République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique
Université Abderrahmane Mira
Faculté de la Technologie

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

ATE Department

Département d'Automatique, Télécommunication et d'Electronique

Projet de Fin d'Etudes

Pour l'obtention du diplôme de Master

Filière : Télécommunications

Spécialité : Réseaux et télécommunications.

Thème

Conception et implémentation d'une architecture SD-WAN pour l'entreprise NAFTAL-Bejaia

Préparé par :

- CHADLI Silia
- HADDADOU Djedjiga

Soutenu le 02/07/2023 devant le jury :

Mme Meriem GHERBI,	Présidente
Mr Omar BESSAAD,	Examinateur
Mr Mohamed AZNI,	Encadrant
Mr Mustapha SAADI,	Co-Encadrant
Mr Adel BOUYOUCEF,	Co-Encadrant

Année universitaire : **2022/2023**

Dédicaces

À mes chers parents, il est difficile pour moi de trouver les mots justes pour exprimer toute ma gratitude envers vous. A chaque étape de ma vie, vous avez été là ; vous m'avez soutenu, guidé et encouragé. Votre amour inconditionnel m'a donné la force nécessaire pour surmonter tous les obstacles.

À la mémoire de mon grand-père maternelle qui nous a quitté cette année, que Dieu le garde dans son vaste paradis.

À mes chères sœurs Cylia, Thinhinane, Maya, et mon petit frère Fardjallah. Notre fraternité est un cadeau précieux, et je chéris chaque instant que nous passons ensemble.

À mes grands-parents paternels et à ma grand-mère maternelle, à qui je souhaite une excellente santé.

À ma meilleure amie Ryma. Je suis profondément reconnaissante de t'avoir à mes côtés et je souhaite que notre amitié perdure pour de nombreuses années encore.

À toute ma famille et mes amis (Akram, Kenza, Silia, Siham) pour leurs encouragements.

À ma binôme Silia pour ton courage.

- Djedjiga

Dédicaces

À ma chère sœur Rima.

Je tiens à te remercier du fond de mon cœur pour ton soutien inconditionnel à chaque instant de ma vie. Tu as toujours été là pour moi, à mes côtés, prête à m'écouter, à me conseiller et à me soutenir dans tous les défis que j'ai pu rencontrer. Que ce soit pendant mes études, mes projets personnels ou mes moments de doute, tu étais toujours là pour me rappeler mes forces, m'encourager à continuer et me rappeler que je suis capable de réaliser de grandes choses.

À mes chers parents.

Je ne trouve pas les mots justes pour exprimer toute ma gratitude envers vous grâce à votre soutien inconditionnel tout au long de mon parcours académique jusqu'à l'obtention de mon diplôme.

À mes chers frères Imad et Adel,

Je tiens à vous exprimer ma profonde gratitude pour votre soutien inconditionnel dans l'obtention de mon diplôme. Votre présence et votre encouragement étaient essentiels tout au long de ce parcours, et je suis extrêmement reconnaissant de vous avoir à mes côtés.

À mes Chères cousines Manal, Sana

Je tiens à vous remercier du fond du cœur pour votre présence constante et pour tout l'amour et le soutien que vous m'avez apportés. Vous êtes des cousines extraordinaires, et je suis profondément reconnaissant d'avoir des personnes aussi merveilleuses dans ma vie.

À mes Chères amies Hlima, Cylia , Kato, Lydia, Saliha, Lyna, Iman, Ouardia

Je souhaite exprimer ma profonde gratitude envers mes amies pour toute l'aide précieuse que vous m'avez apportée. Votre soutien constant et votre présence bienveillante étaient d'une importance capitale dans ma vie, et je tiens à vous remercier du fond du cœur pour tout ce que vous avez fait pour moi.

À ma binôme Djidji pour ton courage.

- Silia

Remerciements

Nous tenons à remercier Dieu, le tout-Puissant, de nous avoir donné la santé, le courage et la patience nécessaires pour mener à bien notre formation et pouvoir réaliser ce travail.

Nos remerciements s'adressent aux président et membres de jury d'avoir accepté d'examiner et évaluer notre travail. Nous exprimons notre sincère gratitude à nos encadrants *Mr. AZNI* et *Mr. SAADI* pour leurs précieux conseils, leurs orientations et leurs soutiens tout au long de notre projet de fin d'études. Ce travail n'aurait pas été possible sans leur accompagnement bienveillant.

Nous remercions aussi notre promoteur, au sein de NAFTAL-Bitume de Bejaia, *Mr. BOUYOUCEF*, pour son accueil, ses suggestions et sa disponibilité durant l'exercice de notre stage pratique.

Enfin, que nos chers parents et familles, trouvent ici l'expression de nos remerciements les plus sincères et les plus profonds en reconnaissance de leurs sacrifices, aides, soutien et encouragement afin de nous assurer cette formation dans les meilleures conditions.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

ADSL	Asymetric Digital Subscriber Line
AES	Advanced Encryption Standard
AH	Authentication Header
API	Application Programming Interface
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
CPE	Customer Premises Equipment
DVR	Distributed Virtual Router
DSL	Digital Subscriber Line
EMS	Element Management System
ETSI	European Telecommunications Standards Institute
ESXi	Elastic Sky X integrated
FEC	Forwarding Equivalence Class
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HA	High availability
HDD	Hard Disk Drive
IaaS	Infrastructure As A Service
IDS	Intrusion Detection System
IKE	Internet Key Exchange
IP	Internet Protocol
ISAKMP	Internet Security Association and Key Management Protocol
IPsec	Internet Protocol Security
KVM	Kernel-based Virtual Machine
LAN	Local Area Network
LFIB	Label Forwarding Information Base
LER	Label Edge Routeur
LSR	Label Switch Router

LSP Label Switch Path

LOS Linux Open Switch

MAC Media Access Control

MAN Metropolitan Area Network

MANO Network Functions Virtualization Management and Orchestration

MPLS Multiprotocol Label Switching

NAT Network Address Translation

NFV Network Fuction Virtualization

NFVI Network Function Virtualisation Infrastructure

NGFW Next-Generation Firewall

OMP Overlay Management Protocol

OVS Open vSwitch

OSPF Open Shortest Path First

PRC Prime de Rendement collectif

PaaS Platform as a service

QoE Quality of Experience

QOS Quality of Service

RAM Random-Access Memory

RADIUS Remote Authentication Dial-In User Service

RESTful Representational State Transfer

SaaS Software As A Service

SDG Système de Gestion de Créance

SDN Sortware Defind Networking

SDS Software-Defined Storage

SNMP (Simple Network Management Protocol

SSD Solid-State Drive

SSH (Secure Shell)

TCP Transmission Control Protocol

TLS Transport Layer Security

VIM Virtualized Infrastructure Manager

VNF Virtual Network Function

VNFC Virtual Network Function Components

VNFM Virtual Network Function Managers

NFVO Virtual Network Function orchestrator

VoIP Voice Over Internet Protocol

VPN Virtual Private Network

VRRP Virtual Router Redundancy Protocol

WAN Wide Area Network

Introduction

La demande croissante de services cloud dans divers secteurs d'activité pose des défis aux réseaux étendus traditionnels. Les services cloud requièrent généralement une bande passante élevée et une faible latence pour offrir une performance optimale. Cependant, les réseaux WAN (Wide Area Network) conventionnels ne sont pas conçus pour répondre à ces exigences et peuvent ne pas fournir le niveau de service nécessaire[1].

Les solutions basées sur la virtualisation des fonctions du réseaux sont apparues comme des solutions prometteuses qui permettent une grande flexibilité des réseaux qui devienent ainsi capable de s'adapter dynamiquement aux exigences de qualité de services (QoS) des applications. Ce paradigme de virtualisation est devenu une réalité dans les réseaux locaux à travers la mise en place des réseaux SDN (Software Defined networks). SD-WAN (Software Defined-Wide Area Networks) est le concept équivalent pour les réseaux étendus. SD-WAN offrent à une organisation la possibilité d'étendre ses capacités en exploitant le WAN de l'entreprise et la connectivité multi-cloud. Le principal avantage du SD-WAN réside dans sa capacité à sélectionner dynamiquement les chemins de connectivité, tels que l'évolution à long terme (LTE) / la cinquième génération (5G) et le réseau internet, offrant ainsi une flexibilité accrue. De plus, le SD-WAN permet la segmentation du trafic entrant et sortant grâce à ses fonctionnalités de mise en forme du trafic. Il permet également de hiérarchiser le trafic en fonction des politiques définies par les utilisateurs et les types d'applications. Par conséquent, les solutions SD-WAN offrent aux entreprises la possibilité de bénéficier d'une connectivité améliorée, d'une sécurité renforcée, d'une gestion simplifiée et d'une flexibilité accrue. Elles permettent d'optimiser les performances des applications, d'améliorer l'ex-

périence utilisateur, de garantir la disponibilité des applications critiques et de réduire les coûts associés aux connexions et à la gestion du réseau.

L'objectif de ce travail de fin d'études est d'explorer et d'analyser la technologie SD-WAN. Spécifiquement, il s'agit de démontrer comment cette technologie peut améliorer les performances, renforcer la sécurité, favoriser la flexibilité et réduire les coûts dans le réseau de l'entreprise NAFTAL-Bejaia. Ceci offre ainsi une base solide pour évaluer le potentiel d'adoption de la technologie SD-WAN et son impact sur les entreprises et les réseaux WAN en général, et sur NAFTAL-Bejaia en particulier.

Le travail présenté dans ce mémoire est structuré en quatre chapitres précédés de cette intoduction et suivis d'une conclusion.

Le premier chapitre sera dédié à l'essentiel des technologies réseaux, couvrant les principaux concepts.

Le deuxième chapitre se concentrera sur la présentation de la structure de l'entreprise NAFTAL-Bitume Bejaia, où nous avons effectué notre stage, ainsi que sur l'analyse du réseau, son fonctionnement et ses limitations.

Le troisième chapitre mettra l'accent sur le concept de SD-WAN (Software-Defined Wide Area Network) en examinant de manière détaillée son fonctionnement, ses différentes caractéristiques et une vue d'ensemble des fournisseurs qui proposent cette solution sur le marché.

Le quatrième chapitre se concentrera sur la mise en pratique de la solution proposée. Nous décrirons les étapes de mise en œuvre.

Ce mémoire se conclut par une conclusion générale qui met en avant notre contribution.

Chapitre 1

Technologies Réseaux

1.1 Introduction

Ce premier chapitre traite des principales technologies réseaux. Nous parlerons dans un premier temps, dans la section 1, des différents types de réseaux informatiques puis, dans la section 2, nous abordons les topologies réseaux usuelles. Nous introduirons par la suite, dans les sections 3, 4, 5, 6, 7, 8 et 9, les spécifictés des réseaux filaires mais aussi celles des réseaux mobiles. Les derniers développements tels que la virtualisation des fonctions réseaux seront ensuite considérés.

1.2 Types de réseaux informatiques

Un réseau informatique est un système de communication qui permet la connectivité et l'échange de données entre les appareils connectés. Les réseaux informatiques se présentent sous de nombreux types différents en fonction de la portée géographique, de l'architecture, de la technologie. Voici quelques types de réseaux courants :

a) Réseau local (LAN)

Un réseau local est limité à une zone géographique restreinte de taille supérieure, s'étendant sur quelques dizaines à centaines de mètres [2], telle qu'un bâtiment. Les LAN permettent aux périphériques de communiquer entre eux et de partager des ressources telles que des fichiers, des imprimantes, les scanners, etc.

b) Réseau métropolitain (MAN)

Un réseau MAN couvre une zone géographique plus grande que les LAN mais plus petite que les WAN. Un MAN peut couvrir une ville, une grande université ou un parc industriel, et peut être utilisé pour connecter plusieurs LANs situés à des endroits différents.

c) Réseau étendu (WAN)

Un WAN couvre une large zone géographique, telle qu'une région, un pays ou même plusieurs pays. Les WAN sont utilisés pour connecter des réseaux locaux distants entre eux, permettant ainsi la communication et le partage de ressources sur de longues distances. Internet est un exemple de WAN mondial.

1.3 Topologie des réseaux informatiques

La topologie des réseaux informatiques définit la manière dont les différents éléments du réseau sont inter-connectés et communiquent entre eux.La figure 1.1 montre les concepts de topologie logique et celui de topologie physique[3].

- **Topologie logique** Elle concerne la manière dont les données se déplacent et sont dirigées à travers les périphériques du réseau, sans tenir compte de la disposition physique de ces périphériques. Elle décrit la voie que prennent les données lorsqu'elles sont transmises entre les différents composants du réseau.
- **Topologie physique** Elle concerne la manière dont les composants matériels, tels que les câbles, les périphériques,etc. sont disposés et interconnectés. Elle définit la configu-

ration physique réelle du réseau, incluant la disposition des câbles, les emplacements des périphériques et les schémas de connexion entre eux [3].

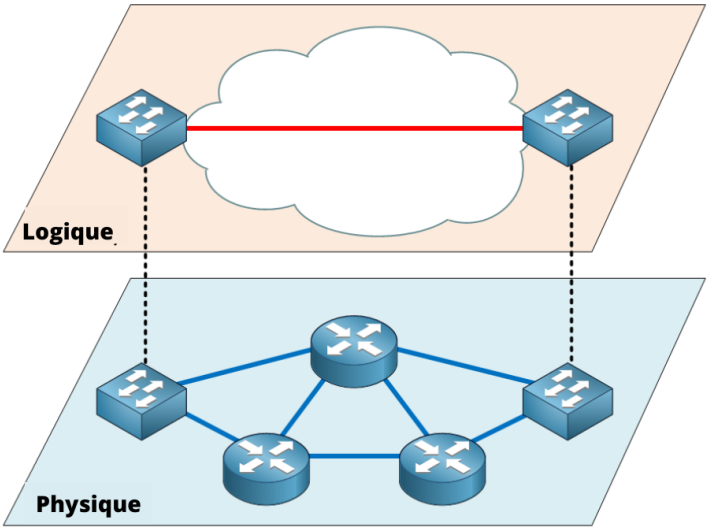
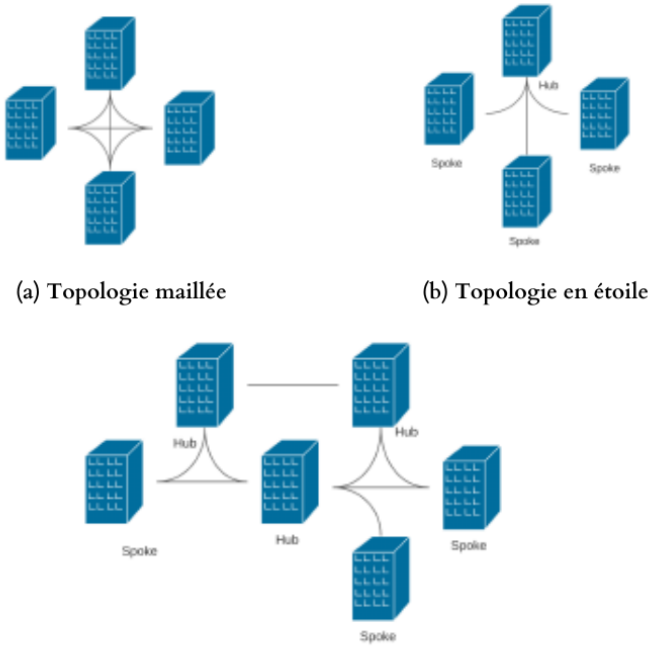


FIGURE 1.1 – Topologies physique et logique.

On distingue généralement les topologies suivantes, comme illustré par la figure 1.2 ci-dessous [4, 2] :



(a) Topologie maillée

(b) Topologie en étoile

(c) Topologie hybride

FIGURE 1.2 – Différentes topologies réseau.

- Topologie maillée : est une configuration de réseau où chaque périphérique est directement relié à tous les autres périphériques du réseau. Chaque nœud a une connexion dédiée et point à point avec tous les autres nœuds, ce qui permet une interconnexion complète et directe entre eux.
- Topologie en étoile : est une configuration de réseau dans laquelle chaque périphérique (spoke) est connecté à un point central (hub).
- Topologie hybride : La topologie hybride est une combinaison de deux ou plusieurs topologies différentes (maillée, en étoile) dans un seul réseau. Elle peut être créée en interconnectant différentes sous-topologies pour tirer parti des avantages de chaque configuration. La topologie hybride permet de répondre à des besoins spécifiques en matière de performance, de redondance et de flexibilité.

1.4 Modèles de réseau étendu hérité

1.4.1 Réseau privé virtuel (VPN)

Un réseau privé virtuel, ou VPN (Virtual Private Network) est un moyen sécurisé de connecter des réseaux locaux distants ou des utilisateurs individuels à un réseau privé via Internet. Il établit un tunnel sécurisé et chiffré pour le transfert des données, ce qui permet aux utilisateurs d'accéder aux ressources du réseau privé de manière sécurisée, même à distance. Un réseau est dit virtuel car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent voir les données [5].

1.4.1.1 Types d'utilisation de VPN

VPN site à site Il permet aux entreprises ayant des bureaux dans plusieurs emplacements fixes de créer des connexions sécurisées entre elles via internet. Généralement ce type de VPN est mis en place par l'interconnexion de deux éléments matériels (routeurs ou pare-feu

ou serveur) situés à la frontière entre le réseau interne et le réseau privé de chaque site.La figure 1.3 illustre le VPN site à site.

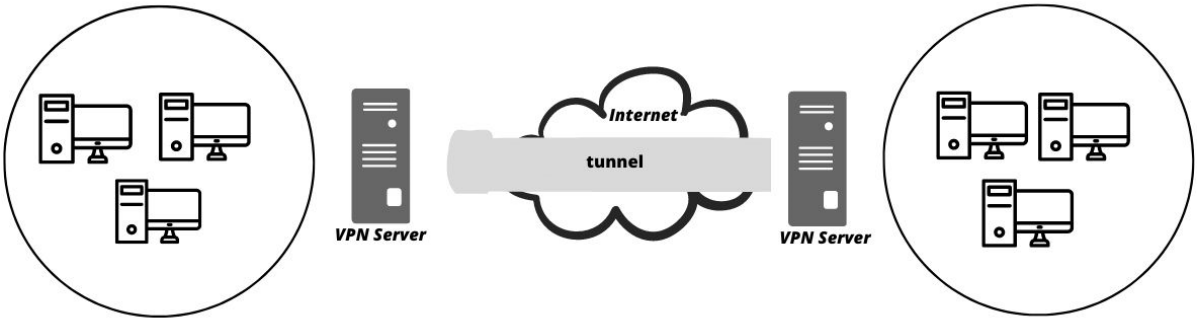


FIGURE 1.3 – VPN site à site

VPN d'accés distant Un VPN d'accès distant est le type de VPN le plus utilisé. Fondamentalement il connecte les utilisateurs à un serveur distant situé dans une zone lointaine, ou dans un autre pays, la figure 1.4 illustre le VPN d'accès distant Ce type de VPN est idéal pour l'utilisation personnelle mais ne convient pas à des fins professionnelles.

C'est pourquoi les entreprises implémentent VPN IPsec d'accès distant pour faciliter l'accès aux ressources internes à des télétravailleurs à travers internet en toute confidentialité et crypte les données du trafic aux cours de ce processus[5].

