hachage utilisé.

- Création d’une liste d’accès afin d’autoriser le trafic entrant depuis le routeur ERSTC vers la succursale. (voir la Figure IV.27)

```
R-SUCCURSALE-B(config)#access-list 110 permit ip 192.168.12.0 0.0.0.255 209.165.200.224
0.0.0.7
```

FIGURE IV.27 – La création d’une liste d’accès sur le routeur de la succursale à Bouira.

— La commande **"access-list 110 permit ip 192.168.12.0 0.0.0.255 209.165.200.224 0.0.0.7"** permet d’autoriser le trafic entrant depuis le routeur ERSTC vers la succursale.

- Création de la crypto map définir le flux de données qui doit subir un traitement de sécurité et le chemin qu’il doit emprunter.(voir la Figure IV.28).

```
R-SUCCURSALE-B(config)#crypto map VPN-MAP 10 ipsec-isakmp
R-SUCCURSALE-B(config-crypto-map)#set peer 11.1.1.9
R-SUCCURSALE-B(config-crypto-map)#set pfs group5
R-SUCCURSALE-B(config-crypto-map)#set security-association lifetime seconds 86400
R-SUCCURSALE-B(config-crypto-map)#match address 110
R-SUCCURSALE-B(config-crypto-map)#set transform-set VPN-SET
R-SUCCURSALE-B(config-crypto-map)#exi
```

FIGURE IV.28 – La création de la crypto map sur le routeur de la succursale à Bouira.

— La commande **"crypto map VPN-MAP 10 ipsec-isakmp"** permet la création d’une carte de chiffrement avec le numéro de séquence est 10. Il est à noter que nous pouvons également utiliser un numéro entre 1-65535 à condition qu’il soit le même pour les deux réseaux.

— La commande **" Set peer 11.1.1.9"** détermine l'adresse de l'interface du routeur ERSTC.

— La commande **"set security-association liftime seconds 86400"** définit la durée de vie de la clé de cryptage.

— La commande **" Set transform-set VPN-SET "** relie les deux configurations VPN-MAP et transform-set.

— La commande **"match address 110 "** correspond l'ACL 110 déjà créé à la crypto map.

- Application de la crypto map sur l'interface de sortie du routeur de la succursale à Bouira.(voir la Figure IV.29).

```
R-SUCCURSALE-B(config)#interface g0/0/1
R-SUCCURSALE-B(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

FIGURE IV.29 – Application de la crypto map sur l'interface de sortie du routeur de la succursale à Bouira.

Le message "ISAKMP is ON " signifie que la crypto map est activée.

B- VPN entre l'ERSTC et la succursale boumerdès.

Pour configurer un VPN site-à-site, nous avons suivi ces étapes :

— Configuration de la première phase ISAKMP : Cette phase permet la création d'une policy isakmp et la définition de ses paramètres.

— Configuration de la deuxième phase IPSEC : Cette phase permet la création d'une transform-set et la définition de ses paramètres.

IV.2.4.3 La configuration du VPN sur le routeur du ERSTC

- Création d'une politique ISAKMP (phase1) et configuration de ses propriétés (voir la Figure IV.30).

```
R-ERSTC(config)#crypto isakmp policy 20
R-ERSTC(config-isakmp)#encryption aes 256
R-ERSTC(config-isakmp)#hash sha
R-ERSTC(config-isakmp)#authentication pre-share
R-ERSTC(config-isakmp)#authentication pre-share
R-ERSTC(config-isakmp)#group 5
R-ERSTC(config-isakmp)#lifetime 86400
R-ERSTC(config-isakmp)#exit
```

FIGURE IV.30 – La création d'une politique ISAKMP sur le routeur ERSTC.

— La commande **"crypto isakmp policy 20"** permet la création de la stratégie isakmp avec le numéro de séquence 20, ce numéro indique le niveau de priorité.
— La commande **"encryption aes 256"** signifie l'algorithme de cryptage utilisé(aes), l'attribut 256 signifie que les clés générées sont codées sur 256 bits.
— La commande **"hash sha"** signifie l'algorithme de hachage utilisé (sha).
— La commande **"encryption pre-share"** signifie la méthode d'authentification utilisée (authentification à clé partagée).
— La commande **"group 5"** correspond à la méthode utilisée pour la génération de la clé symétrique pour le chiffrement des données échangées. L'attribut 5, Signifié que la clé générée est sur 1536 bits.

- Création de la clé partagée (voir la Figure IV.31).

