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

UNIVERSITÉ MOULOUD MAMMERI DE TIZI-OUZOU

جامعة مولود معمري تيزي وزو
ⵜⴰⵙⴷⴰⵡⵉⵜ ⵎⵓⵍⵓⴷ ⵎⴰⵎⵔⵉ ⴰⵜ ⵟⵉⵣⵉ ⵡⵣⵓ
Université Mouloud Mammeri de Tizi-Ouzou

FACULTÉ DU GÉNIE ÉLECTRIQUE ET D'INFORMATIQUE
DÉPARTEMENT DE TÉLÉCOMMUNICATIONS

Mémoire de Master Académique

Domaine : **Sciences et Technologies**
Filière : **Télécommunications**

Spécialité : **Réseaux et Télécommunications**

Présenté par
Manel MOKDAD
Feriel IDRI

Thème

Étude et simulation d'un réseau sécurisé sous Cisco Packet Tracer

Mémoire soutenu publiquement le 25/09/2025. devant le jury composé de :

Président	Mr. Ouadah Mohammed Chamse Eddine	MCA, UMMTO
Promotrice	Mme. Abba Faiza	MCB, UMMTO
Examinatrice	Mme. Hamadouche Hadjira	MAB, UMMTO
Co-Promoteur	Mr. Akel Oussama	Network Engineer, BNH

Remerciements

Nous souhaitons, avant toute chose, exprimer notre profonde gratitude à Madame Abba Faiza, notre promotrice, pour son encadrement bienveillant, sa disponibilité, ses conseils avisés et son accompagnement tout au long de la réalisation de ce mémoire. Sa rigueur, sa patience et ses encouragements ont été d'une grande aide et nous ont permis d'avancer sereinement dans ce travail.

Nous remercions également très sincèrement les membres du jury, pour le temps qu'ils ont consacré à l'évaluation de note mémoire, ainsi que pour l'intérêt qu'ils ont porté à notre travail. Leurs remarques et suggestions sont pour nous une source précieuse d'amélioration et de réflexion.

Nos remerciements s'adressent aussi à nos familles respectives, pour leurs soutiens moral, leurs patience et leur confiance tout au long de notre parcours universitaire. Leur présence constance nous a permis d'aller au bout de ce projet avec détermination. Enfin, nous remercions chaleureusement nos amis pour leur écoute, leurs encouragements et les moments de partage qui nous ont permis de garder notre motivation intacte et l'entraide qui ont rythmé cette belle aventure universitaire

Dédicaces

Nous dédions ce travail à nos familles, pour leur amour inconditionnel, leur soutien moral et leur confiance sans faille tout au long de notre parcours.

A nos parents, qui ont toujours cru en nous, nous encouragent à donner le meilleur de nous-mêmes, et nous ont transmis des valeurs de persévérance et de rigueur.

A nos frères, surs et proches, pour leurs patience et leur présence bienveillante, même dans les moments difficiles.

Nous dédions également ce mémoire à nos amis, pour leurs soutien, leurs encouragements et les instants de complicité qui ont allégé nos journées de travail.

Table des matières

Liste des figures

Liste des tableaux

Abréviations

ACL Access Control list.

ARP Address Resolution Protocol.

ASA Adaptive Security Appliance.

BGP Border Gateway Protocol.

CIDR Classless Interdomain Routing.

CSMA/CD Carrier Sense Multiple Access/ Collision Detection.

DDoS Distributed Denial of Service.

DHCP Dynamic Host Configuration Protocol.

DMZ DeMilitarized Zone.

DNS Domain Name System.

EIGRP Enhanced Interior Gateway Routing Protocol.

FDDI Fiber Distributed Data Interface.

FTP File Transfert Protocol.

HSRP Hot Standby Router Protocol.

HTTP HyperText Transfer Protocol.

HTTPS HyperText Transfer Protocol Secure.

IETF Internet Engineering Task Force.

IP Internet Protocol.

IPS Intrusion Prevention System.

IPSec Internet Protocol Security.

ISO International Organization for Standardization.

ISP Internet Service Provider.

LACP Link Aggregation Control Protocol.

LAN Local Area Network.

LLC Logical Link Control.

MAC Media Access Control.

MAN Metropolitan Area Network.

MAU Multistation Access Unit.

NAT Network Address Translation.

OSI Open System Interconnection.

OSPF Open Shortest Path First.

PAN Personal Area Network.

QoS Quality of Service.

RIP Routing Information Protocol.

SSH Secure Shell.

SSL Secure Sockets Layer.

TCP Transmission Control Protocol.

UDP User Datagram Protocol.

VLAN Virtual Local Area Network.

VLSM Variable Length Subnet Mask.

VPN Virtual Private Network.

WAN Wide Area Network.

Introduction générale

Dans un monde de plus en plus interconnecté, les réseaux informatiques représentent la colonne vertébrale de la communication et du partage d'informations. Que ce soit dans les entreprises, les administrations, ou même les foyers, ils offrent un accès instantané et fluide aux ressources numériques. Cependant, cette expansion de la connectivité entraîne plusieurs défis, en particulier sur le plan de la sécurité.

Face à la multiplication des cyberattaques, des intrusions et des fuites de données, la sécurisation des réseaux est devenue une priorité absolue pour les administrateurs et ingénieurs systèmes. Il ne s'agit plus seulement de mettre en place un réseau fonctionnel, mais aussi d'assurer son intégrité, sa confidentialité et sa disponibilité [1].

Dans ce contexte, la simulation de réseaux informatiques s'impose comme un moyen efficace pour concevoir, tester et valider des architectures réseau avant leur déploiement réel. Cisco Packet Tracer, en particulier, est un outil pédagogique et couramment utilisé qui offre la possibilité de simuler des équipements réseau complexes, tout en intégrant des dispositifs de sécurité tels que des pares-feux, des routeurs ou des commutateurs [2].

Ce mémoire s'aligne sur cette logique. L'objectif est de concevoir et de simuler un réseau informatique sécurisé en utilisant Cisco Packet Tracer. L'étude vise à élaborer une architecture réseau réaliste, intégrant des processus de segmentation, de filtrage et de protection contre les menaces potentielles. Le but est de démontrer comment un environnement virtuel peut servir de laboratoire d'expérimentation pour évaluer différentes stratégies de sécurisation, tout en garantissant les performances et la résilience du réseau.

Ce mémoire s'organise comme suit :

Le premier chapitre présente les généralités et les concepts fondamentaux des réseaux informatiques.

Le deuxième chapitre introduit tout ce qui est sécurité des réseaux en exposant les principales menaces, vulnérabilités et mécanismes de protection (pare-feu, VPN, authentification, segmentation, etc.)

Le troisième chapitre décrit les architectures, les technologies ainsi que la méthodologie utilisée pour la simulation.

Le dernier chapitre présente les étapes de mise en uvre ainsi que la simulation sous Cisco Packet Tracer, l'analyse des résultats et les tests de connectivité effectués.

Chapitre I
Généralités sur les réseaux informatiques

I.1 Introduction

Les réseaux informatiques sont aujourd'hui au cur de la vie moderne. Ils constituent l'infrastructure essentielle qui permet l'échange et le partage d'informations, aussi bien dans les organisations que dans les foyers. Leur rôle dépasse largement la simple interconnexion des ordinateurs : ils facilitent la communication, soutiennent la collaboration et servent de support à de nombreuses applications critiques, qu'il s'agisse de la navigation sur Internet, de la gestion des données ou encore du fonctionnement des systèmes distribués. Dans ce chapitre, nous présentons les notions fondamentales liées aux réseaux informatiques, en abordant leur définition, leur classification, leurs topologies, ainsi que les modèles de référence qui régissent leur fonctionnement. Ces connaissances sont fondamentales pour pouvoir comprendre par la suite des architectures plus avancées et des problématiques liées à la sécurité [3, 4].

I.2 Définition d'un réseau informatique

Un réseau informatique peut être défini comme un ensemble d'équipements reliés entre eux par des supports de transmission, permettant l'échange de données et de services. Ces équipements peuvent être des ordinateurs, des périphériques (imprimantes, caméras IP, etc.) ou encore des dispositifs intermédiaire comme les routeurs et les commutateurs. L'objectif principal d'un réseau est de rendre possible le partage des ressources, qu'il s'agisse de fichiers, d'applications ou d'accès Internet, tout en garantissant la rapidité, la fiabilité et la sécurité des échanges [5].

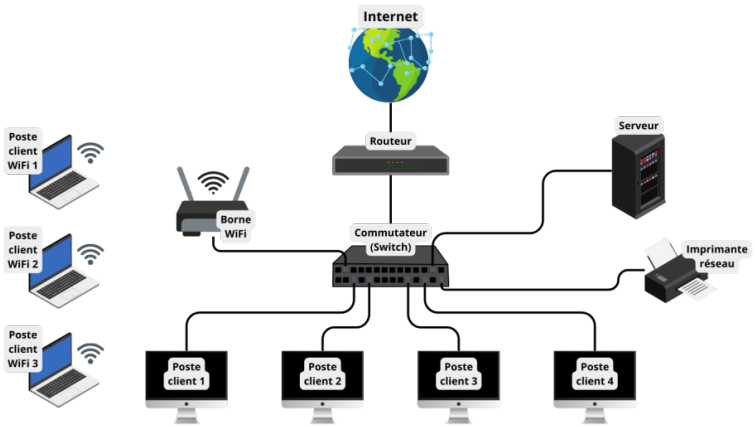

FIGURE I.1 – Représentation d'un réseau informatique [6]

I.3 Classification des réseaux informatiques selon leur étendue

La classification d'un réseau informatique se base sur pleins d'aspects, notamment :

La localisation

La taille (Nombre de machines connectées)

La distance

Le débit

Ces caractéristiques nous permettent de définir quatre catégories distinctes de réseaux.

FIGURE I.2 – Classement des réseaux par leur taille [7]

I.3.1 PAN (Personal Area Network)

Les réseaux personnels, également appelés PAN (Personal Area Network), sont conçus pour permettre aux appareils de communiquer à une échelle individuelle. Ils servent principalement à relier un ordinateur à ses périphériques, tels qu'un écran, un clavier, une souris ou une imprimante. Traditionnellement, ces connexions nécessitent des câbles, ce qui peut rendre leur installation complexe et peu pratique [4].

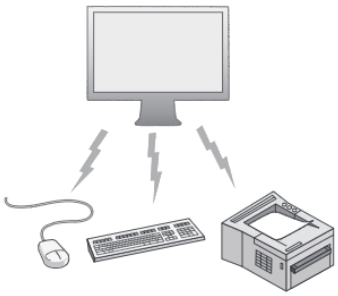

FIGURE I.3 – Représentation d'un PAN [4].

I.3.2 LAN (Local Area Network)

Le LAN est un réseau local qui permet de relier des machines et des périphériques dans un périmètre restreint, allant de quelques mètre à quelques milliers de mètre comme par exemple une maison ou une entreprise. Il est considéré comme un réseau privé et n'est pas accessible pour quelqu'un de l'extérieur à sa zone de déploiement [6].

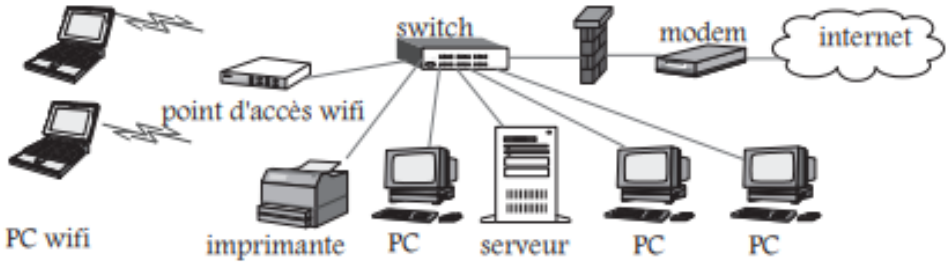

FIGURE I.4 – Représentation d'un LAN [7]

I.3.3 MAN (Metropolitan Area Network)

Un Réseau métropolitain est un réseau reliant plusieurs sous-réseaux LAN situés à proximité géographique l'un de l'autre (environ une dizaines de kilomètres), telle qu'un village ou une ville. Ainsi, un MAN permet de relier plusieurs nuds distants et leur permet de s'échanger et de communiquer simulant un réseau LAN à grande échelle [7].

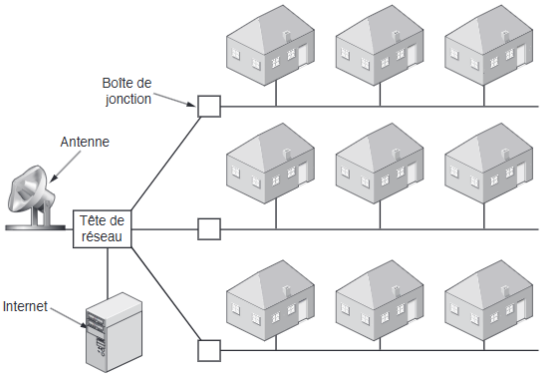

FIGURE I.5 – Représentation d'un MAN [4]

I.3.4 WAN (Wide Area Network)

Un WAN est un réseau ressemblant au MAN mais qui couvre une zone géographique très large, pouvant aller d'un pays à plusieurs continents. Internet constitue l'exemple le plus connu de réseau WAN. Ce type de réseau repose sur l'interconnexion de multiples réseaux MAN et LAN, à travers des liaisons de télécommunication (fibre optique, satellites, etc.) [4].

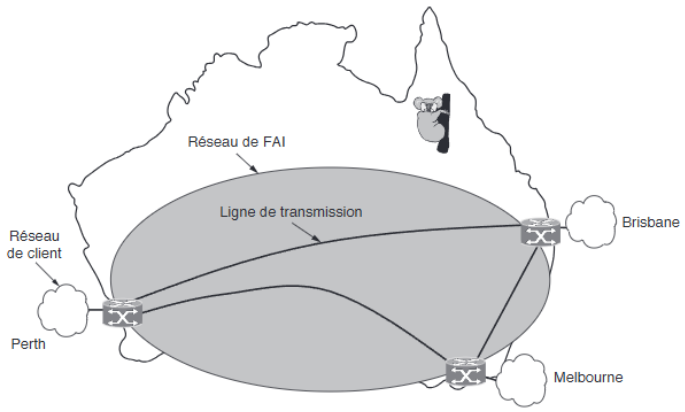

FIGURE I.6 – Représentation d'un WAN [4]

I.4 Topologie des réseaux informatiques

La topologie d'un réseau désigne la manière dont les différents équipements (ordinateurs, câblage, dispositifs d'interconnexion, etc.) sont disposés et connectés entre eux [5] [8].

On distingue deux classes de topologies :

la topologie physique : définie la façon avec laquelle les équipements et machines sont connectés entre eux via les supports physiques illustrant parfaitement la disposition matérielle réelle des liaisons.

La topologie logique : décrit la façon dont les flux de données circulent au sein du réseau.

I.4.1 Topologie physique

I.4.1.1 Topologie en bus

Dans cette topologie tous les équipements sont reliés à un seul et même câble. Pour la fiabilité, une défaillance d'une machine n'affecte pas le fonctionnement du reste du réseau ce qui assure l'intégrité du réseau en lui même [9].

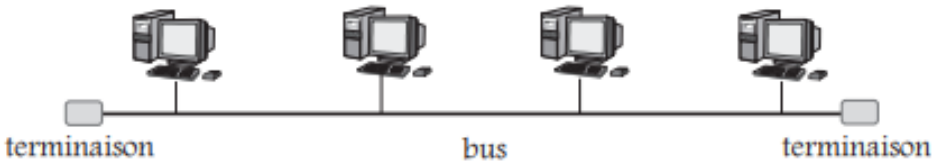

FIGURE I.7 – Topologie en bus [9].

I.4.1.2 Topologie en anneau

Cette topologie utilise une boucle fermée entre toutes les machines qui doivent être connectées, les données passent par toutes les machines qui agissent comme un répéteur en retransmettant le signal. Un MAU (Multistation Access Unit) est souvent utilisé dans ce genre de topologie, jouant le rôle d'anneau [8, 9].

FIGURE I.8 – Topologie en anneau, logique et réelle [9]

I.4.1.3 Topologie en étoile

Tous les équipements sont connectés directement à un équipement central, tel qu'un commutateur ou un concentrateur qui représente le centre de toutes les transmissions.

Cette topologie facilite l'intégration des équipements dans la limite de la capacité du commutateur.

Le fait que toutes les transmissions transitent par l'équipement central simplifie la gestion du réseau. Par ailleurs, une panne d'un équipement terminal n'affecte pas le fonctionnement général du reste du réseau. En revanche, une panne sur le concentrateur immobilise tout le réseau [8, 9].

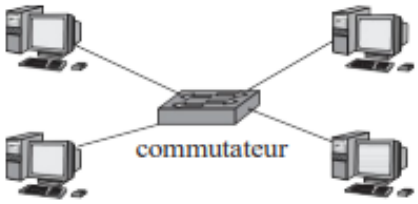

FIGURE I.9 – Topologie en Etoile [9]

I.4.1.4 Topologie arbre

La topologie en arbre combine plusieurs étoiles reliées entre elles de façon hiérarchique. Elle est très répandue dans les réseaux d'entreprise car elle permet d'étendre la couverture et d'organiser les équipements par niveaux. Sa hiérarchisation simplifie l'administration, mais la dépendance aux équipements centraux reste une limite [10].

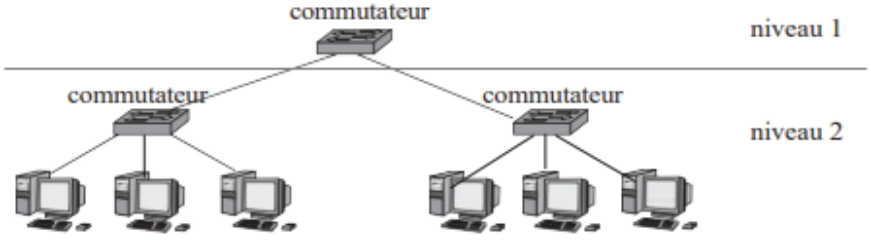

FIGURE I.10 – Topologie en arbre [9]

I.4.1.5 Topologie maillée

C'est une topologie qui est efficace pour contrer les problèmes d'interruptions de communications. Tous les hôtes disposent de leurs propres liaisons avec les autres hôtes. C'est le cas de la structure du réseau Internet qui offre plusieurs itinéraires vers une destination donnée [9].

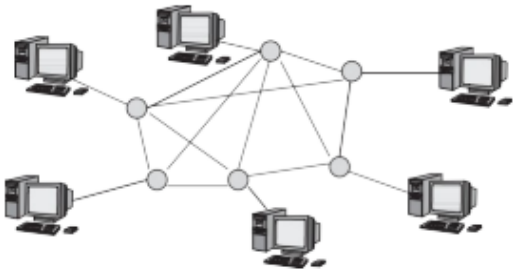

FIGURE I.11 – Topologie maillée [9]

I.4.2 Topologie logique

I.4.2.1 Ethernet

L'Ethernet est le modèle logique le plus courant dans les réseaux locaux, s'appuyant sur une structure physique en étoile. Les données y circulent grâce à un protocole connu sous le nom de CSMA/CD, ce protocole régule l'accès au support de transmission pour éviter toute collision de données [10].

I.4.2.2 Token ring

Elle est basée sur une topologie physique en forme d'anneau, utilisant le système d'accès par jeton.

Dans ce système, seul l'appareil en possession du jeton est autorisé à communiquer ; si un appareil souhaite envoyer des données, il doit attendre jusqu'à ce qu'il reçoive le jeton. Dans un réseau Token Ring, chaque nud du réseau est équipé d'un MAU capable de recevoir des connexions des appareils Et permet d'amplifier le signal en transit [10].

I.4.2.3 Topologie FDDI

La technologie LAN FDDI (Fiber Distributed Data Interface) est une méthode de connexion au réseau qui utilise des câbles en fibre optique.

Le FDDI se compose de deux cercles : un cercle principal et un cercle secondaire.

Le deuxième cercle a pour objectif de corriger les erreurs du premier. Le FDDI emploie un anneau à jeton pour détecter et corriger les erreurs, permettant ainsi au réseau de fonctionner même si une station MAU tombe en panne [10].

I.5 Architecture des réseaux

I.5.1 Client/serveur

Cette architecture repose ceux deux machines/programmes qui interagissent [14] :

Client : celui qui formule une demande de service (par exemple, un navigateur web, une application mobile, un logiciel de messagerie, etc.).

Serveur : celui qui attend, traite et répond aux demandes du client (par exemple, un serveur web, un serveur de messagerie, un serveur de base de données, etc.).

Le fonctionnement repose sur un échange de type requête/réponse, le client envoie ses requêtes au serveur, et le serveurs renvoie des réponses à celles-ci.

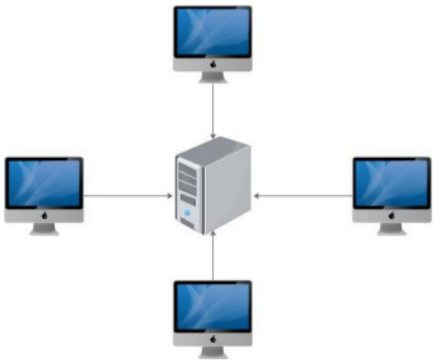

FIGURE I.12 – Architecture Client/serveur

I.5.2 Peer to Peer

L'architecture peer-to-peer contrairement à l'architecture client/serveur est une architecture dans laquelle toutes les machines sont à la fois client et serveur, une même machine peut à la fois faire des requêtes mais aussi traiter les requêtes de ses autres paires grâce à la décentralisation des données, réduisant ainsi la charge de travail sur une seule machine [14].

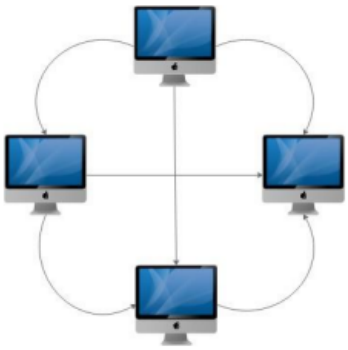

FIGURE I.13 – Architecture Peer to Peer

I.6 Les modèles d'architecture réseau

I.6.1 Modèle OSI

L'OSI (Open system interconnection) est un modèle de réseau établit par l'ISO (International standard organisation), afin de standardiser la communication entre réseaux et équipements hétérogènes c'est-à-dire provenant de différents fabricants.

Il divise le processus réseau en sept couches logiques, chaque couche ayant des propres fonctionnalités et offre des services aux couches immédiatement adjacentes [9].

I.6.1.1 Couche physique

La couche physique appelée niveau 1 ou niveau bits, est chargée de transmettre les bits provenant de la couche liaison de données en utilisant des signaux physiques adaptés au support : signaux électrique, optique ou hertziens. Elle décrit également les caractéristiques de la transmission : câbles, connecteurs et carte réseau, etc [9].

I.6.1.2 Couche liaison de données

La couche liaison de données est la couche numéro 2 du modèle OSI. Son rôle est d'assurer une communication fiable entre deux machines directement connectées dans un réseau local ou sur un lien point à point, elle est divisée en deux sous-couches [11] :

Contrôle de liaison logique (LLC), c'est la sous-couche haute de la liaison de données, elle sert d'interface entre la couche réseau (IP, IPX, etc.) et la sous-couche MAC. Sa fonctionnalité principale est d'identifier les protocoles transportés dans les trames et permettre d'ajouter des informations de contrôle pour faciliter le transit des données.

Contrôle d'accès au support (MAC), c'est la sous-couche la plus basse de la liaison de données, son rôle est de gérer l'accès physique au support de transmission (câble, fibre, Wi-Fi, etc.).

I.6.1.3 Couche réseau

La couche réseau appelée niveau 3 ou niveau paquet, est responsable de l'acheminement des données ou le routage entre différents réseaux grâce à l'adressage qu'elle effectue. Si un nud est inutilisable, alors on redirige les données vers un autre nud [9].

I.6.1.4 Couche transport

La couche transport également appelée niveau 4 ou niveau segments. Elle fournit un service de transport de bout en bout. Cela comprend l'initiation, le maintien et la clôture de la connexion entre deux systèmes. Elle est responsable de la gestion de flux, du contrôle d'erreur et des services qui ne sont pas fournis dans les couches inférieures.TCP et UDP sont les principaux protocoles utilisés dans cette couche [9].

I.6.1.5 Couche session

La couche session permet l'établissement et la fermeture d'une session de communication entre deux machines distantes, tout en garantissant un dialogue synchronisé [9].

I.6.1.6 Couche présentation

Elle permet de standardiser les données afin de permettre aux deux systèmes de communiquer. Elle gère aussi la conversion, compression et cryptage des données [9].

I.6.1.7 Couche application

La couche application offre des services utilisables par les applications comme le FTP pour le transfert de fichiers, le courrier électronique et la messagerie, l'accès aux fichiers distants NFS, le terminal virtuel Telnet etc. [9].

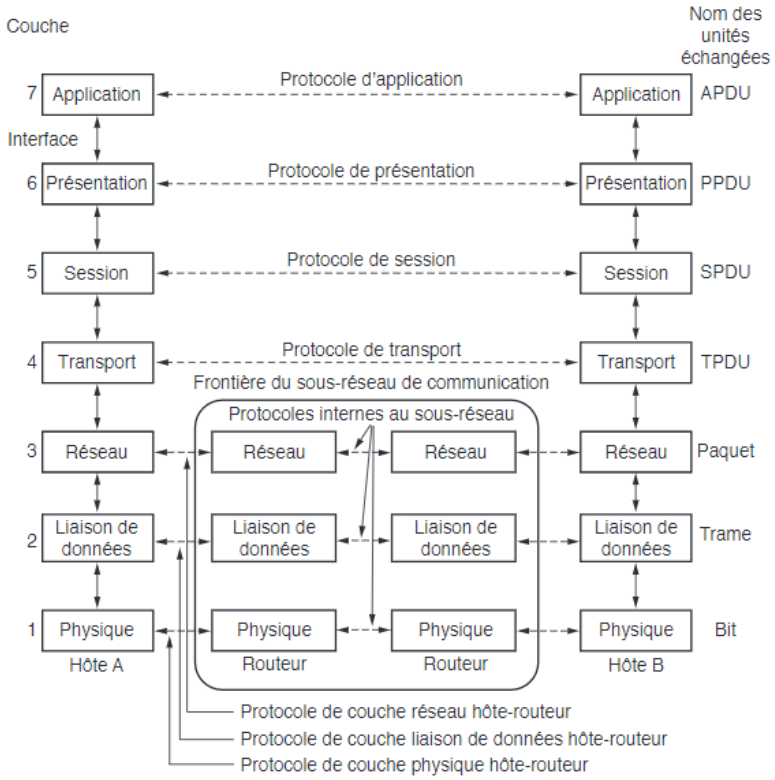

FIGURE I.14 – Le modèle de référence OSI [4]

I.6.2 Modèle TCP/IP

TCP/IP est un modèle regroupant plusieurs protocoles de communication qui permet l'échange de données sur un réseau, notamment Internet. Il repose sur deux éléments fondamentaux : IP (Internet Protocol), chargé de l'adressage et du routage des paquets, et TCP (Transmission Control Protocol), qui garantit la fiabilité et l'intégrité de la transmission. Ensemble, ils forment la base de l'architecture réseau moderne organisée en quatre couches [12].

I.6.2.1 Couche accès au réseau

La couche la plus basse du modèle TCP/IP. Elle correspond aux couches Physique et Liaison de données du modèle OSI. elle gère l'accès physique au support de transmission, encapsule les données en trame et assure l'échange entre les appareils d'un même réseau LAN [12].

I.6.2.2 Couche internet

la couche Internet permet le routage des données à travers différents réseaux, en gérant les adresses et le routage des paquets, et constitue le cur du fonctionnement d'Internet [5].

I.6.2.3 Couche transport

La couche transport assure non seulement l'acheminement des données, mais prend également en charge des aspects liés à la qualité de service, comme la fiabilité, la gestion du flux et la correction des erreurs [5].

I.6.2.4 Couche application

La couche application est celle qui met en relation directe l'utilisateur avec le réseau, en présentant les données de manière exploitable par les programmes. Elle regroupe aussi les fonctions des couches présentation et session du modèle OSI [5].

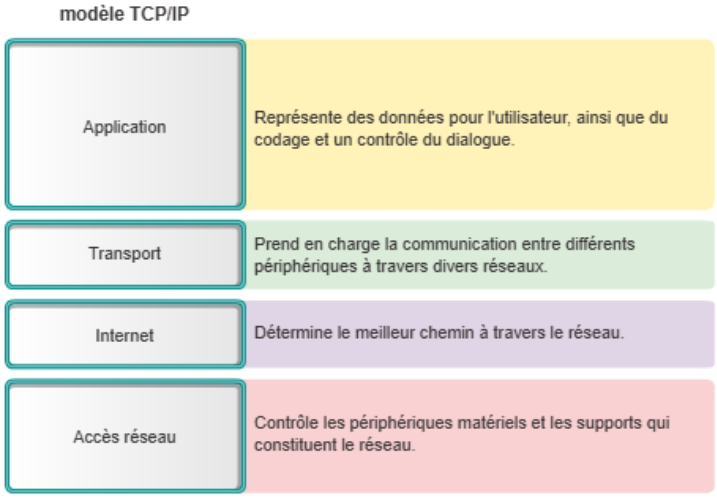

FIGURE I.15 – Modèle TCP/IP [11]

I.6.3 Comparaison

On peut décrire les protocoles qui composent le modèle TCP/IP en se basant sur le modèle OSI. La couche d'accès réseau de TCP/IP qui gère l'accès physique correspond aux couches 1 et 2 du modèle OSI. Les couches 3 et 4 sont similaires dans les deux modèles : IP gère l'adressage et le routage (couche réseau), tandis que le TCP et le UDP s'occupent des transmissions

des données (couche transport). Enfin, la couche application du modèle TCP/IP regroupe les couches 5, 6 et 7 du modèle OSI, facilitant ainsi le fonctionnement des applications réseau [11].

