La 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
MEGHENINE Assia

NEKMI Nawal

Thème

[Élaboration d'une synergie de protocoles de sécurité appliquée à un LAN]

Soutenu le : 24/06/2024

Devant le jury :

Promoteur :	Alouache. Dj	MCA	UMMTO
Co-promoteur :	Lazri. M	Professeur	UMMTO
Président :	Titouni. S	MCA	UMMTO
Examinatrice :	Ziani. N	MCB	UMMTO

Promotion : 2023/2024

Remerciements

La réalisation d'un projet de recherche n'est jamais attribuée uniquement à une seule personne. C'est pourquoi je tiens à remercier sincèrement et à exprimer ma gratitude à tous ceux qui, directement ou indirectement, ont contribué à l'avancement et au succès de ce travail.

En ce moment, nous aimerions exprimer notre sincère appréciation et notre profonde gratitude au Dieu Tout-Puissant et Miséricordieux, qui nous a accordé le courage, la détermination et l'endurance nécessaires pour mener à bien cette entreprise.

Nos vifs remerciements vont également aux membres du jury pour leur volonté d'examiner notre travail et de l'enrichir de leurs suggestions.

Ensuite, nous tenons à remercier notre encadreur ALOUACHE.D et notre co-encadreur LAZRI.M. Leurs conseils, commentaires et contributions écrites ont non seulement façonné nos réflexions, mais ont également alimenté notre détermination à exceller et à donner le meilleur de nous-mêmes. Nous sommes extrêmement reconnaissants de leur confiance inébranlable en nos capacités et de leurs encouragements constants.

De plus, nous tenons à exprimer notre plus sincère gratitude à notre encadreur de stage M. HADDOUS ABDENOUR et à son équipe pour leur soutien et leur assistance inestimables tout au long de notre parcours de recherche. Et à tous mes enseignants.

Enfin, on aimerait exprimer notre gratitude à nos familles et nos amis qui nous ont toujours encouragées dans la poursuite de nos études, ainsi que pour leurs aides, leurs compréhensions et leurs soutiens.

Dédicace 1

Je suis rempli d'un immense bonheur alors que je présente ce travail, témoignage des efforts que j'ai consacrés à mon parcours académique, comme un dévouement sincère aux chères personnes qui ont joué un rôle indispensable dans mes réalisations.

Je dédie le fruit de mes études à mes chers parents, dont les sacrifices inébranlables, l'amour sans limites, les soins doux, le soutien indéfectible et les prières sincères ont été une source constante d'inspiration tout au long de mes efforts académiques.

De plus, j'exprime mon sincère gratitude à ma chère sœur Zahra et mes frères, Islam et Adem, dont les encouragements indéfectibles et le soutien moral ont joué un rôle déterminant dans ma réalisation, ainsi qu'à toute ma famille et mes chères amis Menad, Lounes, Sofiane, Amel, Lina et Malha pour leurs soutien continu tout au long de mon parcours universitaire.

J'espère que ce travail vous apportera la satisfaction que vous désirez depuis longtemps et qu'elle reflète le soutien indéfectible que vous avez toujours apporté.

Je suis profondément reconnaissant pour votre présence constante dans ma vie.

Dédicace 2

J’apporte une grande joie de dédier ce travail, aux personnes chères qui ont joué un rôle essentiel dans ma réussite.

Je suis incroyablement reconnaissant envers mes parents, qui m’ont comblé d’amour, de conseils et d’un soutien indéfectible tout au long de mon parcours universitaire. Leur soutien moral et financier m'a permis de poursuivre les études de mon choix et de réaliser ce mémoire. Un grand merci à eux deux.

Je tiens à exprimer ma plus profonde gratitude à mon mari, qui a toujours été à mes côtés. Votre amour compte pour moi et je chéris notre lien. Que ce soit dans les moments de joie ou de chagrin, tu as toujours été là pour moi, offrant ta présence inébranlable. J'ai une confiance totale en votre fiabilité et je sais que vous me soutiendrez toujours. Merci d'être un mari et un ami si incroyable.

Je dédie ce travail à mon frère Salem, ma sœur Yasmine, mes amis Menad, Sofiane, Lounes, Amel, Lina et Malha, mes sincères remerciements vont à chacun d’entre vous ! pour votre soutien inestimable qui a joué un rôle central dans la transformation de mes aspirations en réalisations tangibles.

Vos conseils ont éclairé la trajectoire vers mon triomphe, et je vous remercie sincèrement.

Sommaire

Chapitre Ⅱ: Généralités sur la sécurité informatique

Chapitre Ⅲ: Étude de l'architecture initiale et proposition des solutions de sécurité

Chapitre Ⅳ: Vérifications et tests de connectivité

Liste des tables

Liste des figures

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

ACL : **A**ccess **C**ontrol **L**ist

ARP : **A**ddress **R**esolution **P**rotcol

ASA : **A**daptive **S**ecurity **A**ppliance

DHCP : **D**ynamic **H**ost **C**onfiguration **P**rotocol

DMZ : **D**e**m**ilitarized **Z**one

DOS : **D**isk **O**perating **S**ystem

ERSTC: **É**tablissement **R**égional **S**upport **T**echnique au **C**ommercial

HD : **H**igh **D**efinition

ICMP : **I**nternet **C**ontrol **M**essage **P**rotocol.

IEEE : **I**nstitue of **E**lectrical and **E**lectronics **E**ngineers

IP : **I**nternet **P**rotocole

IPS : **I**ntrusion **P**revention **S**ystems

LAN : **L**ocal **A**rea **N**etwork

LCD : **L**iquid **C**rystal **D**isplay

MAC : **M**edia **A**ccess **C**ontrol

MAN : **M**étropolitain **A**rea **N**etwok

MITM : **M**an **I**n **T**he **M**iddle

NAT : **N**etwork **A**ddress **T**ranslation

OSI : **O**pen **S**ystems **I**nterconnexion

PAN : **P**ersonal **A**rea **N**etwork

SSH : **S**ecure **S**ocket **S**hell

TCP : **T**ransfert **C**ontrôl **P**rotocol

TFTP : **T**rivial **F**ile **T**ransfer **P**rotocol

VoIP : **V**oice **o**ver **I**nternet **P**rotocol

VLAN : **V**irtual **L**ocal **A**rea **N**etwork

VPN : **V**irtual **P**rivate **N**etwork

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

Introduction

Un réseau informatique est une grille de micro-ordinateurs interconnectés destinés à assurer le transfert de fichiers, le partage de ressources (imprimantes et données), les opérations de messagerie ou encore l'exécution et la maintenance de programmes à distance[1]. Quel que soit le type de systèmes informatiques utilisés au sein d'une entreprise, les réseaux qu'ils forment entre eux sont aujourd'hui essentiels. Les objectifs d'un réseau sont multiples, comme le partage des ressources informatiques et le transfert plus rapide des informations entre les différents partenaires d'une entreprise (employés, managers, fournisseurs, etc.) [2].

Avec le développement de la technologie de nos jours l'utilisateur a accès à toutes les ressources informatiques, grâce à une réelle distribution des applications. La connexion du réseau d'entreprise au réseau Internet a rendu l'ensemble de ses ordinateurs vulnérables aux intrusions et aux risques d'attaques informatiques. A cet effet, le concept de la sécurité de réseau est mis au point.

La sécurité des réseaux informatiques est un sujet important qui favorise la communication et le développement dans divers domaines. Compte tenu de l'expansion et de l'importance croissante des réseaux informatiques, ces réseaux créent des problèmes de sécurité pour les systèmes d'information ; dans la plupart des organisations informatisées, le partage de données directement entre machines est leur principale préoccupation[3]. Les mesures de sécurité doivent être renforcées pour maintenir la confidentialité, l'intégrité et le contrôle d'accès du réseau afin de réduire le risque d'attaque.

Dans ce contexte, nous développons une stratégie de sécurité basée sur l'implémentation de plusieurs protocoles. Cette stratégie est appliquée pour sécuriser le réseau informatique du LAN de l'entreprise d'Algérie Telecom /Direction opérationnelle de wilaya de Tizi ouzou, service ERSTC où nous avons effectué un stage pratique (voir chapitre 3). Dans cette sécurité, nous avons combiné trois protocoles, à savoir un pare feu, des VLAN et

des mots de passe dans les Switch et routeur. Nous avons aussi ajouté à l'architecture une DMZ. Des tests de vérification sont réalisés et ont montré de bonnes performances.

Notre mémoire est structuré en quatre chapitres et une conclusion. Le premier chapitre aborde des généralités sur les réseaux informatiques et ses classifications ainsi que les équipements d'interconnexion. Dans le deuxième chapitre nous allons détaillés le concept de la sécurité réseau et son impact sur les réseaux informatique, tant dis que le chapitre trois étudié une architecture réseau existé et simule des solutions améliorant sa qualité de transmission et de sécurité. Enfin on termine avec un quatrième chapitre contenons des vérifications et tests que nos solutions sont bien placé et une conclusion.

Chapitre I:

Généralités sur les réseaux informatiques

I.1 Préambule

Avant l'avènement des réseaux informatiques, le transfert de données entre ordinateurs était difficile. De nos jours, avec le développement de la technologie, la vitesse de réponse du réseau est si rapide qu'elle affecte tous les aspects de notre vie quotidienne : affaires, banque, travail, etc. Grâce à leur polyvalence et à leur utilisation mondiale, ils peuvent partager des applications, échanger des informations, consulter des bases de données et effectuer des transferts de fichiers entre plusieurs postes distants.

L'objectif de ce chapitre est de décrire le réseau informatique tout en donnant les différentes architectures, ses différents équipements pour sa réalisation, ainsi que les supports de transmission. Aussi, les protocoles de communication, à savoir le modèle OSI et TCP/IP font l'objet de ce chapitre.

I.2 Généralités sur les réseaux

I.2.1 Définition

Un réseau informatique est un système de communication qui permet à plusieurs appareils informatiques, tels que des ordinateurs, des serveurs, des imprimantes, des routeurs, etc., de se connecter et de partager des informations entre eux. Ces appareils sont connectés les uns aux autres par des câbles, des fibrages optiques ou des connexions sans fil, ce qui leur permet de communiquer et d'échanger des données.

I.2.2 Objectifs d'un réseau informatique

Un réseau informatique présente plusieurs avantages :

- **Partage des ressources :** tels que des fichiers, des scanners, des bases de données, etc.
- **Communication et collaboration :** les utilisateurs peuvent échanger des informations et collaborer sur des projets, même s'ils sont géographiquement séparés.
- **Accès à distance :** les utilisateurs peuvent d'accéder à distance à leurs fichiers et à leurs applications, à partir de n'importe quel emplacement.
- **Accès à l'internet :** les utilisateurs peuvent connecter à internet et de profiter des nombreux services en ligne tels que la recherche d'informations, la messagerie électronique, le commerce électronique, etc.

- **Centralisation de la gestion :** permet de garantir la cohérence des données à travers l'ensemble du réseau, la gestion des ressources, réduit les couts liés à la maintenance et à la sécurité.
- **La sécurité :** permet la mise en place des mesures de sécurité pour protéger les données et les ressources partagées.

I.2.3 Classification des réseaux

Les réseaux informatiques peuvent être classés en fonction de leur taille et de leur portée, de leur architecture de topologie, de leur mode de transmission, et de leur mode de communication.

I.2.3.1 Classification selon la taille et la portée

On trouve Quatre types : Les réseaux PAN, LAN, MAN, WAN.

a) Réseaux PAN : (Personal Area Network)

Ces réseaux interconnectent les appareils personnels d'un même utilisateur sur quelques mètres.

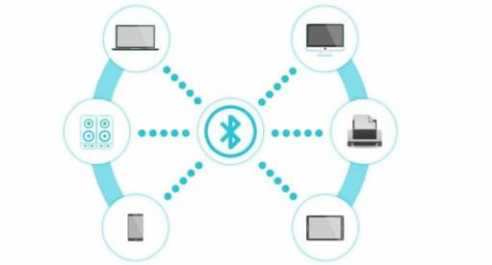

Figure I.1 : Réseau PAN

b) Réseaux LAN : (Local Area Network)

Les réseaux locaux ce sont des réseaux de petite taille qui couvrent une zone géographique limitée, telle qu'un bureau, une maison, une école ou un bâtiment. Les LAN sont généralement utilisés pour permettre le partage de ressources au sein d'une organisation ou d'un groupe restreint d'utilisateurs.

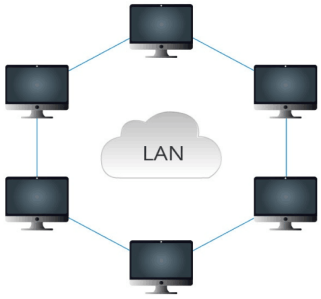

Figure Ⅰ.2 : Réseau LAN

c) Réseaux MAN : (Métropolitain Area Network)

Les réseaux métropolitains ce sont des réseaux de taille intermédiaire qui couvrent une zone métropolitaine, comme une ville ou une région urbaine. Les MAN offrent des connexions haut débit à des organisations ou à des fournisseurs de services internet.

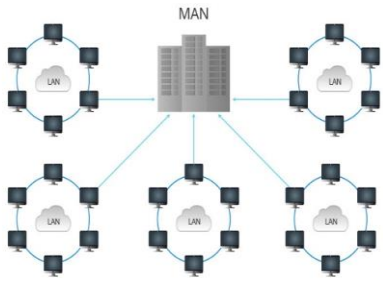

Figure Ⅰ.3 : Réseau MAN

d) Réseaux WAN : (Wide Area Network)

Les réseaux étendus ce sont des réseaux qui couvrent de vastes distances géographiques, tels que des connexions entres des sites distants ou des connexions de longue distance à travers des fournisseurs de services internet. Les WAN permettent de relier plusieurs LAN situés dans différentes régions géographiques.

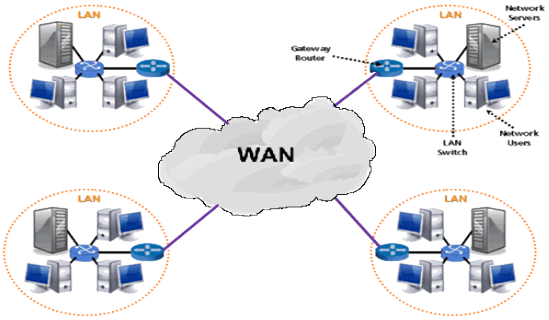

Figure Ⅰ.4 : Réseau WAN

I.2.3.2 Classification selon l'architecture de topologie

L'architecture de topologie décrit la manière dont les appareils sont connectés et interagissent les uns avec les autres. On distingue les topologies suivantes :

a) Topologie en bus

C'est l'organisation la plus simple d'un réseau (voir figure I.5). En effet, dans cette topologie tous les appareils sont connectés à un seul câble principal, appelé bus. Les données sont transmises sur le bus et tous les appareils peuvent les recevoir. Cependant, si le câble principal est endommagé, tout le réseau peut être affecté.

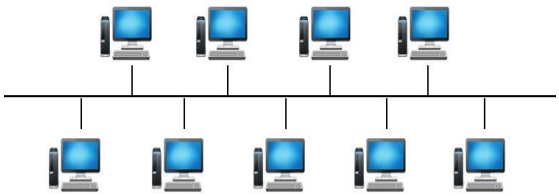

Figure I.5 : Topologie en bus

b) Topologie en étoile

Dans une topologie en étoile, tous les appareils sont connectés à un concentrateur central, également appelé commutateur ou routeur (voir figure I.6). Chaque appareil est connecté individuellement au concentrateur. Si un appareil est déconnecté ou tombe en panne, les autres appareils du réseau ne sont pas affectés.

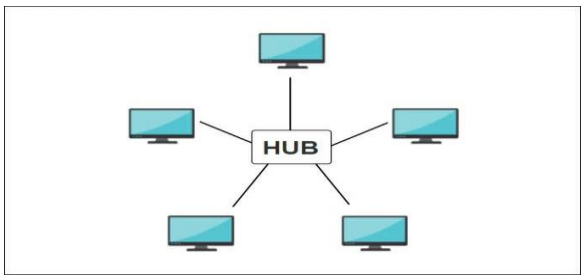

Figure I.6 : Topologie en étoile

c) Topologie en anneau

Dans un réseau possédant une topologie en anneau, chaque appareil est connecté à deux autres appareils, formant un anneau fermé (voir figure I.7). Les données circulent en boucle dans l'anneau, d'appareil en appareil. Chaque

appareil agit comme un répéteur pour relayer les données au suivant. Si un appareil tombe en panne, cela peut affecter la communication sur tout l'anneau.