```
R-ERSTC(config)#crypto isakmp key vpnpb66 address 11.1.1.5
```

FIGURE IV.31 – La création de la clé partagée sur le routeur ERSTC.

— La commande **"crypto isakmp key vpnpb66 address 11.1.1.5"** définit la clé partagée. Dans notre cas, nous avons utilisé la clé 'vpnpb66'.

- Création d'une transform-set et la configuration de ses paramètres (phase 2). (voir la FigureIV.32)

```
R-ERSTC(config)#crypto ipsec transform-set VPNN-SET esp-aes 256 esp-sha-hmac
```

FIGURE IV.32 – La création d'une transform-set sur le routeur ERSTC.

— Dans la configuration présentée en Figure IV.32, nous avons utilisé le protocole de sécurité 'ESP' avec deux paramètres : 'AES' pour l'algorithme de cryptage utilisé et "SHA" pour l'algorithme de hachage utilisé.

- Création d'une liste d'accès afin d'autoriser le trafic entrant depuis la succursale vers le ERSTC (voir la Figure IV.33).

```
R-ERSTC(config)#access-list 100 permit ip 209.165.200.224 0.0.0.7  192.168.11.0 0.0.0.255
```

FIGURE IV.33 – La création d'une liste d'accès sur le routeur ERSTC.

— La commande **"access-list 100 permit ip 209.165.200.224 0.0.0.7 192.168.11.0 0.0.0.255"** permet d'autoriser le trafic entrant depuis la succursale vers ERSTC.

- Création de la crypto map pour définir le flux de données qui doit subir un traitement de sécurité et le chemin qu'il doit emprunter. (voir la Figure IV.34).

```
R-ERSTC(config)#crypto map VPN-MMAP 20 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R-ERSTC(config-crypto-map)#set peer 11.1.1.5
R-ERSTC(config-crypto-map)#set pfs group5
R-ERSTC(config-crypto-map)#set security-association lifetime seconds 86400
R-ERSTC(config-crypto-map)#match address 100
R-ERSTC(config-crypto-map)#set transform-set VPNN-SET
R-ERSTC(config-crypto-map)#exit
```

FIGURE IV.34 – La création de la crypto map sur le routeur ERSTC.

— La commande **"crypto map VPN-MMAP 20 ipsec-isakmp"** permet la création d'une carte de chiffrement avec le numéro de séquence est 20. Il est à noter que nous pouvons également utiliser un numéro entre 1-65535 à condition qu'il soit le même pour les deux réseaux.
— La commande **" Set peer 11.1.1.5"** détermine l'adresse de l'interface de la succursale Boumerdès.
— La commande **"set security-association liftime seconds 86400"** définit la durée de vie de la clé de cryptage.
— La commande **" Set transform-set VPNN-SET "** relie les deux configurations VPN-MMAP et transform-set.
— La commande **"match address 1O0 "** correspond l'ACL 110 déjà créé à la crypto map.

- Application de la crypto map sur l'interface de sortie du routeur (voir la FigureIV.35).

```
R-ERSTC(config)#interface s0/1/0
R-ERSTC(config-if)#crypto map VPN-MMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R-ERSTC(config-if)#END
R-ERSTC#
```

FIGURE IV.35 – Application de la crypto map sur l'interface de sortie du routeur ERSTC.

Le message" ISAKMP is ON " signifie que la crypto map est activée.

IV.2.4.4 La configuration du VPN sur le routeur de la succursale à Boumerdès

- Création d'une politique ISAKMP (phase1) et configuration de ses propriétés (voir la Figure IV.36).

