République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mouloud Mammeri de Tizi-Ouzou

Faculté De Génie Electrique et d'Informatique
Département de Télécommunications

Mémoire de Fin d'Etudes de

MASTER ACADEMIQUE

Filière :

Télécommunications

Spécialité :

Réseaux & Télécommunications

Par :
CHALLAL Kenza
SINI Dyhia

Thème

Mise en point d'une stratégie multi-protocoles pour sécuriser un réseau informatique

Devant le jury :

Présidente :	Mlle. BOUSSOUM.O
Promoteur :	Mr. LAZRI.M
Co-promoteur :	Mr. HAMROUN.A
Examinateur :	Mr. NOUIOUA.N

Remerciement

Tout d'abord, nous remercions Dieu de nous avoir aidées à surmonter toutes les difficultés rencontrées au cours de cette période et à mener à bien ce travail.

Nous adressons nos sincères remerciements à ***Monsieur LAZRI****, notre promoteur, et à* ***Monsieur HAMROUN****, notre co-promoteur, pour leurs précieuses directives et la qualité de leur accompagnement tout au long de ce projet.*

Nous tenons à remercier les membres du jury pour avoir accepté d'évaluer notre travail.

Nous remercions également ***Monsieur HADOUS****, chef d'établissement de l'ERSTC de Tizi Ouzou, ainsi que toute son équipe, pour leur disponibilité et aide.*

Nos remerciements s'adressent également à l'administration ainsi qu'aux professeurs du département de télécommunications pour leurs encouragements et leur soutien.

Enfin, nous exprimons notre profonde gratitude à nos familles et à nos amies pour leur soutien moral tout au long de ce parcours.

Dédicace

Je dédie ce mémoire à la mémoire de mon cher père, que Dieu ait son âme. Ton absence est une douleur profonde, mais ton amour, tes valeurs et tes sacrifices continuent de m'inspirer chaque jour.

À ma mère, pour sa force, sa patience, son amour inconditionnel et son soutien sans faille. Que Dieu te préserve.

À mes sœurs, pour leur affection, leur soutien et leur présence constante dans ma vie.

À ma grand-mère, pour ses prières, sa tendresse et sa sagesse, source de réconfort et d'encouragement.

À mes oncles et à leurs familles, ainsi qu'à mes tantes et leurs familles, pour leur chaleur, leurs encouragements et leur bienveillance.

À mon binôme et à sa famille, pour leur collaboration, leur sérieux, leur soutien et leur générosité tout au long de ce projet.

À mes amis, pour leur présence, leur motivation et leurs mots d'encouragement dans les moments les plus difficiles.

À toutes celles et ceux qui, de près ou de loin, ont contribué à l'aboutissement de ce travail.

Avec tout mon respect et ma profonde gratitude.

Dyhia

Dédicace

Je dédie ce travail à tous ceux qui m'ont soutenu moralement et émotionnellement tout au long de mon parcours universitaire.

À mes chers parents, pour leur amour inconditionnel, leurs sacrifices, leurs conseils et leurs prières. Votre soutien est la base de tout ce que j'ai pu accomplir.

À mes frères et à ma sœur, pour leur motivation et leur présence constante à mes côtés.

À l'épouse de mon frère, pour sa gentillesse et son encouragement.

À ma cousine, pour son soutien et sa bienveillance.

À mes grands-parents et mes tantes, pour leurs sagesses, leurs soutiens et leurs prières silencieuses qui m'ont toujours accompagné.

À mon binôme et sa famille, pour leur sérieux et leur esprit d'équipe tout au long de ce projet.

À mes amis, pour leur présence, leur bonne humeur et leur encouragement et pour tous les moments partagés.

À toutes celles et ceux qui, de près ou de loin, ont contribué à la réussite de ce mémoire.

Avec toute ma reconnaissance.

Kenza

Résumé

Ce mémoire de fin d'étude, présente la mise au point d'une architecture réseau sécurisée, intégrant plusieurs protocoles de sécurité, dont DHCP, SSH, ISAKMP et IPsec. L'objectif principal est de proposer une topologie qui est capable de garantir les objectifs de sécurité entre les différents équipements du réseau.

La stratégie suivie dans ce travail s'appuie sur une simulation faite sur Cisco Packet Tracer, où nous avons configuré une zone DMZ pour renforcer la sécurité des services exposés à l'extérieur tout en isolant le réseau interne, ainsi qu'un tunnel VPN d'accès à distance afin d'assurer des communications chiffrées.

Afin de valider le bon fonctionnement de l'architecture, des tests de connectivité (ping) ainsi que des tests d'accès web ont été réalisés.

Mot clés : sécurité réseau, vulnérabilités, multiprotocole, ASA, DMZ, VPN, IPsec, ISAKMP.

Abstract

This final year thesis presents the development of a secure network architecture integrating several security protocols, including DHCP, SSH, ISAKMP, and IPsec. The main objective is to propose a topology capable of ensuring security objectives between the various network devices.

The strategy followed in this work is based on a simulation performed on Cisco Packet Tracer, where we configured a DMZ zone to strengthen the security of externally exposed services while isolating the internal network, as well as a remote access VPN tunnel to ensure encrypted communications.

To validate the proper functioning of the architecture, connectivity tests (ping) and web access tests were performed.

Keywords: network security, vulnerabilities, multiprotocol, ASA, DMZ, VPN, IPsec, ISAKMP.

ملخص

يعرض هذا البحث في نهاية الدراسة تطوير بنية شبكة آمنة، تدمج عدة بروتوكولات أمنية مثل DHCP وSSH وISAKMP وIPsec. الهدف الرئيسي هو اقتراح طوبولوجيا قادرة على تحقيق أهداف الأمان بين مختلف مكونات الشبكة. تعتمد الاستراتيجية المتبعة في هذا العمل على محاكاة تم تنفيذها باستخدام برنامج Cisco Packet Tracer، حيث قمنا بتهيئة منطقة DMZ لتعزيز أمن الخدمات المكشوفة نحو الخارج مع عزل الشبكة الداخلية، بالإضافة إلى إنشاء نفق VPN للوصول عن بعد لضمان الاتصالات المشفرة.

وللتأكد من فعالية البنية، تم إجراء اختبارات اتصال (ping) وكذلك اختبارات الوصول إلى الويب.

الكلمات المفتاحية: أمن الشبكات، الثغرات، تعدد البروتوكولات، ASA، DMZ، VPN، IPsec، ISAKMP

Sommaire

Chapitre II: La sécurité informatique

CHAPITRE III: Les vulnérabilités

CHAPITRE IV: Simulation et tests d'un réseau informatique sécurisé

Liste des figures

Liste des tableaux

Glossaire

A

AAA: Authentication Authorization Accounting

ACL: Access Control List

ACTEL: Agence Commerciale des Télécommunications

ADSL: Asymmetric Digital Subscriber Line

AH: Authentication Header

ARP: Address Resolution Protocol

ASA: Adaptive Security Appliance

AT: Algérie Télécom

B

BGP: Border Gateway Protocol

C

CA: Certificate Authority

CD: Compact Disc

CMT: Centre de Maintenance Technique

D

DCE: Data Circuit-terminating Equipment

DHCP: Dynamic Host Configuration Protocol

DMZ: Demilitarized Zone

DNAT: Dynamic Network Translation Address

DNS: Domain Name Server

DoS: Denial of Service

DOT: Direction Opérationnelle des Télécommunications

DRT: Direction Régionale des Télécommunications

DTE: Data Terminal Equipment

E

ERSTC: Etablissement Régional Support Technique au Commerciale

ESP: Encapsulation Security Payload

F

FAI: Fournisseur d'Accès à Internet

FTP: File Transfer Protocol

H

HIDS: Host-based IDS

HSDSL: High-Speed Digital Subscriber Line

HTTP: HyperText Transfer Protocol

HTTPS: HyperText Transfer Protocol Secure

I

ICMP: Internet Control Message Protocol

IDS: Intrusion Detection System

IEEE: Institute of Electrical and Electronics Engineers

IoT: Internet of Things

IP: Internet Protocol

IPS: Intrusion Prevention System

IPsec: Internet Protocol Security

IPv4: Internet Protocol version 4

IPv6: Internet Protocol version 6

ISAKMP: Internet Security Association and Key Management Protocol

ISO: International Organization for Standardization

K

KDC: Key Distribution Center

L

LAN: Local Area Network

LDAP: Lightweight Directory Access Protocol

LETTO: Laboratoire des Equipements de Télécommunication

M

MAC: Media Access Control Med

MAN: Metropolitan Area Network

MPLS: Multi-Protocol Label Switching

MITM: Man In The Middle

N

NAS: Network Access Server

NAT: Network Translation Address

NIDS: Network-based IDS

O

OSI: Open System Interconnection

OSPF: Open Shortest Path First

P

PC: Poste de Commandement

PME: Petite et Moyenne Entreprise

POP: Post Office Protocol

P2P: Peer-to-Peer

R

RADIUS: Remote Authentication Dial-In User Service

RIP: Routing Information Protocol

RMS: Réseau Multiservice

S

SHDSL: Symmetric High-bit-rate Digital Subscriber Line

SMS: Short Message Service

SMTP: Simple Mail Transfer Protocol

SNAT: Static Network Translation Address

SPA: Société Par Action

SQL: Structured Query Language

SSH: Secure Shell

SSL: Secure Socket Layer

T

TACACS+: Terminal Access Controller Access-Control System Plus

TCP/IP: Transmission Control Protocol/ Internet Protocol

TCP: Transmission Control Protocol

TLS: Transport Layer Security

TTL: Time To Live

U

UDP: User Datagram Protocol

URL: Uniform Resource Locator

USB: Universal Serial Bus

V

VLAN: Virtual Local Area Network

VoIP: Voice over Internet Protocol

VTP: VLAN Trunking Protocol

VPN: Virtual Private Network

W

WI-FI: Wireless-Fidelity

WAN: Wide Area Network

X

XSS: Cross-Site Scripting

XTACACS: Extended Terminal Access Controller Access-Control System

Introduction Générale

Introduction générale

La sécurité informatique a longtemps été considérée comme un concept essentiel. Ces dernières années, elle a beaucoup évolué pour faire face à toutes sortes d'attaques, comme les virus qui se propagent très vite ou les hackers qui menacent la sécurité du réseau. Cette sécurité informatique est devenue une priorité pour les entreprises disposant d'un réseau informatique, surtout maintenant que beaucoup de choses se font à distance. C'est pourquoi des politiques et des procédures de sécurité sont mises en œuvre. L'arrivée d'Internet et sa généralisation a accentué le besoin de sécuriser d'une façon fiable les réseaux informatiques et les systèmes d'information.

Les systèmes de stockage et les réseaux d'entreprise doivent gérer à la fois la protection des données privées et le partage des données publiques, en d'autres termes, ce qui doit être protégé dans certaines situations et à certaines entités peut être divulgué dans d'autres situations et à d'autres entités. Pour une meilleure gestion, les entreprises font appel à l'usage des pare-feu qui permettent de diviser le réseau en zones avec différents niveaux de sécurité.

De plus, la plupart des entreprises n'ont pas les moyens de connecter leurs réseaux à distance avec des lignes privées ; elles utilisent donc Internet comme moyen de transmission. Pour répondre à ce besoin de communication et assurer la sécurité des données qui transitent, elles utilisent une liaison spécialisée, cette dernière utilise Internet comme support de transmission qui fonctionne avec un protocole d'encapsulation appelé "tunneling" ou VPN (Virtual Private Network).

Dans ce contexte, parmi l'ensemble des mesures de sécurisation possibles, et selon les besoins identifiés pour sécuriser un réseau informatique et la liaison dont laquelle transitent les données, le travail présenté dans ce mémoire met en évidence la stratégie adoptée qui consiste en l'utilisation d'un pare-feu et d'un VPN. D'autres protocoles et mécanismes sont aussi implémentés pour compléter la sécurité, tels que la DMZ, NAT, SSH, DHCP, ISAKMP, IPSEC.

Afin de toucher au côté pratique, nous avons pu effectuer un stage pratique au niveau d'Algérie Télécom. Durant ce stage, nous avons pu manipuler certains équipements d'un réseau informatique, tels que les routeurs, les armoires de brassage, les switchs, etc.

Pour bien structurer notre mémoire, le travail présenté s'organise autour de quatre chapitre dont les principaux objectifs sont décrits dans les paragraphes suivants :

- Dans ce premier chapitre, nous aborderons les notions de base des réseaux informatiques, telles que les différents types de réseaux, les topologies, les

technologies utilisées, l'adressage et le routage IP. Nous expliquerons aussi les modèles en couches qui permettent de comprendre comment les données circulent correctement. Ces notions sont importantes pour la suite de notre étude technique.

- Le deuxième chapitre se focalise sur la sécurité informatique des réseaux, il traitera quelques protocoles de sécurité, et divers mécanismes et méthodes de protection qui ont pour but de faire face aux menaces et attaques qui visent les systèmes informatiques des entreprises.
- Ce nouveau chapitre portera sur les vulnérabilités de la sécurité des réseaux. Nous présenterons les diverses menaces qui peuvent affecter les infrastructures numériques, qu'elles soient actives ou passives. Nous définissons aussi des attaques réseau et logicielles, expliquant leurs types et la manière dont elles peuvent mettre en danger la confidentialité des systèmes informatiques.
- Ce dernier chapitre de ce travail sera consacré à la présentation d'une architecture réseau d'entreprise proposée, où notre objectif est de sécuriser le réseau LAN dans sa communication avec le réseau WAN. On met au point une stratégie multiprotocole, ainsi que l'implémentation d'un tunnel VPN IPsec pour des communications privées et une zone de service proposée aux utilisateurs du réseau WAN. Nous expliquerons la configuration et les équipements utilisés.

Enfin, dans la conclusion générale, nous ferons un récapitulatif du travail effectué en donnant ensuite quelques perspectives.

Chapitre I : Généralités sur les réseaux informatiques

Préambule

Dans un monde de plus en plus interconnecté, les réseaux informatiques jouent un rôle essentiel dans la communication, le partage de données et le fonctionnement des systèmes numériques. Des réseaux de petite taille aux grandes infrastructures d'entreprise, les réseaux facilitent la transmission d'informations et permettent une interconnexion fluide entre les appareils.

Dans ce chapitre, nous mettons en évidence les fondements des réseaux informatiques, leur classification, leurs architectures et les technologies qui les sous-tendent, afin de mieux comprendre leur impact et leur fonctionnement.

I.1. Définition d'un réseau informatique

Un réseau informatique est un ensemble de périphériques informatiques (soft et hard) situés à distance les uns des autres ou bien dans une même pièce, connectés entre eux grâce à des liaisons de transmission afin d'échanger des informations et partager des ressources.

I.2. Objectif d'un réseau informatique

Un réseau informatique peut avoir plusieurs objectifs :

- **Partage de ressources :** fichiers, applications, matériels (imprimantes, caméras de surveillance), connexion à Internet.
- **Communication entre personnes :** courrier électronique, messagerie instantanée…
- **Communication entre processus :** liaison entre ordinateurs industriels.
- **Accès universel à l'information :** bases de données en réseau.
- **Jeux en ligne :** support pour les jeux multijoueur, etc.

I.3. Classification des réseaux informatiques

Nous allons classer les réseaux informatiques selon trois catégories :

I.3.1. Étendue géographique

I.3.1.1. Réseaux locaux

Les réseaux locaux, ou Local Area Network (LAN) en anglais, désignent des infrastructures de communication permettant l'interconnexion des équipements informatiques au moyen de liaisons à haut débit, au sein d'une zone géographique restreinte. Ils sont généralement déployés pour relier les dispositifs d'une même organisation, étage d'immeuble, voire d'un seul bureau.

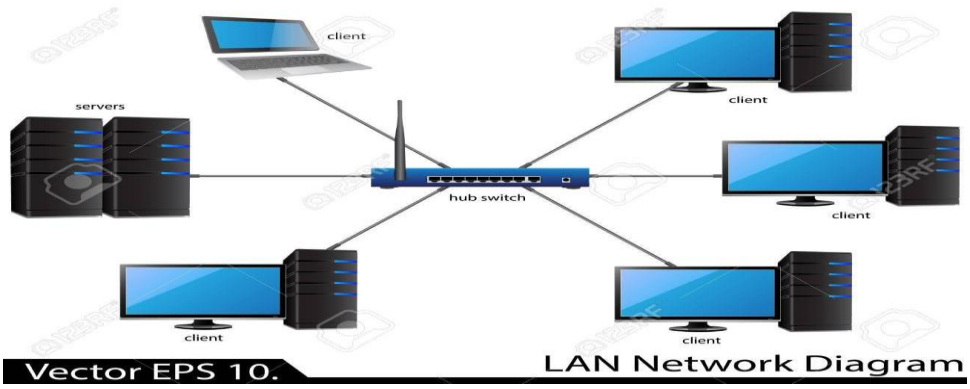

Figure 1: Un réseau LAN

I.3.1.2. Réseaux métropolitains

Les réseaux métropolitains (en anglais MAN : Metropolitan Area Network) couvrent une superficie limitée généralement d'environ 200 km². Ils sont chargés de concentrer le trafic en provenance des réseaux locaux, de gérer l'interconnexion avec le réseau public et d'offrir leurs propres services, comme les réseaux locaux virtuels et le stockage à distance de données informatiques. Les réseaux métropolitains peuvent, par exemple, servir pour relier les différents bâtiments d'un hôpital, d'une université ou d'une entreprise.

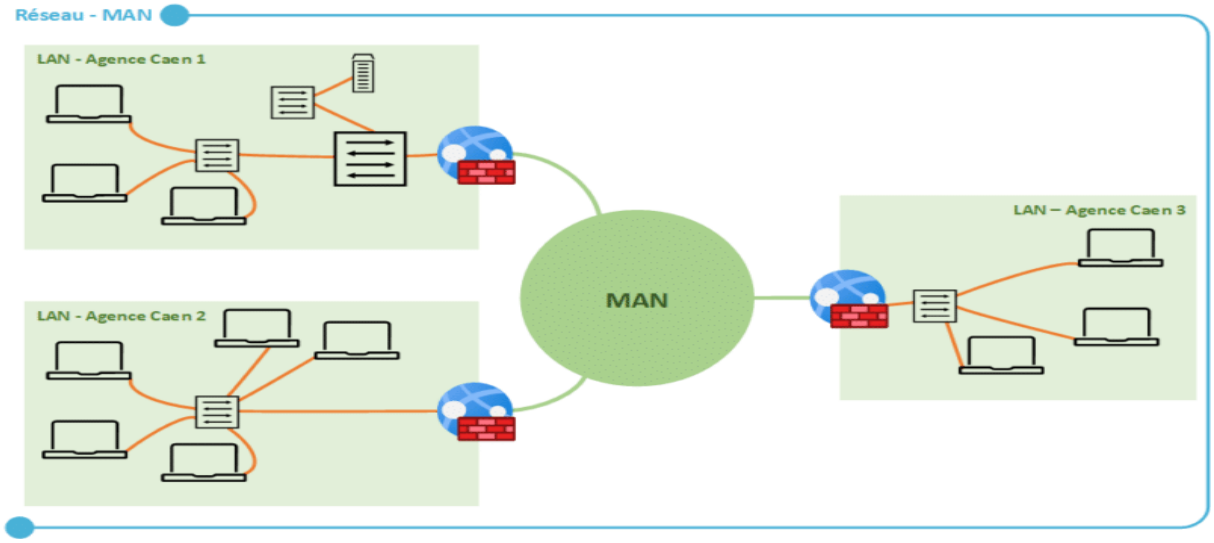

Figure 2: Un réseau MAN

I.3.1.3. Réseaux publics

Un réseau public (en anglais WAN : Wide Area Network) est un réseau de communication qui fournit des services de transmission de données à travers un pays, un continent, voire la planète. Un réseau public peut être établi en reliant deux ou plusieurs réseaux métropolitains pour assurer les

communications. Les réseaux publics utilisent des liens de communication qui consistent en des liaisons louées ou en fibre optique.

Figure 3: Un réseau WAN

I.3.2. Architecture réseau

I.3.2.1. Réseaux pair-à-pair

Un réseau pair-à-pair (peer-to-peer en anglais, abrégé P2P) est une technologie de réseau informatique décentralisé où chaque entité est à la fois client et serveur. Contrairement au réseau client-serveur, tous les ordinateurs du réseau sont connectés les uns aux autres et partagent des ressources telles que des fichiers, des applications et des programmes.

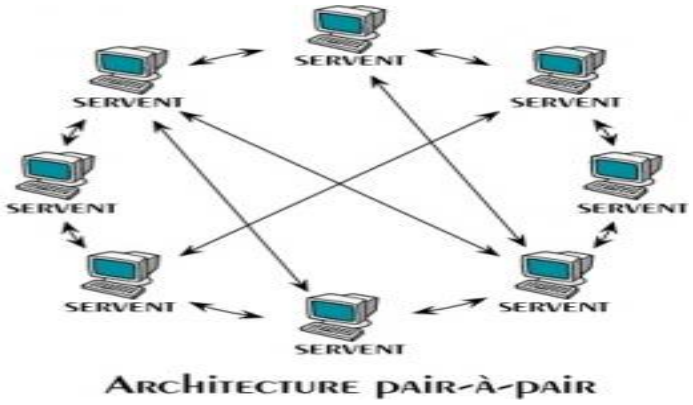

Figure 4: Un réseau P2P

I.3.2.2. Réseaux client-serveur

Le modèle client-serveur, est un modèle informatique qui s'applique à une association bipoint où interviennent deux processus d'application, le client et le serveur. Le client émet une demande de service à un serveur ; le serveur reçoit alors une requête l'informant du service à effectuer, lorsque le

traitement du service par le serveur est terminé, ce dernier envoie la réponse au client et le client reçoit cette réponse sous la forme d'une confirmation.

Dans ce modèle de communication, le temps de traitement de la requête du client, utilisé par le serveur est souvent indéterminé, puisqu'il dépend fortement de la charge du serveur au moment de la réception de l'indication de demande de service. [1]

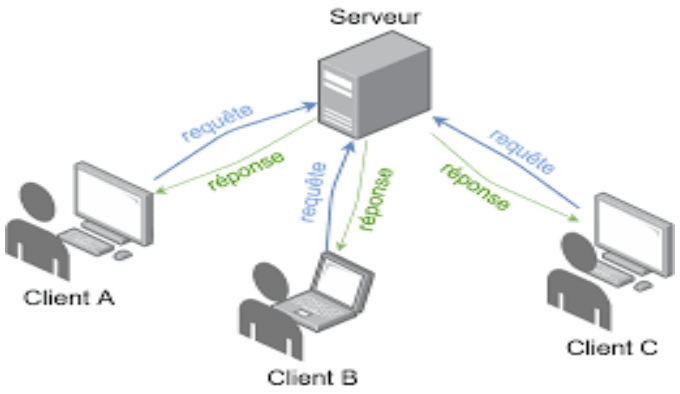

Figure 5: Un réseau client-serveur

I.3.3. Topologies

La topologie d'un réseau local désigne la manière dont les équipements sont interconnectés entre eux par des supports physiques. Et parmi les topologies existantes on distingue :

I.3.3.1. Topologie en bus

Elle est simple à mettre en œuvre, peu coûteuse et permet d'étendre facilement le réseau en ajoutant de nouveaux équipements. Cependant, en cas de rupture du câble principal, l'ensemble du réseau tombe en panne.

Dans cette topologie, chaque poste reçoit l'information mais seul le poste pour lequel le message est destiné traite l'information.

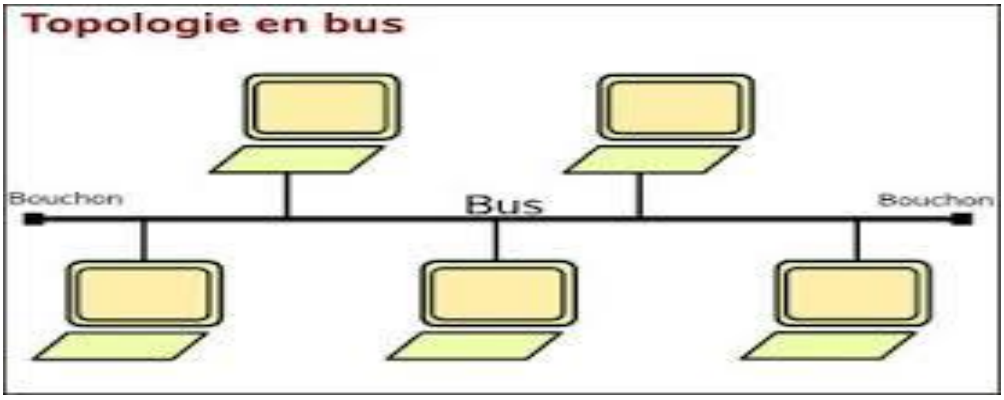

Figure 6: La topologie en bus

I.3.3.2. Topologie en anneau

Cette topologie présente un avantage majeur par rapport à celle en bus : il n'y a aucun risque de collision, car les ordinateurs communiquent chacun à leur tour, donc on a une boucle sur laquelle chaque ordinateur va avoir la parole successivement.

