REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de **T**echnologie

Département **I**ngénierie des **S**ystèmes **E**lectriques

Mémoire de Master

Présenté par

YAHIAOUI Manel

BOULANOUAR Imene

Filière : Télécommunications

Spécialité : Réseaux et **T**élécommunications

THEME :

Implémentation d'une solution SD-WAN Overlay sur une plateforme réseau WAN Multimesh

Soutenu le 30/06/2024 devant le jury composé de :

ACHELI Dalila	Prof	UMBB	Présidente
BELKACEM Samia	MCA	UMBB	Examinatrice
MESSAOUDI Noureddine	Prof	UMBB	Promoteur

Année Universitaire : 2023/2024

Remerciements

D'abord, nous exprimons notre gratitude envers ALLAH le Tout-Puissant pour nous avoir guidé vers les portes du savoir, en nous accordant le courage, la force et la patience tout au long de notre parcours.

Nous tenons à remercie profondément nos chers parents, qui méritent toute notre admiration et notre reconnaissance. Leur amour indéfectible, leur soutien inébranlable et leurs sacrifices constants ont été les fondations de notre épanouissement et de notre joie de vivre. Leur présence réconfortante, leurs encouragements et leurs précieux conseils ont éclairé notre chemin et nous ont donné la détermination nécessaire pour surmonter les difficultés.

Nous tenons également à remercie nos encadrants du stage madame F.RAHI et monsieur A.KAHLA ainsi que l'ensemble des employés du département d'ingénierie technique et de production qui nous ont gratifier de leurs précieux conseils, leur disponibilité et leurs orientations.

Nous exprimons nos sincères remerciements à monsieur ***Noureddine MESSAOUDI*** *le chef de département d'Ingénierie des Systèmes Electriques et notre promoteur pour sa patience et sa disponibilité ainsi que l'ensemble du corps professeur et enseignant de la faculté du Technologie UMBB.*

Merci à nos amie Rim, Hassiba, Chahrazed et Damia pour leur soutien moral et leur amour, vous êtes adorable, love you.

Nous tenons à exprimer nos sincères remerciements à nous même « ***YAHIAOUI Manel, BOULANOUAR Imene*** *» pour notre travail d'équipe, notre compétence et notre patience tout au long de ce projet.*

Enfin, nous remercions les membres de jury pour avoir consacré du temps à évaluer notre travail et l'enrichir avec leurs proposions et leurs conseils.

Dédicaces

A ma chère mère

A mon cher père

Je vous dis merci d'avoir fait de moi celui que je suis aujourd'hui, merci pour tous vos efforces, votre encouragement tout au long de mes études et au long de ma vie, merci pour votre amour, votre patience et vos sacrifices aucun mot ne pourra exprimer toute l'estime, la considération et l'admiration que j'ai pour vous.

A mon frère Rabah et ma belle-sœur Meriem

A mon frère Walid

A ma sœur Mouna

Pour leur soutien et leurs conseils précieux, cette dédicace est une manière pour moi de vous exprimer tout l'amour que je vous porte.

A ma binôme Imene

A mes amies, Chahrazed, Damia, Hassiba, Hayet, Rim

Pour votre amour et votre soutien. Mes années universitaires ont été parmi les périodes les plus enrichissantes et mémorable de ma vie et bien gravé dans ma mémoire grâce à vous mes sœurs.

Et enfin, à mon petit prince Mohamed et ma petite princesse Hiba.

YAHIAOUI Manel

Dédicaces

A mes très chers parents

Il est difficile de trouver les mots justes pour exprimer toute ma gratitude pour les sacrifices que vous avez faits et le soutien inconditionnel que vous m'avez toujours apporté. Votre amour, votre dévouement et votre présence ont été des piliers essentiels dans ma vie.

A ma sœur Mellissa

Merci pour ton soutien constant, ton amour et tes encouragements. Ta présence m'a aidé à surmonter les moments difficiles et à rester motivé tout au long de ce parcours.

À ma binôme Manel

Pour ton soutien indéfectible, ta collaboration et ton amitié tout au long de ce projet.

À tous mes amies, Rim, Chahrazed, Hassiba, Damia

Merci pour ces années merveilleuses passées ensemble. Vous avez rendu ce parcours inoubliable avec votre amour, votre soutien et les souvenirs inestimables que nous avons partagés. Votre amitié a été une source de joie et de force, et je chérirai toujours ces moments passés à vos côtés.

BOULANOUAR Imene

Table des matières

Abréviations

A

ADC: analogue-to-digital-Converter.

API: Application Programming Interface.

B

BGP: Border Gateway Protocol.

C

CAN : convertisseur analogique numérique.

CHAP: Challenge Handshake Authentication Protocol.

CPU: Central Processing Unit.

D

DGAMSP : La direction générale de l'administration des moyens et des systèmes de paiements.

DITP : Direction de l'ingénierie technique et de la production.

DSL : Digital Subscriber Line.

DSLAM : Digital Subscriber Line Multiplexer.

DMVPN : Dynamic Multipoint VPN.

E

EEPROM : mémoire morte effaçable électriquement et programmable.

EIGRP: Enhanced Interior Gateway Routing Protocol.

H

HDLC: High-level Data Link Control.

I

IOS: Internetwork Operating System.

IP: Internet Protocol.

IEEE: Institute of Electrical and Electronics Engineers.

IS-IS: Intermediate System to Intermediate System.

G

GNS3: Graphical Network SImulatoe-3.

K

KvM: Kernel-based Virtual Machine.

L

LAN : Local Area Network.

LCP : protocole de contrôle de liaison.

LCD : écran à cristaux liquides.

LED : Light-Emitting Diode.

LDR : La lumière dépendait des résistances.

LS : lignes spécialisées.

M

MAN: Metropolitan Area Network.

MPLS: Multi Protocol Label Switching.

N

NTC: National Telecommunications Commission.

NCP: Network control protocol.

NGN: Next Generation Network.

NBI: North-Bound Interface.

NHRP: Next Hop Resolution Protocol.

NGFW : Next-generation Firewalls.

O

OSI: Open System Interconnection.

ONF: Open Networking Fondation.

OSPF: Open Shortest Path First.

P

PROM: Programmable Read-Only Memory.

PWM: Pulse Width Modulation.

PPP: Point-to-Point Protocol.

PAP: Plan d'Accompagnement Personnalisé.

Q

QEMU: Quick Emulator.

QoS: Quality of service.

R

RCIU : Le retard de croissance intra-utérin.

RAM : Random Access Memory.

RTD: Round-Trip Delay.

REST: Representational State Transfer.

RMS: Reseau Multi Service.

S

SNMP: Simple Network Management Protocol.

SMUR : Service Mobile d'Urgence et de Réanimation.

SRAM: Static Random Access Memory.

SDN: Software Defined Networking.

SD-WAN: Software Defined-Wide Area Network.

SBI: South-Bound Interface.

SLA : Service Level Argeement

T

TOR : tout ou rien.

Te : Temps d'échantillonnage.

TCP : Transmission Control Protocol.

U

UDP: User Datagram Protocol.

USB: Universal Serial Bus.

V

VDR : Voirie et Réseaux Divers.

VSAT: Very Small Aperture Terminal.

VLAN: Virtual local area network.

VPN: Virtual Private Network.

W

WAN: Wide Area Network.

Liste des figures

Chapitre I : Généralités sur les réseaux informatique

Chapitre II: Software Defined Network

Chapitre III : Etude de solution SD-WAN

Chapitre IV: Réalisation et implémentation

Liste des tableaux

Chapitre I : Généralités sur les réseaux informatique

Chapitre II : Software Defined Network

Chapitre IV: Réalisation et implémentation

الملخص

ازدادت الحاجة إلى الاتصال واسع النطاق بين شبكات المواقع الطرفية للمؤسسات والشبكات المركزية للمكاتب أو مراكز البيانات السحابية، مما أدى إلى تطوير حلول الشبكات الواسعة المعرفة بالبرمجيات. تقوم هذه الحلول بتحسين استخدام روابط الشبكات الواسعة، مما يعالج القضايا الحرجة في إدارة الشبكات الواسعة الهجينة. تطبق فوائد الشبكات المعرفة بالبرمجيات على شبكات المؤسسات وتدمج عناصر من الشبكات التقليدية وشبكات الجيل القادم. يعرف هذا المقال بنية الشبكات الواسعة المعرفة بالبرمجيات، يستعرض أسباب اعتمادها، ويفصل آليات عملها.

الكلمات المفتاحية: الشبكات واسعة النطاق المعرفة بالبرمجيات، الشبكات واسعة النطاق، الشبكات التقليدية، شبكات الجيل القادم.

Abstract

The demand for large-scale connectivity between enterprise site-edge networks and central office or cloud data center networks has increased, leading to the development of SD-WAN solutions. SD-WAN optimizes the use of WAN links, addressing critical issues in managing hybrid WANs. They apply the benefits of SDN to enterprise networks and integrate elements of traditional and next-generation networks. This article defines the SD-WAN architecture, explores the reasons for its adoption, and details its operational mechanisms.

Keywords: Software Defined Wide Area Networking (SD-WAN), Wide Area Networks, Traditional Networks, Next Generation Networks (NGN).

Résumé

La demande de connectivité à grande échelle entre les réseaux de site-edge d'entreprise et les réseaux centraux a augmenté, menant au développement de solutions SD-WAN. Les SD-WAN optimisent l'utilisation des liens WAN, résolvant des problèmes critiques de gestion des WAN hybrides. Ils appliquent les avantages des SDN aux réseaux d'entreprise et intègrent des éléments de réseaux traditionnels et de nouvelle génération. Cet article définit l'architecture SD-WAN, explore les raisons de son adoption et détaille ses mécanismes opérationnels.

Mots-clés : Réseau étendu défini par logiciel (SD-WAN), Réseaux étendus, Réseaux traditionnels, Réseaux de nouvelle génération (NGN).

Introduction générale

Introduction générale

Les infrastructures WAN sont essentielles à chaque entité, indépendamment de sa nature ou de son secteur d'activité, pour le déploiement de leurs applications au-delà des centres de données ou des réseaux locaux. Jadis, ces mêmes entités devaient souscrire à des abonnements en lignes louées dédiées ou des liaisons commutées telles que le coûteux MPLS, dont la gestion, chronophage, exigeait la mobilisation de nombreux ingénieurs réseau, sécurité et supervision.

De plus, ces réseaux anciens, conçus entièrement sur des protocoles de routage dynamique, souffraient d'un manque de réactivité, étaient très limités en matière d'intelligence et n'exploitaient que partiellement le potentiel offert par les liens loués. C'est dans ce contexte particulier, marqué par le besoin d'amélioration, de dématérialisation, de simplification et de réduction des coûts des infrastructures WAN, que s'inscrit l'initiative SD-WAN. Le SD-WAN, ou « Software-Defined Wide Area Network », est présenté par Yves Pellemans, CTO d'Axians France, dans les années vingtaine du siècle actuel comme la nouvelle évolution majeure des télécommunications. Contrairement aux réseaux SDN, qui mettent en œuvre la virtualisation pour améliorer la gestion des centres de données, le SD-WAN permet aux entreprises de construire des WANs de meilleure performance en utilisant un accès internet moins coûteux et plus disponible. L'amélioration de la disponibilité et de la performance est obtenue grâce à de nouvelles fonctionnalités inédites, telles que le routage des flux par application au lieu des stratégies de routage par adresse de destination et l'équilibrage de charge dynamique sur des liens asymétriques.

La révolution SD-WAN ne se limite pas à une amélioration significative des performances ou de la disponibilité du WAN ; elle concrétise une réelle refonte des réseaux WAN par l'introduction du concept de programmabilité, de superposition des réseaux (Underlay et Overlay), la standardisation des mécanismes des plans de contrôle et des plans utilisateurs, et surtout par leur fonctionnement totalement automatisé et orchestré, nécessitant peu voire aucune intervention humaine.

Compte tenu du potentiel futur du SD-WAN, la plupart des constructeurs d'équipements réseau et de sécurité, ainsi que les éditeurs majeurs des plateformes de virtualisation comme Cisco, Huawei, Fortinet ... ont proposé des produits SD-WAN qui rencontrent déjà un franc succès. Toutefois, en dépit de l'engouement généralisé des entreprises et des constructeurs pour le SD-WAN, il reste essentiel d'évaluer les solutions disponibles pour choisir celle qui répond le mieux aux besoins spécifiques de chaque organisation. [17]

C’est donc dans ce cadre de complétude des fonctionnalités manquantes de notre projet que s’inscrit ce présent projet de master, à travers lequel nous implémentons le SD-WAN de Fortinet. La solution SD-WAN de Fortinet s'avère être une option supérieure pour les nouvelles entreprises, offrant une architecture moins complexe, plus efficace et mieux adaptée aux besoins modernes.

Pour bien présenter notre travail, notre mémoire sera structuré sur cinq parties, comme suit :

1. Le premier chapitre titré « Présentation de l’organisme », qui sera consacré à la présentation de l’organisme d’accueil « Banque d’Algérie ».
2. Le deuxième chapitre intitulé « Etat de l’art ». Ce chapitre aborde des généralités et des notions de base sur les réseaux informatiques.
3. Le troisième chapitre intitulé « Introduction au SDN » présente la définition et l’evolution des Sofware Defined Network, son architecture ainsi que le protocole OpenFlow, les contrôleurs SDN et les interfaces de communication.
4. Le quatrième chapitre intitulé « Etude de solution SD-WAN ». Ce chapitre comporte la définition et l’évolution du SD-WAN, son architecture, la différence entre WAN et SD-WAN et la relation entre MPLS et SD-WAN ainsi que son adoption par les différents constructeurs.
5. Le cinquième chapitre intitulé « Réalisation et implémentation ». Ce chapitre nous décrirons les détails d’architecture, les outils de simulation, les différentes configuration et l’implémentation du SD-WAN sur les Firewall Fortigate ainsi que les résultats.

Chapitre I

Généralités sur les réseaux informatique

Introduction

Ce chapitre explore les bases des réseaux de communication, leur architecture, leurs composants et leurs protocoles. Nous examinerons comment ces réseaux facilitent la transmission de données, de la voix et de la vidéo, ainsi que les défis et les tendances émergentes dans ce domaine en constante évolution.

I.1 Définition d'un réseau

Un réseau constitue un regroupement de deux équipements électroniques ou plus, interconnectés par divers moyens de transmission comme les câbles, les lignes téléphoniques, les ondes radio et même les satellites. Son dessein principal est de permettre l'échange et le partage de données ou de ressources entre ses composants. En effet, il se distingue par deux aspects fondamentaux : l'aspect physique et l'aspect logique. L'aspect physique, également connu sous le nom de hardware, représente l'ensemble des éléments matériels tels que les câbles, les cartes réseau et les commutateurs. D'autre part, l'aspect logique, ou software, est constitué de l'ensemble des logiciels et protocoles qui garantissent la communication et la transmission de données au sein du réseau. Cette combinaison entre les éléments matériels et les logiciels intelligents crée un système complexe où les échanges et les interactions prennent vie, permettant ainsi à la connectivité moderne d'atteindre de nouveaux sommets.

I.2 Les principaux équipements d'interconnexions

Les équipements réseau servent à interconnecter les équipements terminaux (hôtes) pour leur permettre de communiquer. Ils assurent le transport des données qui doivent être transférées entre les équipements hôtes (finaux). Ils sont utilisés pour étendre les connexions de câbles, concentrer les connexions et gérer les transferts de données.

- **Les répéteurs (Repeaters)**

Sont des dispositifs permettant d'étendre la distance de câblage d'un réseau local. Leur rôle consiste à amplifier et à répéter les signaux qui leurs parviennent. Il existe également des répéteurs qui en plus régénèrent les signaux. Ceci réduit le bruit et la distorsion. Le répéteur intervient au niveau 1 du modèle OSI.

- **Les Concentrateur (Hub)**

Les concentrateurs sont des appareils simples qui relient plusieurs appareils dans un réseau informatique. Ils amplifient les signaux sur de longues distances et transmettent des données à tous les

appareils connectés, sans effectuer de filtrage ou d'adressage de paquets. Les concentrateurs fonctionnent au niveau physique du modèle OSI et existent en deux types : à port simple et multiport.

- **Les commutateurs (Switches)**

Le commutateur réseau ou switch est un équipement qui relie plusieurs câbles ou fibres dans un réseau informatique. Il s'agit le plus souvent d'un boîtier disposant de plusieurs ports. Il a donc la même apparence qu'un concentrateur (hub). Contrairement à un concentrateur, un commutateur ne se contente pas de reproduire sur tous les ports chaque trame qu'il reçoit. Il sait déterminer sur quel port il doit envoyer une information, en fonction de l'ordinateur auquel elle est destinée.

- **Les Routeurs (Routers)**

Un routeur est un dispositif électronique qui opère au niveau de couches 3 du modèle OSI. Il permet de relier deux ou plusieurs réseaux entre eux permettant ainsi la communication entre des périphériques se trouvant sur des réseaux ou sous-réseaux différents ou sains d'un même réseau.

- **Les points d'accès (Access Point)**

Un point d'accès est un dispositif matériel dans un réseau sans fil qui permet aux appareils Wi-Fi, tels que les ordinateurs portables, les smartphones et les tablettes, de se connecter à un réseau câblé existant. Il reçoit les données sans fil transmises par les appareils et les transfère vers le réseau câblé.

- **Les pare-feu (Firewall)**

Un firewall est un appareil de sécurité réseau qui surveille le trafic réseau entrant et sortant et autorise ou bloque les paquets de donnés en se basant sur un ensemble de règles de sécurité. Il est chargé de dresser une barrière entre le réseau interne et le trafic entrant provenant de sources externes (comme Internet) afin de bloquer le trafic malveillant des virus et des pirates.

I.3 Les types des réseaux informatiques

On peut distinguer diffèrent types de réseaux selon leur taille leur vitesse de transfert des données et aussi leur entendu :

- **LAN (Local Area Network) ou réseau local**

Il s'agir d'un ensemble d'ordinateurs s'étendant sur quelques dizaines à quelques centaines de mètres, Il est couramment utilisé pour le partage de ressources communes, comme des périphériques, des données ou des applications. [2]

- **MAN (Metropolitan Area Network) ou réseau métropolitain**

Interconnectent plusieurs LAN géographiquement proche bien moins étendu qu'un WAN. Les MAN sont souvent utilisés par les fournisseurs d'accès Internet pour relier les centres de données ou par les administrateur/université qui ont besoin de connecter des sites géographiquement situés dans un périmètre relativement restent. [3]

- **WAN (Wide Area Network) ou réseau étendu**

Par opposition au LAN, est l'ensemble des équipements sur lesquels l'entreprise n'a pas un contrôle direct en tant qu'entité. D'un point de vue géographique, l'acronyme WAN désigne les réseaux des opérateurs Internet nettement plus grands que les réseaux d'entreprise. Elle peut se propager entre les villes, les pays ou même les continents. [3]

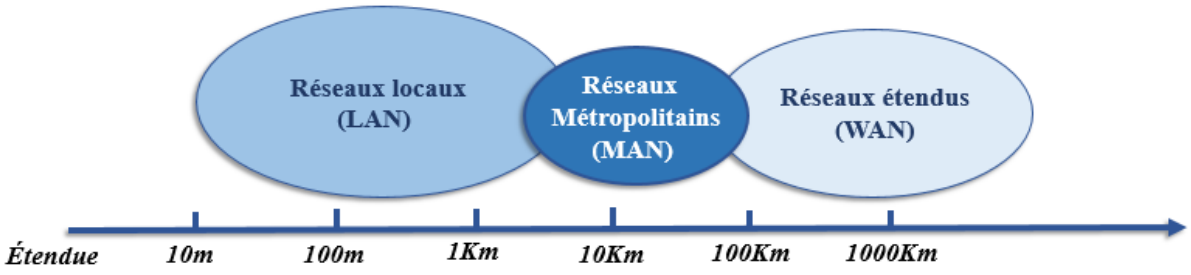


Figure I. 1- Les types des réseaux informatiques

I.4 Les modèles de communications

Des standards sont indispensables pour favoriser l'interopérabilité entre les équipements des fournisseurs et pour stimuler les économies d'échelle. Étant donné la complexité de la tâche de communication, une norme unique ne suffira pas. Au contraire, les fonctions devraient être décomposées en parties plus gérables et organisées sous forme d'architecture de communication. L'architecture constituerait alors le cadre de la normalisation. C'est ainsi que l'Organisation internationale de normalisation (ISO) a créé en 1977 un sous-comité chargé de développer une telle architecture. Le résultat a été le modèle de référence Open Systems Interconnexion (OSI). [4]

Cette architecture hiérarchique est constituée de sept couches distinctes, chacune remplissant une fonction spécifique nécessaire à l'interconnexion. Le modèle OSI définit des niveaux de transmission, mais ne spécifie pas les protocoles eux-mêmes. Il divise l'ensemble des protocoles en sept couches indépendantes, avec deux types de relations définies : les relations verticales entre les couches d'un même système (interfaces) et les relations horizontales liées aux échanges entre deux couches du même niveau (les protocoles). [5]

Entre-temps, un modèle architectural quelque peu différent a émergé du développement des protocoles basés sur Internet et porte le nom de modèle TCP/IP. Grâce aux avancées rapides dans le développement de protocoles au sein du modèle TCP/IP et à leur déploiement par de nombreux fournisseurs, TCP/IP s'est établi comme le modèle "pratique" pour les protocoles de communication.[4]

TCP/IP est généralement utilisé pour désigner une architecture réseau, mais en réalité, il s'agit de deux protocoles étroitement liés : le protocole de transport TCP (Transmission Control Protocol) et le protocole réseau IP (Internet Protocol). Le "modèle TCP/IP" se réfère à une architecture réseau en 4 couches où les protocoles TCP et IP jouent un rôle prédominant en tant qu'implémentation la plus courante. [6]. La figure montre les différentes couches des deux modèles.

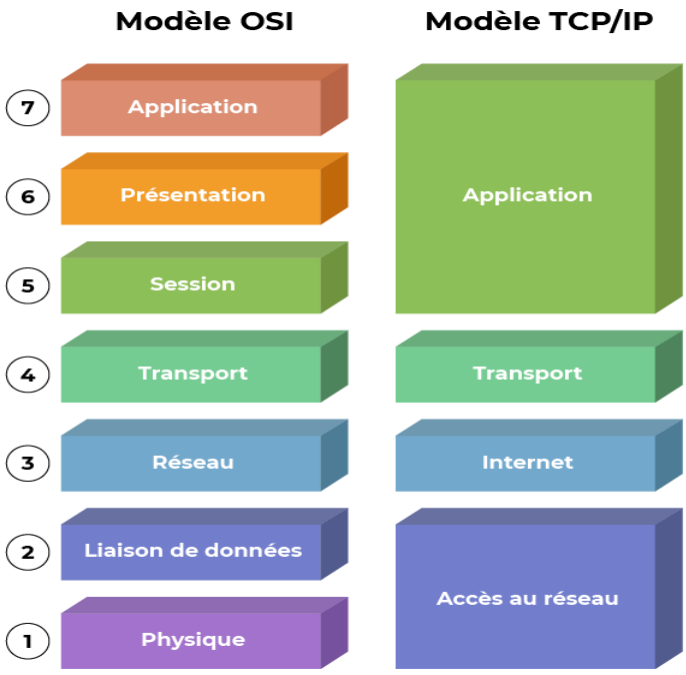


Figure I. 2- Les modèles OSI et TCP/IP

I.5 Les réseaux informatiques traditionnels

I.5.1 Qu'est-ce qu'un réseau traditionnel ?

Le réseau traditionnel fait référence à l'ancienne méthode conventionnelle de mise en réseau qui utilise des dispositifs matériels fixes et dédiés tels que les routeurs et les commutateurs pour contrôler le trafic du réseau qui ont sur une topologie physique prédéterminée, comme le

bus, l'anneau ou l'étoile. Dans un réseau en bus, tous les équipements sont reliés à une ligne de communication principale. Dans un réseau en étoile, chaque équipement est connecté à un commutateur central ou à un concentrateur. Ces dispositifs nécessitent souvent une configuration manuelle par des administrateurs réseau pour effectuer des modifications.

Les réseaux classiques se servaient couramment de protocoles et de technologies standardisés, comme le protocole Ethernet pour la communication sur les réseaux locaux câblés, connue par la norme IEEE 802.3 et basé sur le principe que toutes les machines de réseau sont connectées à une même ligne de communication.

Les réseaux classiques exigeaient des mesures de sécurité telles que des pares-feux pour filtrer les données entrants et sortants, des contrôles d'accès et des ACL afin de limiter et protéger l'accès aux ressources réseau aux utilisateurs autorisés.

I.5.2 Architecture d'un réseau traditionnel

Dans les réseaux traditionnels, l'architecture est généralement conçue de manière hiérarchique, avec différentes couches de dispositifs réseau interconnectés pour assurer la connectivité et la gestion efficace du trafic.

- **La Couche d'accès :** Il s'agit du point d'entrée permettant aux appareils des utilisateurs (tels que les ordinateurs, les téléphones portables, les imprimantes, etc.) d'accéder au réseau. Cette couche est responsable de fournir l'accès aux utilisateurs, l'authentification, les politiques de sécurité et d'autres fonctions, tout en traitant également le trafic local. Les commutateurs jouent un rôle essentiel dans cette couche, en connectant les appareils des utilisateurs au réseau.
- **La couche de distribution** : elle se trouve entre la couche d'accès et la couche principale. Elle assure la connexion des sous-réseaux de la couche d'accès. À ce niveau, le trafic est regroupé, filtré et réparti entre les secteurs à l'aide de la technologie VLAN.
- **La couche centrale (Core)** : elle est le pilier du réseau, assurant la transmission des données et l'échange de trafic à haut débit. Elle relie les différentes couches d'agrégation et garantit une disponibilité et une redondance élevées du réseau. La couche centrale doit se distinguer par sa bande passante élevée, sa faible latence et sa haute disponibilité. [W2]

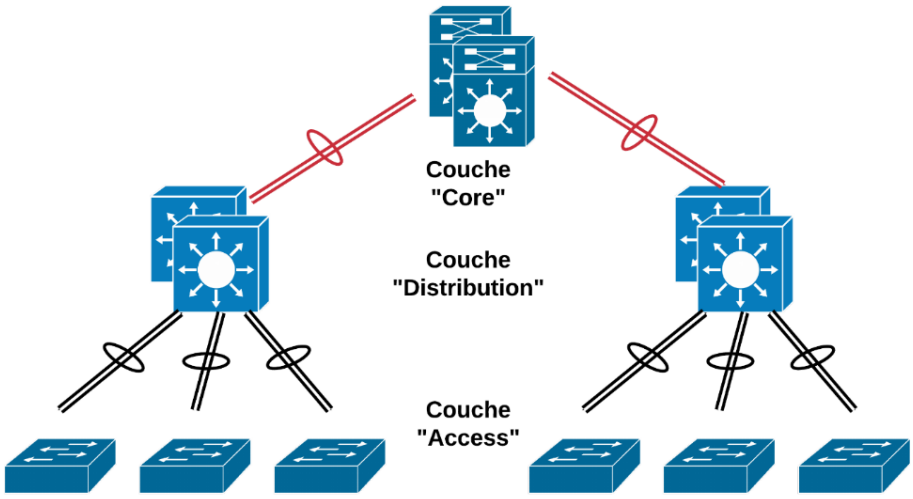


Figure I. 3- Les trois différentes couches du réseau hiératique

Les réseaux traditionnels regroupent généralement les plans de contrôle et de données dans un même équipement, tel que les routeurs et les commutateurs Cela implique que les décisions de routage et de commutation des paquets, ainsi que les opérations de transfert effectif des données, sont toutes réalisées par le même équipement.