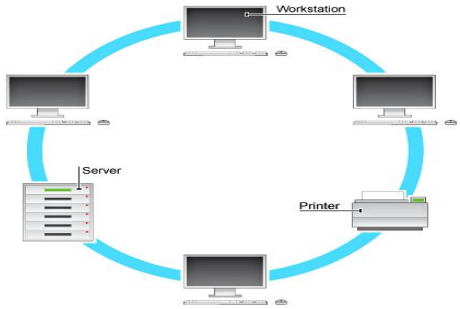

Figure Ⅰ.7 : Topologie en anneau

d) Topologie en arbre

Dans cette architecture les appareils sont connectés selon une structure hiérarchique en forme d'arbre à un commutateur qui est connecté aux sous-réseaux ou aux dispositifs de niveau inférieur (voir figure Ⅰ.8). Cette topologie permet de gérer efficacement de grands réseaux avec des sous-réseaux distincts.

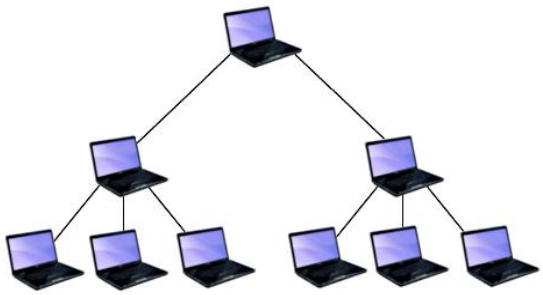

Figure Ⅰ.8 : Topologie en arbre

e) Topologie en maillage

Une topologie maillée (voir figure Ⅰ.9) correspond à plusieurs liaisons points à points. Cette architecture offre une grande redondance et une fiabilité élevée, car plusieurs chemins de communication sont disponibles. Cependant, cela peut nécessiter de nombreux câbles et connexions, rendant le déploiement et la gestion plus complexes.

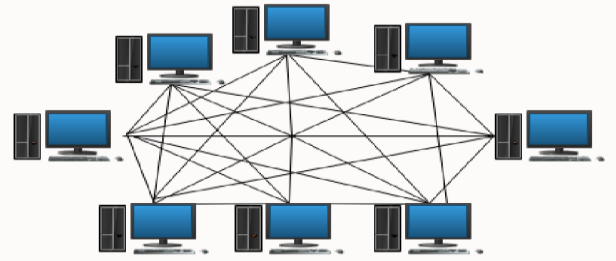

Figure Ⅰ.9 : Topologie maillée

- Ces architectures de topologie peuvent être utilisées individuellement ou combinées pour former des réseaux plus complexes et adaptables en fonction des besoins spécifiques de l'organisation.

Ⅰ.2.3.3 Classification selon leur mode de transmission

Les modes de transmission décrit la manière dont les données sont transmises et reçues entre les appareils connectés. On distingue les modes suivants :

a) Réseaux terrestres câblés

Ce sont des réseaux qui utilisent des câbles physiques pour transmettre les données, ils offrent des performances plus rapides et plus fiable. Par exemple :

- ✓ **La fibre optique**

Utilisé pour transmettre des données à des vitesses élevées sur de langues distances sans perte de signal, car elle est insensible aux interférences électromagnétiques. Elle utilise la lumière comme moyen de transmission des signaux au lieu des signaux électriques utilisés dans les câbles traditionnels en cuivre [1]. La fibre optique est composées d'un mince filament de verre ou de plastique, appelé « fibre », qui transmettre la lumière. Elle est entourée d'une gaine protectrice, pour la protéger des dommages externes.

Figure Ⅰ.10 : Fibre optique

- ✓ **Les câbles coaxiaux**

Utilisés pour transporter des signaux électriques à haute fréquence sur de courtes distances. Ils sont composés d'un conducteur central généralement en cuivre, qui transporte le signal électrique, entouré d'une gaine isolante généralement en plastique, qui le sépare du blindage métallique, ce blindage est généralement en cuivre ou en aluminium, protège le conducteur central et enfin une gaine externe, également en plastique, assure la protection mécanique du câble [1].

Figure Ⅰ.11 : Câble coaxial

- ✓ **Les câbles à paire torsadée**

Sont un type de câbles utilisés pour connecter des appareils dans les réseaux de communication. Ils sont constitués de paires de fils de cuivre isolés, torsadés ensemble pour réduire les interférences électromagnétiques [1].

Figure Ⅰ.12 : Paire torsadée

b) Réseaux sans fil

Les réseaux sans fil sont des réseaux qui utilisent des forme de rayonnement électromagnétique (ondes radio, des micro-ondes ou des infrarouges) pour transmettre les données sans câblage physique.

c) Réseaux à commutation de paquets

Les réseaux à commutation de paquets sont des réseaux qui transmettent les données sous forme de petits paquets de données indépendants. Ces données sont envoyées individuellement sur le réseau et peuvent emprunter des chemins différents pour atteindre leur destination.

I.2.3.4 Classification selon le mode de communication

On distingue deux types :

a) Réseau client serveur

Un client est un système (ordinateur ou programme) qui se connecte à un réseau pour obtenir des informations. Son rôle principal est de communiquer avec le serveur en envoyant des requêtes pour demander des informations ou des actions spécifiques.

Un serveur est un dispositif matériel ou logiciel qui répond aux demandes des clients et fournit des services, des ressources ou des données demandés par les clients.

L'interaction entre le client et le serveur aboutit à une architecture client-serveur.

En effet l'architecture client-serveur (voir figure I.13) spécifie un modèle de communication entre plusieurs ordinateurs sur un réseau, distinguant une ou plusieurs stations serveur. La communication passe par le dialogue entre deux processus. En d'autres termes, le client demande des informations qu'ils doivent être obtenus auprès du serveur.

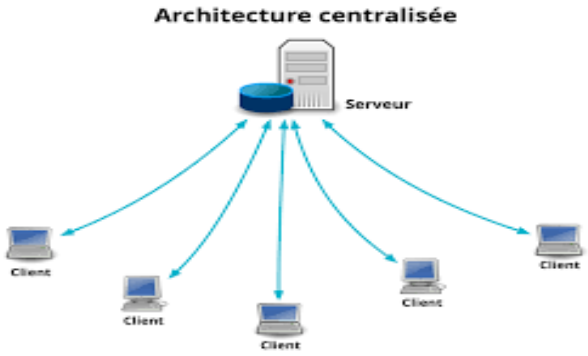

Figure I.13 : Réseau client serveur

- **Avantage**

- La possibilité de prendre en charge un grand nombre de clients
- La sécurité accrue

- **Inconvénient**

- La dépendance des clients vis-à-vis des serveurs
- Le risque de surcharge des serveurs

b) Réseau poste à poste

Contrairement à une architecture de réseau de type client/serveur (voir figure Ⅰ.14), les ordinateurs se connectent directement les uns aux autres pour partager des ressources, des données ou des services sans nécessiter de serveur central [2].

Dans ce type chaque ordinateur peut agir à la fois en tant que client et en tant que serveur, Cela signifie que chacun des ordinateurs du réseau est libre de partager ses ressources.

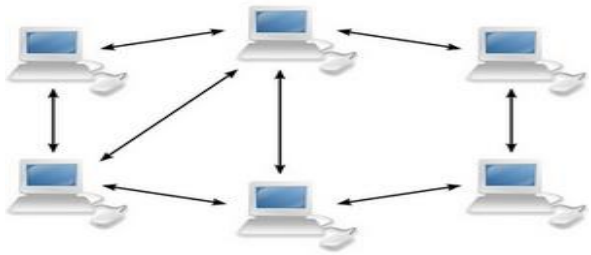

Figure Ⅰ.14 : Réseau poste à poste

- **Avantage**

- La réduction de la dépendance sur un serveur centralisé
- La capacité de tolérance aux pannes

- **Inconvénient**

- Faible sécurité
- Absence de contrôle d'accès aux données

I.2.4 Equipements d'interconnexion

Les équipements d'interconnexion sont des dispositifs matériels utilisés pour connecter les différents composants d'un réseau informatique. Ces équipements permettent d'acheminer les données entre les différents nœuds du réseau, de créer des connexions et de faciliter la communication entre les appareils connectés.

L'interconnexion de réseaux peut être locale ou distant. Dans le cas des réseaux qui sont sur le même site géographique, un équipement standard (répéteur, routeur, etc..) suffit à réaliser physiquement la liaison. Si les réseaux dont distants, il est alors nécessaire de relier ces réseaux par une liaison téléphonique (modems, etc..).

- ✓ **Commutateur (Switch)**

Un commutateur appelé aussi Switch (voir figure I.15), est un appareil qui connecte plusieurs segments (câbles ou fibres optiques) dans les réseaux informatiques et de télécommunications.

Le commutateur crée et met à jour une table de routage, qui dans le cas d'un commutateur Ethernet est la table d'adresses MAC, qui lui indique quels ports dirigent les trames à envoyer vers un certain port.

Figure I.15 : Commutateur

- ✓ **Router**

Un routeur (voir figure I.16) également appelé commutateur de niveau 3 car c'est là que s'effectuent le routage et l'adressage, est un équipement qui Permet d'interconnecter deux ou plusieurs réseaux. Ont les mêmes composants base que l'ordinateur, le routeur choisit le chemin approprié (via la table Routage) dirige les messages vers leur destination.

Figure Ⅰ.16 : Router

✓ **Répéteur**

Un répéteur (voir figure Ⅰ.17) est un appareil qui étend la portée de réseau et améliorer la couverture dans les zones où le signal est faible.

Le rôle principal de cet élément est de recevoir un signal existant provenant d'un routeur ou d'un point d'accès sans fil, de le renforcer, puis de le retransmettre afin d'augmenter la portée du réseau.

Figure Ⅰ.17 : Répéteur

✓ **Concentrateur (Hub)**

Un hub (voir figure Ⅰ.18) est un répéteur qui transmet des signaux via plusieurs ports d'entrée et de sortie. Lorsqu'il reçoit un signal sur un port, il le retransmet vers tous les autres ports, sans distinction, ce qui peut provoquer des collisions de données.

Figure Ⅰ.18 : Concentrateur

✓ **Passerelle**

C’est un système matériel et logiciel permettant de faire la liaison entre deux réseaux de télécommunications, aux caractéristiques différentes (voir Figure I.19).

Lorsque l’utilisateur d’un réseau souhaite accéder à un réseau utilisant un protocole différent, la Gateway examine la légitimité de sa demande, si celle-ci respecte les conditions fixées par l’administrateur du réseau visé, alors la Gateway établit une liaison entre les deux réseaux.

Figure I.19 : Passerelle (Gateway)

✓ **Pont**

Le pont est un organe qui possède des capacités cognitives lui permettant d'identifier la destination des blocs d'informations lorsqu'ils traversent le support physique (voir figure I.20). Sa fonction consiste à trier les trames et à permettre le passage de blocs spécifiquement destinés au réseau auquel il est connecté. En termes simples, le pont relaie uniquement les trames contenant des adresses correspondant aux machines situées au sein du réseau connecté.

Figure I.20 : Pont

I.2.5 Protocoles de communication

Un protocole est un ensemble précis de règles utilisées pour coordonner les communications entre différentes entités de réseau. D’une manière générale, tout accord responsable d’une fonction très spécifique et de cette fonction uniquement.

I.2.5.1 Modèle OSI : (Open Systems Interconnexion)

Afin de standardiser les protocoles de communication des réseaux informatiques, L'ISO (Organisation internationale de normalisation) a publié un modèle théorique de référence décrivant les opérations de communication en réseau qui est le modèle OSI (Open Systems Interconnexion) [3]. Tel qu'il est illustré sur la figure ci-dessous, la référence OSI comporte sept catégories de protocoles, appelés couches. Chaque couche offre un certain nombre de fonctionnalités.

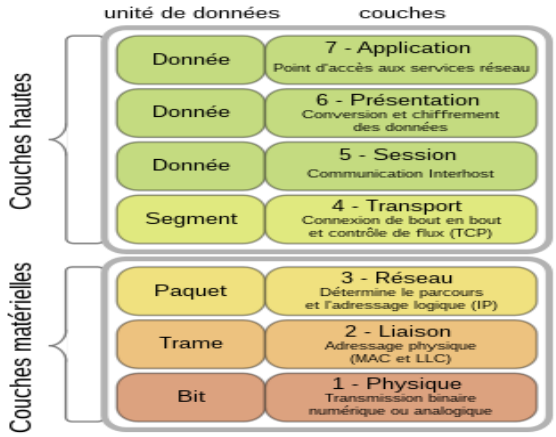

Figure I.21 : Modèle OSI

❖ Les sept couches de modèle OSI sont les suivantes :

- **Couche 1 : physique**

Son rôle est de fournir un support de transmission de communication. Il assure l'établissement et le maintien des connexions physiques. Il comprend donc les spécifications mécaniques et les spécifications électriques.

- **Couche 2 : liaison de données**

Il permet aux machines connectées entre elles de communiquer et son autre rôle important est de détecter les erreurs de transmission. Il garantit que les connexions logiques sont maintenues, Transmission de blocs de données (trame et paquet), détection et correction d'erreurs.

- **Couche 3 : réseau**

Cette couche gère l'adressage à trois niveaux, la sélection du chemin et Le routage des paquets de données à travers un réseau. La couche transport rassemble des règles opérationnelles de bout en bout pour garantir La transparence du réseau par rapport aux couches supérieures. Il s'agit spécifiquement de répondre, Établir la connectivité et la fiabilité des transports.

- **Couche 4 : transport**

La couche transport rassemble des règles opérationnelles de bout en bout pour garantir La transparence du réseau par rapport aux couches supérieures. Il s'agit spécifiquement de répondre, Établir la connectivité et la fiabilité des transports.

- **Couche 5 : session**

Il assure l'échange de données et les transactions entre deux applications distantes. Il assure également la synchronisation et l'ordonnancement des échanges en détectant et en restaurant les échanges lorsque des erreurs surviennent.

- **Couche 6 : présentation**

La couche présentation précise le format des données de l'application (codage MIME, compression, chiffrement).

- **Couche 7 : application**

Cette couche fournit l'interface avec l'application et est la couche la plus proche de l'utilisateur.

I.2.5.2 Modèle TCP/IP : (transfert contrôle protocole / internet protocole)

Un autre modèle simplifié, a vu le jour : le modèle TCP/IP. Ce dernier gouverne aujourd'hui presque tous les réseaux de la planète [4]. Cela représente une simplification du modèle OSI, en regroupant plusieurs couches en quatre couches, comme montre la figure ci-dessous :

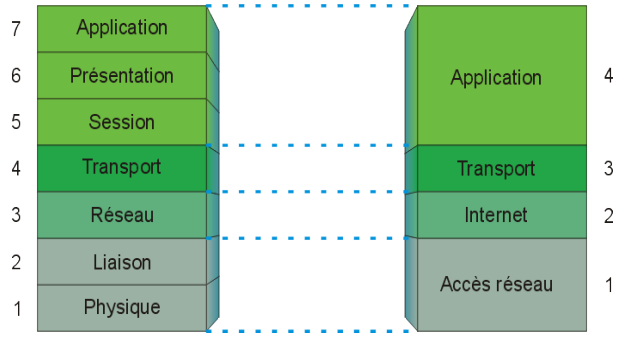

Figure Ⅰ-22 : Modèle TCP/IP

TCP/IP représente en quelque sorte toutes les règles de communication sur Internet Basé sur le concept d'adressage IP, ce qui signifie fournir à chaque appareil une adresse IP Machines en réseau pour pouvoir acheminer les paquets.

❖ Les couches de modèle TCP/IP sont les suivantes :

- **Couche 1 : accès réseau**

  Elle précise la forme sous laquelle les données doivent être transmises quel que soit le type de réseau utilisé.

- **Couche 2 : internet**

  Elle est chargée de fournir les datagrammes.

- **Couche 3 : transport**

  Elle assure le l'acheminement des données, ainsi qu'un mécanisme qui nous permet de connaître l'état du transfert

- **Couche 4 : application**

  Elle englobe les applications standards du réseau.

✓ La **Table Ⅰ.1** donne une comparaison entre les deux modèles.

Modèle OSI	Protocoles	Modèle TCP/IP
Couche application	DNS, SMTP, VOIP…	Couche application
Couche présentation	MIME, HTML, XML, MPEG, Vidéotex…	
Couche session	Telnet, SSH, FTP, HTTP, HTTPS...	
Couche transport	TCP, UDP…	Couche transport
Couche réseau	IPv6, IPv4, RIP, IGRP, OSPF, ICMP…	Couche internet
Couche liaison de données	Ethernet, Token Ring, FDDI, WIFI…	Couche accès au réseau
Couche physique	Médias réseaux et codage (NRZ, Miller…)	

Table Ⅰ.1 : Protocoles des modèles OSI et TCP/IP

Ⅰ.2.6 Architecture logique d'un réseau

Une architecture logique d'un réseau informatique désigne la manière dont laquelle les données sont transmise par le réseau.