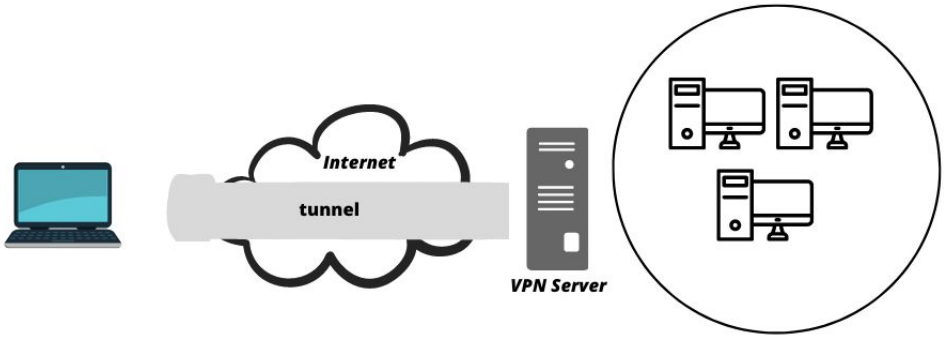


FIGURE 1.4 – VPN d'accès distant

1.4.1.2 Protocole réseaux privés virtuels

Voici le protocole principal le plus utilisé dans le cadre de VPN :

1) **Protocole de sécurité internet (IPsec)**

IPsec (Internet protocole security) est un standard IETF (RFC 2401-2412) qui définit comment un VPN peut être sécurisé sur des réseaux IP. IPsec protège et authentifie les paquets IP entre la source et la destination. IPsec peut protéger le trafic de la couche 3 à la couche 7 [6].

Il sécurise le protocole de communication internet en vérifiant chaque session et avec un cryptage individuel des paquets de données pendant toute la connexion. IPsec est un protocole de sécurité utilisé pour sécuriser les communications sur les réseaux IP. Il offre des mécanismes de sécurité tels que l'authentification, le chiffrement et la confidentialité des données. Il est souvent utilisé pour créer des connexions VPN pour permettre une communication sécurisée entre des réseaux distants.

voici les fonctions de sécurité essentielles de l'IPsec montré par la figure 1.5 :

- **Confidentialité :** IPsec utilise généralement des algorithmes de chiffrement symétrique tels que AES pour rendre les données illisibles pour les parties non autorisées. Les données sont chiffrées avant d'être encapsulées dans des paquets IPsec.
- **Intégrité :** IPsec utilise des mécanismes d'intégrité des données pour détecter toute altération ou modification des paquets IP en transit. Des algorithmes de hachage (par exemple, SHA-1 ou SHA-256) et la clé de sécurité partagée sont utilisés pour générer des sommes de contrôle (hash) des données et s'assurer qu'elles n'ont pas été modifiés entre la source et la destination.
- **Authentification d'origine :** L'authentification d'origine dans IPsec permet de garantir que l'expéditeur des données est bien celui qu'il prétend être. Cela permet de prévenir les attaques de type "homme du milieu".Il existe plusieurs types d'authentification d'origine :

- **Authentification pré-partagée (PSK) :** cette méthode utilise une clé partagée entre les deux extrémités du tunnel VPN pour vérifier l'identité de chaque partie. Cette clé est configurée manuellement sur chaque appareil avant l'établissement de la connexion VPN.
- **Certificats numériques :** cette méthode utilise des certificats numériques émis par une autorité de certification (CA) de confiance. Les certificats sont utilisés pour vérifier l'identité de chaque partie et garantir l'intégrité des données échangées.
- **Protocole d'échange de clés Internet :** IKE est utilisé pour négocier et établir des clés de chiffrement sécurisées entre les deux points. IKE utilise des méthodes d'authentification telles que les certificats numériques ou les identifiants d'utilisateur pour vérifier l'identité de chaque partie.

– **L'échange de clés sécurisées :** IPsec utilise divers groupes de l'algorithme Diffie-Hellman (DH 1...DH 4, DH 14...DH16 et DH 19...DH 24) pour l'établissement d'une connexion à travers l'échange de clé sécurisé.

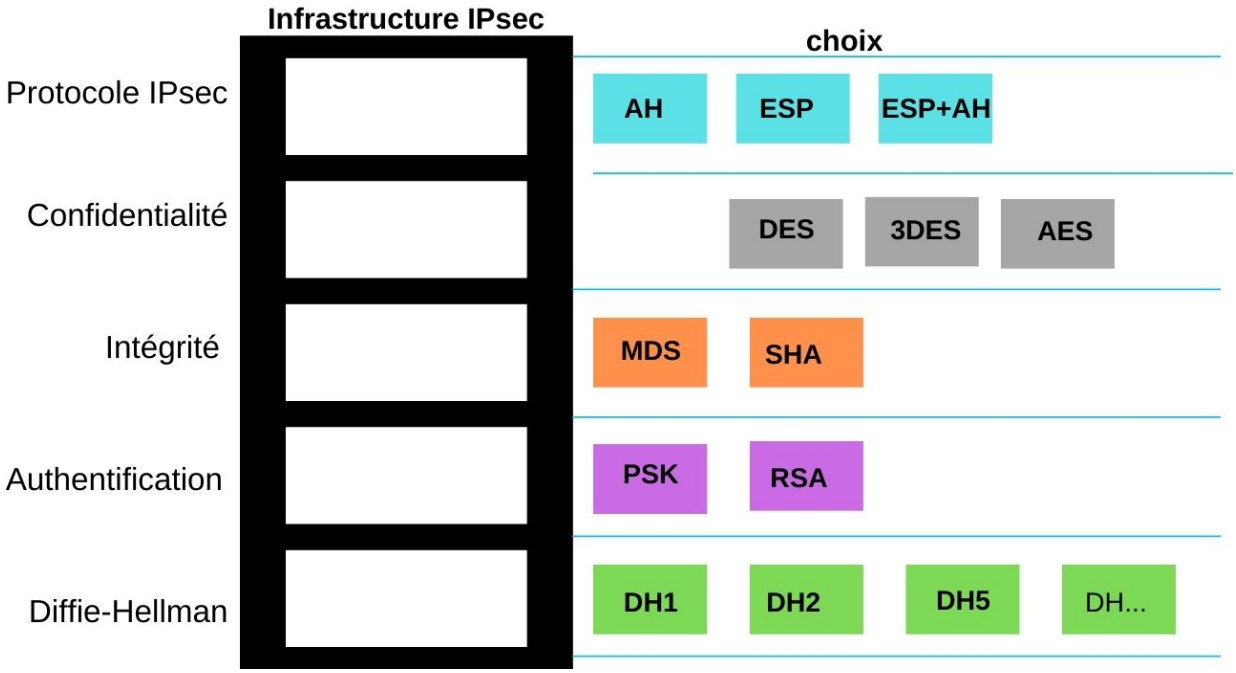


FIGURE 1.5 – Structure des fonctions de sécurité d'IPsec.

1.4.2 Commutation multi-protocoles par étiquettes (MPLS)

MPLS (Multiprotocol Label Switching) offre un service en mode connecté transparent aux applications IP. En fait, MPLS migre un réseau IP routé en un réseau IP commuté, il associe la souplesse du routage de niveau 3 à l'efficacité de l'acheminement de niveau 2. C'est un protocole de conciliation généralement présenté comme un protocole de niveau 2,5. MPLS a été normalisé avec la RFC 3031 en janvier 2001 [7].

Un modéle de référence MPLS est illustré par la figure 1.6 [7]

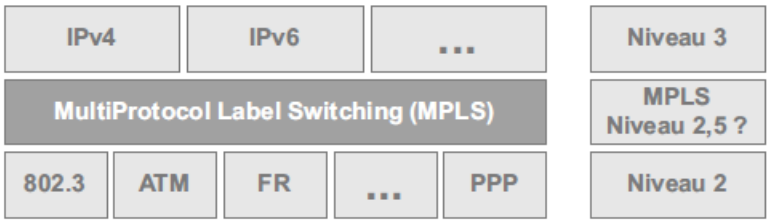


FIGURE 1.6 – Modèle de référence MPLS.

Commutation des labels : Les réseaux IP/MPLS se base sur l'établissement de chemin entre deux machines (LSP). La commutation des paquets circulant sur ce chemin est faite en analysant un label contenu dans l'entête MPLS qui est ajouté entre la couche 2 (souvent Ethernet) et la couche IP. Voici un schéma (figure 1.7) résumant le principe de la commutation de label tout au long d'un chemin [8].

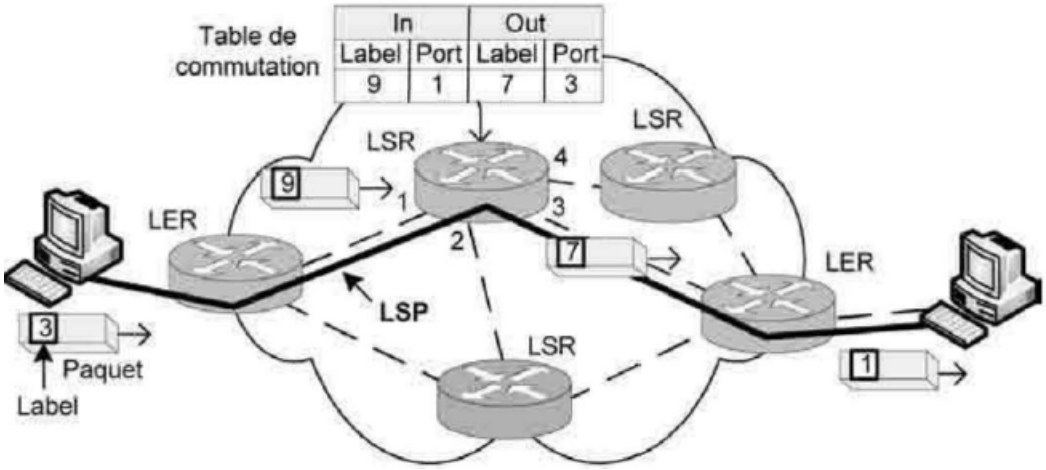


FIGURE 1.7 – Nœud et chemin MPLS.

A l'entrée du réseau MPLS, les paquets IP se voient insérés un label par le "Ingress LER". Ces derniers sont les routeurs MPLS se situant à la périphérie du réseau de l'opérateur. Les paquets labelisés sont ensuite commutés vers le cœur du réseau selon son numéro de label. Les routeurs MPLS du cœur de réseau, les LSR, commute ensuite les labels jusqu'au LER de sortie (Egress LER) Le chemin qui a été pris par le paquet, et préalablement établi, au travers du réseau s'appelle LSP. Le schéma nous montre le détail de la pile de protocole mis en œuvre durant cette transmission, on remarque la présence du label MPLS entre la couche Ethernet et la couche IP. Nous allons maintenant analyser le format de l'en-tête MPLS par la figure 1.8 :

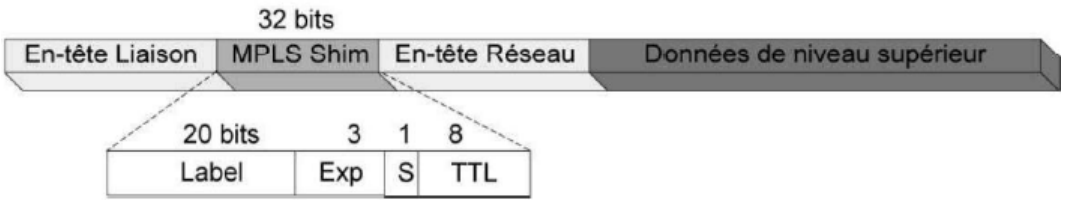


FIGURE 1.8 – En-tête MPLS.

L'entête MPLS a une taille de 4 octets et est composé par les champs suivants :

- Label : numéro de label
- Champ expérimental : utilisé pour gérer la QOS.
- S : Bottom of stack. Le bit "S" est à 1 quand le dernier label de la pile est atteint et on peut empiler des labels (par exemple pour créer des Tunnels).
- TTL : Ce champ à le même rôle que le TTL de l'entête IP. Indique combien de fois encore le paquet sera transmis, il est décrémenté sur chaque routeur et lorsqu'il atteint 0, le paquet est supprimé.

1.5 Types de technologies de connexion internet

Il existe principalement deux types :

1.5.1 Connexion internet filaire

Les connexions filaires sont les courantes pour accéder à Internet. Les technologies filaires incluent :

a) DSL : La DSL est une technologie de connexion Internet haut débit utilisée sur les lignes téléphoniques existantes. La DSL est largement disponible et offre une connexion Internet rapide et fiable.

b) Câble : La technologie de connexion par câble utilise les lignes de câble coaxial existantes pour fournir une connexion Internet à haut débit. Cette technologie est largement disponible et peut être très rapide, mais la qualité de la connexion peut être affectée par le nombre d'utilisateurs du même réseau.

c) Fibre optique : La fibre optique est une technologie de connexion à Internet très rapide qui utilise des câbles en fibre optique pour transmettre des données. Cette technologie est plus coûteuse que le DSL et le câble, mais offre une vitesse de connexion Internet supérieure.

1.5.2 Connexion internet sans fil

Un autre type de connexion internet est la connexion internet mobile ou sans fil, qui peut être utilisée pour assurer la transmission de données entre bureaux ou l'accès internet à des services. En effet, avec l'évolution de la technologie mobile (c'est-à-dire avec les technologies LTE et 5G), il est possible d'établir une connexion internet avec une bande passante et des valeurs de latence qui sont de plus en plus comparables à celles d'une connexion internet filaire [9] [10] . C'est pourquoi les entreprises sont de plus en plus intéressées par l'utilisation de connexions internet mobiles, principalement comme solution de secours.

1.6 Cloud computing

1.6.1 Définition

Le cloud computing est un modèle qui facilite l'accès aux ressources informatiques via un réseau, de manière pratique et à la demande. Ces ressources sont partagées et configurables, comprenant des réseaux, des serveurs, du stockage, des applications et des services. Ils peuvent être rapidement alloués et libérés avec un minimum de gestion et d'intervention de la part des fournisseurs de services[11].

1.6.2 Modèle de déploiement

Les modèle de déploiement les plus utilisés sont :

- **Cloud privé :** Dans le Cloud privé l'infrastructure et les ressources informatiques sont exclusivement utilisées par une seule organisation. Contrairement aux clouds publics, les clouds privés sont déployés et gérés au sein de l'infrastructure informatique interne d'une entreprise ou d'une organisation.
- **Cloud public :** Dans le Cloud public les ressources sont partagées entre plusieurs utilisateurs et organisations, ce qui permet une utilisation efficace des ressources et une réduction des coûts.De plus, il est accessibles via Internet par le grand public ou les organisations.

1.6.3 Elément de cloud computing

Le cloud computing se compose de cinq éléments essentiels[12] :

1. Accès à la demande et en libre-service : Les utilisateurs peuvent accéder aux ressources informatiques (telles que le temps CPU, le stockage réseau, l'utilisation de logiciels, etc.) de manière autonome, selon leurs besoins, sans nécessiter d'interaction directe avec les fournisseurs de services.

2. Accès réseau étendu : Les services cloud peuvent être accessibles via Internet à partir d'une variété d'appareils tels que des ordinateurs portables, des smartphones et des tablettes.
3. Mutualisation des ressources : Les fournisseurs de services cloud combinent les ressources informatiques dans le but de servir plusieurs utilisateurs en utilisant soit le modèle multi-locataires, soit le modèle de virtualisation. Cela implique l'allocation et la réallocation dynamique de différentes ressources physiques et virtuelles en fonction de la demande des utilisateurs.
4. Élasticité rapide : Pour les consommateurs, les ressources informatiques deviennent immédiates plutôt que persistantes : il n'y a pas d'engagement ni de contrat initial, car ils peuvent les utiliser pour évoluer quand ils le souhaitent et les libérer une fois qu'ils ont fini.
5. Prestation mesurée : Bien que les ressources informatiques soient regroupées et partagées par plusieurs consommateurs (c'est-à-dire multi-locataires).Les services cloud proposent un suivi et un reporting de l'utilisation, ce qui permet aux consommateurs de payer uniquement pour les ressources qu'ils consomment réellement.

1.6.4 Modèle de service cloud computing

En plus de ces cinq éléments essentiels, la communauté cloud a largement utilisé les trois modèles de service suivants pour classer les services cloud :

1. Logiciel en tant que service (SaaS) : Les utilisateurs du cloud computing déploient leurs applications sur un environnement d'hébergement accessible via des réseaux à partir de différents clients, tels que des navigateurs web, etc.par les utilisateurs d'applications. Les exemples de SaaS comprennent SalesForce.com, Google Mail, Google Docs, Microsoft Office 365 et bien d'autres.
2. Plate-forme en tant que service (PaaS) : PaaS est une plate-forme de développement qui permet aux utilisateurs de cloud de développer des services et des applications cloud, tels que des services logiciels en tant que service (SaaS), directement sur le cloud

PaaS. Ainsi, la différence entre SaaS et PaaS réside dans le fait que SaaS héberge uniquement des applications cloud prêtes à l'emploi, tandis que PaaS fournit une plateforme de développement qui héberge à la fois des applications cloud prêtes à l'emploi et en cours de développement. Un exemple de PaaS est Google App Engine.

3. Infrastructure en tant que service (IaaS) : Il s'agit d'un service cloud qui fournit des ressources informatiques virtuelles, telles que des serveurs, des réseaux et du stockage, permettant aux utilisateurs de gérer et de contrôler leur infrastructure. Les exemples courants d'IaaS incluent Amazon Web Services (AWS) EC2 et Microsoft Azure Virtual Machines.

1.7 Virtualisation des fonctions réseaux (NFV)

La virtualisation des fonctions réseau permet de transformer en logiciel des services réseau tels que les routeurs, les pare-feux, NAT, IDS, qui étaient auparavant exécutés sur du matériel propriétaire. Chacun de ces éléments à une fonction spécifique dans le réseau. Par exemple, la NAT permet de traduire les adresses IP dans le contexte des communications réseau, tandis qu'un pare-feu protège le réseau contre les menaces externes. Ces équipements intermédiaires, tels que les pare-feux, la NAT, etc., sont traditionnellement déployés de manière stratégique dans le réseau, ce qui entraîne une complexité et une rigidité croissantes. Le déploiement de ces équipements nécessite une expertise technique spécialisée et il est assez coûteux et prend beaucoup de temps. De plus, ces équipements sont propriétaires, autonomes et fermés, ce qui peut entraîner des problèmes complexes pendant ou après le déploiement. Le NFV intervient pour résoudre ces problèmes en réduisant le délai de commercialisation, les coûts liés à l'équipement et en établissant un écosystème solide et évolutif. La gestion et l'orchestration du NFV permettent d'automatiser l'évaluation et les tests des services, ce qui réduit le temps nécessaire à ces tâches.[13]

1.7.1 Définition de la virtualisation des fonctions réseaux

Les normes NFV ont été publiées par l'ETSI en octobre 2013, et le cadre NFV global est présenté dans la figure 1.9 [15].
La proposition de séparer les fonctions réseau du matériel, comme suggéré par NFV, permet de réduire efficacement les dépenses d'investissement et d'exploitation. Ces fonctions réseau peuvent être hébergées sous forme de machines virtuelles sur du matériel COTS et sont appelées fonctions de réseau virtuelles. La mise à l'échelle des machines virtuelles est gérée par NFV pour s'adapter aux variations du trafic dans le centre de données. SDN et la virtualisation des fonctions réseau sont liées mais indépendantes l'une de l'autre. Cependant, NFV est utilisé dans SDN[14] [15].