- **Plan de contrôle (Control Plane) :**

  Le plan de contrôle est un composant essentiel d'un réseau, chargé de prendre des décisions sur la manière dont les données doivent être gérées, routés et traitées. Il joue le rôle de superviseur des données, en coordonnant la communication entre les différents composants et en collectant les données du plan de données. Ils utilisent des protocoles spécifiques pour communiquer, notamment des protocoles de routage comme BGP (Border Gateway Protocol), OSPF (Open Shortest Path First) et IS-IS (Intermediate System to Intermediate System), SNMP (Simple Network Management Protocol), qui permettent au plan de contrôle de prendre des décisions sur la manière dont les données doivent être gérées, acheminées et traitées [W4]

- **Plan de données (Data Plane) :**

Le plan de données assure le transfert effectif des données d'un système à un autre. Il s'agit du pilier central qui permet l'échange de données entre les utilisateurs finaux et les systèmes, dans les deux sens. Il se charge de transmettre les paquets de données d'un appareil source à un appareil de destination, en suivant les itinéraires définis par le plan de contrôle.

En général, les plans de données utilisent le protocole TCP (Transmission Control Protocol) pour assurer une transmission fiable des données en établissant des connexions entre les dispositifs. Cela garantit que les données sont correctement reçues et dans le bon ordre. Cependant, dans les applications où la vitesse de transmission est plus importante que la fiabilité, le protocole UDP (User Datagram Protocol) est utilisé. Contrairement au TCP, l'UDP n'offre pas de garantie de livraison des données ni d'ordre d'arrivée, mais il permet une transmission plus rapide et moins gourmande en ressources. [W4]

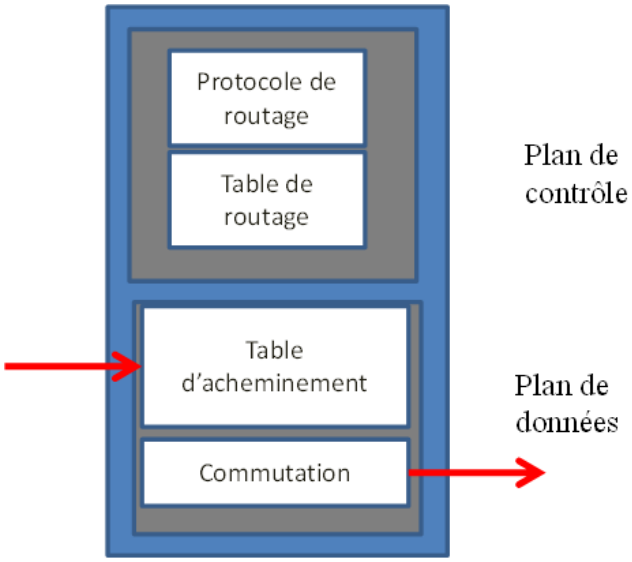


Figure I. 4- Architecture des réseaux traditionnels

I.6 Les réseaux de nouvelle génération (NGN)

I.6.1 Qu'est-ce qu'un réseau NGN

Les NGN sont des réseaux de transport en mode paquet qui permettent la convergence des réseaux Voix/Données et Fixe/Mobile, offrant ainsi des services multimédias accessibles depuis divers réseaux d'accès. Pour répondre aux grandes tendances telles que la flexibilité de l'évolution du réseau, la distribution de l'intelligence dans le réseau et l'ouverture aux services tiers, les NGN évoluent progressivement vers le "tout IP" et sont structurés en couches indépendantes interagissant via des interfaces ouvertes et normalisées.

I.6.2 Architecture des réseaux NGN

La transition vers une architecture NGN se distingue particulièrement par la séparation des fonctions de commutation physique et de contrôle d'appel. L'architecture NGN met en place un modèle en couches qui sépare les fonctions et équipements impliqués dans le transport du

trafic et du contrôle. Un modèle architectural basé sur cinq couches successives peut être défini :

- **La couche d'accès :** elle gère l'accès des équipements utilisateurs au réseau en fonction de la technologie d'accès. Elle comprend les équipements DSLAM pour l'accès DSL.
- **La couche de transport :** elle assure le routage du trafic voix ou données dans le cœur du réseau. La passerelle multimédia (MGW) adapte les protocoles de transport aux différents types de réseaux physiques.
- **La couche de contrôle** : elle gère les fonctions de contrôle des services, notamment le contrôle des appels pour le service voix. Le serveur d'appel, ou "softswitch", fournit l'équivalent de la fonction de commutation dans un réseau NGN.
- **La couche de services :** elle fournit les services dans un réseau NGN. Elle comprend les serveurs d'application et les "enablers" qui sont des fonctionnalités utilisées par plusieurs applications. Cette couche inclut généralement des serveurs d'application SIP pour gérer des sessions multimédias et des services de voix sur IP.
- **La couche applications** : cette couche regroupe les services et applications offerts dans une architecture NGN, y compris les services IP et les services vocaux existants du réseau intelligent. Elle comprend également l'environnement de création de services ouvert aux fournisseurs tiers. Le développement d'applications repose sur les serveurs d'application et les enablers de la couche d'exécution des services.

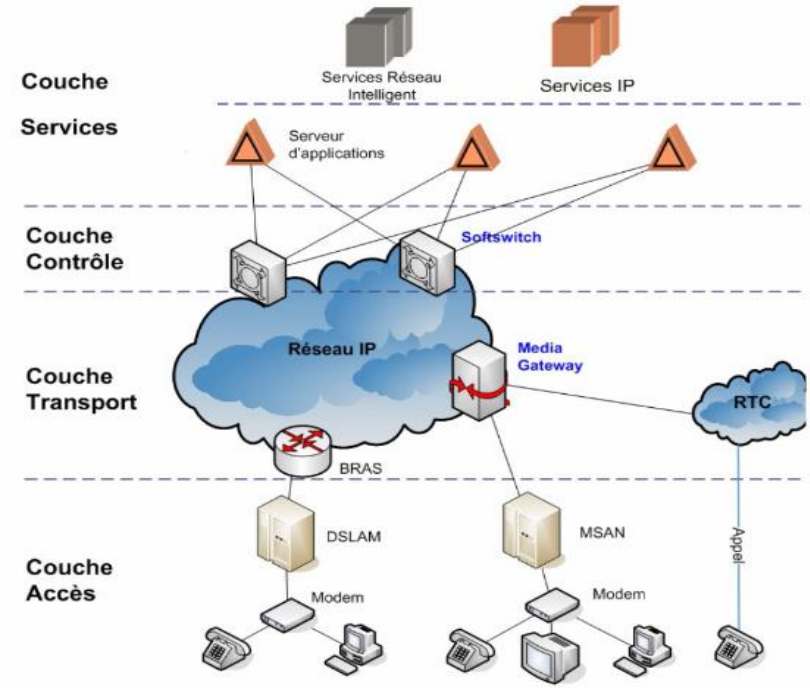


Figure I. 5- Architecture des réseaux NGN

La dissociation du contrôle et de la partie transport dans la couche de contrôle est cruciale. En séparant ses fonctions, les réseaux de nouvelle génération peuvent gérer plus efficacement les services et les flux de données. Cette séparation permet une gestion dynamique des services. Facilitant la modification des politiques de contrôle sans perturber le flux de données. Ainsi, cette association renforce la flexibilité et l'efficacité des opérations réseau, offrant une architecture évolutive pour répondre aux besoins changeants des services de. Communication moderne. [W6]

I.6.3 Les protocoles des réseaux NGN

Dans l'univers des télécommunications contemporaines, les protocoles de réseau jouent un rôle essentiel dans la prestation de services de communication avancés et fiables. Les réseaux de nouvelle génération (NGN) symbolisent la progression technologique des infrastructures de télécommunications, en intégrant des protocoles sophistiqués afin de répondre aux demandes grandissantes en termes de bande passante, de qualité de service et de diversité des services proposés.

- **Multiprotocol Label Switching (MPLS)**

Dans les réseaux informatiques traditionnels, les routeurs sont confrontés à un défi majeur : ils doivent acheminer les paquets de données en se basant uniquement sur les adresses IP de destination, ce qui entraîne une inefficacité dans la gestion du trafic. Cette limitation est due au protocole BGP. Afin d'optimiser les chemins empruntés, il est nécessaire de trouver des solutions pour pallier cette limitation.

Le MPLS utilise des "labels" pour acheminer efficacement les paquets de données vers des routeurs de la même classe. Seuls les routeurs de départ et d'arrivée ont besoin de connaître les informations sur la destination, ce qui permet une gestion efficace du trafic. Cette approche permet au réseau MPLS de traiter les paquets en fonction de leurs caractéristiques spécifiques, comme l'origine, le type d'application ou la qualité de service requise.

Le protocole MPLS suit un processus en quatre étapes pour acheminer de manière efficace les paquets de données à travers le réseau. La première étape consiste à attribuer des étiquettes aux paquets dès leur entrée dans le réseau, permettant aux routeurs MPLS de les identifier et de les traiter efficacement. En utilisant ces étiquettes, les routeurs déterminent le chemin optimal pour chaque paquet, assurant une transmission rapide et évitant les problèmes de congestion. Une fois les paquets arrivés à destination, les étiquettes sont retirées avant d'être transférés sur le réseau public. Ce processus permet une transmission efficace des données et une intégration transparente avec les réseaux publics. [W7]

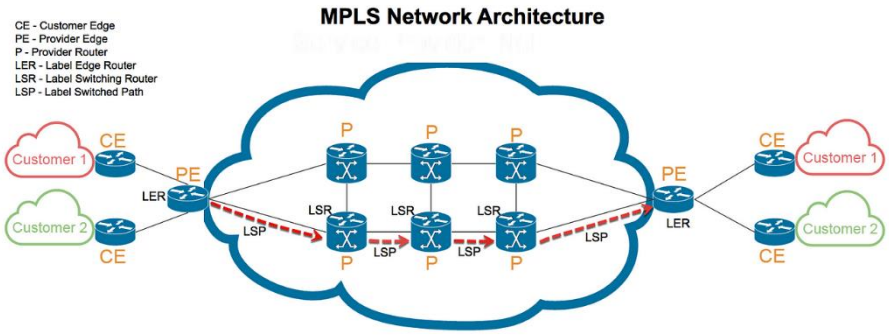


Figure I. 6- Architecture MPLS

- **PPP (point to point)**

C'est un protocole de transmission Internet qui établit une connexion entre deux hôtes sur une liaison point à point, faisant partie de la couche liaison de données du modèle OSI. Son but est de remplacer le protocole SLIP en offrant plus de flexibilité et de fiabilité pour les connexions à distance. Il utilise une séquence d'initialisation pour établir la connexion, impliquant l'envoi et la réception de paquets de données pour vérifier la qualité de la connexion et configurer les paramètres de liaison. Une fois la connexion établie, PPP peut transmettre des données à la vitesse maximale de la liaison série.

PPP offre également des fonctionnalités de compression de données et de détection d'erreurs pour améliorer la qualité de la transmission des données. Il peut être utilisé avec des protocoles de sécurité comme PAP et CHAP pour authentifier les utilisateurs distants. [W8]

- **HDLC (High-level Data Link Control)**

Le protocole HDLC (High-level Data Link Control) est un protocole de communication développé par l'Organisation internationale de normalisation (ISO) pour la transmission, la réception et le contrôle des données sur les réseaux de télécommunications. Il assure la sécurité, l'intégrité et la synchronisation des données entre l'émetteur et le destinataire. Utilisé dans diverses applications comme les réseaux locaux (LAN), les réseaux étendus (WAN) et les systèmes de transmission longue distance, le HDLC est compatible avec différents supports de transmission, tels que la fibre optique, le câble en cuivre et la radiofréquence. [W9]

I.6.4 Les méthodes et les technologies de communication

Ce sont les techniques utilisées pour établir une connexion entre les équipements d'un réseau NGN et qui facilitent la communication et l'échange de données entre différents systèmes. Ils permettent la transmission de signaux, de données ou d'énergie en fournissant les moyens

nécessaires pour des connexions fiables et efficaces. Parmi ces méthodes et ces technologies les plus couramment utilisés, on trouve :

- **Lignes spécialisées :** Les lignes spécialisées sont des connexions dédiées entre deux points qui offrent une bande passante garantie et une qualité de service constante. Elles peuvent être utilisées pour connecter des sites distants, des centres de données ou des points d'accès à Internet. Les lignes spécialisées comprennent des technologies telles que les lignes T1, T3, E1 et E3, qui fournissent des débits de données fixes et des garanties de service. [W10]
- **IP/MPLS :** IP/MPLS est une technologie de pointe largement utilisée dans les réseaux de télécommunications pour améliorer l'efficacité et la fiabilité des communications. En combinant les avantages de MPLS avec les fonctionnalités de routage de l'IP traditionnel, IP/MPLS offre une solution puissante pour la commutation de paquets. En utilisant des étiquettes MPLS, IP/MPLS permet une commutation plus efficace du trafic en créant des chemins définis par les étiquettes, ce qui réduit la latence et offre une qualité de service différenciée pour différents types de trafic. En tant que support d'interconnexion, IP/MPLS relie de manière fiable et sécurisée divers sites, réseaux et fournisseurs de services, facilitant ainsi la connectivité et la communication entre les différents éléments du réseau.
- **Connexion par satellite (VSAT) :** Le VSAT (Very Small Aperture Terminal) est un équipement de télécommunication par satellite permettant de connecter les réseaux terrestres en utilisant des satellites géostationnaires pour émettre et recevoir des données. La technologie VSAT a favorisé le développement de réseaux multi-technologies à grande échelle, facilitant le transfert de données, la téléphonie, l'Internet et diverses transactions d'entreprise. Le VSAT utilise une antenne de 1m à 3,7m et permet une liaison directe entre une station cliente et un système central. Il est crucial pour interconnecter des sites distants avec le site principal pour des services comme la visioconférence, la téléphonie et les données. [W11]
- **VPN :** Virtuel private network (réseau privé virtuel) permet à des sites distants de communiquer de manière sécurisée via Internet en utilisant la cryptographie et la tunnelisation. Les données sont chiffrées et encapsulées avant transmission, assurant confidentialité, authenticité et intégrité. Le VPN utilise un protocole de tunnelisation pour transmettre des données cryptées. Lorsqu'un utilisateur se connecte, sa requête est envoyée en clair à la passerelle, puis transmise cryptée au réseau distant. Les données

sont déchiffrées et transmises à l'utilisateur. Toutes les données passent par le même portail pour gérer la sécurité des accès et le trafic. [7].

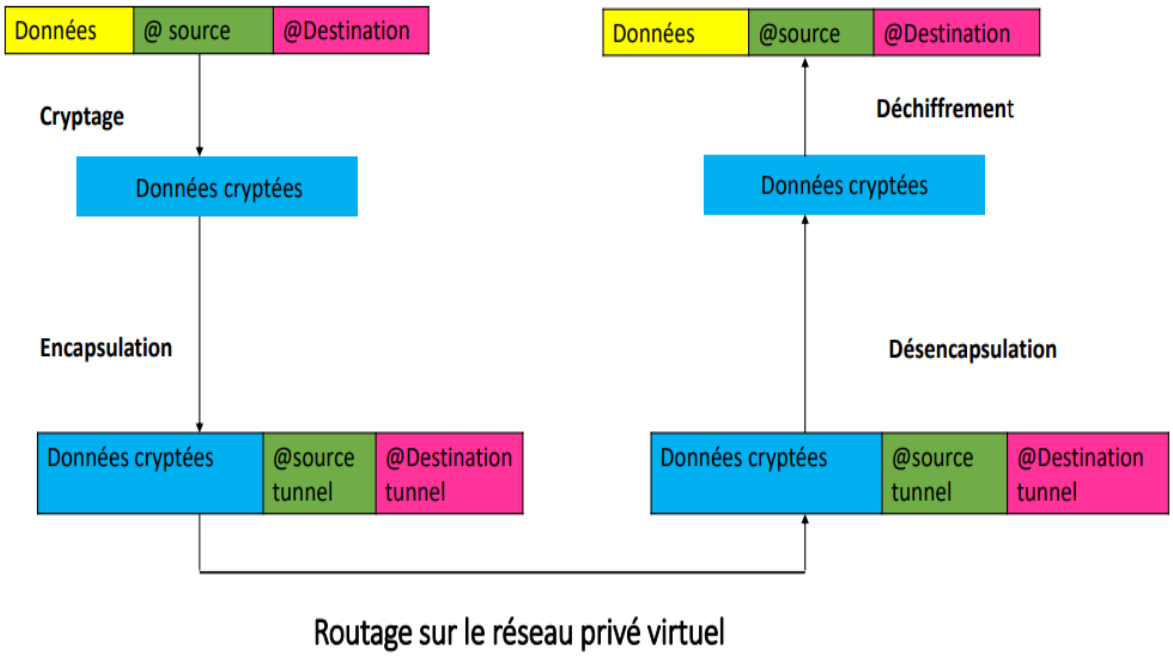


Figure II. 7- Fonctionnement du VPN

I.7 Comparaison entre les réseaux traditionnels et les réseaux NGN

Le tableau II.1 montre une comparaison entre les réseaux traditionnels et les réseaux de nouvelles génération (NGN).

Tableau I. 1- Caractéristiques des réseaux traditionnels et réseaux NGN

Caractéristique	Réseaux NGN	Réseaux Traditionnels
Architecture	Basée sur des technologies numériques et des protocoles IP/MPLS.	Basée sur des infrastructures analogiques et des protocoles spécifiques à chaque service (ex : commutation du circuit).
Flexibilité	Plus grande flexibilité pour prendre en charge une variété de services de communication.	Moins de flexibilité en raison de l'architecture et des protocoles spécialisés pour chaque service.
Évolutivité	Facilité d'évolutivité pour répondre à la demande croissante de bande passante et de nouveaux services, grâce à une architecture basée sur IP et à une virtualisation des fonctions réseau (NFV).	L'évolutivité peut être limitée en raison de la nécessité de mettre à niveau ou de remplacer physiquement les équipements pour prendre en charge de nouvelles technologies ou services.
Gestion des ressources	Gestion centralisée et automatisée des ressources réseau, permettant une allocation plus efficace des capacités et une optimisation des performances.	Gestion plus complexe et décentralisée des ressources, avec souvent des configurations manuelles et des interventions humaines pour les ajustements et les réparations.
Coût opérationnel	Potentiellement des coûts opérationnels plus bas grâce à l'automatisation, à la virtualisation et à la consolidation des fonctions réseau.	Les coûts opérationnels peuvent être plus élevés en raison de la nécessité de maintenir des réseaux distincts pour différents types de services, ainsi que de la gestion manuelle des ressources et des configurations.
Fiabilité	Amélioration de la fiabilité grâce à la redondance, à la résilience et à la répartition de charge intégrées dans les architectures NGN, ainsi qu'à la capacité de détection et de récupération automatiques des pannes.	La fiabilité peut varier en fonction de la qualité et de l'âge des équipements, ainsi que de la complexité des réseaux hérités, avec des temps de récupération potentiellement plus longs en cas de panne.

I.8 Les réseaux underlay et overlay

Avec l'évolution continue de la technologie, les entreprises cherchent constamment des moyens d'optimiser leur infrastructure réseau. L'une des façons les plus efficaces de le faire est la virtualisation réseau. La virtualisation réseau consiste à créer une version virtuelle d'un réseau, permettant aux administrateurs de gérer et d'optimiser les ressources réseau de manière plus efficace. Il existe deux composants clés de la virtualisation réseau : les réseaux de superposition (overlay network) et les réseaux sous-jacents (Underlay network).

I.8.1 Réseau Underlay (Underlay Network)

Un réseau sous-jacent est l'infrastructure physique qui soutient les réseaux de superposition. Comme illustré dans la figure II.8, il s'agit d'un réseau physique composé de divers types d'appareils, chargé de transmettre les paquets de données entre les différents réseaux.

L'infrastructure sous-jacente (Underlay) est essentielle pour assurer le bon fonctionnement du réseau virtuel. Elle est composée de différents éléments tels que les commutateurs, les routeurs et d'autres équipements de réseau qui permettent le transport des paquets de données entre les appareils physiques. La principale fonction de cette infrastructure est de transférer les données de manière rapide et efficace, en minimisant la latence et en maximisant les performances.

Pour atteindre cet objectif, des protocoles de routage traditionnels tels que OSPF (Open Shortest Path First) et BGP (Border Gateway Protocol) sont utilisés. Ces protocoles permettent de déterminer le chemin le plus court entre les appareils, ce qui contribue à améliorer encore les performances du réseau. Grâce à ces protocoles, les données peuvent être acheminées de manière optimale, en évitant les congestions et en assurant une livraison rapide. [W12]

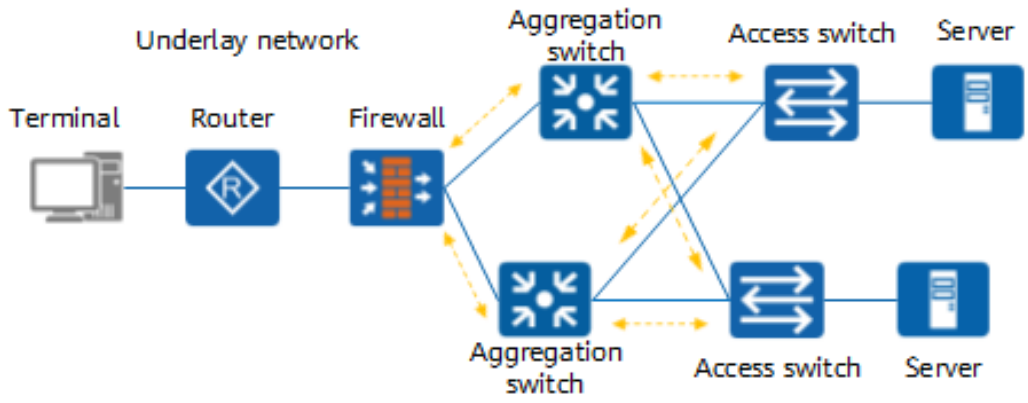


Figure I. 8- Architecture du réseau Underlay

I.8.2 Réseau Overlay (Overlay Network)

Un réseau superposé est un réseau virtuel flexible et évolutif créé au-dessus d'un réseau sous-jacent. Il permet aux administrateurs de configurer des réseaux virtuels en encapsulant les données avec des en-têtes supplémentaires. Cela permet de créer des réseaux virtuels indépendants de la topologie physique, facilitant la gestion des environnements de centre de données complexes. Le réseau superposé peut être utilisé pour isoler le trafic, créer des topologies personnalisées et assurer une connectivité sécurisée entre différents départements.

- Les appareils sur les réseaux superposés sont interconnectés via des liens logiques, formant des topologies superposées. Des tunnels sont établis entre ces appareils pour transmettre les paquets de données. Lors de l'envoi d'un paquet, un appareil ajoute un nouvel en-tête IP et un en-tête de tunnel, masquant l'en-tête IP interne. Le paquet est ensuite transmis en fonction du nouvel en-tête IP. Lorsqu'il est reçu par un autre appareil, celui-ci supprime les en-têtes externes et de tunnel pour obtenir le paquet d'origine. Le réseau superposé est ainsi indépendant du réseau sous-jacent. Les réseaux superposés prennent en charge divers protocoles et normes réseau, tels que VXLAN, NVGRE, SST, GRE, NVO3 et EVPN. [W12]

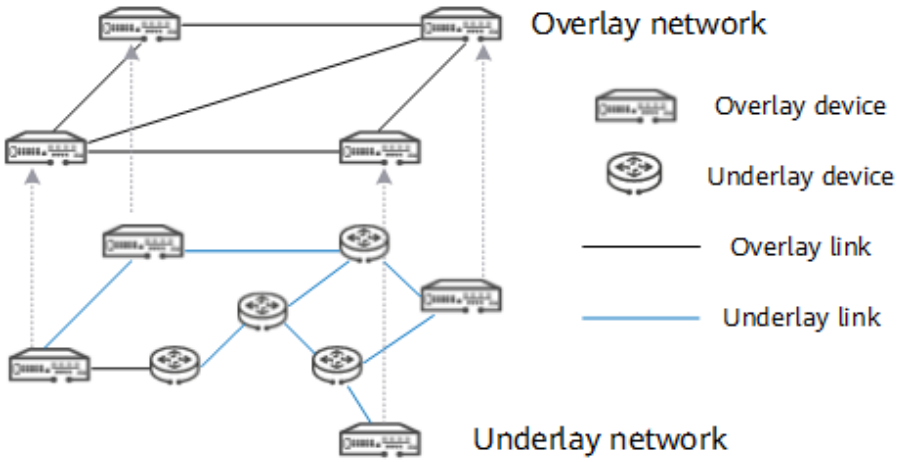


Figure I. 9- Architecture réseau Overlay

I.9 Réseau Multimesh

Un réseau maillé (mesh) est un type de réseau où les dispositifs, ou nœuds, sont connectés de manière que certains, voire tous, aient plusieurs chemins vers d'autres nœuds, assurant ainsi la redondance et la résilience du réseau en cas de défaillance. Dans un maillage complet, chaque nœud est directement connecté à tous les autres nœuds, tandis que dans un maillage partiel,

seuls certains nœuds ont des connexions multiples. Le choix des nœuds à relier dépend de divers facteurs tels que le schéma de trafic et le risque de défaillance.

La figure II. 10 montre une représentation graphique un réseau maillé partiel composé de six nœuds. Les connexions d'un réseau complet ou partiel peuvent être filaires ou sans fil.

Le réseau multimesh est une évolution du concept de réseau mesh, où plusieurs maillages sont interconnectés pour former un réseau plus étendu et complexe. Chaque maillage est considéré comme une entité autonome avec ses propres nœuds et connexions, puis ces maillages sont reliés les uns aux autres pour permettre une communication entre eux. Les réseaux multimesh sont utilisés dans des situations nécessitant une connectivité étendue entre des zones géographiquement dispersées, tout en conservant la redondance et la résilience propres aux réseaux mesh.