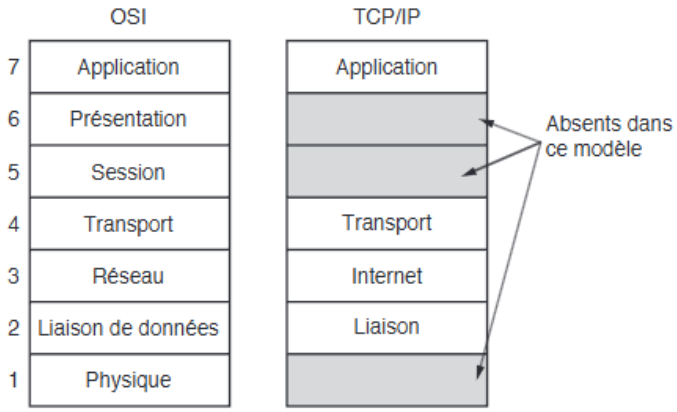

FIGURE I.16 – Le modèle de référence TCP/IP [4]

I.6.4 Encapsulations et désencapsulations de données

L'encapsulation de données consiste à ajouter des en-têtes de protocole supplémentaires qui assurent la transmission des paquets de données c'est-à-dire les données initiales sont encapsulées ou enveloppées dans plusieurs protocoles avant leur transmission.

Sur l'hôte destinataire, ce processus est inversé. La désencapsulation est le processus inverse, à l'arrivée, chaque couche retire l'enveloppe correspondante pour transmettre la donnée à la couche supérieure [11].

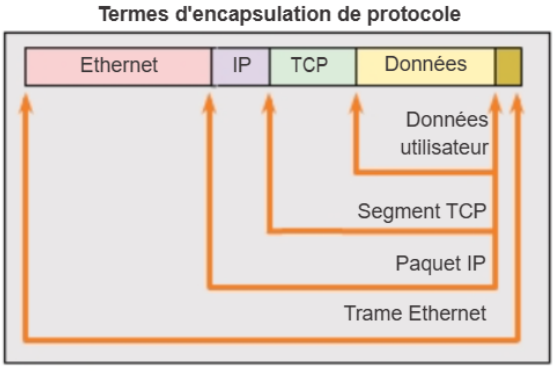

FIGURE I.17 – Encapsulation des protocoles [11]

I.7 Adressage IP

Chacun des éléments d'un réseau qu'il s'agisse d'un simple LAN ou du réseau Internet utilisant le protocole IP doit avoir une adresse IP unique sur ce réseau.

Ainsi, chaque ordinateur, interface de routeur et périphérique réseau (tels que les imprimantes, caméras, etc.) sera pris en compte et aura sa propre adresse distincte.

L'adresse IP sert donc, d'une part, à distinguer chaque composant de manière unique dans l'ensemble du système d'information, et d'autre part, à effectuer le routage des datagrammes IP au sein du réseau [9].

I.7.1 Le protocole IP

Le protocole IP est un protocole de la couche Internet du modèle TCP/IP, responsable du routage et l'adressage des données sur les réseaux. Il permet aux paquets de transiter d'une source à une destination, que ça soit dans le même réseau ou entre deux réseaux différents.

Le protocole IP est caractérisé par [11] :

Manque de fiabilité : IP ne garantit pas l'acheminement des données ni leur ordre de transmission ; c'est le rôle du protocole TCP si nécessaire.

Indépendant du support : le fonctionnement est indépendant du support qui transporte les données.

Protocoles complémentaires : certaines tâches nécessitent d'autres protocoles pour que la communication fonctionne correctement tel que ICMP et l'ARP.

I.7.2 IPv4

Une adresse IPv4 est un identifiant sur 32 bits (4 octets) codés en décimales, et séparées par des points. Elle est constituée d'une partie réseau (ID-Réseau), qui indique le réseau auquel la machine est rattachée, et d'une partie hôte (ID-Machine), qui permet d'identifier précisément l'ordinateur au sein de ce réseau [13].

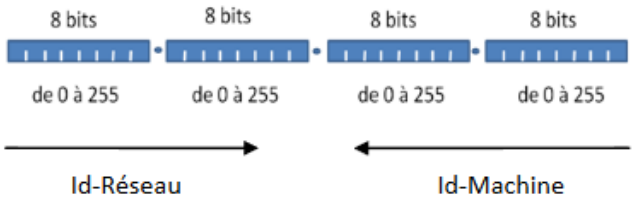

FIGURE I.18 – Adresse IP [7]

I.7.2.1 Adresse réseau

Dans une adresse IP, lorsque tous les bits de la partie hôte sont à zéro, on obtient l'adresse réseau. Elle est utilisée, notamment par les routeurs, pour identifier et atteindre un réseau sans avoir besoin de connaître l'adresse IP précise d'un appareil. C'est pourquoi cette adresse ne peut être attribuée à aucun équipement du réseau [9].

I.7.2.2 Masque de sous-réseau

Un masque de sous-réseau est une suite de bits qui sépare la partie réseau de la partie hôte d'une adresse IP. Il permet d'identifier si deux adresses appartiennent au même réseau ou à des

réseaux différents. De plus, il définit l'étendue du réseau et facilite l'organisation des adresses IPv4 afin d'optimiser le routage et la gestion des sous-réseaux [16].

I.7.2.3 Passerelle par défaut (Default Gateway)

La passerelle par défaut est l'adresse qui permet d'acheminer le trafic d'un réseau local vers des réseaux extérieurs. Elle joue ainsi le rôle de point de sortie du réseau local vers d'autres réseaux, comme Internet [11].

I.7.2.4 Types d'adresses IPv4

Il existe plusieurs type d'adresse IPv4 [9, 13] :

Monodiffusion (Unicast) : Une adresse unique attribuée à un périphérique, permettant une communication directe entre deux hôtes.

Diffusion (Broadcast) : Lorsque tous les bits de la partie hôte d'une adresse IP sont à 1, on obtient l'adresse de diffusion. Elle permet d'envoyer un message simultanément à toutes les machines appartenant au même réseau, mais ne peut pas être assignée à un périphérique.

Multidiffusion (Multicast) : Une adresse réservée à un groupe d'hôtes afin de transmettre les données à plusieurs destinataires sélectionnés, tout en limitant le trafic. Les adresses comprises entre 224.0.0.0 et 239.255.255.255 sont dédiées à la multidiffusion en IPv4.

Adresse de bouclage (Loopback) : C'est une adresse utilisée par une interface pour s'envoyer un message a elle-même et vérifier le bon fonctionnement de la carte réseau. Un Ping vers 127.0.0.1 (l'adresse de Loopback) doit produire une réponse appropriée.

I.7.2.5 Les différentes Classes d'adresses IP

IPv4 repose sur une structure d'adresses classées, où les quatre premiers bits définissent la classe [16].

Classe	Bits de départ	Plage d'adresses	Masque de sous-réseau
A	0	1.0.0.0 – 126.255.255.255	255.0.0.0 (/8)
B	10	128.0.0.0 – 191.255.255.255	255.255.0.0 (/16)
C	110	192.0.0.0 – 223.255.255.255	255.255.255.0 (/24)
D	1110	224.0.0.0 – 239.255.255.255	Non définie
E	11110	240.0.0.0 – 255.255.255.255	Non définie

TABLEAU I.1 – Classes d'adresses IP et leurs caractéristiques [16].

- Adresses IP publiques : ce sont des adresses attribuées par l'organisation officielle IANA (Internet Assigned Numbers Authority) et servent à identifier de façon unique un réseau à l'échelle mondiale. Par exemple, l'adresse 209.85.135.147 correspond à la version française de Google [15].

- Adresses IP privées : Ces adresses servent à identifier un hôte à l'intérieur d'un réseau local. Contrairement aux adresses publiques, elles ne peuvent pas être routées sur Internet, et nécessitent l'utilisation d'un système de traduction d'adresses (NAT) pour communiquer avec l'extérieur les plages d'adresses privées sont [15] :
  - Classe A : 10.0.0.0.à 10.255.255.255
  - Classe B : 172.16.0.0 à 172.31.255.255
  - Classe C : 192.168.0.0 à 192.168.255.255

  Seules les adresses des classes A, B et C peuvent être attribuées à des interfaces (adresse Unicast).

  La classe D est réservée aux adresses Multicast, tandis que la classe E est destinée à des usages expérimentaux ou scientifiques [13].

I.7.2.6 La notation CIDR (Classless InterDomain Routing)

Le CIDR permet d'indiquer directement dans l'adresse IP le nombre de bits qui définissent la partie réseau de l'adresse, cela correspond au nombre de bits attribués à la partie réseau du masque sous-réseaux, plutôt que de représenter le masque sous-réseaux d'une adresse en notation décimale pointée, le CIDR propose d'écrire l'adresse suivie de ń / nombre de bits a 1 ż, par exemple : 255.255.255.192 => 26 bits à 1 => ń /26 ż [13].

I.7.2.7 Les sous-réseaux

Les sous-réseaux (ou subnetting) permettent de diviser un réseau IP en plusieurs segments plus petits en empruntant des bits à la partie hôte pour les ajouter à la partie réseau. Chaque sous-réseau possède sa propre plage d'adresses, son identifiant réseau et une adresse de broadcast, ce qui facilite l'organisation, la gestion et l'exploitation efficace des réseaux [16].

I.7.2.8 VLSM

Le VLSM (Variable Length Subnet Mask) fonctionne de manière similaire au subnetting classique mais offre plus de flexibilité. Plutôt que de créer plusieurs sous réseaux de même taille, il est possible d'adapter la taille de chaque sous-réseau selon le nombre d'appareils requis afin d'éviter le gaspillage d'adresses IP [16].

I.7.3 IPv6

Face à l'insuffisance de l'adressage IPV4, L'IETF a proposé l'IPv6, la nouvelle version du protocole IP conçu pour remplacer l'IPv4.

L'IPV6 se distingue par une capacité d'adressage supérieure, un en-tête simplifié et optimisé ainsi que la possibilité d'autoconfiguration (SLAAC). Il intègre également le protocole IPSec

qui offre des fonctions d'authentification et de chiffrement directement dans l'en-tête des paquets ainsi que l'élimination du NAT grâce à sa capacité d'adressage, ce qui permet de sécuriser les communications [9].

I.8 Les différents dispositifs de la connectivité

La mise en réseau de machines, PC, imprimantes, scanners, caméraetc., nécessite l'usage d'équipements d'interconnexion divers qui fonctionnent chacun à un niveau spécifique du modèle OSI dans le but d'assurer une communication fluide entre les composants du réseau.

I.8.1 Le Répéteur

Un répéteur est un équipement qui opère au niveau 1 du modèle OSI. Il permet de régénérer et renforcer le signal en l'amplifiant lorsqu'il s'affaiblit et subit des distorsions en raison de la distance qui sépare deux équipements, le répéteur ne fais donc aucun traitement de données et se contente de copier bit par bit tout ce qu'il reçoit [9].

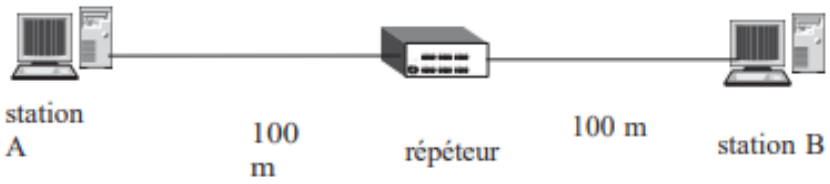

FIGURE I.19 – Répéteur [9]

I.8.2 Le concentrateur

Le concentrateur ou Hub est un équipement permettant de connecter plusieurs hôtes disposés en étoile afin de leur donner accès au réseau. Comme le répéteur, il intervient uniquement au niveau de la couche physique. Il se contente de récupérer les données qui lui parviennent par l'un de ses ports pour les transférer sur l'ensemble de ses autres ports. De nos jours, les concentrateurs sont peu courants, car ils ont été remplacés par des équipements plus efficaces tels que les commutateurs, offrant une meilleure gestion du trafic réseau [9].

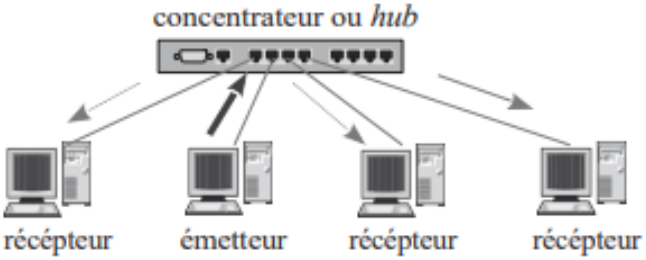

FIGURE I.20 – Concentrateur [9]

I.8.3 Le commutateur

Un commutateur ou Switch est un équipement multiports similaire au hub, mais intervenant au niveau de la couche 2. Il analyse les adresses MAC des trames reçues sur un port pour les rediriger uniquement vers les ports destinataires ce qui permet de réduire les collisions et améliorer la performance du réseau : c'est ce qu'on appelle la commutation de données, aujourd'hui les commutateurs sont indispensables dans les réseaux LAN et peuvent être administrables ce qui permet l'ajout de fonctionnalités supplémentaires tel que les VLANs, l'Access à distance via SSH ou Telnet et bien d'autres. Il existe cependant des switches de niveau 3 appelées switches multicouches [9].

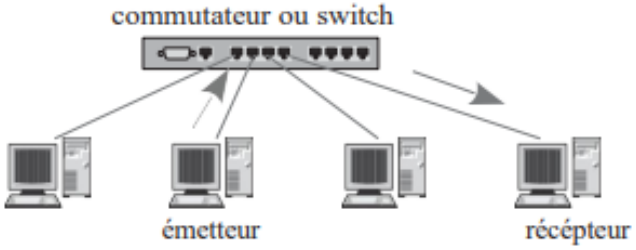

FIGURE I.21 – Commutateur [9]

I.8.4 Le Routeur

Un routeur est un équipement essentiel des réseaux informatiques, Il fonctionne au niveau de la couche réseau du modèle OSI. Il assure la liaison de plusieurs réseaux distincts à travers le routage, en fonction de l'adresse IP, de l'itinéraire qu'un paquet devrait emprunter pour arriver à destination que ce soit dans un autre réseau ou via internet, au-delà de ses fonctions de base, il peut également inclure des services comme le NAT, le DHCP ou des fonctions de sécurité [9].

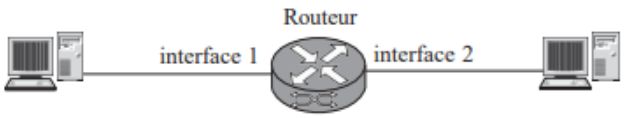

FIGURE I.22 – Routeur [9]

I.8.5 Le Pont

Le pont est un équipement à deux ports qui assure la liaison entre des réseaux fonctionnant avec des supports physiques différents, par exemple un réseau filaire et un réseau sans fil. Contrairement au répéteur qui travaille au niveau physique, le pont fonctionne au niveau de la couche liaison de données. Il peut analyser les trames qui passent par ses ports et ne transmettre que celles qui sont destinées à l'autre réseau. Le pont tend à disparaître au profit du commutateur qui remplit les mêmes fonctions tout en offrant davantage de ports et de meilleures performances [9].

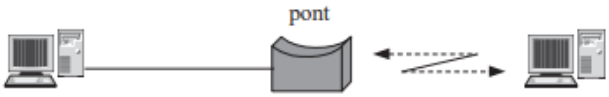

FIGURE I.23 – Pont [9]

I.9 Conclusion

Dans ce premier chapitre on a abordé les bases fondamentales nécessaires à la compréhension des réseaux informatiques. Après avoir défini ce qu'un réseau, nous avons distingué les différents types existants en fonction de leurs portées et de leur usage, tel que les réseaux personnels (PAN), locaux (LAN), métropolitains (MAN) et étendus (WAN).

Nous avons ensuite exploré les topologies physiques et logiques qui structurent les réseaux, ainsi que les principales architectures d'échanges de données, notamment les modèles client-serveur et pair-à-pair. Les modèles d'architecture réseau, en particulier le modèle OSI et le modèle TCP/IP, ont été examinés pour comprendre le fonctionnement en couches et l'organisation des communications. L'étude de l'adressage IP et des protocoles associés a permis de mieux appréhender les mécanismes d'identification et de routage au sein d'un réseau.

Enfin, une présentation des dispositifs de connectivité tels que les routeurs, commutateurs ou répéteurs a permis d'illustrer concrètement les éléments matériels qui rendent possible l'interconnexion et la transmission des données.

Ainsi, ce chapitre constitue une base solide pour aborder les aspects plus techniques et spécifiques du domaine des réseaux informatiques dans les chapitres suivants.

Chapitre II
La sécurité des réseaux

II.1 Introduction

La sécurité des systèmes et des réseaux informatiques représente un aspect indispensable de la cybersécurité face au divers menaces internes et externe. Face à l'évolution constante et de plus en plus complexe des cyberattaques, l'adoption de mesures de sécurité solides s'avère indispensable pour empêcher tout accès illicite aux ressources du réseau, ainsi que pour identifier et contrer les attaques en temps réel. La sécurité entraine généralement la mise en uvre de moyens techniques et principalement de solutions préventives. Il est donc nécessaire que l'entreprise soit formée et consciente des risques. Ainsi il est nécessaire d'établir une politique de sécurité efficace basée sur la collaboration des employés et l'utilisation d'équipements et techniques sécurisés tout en garantissant une protection contre toute sorte d'attaques informatiques Ce chapitre abordera les différents éléments liés à la sécurité, les types d'attaques, les mécanismes de détection et de protection des réseaux informatiques [17] [18].

II.2 Définition de la sécurité des réseaux informatiques

La sécurité des réseaux informatiques représente l'ensemble des politiques, procédures et mécanismes techniques mis en place pour protéger les ressources d'un réseau informatique. Elle vise à empêcher les accès non autorisés, à limiter les risques d'altération ou de perte de données, et à garantir le bon fonctionnement des services pour les utilisateurs [19].

II.3 Importance de la sécurité

Donner de l'importance à la sécurité relèvent de plusieurs raisons :

La sécurité informatique protège les données personnelles et organisationnelles contre tout accès non autorisé.

L'éducation en cybersécurité est essentielle pour prévenir les attaques et les failles de sécurité.

Maintenir les systèmes à jour et utiliser des mots de passe forts sont essentiels pour une bonne protection.

II.4 Défi de la sécurité informatique

La sécurité informatique fait face aujourd'hui à plusieurs défis majeurs, en raison de l'évolution rapide des technologies et de la multiplication des cybermenaces. La sécurisation des systèmes d'information ne se limite pas à l'installation de solutions technique, elle nécessite une approche globale [20].

Parmi les principaux défis rencontrés :

La complexité croissante des infrastructures : la surface d'attaque s'élargit considérablement, rendant plus difficile la surveillance et le contrôle d'accès.

L'évolution constante des menaces : Les cyberattaques deviennent de plus en plus sophistiquées, difficiles à détecter. Des techniques telles que les ransomwares, les attaques phishing nécessitent des capacités de détection et de réponse en constante évolution.

La vulnérabilité humaine : L'utilisateur reste souvent le maillon faible du système. Le manque de sensibilisation, les erreurs de manipulation, ou encore l'utilisation de mots de passe faibles exposent les systèmes à des risques importants.

L'équilibre entre sécurité et performance : renforcer la sécurité ne doit pas nuire à la disponibilité ou à la performance des systèmes.

II.5 Enjeux de la sécurité informatique

La figure II-1 montre les différents critères de la sécurité qui doivent être pris en compte lors de la mise en place d'une politique de sécurité dans un système d'informatique.

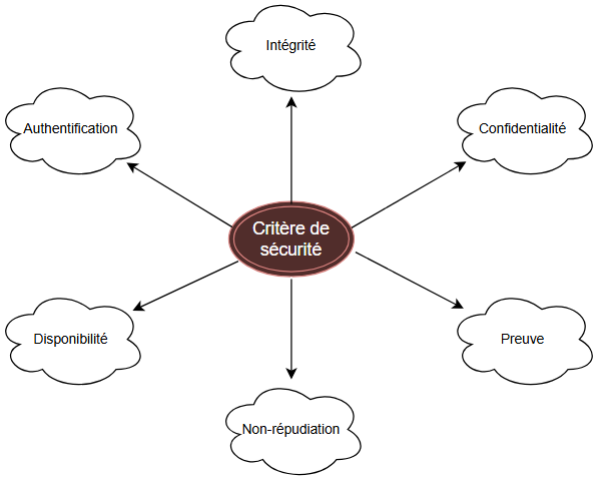

FIGURE II.1 – Critères de sécurité

II.5.1 La confidentialité

La confidentialité garantit que seules les personnes autorisées ont accès à l'information, et qu'elle ne sera pas divulguée en dehors d'un cadre défini [17].

II.5.2 L'intégrité

L'intégrité est la certitude que les données restent inchangées ou non altérée et que les processus de traitement sont complets [19].

II.5.3 L'authentification

L'authentification consiste à vérifier l'identité des utilisateurs, équipements ou services souhaitant accéder au réseau. Elle peut se faire par mot de passe, carte à puce, certificat numérique ou encore biométrie [19].

II.5.4 La disponibilité

La disponibilité garantit que les individus autorisés peuvent accéder à l'information lorsqu'ils en ont besoin ou dans les délais nécessaires pour son traitement [19].

II.5.5 La non-répudiation

La non-répudiation sert à établir la preuve qu'une entité a participé à un échange de données [19].

II.5.6 La preuve

La preuve consiste à vérifier que l'émetteur de l'information est correctement identifié et dispose des droits et accès requis, tout en s'assurant que le récepteur autorisé a bien la permission de consulter cette information [19].

II.6 Concepts et définitions en sécurité des réseaux

II.6.1 Vulnérabilité

Une vulnérabilité est une faille exploitable dans un système informatique, représentant le niveau d'exposition face à une menace. Elle peut permettre à cette dernière de compromettre la sécurité, l'intégrité, la confidentialité ou le bon fonctionnement du système. Une vulnérabilité peut résulter d'un défaut logiciel, d'une erreur de configuration ou d'une lacune organisationnelle [20].

II.6.2 Risque

Il s'agit de la probabilité qu'un incident de sécurité se produise lorsqu'une vulnérabilité est exposée face à une population malintentionnée qui cherchera à l'exploiter [20].

II.6.3 Attaques

Une attaque désigne le moyen d'exploiter une faille de sécurité en exerçant une action volontaire offensive ou malveillante dans le but de perturber, endommager ou prendre le contrôle d'un système. Elle peut cibler la confidentialité, l'intégrité ou la disponibilité des ressources du réseau. Les attaques peuvent être classées en deux types :

Attaques passives : Le but est d'intercepter les informations en cours de transmission sans perturber le système.

Attaques actives : Elles impliquent des modifications des données ou la création de fausses informations et perturbe le système [18].

II.6.4 Les hackers

Le terme hacker désigne une personne qui s'introduit sans autorisation dans les systèmes d'information. Dans un premier temps, les hackers visant une intrusion dans les systèmes informatiques recherchent des failles, soit des vulnérabilités qui compromettent la sécurité du système, dans divers éléments tels que les systèmes d'exploitation, les protocoles, les applications ou le personnel d'une organisation afin de l'exploiter et extraire le maximum d'informations sur l'architecture du réseau et du système. Dans le scénario le plus défavorable, cela pourrait entraîner des dégradations au niveau des données ou des applications. Toutefois, il n'est pas toujours facile de détecter sa présence sur les systèmes ni de connaître ce qu'il a provoqué comme dégâts [20] [21].

II.6.5 Programmes malveillants

Le terme Malware se réfère à un programme ou une partie de programme conçu pour perturber ou compromettre un système informatique. Leurs impacts peuvent se propager à l'ensemble du réseau de l'entreprise en infectant d'autres équipements [19].

II.6.5.1 Virus

Un virus est un logiciel auto-producteur qui s'attache à un programme légitime et qui a la capacité de se propager à d'autres dispositifs du réseau informatique en modifiant d'autres programmes pour y inclure une copie de lui-même, dans le but de causer des dysfonctionnements dans les systèmes informatiques ainsi que des altérations ou suppressions des données [21].

II.6.5.2 Ver

Un ver informatique est un programme malveillant capable de se reproduire automatiquement sur différents ordinateurs via un réseau, comme Internet. Contrairement à un virus, il n'a pas besoin d'un autre programme pour se propager, utilisant directement les ressources de l'ordinateur infecté. Il peut surveiller le système hôte, offrir une porte d'accès aux hackers, détruire des données et générer un grand nombre de requêtes vers un serveur afin de provoquer un déni de service [19].

II.6.5.3 Cheval de trois (Trojans)

Un cheval de Troie est un programme qui semble inoffensif mais est conçu pour exécuter discrètement des actions à l'insu de l'utilisateur. Il exploite généralement les droits de ce dernier pour voler ou endommager des données, ou pour créer une porte dérobée permettant à un attaquant de prendre le contrôle de l'ordinateur à distance [19].

II.6.5.4 Spyware

Un logiciel spyware (en français espion") est un logiciel malveillant conçu pour s'installer discrètement sur un ordinateur afin de rassembler et de transmettre des données à son créateur ou à un tiers, souvent sans que l'utilisateur ne s'en aperçoive [19].

II.6.5.5 Rootkit

Un rootkit ("jeu de démarrage" en français) est un programme malveillant qui a pour but de cacher sa présence ainsi que celle d'autres programmes dangereux, aussi bien à l'utilisateur qu'aux outils de sécurité comme les antivirus ou le pare-feu. Il agit en modifiant en profondeur le système d'exploitation, ce qui le rend un peu plus difficile à détecter [19].

II.6.5.6 Ransomwares (Rançongiciel)

Les rançongiciels, également appelés ransomwares, sont des programmes malveillants qui ont pour but de soutirer de l'argent à leurs victimes, Ils cryptent entièrement ou partiellement les données de l'ordinateur de la personne ciblée, puis affiche un message demandant le paiement d'une rançon pour les restituer. Certaines variantes s'attaquent aussi aux sauvegardes pour empêcher toute récupération [20].

II.7 Les étapes d'une attaque

La plupart des attaques informatiques, qu'elles soient simples ou complexes, suivent généralement les étapes suivantes [22] :

1. **Identification de la cible :** l'attaquant collecte des informations sur la cible en exploitant des données publiques, sans encore engager d'action hostile.
2. **Le scanning :** cette étape permet de compléter les informations obtenues, en identifiant les adresses IP, les services utilisés, le système d'exploitation, les versions des services, le sous-réseau, et les règles de pare-feu.
3. **L'exploitation :** cette étape consiste à exploiter les vulnérabilités détectées à partir des informations recueillies de la cible qu'il s'agisse des protocoles, des systèmes d'exploitation ou des services et applications en place sur le réseau.
4. **La progression :** l'objectif final du pirate est d'accéder aux droits root (racine) sur un système, lui permettant ainsi d'effectuer toutes ses actions souhaitées (inspecter la machine, collecter des informations, installer des backdoors, effacer les traces, etc.).

II.8 Les types d'attaques

Les hackers emploient diverses techniques d'attaques qui peuvent être classées en trois catégories distinctes :

Les attaques directes : Cible directement la victime depuis l'ordinateur de l'attaquant. En vérité, les outils de piratage qu'ils emploient sont peu configurables, et bon nombre de ces applications transmettent directement les paquets à la cible. Dans ce cas, il est facile de retracer l'attaque et identifier l'attaquant [23].

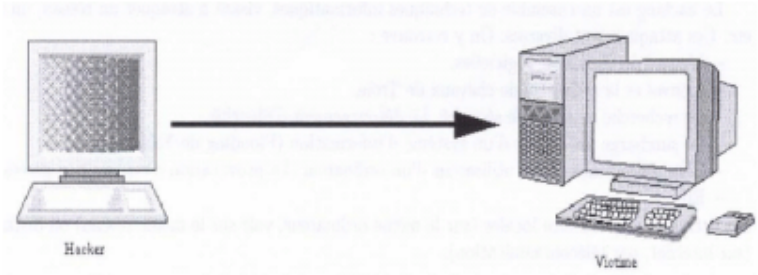

FIGURE II.2 – Attaque directe [23]

Les attaques indirectes par rebond : cette attaque est souvent utilisée car les paquets sont d'abord transmis à l'ordinateur relais qui le renvoie vers la cible. Le rebond offre deux avantages [23] :

Masquer l'adresse IP du pirate.

Exploite les ressources et la puissance (CPU, a bande passante) de l'ordinateur intermédiaire pour attaquer.

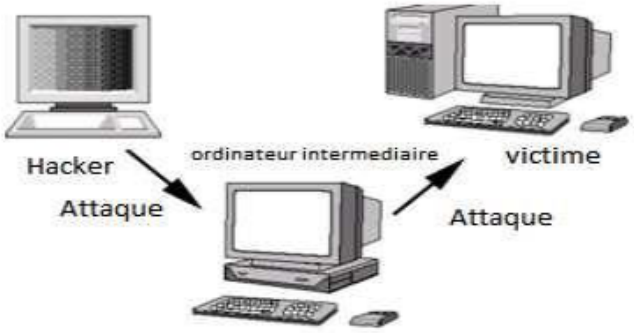

FIGURE II.3 – Attaque indirecte par rebond [23]

Les attaques indirectes par réponse : Il s'agit d'une variante de l'attaque par rebond. Le principe reste similaire pour le pirate, mais au lieu d'envoyer directement une attaque à un ordinateur intermédiaire pour qu'il la relaie, le hacker se contente d'envoyer une requête. C'est alors la réponse à cette requête qui est dirigée vers l'ordinateur cible [23].

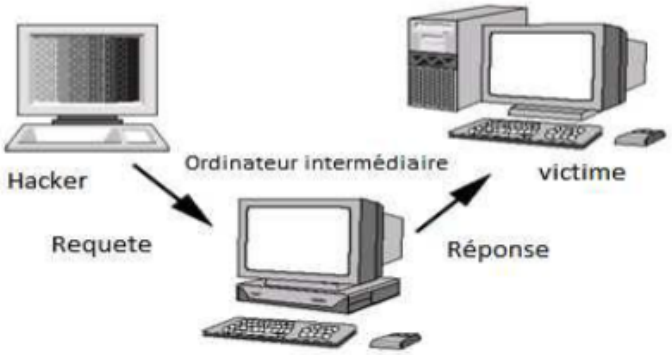

FIGURE II.4 – Attaque indirecte par réponse [23]

II.9 Les Techniques d'attaques

Une attaque est l'exploitation d'une faille d'un système informatique tel qu'un système d'exploitation, un logiciel ou bien même l'utilisateur. Généralement à des fins nuisibles et sans l'accord du propriétaire.

Afin de mieux s'en protéger, il est essentiel de connaître les principales techniques d'attaques pour mieux s'y préparer [20].

II.9.1 Les attaques réseaux

Les attaques réseaux visent le réseau lui-même ou ont un impact sur celui-ci, en exploitant les faiblesses de sécurité des protocoles réseau, les systèmes d'exploitation ou les équipements réseau tels que les routeurs, les serveurs ou encore les terminaux connectés par le biais du réseau [23].