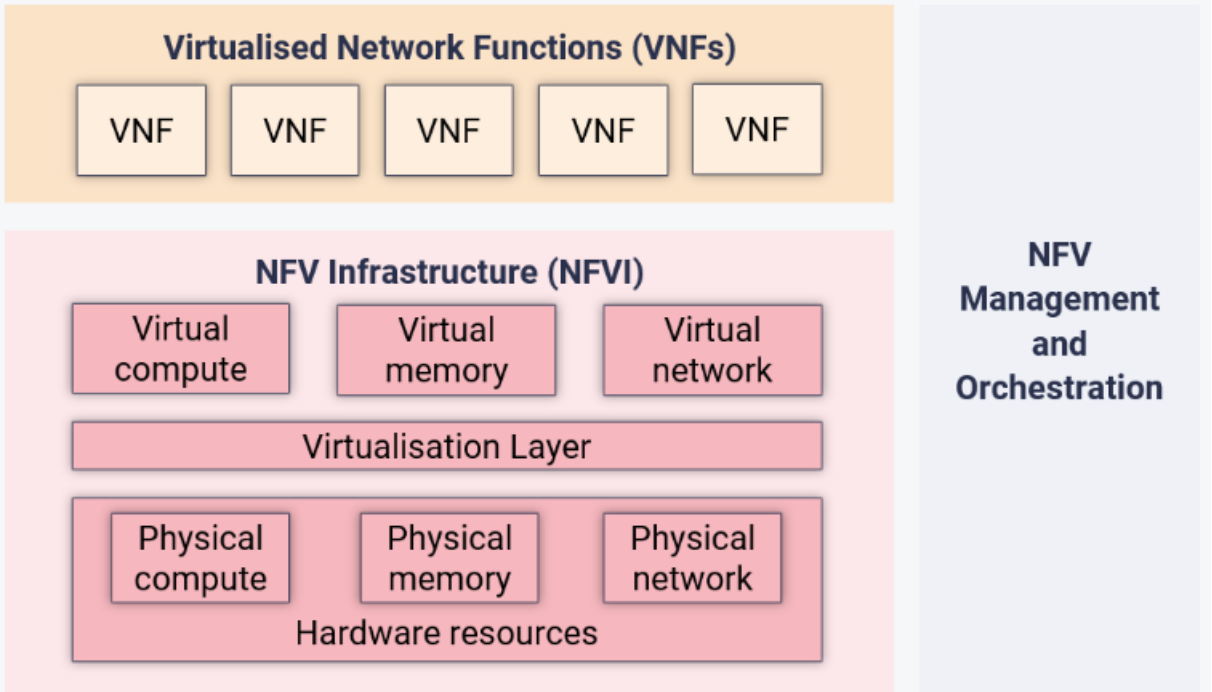


FIGURE 1.9 – Haut niveau du cadre NFV.

Le schéma de haut niveau du cadre NFV met en évidence trois composants essentiels : NFVI correspond au plan de données, qui transmet les données et fournit des ressources pour l'exécution des services de réseau, VNF correspond au plan d'application, qui héberge divers types de VNF pouvant être considérés comme des applications, et MANO correspond

au plan de contrôle, qui est responsable de l'établissement des connexions entre les différentes VNF et de l'orchestration des ressources dans NFVI. Le schéma présenté dans la figure 1.9 offre une vue d'ensemble du cadre NFV, tandis que la figure 1.10, ci-dessous, illustre une architecture de référence NFV plus détaillée, où les composants NFV peuvent être subdivisés en composants plus spécifiques [13, 16].

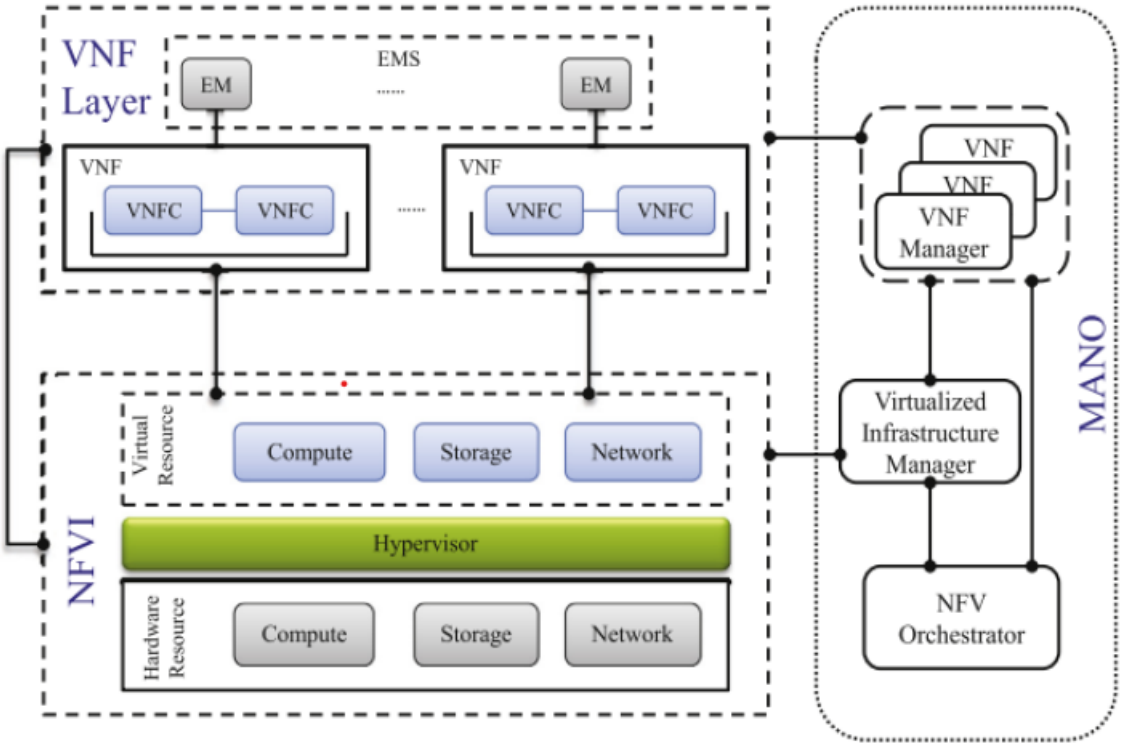


FIGURE 1.10 – Cadre architectural de référence ETSI NFV.

1.7.2 Infrastructure de virtualisation des fonctions réseau

Le NFVI englobe l'ensemble des éléments d'infrastructure, qu'ils soient matériels ou logiciels, qui forment le cadre permettant le déploiement, la gestion et l'exécution des VNF. Les ressources physiques de la NFVI comprennent les systèmes informatiques, de stockage et de réseau, offrant ainsi une connectivité à faible latence et un coût de réseau réduit. Comme illustré dans la figure 1.10, le NFVI se divise en trois parties : l'infrastructure physique, la couche de virtualisation et l'infrastructure de virtualisation [17].

1) **Couche d'infrastructure physique**

Cette section englobe une variété de ressources matérielles essentielles pour exécuter les fonctions réseau. On y retrouve trois types de matériels : les matériels de calcul (serveurs , RAM...), les matériels de stockage (disques durs, NAS...) et les matériels réseau (routeurs, commutateurs et pare-feu...). Les détails de chacun de ces matériels sont présentés dans les sous-sections suivantes.[18]

- Matériel de calcul : Le matériel de calcul désigne les nœuds de calcul à usage général qui sont gérés par l'ensemble d'instructions interne. Dans le contexte de la NFV, chaque nœud de calcul peut être implémenté sous forme de processeur monocœur ou multicœur, également connu sous le nom de CPU.[19]
- Matériel de stockage : Le matériel de stockage stocke des informations, qu'elles soient temporaires ou permanentes. Il se compose de serveurs de stockage qui intègrent un grand nombre de disques SSD et de disques HDD, ainsi qu'une quantité limitée de puissance de calcul et de mémoire. L'espace de stockage de ces serveurs peut être augmenté en ajoutant de nouveaux disques externes.
- Matériels réseau : Le matériel de réseau se présente généralement sous la forme de commutateurs L2/L3 propriétaires. Dans le contexte de la NFV, ces dispositifs propriétaires sont progressivement remplacés par des dispositifs standard, qui supportent OpenFlow ou les protocoles de routage conventionnels, ou les deux à la fois.[13]

2) **Couche de virtualisation**

Dans l'architecture NFVI, la couche de virtualisation est positionnée entre l'infrastructure virtuelle et l'infrastructure physique. Son objectif principal est d'émuler l'infrastructure physique et de la fournir sous forme d'infrastructure virtuelle nécessaire aux machines virtuelles dans la couche VNF. Cette couche fait usage d'un hyperviseur pour partitionner les ressources physiques et les attribuer aux machines virtuelles. Dans le contexte de la NFV[13].

3) **Couche d'infrastructure virtuelle**

La couche d'infrastructure virtuelle est positionnée directement au-dessus de la couche de virtualisation. Elle comprend trois éléments clés qui jouent un rôle crucial dans la création d'un environnement virtuel dans la NFV :

- Calcul virtuel : Dans le Calcul virtuel L'hyperviseur virtualise les composants de traitement matériel en utilisant des API telles que libvirt pour KVM et vCenter pour ESXi. Cette virtualisation permet d'acquérir et de gérer des ressources informatiques virtuelles de manière efficace.[13]
- Stockage virtuel : Les ressources de stockage virtuelles sont obtenues grâce à la virtualisation des ressources de stockage matérielles. Le logiciel de gestion du stockage est dissocié du matériel sous-jacent, ce qui crée un pool de ressources de stockage virtuelles offrant des fonctionnalités telles que les instantanés et la sauvegarde. Une autre technologie de virtualisation du stockage est le stockage défini par logiciel, qui sépare le logiciel de contrôle et de gestion du matériel sous-jacent, permettant ainsi la création d'un réseau virtualisé de ressources de stockage.
- Réseau virtuel : La virtualisation du réseau consiste à virtualiser les fonctionnalités de mise en réseau matérielles. Cela permet de créer des environnements de réseau virtuels qui interconnectent des machines virtuelles, des serveurs virtuels et d'autres composants. Les éléments clés de la virtualisation du réseau sont des fonctionnalités logicielles telles que les commutateurs virtuels et les adaptateurs Ethernet virtuels [13].

1.7.3 Gestion et orchestration NFV

Le NFV MANO est chargé de la gestion de tout le contexte virtualisé dans le cadre du NFV, comprenant la virtualisation, l'orchestration des ressources, la gestion du cycle de vie des instances VNF et la gestion des interfaces entre les modules. Selon l'ETSI, les responsabilités sont classées en trois catégories : le gestionnaire d'infrastructure virtualisée, l'orchestrateur NFV et le gestionnaire VNF. Le NFVO est principalement responsable de l'orches-

tration des ressources NFVI et de la gestion du cycle de vie des VNF pour fournir un service réseau optimal. La VNFM est responsable de la gestion de plusieurs instances de VNF et peut être affectée à la gestion de plusieurs instances VNF. Le VIM gère et contrôle les ressources NFVI, comme le réseau, l'informatique et le stockage, et peut être personnalisé pour gérer un type spécifique de ressources NFVI. Par exemple, un gestionnaire d'infrastructure WAN établit une connectivité entre les points d'extrémité au sein du réseau. Le VIM peut également gérer les ressources virtuelles de calcul, de stockage et de réseau dans le NFVI à travers certaines de ses interfaces externes [13].

1.7.4 Fonction de réseau virtuel

La couche de fonction de réseau virtuel constitue la partie supérieure de l'architecture NFV définie par l'ETSI. Elle englobe les fonctions de réseau virtuel qui remplacent les fonctions de réseau physique traditionnelles. Les VNF peuvent être interconnectées pour créer des environnements de réseaux virtuels. Ces VNF s'exécutent sur des machines virtuelles, utilisant l'infrastructure fournie par le NFVI. Les VNF offrent des fonctionnalités de réseau sous forme de logiciels, qui étaient auparavant assurées par des équipements matériels spécialisés et propriétaires. Dans le cadre des VNF, des équipements matériels standard, communément appelés COTS, sont utilisés au niveau de la couche NFVI pour héberger les VNF. Chaque VNF présent dans la couche VNF est isolé des autres, et il est constitué de plusieurs VNFC. La gestion de ces composants est assurée par un système de gestion des éléments EMS. Plusieurs éléments sont gérés dans un seul domaine, formant ainsi un système de gestion des éléments EMS.

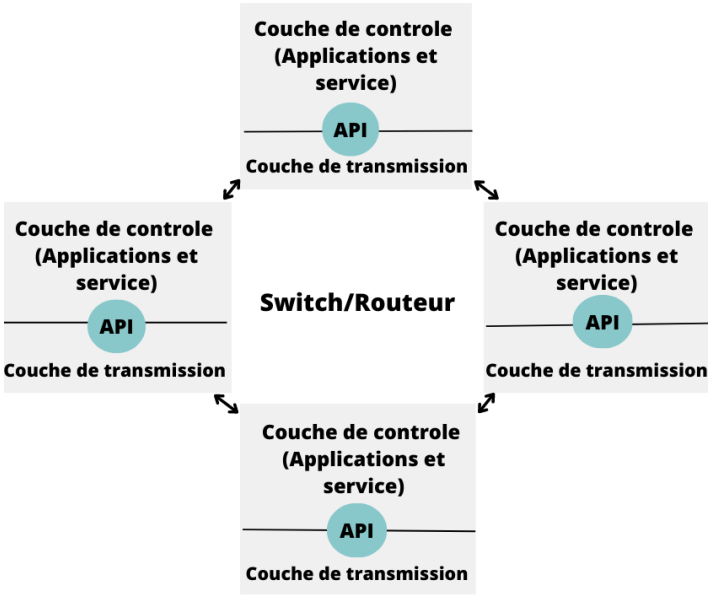
L'EMS fait partie de la couche VNF et collabore avec les VNFM pour échanger des informations relatives aux VNF et les gérer. Le chaînage de plusieurs VNF peut être effectué en fonction des besoins de l'entreprise, lorsque les VNF sont répartis à différents emplacements et sélectionnés de manière dynamique pour former une chaîne de services [13].

1.8 Réseau défini par logiciel (SDN)

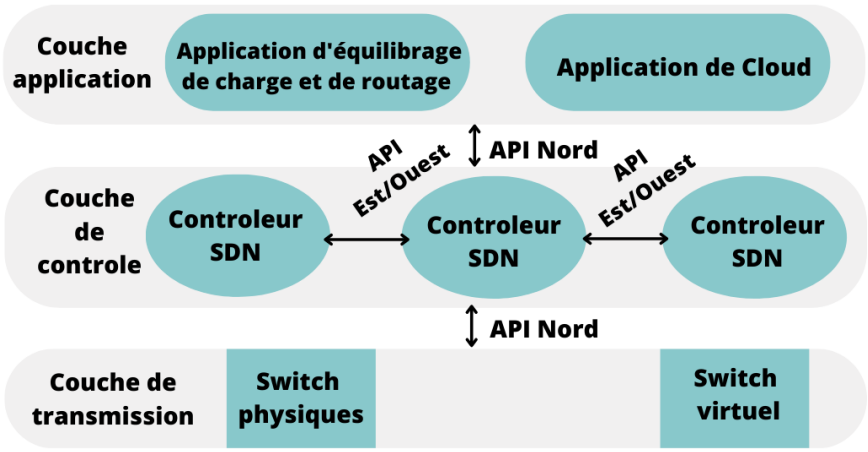
Selon l'ONF [20] SDN est une architecture qui sépare le plan de contrôle du plan de données, et unifie les plans de contrôle dans un logiciel de contrôle externe appelé « Contrôleur », pour gérer plusieurs éléments du plan de données via des APIs. Notons que l'ONF regroupe plus de 100 entreprises comportant les géants du web, les opérateurs de télécoms et les fabricants ce qui montre l'intérêt immense des industriels pour SDN [21]. Dans cette section, nous présentons l'architecture du SDN, son fonctionnement et décrivons ses principales composantes.

1.8.1 Architecture SDN

Dans un réseau, chaque équipement réseau est composé d'un plan de données et d'un plan de contrôle. L'objectif principal du plan de données est l'acheminement des données, tandis que le plan de contrôle se charge de l'ensemble des décisions de contrôle du réseau, par exemple pour décider à partir de quelle interface les données sont acheminées. Dans un réseau traditionnel, le plan de données et le plan de contrôle sont intégrés au sein du même équipement et les décisions sont prises localement par chaque équipement [21]. Le paradigme SDN met en avant l'idée de séparer le plan de données et le plan de contrôle. Comme le montre la Figure 1.11, les fonctions de contrôle du réseau sont déchargées de l'équipement réseau et placées dans des composants logiciels sur des périphériques externes dédiés appelés contrôleurs SDN.



(a) Réseaux traditionnel



(b) Réseaux SDN

FIGURE 1.11 – Comparaison entre l'architecture des réseaux traditionnel (a) et celle des réseaux SDN (b)

Le SDN est composé principalement de trois couches et d'interfaces de communication : [22]

1.8.1.1 Couches SDN

1. **Couche de transmission :** Également appelé "plan de données", il se compose de périphériques de d'acheminement tels que des commutateurs et des routeurs. Leur travail principal est de transmettre des données et de collecter des statistiques.

2. **Couche de contrôle :** Appelé aussi "plan de contrôle", il se compose principalement d'un ou plusieurs contrôleurs SDN dont le rôle est de contrôler et de gérer les équipements de l'infrastructure via des interfaces appelées "API sud".
3. **Couche application :** Représente les applications qui aident à fournir de nouvelles fonctionnalités réseau telles que l'ingénierie du trafic, la qualité de service et la sécurité. Ces applications sont construites à l'aide d'une interface de programmation appelée "API Nord".

1.8.2 Interfaces de communications

Il existe trois types d'interfaces permettent aux contrôleurs d'interagir avec les autres couches à travers les interfaces Sud et Nord et avec les autres contrôleurs à travers une interface Est-Ouest.

1. **Interface nord :** Les interfaces nord permettent aux applications d'envoyer des requêtes et des commandes au contrôleur SDN pour configurer et gérer le réseau et récupérer des informations. Les interfaces nord les plus courantes sont les API RESTful [20] qui sont des interfaces standardisées basées sur HTTP qui permettent aux applications de communiquer avec le contrôleur SDN.
2. **Interface Sud :** Les interfaces Sud représentent les interfaces de communication, qui permettent au contrôleur SDN d'interagir avec les périphériques de la couche d'infrastructure, tel que les commutateurs, et les routeurs. OpenFlow est le protocole le plus utilisé et déployé comme interface Sud, qui a été standardisé par l'ONF dont la dernière version est 1.5.1[24]. Plus de détails sur le protocole OpenFlow dans la section 1.8.3.
3. **Interface est/ouest :** Les interfaces Est/Ouest sont des interfaces de communication qui permettent la communication entre les contrôleurs dans une architecture multi-contrôleurs pour synchroniser l'état du réseau[23]. Ces architectures sont très récentes et il n'existe actuellement aucun standard de communication entre contrôleurs.

1.8.3 OpenFlow

1.8.3.1 Architecture OpenFlow

L'architecture Openflow est l'implémentation réelle des réseaux SDN, Cette architecture est basée principalement sur trois composantes : le plan de données, qui est composée des switches Openflow ; le plan de contrôle, constitué par des contrôleurs Openflow ; une chaîne sécurisée qui permettent aux commutateurs de se connecter au plan de contrôle. Selon la spécification d'ONF[25], un commutateur Openflow doit contenir un ou plusieurs tables de flux, ces tables de flux contiennent plusieurs entrées qui correspondent à des règles, où chacune est constituée principalement des trois champs suivants :

FIGURE 1.12 – Structure d'une entrée de table de flux d'un commutateur.

1. **En-tête de paquet :** le champ En-tête de paquet Contient les informations nécessaires pour définir un flux de données et déterminer à quels paquets cette règle s'applique. Les en-têtes de paquet peuvent identifier différents protocoles tels qu'Ethernet, IPv4, IPv6, MPLS, etc., selon la spécification Openflow utilisée.
2. **Compteur :** le champ Compteur est réservé à la collecte des statistiques de flux. Ils enregistrent le nombre de paquets et d'octets reçus de chaque flux, et le temps écoulé depuis le dernier transfert de flux
3. **Action :** le champ Action Spécifie comment gérer les paquets dans le flux. L'action peut être l'une des suivantes : Transférer le paquet vers un ou plusieurs ports, supprimer le paquet, transférer le paquet vers le contrôleur, ou modifier le champ d'en-tête de paquet.