Les réseaux multimesh offrent une connectivité étendue, une redondance élevée et une résilience exceptionnelle grâce à leur architecture décentralisée et auto-organisatrice. Ils permettent une flexibilité sans précédent dans la conception, le déploiement et la gestion des réseaux, tout en offrant une performance optimale et une efficacité opérationnelle accrue. Ils sont bien positionnés pour relever les défis futurs des communications réseau grâce à leur capacité à s'adapter aux environnements changeants et à optimiser l'utilisation des ressources disponibles. [W13]

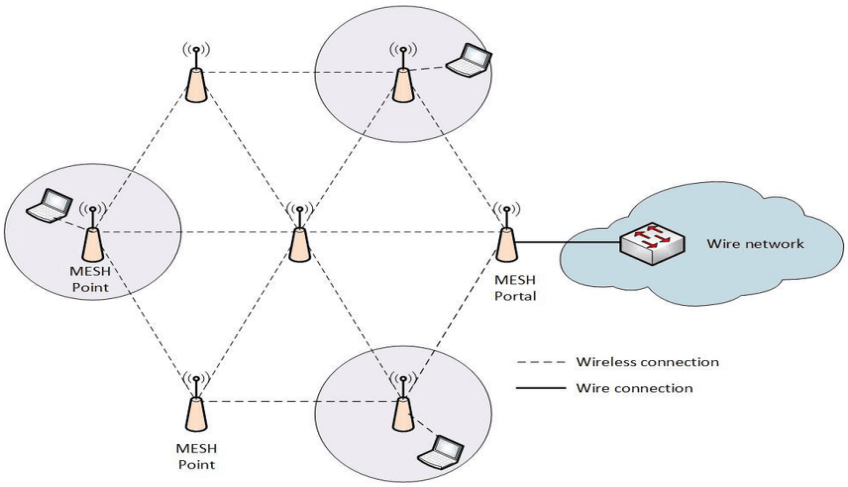


Figure I. 10- Réseau maillé partiel composé de six nœuds

Conclusion

En conclusions, ce chapitre a été introduit afin de mieux appréhender quelques généralités sur les réseaux informatiques, soulignant ainsi l'importance de maîtriser les concepts fondamentaux de ces réseaux pour garantir la qualité de notre travail.

Chapitre II

Introduction au SDN

Introduction

Dans ces dernières années Les réseaux informatiques traditionnels ont connu de grands défis liés aux applications modernes et à l'augmentation du nombre d'utilisateurs et d'appareils. Les réseaux définis par logiciels ou Software Defined Network (SDN) se sont imposés comme une solution pour répondre à la nature dynamique des applications en centralisant la gestion logique dans des contrôleurs. Un paradigme qui vient perturber le domaine du réseau en promettant de changer notre perspective de l'infrastructure.

Dans ce chapitre nous allons voire c'est quoi un SDN en revenant à la source de son évolution, comprendre son principe de fonctionnement et son architecture. Ensuite nous nous étalerons sur le principe d'Openflow et de leurs éléments.

II.1Terminologie et définition

Le terme SDN a été inventé à l'origine pour représenter les idées et le travail d'OpenFlow à l'Université de Stanford à Stanford en Californie, USA. Tel que défini initialement, le SDN fait référence à une architecture réseau dans laquelle l'état de transmission dans le plan de données est géré à distance par un plan de contrôle découplé du précédent. La logique du SDN rassemble les plans de contrôle de plusieurs périphériques en un seul logiciel externe appelé "Contrôleur". Le contrôle est déplacé vers un contrôleur SDN centralisé, prenant des décisions sur la manière dont le trafic doit être acheminé, tandis que les commutateurs et routeurs dans le plan de données sont déchargés de cette responsabilité et exécutent simplement les instructions du contrôleur via des protocoles tels qu'OpenFlow. Les contrôleurs offrent une vision globale du réseau, ce qui permet de gérer l'infrastructure à travers des interfaces de communication appelées APIs.[8]

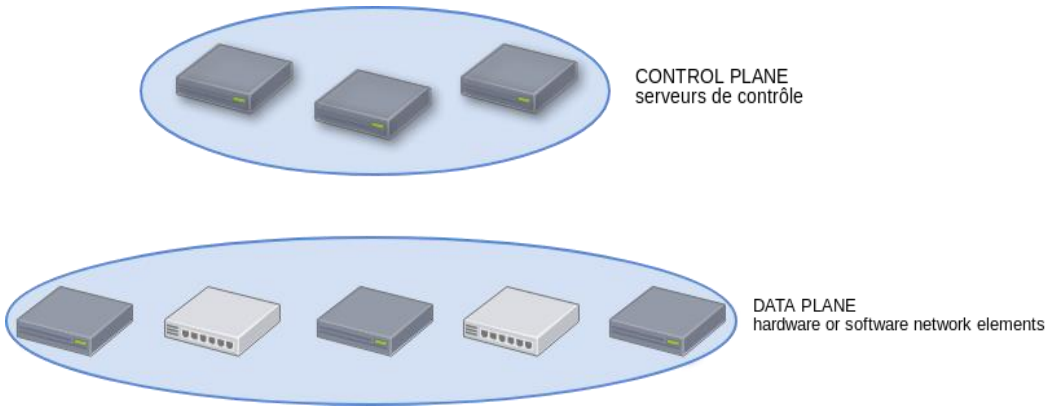
II.2 Historique et Evolution

Le Software Defined Networking, ou SDN, a émergé au début des années 2000, en réponse à l'augmentation du trafic réseau qui mettait en évidence les limites des systèmes traditionnels. Le SDN a apporté une approche novatrice en matière de gestion des réseaux, offrant ainsi une flexibilité et une adaptation accrues. Cette évolution a marqué un passage de la gestion réseau traditionnelle à une approche plus moderne, ouvrant ainsi la voie à de nombreuses nouvelles possibilités. Avec le temps, le SDN a bénéficié de nombreuses améliorations grâce aux progrès technologiques et aux collaborations entre les différents acteurs de domaine. Chaque

amélioration a contribué à faire du SDN une solution privilégiée pour les entreprises cherchant à moderniser leur gestion réseau. [W14]

II.3 Principe de fonctionnement

L'approche SDN consiste à séparer le plan de contrôle du plan de transmission. Le plan de contrôle est centralisé et mutualisé entre tous les équipements, tandis que le plan de transmission est limité à la fonction de transmission des données. Les serveurs chargés de fournir le plan de contrôle de la solution SDN sont généralement appelés contrôleurs SDN qui ont une vision globale de l'infrastructure en temps réel, ce qui leur permet de prendre des décisions qui impactent l'ensemble du réseau. Cette approche offre une grande flexibilité dans l'allocation des ressources et permet de proposer une large gamme de services aux clients. [W15]



FigureII. 1- Principe du SDN

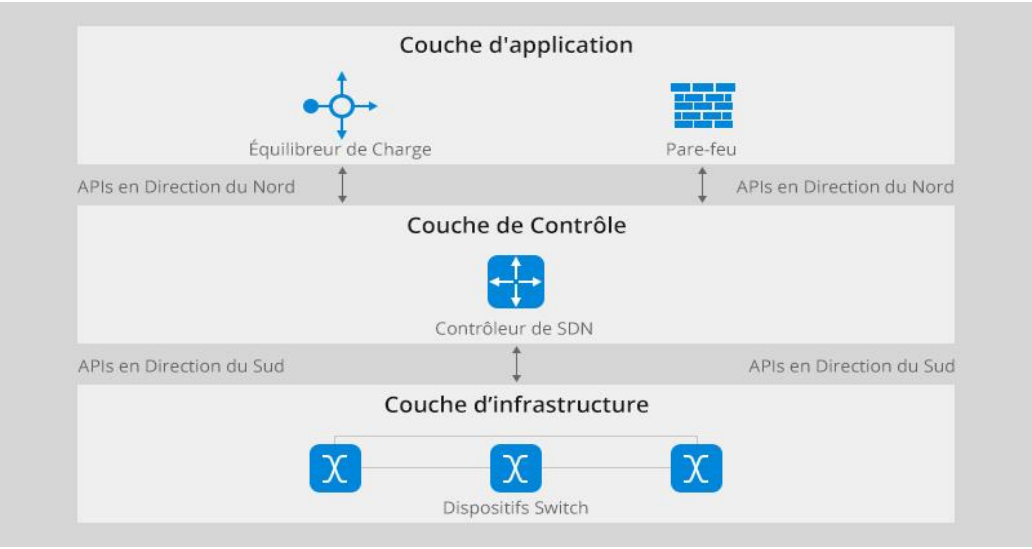
II.4 Architecture du SDN

L'Open Networking Fondation définit une architecture de haut niveau pour SDN avec trois couches principales. L'ONF propose un modèle de référence pour le SDN qui se compose de trois couches : la première est l'infrastructure, la deuxième est le contrôle et la troisième est l'application, communiquant entre elles par le biais d'interfaces APIs (comme le montre la Figure II.2)

- **La couche infrastructure (Data Plan) :** La première couche du modèle de référence pour le SDN est principalement composée d'équipements physiques ou virtuels, tels que les switchs et les routeurs. Ces équipements sont responsables de la gestion du trafic au sein du réseau. Leur rôle principal est de recueillir les informations sur le réseau, telles que la topologie actuelle, les statistiques de trafic et la densité d'utilisation, et de les transmettre au contrôleur. Ils sont également chargés de traiter les paquets en

fonction des règles de gestion fournies par le contrôleur. Les équipements physiques sont connectés les uns aux autres via différents supports de transmission, tels que les câbles en cuivre, la fibre optique ou les liaisons par faisceaux hertziens. Enfin, ils sont responsables de l'acheminement, de la fragmentation et du réassemblage des paquets de données. Un dispositif de transmission compatible OpenFlow repose sur un pipeline de tables de flux où chaque entrée comporte trois parties : une règle de correspondance, des actions à exécuter sur les paquets correspondants et des compteurs qui enregistrent des statistiques sur ces paquets. [9] [W15]

- **La couche de contrôle (Control Plan) :** C'est le cerveau du réseau qui englobe la plupart des opérations de calcul. La couche de contrôle s'appuie sur le contrôleur SDN et c'est une couche logicielle permettant de contrôler l'infrastructure en établissant des règles à respecter. Elle connecte l'infrastructure réseau à la couche application via deux interfaces. L'interface sud (interface South-Bound) permet d'importer les règles de transmission des paquets depuis le contrôleur, d'envoyer l'état du réseau et de prendre en charge le protocole OpenFlow, qui agit directement sur le plan de données. Elle est également responsable de la mise en place des tables de routage. L'interface nord (North-Bound interface) permet aux applications d'accéder aux données des switchs et de définir les règles de transfert de paquets via des API. [9] [10] [W15]
- **La couche application** : Cette couche contient des programmes qui transmettent des instructions spécifiques au contrôleur SDN. Cela donne la possibilité aux administrateurs de configurer, gérer, sécuriser et optimiser les ressources du réseau via ces applications.[9][10]



FigureII. 2- Architecture du SDN

II.5 L'OpenFlow

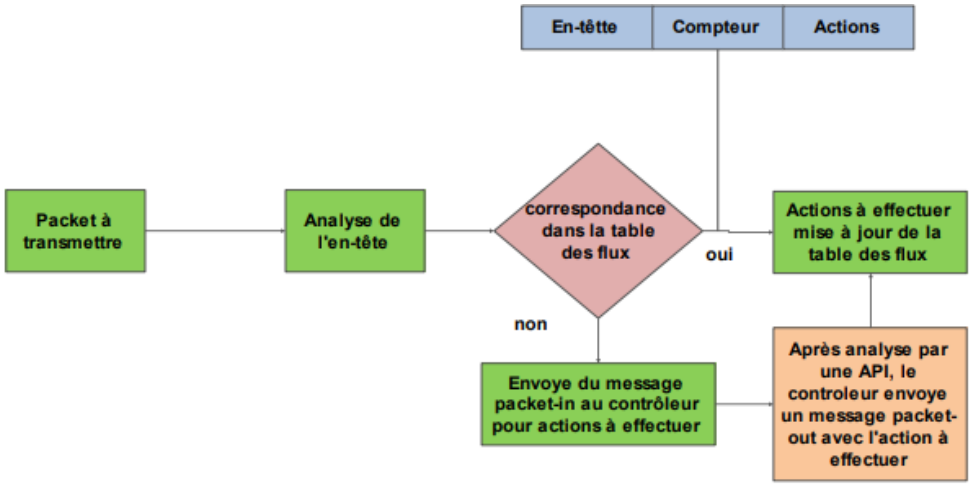
OpenFlow représente une spécification développée par l'Open Networking Foundation (ONF) qui établit une infrastructure de commutation basée sur les flux ainsi qu'une interface de programmation normalisée pour les applications. Il s'agit d'un standard ouvert qui permet de gérer le trafic et de tester des protocoles au sein d'un réseau existant en faisant appel à un contrôleur. En recourant à OpenFlow, il est réalisable de contrôler les chemins du trafic à travers un réseau en créant, éliminant et modifiant les flux dans chaque dispositif.[11][12]

II.5.1 Fonctionnement d'OpenFlow

OpenFlow établit un lien entre le plan de contrôle et le plan de données. Les messages sont échangés lors d'une session TCP établie via le port 6653 du serveur contrôleur. Le comportement d'un commutateur OpenFlow est déterminé par une ou plusieurs tables de flux (flow table). Chaque table représente un ensemble de flux, qui consistent en une liste de critères relatifs au contenu d'une trame, associée à des actions de traitement à appliquer aux trames correspondantes.

Lorsqu'un paquet arrive au commutateur, les valeurs de ses en-têtes sont vérifiées par rapport aux ensembles de valeurs enregistrés dans la première table de flux du commutateur illustré à la figure III.2. Les actions possibles sont variées : transfert du cadre par une interface, suppression, modification des champs d'en-têtes, et/ou transmission du traitement à une table de flux ultérieure, demande de directive au contrôleur.

Lorsque le contrôleur reçoit un message packet-in du switch, lui demandant l'action à effectuer, il analyse le paquet en utilisant les APIs du plan de contrôle. Ensuite, il envoie les instructions au switch via le message packet-out. [13]



FigureII. 3- Schéma base d'échange entre le commutateur et le contrôle via OpenFlow

II.5.2 Table de flux (Flow table)

Les requêtes de fonctionnalité de table OpenFlow donnent la possibilité à un contrôleur OpenFlow d'interroger les capacités des tables de flux existantes d'un périphérique géré par OpenFlow ou de les configurer selon les paramètres fournis. Il est possible de configurer toutes les tables avec un sous-ensemble spécifique de capacités de correspondance et d'action. De plus, les tailles des tables peuvent être ajustées en cours d'exécution. Lorsqu'une nouvelle configuration de table de flux est appliquée avec succès, les entrées de flux des anciennes tables de flux sont supprimées sans notification. Les tables de flux configurées de façon dynamique ne sont pas persistantes après le redémarrage du système. Un pipeline par défaut est automatiquement établi au démarrage de l'appareil. Lorsqu'une nouvelle table de flux est configurée en réponse à une demande du contrôleur OpenFlow, tout le trafic existant passant par les flux précédemment établis est effacé. [14]

Une table de flux se compose d'entrées de flux. Chaque entrée du tableau des flux contient :

TableauII. 1- Structure d'une entrée du flux

Match Fields	Priority	Counters		Instructions	TimeOuts	Cookie	Flags

Match Fields : Pour les comparer aux paquets. Il s'agit du port d'entrée et des en-têtes des paquets et, éventuellement, d'autres champs du pipeline tels que les métadonnées spécifiées dans un tableau précédent.

Priority : La priorité de correspondance de l'entrée de flux.

Counters : Mis à jour lorsque les paquets correspondent.

Instructions : Pour modifier l'ensemble des actions ou le traitement du pipeline.

TimeOuts : La durée maximale ou le temps d'inactivité avant que le flux ne soit expiré par le commutateur.

Cookie : Valeur de données opaques choisie par le contrôleur. Peut être utilisée par le contrôleur pour filtrer les statistiques de flux, la modification et la suppression de flux. Non utilisé lors du traitement des paquets.

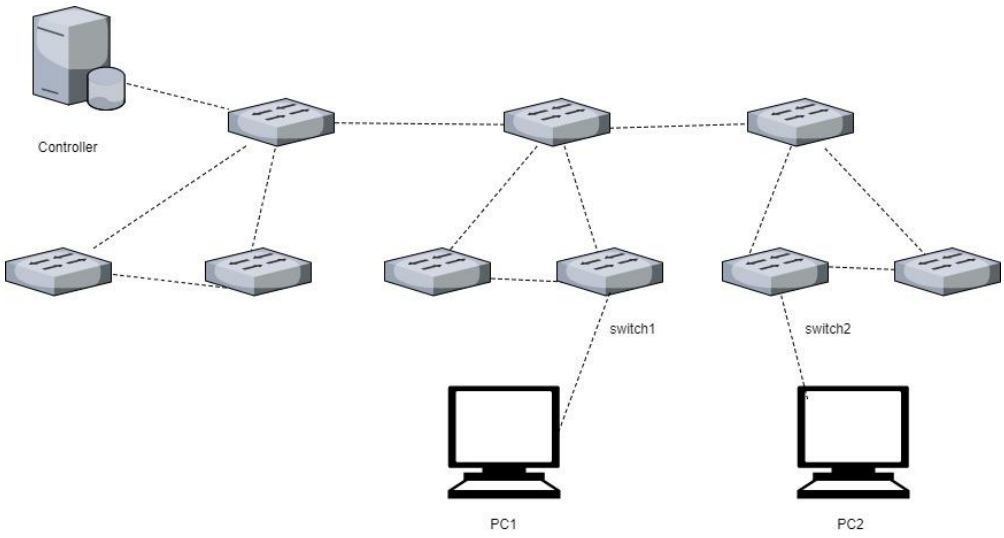
Flags : Pour modifient la manière dont les entrées de flux sont gérées. [12].

II.6 Les contrôleurs SDN

Dans l'architecture SDN, le contrôleur est une application essentielle qui assure la gestion du contrôle de flux pour améliorer la gestion du réseau et optimiser les performances des applications.En utilisant un contrôleur SDN, il devient possible d'effectuer rapidement des

modifications sur le réseau en convertissant une demande globale, telle que la mise en priorité d'une application particulière, en une série d'opérations sur les équipements réseau. La capacité du contrôleur à traduire des demandes globales en opérations spécifiques sur les équipements réseau est un élément essentiel pour une gestion efficace des réseaux SDN.

Le contrôleur SDN communique avec les équipements réseau en utilisant une ou plusieurs API, aussi appelées interfaces sud. OpenFlow est une API sud qui agit directement sur le plan de données, permettant ainsi au contrôleur de contrôler le comportement des commutateurs sous-jacents. Cette communication centralisée entre le contrôleur et les équipements réseau via une API sud est un élément fondamental de l'architecture SDN, offrant une plus grande flexibilité et une meilleure gestion des ressources.[14]



FigureII 4- Placement d'un contrôleur SDN

II.6.1 Types de contrôleurs SDN et leurs propriétés

Le tableau II.2 montre les différents contrôleurs SDN et leurs propriétés. [8]

TableauII. 2- Contrôleurs SDN et leurs propriétés

Contrôleur SDN	Protocole	Architecture	Langage de programmation	API supportés	Plateformes supportées
Beacon	OpenFlow	Centralisée	Java	Ad-Hoc API	Linux Windows
DISCO	OpenFlow	Centralisée	Java	REST API	Linux Windows
IRIS	OpenFlow OVSDB	Centralisée	Java	REST API	Linux Windows
Meastro	OpenFlow	Centralisée	Java	Ad-Hoc API	Linux Windows Mac OS
OpenDaylight	OpenFlow OVSDB	Déstribuée	Java	REST API	Linux
NOX	OpenFlow	Centralisée	C++	Ad-Hoc API	Linux Windows Mac OS
POX	OpenFlow	Centralisée	Python	Ad-Hoc API	Linux Windows Mac OS
Floodlight	OpenFlow	Centralisée	Java	REST API	Linux Windows Mac OS
Ryu	OpenFlow OVSDB	Centralisée	Python	Ad-Hoc API	Linux

II.7 Les interfaces de communication

Afin de faciliter l'interaction entre le contrôleur SDN et les différentes couches du réseau, les API, ou interfaces de communication, sont mises en place. Selon la position hiérarchique de la couche, ces interfaces sont désignées par les termes Nord, Sud, Est et Ouest. L'interface Sud est utilisée pour communiquer avec une couche inférieure (Underlay), tandis que l'interface Nord est utilisée pour communiquer avec des couches supérieures. Les interfaces Est/Ouest permettent la communication entre différents contrôleurs.[10]

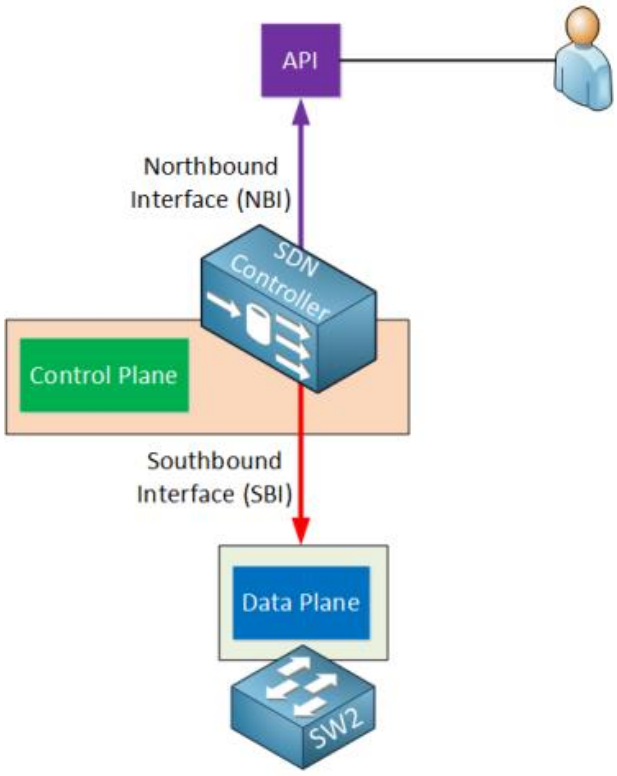
II.7.1 Interface Nord NBI (North-Bound Interface)

Les interfaces Nord sont utilisées pour configurer les éléments de transmission en utilisant l'abstraction du réseau fournie par le plan de contrôle. En d'autres termes, elles facilitent la communication entre le contrôleur et la couche applicative. Elles sont plus perçues comme des API que comme des protocoles de programmation et de gestion de réseau.

D'après l'ONF (Open Networking Foundation, 2012), il est possible de caractériser plusieurs niveaux d'abstraction et différents cas d'utilisation, ce qui implique qu'il existe plusieurs interfaces Nord pour répondre à tous les cas d'utilisation. Parmi les propositions des industriels, une API basée sur REST API (Representational State Transfer) est proposée afin de fournir une interface programmable utilisable par les applications.[10]

II.7.2 Interface Sud SBI (South-Bound Interface)

L'interface Sud API est une composante critique d'un système SDN, elle permet au contrôleur de gérer le comportement du réseau en contrôlant les flux entrants de tous les commutateurs sous-jacents. L'API South-bound offre une interface commune aux couches supérieures, permettant au contrôleur d'utiliser des API vers le sud telles qu'OpenFlow, POF, OpFlex et OpenState, ainsi que des plugins de protocoles pour gérer les périphériques physiques ou virtuels existants ou nouveaux. Actuellement, OpenFlow est considéré comme la norme la plus acceptée pour la norme de SBI.[15]



FigureII. 5- Les interfaces Nord et Sud (NBI et SBI)

II.8 Avantages du SDN

L'objectif des améliorations apportées par SDN est de simplifier l'administration des réseaux et d'accroître la flexibilité de l'utilisation des ressources du réseau par les

applications, tout comme la virtualisation des serveurs l'a fait. Les atouts essentiels dans l'environnement SDN sont les suivants :

- **Gestion plus efficace du réseau :** Le SDN offre une visibilité en temps réel sur les performances du réseau ce qui facilite l'optimisation de sa qualité et la gestion de son efficacité. [W16]
- **Economie des couts :** Dans les réseaux traditionnels, la redondance était considérée comme le moyen le plus efficace pour renforcer la disponibilité du réseau. Cependant, cela impliquait l'ajout d'équipements supplémentaires, de circuits supplémentaires et donc de coûts supplémentaires. Etant donné que le SDN offre la capacité de rediriger automatiquement le trafic en temps réel ou de mettre en place de nouvelles fonctions et routes, ce qui permet aux administrateurs d'augmenter la disponibilité du réseau sans avoir à ajouter de nouveaux équipements ni à augmenter les coûts**.** [W16]
- **Evolutivité plus rapide :** Le SDN permet aux administrateurs d'ajuster rapidement leurs besoins fonctionnels, même dans le cadre de topologies étendues, en leur offrant une capacité opérationnelle. [W16]

Conclusion

Les réseaux définis par logiciel (SDN) représentent une approche novatrice pour superviser et contrôler les infrastructures réseau. En séparant les plans de données, de contrôle et de gestion, et en utilisant des interfaces et des protocoles ouverts, les SDN permettent une gestion centralisée, une automatisation et une adapte.

Le SDN a donné naissance à plusieurs approches dérivées, telles que le SDS pour la gestion du stockage, le SD-Access pour la gestion des réseaux locaux et le SD-WAN pour la gestion des réseaux étendus que nous l’aborderons dans le chapitre suivant.

Chapitre III

Etude de solution SD-WAN

Introduction

Dans ce chapitre nous allons explorer le concept de SD-WAN (Software-Defined Wide Area Network) en détaillant son architecture, son fonctionnement et l'utilisation des réseaux superposés (overlay). Nous examinerons comment le SD-WAN révolutionne la connectivité des réseaux d'entreprise en offrant une gestion centralisée, une flexibilité accrue et une optimisation des performances pour répondre aux besoins évolutifs des entreprises modernes.

III.1 Définition

Le SD-WAN, ou Software-Defined Wide Area Network, est une technologie innovante qui révolutionne la connectivité Internet professionnelle en appliquant les principes du SDN au réseau étendu (WAN). Il crée un réseau logique entre les différents sites d'une entreprise, géré par des fournisseurs de services SD-WAN, avec une gestion centralisée via un site central. Contrairement aux WAN traditionnels utilisant des technologies comme le MPLS pour la sécurité et la performance, le SD-WAN superpose un réseau virtuel à l'infrastructure physique existante, permettant une gestion agile et flexible des connexions. Grâce à une console centralisée, les administrateurs peuvent configurer et surveiller le réseau de manière cohérente. Le SD-WAN optimise dynamiquement le trafic en choisissant les meilleures liaisons disponibles et priorise les applications critiques. Il combine différentes technologies de connectivité, permettant d'utiliser simultanément plusieurs liaisons pour maximiser les débits et assurer la qualité de service comme le montre la Figure 4.1. En cas de défaillance, le trafic est automatiquement redirigé vers un autre chemin plus performant. Cette approche offre une flexibilité accrue, permettant d'ajuster rapidement la bande passante et les configurations selon les besoins de l'entreprise, tout en optimisant les coûts et en améliorant l'expérience utilisateur. [20]

III.2 Histoire et évolution du SD-WAN

Les technologies modernes de réseau SD et SD-WAN ont évolué à partir de solutions de réseau antérieures telles que les lignes louées point à point (PPP), le relais de trame et le MPLS. Le PPP était le mode original de connexion de plusieurs réseaux locaux (LAN) avant que le relais de trame ne supprime la nécessité d'acheter et de gérer des liens de connexion individuels entre différents sites d'entreprise. La connexion MPLS a apporté d'autres améliorations en réunissant des fonctions auparavant séparées, telles que la voix, la vidéo et les réseaux de données, sur le même réseau à l'aide de la technologie basée sur le protocole Internet (IP).