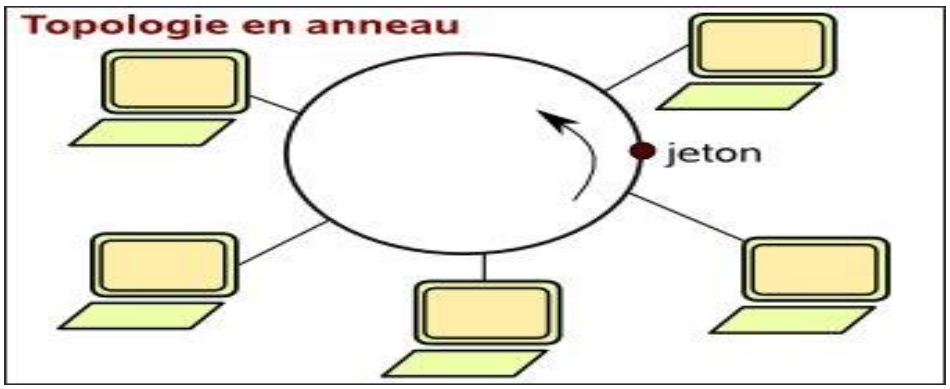

Figure 7: La topologie en anneau

I.3.3.3. Topologie en étoile

C'est la topologie la plus courante, où les ordinateurs sont reliés à un serveur central appelé concentrateur. Cette topologie permet d'ajouter facilement des équipements et facilite la gestion du réseau. En revanche elle est coûteuse. Une connexion défectueuse n'affecte pas l'ensemble du réseau. Cependant, si le concentrateur présente une défaillance, tous les ordinateurs connectés ne peuvent plus communiquer entre eux.

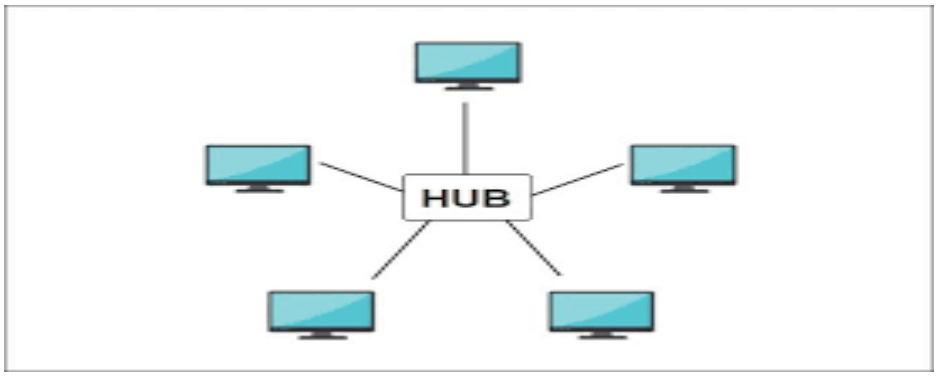

Figure 8: La topologie en étoile

I.3.3.4. Topologie maillée

La topologie maillée est un type de topologie de réseau dans lequel chaque nœud est entièrement connecté à tous les autres nœuds via une liaison dédiée.

L'interconnexion est totale, ce qui garantit une fiabilité optimale du réseau. En revanche, cette solution est coûteuse en câblage.

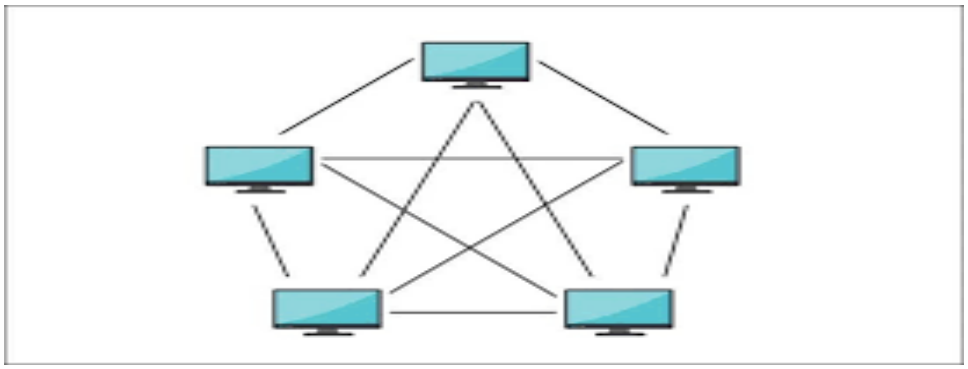

Figure 9: La topologie maillée

I.4. Supports de transmission

Dans un monde où les communications numériques sont essentielles, la transmission des données joue un rôle crucial dans le fonctionnement des réseaux informatiques. Afin de transmettre des informations d'un point à un autre, il faut un canal qui servira de chemin pour le passage de ces informations, ce canal est appelé canal de transmission ou support de transmission.

Dans un réseau informatique, on distingue deux catégories de supports de transmission :

I.4.1. Supports de transmission filaires

I.4.1.1. Câbles coaxiaux

Le câble coaxial est le premier support utilisé par les réseaux locaux. Il est composé d'une partie centrale « âme » qui est un fil en cuivre, d'une enveloppe isolante, d'un blindage métallique tressé et d'une gaine extérieure.

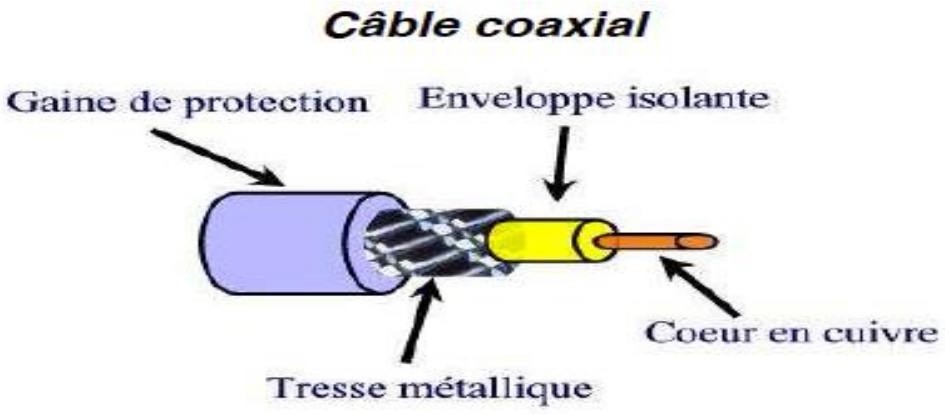

Figure 10: Un câble coaxial

I.4.1.2. Câbles à paires torsadées

Après le câble coaxial, la paire de fils torsadés a été la plus utilisée dans l'installation de réseaux locaux. La paire torsadée, comme son nom l'indique, est constituée de deux fils torsadés en cuivre, protégés chacun par une enveloppe isolante.

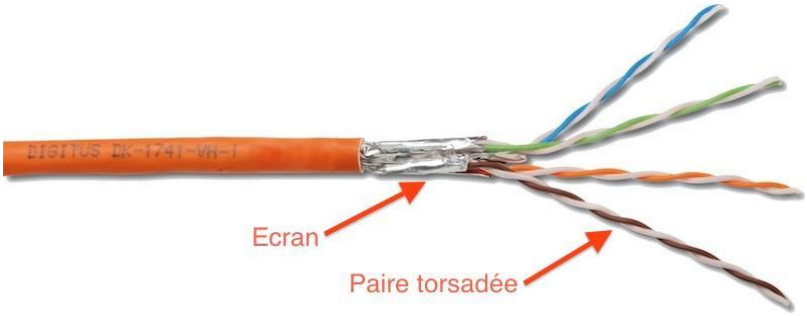

Figure 11: Un câble à paire torsadée

I.4.1.3. Câbles à fibre optique

La fibre optique est une technologie qui permet de transmettre des données à très haute vitesse en utilisant des fils en verre ou en plastique très fins. Contrairement aux câbles en cuivre, qui transmettent les signaux électriques, les câbles en fibre optique transmettent les données sous forme de signaux lumineux.

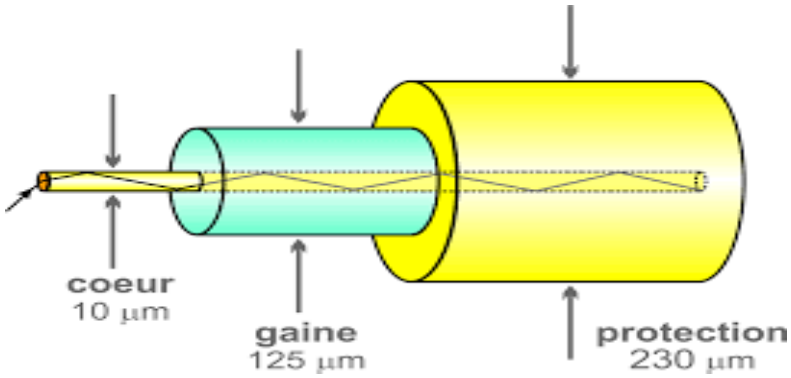

Figure 12: Un câble à fibre optique

I.4.2. Supports de transmission sans fil

I.4.2.1. Liaisons infrarouges

La transmission des données par faisceau lumineux rouge repose sur une technologie efficace mais sensible aux interférences lumineuses. Grâce à la production en grande quantité des composants, cette solution reste abordable, et bien adaptée aux environnements intérieurs. Cependant, son

utilisation en extérieur est limitée en raison des perturbations atmosphériques qui peuvent affecter la qualité du signal. [2]

I.4.2.2. Laser

Comme pour la transmission en infrarouge, cette technique nécessite un champ de visibilité direct, sensible au problème d'alignement entre le laser et la photodiode. Cependant, elle est résistante aux interférences et aux perturbations, mais sensible aux conditions atmosphériques.

I.4.2.3. Ondes radios terrestres

Les technologies de transmission par radio sont aujourd'hui privilégiées, quelle que soit la taille du réseau. Plutôt que les ondes à bande étroite, les systèmes modernes adoptent le spectre étalé (Spread Spectrum), qui offre une meilleure résistance aux interférences. Ces réseaux ont de nombreuses applications. Par exemple, des ponts sans fil facilitent l'interconnexion de réseaux locaux sans recourir à des supports physiques limités (filaires). L'essor des ordinateurs portables et des périphériques mobiles a largement contribué à la démocratisation des connexions radio, notamment via le Bluetooth et le Wi-Fi. [2]

I.5. Techniques de transfert des données

I.5.1. Commutation de circuits

La commutation de circuit est une méthode de transfert de données consistant à établir un circuit dédié au sein d'un réseau. Dans ce type de scénario, un circuit constitué de lignes de communication entre un nœud émetteur et un nœud récepteur, est réservé le temps de la communication afin de permettre le transfert de données, et est libéré à la fin de la transmission. [3]

I.5.2. Commutation de paquets

Lors d'une transmission de données par commutation de paquets, les données à transmettre sont découpées en paquets de données (nous parlons de la segmentation), puis émis indépendamment sur le réseau. Les nœuds du réseau sont libres de déterminer la route de chaque paquet individuellement, selon leur table de routage. Les paquets ainsi émis peuvent emprunter des routes différentes et sont réassemblés à l'arrivée par le nœud destinataire. Dans ce type de scénario, les paquets peuvent arriver dans un ordre différent de l'ordre d'envoi, et peuvent éventuellement se perdre. [3]

I.6. Modèles de communication

I.6.1. Modèle OSI

C'est un modèle de référence défini par ISO en 1984, nommé Open System Interconnection destiné à normaliser les échanges entre deux machines. Il définit ainsi ce que doit être une communication réseau complète. L'ensemble du processus est ainsi découpé en sept couches hiérarchiques. Il définit précisément les fonctions associées à chaque couche. [4]

Les couches sont réparties selon les utilisations suivantes :

- Les couches 1 à 3 sont orientées transmission.
- La couche 4 est une couche intermédiaire.
- Les couches 5 à 7 sont orientées traitement.

Le rôle de chaque couche est :

- **Couche 1 :** Physique

La couche physique se charge de la transmission et de la conversion des signaux en bits sur un canal de communication, gère aussi les caractéristiques physiques (câbles, fréquences radio, modulation). En pratique, elle est toujours réalisée par un circuit électronique spécifique.

- **Couche 2** : Liaison de données

Cette couche assure la transmission d'informations entre deux ou plusieurs systèmes immédiatement adjacents. Elle détecte et corrige, dans la mesure du possible les erreurs issues de la couche physique. Les objets échangés sont souvent appelés trames.

- **Couche 3** : Réseau

La couche réseau contrôle et assure la connectivité et la sélection du trajet entre deux systèmes d'extrémité qui peuvent être situés dans des réseaux géographiquement dispersés. Nous trouvons à ce niveau des notions de routage et d'adressage. À ce niveau les informations traitées sont des paquets.

- **Couche 4 :** Transport

La couche transport gère les communications entre processus. Cela signifie qu'un programme, une application, utilise la couche 4 pour établir une transmission avec une autre application. La couche transport accepte des données de la couche supérieure, les divise en unités plus petites si c'est nécessaire, les transmet à la couche réseau, et s'assure qu'elles arrivent correctement à l'autre bout.

➢ **Couche 5 :** Session

Permet aux utilisateurs d'établir des sessions. Une session offre divers services, parmi lesquels, la gestion du dialogue (suivi de la transmission) et la synchronisation (gestion de points de reprise permettant aux longues transmissions de reprendre là où elles en étaient suite à une interruption).

➢ **Couche 6 :** Présentation

À la différence des couches les plus basses qui sont principalement concernées par le déplacement des bits, la couche de présentation s'intéresse à la syntaxe et à la sémantique (signification des programmes) des informations transmises.

➢ **Couche 7 :** Application

La couche applications contient une variété de protocoles qui sont utiles aux utilisateurs. HTTP (HyperText Transfer Protocol), qui forme la base du World Wide Web, est un protocole d'application largement utilisé. Lorsqu'un navigateur doit afficher une page Web, il transmet le nom de la page au serveur au moyen du protocole HTTP. Le serveur envoie la page en guise de réponse. D'autres protocoles d'application sont utilisés pour le transfert de fichiers, le courrier électronique et les nouvelles.

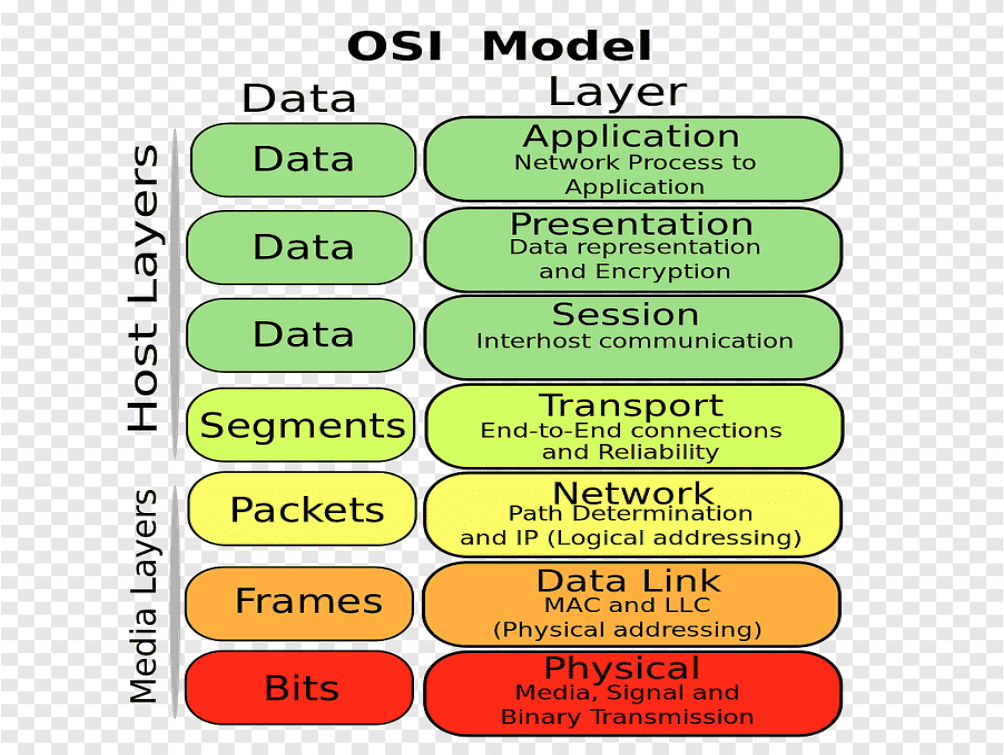

Figure 13: Le modèle OSI

I.6.2. Modèle TCP/IP

Le modèle TCP/IP (Transmission Control Protocol / Internet Protocol) est un modèle en 4 couches, qui décrit la fonctionnalité des protocoles qui constituent la suite de protocoles TCP/IP. Ces protocoles, qui sont présents sur les hôtes émetteurs et récepteurs, interagissent pour fournir une livraison de bout en bout sur l'inter-réseau. [4]

- **Couche Network Access (accès réseau)**

Elle n'a pas de contenu défini dans le modèle TCP/IP. Elle est responsable des trames émises et reçues et définit, sur son interface avec la couche Internet, les caractéristiques de la trame en question. Tout type de réseau physique peut être utilisé ici.

- **Couche Internet**

Elle s'occupe de l'adressage logique, de l'encapsulation des paquets de données et du routage. Le protocole central de cette couche est IP (pour Internet Protocol), mais d'autres protocoles et services sont présents dans cette couche comme le protocole ICMP (pour Internet Control Message Protocol) qui gère entre autres les fonctions de diagnostic du réseau.

- **Couche Host-to-Host (transport)**

Souvent qualifiée de couche transport, mais qui regroupe également des fonctions de la couche session du modèle OSI, fournit principalement deux ensembles de services : TCP (Transmission Control Protocol), service orienté connexion avec acquittement des données transmises, et UDP (User Datagram Protocol), service non connecté où chaque paquet émis est indépendant des autres.

- **Couche Process (application)**

Souvent appelée couche application, définit les protocoles utilisés pour l'échange de données par exemple FTP (File Transfer Protocol) pour le transfert de fichiers ou SMTP (Simple Mail Transfer Protocol) pour l'envoi de courriels.

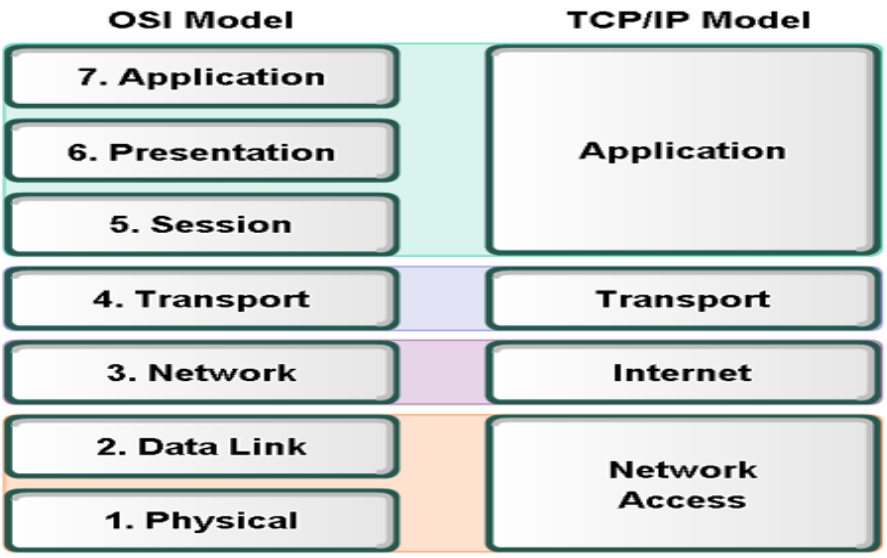

Figure 14: Le modèle TCP/IP

I.7. Technologie Ethernet

Ethernet est une technologie de réseau local (LAN) largement utilisée pour connecter des appareils dans un réseau filaire. Elle définit les normes pour la transmission de données entre des dispositifs connectés, tels que les ordinateurs, les imprimantes, les serveurs et les routeurs, au sein d'un même réseau.

Ethernet est régie par la norme IEEE 802.3 et est l'une des technologies de réseau les plus répandues dans le monde.

I.8. Intranet

Le mot intranet est composé de deux mots **«** Intra » signifie « intérieur **»** en latin et « net » fait référence à « Internet » en anglais, l'ensemble signifie « réseau interne ». C'est la révolution culturelle d'Internet à l'intérieur de l'entreprise.

L'Intranet est un réseau d'entreprise ou d'organisation qui relie les employés internes d'un même réseau entre eux et permet des échanges au sein de la même entreprise. L'accès des participants est contrôlé par un nom d'utilisateur et un mot de passe donné par l'entreprise. Tous les utilisateurs de l'Intranet n'ont en effet pas accès à tous les domaines de l'entreprise. La limitation des droits d'accès peut être utilisée, par exemple, pour rendre l'information disponible uniquement à certains départements.

Grâce à certaines applications Intranet, les employés peuvent fournir des dossiers, des messages, fixer des rendez-vous ou transmettre d'autres informations à l'ensemble des employés de

l'entreprise ou à des groupes spécifiques de personnes au sein de la société et cela simplement en quelques clics.

L'avantage majeur de cette technologie est la sécurité, l'échange rapide de l'information et l'archivage des données, clairement catégorisées et structurées de manière logique.

I.9. Extranet

L'extranet est un réseau informatique qui permet à une entreprise ou une organisation de partager de manière sécurisée des informations ou des ressources avec des utilisateurs externes comme des partenaires, les clients, les fournisseurs ou les internes, comme les employés de la même entreprise.

Ces utilisateurs externes n'ont pas accès à l'ensemble de l'Intranet (les utilisateurs internes), mais seulement à certaines zones.

Dans un Extranet, les contrôles d'accès ainsi que les groupes et les rôles des utilisateurs déterminent également à quelles informations les participants peuvent accéder. Par exemple, les fournisseurs et les clients ont des droits d'accès différents.

I.10. Adresse IP (Internet Protocol)

I.10.1 Définition

L'adresse logique ou l'adresse IP (Internet Protocol Address) est une suite de chiffres attribuée à chaque appareil connecté à un réseau informatique ou à Internet. Les adresses IP permettent d'identifier et de différencier des appareils en ligne, y compris les ordinateurs, les téléphones portables et les imprimantes. Elle est utilisée pour acheminer les paquets de données sur Internet et sur d'autres réseaux.

I.10.2. Versions du protocole IP

Le protocole IP comporte deux versions :

- **IPv4 (Internet Protocol Version 4)**

C'est la version la plus utilisée. Elle utilise des adresses IP de 32 bits, exprimées sous la forme de quatre octets séparés par des points.

- Par exemple : 192.168.0.1

Elle offre environ 4,3 milliards d'adresses uniques, ce qui était suffisant lorsque le protocole a été développé. Cependant, avec la croissance rapide d'Internet, le nombre d'adresses IPv4 disponibles a rapidement été épuisé.

- **IPv6 (Internet Protocol Version 6)**

Elle a été développée pour résoudre cette limitation en introduisant des adresses IP de 128 bits. Ces adresses sont exprimées sous la forme de huit groupes de quatre chiffres hexadécimaux, séparés par des deux-points.

- Par exemple : 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Les adresses IPv6 offrent un espace d'adressage beaucoup plus vaste, permettant un nombre pratiquement illimité d'adresses IP uniques.

I.10.3. Classes d'adresse IPv4 et leurs plages

- **Classe A** : Le premier octet a une valeur comprise entre 1 et 126, il désigne le numéro de réseau. Les trois autres octets correspondent à l'adresse de l'hôte.
- **Classe B :** Le premier octet a une valeur comprise entre 128 et 191. Les deux premiers octets désignent le numéro de réseau. Les deux autres octets correspondent à l'adresse de l'hôte.
- **Classe C** : Le premier octet a une valeur comprise entre 192 et 223. Les trois premiers octets désignent le numéro de réseau. Le dernier octet correspond à l'adresse de l'hôte.
- **Classe D** : sa plage d'adressage est de 224 à 239. Soit 3 bits de poids fort égaux à 1. Il s'agit d'une zone d'adresses dédiées aux services de multidiffusion vers des groupes d'hôtes.
- **Classe E** : Le premier octet a une valeur comprise entre 240 et 255. Il s'agit d'une zone d'adresses réservées aux expérimentations. Ces adresses ne doivent pas être utilisées pour adresser des hôtes ou des groupes d'hôtes.

Le tableau ci-dessous montre la répartition des adresses IPv4 selon leurs classes, plages et leurs masques sous réseau :

Classe	Plage d'adresse	Premier octet	Masque sous réseau par défaut	Utilisation
A	1.0.0.0 - 126.255.255.255	1 - 126	255.0.0.0 / 8	Grands réseaux (FAI, Multinationales)
B	128.0.0.0 - 191.255.255.255	128 - 191	255.255.0.0 / 16	Réseaux de taille moyenne (universités, grandes entreprises)
C	192.0.0.0 - 223.255.255.255	192 - 223	255.255.255.0 / 24	Petits réseaux(PME, domiciles)
D	224.0.0.0 - 239.255.255.255	224 - 239	pas de masque réseau	Diffusion de paquets à plusieurs hôtes (VoIP, streaming)
E	240.0.0.0 - 255.255.255.255	240 - 255	pas de masque réseau	Réservé aux tests et à la recherche

Tableau 1: Les classes d'adresse IPv4 et leurs plages

I.11. Routage IP

Le routage IP est un processus clé dans les réseaux informatiques qui permet l'échange des données entre différents réseaux en utilisant des adresses IP. Chaque appareil possède une adresse IP unique, et les routeurs jouent un rôle central en examinant ces adresses pour déterminer le meilleur chemin à suivre. Ils utilisent des tables de routage, qui contiennent des informations sur les réseaux disponibles et les passerelles à utiliser. [5]

Ces tables peuvent être configurées manuellement (routage statique) ou mises à jour automatiquement grâce à des protocoles, et les types de routage sont :

- **Routage statique**

Le routage statique repose sur une configuration manuelle des routes par un administrateur réseau. Les chemins sont définis explicitement dans la table de routage des routeurs, ce qui le rend simple à mettre en œuvre pour de petits réseaux. Cependant, il ne s'adapte pas aux changements de topologie et nécessite une intervention manuelle en cas de panne ou d'ajout de nouveaux réseaux.