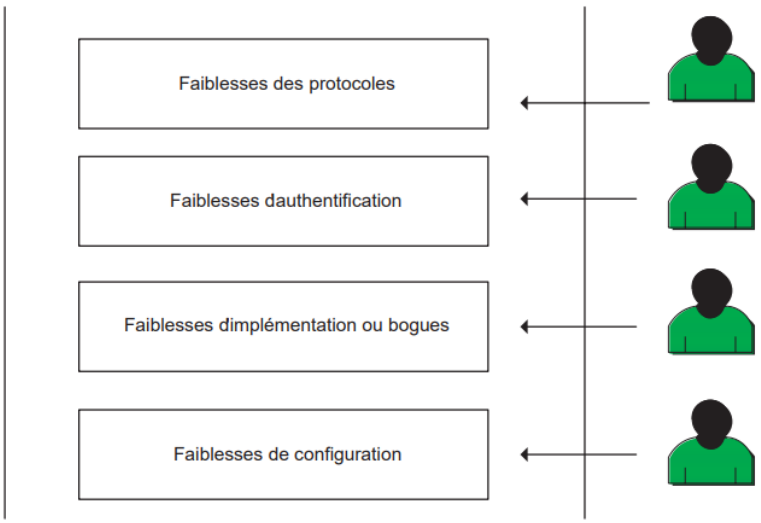

FIGURE II.5 – Les faiblesses de sécurité réseau [23]

Voici quelques exemples les plus courants d'attaques réseaux :

II.9.1.1 IP Spoofing

Cette attaque consiste à usurper l'adresse IP d'une machine en modifiant l'adresse IP source dans les paquets envoyés. Cela permet au pirate de masquer l'origine de l'attaque ou d'accéder à des services auxquels il n'était pas autorisé [24].

II.9.1.2 DNS Spoofing

Cette attaque consiste à envoyer des fausses réponses aux requêtes DNS émise par la victime. C'est-à-dire, attribuer une fausse adresse IP à un nom de domaine pour rediriger les utilisateurs, sans qu'ils ne s'en rendent compte, vers des sites pirates où ils transmettent leurs identifiants en toute sécurité [24].

On distingue deux méthodes principales pour effectuer cette attaque :

Empoisonnement du cache DNS

L'empoisonnement du cache DNS consiste à induire en erreur les serveurs DNS en leur présentant une réponse supposée valide à une requête, alors qu'en réalité, il s'agit d'une réponse falsifiée. Une fois le serveur DNS empoisonné, les données sont stockées en cache, exposant par conséquent tous les utilisateurs de ce serveur à des risques.

Par exemple, ce type d'attaque permet de rediriger un utilisateur vers un site web trompeur dont le contenu est utilisé pour la fraude ou qui sert de voie d'entrée pour des virus et autres logiciels malveillants [24].

DNS ID Spoofing

Le DNS ID Spoofing exploite le champ d'identification de l'en-tête DNS, qui sert à faire correspondre chaque réponse à la requête qui l'a générée. L'attaque consiste à envoyer une fausse réponse à une requête DNS avant que la vraie réponse n'arrive au serveur, en devinant l'identifiant (ID) de la requête. Sur un réseau local, il est facile de prédire cet ID en écoutant le trafic (sniffing) [24].

II.9.1.3 ARP Spoofing

L'ARP spoofing vise à détourner le trafic destiné à une machine vers une autre en modifiant les associations entre les adresses IP et les adresses MAC au sein du réseau local. Un attaquant peut se faire passer pour une autre machine et intercepter silencieusement les paquets transmis ou les modifier avant de les ré-acheminer vers leur véritable destinataire.

L'objectif est identique à celui du spoofing IP, cependant l'ARP Spoofing opère au niveau de la couche liaison de données. Lorsqu'un appareil doit envoyer un paquet IP, il a besoin de connaître l'adresse MAC correspondante à l'adresse IP de destination. Pour l'obtenir, il diffuse une requête ARP en broadcast sur le réseau local. Cette requête pose la question : ń Quelle est l'adresse MAC associée à cette adresse IP ? ż La machine qui possède l'adresse IP cible répond par un paquet ARP contenant son adresse MAC, que l'émetteur garde dans son cache ARP pendant une durée limitée.

L'attaque consiste à empoisonner ce cache ARP de la victime en lui envoyant de fausses réponses ARP indiquant que l'adresse MAC de la passerelle ou d'une autre machine appartient en réalité à l'attaquant. La victime envoie alors tout son trafic à l'adresse MAC de l'attaquant, qui peut l'observer, le modifier, puis le router vers la destination réelle, sans que la victime ne s'en rende nécessairement compte [24].

II.9.1.4 TCP Session Hijacking (désynchronisation)

Le TCP Session Hijacking par désynchronisation consiste à détourner un flux TCP afin de contourner une authentification par mot de passe. Comme la vérification d'identité n'a lieu qu'au moment de l'ouverture de la session, un attaquant qui réussit cette manipulation peut s'emparer de la connexion et en profiter pendant toute sa durée.

L'attaque débute par une phase d'écoute du réseau (sniffing) afin d'identifier le moment où une authentification a eu lieu. L'attaquant envoie alors un paquet utilisant l'adresse IP de la victime et le numéro d'acquittement TCP attendu par le serveur. Ce paquet a pour effet de désynchroniser la session TCP entre la victime et le serveur, tout en permettant à l'attaquant d'y injecter des commandes via la session déjà établie [24].

II.9.2 Les attaques applicatives

Les attaques applicatives exploitent principalement des vulnérabilités propres aux applications utilisées. Elles peuvent être classées en fonction de leur origine ou de la manière dont elles ciblent les applications.

II.9.2.1 Man in the middle

Le but principal d'une attaque Man-in-the-Middle (MiTM) est de détourner le trafic entre deux machines afin d'intercepter, modifier ou perturber les données échangées.

Par exemple, lorsqu'un client communique avec un serveur, un attaquant peut intercepter les requêtes du client en les redirigeant vers son propre serveur, puis altérer ces requêtes avant de les transmettre au serveur légitime et faire de même pour les réponses. Ainsi, l'attaquant a accès à l'intégralité des échanges et peut en extraire des informations sensibles sans que le client ou le serveur ne s'en aperçoive.

Le MiTM est un concept large qui recouvre plusieurs techniques exploitant ce même principe. Parmi elles, on trouve des variantes spécifiques comme le DNS Man-in-the-Middle, qui combine le détournement DNS avec une interception du trafic entre un client et un serveur web [24].

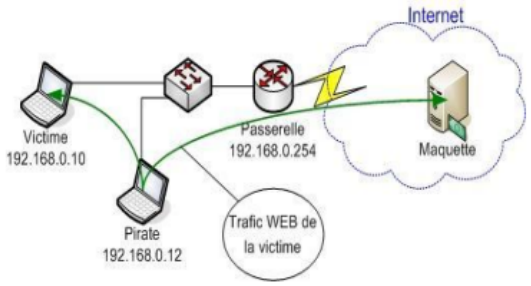

FIGURE II.6 – Man in the middle [25]

II.9.2.2 Le Déni de service (DOS)

Le déni de service (DoS) vise à rendre un service indisponible pour ses utilisateurs. Cela peut se faire de plusieurs manières : au niveau réseau en saturant la bande passante ou les ressources d'un équipement pour le rendre inopérant, ou au niveau applicatif en exploitant des failles pour provoquer le plantage d'un programme distant.

En tirant parti de vulnérabilités, un attaquant peut rendre inaccessible un service tel qu'un serveur web ou de messagerie, voire compromettre l'accès à l'ensemble d'un système.

Les méthodes courantes incluent les inondations de trafic, l'épuisement de ressources (CPU, mémoire, connexions) et l'envoi de requêtes spécialement conçues pour rendre une application ou un composant réseau obsolète [25].

II.9.2.3 SYN Flooding

Le SYN Flooding consiste à submerger une machine cible avec un grand nombre de tentatives de connexion TCP incomplètes. Il exploite le TCP three-way handshake : l'émetteur envoie un SYN, la cible répond par un SYN-ACK, puis l'émetteur doit renvoyer un ACK pour finaliser la connexion.

L'attaquant envoie un très grand nombre de requêtes SYN et ne répond jamais aux SYN-ACK. La cible garde alors de nombreuses connexions semi-ouvertes en attente, qui consomment des ressources mémoire et des descripteurs de connexion. Au bout d'un certain temps, la capacité de la machine est saturée et elle ne peut plus établir de nouvelles connexions légitimes, provoquant un déni de service [24].

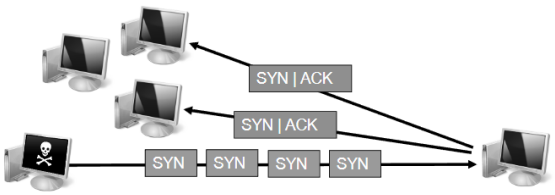

FIGURE II.7 – SYN Flooding [17]

II.9.2.4 UDP Flooding

L'UDP Flooding exploite l'absence de mécanismes de contrôle de flux et de congestion dans le protocole UDP. L'attaquant envoie un grand nombre de paquets UDP vers la victime, saturant la bande passante et les ressources réseau. Cette surcharge provoque une congestion généralisée et peut épuiser la capacité de traitement ou la mémoire des hôtes ciblés, entraînant une indisponibilité ou une dégradation des services [25].

II.9.2.5 Smurfing

Le smurfing est une attaque d'amplification du trafic ICMP. L'attaquant envoie des requêtes ICMP Echo (ping) à l'adresse de broadcast d'un réseau tout en usurpant l'adresse IP source pour faire croire que ces requêtes proviennent de la victime. Toutes les machines du réseau de diffusion répondent alors par des ICMP Echo Reply à l'adresse usurpée, multipliant ainsi le volume de trafic reçu par la cible par le nombre d'hôtes présents sur ce réseau. Le flot de réponses provoque une saturation de la bande passante et des ressources, ce qui entraine un déni de service pour la cible et souvent pour l'ensemble du réseau impliqué [24].

II.9.2.6 Déni de service distribué (DDOS)

Le déni de service distribué (DDoS) consiste à amplifier une attaque de déni de service en la lançant simultanément depuis un grand nombre de machines compromises. L'attaquant compromet d'abord ces machines pour constituer un réseau d'ordinateurs sous son contrôle (un botnet). Une fois le contrôle établi, il suffit d'ordonner à toutes les machines compromises d'attaquer la même cible en même temps (par exemple via un SYN Flood, des requêtes UDP massives, des pings ICMP, etc.).

L'intensité et la distribution géographique du trafic rendent l'attaque beaucoup plus difficile à contrer qu'un simple DoS : la cible et les infrastructures intermédiaires peuvent être rapidement saturées, rendant les services complètement indisponibles pour les utilisateurs légitimes [25].

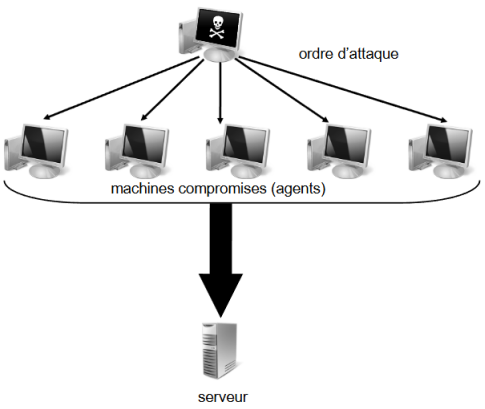

FIGURE II.8 – Attaque DDoS [17]

II.9.2.7 Porte dérobée (Backdoors)

Une porte dérobée est une faille de sécurité volontairement crée par un hacker pour lui permettre de garder un accès à un système, elle peut être installée automatiquement via un malwares tel qu'un virus ou un trojan, ou de manière manuelle par le pirate après avoir infiltré le système. On se sert souvent des chevaux de Troie pour cet objectif, car ils se déguisent en logiciels légitimes tout en offrant un accès dissimulé [20].

II.10 Motivation des attaques

Les attaques informatiques sont généralement motivés à des fins spécifiques, il est nécessaire de les connaitre afin de mieux s'en protéger. Voici les principales motivations des hackeurs [26] :

Intrusion dans le système.

Vol de données sensibles qu'elles soient industrielles, personnelles, commerciales ou organisationnelles.

Perturbation d'un service, en le rendant inutilisable pour ses utilisateurs, comme lors d'une attaque par déni de service (DoS).

Exploiter les ressources d'un système, comme sa bande passante, sans y être autorisé.

Atteinte à la vie privée, en accédant ou diffusant des données personnelles sans consentement.

Usurpation d'identité, dans le but de tromper ou d'accéder à des services de manière frauduleuse.

II.11 Les mécanismes de prévention et détections d'attaques

II.11.1 Les systèmes de prévention d'intrusion (IPS)

Les systèmes de prévention d'intrusion (IPS) regroupent des composants matériels et logiciels conçus pour bloquer automatiquement toute activité considérée comme suspecte. Leur rôle est d'intervenir en temps réel afin de neutraliser les menaces détectées et ainsi protéger le système avant qu'elles ne puissent causer des dommages [25].

II.11.2 Les systèmes de détection d'intrusions (IDS)

La détection d'intrusions consiste à surveiller et analyser les événements d'un système informatique ou d'un réseau pour repérer toute activité malveillante. Un IDS (Intrusion Detection System) est un logiciel ou un dispositif matériel qui automatise cette surveillance et cette analyse, permettant d'identifier rapidement les comportements suspects ou anormaux [25].

II.12 Protection contre les intrusions réseau

II.12.1 Les Firewalls

II.12.1.1 Définition

Un pare-feu (ou firewall) est un dispositif, matériel ou logiciel, conçu pour protéger un réseau contre les intrusions provenant de réseaux externes, notamment Internet. Il agit comme une passerelle filtrante entre le réseau interne et l'extérieur, contrôlant et régulant les paquets de données échangés selon des règles de sécurité définies [27].

Un pare-feu peut prendre deux formes principales :

Logiciel : installé directement sur un ordinateur ou un serveur.

Équipement réseau dédié : placé entre le réseau local et Internet pour assurer le filtrage et la protection.

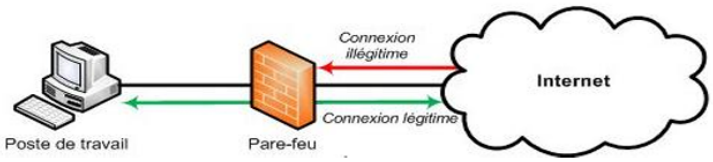

FIGURE II.9 – Firewalls [27]

II.12.1.2 Les fonctions d'un firewall

Un firewall applique un ensemble de règles prédéfinies pour contrôler le trafic réseau, telles que [27] :

Autoriser ou bloquer une connexion (allow/deny).

Rejeter une demande de connexion sans notifier l'émetteur (drop).

Autoriser ou interdire l'accès à un service spécifique.

Imposer l'utilisation d'un protocole particulier.

Autoriser ou bloquer certaines adresses IP source ou destination.

Vérifier et inspecter la conformité du trafic aux règles établies.

Ces règles servent à appliquer un filtrage du trafic conformément à la politique de sécurité établie par l'organisation.

II.12.2 Les avantages et limites des firewalls dans les réseaux

II.12.2.1 Avantages

Les firewalls offrent plusieurs avantages pour la sécurité et la gestion du réseau [54] :

Renforcement de la sécurité : Le firewall agit comme une première barrière contre les intrusions, les attaques malveillantes et les accès non autorisés.

Contrôle du trafic réseau : il permet de filtrer le trafic entrant et sortant selon des règles prédéfinies, assurant ainsi une meilleure maitrise des communications.

Réduction des risques : en bloquant les ports et services inutiles, le pare-feu limite les surfaces d'attaque potentielles.

Surveillance du réseau : Certains firewalls intègrent des fonctions de journalisation (logs) et d'alertes, utiles pour l'analyse des incidents.

II.12.2.2 Limites

Cependant, les firewalls présentent aussi certaines limites qu'il convient de connaître [55] :

Protection limitée : Un firewall ne protège pas contre toutes les menaces, notamment celles qui proviennent de l'intérieur du réseau ou via des fichiers malveillants.

Complexité de configuration : Une mauvaise configuration peut compromettre la sécurité ou bloquer des services essentiels.

Maintenance continue : Les règles doivent être régulièrement mises à jour pour rester efficaces face à l'évolution des menaces.

Impact sur les performances : Le filtrage intensif peut ralentir le trafic réseau si le matériel n'est pas dimensionné correctement.

II.12.3 DMZ

Une zone démilitarisée (ou DMZ, pour DeMilitarized Zone) est une partie du réseau isolée qui n'appartient ni au réseau interne privé ni à Internet.

Elle est utilisée lorsqu'un ou plusieurs serveurs internes par exemple des serveurs web, de messagerie ou FTP doivent être accessibles depuis l'extérieur. La DMZ permet de rendre ces ressources disponibles à la fois pour le réseau interne et pour des utilisateurs externes, tout en limitant les risques pour la sécurité globale de l'entreprise. Elle offre un niveau de sécurité intermédiaire, centralisant les services exposés sans compromettre le réseau interne [8].

II.12.3.1 Architecture de la DMZ

La politique de sécurité appliquée à une DMZ suit généralement les principes suivants :

Source	Destination	Règle
Réseau externe	DMZ	Autorisé
Réseau externe	Réseau interne	Interdit
Réseau interne	DMZ	Autorisé
Réseau interne	Réseau externe	Interdit
DMZ	Réseau interne	Interdit
DMZ	Réseau externe	Refusé

TABLEAU II.2 – Politiques de trafic entre le réseau interne, externe et la DMZ [27].

Ces règles visent à isoler la DMZ tout en permettant l'accès contrôlé aux services qu'elle héberge, assurant ainsi une séparation sécurisée entre les réseaux interne et externe [27].

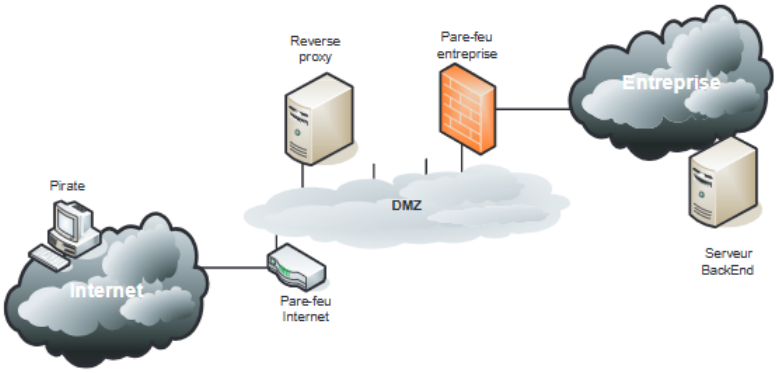

FIGURE II.10 – Zone DMZ [27]

II.12.4 Avantages et limites de l'utilisation d'une DMZ dans un réseau :

II.12.4.1 Avantages

La DMZ présente plusieurs avantages pour renforcer la sécurité et organiser les services réseau [56] :

Sécurité renforcée : La DMZ permet de séparer les services accessibles depuis l'extérieur (comme les serveurs Web ou FTP) du réseau interne, réduisant ainsi les risques en cas de compromissions.

Protection du réseau interne : Même si un attaquant réussit à accéder à un service dans la DMZ, il reste isolé du réseau interne, limitant l'étendue de l'attaque.

Contrôle du trafic : Le trafic entre l'extérieur, la DMZ et le réseau interne peut être strictement contrôlé à l'aide de règles de pare-feu.

Centralisation des services publics : Elle permet de regrouper dans une même zone les services destinés à être exposés au public, facilitant leurs gestion et surveillance.

II.12.4.2 Limites

Malgré ses avantages, la DMZ présente également certaines limites [56] :

Complexité de configuration : La mise en place d'une DMZ nécessite une bonne maîtrise des règles de sécurité, des VLANs et des pare-feux, ce qui peut être complexe.

Coût d'infrastructure : Elle peut nécessiter du matériel supplémentaire (firewalls, switches, serveurs dédiés), augmentant le coût global du réseau.

Pas une solution complète : La DMZ ne protège pas contre tous les types d'attaques, notamment celles venant de l'intérieur ou les attaques applicatives ciblant les services dans la DMZ.

II.12.5 Proxy

Un serveur proxy est une machine intermédiaire située entre les ordinateurs d'un réseau local et Internet. Il agit pour le compte des applications clientes en exécutant leurs requêtes sur Internet.

Lorsqu'un utilisateur utilise une application configurée pour passer par un proxy, l'application envoie d'abord sa requête au serveur proxy. Celui-ci relaie la requête vers le serveur cible sur Internet, récupère la réponse, puis la transmet à l'application cliente. Ce mécanisme permet de masquer l'adresse réelle de l'utilisateur, de contrôler et filtrer le trafic, et parfois de mettre en cache les réponses pour améliorer les performances [21].

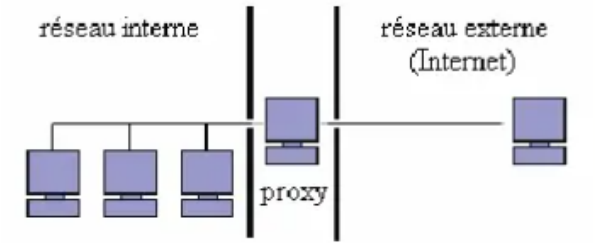

FIGURE II.11 – Proxy [21]

II.12.6 Avantages et limites de l'utilisation d'un proxy dans un réseau

II.12.6.1 Avantages

On peut citer plusieurs avantages liés au proxy, notamment [21]

Filtrage des contenus : Le proxy permet de contrôler les sites web accessibles par les utilisateurs. Cela bloque les contenus inappropriés.

Amélioration des performances : En stockant temporairement des pages web fréquemment consultées, le proxy réduit le temps de chargement et la consommation de bande passante.

Anonymat et confidentialité : Il masque l'adresse IP réelle de l'utilisateur.

Sécurité réseau renforcée : Le proxy peut détecter et bloquer certains types de menaces (les sites malveillants).

II.12.6.2 Limites

Malgré ses avantages, il y a quand-même certains inconvénients [21] :

Complexité de configuration : Mettre en place un proxy efficace demande une configuration correcte, notamment au niveau des règles de filtrage, mise en cache, et de la sécurité.

Risque de points de défaillance : Si le proxy tombe en passe, l'accès à Internet peut être bloqué pour tous les utilisateurs dépendants de ce service.

Ne protège pas contre toutes les menaces : Le proxy n'assure pas une protection complète contre les attaques sophistiquées comme les malwares intégrés dans des fichiers ou les attaques chiffrées.

II.12.7 Les réseaux privés virtuels (VPN)

Les réseaux internes d'entreprise sont traditionnellement limités à l'organisation. Toutefois, avec l'essor des échanges à distance, il devient nécessaire de connecter ces réseaux à Internet pour communiquer avec des filiales, des clients ou du personnel éloigné.

Un VPN (Virtual Private Network) permet de relier de manière sécurisée des réseaux internes via Internet, en encapsulant les données dans un tunnel chiffré. Ce tunneling garantit la confidentialité et l'intégrité des informations, même sur des infrastructures publiques.

On parle de ń réseau virtuel ż car il connecte deux réseaux physiques par un support externe comme Internet, et de ń privé ż car seuls les utilisateurs autorisés peuvent accéder aux données échangées. Le VPN offre ainsi un moyen sûr de partager des ressources à distance [20].

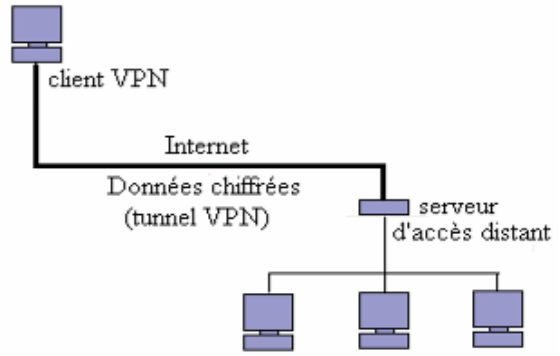

FIGURE II.12 – VPN [21]

II.12.7.1 Types de VPN

VPN d'accès

Le VPN d'accès à distance est le plus couramment utilisé. Il permet aux utilisateurs de se connecter à un réseau privé via un serveur sécurisé. Les données sont transmises à travers un tunnel virtuel, assurant une connexion sécurisée entre l'appareil de l'utilisateur et le réseau privé.

VPN site à site

Ce type de VPN est généralement employé par les grandes entreprises pour relier plusieurs succursales. Il permet aux utilisateurs situés dans différents sites d'accéder aux ressources partagées comme s'ils faisaient partie d'un même réseau local.

VPN Intranet Le VPN intranet sert à connecter plusieurs intranets d'une même entreprise, notamment lorsqu'elle possède plusieurs sites à distance. L'objectif principal est de garantir la sécurité et l'intégrité des données échangées entre les différents sites.

VPN Extranet

Dans une entreprise, un extranet VPN sert à créer un lien sécurisé avec les clients et les partenaires, pour qu'ils puissent accéder à certaines informations sans mettre en danger le réseau interne [29].

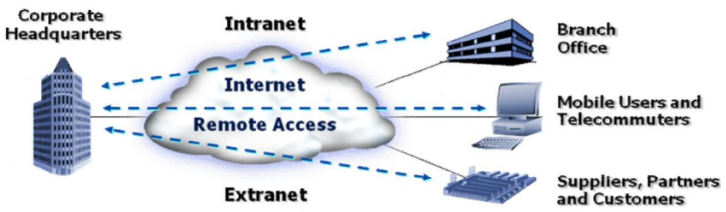

FIGURE II.13 – Fonctionnement du VPN [29]

II.12.7.2 Avantages d'utilisation d'un VPN

Le VPN comporte plusieurs avantages lors de son utilisation :

Confidentialité des communications : Le VPN chiffre les données entre l'utilisateur et le réseau.

Accès distant sécurisé : Il permet aux utilisateurs d'accéder aux ressources internes de l'entreprise ou de l'établissement n'importe où, de manière sécurisée.

Protection sur les réseaux publics : Sur des connexions Wi-Fi publiques (cafés, hôtels), le VPN protège contre les attaques de type ń man-in-the-middle ż [29].

II.12.7.3 Limites d'utilisation d'un VPN

La mise en place d'un VPN engendre un certain coût initial et des frais de maintenance réguliers. De plus, il peut provoquer un ralentissement de la connexion, ce qui impacte l'expérience des utilisateurs. Il existe également un risque qu'il soit détecté et bloqué, limitant ainsi son efficacité sur le long terme [29].

II.12.7.4 Les protocoles de tunnelisation

Les principaux protocoles de tunnelisation utilisés pour établir des VPN sont :

Protocole	Couche	Fonctionnalité	Entreprise(s) à l'origine
PPTP	2	Établissement de tunnels point-à-point pour VPN	Microsoft, 3Com, Ascend, US Robotics, ECI Telematics
L2F	2	Tunnelisation de niveau 2 pour VPN (quasi-obsolète)	Cisco, Northern Telecom, Shiva
L2TP	2	Combine les fonctionnalités de PPTP et L2F pour compatibilité et sécurité	Microsoft, Cisco
IPSec	3	Transport sécurisé de données chiffrées sur les réseaux IP	IETF (standardisé, utilisé par plusieurs entreprises)

TABLEAU II.3 – Principaux protocoles de tunnelisation pour VPN [27].

II.12.8 Antivirus

Un antivirus est un logiciel conçu pour détecter, neutraliser et supprimer les programmes malveillants (malwares). Il analyse les fichiers entrants, qu'ils proviennent de téléchargements ou de courriels, ainsi que la mémoire vive de l'ordinateur et les périphériques de stockage tels que les disques durs internes et externes, les clés USB et les cartes mémoire flash [20].

La détection des logiciels nuisibles repose principalement sur trois méthodes :

Analyse par signatures : identification d'un code déjà connu et enregistré dans une base de données.

Analyse comportementale : surveillance du comportement d'un logiciel pour repérer des actions suspectes.

Détection : reconnaissance de motifs ou de codes caractéristiques de virus.

II.12.9 ACL(Access Control List)

Les listes de contrôle d'accès (ACL) sont des ensembles de règles définissant quelles connexions ou quels types de trafic réseau sont autorisés ou refusés. Elles permettent de réguler le trafic entrant et sortant d'un réseau en fonction de critères précis [20].

On distingue deux types d'ACL :

ACL standard : filtrent le trafic uniquement selon l'adresse IP source et destination des paquets.

ACL étendues : offrent un filtrage plus précis en prenant en compte plusieurs paramètres, tels que le type de protocole, l'adresse IP source et destination, les ports TCP ou UDP source et destination, ainsi que des informations optionnelles sur le protocole. Cela permet un contrôle beaucoup plus fin du trafic réseau.

II.12.10 Les protocoles de sécurité

II.12.10.1 Protocole IPSec

IPSec (Internet Protocole Security) est un protocole de niveau 3 qui assure la sécurité des communications IP sur un réseau. Il est largement utilisé pour créer des réseaux privés virtuels (VPN) et sécuriser les accès distants à un internet. IPSec garantit des services essentiels tels que la confidentialité, l'authentification et l'intégrité des données, en s'appuyant sur des mécanismes cryptographiques qui offre un niveau de sécurité élevé [20].

IPSec propose deux protocoles pour différents niveaux de protection :

Authentication Header (AH) : assure uniquement l'authentification, l'intégrité des données et la protection contre la relecture de paquets (anti-replay), une technique où un intrus renvoie des paquets capturés pour tromper le système.

Encapsulating Security Payload (ESP) : offre les mêmes services que ń AH ż tout en ajoutant la confidentialité grâce au chiffrement des données.

II.12.10.2 Protocole SSL

Le protocole SSL (Secure Sockets Layer) est utilisé pour sécuriser les échanges sur Internet. Il chiffre les communications entre deux machines afin de garantir la confidentialité des données, l'authentification des utilisateurs et serveurs et l'intégrité des informations transmises [20].

Les étapes d'authentifications du serveur avec SSL sont :

1. Le navigateur du client initie une demande de connexion sécurisée auprès du serveur.
2. En réponse, le serveur transmet son certificat numérique au client.
3. Ce certificat est accompagné d'une liste des algorithmes cryptographiques que le serveur prend en charge pour établir une communication sécurisée.
4. Le client analyse cette liste est choisi l'algorithme qu'il souhaite utiliser.
5. Le serveur confirme ce choix en renvoyant à nouveau son certificat avec les informations cryptographiques nécessaires.
6. Le navigateur du client vérifie alors la validité du certificat, notamment s'il est signé par une autorité de certification reconnu.
7. Si cette vérification est réussie, le client génère une clé secrète de session, qu'il chiffre à l'aide de la clé publique du serveur.