1.8.4 Fonctionnement Openflow

Quand un paquet est reçu par le commutateur, son champ d'entête est examiné et comparé avec le champ "Match"dans les entrées de la table de flux. Si le match est identifié, le commutateur exécute l'action correspondante dans la table de flux. Par contre, s'il n'y a pas de match (1), une demande est envoyée au contrôleur (2) sous la forme d'un "Packet-in", puis le contrôleur décide selon sa configuration une action pour ce paquet, et envoie une nouvelle règle de transmission sous la forme d'un "Packet-out" et "Flow-mod" au commutateur (3). Enfin, la table de flux du commutateur est actualisée (4). La Figure 1.13 décrit le processus de transmission d'un paquet avec Openflow.[26]

FIGURE 1.13 – Processus de transmission d'un paquet avec openflow.

L'échange d'informations entre le commutateur et le contrôleur s'effectue par l'envoi de messages via un canal de contrôle sécurisé en utilisant TLS(protocole de sécurité utilisé pour sécuriser les communications).

1.9 Réseau étendu défini par logiciel

Le SD-WAN est une technologie dérivée de SDN. SD-WAN est une technologie de gestion des réseaux étendus qui apporte une approche moderne et efficace à la connectivité des

sites distants. Contrairement aux réseaux WAN traditionnels, qui utilisent principalement des connexions MPLS coûteuses et nécessitent une gestion manuelle complexe, le SD-WAN repose sur des principes de virtualisation, d'automatisation et de centralisation du contrôle pour plus de détail voir chapitre 2.

1.10 Conclusion

Dans ce chapitre, nous avons exploré divers aspects des réseaux et des technologies associées. Ces technologies jouent un rôle essentiel dans la transformation des réseaux, offrant des solutions innovantes pour répondre aux besoins croissants en matière de connectivité, de sécurité et de gestion des réseaux. Elles ouvrent de nouvelles possibilités pour les entreprises en termes de flexibilité, de rentabilité et de performances des réseaux.

Chapitre 2

Le réseau de l'entreprise NAFTAL-Bejaia

2.1 Introduction

Dans le premier chapitre , nous avons étudié sommairement les technologies réseaux. Dans ce chapitre, nous considérons les technologies réseaux au sein de l'entreprise NAFTAL de Bejaia. Nous commencerons par une présentation de l'organigramme de l'entreprise NAFTAL puis, nous présenterons la structure du réseau local de l'entreprise et les échanges avec la succursale d'Alger. Nous présenterons aussi les différents services qui la constituent, et nous expliquerons la problématique que nous traitons dans ce mémoire et qui a fait l'objet de notre stage au sein de l'entreprise.

2.2 L'Entreprise NAFTAL

Naftal, filiale à 100% du Groupe Sonatrach, est une société par actions (SPA) avec un capital social de 40 000 000 000 DA. Établie en 1982, elle opère principalement dans le domaine de la commercialisation des produits pétroliers et dérivés sur le marché national. Sa mission principale est d'assurer la distribution et la vente de ces produits. Elle intervient également dans le domaine de[27] :

- L'enfûtage des GPL;

- La formulation des bitumes ;
- La distribution, le stockage et la commercialisation des carburants, GPL, lubrifiants, bitumes, pneumatiques, GPL/carburant, produits spéciaux ;
- Le transport des produits pétroliers.

2.3 Missions et moyens de l'entreprise

2.3.1 Missions

La principale mission de l'entreprise NAFTAL consiste à distribuer et commercialiser cinq produits pétroliers et leurs dérivés sur le marché national. Ces cinq produits sont :

- Carburants lubrifiants et produits spéciaux qui constituent 75% de chiffre d'affaires de l'entreprise.
- Les gaz de pétrole liquéfié GPL en tant que butane conditionné.
- Les carburants et lubrifiants marins et l'aviation.
- Les bitumes.
- Les pneumatiques qui dépendent totalement de l'importation.

Par ailleurs, l'entreprise a l'obligation de :

- Organiser et développer l'activité commerciale sur le territoire national.
- Procéder à toutes les études du marché de consommation de produits pétroliers.
- Développer une image de marque et de qualité des produits pétroliers NAFTAL.

2.3.2 Moyens

Afin de remplir ses missions, NAFTAL dispose d'un important potentiel humain et matériel qui se compose de la manière suivante :

- **Moyens humains :** L'entreprise NAFTAL accorde une attention particulière à la formation et à la mise à niveau de son personnel afin de préparer sa ressource humaine et de faire face à la concurrence. À titre d'exemple, en 2007, NAFTAL a consacré un montant de 9 858 202.00 millions de DA, ce qui représente 3.4% de sa masse salariale, à des activités de formation. La formation des agents de NAFTAL est axée principalement sur les domaines suivants :
  - Le management
  - Le marketing
  - La distribution
  - Les sciences des risques industriels et technologiques.
- **Moyens matériaux :** Comportent :
  - 80 Centres de distribution et stockage
  - 41 Centres d'emplissage
  - 15 Unîtes de formulation bitumes
  - 49 Dépôts
  - 24 Centres d'aviation
  - 06 Centres marins
  - 1800 Stations-service dont 1100 appartiennent aux privés.

2.4 Organisation de NAFTAL

L'organisation de NAFTAL repose sur la centralité de ses métiers de base et de ses différents produits. Sa structure se compose de cinq branches distinctes.

1. Branche GPL (Gaz Pétrole Liquide).
2. Branche carburante.
3. Branche commercialisation (Lubrifiants, Pneumatique, Bitume).

4. Branche activité internationale.

L'organigramme de l'entreprise est schématisé de manière à refléter sa structure hiérarchique par la figure 2.1.

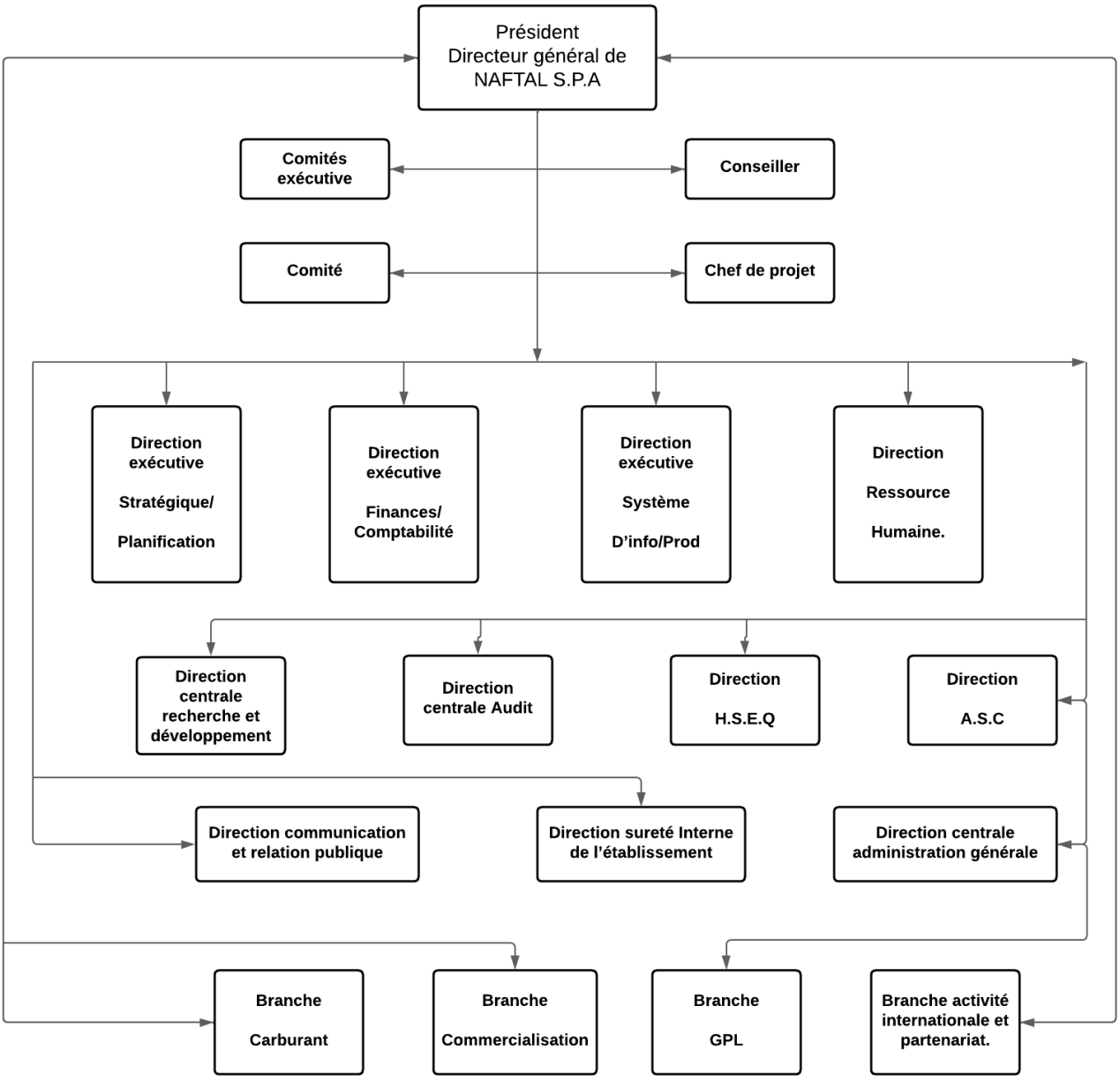


FIGURE 2.1 – Organigramme de la direction générale de NAFTAL.

2.5 Présentation du centre Bitume

Un centre Bitume est généralement composé de différents éléments et zones spécifiques pour le stockage et le traitement du bitume.

2.5.1 Définition de bitume

Le bitume est un produit dérivé du raffinage du pétrole, représentant la fraction la plus lourde. Il est obtenu par le processus de distillation sous vide du résidu issu de la distillation atmosphérique. À la suite de ce processus, on obtient un résidu viscoélastique de couleur noire situé au fond de la colonne de distillation sous vide.

2.5.2 Répartition géographique des centres bitumes

Les centres bitumes de NAFTAL sont répartis dans quatre régions à travers le territoire national.

- Les centres bitumes de la région centre
  1. BTM Alger
  2. BTM Ain-Defla

- Les centres bitumes de la région Est
  1. BTM Oum-El-Bouaghi
  2. BTM Batna
  3. BTM Bejaia
  4. BTM Skikda
  5. BTM El Eulma
  6. BTM Annaba

- Les centres bitumes de la région ouest
  1. BTM Oran

2. BTM Mostaganem
3. BTM Ain-Sefra

- Les centres bitumes de la région sud
  1. BTM Touggourt
  2. BTM Ain-Salah
  3. BTM Ghardaia
  4. BTM Tamanrasset

2.6 Services de l'entreprise NAFTAL-Bitume de Bejaia

Au sein de l'entreprise NAFTAL Bitume Bejaïa, il existe plusieurs services distincts qui sont en mesure de répondre aux besoins de l'entreprise, chacun ayant ses propres domaines de spécialisation, compétences et attributions spécifiques en matière de fonctionnement et de gestion. Parmi les services existants, le service commercial est chargé de la vente de produits, le service marketing élabore les stratégies de communication et de promotion, le service technique est dédié à la maintenance et la réparation des équipements et des installations. La figure 2.2 montre une représentation graphique de la structure hiérarchique de l'entreprise, qui permet de visualiser les différents niveaux de responsabilités et les relations entre les différents départements et postes.

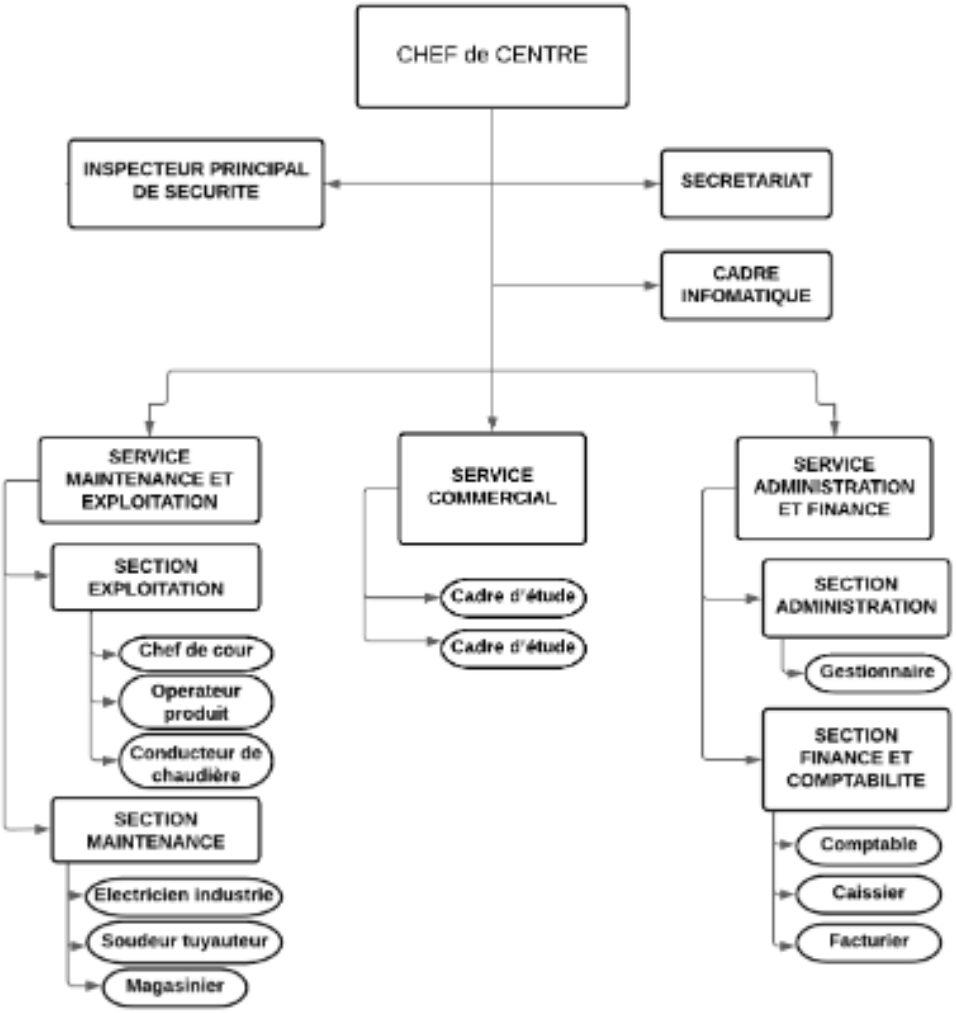


FIGURE 2.2 – Organigramme du centre NAFTAL Bitume de Bejaia.

2.7 Gestion informatique des services

La gestion informatique des services vise à aligner les services informatiques sur les besoins de l'entreprise, à améliorer la qualité des services et à optimiser l'efficacité des services informatiques.Cette dernière est essentielle pour aider les entreprises à atteindre leurs objectifs stratégiques en utilisant efficacement les ressources informatiques. Elle est également importante pour maintenir la satisfaction des utilisateurs finaux en fournissant des services informatiques fiables et de qualité.

a) **Rôle du service informatique :** Consiste à assurer la maintenance du matériels et logiciels informatiques, les systèmes et applications ainsi suivre les différentes activités d'administration du réseau et encore l'analyse des états et veiller au recueil de l'information.

b) **Applications des services :** Chaque service est constitué d'une ou plusieurs applications informatiques dont les bases de données sont situées au niveau central (Alger).

- **service informatique :** utilise une application de gestion appelé PRC (Prime de Rendement Collectif) dédié au calcul des primes pour les employés s'ils atteignent l'objectif de l'entreprise.
- **service technique et exploitation :** utilise les applications suivantes : gestion des stocks, suivi de parc roulant, suivi des maintenances.
- **service commercial :** vu l'importance d'avoir un débit élevé pour simplifier la synchronisation, ce service utilise l'application SDCOM en mode non connecté basé sur les réplications des données vers les serveurs central au niveau d'Alger et l'application SDG (Système de Gestion de Créance).
- **service finance et comptabilité :** utilise des applications en mode connecté tel que l'application NAFTIMO dédiée à la gestion du patrimoine de NAFTAL et l'application NAFTCOMPTA.

2.8 Analyse du réseau informatique

Dans l'analyse du réseau informatique, nous avons pris en considération les éléments suivants : les équipements réseaux existants, le fonctionnement actuel ainsi que les limitations identifiées. Ces éléments ont été détaillés dans les sous-sections suivantes afin de fournir une évaluation complète et des recommandations pour améliorer l'efficacité et la performance du réseau.

2.8.1 Équipements réseaux existants

Il existe une variété d'équipements réseau essentiels pour connecter, gérer et sécuriser les réseaux informatiques. On peut citer les routeurs pour acheminer les paquets de données, des commutateurs pour relier les périphériques au sein d'un réseau local, des pare-feux pour filtrer le trafic et protéger contre les attaques, des points d'accès sans fil pour offrir une connectivité Wi-Fi aux employés, des serveurs pour héberger des applications et des données, des baies de stockage pour centraliser et gérer les données, et des solutions de virtualisation pour créer des environnements réseau virtuels flexibles et évolutifs.

L'armoire de brassage contient :
- 01 Routeur CISCO de la gamme Cisco 2900.
- 02 commutateurs CISCO de la gamme Cisco Catalyst 2960.

2.8.2 Fonctionnement actuel

NAFTAL bénéficie d'un réseau informatique étendu couvrant plusieurs Wilayas. Il est interconnecté grâce à des VPN basés sur Internet ADSL ainsi que des VPN basés sur la technologie 4G d'Ooredoo. Cette infrastructure permet une connectivité étendue et sécurisée entre les différents sites de l'entreprise, facilitant ainsi la communication et le partage de données. Les deux types de connextion VPN offrent un accès distant aux ressources réseau avec une connectivité fiable, sécurisé. Les deux technologies de réseau sont fonctionnelles en alternance même si elles offrent à NAFTAL une infrastructure solide pour soutenir ses opérations dans les différentes Wilayas. Néanmoins elle présente quelques limitations.

FIGURE 2.3 – Architecture réseau de Bitume vers Alger.

2.8.3 Limitations

Le réseau de NAFTAL, utilisant le routeur Cisco de la série 2900, rencontre des problèmes de simultanéité entre les deux lignes de connexion. Même lorsque la connexion Internet ADSL atteint 2 Mbps, la connexion 4G Ooredoo ne prend pas automatiquement le relais, le fait qu'elle nécessite une intervention manuelle pour effectuer la transition. En outre, le réseau connaît des problèmes de bande passante limitée, entraînant une faible performance lors des transferts de données. Des problèmes de latence élevée sont également présents, impactant la réactivité du réseau et causant des retards indésirables. Pour garantir un fonctionnement stable et efficace du réseau de NAFTAL, une solution prometteuse est l'adoption de la technologie SD-WAN, qui peut aider à résoudre ces problèmes.

2.9 Conclusion

Ce chapitre nous a permis de développer une compréhension approfondie du réseau d'entreprise NAFTAL BITUMES de BEJAIA, où nous avons effectué notre stage pratique. Au cours de cette étude, nous avons identifié les lacunes et les faiblesses du réseau, ce qui nous a permis de proposer des solutions pour remédier à ces problèmes et améliorer le réseau de manière significative. En particulier, nous nous interesserons à la solution Fortinet SD-WAN.