- **Routage dynamique**

Le routage dynamique utilise des protocoles (comme RIP, OSPF ou BGP) pour permettre aux routeurs d'échanger automatiquement des informations sur les réseaux disponibles. Il s'adapte aux changements de topologie, comme les pannes ou l'ajout de nouveaux routeurs, sans intervention manuelle. Il est idéal pour les grands réseaux complexes, mais nécessite plus de ressources et une configuration plus approfondie.

- **Routage par défaut**

Le routage par défaut est une forme simplifiée de routage où un routeur envoie tout le trafic dont il ne connaît pas la destination vers une passerelle par défaut (ou Gateway). Il est souvent utilisé pour connecter un réseau local à Internet, évitant ainsi de configurer des routes spécifiques pour chaque destination externe.

Bien que pratique, il peut entraîner un routage sous-optimal si mal configuré.

Conclusion

Dans ce premier chapitre, nous avons exposé certaines notions de base des réseaux informatiques. Grâce à leur fiabilité en matière de communication, ils sont devenus indispensables dans le milieu professionnel actuel.

Nous avons ensuite illustré les divers moyens de transmission ainsi que les méthodes de commutation qui simplifient l'échange d'informations entre plusieurs utilisateurs. Puis, nous avons examiné les divers niveaux des architectures protocolaires des réseaux (le modèle OSI et le TCP/IP), qui synthétisent les diverses fonctionnalités employées dans ces réseaux.

Ensuite, nous avons présenté la technologie Ethernet qui est la plus couramment utilisée actuellement, ainsi que la notion Intranet et Extranet.

Dans le chapitre suivant, nous allons voir la sécurité des réseaux informatiques, en explorant les mécanismes associés afin de sécuriser un réseau informatique.

Chapitre II : Sécurité informatique

Préambule

Aujourd'hui, les technologies numériques jouent un rôle essentiel dans presque tous les domaines d'activité. Pour cette raison, la sécurité informatique est devenue un sujet fondamental afin de faire face aux menaces et aux attaques qui deviennent de plus en plus complexes.

Dans ce chapitre, nous visons à définir les principes fondamentaux de la sécurité informatique, en mettant en évidence les notions de sécurité comme les mécanismes et les protocoles de sécurité. Une bonne compréhension de ces solutions permet d'élaborer des stratégies de protection efficaces qui assurent la confidentialité, l'intégrité et la disponibilité des données.

II.1. Sécurité dans un réseau informatique

II.1.1. Définition

La sécurité informatique est l'ensemble des techniques et d'outils qui visent à garantir la protection des données sensibles des systèmes informatiques contre les menaces, les risques ou tout accès non autorisé, notamment via Internet.

II.1.2. Objectifs de la sécurité informatique

Les objectifs de la sécurité informatique définissent les besoins des utilisateurs en matière de protection des systèmes. Il existe trois principaux objectifs à garantir qui sont :

• La confidentialité

La confidentialité des données est essentielle pour garantir la protection des informations sensibles. Elle signifie que l'accès aux informations n'est permis que par des personnes autorisées. Il existe certaines mesures à mettre en place pour garantir la confidentialité des informations telles que :

- ***Le chiffrement :*** c'est-à-dire que les données doivent être chiffrées pendant leur stockage et leur transmission.
- ***Contrôles d'accès :*** utilisation de mots de passe robustes, de l'authentification à deux facteurs, etc.
- ***Politiques de confidentialité :*** qui doivent être établies pour tous les employés.

• L'intégrité

En termes de sécurité, l'intégrité signifie que les données reçues ou stockées dans les réseaux informatiques ne peuvent être détruites ou modifiées que par des personnes autorisées.

• **La disponibilité**

La disponibilité a pour objectif de garantir l'accès à une application, un système et de s'assurer que l'information soit disponible à n'importe quel moment.

À ces trois derniers critères, nous ajoutons :

• **L'identification et l'authentification :** cela consiste à vérifier l'identité annoncée et à s'assurer de la non-usurpation de l'identité d'une entité. Elle garantit que la personne qui communique est bien celle qu'elle prétend être.

• **La non-répudiation :** c'est le fait de ne pas pouvoir nier ou rejeter qu'un événement a eu lieu.

II.2. Mécanismes de sécurité

II.2.1. Firewall

Un firewall, ou pare-feu en français, est un mécanisme de sécurité dont la fonction est dérivée de son nom ; protéger votre appareil de toute interférence externe ou toute pénétration de pirate informatique.

Il contrôle le trafic entre votre réseau sécurisé (interne) et tout autre réseau non sécurisé (externe) comme Internet. Il filtre les flux de données entrants et sortants d'un système informatique en fonction d'un ensemble de règles de protection de base.

Ces règles contrôlent la manière dont un pare-feu régule le flux du trafic web à travers votre réseau interne et vos périphériques informatiques privés. Quel que soit leur type, tous les pare-feu peuvent filtrer à partir d'une combinaison des éléments suivants [6] :

- **La source :** d'où provient une tentative de connexion.
- **La destination :** où une tentative de connexion est censée aller.
- **Le contenu :** ce qu'une tentative de connexion essaie d'envoyer.
- **Protocoles par paquets :** le « langage » utilisé par une tentative de connexion pour transmettre son message. Parmi les protocoles réseau que les hôtes utilisent pour « parler » entre eux nous trouvons les protocoles TCP/IP, principalement utilisés pour communiquer sur Internet et au sein des intranets/sous-réseaux.
- **Les protocoles d'application :** les protocoles courants comprennent HTTP, Telnet, FTP, DNS et SSH, etc.

Nous pouvons le considérer comme un agent de sécurité à l'entrée d'une entreprise, qui vérifie l'identité de chaque personne tentant d'entrer ou de sortir de cette entreprise.

II.2.2. Proxys

Un serveur proxy est un ordinateur ou un réseau qui joue le rôle d'un intermédiaire entre les utilisateurs (les machines locales) et Internet.

En général, lorsque vous consultez une page web, il suffit d'ouvrir un navigateur et de taper l'adresse de la page que vous voulez, et vous allez la récupérer à partir de son serveur web, mais dans le cas où vous utilisez un serveur proxy, l'utilisateur va d'abord se connecter à ce serveur et lui envoyer sa requête, puis le proxy va à son tour transmettre le message au serveur distant, télécharger les informations et les renvoyer à l'utilisateur afin de garantir la confidentialité de l'utilisateur en masquant son adresse IP.

II.2.3. VPN

II.2.3.1. Définition

Le VPN (Virtual Private Network), ou réseau privé virtuel, est un modèle essentiel dans les architectures modernes de sécurité. Il est constitué d'un ensemble de LAN privés et une fois que le VPN est activé, un tunnel sécurisé est constitué entre ces LAN et les relie à travers l'Internet, dans lesquels les données sont cryptées et restent privées et aucune journalisation n'est impliquée.

Ce tunnel virtuel sert à cacher et à rendre inexploitables toutes les données de navigation qui transitent par lui au moyen d'un processus de chiffrement.

II.2.3.2. Types de VPN

II.2.3.2.1. VPN site to site

Un VPN site à site est une connexion configurée entre deux ou plusieurs réseaux distants de manière à faire en sorte qu'ils puissent communiquer comme s'ils étaient sur le même réseau et qu'un simple routeur les séparait, tels que les réseaux d'entreprises et les réseaux des filiales. De nombreuses entreprises utilisent des VPN site à site pour connecter en toute sécurité leur réseau central à celui de leurs sites distants, d'une manière transparente pour communiquer et partager des ressources, créant ainsi un seul et même réseau.

II.2.3.2.2. VPN d'accès à distance

Un VPN d'accès à distance, également appelé VPN client à site, comme son nom l'indique, fournit un accès crypté aux ressources à distance. Les entreprises utilisent aussi ce type de VPN car il permet à leurs employés d'accéder à leur réseau privé lorsqu'ils voyagent ou travaillent à domicile.

II.2.3.2.3. VPN personnel

Le VPN personnel, parfois aussi appelé VPN « grand public » ou « commercial », crypte votre connexion, masque votre identité en ligne, et vous permet de simuler votre localisation géographique, c'est-à-dire, il agit comme un intermédiaire entre votre appareil et les services en ligne auxquels vous souhaitez accéder. Un VPN personnel diffère d'un VPN d'accès à distance en ce qu'il ne vous donne pas accès à un réseau privé.

II.2.3.2.4. VPN mobile

Alors que les VPN d'accès à distance vous permettent de vous connecter à un réseau local depuis n'importe où, ils supposent que l'utilisateur restera à un seul endroit. Si l'utilisateur se déconnecte, le tunnel IP se ferme. Un VPN mobile est une meilleure option qu'un VPN d'accès à distance si l'utilisateur risque de ne pas avoir une connexion stable sur le même réseau pendant toute la session. Avec un VPN mobile, la connexion VPN persiste même si l'utilisateur change de réseau Wi-Fi ou cellulaire, perd la connectivité ou éteint son appareil pendant un certain temps.

II.2.4. VLAN

II.2.4.1. Définition

Un VLAN ou réseau local virtuel est un réseau informatique logique qui offre un moyen de regrouper plusieurs stations de travail indépendamment. Un groupe de stations dans un VLAN communiquent comme s'ils étaient reliés au même câble. Il permet de diviser un seul réseau physique en deux ou plusieurs réseaux logiques.

II.2.4.2. Types des VLAN

Il existe quartes types différents de VLAN :

- **VLAN par défaut :** tous les ports de commutateurs font partie du VLAN par défaut juste après le démarrage initial du commutateur.
- **VLAN natif :** est un VLAN spécial effectué à un port Trunk 802.1.Q dans lequel le trafic non étiqueté traverse sans aucune balise VLAN. Il est utilisé pour partager des informations par certains protocoles comme VTP. Pour des raisons de sécurité, il est conseillé de le modifier afin qu'il ne correspond pas au VLAN par défaut.
- **VLAN de données :** c'est configuré pour transmettre le trafic généré par l'utilisateur.
- **VLAN de gestion :** c'est configuré pour accéder aux fonctionnalités de gestion d'un commutateur.

II.2.4.3. Attribution des VLAN

Nous avons classé les VLAN selon trois niveaux comme suite [7] :

- **VLAN de niveau 1 (ou VLAN par port) :** chaque port du commutateur est affecté à un VLAN, donc chaque carte réseau est affectée à un VLAN en fonction de son port de connexion.
- **VLAN de niveau 2 (ou VLAN par adresse MAC) :** chaque adresse MAC est affectée à un VLAN, donc chaque port du commutateur doit être affecté dynamiquement à un VLAN en fonction de l'adresse MAC de la carte réseau qui y est connectée.
- **VLAN de niveau 3 (ou VLAN par adresse IP) :** chaque carte réseau est affectée à un VLAN en fonction de son adresse IP, donc chaque port du commutateur doit être affecté dynamiquement à un VLAN en fonction de l'adresse IP de la carte réseau qui y est connectée.

II.2.4.4. Liens Trunk

Les liens Trunk sont des connexions physiques entre plusieurs switches permettant de faire transiter plusieurs VLAN sur une seule connexion physique (même port). Les ports Trunk permettant d'indiquer dans chaque trame envoyée le numéro de VLAN auquel elle appartient et cela grâce à des en-têtes que le switch ajoute à la trame.

Cet en-tête contient plusieurs données, telles que « Les Tag VLAN », ces tags VLAN ajoutés aux paquets de données indiquent à quel réseau virtuel les paquets appartiennent. À la fin, les switches analysent ces étiquettes et font circuler les paquets de données vers le bon VLAN.

II.2.4.5. Routage inter-VLAN

Il consiste à faire communiquer deux ou plusieurs VLAN, ce routage est faisable en utilisant un routeur qui a traditionnellement son rôle comme un intermédiaire et fait router un ensemble de VLAN ou bien un switch de niveau trois (3) qui est capable d'effectuer les tâches de routage inter-VLAN. [8]

II.2.5. DMZ

II.2.5.1. Définition

Une DMZ ou une zone démilitarisée, est un sous-réseau isolé qui ne fait partie ni du réseau interne LAN ni d'Internet, mais sert comme un intermédiaire entre eux. Son objectif est de permettre à un réseau LAN privé d'accéder à des réseaux non fiables tels qu'Internet en toute sécurité.

La DMZ héberge des serveurs du réseau interne qui ont besoin d'être accessibles depuis l'extérieur, ce qui signifie que les personnes de l'extérieur n'ont jamais accès directement à des ressources du LAN. Ces zones sont isolées par des firewalls avec des règles de filtrage.

II.2.5.2. Types de DMZ

II.2.5.2.1. Un seul pare-feu

Dans cette architecture, un seul pare-feu avec trois interfaces est utilisé. Une interface se connecte au réseau interne LAN, l'autre au réseau externe (Internet), et la dernière sera connectée à la DMZ. Ce seul pare-feu va contrôler le trafic entre Internet et la DMZ et entre le réseau LAN et la DMZ.

Cette configuration est simple et économique, mais offre moins de sécurité par rapport aux autres configurations, car si cet unique pare-feu est compromis, cette architecture tombe (figure 15).

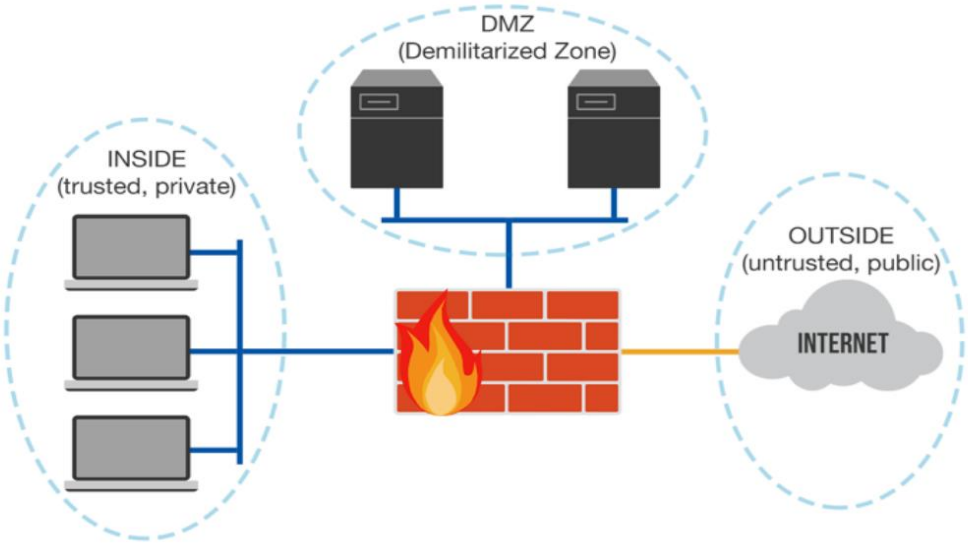

Figure 15: DMZ avec un seul pare-feu

II.2.5.2.2. Deux pare-feu

Dans cette architecture, nous utilisons deux pare-feu, créant un environnement plus sécurisé où nous configurons le premier pare-feu comme un pare-feu externe qui connecte la DMZ à l'internet, tandis que le deuxième pare-feu est configuré comme un pare-feu interne qui connecte la DMZ au réseau interne.

La figure 16 montre une DMZ avec une couche de sécurité supplémentaire, car un attaquant doit pénétrer les deux pare-feu pour accéder au réseau interne.

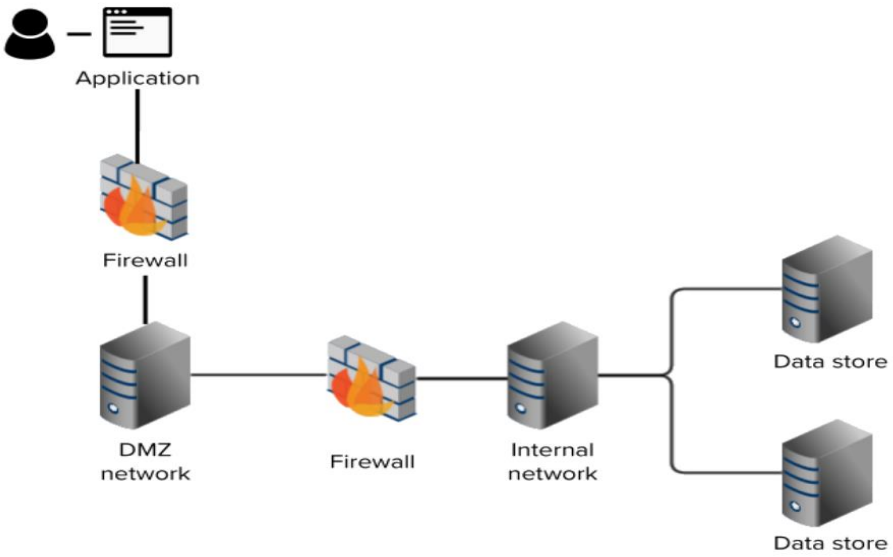

Figure 16: DMZ avec deux pare-feu

II.2.5.2.3. DMZ Basée sur le cloud

Ce type de DMZ est devenu plus courant. La DMZ est hébergée sur un cloud comme Google Cloud pour gérer des services exposés sur Internet et protéger les services et les données hébergées sur le cloud avec un accès sécurisé pour les utilisateurs distants.

II.2.6. NAT

II.2.6.1. Définition

Le Network Address Translation (NAT), ou traduction d'adresse réseau, est un mécanisme utilisé pour économiser les adresses IP et simplifier la gestion de l'adressage IP. Il permet de changer une adresse IP privée du réseau interne en la traduisant en une adresse IP publique routable. Cela permet de transporter le paquet sur des réseaux externes publics tels qu'Internet.

Ainsi, le NAT permet de masquer les adresses privées des réseaux locaux derrière une adresse publique.

II.2.6.2. Types de NAT

Il existe deux types de NAT qui sont :

- **NAT statique (SNAT)**

SNAT (Static Network Address Translation) est l'association d'une adresse IP interne à une adresse IP publique de façon fixe. C'est le pare-feu qui s'en occupe : il remplace l'adresse interne par l'adresse externe dans chaque en-tête IP du paquet qui sort du réseau.

- **NAT dynamique (DNAT)**

Le NAT dynamique permet à plusieurs adresses IP privées d'utiliser une seule adresse IP publique pour accéder à Internet. Cela s'appelle aussi « IP masquerading » et permet à plusieurs appareils d'un réseau local de partager une même adresse publique.

II.3. Autres mécanismes de sécurité

II.3.1. Cryptographie

C'est un ensemble de techniques permettant de transformer les données dans le but de masquer leur contenu, empêcher leur modification ou leur suppression et leur utilisation illégale. Cela permet d'obtenir un texte en effectuant une transformation inverse (grâce à des algorithmes de déchiffrement). Elle sert non seulement à préserver la confidentialité des données, mais aussi à garantir leur intégrité et leur authenticité. La taille des clés de chiffrement dépend de la sensibilité des données à protéger. Plus ces clés sont longues, plus le nombre de possibilités de clés est important. Par conséquent, il sera difficile de deviner la clé.

Il existe deux principes de cryptage : le cryptage symétrique, basé sur l'utilisation d'une clé privée, et le cryptage asymétrique, qui repose sur un codage à deux clés, une privée et l'autre publique. [9]

• Cryptage asymétrique

La cryptographie asymétrique ou cryptographie à clé publique, est une méthode de chiffrement qui utilise une clé publique accessible par tout le monde et une clé privée, connue uniquement de l'utilisateur pour chiffrer et déchiffrer les données.

Le chiffrement asymétrique ajoute un niveau de sécurité supplémentaire, car la clé privée d'un individu n'est jamais partagée.

• Cryptage symétrique

Le cryptage symétrique ou cryptage à clé privée est un algorithme qui utilise la même clé privée pour chiffrer et déchiffrer les données. Le chiffrement symétrique est généralement plus rapide et plus efficace, mais plus vulnérable aux attaques.

II.3.2. ACL

II.3.2.1. Définition

Les ACL (Access Control List) ou listes de contrôle d'accès, sont une collection de règles qui sont appliquées au trafic réseau afin de les filtrer, permettre ou interdire la commutation des paquets de données en fonction des règles spécifiques telles que les adresses source et destination, les protocoles de transport, les ports, etc.

Les ACL sont importantes pour établir des politiques de sécurité, gérer l'accès aux ressources du réseau et réduire les risques d'attaques. [10]

II.3.2.2. Types d'ACL

- **ACL Standard :** les listes de contrôle standard permettant de filtrer le trafic uniquement sur les adresses IP source d'un paquet de données. Ce type est le plus basique et peut être utilisé pour des installations simples, mais il n'offre pas une sécurité renforcée.
- **ACL Étendues :** sont plus utilisées que les ACL Standard, car elles offrent une plage de contrôle plus large. Elles filtrent les adresses IP source et destination des paquets de données et peuvent être également utilisées pour filtrer le trafic en fonction des protocoles comme TCP et UDP ainsi que les numéros de ports.
- **ACL nommées :** variantes des ACL Standard et/ou Étendues mais avec une attribution des noms au lieu de numéros.
- **ACL dynamiques et ACL réflexives :** utilisées pour des sessions temporaires ou un filtrage avancé.

II.3.3. Signature

La signature est un mécanisme cryptographique utilisé pour authentifier et sécuriser des fichiers, messages ou documents électroniques liés à une entité (entreprise, organisation, personne). Nous distinguons deux types de signatures essentielles :

II.3.3.1. Signature numérique

Cette signature repose sur un algorithme de chiffrement asymétrique qui utilise une clé privée pour signer et une clé publique pour vérifier la signature, donc son fonctionnement repose sur deux étapes : la création et la vérification.

D'abord, l'expéditeur transforme son document en une empreinte unique créée grâce à une fonction de hachage, puis il chiffre cette dernière avec sa clé privée et elle devient la signature numérique. Ensuite, il envoie le document avec cette signature au destinataire.

À la réception du document, le destinataire déchiffre la signature en utilisant la clé publique du signataire et vérifie si l'empreinte correspond à celle du document reçu. Si elle correspond, cela signifie que le document n'a pas été modifié et provient de l'expéditeur.

II.3.3.2. Signature logicielle

C'est un type de signature utilisée par les éditeurs de logiciels. Ils signent leur logiciel avec un certificat numérique délivré par une autorité de certification (CA). Lors de l'installation, la machine vérifie la signature, si elle est valide, l'installation continue ; sinon une alerte de sécurité s'affiche.

II.3.3.3. Certificats

Les certificats numériques sont des fichiers utilisés pour valider l'identité numérique des sites web, des adresses électroniques, des entreprises ou des individus et pour sécuriser la communication. Les clés publiques sont publiées avec un certificat numérique pour le destinataire appelé « certificat de clé publique », et délivrées par l'organisation Autorité de Certification (CA) qui signe ce certificat avec sa propre clé privée.

À l'intérieur, nous trouvons le nom du certificat et son utilisation, des informations identifiant le propriétaire de la clé publique et la clé publique elle-même, la date d'expiration et le nom de l'organisme du certificat.

II.4. Protocoles de sécurité

II.4.1. Définition

Les protocoles de sécurité sont des règles et des procédures établies pour protéger les systèmes, les données et les réseaux contre les attaques et les menaces.

II.4.2. Protocoles de chiffrement et de sécurisation de communication

II.4.2.1. IPSec (Internet Protocol Security)

IPSec est une suite de protocoles conçue pour sécuriser les communications IP (Internet Protocol) sur un réseau en chiffrant et en authentifiant les paquets de données sur la couche 3 (réseau) du modèle OSI. [11]

Il est largement utilisé pour les réseaux VPN, et fournit quatre services de sécurité :

- **Authentification des données :** IPSec permet de s'assurer que chaque paquet échangé a bien été émis par la bonne machine et qu'il est bien destiné à la machine de destination.
- **Confidentialité des données échangées :** il est possible de chiffrer le contenu des paquets IP pour empêcher une personne extérieure de le lire.
- **Intégrité des données échangées :** IPSec permet de s'assurer qu'aucun paquet n'a subi de modifications durant son trajet.
- **Protection contre l'analyse du trafic :** IPSec permet de chiffrer les adresses réelles de l'expéditeur et du destinataire, ainsi que tout l'en-tête IP correspondant.

IPSec repose sur deux principaux protocoles :

- **AH (Authentication Header) :** il assure l'intégrité et l'authentification des paquets IP et protège contre la modification des données.
- **ESP (Encapsulation Security Payload) :** il assure la confidentialité, l'intégrité et l'authentification et chiffre les données pour empêcher leur lecture par les tiers.

II.4.2.2. HTTPS (HyperText Transfer Protocol Secure)

Le protocole HTTPS (HyperText Transfer Protocol Secure) est une extension sécurisée du protocole HTTP, le « S » pour « Secure » (sécurisé) signifie que les données échangées entre le navigateur web et le site web sont chiffrées.

Il crypte les communications pour protéger la confidentialité et l'intégrité des données, ce qui est essentiel pour les transactions en ligne et la protection des informations sensibles.