II.12.10.3 Protocole HTTPs

HTTPS est une version sécurisée du protocole HTTP, utilisée pour protéger les échanges lors de la navigation web. Il fournit des mécanismes de chiffrement et d'authentification, garantissant un niveau de sécurité élevé dans les communications entre les sites web et les navigateurs. HTTPS combine :

Cryptographie asymétrique pour l'authentification des parties (serveur et parfois client).

Cryptographie symétrique pour le chiffrement des communications.

Contrairement à SSL qui fonctionne au niveau de la couche transport, HTTPS sécurise les échanges au niveau des messages HTTP, en appliquant des certificats pour protéger individuellement les documents et contenus HTML. Ainsi, SSL sécurise la connexion réseau, tandis que HTTPS garantit des échanges HTTP sécurisés [20].

II.12.10.4 SSH (Secure Shell)

Le protocole SSH se sert du chiffrement pour sécuriser la connexion entre un client et un serveur. Pour se défendre contre les attaques réseau, l'authentification de l'utilisateur, les commandes, les sorties et les transferts de fichiers sont chiffrés. On l'utilise souvent pour le contrôle à distance de serveurs, l'administration d'infrastructures et le transfert de fichiers [30].

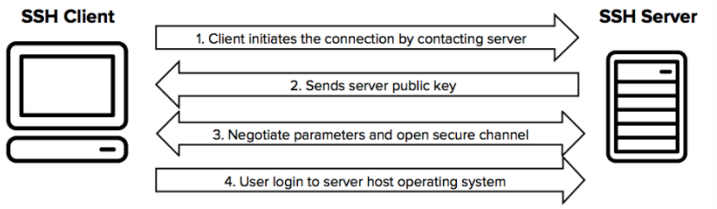

FIGURE II.14 – Protocole SSH

II.13 Conclusion

La sécurité des réseaux représente un enjeu stratégique majeur dans tout environnement informatique, en raison de l'augmentation constante des menaces et de la complexité des attaques. Ce chapitre a permis de poser les fondements théoriques de la sécurité informatique en abordant les principes essentiels qui constituent le socle sur lequel reposent les politiques de sécurité efficaces.

L'analyse des concepts fondamentaux tels que la vulnérabilité, le risque, la menace ou encore les contre-mesures a permis de mieux cerner les différentes dimensions de la sécurité des réseaux.

Chapitre III
Etude de l'architecture réseau

III.1 Introduction

Ce chapitre est consacré à l'étude de l'architecture réseau mise en place dans le cadre de ce projet. L'architecture réseau représente la structure logique et physique du réseau, c'est la manière dont les différents équipements et technologies sont organisés pour permettre la communication, la sécurité, et l'efficacité des échanges de données.

L'objectif de ce chapitre est de présenter les différentes zones qui compose cette architecture (WAN, Campus, Agence), ainsi que les rôles qu'elles jouent au sein du réseau global. Nous verrons également les protocoles utilisés, les dispositifs de sécurité déployés.

Cette étude permettra de mieux comprendre l'organisation du réseau et de justifier les choix techniques réalisés en matière de conception et de sécurisation.

III.2 Les zones fonctionnelles d'un réseau d'entreprises

Les zones fonctionnelles d'un réseau d'entreprise représentent des parties logiques ou physiques du réseau structurées en fonction de leur rôle et leur niveau de sécurité. On retrouve généralement les zones suivantes dans la majorité des architectures d'entreprises :

III.2.1 Zone WAN

La zone WAN est le point d'interconnexion du réseau d'entreprise avec l'extérieur y compris Internet et les sites distants. Elle représente toutes les connexions qui relie les différents sites géographiques de l'organisation (siège, agences, data centers, filiales, etc.), souvent répartis à l'échelle régionale, nationale ou internationale. Le WAN est souvent géré en collaboration avec un fournisseur de services, avec des politiques de redondance, de qualité de service (QoS) et de sécurité (chiffrement, filtrage) [31].

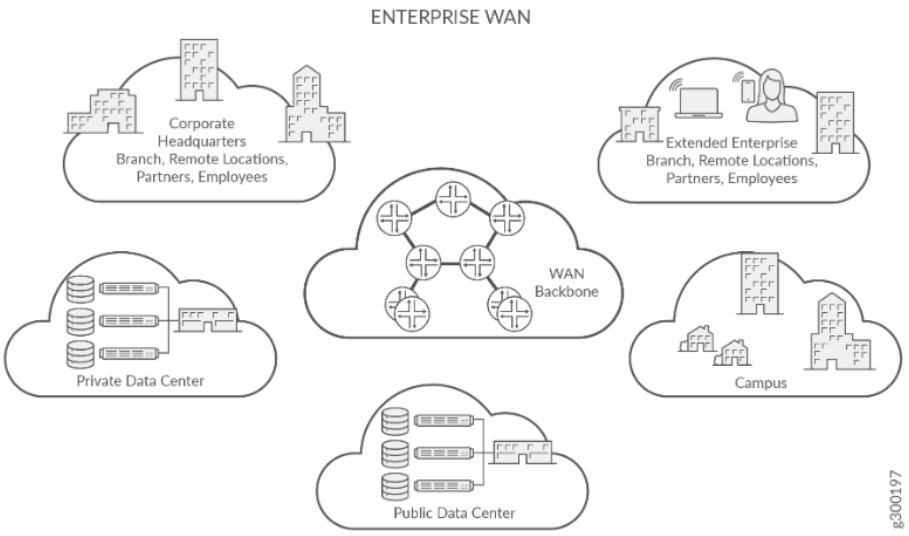

FIGURE III.1 – WAN d'entreprise [32]

III.2.1.1 Définition d'ISP

Un ISP (Internet Service Provider) est une entreprise ou un organisme qui fournit un accès à Internet aux particuliers, entreprises ou organisations. L'ISP met à disposition des connexions Internet via différentes technologies comme la fibre optique, le câble, le DSL, ou encore le satellite. L'ISP est le lien technique entre l'utilisateur final et le réseau Internet mondial. Il possède les infrastructures nécessaires (lignes télécom, serveurs, points de présence) pour assurer la connectivité et la gestion du trafic Internet pour ses clients [33].

III.2.2 Zone Campus

On considère généralement le campus d'entreprise comme la partie de l'infrastructure informatique qui fournit un accès aux services et ressources de communication aux utilisateurs finaux et les appareils répartis sur un même site géographique.

Le cur du campus assure l'interconnexion entre l'accès au campus, le Data Center et les parties WAN du réseau.

Le réseau de campus intègre des services essentiels tels que le transport et la gestion des données, la haute disponibilité, la sécurité, ainsi que l'administration globale du réseau. Ces éléments offrent à l'entreprise la possibilité d'assurer un accès fiable et continu aux applications, de sécuriser ses échanges, d'assurer la mobilité des utilisateurs, de virtualiser certains services, et de gérer efficacement l'ensemble du système [34].

Le réseau campus est généralement structuré en trois couches essentielles : la couche Core (Noyau), la couche distribution et la couche Accès.

III.2.2.1 Modèle hiérarchique du Réseau campus

Un élément clé pour le succès de l'implémentation de toute conception de réseau de campus est de suivre de bonnes structures de conception. Un système structuré se base sur deux principes complémentaires : la hiérarchie et la modularité

La division d'une tâche ou d'un système en éléments offre plusieurs avantages immédiats. Chaque composant ou module peut être conçu de manière autonome par rapport à la conception globale et tous les modules peuvent être utilisés en tant qu'éléments semi-indépendants, offrant ainsi une plus grande disponibilité globale du système, ainsi qu'une gestion et un management plus simples.

En commençant par les bases, un modèle hiérarchique à trois niveaux est défini par un modèle incluant les couches Core, Distribution et Access, comme le montre la figure [34].

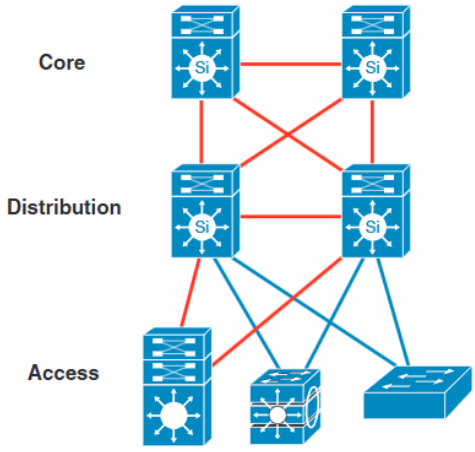

FIGURE III.2 – Les couches de la hiérarchie a trois niveaux. [34]

Couche Access

La couche Access représente le niveau initial du modèle hiérarchique campus. C'est l'endroit où les équipements finaux tels que les ordinateurs, les imprimantes, les caméras, etc. se raccordent à la partie câblée du réseau de campus à travers un switch appelé ń switch Access ż qui fournit la majorité des services tel que la connectivité aux périphériques finaux, la Haute Disponibilité, la Convergence ainsi que la sécurité [34].

Couche distribution

La couche de distribution du réseau représente le point de transition entre la couche Access et core. Cette couche constitue l'endroit où la manipulation de paquets peut avoir lieu et permet d'établir une frontière ou des limites.

Elle constitue un point d'agrégation pour tous les commutateurs d'accès et fait partie intégrante du bloc de distribution d'accès en offrant des services de connectivité et de gestion pour les flux de trafic au sein du bloc de distribution d'accès [34].

Couche Core

La couche Core constitue le cur du réseau du campus, souvent appelée ń backbone ż, qui relie tous les éléments de l'architecture. Elle assure la connectivité entre les appareils finaux, les services informatiques et de stockage situés dans le Data Center, ainsi que les autres zones et services du réseau. Fonctionnant comme un agrégateur, elle connecte le campus à l'ensemble du réseau. La couche Core offre un nombre limité de services mais est conçue pour être hautement disponible et opérationnelle en permanence, avec pour objectif principal d'assurer une redondance optimale et une récupération quasi immédiate du flux de données en cas de défaillance d'un composant [34].

III.2.2.2 Architecture 2-tier

Dans notre conception, nous avons retenu une architecture 2-tier, parfois désignée sous le terme collapsed core. Ce modèle repose sur deux niveaux principaux : la couche d'accès, qui regroupe les utilisateurs, les serveurs et les différents périphériques réseau, et la couche cur/distribution, dédiée au transit rapide et fiable des données entre les zones fonctionnelles.

Contrairement à l'architecture 3-tier, où les couches cur et distribution sont séparées, le modèle 2-tier fusionne ces deux fonctions dans un même niveau [35].

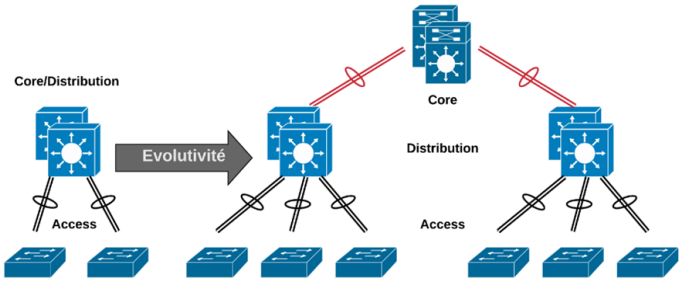

FIGURE III.3 – Comparaison entre la hiérarchie à deux et trois niveaux [47].

III.2.3 Zone DMZ

La DMZ (Demilitarized Zone), ou zone démilitarisée, est une zone tampon située entre le réseau interne sécurisé d'un (LAN) et le réseau externe non sécurisé. Elle est conçue pour héberger les services accessibles depuis l'exterieur, tout en protégeant les ressources internes de l'entreprise.

La DMZ est déployée entre deux pare-feux et permet d'exposer certains services (tels que des serveurs web, FTP, DNS ou messagerie) aux utilisateurs externes, sans donner un accès direct au réseau interne. En cas de compromission, la DMZ isole l'attaque et empêche la propagation vers les systèmes critiques [56].

III.2.4 Datacenter

Un datacenter est une infrastructure physique qui regroupe des équipements informatiques critiques d'une organisation tels que serveurs, systèmes de stockage et dispositifs Wi-fi ..etc, Il est conçu pour garantir une haute disponibilité, une sécurité physique et logique renforcée ainsi qu'une capacité de traitement et de stockage évolutive [53].

III.2.5 Les serveurs

Il s'agit d'un dispositif à la fois matériel et logiciel qui offre des services à un ou plusieurs clients simultanément. Il existe plusieurs types de serveurs, chacun d'entre eux remplie un objectif et une tâche précise [36].

III.2.5.1 Serveur DHCP

Un serveur DHCP (Dynamic Host Configuration Protocol) est chargé d'attribuer automatiquement des adresses IP et d'autres paramètres réseau (masque de sous-réseau, passerelle par défaut, DNS) aux clients qui en font la demande. Cette automatisation réduit les erreurs de configuration et facilite l'administration réseau [36].

III.2.5.2 Serveur Mail

Le serveur de messagerie gère l'envoi, la réception et le stockage des courriers électroniques via des protocoles tels que SMTP.

Il peut également intégrer des services de filtrage anti-spam et antivirus pour sécuriser les communications [36].

III.2.5.3 Serveur Radius

Un serveur RADIUS (Remote Authentication Dial-In User Service) est utilisé pour centraliser l'authentification, l'autorisation et la facturation des utilisateurs qui se connectent à un réseau, notamment dans les environnements Wi-Fi d'entreprise. Il fonctionne sur la base d'échanges sécurisés entre le client, le serveur d'accès et le serveur d'authentification [36].

III.2.5.4 Serveur Web

Un serveur web au sein d'une configuration réseau représente un serveur applicatif dont l'objectif principal est de stocker, gérer et redistribuer des ressources HTTP/HTTPS (pages HTML, images, scripts, etc.) aux utilisateurs finaux (navigateurs, API consommateurs) [36].

III.2.5.5 Serveur DNS

Un serveur DNS, ou Domain Name System se traduit en système de nom de domaine. Il s'agit d'un service informatique qui convertit les noms de domaines des sites web en adresse IP numérique pouvant être traitée facilement, facilitant ainsi un enregistrement pratique et efficace. Il est élaboré pour être utilisé sur Internet et Intranet [37].

III.2.5.6 Serveur FTP

Le serveur FTP (File Transfert Protocol) est une forme de communication basée sur un protocole standard. Il s'agit d'un serveur qui facilite le transfert de fichiers entre deux ordinateurs, ou plus précisément entre un serveur et un client. Le serveur FTP reçoit des requêtes provenant d'un client. C'est surtout pour avoir accès à une base de données spécifique. Si le client est autorisé à le faire, la requête sera approuvée ; sinon, elle sera refusée.

Un serveur FTP offre la possibilité de protéger les informations d'une personne ou d'une société. Il restreint l'accès aux personnes disposant d'autorisations [37].

III.3 Les protocoles et technologie réseaux

III.3.1 VLAN

III.3.1.1 Définition

Un réseau local virtuel (VLAN, Virtual Local Area Network) est un domaine de diffusion logique au sein d'un réseau local physique existant. Cette technologie permet de segmenter un réseau en plusieurs sous-réseaux logiques indépendants, facilitant l'organisation des appareils selon des critères tels que la fonction, le département ou le niveau de sécurité [9] [59].

Les VLANs fonctionnent selon deux modes principaux :

Mode access : le port est associé à un seul VLAN et ne transmet que le trafic non étiqueté. Ce mode est utilisé pour connecter des dispositifs finaux comme des ordinateurs ou des imprimantes.

Mode trunk : le port transporte simultanément le trafic de plusieurs VLANs en utilisant des étiquettes VLAN, généralement via le protocole IEEE 802.1Q.

III.3.1.2 Le Trunk

Le trunk est une connexion physique unique qui permet de transporter simultanément le trafic de plusieurs VLANs entre des équipements réseau, tels que des commutateurs ou des routeurs. Les trames circulant sur le trunk sont étiquetées avec un identifiant de VLAN (VLAN ID), ce qui garantit qu'elles restent associées à leur VLAN d'origine ou à leur domaine de diffusion. Cette configuration est cruciale pour préserver la segmentation logique du réseau tout en optimisant l'utilisation des infrastructures physiques [58].

III.3.1.3 Création des VLANs

Les VLANs peuvent être créés de différentes manières [59] :

VLAN basé sur le port : les ports du commutateur sont associés à des VLAN avec des numéros d'identification uniques, l'adresse MAC du port est liée au VLAN assigné, ce qui permet une configuration simple mais a pour inconvénient que le VLAN est lié aux ports et non aux terminaux, nécessitant une reconfiguration si un terminal est déplacé d'un port à un autre. Cette méthode est couramment utilisée dans les réseaux d'entreprise où les postes de travail sont fixes.

VLAN basé sur l'adresse MAC : Ici, l'appartenance à un VLAN est déterminée par l'adresse MAC de l'appareil, indépendamment du port physique utilisé. Le commutateur maintient une table associant les adresses MAC aux VLANs correspondants. Cette méthode améliore la sécurité et la flexibilité du réseau, même si les utilisateurs changent d'emplacement physique, une approche qui est adaptée aux environnements où la mobilité est fréquente, comme les bureaux partagés ou les espaces de coworking.

VLAN basé sur le protocole : Les VLANs sont attribués en fonction des types de protocole et des formats d'encapsulation des trames. Cette méthode est utile pour les réseaux comportant plusieurs protocoles.

VLAN basé sur le sous-réseau IP : Dans cette configuration, les VLANs sont définis en fonction des sous-réseaux IP. Le commutateur attribue les trames entrantes à un VLAN en se basant sur l'adresse IP source. Cette technologie est efficace pour des réseaux publics avec une demande de mobilité et de gestion simplifiée.

III.3.1.4 VTP (VLAN Trunking Protocol)

VTP est un protocole développé par CISCO pour la gestion et la configuration des VLANs. Il permet la configuration d'un VLAN depuis un unique commutateur, par la suite tout changement dans la configuration sera propagé et partagé avec tous les autres commutateurs du domaine du VTP, évitant ainsi de devoir configurer manuellement chaque commutateur [59].

III.3.1.5 Routage inter-VLAN

Le routage inter-VLAN est une technique permettant la communication entre différents VLANs au sein d'un réseau. Par défaut, les VLANs segmentent un réseau pour isoler le trafic, mais cela empêche les appareils situés sur des VLANs distincts de communiquer directement. Le routage inter-VLAN résout ce problème en permettant le transfert de données entre ces derniers. Le routage inter-VLAN utilise un dispositif de couche 3, comme un routeur ou un commutateur de couche 3, pour transférer les données entre ces VLANs. Cela se fait en configurant des interfaces virtuelles ou des sous-interfaces, chacune associée à un VLAN spécifique, permettant ainsi le transfert de paquets entre les VLANs tout en maintenant leur isolation logique [9].

III.3.1.6 Avantages des VLANs

Les VLANs offrent plusieurs avantages [59] :

Réduction du trafic de diffusion : les messages de diffusion, comme les requêtes ARP, restent limités à l'intérieur d'un VLAN, ce qui permet de restreindre les diffusions d'un serveur uniquement aux clients concernés.

Création de groupes de travail indépendants de l'infrastructure physique : les postes peuvent être déplacés sans nécessiter de reconfiguration du réseau virtuel.

Renforcement de la sécurité : le contrôle des communications entre VLANs via des routeurs permet de filtrer et de restreindre le trafic inter-VLAN.

Indépendance vis-à-vis de l'infrastructure physique : un switch peut gérer plusieurs VLANs, et un même VLAN peut s'étendre sur plusieurs commutateurs, offrant une flexibilité et une scalabilité accrues.

III.3.2 STP

Le Spanning Tree Protocol (STP) est un protocole utilisé dans les réseaux locaux (LAN) pour éviter les boucles de broadcast. Une boucle se produit lorsqu'un paquet de données tourne en cercle entre les équipements du réseau, ce qui peut provoquer des erreurs de transmission et surcharge la bande passante.

STP crée un arbre de transmission qui connecte tous les équipements du réseau, en garantissant qu'il n'y a pas de boucles. Chaque équipement échange des informations STP pour déterminer le chemin optimal pour envoyer les paquets. Si une boucle est détectée, STP bloque les interfaces concernées pour l'arrêter [27] [59].

III.3.3 DHCP

Le DHCP (Dynamic Host Configuration Protocol) est un protocole réseau essentiel qui permet d'attribuer automatiquement des adresses IP aux machines lorsqu'elles se connectent à un réseau. Grâce à ce mécanisme, chaque appareil reçoit non seulement une adresse IP unique, mais aussi d'autres informations réseau importantes telles que le masque de sous-réseau, la passerelle par défaut et les serveurs DNS. Cela simplifie grandement la gestion des réseaux, notamment dans les environnements comportant un grand nombre d'hôtes, en évitant les conflits d'adresses IP et en réduisant les erreurs liées à une configuration manuelle.

Le DHCP permet également de gérer efficacement les adresses IP disponibles, en les allouant pour une durée limitée (bail), ce qui optimise l'utilisation des ressources réseau et facilite la mobilité des appareils [8].

III.3.4 Etherchannel (LACP)

La technologie EtherChannel, initialement développée par Cisco, permet d'agréger plusieurs liens physiques Ethernet identiques pour former un seul lien logique entre deux équipements réseau, tels que des commutateurs, des routeurs ou des serveurs. Cette agrégation de liens offre plusieurs avantages tel que l'augmentation de la bande passante disponible, la répartition du trafic sur plusieurs connexions, et amélioration de la tolérance aux pannes, puisque la défaillance d'un lien physique n'interrompt pas la communication.

EtherChannel prend également en charge le protocole LACP (Link Aggregation Control Protocol), qui permet de négocier automatiquement l'agrégation des liens entre les appareils compatibles et de gérer dynamiquement l'ajout ou la suppression de liens dans le groupe. Cette technologie constitue ainsi une solution efficace pour optimiser les performances réseau et renforcer sa fiabilité [38].

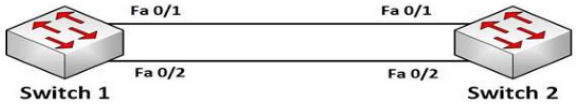

FIGURE III.4 – Schéma illustre l'interconnexion de deux switches avec Etherchannel [16]

III.3.5 Protocole HSRP

HSRP (Hot Standby Router Protocol) est un protocole de redondance de passerelle, développé par Cisco, qui assure la continuité du service réseau en cas de défaillance d'un routeur. Le principe repose sur l'utilisation d'une adresse IP virtuelle partagée entre plusieurs routeurs d'un même réseau local. Parmi ces routeurs, un est élu Active et prend en charge le trafic en tant que passerelle par défaut, en répondant aux requêtes ARP des hôtes. Un second routeur est placé en Standby, prêt à prendre le relais immédiatement si le routeur actif tombe en panne, tandis que tous les autres restent en état Listen, surveillant simplement l'activité du groupe HSRP. Grâce à cette architecture, HSRP garantit une redondance, minimisant les interruptions de service pour les utilisateurs du réseau.

III.3.6 Protocole de routage

Le routage consiste à déterminer le chemin optimal pour atteindre la destination en se basant sur son adresse IP. Lorsqu'un paquet est envoyé par un hôte et que sa destination ne se trouve pas dans le réseau ou sous-réseau local, il doit être transmis à un routeur. Ce routeur agit comme un intermédiaire, acheminant le paquet vers un autre routeur ou réseau qui rapproche progressivement le paquet de sa destination finale.

Les protocoles de routage définissent les règles et algorithmes utilisés par les routeurs pour décider du meilleur chemin à suivre. Ils peuvent être statique (routes définies manuellement) ou dynamique (routes ajustées automatiquement en fonction de l'état du réseau), garantissant ainsi une communication efficace et fiable entre différents réseaux [8].

III.3.6.1 Routage statique

Le routage statique est une méthode de configuration manuelle des routes dans une table de routage. Il permet de déterminer avec précision le chemin qu'un paquet doit emprunter pour atteindre sa destination.

Ce type de routage est principalement utilisé dans les réseaux de petite taille ou pour des chemins bien définis et stables. Bien que limité en flexibilité et en tolérance aux pannes, le routage statique présente des avantages en termes de simplicité, de performance et de sécurité [39].

III.3.6.2 Routage dynamique

Le routage dynamique est un mécanisme de gestion des routes dans un réseau informatique, Ce type de routage est particulièrement adapté aux réseaux en constante évolution, car il s'ajuste automatiquement aux modifications de topologie telles que les pannes, l'ajout ou suppression d'équipements.

Grâce à sa capacité d'adaptation, le routage dynamique permet une convergence rapide et optimise le cheminement des données en tenant compte des critères tels que la charge du réseau,

la fiabilité des liens, ou la bande passante disponible. Ce mécanisme convient aussi bien aux réseaux locaux (LAN) qu'aux réseaux étandue (WAN).

Parmi les protocoles de routage dynamique les plus utilisés, On trouve le RIP (Routing Information Protocol), OSPF (Open Shortest Path First), EIGRP (Enhanced Interior Gateway Routing Protocol) et BGP (Border Gateway Protocol). Ce type de routage est particulièrement adapté aux réseaux de grande taille ou à des topologies qui changent [39].

III.3.7 Différents type de routage dynamique

III.3.7.1 RIP

Le Routing Information Protocol (RIP) est un protocole de routage dynamique de type vecteur de distance. Il permet aux routeurs d'échanger périodiquement des informations de routage en fonction du nombre de sauts nécessaire pour atteindre un réseau donné. RIP présente plusieurs limitations, une portée restreinte (15 sauts maximum). Il reste adapté aux réseaux de petite taille ou aux environnements pédagogiques [40].

III.3.7.2 OSPF

Le protocole OSPF (Open Shortest Path First) est un protocole de routage dynamique à état de lien, largement utilisé pour les réseaux IP de taille moyenne à grande. Il permet une organisation logique du réseau en zones (areas), ce qui limite la propagation des mises à jour et évite une surcharge excessive sur l'ensemble du réseau. Chaque zone peut agréger les routes et restreindre la diffusion des informations de sous-réseaux uniquement aux zones concernées, améliorant ainsi l'efficacité du routage et la scalabilité.

OSPF supporte également l'authentification des informations de routage, offrant une sécurité supplémentaire grâce à l'utilisation de mots de passe pour valider les mises à jour entre routeurs [41].

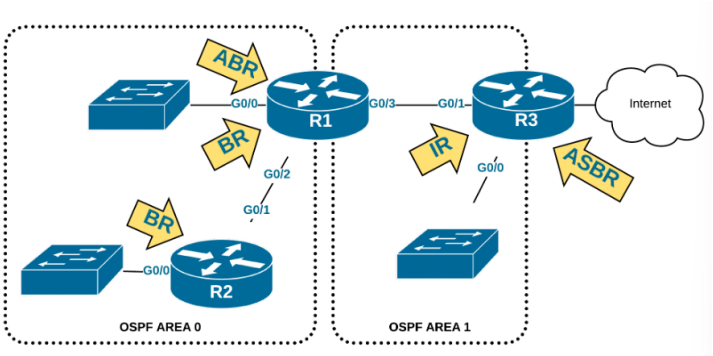

FIGURE III.5 – Protocole OSPF Multi-area [42].

III.3.7.3 EIGRP

EIGRP est un protocole de routage évolué à vecteur de distance développé par Cisco. Il utilise l'algorithme DUAL (Diffusing Update Algorithm) pour déterminer le chemin le plus

court vers une destination dans un réseau.

Bien qu'il soit un protocole à vecteur de distance, EIGRP intègre également certaines fonctionnalités des protocoles à état de lien, comme la détection rapide des changements de topologie et l'optimisation des routes. Ce qui signifie que le protocole ajuste rapidement ses tables de routage lorsqu'un lien tombe ou qu'un chemin plus optimal est disponible. Cette combinaison permet au protocole d'être flexible et adapté à de nombreuses topologies et supports réseaux différents. De plus, il minimise le trafic réseau en ne diffusant que les mises à jour nécessaires, ce qui améliore l'efficacité globale du réseau [43].

III.3.7.4 BGP

Le Border Gateway Protocol (BGP) est une norme de l'IETF (Internet Engineering Task Force) et le plus évolutif de tous les protocoles de routage.

Il est le protocole de routage de l'Internet mondial, ainsi que des réseaux privés des fournisseurs de services. BGP a étendu son objectif initial de transport d'informations d'accessibilité à internet et peut désormais transporter des routes pour la multidiffusion, l'IPV6, les VPNs et diverses autres données [39].

III.3.8 Network Address translation (NAT)

Le Network Address translation (NAT) est une technique utilisée dans les réseaux informatiques pour traduire les adresses IP d'un réseau privé en adresses IP publiques, et inversement. Cette conversion est généralement effectuée par un routeur ou un pare-feu placé à la frontière entre le réseau internet et Internet. Dans le contexte de notre architecture, le NAT est mis en uvre sur les pare-feux Cisco ASA situés entre la zone WAN et les zones internes (Campus, DMZ, Datacenter). Il permet :

La mutualisation des adresses IP publiques : plusieurs hôtes internes peuvent partager une même adresse IP publique pour communiquer avec Internet.

La protection de la structure internet : les adresses IP privées ne sont pas directement visibles depuis l'extérieur, réduisant ainsi la surface d'attaque [44].

III.3.9 L'authentification

L'authentification sur un réseau d'entreprise consiste à confirmer les identités grâce à l'utilisation d'un mot de passe pour gérer l'accès aux ressources du réseau. En d'autres termes, le système garantit que seuls les utilisateurs, équipements ou services autorisés et disposant des permissions appropriées ont la possibilité de se connecter et de partager des informations sur le réseau [57].

III.4 Conclusion

Dans ce chapitre, nous avons détailler les différentes zones fonctionnelles de notre architecture réseau (WAN, Campus, DMZ, DataCenter) ainsi que les serveurs et services essentiels qui la composent. Nous avons également passé en revue les principaux protocoles et technologies mis en uvre, tels que VLAN, STP, DHCP, EtherChannel, HSRP, ainsi que les mécanismes de routage et de traduction d'adresses.

Cette conception, pensée pour assurer à la fois la performance, évolutivité et sécurité, permet de garantir la continuité des services tout en réduisant les risques liés aux pannes ou aux intrusions. Les choix technologiques opérés visent à offrir une infrastructure robuste, et de résister aux menaces potentielles.

Chapitre IV
Simulation de l'architecture réseau

IV.1 Introduction

Dans ce chapitre, nous abordons la phase de simulation de l'architecture réseau proposée dans le cadre de ce mémoire, en utilisant l'outil de simulation Cisco Packet Tracer. L'objectif est de représenter un réseau structuré autour de trois zones principales : une zone WAN configurée avec le protocole de routage dynamique OSPF, une zone Agence, symbolisant un site distant avec ses propres équipements et sous-réseau ; et enfin une zone Campus, plus étendue et segmentée grâce à l'implémentation de VLANs.