Chapitre 3

La technologie SD-WAN

3.1 Introduction

Dans le chapitre précédent, nous avons présenté et identifié les limitations du réseau NAFTAL-Bitume Bejaia. Ce chapitre présente la solution SDWAN pour remédier à ces limitations. Nous aborderons dans la section 2, 3 et 4 ses composants essentiels ainsi que ses caractéristiques spécifiques. Ensuite, dans la section 5, nous passerons en revue les fournisseurs offrant cette solution ainsi que les composants associés à chacun d'entre eux. Enfin, nous conclurons avec les apports que cette solution a apportée à l'entreprise en terme d'efficacité, de flexibilité et sécurité.

3.2 Réseau étendu défini par logiciel (SD-WAN)

Le SD-WAN est une technologie dérivée de SDN. SD-WAN est une solution de réseau virtuel qui permet de créer un réseau étendu sécurisé, fiable et performant. Il utilise un système logiciel pour centraliser, configurer et automatiser la gestion et le fonctionnement de la connectivité réseau, ce qui permet aux entreprises de connecter facilement leurs succursales et leurs sites distants au réseau central. Avec le SD-WAN, l'objectif final est de créer un réseau crypté unique, sécurisé et commun qui peut utiliser l'Internet à large bande, LTE, les lignes louées ou toute combinaison de circuits disponibles de manière intelligente et effi-

cace. En outre, un environnement SD-WAN correctement mis en œuvre devrait être en mesure de basculer de manière transparente les sessions de réseau entre les circuits en fonction des besoins, sans interruption des services [28].

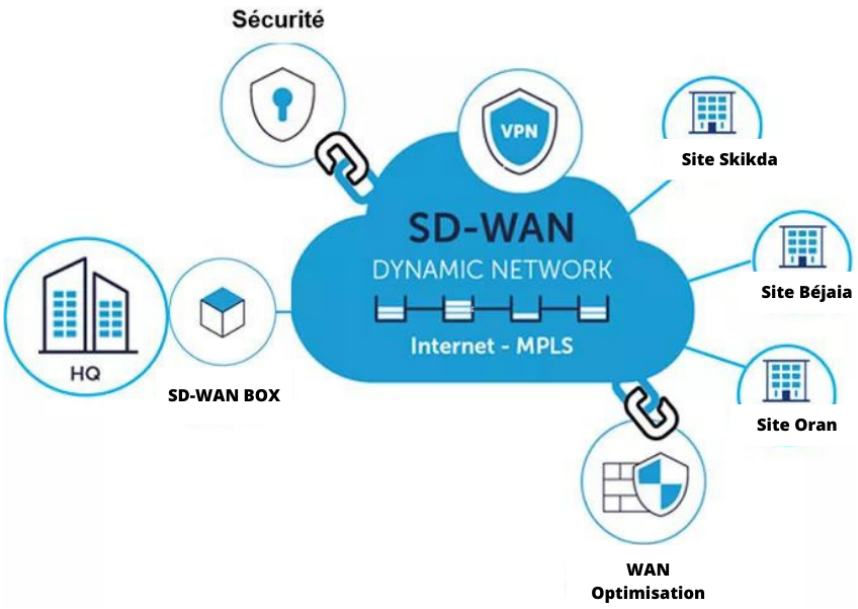


FIGURE 3.1 – Architecture globale du SD-WAN

3.3 Composants du SD-WAN

Le SD-WAN peut être décomposé en trois couches :

1. **Gestion et Orchestration :**

   La couche de gestion et d'orchestration joue un rôle essentiel dans la gestion, le contrôle et la coordination des éléments du réseau. Cette couche est responsable de la configuration, du déploiement, de la surveillance et de la gestion des politiques de trafic au sein du SD-WAN. [29]

   Voici quelques-unes des principales fonctions et responsabilités de la couche de gestion et d'orchestration dans un réseau SD-WAN [30, 31] :

   - **Configuration et déploiement :** La couche de gestion et d'orchestration permet de configurer et de déployer les différents éléments du réseau SD-WAN, tels que

les dispositifs de passerelle SD-WAN, les contrôleurs, les points de terminaison, etc. Elle facilite également la mise à jour et la gestion des configurations de ces éléments.

- **Gestion des politiques :** Cette couche permet de définir et de gérer les politiques de trafic du réseau SD-WAN. Elle permet de spécifier les règles de routage, de priorisation du trafic, de sécurisation et d'optimisation du réseau. Les politiques peuvent être basées sur divers critères, tels que l'application, le type de trafic, la bande passante disponible, etc.
- **Surveillance et gestion des performances :** La couche de gestion et d'orchestration surveille en permanence les performances du réseau SD-WAN. Elle collecte des informations sur le trafic, la latence, la gigue, la perte de paquets, la bande passante utilisée, etc. Ces informations permettent d'évaluer la santé du réseau et d'identifier les problèmes de performance ou de congestion.
- **Orchestration du réseau :** Cette couche coordonne les différents éléments du réseau SD-WAN . Elle gère la connectivité entre les sites distants, les connexions Internet, les liens MPLS, les connexions VPN, etc. Elle peut également effectuer des opérations d'agrégation de liens, de répartition de charge et de redondance pour optimiser la connectivité et la disponibilité du réseau.
- **Sécurité et politique d'accès :** La couche de gestion et d'orchestration prend en charge la mise en œuvre des politiques de sécurité du réseau SD-WAN. Elle peut fournir des fonctionnalités de pare-feu, de chiffrement, de détection des menaces et de segmentation du réseau. Elle permet également de gérer les politiques d'accès et les autorisations des utilisateurs, en définissant des règles de contrôle d'accès et en intégrant des mécanismes d'authentification et d'identification.

2. **Contrôle, plan de données et sécurité :**

La couche de contrôle, de plan de données et de sécurité est une composante essentielle qui permet de gérer le trafic, d'optimiser les performances et de garantir la sécurité des communications au sein du réseau. Cette couche est responsable de la

gestion de l'acheminement des données, de l'application des politiques de sécurité et de la supervision du trafic[4].

Voici les principales fonctions et responsabilités de la couche de contrôle, de plan de données et de sécurité dans un réseau SD-WAN [31, 1] :

- **Contrôle de trafic :** Cette couche est chargée de contrôler le flux de trafic dans le réseau SD-WAN. Elle utilise des mécanismes d'acheminement intelligents pour déterminer le meilleur chemin pour les paquets de données en fonction des politiques de routage définies. Cela permet d'optimiser la performance du réseau en choisissant les liens les plus appropriés en termes de latence, de bande passante et de disponibilité.
- **Plan de données :** La couche de plan de données est responsable du transfert des paquets de données à travers le réseau SD-WAN. Elle assure le transport efficace des données en utilisant des techniques telles que la répartition de charge, la déduplication, la compression et la correction d'erreur. Cette couche permet également d'établir des tunnels sécurisés (comme les VPN) pour protéger les données transitant sur le réseau.
- **Supervision et surveillance :** La couche de contrôle, de plan de données et de sécurité supervise en permanence le trafic du réseau SD-WAN. Elle collecte des informations sur les performances du réseau, la latence, la bande passante utilisée, les erreurs de transmission, les menaces potentielles, etc. Ces données sont utilisées pour optimiser les performances du réseau, détecter les problèmes potentiels et prendre des mesures correctives.
- **Gestion des politiques de sécurité :** Cette couche permet de définir et d'appliquer des politiques de sécurité cohérentes sur l'ensemble du réseau SD-WAN. Elle facilite la gestion centralisée des règles de sécurité, telles que les politiques de filtrage, les règles de pare-feu, les politiques de VPN, etc. Cela garantit une sécurité uniforme et cohérente pour toutes les communications au sein du réseau.

3. **Accès au réseau** La couche d'accès au réseau joue un rôle crucial en fournissant une

connectivité aux sites distants, aux utilisateurs et aux appareils. Cette couche est responsable de l'établissement des connexions, de la gestion des accès et de l'optimisation de la connectivité. Voici les principales fonctions et responsabilités de la couche d'accès au réseau dans un réseau SD-WAN [30] :

- **Connexion aux sites distants :** La couche d'accès au réseau facilite la connectivité entre les sites distants et le réseau SD-WAN. Elle permet d'établir des connexions fiables et sécurisées, que ce soit via des liens MPLS traditionnels, des connexions Internet haut débit ou des technologies sans fil. Elle peut également gérer l'agrégation de liens pour optimiser la bande passante disponible.
- **Gestion des accès utilisateurs :** Cette couche permet de gérer les accès des utilisateurs au réseau SD-WAN. Elle offre des mécanismes d'authentification et d'identification pour s'assurer que seuls les utilisateurs autorisés peuvent accéder aux ressources du réseau. Cela peut inclure l'intégration de protocoles d'authentification tels que RADIUS (Remote Authentication Dial-In User Service).
- **Optimisation de la connectivité :** La couche d'accès au réseau optimise la connectivité en choisissant les meilleures options d'accès en fonction des exigences de performance, de coût et de disponibilité. Elle peut effectuer une sélection intelligente des liens disponibles en fonction des conditions du réseau, en utilisant des techniques telles que la répartition de charge, la détection de liens dégradés et la commutation sans interruption.
- **Gestion des politiques de trafic :** Cette couche gère les politiques de trafic pour définir le comportement des connexions d'accès au réseau. Elle peut définir des règles pour la priorisation du trafic, la gestion de la bande passante, QoS et d'autres paramètres liés à la performance. Cela permet de garantir des performances optimales pour les applications critiques et de limiter l'impact des applications

3.4 Protocoles utilisés dans la technologie SD-WAN

Dans une technologie SD-WAN, plusieurs protocoles sont employés , Voici quelques-uns des protocoles fréquemment [41, 44] :

- BGP (Border Gateway Protocol) : BGP est un protocole de routage utilisé pour établir et maintenir les tables de routage entre les différents sites d'un réseau SD-WAN. Il permet aux routeurs de prendre des décisions de routage intelligentes en fonction des politiques définies.
- OSPF (Open Shortest Path First) : OSPF est un protocole de routage intérieur utilisé pour déterminer les meilleures routes au sein d'un réseau SD-WAN. Il favorise la convergence rapide et l'efficacité du routage en échangeant des informations de routage entre les routeurs.
- SNMP (Simple Network Management Protocol) : SNMP est un protocole de gestion utilisé pour surveiller et gérer les équipements d'un réseau SD-WAN. Il permet la collecte d'informations. Il permet également la configuration à distance des équipements SD-WAN. Les administrateurs peuvent utiliser SNMP pour modifier les paramètres de configuration des équipements, tels que les adresses IP, les règles de routage, les règles de pare-feu, etc. Cela facilite la gestion centralisée des équipements et simplifie les tâches de configuration et de maintenance.
- GRE (Generic Routing Encapsulation) : GRE est un protocole de mise en encapsulation utilisé pour créer des tunnels virtuels dans un réseau SD-WAN. Il permet d'acheminer différents types de trafic entre les sites distants de manière transparente.
- Le protocole Syslog : Syslog est essentiel dans les réseaux SD-WAN. Il collecte et transfère les messages de journalisation vers un serveur centralisé, appelé "syslog server". Les appareils et les applications du réseau envoient des événements et des informations de journalisation à ce serveur, qui les stocke, les analyse et les gère. Cela permet une surveillance et un dépannage efficaces du réseau.ce protocole est utilisé pour enregistrer les événements de sécurité, les erreurs de routage, les performances du réseau,

et d'autres informations pertinentes. Il aide les administrateurs à comprendre l'état du réseau, à diagnostiquer les problèmes et à prendre des mesures appropriées pour garantir un fonctionnement optimal du SD-WAN.

- API propriétaires : Ces API propriétaires facilitent la configuration, la gestion et la surveillance des appareils SD-WAN, ainsi que l'automatisation des opérations réseau. Elles permettent également d'accéder aux données et aux statistiques de performance du réseau, ce qui contribue à une meilleure visibilité et prise de décision dans un environnement SD-WAN.
- SSH (Secure Shell) :SSH est utilisé par FortiManager pour établir une connexion sécurisée avec les appareils du réseau SD-WAN. Cela permet aux administrateurs d'accéder aux appareils et de les configurer de manière sécurisée.
- REST API (Representational State Transfer Application Programming Interface) : FortiManager propose une interface de programmation RESTful API pour permettre une intégration et une automatisation faciles avec d'autres systèmes et applications du réseau SD-WAN. Cela permet aux administrateurs d'effectuer des opérations de gestion à distance, telles que la configuration des appareils et la gestion des politiques.

3.5 Caractéristiques principales de SD-WAN

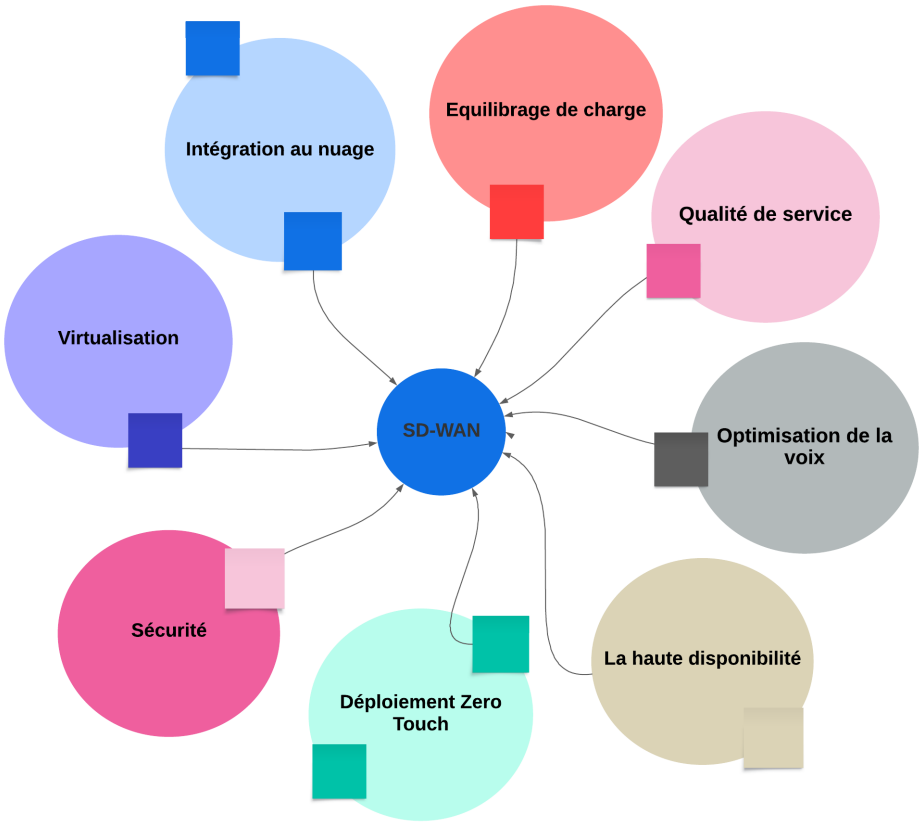


FIGURE 3.2 – Caractéristiques du SD-WAN.

- **Virtualisation :** Le réseau étendu défini par logiciel, est abstrait du matériel de réseau et fonctionne sur son réseau virtuel superposé avec ses composants. Cette indépendance par rapport au réseau matériel sous-jacent confère au SD-WAN une grande flexibilité. Il peut utiliser différentes liaisons, telles que LTE ou Internet à large bande, entre une succursale et un centre de données ou un fournisseur de services SaaS. Dans les configurations traditionnelles, toutes les succursales acheminent leur trafic vers le centre de données, peu importe sa nature. Cela peut entraîner une augmentation de la latence, une congestion de la liaison et des performances médiocres des applications. Avec le SD-WAN, qui peut utiliser plusieurs liaisons au niveau de la succursale et du centre de données, le trafic devient prioritaire et toutes les liaisons disponibles sont exploitées.

Par exemple, il peut utiliser le MPLS pour le trafic critique destiné au centre de données, tandis que le LTE ou la large bande peut être utilisé pour le trafic d'application vers un fournisseur de services en nuage, grâce à la segmentation du trafic d'application. Il utilise intelligemment les liaisons et, en cas de dégradation des performances d'une liaison, il bascule automatiquement vers les autres liaisons disponibles. De plus, grâce à l'abstraction logicielle et matérielle, il facilite l'installation de nouvelles liaisons[32].

- **Intégration au nuage :** L'intégration des services cloud tels que SaaS, PaaS et IaaS est de plus en plus demandée en raison de l'augmentation rapide des services et des applications hébergés dans le cloud. Traditionnellement, l'accès aux services cloud se fait par le biais d'un centre de données ou d'une passerelle internet centralisée, ce qui peut entraîner des latences élevées et une expérience utilisateur médiocre. Cependant, les implémentations de SD-WAN, telles que Cisco SD-WAN, offrent des solutions de connexion cloud qui contournent ces contraintes. Ces solutions permettent un accès direct à Internet à partir des succursales ou des centres régionaux, optimisant ainsi la qualité de l'expérience et réduisant le trafic sur le réseau de l'entreprise. En utilisant dynamiquement le meilleur chemin en fonction des types de services[4].
- **Equilibrage de charge :** Le SD-WAN offre une fonctionnalité d'équilibrage de charge qui permet d'utiliser efficacement plusieurs liens pour acheminer le trafic. Cette fonctionnalité repose sur des politiques ou sur l'état du réseau. Le SD-WAN peut établir un tunnel VPN pour chaque liaison WAN physique, et en fonction de l'état de chaque liaison en termes de congestion, de latence et de défaillance, les bords du SD-WAN peuvent décider de rediriger une partie du trafic vers une liaison alternative. Cette approche permet de réduire la saturation, de choisir les meilleures liaisons pour chaque application et de donner la priorité aux applications. L'administrateur du réseau a également la possibilité de limiter la bande passante d'une liaison spécifique afin d'éviter la surcharge, et de limiter la bande passante utilisée par un seul utilisateur pour prévenir la saturation du réseau due à un trafic excessif de certains utilisateurs connectés[33].
- **Qualité de service :** La QoS (Quality of Service est utilisée pour hiérarchiser et prioriser le trafic en fonction de ses exigences de performance, garantissant ainsi une bande

passante suffisante, une faible latence, une faible gigue (jitter) et une faible perte de paquets aux applications critiques.

La perte de paquets qui se produit lorsque les liaisons réseau se congestionnent et que les routeurs et les commutateurs commencent à ne plus tenir compte des paquets. Quand ce phénomène a lieu lors d'une communication en temps réel, par exemple au cours d'un appel vocal ou vidéo, des instabilités ou des trous peuvent apparaître lors de la transmission.

La gigue peut apparaître en cas d'encombrement du réseau, de dérive temporelle ou de changement d'acheminement. Si elle est trop importante, la qualité de la communication vocale ou vidéo se dégrade.

La latence est la durée du trajet d'un paquet de sa source jusqu'à sa destination. Elle doit s'approcher autant que possible de zéro. Si un appel vocal sur IP (VoIP) a une latence élevée, on entend de l'écho et un mélange de sons.

La bande passante est la capacité maximale de transmission, d'un point à un autre, d'un volume de données sur une ligne de communication en un temps donné. La QoS optimise le réseau en en gérant la bande passante et en hiérarchisant les applications selon les ressources dont elles ont besoin.

- **Optimisation de la voix :** Deux des flux les plus exposés à la perte de performance, et donc à une faible QoE pour les utilisateurs, sont les flux VoIP et les flux de streaming. Pour les flux VoIP, il est essentiel d'avoir à la fois une bande passante suffisante et une gigue minimale ainsi qu'une latence réduite.
  Les problèmes liés au VoIP sont généralement liés à la transmission du trafic VoIP par une seule liaison. Avec l'introduction du SD-WAN, il est possible de choisir entre plusieurs liens et de décider en temps réel lequel utiliser en fonction des conditions actuelles du réseau. Le choix du lien permet d'obtenir une meilleure qualité d'expérience de l'appel, faible latence et de gigue[34]. Par ailleurs, les fournisseurs adoptent de plus

en plus l'utilisation d'une technique particulière appelée duplication package. Cette technique consiste à envoyer la même information sur deux liaisons physiques différentes, comme l'illustre la figure 3.3. De cette manière, en cas de perte de paquets, il suffira d'utiliser le flux de secours pour obtenir les paquets perdus. L'inconvénient de cette technique est une utilisation importante de la bande passante, mais, grâce à l'augmentation constante de la bande passante offerte par les fournisseurs, cette méthode peut être acceptable dans certains scénarios. En outre, dans le cas où la bande passante supplémentaire est requise par d'autres applications, il est possible de mettre fin à la deuxième liaison et de réduire ainsi la bande passante utilisée pour un appel VoIP.