```
R-SUCCURSALE-BM(config)#crypto isakmp policy 20
R-SUCCURSALE-BM(config-isakmp)#encryption aes 256
R-SUCCURSALE-BM(config-isakmp)#hash sha
R-SUCCURSALE-BM(config-isakmp)#authentication pre-share
R-SUCCURSALE-BM(config-isakmp)#authentication pre-share
R-SUCCURSALE-BM(config-isakmp)#group 5
R-SUCCURSALE-BM(config-isakmp)#lifetime 86400
R-SUCCURSALE-BM(config-isakmp)#exit
```

FIGURE IV.36 – La création d'une politique ISAKMP sur le routeur de succursale à Boumerdès.

— La commande **"crypto isakmp policy 20"** permet la création de la stratégie isakmp avec le numéro de séquence 20, ce numéro indique le niveau de priorité.
— La commande **"encryption aes 256"** signifie l'algorithme de cryptage utilisé(aes), l'attribut 256 signifie que les clés générées sont codées sur 256 bits.
— La commande **"hash sha"** signifie l'algorithme de hachage utilisé (sha).
— La commande **"encryption pre-share"** signifie la méthode d'authentification utilisée (authentification à clé partagée).
— La commande **"group 5"** correspond à la méthode utilisée pour la génération de la clé symétrique pour le chiffrement des données échangées. L'attribut 5,signifie que la clé générée est sur 1536 bits.

- Création de la clé partagée (voir la Figure IV.37).

```
R-SUCCURSALE-BM(config-isakmp)#exit
R-SUCCURSALE-BM(config)#crypto isakmp key vpnpb66 address 11.1.1.9
```

FIGURE IV.37 – La création de la clé partagée sur le routeur de la succursale à Boumerdès.

— La commande **"crypto isakmp key vpnpb66 address 11.1.1.9"** définit la clé partagée. Dans notre cas, nous avons utilisé la clé 'vpnpb66'.

- Création d'une transform-set et la configuration de ses paramètres (phase 2) (voir la FigureIV.38)

```
R.DOT.T.O(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```

FIGURE IV.38 – La création d'une transform-set sur le routeur de la succursale à Boumerdès.

— Dans la configuration montrée en Figure IV.38, nous avons utilisé le protocole de sécurité 'ESP'avec les paramètres : 'AES'qui pour l'algorithme de cryptage utilisé et "SHA" pour e l'algorithme de hachage utilisé.

- Création d'une liste d'accès afin d'autoriser le trafic entrant depuis le routeur ERSTC vers la succursale. (voir la Figure IV.39)

```
R-SUCCURSALE-BM(config)#access-list 100 permit ip 192.168.11.0 0.0.0.255 209.165.200.224
0.0.0.7
```

FIGURE IV.39 – La création d'une liste d'accès sur le routeur de la succursale à Boumerdès.

— La commande **"access-list 100 permit ip 192.168.11.0 0.0.0.255 209.165.200.224 0.0.0.7"** permet d'autoriser le trafic entrant depuis le routeur ERSTC vers la succursale.

- Création de la crypto map pour définir le flux de données qui doit subir un traitement de sécurité et le chemin qu'il doit emprunter. (voir la Figure IV.40).

```
R-SUCCURSALE-BM(config)#crypto map VPN-MMAP 20 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R-SUCCURSALE-BM(config-crypto-map)#set peer 11.1.1.9
R-SUCCURSALE-BM(config-crypto-map)#set pfs group5
R-SUCCURSALE-BM(config-crypto-map)#set security-association lifetime seconds 86400
R-SUCCURSALE-BM(config-crypto-map)#match address 100
R-SUCCURSALE-BM(config-crypto-map)#set transform-set VPNN-SET
R-SUCCURSALE-BM(config-crypto-map)#exit
```

FIGURE IV.40 – La création de la crypto map sur le routeur de la succursale à Boumerdès.

— La commande **"crypto map VPN-MAP 20 ipsec-isakmp"** permet la création d'une carte de chiffrement avec le numéro de séquence est 20. Il est à noter que nous pouvons également utiliser un numéro entre 1-65535 à condition qu'il soit le même pour les deux réseaux.

— La commande **"Set peer 11.1.1.9"** détermine l'adresse de l'interface du routeur ERSTC.

— La commande **"set security-association liftime seconds 86400"** définit la durée de vie de la clé de cryptage.

— La commande **" Set transform-set VPNN-SET "** relie les deux configurations VPN-MMAP et transform-set.

— La commande **"match address 100 "** correspond l'ACL 100 déjà créé à la crypto map.