II.4.2.3. SSL/TLS (Secure Sockets Layer / Transport Layer Security)

SSL/TLS est un protocole de sécurité Internet basé sur le chiffrement. Il est développé dans le but de garantir la confidentialité, l'authentification et l'intégrité des données dans les communications Internet. Son principe consiste à établir un canal de communication sécurisé entre un client et un serveur, TLS est l'évolution de SSL, utilisé aujourd'hui. [11]

Voici le fonctionnement de ce protocole :

- Un client envoie une demande de connexion sécurisée, spécifiant la version du TLS prise en charge et les suites cryptographiques disponibles.
- Le serveur répond par la version TLS choisie et l'algorithme de chiffrement à utiliser sur son certificat SSL/TLS qui contient sa clé publique.
- Le client vérifie l'authenticité du certificat et sa validité.
- Un échange de clés a lieu pour établir une connexion chiffrée.
- Une clé de session est générée et utilisée pour chiffrer les communications.

II.4.2.4. SSH (Secure Shell)

Secure Shell (SSH) est un protocole réseau cryptographique utilisé pour exploiter en toute sécurité des services réseau sur un réseau non sécurisé. Il utilise une architecture client-serveur et une cryptographie à clé publique pour l'authentification, garantissant que la connexion entre le client et le serveur est sécurisée. SSH est indispensable pour l'administration sécurisée des serveurs et le transfert sécurisé de fichiers car il repose sur la méthode du tunnellisation.

Dans un réseau, le protocole SSH fonctionne selon l'architecture client-serveur:

- Le client SSH initie une connexion au serveur SSH.
- Le serveur authentifie l'utilisateur en demandant nom d'utilisateur et un mot de passe, sous format crypté.
- Une fois la connexion établie, toutes les données échangées par la suite sont cryptées.

II.4.3. Protocoles d'authentification et de gestion d'accès

Ce sont les protocoles qui assurent l'AAA (Authentication, Authorization, Accounting). Ces protocoles permettent de sécuriser l'accès aux ressources des réseaux, garantissant :

- **L'authentification :** il s'agit de la vérification de l'identité de l'utilisateur en entrant son nom d'utilisateur et son mot de passe.
- **L'autorisation :** elle définit les autorisations et les accès de l'utilisateur.
- **La comptabilité :** elle enregistre les actions effectuées par les utilisateurs sur les périphériques réseau.

II.4.3.1. RADIUS (Remote Authentication Dial-In User Service)

RADIUS est un protocole client-serveur et aussi un logiciel qui permet aux serveurs d'accès distant de communiquer avec un serveur central pour authentifier les utilisateurs connectés et autoriser leur accès au système ou au service demandé.

RADIUS repose principalement :

• Sur un serveur (le serveur RADIUS), relié à une base d'identification comme une base de données ou un annuaire LDAP, etc.)

• Sur un client RADIUS, appelé NAS (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur.

Si un utilisateur tente de se connecter au réseau en entrant un nom d'utilisateur et un mot de passe :

- Le client RADIUS (routeur, switch, point d'accès Wi-Fi) envoie une demande d'authentification (Access-Request) au serveur RADIUS.
- Le serveur RADIUS vérifie les informations d'identification dans sa base de données.
- Si les informations sont valides, le serveur renvoie une réponse Access-Accept avec des paramètres d'autorisation ; sinon le serveur renvoie une réponse Access-Reject.
- Une fois la session établie, le client RADIUS peut envoyer des messages de comptabilité afin d'enregistrer l'utilisation (durée de la session, volume de données transférées). [12]

II.4.3.2. Kerberos

C'est un protocole d'authentification réseau qui repose sur un mécanisme de clés secrètes, sur l'utilisation de tickets et sur une entité appelée KDC (Key Distribution Center), pour permettre aux utilisateurs de prouver leur identité de manière sécurisée, sans transmettre de mots de passe en clair sur le réseau.

Son principal objectif est de garantir l'authentification simultanée et la sécurisation des accès aux services réseau, notamment dans des environnements comme Unix/Linux et les applications d'entreprise.

II.4.3.3. TACACS+ (Terminal Access Controller Access-Control System Plus)

C'est un protocole d'authentification développé par Cisco, utilisé pour gérer l'accès aux équipements réseau. TACACS+ est une évolution des protocoles TACACS et XTACACS. Il permet aux administrateurs réseau de gérer et de contrôler l'accès des utilisateurs aux périphériques et aux ressources réseau.

Ce protocole fonctionne en utilisant un serveur centralisé pour authentifier les utilisateurs, déterminer leurs autorisations et surveiller leurs activités sur les périphériques réseau. Les utilisateurs fournissent leurs informations d'identification (nom d'utilisateur et mot de passe), qui sont ensuite vérifiées par le serveur TACACS+ par rapport à une base de données d'utilisateurs autorisés. Si les informations d'identification sont valides, l'utilisateur obtient l'accès et ses autorisations sont appliquées en fonction de son niveau d'autorisation. [12]

II.4.4. Protocoles de détection et de prévention d'intrusion

II.4.4.1. IDS (Intrusion Detection System)

C'est un système de détection d'intrusion qui surveille le trafic réseau et recherche les menaces connues et les activités suspectes ou malveillantes au sein d'un réseau. Il se divise en deux types :

- **NIDS (Network-based IDS) :** il surveille le trafic entrant et sortant du réseau.
- **HIDS (Host-based IDS) :** il surveille les activités sur des hôtes individuels.

II.4.4.2. IPS (Intrusion Prevention System)

Il fonctionne de même que IDS mais de plus il bloque automatiquement les menaces détectées en temps réel, il agit comme une barrière de protection entre le monde extérieur et le réseau interne.

De nos jours, les entreprises utilisent IDS et IPS en même temps, car IPS protège contre les menaces connues, tandis que IDS permet de détecter les nouvelles attaques.

Conclusion

Dans ce chapitre, nous avons présenté les différentes notions fondamentales de la sécurité informatique, ainsi que les méthodes de sécurité et les protocoles utilisés pour protéger les réseaux contre les hackers.

Dans le chapitre qui suit, nous allons voir les failles de sécurité des réseaux informatiques et comment elles fonctionnent.

Chapitre III : Les vulnérabilités

Préambule

De nos jours, avec l'évolution des nouvelles technologies, l'utilisation d'Internet est devenue moins sûre. Les vulnérabilités exposent les systèmes informatiques à des menaces et à des risques, les rendant susceptibles d'être attaqués de multiples manières.

Ce chapitre présente les différentes failles réseau, en mettant en évidence les menaces les plus fréquentes et les différentes formes d'attaques fréquemment rencontrées. Une métrisation de ces risques permet de crée des stratégies de protection efficaces pour sécuriser les données.

III.1. Vulnérabilités

Les vulnérabilités informatiques sont des défauts de sécurité ou des faiblesses dans un système ou un logiciel, pouvant être exploitées par une personne mal intentionnée, ce qui lui permet d'altérer le fonctionnement normal d'un système informatique ainsi que la confidentialité et l'intégrité des données qu'il contient.

III.2. Causes pour sécuriser un réseau informatique

Parmi les causes pour sécuriser un réseau informatique, nous citons :

III.2.1. Menaces

III.2.1.1. Définition

Une menace informatique désigne toute action susceptible de compromettre les critères de la sécurité d'un système informatique. Elle peut être causée par des personnes mal intentionnées, des éléments ou des facteurs naturels

III.2.1.2. Types de menaces

Ces types peuvent être regroupés selon leur :

III.2.1.2.1. Origine

A. **Menaces intentionnelles :** sont des actions exécutées par des utilisateurs qui accèdent de façon malveillante à des informations sensibles pour leur propre bénéfice et pour violer la sécurité des entreprises.
B. **Menaces accidentelles :** sont des menaces non intentionnelles qui sont réalisées sans qu'il y ait aucune préméditation. Elles peuvent être des pannes, des dysfonctionnements matériels et/ou logiciels, des erreurs de transmission, de saisie ou des mauvaises configurations. Elles sont le fait des incendies, des explosions ou des tempêtes.

III.2.1.2.2. Comportement

A. **Menaces actives :** ce type de menace implique des actions directes sur le système comme la modification des informations ou des logiciels, la création de données ou l'injection de codes malveillants afin d'introduire de fausses informations ou de perturber le bon fonctionnement de ce système.
B. **Menaces passives :** sont des menaces qui se limitent à copier ou à écouter des données sur le réseau sans les modifier. Elles sont effectuées pour collecter des informations sensibles. Dans ce cas, elles nuisent à la confidentialité des données.

III.2.2. Attaques

III.2.2.1. Définition

Désigne toute tentative d'accès malveillant (non autorisée) à un système ou un réseau informatique dans le but de causer des dommages. Elles visent à perturber, détruire ou supprimer les données de ces systèmes.

III.2.2.2. Types d'attaques

Il existe différentes attaques que nous avons classés selon trois catégories :

III.2.2.2.1. Attaques par ingénierie sociale

Parmi les types d'attaques par ingénierie sociale nous citons:

A. **Attaques de Watering Hole**

Une attaque de type Watering Hole (ou point d'eau) est une technique de cyberattaque ciblée qui consiste à compromettre un site web ou une plateforme en ligne fréquemment visitée par un groupe ciblé. L'attaquant modifie le site pour y intégrer des codes malveillants, dans le but d'infecter les visiteurs et ainsi accéder à leurs systèmes ou informations sensibles.

B. **Attaques par Hameçonnage ou Phishing**

Il s'agit d'une attaque où un attaquant malveillant attire la victime par l'envoi d'un mail contenant une pièce jointe, ou un lien frauduleux afin de le piéger pour qu'il partage des informations sensibles comme le nom d'utilisateur, le mot de passe ou des numéros de cartes de paiement.

III.2.2.2.2. Attaques logicielles

A. **Un ver**

Un ver (Worm) informatique est un virus particulier. Il s'agit d'un programme qui peut se propager, se reproduire et se déplacer à travers un réseau sans l'utilisation d'un support physique ou logiciel. Il

exploite les ressources du système de l'ordinateur infecté pour espionner, détruire des données et générer de multiples requêtes.

B. Un virus

Un virus informatique est un programme auto-réplicatif qui s'insère dans des fichiers ou logiciels légitimes, appelés hôtes, afin de se propager sans l'autorisation de l'utilisateur. Initialement conçu sans intention malveillante, il est désormais souvent associé à du code nuisible et peut perturber, endommager ou altérer le fonctionnement de l'ordinateur infecté. Sa diffusion s'effectue par divers moyens d'échange de données numériques, tels que les réseaux informatiques, Internet, les supports amovibles (clé USB, CD, disquettes) ou encore par l'intermédiaire de courriers électroniques et leurs pièces jointes.

C. Cheval de Troie

Un cheval de Troie (ou Trojan) est un programme malveillant qui se cache dans un autre programme sain que lorsque la victime lance ce dernier, elle lance aussi le cheval de Troie caché afin d'avoir le contrôle sur l'ordinateur de la victime. Il peut servir à voler des mots de passe, à copier des données sensibles ou à autoriser des accès à des parties protégées du réseau à des personnes se connectant de l'extérieur. Contrairement au ver, le cheval de Troie ne se réplique pas.

D. Bombe logique

Une bombe logique est une partie d'un programme malveillant (virus, cheval de Troie, etc.) souvent associé à un cheval de Troie. Une bombe logique contient une partie de code conditionnelle qui s'activera une fois la condition réalisée (temps, date, action, signal, …) et non lors de l'installation de la bombe logique. Par exemple : un cheval de Troie associé à un écran de veille, la bombe logique explosera après quelques heures de veille.

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

III.2.2.2.3. Attaques réseau

A. Attaque par le DoS

Une attaque par déni de service (DoS, Denial of Service) est une tentative malveillante, qui consiste à envoyer un grand nombre de paquets inutiles vers un réseau, ce qui surcharge les services et les ressources informatiques du réseau. En général, les attaques de DoS visent principalement les serveurs, afin qu'ils ne puissent être utilisés ou consultés. [13]

B. Attaque de MITM

L'attaque de l'homme du milieu (Man-In-The-Middle, MITM) ou attaque de l'intercepteur, est une technique d'attaque où un pirate intercepte la communication entre deux parties, sans que ni l'une ni l'autre puisse se douter que le canal de communication entre elles a été compromis. La machine du pirate joue le rôle d'un proxy ainsi, il pourra accéder à toutes les données et obtenir les informations sans que les utilisateurs s'en rendent compte.

C. Attaques par l'Usurpation d'identité

C'est lorsqu'un attaquant se fait passer pour un autre utilisateur en utilisant les données personnelles de ce dernier sans son accord et réalise différents actes en son nom.

Les techniques d'usurpation d'identité sont :

C.1. Usurpation d'adresse IP (Spoofing IP)

C'est une technique d'attaque utilisée par les cybercriminels pour masquer leurs adresses IP et utiliser une autre adresse falsifiée. Cette tactique leur permet de contourner les systèmes de sécurité, masquer leur identité et mener diverses attaques dans le but de contourner les règles de filtrage mises en place. [14]

C.2. Détournement DNS (DNS Spoofing)

C'est une technique d'attaque très dangereuse, où le pirate remplace les informations du système de résolution des noms de domaine par une fausse adresse DNS contrôlée par l'attaquant. À cet effet, l'utilisateur reçoit une fausse requête DNS qui le redirige vers un site web frauduleux qui ressemble à l'original. Le DNS spoofing est utilisé pour voler l'identité de l'utilisateur ainsi que le mot de passe, informations bancaires ou pour infecter l'appareil par des virus et surveiller ces activités. [15]

C.3. ARP Spoofing

C'est une cyberattaque ciblée que sur les réseaux locaux, où un acteur malveillant envoie des messages ARP (Address Resolution Protocol) falsifiés sur un réseau. Cela permet à l'attaquant d'associer son adresse MAC à une adresse IP d'un périphérique légitime de réseau. Une fois cette étape est faite, l'attaquant intercepte tout le trafic destiné à cette adresse IP, il peut modifier ou arrêter les données en transit. [14]

III.2.2.2.4. Injections en sécurité informatique

En informatique, les injections sont des attaques où les pirates insèrent des codes malveillants dans un système fragile pour voler, modifier les données ou prendre le contrôle du système. Les types les plus courants sont :

A. Injection SQL

C'est un type d'attaque dans lequel le cybercriminel exploite les failles dans une application pour manipuler une base de données. Elle se produit lorsqu'un site web ne sécurise pas bien ses entrées d'utilisateurs. Le pirate injecte dans cette faille un code SQL malveillant dans ces entrées, ce qui lui permet d'accéder à la base de données et à exécuter des commandes non autorisées. [15]

B. Injection de script (XSS-Cross-Site Scripting)

Cette attaque consiste à insérer un code JavaScript malveillant dans un site web. Cette faille se produit lorsque le site web ne filtre pas correctement les entrées d'utilisateurs, ce qui permet au pirate d'ajouter une URL ou un formulaire. Ensuite, le code malveillant est exécuté par les visiteurs de la page web.

Conclusion

Dans ce chapitre, nous avons présenté les différents types d'attaques et de menaces, ainsi que leurs effets sur le réseau.

Dans le dernier chapitre, nous étudierons le cas d'une architecture sécurisée que nous avons proposée pour renforcer le niveau de sécurité en appliquant de multiples protocoles.

Chapitre IV : Simulation et tests d’un réseau informatique sécurisé

Préambule

L'objectif de ce chapitre est de présenter la mise en place d'une topologie réseau représentative, utilisant plusieurs protocoles et mécanismes de sécurité tels que le pare-feu, la DMZ et le VPN.

Pour ce faire, nous montrons dans un premier temps une architecture d'un réseau informatique où nous avons mis en évidence l'intégration de la sécurité. Dans un second temps, une description détaillée des équipements utilisés est donnée.

Afin de montrer la fiabilité de notre solution de sécurité réseau, nous avons fait une simulation sous le logiciel Cisco Packet Tracer. Nous avons ainsi pu illustrer le fonctionnement des équipements, l'application des politiques de sécurité ainsi que le comportement du réseau dans des conditions simulées.

Les différents tests réalisés ont montré l'efficacité de la solution. En effet, des pings entre le réseau Inside et le réseau Ouside sont effectués avec succès.

IV.1. Présentation d'organisme d'accueil

IV.1.1. Historique d'Algérie Télécom

Régie par la loi 2000/03 du 5 aout 2000. Algérie Télécom est née pour relever le défi de l'ouverture du marché des télécommunications annoncées par des réformes engagées par le pays. Algérie Télécom jouit d'un statut d'entreprise publique économique. Ce statut établit la forme juridique d'une société par action SPA.

Compte tenu du rôle que jouent les télécommunications dans le développement économique, social, culturel, et en adéquation avec les objectifs assignés pour remplir les retards marqué dans ce domaine.

Algérie Télécom a inscrit des actions multiples qu'elle doit réaliser avec succès pour répondre aux besoins de sa clientèle et assure une présentation des services et la qualité.

Le challenge d'Algérie Télécom en sa qualité d'opérateur historique est d'être leader dans son domaine et nourri des ambitions de devenir un business partenaire incontournable à l'échelle régionale et nationale.

Algérie Télécom s'est engagée comme acteur principal dans la mise en œuvre de programme de développement de société de l'information en Algérie. Compte tenu des besoins de la clientèle dans les différents segments des services des Télécommunications.

Algérie Télécom se propose de construire des relations d'affaires à long terme avec les opérateurs économique intéressés par le secteur des télécommunications et des multimédias.

IV.1.2. Principaux objectifs d'Algérie Télécom

- Valoriser l'offre de services téléphoniques et faciliter l'accès aux services de télécommunications pour un maximum d'utilisateurs, notamment dans les zones rurales.
- Améliorer la qualité des services offerts et élargir la gamme de prestations proposées pour rendre les services de télécommunications plus compétitifs.
- Établir un réseau national de télécommunications fiable et connecté aux autoroutes de l'information.
- Mettre en œuvre une approche marketing innovante et une politique de communication efficace.

IV.1.3. Organigramme d'Algérie Télécom

La figure 17 montre l'organisation générale d'Algérie Télécom par bloc :

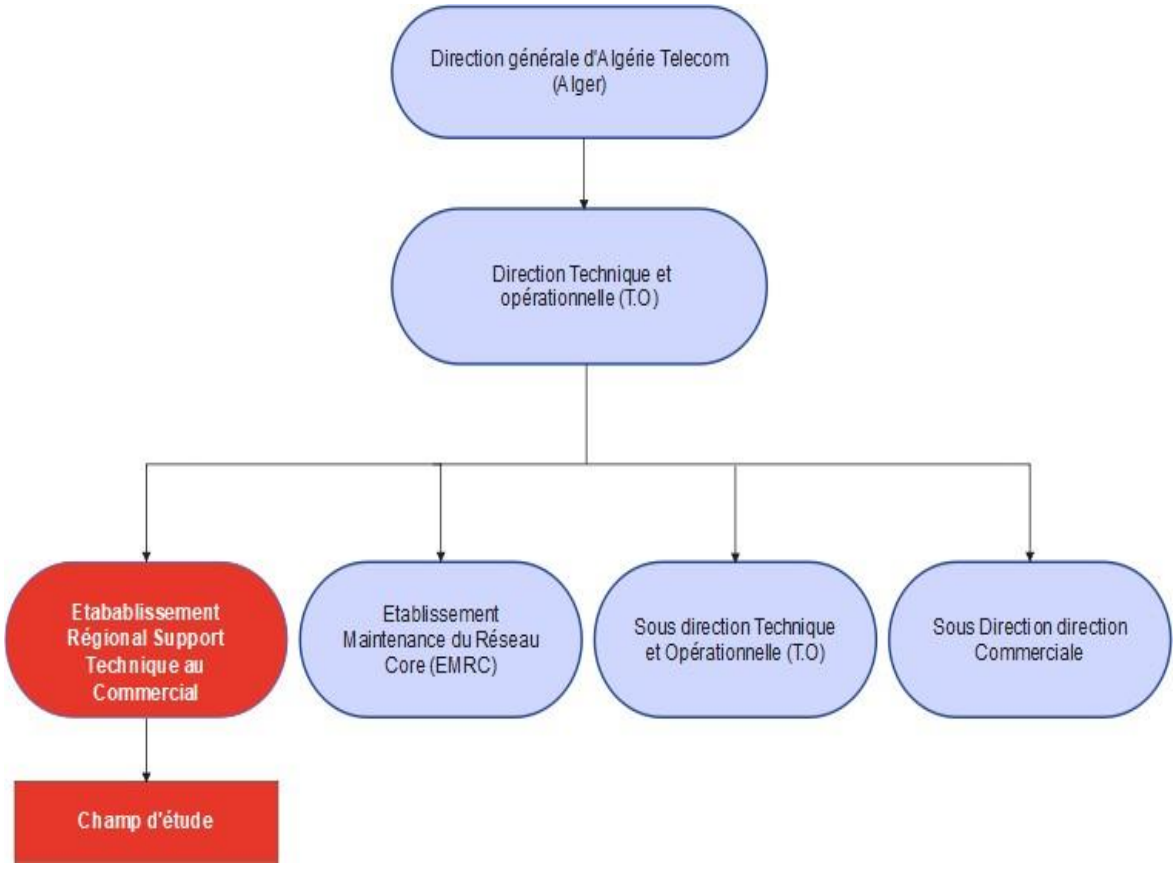

Figure 17: Organigramme général d'Algérie Télécom

IV.1.3.1. Description champs d'étude ERSTC

Le Laboratoire des Equipements de Télécommunication (LETTO) a été renommé Etablissement Régional Support Technique au Commerciale (ERSTC) suit à la Direction technique et opérationnel T.O de la Direction Générale Algérie Télécom.

Ce laboratoire régional est créé en 2009 pour répondre aux besoins des clients d'Algérie Télécom en matière de création et maintenance des réseaux d'entreprises. Il se compose d'un chef de centre et équipe d'Ingénieurs et de Techniciens.

IV.1.4. Organigramme ERSTC

La figure suivante montre l'organigramme ERSTC :

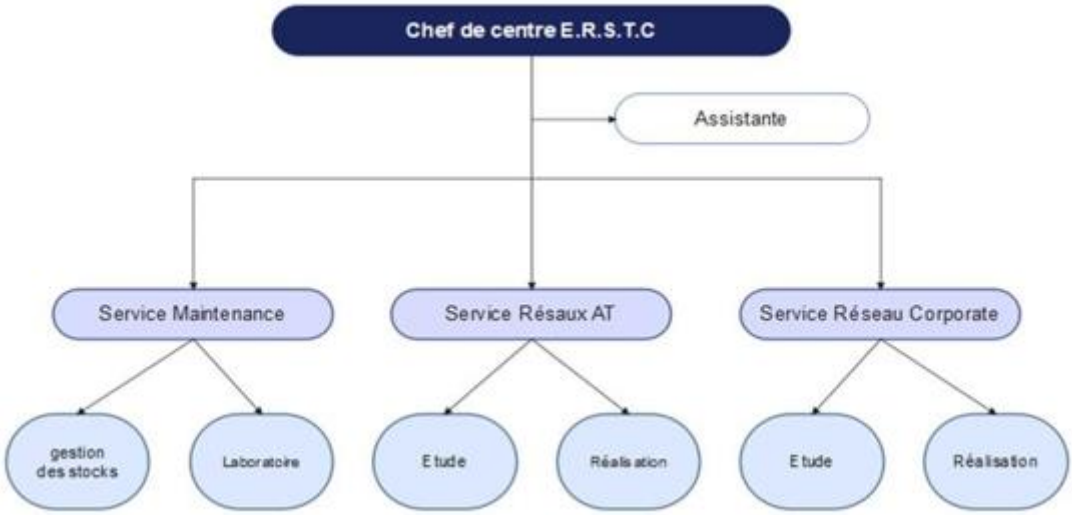

Figure 18 : Organigramme ERSTC

IV.1.4.1. Description de l'organigramme ERSTC

Par le schéma organisationnel de l'établissement régional du support technique au commercial présenté ci-dessus, nous pouvons remarquer que le centre se reparti en trois services sous l'autorité d'un chef de service :

Chef d'établissement : il est le responsable de tout le service (ERSTC). C'est par lui que toutes les activités et projets gérés par l'ERSTC déroulent ; de ce fait les fonctions de celui-ci se présentent pareillement :

- La réalisation des ordres de mission.
- L'accord des congés quel que soit la nature.

- La coordination des interventions à distance chez las agences d'AT et les structures corporates.
- Coordination de l'archivage de toutes les informations sur les activités de l'ERSTC.

Service de maintenance : Ce service de l'ERSTC est directement rattaché au matériel de l'Algérie télécom dans toute la région, ainsi il est chargé de :

- Assure la gestion des entrées/sorties des équipements réseaux (structure corporate ou agences A.T).
- Assure la maintenance de toutes sortes de matériels d'Algérie Télécom (A.T) de la région (c'est-à-dire des trois wilayas qui sont : Tizi-Ouzou, Bouira, Boumerdes).

Service réseau d'Algérie Télécom : Ce service de l'ERSTC s'occupe de :

- L'étude et la réalisation des réseaux LAN et WAN des différentes structures d'Algérie télécom de la région.
- Configuration et installations des différentes applications d'Algérie télécom.
- Assure la continuité et le bon fonctionnement de réseaux intranet d'Algérie Télécom.