Dans les années 2000, la commutation multiprotocole par étiquette (MPLS) est devenue populaire. MPLS a rapidement dépassé le relais de trame en termes de popularité en raison de la façon dont il exploite la technologie basée sur le protocole Internet (IP) pour réunir sur le même réseau des fonctions auparavant séparées, telles que la voix, la vidéo et les réseaux de données. Aujourd'hui, MPLS est la technologie la plus couramment utilisée pour les réseaux étendus d'entreprise, et elle est toujours appréciée pour la réduction de la latence et les avantages en termes de qualité de service (QoS) qu'elle offre. Dans les années 2010, plus précisément en 2013, le SD-WAN a vu le jour, et au fur et à mesure que les technologues examinaient les avantages du SD-WAN, ils se sont rendu compte que le SD-WAN présentait de nombreux avantages par rapport au MPLS, de la même manière que le MPLS présentait plus d'avantages que le relais de trame. Pour simplifier, les réseaux SD offrent une qualité de service de niveau MPLS tout en étant beaucoup moins coûteux et beaucoup plus faciles à faire évoluer. [W17]

III.3 Architecture SD-WAN

L'abstraction architecturale divise le réseau en plans de contrôle et de transport, améliorant ainsi la supervision et la réactivité du réseau. Dans l'architecture SD-WAN, le contrôle est séparé du matériel pour simplifier la gestion du réseau et améliorer les services et l'expérience utilisateur. Les passerelles SD-WAN permettent aux appareils de succursales de maintenir plusieurs connexions via différents mécanismes de transport, renforcés par un VPN pour la sécurité. [W18]

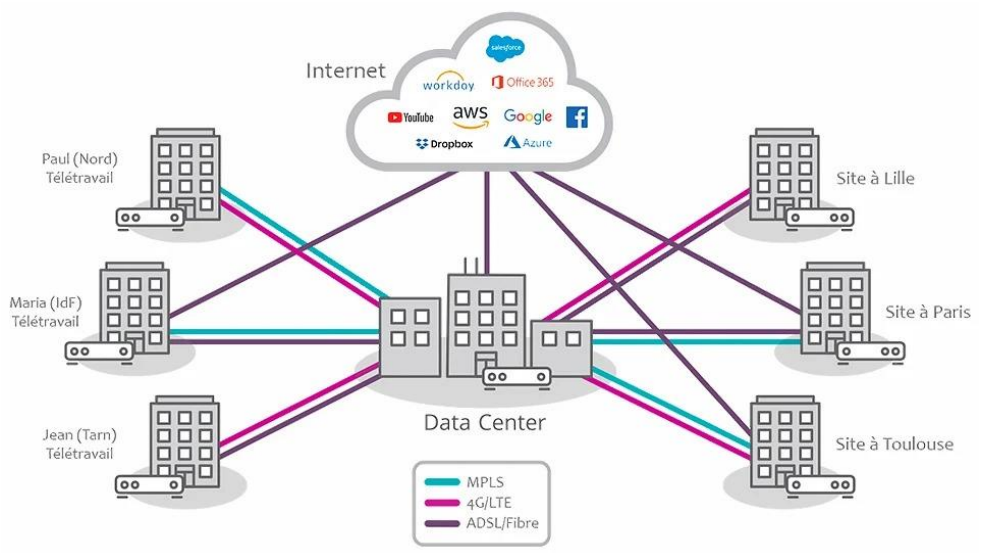


Figure III. 1- Architecture SD-WAN

Il existe différentes implémentations de SD-WAN qui donnent lieu à des architectures variables. Trois types principaux sont couramment utilisés :

- **ON-PREM-ONLY :** Ce service est déployé sur site uniquement (dans des routeurs conventionnels) donc c'est une connectivité à maillage complet entre les bureaux distants. Cette solution est utilisée avec les entreprises qui n'ont pas d'applications Cloud hébergées sur leurs réseaux et ne peuvent pas supporter les coûts supplémentaires liés au service SD-WAN basé sur le cloud donc il n'est pas possible de se connecter à des passerelles cloud.
- **Cloud-Enabled :** Le service basé sur le cloud est destiné aux entreprises ayant une infrastructure informatique en Cloud et qui souhaitent optimiser leur accès aux applications cloud privé ou public. A l'aide d'une passerelle cloud, qui est considérée comme une passerelle pour toutes les principales applications cloud (par exemple : Office 365, Azure, Salesforce, etc.), la session cloud reste active en cas de défaillance de la connexion Internet de l'entreprise lors de l'utilisation d'une application cloud.
- **Solution Hybride** : Une solution hybride intègre les services du On-Prem-Only et les services du Cloud-Enabled dans un seul service. [W18]

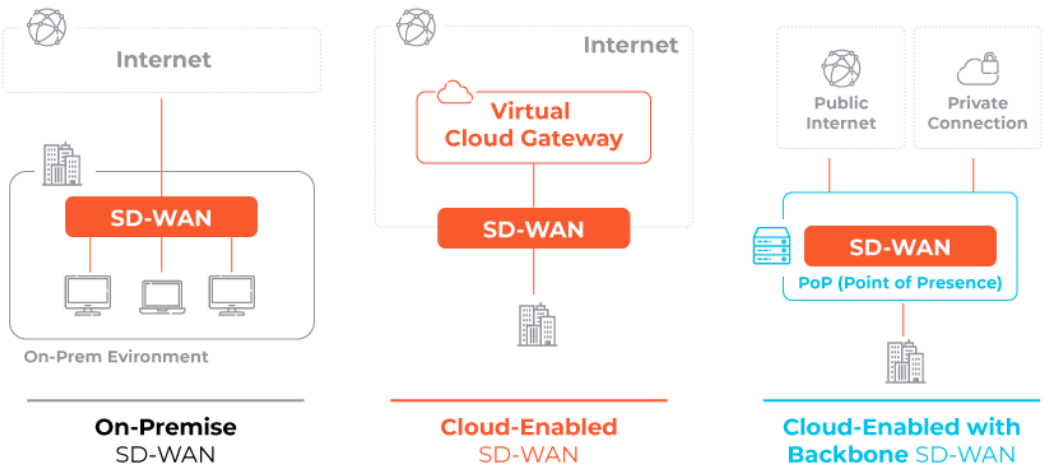


Figure III. 2- Types d'architectures SD-WAN

IV.4 La différence entre un réseau WAN et SD-WAN

Comparé au WAN traditionnel, le SD-WAN présente une architecture WAN virtuelle et une technologie pilotée par logiciel. Son élément clé est son système de contrôle central, qui permet

un contrôle centralisé via des ressources matérielles virtualisées, permettant des connexions réseau, des politiques de sécurité, des flux d'applications et la gestion du trafic peut être séparée du matériel connexe.

De plus, les méthodes de déploiement et de gestion du SD-WAN et du WAN sont généralement différentes. SD-WAN est une technologie logicielle qui couvre le réseau existant. Le WAN défini par logiciel n'utilise pas de matériel existant avec un logiciel. Au lieu de cela, après avoir standardisé le matériel, il est uniformément déployé par le contrôleur SD-WAN. Avec le SD-WAN, le réseau physique et le réseau logique sont séparés. Il sépare le réseau du plan de gestion et déconnecte les tâches de gestion et de surveillance du trafic du matériel.

En plus des limitations matérielles, la construction d'un WAN est également longue et laborieuse, en particulier dans le contexte de la vague numérique qui balaie tous les horizons ces dernières années, de plus en plus d'entreprises choisissent d'aller vers le cloud, et il semble que le WAN dépend des connexions propriétaires et de la construction matérielle. Et un grand nombre d'architectures d'exploitation et de maintenance lourdes ne sont pas adaptées au stade actuel. [W19]

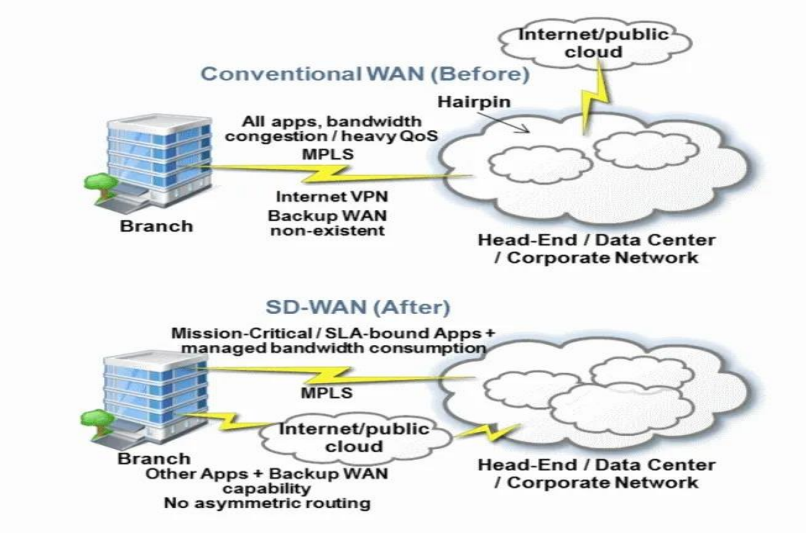


Figure III. 3- Architecture WAN traditionnel VS Architecture SD-WAN

IV.5 Relation entre MPLS et SD-WAN

Le SD-WAN permet de créer un réseau étendu (WAN) hybride en combinant différentes technologies, tout en conservant l'utilisation du MPLS. Cette approche assure une optimisation intelligente des flux de données des applications entre les sites distants et le cloud privé du siège social de l'entreprise, tout en accélérant l'accès aux services hébergés dans le cloud public.

Dans un WAN hybride basé sur le SD-WAN, les flux de données sont routés de manière dynamique via les connexions les plus appropriées en fonction des exigences de performance, de sécurité et de coût de chaque application. Par exemple, les applications critiques ou sensibles à la latence peuvent continuer à être acheminées via les circuits MPLS pour garantir une qualité de service (QoS) élevée, tandis que les applications moins sensibles peuvent utiliser des liens Internet moins coûteux. [W20]

Cette approche présente plusieurs avantages :

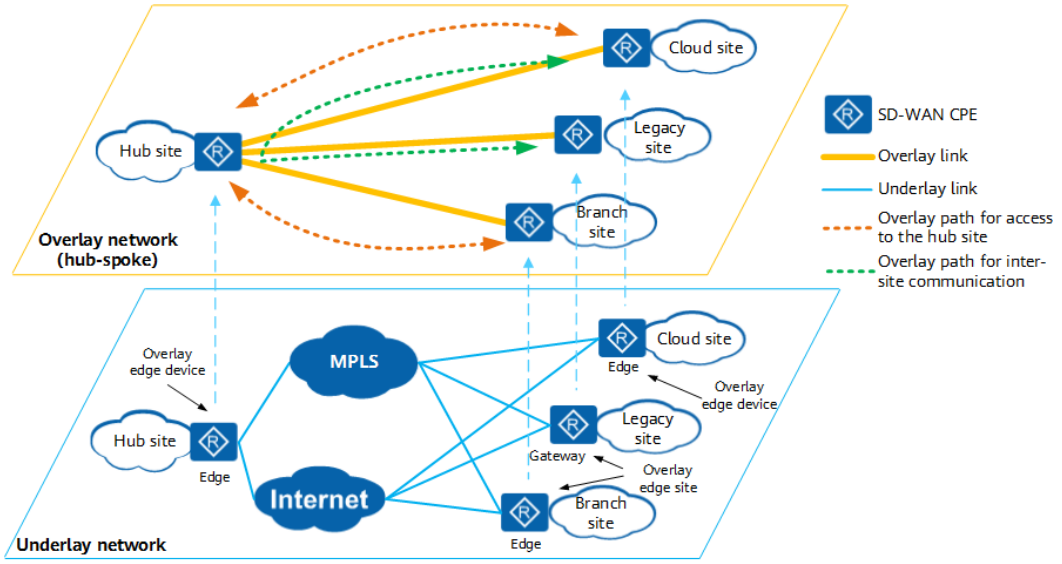
- **Optimisation de la bande passante :** Le SD-WAN utilise des technologies telles que la déduplication, la compression et la mise en cache pour maximiser l'utilisation de la bande passante disponible, améliorant ainsi les performances globales du réseau.
- **Flexibilité et agilité :** En permettant l'utilisation de différents types de connexions, y compris MPLS, Internet et LTE, le SD-WAN offre une flexibilité accrue pour répondre aux besoins évolutifs des entreprises et des applications.
- **Réduction des coûts :** En tirant parti des connexions Internet moins chères pour le trafic non critique, les entreprises peuvent réduire leurs dépenses liées au réseau tout en maintenant un niveau de performance élevé pour les applications prioritaires.
- **Visibilité et contrôle améliorés :** Les solutions SD-WAN offrent une visibilité granulaire sur le trafic réseau et permettent un contrôle centralisé sur le déploiement et la gestion des politiques de sécurité et de QoS. [W20]

III.6 SD-WAN Overlay Network

La structure du réseau sous-jacent (underlay) SD-WAN repose sur un réseau étendu utilisant des liens hybrides pour interconnecter les sièges sociaux, les sites distants et les sites cloud. Il adopte également une topologie logique de réseau superposé (overlay), capable de répondre aux exigences d'interconnexion et d'intercommunication dans divers scénarios. En général, les réseaux SD-WAN se composent d'équipements situés chez le client (CPE), classés comme périphériques de bord et passerelles. Par conséquent, le réseau SD-WAN, construit à partir des réseaux de superposition (overlay) et sous-jacents (underlay), peut être adapté en fonction de l'échelle du réseau de l'entreprise, du nombre de sites centraux et des exigences de communication entre les sites.

En tant que solution d'architecture de réseau sous-jacent (underlay) la plus utilisée dans les centres de données, le réseau de tissu (fabric network) du centre de données présente des avantages en termes de fiabilité, d'efficacité, de scalabilité et de performance. Les

commutateurs de centre de données FS aide à construire un réseau de tissu, résolvant les problèmes de goulots d'étranglement liés à l'échelle et à l'expansion des réseaux de centres de données.



FigureIII. 4- SD-WAN Overlay network

III.7 Adoption de l'approche par différents constructeurs

III.7.1 Cisco SD-WAN

La solution Cisco SD-WAN simplifie la connexion entre les sites distants et les centres de données, ainsi que la communication avec les applications et services cloud. Intégrant routage, sécurité, gestion centralisée et orchestration, Cisco SD-WAN est multi-locataire, basé dans le cloud, automatisé, sécurisé, évolutif et adapté aux applications grâce à des analyses approfondies. Il garantit une meilleure expérience utilisateur pour les applications et services cloud.

III.7.1.1 Architecture de Cisco SD-WAN

La solution Cisco SD-WAN adopte une architecture où le plan de contrôle et le plan de données sont séparés, complétés par des couches supplémentaires. La nouvelle architecture comprend un plan d'orchestration, un plan de gestion, un plan de contrôle et un plan de données.

- **Plan d'orchestration :** Facilite l'intégration automatisée des routeurs SD-WAN dans la superposition SD-WAN.
- **Plan de gestion :** Responsable de la configuration centralisée, du dépannage, de la surveillance et des rapports de journalisation.

- **Plan de contrôle :** Construit et maintient la topologie du réseau, prenant des décisions concernant les flux de trafic.
- **Plan de données** : Responsable de la transmission des paquets en fonction des décisions prises par le plan de contrôle.

En général, la solution Cisco SD-WAN fonctionne en établissant automatiquement des tunnels GRE/IPsec entre tous les éléments constituant le plan de données du domaine (les Edges), indépendamment du type de réseau utilisé, que ce soit MPLS, Internet, LTE, ou autre.

Les composants clés de la solution Cisco SD-WAN incluent vManage, vBond et vSmart. vManage est l'interface utilisateur principale pour la gestion, vBond gère le provisionnement et l'authentification, et vSmart est le cerveau du réseau SD-WAN de Cisco.[W21]

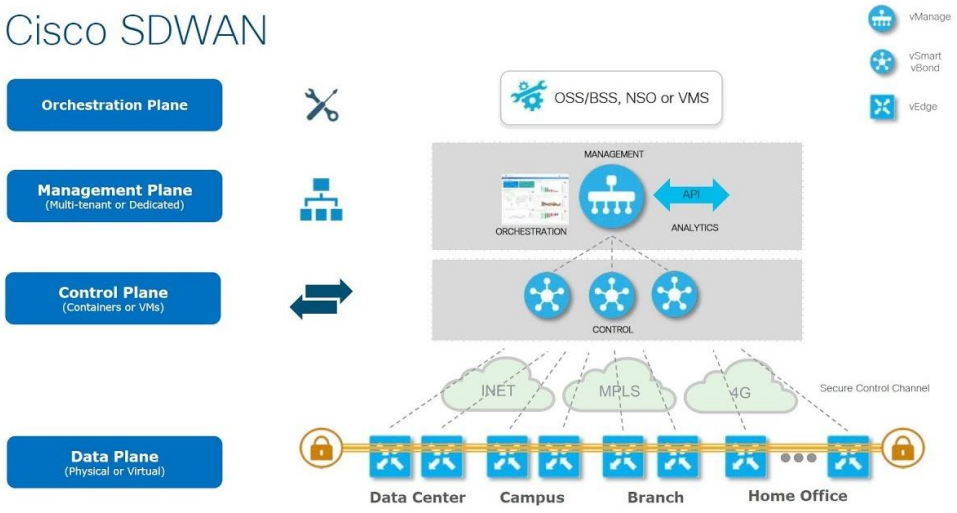


Figure III. 5- Architecture Cisco SD-WAN

III.7.2 Huawei SD-WAN

La solution Huawei SD-WAN résout les problèmes des réseaux d'entreprise, tels que les architectures WAN fermées, les difficultés de service, le déploiement lent des services et la gestion complexe des opérations et de la maintenance. Elle permet des interconnexions à la demande entre les succursales, les centres de données et les clouds. Avec des fonctionnalités telles que la redirection intelligente du trafic basée sur les applications, l'accélération et une gestion intelligente des opérations et de la maintenance, la solution SD-WAN améliore l'expérience des services dans les interconnexions WAN des entreprises. [W22]

III.7.2.1 Architecture Huawei SD-WAN

La figure ci-dessous montre l'architecture du Huawei SD-WAN. La solution Huawei SD-WAN comprend trois couches comme le montre la figure ci-dessus :

- **La couche de connexion réseau (Network connection layer) :** Les entreprises déploient des routeurs NetEngine AR rentables et utilisent la technologie de superposition pour construire des interconnexions réseau complètes entre les sièges sociaux, les succursales et les clouds publics ou privés à la demande, via des liens tels que des liens Internet et des lignes privées traditionnelles.
- **La couche de contrôle (Control layer) :** Les routeurs réfléchissants (RRs) travaillent avec iMaster NCE pour mettre en œuvre le déploiement automatique et la configuration des réseaux dans chaque zone, la fourniture automatique de politiques, le transfert de routes entre les sites de chaque zone, et l'interconnexion des réseaux interzones.
- **La couche de gestion (Management layer) :** iMaster NCE met en œuvre une gestion complète des services d'interconnexion d'entreprise. Dans la direction sud, iMaster NCE utilise NETCONF/YANG pour mettre en œuvre une gestion unifiée des dispositifs tels que les RRs et les CPEs, la cartographie CPE-RR et l'orchestration, la configuration et l'orchestration de différentes topologies de réseau privé virtuel (VPN), ainsi que la gestion et la provision des politiques de service réseau. Dans la direction nord, iMaster NCE fournit des API RESTful standard pour une interconnexion facile avec des applications tierces et des plateformes cloud. [W22]

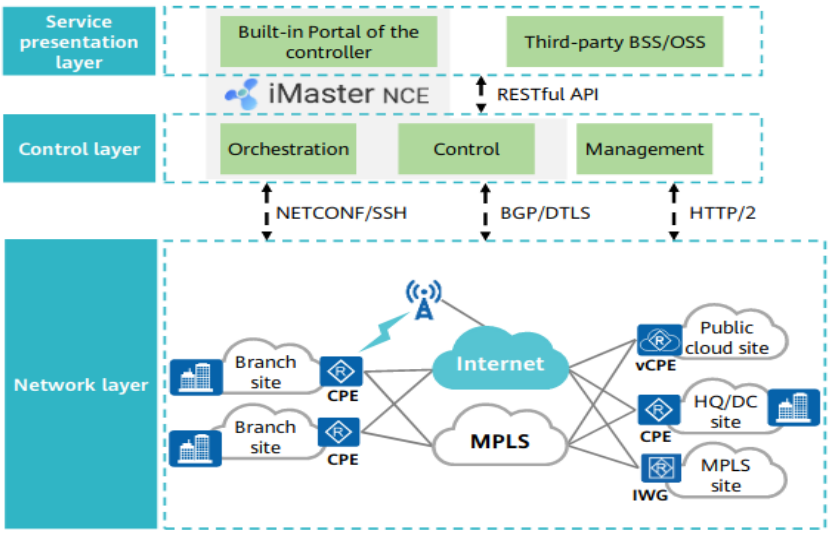


Figure III. 6- Architecture Huawei SD-WAN

III.7.3 Fortinet SD-WAN

Le SD-WAN sécurisé de Fortinet (secure SD-WAN) est conçu pour les entreprises axées sur le cloud, soucieuses de la sécurité et de portée mondiale, ainsi que pour les effectifs hybrides. Leur approche de mise en réseau sécurisé repose sur un système d'exploitation unique qui consolide les fonctions SD-WAN, pare-feu nouvelle génération (NGFW), routage avancé et passerelle d'application ZTNA.

Le Secure SD-WAN est une technologie intégrée dans les firewalls Fortigate, permettant aux entreprises de combiner les fonctionnalités d'un firewall NGFW et d'un SD-WAN sur une même plateforme. Cette solution vise à répondre à plusieurs défis courants rencontrés par les entreprises :

- L'adoption croissante d'applications SaaS (comme Office 365) et de services cloud publics, utilisant Internet comme principal support.
- Le besoin accru de flexibilité et d'agilité dans la gestion et l'administration des architectures WAN.
- L'amélioration de l'expérience utilisateur.
- La globalisation et l'optimisation des ressources WAN.
- La nécessité d'une visibilité accrue, de monitoring et de reporting pour renforcer la sécurité globale.

La solution intègre une gestion d'architecture overlay, un contrôle avancé de la métrologie et du routage applicatif intelligent, des solutions de remédiation WAN, une interconnexion avec les clouds publics, une gestion centralisée avec automatisation et "Zero Touch Provisioning", ainsi qu'une visibilité complète avec tableaux de bord et rapports détaillés. [W23]

III.7.3.1 Architecture Fortinet secure SD-WAN

L'overlay est l'un des éléments fondamentaux d'une architecture SD-WAN. Le FortiGate a la capacité de gérer diverses architectures qui se combinent pour former une solution globale :

- **Hub&Spoke**

En architecture Hub & Spoke, un ou plusieurs centres de regroupement, souvent appelés hubs, servent de points centraux pour connecter tous les sites distants du réseau à travers des tunnels IPSec overlay. Dans ce schéma, tous les échanges de données entre les sites distants passent toujours par ces centres de regroupement. Cette configuration permet un contrôle centralisé du trafic et une gestion simplifiée, car les politiques de sécurité et les règles de routage peuvent être appliquées de manière cohérente au niveau des hubs. De plus, cela permet

également de concentrer les ressources de sécurité et de surveillance sur un nombre limité de points, ce qui peut être avantageux en termes de performances et de gestion des risques. Cependant, cette approche peut introduire un point unique de défaillance et des goulets d'étranglement potentiels au niveau des hubs, ce qui nécessite une conception soigneuse pour assurer la résilience et les performances du réseau. [W24]

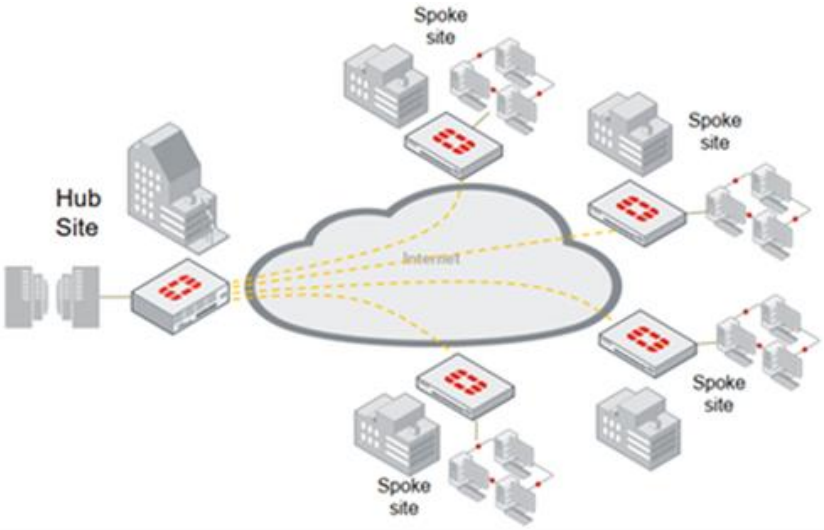


Figure III. 7- Architecture Hub&Spoke SD-WAN

- **Full mesh**

En architecture full mesh, chaque FortiGate établit une connexion directe avec chaque autre FortiGate dans le réseau, formant ainsi un réseau d'overlay où tous les sites sont interconnectés les uns aux autres. Cela signifie que chaque site peut communiquer directement avec n'importe quel autre site via des tunnels sécurisés. Cependant, bien que cette méthode soit possible, elle peut devenir complexe à gérer et à maintenir à mesure que le nombre de sites augmente, car le nombre de tunnels nécessaires croît de manière quadratique avec le nombre de sites. Pour cette raison, l'architecture ADVPN (Auto Discovery VPN) est souvent préférée. ADVPN utilise des tunnels dynamiques et permet aux sites de communiquer de manière efficace et sécurisée sans nécessiter une configuration manuelle et un nombre excessif de tunnels. [W24]

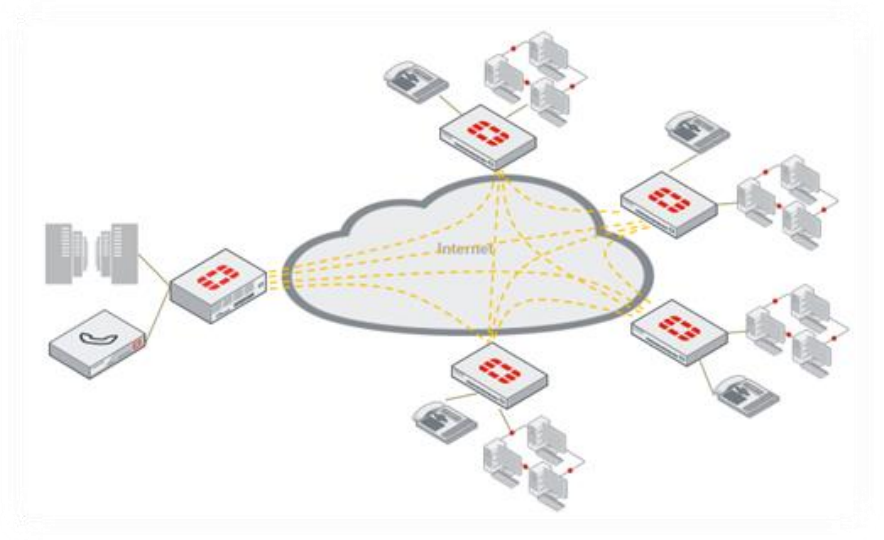


Figure III. 8- Architecture Full mesh SD-WAN

III.7.3.2 Les Composants essentiels

Fortinet Secure SD-WAN est composé du seul logiciel développé organiquement dans l'industrie, complété par une plateforme accélérée par ASIC, afin de fournir la solution SD-WAN la plus complète.