- Application de la crypto map sur l'interface de sortie du routeur de la succursale à Boumerdès.(voir la Figure IV.41).

```
R-SUCCURSALE-BM(config)#interface g0/0/0
R-SUCCURSALE-BM(config-if)#crypto map VPN-MMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R-SUCCURSALE-BM(config-if)#
```

FIGURE IV.41 – Application de la crypto map sur l'interface de sortie du routeur de la succursale à Boumerdès.

Le message "ISAKMP is ON " signifie que la crypto map est activée.

IV.3 Résultats et tests

IV.3.1 Le résultat du test de fonctionnement du VPN

- Les Figures IV.42, IV.43, IV.44 montrent le résultat de la commande **"show crypto isakmp sa"** sur le routeur des sites ERSTC, Bouira, Boumerdès.

```
R-ERSTC#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
11.1.1.1        11.1.1.9        QM_IDLE           1012    0 ACTIVE

11.1.1.5        11.1.1.9        QM_IDLE           1047    0 ACTIVE
```

FIGURE IV.42 – Le résultat de la commande ”show crypto isakmp” sur le routeur de site ERSTC.

```
R-SUCCURSALE-B#sho crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
11.1.1.9        11.1.1.1        QM_IDLE           1029    0 ACTIVE
```

FIGURE IV.43 – Le résultat de la commande ”show crypto isakmp” sur le routeur de site Bouira.

```
R-SUCCURSALE-BM#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
11.1.1.9        11.1.1.5        QM_IDLE           1065    0 ACTIVE
```

FIGURE IV.44 – Le résultat de la commande ”show crypto isakmp” sur le routeur de site Boumerdès.

— D’après Les Figures IV.42, IV.43, IV.44 le tunnel VPN est correctement configuré sur les routeurs (voir les états (state) et les statuts dans les trois Figures).

- Les Figures IV.45, IV.46, montrent le résultat de la commande **”show crypto ipsec sa”** sur le routeur de l’ERSTC.

```
R-ERSTC#show crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN-MMAP, local addr 11.1.1.9

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (209.165.200.224/255.255.255.248/0/0)
   remote  ident (addr/mask/prot/port): (192.168.11.0/255.255.255.0/0/0)
   current_peer 11.1.1.5 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
```

FIGURE IV.45 – Le résultat de la commande ”show crypto ipsec sa” sur le routeur de l’ERSTC .

```
R-ERSTC#show crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: VPN-MAP, local addr 11.1.1.9

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (209.165.200.224/255.255.255.248/0/0)
   remote  ident (addr/mask/prot/port): (192.168.12.0/255.255.255.0/0/0)
   current_peer 11.1.1.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
   #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0
```

FIGURE IV.46 – Le résultat de la commande ”show crypto ipsec sa” sur le routeur de l’ERSTC.

— D’après Les Figures IV.45, IV.46, nous constatons que le chemin emprunté par le trafic entre le réseau local du site ERSTC et les deux succursales est bien crypté (voir les deux dernières lignes du résultat de la commande "Show crypto ipsec sa" dans les deux Figures).