Ⅰ.2.6.1 Adressage IP

Sur Internet, les ordinateurs communiquent entre eux via le protocole Internet (IP), qui utilise des adresses numériques (appelées adresses IP), de sorte que chaque ordinateur du réseau possède une adresse IP unique sur le réseau. Une adresse IP (Internet Protocol) est constituée d'un nombre binaire de 32 bits. Pour faciliter la lecture et la manipulation de cette adresse on la représente plutôt en notation décimale pointée. Par exemple :

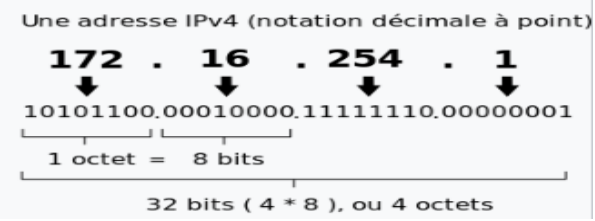

Figure Ⅰ.23 : Adresse IP

a) Structure

L'adresse IP identifie l'emplacement d'un hôte sur le réseau, codée sur 4 octets, contient un identifiant de réseau (Net ID) et un identifiant d'hôtes (Host ID), comme montre l'exemple de la figure ci-dessous :

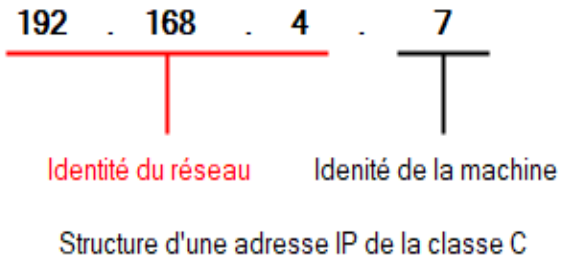

Figure Ⅰ.24: Structure d'adresse IP

Dans le cas d'un réseau « standard » (pas de sous-réseaux), la partie identifiant du réseau peut être codée sur 1, 2 ou 3 octets. Le nombre de bits restant dans la partie ID d'hôte détermine le nombre de périphériques pouvant se connecter au réseau.

b) Classes d'adresse IP

En fonction de nombre d'appareils (machines) pouvant se connecter au réseau, une adresse IP est classée en cinq classes A, B, C, D ou E (voir figure Ⅰ.25), le nombre d'hôtes (machine) et de sous-réseaux varie d'une classe à l'autre.

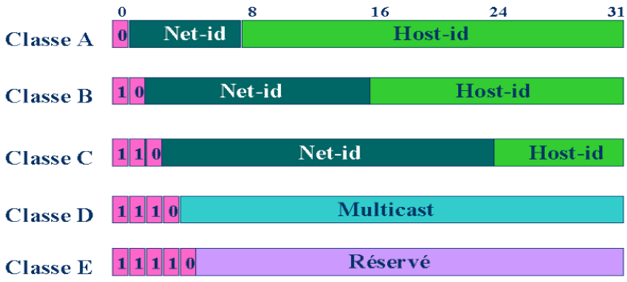

Figure Ⅰ-25: Classes d'adresse IP

✓ La **Table Ⅰ.2** donne le nombre de machines/ Sous-réseaux dans chaque classe

A	1. x. y. z à 127. x. y. z 127 réseaux 16 777 216 machines (2^24)
B	128.0. x. y à 191.255. x. y 16 384 réseaux (2^14) 65536 machines (2^16)
C	192.0.0. z à 223.255.255. z 2097152 réseaux (2^21) 256 machines (2^8)
D	244.0.0.0 à 239.255.255.255
E	240.0.0.0 à 247.255.255.255

Table Ⅰ.2 : Nombres de machines/ Sous-réseaux dans chaque classe

Ⅰ.2.6.2 Plan d'adressage

Lorsque vous devez créer un réseau d'entreprise limité à un seul site ou interconnectant différents sites de votre organisation, des plans d'adressage doivent être pris en compte. Le but de cette opération est de définir une adresse IP pour chaque réseau physique (LAN et WAN). Chaque ordinateur, chaque composant actif doit disposer d'un moyen d'être identifié sur le réseau. Pour cela, attribuez-lui une adresse IP. Il existe deux types d'adressage IP, **«** Privé» qui permet la communication interentreprises, et « Public » qui est utilisé pour communiquer avec Internet. Des organismes spécialisés fournissent des adresses IP publiques. Par conséquent, vous devez définir un plan d'adressage IP privé.

Ⅰ.2.6.3 Routage

Les réseaux IP et Internet sont constitués d'un ensemble de réseaux connectés via des machines spécifiques appelées routeurs. Pour les communications au sein de ces réseaux, le protocole IP est capable de sélectionner un chemin, également appelé route, le long du quel les paquets seront progressivement relayés vers le destinataire. C'est ainsi que le routage IP fonctionne de manière totalement décentralisée au niveau des machines qui composent le réseau. Personne n'a une idée complète de l'itinéraire qu'empruntera un paquet.

I.2.6.4 Adressage MAC

Une adresse MAC est une adresse de couche liaison de données standardisée requise par chaque unité connectée à un réseau local. C'est l'adresse qui représente la carte réseau. L'adresse MAC est composée de 6 octets et sa structure est standardisée par l'IEEE. Il est divisé en deux parties d'égale longueur. Le plus important identifie le fabricant de la carte réseau, tandis que le moins important est attribué de manière unique à chaque carte réseau par le fabricant lui-même. Cette paire garantit que l'adresse MAC est globalement unique. Également appelée adresse matérielle, adresse de couche MAC ou adresse physique.

I.3 Discussion

Dans ce chapitre, nous avons décrit les concepts généraux liés aux réseaux informatiques pour partager le serveur (offre beaucoup de flexibilité). Parmi ces concepts, nous avons discuté de la classification de ces derniers selon leur étendue géographique, la topologie d'un réseau LAN et ses composants matériels et son adressage sont également abordés. Comprendre ces concepts est une étape nécessaire pour appréhender pleinement l'environnement réseau. La mise en réseau permet d'accéder à un grand nombre de ressources, c'est pourquoi nous constatons une demande croissante d'utilisation du réseau. En conséquence, le risque d'attaques effectué par des logiciels malveillants augmente et la mise en place d'une solution de protection est indispensable. Le prochain chapitre comprendra une présentation des types d'attaque et une liste de protocoles de sécurité qui peut être implémentée.

Chapitre II :

Généralités sur la sécurité informatique

Ⅱ.1 Préambule

Les réseaux informatiques sont devenus un outil essentiel pour la plupart des gens et les entreprises, elles l'utilisent pour échanger des informations avec leurs bureaux institutions, des bureaux aux domiciles, les emplacements de leurs partenaires commerciaux et Travailleurs à distance, etc. Mais le problème est de garantir que le message qui circule dans le réseau reste protégé. Il y a de plus en plus de techniques pour les protéger, mais il y a aussi plusieurs techniques pour les attaquer.

Dans ce chapitre nous allons détaillés le concept de la sécurité informatique, ses objectifs et de son impact sur les réseaux et des mécanismes fondamentaux de sécurité.

Ⅱ.2 Sécurité informatique

Ⅱ.2.1 Définition

La sécurité informatique fait référence à la protection des systèmes informatiques et des données contre les menaces, les attaques et les accès non autorisés ; elle consiste à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. Cela implique la mise en place de mesures de sécurité telles que le chiffrement des données, les pare-feu…etc.

Ⅱ.2.2 Objectifs de la sécurité informatique

La protection de l'actif crucial de l'organisation, le système d'information, est de la plus haute importance. L'objectif de la sécurité du système d'information est de garantir la préservation des attributs suivants :

- **La disponibilité**

  Le système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.

- **L'intégrité**

  Les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets.

- **Les confidentialités**

Seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

- **L'authentification**

L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

- **La non-répudiation**

Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

Ⅱ.2.3 Types de sécurité

On distingue trois catégories de sécurité réseau :

a) La sécurité physique

La sécurité physique concerne tous les aspects liés à l'environnement dans lequel les ressources sont installées. Elle peut inclure :

- ✓ la sécurité physique des salles de serveurs, des périphériques réseau, etc.
- ✓ la prévention des accidents et des incendies.
- ✓ les systèmes de l'alimentation ininterrompue.
- ✓ la surveillance vidéo, etc.

b) La sécurité logique

La sécurité logique fait référence à la mise en œuvre d'un système de contrôle d'accès, par logiciel, pour sécuriser les ressources [5] . Elle peut inclure :

- ✓ l'application d'une stratégie de sécurité fiable pour les mots de passe.
- ✓ l'instauration d'un modèle d'accès s'appuyant sur l'authentification, l'autorisation et la traçabilité.
- ✓ la configuration correcte des pare-feu de réseau.
- ✓ l'installation des IPS (systèmes de prévention d'intrusion).
- ✓ l'utilisation des VPN (réseau privé virtuel), etc.

c) Sécurité administrative

La sécurité administrative permet d'assurer le contrôle interne d'une organisation à l'aide d'un manuel des procédures [5]. Elle peut inclure :

- ✓ définir les responsabilités respectives des différents intervenants ou opérateurs.
- ✓ la prévention des erreurs et des fraudes.
- ✓ protéger l'intégrité des biens et des ressources de l'entreprise.
- ✓ assurer l'enregistrement de toutes les opérations concernant la manipulation du matériel.
- ✓ gérer rationnellement les biens de l'entreprise.
- ✓ assurer une gestion efficace et influente des activités.

Ⅱ.2.4 Politique de sécurité

Cette politique est un ensemble de règles qui précisent les comportements autorisés et interdits dans le domaine de la sécurité. C'est un document qui contient toutes les réponses aux questions que se posent les ingénieurs chargés de recherche lorsqu'ils résolvent des problèmes de sécurité. Un aspect d'un projet informatique. Le succès de cette dernière dépend de la prise en compte dès le départ de facteurs tels que les contraintes de sécurité.

Une politique de sécurité est donc un document confidentiel qui fournit un ensemble d'instructions de sécurité classées par thème, ignorant les contingences matérielles et techniques.

Ⅱ.2.5 Classification des attaques

Tout ordinateur connecté à un réseau informatique peut être vulnérable à attaque. Il s'agit de l'utilisation de systèmes informatiques (système d'exploitation, logiciel, etc.) ou encore utilisé par les utilisateurs à des fins non autorisées par l'opérateur système [6].

Sur le réseau Internet, les attaques continuent de se produire, et les attaques se sont produites à plusieurs reprises. Chaque minute sur chaque machine connectée. La plupart de ces attaques sont initiées automatiquement depuis les machines infectées (via virus, chevaux de Troie, vers, etc.), à l'insu de son propriétaire.

Ⅱ.2.5.1 Buts d'attaques

Les buts d'attaques sont :

- ✓ **Interruption :** Vise la disponibilité des informations.

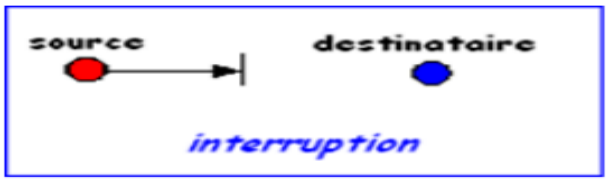

Figure Ⅱ.1: Interruption des données

- ✓ **Interception:** Vise la confidentialité des informations.

Figure Ⅱ.2: Interception des données

- ✓ **Modification** : vise l'intégrité des informations.

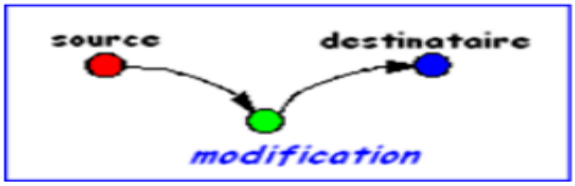

Figure Ⅱ.3: Modification des données

- ✓ **Fabrication** : Vise l'authenticité de la source ou de la destination.

Figure Ⅱ.4: Fabrication des données

Ⅱ.2.5.2 Types d'attaques

Il existe trois familles distinctes dans lesquelles peuvent être classées les différentes techniques d'attaque utilisées par les individus malveillants :

a) Les attaques directes

C'est l'attaque la plus simple (Figure Ⅱ.5). Les pirates utilisent des scripts d'attaque pour attaquer leurs victimes directement depuis leur ordinateur, (elle est faiblement configurable**).**

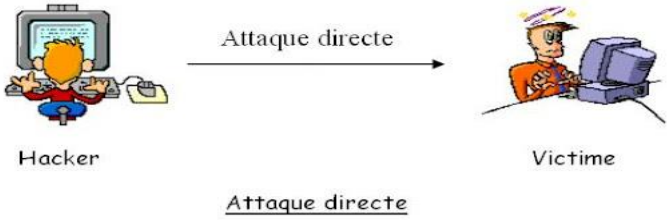

Figure Ⅱ.5: Attaque directe

b) Les attaques indirectes par rebond

D'après la figure ci-dessous, nous pouvons voir que dans ce cas, la machine cible est attaquée via une autre machine.

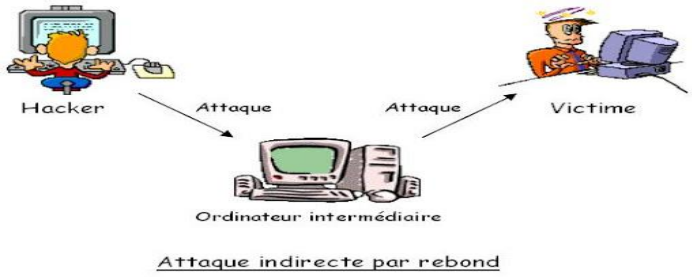

Figure Ⅱ.6: Attaque par rebond

c) Les attaques indirectes par réponse

Cette attaque est un dérivé de la précédente (voir figure Ⅱ.7). La réponse à la première attaque représente une attaque plus malveillante contre la machine cible.

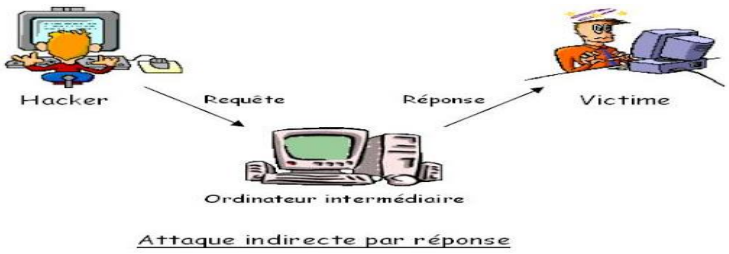

Figure Ⅱ.7: Attaque indirecte par réponse

Ⅱ.2.5.3 Attaques sur les réseaux

a) Attaque par usurpation d'adresse IP (IP spoofing)

Cette attaque consiste à remplacer l'adresse IP de l'expéditeur du paquet IP par une adresse IP d'une autre machine, comme montre cette figure :

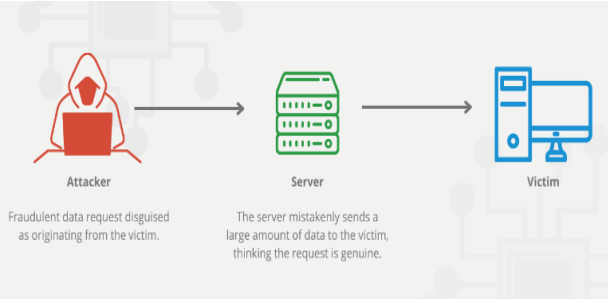

Figure Ⅱ.8: Attaque par adresse IP

b) Attaque par usurpation d'adresse MAC (MAC spoofing) :

Il s'agit de se faire passer pour une machine autorisée (voir figure Ⅱ.9). Un intrus utiliserait simplement l'identité (adresse MAC) de la machine autorisée à utiliser un service donné.

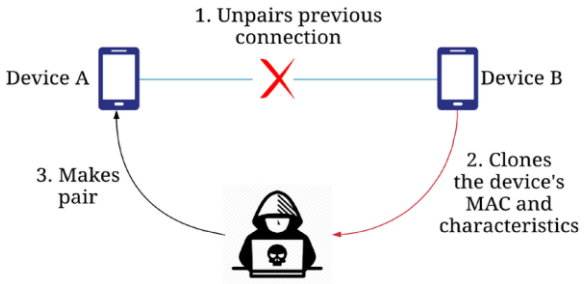

Figure Ⅱ.9 : Attaque par adresse MAC

c) ARP Spoofing :

D’après la figure ci-dessous, on peut noter que cette attaque permet de rediriger le trafic d'un ordinateur vers un autre. Grâce à ça Rediriger les mauvais acteurs peuvent se faire passer pour quelqu'un d'autre.