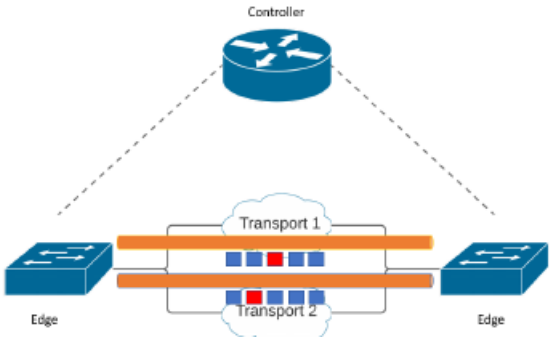


FIGURE 3.3 – Stratégies d'optimisation de la VoIP.

- **La haute disponibilité** HA est une propriété d'un système qui vise à assurer un niveau de fonctionnement supérieur à la normale en mettant en place un ensemble de procédures et de mesures. La HA est exprimée en pourcentage, variant de 0 à 100, où 100 correspond à une infrastructure réseau toujours opérationnelle. L'un des principaux aspects de La haute disponibilité est lié au basculement, c'est-à-dire à la capacité de créer une redondance au niveau de l'équipement et/ou des liens afin de maintenir l'ensemble de l'infrastructure en état de marche. Il doit avoir lieu à tous les niveaux du SD-WAN : les plans de données, de contrôle et d'application, ainsi que les connexions entre les différents niveaux.

Plan de gestion Plan de gestion Le niveau de gestion du SD-WAN est assuré par une grappe d'applications. Les clusters sont situés dans le même centre de données et sont tous actifs en même temps. En outre, pour maintenir la redondance géographique, ils sont également dupliqués dans différents centres de données, auquel cas les applications doivent rester actives/passives[35]. En outre, les applications sont conçues de manière modulaire afin d'éviter les défaillances en cascade entre les différents services, et donc de limiter les inefficacités entre les différentes fonctions du niveau de gestion. Enfin, en cas de panne générale (par exemple, causée par la non-accessibilité de tous les serveurs de gestion), le SD-WAN est conçu pour maintenir l'état actuel et donc garantir le fonctionnement tout en maintenant les politiques de l'état actuel[36].

Plan de control Au niveau du contrôle, il existe différentes approches utilisées pour assurer la haute disponibilité en cas de défaillance d'un ou de plusieurs contrôleurs. Certaines de ces approches incluent l'utilisation de SMaRtLight[37], qui est un magasin de données permettant une sauvegarde immédiate en cas de panne d'un contrôleur. Cette approche permet de copier la configuration vers un autre contrôleur.

Plan de donnée En ce qui concerne la partie des données, la haute disponibilité peut être atteinte en connectant deux routeurs et en les configurant avec le protocole VRRP Le VRRP permet de regrouper plusieurs routeurs physiques et de les consolider en un seul routeur virtuel (c'est-à-dire un routeur avec une adresse IP virtuelle), comme illustré dans la figure3.4[43] [4].

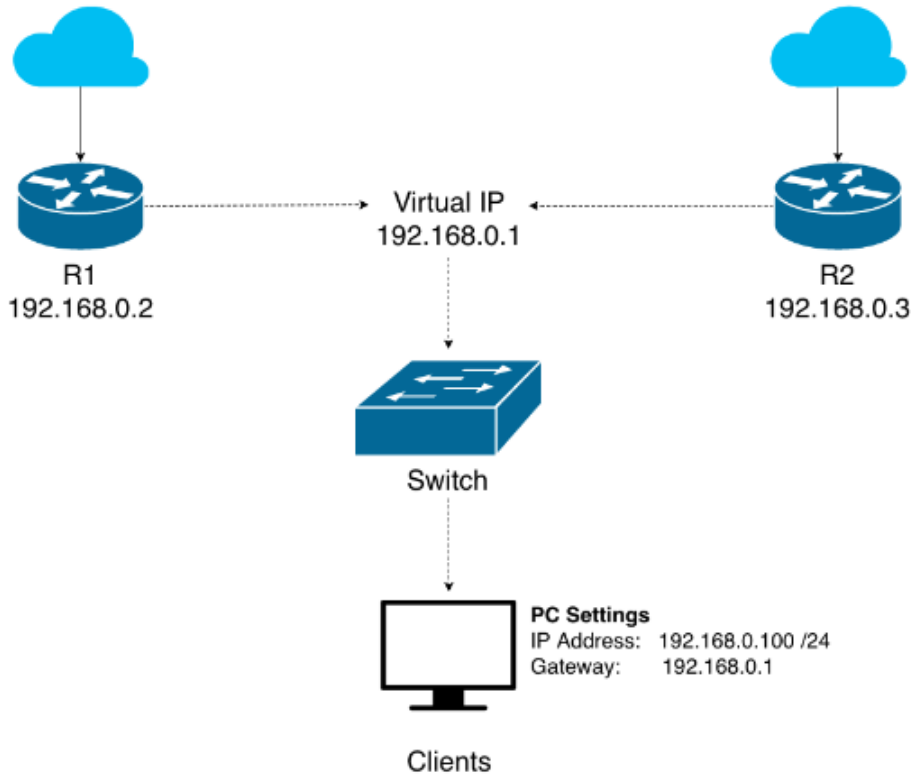


FIGURE 3.4 – Protocole de redondance de routeur virtuel.

- **Déploiement Zero Touch :** Il fait référence à un processus de déploiement automatisé et simplifié des périphériques SD-WAN, qui nécessite un minimum d'interventions manuelles. Avec le déploiement ZeroTouch, les appareils SD-WAN peuvent être configurés et déployés sans qu'un technicien doive se rendre physiquement sur le site. Les appareils sont préconfigurés en usine avec les paramètres appropriés et peuvent être expédiés directement aux sites distants. Les politiques de sécurité, les règles de routage et d'autres paramètres de configuration peuvent être déployés de manière centralisée à partir du contrôleur SD-WAN. Le déploiement ZeroTouch permet d'économiser du temps, des ressources et des coûts en simplifiant et en accélérant le processus de déploiement des appareils SD-WAN [39].
- **Sécurité :** Avec le SD-WAN, les administrateurs réseau peuvent gérer et orchestrer de manière centralisée les composants du réseau, y compris la sécurité. Il offre une meilleure sécurité que le WAN traditionnel en virtualisant les fonctions de sécurité ainsi que d'autres fonctions. Le SD-WAN utilise couramment des VPN basés sur IPsec pour ga-

rantir la sécurité du trafic sur l'internet public. Les VPN jouent un rôle clé dans la sécurité du SD-WAN en offrant une visibilité et un contrôle supplémentaires par rapport aux réseaux étendus traditionnels. Les administrateurs réseau peuvent surveiller le réseau et s'assurer que les éléments et les politiques de sécurité fonctionnent correctement. Un élément clé supplémentaire de la sécurité du SD-WAN est le pare-feu de nouvelle génération, qui est une version virtuelle capable d'inspecter en profondeur les paquets. Il peut intégrer plusieurs fonctions virtualisées, telles que la détection des applications, la détection et la prévention des intrusions, l'antivirus, etc. Grâce à la virtualisation des fonctions réseau, le SD-WAN peut placer ces fonctions de sécurité là où elles sont nécessaires pour une application spécifique[39] [40].

3.6 Fournisseurs de solutions SD-WAN

De nombreuses entreprises qui proposent des solutions et des produits SD-WAN sont présentes sur le marché. Chacune de ces entreprises propose ses propres solutions et outils. Chaque année, Gartner, un organisme de recherche et de conseil indépendant hautement respecté, publie un rapport intitulé "Magic quadrant for WAN-edge infrastructure" qui offre une analyse et un examen détaillés des différents fournisseurs présents sur le marché mondial des infrastructures de périphérie de réseau étendu. La figure 3.5 illustre le schéma du quadrant magique pour l'infrastructure de périphérie de réseau étendu publié par Gartner en septembre 2022 [42].

Gartner utilise une approche en quatre quadrants qui sont les leaders, les visionnaires, les challengers et les acteurs de niche. Ces quadrants sont basés sur deux critères principaux : la capacité d'exécution et l'exhaustivité de la vision. On peut observer que des fournisseurs Cisco, Fortinet, VMware, Versa Networks et Palo Alto Networks sont classés en tant que leaders dans le domaine des solutions SD-WAN. Juniper Networks est quant à lui considéré comme un visionnaire, tandis que Huawei est classé comme un challenger dans ce domaine. D'autres fournisseurs tels que Barracuda, Citrix et d'autres encore sont considérés comme des acteurs de niche dans le domaine des solutions SD-WAN[42]. Nous nous

intéresserons par la suite aux 3 leaders des solutions SDWAN, et nous décrirons leurs composants essentiels.

FIGURE 3.5 – Les meilleurs fournisseurs de SD-WAN selon le rapport 2022 de Gartner.

3.6.1 Solution Fortinet SD-WAN

Fortinet est une entreprise spécialisée dans le domaine de la sécurité des réseaux, offrant une gamme complète de produits tels que les pare-feu, les systèmes de prévention des intrusions et bien d'autres. Fortinet propose une solution sécurisée de SD-WAN intégrée à ses pare-feux FortiGate, disponible en tant que service. Cette solution combine les fonctionnalités de mise en réseau et de sécurité de FortiGate dans un seul appareil. Le pare-feu FortiGate, qui peut être un CPE (fait référence à l'équipement situé chez le client) physique propriétaire ou une machine virtuelle hébergée sur un équipement client universel, agit en

tant qu'appareil capable d'exécuter des VNF. Cette appareil est gérée par un orchestrateur dans FortiManager, offrant une gestion centralisée et simplifiée de l'ensemble du système [28]. Nous détaillerons ci-dessous ses différents composants essentiels et leur principe de fonctionnement :

3.6.1.1 Composants SD-WAN

La solution SD-WAN de Fortinet se compose de plusieurs éléments voir figure3.6. Les composants essentiels qui constituent la solution SD-WAN sécurisée de Fortinet sont FortiGate, FortiManager, FortiAnalyzer [43, 44].

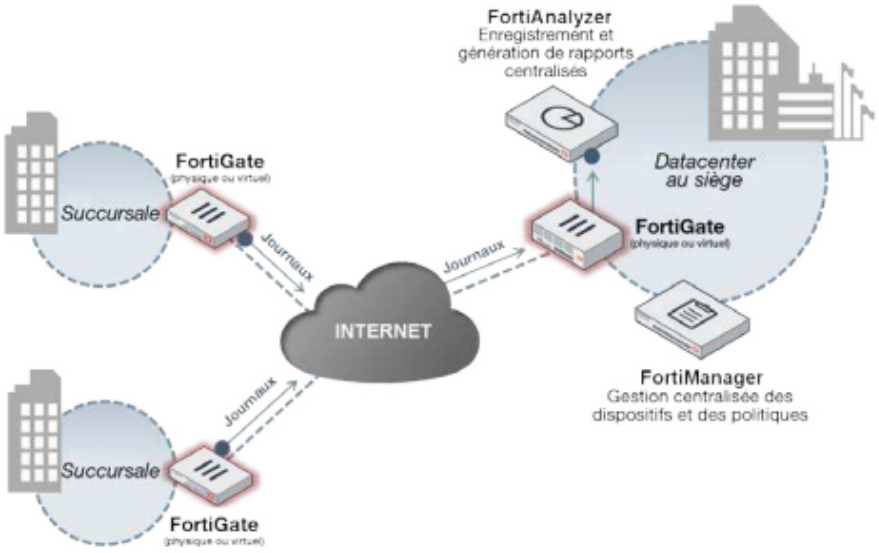


FIGURE 3.6 – Composants Fortinet SD-WAN.

- **FortiGate :** FortiGate est le CPE (Customer Premises Equipment) SD-WAN et le pare-feu de nouvelle génération qui est déployé sur les sites des succursales et dans le centre de données montrer pat la figure 3.7. Il fonctionne sur un système d'exploitation propriétaire FortiOS, le composant de base de la solution Secure SD-WAN. Il offre des fonctions de sécurité avancées, des capacités SD-WAN et une prise en charge des protocoles de routage. Les fonctionnalités de FortiGate comprennent l'inspection SSL, l'antivirus, l'anti-botnet, le contrôle des applications, l'optimisation du WAN via l'optimisation des protocoles, la priorité des paquets et l'appariement VPN. Pour les petits déploie-

ments, FortiGate agit comme un plan de gestion, de contrôle et de données.

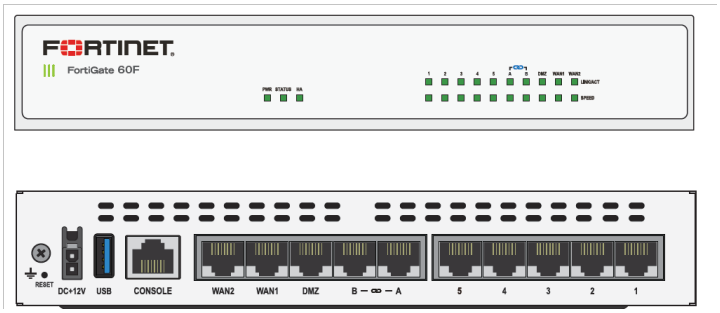


FIGURE 3.7 – Pare-feu FortiGate 60F.

- **FortiManager :** FortiManager assure la gestion et l'orchestration centralisées des appareils SD-WAN, qu'ils soient déployés sur site ou dans le cloud. Peu importe leur emplacement, il maintient une connectivité avec chaque appareil FortiGate. Il offre une vue d'ensemble du réseau global et surveille les accords de niveau de service (SLA) du réseau. FortiManager fournit des modèles pour la configuration des politiques de sécurité SD-WAN. Il prend également en charge les API et les connecteurs de la structure de sécurité, facilitant ainsi une intégration fluide dans le flux de travail de toute organisation.
- **FortiAnalyzer :** FortiAnalyzer est responsables de la fourniture de la solution SD-WAN dans son ensemble, permet d'afficher des données historiques et des journaux provenant des appareils de sécurité Fortinet, tels que les pare-feux FortiGate.permet de collecter, d'analyser et de générer des rapports sur les données de logs.

3.6.1.2 Principes de conception

Lors de la conception d'une solution SD-WAN, il est recommandé de suivre les cinq piliers clés suivants [45] :

1. **Infrastructure physique sous-jacente :** Identifier les liaisons WAN disponibles telles que les liens haut débit, MPLS, les connexions 4G/5G LTE, etc. Identifiez les caractéristiques de chaque liaison, y compris la bande passante, la qualité, la fiabilité (perte de paquets, latence et gigue) et le coût.

2. **Infrastructure physique :** Les superpositions VPN sont nécessaires lorsque le trafic doit transiter par plusieurs sites. Il s'agit généralement de tunnels IPsec de site à site qui interconnectent les succursales, les centres de données et le cloud, formant une topologie en étoile.
3. **Routage :** Le SD-WAN utilise le routage traditionnel pour créer la table de routage de base pour atteindre différentes destinations, mais utilise des règles SD-WAN pour diriger le trafic. Cela permet de baser la direction sur des critères tels que la destination, le service Internet, l'application, la balise d'itinéraire et la santé du lien.
4. **Sécurité :** Pour garantir la sécurité, il est essentiel de mettre en place des politiques de contrôle d'accès et d'appliquer les mesures de protection appropriées en utilisant les fonctionnalités de NGFW de FortiGate.
5. **SD-WAN**

   - membres SD-WAN : Les membres SD-WAN, également appelés points d'extrémité SD-WAN, sont les dispositifs ou les nœuds du réseau qui participent au déploiement et au fonctionnement du SD-WAN. Ces membres peuvent être des routeurs, des pare-feu ou d'autres appareils réseau qui sont configurés pour se connecter au réseau SD-WAN.

   - Zones SD-WAN : Les zones SD-WAN font référence à des groupes logiques d'interfaces membres SD-WAN regroupées ensemble en fonction de critères spécifiques. Les zones permettent d'organiser les interfaces membres du réseau SD-WAN et de configurer des stratégies de routage en utilisant ces zones comme interfaces source et destination.

   - SLA de performance : Également appelés bilans de santé, les SLA de performance sont utilisés pour surveiller la qualité des liens de l'interface membre et pour détecter les échecs de liaison. Lorsque le SLA tombe en dessous d'un seuil configuré, l'itinéraire peut être supprimé et le trafic peut être dirigé vers différents liens dans la règle SD-WAN.

   Les bilans de santé SLA utilisent le sondage actif ou passif :

   -Sondage actif : Le sondage actif implique l'envoi délibéré de paquets de test sur le réseau pour évaluer la performance. Les dispositifs ou les outils de surveillance envoient régulièrement des paquets de test à des intervalles préconfigurés vers des des-

tinations spécifiques. Ces paquets sont ensuite mesurés pour déterminer la qualité de la connexion, la latence, le débit, etc. -Sondage passif : Le sondage passif implique la surveillance et l'analyse du trafic réseau existant sans générer de trafic supplémentaire. Les outils de surveillance enregistrent les données sur le trafic réel traversant le réseau et analysent ces informations pour évaluer les performances.

-Règles SD-WAN : Également appelées services, les règles SD-WAN contrôlent la sélection du chemin. Le trafic spécifique peut être envoyé dynamiquement vers le meilleur lien, ou utiliser un itinéraire spécifique.

Les règles contrôlent la stratégie utilisée par FortiGate lors de la sélection de l'interface du trafic sortant, les SLA surveillés lors de la sélection de l'interface sortante et les critères de sélection du trafic qui adhère à la règle. Lorsqu'aucune règle SD-WAN ne correspond au trafic, la règle implicite s'applique.

3.6.2 Solution Cisco SD-WAN

Cisco SD-WAN offre une solution WAN définie par logiciel qui permet aux entreprises et aux organisations de connecter les utilisateurs à leurs applications en toute sécurité. Il fournit une superposition logicielle qui s'exécute sur le transport réseau standard, y compris MPLS, Internet, etc. pour fournir des applications et des services. Le réseau superposé étend le réseau de l'organisation aux environnements IaaS et multicloud, accélérant ainsi leur transition vers le cloud.

La solution SD-WAN la plus populaire et la plus utilisée est Viptela. Basé sur Cisco SD-WAN, elle offre aux clients une solution clé en main pour un réseau IP virtuel sécurisé, déployée automatiquement et offrant une connectivité any-to-any pour les services logiciels de nouvelle génération. Cette architecture se compose de quatre éléments fondamentaux le contrôleur vSmart, vManage, vEdge et l'orchestrateur vBond représenter par la figure 3.8 [46].