IV.3.2 Résultats du test de fonctionnement du pare-feu

IV.3.2.1 Le résultat du test d’accès au serveur Base De Données

La Figure IV.47 montre le résultat de la commande "ping" depuis un hôte des succursales vers le serveur BDD.

```
C:\>ping 209.165.200.228

Pinging 209.165.200.228 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 209.165.200.228:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

FIGURE IV.47 – Le résultat de la commande "ping" depuis un hôte des succursales vers le serveur BDD.

- D’après la Figure IV.47, nous remarquons qu’aucun hôte des succursales ne peut effectuer une requête ICMP aux serveurs base de données de la DMZ. l’accès à ce serveur est

restreint pour des raisons de sécurité, mais la DMZ reste accessible aux utilisateurs, même externes. Cette politique de sécurité vise à protéger les données sensibles des serveurs de base de données. En cas d'évolutivité, comme l'ajout d'un autre serveur, tel qu'un serveur WEB, la DMZ est conçue pour permettre l'accès à ces nouveaux services tout en maintenant des restrictions strictes sur l'accès aux données sensibles.

La Figure IV.48 montre le résultat de la commande "ping" depuis le serveur BDD vers un hôte du réseau externe.

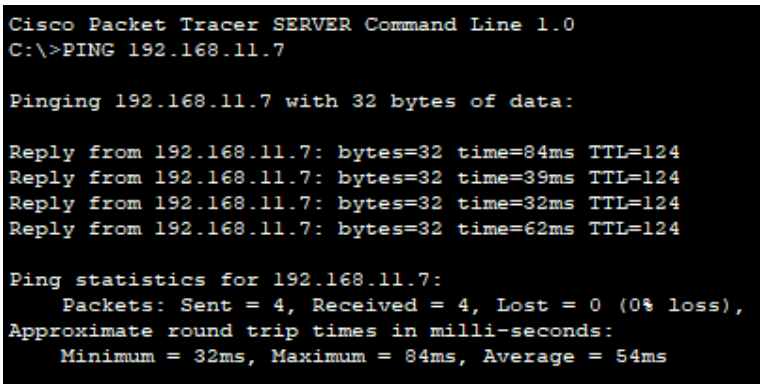


FIGURE IV.48 – Le résultat de la commande "ping" depuis le serveur BDD vers un hôte du réseau externe.

- D'après la Figure IV.48, nous constatons que le serveur BDD peut accéder aux hôtes du réseau externe.

La Figure IV.49 montre le résultat de la commande "ping" depuis un hôte du réseau interne vers le serveur BDD.

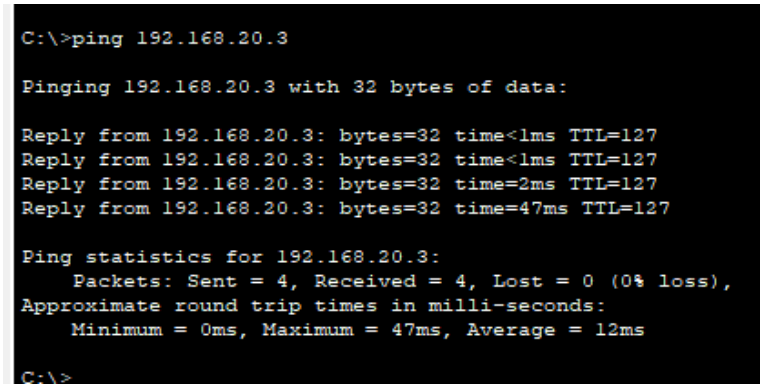


FIGURE IV.49 – Le résultat de la commande "ping" depuis un hôte du réseau interne vers le serveur BDD.

- D'après la Figure IV.49, nous remarquons que les hôtes de réseau interne peuvent accéder aux serveurs de la DMZ.

IV.3.3 Le résultat du test d'accès au réseau interne

La Figure IV.50 montre le résultat de la commande "ping" depuis un hôte du réseau externe vers un hôte du réseau interne.

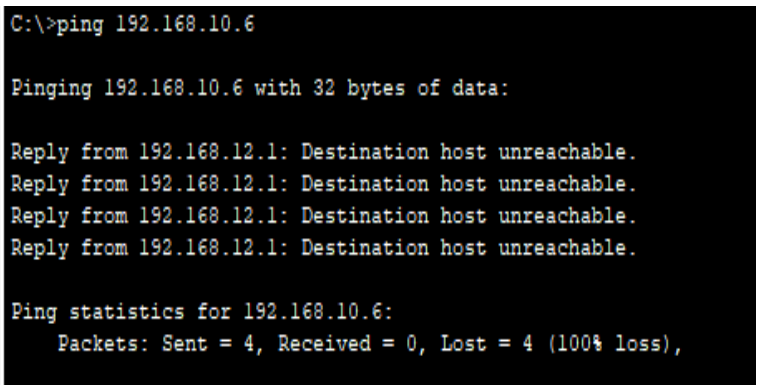


FIGURE IV.50 – Le résultat de la commande "ping" depuis un hôte du réseau externe vers un hôte du réseau interne.

- D'après la Figure IV.50, nous constatons qu'aucun hôte du réseau externe peut accéder aux hôtes du réseau interne.

IV.3.4 Résultat et tests d'accès du réseau interne vers le réseau externe

La Figure IV.51 montre le résultat de la commande "ping" depuis un hôte du réseau interne vers un hôte du réseau externe.

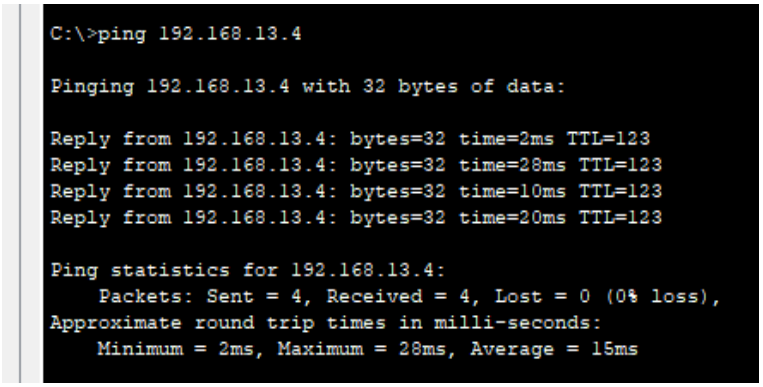


FIGURE IV.51 – Le résultat de la commande "ping" depuis un hôte du réseau interne un hôte du réseau externe

- D'après la Figure IV.51, nous remarquons que l'hôte du réseau interne peut accéder aux hôtes du réseau externe.

IV.3.5 Le résultat des connexions SSH au pare-feu ASA

La Figure IV.52 montre le résultat du test d'accès 'à distance au pare-feu ASA depuis l'hôte admin du réseau interne.

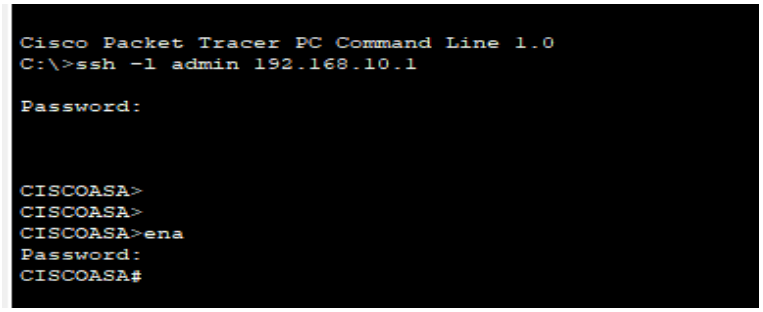


FIGURE IV.52 – Le résultat d'une connexion SSH depuis l'hôte admin du réseau interne au pare-feu ASA.