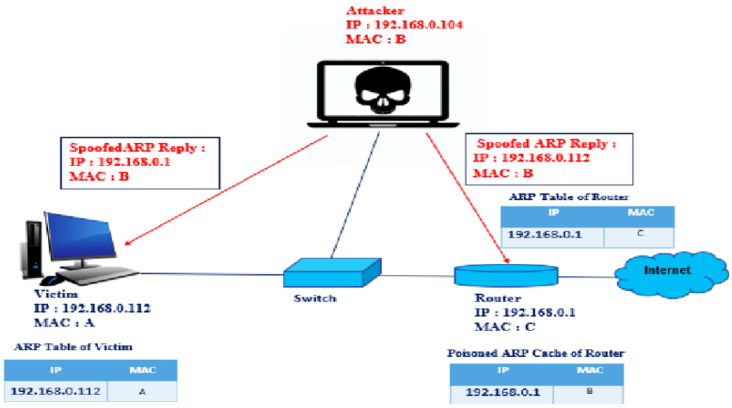

Figure Ⅱ.10: ARP Spoofing

d) Attaque de mot de passe

Obtenir la procédure pour récupérer votre mot de passe est très simple, pour accéder aux services à l'aide de logiciels spéciaux tels que des enregistreurs de frappe. Il Permet en fait d'enregistrer les frappes au clavier, espionnant électroniquement les utilisateurs ordinateur.

e) Portes dérobées (Backdoor)

Les portes dérobées sont souvent introduites par les développeurs de logiciels. Ce Créez un chemin non surveillé pour accéder à l'ordinateur de la victime. Une fois que le logiciel développé dispose d'une porte dérobée installée, l'attaquant aura la possibilité de surveiller le comportement des utilisateurs et de copier ou détruire des données ou avoir la capacité de contrôler des ordinateurs (réseaux).

f) Man In The Middle (MITM)

Man In The Middle (voir figure Ⅱ.11) est une redirection complète du trafic échangé entre deux machines. Chaque interlocuteur pense communiquer directement avec l’autre, alors qu’en réalité il s’adresse à une troisième machine qui fait office d’intercepteur de ces données.

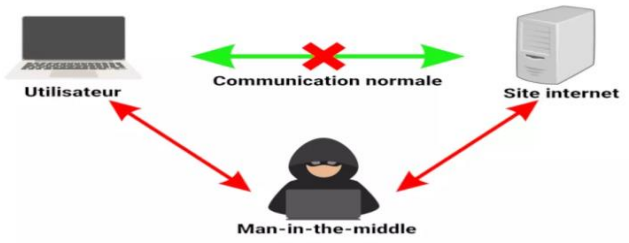

Figure Ⅱ.11: Man In The Middle

Ⅱ.2.5.4 Attaques logiciel

a) Le cheval de Troie

Ce terme fait référence à presque tous les programmes installés d'une manière ou d'une autre. Usurpation (généralement via un e-mail ou une page Web piégée) pour accomplir une mission hostile à l'insu de l'utilisateur.

b) Le virus

Un virus informatique est un programme qui : infecte, se reproduit et a des fonctions nuisibles. La fonction d'infection permet aux virus d'utiliser des langages de script pour pirater des programmes et des données. En accédant à ces derniers, le code du virus est d'abord exécuté silencieusement (pendant la phase de multiplication il infecte d'autres fichiers) puis devient visible (activation de fonctionnalités nuisibles).

c) Les vers informatiques

Les vers sont des logiciels malveillants qui se répliquent sur plusieurs ordinateurs en utilisant : réseau informatique. Contrairement aux virus informatiques, les vers ne nécessitent pas le programme hôte se réplique en profitant des différentes ressources de l'ordinateur qui l'héberge pour assurer sa réplication.

d) Un spyware

Logiciel espion installé sur un ordinateur dans le but de collecter et Transmission d'informations à l'insu de l'utilisateur.

e) Le déni de service (attaque DOS)

Le principe de cette attaque consiste à envoyer des IP ou des paquets de taille ou de structure inhabituelle pour provoquer un état saturé ou instable des machines victimes et les empêcher de fournir les services requis.

Ⅱ.2.6 Types de menaces

Les menaces informatiques représentent des types d'opérations qui peuvent absolument nuire à un système informatique. En matière de sécurité informatique, les menaces peuvent être le résultat de diverses actions provenant de sources multiples et de différents types.

a) Menaces passives

Il s'agit essentiellement de copier ou d'écouter les informations contenues dans un fichier. Ces attaques compromettent la confidentialité des données. Dans ce cas, la personne qui obtient la copie ne tente pas de modifier ces informations ou le système. Ce type de menace est difficile à détecter.

b) Menaces actives

Ils compromettent l'intégrité des données. Dans ce cas, l'intégralité ou l'existence d'une chose le système est compromis. C'est un fait, les accidents représentent 26 % des menaces. Incendie, panne d'équipement ou de réseau, défauts de qualité. 17 % des menaces sont dues à une erreur de l'utilisateur. 57 % étaient malveillants, dont 80 % provenaient de sources internes. Il s'agit d'actions telles que : vol d'appareil, intrusion, écoute réseau, attaques logiques (virus, modifications, etc.).

Ⅱ.2.7 Mécanismes de défense

Le but d'un mécanisme de défense est d'identifier, de contrecarrer et de contrecarrer les failles de sécurité. Il existe plusieurs mécanismes, par exemple :

- ✓ **Cryptographie**

Le domaine de la cryptographie utilise des principes mathématiques pour coder et décoder les données, offrant ainsi un moyen de protéger les informations sensibles pendant le stockage ou la transmission sur des réseaux non sécurisés

comme Internet. Cela garantit que seul le destinataire prévu peut accéder et déchiffrer le contenu, en préservant sa confidentialité.

- ✓ **Signature numérique**

L'ajout de données a pour but de garantir l'intégrité et l'authenticité de la source des données existantes.

- ✓ **Bourrage de trafic**

Pour maintenir la confidentialité, notamment en ce qui concerne la quantité de trafic, des données sont incorporées.

- ✓ **Notarisation**

Le recours à un tiers fiable pour proposer des services de sécurité spécifiques.

- ✓ **Contrôle d'accès**

Vérifie les privilèges d'accès aux données d'un acteur mais ne gêne pas. Profiter d'une faiblesse.

- ✓ **Antivirus**

Le but d'un logiciel de protection informatique est de se prémunir contre les logiciels malveillants. Cependant, il n'offre pas de protection contre un utilisateur non autorisé utilisant un logiciel légitime, ni n'empêche un utilisateur autorisé d'accéder à une ressource sans autorisation appropriée.

- ✓ **Pare-feu**

L'élément chargé de superviser et de gérer le flux de communications au sein d'un réseau informatique est connu sous le nom d'applicateur de politique de sécurité réseau. Son rôle principal est de faire respecter la politique de sécurité du réseau établie, qui décrit les lignes directrices et les réglementations régissant le réseau.

L'autorisation ou la restriction des communications ne constitue pas un moyen de dissuasion pour un attaquant qui pourrait exploiter une connexion autorisée pour cibler le système. De plus, il ne protège pas contre une attaque provenant du réseau interne.

✓ **Protection physique**

Même s'il est possible d'offrir une protection complète, il est possible qu'elle soit jugée excessive. Une action possible à considérer serait l'isolement complet de votre système, à titre d'exemple.

Ⅱ.2.8 Comment sécuriser un réseau informatique

Assurer la sécurité des données critiques de l'entreprise implique la mise en œuvre de mesures visant à maintenir les propriétés de sécurité, ainsi que l'application des réglementations décrites dans une politique de sécurité, qui comprend diverses règles [7].

Ⅱ.2.8.1 VLAN (Réseaux locaux virtuels)

Ⅱ.2.8.1.1 Définition

Un réseau local virtuel (voir figure Ⅱ.12) est un groupe logique d'appareils ou d'utilisateurs pouvant Regroupez par fonction, service ou application, quel que soit l'emplacement de leur segment physique. La configuration d'un réseau local virtuel se fait dans un Switch via un logiciel. Les VLAN ne sont pas standardisés et nécessitent l'utilisation de logiciels propriétaires vendus par les fournisseurs de commutateurs.

Figure Ⅱ.12: Architecture avec VLAN

Ⅱ.2.8.1.2 Fonctionnement des VLAN par leurs types

✓ **VLAN de niveau 1 (ou VLAN par port)**

Il définit les ports du Switch qui appartiennent à tel ou tel VLAN. Cela permet entre autres de différencier physiquement quels ports appartiennent à quels VLAN. L'inconvénient persiste : si le serveur détenant les adresses MAC tombe en panne, tout le réseau est paralysé.

- ✓ **VLAN de niveau 2 (ou VLAN par adresse MAC)**

Il arrive automatiquement à indiquer les adresses MAC des appareils qu'on veut associer au VLAN, cette solution est plus fiable comparer au Vlan de niveau 1, car peu importe le port sur lequel le périphérique se connecte, il sera associer au VLAN dont l'adresse MAC est configurée.

- ✓ **VLAN de niveau 3**

Il suit le même principe que les VLAN de niveau 2 mais diffère dans la manière dont nous spécifions les adresses IP (ou une plage d'IP) qui font partie de chaque VLAN. La mise en œuvre de VLAN nécessite un commutateur gérable et capable de gérer les VLAN au niveau requis, ce qui signifie que des niveaux de VLAN plus élevés impliquent un coût plus élevé pour l'acquisition du commutateur.

Ⅱ.2.8.1.3 Avantages des VLAN

Les facteurs influençant un réseau sont les suivants : réduire la charge de trafic grâce à la minimisation des domaines de diffusion ; formation de groupes virtuels; le renforcement de la sécurité, qui est le plus courant ; une simplification de l'administration, moins répandue mais toujours présente ; et enfin la réduction des coûts.

Ⅱ.2.8.1.4 Différence entre LAN et VLAN

Un domaine de diffusion englobe un réseau local (LAN), dans lequel tous les hôtes du réseau reçoivent des messages de diffusion de tout autre hôte.

Selon le modèle OSI, un réseau local est confiné par l'interface des équipements de niveau 3 au niveau de la couche réseau.

Un VLAN, qui signifie réseau local virtuel, est un type de réseau local réparti sur les équipements de niveau 2 du modèle OSI, en particulier la couche liaison. Cela signifie que le domaine de diffusion est également distribué sur ces appareils de niveau 2. Par conséquent, tous les hôtes du même réseau local, ou domaine de diffusion, forment un groupe logique distinct de la configuration physique du réseau.

Ⅱ.2.8.2 Firewall

Ⅱ.2.8.2.1 Définition

Dans le domaine informatique, un pare-feu est un dispositif qui protège le réseau privé de l'espace public. Essentiellement, il sert de facteur de démarcation entre ces deux domaines.

Le réseau privé ne peut atteindre l'extérieur que par son intermédiaire. C'est ainsi qu'il sécurise le réseau privé de tout... Les attaques proviennent de l'extérieur via Internet et peuvent également avoir une certaine influence sur les actions menées au sein d'un réseau privé [8].

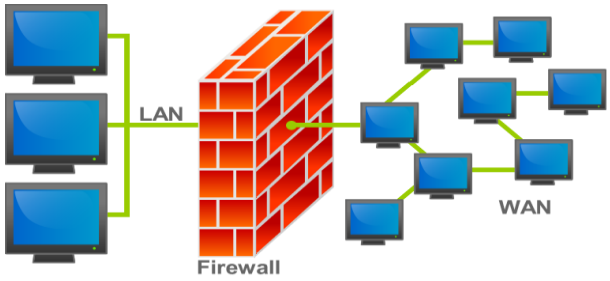

Figure Ⅱ.13: Emplacement d'un Firewall

Ⅱ.2.8.2.2 Rôle d'un firewall

Son rôle essentiel dispose de deux techniques de base :

- ✓ **Le filtrage des paquets de données**

La principale technique de protection d'un réseau. Chaque paquet reçu doit être comparé à un ensemble de règles prédéterminées pour déterminer comment il doit être traité et réaliser.

- ✓ **Courroie de transmission**

Une autre utilisation d'un pare-feu consiste à dissimuler les machines derrière lui. De cette manière, un serveur peut simuler l'identité de la véritable machine source d'un paquet.

Ⅱ.2.8.2.3 Principe de fonctionnement

En réalité, le Firewall peut être classé en deux catégories principales :

- ✓ **Firewall IP Filter ou Chokes**

Ce pare-feu particulier fonctionne au niveau du réseau et régule le mouvement des paquets en fonction de leur source, destination, ports et contenu. Il s'agit d'un système simple à configurer en mettant en œuvre un ensemble de règles qui régissent l'entrée et la sortie des paquets du réseau privé [8]. Cela peut être fait sur un ordinateur ou un appareil de communication qui permettra l'activation de la limitation du flux de paquets entre les réseaux.

- ✓ **Gates**

Un programme, un appareil ou un ordinateur qui reçoit des connexions réseau externes et les transmet au réseau privé est appelé porte. L'accès à cette porte est strictement réservé à l'administrateur, garantissant la sécurité et empêchant tout accès non autorisé aux utilisateurs.

Ⅱ.3 Discussion

Dans ce chapitre, nous avons exposé les attaques les plus courantes, les concepts de sécurité, ainsi que les mécanismes de défense. L'objectif de la sécurité informatique est de garantir la protection des ressources matérielles ou logicielles d'une entreprise et la sécurisation des données partagées grâce à un système fiable et sûr. Étant donné la diversité des menaces et des attaques qui rendent les systèmes informatisés vulnérables, la sécurité repose sur diverses mécanismes et logiciels afin de garantir la fiabilité du système et garantir les connexions et le partage.

Chapitre III : Étude de l’architecture initiale et proposition des solutions de sécurité

Ⅲ.1 Préambule

L'objectif de ce chapitre est l'étude de l'architecture du réseau informatique disponible au niveau de d'Algérie Telecom/Direction opérationnelle de Tizi ouzou. Pour cela, nous avons décrit les différents équipements constituant cette architecture et nous avons identifié également les différentes failles pour proposer une stratégie de sécurité répondant aux exigences de l'entreprise. De plus, dans cette partie nous avons montré aussi le mécanisme de configuration des différents équipements.

Cette démarche permet de mettre en évidence les étapes à réaliser pour implémenter notre solution dans un environnement pratique et réel.

Ⅲ.2 Présentation de l'organisme d'accueil

Ⅲ.2.1 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 busines 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 segmentes des services des Télécommunications.

Ⅲ2.2 Principaux objectifs d'Algérie Télécom :

A travers donc son activité, Algérie Télécom s'est attribué les objectifs suivants :

- ✓ Valoriser l'offre de services téléphoniques et faciliter l'accès aux services de télécommunications au plus grand nombre d'usagers, en particulier en zones rurales.
- ✓ Accroître la qualité de services offerts et la gamme de prestations rendues et rendre plus compétitifs les services de télécommunications.
- ✓ Mettre au point un réseau national de télécommunication fiable et connecté aux autoroutes de l'information.
- ✓ Devenir un opérateur multimédia.
- ✓ Mettre en place une démarche marketing innovante et une politique de communication efficace.
- ✓ Globalement Algérie Télécom veille à participer à la promotion de la société d'information en Algérie doté de trois buts : rentabilité, efficacité et qualité de services.

Ⅲ2.3 Principales missions d'Algérie Télécom

Algérie Télécom a principalement pour mission de :

- ✓ Procurer à sa clientèle des services de télécommunication permettant le transport et l'échange de la voix, de message écrit, de données numériques et d'informations audiovisuelles.
- ✓ Mettre au point et gérer les réseaux publics et privés de télécommunication.
- ✓ Etablir, exploiter et gérer les interconnexions avec tous les opérateurs des réseaux.

Ⅲ2.4 Organisation d'Algérie Telecom :

Algérie Télécom est organisée en direction centrales, régionale et directions opérationnelles de wilaya auteur de ses métiers fixes et services, et d'autre part des fonctions supports réseaux. A cette structure s'ajoutent trois filiales spécialisées et de dimension nationales.

- ✓ La filiale de téléphonie mobile « Algérie Télécom mobile : Mobilis »
- ✓ La filiale des télécommunications par satellite « Algérie Télécom Satellite : ATS »
- ✓ La filiale des services internet « Algérie Télécom Internet DJAWEB : ATI »

Algérie Télécom s'implique dans le développement socio-économique du pays à travers la fourniture des services de Télécommunication. En outre, elle met en œuvre des moyens importants pour rattacher les localités isolées.