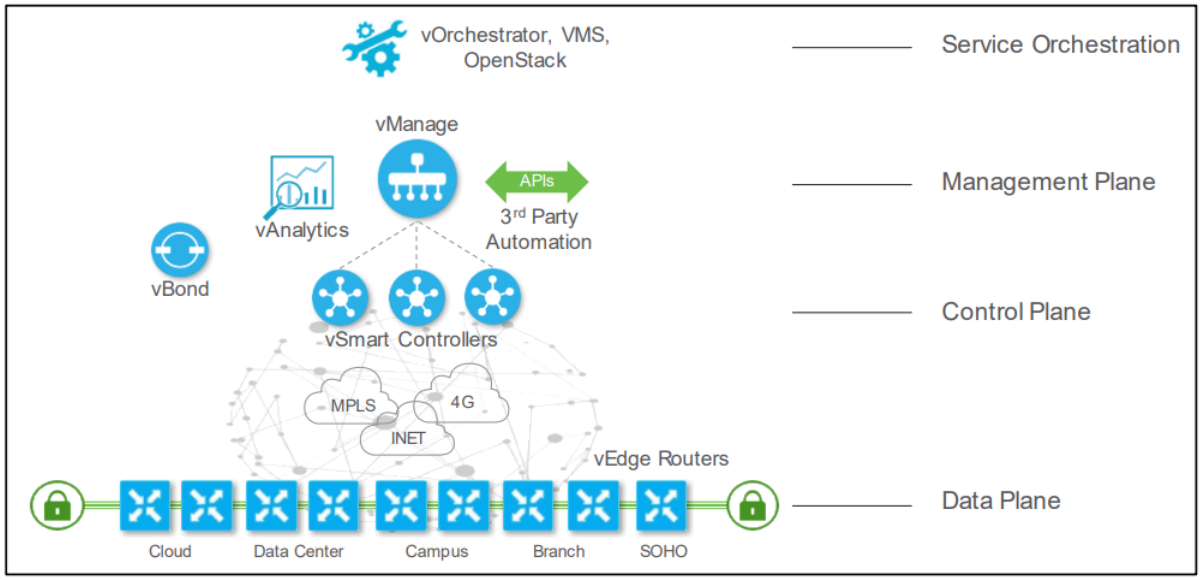


FIGURE 3.8 – Composants de la solution Cisco SD-WAN.

– **Cisco vManage :** vManage se situe au sommet de la hiérarchie architecturale SD-WAN, fournit une interface de contrôle et de gestion centralisée au réseau sous-jacent. Fournissant des tableaux de bord monolocataires ou multi-locataires selon les exigences des clients. Les administrateurs réseau peuvent exécuter diverses fonctions telles que la surveillance, le dépannage, la configuration et le déploiement à partir du tableau de bord vManage. Il fournit un riche ensemble d'API REST qui permettent une automatisation et une intégration personnalisées avec des systèmes ou des outils d'orchestration [47].

– **Cisco vSmart :** Le contrôleur Cisco vSmart estla plateforme de contrôleur centralisé dans l'architecture Cisco SD-WAN ainsi le cerveau de réseau. Il est en charge de l'application Politique de l'entreprise définie dans vManage.Overlay Management Protocol (OMP) est utilisé pour échanger des informations entre les succursales et les contrôleurs Cisco vSmart. Lorsqu'un appareil est mis en ligne dans une succursale, ses informations de routage sont d'abord transmises au contrôleur vSmart.Il utilise un protocole appelé OMPpour échanger des informations entre les succursales et les contrôleurs Cisco vSmart. Les contrôleurs vSmart sont gérés par vManage et sont des composants essentiels du réseau. Ils sont mis en œuvre selon une approche redondante, offrant à la fois une redondance et une évolutivité au niveau du plan de contrôle. Chaque

routeurvEdgedoit être en session avec un contrôleur vSmart en tout temps, bien que des mesures de redondance et de récupération soient intégrées à l'architecture[47].

Le protocole de gestion Overlay : Le protocole de gestion overlay est utilisé dans Cisco SD-WAN pour gérer le réseau overlay. OMP permet l'échange sécurisé d'informations de plan de contrôle entre les routeurs WAN Edge et les contrôleurs vSmart, comme illustré dans la Figure 3.9[4]. Ces informations de plan de contrôle incluent les préfixes de routage, les routes de prochain saut, les clés de chiffrement et les informations de politique. Par défaut, OMP permet une topologie en maillage complet entre les routeurs WAN Edge[46].

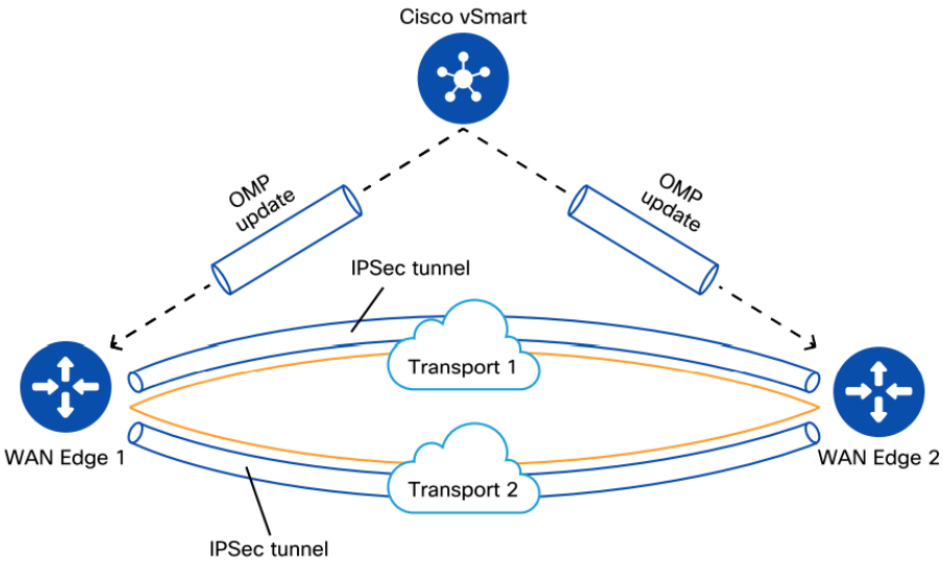


FIGURE 3.9 – Protocole de gestion Overlay

– **Cisco vBond :** Dans Le contrôleur Cisco vBond rend possible la configuration sans intervention (zero-touch provisioning). Il est également responsable de l'authentification des appareils, de la distribution des informations de contrôle et de gestion, ainsi que du traversée NAT. Le contrôleur vBond est chargé de l'intégration des nouveaux appareils installés sur les sites distants. Il partage les informations réseau avec d'autres appareils après avoir compris le réseau[47].

– **Cisco WAN Edge routeur :**

Les routeurs Cisco WAN Edge sont des équipements réseau spécifiquement conçus pour les réseaux étendus (WAN) et font partie de la gamme de produits Cisco SD-WAN (Software-Defined Wide Area Network). Ces routeurs offrent des fonctionnalités avancées pour la connectivité, la sécurité et la gestion des réseaux d'entreprise.
Voici quelques-uns des routeurs Cisco WAN Edge couramment utilisés [46] :

1. **Cisco ISR (Integrated Services Router) :** Les routeurs Cisco ISR sont des appareils polyvalents qui combinent des fonctionnalités de routage, de commutation, de sécurité et d'autres services intégrés. Ils offrent une connectivité WAN fiable et évolutive, avec une prise en charge de diverses interfaces et options de connectivité.
2. **Cisco ASR (Aggregation Services Router) :** Les routeurs Cisco ASR sont conçus pour les réseaux de grande envergure et les environnements à forte demande de bande passante. Ils offrent des performances élevées, une évolutivité avancée et une résilience du réseau pour les déploiements WAN exigeants.
3. **Cisco vEdge Router :** Le routeur vEdge fait partie de la solution Viptela SD-WAN acquise par Cisco. Il est conçu spécifiquement pour les déploiements SD-WAN et offre une connectivité sécurisée et optimisée sur des liens WAN hétérogènes, y compris Internet, MPLS et LTE.
4. **Cisco CSR (Cloud Services Router) :** Le routeur CSR est une version virtuelle du routeur Cisco WAN Edge qui peut être déployée dans des environnements de cloud public ou privé. Il offre une connectivité et une sécurité avancées pour les déploiements de réseau dans le cloud.

3.7 Conclusion

ce chapitre nous a donné l'opportunité d'approfondir notre compréhension de la solution SD-WAN et de ses caractéristiques, notamment en ce qui concerne l'amélioration et

l'optimisation des coûts d'infrastructure, tout en maintenant une qualité de service satisfaisante pour les entreprises.

Chapitre 4

Une solution SD-WAN pour l'entreprise NAFTAL-Bejaia

4.1 Introduction

Le présent chapitre traite de notre solution proposée pour le réseau de NAFTAL-Bejaia, ainsi que des améliorations envisagées pour optimiser le fonctionnement de celui-ci. Dans la section 4.2, nous reprenons l'architecture existante du réseau de l'entreprise et nous rappellerons donc les motivations conduisant à l'ambition de l'utilisation de la technologie SD-WAN pour améliorer les performances du réseau. La section 4.3 est consacrée à Pfsense, un parefeu qui permettra de multiplexer entre deux lignes et qui assurera une sorte de load balancing pour un usage optimal du réseau.

4.2 Structure actuelle du réseau de l'entreprise NAFTAL

La Figure 4.1 illustre la topologie du réseau de l'entreprisse NAFTAL.

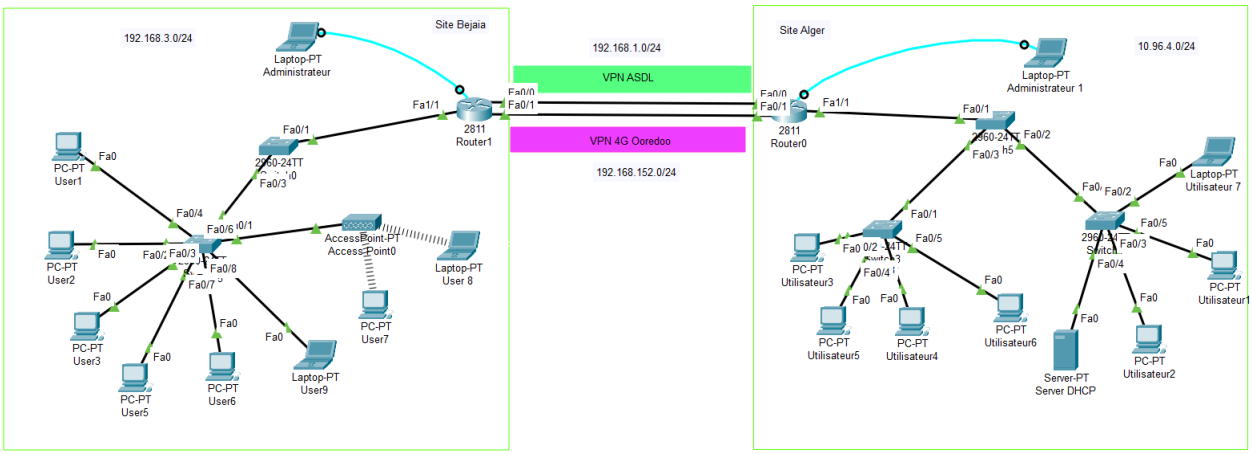


FIGURE 4.1 – Architecture de réseau NAFTAL.

Comme nous l'avions signalé dans la section 2.8, ce réseau souffre de plusieurs limitations. Ceci motive la proposition d'une nouvelle architecture basée sur les réseaux virtuels SD-WAN avec des performances élevées et qui sera donc plus adaptée pour répondre aux besoins de communications de l'entreprise ; c'est l'objet de la section qui suit.

4.3 Proposition d'une solution SD-WAN

Dans cette section, nous allons vous présenter l'architecture que nous avons souhaité mettre en place afin de résoudre le problème de réseau de l'entreprise NAFTAL. Nous détaillerons notre proposition dans les sous-sections qui suivent.

4.3.1 Architecture de la solution proposée

Dans notre proposition, nous avons mis l'accent sur la solution SD-WAN de Fortinet. Une illustration schématique est présentée dans la figure4.2.

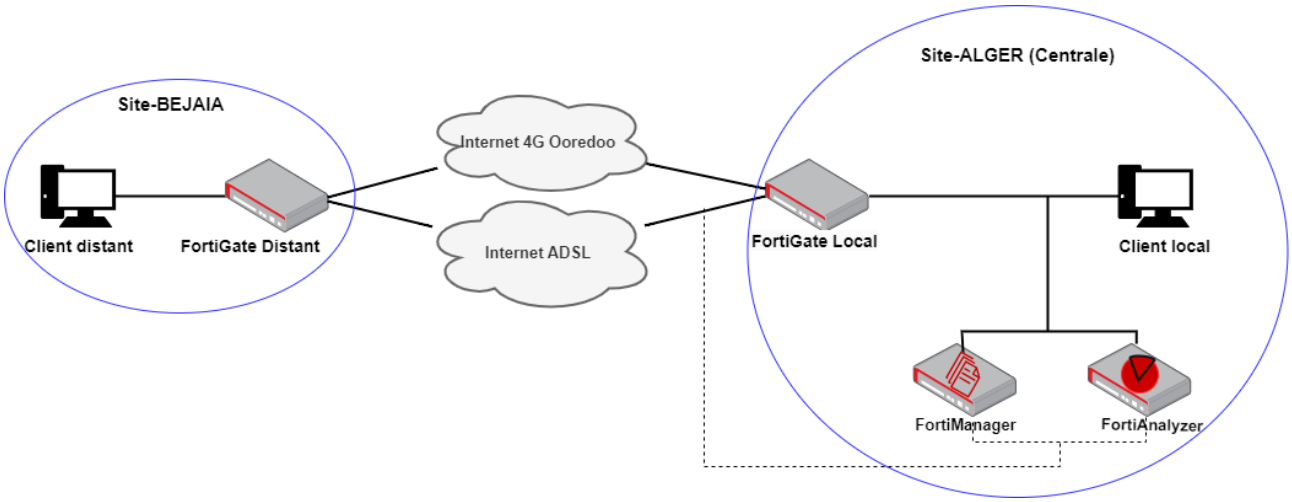


FIGURE 4.2 – Architecture de la solution proposée.

4.3.1.1 Fonctionnement

Cette architecture vise à simplifier et centraliser la gestion du réseau en permettant la connectivité fiable et sécurisée entre le site-BEJAIA et le site-ALGER. Les deux sites distants est équipé d'un routeur FortiGate SD-WAN qui est connecté à deux connexions Internet (ADSL et 4G-Ooredoo) pour assurer la disponibilité du réseau. Ce routeur utilise le protocole VPN (Virtual Private Network) pour établir des connexions optimales en utilisant efficacement la bande passante disponible. Dans le site-ALGER on a implémente un FortiManager et FortiAnalyzer.

FortiManager facilite la configuration et la gestion des politiques SD-WAN, des interfaces réseau, des règles de routage et des connexions VPN. Configurant les adresses IP, les masques de sous-réseau, les paramètres de liaison et les VLAN pour les appareils SD-WAN. De plus, ils peuvent utiliser OSPF ou BGP pour le routage dynamique, permettant ainsi une convergence automatique et une optimisation des chemins. Il facilite également la configuration des connexions VPN, incluant les types de tunnels, les clés de chiffrement, les paramètres d'authentification et les règles de correspondance.

FortiAnalyzer Il offre une visibilité approfondie sur les activités du réseau, la sécurité et les performances. Grâce à cette fonctionnalité, les administrateurs peuvent détecter les me-

naces, améliorer les performances du réseau et maintenir un environnement sécurisé dans le contexte du SD-WAN.

4.3.1.2 Avantages de la solution

Notre proposition d'architecture offre de nombreux avantages pour le réseau actuel de l'entreprise NAFTAL. Voici quelques-uns des principaux avantages :

- Avec l'inclusion du FortiManager, NAFTAL bénéficiera d'une gestion centralisée et simplifiée de tous les équipements réseau. Offrant une interface conviviale pour la configuration, la surveillance et la gestion des appareils Fortinet. Cette centralisation réduit la complexité de la gestion des équipements, facilite la maintenance et les mises à jour du réseau, et permet une administration plus efficace.
- L'utilisation de FortiAnalyzer permettra de collecter et d'analyser des statistiques détaillées sur le réseau. Cela offrira à NAFTAL la possibilité de surveiller les performances du réseau, d'identifier les éventuels points de congestion et d'identifier les problèmes de sécurité potentiels.
- La mise en place d'un mécanisme d'équilibrage de charge permettra de répartir intelligemment la charge du trafic réseau sur plusieurs liens, en réduisant les temps de latence, de perte de packet et d'augmenter la bande passante disponible
- Des fonctionnalités de sécurité avancées, telles que le chiffrement du trafic, les pare-feu intégrés et la détection des menaces, seront intégrées.

4.3.1.3 Le choix lié à l'implémentation de la solution Fortinet SD-WAN

Nous avons choisi d'utiliser l'émulateur EVE-NG pour mettre en place la solution SD-WAN Fortinet, plutôt que les simulateurs GNS3 et Packet Tracer car ils sont davantage adaptés aux scénarios de réseaux locaux et de réseaux locaux virtuels plutôt qu'aux déploiements SD-WAN complexes, selon nos recherches. Ces outils peuvent ne pas offrir une prise en charge complète des fonctionnalités spécifiques aux solutions SD-WAN. En revanche, EVE-NG se distingue par son interface utilisateur conviviale et sa capacité avancée de visualisa-

tion, ce qui facilite grandement la configuration, la gestion et la validation des déploiements SD-WAN.

Cependant, nous avons rencontré des difficultés liées au coût des images iOS des routeurs nécessaires pour les fonctionnalités SD-WAN, qui ne sont pas disponibles gratuitement. Les besoins en termes de mémoire (RAM) pour exécuter EVE-NG peuvent varier en fonction de la taille et de la complexité de la topologie du réseau SD-WAN que nous souhaitons simuler. Pour mener à bien cette simulation. Un PC doté au moins de 16 Go de RAM est requis. Le routeur FortiGate nécessite 2 Go de RAM, tandis que le FortiManager et le FortiAnalyzer nécessitent chacun 6 Go de RAM.

Cette figure4.3 montre la plateform de simulature EVE-NG.

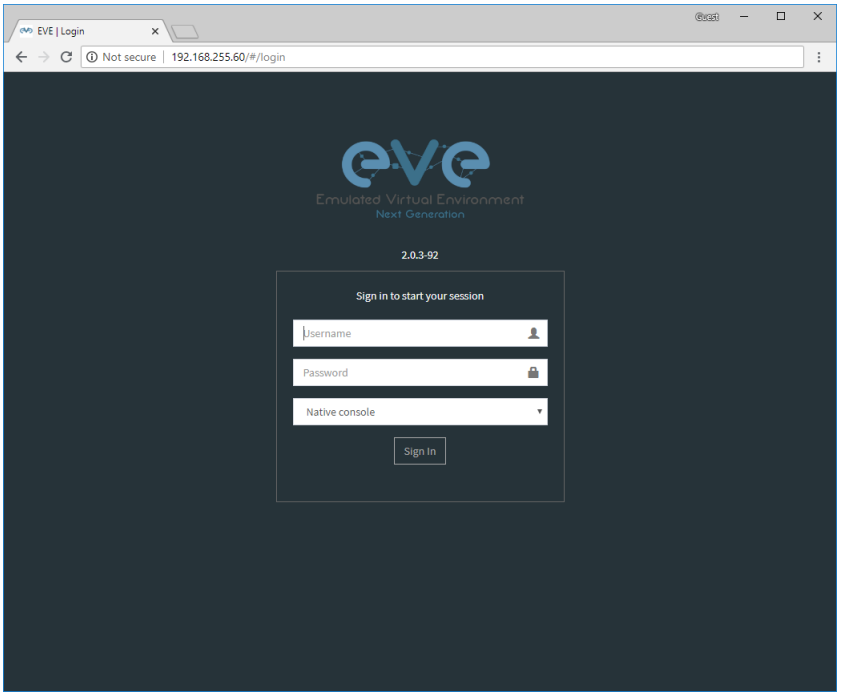


FIGURE 4.3 – Plate-forme EVE-NG

Bien que nous considérions l'utilisation d'EVE-NG, nous sommes conscients qu'il existe d'autres alternatives. Nous envisageons notamment l'utilisation d'un pare-feu PFsense comme solution de rechange. Ce dernier ne propose pas nativement une fonctionnalité SD-WAN, mais il peut être configuré pour prendre en charge SD-WAN en utilisant des techniques de routage avancées et des règles de trafic spécifiques.