Voici les principaux composants et fonctionnalités du SD-WAN Fortinet, centrés autour des appliances FortiGate utilisant FortiOS :

- **FortiGate :**

FortiGate est l'appliance pare-feu principale de Fortinet, intégrant des fonctionnalités de sécurité avancées et de SD-WAN sur une plateforme unique. Doté d'un pare-feu de nouvelle génération (NGFW), il offre une protection complète contre les menaces, le contrôle des applications et la prévention des intrusions (IPS). FortiGate supporte également le SD-WAN, permettant une connectivité sécurisée et optimisée sur divers liens WAN tels que MPLS, Internet et LTE. Avec l'inspection SSL pour la détection des menaces dans le trafic chiffré, il intègre également une protection avancée contre les menaces (ATP) via les services de sécurité FortiGuard. Géré par FortiManager pour une gestion centralisée, FortiGate assure le façonnage du trafic, la qualité de service (QoS) et la priorisation des applications critiques, tout en offrant une visibilité complète et des rapports détaillés. [W25]

- **FortiOS :**

FortiOS est le système d'exploitation polyvalent qui alimente les appliances de sécurité Fortinet, telles que FortiGate. FortiOS offre une gamme complète de services de sécurité et de

gestion, intégrant la sécurité avancée, le SD-WAN, le contrôle des applications, la prévention des intrusions, la gestion des identités et bien plus encore. Il permet une gestion centralisée via FortiManager et fournit des analyses approfondies via FortiAnalyzer, tout en intégrant des mises à jour en temps réel et des services d'intelligence des menaces grâce à FortiGuard Security Services. [W25]

- **FortiManager :**

FortiManager est une plateforme de gestion centralisée qui offre la gestion de la configuration, la surveillance et l'automatisation pour les dispositifs Fortinet, y compris les pare-feu FortiGate utilisés dans les déploiements SD-WAN. Elle permet aux administrateurs de gérer de manière centralisée les politiques, les mises à jour de firmware et les modifications de configuration sur plusieurs appareils FortiGate. [W25]

- **FortiAnalyzer :**

FortiAnalyzer est une appliance centralisée de journalisation, d'analyse et de génération de rapports qui fournit des informations sur le trafic réseau, les événements de sécurité et les performances. Elle collecte des journaux à partir des pare-feu FortiGate et autres dispositifs Fortinet, aidant les équipes NOC à surveiller et analyser l'activité réseau. [W25]

- **Services de sécurité FortiGuard :**

Les services de sécurité FortiGuard comprennent une gamme d'abonnements de sécurité qui offrent des mises à jour en temps réel et une protection contre les dernières menaces. Cela inclut l'antivirus, la prévention des intrusions, le filtrage web et le contrôle des applications. [W25]

Conclusion

Ce chapitre a exploré le concept du SD-WAN, son architecture de base, ainsi que son évolution historique. Nous avons également examiné les différentes solutions proposées par des fournisseurs majeurs tels que Huawei, Fortinet et Cisco. Après une analyse approfondie des options disponibles, nous avons choisi de mettre en œuvre la solution SD-WAN de Fortinet en raison de ses fonctionnalités robustes, de sa flexibilité et de son efficacité prouvée dans divers scénarios.

Chapitre IV

Réalisation et Implémentation

Introduction

Dans ce chapitre, nous allons voir l'architecture Underlay que nous proposons. Nous allons d'abord décrire les détails de l'architecture : d'abord l'architecture de base, les sites principaux et les sites distants, ensuite les outils de simulation utilisé. Après nous verrons la table d'adressage et l'architecture détaillée ainsi que les ressources matérielles et logicielles utilisé. Ensuite nous allons voir les différentes configurations de notre architecture Underlay : les configurations de base, le routage statique et dynamique, le tests effectués pour s'assurer leur bon fonctionnement, la configuration du DMVPN. Par la suite, nous allons voir l'implémentation de la solution SD-WAN Overlay de Fortinet : d'abord le déploiement des pares-feux FortiGtae et l'architecture, ensuite la mise en place de SD-WAN Fortinet sur la Plateforme Graphique FortiGate : la configuration des interfaces et des adresses, les zones SD-WAN, ajustement des Performances SLA, test de Fonctionnement et Résultats.

IV.1 Architecture de base

L'architecture que nous proposons est composé du site de production, aussi appelé site principale, de son site de secours (Backup) qui est une réplication du premier situé à un emplacement géographique différents. Les modifications apportées au site principale seront retransmises à temps réel et dans les moindres détails au site backup, ces deux sites seront reliés par des lignes spécialisés (LS). Enfin, nous disposerons de trois sites distants situés dans trois wilayas différentes qui seront les succursales de l'entreprise.

- Site Alger
- Site Tizi Ouzou
- Site Sétif

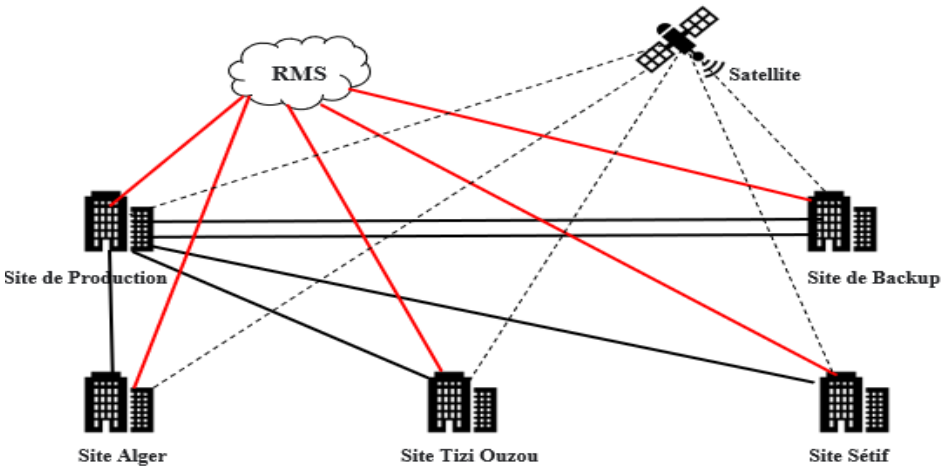


Figure IV. 1- Architecture de base

L'interconnexion des sites se fait de la manière suivante avec trois types de lisions : les lignes spécialisés qui relient les différents routeurs au site principal, c'est donc des liaisons "point à point", en cas d'éventuels problèmes ou de coupures de connexions, il y a un basculement automatique vers le réseau de secours. Des lignes qui passent par le RMS (Réseau Multi Service) d'Algérie Télécom qui utilise la technologie MPLS. Des lignes qui traversent le satellite avec l'implémentation de la technologie VSAT (Very Small Aperture Terminal). Afin de sécuriser les communications sur ce réseau. Nous avons implémenté un VPN avec la technologie DMVPN selon un modèle Hub and Spoke.

Les routeurs du site centrale et celui du Backup seront configurés comme des Hubs et ceux des sites distants seront configurés comme des Spokes.

IV.2 Le site principal et son backup

Le Site Principale est un site de production, il faudra par conséquent assurer la haute disponibilité de ce dernier. Dans son cœur se trouve un des deux datacenters de l'entreprise, vu l'importance accrue de ce siège donc deux serveurs, serveur Active Directory et serveur IP phone ; un réseau local qui sera constitué de plusieurs postes clients. Compte tenu de l'importance accrue de ce site, les ressources de sauvegarde, telles que le serveur IP Phone et le serveur Active Directory, seront répliquées de manière identique pour prendre le relais en cas de panne éventuelle au niveau du site principale.

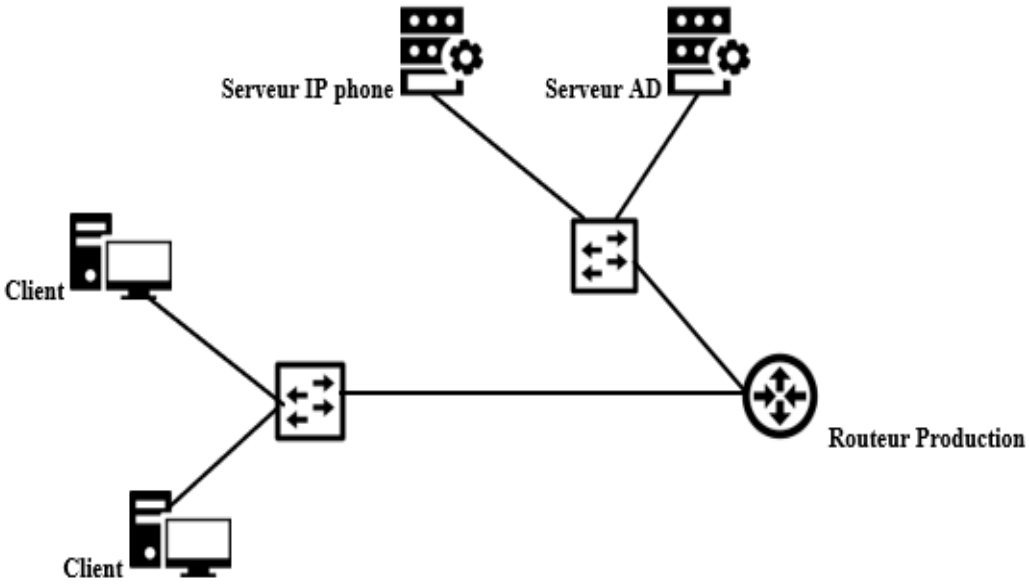


Figure IV. 2- Architecture du site de production

IV.3 Les sites distants

Les trois sites distants vont représenter des succursales c'est à dire des sièges distants. La banque d'Algérie possède 49 succursales dispersées dans tout le pays. Cependant, dans notre cas, nous nous limiterons à la simulation de seulement trois d'entre elles, car elles sont configurées de manière similaire. La simulation d'un nombre aussi élevé de sites nécessiterait une quantité considérable de ressources. La continuité des communications sera assurée notamment grâce à la redondance et la réplication du routeur principal pour chaque site.

Dans chaque site est relié par des liaisons Ethernet (LS) vers le routeur de production et par des liaisons séries vers le nuage RMS et vers8 le Satellite respectivement.

Le VPN sera implémenté au niveau du routeur de chaque site qui sera configure comme un spoke (client VPN).

La FigureV.3 montre l'architecture des sites distants.

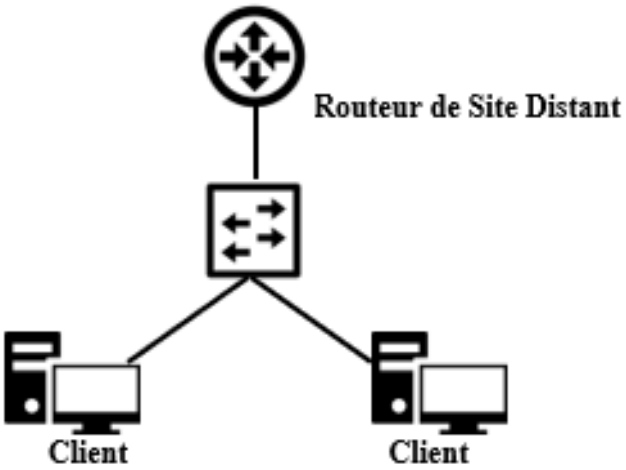


Figure IV. 3- Architecture des sites distants

V.4 Outils de simulation

V.4.1 GNS3

Graphical Network SImulatoe-3 ou GNS3 est un logiciel écrit en python qui offre la possibilité de simuler de manière graphique et précise des réseaux informatiques. Cette plateforme open source est mise à disposition gratuitement. Elle est largement utilisée par de prestigieuses entreprises et organisations. GNS3 permet la combinaison de modules réels et virtuels. Il prend en charge également des outils comme VirtualBox, WMWare…etc. [W33]

GNS3 se compose de deux parties : une interface graphique et un serveur. L'interface graphique est le côté client du simulateur, où les topologies peuvent être créées et gérées. Elle est installée localement sur l'ordinateur de l'utilisateur. Les équipements créés sur cette interface doivent être hébergés sur un serveur. GNS3 propose trois options pour le serveur : un serveur local, une machine virtuelle locale ou une machine virtuelle distante. [W34]

Pour notre cas, nous avons choisi d'utiliser une machine virtuelle locale car elle permet de simuler un plus grand nombre d'équipements et de topologies plus complexes, tout en évitant les problèmes de connectivité liés à une machine distante

Figure IV. 4- GNS3

V.4.2 VMware Workstation Player

VMware Workstation Player est un outil qui permet de créer des machines virtuelles afin d'y installer un système d'exploitation différent de celui de la machine hôte. Il prend en charge plus de 200 systèmes d'exploitation (Windows, Linux…). IL est a été développé dans le but d'être utilisé comme une machine virtuelle graphique unique ou en ligne de commande. Cela en fait un choix parfait pour exécuter un système d'exploitation différent dans une sandbox isolée et sécurisée sur un ordinateur grand public. Il est également très utilisé dans le domaine de l'éducation pour approfondir les connaissances sur les technologies de l'information et les systèmes informatiques.

L'installation de VMware Workstation Player se fait directement sur le système d'exploitation hôte, ce qui lui permet d'utiliser la gestion des périphériques de l'hôte pour prendre en charge une grande variété de configurations matérielles. [W35] [W36]

Dans notre cas, nous avons utilisé VMware Workstation 16 Player.

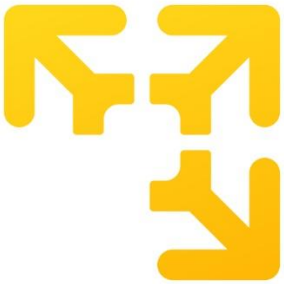


Figure IV. 5- VMware Workstation Player

IV.4.3 QEMU

Quick Emulator ou QEMU est un émulateur de machine et un virtualiseur générique et open source. Il existe différentes façons d'utiliser QEMU. La plus répandue est l'émulation de système, où il offre un modèle virtuel complet d'une machine (CPU, mémoire et périphériques émulés) pour exécuter un système d'exploitation invité. Dans ce mode, le CPU peut être entièrement émulé, ou il peut fonctionner avec un hyperviseur tel que KVM, Xen ou Hypervisor.Framework pour permettre à l'invité de fonctionner directement sur le CPU de l'hôte. La deuxième façon d'utiliser QEMU est l'émulation en mode utilisateur, où QEMU peut lancer des processus compilés pour un CPU sur un autre CPU. Dans ce mode, l'unité centrale est toujours émulée.

QEMU offre un ensemble d'utilitaires de ligne de commande autonomes, y compris qemu-img pour la création et la modification d'images disque. [W37]

IV.5 Tables d'adressage

Le tableau **IV**.1 montre les différents réseaux de notre architecture underlay et leurs utilisations ainsi que leurs sous réseaux.

IV.6 Architecture Underlay détaillée

La Figure **IV**.6 montre l'architecture underlay proposé complète avec tous les détails.

Tableau IV. 1- Table d'adressage

Réseau	Description	Adresse IP	Sous-réseau	Adresse IP
LS P2P	Utilisé pour adresser les LS qui relient les sites autres au site de production	10.10.10.0/24	Prod-Backup	10.10.10.0/30
			Prod-Site 1	10.10.10.4/30
			Prod-Site 2	10.10.10.8/30
			Prod-Site 3	10.10.10.12/30
LANs	Utilisé pour adresser les différents réseaux locaux	192.168.x.0/24	Production	192.168.1.0/24
			Backup	192.168.2.0/24
			Site 1	192.168.16.0/24
			Site 2	192.168.15.0/24
			Site 3	192.168.19.0/24
P2P RMS	Utilisé pour adresser les liaisons point-à-point qui relient les sites au nuage RMS	172.16.1.0/24	RMS-Prod	172.16.1.0/30
			RMS-Backup	172.16.1.4/30
			RMS-Site 1	172.16.1.8/30
			RMS-Site 2	172.16.1.12/30
			RMS-Site 3	172.16.1.16/30
P2P Satellite	Utilisé pour adresser les liaisons qui relient les sites au satellite	10.0.0.0/24	Satellite-Prod	10.4.0.0/16
			Satellite-Backup	10.5.0.0/16
			Satellite-Site 1	10.1.0.0/16
			Satellite-Site 2	10.2.0.0/16
			Satellite-Site 3	10.3.0.0/16
Zones serveurs	Utilisé pour adresser les deux zones de serveurs	10.10.2.0/24	Serveur Prod	10.10.2.0/28
			Serveur Backup	10.10.16/28
VPN	Utiliser pour adresser le réseau VPN	172.30.1.0/24		

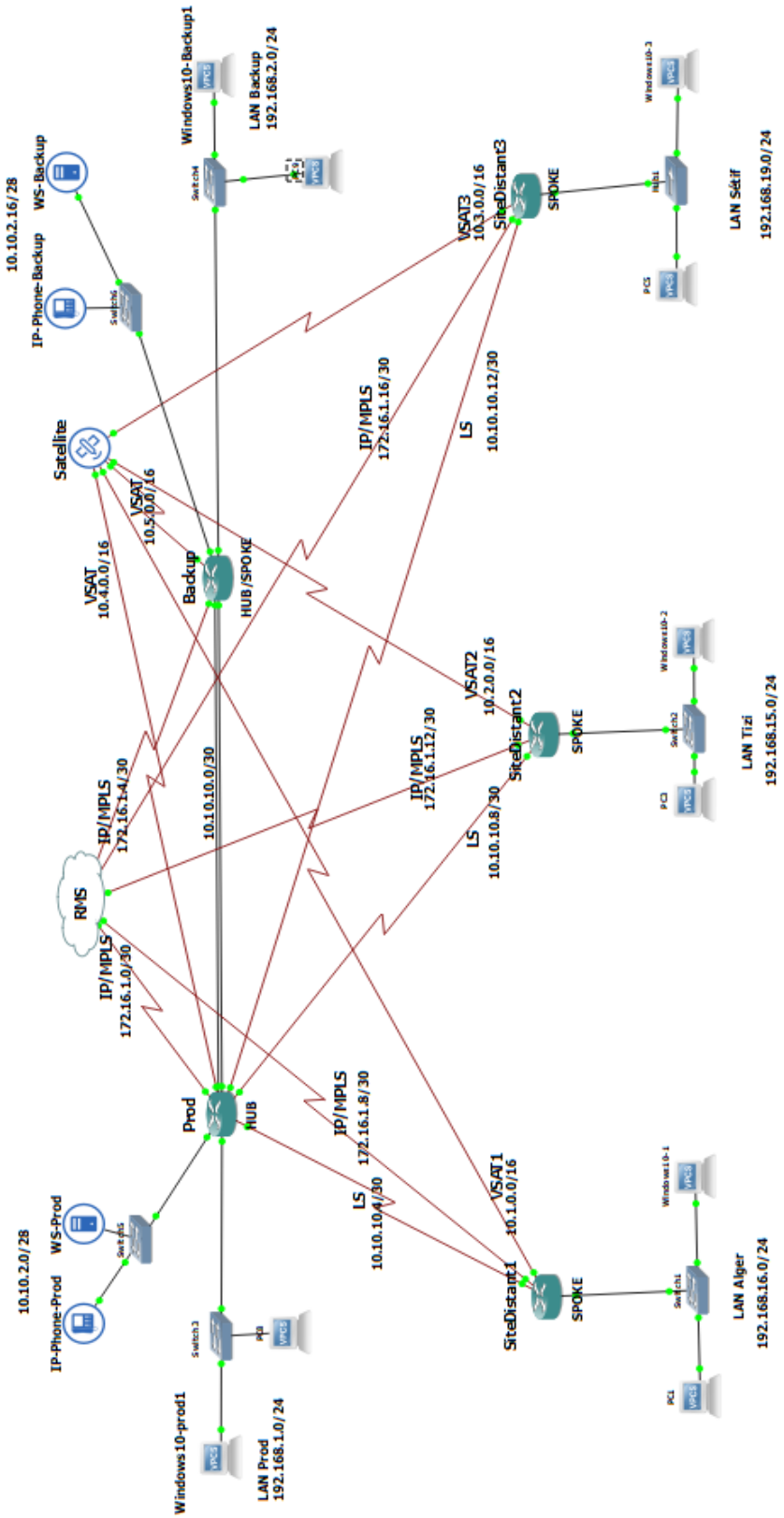


Figure IV. 6- Architecture Underlay détaillée

IV.7 Ressources matérielles

Pour réaliser et simuler notre architecture nous avons utilisé une machine avec les caractéristiques suivantes :

-Système d'exploitation : Windows 10 pro

-Types du système : Système d'exploitation 64 bits, processeur x64

-Processeur : Intel(R) Core (TM) i3-5005U

-RAM : 8 Go

-Disque : SSD 256 Go

IV.8 Ressources logicielles

Afin de réussir notre simulation, nous avons utilisé plusieurs machines virtuelles, des images IOS ainsi que des images Qemu que nous détaillerons par la suite :

IV.8.1 Machines virtuelles

IV.8.1.1 Windows Server

Windows Server est une gamme de systèmes d'exploitation développés par Microsoft qui offrent un support pour la gestion en entreprise, le stockage de données, les applications et les communications. Les versions antérieures de Windows Server mettaient l'accent sur la stabilité, la sécurité, le réseau et diverses améliorations du système de fichiers. Des améliorations supplémentaires ont également été apportées aux technologies de déploiement, ainsi qu'un support matériel amélioré. [W38]

Afin de gérer l'authentification des utilisateurs, nous avons déployé les machines Windows Server indiquées dans le tableau **IV**.2.

Tableau V. 2- Machines Windows Server déployées

Machines	Système d'exploitation	Site	Adresse IP
WS Prod	Windows Server 2022	Production	10.10.2.3/28
WS Backup	Windows Server 2022	Backup	10.10.2.18/28

IV.8.1.2 Windows 10

Pour simuler les postes clients, nous avons opté pour des machines Windows. Chaque site a été équipé d'une machine comme le montre le tableau **IV**.3.

Tableau IV. 3- Machines Windows 10 déployées

Machines	Site	Adresse
Windows 10-Prod	Production	192.168.1.2
Windows 10-Backup	Backup	192.168.2.2
Windows 10-1	Site 1	192.168.16.2
Windows 10-2	Site 2	192.168.15.2
Windows 10-3	Site 3	192.168.19.2

IV.8.2 Images IOS

Une image IOS ou Inernetwork Operationg System est le système d'exploitation qui fonctionne sur un routeur Cisco. Il contient les fichiers système et les utilitaires nécessaires au bon fonctionnement du routeur. Ces images sont utilisées dans GNS3 pour émuler ces routeurs.

Nous avons utilisé l'images suivante :

- C7200 153-3.XB12

Le tableau **IV**.4 montre la liste des différents routeurs que nous avons mis en place.