Ⅲ.2.5 Situation géographique d'Algérie Télécom / DO de Tizi ouzou

La situation géographique de la direction opérationnelle de la wilaya de Tizi ouzou est illustrée par la figure Ⅲ-1 :

Figure Ⅲ.1: Situation géographique d'Algérie Télécom

Ⅲ.3 Logiciel de simulation

Cisco Packet Tracer est un simulateur de réseau largement utilisé pour la conception, la configuration et la simulation de réseaux. Grâce à son interface conviviale, les utilisateurs peuvent créer des topologies virtuelles, établir des connexions entre les périphériques réseau et configurer leurs paramètres. Cet outil est largement utilisé dans les programmes de formation en réseau pour acquérir des compétences pratiques et une compréhension globale des principes du réseau. Permet aux utilisateurs de tester les configurations en toute sécurité, d'explorer divers scénarios et de résoudre efficacement les problèmes.

Figure Ⅲ.2: Cisco Packet Tracer

La création des schémas du réseau qu'on veut réaliser se fait par l'interface principale de Cisco Packet Tracer, représentée par la figure ci-dessous :

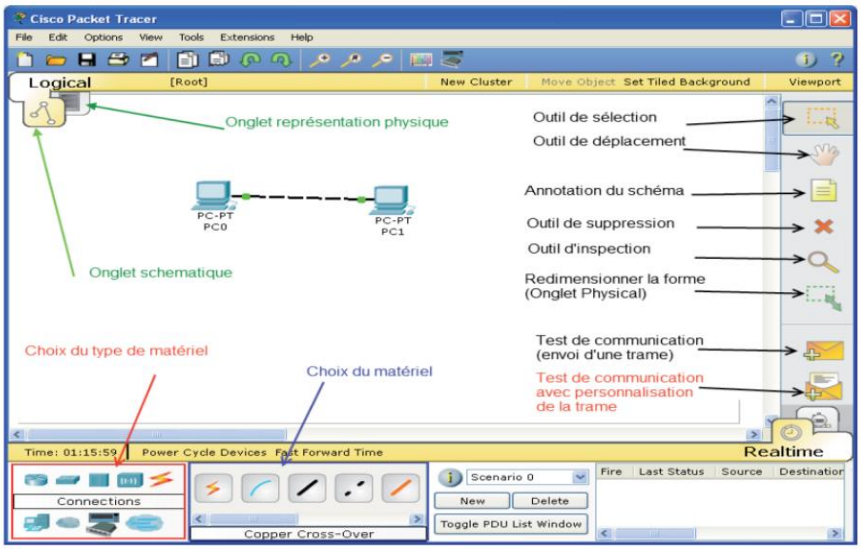

Figure Ⅲ.3 : Fenêtre principale de Cisco Packet Tracer

Pour construire le réseau, vous devrez sélectionner l'un des appareils représentés dans les différentes icônes affichées sur la figure. Cliquez simplement sur l'appareil souhaité et faites-le glisser dans la zone désignée pour établir le réseau.

Figure Ⅲ.4 : Appareils de Cisco Packet Tracer

Pour établir les connexions entre les différents équipements, accédez à la catégorie «connexions » et sélectionnez l'option de câblage souhaitée.

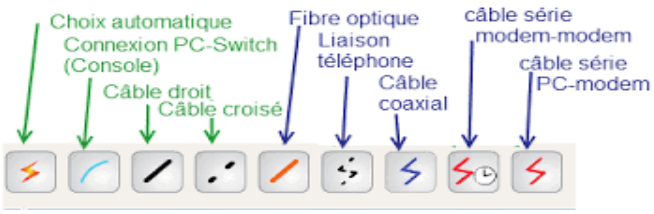

Figure Ⅲ.5 : Câblages

Ⅲ.4 Présentation du réseau initial

Comme nous avons mentionné précédemment, notre apport consiste à sécuriser et améliorer l'architecture du réseau déjà établie au sein de l'agence Algérie Télécom/DO de la wilaya de Tizi ouzou (voir figure Ⅲ.6). L'étude de cette architecture permet de mettre en évidence ses points faibles et failles.

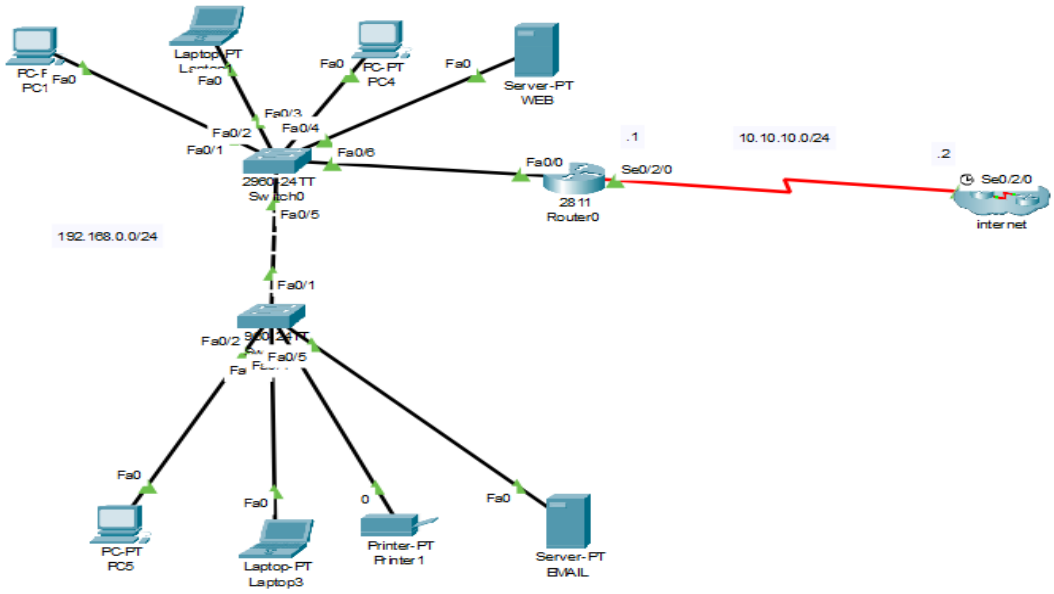

Figure Ⅲ.6 : Architecture du réseau initial

Le réseau contient deux Switchs attachés chacun à des ordinateurs, Laptops et Serveurs, tout ces équipements sont reliés à un Routeur formant ainsi un réseau LAN qui se connecte directement à un réseau WAN qui est l'internet.

Ⅲ.4.1 Description des équipements

Les différents équipements utilisés pour la réalisation du réseau informatique sont :

- **Router CISCO 2811 :** offre des performances et une modularité exceptionnelles dont :
  - Une prise en charge étendue de différents protocoles de routage
  - Des fonctionnalités de sécurité intégrées
  - la capacité d'exécuter des services VoIP

- Des options de gestion avancées et adaptée aux environnements qui exigent une connectivité fiable et sécurisée

➢ **Commutateur (Switch) CISCO Catalyst série 2960 :** Sert à maximiser l'efficacité dans un court laps de temps et garantir une intégration transparente avec diverses interfaces Ethernet et il permet aussi intégrez des mesures de sécurité dans la fonctionnalité complète, ce qui le rend parfait pour les paramètres d'entreprise et de centre de données.

➢ **Serveurs :** Offre aux utilisateurs la possibilité d'accéder aux fichiers, d'exécuter des programmes, de stocker des données, d'utiliser les services de communication et de gérer l'accès au réseau.

➢ **Câbles RJ45 :** Egalement appelé connexion filaire, permet la transmission transparente des données informatiques en reliant différents appareils entre eux. Il se connecte sans effort à votre box internet, ordinateur, console, décodeur, téléviseurs…, facilitant ainsi un transfert de données.

➢ **Ordinateurs (PC et Laptop) :** dans un réseau informatique, les ordinateurs jouent à la fois le rôle de serveur et celui de client. Ils émettent et reçoivent des données [8].

III.5 Étude critique et solutions proposées

Nous avons noté et constaté que le réseau manque en sécurité et ses failles sont:

- le réseau est installé anarchiquement et non administré.
- le réseau installé est non sécurisé contre les intrusions d'une façon fiable.
- Le réseau Local est relié à l'internet ce qui le rend vulnérable aux menaces qui viennent de l'extérieur.

Après cette étude détaillée de l'architecture existante, et afin de remédier aux problèmes et les failles cités précédemment, nous avons proposé les solutions suivantes :

- Création des vlan qui protègera le réseau intérieur et qui permettra une gestion plus efficace du trafic réseau : donc on aura plusieurs zones et non une seule adresse réseau ce qui rend l'accès moins facile par les intrus.
- Implémentation d'un firewall qui va filtrer les attaques réseau.

- Intégration d'une DMZ qui nous permettra d'isoler nos servers accessible depuis l'extérieur.
- Mettre des mots de passe aux Switch et Router ce qui évitera l'accès des intrus à nos périphériques.

Ⅲ.6 Nouvelle architecture

Nous avons identifié de multiples vulnérabilités tant au niveau de l'architecture que du système, ce qui en fait une cible attractive pour les pirates. Pour répondre à cette préoccupation, nous avons mis en œuvre les modifications nécessaires pour améliorer la sécurité du réseau informatique de l'entreprise.

En conséquence, nous avons renforcé l'architecture existante en incorporant un pare-feu avec une zone DMZ où nous pouvons mettre les serveurs accessibles par le publique. De plus, nous avons ajouté un service de la téléphonie IP en créant deux VLANs (VOICE et DATA), renforçant ainsi la sécurité du réseau interne. Afin de sécuriser au maximum les routeurs et les Switchs contre les cybers attaques et les pirates, l'accès à ces derniers est protégé par mot de passe. L'architecture proposée est illustrée par la figure III.7.

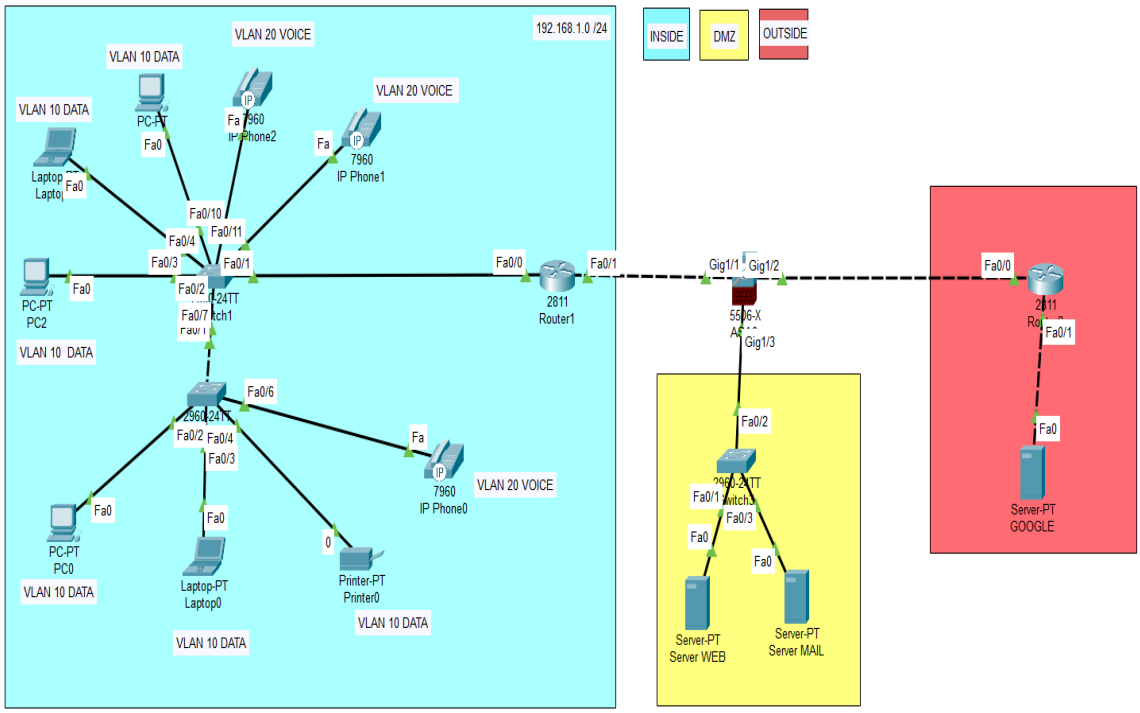

Figure Ⅲ.7 : Architecture du réseau sécurisé

Comme nous pouvons le voir dans la nouvelle architecture le réseau est doté par d'autres équipements pour mieux sécuriser et améliorer le fonctionnement. Ces équipements sont :

- **IP Phone CISCO CP-7960 :** L'écran LCD offre une interface conviviale et prend en charge les fonctionnalités de téléphonie avancées, notamment le transfert d'appel et la messagerie vocale. Les appels sont clairs et compréhensibles grâce à une qualité audio HD améliorée grâce à l'utilisation de protocoles de cryptage transparents pour un accès réseau. Facilement intégré aux systèmes de gestion et aux réseaux téléphoniques actuels, la durabilité et la fiabilité du produit le rendent idéal pour une utilisation professionnelle quotidienne.
- **Cisco ASA 5506 (pare-feu) :** Les principales fonctions du système comprennent le filtrage du réseau, la sécurité des applications, la gestion des connexions, la surveillance et la journalisation complète, le contrôle d'accès restreint et la gestion automatique des mises à jour.

Ⅲ.7 Mise en marche de la nouvelle architecture

Pour la mise en service du réseau informatique, nous avons procédé ainsi :

Ⅲ.7.1 Elaboration du Plan d'adressage du réseau

L'attribution d'adresses IP aux appareils est un élément essentiel de la configuration du réseau. Ce plan d'adressage joue un rôle central dans la gestion des adresses, en évitant les conflits et en facilitant une communication fluide entre les appareils. En classant les appareils en sous-réseaux en fonction de leurs fonctions ou de leur emplacement physique, le plan maximise l'utilisation des ressources réseau et rationalise l'administration des adresses IP (voir Tableau III.1).

INSIDE	Switch 1	Interface F0/2-4	VLAN : DATA 192.168.10.0/24
		Interface F0/10-11	VLAN : VOICE 192.168.20.0/24
	Switch 2	Interface F0/2-4	VLAN : DATA 192.168.10.0 /24
		Interface F0/6	VLAN : VOICE 192.168.20.0 /24
	IP Phones	Interface Fa0	Configuration fournit par DHCP
	PC et Laptop	Interface Fa0	Configuration fournit par DHCP
	Router	Interface F0/0	/
		Interface F0/0.10	192.168.10.1 /24
		Interface F0/0.20	192.168.20.1 /24
		Interface F0/1	192.168.1.2 /24
DMZ	Server WEB	Interface Fa0	192.168.2.3 /24
	Server MAIL	Interface Fa0	192.168.2.4 /24
	Pare-feu ASA	Interface Gig1/1	192.168.1.1 /24
		Interface Gig1/2	203.1.1.1 /24
		Interface Gig1/3	192.168.2.1 /24
OUTSIDE	Router 2	Interface F0/0	203.1.1.2 /24
		Interface F0/1	8.8.8.1 /24
	Server GOOGLE	Interface Fa0	8.8.8.8 /24

Tableau Ⅲ1: Plan d'adressage du réseau

Ⅲ.7.2 Installation des VLANs

Au sein d'un réseau physique, un réseau local virtuel (VLAN) est un sous-réseau intelligible qui est établi. Contrairement à un réseau local conventionnel, où tous les appareils résident sur un segment de réseau partagé, un VLAN permet de catégoriser les appareils selon des critères spécifiques, tels que leur fonction, leur service ou leur niveau de sécurité. Chaque VLAN fonctionne de manière autonome des autres, permettant une configuration et une gestion individuelles.

a) Création des VLAN

Nous devons d'abord créer les vlan en utilisant la commande suivante :

- **Configuration :**

Switch(config)#vlan « numero du vlan

Switch(config)#name donner un nom

- **Application :**

Dans cette étape nous avons créé deux VLAN, VLAN 10 appelé DATA pour les données et le VLAN 20 appelé VOICE pour la voix comme montre les figures ci-dessous :

✓ Switch1

```
Switch>ENA
Password:
Switch#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#VLAN 10
Switch(config-vlan)#NAME DATA
Switch(config-vlan)#EXIT
Switch(config)#VLAN 20
Switch(config-vlan)#NAME VOICE
Switch(config-vlan)#EXIT
Switch(config)#
```

Figure Ⅲ.8 : Création des VLANs dans S1

✓ Switch 2

```
switch2(config)#VLAN 10
switch2(config-vlan)#NAME DATA
switch2(config-vlan)#EXIT
switch2(config)#VLAN 20
switch2(config-vlan)#NAME VOICE
switch2(config-vlan)#EXIT
switch2(config)#
```

Figure Ⅲ.9 : Création des VLANs dans S2

b) Assignation des ports aux vlan

Il existe deux modes pour attribuer chaque port à son VLAN :

❖ **Mode access**

Ce mode est utilisé pour les connexions de terminaux d'appareils appartenant à un seul VLAN.