La Figure IV.53 montre le résultat du test d'accès à distance au pare-feu ASA depuis un hôte utilisateur du réseau interne.

FIGURE IV.53 – Le résultat d'une connexion SSH depuis un hôte utilisateur du réseau interne au pare-feu ASA.

— D'après les Figures IV.52et IV.53, on remarque l'accès SSH au par-feu est autorisé uniquement pour l'hôte admin.

Conclusion

Ce dernier chapitre a été consacré à la mise en œuvre des solutions proposées dans le chapitre trois en utilisant le simulateur Packet Tracer. Tout d'abord, nous avons configuré

un VPN site à site entre le site ERSTC et les deux succursales. Ensuite, nous avons configuré le pare-feu ASA. Enfin, nous avons vérifié la bonne configuration de ces solutions par des tests.

Conclusion Générale et Perspectives

Ce mémoire, réalisé dans le cadre d'un projet de fin d'études, aborde la sécurité des réseaux informatiques, en particulier ceux de l'ERSTC d'Algérie Télécom à Tizi-Ouzou. Il propose une nouvelle architecture sécurisée conçue pour répondre aux exigences particulières de cet environnement, dans le but de renforcer la protection des données sensibles.

Notre mémoire commence par l'introduction des bases nécessaires, en explorant les principes fondamentaux des réseaux informatiques (types de réseaux, les composants essentiels, l'adressage et le NAT), ainsi que les défis de la sécurité informatique (objectifs clés, menaces courantes, types d'attaques et méthodes de protection). Cette exploration vise à fournir un cadre de compréhension pour notre étude. Ensuite, nous avons précédé à une analyse détaillée du réseau actuel de l'ERSTC, identifiant avec précision ses points faibles et ses vulnérabilités. Sur cette base, nous avons développé une proposition d'architecture réseau sécurisée, incluant la mise en place d'un pare-feu ASA, d'un VPN site à site. Enfin, nous avons mené une série de tests à l'aide du simulateur Cisco Packet Tracer afin de vérifier le bon fonctionnement de l'architecture réseau sécurisée proposée.

Ce mémoire a été une expérience enrichissante qui nous a permis de renforcer nos compétences en résolution de problèmes dans le domaine des réseaux de télécommunication. Cette expérience nous a ouvert de nouvelles perspectives et nous a rapproché du monde professionnel. Nous avons acquis des connaissances approfondies sur les réseaux informatiques et leur sécurité, ce qui constitue un atout précieux pour notre carrière future. Nous espérons pouvoir appliquer cette étude dans nos projets à venir et partager ces connaissances avec d'autres étudiants afin d'enrichir leur savoir.

Dans le cadre de ce projet, nous avons principalement utilisé le simulateur Cisco Packet Tracer pour évaluer notre solution de sécurité réseau de manière virtuelle, et nous considérons que nous avons atteint notre objectif principal. Toutefois, notre prochaine étape consistera à déployer cette solution sur des équipements réels afin d'évaluer son efficacité dans des conditions opérationnelles réelles. Nous prévoyons d'intégrer plusieurs dispositifs de sécurité avancés pour renforcer notre architecture sécurisée. Tout d'abord, nous