Ce chapitre va d'abord détailler l'outil de simulation, puis présenter la topologie retenue, le choix des équipements, et les configurations appliquées, ainsi que les tests menés afin de vérifier la connectivité, le bon fonctionnement du routage, l'accessibilité entre les différentes zones.

IV.2 Présentation de l'outil de simulation

IV.2.1 Aperçu de Cisco Packet Tracer

Cisco Packet Tracer est un logiciel de simulation réseau développé par Cisco Systems conçu pour l'enseignement et l'apprentissage des concepts liés aux réseaux informatiques. Il permet de concevoir des topologies réseau, de simuler le fonctionnement de réseaux modernes, et d'explorer de manière interactive divers protocoles et technologies. Cet outil, largement intégré dans les programmes de formation de la Cisco Networking Academy, offre un environnement interactif permettant de créer, configurer et tester des architectures réseau sans nécessiter d'équipements physiques [45].

IV.2.1.1 Installation de Packet Tracer

Pour télécharger Cisco Packet Tracer, il est nécessaire de se rendre sur le site officiel de la Cisco Networking Academy à l'adresse suivante : https://www.netacad.com. Une fois connecté avec ses identifiants de la plateforme, il suffit de cliquer sur l'icône dédiée à packet Tracer, puis de sélectionner le fichier d'installation correspondant au système d'exploitation utilisé (Windows, MacOS ou linux) [45].

Windows : Le programme d'installation est fourni sous la forme d'un fichier exécutable, généralement nommé Packettracer_Setup6.0.1.exe, Il suffit d'ouvrir ce fichier pour lancer l'assistant d'installation, d'accepter les conditions de la licence, de choisir le répertoire d'installation souhaité, puis de démarrer le processus.

IV.2.1.2 Les différentes zones de l'environnement Cisco Packet Tracer

L'interface de Cisco Packet Tracer se compose de plusieurs zones, chacune jouant un rôle précis dans la création et la gestion des réseaux. Les différentes sections sont numérotées dans la figure suivante et expliquées ensuite [45].

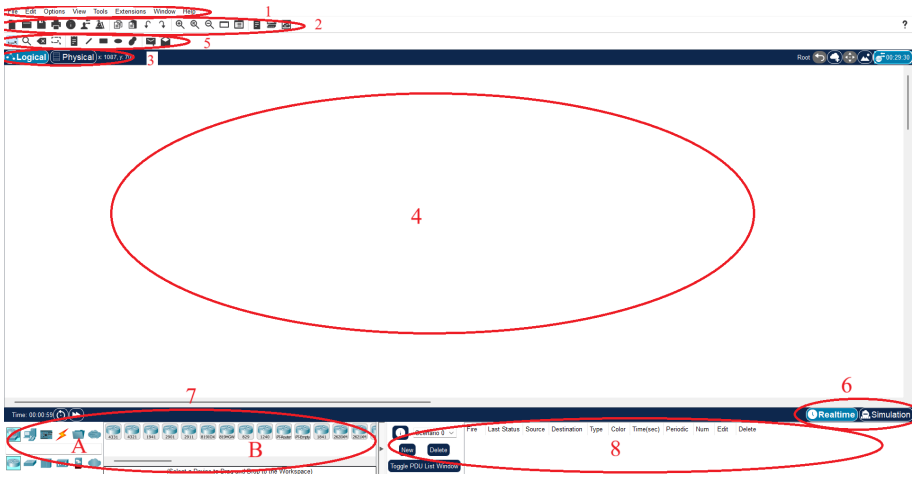

FIGURE IV.1 – Aperçu des différentes zones de l'interface de simulation Cisco Packet Tracer

Area 1 : Barre de menu

Il s'agit de la barre classique que l'on retrouve dans la plupart des applications. Elle permet d'effectuer des actions comme ouvrir, enregistrer, imprimer ou modifier les préférences du logiciel.

Area 2 : Barre d'outils principale

Cette barre contient des icônes de raccourci vers les fonctions fréquemment utilisées, telles que l'ouverture ou l'enregistrement de projets, le zoom, l'annulation/répétition des actions, ainsi qu'un bouton pour saisir des informations sur le réseau en cours.

Area 3 : Onglets espace logique / physique

Ces onglets permettent de basculer entre deux vues différentes : l'espace logique (où l'on conçoit la topologie réseau) et l'espace physique (qui représente la disposition physique des équipements).

Area 4 : Espace de travail

C'est la zone centrale de l'interface, dédiée à la création des topologies réseau et à l'exécution des simulations.

Area 5 : Barre d'outils commune

Elle regroupe des outils utiles pour manipuler la topologie : sélection, déplacement, ajout de notes, suppression d'éléments, inspection, redimensionnement de formes, injecter des paquets.

Area 6 : Onglets Temps réel / Simulation

Ces onglets permettent de basculer entre deux modes : le mode Temps réel et simulation. Aussi des boutons permettent également de capturer, d'avancer ou de ralentir la progression du trafic.

Area 7 : Boîte des composants réseau

Cet espace regroupe tous les équipements disponibles dans Packet Tracer, qu'ils soient terminaux, commutateurs, routeurs. etc. Il est divisé en deux :

Area 7A : Sélection des types d'appareils

Elle permet de choisir une catégorie d'équipements (routeurs, commutateurs, concentrateurs, les bornes sans fil, les connexions, les PC, les réseaux étendus, des appareils divers, Les connexions multi-usagers.)

Area 7B : Sélection spécifique des appareils

Une fois une catégorie sélectionnée, cette zone affiche les modèles d'équipements correspondants disponible à l'ajout dans la topologie

Area 8 : Boîte des paquets personnalisés

Permet de créer des paquets personnalisés pour tester le comportement de la topologie. Les résultats sont affichés sous forme de liste.

IV.3 Présentation de la topologie réalisée sur Cisco Packet Tracer

La conception du réseau constitue la base du projet, car elle permet de définir clairement la topologie, les zones et les interconnexions. Cela garantit une segmentation efficace pour limiter les accès non autorisés.

La topologie ci-dessous représente l'architecture globale mise en place dans notre infrastructure réseau. Elle est structurée autour de plusieurs zones logiques (Campus, EDGE, DMZ, Datacenter, WAN), chacune remplissant un rôle précis dans l'organisation et la gestion du trafic.

Campus : regroupe les utilisateurs finaux ainsi que les départements de l'entreprise, c'est la zone d'accès qui relies les ordinateurs, les imprimantes et le réseau Wi-Fi

EDGE : c'est la zone de control entre le réseau interne et externe. Elle intègre les deux firewalls chargés de filtrer et d'inspecter le trafic.

WAN : c'est la partie WAN chargé de filtrer et d'inspecter le trafic.

Datacenter : Héberge les serveurs critiques de l'entreprise garantissant la disponibilité des services leurs performances.

DMZ : zone intermédiaire hébergeant les serveurs qui peuvent être atteints depuis l'extérieur (Web, FTP, Mail). Elle autorise la mise en ligne de services tout en les isolant du réseau interne pour limiter les risques en cas de compromission.

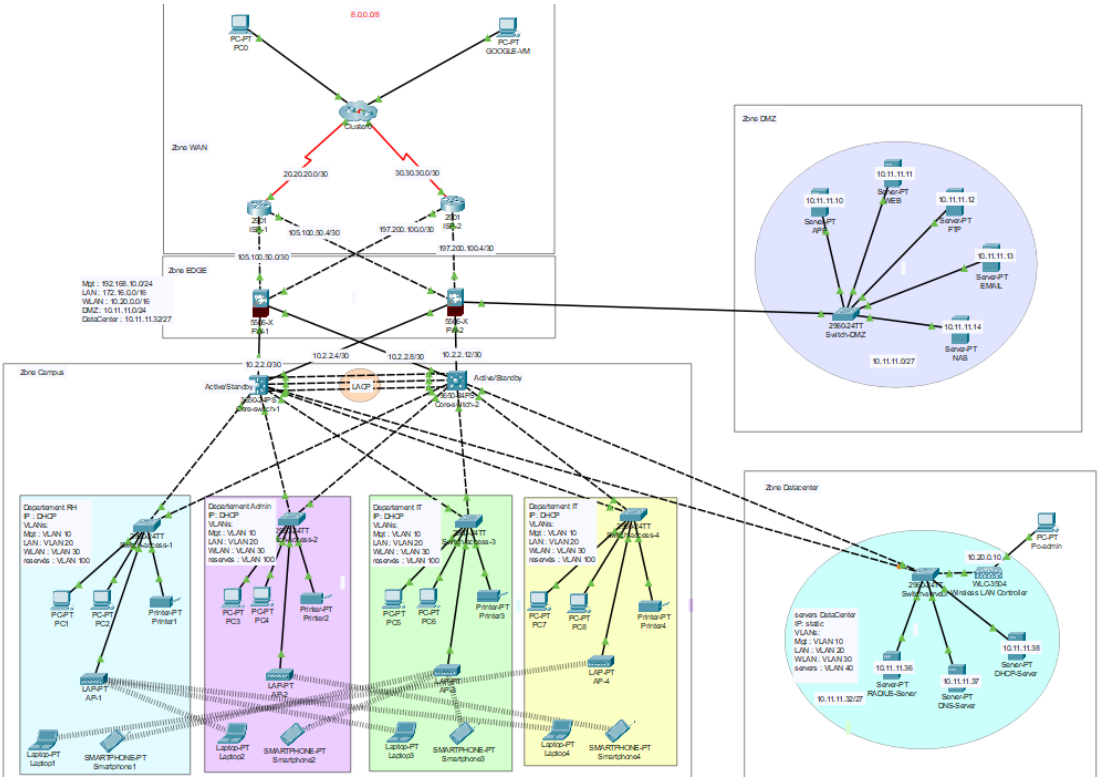

FIGURE IV.2 – Topologie générale simulée

IV.3.1 Matériel simulé

Le matériel et composants utilisés lors de cette simulation sont présentés dans ce tableau ci-dessous :

Matériel	Modèle	Quantité	Fonction principale
Routeurs	Cisco 2911	3	Connexion WAN / routage principal
Pare-feu	Cisco ASA 5506-X	2	Sécurisation des flux, segmentation DMZ
Switch cur	Core-switch 3650-24PS	2	Agrégation, routage inter-VLAN
Switch access	2960-24TT	4	Connexion des PC, imprimantes, AP Wi-Fi
Switch DMZ	2960-24TT	1	Connexion des serveurs DMZ
Contrôleur WLC	WLC-2504	1	Gestion des AP légers et réseau Wi-Fi
Points d'accès légers	LAP-PT	4	Connexion sans fil des terminaux mobiles
Imprimantes réseau	Printer-PT	4	Impression partagée dans les salles
Postes clients	PC-PT	10	Stations bureautiques fixes
Laptops	Laptop-PT	4	Postes mobiles connectés en Wi-Fi
Smartphones	Smartphone-PT	4	Accès au réseau via Wi-Fi
Serveurs	Serveur-PT	6	Services DNS, Web, Mail, FTP
Câbles droits	-	-	Connexion des PC et serveurs aux switches
Câble série	-	-	Connexion au port console pour la configuration et la gestion des équipements réseau

TABLEAU IV.4 – Matériel réseau et leurs fonctions principales

IV.4 Configuration du réseau

IV.4.1 La table d'adressage

Catégories	Adresses réseau	Masque sous-réseau	Adresses IP utilisables par les hôtes	Passerelles	Adresses broadcast
Management	192.168.10.0	255.255.255.0 (/24)	192.168.10.1 à 192.168.10.254	192.168.10.1	192.168.10.255
WLAN	10.20.0.0	255.255.0.0 (/16)	10.20.0.1 à 10.20.255.254	10.20.0.1	10.20.255.254
LAN	172.16.0.0	255.255.0.0 (/16)	172.16.0.1 à 172.16.255.254	172.16.0.1	172.16.255.255
DMZ	10.11.11.0	255.255.255.0 (/24)	10.11.11.1 à 10.11.11.30	10.11.11.1	10.11.11.31
Datacenter	10.11.11.32	255.255.255.224 (/27)	10.11.11.33 à 10.11.11.62	10.11.11.33	10.11.11.63

TABLEAU IV.5 – Table d'adressage de la topologie simulée

IV.4.2 Les VLANs utilisés

Nom VLAN	ID VLAN	Adresse de sous-réseau	Description
VLAN-MGMT	10	192.168.10.0/24	VLAN pour Management des équipements
VLAN-LAN	20	172.16.0.0/16	VLAN utilisé pour la connexion des PC et équipements fixes
VLAN-WLAN	30	10.20.0.0/16	VLAN dédié au trafic Wi-Fi des utilisateurs
VLAN-Réservé	100	-	VLAN réservé au LAN interne, avec désactivation des interfaces non utilisées pour renforcer la sécurité
VLAN-Servers	40	10.11.11.32/27	VLAN dédié aux serveurs du datacenter

TABLEAU IV.6 – Configuration des VLANs de la topologie simulée

IV.4.3 Table d'adressage entre le Cloud, ISP, Firewall, Routers et multilayer switch

Interconnexions	Adresses IP	Masque sous-réseau
CLOUD Area	8.0.0.0	255.0.0.0 (/8)
ISP1-Internet	20.20.20.0	255.255.255.252 (/30)
ISP2-Internet	30.30.30.0	255.255.255.252 (/30)
ISP1-FWL1	105.100.50.0	255.255.255.252 (/30)
ISP1-FWL2	105.100.50.4	255.255.255.252 (/30)
ISP2-FWL1	205.200.100.0	255.255.255.252 (/30)
ISP2-FWL2	205.200.100.4	255.255.255.252 (/30)
FWL1 to MLSW1	10.2.2.0	255.255.255.252 (/30)
FWL1 to MLSW2	10.2.2.4	255.255.255.252 (/30)
FWL2 to MLSW1	10.2.2.8	255.255.255.252 (/30)
FWL2 to MLSW2	10.2.2.12	255.255.255.252 (/30)

TABLEAU IV.7 – Table des interconnexions et de leurs adresses IP

IV.4.4 Configuration de base

Dans cette partie, on configure les paramètres de base tel que les noms d'hôtes, les mots de passe, l'activation de SSH et l'utilisation d'ACL standard, pour assurer une administration sécurisée des équipements, en limitant l'accès aux postes autorisés (VLAN Management) tout en chiffrant les communications.

On effectue cette configuration sur tous les switches Multi-layer et Access de la topologie.

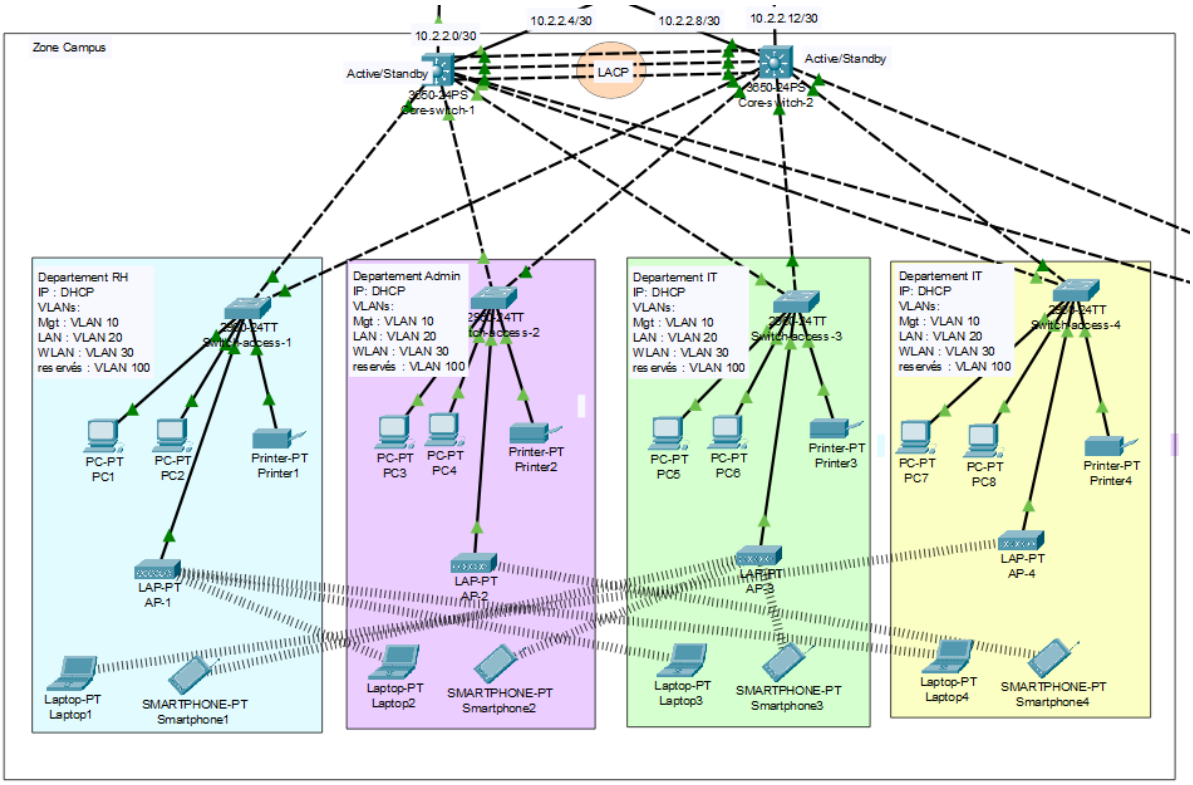

FIGURE IV.3 – Zone Campus

On va présenter la configuration en générale de tous les équipements avec un exemple configuré.

On prend l'exemple du premier Switch Access de l'architecture :

```
Switch> enable                                    (Passe en mode
   privilegie)
Switch# configure terminale                (Accede au mode de
   configuration globale)
! Configuration de la ligne console
Switch-access-1(config)#line console 0
Switch-access-1(config-line)# password cisco123 (Mot de passe d'
   acces via la console)
Switch-access-1(config-line)# login ( Active la demande de mot de
    passe)
Switch-access-1(config-line)# exec-timeout 3 0 ( Delai d'
   inactivite de 3
```

```
minutes)
Switch-access-1(config-line)# logging synchronous ( Evite les
   interruptions
lors de la saisie)
! Configuration de base de la securite
Switch-access-1(config)# enable password cisco123 (Mot de passe
   pour le mode
privilegie)
Switch-access-1(config)# banner motd "ACCCES NON AUTORISER" (
   Message
d'avertissement)
Switch-access-1(config)# no ip domain-lookup ( Desactive la
   recherche DNS
inutile)
Switch-access-1(config)# service password-encryption ( Chiffre
   les mots de passe
dans la configuration)
! Creation d'un utilisateur local pour SSH
Switch-access-1(config)# username cisco password cisco123
! Preparation pour SSH
Switch-access-1(config)# ip domain-name cisco.com ( Nom de
   domaine necessaire
a la generation de la cle)
Switch-access-1(config)# crypto key generate rsa general-keys
   modulus 1024
(Genere une cle RSA 1024 bits)
Switch-access-1(config)# ip ssh version 2 ( Force l'utilisation
   de SSH version
2)
! Configuration des lignes VTY (acces distant)
Switch-access-1(config)# line vty 0 15
Switch-access-1(config-line)# login local ( Authentification par
   compte
local)
Switch-access-1(config-line)# transport input ssh ( Autorise
   uniquement
SSH)
! Restriction d'acces par ACL
Switch-access-1(config)# access-list 1 permit 192.168.10.0
   0.0.0.255
(Autorise uniquement le reseau 192.168.10.0/24)
Switch-access-1(config)# access-list 1 deny any ( Refuse tout le
   reste)
```

```
Switch-access-1(config)# line vty 0 15
Switch-access-1(config-line)# access-class 1 in ( Applique l'ACL
   sur les
acces distants)
Switch-access-1(config)# do wr
```

IV.4.5 Création et affectation des VLANs ainsi que configuration des ports en mode accès et trunk sur les switchs access 1-2-3-4 et switch serveur

L'attribution des VLANs et la configuration des ports en mode accès ou truck segmentent logiquement le réseau prévenant ainsi la propagation d'attaques d'un vlan a un autre, tout en empêchant l'ajout de commutateurs non autorisés.

```
Switch-access-1 > enable ( Passe en mode privilegie)
Switch-access-1#Configure terminale (Accede au mode de
   configuration
globale)
! Configuration de l'interface
Switch-access-1(config)# interface range fa0/ - 2
Switch-access-1(config-if-range)#Switchport mode trunk (Configure
    les
interfaces en mode trunk)
Switch-access-1(config-if-range)#exit (Quitte la configuration
d'interface)

! Creation du vlan 10
Switch-access-1(config)#vlan 10
Switch-access-1(config-vlan)#name Mgt (VLAN pour la gestion)
Switch-access-1(config-vlan)#exit (Quitte la config VLAN)

! Creation du vlan 20
Switch-access-1(config)#vlan 20
Switch-access-1(config-vlan)#name LAN (VLAN pour le reseau local)
Switch-access-1(config-vlan)#exit
! Creation du vlan 30
Switch-access-1(config)#vlan 30
Switch-access-1(config-vlan)#name WLAN (VLAN pour le reseau sans
   fil)
Switch-access-1(config-vlan)#exit
! Creation du vlan 100
Switch-access-1(config)#vlan 100
Switch-access-1(config-vlan)#name Reserve (VLAN reserve)
```

```
Switch-access-1(config-vlan)#exit
! Configuration des interfaces
Switch-access-1(config)#interface range fa0/3 - 5 (Selectionne
   les
interface FastEthernet 0/3 a 0/5)
Switch-access-1(config-if-range)#switchport mode access (
   Configure les
ports en mode acces)
Switch-access-1(config-if-range)#switchport access vlan 20 (
   Associe ces
ports au VLAN 20)
Switch-access-1(config-if-range)#no shutdown (Active les
   interfaces)
Switch-access-1(config-if-range)#exit
Switch-access-1(config)#interface fa 0/6
Switch-access-1(config-if)#switchport mode access (Configure le
   port en mode
acces)
Switch-access-1(config-if)#switchport access vlan 30 (Associe le
   port au
VLAN 30)
Switch-access-1(config-if)#exit
Switch-access-1(config)#interface range fa0/7 - 24 , gi0/1 - 2
(Selectionne une plage d'interfaces FastEhernet et
   GigabitEthernet)
Switch-access-1(config-if-range)#switchport mode access (
   Configure les
ports en mode acces)
Switch-access-1(config-if-range)#switchport access vlan 100 (
   Associe ces
ports au VLAN 100)
```

Configuration du switch-core 1

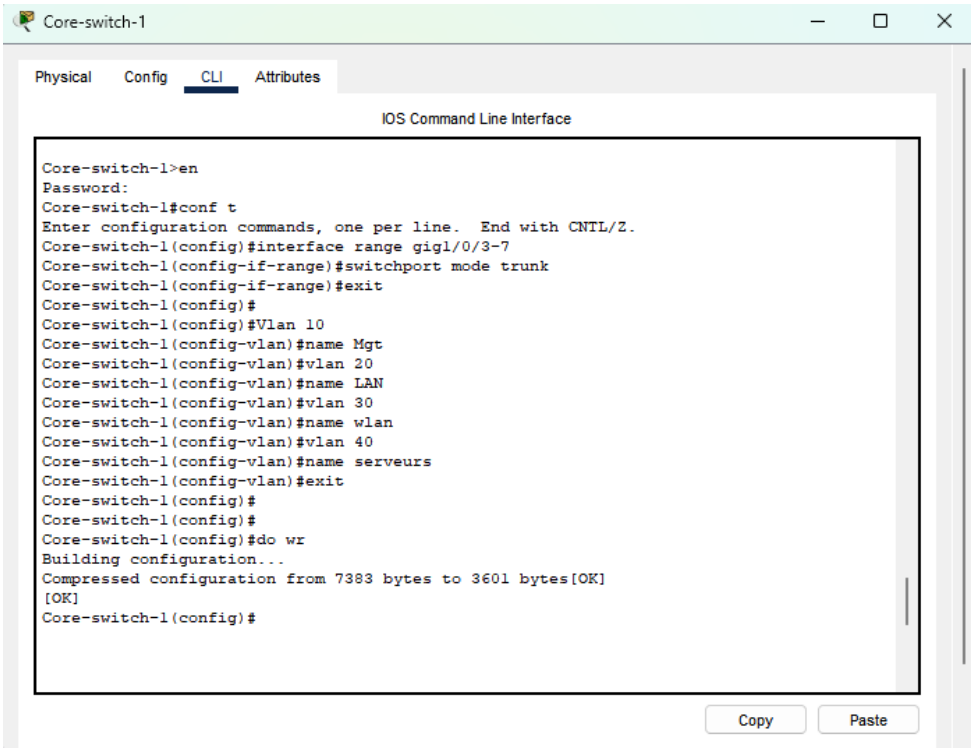

FIGURE IV.4 – Creation des Vlans sur Core-switch-1

Configuration du switch-core 2

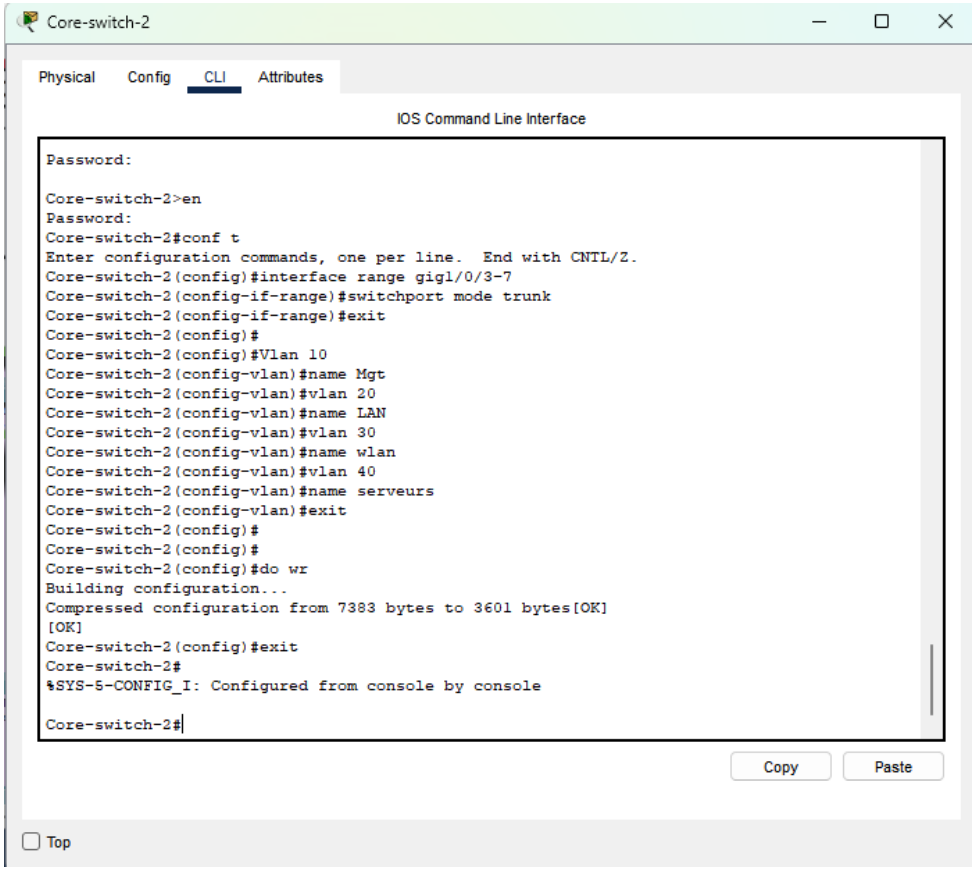

FIGURE IV.5 – Creation des Vlans sur core-switch 2

IV.4.6 Configuration de STP PortFast et BPDUguard sur tous les ports d'accès.

On active les Spanning Tree sur les interfaces en mode access, PostFast est une fonctionnalité de Spaning Tree Protocol qui permet à un port en mode accès (connecté à un PC, imprimante, etc.) de passer immédiatement à l'état de forwarding, en sautant les états d'écoute et d'apprentissage de STP. Son utilité est d'accélérer la connexion des hôtes, évite les délais à chaque redémarrage de port.

Ensuite on active le BPDUguard (Bridge Protocol Data Unit) qui sécurise le port contre la connexion d'un faux switch et sécurise la perturbation du réseau

```
Switch-access-1 > enable
Switch-access-1#Configure terminale
!Configuration de STP PortFast
Switch-access-1(config)#interface range fa0/3 - 24 (Selectionne
   les
interfaces FastEthernet de 3 a 24)
Switch-access-1(config-if-range)#spanning-tree portfast (Active
PortFast pour permettre un passage immediat en mode forwarding)
!Configuration de BPDUguard
Switch-access-1(config-if-range)#spanning-tree bpduguard enable (
   Active BPDU
Guard pour desactiver le port si un BPDU est recu < protection
   contre les boucles >)
Switch-access-1(config-if-range)#exit
Switch-access-1(config)#do wr
```

IV.4.7 Configuration de l'Etherchannel (LACP)

On passe ensuite à la configuration de l'EtherChannel qui augmente la bande passante et assure la redondance entre les liens, ce qui réduit le risque de coupure.