Tableau IV. 4- Routeurs mis en place

Routeur	Site	Fonction	Nombre d'interfaces
Prod	Production	Routeur principal	9
Backup	Backup	Routeur de secours	6
SiteDistant1	Site 1	Routeur principal	4
SiteDistant2	Site 2	Routeur principal	4
SiteDistant2	Site 3	Routeur principal	4

IV.9 Configuration d'architecture Underlay

IV.9.1 Configuration de base des routeurs

Pour le nuage RMS et le satellite nous avons utilisé des routeurs et nous avons changé leurs symboles.

```
Prod#sh ip int br
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            unassigned      YES NVRAM  administratively down down

Serial1/0                  172.16.1.2      YES NVRAM  up                    up

Serial1/1                  10.10.10.9      YES NVRAM  up                    up

Serial1/2                  10.10.10.13     YES NVRAM  up                    up

Serial1/3                  10.10.10.5      YES NVRAM  up                    up

FastEthernet2/0            10.10.10.1      YES NVRAM  up                    up

FastEthernet3/0            192.168.1.1     YES NVRAM  up                    up

FastEthernet3/1            10.10.2.1       YES manual up                    up

Serial4/0                  10.4.0.2        YES NVRAM  up                    up
```

Figure IV. 7- Configuration de base du routeur Prod

```
Backup#sh ip int br
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            unassigned      YES NVRAM  administratively down down

FastEthernet1/0            10.10.10.2      YES NVRAM  up                    up

Serial2/0                  172.16.1.6      YES manual up                    up

Serial2/1                  10.5.0.2        YES manual up                    up

Serial2/2                  unassigned      YES NVRAM  administratively down down

Serial2/3                  unassigned      YES NVRAM  administratively down down

FastEthernet3/0            192.168.2.1     YES NVRAM  up                    up

FastEthernet3/1            10.10.2.17      YES manual up                    up
```

Figure IV. 8- Configuration de base du routeur Backup

```
SiteDistant1#sh ip int br
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            192.168.16.1    YES NVRAM  up                    up

FastEthernet1/0            unassigned      YES NVRAM  administratively down down

Serial2/0                  172.16.1.10     YES NVRAM  up                    up

Serial2/1                  10.10.10.6      YES NVRAM  up                    up

Serial2/2                  10.1.0.2        YES NVRAM  up                    up
```

Figure IV. 9- Configuration de base du routeur du site 1

```
iteDistant2#sh ip int br
nterface                  IP-Address      OK? Method Status                Prot
col
astEthernet0/0            192.168.15.1    YES NVRAM  up                    up

astEthernet1/0            unassigned      YES NVRAM  administratively down down

erial2/0                  10.10.10.10     YES NVRAM  up                    up

erial2/1                  172.16.1.14     YES NVRAM  up                    up

erial2/2                  10.2.0.2        YES manual up                    down
```

Figure IV. 10- Configuration de base du routeur du site 2

```
SiteDistant3#sh ip int br
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            192.168.19.1    YES NVRAM  up                    up

FastEthernet1/0            unassigned      YES NVRAM  administratively down down

Serial2/0                  10.10.10.14     YES NVRAM  up                    up

Serial2/1                  172.16.1.18     YES NVRAM  up                    up

Serial2/2                  10.3.0.2        YES manual up                    down
```

Figure IV. 11- Configuration de base du routeur du site 3

```
RMS#show ip int br
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            unassigned      YES unset  administratively down down

Serial1/0                  172.16.1.1      YES manual up                    up

Serial1/1                  172.16.1.5      YES manual up                    up

Serial1/2                  172.16.1.9      YES manual up                    up

Serial1/3                  172.16.1.13     YES manual up                    up

Serial2/0                  172.16.1.17     YES manual up                    up
```

Figure IV. 12- Configuration du nuage RMS

```
Satellite#sh ip int br
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            unassigned      YES NVRAM  administratively down down

Serial1/0                  10.1.0.1        YES NVRAM  up                    up

Serial1/1                  10.4.0.1        YES NVRAM  up                    up

Serial1/2                  10.2.0.1        YES NVRAM  up                    up

Serial1/3                  10.3.0.1        YES NVRAM  up                    up

Serial2/0                  10.5.0.1        YES manual up                    up
```

Figure IV. 13- Configuration de base du Satellite

IV.9.2 Le routage

IV.9.2.1 Routage statique

Afin d'assurer le routage de trafic entre les différents sites, nous avons utilisé du routage statique et dynamique. Nous avons mis en place des routes statique entre le routeur de production et son Backup ainsi que des routes dans chaque routeur qui mène vers le nuage RMS et le satellite. Les figures IV.18, IV.19, IV.20, IV.21 et IV.22 illustrent la configuration des routes statiques. La configuration des autres sites distants se fait de la même manière.

```
Prod#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Prod(config)#ip route 192.168.2.0 255.255.255.0 10.10.10.2
Prod(config)#ip route 10.10.2.16 255.255.255.240 10.10.10.2
Prod(config)#ip route 172.16.1.8 255.255.255.252 172.16.1.1
Prod(config)#ip route 10.5.0.0 255.255.0.0 10.4.1.1
Prod(config)#ip route 10.1.0.0 255.255.0.0 10.4.1.1
Prod(config)#ip route 172.16.1.4 255.255.255.252 172.16.1.1
```

Figure IV. 14- Configuration du routage statique au niveau du routeur Prod

```
Backup#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Backup(config)#ip route 192.168.1.0 255.255.255.0 10.10.10.1
Backup(config)#ip route 10.10.2.0 255.255.255.240 10.10.10.1
Backup(config)#ip route 172.16.1.0 255.255.255.252 172.16.1.5
Backup(config)#ip route 172.16.1.8 255.255.255.252 172.16.1.5
Backup(config)#
Backup(config)#ip route 10.4.0.0 255.255.0.0 10.5.0.1
Backup(config)#ip route 10.1.0.0 255.255.0.0 10.5.0.1
```

Figure IV. 15- Configuration du routage statique au niveau du routeur Backup

```
RMS#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RMS(config)#ip route 192.168.1.0 255.255.255.0 172.16.1.2
RMS(config)#ip route 10.10.2.0 255.255.255.240 172.16.1.2
RMS(config)#ip route 192.168.2.0 255.255.255.0 172.16.1.6
RMS(config)#ip route 10.10.2.16 255.255.255.240 172.16.1.6
RMS(config)#ip route 192.168.16.0 255.255.255.0 172.16.1.10
```

Figure IV. 16- Configuration du routage statique au niveau du nuage RMS

```
Satellite#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Satellite(config)#ip route 192.168.1.0 255.255.255.0 10.4.0.2
Satellite(config)#ip route 10.10.2.0 255.255.255.240 10.4.0.2
Satellite(config)#ip route 192.168.2.0 255.255.255.0 10.5.0.2
Satellite(config)#ip route 10.10.2.16 255.255.255.240 10.5.0.2
Satellite(config)#ip route 192.168.16.0 255.255.255.0 10.1.0.2
```

Figure IV. 17- Configuration du routage statique au niveau du Satellite

```
SiteDistant1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SiteDistant1(config)#ip route 172.16.1.0 255.255.255.252 172.16.1.9
SiteDistant1(config)#ip route 172.16.1.4 255.255.255.252 172.16.1.9
SiteDistant1(config)#ip route 10.4.0.0 255.255.0.0 10.1.0.1
SiteDistant1(config)#ip route 10.5.0.0 255.255.0.0 10.1.0.1
```

Figure IV. 18- Configuration du routage statique au niveau du SiteDistant 1

IV.9.2.2 Routage dynamique

Pour les lignes spécialisés, nous avons opté pour le protocole de routage dynamique EIGRP (voir dans Annexe B) en raison de sa rapidité et de sa simplicité de déploiement. Il prend également en compte la vitesse de la bande passante et le délai pour déterminer le chemin optimal.

Les figures IV.19, IV.20, IV.21, IV.22 montre la configuration du protocole EIGRP au niveau des différents routeurs.

```
Prod#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Prod(config)#router eigrp ?
  <1-65535>  Autonomous System
  WORD       EIGRP Virtual-Instance Name

Prod(config)#router eigrp 2
Prod(config-router)#network 10.10.10.4 0.0.0.3
Prod(config-router)#network 10.10.10.8 0.0.0.3
Prod(config-router)#network 10.10.10.12 0.0.0.3
Prod(config-router)#network 192.168.1.0 0.0.0.255
Prod(config-router)#network 10.10.2.0 0.0.0.15
```

Figure IV. 19- Configuration du routage dynamique au niveau du routeur Prod

```
SiteDistant1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SiteDistant1(config)#router eigrp 2
SiteDistant1(config-router)#network 192.168.16.0 0.0.0.255
SiteDistant1(config-router)#network 10.10.10.4 0.0.0.3
SiteDistant1(config-router)#
*Apr 25 18:49:35.466: %DUAL-5-NBRCHANGE: EIGRP-IPv4 2: Neighbor 10.10.10.5 (Seri
al2/1) is up: new adjacency
SiteDistant1(config-router)#exit
SiteDistant1(config)#
```

Figure IV. 20- Configuration du routage dynamique au niveau du SiteDistant 1

```
SiteDistant2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SiteDistant2(config)#router eigrp 2
SiteDistant2(config-router)#network 192.168.15.0 0.0.0.255
SiteDistant2(config-router)#network 10.10.10.8 0.0.0.3
SiteDistant2(config-router)#
*Apr 25 18:42:20.338: %DUAL-5-NBRCHANGE: EIGRP-IPv4 2: Neighbor 10.10.10.9 (Seri
al2/0) is up: new adjacency
SiteDistant2(config-router)#exit
SiteDistant2(config)#
```

Figure IV. 21- Configuration du routage dynamique au niveau du SiteDistant 2

```
SiteDistant3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SiteDistant3(config)#router eigrp 2
SiteDistant3(config-router)#network 192.168.19.0 0.0.0.255
SiteDistant3(config-router)#network 10.10.10.12 0.0.0.3
SiteDistant3(config-router)#
*Apr 25 18:54:01.398: %DUAL-5-NBRCHANGE: EIGRP-IPv4 2: Neighbor 10.10.10.13 (Ser
ial2/0) is up: new adjacency
SiteDistant3(config-router)#exit
SiteDistant3(config)#
```

Figure IV. 22- Configuration du routage dynamique au niveau du SiteDistant 3

IV.9.2.3 Authentification du protocole de routage dynamique

Afin de garantir la sécurité des mises à jour de routage, nous avons mis en place une authentification EIGRP. Nous avons généré une clé unique entre le routeur Prod et chacun des trois sites distants et une clé pour le réseau virtuel. Ensuite, nous avons attribué chaque clé à l'interface correspondante. La figure IV.26 illustre la création et l'attribution de la clé Prod-SitesDistant1, qui permet d'authentifier les routeurs Prod et SiteDistant1.

```
Prod#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Prod(config)#key chain Prod-SiteDistant1
Prod(config-keychain)#key 1
Prod(config-keychain-key)#key-string p@SD$$1prodsitedist1
Prod(config-keychain-key)#exit
Prod(config-keychain)#exit
Prod(config)#interface port-channel1
Prod(config-if)#ip authentication key-chain eigrp 2 Prod-SiteDistant1
Prod(config-if)#ip authentication mode eigrp 2 md5
Prod(config-if)#exit
```

Figure IV. 23- Création et affectation d'une clé pour l'authentification entre le routeur Prod et SiteDistant1

IV.9.3 Test de basculement

Pour tester le bon fonctionnement du routage nous avons effectué un ping à partir de la machine Windows10-prod située au LAN Prod vers la machine Windows10-1 située au Lan site 1 (Alger) comme le montre la figure V.23.

Nous avons également effectué un ping à partir de la machine Windows10-1 vers la machine WS-Prod située à la zone de serveurs Prod montré dans la figure V.24.

Windows10-prod - PuTTY

```
VPCS> ping 192.168.16.2/24

84 bytes from 192.168.16.2 icmp_seq=1 ttl=62 time=46.130 ms
84 bytes from 192.168.16.2 icmp_seq=2 ttl=62 time=36.546 ms
84 bytes from 192.168.16.2 icmp_seq=3 ttl=62 time=29.611 ms
84 bytes from 192.168.16.2 icmp_seq=4 ttl=62 time=35.138 ms
84 bytes from 192.168.16.2 icmp_seq=5 ttl=62 time=46.362 ms
```

Figure IV. 24- Basculement de client LAN Prod vers le client LAN Site1 (Alger)

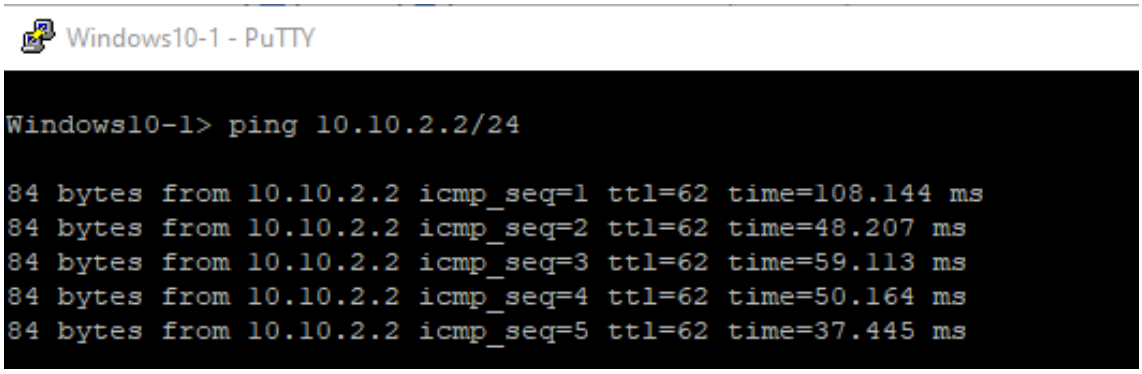


Figure IV. 25- Basculement de client LAN Site 1 vers serveur WS-Prod

IV.9.4 Configuration du DMVPN

Pour sécuriser la connexion entre les différents sites, nous avons implémenter un DMVPN (voir Annexe B). Il convient de réaliser deux types de configurations : celles dédiées aux hubs et celles aux spokes comme le montre le tableau V.5, pour une gestion centralisée du réseau.

La figure IV.26 montre la configuration du routeur Prod comme hub et la figure V.30 montre celle du routeur SiteDistant 1 comme spoke. En ce qui concerne le routeur Backup, tel qu'indiqué dans la figure IV.28, il joue à la fois le rôle de hub et de spoke. Il agit en tant que spoke lorsque le routeur Prod est fonctionnel, et en tant que hub lorsque ce dernier est en panne.

Les figures IV.27, IV.29 et IV.31 montre la nouvelle interface Tunnel0 dans le tableau de bord des interfaces des routeurs.

Une fois que le VPN est établi, il est nécessaire d'activer le routage sur celui-ci. La figure IV.32 illustre la configuration du routage sur le réseau virtuel sur le routeur Prod, et cette configuration est similaire pour les autres routeurs. Étant donné que les routes passant par le réseau virtuel ont une métrique plus élevée principalement en raison du délai (voir la formule de calcul de la métrique EIGRP (voir dans Annexe B), le réseau physique, c'est-à-dire les lignes spécialisées, est toujours privilégié sur le réseau virtuel.

Tableau IV. 5- Configurations des Hubs et des Spokes

Hub	Spoke
-Créer une interface virtuelle -Attribuer une adresse IP à cette interface -Désactiver les redirections IP -Configurer une chaine d'authentification NHRP (voir dans Annexe B). -Autoriser l'ajout automatique des routeurs aux mappage NHRP -Attribuer un identifiant à la configuration NHRP -Préciser l'interface source du tunnel -Activer l'encapsulation GRE et préciser que c'est un tunnel multipoint	-Créer une interface virtuelle -Attribuer une adresse IP à cette interface -Désactiver les redirections IP -Configurer une chaine d'authentification NHRP (voir dans Annexe B). -Autoriser l'ajout automatique des routeurs aux mappage NHRP - Mapper de manière statique les adresses logiques aux physiques des hubs -Mettre en place l'utilisation d'un protocole de routage dynamique entre le spoke et le hub et l'envoie des paquets de multidiffusion au hub -Attribuer un identifiant à la configuration NHRP -Configurer le hub en tant que serveur de saut suivant NHRP -Préciser l'interface source du tunnel -Activer l'encapsulation GRE préciser que c'est un tunnel multipoint

```
Prod#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Prod(config)#interface Tunnel 0
Prod(config-if)#
*Apr 25 19:47:11.574: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
Prod(config-if)#description VPN HUB_MPLS
Prod(config-if)#ip address 172.30.1.1 255.255.255.0
Prod(config-if)#no ip redirects
Prod(config-if)#ip nhrp authentication dmvpn
Prod(config-if)#ip nhrp map multicast dynamic
Prod(config-if)#ip nhrp network-id 1
Prod(config-if)#tunnel source se1/0
Prod(config-if)#tunnel mode gre multipoint
Prod(config-if)#exit
Prod(config)#
```

Figure IV. 26- Configuration du DMVPN au niveau du routeur Prod

```
Tunnel0                172.30.1.1      YES manual up
```

Figure IV. 27- Interface Tunnel0 au niveau du routeur Prod

```
Backup#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Backup(config)#interface Tunnel 0
Backup(config-if)#
*Apr 25 20:24:16.938: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
Backup(config-if)#description VPN HUB_MPLS
Backup(config-if)#ip address 172.30.1.2 255.255.255.0
Backup(config-if)#no ip redirects
Backup(config-if)#ip nhrp authentication dmvpn
Backup(config-if)#ip nhrp map multicast dynamic
Backup(config-if)#ip nhrp network-id 1
Backup(config-if)#tunnel source se2/0
Backup(config-if)#tunnel mode gre multipoint
Backup(config-if)#
Backup(config-if)#ip nhrp map multicast dynamic
Backup(config-if)#ip nhrp map 172.30.1.1 172.16.1.2
Backup(config-if)#ip nhrp map multicast 172.16.1.2
Backup(config-if)#ip nhrp nhs 172.30.1.1
Backup(config-if)#exit
Backup(config)#exit
Backup#
```

Figure IV. 28- Configuration du DMVPN au niveau du routeur Backup

```
Tunnel0                172.30.1.2      YES NVRAM  up                    up
```

Figure IV. 29- Interface Tunnel0 au niveau du routeur Backup

```
SiteDistant1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SiteDistant1(config)#interface Tunnel 0
SiteDistant1(config-if)#
*Apr 25 20:44:24.102: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
SiteDistant1(config-if)#description SiteDistant 1 mGRE - DMVPN Tunnel
SiteDistant1(config-if)#ip address 172.30.1.3 255.255.255.0
SiteDistant1(config-if)#no ip redirects
SiteDistant1(config-if)#ip nhrp authentication dmvpn
SiteDistant1(config-if)#ip nhrp multicast dynamic
SiteDistant1(config-if)#ip nhrp map 172.30.1.1 172.16.1.2
SiteDistant1(config-if)#ip nhrp map 172.30.1.2 172.16.1.6
SiteDistant1(config-if)#ip nhrp map multicast 172.16.1.2
SiteDistant1(config-if)#ip nhrp map multicast 172.16.1.6
SiteDistant1(config-if)#ip network-id 1
SiteDistant1(config-if)#ip nhrp nhs 172.30.1.1
SiteDistant1(config-if)#ip nhrp nhs 172.30.1.2
SiteDistant1(config-if)#tunnel source se2/0
SiteDistant1(config-if)#tunnel mode gre multipoint
SiteDistant1(config-if)#exit
SiteDistant1(config)#
```

Figure IV. 30- Configuration du DMVPN au niveau du routeur du SiteDistant 1

```
Tunnel0                172.30.1.3      YES NVRAM  up                    up
```

Figure IV. 31- Interface Tunnel0 au niveau du routeur du SiteDistant 1

```
Prod#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Prod(config)#router eigrp 2
Prod(config-router)#network 172.30.1.0 0.0.0.255
Prod(config-router)#exit
Prod(config)#
```

Figure IV. 32- Configuration du routage sur le réseau virtuel au niveau du routeur Prod

IV.10 Implémentation du SD-WAN Overlay

IV.10.1 Déploiment des par-feus Fortigate

IV.10.1.1 Fortigate NGFW

Fortigate NGFW est un pare-feu réseau développé par le constructeur Fortinet considéré comme le pare-feu réseau le plus répandu à l'échelle mondiale. Le FortiGate NGFW offre une protection de sécurité avancée et une surveillance des menaces inégalées grâce à l'intelligence artificielle. Il permet également une visibilité complète et une convergence optimale entre la sécurité et le réseau. [W7]

Pour implémenter le SD-WAN overlay, nous avons d'abord placé les par-feus Fortigate sur notre architecture underlay existante, qui offrent un SD-WAN sécurisé rapide, évolutif et flexible sur site.

Ces Firewalls de Fortinet ont la capacité de détecter et d'analyser le trafic de la couche 7 du modèle OSI, ce qui signifie qu'ils permettent la mise en place des policies basées sur les applications pour autoriser ou bloquer le trafic réseau, et non seulement sur les adresses IP. Par conséquent, il est possible de limiter l'accès à une application aux seuls utilisateurs concernés, au lieu d'accorder l'accès à tout un réseau.

Remarque : Après la mise en place des pares-feux, évidemment il va y avoir des modifications dans l'adressages d'où le routage.

Le tableau IV.6 montre les différents pares-feux que nous avons mis en place.

Tableau IV. 6- Pares-feux Fortigate NGFW déployés

Pare-feu	Nombre d'interface	Interface	Adresse IP
Production	3	Intranet	10.10.1.2
		LAN utilisateurs	192.162.1.1
		Zone Serveurs	10.10.2.1
Backup	3	Intranet	10.10.1.6
		LAN utilisateurs	192.168.5.1
		Zone Serveurs	10.10.2.17
Site 1	2	Intranet	10.10.1.3
		LAN	192.168.16.1
Site 2	2	Intranet	10.10.1.11
		LAN	192.168.15.1
Site 3	2	Intranet	10.10.1.19
		LAN	192.168.19.1

IV.10.2 Architecture Underlay/Overlay

La figure IV.33 montre l'architecture après la mise en place des Fortigate NGFW.

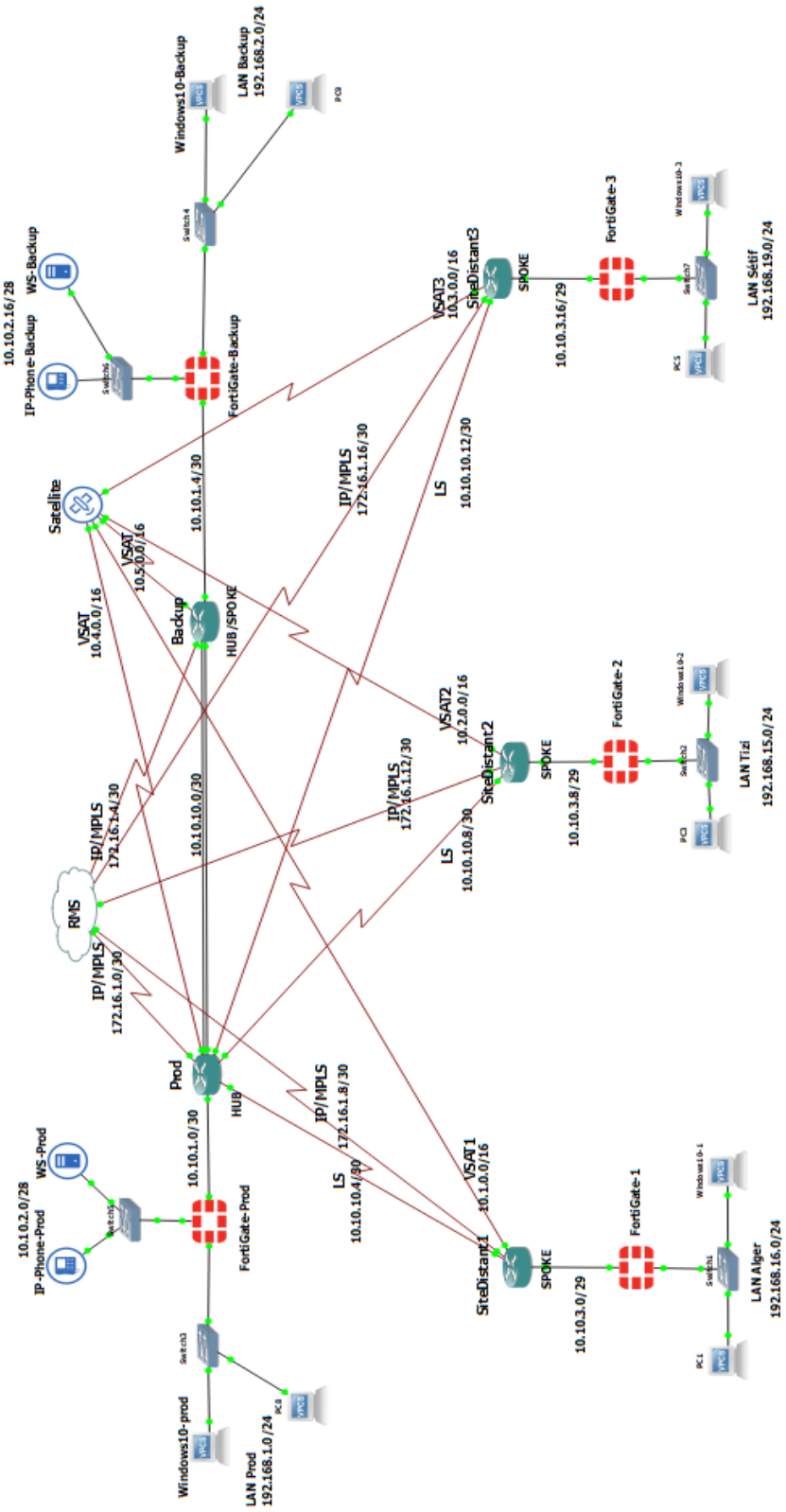


Figure IV. 33- Architecture après la mise en place des pares-feux Fortigate NGFW

IV.10.3 Mise en Place de SD-WAN Fortinet sur la Plateforme Graphique FortiGate

IV.10.3.1 configuration des interfaces

La figure IV.34 Montre la configuration des interfaces du pare-feu de site distant 1. Pour l'interface management nous avons autorisé l'accès http et https pour permettre l'accès à l'interface graphique du pare-feu, quant au reste des interfaces nous avons permis le Ping pour tester la connectivité.

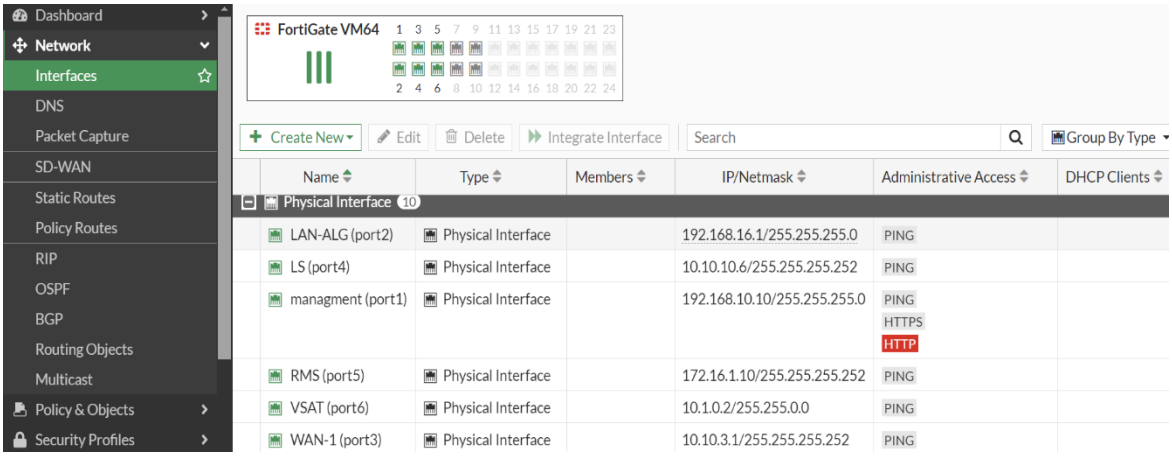


Figure IV. 34- Résultat de la configuration des interfaces du site distant 1

IV.10.3.2 Configuration des Adresses

Nous allons à présent configurer les adresses IP des serveurs et des ordinateurs dans l'interface graphique de FortiGate. Prenons l'exemple du serveur Voice/data WS. PROD et de l'ordinateur Windows10.1. Pour commencer, nous nous rendons dans Policy & Objects > Addresses. Pour ajouter une nouvelle adresse, il suffit de cliquer sur "add new " et de remplir les informations requises. Par exemple, pour le serveur, nous indiquons le nom WS. PROD, l'adresse IP du serveur 10.10.2.3 de type IP range comme le montre la figure IV.35. De même, pour l'ordinateur du réseau local, nous spécifions le nom Windows10.1 et l'adresse IP de l'ordinateur. Une fois les détails remplis, il ne reste plus qu'à cliquer sur OK pour enregistrer chaque adresse. Enfin, si nécessaire, nous pouvons configurer des politiques de sécurité pour autoriser le trafic entre le serveur et l'ordinateur Windows.