envisageons de mettre en place un système de détection d'intrusion (IDS) afin de détecter les anomalies dans les modèles de trafic et d'alerter les administrateurs sur des activités potentiellement malveillantes. En parallèle, nous planifions l'intégration d'un système de prévention d'intrusion (IPS) qui agira de manière proactive en bloquant les attaques dès leur détection en temps réel. De plus, nous projetons de mettre en œuvre un pare-feu applicatif pour sécuriser les applications Web en filtrant et en surveillant le trafic HTTP entre les applications web et Internet. Cette mesure renforcera la sécurité en protégeant spécifiquement les applications contre les attaques ciblées.

Bibliographie

[1] J. Dordoigne, *Réseaux informatiques : Notions fondamentales (Protocoles, Architecture, Réseaux sans fil, Virtualisation, Sécurité, IPv6*, Editions ENI, 2011.

[2] Cisco Networking Academy, *Module 4 : Couche physique* , Cisco et /ou ses filiales, https ://www.netacad.com (consulté le 8/02/2024).

[3] D.Lenge, *Mise en place d'une politique de sécurité et amelioration d'une architecture client-serveur*, Université de Kamina, 2019, https ://www.memoireonline.com/07/21/11937/Mise-en-place-dune-politique-de-securite-et-amelioration-dune-architecture-client-serveur8.html, (consulté le 28/05/2024).

[4] M. Jean-Michel, *Les fibres optiques : notions fondamentales (câbles, connectique, composants, Protocoles, réseaux,etc)*, Éditions ENI, 2015.

[5] R.BEDRA,*Supports de Transmission*, Université Mousfa-Benboulaid-Batna 2-Faculté de la technologie Département d'Électronique,2019-2020, https ://staff.univ-batna2.dz (consulté le 15/03/2024).

[6] cisco.goffinet.org/ccna/fondamentaux/protocoles-modeles-communication, (consulté le 22/05/2024).

[7] www.pucker-up.net/quelle-est-la-structure-dun-cable-coaxial, (consulté le 14/06/2024).

[8] G. Pujolle, *Cours réseaux et télécoms : avec exercices corrigés*,Editions EYROLLES Paris 2004.

[9] M. Hamouma , *cours de routage et interconnexion Master Réseaux et systèmes distribués, université de Batna 2 département informatique"* ,2022.

[10] S.Ghernaouti-Hélie préface de M.Riguidel, *Sécurité informatique et réseaux : cours et exercices corrigés*.3 e édition 2011.

[11] S.GHernaouti,*cybersécurité sécurité informatique et réseaux* ,5 e éditions 2016 .

[12] L. LEVIER,*Mise en oeuvre d'un pare-feu gratuit à base d'IP Filter*,Techniques de l'Ingénieur publier le 10 mai 2007.

[13] D.DROMAD,D.SERET,*Architecture des Réseaux* ,Pearson Education France 2006.

[14] Damien.SO, *, cours adressage IP et masque de sous-réseau*, publié le 3 novembre 2023, https ://www.formip.com/pages/blog/adressage-ip, (consulté le 20/05/2024).

[15] https ://www.netacad.com/Courses / Networking / CCNA : Introduction to Networks.

[16] https ://www.cloudflare.com/fr-fr/learning/network-layer/what-is-a-subnet/, (consulté le 13/06/2024).

[17] Support de cours, Université des sciences et de technologie d4oran Mohamed Boudiaf, 2eme Année LMD/S4 Module Réseaux de communication ,https ://univ-usto.dz/images/coursenligne/Rcom-chapitre1-partie2.2.pdf,(consulté le 25/04/2024).