Service réseau Corporate : Cette branche de l'ERSTC s'occupe de :

- Etude et réalisation de différentes propositions et solutions des structures Corporates.
- Configuration et installations de différentes applications chez les structures corporates.
- Assure la continuité et le bon fonctionnement des différentes liaisons(ADSL, SHDSL, VPN, WIFI, FIBRE OPTIQUE) pour les clients corporates par l'entretien et la relève des dérangements.

IV.1.4.2. Rôle d'ERSTC

Ce laboratoire est chargé d'intervenir sur les trois wilayas : Tizi-Ouzou, Boumerdes, et Bouira, pour la Prise en charge des dérangements signalés par lesclients (NAFTAL, CASNOS, Banques…). Ainsi que la réparation et maintenance des équipements informatiques, bureautiques et télécommunications de l'entreprise ALGERIE TELECOM (ACTEL, CMT,DOT, DRT…).

IV.1.4.3. Activités du champ d'étude ERSTC

Le centre E.R.S.T.C est impliqué dans une multitude d'activités à l'intérieur et à l'extérieur d'Algérie Telecom tel que :

- Etudes et réalisation des réseaux filaires et wifi.
- Configuration software et hardware des différents équipements réseaux (modems, routeurs, firewall…etc.).

- Mise en service et test de bon fonctionnement des différentes liaisons (VPN, IP fixe, ADSL, HSDSL, RMS...etc.).
- Diagnostics et relèvent de dérangements des liaisons.
- Configurations des différentes applications web du réseau intranet.
- Assurer la continuité des liaisons des différentes structures d'Algérie Telecom.
- Maintenances software et hardware de toutes sortes d'équipements réseaux et informatiques à distance pour les structure d'Algérie Telecom.
- Il assure la prise en charge des stagiaires durant leur période d'apprentissage.
- Et à la demande de la Direction Générale, le service E.R.S.T.C assure des missions en dehors de leur région sur le territoire national.

IV.2. Présentation du logiciel de simulation

Cisco Packet Tracer est un outil logiciel complet de simulation de réseau conçu pour l'enseignement et l'apprentissage des topologies de réseau et des réseaux informatiques modernes. Il permet aux utilisateurs de pratiquer la mise en réseau, l'IoT et la cyber sécurité dans un environnement de laboratoire virtuel sans avoir besoin de matériel physique.

Cet outil est créé par Cisco Systems **(**entreprise californienne créée en 1984 spécialisée dans les équipements réseaux*)* qui le fournit gratuitement aux centres de formation, étudiants et diplômés participant ou ayant participé aux programmes de formation Cisco.

IV.3. Architecture d'un réseau sécurisé d'une entreprise

L'objectif de cette topologie est de mettre une stratégie multi-protocoles pour sécuriser notre réseau interne. Dans laquelle nous avons utilisé deux dispositifs de sécurité ASA 5505 configurés avec des règles ACL pour filtrer le trafic entrant et sortant, en n'autorisant que les flux nécessaires, par exemple autoriser uniquement les ports HTTPS vers le serveur web et pour isoler les différentes zones du réseau (Inside, Outside et DMZ). Des routes statiques ou un protocole de routage sont utilisés entre les routeurs (R1, R2 et R3) et les sous-réseaux.

L'accès aux équipements doit être restreint avec des mots de passe, le chiffrement SSH au lieu de Telnet, et un contrôle d'accès basé sur les adresses IP.

Enfin, nous avons implémenté un tunnel VPN d'accès à distance entre R1 et R2, qui permet de fournir un accès aux employés travaillant à distance ou à un partenaire distant tout en assurant la sécurité des données lors de l'échange via des protocoles de cryptage et de sécurité.

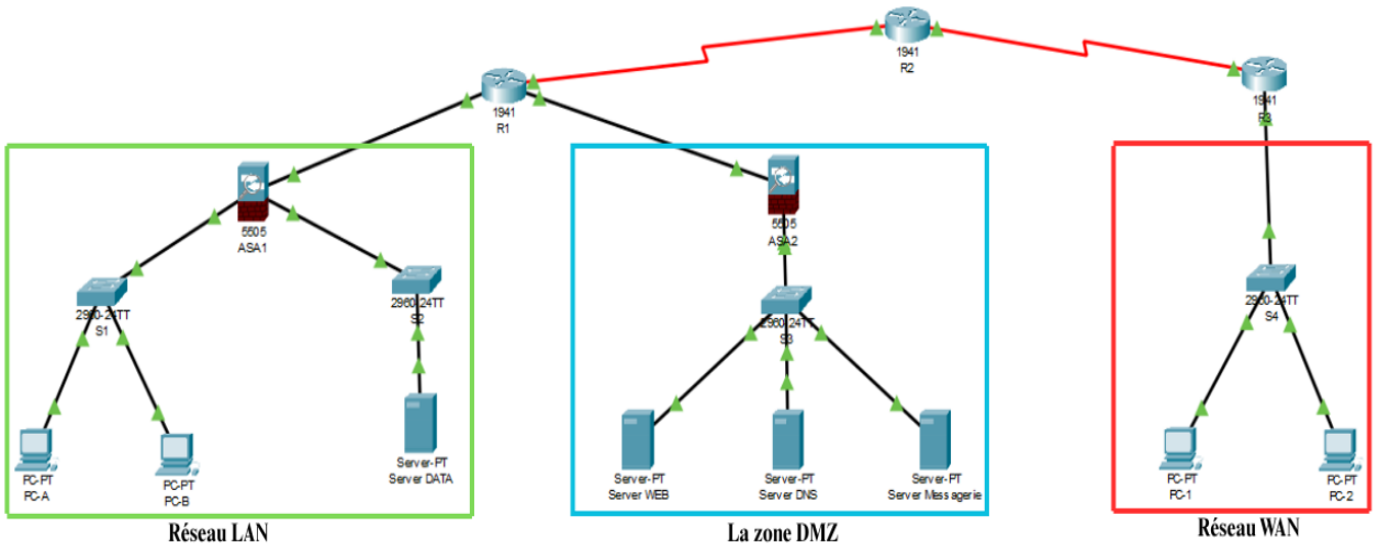

Figure 19: Architecture sécurisée proposée

IV.3.1. Matériels utilisés

- **Les ordinateurs :** utilisés comme des postes de travail et pour le réseau Internet.
- **Les serveurs :** utilisés pour exécuter des services critiques comme la base de données, serveur web, serveur messagerie et DNS.
- **Les commutateurs (2960) :** appelés Switch, fonctionnent à l'intérieur du réseau afin de commuter le trafic entre les PC en utilisant l'adresse MAC. Ils fonctionnent sur la couche 2 du modèle OSI.
- **Les routeurs (1941) :** sont conçus pour transmettre des paquets de données entre différents réseaux en fonction de leurs adresses IP. Ils fonctionnent sur la couche 3 du modèle OSI.
- **Câble droit :** standard Ethernet pour connecter les équipements opérant dans les différentes couches du modèle OSI.
- **Câble croisé :** standard Ethernet pour connecter les équipements opérant dans les mêmes couches du modèle OSI.
- **Câbles DCE et DTE :** les connexions série se font entre deux ports série. Elles sont souvent utilisées pour simuler des liens WAN. Le signal d'horloge (le Clocking) doit être activé sur le câble DCE pour activer la connexion. En fonction du premier câble sélectionné (DTE ou DCE) le deuxième sera forcément de l'autre type afin d'assurer la connexion.
- **ASA 5505 :** c'est l'acronyme de Adaptive Security Appliance, est un pare-feu développé par Cisco Systems, conçu pour assurer la sécurité des réseaux à partir de filtrage de paquets, le contrôle d'accès (ACL), la traduction d'adresses (NAT), l'inspection du trafic et le VPN.

- **DMZ :** permet de sécuriser les serveurs publiés sur Internet tout en protégeant le réseau interne.

IV.3.2. Mode de configuration

Le tableau 2 présente les adresses IP attribuées à chaque interface réseau, accompagnées de leur masque de sous-réseau et de la passerelle par défaut correspondante :

Dispositif	Interface	Adresse IP	Masque sous réseau	Passerelle par Défaut
R1	S0/0/0	194.1.1.1	255.255.255.252	/
	Gig0/0	172.16.16.1	255.255.255.0	/
	Gig0/1	194.10.1.1	255.255.255.252	/
R2	S0/0/0	194.1.1.2	255.255.255.252	/
	S0/0/1	194.1.2.2	255.255.255.252	/
R3	S0/0/1	194.1.2.1	255.255.255.252	/
	Gig0/0	192.168.10.1	255.255.255.0	/
ASA1	Et0/0	192.168.4.1	255.255.255.0	/
	Et0/1	192.168.5.1	255.255.255.0	/
	Et0/2	172.16.16.2	255.255.255.0	/
ASA2	Et0/0	192.168.6.1	255.255.255.0	/
	Et0/2	194.10.1.2	255.255.255.252	/
Server WEB	/	192.168.6.3	255.255.255.0	192.168.6.1
Server Messagerie	/	192.168.6.4	255.255.255.0	192.168.6.1
PC-A	/	192.168.5.3	255.255.255.0	192.168.5.1
PC-1	/	192.168.10.11	255.255.255.0	192.168.10.1
PC-2	/	192.168.10.12	255.255.255.0	192.168.10.1

Tableau 2: Tables d'adressage

IV.3.2.1. Configuration des routeurs

Avant tout, la première étape consiste à vérifier que la licence du pack technologique de sécurité est activée sur chaque routeur, en utilisant la commande **« show version »,** car cela est nécessaire pour permettre l'exécution de certaines commandes :

```
Technology Package License Information for Module:'c1900'

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

Configuration register is 0x2102
```

Figure 20: Vérification de la licence du pack technologique de sécurité

Comme nous avons vu dans la figure 20, le module du **« security »** n'est pas activé. Afin de l'activer nous suivons les étapes qui sont montrées dans les figures qui suit :

```
Press RETURN to get started!


Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#license boot module c1900 technology-package securityk9
```

Figure 21: Activation du module de sécurité

Après l'exécution de cette commande, nous acceptons la licence (figure 22), enregistrer la configuration et redémarrer le routeur (figure 23):

```
Your acceptance of this agreement for the software features on one
product shall be deemed your acceptance with respect to all such
software on all Cisco products you purchase which includes the same
software. (The foregoing notwithstanding, you must purchase a license
for each software feature you use past the 60 days evaluation period,
so that if you enable a software feature on 1000 devices, you must
purchase 1000 licenses for use past the 60 day evaluation period.)

Activation of the software command line interface will be evidence of
your acceptance of this agreement.

ACCEPT? [yes/no]: yes
```

Figure 22: L'acceptation de l'agrément

```
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#reload
Proceed with reload? [confirm]
```

Figure 23: L'enregistrement de la configuration et le redémarrage de R1

Nous exécutons à nouveau la commande **« show version »** pour vérifier l'activation de la licence du module **« securityk9 »** (figure 24).

```
Technology Package License Information for Module:'c1900'

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

Configuration register is 0x2102
```

Figure 24: Vérification de l'activation de la licence du pack technologique de sécurité

Nous refaisons la même chose pour les deux autres routeurs R2 et R3.

La deuxième étape consiste à attribuer des adresses IP pour chaque interface routeur utilisée ainsi que le routage nécessaire :

R1 :

La configuration est la suivante :

```
R1(config)#int gig0/0
R1(config-if)#ip add 172.16.16.1 255.255.255.0
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R1(config-if)#exit
R1(config)#int gig0/1
R1(config-if)#ip add 194.10.1.1 255.255.255.252
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

R1(config-if)#exit
R1(config)#int s0/0/0
R1(config-if)#ip add 194.1.1.1 255.255.255.252
R1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit
R1(config)#
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#ip route 192.168.5.0 255.255.255.0 172.16.16.2
R1(config)#ip route 192.168.6.0 255.255.255.0 194.10.1.2
R1(config)#
```

Figure 25: Configuration des interfaces de R1

Du même pour le routeur 2 et le routeur 3, voire les figures 26 et 27:

```
R2(config)#int s0/0/0
R2(config-if)#ip add 194.1.1.2 255.255.255.252
R2(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R2(config-if)#exit
R2(config)#int s0/0/1
R2(config-if)#ip add 194.1.2.2 255.255.255.252
R2(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#exit
R2(config)#
R2(config)#ip route 0.0.0.0 0.0.0.0 194.1.1.1
R2(config)#ip route 192.168.10.0 255.255.255.0 194.1.2.1
```

Figure 26: Configuration des interfaces de R2

```
R3(config)#int gig0/0
R3(config-if)#ip address 192.168.10.1 255.255.255.0
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R3(config-if)#exit
R3(config)#int s0/0/1
R3(config-if)#ip address 194.1.2.1 255.255.255.252
R3(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R3(config-if)#exit
R3(config)#
R3(config)#ip route 0.0.0.0 0.0.0.0 Serial0/0/1
```

Figure 27: Configuration des interfaces de R3

IV.3.2.2. Configuration des pare-feu

La configuration de l'ASA, se fait comme tout autre équipement Cisco, mais avec le modèle ASA 5505 l'attribution des adresses se fait avec des interfaces VLAN au lieu des interfaces physiques. Ensuite il faut donner un nom, une adresse IP et un niveau de sécurité pour chaque interface utilisée.

Chacune de ces interfaces possède un niveau de sécurité spécifique allant de 0 à 100. Plus ce niveau est élevé, plus la zone est sécurisée.

• L'interface **Inside** qui présente le réseau interne, reçoit par défaut un niveau de sécurité de 100, ce qui la rend la zone la plus fiable. Depuis cette zone le trafic est autorisé vers toutes les autres zones qui possèdent un niveau de sécurité inférieure comme la DMZ et l'OUTSIDE, sauf si nous l'interdirons par des règles d'ACL.

• L'interface **Outside** qui présente le réseau externe, reçoit par défaut un niveau de sécurité de 0, ce qui la rend la zone la moins sécurisée. Le trafic venant de cette zone vers l'Inside ou la DMZ est bloqué sauf si nous l'autorisons par des règles spécifiques.

• L'interface **DMZ** qui héberge les serveurs accessibles depuis internet comme serveur web ou un serveur messagerie, généralement possède un niveau de sécurité intermédiaire qui se situe entre 50 et 70. Ce qui signifie qu'elle est moins sécurisée que l'Inside et plus sécurisée que l'Outside.

Avec ce système de sécurité l'ASA aura un comportement de filtrage de base intelligent, même avec l'absence des règles d'ACL. Ensuite, si nous voulons renforcer la sécurité nous ajoutons ces règles selon le besoin.

- **Configuration nom d'hôte, nom de domaine et le mot de passe**

Les figures 28 et 29 montrent la configuration initiale des pare-feu ASA1 et ASA2 respectivement :

ASA1 :

```
ciscoasa>en
Password:
ciscoasa#conf t
ciscoasa(config)#hostname ASA1
ASA1(config)#domain-name ciscosecurity.com
ASA1(config)#enable password asa123
ASA1(config)#
```

Figure 28: Configuration du mode privilégié de ASA1

ASA2 :

```
ciscoasa>en
Password:
ciscoasa#conf t
ciscoasa(config)#hostname ASA2
ASA2(config)#enable password asa123
ASA2(config)#
```

Figure 29: Configuration du mode privilégié de ASA2

- **Configuration des interfaces de l'ASA**

La configuration des interfaces des deux pare-feu est illustrée dans les figures 30 et 31:

ASA1 :

```
ASA1(config)#
ASA1(config)#int vlan 1
ASA1(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.
ASA1(config-if)#ip address 192.168.5.1 255.255.255.0
ASA1(config-if)#no shut
ASA1(config-if)#exit
ASA1(config)#
ASA1(config)#int vlan 2
ASA1(config-if)# nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ASA1(config-if)#security-level 70
ASA1(config-if)# ip address 192.168.4.1 255.255.255.0
ASA1(config-if)#no shut
ASA1(config-if)#exit
ASA1(config)#
ASA1(config)#int vlan 3
ASA1(config-if)#nameif outside
ERROR: This license does not allow configuring more than 2 interfaces with nameif and
without a "no forward" command on this interface or on 1 interface(s) with nameif already
configured.
ASA1(config-if)#no forward interface Vlan2
ASA1(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
ASA1(config-if)#ip address 172.16.16.2 255.255.255.0
ASA1(config-if)#no shut
ASA1(config-if)#exit
```

Figure 30: Configuration des interfaces de l'ASA1

ASA2 :

```
ASA2(config)#
ASA2(config)#int vlan 2
ASA2(config-if)#nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ASA2(config-if)#security-level 50
ASA2(config-if)#ip address 192.168.6.1 255.255.255.0
ASA2(config-if)#no shut
ASA2(config-if)#exit
ASA2(config)#
ASA2(config)#int vlan 3
ASA2(config-if)#nameif outside
INFO: Security level for "outside" set to 0 by default.
ASA2(config-if)#ip address 194.10.1.2 255.255.255.252
ASA2(config-if)#no shut
ASA2(config-if)#exit
ASA2(config)#
ASA2(config)#int vlan 1
ASA2(config-if)#ip address 194.1.1.2 255.255.255.252
ASA2(config-if)#no shut
ASA2(config-if)#exit
ASA2(config)#
```

Figure 31: Configuration des interfaces de l'ASA2

- **L'activation des interfaces de l'ASA**

Les figures 32 et 33, représentent l'activation des interfaces des pare-feu ASA1 et ASA2 respectivement :

ASA1 :

```
ASA1(config)#
ASA1(config)#int e0/0
ASA1(config-if)#switchport access vlan 2
ASA1(config-if)#no shut
ASA1(config-if)#exit
ASA1(config)#
ASA1(config)#int e0/1
ASA1(config-if)#switchport access vlan 1
ASA1(config-if)#no shut
ASA1(config-if)#exit
ASA1(config)#
ASA1(config)#int e0/2
ASA1(config-if)#switchport access vlan 3
ASA1(config-if)#no shut
ASA1(config-if)#exit
ASA1(config)#
```

Figure 32: L'activation des interfaces de l'ASA1

Du même pour ASA2 :

```
ASA2(config)#
ASA2(config)#int e0/0
ASA2(config-if)#switchport access vlan 2
ASA2(config-if)#no shut
ASA2(config-if)#exit
ASA2(config)#
ASA2(config)#int e0/2
ASA2(config-if)#switchport access vlan 3
ASA2(config-if)#no shut
ASA2(config-if)#exit
ASA2(config)#
```

Figure 33: L'activation des interfaces de l'ASA2

Vérification: Nous avons effectué un ping depuis le PC-A (192.168.5.3) vers le Server DATA (192.168.4.3) pour vérifier la notion des niveaux de sécurité comme le montre la figure ci-dessous.

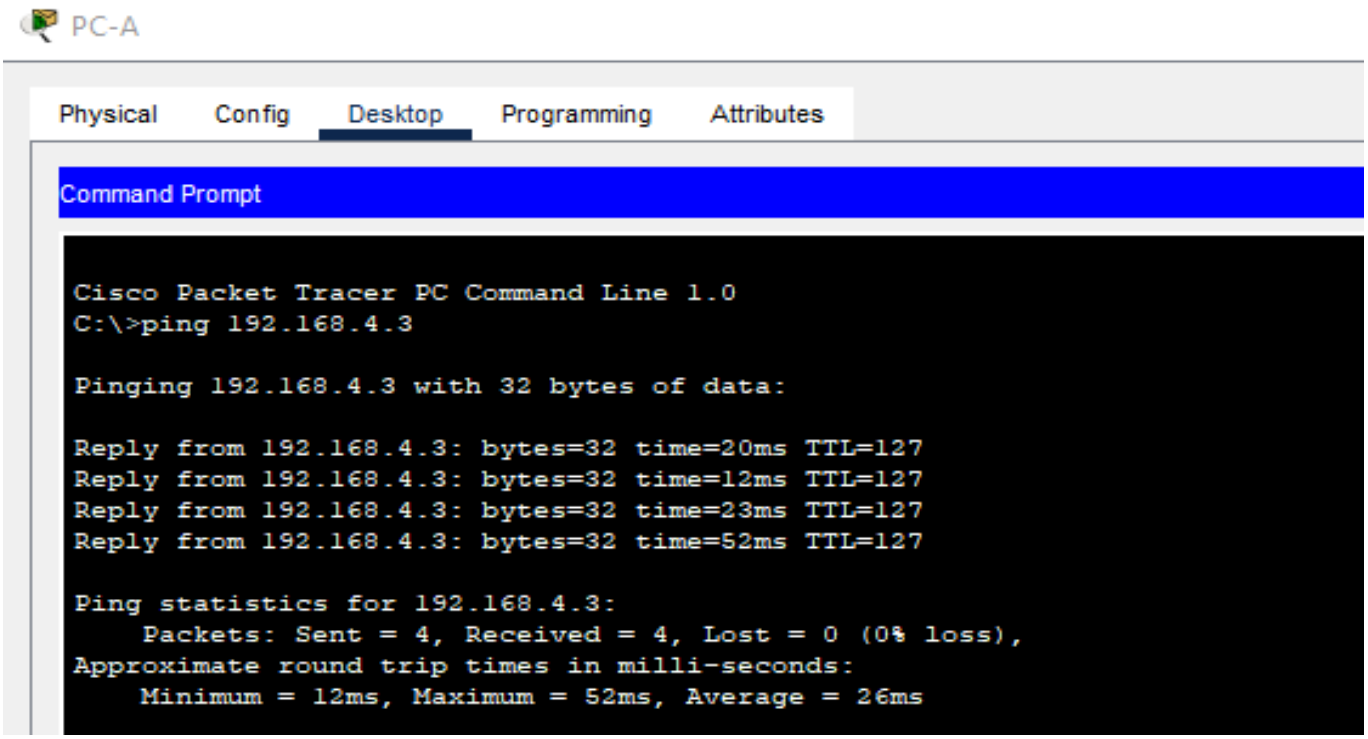

Figure 34: Ping depuis le PC-A vers le Server DATA

- **Configuration du protocole de routage**

La mise en place du routage par défaut sur ASA1 et ASA2 est donné par les figures 35 et 36 :

ASA1 :

```
ASA1(config)#
ASA1(config)#route outside 0.0.0.0 0.0.0.0 172.16.16.1
ASA1(config)#
```

Figure 35: Configuration des routes sur ASA1

ASA2 :

```
ASA2(config)#
ASA2(config)#route outside 0.0.0.0 0.0.0.0 194.10.1.1
ASA2(config)#
```

Figure 36: Configuration des routes sur ASA2

Vérification : Nous avons effectué un ping depuis l'ASA1 et depuis l'ASA2 vers R1 (194.1.1.1), pour vérifier la transmission du trafic (figure 37 et 38).

```
ASA1#
ASA1#ping 194.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 194.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/17 ms
```

Figure 37: Ping depuis ASA1 vers R1

```
ASA2#
ASA2#ping 194.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 194.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Figure 38: Ping depuis ASA2 vers R1

- **Configuration du protocole ICMP**

L'ICMP est principalement utilisé pour tester la connectivité en utilisant la commande **« Ping »** ou signaler des erreurs par exemple **« hôte injoignable »** ou **« TTL »** expiré.

Mais avec un pare-feu ASA**,** l'ICMP est traité de manière différente des autres types de trafic. Par défaut, l'ASA bloque les requêtes ICMP entrantes de zones moins sécurisées par exemple de l'extérieure vers des zones plus sécurisées comme le réseau interne, même si une ACL les autorise. [16]

Alors pour résoudre ce problème il faut activer l'inspection ICMP avec les commandes suivantes illustrées dans la figure 39:

```
ASA1(config)#class-map inspection_default
ASA1(config-cmap)#match default-inspection-traffic
ASA1(config-cmap)#exit
ASA1(config)#policy-map global_policy
ASA1(config-pmap)#class inspection_default
ASA1(config-pmap-c)#inspect icmp
ASA1(config-pmap-c)#exit
ASA1(config)#service-policy global_policy global
ASA1(config)#
```

Figure 39: Configuration du protocole ICMP

Ainsi, l'ASA peut inspecter les paquets ICMP et gérer leur état, ce qui est utile pour autoriser un ping initié depuis l'intérieur tout en protégeant contre les tentatives de balayage depuis l'extérieur.

Nous répétons ensuite la même opération avec l'ASA2.

Vérification : Nous avons effectué un ping depuis le PC-1 vers R1 (194.10.1.1), afin de vérifier l'activation du protocole ICMP comme le montre la figure suivante.