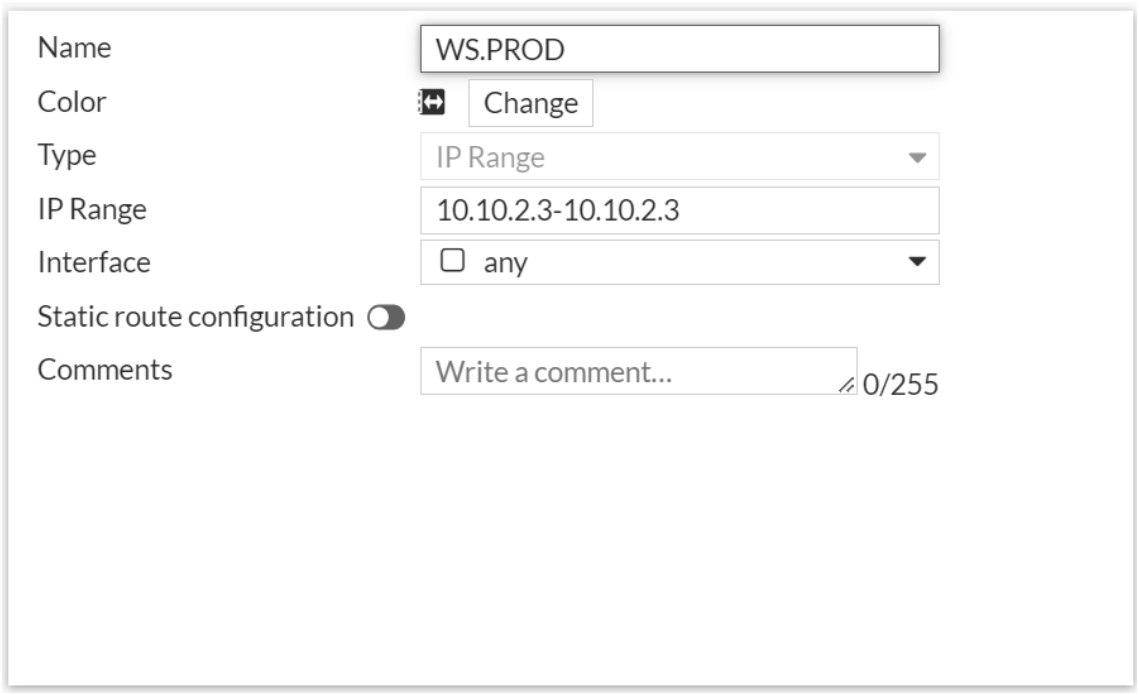


Figure IV. 35- Configuration des adresses du server voix/data WS. PROD

WS.PROD	10.10.2.3 - 10.10.2.3		Address
window10-1	192.168.16.0/24		Address

Figure IV. 36- Résultat de configuration des adresses du serveur et de la machine Windows

Il est nécessaire de configurer les adresses IP de nos serveurs et PC avant de mettre en place le SD-WAN dans FortiGate afin d'assurer une gestion optimale du trafic réseau, une sécurité adéquate et une configuration précise du SD-WAN. Cette étape garantit également que les flux de trafic sont acheminés correctement vers les destinations appropriées, ce qui permet d'optimiser les performances de notre réseau.

IV.10.3.3 Configuration de routage statique

Le processus de configuration est similaire à celui décrit précédemment, mais cette fois-ci, nous l'avons réalisé dans l'interface graphique de FortiGate. Afin de mettre en place le routage statique sur notre FortiGate , nous avons créé des routes pour chaque Next hop requis. Nous avons tout d'abord établi une route vers le réseau du routeur du site distant 1, en utilisant l'adresse IP du routeur comme prochain saut. Ensuite, nous avons défini des routes distinctes pour chaque liaison (LS, VSAT, RMS) en utilisant l'adresse IP du routeur comme prochain saut pour chaque réseau spécifique. De plus, nous avons ajouté une route pour le deuxième FortiGate via le routeur prod, ainsi qu'une dernière route vers notre serveur à travers le

deuxième FortiGate. Ces paramétrages assurent que le trafic est correctement dirigé à travers les divers appareils de notre réseau en fonction des besoins.

Figure IV. 37- La table du routage statique

IV.10.3.4 mise en place des zones et members SD-WAN

Les zones SD-WAN améliorent la gestion du trafic réseau en regroupant des interfaces similaires en une seule entité de gestion.

Nous pouvons soit créé une zone SD-WAN ou utiliser les zones par défaut qui existent déjà et sur lesquelles on peut appliquer les modifications désirées. Dans notre cas on éditera la zone VirtualWan-link.

Nous ajouterons également de nouveaux membres à cette zone, Pour créer un SD-WAN member accéder à la Configuration des Zones SD-WAN

- Cliquez sur Create New.
- Cliquez sur SD-WAN member
  Comme le montre la figure si dessous :

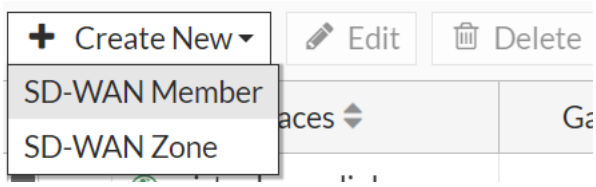


Figure IV. 38- La première étape pour crée SD-WAN member

Nous allons créer trois SD-WAN members : LS, RMS, et V-SAT. Chaque member SD-WAN sera associée à son interface respective pour optimiser la gestion du trafic et garantir une performance réseau adéquate.

- Remplissez les détails pour la nouvelle SD-WAN member comme le montre les figures IV.39, IV.40, IV.41 :

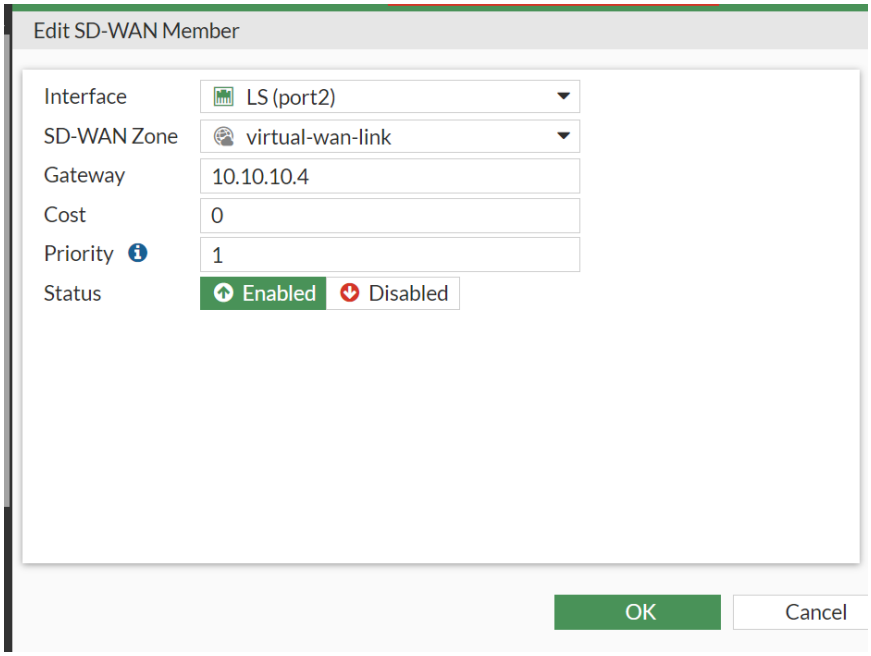


Figure IV. 39- Attribuation de l'interface LS dans la zone SD-WAN

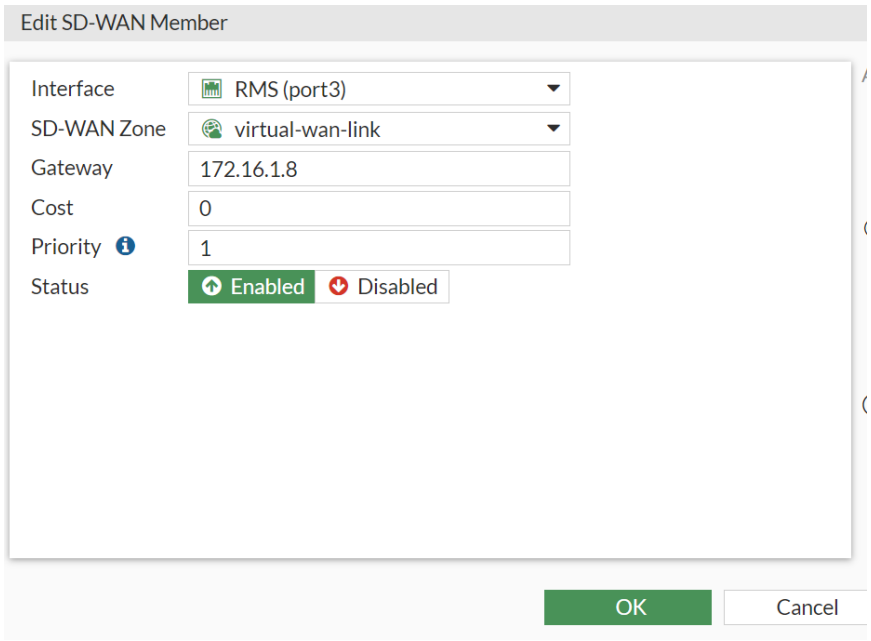


Figure IV. 40- Attribuation de l'interface RMS dans la zone SD-WAN

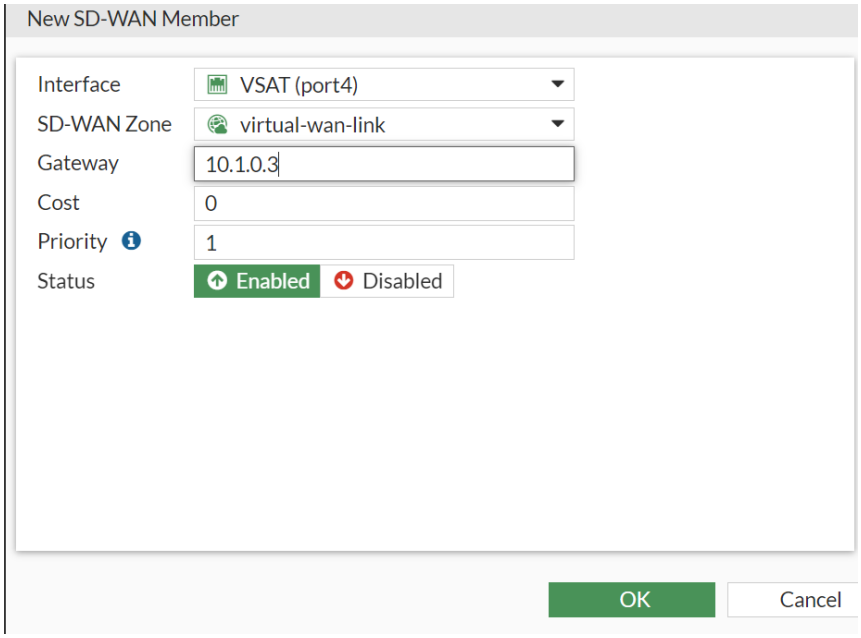


Figure IV. 41- Attribuation de l'interface VSAT dans la zone SD-WAN

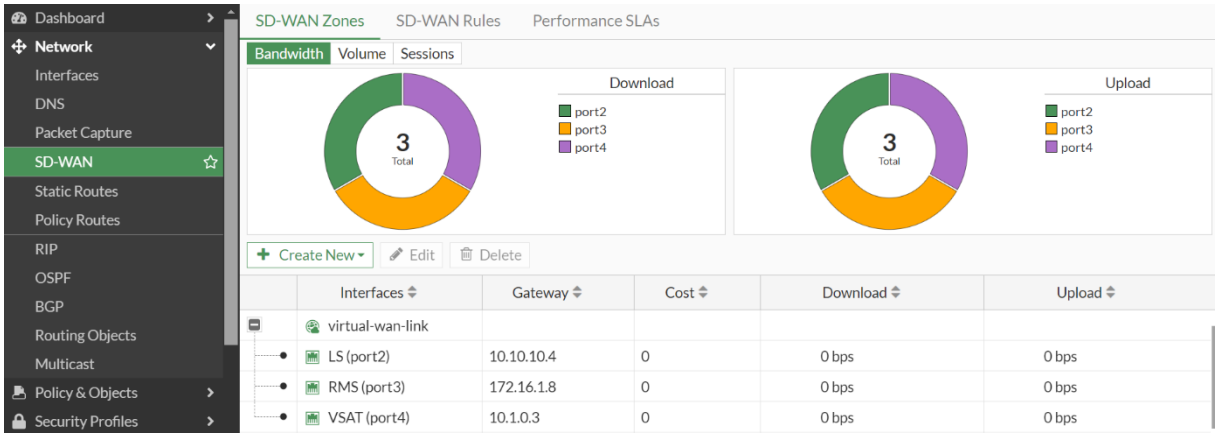


Figure IV. 42- Affichage de la conception du SD-WAN zone

IV.10.3.5 Ajustement des Performances SLA

Après avoir créé les membres SD-WAN (LS, RMS, V-SAT) et les avoir associées à leurs interfaces respectives, l'étape suivante consiste à ajuster les performances SLA (Service Level Agreement) pour garantir que chaque type de trafic respecte les exigences de qualité de service (QoS). Dans notre cas, nous allons créer deux types de SLA : un pour le trafic voix et un pour le trafic data. Pour le trafic voix, nous utiliserons les liaisons LS et RMS, et pour le trafic data, nous utiliserons les liaisons RMS, LS, et VSAT, dans cet ordre.

- Étapes de Configuration des Performances SLA
  - Cliquez sur performance SLAs.

- Cliquez sur Create New.
- Donner un nom de “VOICE” pour le trafic voix et “DATA” pour le trafic data

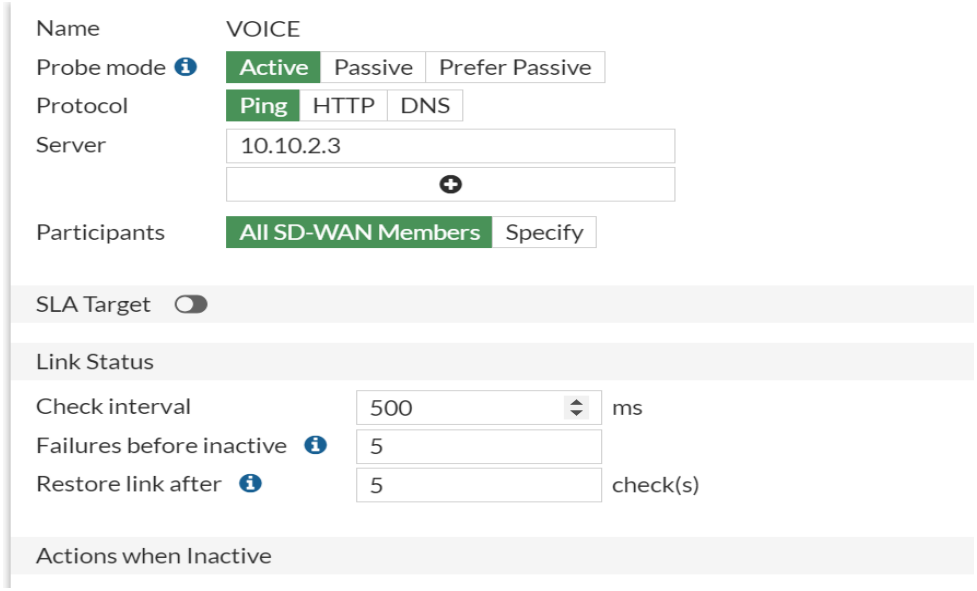


Figure IV. 43- Ajustement du SLA du trafic voix

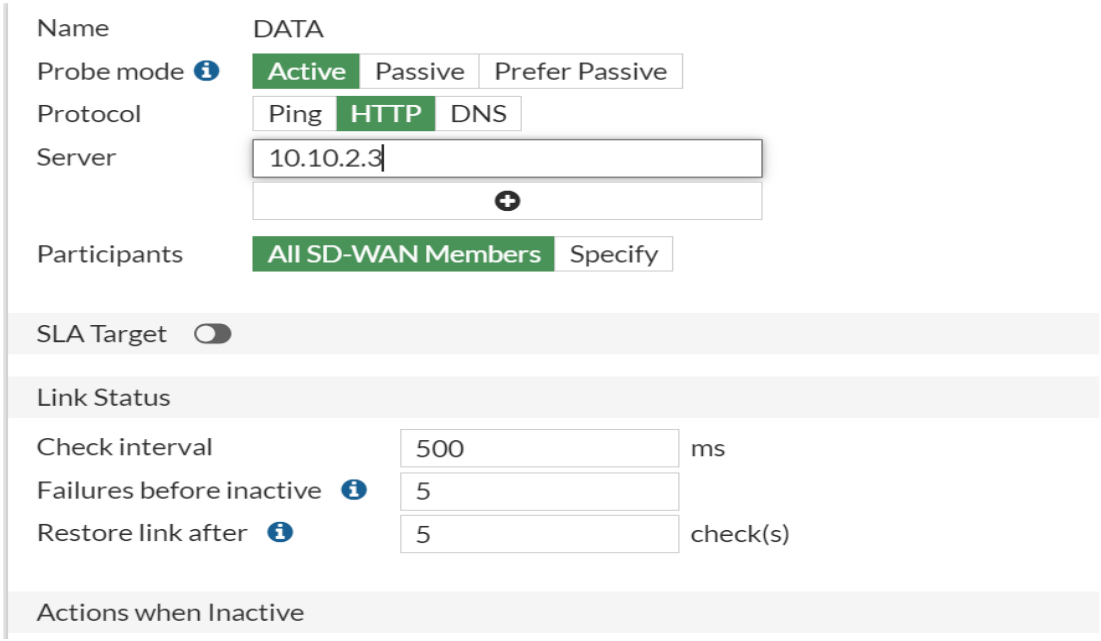


Figure IV. 44- Ajustement du SLA du trafic data

Dans notre cas, nous avons choisi de ne pas ajuster les paramètres de jitter, latence et perte de paquets directement dans la configuration des SLA. Au lieu de cela, nous préférons effectuer ces ajustements dans les règles SD-WAN pour une gestion plus granulaire et flexible.

IV.10.3.6 Configuration des Règles SD-WAN

Nous avons configuré des règles SD-WAN sur FortiGate afin d'optimiser la performance du réseau en priorisant le trafic Voix et Data. Voici les détails de notre configuration :

Nous avons tout d'abord sélectionné l'adresses IP source ainsi que l'adresses IP destination. Ensuite, nous avons choisi meilleure qualité (best quality) comme une stratégie pour choisir les interfaces sortantes dans l'ordre de priorité (par exemple, LS, puis RMS pour le Trafic voix) pour assurer une gestion efficace du trafic sur notre réseau.

- Trafic Voix :

- Jitter : Nous avons configuré un jitter de ≤ 20 ms. Cela garantit une transmission audio fluide et sans interruptions pour les appels VoIP.

- Latence : Une latence de ≤ 150 ms a été choisie pour maintenir des conversations vocales réactives et sans délai perceptible.

- Perte de Paquets : Nous avons limité la perte de paquets à ≤ 1%, minimisant ainsi les distorsions dans la qualité audio.

- Bande Passante : Nous avons alloué entre 100 kbps et 150 kbps par appel VoIP, assurant un flux audio constant et de haute qualité.

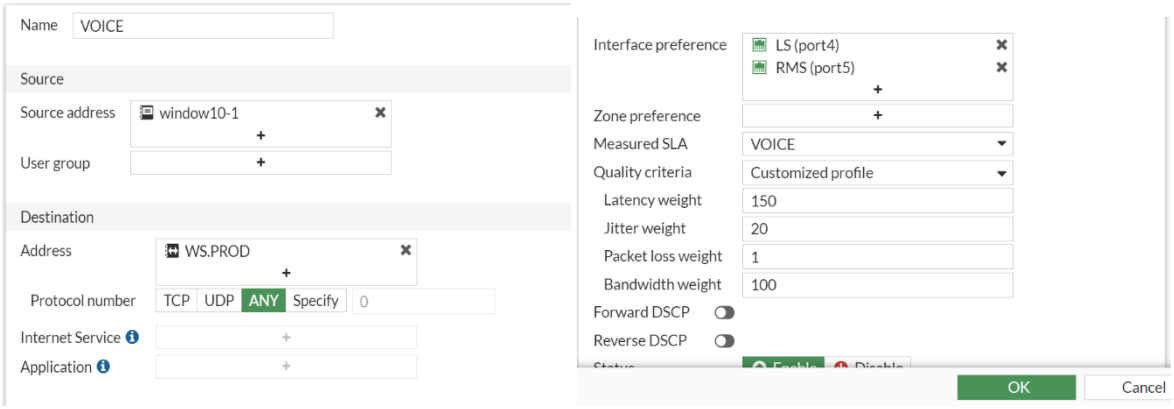


Figure IV. 45- Configuration des règles du trafic voix

- Trafic Data :

- Jitter : Pour le trafic Data, un jitter de ≤ 50 ms a été configuré pour garantir des performances suffisantes pour les applications data.

- Latence : Une latence de ≤ 300 ms a été définie, ce qui est acceptable pour les applications data.

- Perte de Paquets : Une perte de paquets de ≤ 2%

- Bande Passante : 500 kbps pour les meilleures performances.

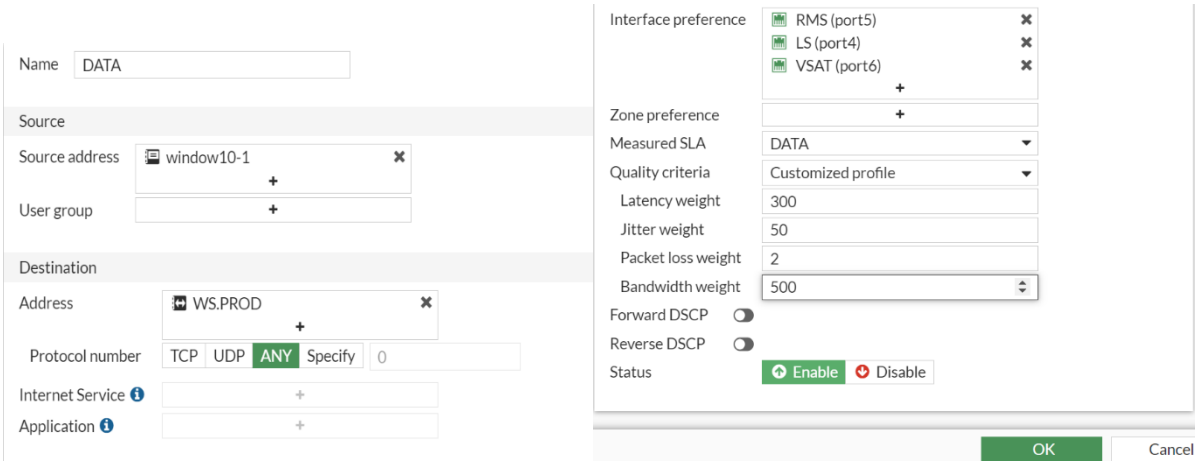


Figure IV. 46- Configuration des règles du trafic Data

Avant de procéder aux tests, nous avons appliqué les mêmes procédures sur l'autre FortiGate pour garantir que le trafic peut revenir du serveur au PC Windows 10. Cela inclut la configuration des interfaces, des routes statiques, des zones SD-WAN et des règles de performance SLA, avec des ajustements spécifiques aux adresses IP appropriées. Cette réplique de configuration permet d'assurer que le flux de données est correctement acheminé dans les deux sens, entre le PC Windows et le serveur, via les routes et interfaces définies.

IV.10.3.7 Test de Fonctionnement et Résultats de la Simulation du Trafic Voix

Pour tester la configuration SD-WAN de Fortinet, nous avons créé une machine virtuelle dans VMware afin de simuler un PC Windows 10 et émuler le trafic réseau. Cette machine virtuelle a été configurée avec des adresses IP correspondant aux interfaces configurées sur le FortiGate. Nous avons utilisé cette machine virtuelle pour effectuer des tests de connectivité en utilisant des commandes de ping pour vérifier la communication avec le FortiGate

1. Création de la Machine Virtuelle :

- Plateforme : VMware
- Objectif : Simuler le trafic réseau pour les tests.

2. Configuration de la Machine Virtuelle :

- Adresses IP : Configurées pour correspondre aux interfaces testées.

Les adresses IP ont été attribuées à la machine virtuelle pour correspondre aux interfaces configurées sur le FortiGate.

3. Tests de Connectivité

- Ping : Utilisé pour vérifier la connectivité entre la VM et les interfaces FortiGate.

Ces tests étaient essentiels pour évaluer le basculement du trafic voix et le load balancing pour vérifier la performance et l'efficacité de notre solution SD-WAN Fortinet et nous avons obtenu le résultat si dessous. Nous pouvons observer plusieurs cercles colorés représentant les ports utilisés :

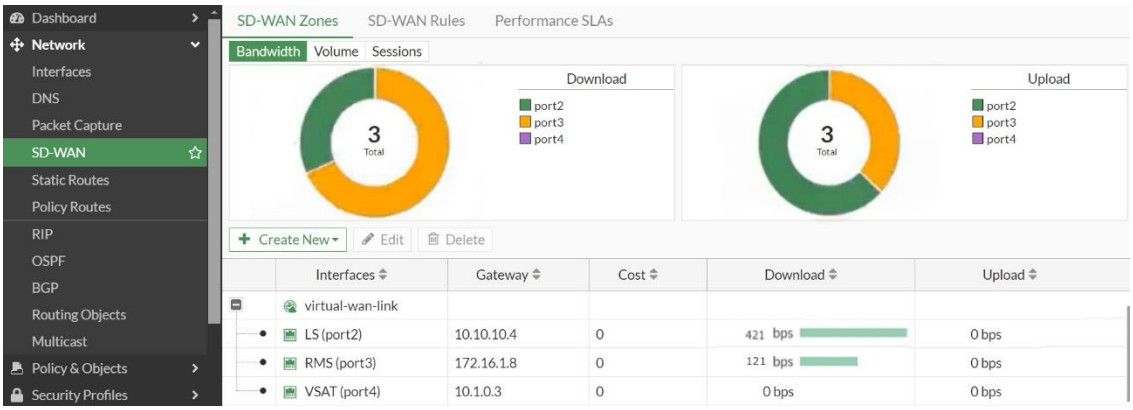


Figure IV. 47- Affichage de la répartition de charge entre les interfaces

Le port VSAT n'a pas été utilisé pour le trafic voix, conformément aux configurations établies. En conséquence, il n'est pas visible dans les cercles représentant les ports utilisés pour le trafic voix sur la figure IV.47. Cette configuration permet de réserver le port VSAT pour d'autres types de trafic ou pour des situations où les autres liens seraient indisponibles, tout en s'assurant que le trafic voix bénéficie de la meilleure connexion possible.