[18] M.Messous,*" Mise en place d'un système de sécurité basé sur l'authentification dans un réseau IP"*, thèse de doctorat, Université Mouloud Mammeri, 2015.

[19] G. Marconato , *"Evaluation quantitative de la sécurité informatique : approche par les vulnérabilités"*, thèse de doctorat, INSA de Toulouse, France, 2009.

[20] M,A.FERRAG , *"Sécurité informatique" support de cours*, Université 8 mai 1945-Guelma Faculté des mathématiques, de l'informatique et des sciences de la matière Département Informatique,2018,https ://www.researchgate.net/publication/350495879 (consulté le 4/03/2024).

[21] L.ANTOINE, *"Cybersécurité : Qu'est-ce que l'authentification et pourquoi c'est crucial en matière de sécurité informatique ?*,January 12/2022, https ://www.cyberuniversity.com/post/quest-ce-que-lauthentification-et-pourquoi-cest-crucial-en-matiere-de-securite-informatique, (consulté le 15/05/2024).

[22] E.VINCENT, R.COLOMBIER , *"GMSI informatique"*, projet SAS , 2011.

[23] V.Remazeilles, *La sécurité des réseaux avec CISCO* ,Éditions ENI 2009.

[24] CH.HAMZA,*IPsec"Internet Protocol Security"* 2023, https ://forum.huawei.com/enterprise/fr/ipsec-internet-protocol-security, (consulté le 26/05/2024).

[25] J.FRANÇOIS PILLOU, J.PHILIPPE BAY *"Tout sur la sécurité informatique*, 3 e édition 2009.

[26] Techniques de l'ingénieur, *Administration de réseaux,applications et mise en oeuvre*, 2e édition 2012.

[27] R.Corvalan,E. Corvalan, Y. Le Corvic,*Les VPN : principes, conception et déploiement des réseaux privés virtuels*, 2 e édition DUNOD octobre 2005.

[28] S.ALI,*"Sécurité des réseaux informatique"*, ISTE édition, 2019.

[29] M. LAURENT,*Pare-feu - Couteau suisse de la sécurité informatique*,Techniques de l'Ingénieur publier le 10 octobre 2017.

[30] A.SALEM ZAIDOUN,*"Sécurité informatique : consepts et outils "*, 2023, https ://www.decitre.fr/livres/securite-informatique-9781784059071.html, (consulté le 10/06/2024).

[31] A.HAKIM,D.ADRIEN,D.SIDNEY,*"La protection des réseaux contre les attaques DOS"*,Université Paris Descarte (2009).

[32] *Cisco Networking Academy , Chapitre 1 : Réseaux Locaux Virtuels*.

[33] S. Ghernaouti, *Cybersécurité - 6e éd. : Analyser les risques, mettre en oeuvre les solutions.* Dunod, 2019.

[34] Cisco Networking Academy ,*cours introduction aux réseaux, module 16 : Principes fondamentaux de la sécurité du réseau*, https ://www.netacad.com (consulté le 19/06/2024).

[35] R. Boukharrou, *Sécurit des réseaux.* Support de cours en sécurité des réseaux,Universit´e Abdelhamid Mehri Constantine 2, 2019.

[36] Acissi, dirigé par J.Musset ,*Sécurité informatique - Ethical Hacking : Apprendre l'attaque pour mieux se défendre*,Éditions ENI 2012.

[37] N. Labraoui,*Sécurité Informatique Chapitre 1 : Notions Fondamentales*,Université Abou Bakr Belkaid Faculté des sciences Département d'Informatique ,Master 1 Réseaux et systèmes distribués 2019-2020

[38] *https ://www.algerietelecom.dz*, (consulté le 24/06/2024).

[39] P. Gomez et P. Bichon, *Comprendre les réseaux d'entreprise*,,Éditions EYROLLES, Paris 1993.