```
C:\>ping 194.10.1.1

Pinging 194.10.1.1 with 32 bytes of data:

Reply from 194.10.1.1: bytes=32 time=2ms TTL=253
Reply from 194.10.1.1: bytes=32 time=34ms TTL=253
Reply from 194.10.1.1: bytes=32 time=36ms TTL=253
Reply from 194.10.1.1: bytes=32 time=10ms TTL=253

Ping statistics for 194.10.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 36ms, Average = 20ms
```

Figure 40: Ping depuis le PC-1 vers R1

- **Configuration du NAT**

Dans ce réseau, le LAN utilise des adresses IP privées que nous ne pouvons pas utiliser directement sur le WAN, alors pour permettre aux postes du réseau interne d'accéder à l'Internet, nous utilisons le NAT dynamique qui sera configuré sur le pare-feu ASA1. Ce mécanisme consiste à traduire les adresses privées en une adresse publique partagée.

Sur ASA2, les serveurs de la DMZ ont des adresses publiques afin d'être accessibles depuis l'extérieur, pour cela, nous configurons un NAT statique qui attribue à chaque serveur une adresse publique fixe.

Au final, nous aurons d'un côté des postes internes qui peuvent sortir vers Internet et de l'autre côté des serveurs qui peuvent être joints depuis l'extérieur, tout en étant protégés par le pare-feu.
La figure suivante représente la configuration du trafic depuis l'intérieure vers l'extérieure sur ASA1:

```
ASA1(config)#
ASA1(config)#object network inside-net
ASA1(config-network-object)#subnet 192.168.5.0 255.255.255.0
ASA1(config-network-object)#nat (inside,outside) dynamic interface
ASA1(config-network-object)#end
ASA1#
```

Figure 41: Configuration du NAT sur l'ASA1

Vérification : La figure suivante montre un ping depuis le PC-A (192.168.5.3) vers les serveurs de la zone DMZ (192.168.6.0).

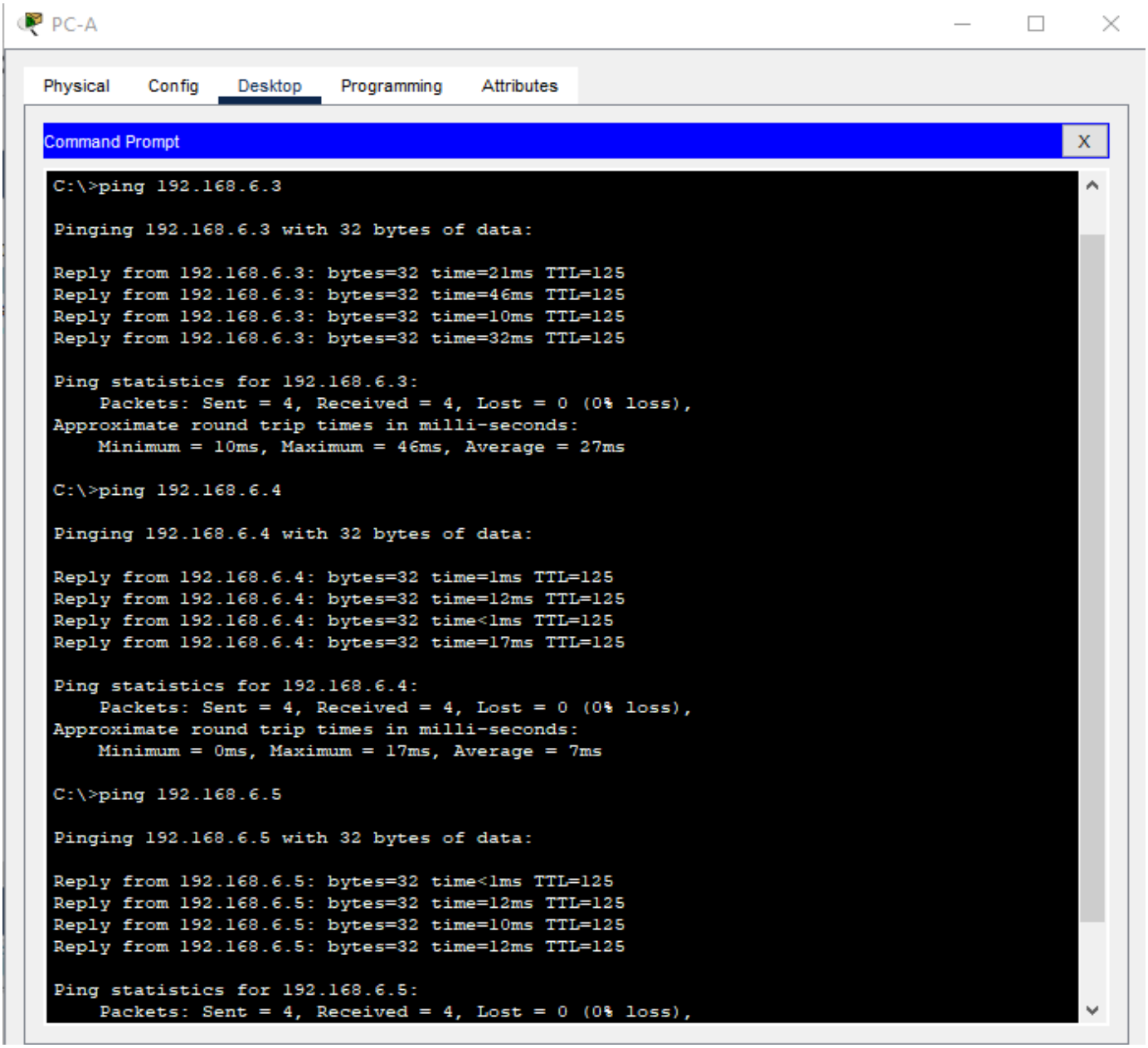

Figure 42: Ping depuis le PC-A vers les serveurs de la zone DMZ

La figure 43 montre la configuration du NAT pour le Server WEB de la zone DMZ vers l'extérieure sur ASA2 :

```
ASA2(config)#object network dmz-web
ASA2(config-network-object)#host 192.168.6.3
ASA2(config-network-object)#nat (dmz,outside) static 194.10.1.2
ASA2(config-network-object)#exit
ASA2#
```

Figure 43: Configuration du NAT sur l'ASA2

Vérification : Effectuer un ping depuis PC-1 et PC-A respectivement (figure 44, 45) vers l'adresse publique du Server WEB (194.10.1.2).

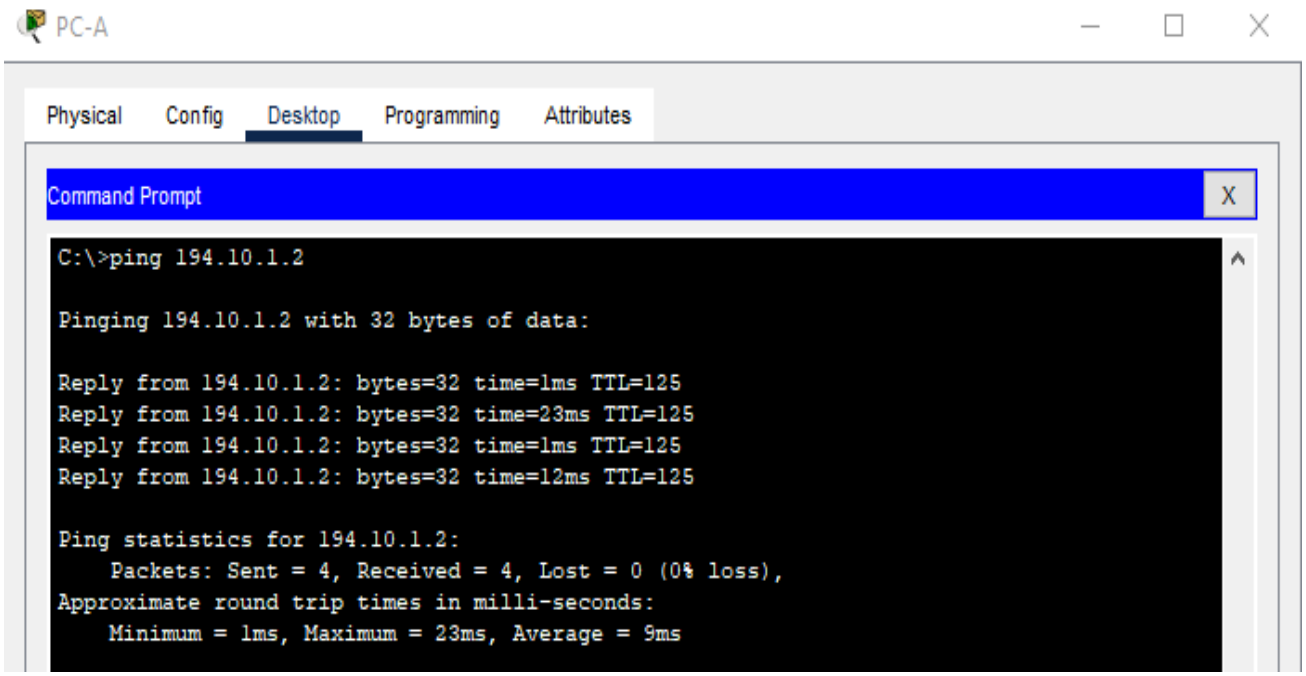

Figure 44: Ping depuis le PC-1 vers l'adresse publique du Server WEB

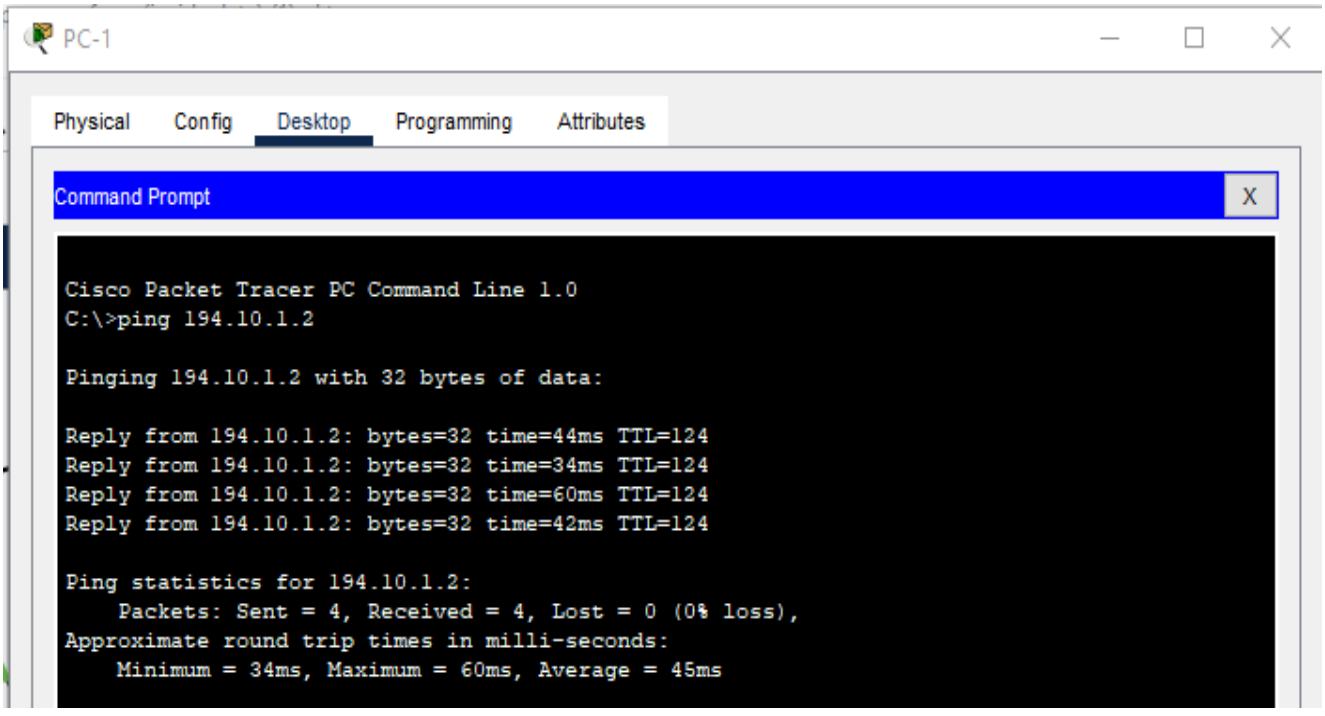

Figure 45: Ping depuis le PC-A vers l'adresse publique du Server WEB

- **Configuration des règles d'ACL**

En utilisant des règles d'ACL, cela nous permet d'autoriser ou bloquer les flux qui circulent d'une extrémité à une autre en fonction des critères comme les adresses IP source ou destination, le protocole TCP ou ICMP ou encore le numéro de port. Ce mécanisme permet d'autoriser l'accès à une ressource pour quelqu'un qui ne fait pas partie du groupe principal sans impacter les autres.

Donc pour permettre le trafic entre un réseau moins sécurisé et un réseau plus fiable, il est nécessaire de créer des listes de contrôle d'accès ACL.

Nous avons ajouté une access-liste sur ASA2, pour permettre aux postes du réseau LAN d'accéder au server web avec son adresse privée (figure 46) :

```
ASA2(config)#
ASA2(config)#access-list inside-web extended permit ip 192.168.5.0 255.255.255.0 host 192.168.6.3
ASA2(config)#access-list extended permit tcp any object dmz-web eq www
ASA2(config)#
```

Figure 46: Configuration des ACL sur l'ASA2

- **Configuration du DHCP**

Sur la figure suivante, nous observons la configuration du DHCP pour le réseau interne :

```
ASA1(config)#
ASA1(config)#dhcpd address 192.168.5.10-192.168.5.30 inside
ASA1(config)#dhcpd dns 192.168.6.4 interface inside
ASA1(config)#dhcpd enable inside
```

Figure 47: Configuration du protocole DHCP

Vérification : Configurer le DHCP pour le PC-B de la zone Inside (figure 48).

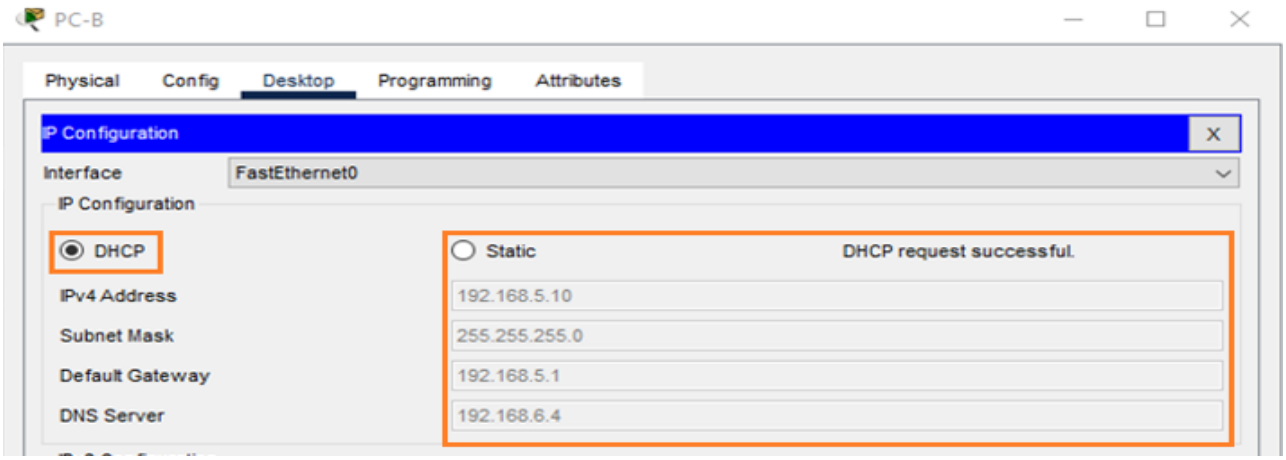

Figure 48: Configuration du protocole DHCP sur le PC-B

- **Configuration du SSH**

La figure suivante montre la configuration du protocole SSH sur ASA1 :

```
ASA1(config)#
ASA1(config)#username KENZA password DYHIA
ASA1(config)#aaa authentication ssh console LOCAL
ASA1(config)#ssh 192.168.5.0 255.255.255.0 inside
ASA1(config)#ssh 192.168.10.11 255.255.255.255 outside
ASA1(config)#ssh timeout 15
ASA1(config)#
```

Figure 49: Configuration du protocole SSH sur ASA1

Vérification: L'établissement d'une session SSH sur le pare-feu ASA1 est donné dans les figures 50 et 51.

Depuis le PC-1 vers l'ASA1 (172.16.16.1) :

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l KENZA 172.16.16.2

Password:


ASA1>
```

Figure 50: Vérification du protocole SSH sur PC-1

Depuis le PC-A vers l'ASA1 (192.168.5.1) :

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l KENZA 192.168.5.1

Password:



ASA1>
```

Figure 51: Vérification du protocole SSH sur PC-A

La figure suivante montre la configuration du protocole SSH sur ASA2 :

```
ASA2(config)#
ASA2(config)#username admin password admin
ASA2(config)#aaa authentication ssh console LOCAL
ASA2(config)#ssh 192.168.5.0 255.255.255.0 outside
ASA2(config)#ssh 192.168.10.0 255.255.255.0 outside
ASA2(config)#ssh timeout 15
ASA2(config)#
```

Figure 52: Configuration du protocole SSH sur ASA2

Vérification: L'établissement d'une session SSH sur le pare-feu ASA2 est donné dans les figures 53 et 54.

Depuis le PC-A et du PC-1 vers l'ASA2 (194.10.1.2), respectivement :

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 194.10.1.2

Password:



ASA2>
```

Figure 53: Vérification du protocole SSH sur PC-A

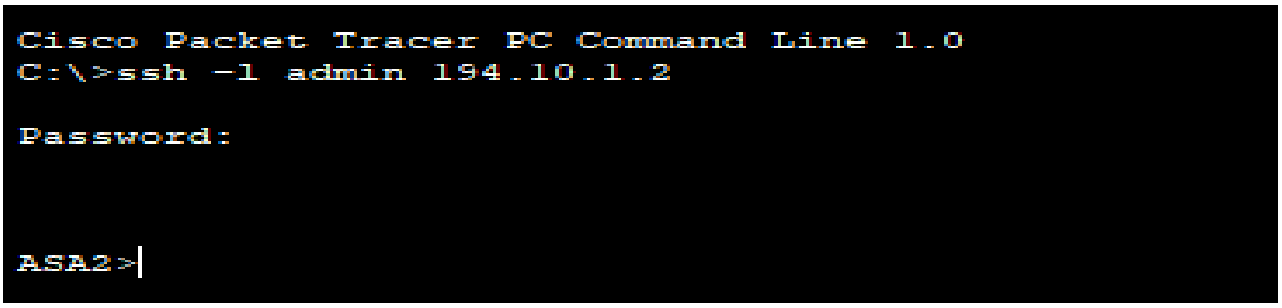

Figure 54: Vérification du protocole SSH sur PC-1

IV.3.2.3. Configuration de la zone DMZ

- **Configuration du Server WEB**

L'attribution de l'adresse IP, du masque de sous réseau, de la passerelle et du DNS (figure 55) :

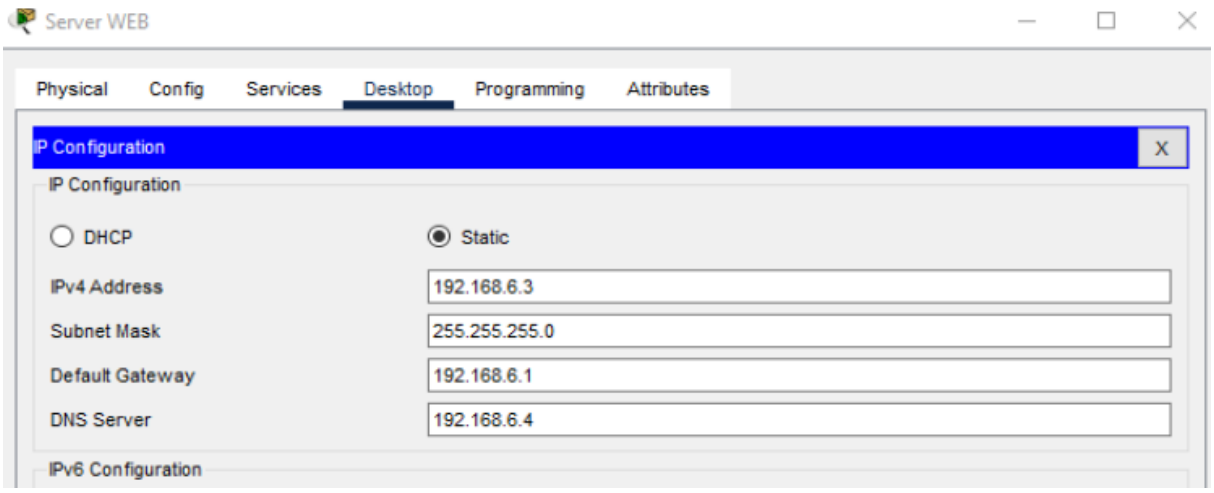

Figure 55: Attribution d'une adresse IP au Server WEB

L'activation du protocole HTTPS uniquement ainsi que l'importation du contenu de la page web est illustré dans la figure ci-dessous :

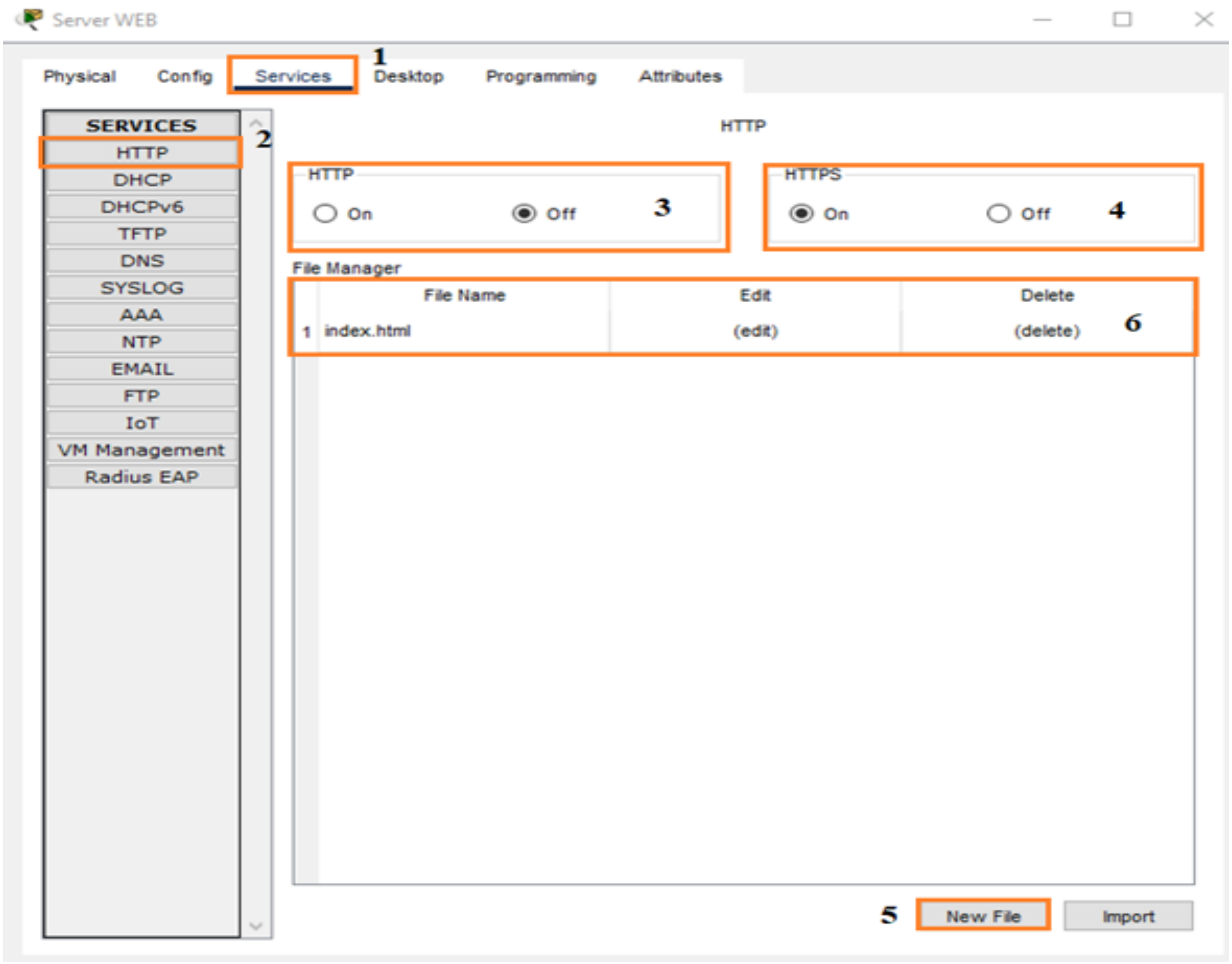

Figure 56: Configuration du Server WEB

Vérification : Dans le navigateur web du PC-1, nous testons l'accès au Server WEB en saisissant l'adresse : https://194.10.1.2 (figure 57).