- **Configuration:**

Switch(config)#interface f0/’’n’’

Switch(config)#switchport mode access

Switch(config)#switchport access vlan ’’num du vlan’’

- **Application:**

Voici l’application de ce mode sur le réseau :

✓ Switch 1

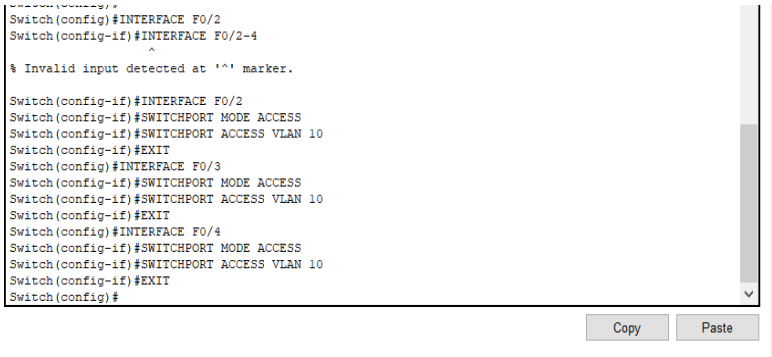

Figure Ⅲ.10: Configuration de mode access dans S1

✓ Switch 2

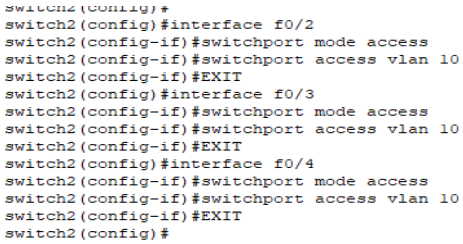

Figure Ⅲ.11: Configuration de mode access dans S2

❖ **Mode trunk**

Un trunk est une connexion physique sur laquelle on transmet le trafic de plusieurs VLANs. Dans cette étape nous configurons le port qui relie entre le Switch et le Router.

- **Configuration:**

Switch(config)#interface f0/''n''

Switch(config)#switchport mode trunk

Switch(config)#switchport trunk allowed vlan ''indiquer tout les vlans''

- **Application:**

✓ Switch 1

```
Switch(config-if)#EXIT
Switch(config)#INTERFACE F0/7
Switch(config-if)#SWITCHPORT MODE TRUNK
Switch(config-if)#SWITCHPORT TRUNK ALLOWED VLAN 1,10,20
Switch(config-if)#EXIT
Switch(config)#INTERFACE F0/1
Switch(config-if)#SWITCHPORT MODE TRUNK
Switch(config-if)#SWITCHPORT TRUNK ALLOWED VLAN 1,10,20
Switch(config-if)#EXIT
Switch(config)#
```

Figure Ⅲ.12: Configuration de mode trunk dans S1

✓ Switch 2

```
switch2(config)#
switch2(config)#INTERFACE F0/1
switch2(config-if)#SWITCHPORT MODE TRUNK
switch2(config-if)#SWITCHPORT TRUNK ALLOWED VLAN 1,10,20
switch2(config-if)#EXIT
switch2(config)#
```

Figure Ⅲ.13: Application de mode trunk dans S2

c) Création des sous-interfaces dans le routeur

Cette étape permet à plusieurs VLANs différents de se communiquer, aussi avoir deux interfaces en un port ce qui rends le piratage moins facile.

- **Configuration :**

Router (config-subif)#interface F0/n.’’num du vlan’’
Router (config-subif)#encapsulation dot1Q ’’num du vlan’’
Router (config-subif)#ip address ’’getway de mon réseau vlan’’
Router (config-subif)#no shutdown

- **Application**

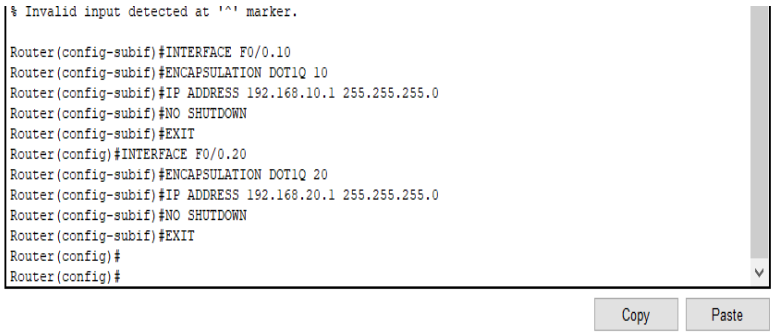

Figure Ⅲ.14 : Création des sous-interfaces dans le routeur

Apres la création des sous-interfaces il faut toujours les activer en utilisant la commande « **NO SHUTDOWN ».**

Ⅲ.7.3 Intégration de la téléphonie IP

Pour faciliter la communication vocale entre les utilisateurs de notre réseau, nous intégrerons la technologie VOIP. Cette configuration de téléphonies IP, nous permettra la transmission de voix de haute qualité sur le réseau IP, permettant ainsi une communication vocale transparente et de qualité professionnelle entre les utilisateurs.

a) Services téléphoniques

Le processus de configuration des services téléphoniques implique la mise en œuvre et l'administration de diverses fonctionnalités de téléphonie sur le réseau. Cela inclut la configuration des téléphones IP, des lignes téléphoniques et des numéros de poste, entre autres aspects. En établissant cette configuration, les utilisateurs sont en mesure de participer efficacement aux appels téléphoniques entrants et sortants.

La mise en place de services téléphoniques garantit une communication transparente et fiable au sein de l'organisation, offrant aux utilisateurs une expérience téléphonique soignée et professionnelle.

- **Configuration :**

Router(config)#telephony-service

Router(config-telephony)# max-ephones ‘’nombre de poste telephonique’’

Router(config-telephony)# max-dn ‘’nombre de poste telephonique’’

Router(config-telephony)# ip source-address ‘’getway du vlan voice’’ port 2000

Router(config-telephony)# auto assign 1 to ’’n’’

Router(config)#ephone-dn ’’n’’

Router(config-ephone-dn)# number ’’num’’

- **Application :**

✓ **Paramètre Call Manager Express**

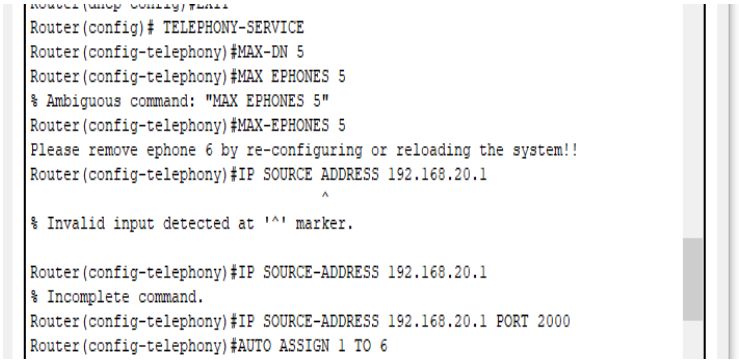

Figure Ⅲ.15 : Configuration des paramètres Call Manager Express

Nous avons configuré 5 téléphones au maximum et l’adresse IP à partir de laquelle les téléphones seront enregistrés ainsi le port utilisé par chaque téléphone (valeur par défaut est 2000).

✓ **Services téléphoniques**

Cette partie consiste à configurer les paramètres de chaque téléphone, comme illustre la figure ci-dessous:

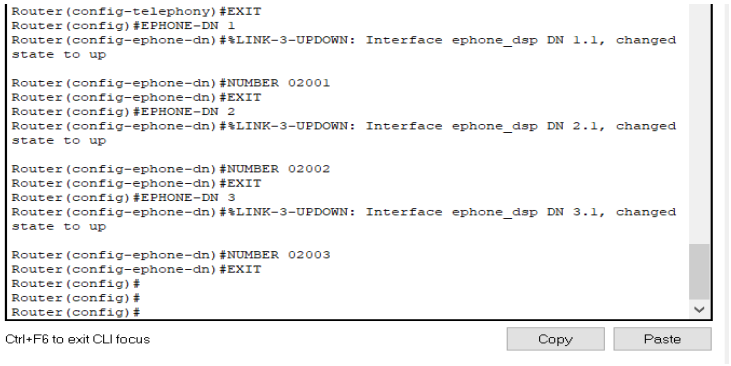

Figure Ⅲ.16 : Configuration des services téléphoniques

b) Définition de routeur comme DHCP serveur

Pour simplifier la gestion et l'attribution des adresses IP pour les administrateurs, nous donnons au routeur le rôle de serveur DHCP, permettant l'attribution dynamique des adresses IP et la configuration des paramètres réseau client (voir figure Ⅲ-17).

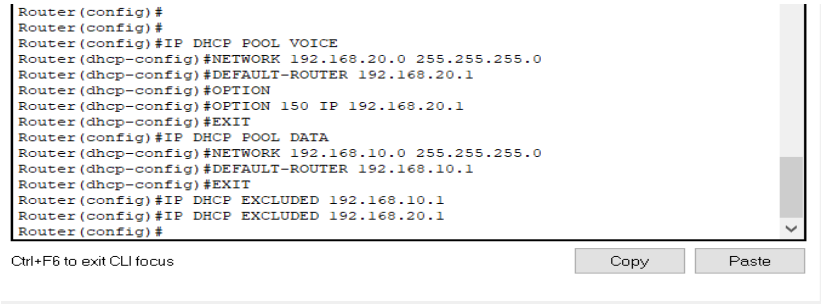

Figure Ⅲ.17 : configuration de routeur comme DHCP serveur

Option 150 : Permet d'indiquer l'adresse IP du serveur TFTP aux téléphones IP pour télécharger leurs fichiers de configuration.

Ⅲ.7.4 Mots de passe pour Switchs, Router et Firewall :

Il est possible de configurer les équipements pour qu'ils exigent un mot de passe lorsqu'un utilisateur tente d'y accéder au mode d'exécution privilégié.

a) Switch

- **Configuration :**

```
Switch(config)#enable secret ''saisir un mot de passe''
```

- **Application :**
  - ✓ Switch 1

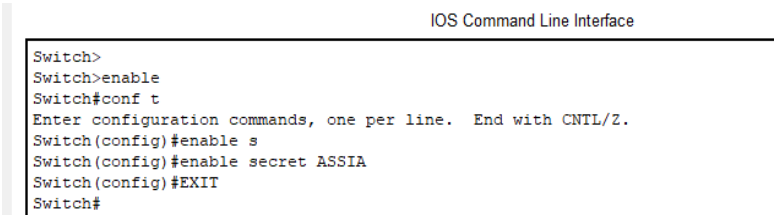

Figure Ⅲ.18 : Sécurisation de S1 avec un mot de passe

  - ✓ Switch 2

```
switch2#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
switch2(config)#ENABLE SECRET NAWAL
switch2(config)#EXIT
switch2#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure Ⅲ.19 : Sécurisation de S2 avec un mot de passe

b) Router

- **Configuration :**

Router (config)#line console 0

Router (config)#password ’’saisir un pasword’’

Router (config)#login

- **Application :**

```
Router>ena
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password TLC2024
Router(config-line)#login
Router(config-line)#exit
Router(config)#
```

Figure Ⅲ.20 : Sécurisation de routeur avec un mot de passe

c) Pare-feu

- **Configuration :**

```
Ciscoasa (config)#enable password ’’ insirez un password’’
```

- **Application :**

```
% Invalid input detected at '^' marker.

ciscoasa(config)#ENABLE PASSWORD ASA2024
ciscoasa(config)#EXIT
ciscoasa#EXIT

Logoff
Type help or '?' for a list of available commands.
```

Figure Ⅲ.21 : Sécurisation de pare-feu avec un mot de passe

Ⅲ.7.5 Pare-feu :

En implémentant un pare-feu, les utilisateurs ont la possibilité de filtrer les ports et de restreindre les communications, ce qui leur permet d'exercer un meilleur contrôle sur le trafic interne et externe par la configuration de :

a) NAT

Le processus de NAT (Network Address Translation) implique la modification des adresses IP et des ports de la source et de la destination. Cette traduction d'adresses contribue à diminuer la demande d'adresses IPv4 publiques et à les dissimuler. L'attribution des plages d'adresses de réseau privé est généralement effectuée par des routeurs ou des pare-feu.

- **Configuration :**

```
ciscoasa (config) #object network inside-netwok
ciscoasa (config) #subnet “inside network, netmask”
ciscoasa (config) #nat (inside,outside) dynamic interface
ciscoasa (config) #end
```

- **Application :**

```
ciscoasa(config)#
ciscoasa(config)#object network inside-network
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#NAT (inside,outside) dynamic interface
ciscoasa(config-network-object)#end
```

Figure Ⅲ.22 : Configuration de NAT pour ASA

b) ACL

Les listes de contrôle d'accès (ACL) sont des réglementations appliquées au trafic qui traverse les interfaces d'un routeur, qu'il soit entrant ou sortant. Ces ACL ont pour objectif d'examiner le trafic et de prendre la décision de transmettre ou non les paquets qui transitent par les interfaces. Afin de procéder à cette détermination, le routeur examine l'en-tête de chaque paquet et l'évalue par rapport aux critères spécifiés dans les ACL.

- **Configuration :**

ciscoasa (config) #access-list “list name” extended permit tcp any any

ciscoasa (config) #access-list “list name” extended permit icmp any any

ciscoasa (config) #access-group “list name” in interface outside

- **Application :**

```
ciscoasa(config)#access-list inside_to_outside extended permit tcp any any
ciscoasa(config)#access-list inside_to_outside extended permit icmp any any
ciscoasa(config)#access-group inside_to_outside in interface outside
ciscoasa(config)#exit
```

Figure Ⅲ.23: Configuration des ACL pour ASA

c) SSH

Pour les connexions de gestion, il est recommandé d'utiliser SSH au lieu de Telnet. Contrairement à Telnet, qui utilise une communication en texte brut non sécurisée, SSH garantit la sécurité des connexions à distance grâce à un cryptage robuste de toutes les données transmises entre appareils.

- **Configuration :**

ciscoasa (config) #username admin password “password”
ciscoasa (config) #aaa authentication ssh console local
ciscoasa (config) #ssh “network and netmask” inside
ciscoasa (config) #ssh “network and netmask” outside
ciscoasa (config) #ssh timeout

- **Application :**

```
ciscoasa(config)#username admin password admin1
ciscoasa(config)#aaa authentication ssh console local
ciscoasa(config)#ssh 192.168.10.0 255.255.255.0 inside
ciscoasa(config)#ssh 192.168.20.0 255.255.255.0 inside
ciscoasa(config)#ssh 8.8.8.8 255.255.255.255 outside
ciscoasa(config)#ssh timeout 10
```

Figure Ⅲ.24 : Configuration de SSH pour ASA

d) ICMP

En règle générale, le ping provenant du côté considéré comme le plus sécurisé devrait fonctionner sans aucun problème. Cependant, l'ASA ne surveille pas automatiquement l'état de l'ICMP. Pour résoudre ce problème, nous pouvons saisir les commandes suivantes pour activer l'inspection ICMP.