Configuration du LACP sur le core-switch 1 et 2 :

```
Core-switch-1>enable
Password : cisco123
Core-switch-1#configure terminal
Core-switch-1 (config)#interface range gig1/0/8 - 10 (Selectionne
    les
interfaces GigabitEthernet de 1/0/8 a 1/0/10)
!Configuration de l'Etherchannel (LACP)
Core-switch-1 (config-if-range)#channel-group 1 mode active (
   Ajout les
interfaces au groupe d'agregation num 1 < port-channel 1 > en
   mode active)
```

```
!Configuration du port-channel 1
Core-switch-1 (config-if-range)#interface port-channel 1
Core-switch-1 (config-if)#switchport mode trunk (configure le
port-channel en mode trunk)
Core-switch-1 (config-if)#exit
Core-switch-1 (config)#do wr
```

IV.4.8 Configuration des adresses IP et des sous-réseaux :

Configuration des adresses IP des interfaces L3 des switches multi-layer 1 et 2

```
Core-switch-1(config)#interface range gig1/0/1 - 2
!Active le routage IP sur le switch
Core-switch-1(config-if-range)#ip routing
!Configuration de l'interface GigabitEthernet 1/0/1
72
Core-switch-1(config)#interface gig1/0/1
Core-switch-1(config-if)#no switchport (Passe l'interface en mode
Layer 3)
Core-switch-1(config-if)#ip address 10.2.2.1 255.255.255.252 (
   Adresse
IP et masque)
Core-switch-1(config-if)#no shutdown (Active l'interface)
Core-switch-1(config-if)#exit
!Configuration de l'interface GigabitEthernet 1/0/2
Core-switch-1(config)#interface gig1/0/2
Core-switch-1(config-if)#no switchport
Core-switch-1(config-if)#ip address 10.2.2.5 255.255.255.252
Core-switch-1(config-if)#no shutdown
Core-switch-1(config-if)#exit
Core-switch-1(config)#do wr
```

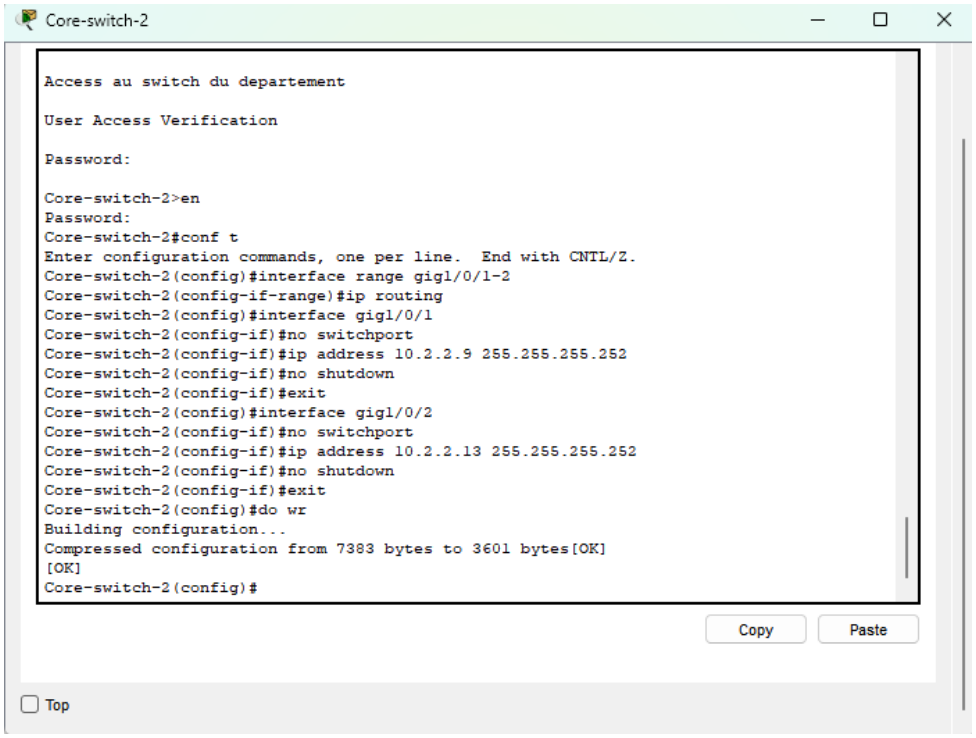

FIGURE IV.6 – Configuration des adresses IP sur Core-switch 2

Configuration des adresses IP des Routeurs (ISP)

ISP 1 :

```
!Configuration de l'interface GigabitEthernet 0/0
Router(config)#interface gig0/0
Router(config-if)#ip address 105.100.50.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
!Sauvegarde de la configuration
Router(config)#do wr
!Configuration de l'interface GigabitEthernet 0/1
Router(config)#interface gig0/1
Router(config-if)#ip address 105.100.50.5 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
!Configuration de l'interface Serial 0/0/0
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 20.20.20.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)# do wr
```

ISP 2 :

```
Router(config)#interface gig0/0
Router(config-if)#ip address 197.200.100.1 255.255.255.252
```

```
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface gig0/1
Router(config-if)#ip address 197.200.100.5 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial0/0/0
Router(config-if)#ip address 30.30.30.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#do wr
```

Internet :

```
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 20.20.20.2 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/0/1
Router(config-if)#ip address 30.30.30.2 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface gig0/0
Router(config-if)#ip address 8.0.0.1 255.0.0.0
Router(config-if)#no shutdown
75
Router(config-if)#exit
Router(config-if)#do wr
```

IV.4.9 Configuration du HSRP et du routage inter-VLAN sur les multi layer switch plus IP DHCP helper adresses

On veut distribuer le trafic entre les deux switch Core qui seront alors Active pour certains VLANs et Standby pour les autres

Le Switch Core 1 sera actif pour le Vlan 10 (MGT) et Vlan 20 (LAN) et passif pour le Vlan 30 et 40

Le switch Core 2 sera actif pour le Vlan 30 (WLAN) et Vlan 40 (Servers) et passif pour le Vlan 10 et 20

Pour cela on attribue l'adresse IP la plus élevée (hors l'adresse IP virtuel du vlan et la secondaire)

Configuration des vlan 10 et 20 pour lesquels le switch Core 1 sera le switch actif

```
!Configuration du VLAN 10
Core-switch-1(config)#interface vlan 10
Core-switch-1(config-if)#no shutdown (Active l'interface VLAN)
Core-switch-1(config-if)#ip address 192.168.10.3 255.255.255.0
(Ip de l'interface VLAN 10)
!Configuration HSRP
Core-switch-1(config-if)#standby 10 ip 192.168.10.1 (IP virtuelle
    HSRP pour
VLAN 10)

%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Standby -> Active

Core-switch-1(config-if)#ip helper-address 10.11.11.38 (Redirige
   les requetes
DHCP vers le serveur DHCP)
Core-switch-1(config-if)#exit
!Configuration du VLAN 20
Core-switch-1(config)#interface vlan 20
Core-switch-1(config-if)#no shutdown
Core-switch-1(config-if)#ip address 172.16.0.3 255.255.0.0

Core-switch-1(config-if)#standby 20 ip 172.16.0.1
Core-switch-1(config-if)#ip helper-address 10.11.11.38

%HSRP-6-STATECHANGE: Vlan20 Grp 20 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan20 Grp 20 state Standby -> Active
Core-switch-1(config-if)#exit
```

Configuration des vlan 30 et 40 pour lesquels le switch core 1 sera le switch passif

```
!Configuration du VLAN 30
Core-switch-1(config)#interface vlan 30
Core-switch-1(config-if)#no shutdown
core-switch-1(config-if)#ip address 10.20.0.2 255.255.0.0
!Configuration HSRP
core-switch-1(config-if)#standby 30 ip 10.20.0.1
ore-switch-1(config-if)#ip helper-address 10.11.11.38

%HSRP-6-STATECHANGE: Vlan30 Grp 20 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan30 Grp 20 state Standby -> Active
```

```
!Configuration du VLAN 30
Core-switch-1(config)#interface vlan 40
Core-switch-1(config-if)#no shutdown
ccore-switch-1(config-if)#ip address 10.11.11.34 255.255.255.224
core-switch-1(config-if)#standby 40 ip 10.11.11.33

%HSRP-6-STATECHANGE: Vlan40 Grp 40 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan40 Grp 40 state Standby -> Active
```

IP DHCP helper adresses : A quoi sert cette commande ?

Elle est utilisée pour relayer les requêtes de broadcast UDP, notamment DHCP Discover, d'un réseau local (VLAN) vers un serveur DHCP situé dans un autre réseau.

De la même manière on configure le switch core 2

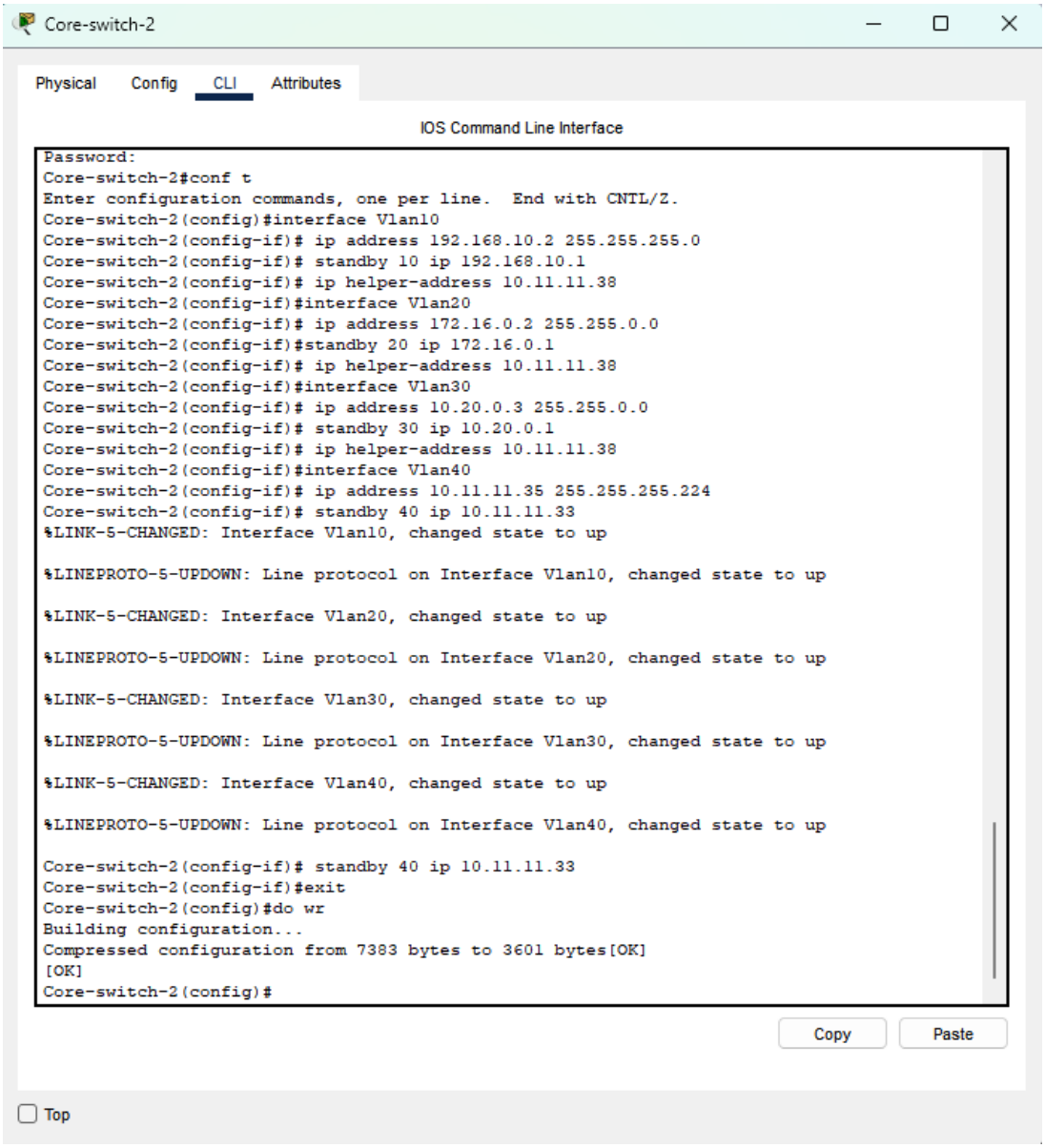

FIGURE IV.7 – Configuration HSRP et DHCP

Show standby brief

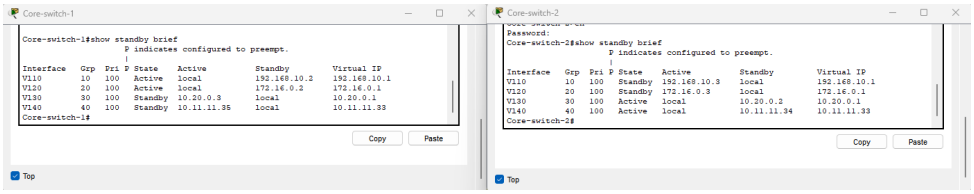

FIGURE IV.8 – Standby brief

IV.4.10 Attributions des adresses statiques au datacenter

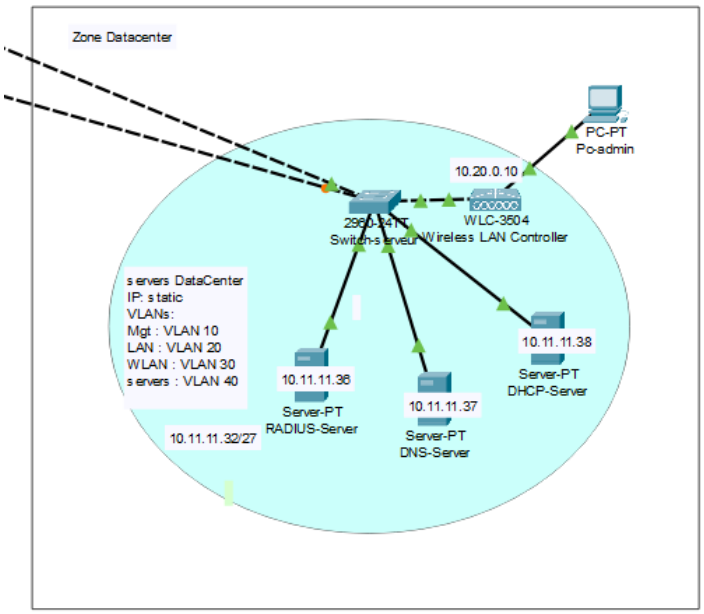

FIGURE IV.9 – Zone Datacenter

Radius Server :

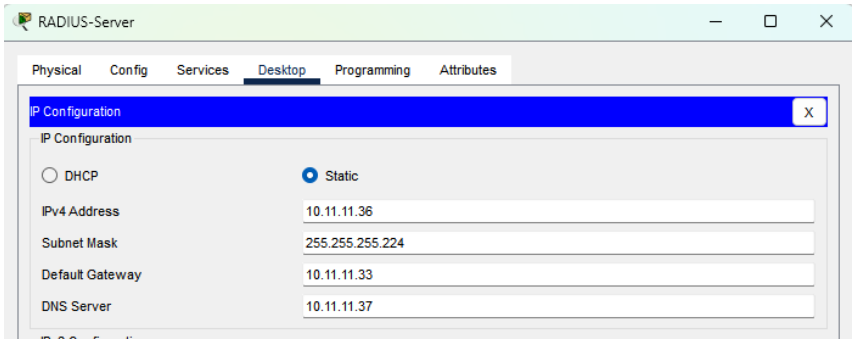

FIGURE IV.10 – Configuration du serveur Radius

DNS Server :

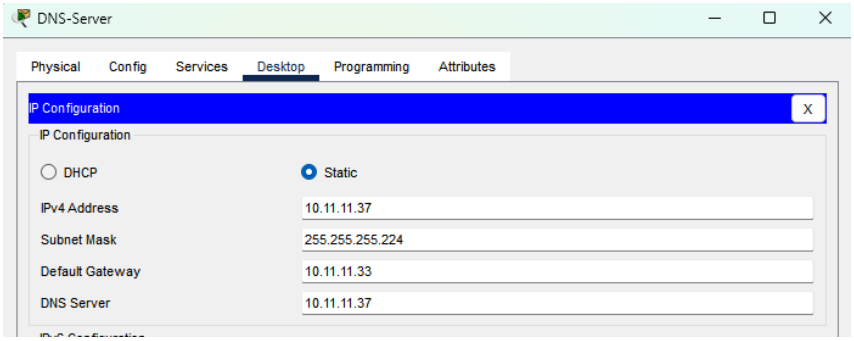

FIGURE IV.11 – Configuration du serveur DNS

DHCP Server :

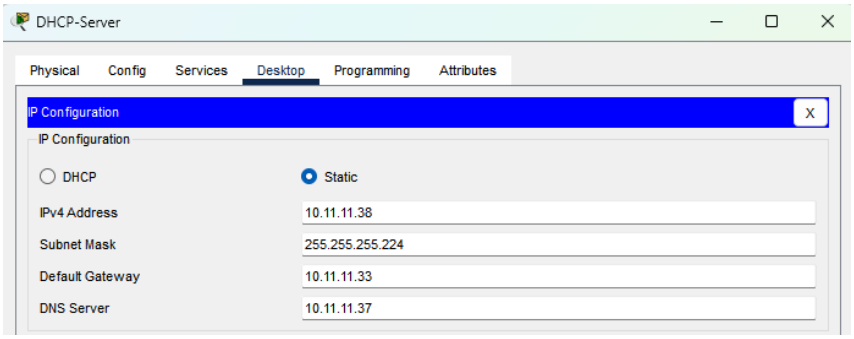

FIGURE IV.12 – Configuration du serveur DHCP

IV.4.11 Attribution des adresses IP Static a la DMZ

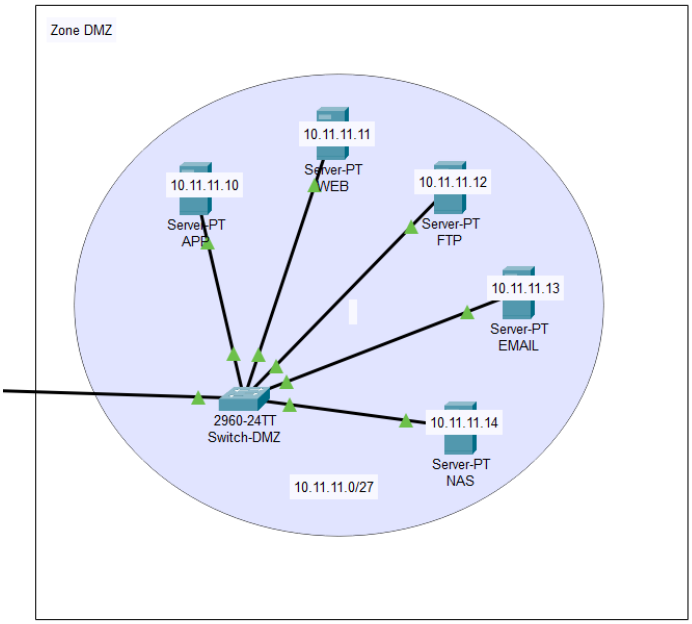

FIGURE IV.13 – Zone DMZ

Server WEB :

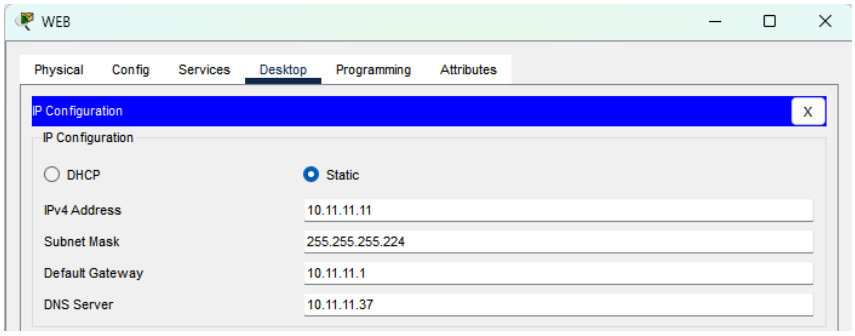

FIGURE IV.14 – Configuration du serveur WEB

Server FTP :

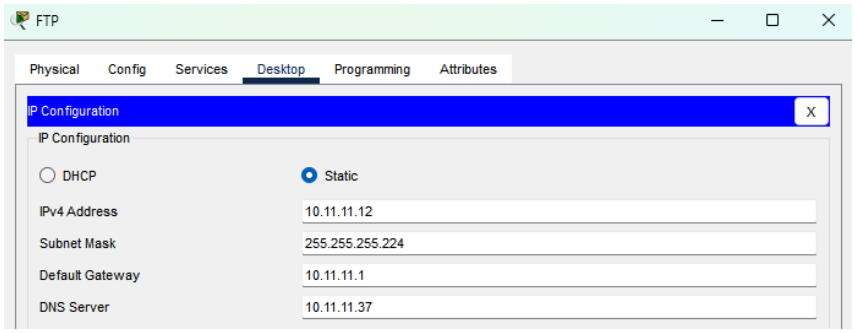

FIGURE IV.15 – Configuration du serveur FTP

Server EMAIL :

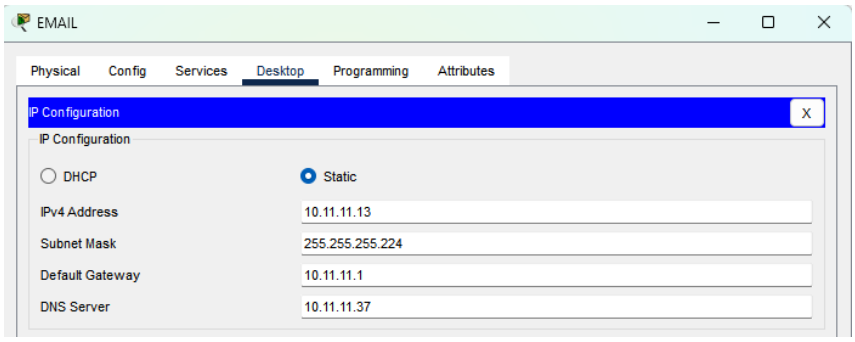

FIGURE IV.16 – Configuration du serveur EMAIL

Server NAS :

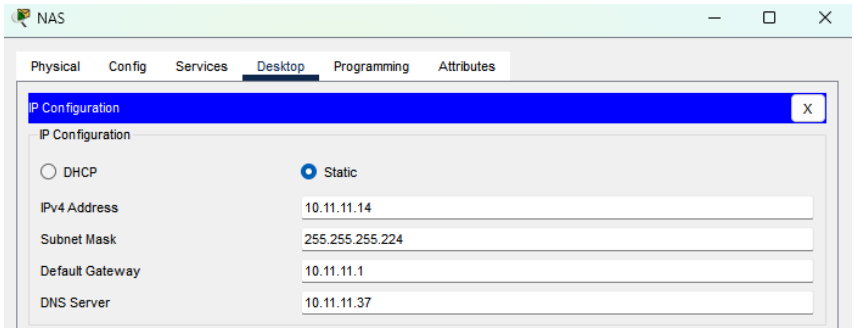

FIGURE IV.17 – Configuration du serveur NAS

IV.4.12 La configuration du serveur DHCP

Le serveur DHCP va nous permettre de distribuer automatiquement les paramètres réseau (Adresse IP, Masque sous réseau, passerelle par défaut et adresse du DNS server).

1. **Configuration DHCP du VLAN MGT :**

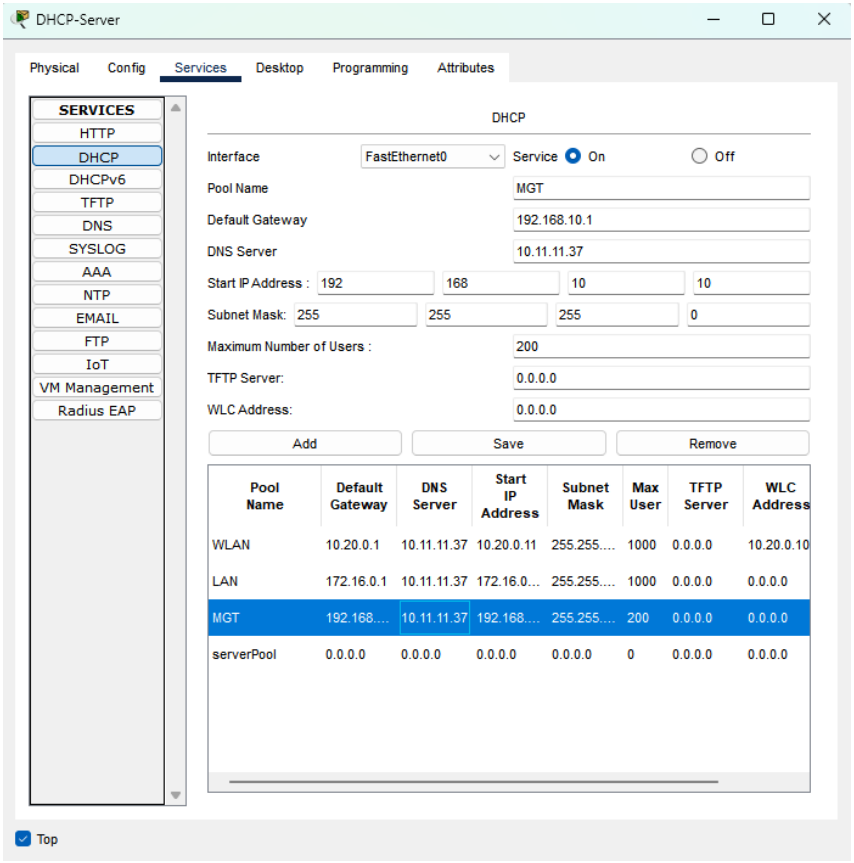

FIGURE IV.18 – Configuration DHCP du VLAN MGT

2. **Configuration DHCP du VLAN LAN :**

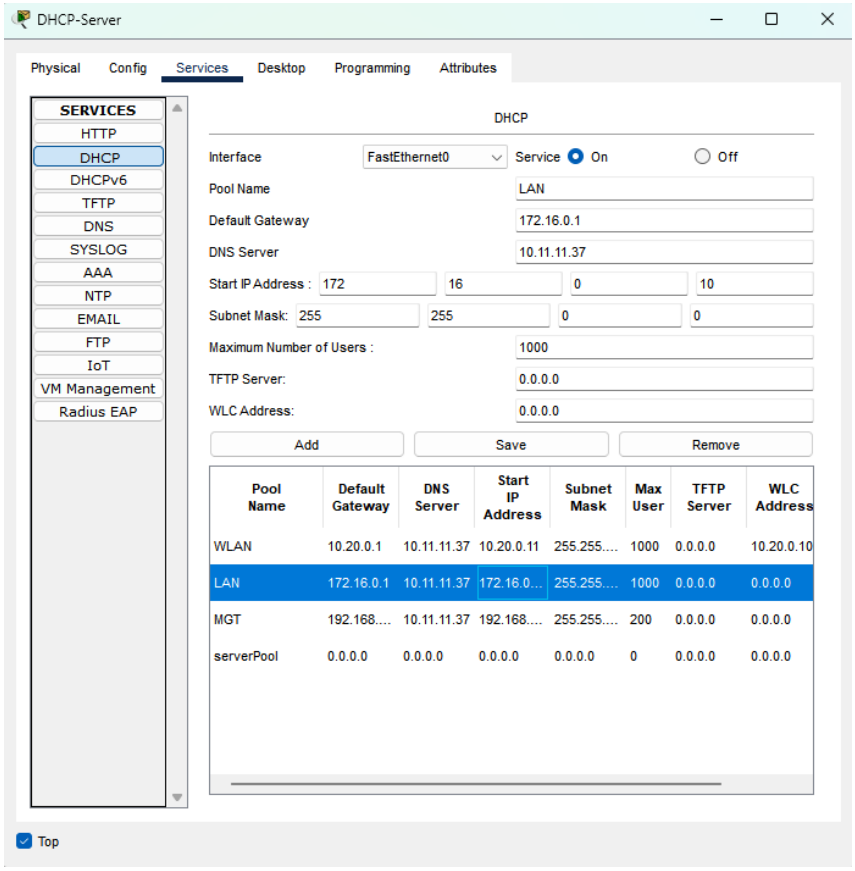

FIGURE IV.19 – Configuration DHCP du VLAN LAN

3. **Configuration DHCP du VLAN WLAN :**

   Pendant la configuration du DHCP du vlan WLAN, on met l'adresse du WLC (Wireless LAN Controller) pour permettre aux points d'accès (AP) et aux appareils sans fil de le localiser automatiquement car il centralise la gestion du réseau WI-FI.

   Dès leur activation, les AP seront en mesure de se lier au WLC, d'obtenir leur configuration et de fonctionner correctement sans nécessiter d'intervention manuelle.

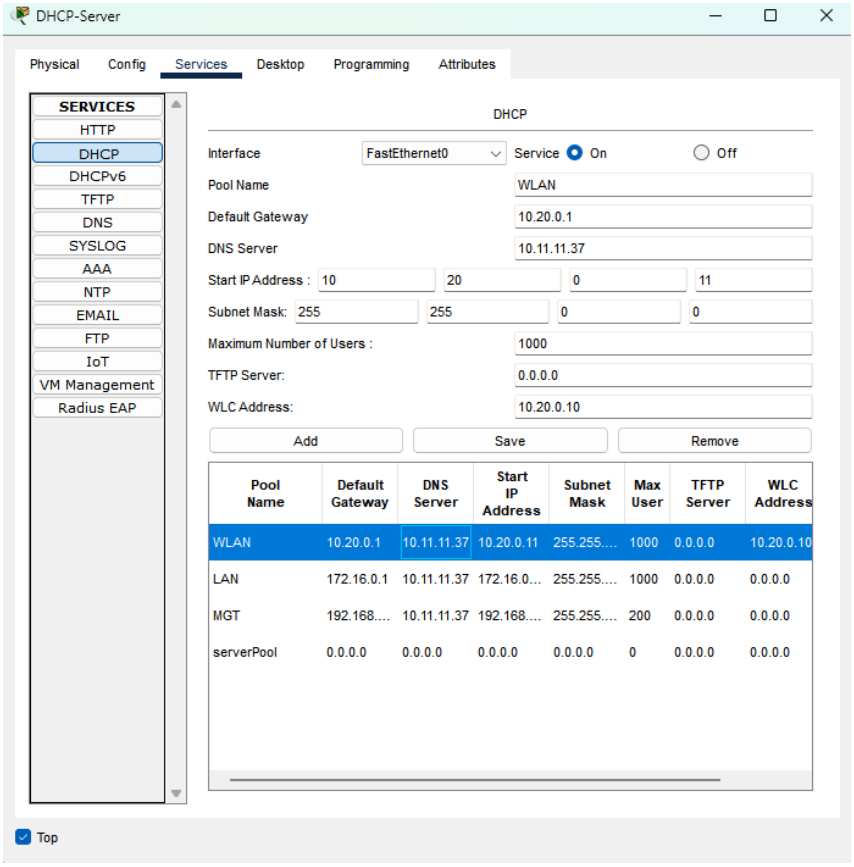

FIGURE IV.20 – Configuration DHCP du VLAN WLAN

IV.4.13 Configuration de OSPF dans les multi layer switch et les routeurs

Le protocole de routage dynamique OSPF, configuré avec l'authentification facilitera le routage entre zones et prévient l'injection de routes falsifiées, garantissant ainsi une connectivité fiable.