Figure 57: Accéder à la page web avec l'adresse publique du Server WEB

- **Configuration du Server DNS**

L'attribution de l'adresse IP, du masque de sous réseau, de la passerelle et du DNS (figure 58) :

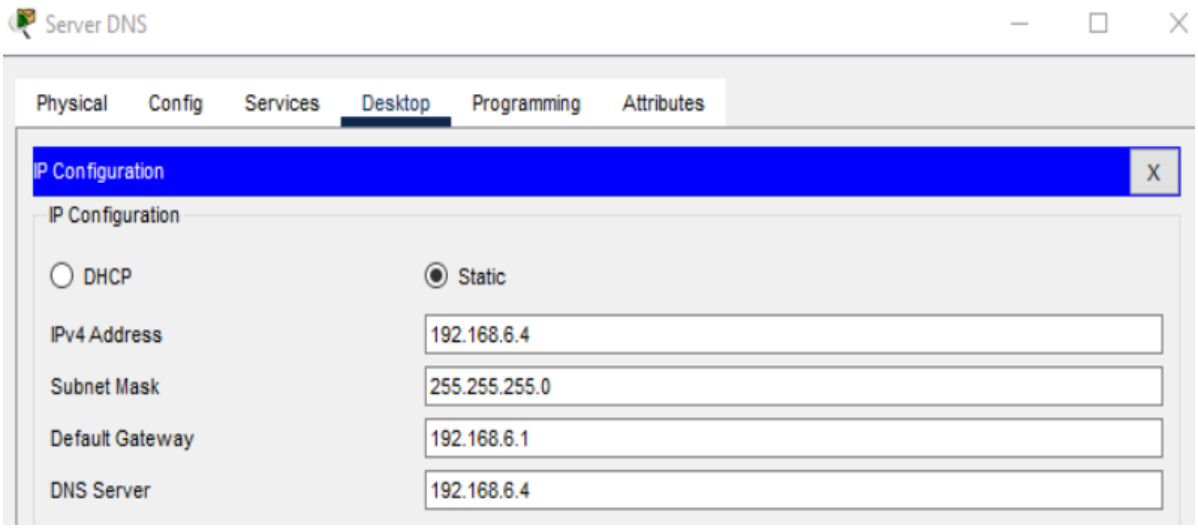

Figure 58: Attribution d'une adresse IP au Server DNS

Dans la figure qui suit, nous activons le service DNS et lui attribuons un nom de domaine (technova.com) :

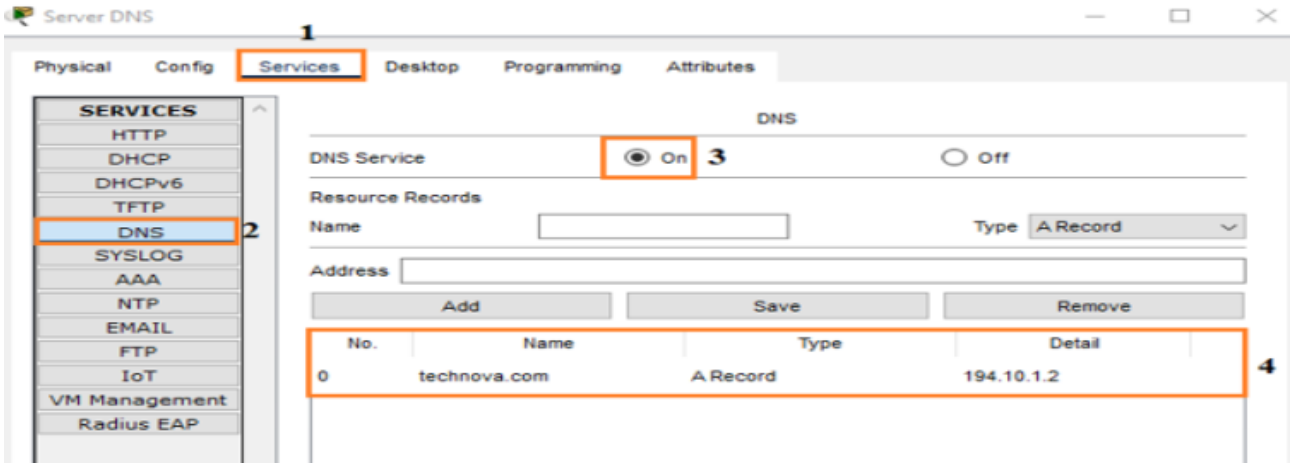

Figure 59: Configuration du Server DNS

Vérification : Accéder à la page web avec le nom de domaine au lieu de l'adresse IP publique, afin de vérifier le bon fonctionnement du service DNS, comme la figure ci-dessous le montre.

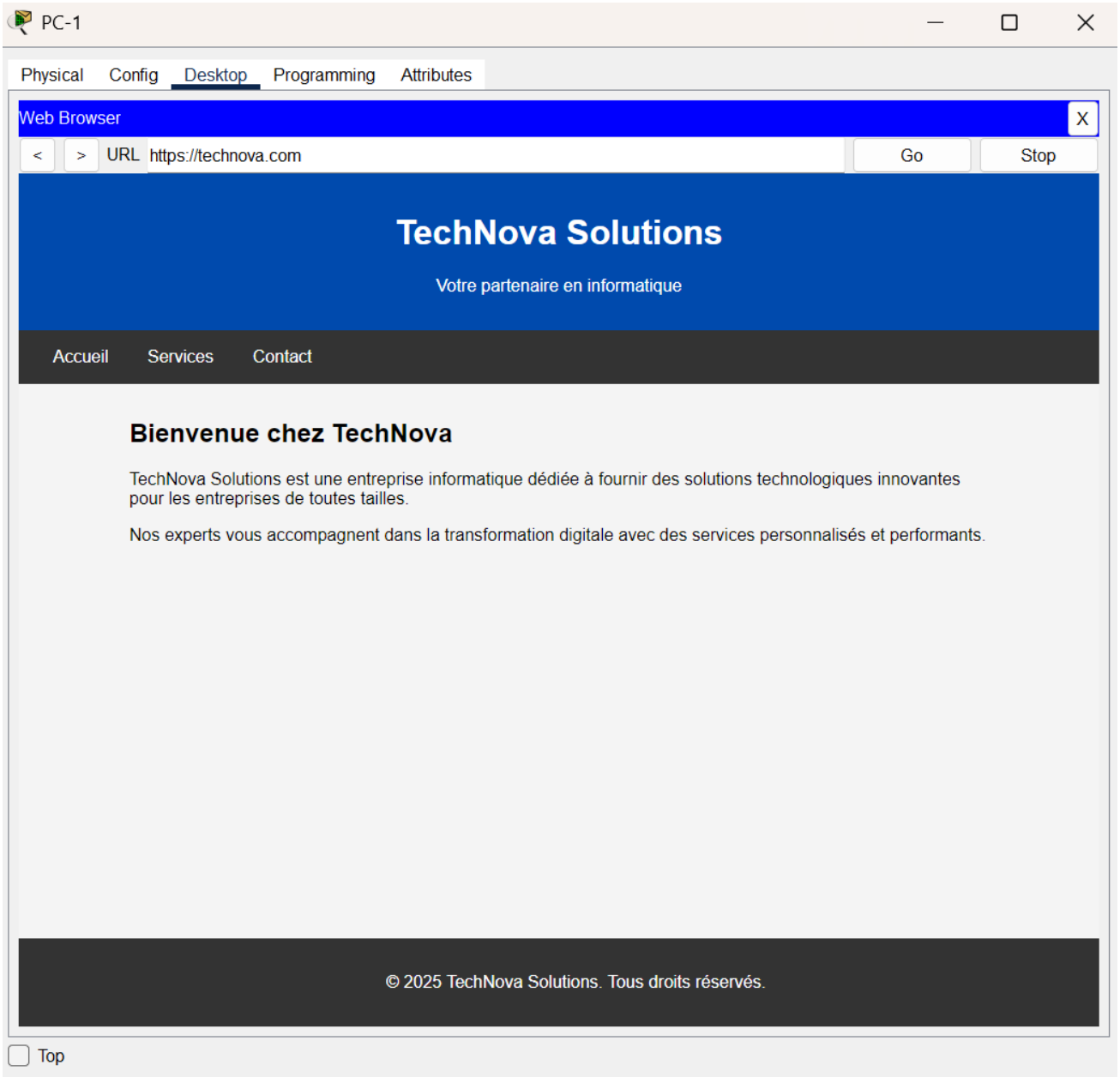

Figure 60: Accéder à la page web avec le nom de domaine

- **Configuration du Server Messagerie**

L'attribution de l'adresse IP, du masque de sous réseau, de la passerelle (figure 61) :

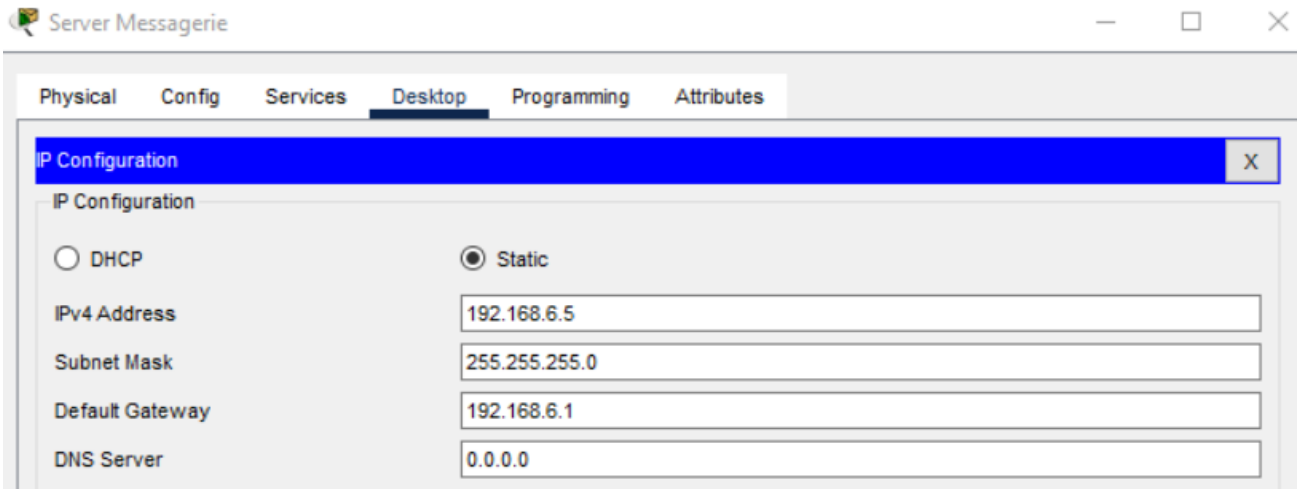

Figure 61: Attribution d'une adresse IP au Server Messagerie

La figure 62 importe l'activation des services POP et SMTP et la création des boites mail:

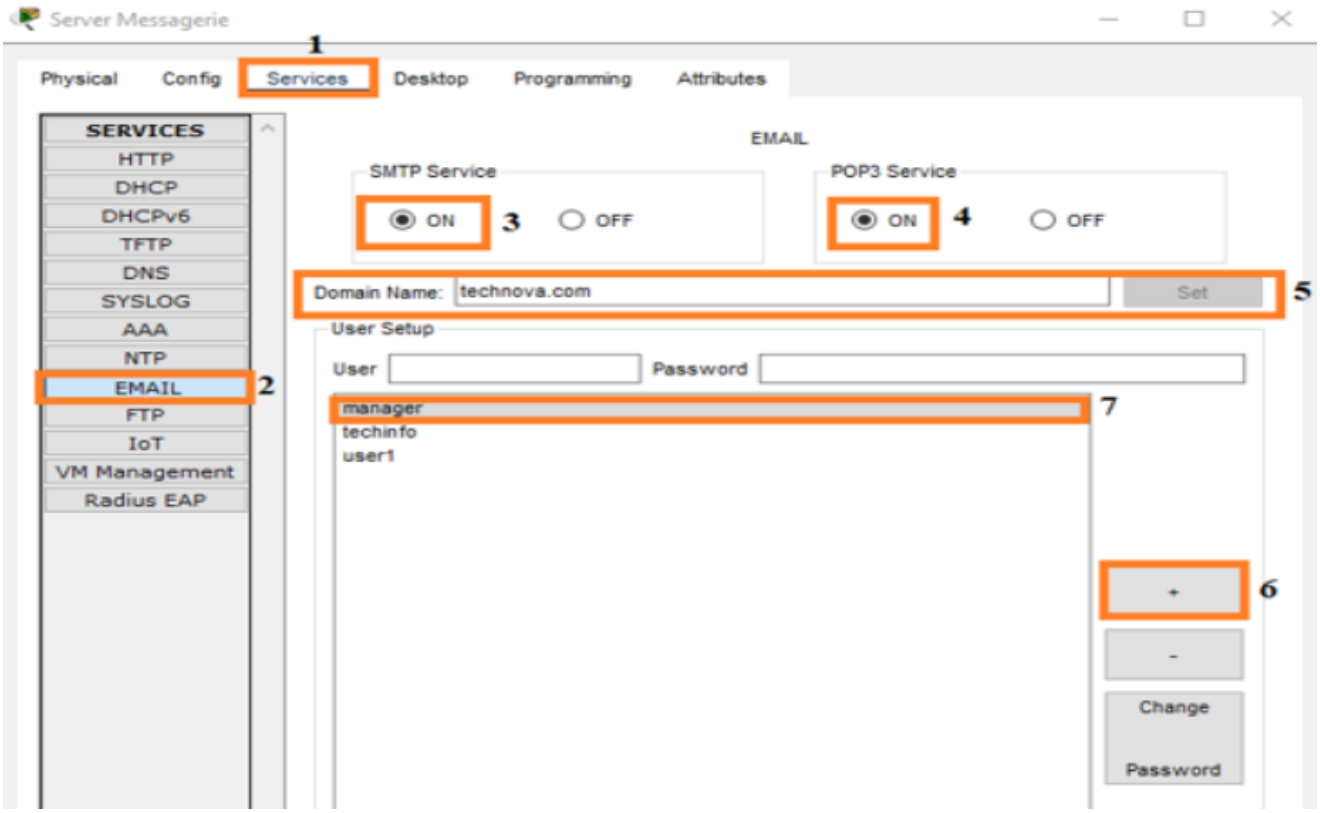

Figure 62: Configuration du Server Messagerie

Sur le PC-A, nous cliquons sur desktop et nous complétons les informations du destinataire Manager comme indiqué dans la figure ci-dessous :

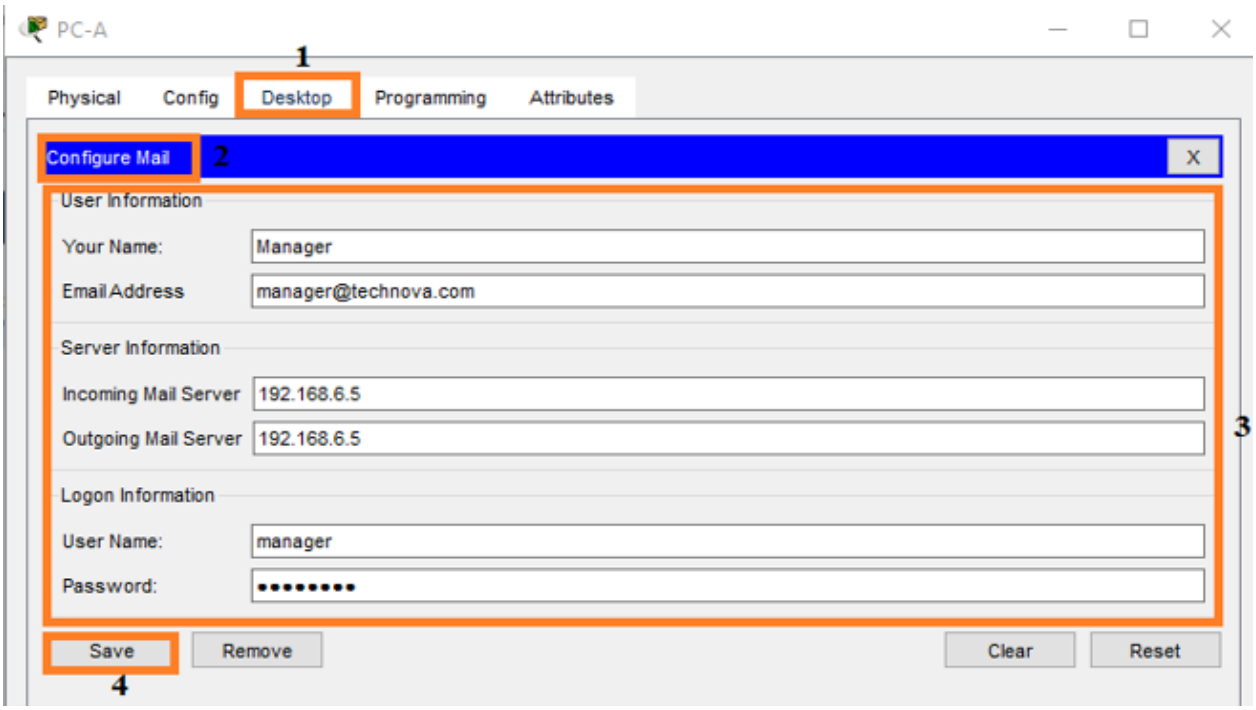

Figure 63: Création d'un compte mail pour le Manager sur PC-A

Sur le PC-1, nous cliquons sur desktop et nous complétons les informations de l'expéditeur User1 comme indiqué dans la figure ci-dessous :

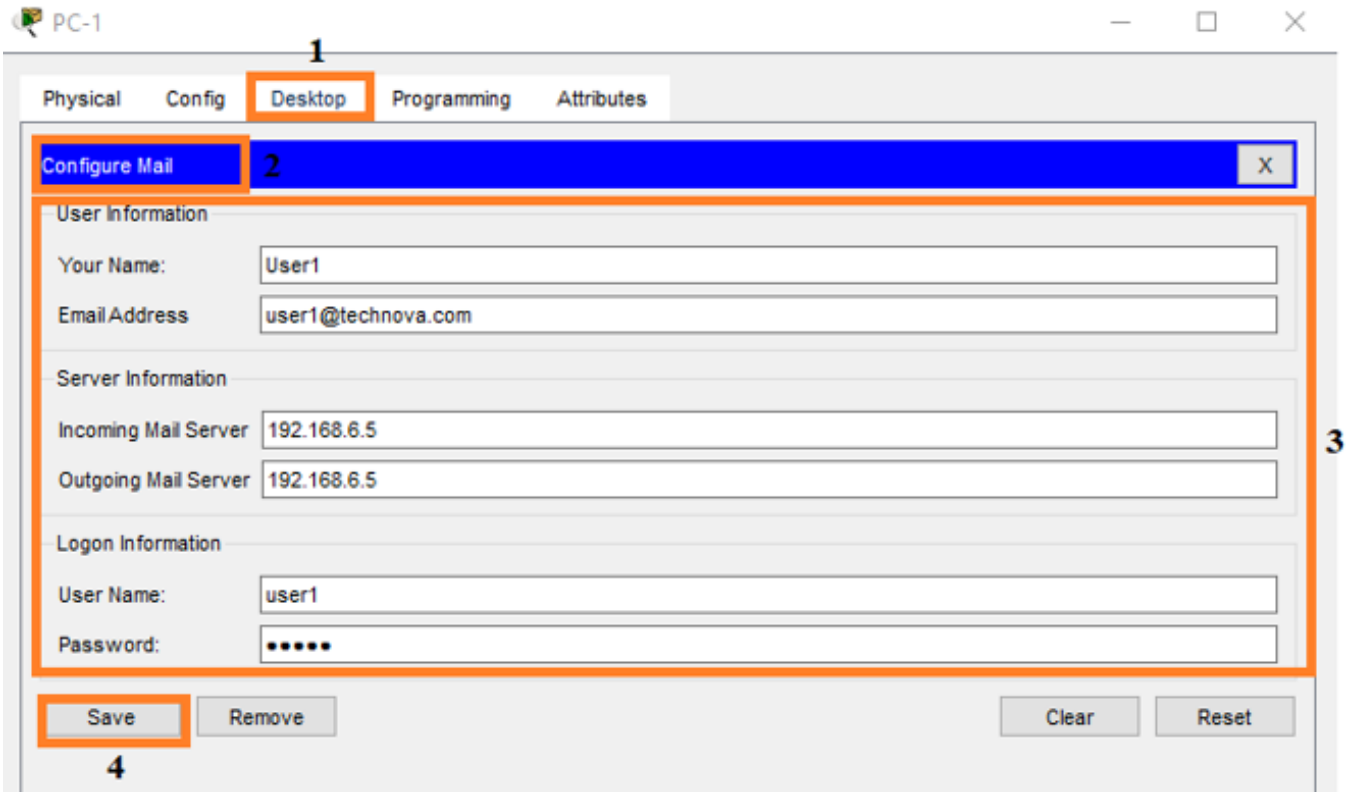

Figure 64: Création d'un compte mail pour User1 sur PC-1

Nous sélectionnons le bouton « Composer » et dans la fenêtre suivante qui s'affiche, nous rédigeons notre mail (figure 65) :

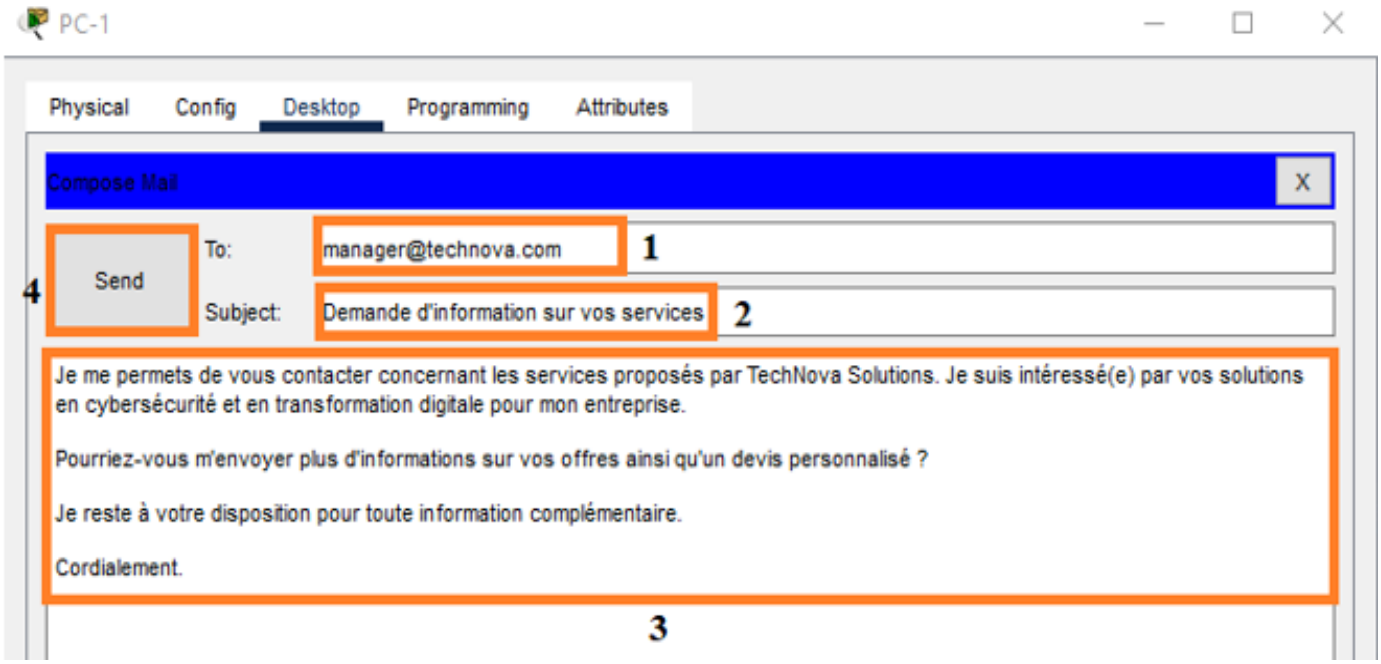

Figure 65: L'envoi d'un mail depuis le PC-1 vers la boîte mail du Manager

Dans la figure 66, nous remarquons que le message est envoyé avec succès :

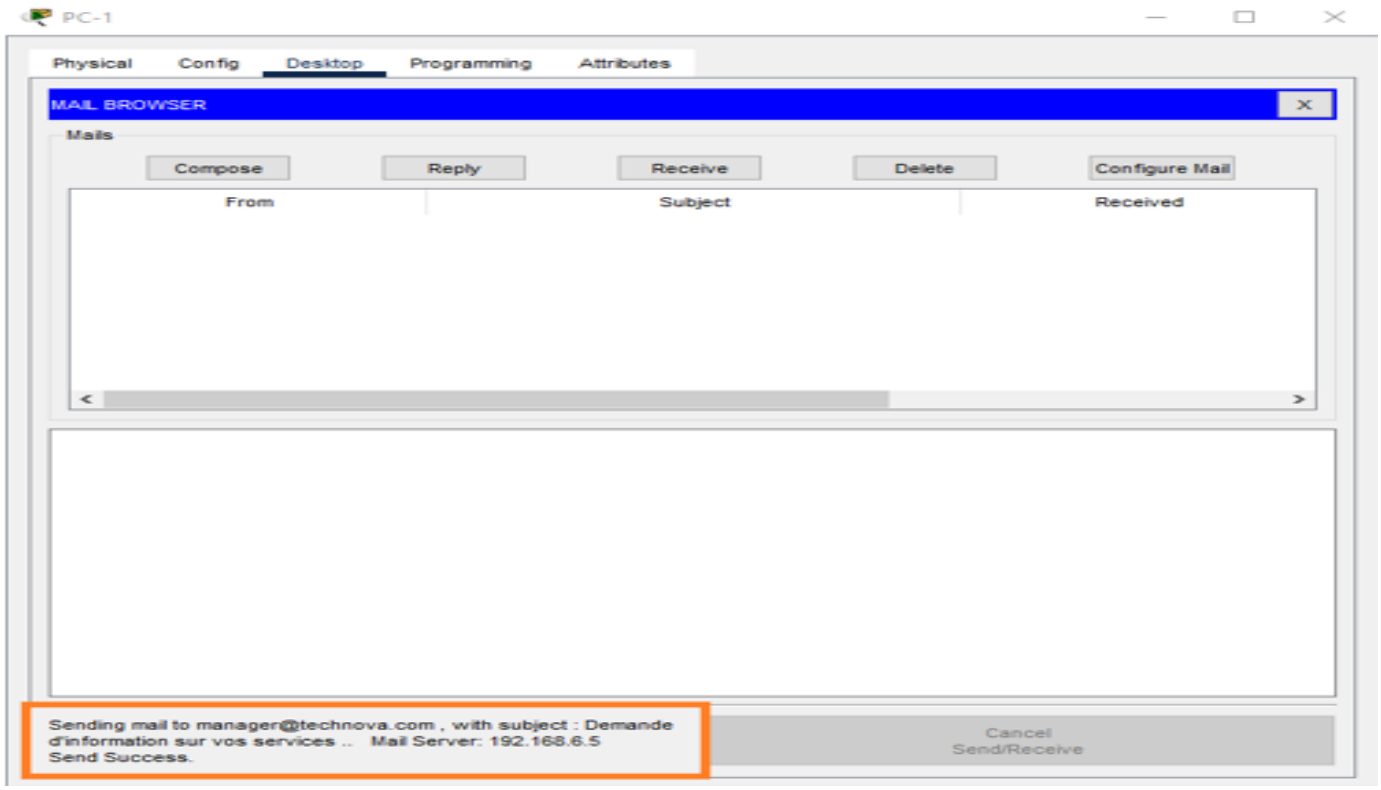

Figure 66: Le mail est bien envoyé

La figure ci-dessous montre que le PC-A du Manager reçoit l'e-mail envoyé par User1.