```
ciscoasa#conf t
ciscoasa(config)#class-map inspection_default
ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#exit
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#exit
```

Figure Ⅲ.25 : Configuration de l’ICMP

Ⅲ.7.6 DMZ

Pour créer une protection entre le réseau LAN et l'environnement externe, nous avons mis en place une DMZ. Cette zone désignée sert de barrière, permettant l'accès au réseau Web depuis des sources extérieures. Cependant, tout trafic Internet destiné au réseau LAN doit d'abord traverser la zone démilitarisé que nous devons configurer comme suit:

a) Le NAT

- **Configuration :**

ciscoasa (config) #object network dmz-server

ciscoasa (config) #host “server address”

ciscoasa (config) #nat (dmz,outside) static “public address”

ciscoasa (config) #end

- **Application :**

```
ciscoasa#conf t
ciscoasa(config)#object network dmz-server
ciscoasa(config-network-object)#host 192.168.2.3
ciscoasa(config-network-object)#nat (dmz,outside) static 203.1.1.7
ciscoasa(config-network-object)#EXIT
ciscoasa#CONF T
ciscoasa(config)#object network dmz-server
ciscoasa(config-network-object)#host 192.168.2.4
ciscoasa(config-network-object)#nat (dmz,outside) static 203.1.1.8
ciscoasa(config-network-object)#END
ciscoasa#
```

Figure Ⅲ.26 : Configuration de NAT pour la DMZ

b) Les ACL

- **Configuration :**

ciscoasa (config) #access-list “list name” extended permit ip any host “server address”

ciscoasa (config) #access-list “list name” permit icmp any host “server address”

ciscoasa (config) #access-list “list name” permit tcp any host “server address”

ciscoasa (config) #access-group “list name” in interface outside

- **Application :**

```
ciscoasa(config)#access-list outside-dmz extended permit ip any host 192.168.2.3
ciscoasa(config)#access-list outside-dmz permit icmp any host 192.168.2.3
ciscoasa(config)#access-list outside-dmz permit tcp any host 192.168.2.3
ciscoasa(config)#access-group outside-dmz in interface outside
ciscoasa(config)#
ciscoasa(config)#access-list outside-dmz extended permit ip any host 192.168.2.4
ciscoasa(config)#access-list outside-dmz permit icmp any host 192.168.2.4
ciscoasa(config)#access-list outside-dmz permit tcp any host 192.168.2.4
ciscoasa(config)#access-group outside-dmz in interface outside
ciscoasa(config)#
```

Figure Ⅲ.27: Configuration des ACL pour la DMZ

Ⅲ.8 Discussion

Dans ce chapitre, nous avons présenté et étudié l'architecture du réseau informatique LAN de l'entreprise. Ainsi, nous avons pu mettre en évidence les failles en termes de sécurité et de fonctionnement. De ce fait, nous avons proposé des solutions de sécurité et des méthodes pour améliorer le transfert de données. Les configurations de mise en service ont été aussi données dans ce chapitre.

Dans le prochain chapitre, pour vérifier le fonctionnement de la nouvelle architecture, nous avons réalisé un ensemble de tests.

Chapitre Ⅳ:

Vérifications et tests de connectivité

Ⅳ.1 Préambule

Afin de vérifier la fonctionnalité du réseau informatique avec sa nouvelle architecture, nous réaliserons des tests sur les configurations préalablement établies et décrites dans le chapitre précédent. La commande PING sera utilisée sur chaque console d'équipement dans le cadre du processus de test. Cette commande permet de tester la connectivité entre les différents équipements constituant l'architecture. De plus, il est possible de vérifier la connexion au réseau internet.

Ⅳ.2 Vérifications des configurations

Dans cette présentation, nous vérifierons la configuration complète des équipements du réseau local.

Ⅳ.2.1 Configurations des Switchs

❖ **Sécurisation de l'accès au mode d'exécution privilégié**

✓ Switch 1

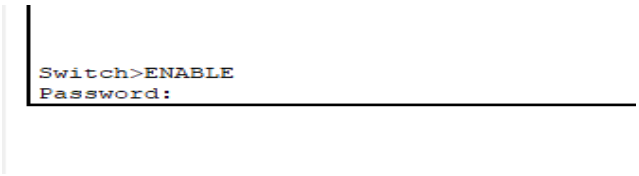

Figure Ⅳ.1 : Vérification de la sécurisation de S1

✓ Switch 2

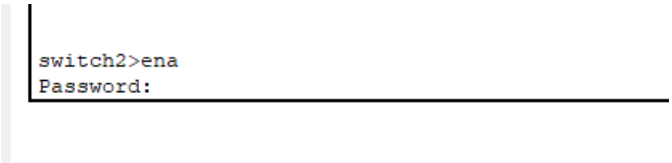

Figure Ⅳ.2 : Vérification de la sécurisation de S2

Ces deux captures nous montre que ne nous pouvons pas accéder au mode privilégié sans mot de passe ce qui protégera nos périphériques.

❖ **Création des VLAN**

Nous tapons la commande **« SHOW VLAN BRIEF »** pour afficher les informations sur les VLANs, comme la montre les figures ci –dessous :

✓ Switch1

```
Switch#SH V
Switch#SH VL
Switch#SH VLan B
Switch#SH VLan Brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                   Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                   Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                   Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                   Fa0/24, Gig0/1, Gig0/2
10   DATA                                active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
20   VOICE                               active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                   Fa0/14, Fa0/15, Fa0/16
40   VLAN0040                            active
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
```

Figure Ⅳ.3 : vérification de la création des VLANs sur S1

✓ Switch 2

```
switch2#SH VLAN B
switch2#SH VLAN Brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/4, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                   Gig0/1, Gig0/2
10   DATA                                active    Fa0/2, Fa0/3
20   VOICE                               active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                   Fa0/10, Fa0/11, Fa0/12
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
switch2#
```

Figure Ⅳ.4 : Vérification de la création des VLANs sur S2

D’après ces captures nous constatons que les VLANs (DATA et VOICE) ont été crées avec succès sur les deux Switchs.

❖ **Appartenance de ports aux VLAN**

✓ Switch 1

```
Switch#sh vlan b
Switch#sh vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/5, Fa0/8, Fa0/9, Fa0/10
                                                   Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                   Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                   Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                   Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   DATA                                active    Fa0/2, Fa0/3, Fa0/4
20   VOICE                               active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                   Fa0/14, Fa0/15, Fa0/16
40   VLAN0040                            active
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
Switch#
```

Figure Ⅳ.5 : Vérification de l’appartenance de ports aux VLAN sur S1

✓ Switch 2

```
switch2#SH VLAN B
switch2#SH VLAN Brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                 Gig0/2
10   DATA                              active    Fa0/2, Fa0/3, Fa0/4
20   VOICE                             active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
switch2#
```

Figure Ⅳ.6 : Vérification de l'appartenance de ports aux VLAN sur S2

D'après ces figures, nous pouvons voir que les ports voulu sont associés à leurs VLAN.

Ⅳ.2.2 Configurations de Routeur

❖ **Sécurisation de router de l'accès au mode d'exécution privilégié**

```
User Access Verification

Password:
```

Figure Ⅳ.7 : Vérification de la sécurisation de routeur

Cette figure illustre clairement que l'accès au mode privilégié et interdis sans mot de passe.

❖ **Création des sous-interfaces pour les VLAN**

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
!
```

Figure Ⅳ.8 : Vérification de la création des sous-interfaces pour les VLANs

La figure montre que nous avons crée deux sous-interfaces en un seul port, ce qui signifie qu'une seule interface physique de routeur permet de relier le trafic entre les deux VLANs.

❖ **Définition de routeur comme DHCP serveur**

```
!
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.20.1
!
ip dhcp pool VOICE
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 option 150 ip 192.168.20.1
ip dhcp pool DATA
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
ip dhcp pool data
 default-router 192.168.10.1
 dns-server 8.8.8.8
ip dhcp pool voice
 default-router 192.168.20.1
 dns-server 8.8.8.8
!
```

Figure Ⅳ.9 : vérification de la configuration de routeur comme DHCP serveur

En examinant la figure, nous avons noté que le routeur est configuré pour être un distributeur d'adresses IP, cela permet aux utilisateurs qui se connectent sur le réseau d'obtenir dynamiquement et automatiquement leurs configurations IP.

❖ **Configuration des paramètres Call Manager Express**

```
telephony-service
 max-ephones 5
 max-dn 5
 ip source-address 192.168.20.1 port 2000
 auto assign 1 to 6
!
ephone-dn 1
 number 02001
!
ephone-dn 2
 number 02002
!
ephone-dn 3
 number 02003
!
```

Figure Ⅳ.10 : Vérification de la configuration des paramètres Call Managers Express

Cette capture d'écran montre les paramètres de services téléphoniques que nous avons configuré.

❖ **Activation de l'OSPF**

```
!
router ospf 1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
!
```

Figure Ⅳ.11 : vérification de l'activation de l'OSPF

Ⅳ.2.3 Configurations de Pare-feu ASA

❖ **Sécurisation de l'accès au mode d'exécution privilégié**

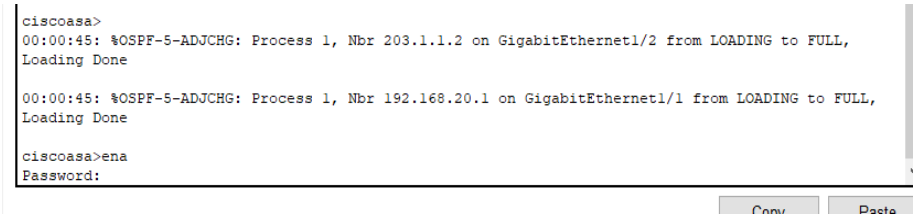

Figure Ⅳ.12 : Vérification de la sécurisation de Pare-feu ASA

Comme montre dans la figure ci-dessus, l'accès au mode privilégié dans le pare-feu ASA nécessite un mot de passe.

❖ **Configuration des interfaces Inside, Outside et Dmz**

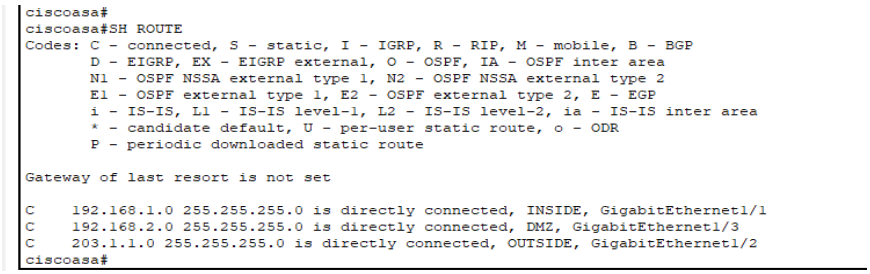

Figure Ⅳ.13 : Vérification de la configuration des interfaces de pare-feu

D'après cette figure, nous pouvons voir l'existence des trois zones (Inside, Outside et DMZ) dans le Pare-feu ASA.

❖ **Configuration des protocoles de routage**

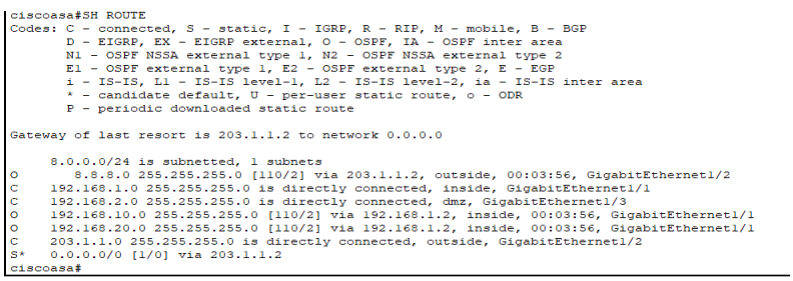

Figure Ⅳ.14 : Vérification de la Configuration des Protocoles de routage

Cette figure illustre l'apparition de la route par défaut et le protocole OSPF.

❖ **Configuration de l'ICMP :**

Un Ping d'un PC2 vers le Routeur Outside (203.1.1.2)

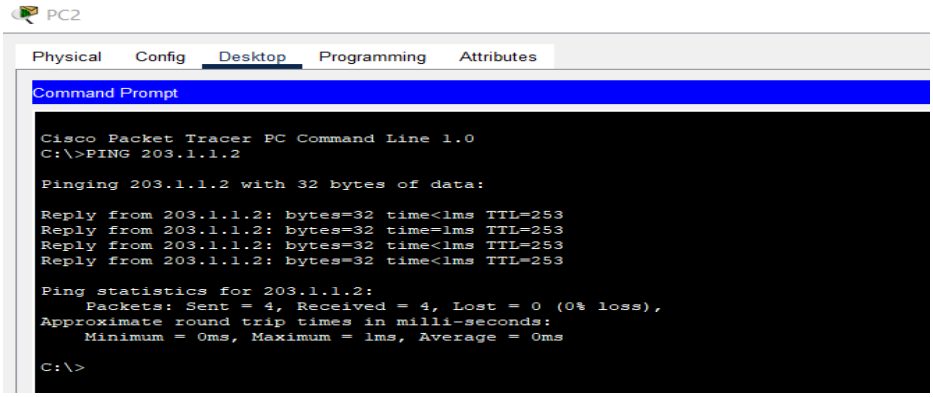

Figure Ⅳ.15 : Test de configuration de l'ICMP

Comme indiqué par la figure Ⅳ-15, le test par le ping montre une communication de LAN vers l'extérieur ce qui indique que l'ICMP est bien configuré.

❖ **Établissement d'une session SSH :**

✓ Du serveur GOOGLE vers l'ASA (203.1.1.1) :

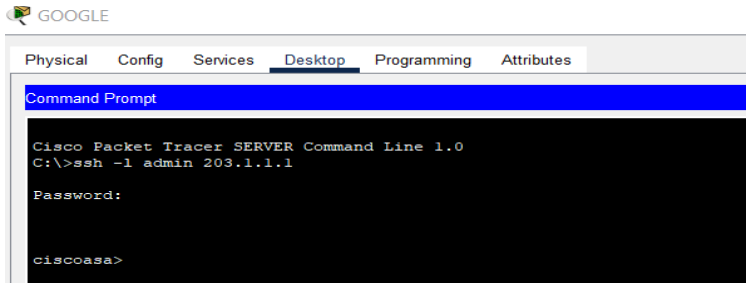

Figure Ⅳ.16 : Test de configuration de SSH 1

✓ Du PC2 vers l'ASA (192.168.1.1) :

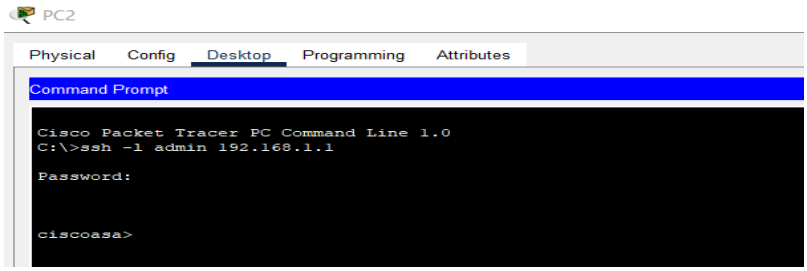

Figure Ⅳ.17 : Test de configuration SSH 2

Ⅳ.3 Tests de connectivité

Ici, nous montrerons la connectivité entre les différents équipements.

Ⅳ.3.1 Fonctionnement des VLANs

❖ **Ping du PC2 au PC0**

Nous allons réaliser un ping entre deux utilisateurs du même VLAN (DATA), PC2 (192.168.10.4) et PC0 (192.168.10.2)

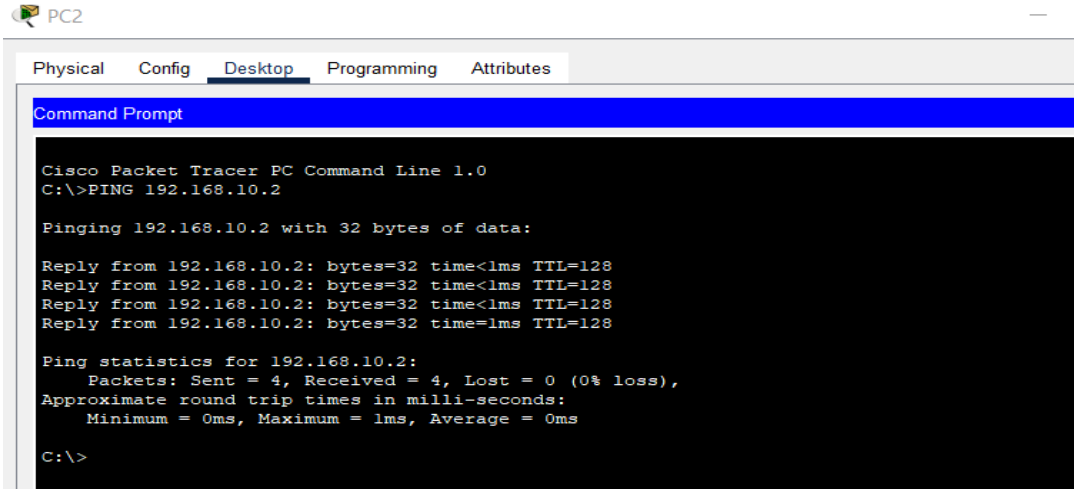

Figure Ⅳ.18 : Test de connectivité entre deux utilisateurs du même VLAN

Selon la figure, nous pouvons voir qu'un ping est effectué entre deux utilisateurs du même VLAN, la connexion est établit entre PC1 et PC0.