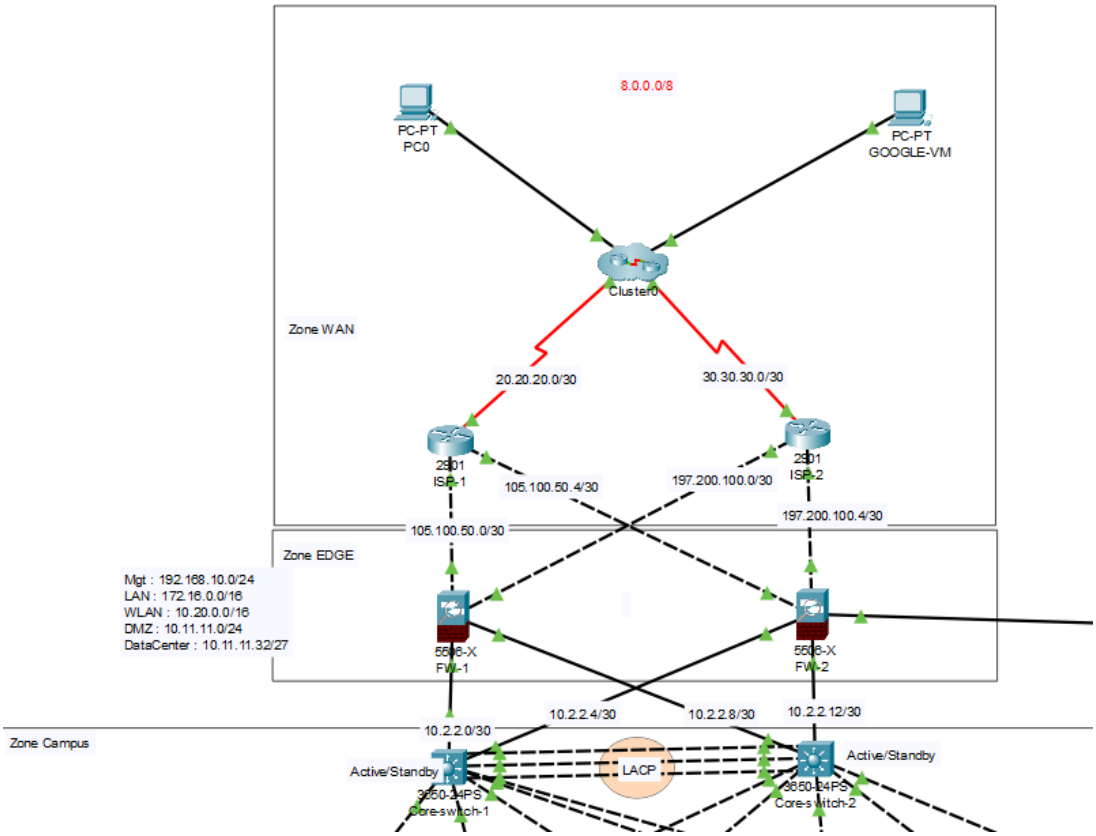

FIGURE IV.21 – Architecture de la zone WAN et EDGE

1. **Configuration de OSPF dans le switch multi layer 1**

```
!Activation du processus OSPF numero 1
Core-switch-1(config)#router ospf 1
Core-switch-1(config-router)#router-id 1.1.1.1 (defini l'ID
   du routeur
OSPF)
!Annonce des reseau dans la zone 0
Core-switch-1(config-router)#network 10.2.2.0 0.0.0.3 area 0
Core-switch-1(config-router)#network 10.2.2.4 0.0.0.3 area 0
Core-switch-1(config-router)#network 192.168.10.0 0.0.0.255
   area 0
Core-switch-1(config-router)#network 172.16.0.0 0.0.255.255
   area 0
Core-switch-1(config-router)#network 10.20.0.0 0.0.255.255
   area 0
Core-switch-1(config-router)#network 10.11.11.32 0.0.0.31
   area 0
Core-switch-1(config-router)#exit
Core-switch-1(config)#do wr
```

2. **Configuration de OSPF dans le switch multi layer 2**

```
!Activation du processus OSPF numero 1
Core-switch-2(config)#router ospf 1
Core-switch-2(config-router)#router-id 2.2.2.2
!Annonce des reseau dans la zone 0
Core-switch-2(config-router)#network 10.2.2.8 0.0.0.3 area 0
Core-switch-2(config-router)#network 10.2.2.12 0.0.0.3 area 0
Core-switch-2(config-router)#network 192.168.10.0 0.0.0.255
   area 0
Core-switch-2(config-router)#network 172.16.0.0 0.0.255.255
   area 0
Core-switch-2(config-router)#network 10.20.0.0 0.0.255.255
   area 0
Core-switch-2(config-router)#network 10.11.11.32 0.0.0.31
   area 0
Core-switch-2(config-router)#exit
Core-switch-2(config)#do wr
```

3. **Configuration de OSPF dans ISP 1**

```
!Activation du processus OSPF numero 1
Router(config)#router ospf 1
Router(config-router)#router-id 3.3.3.3
!Annonce des reseau dans la zone 0
Router(config-router)#network 105.100.50.0 0.0.0.3 area 0
Router(config-router)#network 105.100.50.4 0.0.0.3 area 0
Router(config-router)#network 20.20.20.0 0.0.0.3 area 0
Router(config-router)#exit
Router(config)#do wr
```

4. **Configuration de OSPF dans ISP 2**

```
Router(config)#router ospf 1
Router(config-router)#router-id 4.4.4.4
Router(config-router)#network 197.200.100.0 0.0.0.3 area 0
Router(config-router)#network 197.200.100.4 0.0.0.3 area 0
Router(config-router)#network 30.30.30.0 0.0.0.3 area 0
Router(config-router)#exit
Router(config)#do wr
```

5. **Configuration de OSPF dans Internet**

```
Router(config)#router ospf 1
Router(config-router)#router-id 5.5.5.5
Router(config-router)#network 20.20.20.0 0.0.0.3 area 0
Router(config-router)#network 30.30.30.0 0.0.0.3 area 0
```

```
Router(config-router)#network 8.0.0.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#do wr
```

6. **Configuration de l'authentification**

   L'authentification OSPF sécurise les échanges entre les routeurs afin qu'un routeur non autorisé ne puisse pas s'insérer dans le réseau OSPF et injecter des fausses routes.

```
Router(config)# interface gi 0/0
Router(config-if)# ip ospf authentication message-digest
Router(config-if)# ip ospf message-digest-key md5 Cisco123
Router(config-if)#exit
Router(config)#router ospf 1
Router(config-router)# area 0 authentification message-digest
```

IV.4.14 Configuration des Firewalls ASA

On configure les adresses IP des interfaces, les niveaux de sécurité et les zones (INSIDE, OUTSIDE et DMZ)

Par défaut, le firewall bloque tout le trafic venant d'une zone d'un niveau de sécurité bas (Security level 0) à élever (Security level 100) et donc tout trafic venant de la zone OUTSIDE a la zone INSIDE du firewall.

Configuration pour le Firewall 1

```
ciscoasa(config)#hostname FW-1
!Configuration de l'interface GigabitEthernet 1/3 (reseau interne
    1)
FW-1(config)#interface gig1/3
FW-1(config-if)#ip address 10.2.2.2 255.255.255.252
FW-1(config-if)#no shutdown
FW-1(config-if)#nameif INSIDE1 (Nom logique de l'interface)
INFO: Security level for "INSIDE1" set to 0 by default.
FW-1(config-if)#security-level 100 (Niveau de securite maximal <
   reseau interne>)
FW-1(config-if)#exit
!Configuration de l'interface GigabitEthernet 1/4 (reseau interne
    2)
FW-1(config)#interface gig1/4
FW-1(config-if)#ip address 10.2.2.10 255.255.255.252
FW-1(config-if)#no shutdown
FW-1(config-if)#nameif INSIDE2 (Nom logique de l'interface)
INFO: Security level for "INSIDE2" set to 0 by default.
FW-1(config-if)#security-level 100 (Niveau de securite maximal <
   reseau interne>)
```

```
FW-1(config-if)#exit
!Configuration de l'interface GigabitEthernet 1/1 (reseau externe
    1)
FW-1(config)#interface gig1/1
FW-1(config-if)#ip address 105.100.20.2 255.255.255.252
FW-1(config-if)#no shutdown
FW-1(config-if)#nameif OUTSIDE1 (Nom logique de l'interface)
INFO: Security level for "OUTSIDE1" set to 0 by default.
FW-1(config-if)#security-level 0 (Niveau de securite minimal <
   reseau externe>)
FW-1(config-if)#exit
!Configuration de l'interface GigabitEthernet 1/2 (reseau externe
    2)
FW-1(config)#interface gig1/2
FW-1(config-if)#ip address 197.200.100.2 255.255.255.252
FW-1(config-if)#no shutdown
FW-1(config-if)#nameif OUTSIDE2 (Nom logique de l'interface)
INFO: Security level for "OUTSIDE2" set to 0 by default.
FW-1(config-if)#security-level 0 (Niveau de securite minimal <
   reseau externe>)
FW-1(config-if)#exit
FW-1(config)#wr mem
```

Configuration pour le Firewall 2

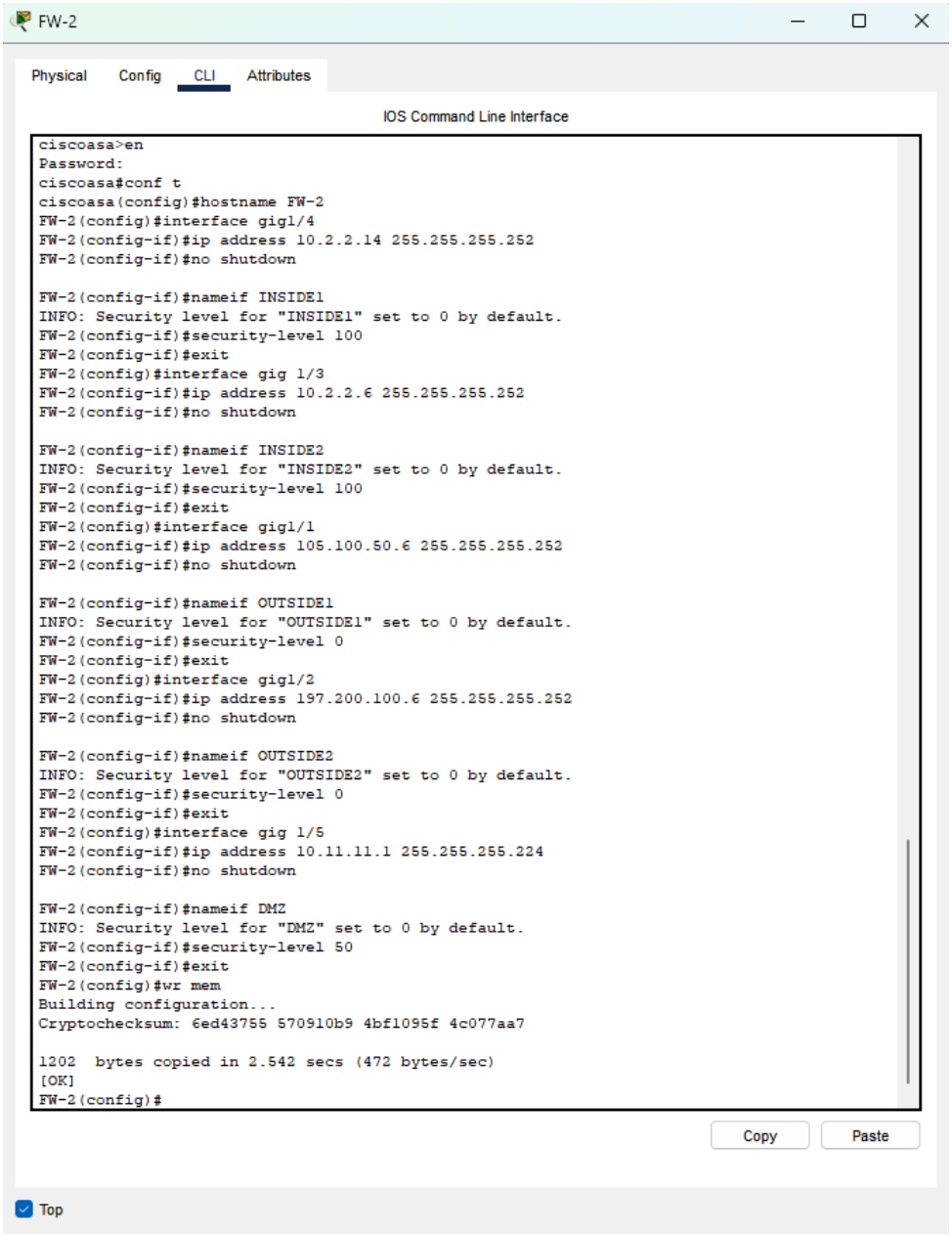

FIGURE IV.22 – Configuration du FW 2

IV.4.15 Firewall routing OSPF + static routes

Dans cette partie, on configure deux choses principales :

1. Définir deux routes par défaut

   La première via OUTSIDE1 (prioritaire)

   La seconde via OUTSIDE2 (backup)

2. Activer OSPF et annoncer les réseaux

Firewall 1

```
!Definition des routes statiques par defaut
FW-1(config)#route OUTSIDE1 0.0.0.0 0.0.0.0 105.100.50.1 (Route
   par defaut vers
la passerelle sur OUTSIDE1)
FW-1(config)#route OUTSIDE2 0.0.0.0 0.0.0.0 197.200.100.1 70 (
   Route par defaut
secondaire avec metrique 70)
!Activation et configuration du processus OSPF
FW-1(config)#router ospf 1
FW-1(config-router)#router-id 6.6.6.6
FW-1(config-router)#network 105.100.50.0 255.255.255.252 area 0
(publie le reseau OUTSIDE1 dans l'aire 0)
FW-1(config-router)#network 197.200.100.0 255.255.255.252 area 0
(publie le reseau OUTSIDE2 dans l'aire 0)
FW-1(config-router)#network 10.2.2.0 255.255.255.252 area 0
(publie le reseau interne)
FW-1(config-router)#network 10.2.2.4 255.255.255.252 area 0
(publie le second reseau interne)
FW-1(config-router)#exit
FW-1(config)#wr mem
```

Firewall 2

```
FW-2(config)#route OUTSIDE1 0.0.0.0 0.0.0.0 105.100.50.5 70
FW-2(config)#route OUTSIDE2 0.0.0.0 0.0.0.0 197.200.100.5
FW-2(config)#router ospf 1
FW-2(config-router)#router-id 7.7.7.7
FW-2(config-router)#network 197.200.100.4 255.255.255.252 area 0
FW-2(config-router)#network 105.100.50.4 255.255.255.252 area 0
FW-2(config-router)#network 10.2.2.4 255.255.255.252 area 0
FW-2(config-router)#network 10.2.2.12 255.255.255.252 area 0
FW-2(config-router)#network 10.11.11.0 255.255.255.252 area 0
FW-2(config-router)#exit
FW-2(config)#wr mem
```

IV.4.16 Configuration du NAT (LAN ET WLAN)

Le NAT est une technique qui permet de traduire les adresse IP privées utilisées à l'intérieur d'un réseau en adresse IP publique ou en d'autres plages d'adresses IP.

Dans cette configuration, nous utilisons un NAT dynamique basé sur l'adresse IP de sortie des interfaces OUTSIDE1 et OUTSIDE2.

Cela permet :

1. D'assurer la connectivité des VLAN internes (LAN et WLAN) vers l'extérieur.
2. De masquer l'adressage interne pour des raisons de sécurité.

Firewall 1

```
!NAT pour LAN depuis INSIDE1 vers OUTSIDE1
FW-1(config)#object network LAN-INSIDE1-LAN-OUTSIDE1
FW-1(config-network-object)#subnet 172.16.0.0 255.255.0.0 (reseau
    interne LANINSIDE1)
FW-1(config-network-object)#nat (INSIDE1, OUTSIDE1) dynamic
   interface
(NAT dynamique utilisant l'IP de l'interface OUTSIDE1)
!NAT pour LAN depuis INSIDE2 vers OUTSIDE1
FW-1(config-network-object)#object network LAN-INSIDE2-LAN-
   OUTSIDE1
FW-1(config-network-object)#subnet 172.16.0.0 255.255.0.0 (reseau
    interne LANINSIDE2)
FW-1(config-network-object)#nat(INSIDE2, OUTSIDE1) dynamic
   interface
(NAT dynamique utilisant l'IP de l'interface OUTSIDE1)
!NAT pour WLAN depuis INSIDE1 vers OUTSIDE1
FW-1(config-network-object)#object network WLAN-INSIDE1-WLAN-
   OUTSIDE1 (reseau
interne WLAN-INSIDE1)
FW-1(config-network-object)#subnet 10.20.0.0 255.255.0.0 (NAT
   dynamique utilisant
l'IP de l'interface OUTSIDE1)
FW-1(config-network-object)#nat (INSIDE1, OUTSIDE1) dynamic
   interface
!NAT pour WLAN depuis INSIDE2 vers OUTSIDE1
FW-1(config-network-object)#object network WLAN-INSIDE2-WLAN-
   OUTSIDE1
FW-1(config-network-object)#subnet 10.20.0.0 255.255.0.0
FW-1(config-network-object)#nat (INSIDE2, OUTSIDE1) dynamic
   interface
FW-1(config-network-object)#exit
!NAT pour LAN depuis INSIDE1 vers OUTSIDE1
FW-1(config)#object network LAN-INSIDE1-LAN-OUTSIDE1
FW-1(config-network-object)#object network LAN-INSIDE1-LAN-
   OUTSIDE2
FW-1(config-network-object)#subnet 172.16.0.0 255.255.0.0
FW-1(config-network-object)#nat(INSIDE1, OUTSIDE2) dynamic
   interface
!NAT pour LAN depuis INSIDE2 vers OUTSIDE2
```

```
FW-1(config-network-object)#object network LAN-INSIDE2-LAN-
   OUTSIDE2
FW-1(config-network-object)#subnet 172.16.0.0 255.255.0.0
FW-1(config-network-object)#nat (INSIDE2, OUTSIDE2) dynamic
   interface
!NAT pour WLAN depuis INSIDE1 vers OUTSIDE2
FW-1(config-network-object)#object network WLAN-INSIDE1-WLAN-
   OUTSIDE2
FW-1(config-network-object)#subnet 10.20.0.0 255.255.0.0
FW-1(config-network-object)#nat (INSIDE1, OUTSIDE2) dynamic
   interface
!NAT pour WLAN depuis INSIDE2 vers OUTSIDE2
FW-1(config-network-object)#object network WLAN-INSIDE2-WLAN-
   OUTSIDE2
FW-1(config-network-object)#subnet 10.20.0.0 255.255.0.0
FW-1(config-network-object)#nat (INSIDE2, OUTSIDE2) dynamic
   interface
FW-1(config-network-object)#exit
```

Firewall 2

FIGURE IV.23 – Configuration du NAT sur le FW 2

IV.4.17 Configuration de politique d'inspection du firewall

Dans la configuration de politique d'inspection on crée des règles qui autorise certains services.

ICMP : autorise le ping et les messages de diagnostic réseau

TCP eq 80 : autorise les requêtes http

TCP et UDP eq 53 : autorise les requêtes DNS

On applique ensuite l'ACL aux interfaces OUTSIDE1 et 2 dans le sens entrant (in).

Firewall 1

```
FW-1#conf t
FW-1(config)#access-list 1 extended permit icmp any any
FW-1(config)#access-list 1 extended permit tcp any any eq 80
FW-1(config)#access-list 1 extended permit tcp any any eq 53
FW-1(config)#access-list 1 extended permit udp any any eq 53
FW-1(config)#access-group 1 in interface OUTSIDE1
FW-1(config)#access-group 1 in interface OUTSIDE2
FW-1(config)#
```

FIGURE IV.24 – Configuration de la politique d'inspection sur le FW 1

Firewall 2

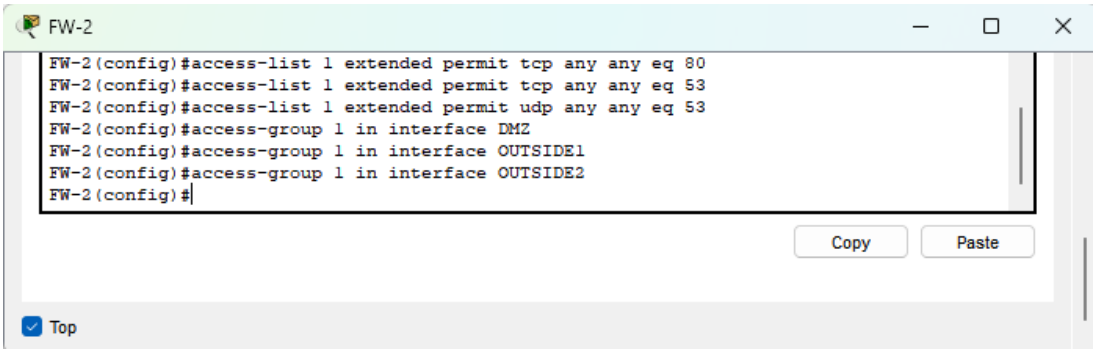

FIGURE IV.25 – Configuration de la politique d'inspection sur le FW 2

IV.4.18 Configuration du Wireless LAN Controller

Un Wireless LAN Controller (WLC) est un équipement réseau qui centralise la gestion des points d'accès wifi. Il applique automatiquement la configuration des paramètres tel que le SSID, La sécurité (WPA2/WPA3), l'affectation des VLANs etc. il améliore donc la sécurité et la gestion du réseau sans fil en garantissant une couverture homogène.

1. On commence par affecter les adresses IP correspondantes au WLC et au pc admin

WLC

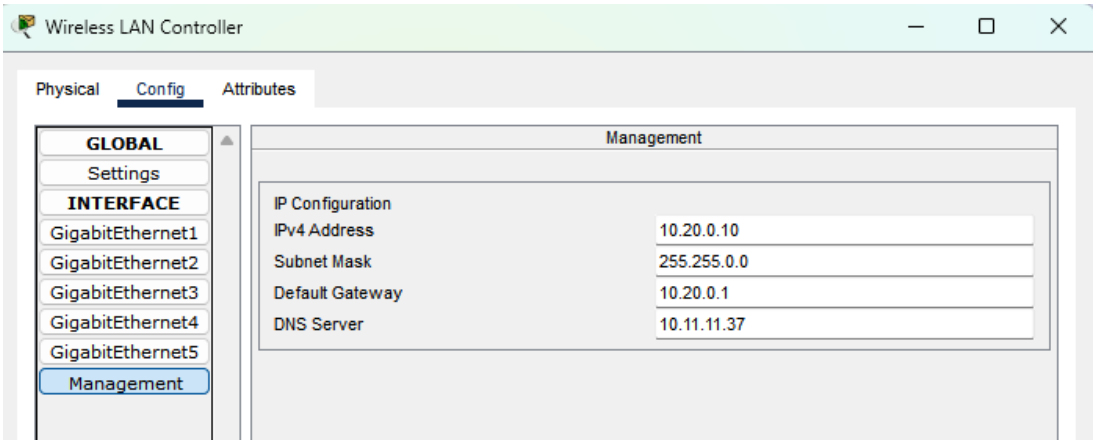

FIGURE IV.26 – Configuration du WLC

PC-Admin

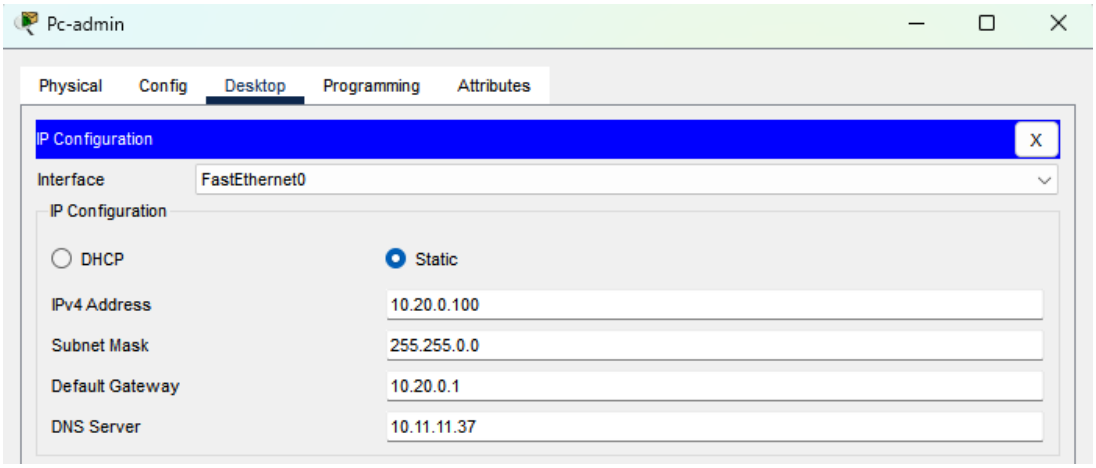

FIGURE IV.27 – Configuration du PC-Admin

2. On accède ensuite à l'interface graphique du Wireless LAN Controller depuis le pc-admin On crée un compte administrateur dans le but de sécuriser l'accès au WLC, Cet accès permettra de gérer et configurer les points d'accès et les réseaux Wi-Fi.

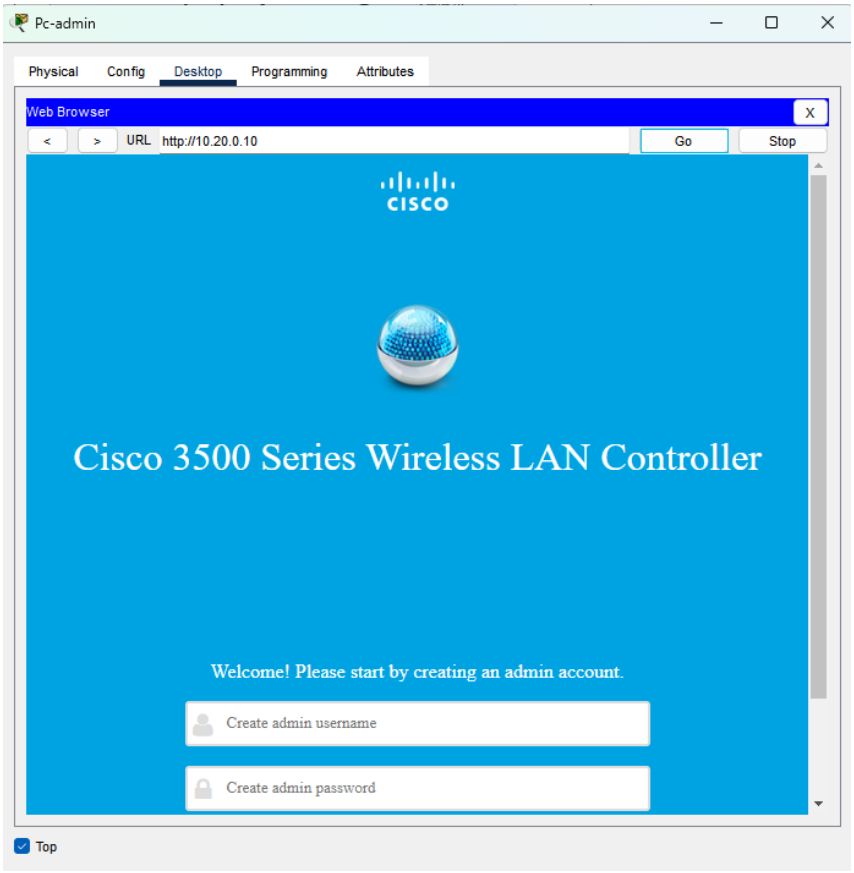

FIGURE IV.28 – Interface graphique du WLC

3. On crée un wifi pour les employeurs

Section controller settings :

Management IP Adress : 10.20.0.10 Adresse utilisée pour administrer le WLC

Subnet mask : 255.255.0.0 Définir le masque sous réseau.

Default Gateway : 10.20.0.1 Passerelle vers le réseau extérieur.

Management VLAN ID : 0 VLAN de gestion

Wireless Network Settings :

Employee Network : Création d'un SSID nommé EMPLOYES avec sécurité WPA2 Personal.

Passphrase : Mot de passe Wi-Fi pour les employés

Advanced Settings :

Virtual IP Address : 192.0.2.1 Adresse IP virtuelle utilisée pour certaines fonctions internes du WLC.

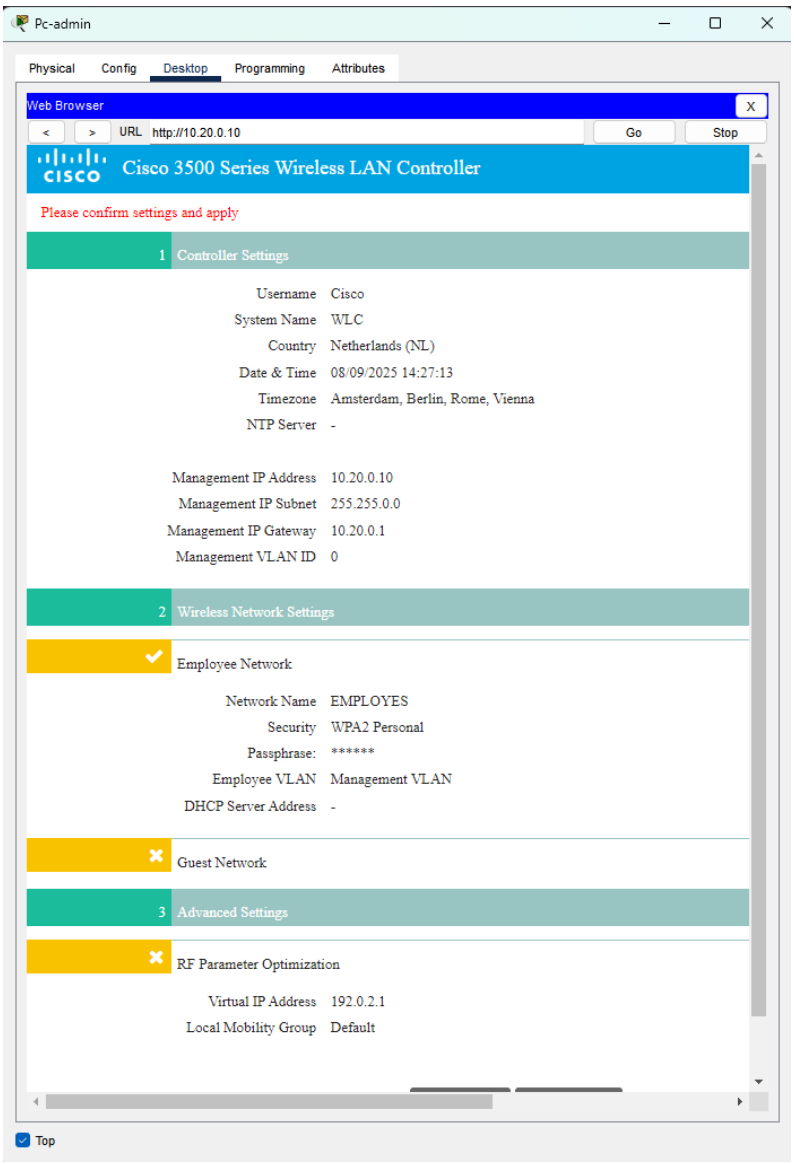

FIGURE IV.29 – Création du wifi pour les employées

4. On crée un wifi pour les visiteurs

   Ce réseau est généralement isolé du réseau interne, avec accès limité à Internet.