La ligne LS a été choisie comme la première option pour le trafic voix, comme configurée dans les paramètres de SD-WAN. Cette décision est basée sur les exigences spécifiques de la voix sur IP (VoIP) qui nécessite une faible latence et une stabilité élevée. Le jitter, qui mesure la variation du délai des paquets, a été évalué et optimisé pour cette ligne afin de garantir une qualité de service (QoS) supérieure pour les communications vocales.

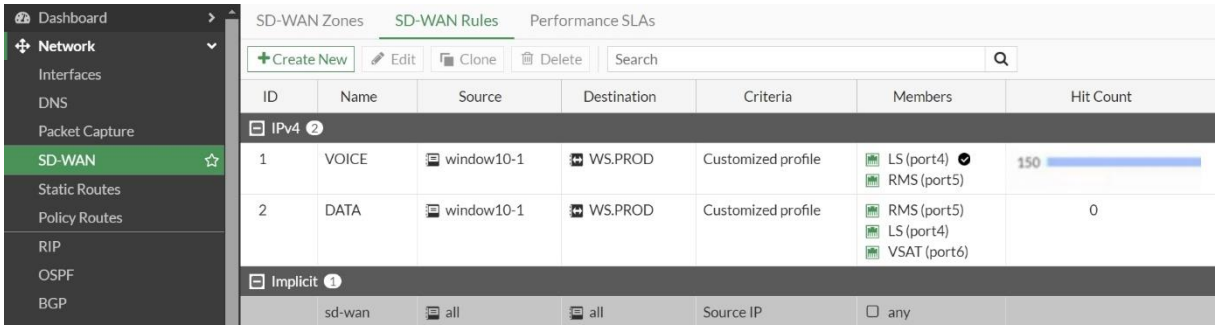


Figure IV. 48- Visualisation de l'état de fonctionnement

L'affichage du graphique SLA est un autre outil à ne pas manquer et qui suscitera l'attention des administrateurs. Il s'agit d'un affichage en direct des graphiques de performance de chaque lien du réseau, y compris jitter, latence et perte de paquets. Certains des métriques utilisées pour mesurer la qualité du lien incluent : Jitter est mesuré en tant que la variation des temps d'arrivée des paquets. Un jitter nul permet à la VoIP de fonctionner sans heurts.

Latence est mesurée à travers la durée qu'il faut pour qu'un paquet de données traverse le lien. Plus la latence est faible, plus les communications en temps réel sont efficaces.

Perte de Paquets est mesurée en pourcentage de paquets perdus en transit. Une faible perte de paquet est cruciale pour l'intégrité des données.

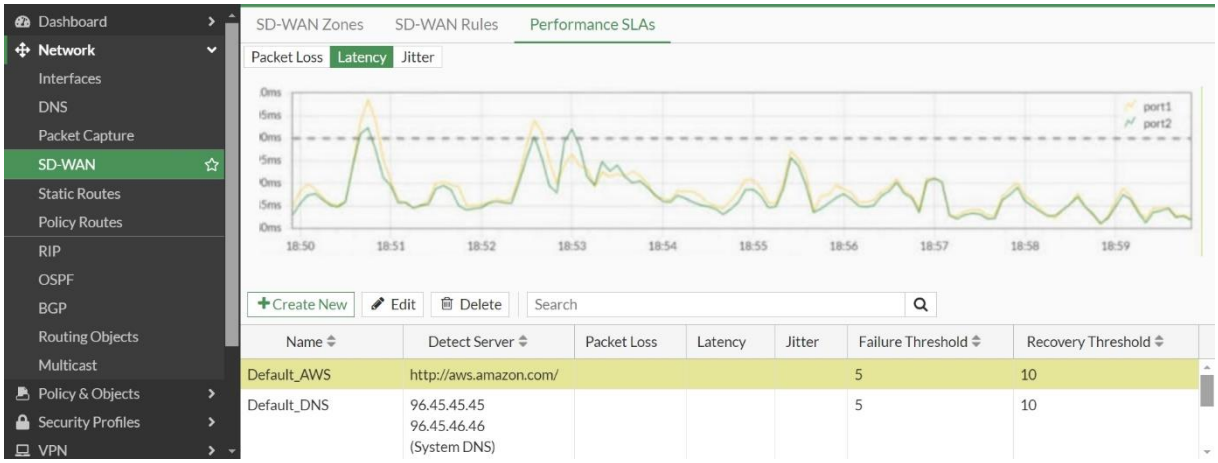


Figure IV. 49- Graphique de performance SLA SD-WAN

Conclusion

Dans ce chapitre, nous avons décrit l'architecture de base avec tous ces détails et les ressources utilisé, puis la configuration de cette architecture, ensuite l'implémentation et la simulation de notre solution overlay SD-WAN sur notre architecture : d'abord le déploiement des Fortigate NGFW, ensuite la configuration des interfaces, les adresses IP et le routage sur la plateforme Fortigate, puis la définition des zones SD-WAN et le test.

Conclusion générale

Conclusion générale

Ce mémoire a exploré l'importance des infrastructures WAN modernes et les défis associés aux réseaux traditionnels. Après avoir étudié les limitations des réseaux traditionnels et l'évolution vers les réseaux de nouvelle génération (NGN), nous nous sommes concentrés sur le SD-WAN. Les réseaux WAN traditionnels souffraient de problèmes de réactivité, de complexité de gestion et de coûts élevés. En revanche, le SD-WAN offre une solution innovante avec des capacités de virtualisation et de programmabilité, permettant une gestion optimisée des réseaux étendus.

En analysant les différentes solutions disponibles, nous avons choisi d'implémenter le SD-WAN de Fortinet en raison de ses fonctionnalités avancées et de sa robustesse. L'implémentation pratique de cette solution sur une plateforme réseau WAN multi-mesh a montré des améliorations significatives en termes de gestion de la bande passante, de résilience du réseau et de simplification de l'architecture. Les tests effectués ont confirmé que cette solution répond efficacement aux exigences des environnements réseau modernes, en offrant une architecture moins complexe et plus performante.

Ce projet de master a permis de démontrer les avantages pratiques de la solution SD-WAN de Fortinet pour les entreprises. Cette solution représente une option supérieure pour les nouvelles entreprises, offrant une infrastructure réseau performante, adaptable et moins complexe. En adoptant cette solution, les entreprises peuvent optimiser leurs ressources réseau et améliorer les performances de leurs infrastructures WAN.

Bibliographie

Bibliographie

[1] Mohamed Chahidi, Amira Aboura. Le système bancaire algérien : Évolution historique. Libéralisation du secteur et défi de modernisation. Journal of Economics and Management. Université Ahmed Draya, d'Adrar, 01-03-2017

[2] Atelin, P. « Réseaux informatiques Notions fondamentales », 3éme édition, Ed ENI, 2006

[3] Bellili, N. « *Sécurité et Monitoring d'un réseau informatique. Cas SARL RAMDY* », mémoire de Master, Université A/Mira de Bejaia, 2021

[4] Mohammed M Alani. Guide to OSI and TCP/IP models. Springer cham heidelberg New-York dordrecht LONDON,2017.

[5] Madani, H. « *Planification sur un réseau mobile basé sur une topologie IP* », mémoire de Master. Université Abderrahmane MIRA de Béjaia, 2013

[6] Zeghida, A. *« Communication entre station S7-1200 et plateforme Arduino via Modbus TCP/IP* », mémoire de Master. Université Badji Mokhtar-Annaba, 2016

[7] Sadoud.L, saddedine .M, « *Implémentation d'une solution d'interconnexion entre deux forets différents avec une relation d'approbation et VPN site a site* ». Mémoire de Master. Université MOULOUD MAMMERI, TIZI-OUZOU.

[8] CHIKHI.Mehdi, DJEMIL Adel « *Etude et implémentation de l'approche Software Defined Network dans un réseau local* ». Mémoire de Master. Université SAAD DAHLEB, BLIDA

[9] Jérôme Durand, « *Le SDN pour les nuls* », Montpellier, Article JRES 2015.

[10] AICHAOUI.A, AITBELKACEM.Y *« Etude et implémentation d'une architecture SDN LAN* » Mémoire de Fin d'Etudes De MASTER ACADEMIQUE. UNIVERSITE Mouloud MAMMERI -TIZI- OUZOU

[11] Junos® OS OpenFlow User Guide (juniper.net)

[12] Open Networking Fondation, « *OpenFlow Switch Specification* », PDF, le 27 Septembre 2013

[13] Traore Issa, Kouassi Brou Médard, Atta A. Ferdinand « *Etude du nomadisme dans un Cloud éducatif administré par la technologie SDN/OpenFlow* ». Actes de la conférence

WACREN 2016, Institut de recherches mathématique Université Félix Houphouët-Boigny, Abidjan, Côte d'Ivoire.

[14] GUETTACHE.O, HAMDI.M « *Etude et implémentation d'une approche SDN dans un réseau LAN* ». UNIVERSITE M'HAMED BOUGARA BOUMERDES, FACULTE DE TECHNOLOGIE.

[15] H. Jamjoom, D. Williams, et U. Sharma, « *Don't call them middleboxes, call them middlepipes* », HotSDN 2014 - Proc. ACM SIGCOMM 2014 Workshop Hot Topics Software Defined Networking. Août 2014.

[16] LAOUAR.A, BOUAZIZ.A « *IPv6 Traffic-Controller : Un assistant pour le contrôle du trafic IPv6 dans un réseau SDN* ». Mémoire de Master. Centre Universitaire ABDELHAFID BOUSSOUF, MILA

[17] BEN SAAD.N « *Migration Graduelle d'une infrastructure DMVPN*
Vers Une architecture SD-WAN Au Niveau de NAFTAL ». Mémoire de Master. Université SAAD DAHLAB Blida-1-Faculté de Sciences.

Webographie

[W1] https://www.bank-of-algeria.dz/ , consulte le 15-03-2024

[W2] https://www.fibermall.com/fr/blog/core-distribution-and-assess-layer.htm, consulte le 15-03-2024

[W3] https://cisco.goffinet.org/ccna/ethernet/principes-conception-lan-cisco/, consulte le 18-03-2024

[W4]https://www.snaplogic.com/blog/data-plane-vs-control-plane-whats-the-difference, consulté le 20/03/2024

[W6] https://www.arcep.fr/uploads/tx_gspublication/etd-ovum-ngn-0106.pdf, consulte le 20-03-2024

[W7] https://www.napsis.fr/actualite/mpls/, consulte le 30-03-2024

[W8]https://forum.huawei.com/enterprise/fr/c-est-quoi-le-protocole-ppp-point-to-point-protocol/thread/667501764628332545-667481008070602752, consulte le 31-03-2024

[W9]https://polaridad.es/fr/protocolo-hdlc-guia-completa-del-sdlc-synchronous-data-link-control/ , consulte le 31-03-2024

[W10]https://www.scribd.com/document/644147221/Chapitre-3-Liaisons-Specialisees, consulte le 02-04-2024

[W11] https://globaltelnetworks.net/1-connexion-internet-par-satellite, consulte le 03-04-2024

[W12] https://community.fs.com/article/a-closer-look-at-overlay-and-underlay-network.html, consulté le 05-04-2024

[W13] https://actualiteinformatique.fr/internet-of-things-iot/definition-mesh-network,consulte le 07-04-2024

[W14] https://www.niagara.tech/blog/tout-savoir-sur-le-software-defined-networking#:~:text=Software%20Defined%20Networking%20%3F-,Historique%20et%20%C3%A9volution%20du%20SDN,r%C3%A9seaux%2C%20plus%20flexible%20et%20adapt%C3%A9e ,consulte le 01-04-2024

[W15] https://blog.wescale.fr/sdn-principes-et-fonctionnement , consulté le 01-04-2024

[W16] https://www.gdit.com/perspectives/latest/4-benefits-of-moving-to-software-defined-networking/ , consulté le 30-03-2024

[W17] https://www.fortinet.com/resources/cyberglossary/sd-wan-explained, consulté le 09-05-2024

[W18] https://forum.huawei.com/enterprise/fr/diff%C3%A9rences-entre-wan-et-sd-wan/thread/, consulté le 09-05-2024

[W19] https://securuscomms.co.uk/what-is-hybrid-sd-wan/ , consulté le 11-05-2024

[W20] https://www.paloaltonetworks.com/cyberpedia/sd-wan-architecture, consulté le 12-05-2024

[W21] https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf, consulté le 12-05-2024

[W22] Huawei SD-WAN Solution Datasheet.pdf, consulté le 12-05-2024

[W23] sb-sdwan-simplified-operations.pdf, consulté le 13-05-2024

[W24] https://www.digital-liance.com/actualite/255-sd-wan-fortinet-la-solution-pour-votre-entreprise.html , consulté le 15-05-2024

[W25] https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinet_secure_sdwan.pdf, consulté le 15-05-2024

[W26] https://gns3.fr.softonic.com/ , consulté le 01-05-2024

[W27] https://docs.gns3.com/docs/ , consulté le 01-05-2024

[W28] https://www.blogdumoderateur.com/tools/vmware-workstation-player/, consulté le 01- 05-2024

[W29] https://accesscomputer.ma/fr/page/Qu%E2%80%99est-ce-que-VMware-Workstation, consulté le 01-05-2024

[W30] https://www.qemu.org/docs/master/about/index.html, consulté le 01-05-2024

[W31] https://learn.microsoft.com/fr-fr/windows/win32/srvnodes/windows-server, consulté le 05-05-2024

[W32] https://www.fortinet.com/fr/products/rugged-firewall#:~:text=FortiGate%20NGFW%20est%20le%20pare,la%20s%C3%A9curit%C3%A9%20et%20du%20r%C3%A9seau, consulté le 16-05-2024

[W33] https://cisco.goffinet.org/ccna/eigrp/protocole-eigrp/, consulté le 03-06-2024

[W34] https://www.ciscopress.com/articles/article.asp?p=2999383&seqNum=4, consulté le 03-06-2024

[W35] https://notes.networklessons.com/nhrp, consulté le 05-06-2024

[W36] https://networklessons.com/cisco/ccie-enterprise-infrastructure/introduction-to-dmvpn#NHRP_Next_Hop_Resolution_Protocol, consulté le 05-06-2024

[W37] WWW.algérietélécom.dz, consulté le 11-06-2024

ANNEXES

Annexes A

A.1 La banque d'Algérie

La Banque Centrale d'Algérie fut créée par la loi 62-144 votée par l'assemblée constituante le 13 décembre 1962, portant création et constitution des statuts de la Banque Centrale. Quelques aménagements ont été apportés durant les années 1970 et le début des années 1980 lançant de ce fait, le processus de la réforme du système financier national. Cependant, c'est la promulgation de la loi sur la monnaie et le crédit de 1990 qui a donné à la Banque d'Algérie son indépendance de toute tutelle. Ainsi, la direction, l'administration et la surveillance de la Banque sont assurées respectivement par le Gouverneur, le Conseil d'administration qui est présidé par le Gouverneur et par deux censeurs. Le Conseil d'administration est composé de trois vice-gouverneurs et de trois hauts fonctionnaires dont les compétences dans les domaines économique et financier doivent être avérées.

Le Gouverneur ainsi que les trois vice-gouverneurs sont nommés via décret présidentiel. Les autres membres du Conseil d'administration sont désignés par décret exécutif. Quant aux censeurs, ils sont nommés par décret présidentiel, sur proposition du Ministre chargé des finances. [W1]

A.2 Les missions de la BA

Les missions de la Banque d'Algérie sont au cœur de sa contribution à la stabilité financière et économique du pays, elle a plus missions essentielles à assurer notamment :

a. Stabilité monétaire

La Banque d'Algérie a pour mission de veiller à la stabilité des prix en tant qu'objectif de la politique monétaire. Elle est chargée de régler la circulation monétaire, de diriger et de contrôler, par tous les moyens appropriés, la distribution du crédit, de réguler la liquidité, de veiller à la bonne gestion des engagements financiers à l'égard de l'étranger, de réguler le marché des changes et de s'assurer de la sécurité et de la solidité du système bancaire. [1]

b. Systèmes de paiement

La Banque d'Algérie surveille et veille au bon fonctionnement, à l'efficience et à la sécurité des systèmes de paiement. Les règles applicables aux systèmes de paiement sont édictées par voie de règlements du Conseil de la Monnaie et du Crédit. [1]

c. Organisation du marché des changes

La Banque d'Algérie organise le marché des changes dans le cadre de la politique de change arrêtée par le Conseil de la Monnaie et du Crédit, dans le respect des engagements internationaux souscrits par l'Algérie. [1]

d. Emission de la Monnaie

L'État délègue à titre exclusif à la Banque d'Algérie, le privilège d'émettre la monnaie fiduciaire à savoir les billets de banque et pièces de monnaie. La Banque d'Algérie détermine les signes recognitifs d'un billet ou d'une pièce et fixe les modalités de contrôle de leur fabrication et de leur destruction. [1]

e. Supervision bancaire

La Banque d'Algérie établit les conditions générales dans lesquelles les banques et les établissements financiers algériens et étrangers, peuvent être autorisés à se constituer en Algérie et à y opérer. Elle établit les conditions dans lesquelles cette autorisation peut être modifiée ou retirée.

La Banque d'Algérie détermine également, toutes les normes que chaque banque doit respecter en permanence. [1]

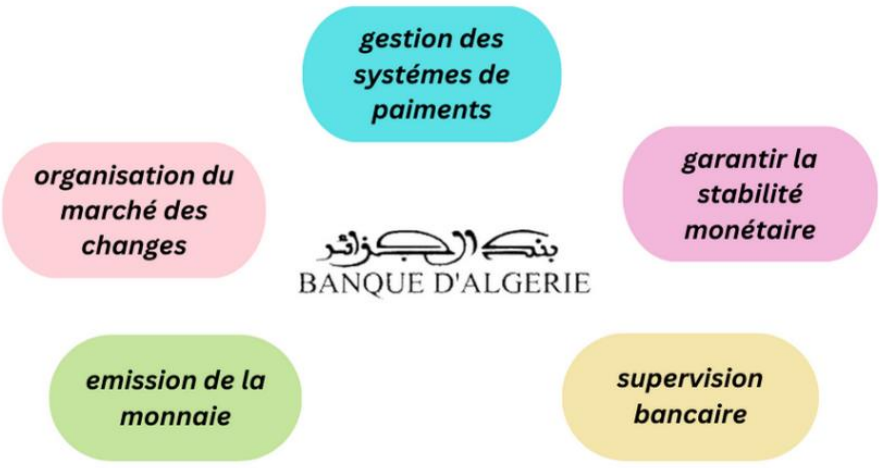


Figure A.1 - Les différentes missions de la BA

A.3 Organisation de la BA

Pour mener à bien ses missions, la Banque d'Algérie est organisée au niveau central en directions générales s'occupant des départements d'études, d'inspection et des activités bancaires. L'organisation de la Banque d'Algérie est également composée de deux directions Générales gérant des aspects spécifiques liés à l'émission de billets et à la formation bancaire.

La Banque d'Algérie dispose, en outre d'un réseau composé de 49 agences et succursales, lui assurant une présence effective dans chacune des wilayas du pays : les agences et succursales sont coordonnées par trois directions régionales implantées dans les villes d'Alger, Oran et Annaba.

Un vaste programme de modernisation des équipements et des méthodes de travail ainsi que des programmes de formation ont été mis en œuvre afin de permettre à la Banque d'Algérie de répondre et de veiller à ce que le système bancaire en général réponde aux exigences du nouveau contexte, tant national qu'international. [1]

A.3.1 La direction générale de l'administration des moyens et des systèmes de paiements (DGAMSP)

L'administration des moyens et des systèmes de paiement est assurée par plusieurs directions en charges de différentes missions, à savoir les systèmes de paiement, l'informatique et les techniques de production ainsi que la prise en charge des travaux des études et des développements ainsi que des acquisitions de logiciels destinés à la gestion et à la mise en œuvre du système d'information de la Banque. [1]

Notre projet se déroulera au sein de la DGAMSP ; plus spécifiquement Il se concentra sur la direction de l'ingénierie technique et de la production (DITP). La DITP a pour mission principale la gestion du réseau et la sécurité de la Banque d'Algérie.

A.4 Organigramme détaillé de la banque d'Algérie

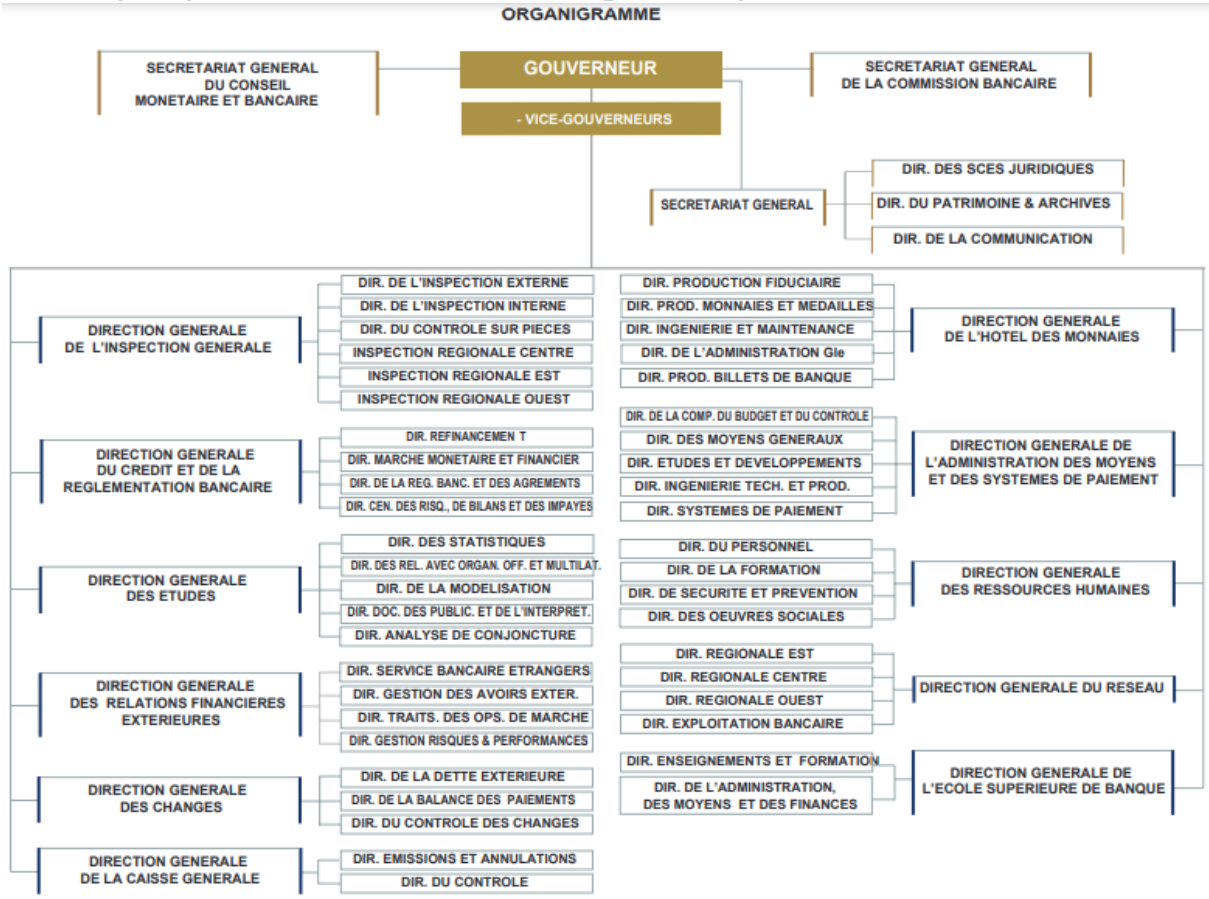


Figure A.2- Organigramme détaillé de la banque d'Algérie

Annexes B

B.1 EIGRP

Enhanced Interior Gateway Routing Protocol, le protocole de routage dynamique exclusif EIGRP est largement privilégié dans les réseaux Cisco Systems. EIGRP est un protocole de routage dynamique interne très performant. Il offre une convergence rapide et prend en charge à la fois les protocoles IPv4 et IPv6. Il permet un contrôle précis de la métrique pour influencer les entrées de la table de routage. Ainsi, EIGRP peut équilibrer la charge du trafic sur des liens de coûts différents. [W33]

L'EIGRP utilise des valeurs K pour définir les facteurs que la formule utilise et l'impact associé à un facteur lors du calcul de la métrique. On pense souvent à tort que les valeurs K s'appliquent directement à la bande passante, à la charge, au délai ou à la fiabilité. Par exemple, K1 et K2 font tous deux références à la bande passante (BW).

BW représente la liaison la plus lente du chemin, ramenée à une liaison de 10 Gbps (107). La vitesse de la liaison est collectée à partir de la bande passante configurée sur une interface. Delay est la mesure totale du retard sur le chemin, mesurée en dizaines de microsecondes (µs).

La formule EIGRP est basée sur la formule métrique IGRP, sauf que la sortie est multipliée par 256 pour faire passer la métrique de 24 bits à 32 bits. [W34]

$$\text{Metric} = 256 * \left[\left(K_1 * \frac{10^7}{\text{Min. Bandwidth}} + \frac{\frac{K_2 * 10^7}{\text{Min. Bandwidth}}}{256 - \text{Load}} + \frac{K_3 * \text{Total Delay}}{10} \right) * \frac{K_5}{K_4 + \text{Reliability}} \right]$$

B.2 NHRP

Le protocole NHRP (Next Hop Resolution Protocol) est une fonction de configuration automatisée utilisée pour améliorer l'efficacité du routage sur les réseaux à accès multiple non radiodiffusé (NBMA). Il est largement utilisé dans les réseaux DMVPN pour permettre aux rayons de déterminer le meilleur chemin vers les réseaux se trouvant sur d'autres rayons d'une telle topologie. [W35]

B.3 DMVPN

DMVPN (Dynamic Multipoint VPN) est une technique de routage que nous pouvons utiliser pour construire un réseau VPN avec plusieurs sites sans avoir à configurer statiquement tous les appareils. Il s'agit d'un réseau « hub and spoke » où les spokes peuvent communiquer entre eux directement sans passer par le hub. Le cryptage est pris en charge par IPsec, ce qui fait du DMVPN un choix populaire pour connecter différents sites à l'aide de connexions internet

ordinaires. Il s'agit d'une excellente solution de secours ou d'une alternative aux réseaux privés tels que le VPN MPLS. [W36]

Annexes C

C.1 RMS

Le Réseau Multi Services (RMS) d'Algérie Télécom est un réseau de nouvelle génération NGN, utilisant la technologie IP/MPLS et couvrant l'ensemble du territoire national. Il garantit un transfert rapide et sécurisé des données, assurant une communication fiable et de qualité entre les sites distants, tout en évitant la saturation du réseau. [W37]

{وَآخِرُ دَعْوَاهُمْ أَنِ الْحَمْدُ لِلّهِ ربّ الْعَالَمِينَ (١٠)}