❖ **Appel de l'IP Phone1 vers IP Phone0**

Nous allons effectuer un appel du l'IP Phone 1 (VLAN VOICE) vers l'IP Phone 0 (VLAN VOICE). IP Phone1 (02003), IP Phone0 (02002)

Figure Ⅳ.19 : Affectation d'un appel de IP Phone1 vers IP Phone0

❖ **Ping du PC0 (VLAN DATA) au l'IP Phone1 (VLAN VOICE)**

Nous allons réaliser un ping entre deux utilisateurs qui se trouvent dans des VLANs différents**.** PC0 (192.168.10.2), IP Phone1 (192.168.20.3)

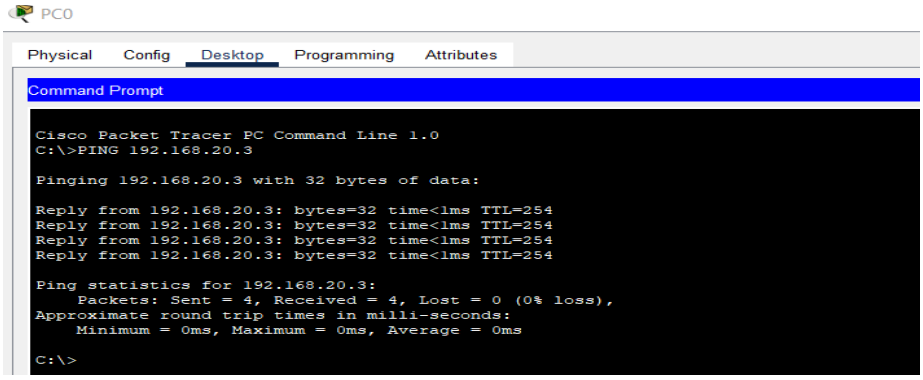

Figure Ⅳ.20 : Test de connectivité entre utilisateurs de deux VLAN différents

D’après cette capture d’écran, nous pouvons voir que le ping est effectué et que la connexion entre utilisateurs de deux VLAN différents est établit avec succès.

- Nous remarquons ici que les tests de connectivité ont réussi et que l’inter VLAN fonctionne très bien.

Ⅳ.3.2 Fonctionnement de Pare-feu

Ici nous allons montrer la bonne communication entre le réseau LAN et l’accès internet.

❖ **LAN vers DMZ**

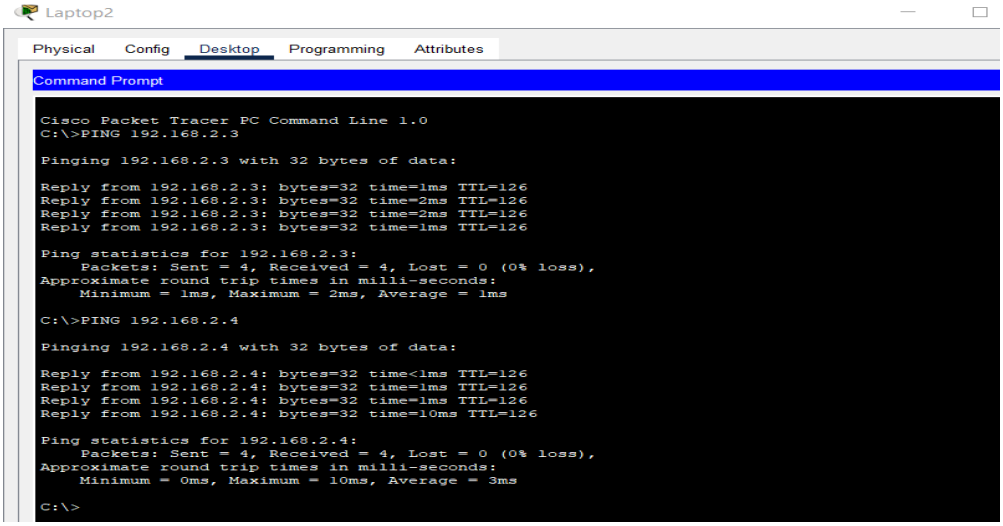

Figure Ⅳ.21 : Test de connectivité entre le LAN et la DMZ

Cette figure illustre que les machines qui se trouvent sur le réseau local peuvent accéder aux serveurs qui se trouvent sur le DMZ avec des adresses privées.

❖ **LAN vers WAN**

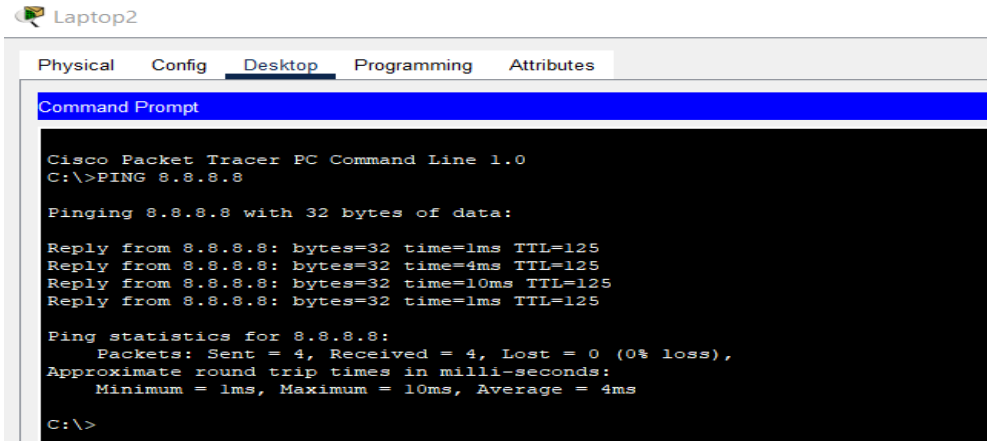

Figure Ⅳ.22 : Test de connectivité entre le LAN et le WAN

D’après la figure, nous pouvons voir que les machines qui se trouvent sur le réseau local peuvent accéder à internet et que le serveur DNS est bien configuré, car cette requête fait appelle en premier lieu au serveur DNS pour recevoir les IPs des serveurs de la DMZ puis on teste notre connexion à ce serveur.

❖ **WAN vers DMZ**

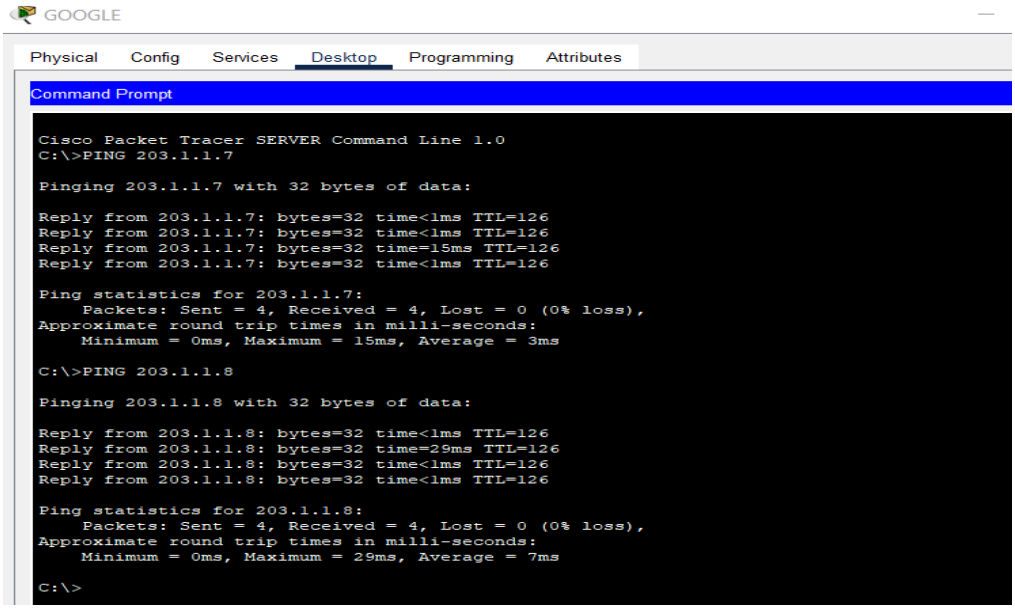

Figure Ⅳ.23 : Test de connectivité entre le WAN et la DMZ

D’après cette figure, nous constatons que le réseau WAN peut accéder aux serveurs Web et Mail de la DMZ à partir des adresses publics.

❖ **WAN vers LAN**

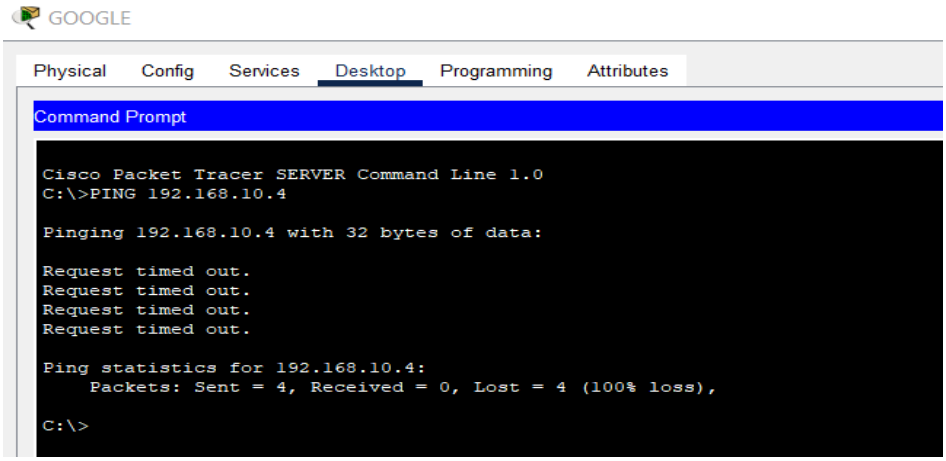

Figure Ⅳ.24 : Test de connectivité entre le WAN et le LAN

D’après ce test, nous pouvons noter que l’accès Internet à notre réseau LAN est impossible. Ce qui signifie que notre solution a réussi.

Ⅳ.4 Discussion

Dans ce chapitre, nous avons procédé à des tests et à des vérifications de notre conception et de la mise en œuvre de l'architecture adoptée. Ces tests ont été réalisés pour voir le niveau de sécurité mis en place grâce à la synergie des différents protocoles de sécurité. Selon les résultats des différents tests, le fonctionnement a été optimisé et la sécurité a été assurée en le constatant grâce aux différents Pings que nous avons effectués.

Conclusion :

Le travail que nous avons présenté dans ce mémoire a consisté en la sécurisation d'un réseau informatique de type LAN pour entrepris. En premier lieu, nous avons présenté des généralités sur les réseaux informatiques et la sécurité informatique. En second lieu, pour répondre à notre objectif, nous avons analysé et étudié le réseau informatique de centre ERSTC d'Algérie Télécom pour lequel nous avons intégré une politique de sécurité. Ainsi, nous avons identifié des failles concernant le fonctionnement et en particulier, nous avons constaté un niveau de sécurité très faible. Grace à cette étude, nous avons élaboré une stratégie permettant à la fois d'optimiser le fonctionnement et d'intégrer la sécurité. Pour ce faire, une nouvelle architecture a été proposée. Dans cette architecture, nous avons combiné un Pare-feu, une DMZ et des VLAN, un pare-feu pour améliorer la capacité à gérer efficacement le trafic interne et externe et protéger le réseau local contre d'éventuelles attaques basées sur Internet, une DMZ pour établir une protection qui sépare le réseau LAN de l'environnement externe, garantissant ainsi une sécurité renforcée et des VLANs pour contenir et minimiser les dommages potentiels. De plus, nous avons intégré la VoIP pour assurer une communication vocale claire et professionnelle entre les utilisateurs de réseau. Enfin nous avons introduit des mots de passe au niveau de Switch et router.

Afin de montrer la fiabilité de notre solution, nous avons simulé l'architecture du réseau proposée avec les nouveaux équipements en utilisant le simulateur CISCO Packet Tracer. Sur ce simulateur, nous avons effectué toutes les configurations nécessaires pour un meilleur fonctionnement. Des tests ont été effectués en utilisant la commande Ping qui permet de vérifier la connectivité des équipements. Selon ces tests, la solution de sécurité proposée est satisfaisante. En effet, en fonction du cahier de charge établi, les connectivités constatées sont en parfaite corrélation.

Malgré le niveau de sécurité assuré par cette stratégie, des améliorations peuvent être envisagées. Dans cette optique, il est possible d'intégrer d'autre protocole, tel que le VPN.

Références

[1] Dental.Lifeline, NETWORK, Metropolitan Area, NETWORK,Local Area, et al.Definition.Available at : dentalifeline.org.Accessed February,2016,vol.9.

[2] jacques Philippe,réseau intranet et internet, ellipses 2010.

[3] Solange Ghernaouti-Hélie- Sécurité informatique et réseaux- Dunod,2011.

[4] P.Guy. Initiation-ux-réseaux, Eyrolles 8ème édition,2014.

[5] Sadiqui.A Sécurité des réseaux informatiques, publié en grande Bretagne 2019 ISLTE Editions Ltd.

[6] J-F. Pillou, J-p. Bay, 2009. Tout sur la sécurité informatique, Edition Eyrolles, France.

[7] G.DESGEORGE. La sécurité des réseaux ,3eme édition Dunod ,2012.

[8] https://www.uplink.fr/blog/informatique/quest-ce-quun-reseau-informatique.

Résumé en français

Dans ce mémoire, notre objectif principal était d'améliorer la sécurité des réseaux informatiques de type LAN utilisés par les entreprises. Pour atteindre cet objectif, nous avons commencé par donner un aperçu des réseaux et de la sécurité informatique. Nous avons ensuite procédé à une analyse approfondie du réseau informatique du centre ERSTC d'Algérie Télécom, dans le but de mettre en œuvre une politique de sécurité globale. Lors de notre analyse, nous avons identifié plusieurs faiblesses opérationnelles, notant notamment un manque important de mesures de sécurité. En utilisant les informations tirées de notre étude, nous avons élaboré une stratégie pour améliorer à la fois la fonctionnalité et la sécurité. Dans le cadre de cette stratégie, nous avons proposé une nouvelle architecture pour améliorer la gestion du trafic interne et externe et protéger le réseau local contre les attaques potentielles provenant d'Internet, nous avons mis en place un pare-feu. De plus, nous avons établi une DMZ pour fournir une couche de protection supplémentaire, isolant efficacement le réseau LAN de l'environnement externe et garantissant une sécurité accrue. De plus, des VLAN ont été mis en œuvre pour confiner et atténuer tout dommage potentiel. Enfin, des mots de passe ont été implémentés au niveau du commutateur et du routeur.

Pour démontrer la fiabilité de notre solution, nous avons effectué une simulation de la structure de réseau suggérée à l'aide du simulateur CISCO Packet Tracer, intégrant les nouveaux équipements. Grâce à ce simulateur, nous avons méticuleusement configuré tous les paramètres essentiels pour garantir des performances optimales. Pour évaluer la connectivité, nous avons effectué des tests à l'aide de la commande Ping. Sur la base des résultats de ces tests, nous pouvons affirmer avec confiance que la solution de sécurité proposée répond aux attentes et est jugée satisfaisante.

Résumé en anglais

In this thesis, our main objective was to improve the security of LAN-type computer networks used by companies. To achieve this goal, we started by providing an overview of networking and IT security. We then carried out an in-depth analysis of the computer network of the ERSTC center of Algérie Télécom, with the aim of implementing a global security policy. During our analysis, we identified several operational weaknesses, including a significant lack of security measures. Using the insights from our study, we developed a strategy to improve both functionality and security. As part of this strategy, we proposed a new architecture to improve internal and external traffic management and protect the local network against potential attacks from the Internet, we implemented a firewall. Additionally, we established a DMZ to provide an additional layer of protection, effectively isolating the LAN from the external environment and ensuring increased security. Additionally, VLANs have been implemented to contain and mitigate any potential damage. Finally, passwords were implemented at the switch and router level.

To demonstrate the reliability of our solution, we performed a simulation of the suggested network structure using the CISCO Packet Tracer simulator, integrating the new equipment. Using this simulator, we have meticulously configured all the essential parameters to ensure optimal performance. To assess connectivity, we performed tests using the Ping command. Based on the results of these tests, we can confidently say that the proposed security solution meets expectations and is rated satisfactory.

Mots clés : Types de réseaux informatiques, les architectures des réseaux LAN, les topologies des réseaux LAN, le modèle de référence OSI, le modèle TCP/IP, les modes de transmission, les équipements d'interconnexion réseaux, les techniques de commutation, DHCP, ICMP, sécurité réseau, les attaques informatiques, VLAN, Firewall, DMZ, ACL, NAT.