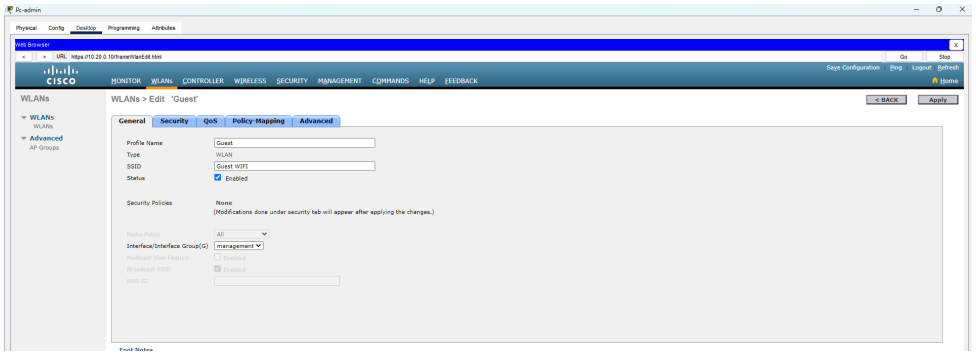

FIGURE IV.30 – Création du wifi Guest

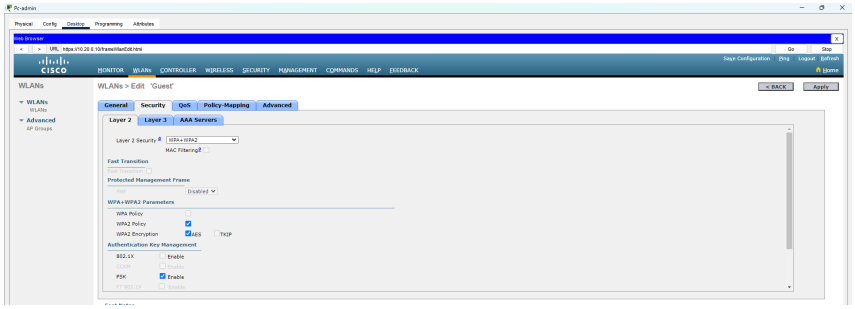

FIGURE IV.31 – Configuration du wifi Guest

5. On aura donc 2 réseaux wifi au sein de l'entreprise

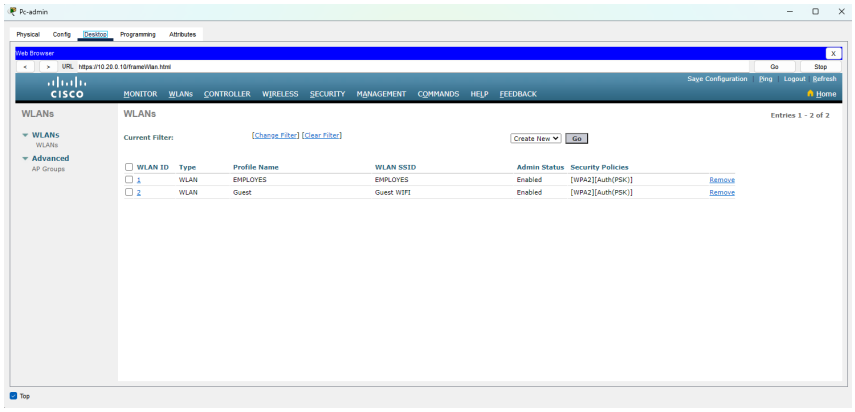

FIGURE IV.32 – Figure montrant les deux wifi crée

IV.4.19 Synchronisation du WLC avec les Access point

La synchronisation permet aux points d'accès de recevoir automatiquement leur configuration depuis le contrôleur

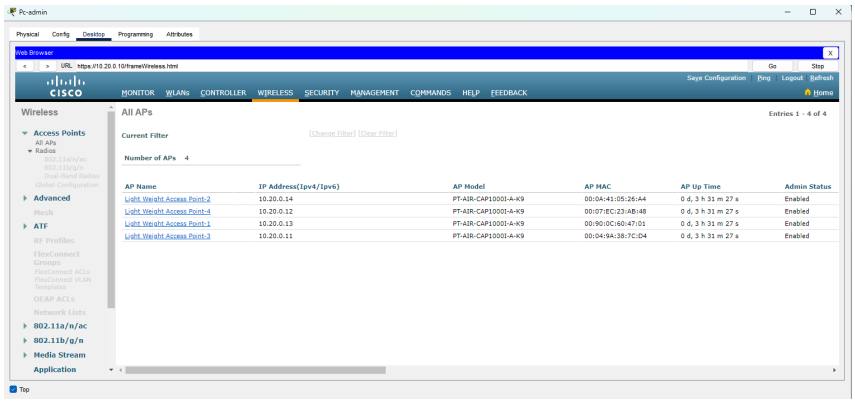

FIGURE IV.33 – Synchronisation WLC avec les access point

Nos points d'accès montrent les deux réseaux wifi disponibles

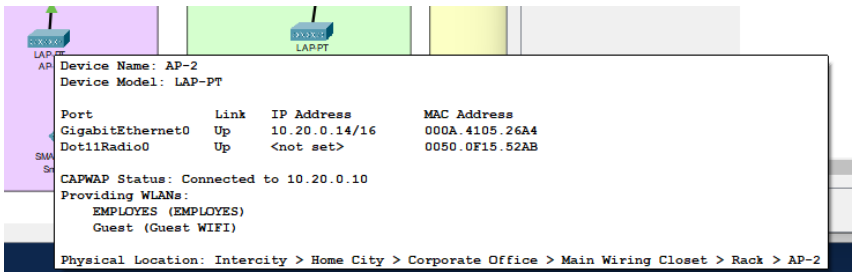

FIGURE IV.34 – Figure montrant les deux wifi disponibles

On connecte ensuite l'ensemble des appareils sans fils au point d'accès et au réseau wifi correspondant

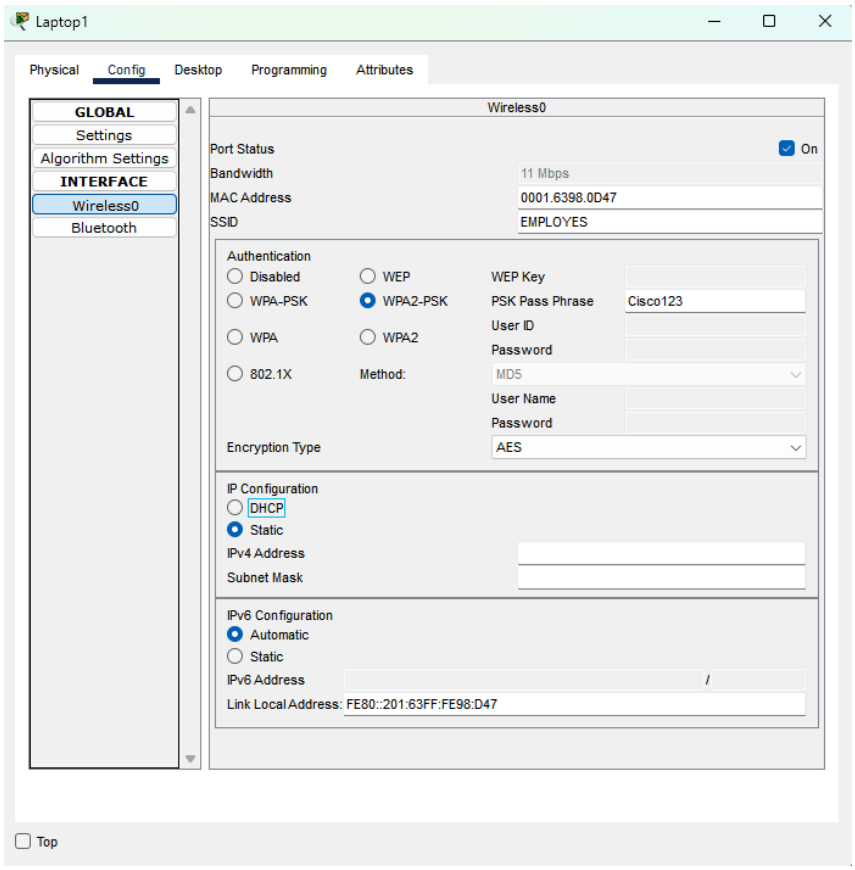

FIGURE IV.35 – Connection des appareils sans fils au point d'accès

IV.5 Tests fonctionnels

L'objectif de ses tests est de vérifier que le réseau répond parfaitement aux besoins de communication et de redondance.

Ping intra-vlan

On ping deux appareils appartenant au même vlan (exemple VLAN20 LAN)

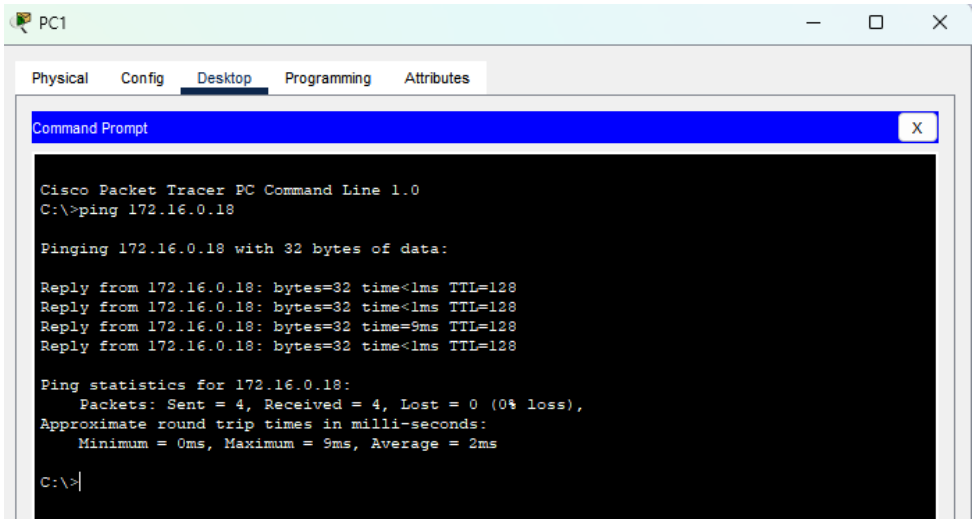

FIGURE IV.36 – ping entre PC1 et PC2

Ping inter-VLAN

On ping depuis le PC 1 apparentant au Vlan LAN (Vlan 20) vers le laptop 1 appartenant au Vlan WLAN (Vlan 30).

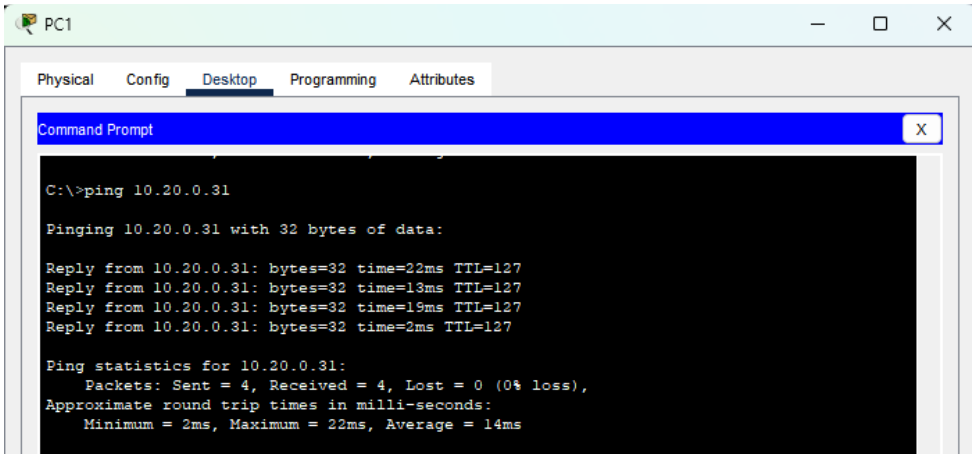

FIGURE IV.37 – Ping entre PC1 et Laptop1

Ping vers la DMZ

On ping depuis le PC 1 vers le serveur Web qui se retrouve dans la zone DMZ

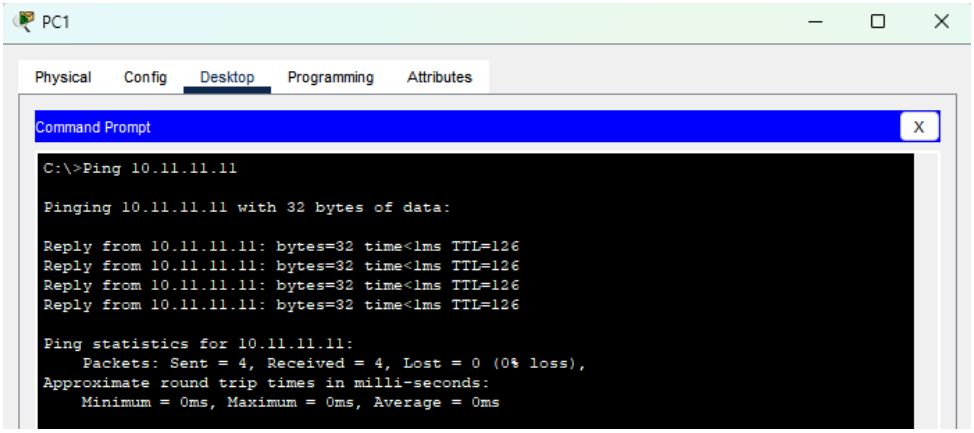

FIGURE IV.38 – Ping entre PC1 et Serveur Web

Ping vers Internet

On essaie de ping depuis le PC1 de la zone campus au réseau 8.0.0.0/8

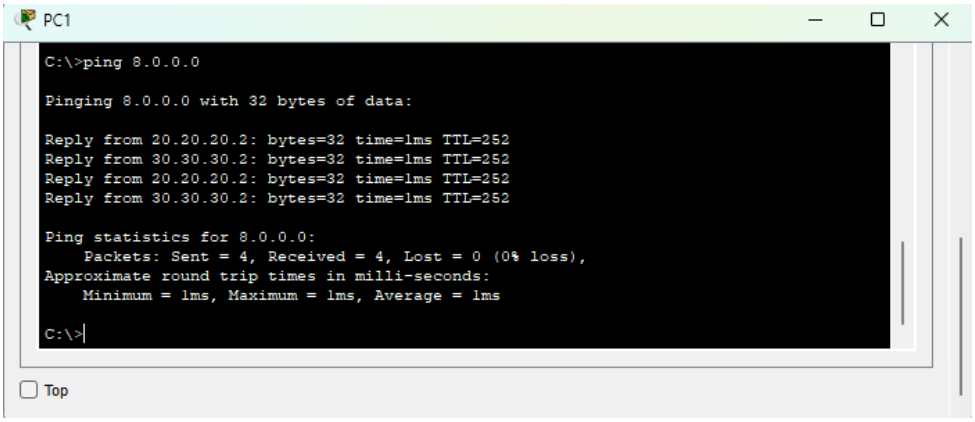

FIGURE IV.39 – Ping entre PC1 et Internet

IV.6 Mesure de sécurité utilisé pour sécuriser la topologie

Durant la mise en place et la configuration de cette architecture, plusieurs mesures de sécurité ont été intégrées afin de renforcer la sécurité du réseau. Dans ce paragraphe on revient sur les mesures utilisées tout au long de la configuration qui nous garantissent un réseau fonctionnel et surtout sécurisé dans sa globalité.

Les mots de passes : qui protègent l'accès aux équipements réseau contre toute connexion non autorisée.

L'activation du SSH : remplace Telnet et garantit une administration chiffrée.

L'utilisation des ACL : limite l'accès aux ressources et aux équipements en filtrant le trafic selon les adresses IP ou les protocoles.

La segmentation du réseau en VLAN : en isolant les réseaux LAN et VLAN et réduit la propagation des attaques d'un réseau à l'autre.

La configuration du STP BPDU Guard et STP Port Fast : évitent les boucles et bloquent les tentatives d'ajout de switch non autorisés.

L'utilisation de l'Etherchannel : assure redondance et continuité de service en cas de coupure d'un lien physique.

HSRP : garantit la disponibilité de la passerelle par défaut même en cas de panne d'un routeur ou d'un switch de couche 3.

L'authentification OSPF : protège le protocole de routage contre l'injection de routes frauduleuses ou de routeurs non autorisés.

L'utilisation de firewall ASA : contrôle et filtre le trafic entre les zones, empêchant les accès non autorisés.

L'utilisation du NAT : masque les adresses IP internes, ce qui rend le réseau interne moins exposé aux attaques externes.

Les politiques d'inspection : autorisent uniquement certain service tel que ICMP (Ping), http, DNS et bloquent les connexions suspectes ou non conformes.

IV.7 Conclusion

Dans ce quatrième chapitre, nous avons procédé à la simulation de l'architecture réseau conçue sous Cisco Packet Tracer. Après avoir défini la topologie et les équipements utilisés, nous avons détaillé les différentes étapes de configuration, allant de la création des VLANs, du routage inter-VLAN et du protocole HSRP, jusqu'à l'intégration des mécanismes de sécurité.

Les tests fonctionnels réalisés ont validé la connectivité entre les différentes zones (WAN, Campus, DMZ, Datacenter) et confirmé l'efficacité des dispositifs de sécurité intégrés. Nous estimons ainsi avoir atteint l'objectif principal de ce travail : Etudier et simuler un réseau informatique sécurisé.

Conclusion générale

Ce mémoire a porté sur l'étude et la simulation d'une architecture réseau sécurisée à l'aide de Cisco packet Tracer. Après avoir présenté les concepts fondamentaux liés aux réseaux informatiques et aux enjeux de la sécurité, nous avont proposé une architecture hiérarchisée intégrant différentes zones fonctionnelles telles que le WAN, Campus, la DMZ et le Datacenter.

La conception a reposé sur l'utilisation de mécanismes essentiels comme la segmentation par VLAN, le routage inter-VLAN, et protocole HSRP pour la redondance, le routage dynamique OSPF, ainsi que la mise en place d'un pare-feu ASA et d'un contrôleur sans fil pour assurer un contrôle rigoureux des flux de répondre aux exigences de disponibilité, de performance et de sécurité.

La phase de simulation a représenté la concrétisation pratique de cette architecture. Les configurations détaillées réalisées et les tests fonctionnels effectués ont confirmé le fonctionnement de notre architecture.

Ainsi, nous estimons avoir atteint l'objectif principal de ce travail : étudier et simuler un réseau informatique sécurisé, capable de répondre aux besoins actuels en termes de performances, de protections des ressources. Ce mémoire a également constitué une occasion d'approfondir notre maitrise des outils de simulation, de solidifier nos connaissances sur les protocoles et mécanismes de sécurité.

Perspectives

Au-delà des résultats obtenus, plusieurs pistes damélioration et dextension peuvent être envisagées afin de renforcer la robustesse, la sécurité et lévolutivité de larchitecture proposée ; les principales perspectives sont présentées ci-dessous :

Faire évoluer la zone Campus vers une architecture 3-tier (Core/Distribution/Access) et tester la tolérance aux pannes (liens, équipements).

Mettre les pares-feux en haute disponibilité (actif/veille) et ajouter un VPN site-à-site + accès distant.

Etendre le plan de routage (OSPF multi-aires, redistribution)

Automatiser la configuration et rejouer la maquette sous GNS3 avec images réelles pour des tests plus proches du terrain.

Approfondir la sécurité WLAN (WPA2-Enterprise, politique invité) et évaluer IDS/IPS avec scénarios dattaque contrôlés.

Bibliographie

[1] N. Sfetcu, *Les menaces persistantes avancées en cybersécurité - La guerre cybernétique*, Multimedia Publishing, 2024.

[2] V. Remazeilles, *La sécurité des réseaux avec Cisco*, Saint-Herblain, France : Editions ENI, 2009.

[3] D. Dromard et S. Dominique, *Architecture des réseaux*, Pearson, 2006.

[4] A. Tanenbaum et D. Wetherall, *Réseaux*, Pearson, 2011.

[5] A. Boussouf, *Reseaux 2ème année informatique*, Mila, 2022/2023.

[6] P. Jaquet, *Les réseaux informatiques*, 2015.

[7] S. Brahimi, *Support de cours Réseaux de communication pour 2ème année licence informatique*, Département Informatique : Université Guelma.

[8] S. Lohier et D. Present, *Réseaux et transmissions*, Dunod, 2020.

[9] B. Jarray, *Réseaux informatiques, Adressage IP, modèle OSI, Ethernet, VLAN, routage Cours et exercices corrigés*, Ellipses, 2015.

[10] M. Bourois, ńCours de réseau,ż 2017/2018. [En ligne]. Disponible : `https://www.studocu.com/frca/document/universite-de-sherbrooke/reseaux-et-systemes-informatiques/reseau-notes-decours-1/2209692`. [Accès le 28/02/2025].

[11] Cisco Networking Academy, [En ligne]. Disponible : `https://cisco.ofppt.info/ccna1/index.html`. [Accès le 17/03/2025].

[12] B. Petit, *Architecture des réseaux*, Ellipses, 2010.

[13] F. Goffinet, ńAdressage IPV4,ż 09/08/2020. [En ligne]. Disponible : `https://cisco.goffinet.org/ccna/ipv4/adressage-ipv4/`. [Accès le 28/04/2025].

[14] P. Spathis, *Technologies et protocoles Internet*, Éditions Ellipses, 2023.

[15] P. Jaquet, *Les réseaux informatiques*, `https://www.jaquet.org`, 2015.

[16] ńCours sur subnetting,ż [En ligne]. Disponible : `http://robert.cireddu.free.fr/SNIR/Cours%20sur%20le%20subnetting.pdf`. [Accès le 29/04/2025].

[17] C. Bulfone, *Sécurité des réseaux*.

[18] M. Denou, *Securité des réseaux*, Master CNS, Université d'Evry, 2020.

[19] E. Mabo, *La sécurité des systèmes informatiques (théorie)*, support de cours, 2010.

[20] J.-F. P. et J.-P. Bay, *Tout sur la sécurité informatique*, 2ème édition, Dunod.

[21] J.-F. Carpentier, *La sécurité informatique dans la petite entreprise, Etat de l'art et bonnes pratiques*, 3ème édition, Editions ENI, 2016.

[22] R. Manglik, ńHacking techniques,ż [En ligne]. Disponible : https://books.google.fr/books?id=CIhREQAAQBAJ&pg=PA73. [Accès le 18/05/2025].

[23] Y. C. Douas, *Les types d'attaques informatiques*, OFPPT, 2010.

[24] E. Detoisien, ńLes attaques externes,ż [En ligne]. Disponible : https://doc.lagout.org/network/2003_attaques_externes.pdf. [Accès le 18/05/2025].

[25] D. H. Diboun Terkouia, ńMise en place d'une solution de securité d'un réseau informatique. Cas d'une banque,ż 2013/2014.

[26] B. I. et G. Anais, *Mémoire de fin d'étude : étude et mise en place des liaisons virtuelles (VLAN, VPN)*, Béjaia, 2021.

[27] C. Llorens, *Tableau de bord de la sécurité réseau*, 2e édition.

[28] A. Ghattas, ńNotions de securité des reseaux informatiques,ż OFPPT, septembre 2008.

[29] P. M. R. K. Y. et M. C. P. S. K. Rai, *Cyber Security*, Boca Raton Publishers, 2019.

[30] ńSSH Academy,ż [En ligne]. Disponible : https://www.ssh.com/academy/ssh. [Accès le 27/04/2025].

[31] M. M. et M. Nacer, *Mémoire de Fin d'Etudes : Sécurisation d'une infrastructure LAN/WAN*, 2015.

[32] ńArchitecture de référence : Conception de réseau WAN d'entreprise,ż Juniper Networks. [En ligne]. Disponible : https://www.juniper.net/documentation/fr/releaseindependent/solutions/information-products/topic-collections/broadband-edge-refarch/jd0e161.html.

[33] ńISP : qu'est-ce que c'est ?,ż [En ligne]. Disponible : https://www.futurasciences.com/tech/definitions/internet-isp-482/. [Accès le 08/05/2025].

[34] Cisco, *Enterprise Campus 3.0 Architecture : Overview and Framework*, Cisco Systems, Inc.

[35] M. A. M. et J. D. L. C. DeCusatis, *Handbook of Fiber Optic Data Communication : A Practical Guide to Optical Networking*, 4e éd., Waltham, MA, USA : 2013.

[36] C. Servin, *Réseaux et télécoms - Cours et exercices corrigés*, Dunod, 2003.

[37] S. Paz, ńServeur DNS, FTP et proxy,ż [En ligne]. Disponible : https://www.multihardware.com/blog/serveur-dns-ftp-et-proxy-que-faut-il-savoir. [Accès le 08/05/2025].

[38] K. H. et M. A. Lynda, *Mémoire de fin d'étude : La Haute Disponibilité des Réseaux (HSRP), cas d'étude : Réseau LAN de CEVITAL Agro-industrie*, Mira, Bejaia, 2022.

[39] A. Bron, *Services et Réseaux, version 5.0 (Routage statique et dynamique)*, Lulu.com, 2011.

[40] M. Kadoch, *Protocoles et réseaux locaux*, 2e éd. revue et augmentée, Québec, Canada, 2012.

[41] ńIntroduction au protocole de routage dynamique OSPF,ż [En ligne]. Disponible : https://cisco.goffinet.org/ccna/ospf/introduction-au-protocole-routage-dynamique-ospf/. [Accès le 14/04/2025].

[42] ńComprendre et utiliser le protocole Enhanced Interior Gateway Routing,ż [En ligne]. Disponible : https://www.cisco.com/c/fr_ca/support/docs/ip/enhanced-interior-gateway-routing-protocoleigrp/16406-eigrptoc.html. [Accès le 14/04/2025].

[43] CCNA, ńEIGRP,ż [En ligne]. Disponible : https://cisco.ofppt.info/ccna3/course/module7/index.html#7.0.1.1. [Accès le 03/05/2025].

[44] B. Dutcher, *The NAT Handbook : Implementing and Managing Network Address Translation*, New York, NY, USA : John Wiley & Sons, 2000.

[45] J. A., *Packet Tracer Network Simulator*, Packet Publishing, 2014.

[46] D. Lowe, *Networking for Dummies*, 12e éd., For Dummies, 2020.

[47] F. Goffinet, ńPrincipes de conception LAN,ż [En ligne]. Disponible : https://cisco.goffinet.org/ccna/ethernet/principes-conception-lan-cisco/. [Accès le 12/04/2025].

[48] A. S. et B. Benmammar, ńLa sécurité intelligente des réseaux informatiques,ż in *Gestion et contrôle intelligents des réseaux*, 2020.

[49] F. Goffinet, ńRedondance de passerelle protocole HSRP,ż [En ligne]. Disponible : https://cisco.goffinet.org/ccna/disponibilite-lan/redondance-de-passerelle-host-standby-router-protocol-hsrp/. [Accès le 15/04/2025].

[50] R. Sanchez, *Les réseaux locaux virtuels*, 2006.

[51] C. Bulfone, ńSécurité des réseaux,ż Master MIASHS/DCISS, 2023/2024.

[52] O. S. et J. Frahim, *Cisco ASA : All-in-One Firewall, IPS, and VPN Services*, Cisco Press.

[53] A. V. de Toledo, *Conception et simulation d'une architecture réseau d'entreprise* Mémoire de Master, Univ. Paris-Est, France, 2019.

[54] Cybellium Ltd., *Mastering Firewalls*, Cybellium Ltd., 2023.

[55] S. K. Rai, P. Mishra, R. K. Yadav, et M. C. Pandey, *Cyber Security*, Boca Raton, FL, USA : Boca Raton Publishers, 2019.

[56] G. A. Donahue, *Network Warrior*, Royaume-Uni : O'Reilly Media, 2011.

[57] W. Stallings and L. Brown, *Computer Security : Principles and Practice*, 5th ed., Pearson, 2024.

[58] M. Kadoch, *Protocoles et réseaux locaux*, 2e éd. revue et augmentée. Québec, Canada : Presses de l'Université du Québec, 2003.

[59] F. Pignet, *Réseaux informatique, Supervision et Administration*, Edition ENI, 2007.

Résumé

Ce mémoire présente létude, la conception et la simulation dun réseau dentreprise sécurisé à laide de Cisco packet Tracer. Après un rappel des principes fondamentaux des réseaux et des enjeux de la cybersécurité, une architecture hiérarchisée multi-zones (WAN, Campus, DMZ, Datacenter) est définie puis implémentée.

La solution met en uvre la segmentation par VLAN et le routage inter-VLAN, la sécurisation de couche 2 (STP/PortFast/BPDU Guard), lagrégation de liens (LACP), redondance de passerelle (HSRP), adressage dynamique (DHCP), le routage OSPF, la traduction dadresses (NAT), des listes de contrôle daccès (ACL) et un pare-feu ASA, ainsi quune infrastructure WLAN pilotée par contrôleur (WLC).

Les tests de connectivité, de redondance et de filtrage démontrent que larchitecture proposée répond aux objectifs de disponibilité, de confidentialité et dintégrité, et valident lintérêt de la simulation pour évaluer des choix techniques avant un déploiement réel

Mots-clés : Réseau dentreprise, Sécurité, VLAN, STP, HSRP, DHCP, OSPF, NAT, ACL, Pare-feu ASA, WLAN, DMZ, Simulation, Cisco Packet Tracer.

Abstract

This thesis presents the study, design, and simulation of a secure enterprise network using Cisco Packet Tracer. After reviewing networking fundamentals and cybersecurity requirements, a multi-zone hierarchical architecture (WAN, Campus, DMZ, Datacenter) is specified and implemented.

The solution integrates VLAN segmentation and inter-VLAN routing, Layer-2 hardening (STP/PortFast/BPDU Guard), link aggregation (LACP), first-hop redundancy (HSRP), dynamic addressing (DHCP), OSPF routing, Network Address Translation (NAT), Access Control Lists (ACLs), and an ASA firewall, as well as a controller-based WLAN (WLC).

Connectivity, redundancy, and filtering tests show that the proposed design meets availability, confidentiality, and integrity goals, confirming the value of simulation to validate technical choice prior to real-world deployment.

Keywords : Enterprise network, Security, VLAN, STP, HSRP, OSPF, NAT, ACL, ASA firewall, WLAN, DMZ, Simulation, Cisco Packet Tracer.