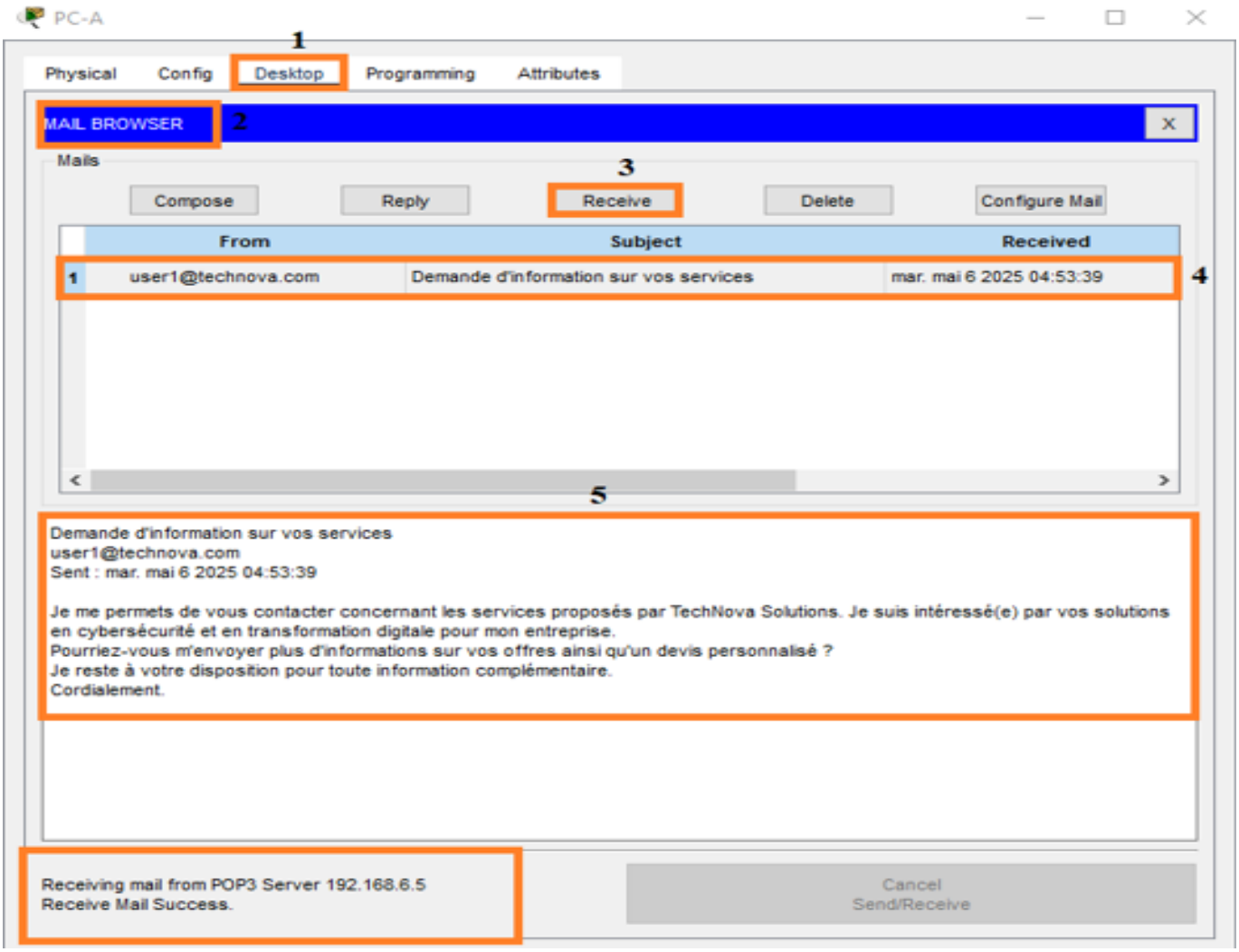

Figure 67: Le mail est bien reçu par le destinataire

IV.3.2.4. Configuration d'un VPN

Pour permettre à un employé distant d'accéder au réseau, tout en assurant la sécurité lors de l'échange de données, un VPN IPsec d'accès à distance a été configurer entre les deux routeurs R1 et R3, utilisant des protocoles de chiffrement et de sécurité.

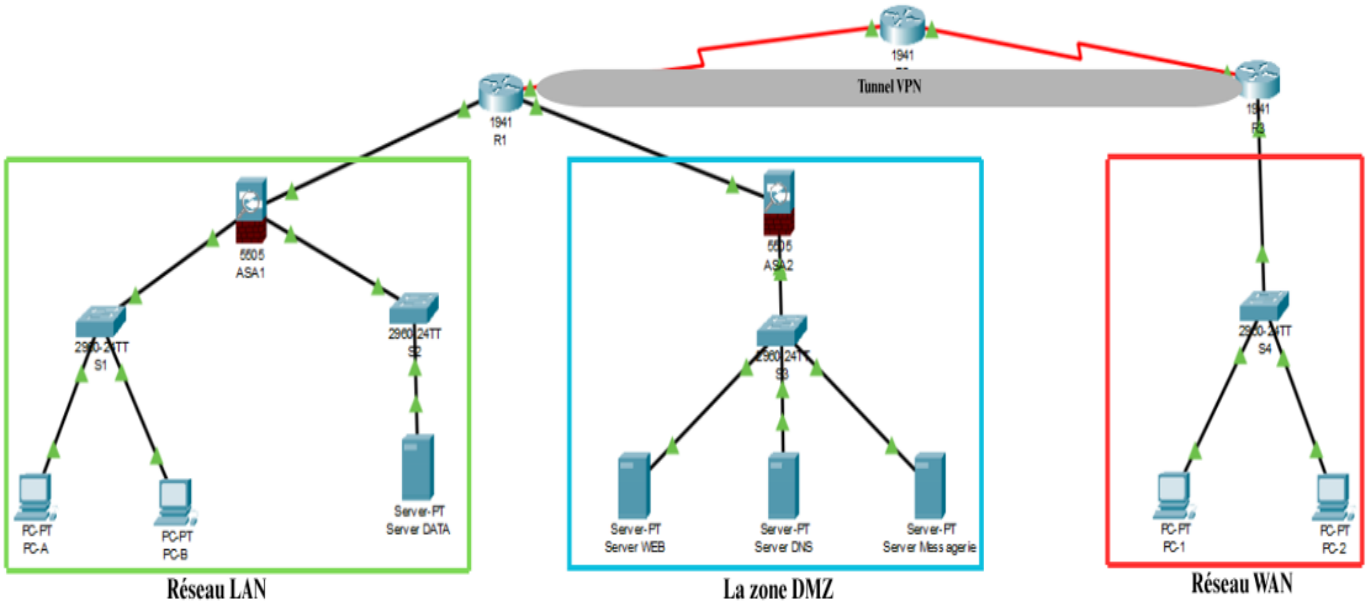

Figure 68: Tunnel VPN

Voici les étapes principales pour la création de ce VPN [17]:

Étape 1 : Création d'une liste d'accès 110 pour identifier le trafic à chiffrer sur R1 et R3, illustrée respectivement dans les figures 69 et 70.

```
R1(config)#access-list 110 permit ip 192.168.5.0 0.0.0.255 192.168.10.0 0.0.0.255
```

Figure 69: Création d'une liste d'accès sur R1

```
R3(config)#access-list 110 permit ip 192.168.10.0 0.0.0.255 192.168.5.0 0.0.0.255
```

Figure 70: Création d'une liste d'accès sur R3

Étape 2 : Définition de la politique ISAKMP, de la clé partagée et de l'adresse du pair (Phase 1) sur R1 et R3, illustrée respectivement dans les figures 71 et 72.

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)# encr aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)#exit
R1(config)#crypto isakmp key cisco address 194.1.2.1
```

Figure 71: Configuration de la phase 1 sur R1

```
R3(config)#crypto isakmp policy 10
R3(config-isakmp)# encr aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)#exit
R3(config)#crypto isakmp key cisco address 194.1.1.1
```

Figure 72: Configuration de la phase 1 sur R3

Étape 3 : Configuration du la **« transform-set VPN-SET »** et de la carte de chiffrement **« VPN-MAP »** (Phase 2), sur R1 et R3 comme le montrent les figures 73 et 74.

```
R1(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 194.1.2.1
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)#exit
```

Figure 73: Configuration de la phase 2 sur R1

```
R3(config)#crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 194.1.1.1
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)#exit
```

Figure 74: Configuration de la Phase 2 sur R3

Étape 4 : L'application de la carte de chiffrement à l'interface de sortie (WAN), sur R1 et R3 est présentée respectivement dans les figures 75 et 76.

```
R1(config)#int s0/0/0
R1(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Figure 75: Application de la crypto-map sur l'interface de sortie de R1

```
R3(config)#int s0/0/1
R3(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Figure 76: Application de la crypto-map sur l'interface de sortie de R3

IV.3.2.4.1. Vérification du tunnel VPN avant le trafic intéressant

- **Vérification du protocole ISAKMP**

Pour vérifier l'existence du protocole ISAKMP, nous utilisons la commande « **show crypto isakmp sa** » :

```
R1#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status

IPv6 Crypto ISAKMP SA
```

Figure 77: Vérification du protocole ISAKMP sur R1 avant le trafic intéressant

```
R3#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status

IPv6 Crypto ISAKMP SA
```

Figure 78: Vérification du protocole ISAKMP sur R3 avant le trafic intéressant

- **Vérification du protocole IPsec**

Pour vérifier le protocole IPsec, nous tapons la commande « **show crypto ipsec sa** » comme c'est montré dans les figures 79 et 80 pour les deux routeurs :

R1 :

```
R1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 194.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.5.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   current_peer 194.1.2.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 194.1.1.1, remote crypto endpt.:194.1.2.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)
```

Figure 79: Vérification du protocole IPsec sur R1 avant le trafic intéressant

R3 :

```
R3#show crypto ipsec sa

interface: Serial0/0/1
    Crypto map tag: VPN-MAP, local addr 194.1.2.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.5.0/255.255.255.0/0/0)
   current_peer 194.1.1.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 194.1.2.1, remote crypto endpt.:194.1.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/1
     current outbound spi: 0x0(0)
```

Figure 80: Vérification du protocole IPsec sur R3 avant le trafic intéressant

IV.3.2.4.2. Création du trafic intéressant (Test de connexion)

Pour tester la connexion VPN, nous envoyons une requête ping de PC-A (192.168.5.3) vers PC-1 (192.168.10.11) et vice versa :

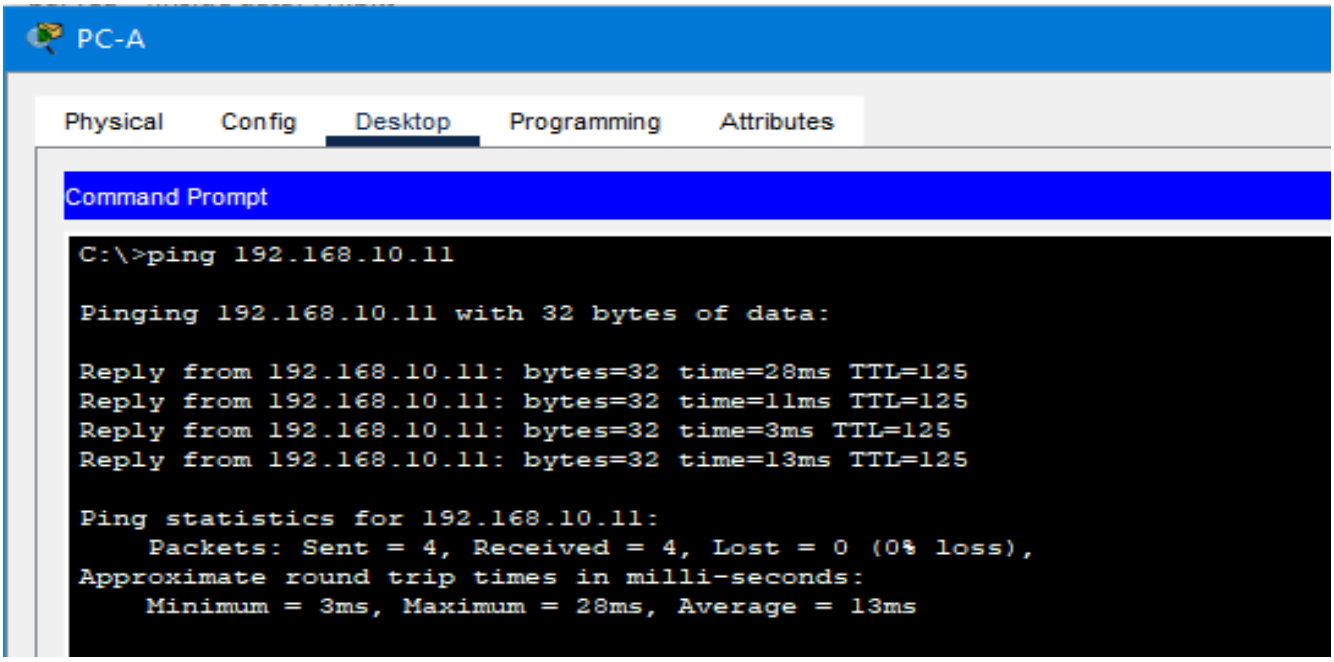

Figure 81: Ping depuis PC-A vers PC-1

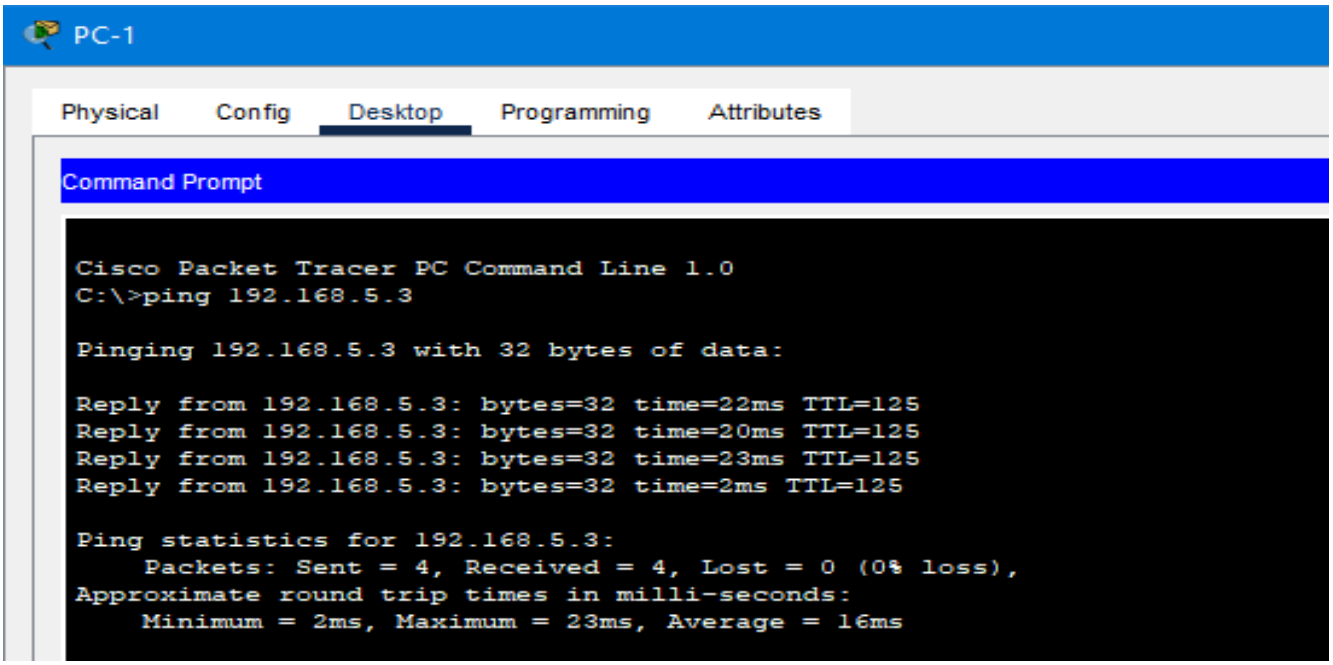

Figure 82: Ping depuis PC-1 vers PC-A

IV.3.2.4.3. Vérification du tunnel VPN après le trafic intéressant

- **Vérification de la crypto-map**

Avec la commande **« show crypto map »**, nous vérifions la création de la carte de chiffrement VPN-MAP sur R1 et R3 (figures 83 et 84 respectivement) :

R1 :

```
R1#show crypto map
Crypto Map VPN-MAP 10 ipsec-isakmp
        Peer = 194.1.2.1
        Extended IP access list 110
            access-list 110 permit ip 192.168.5.0 0.0.0.255 192.168.10.0 0.0.0.255
        Current peer: 194.1.2.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                VPN-SET,
        }
        Interfaces using crypto map VPN-MAP:
                Serial0/0/0
```

Figure 83: Vérification de la crypto-map sur R1 après le trafic intéressant

R3 :

```
R3#show crypto map
Crypto Map VPN-MAP 10 ipsec-isakmp
        Peer = 194.1.1.1
        Extended IP access list 110
            access-list 110 permit ip 192.168.10.0 0.0.0.255 192.168.5.0 0.0.0.255
        Current peer: 194.1.1.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                VPN-SET,
        }
        Interfaces using crypto map VPN-MAP:
                Serial0/0/1
```

Figure 84: Vérification de la crypto-map sur R3 après le trafic intéressant

- **Vérification du protocole ISAKMP**

R1 :

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
194.1.2.1       194.1.1.1       QM_IDLE           1004    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

Figure 85: Vérification du protocole ISAKMP sur R1 après le trafic intéressant

R3 :

```
R3#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
194.1.1.1       194.1.2.1       QM_IDLE           1090    0 ACTIVE

IPv6 Crypto ISAKMP SA
```

Figure 86: Vérification du protocole ISAKMP sur R3 après le trafic intéressant

- **Vérification du protocole IPsec**

Comme montre les figures 87 et 88 suivantes, le protocole IPSEC est bien configuré :

R1 :

```
R1#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 194.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.5.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   current_peer 194.1.2.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 0
   #pkts decaps: 25, #pkts decrypt: 25, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 194.1.1.1, remote crypto endpt.:194.1.2.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x49C5DA19(1237703193)
```

Figure 87: Vérification du protocole IPsec sur R1 après le trafic intéressant

R3 :

```
R3#show crypto ipsec sa

interface: Serial0/0/1
    Crypto map tag: VPN-MAP, local addr 194.1.2.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.5.0/255.255.255.0/0/0)
   current_peer 194.1.1.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 25, #pkts encrypt: 25, #pkts digest: 0
   #pkts decaps: 26, #pkts decrypt: 26, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 194.1.2.1, remote crypto endpt.:194.1.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/1
     current outbound spi: 0xB964B4B7(3110384823)
```

Figure 88: Vérification du protocole IPsec sur R3 après le trafic intéressant

Conclusion

Dans ce chapitre, nous avons étudié une stratégie multiprotocole ainsi que des mécanismes de sécurité pour protéger notre réseau LAN.

Les solutions implémentées comprennent la configuration de deux firewalls ASA utilisant des ACL, le NAT, le SSH, le DHCP, l'ICMP et la DMZ, dans le but d'assurer la sécurité et la disponibilité des données.

D'après les résultats de la simulation obtenue, il ressort que le réseau interne communique avec l'extérieur en toute sécurité et les utilisateurs externes peuvent accéder aux services exposés en DMZ.

Conclusion Générale

Conclusion générale

Dans ce travail, nous avons implémenté une politique de sécurité pour sécuriser une architecture d'une entreprise. L'objectif principal de l'étude est de concevoir et d'implémenter une solution qui devait assurer la sécurité des informations du réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies. Cette politique est basée sur la segmentation du réseau en zones de sécurité différentes dans lesquelles nous trouvons "Inside", "Outside" et "DMZ".

Cette décomposition s'est faite via les pare-feu que nous avons configuré et qui nécessitent l'utilisation des ACL (Access Control List), la traduction d'adresses NAT pour les interfaces et les protocoles de sécurité SSH (Secure Shell) pour administrer les firewalls à distance et le protocole DHCP (Dynamic Host Configuration Protocol) pour attribuer les adresses IP automatiquement.

Pour renforcer la sécurité des données échangées, nous avons utilisé une liaison spéciale, en plus du pare-feu, qui est le VPN d'accès à distance, de sorte que les données transmises dans un tunnel IPsec soient cryptées et cachées lors de la transmission sur Internet. Le VPN est très performant.

Pour réaliser notre simulation, nous avons choisi Cisco Packet Tracer, dans lequel nous avons réalisé une architecture d'entreprise, puis nous y avons implémenté deux pare-feu et un tunnel VPN IPsec d'accès à distance. Plusieurs tests ont été effectués pour vérifier les communications dans notre architecture. D'après ces tests, nous avons constaté que le réseau interne est bien protégé contre toute intrusion extérieure et que le tunnel VPN est fonctionnel, donc toutes les informations circulant à l'intérieur du tunnel seront protégées.

La solution de sécurité réalisée durant ce travail est à la portée de toutes les entreprises et sociétés. Elle peut être adaptée en fonction des besoins spécifiques de chaque entreprise.

Comme perspectives de ce travail, afin d'optimiser la sécurité et d'assurer en permanence la communication, il est intéressant d'intégrer une liaison MPLS (Multi-Protocol Label Switching) qui est une technologie de commutation utilisée par les opérateurs pour acheminer les données plus rapidement en utilisant des étiquettes (labels) au lieu des adresses IP classiques. Lorsqu'il est utilisé pour créer un VPN, nous parlons de VPN MPLS. Ce type de VPN permet de relier plusieurs sites d'une entreprise à travers le réseau privé d'un opérateur, sans passer par Internet. Le VPN MPLS offre ainsi une connexion sécurisée, performante et fiable, tout en garantissant une qualité de service grâce à la gestion prioritaire des différents

types de trafic (voix, vidéo, données, etc.). En résumé, le VPN MPLS est une application de la technologie MPLS au service des réseaux privés d'entreprise.

Les références bibliographiques

[1] **Lorenz, Pascal. (1994).** *Le temps dans les architectures de communication : application au réseau de terrain FIP* (Thèse de doctorat, Institut National Polytechnique de Lorraine).

[2] ***Support de cours*** *– Réseau FST – Chapitre 4 : Supports de transmission*

[3] **Université Mouloud Mammeri**. *Support de cours – VOIP – Chapitre 1 : Généralités et fondements de base.*

[4] **Université Mouloud Mammeri**. *Support de cours – VOIP – Chapitre 2 : Protocoles multimédia.*

[5] https://dspace.ummto.dz/server/api/core/bitstreams/a31ced85-6969-4324-af2f-42a5b7dd9a74/content (consulté le 20 mai 2025).

[6] **Kaspersky.** *Qu'est-ce qu'un pare-feu ? Fonctionnement des pare-feu et types de pare-feu*. Disponible sur : https://www.kaspersky.fr (consulté le 20 mai 2025).

[7] **Goueth.J.** *Routage entre réseaux locaux virtuels (VLAN)*, Le blog de Jacques Goueth. (consulté le 20 mai 2025).

[8]http://dlibrary.univboumerdes.dz:8080/jspui/bitstream/123456789/10216/1/Aliloui%2C%20Rania-Dahmani%2C%20Fatma%20Zohra.pdf (consulté le 20 mai 2025).

[9] **Guillaume Desgeorge.** La sécurité des réseaux, 2000. (consulté le 20 mai 2025).

[10] **AMRAR Salim.** *Mise en œuvre de la sécurité d'un réseau d'entreprise en utilisant les ACLs,* Mémoire de fin d'étude, Master Réseaux et Télécommunication, Université Mouloud Mammeri de Tizi-Ouzou, 2015/2016.

[11] **Université Abdelhamid Mehri - Constantine 2. (2020).** *Support de cours Systèmes et Réseaux d'Entreprise (SERE)*.

[12] https://fr.slideshare.net/slideshow/radius-et-tacacspptx/256820295 (consulté le 20 mai 2025).

[13] **IT-Connect.** *Qu'est-ce qu'une attaque DDoS ?*

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

[15] https://www.kaspersky.fr/resource-center/definitions/sql-injection/ what-is-dns-hijacking (consulté le 20 mai 2025).

[16] **BAJOU L. & BOUZIDI A.** *Mise en œuvre d'un réseau sécurisé en utilisant des protocoles de sécurité dans Cisco Packet Tracer*, Mémoire de fin d'études, Université Badji Mokhtar Annaba, Département d'Informatique, 2022.

[17] **TP Cisco Packet Tracer**. *Configuration de VPN (facultatif).*