4.4 Architecture à base de Pfsense

Le PFsense offre des fonctionnalités avancées en termes de pare-feu et de routage, ce qui en fait une option intéressante pour compléter notre processus de validation. La figure 4.4 illustre la solution proposée.

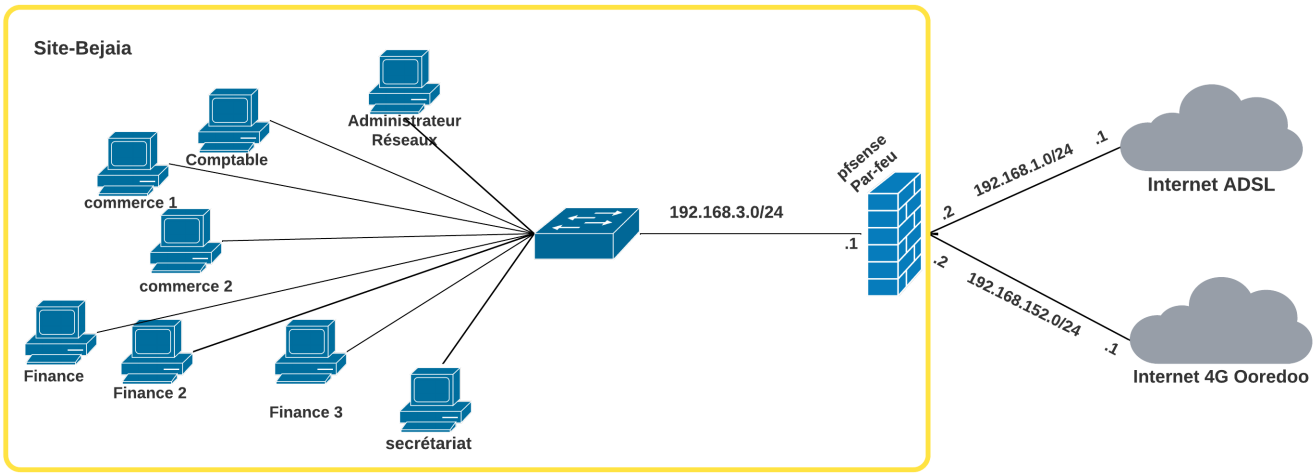


FIGURE 4.4 – Schéma explicatif de la solution proposé.

Dans notre travail nous mettons en place la solution SD-WAN basée sur le pare-feu pfsense. Les taches essentieles à réaliser se présentent comme suit :

— Activation des cartes réseaux.

— Activation des protocoles de sécurité pfsense.

— Activation serveur DNS.

— Activation serveur DHCP.

— Configuration Multi-WAN.

Les adresses réseaux utilisées sont représentées dans le tableau 4.1

Nom	Adress ip	masque	passerelle
WAN-ADSL	192.168.1.2	255.255.255.0	192.168.1.1
LAN	192.168.3.1	255.255.255.0	/
WAN-4G-Ooredoo	192.168.152.2	255.255.255.0	192.168.152.1

TABLE 4.1 – Plan d'adressage IPv4

4.4.1 Présentation des outils utilisés

4.4.1.1 VMware Workstation

VMware Workstation est un logiciel de virtualisation puissant qui permet de créer et de gérer des machines virtuelles sur un ordinateur hôte.

FIGURE 4.5 – Logo Vmware

Installation de Vmware Nous donnons ci-dessous les étapes détaillées d'installation de VMware Workstation. Pour télécharger et installer le produit VMware, nous pouvons nous référer au site officiel. La version utilisée est la dernière disponible, soit la version 17 de VMware Workstation.

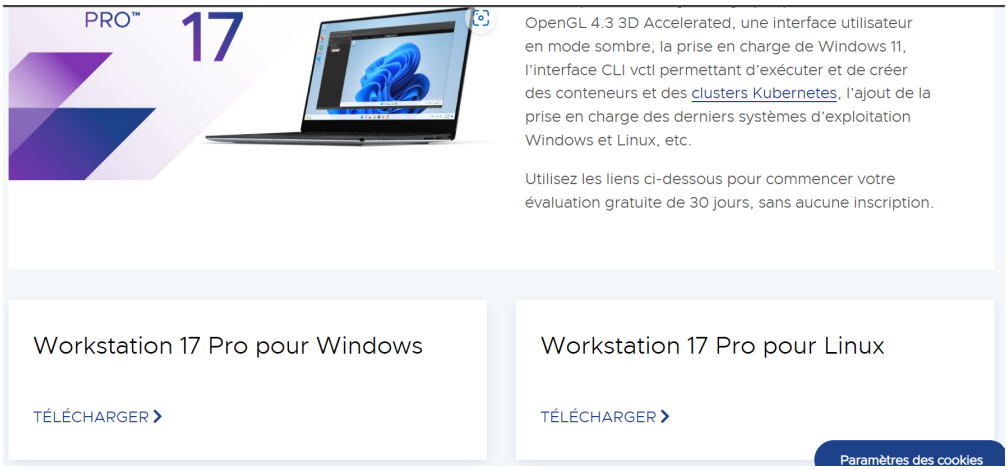


FIGURE 4.6 – Étape 1.

Une fois le téléchargement terminé, l'installation se fait en exécutant le programme d'installation. Une fenêtre contextuelle apparaîtra.

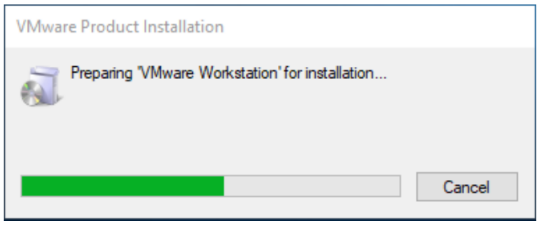


FIGURE 4.7 – Étape 2.

Après l'initialisation terminée, l'installation est prête à être éffectuée.

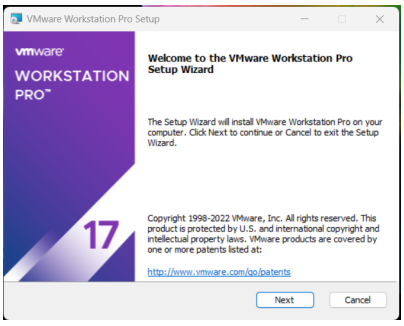


FIGURE 4.8 – Étape 3.

À cette étape, VMware Workstation est prêt à s'installer.

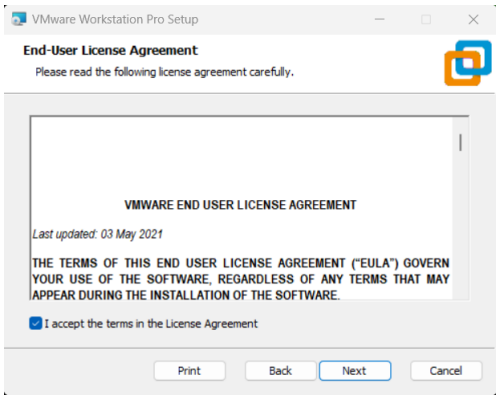


FIGURE 4.9 – Étape 4.

Nous pouvons procéder en confirmant et continuant l'installation.

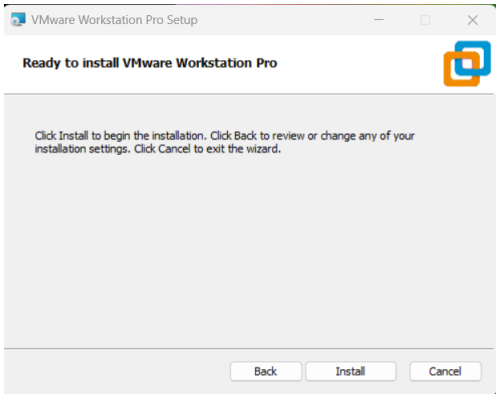


FIGURE 4.10 – Étape 5.

Une fois l'installation terminée, le produit est prêt à être utilisé.

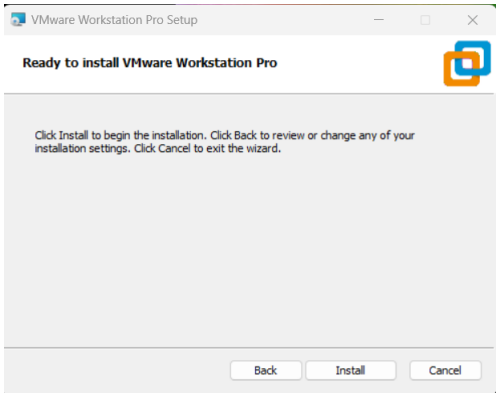


FIGURE 4.11 – Étape 6.

Enfin, cela ouvrira une fenêtre de VMware Workstation Pro.

4.4.1.2 Installation du pare-feu pfsense

Le pare-feu pfsense est un logiciel open-source basé sur FreeBSD qui combine les fonctionnalités d'un routeur et d'un pare-feu. Il propose des capacités avancées en matière de routage et de sécurité réseau, offrant ainsi une alternative libre aux outils de services utilisés généralement sur les routeurs propriétaires professionnels.

FIGURE 4.12 – Logo pfsense

Nous effectuons l'installation de pfSense sur une machine virtuelle en utilisant VMware Workstation. La procédure d'installation reste semblable à celle d'une machine physique.

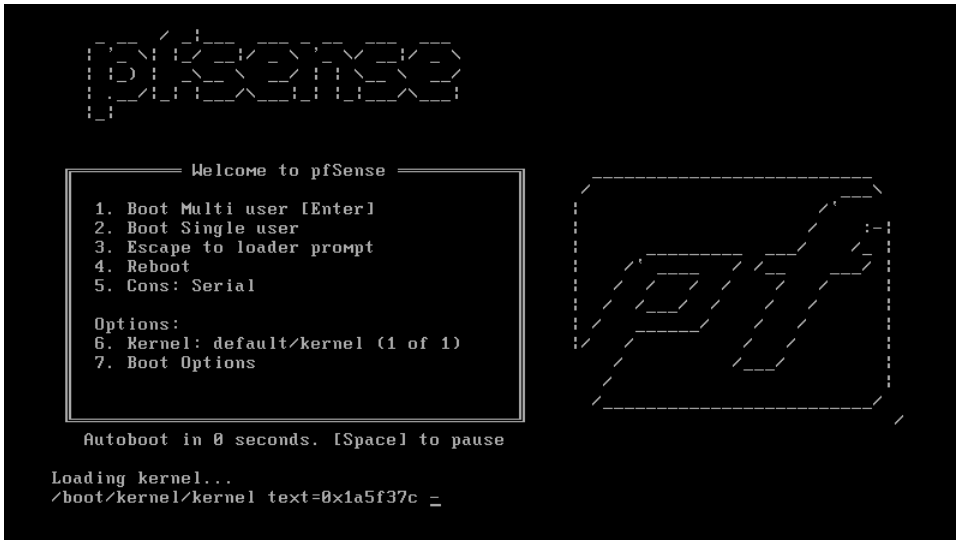


FIGURE 4.13 – Bienvenue pfSense

Un contrat de licence doit être accepté pour pouvoir lancer le processus d'installation.

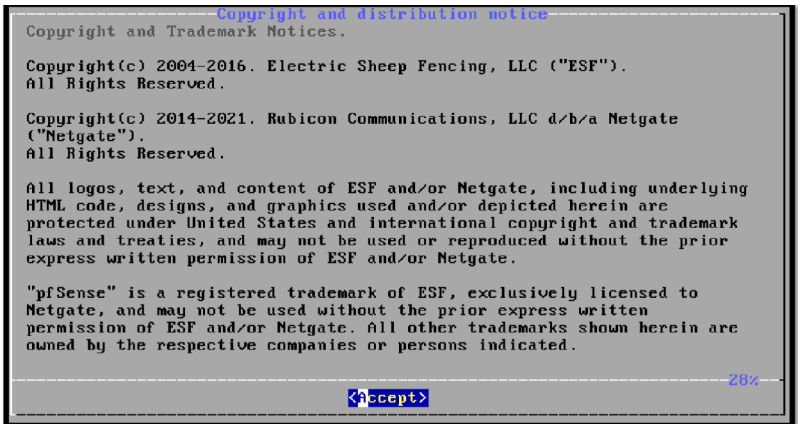


FIGURE 4.14 – Contrat licence de pfSense

Tout d'abord, on sélectionne l'option d'installation sur l'écran d'accueil

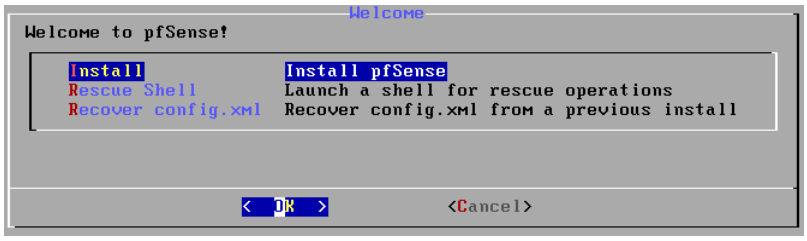


FIGURE 4.15 – Installation pfSense

Ensuite, le choix de l'option Auto (UFS) est nécessaire pour effectuer le partitionnement automatique du disque.

FIGURE 4.16 – Partitionnement de disque

Le système lancera l'installation automatique du pfSense, en choisissant l'option Non de la configuration manuelle.

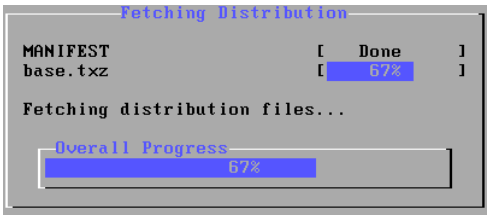


FIGURE 4.17 – Récupération des fichiers de distribution

A la fin une fenêtre de redémarrage apparaîtra afin de lancer le firewall.

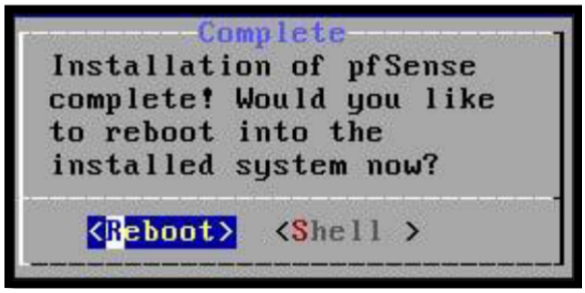


FIGURE 4.18 – Installation complète

4.4.1.3 Configuration pfsense

La configuration nécessite les étapes suivantes :

1. **Activation des cartes réseaux**

   Pfsense est capable de détecter automatiquement les adresses réseau disponibles. Ainsi, nous allons attribuer une adresse IP à chaque interface. Pour cela, nous sélectionnons l'option "2" dans le menu principal de pfsense afin de modifier les interfaces WAN, LAN et opt1. Ensuite, nous choisissons le numéro correspondant à chaque interface pour modifier son adresse.

   Dans l'ordre de simplifier la manipulation, il est important de noter que chaque interface passe par les mêmes étapes. Une démonstration de configuration pour une seule interface est faite afin d'éviter des répétitions inutiles.

FIGURE 4.19 – Choix de l'interface.

Une fois que toutes les configurations des interfaces sont terminées, on obtiendra le résultat de la figure 4.20 :

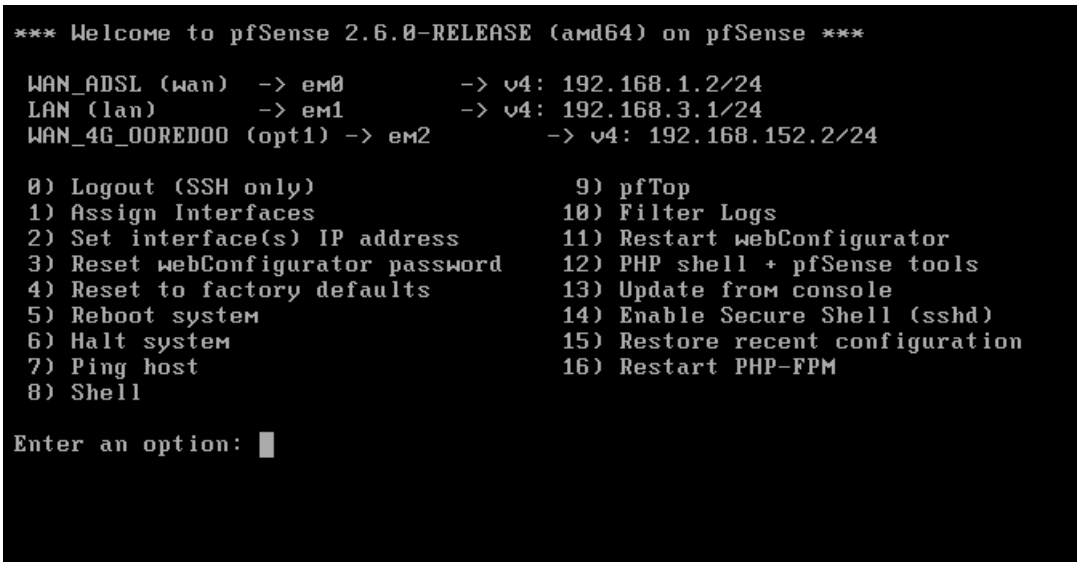


FIGURE 4.20 – Affichage des interfaces.

Pour accéder à l'interface web de Pfsense, on utilise l'adresse IP LAN et les informations d'identification suivantes : "Nom d'utilisateur : admin", "Mot de passe : pfsense".

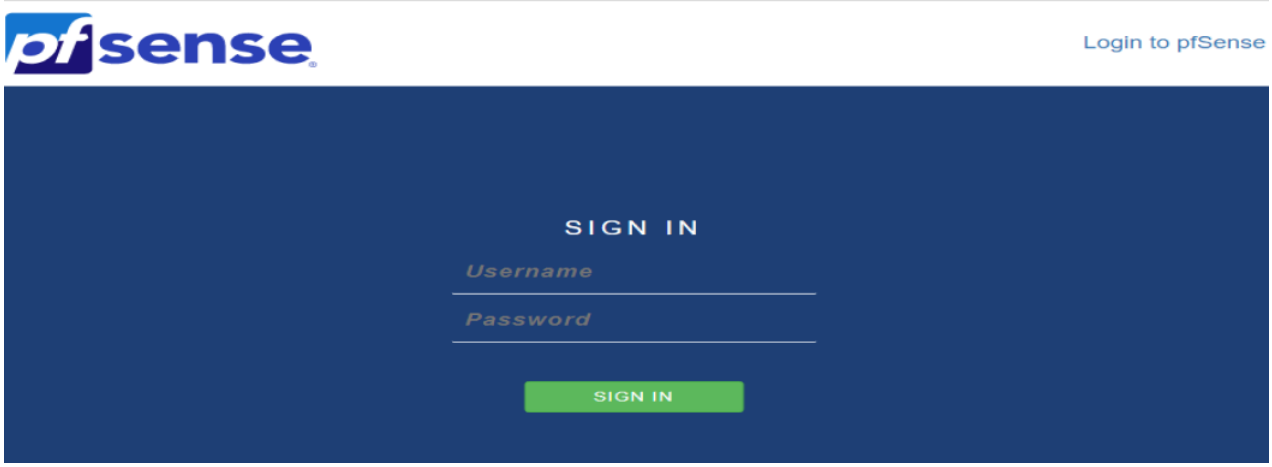


FIGURE 4.21 – Page d'authentification.

La page d'accueil pfsense s'affiche.

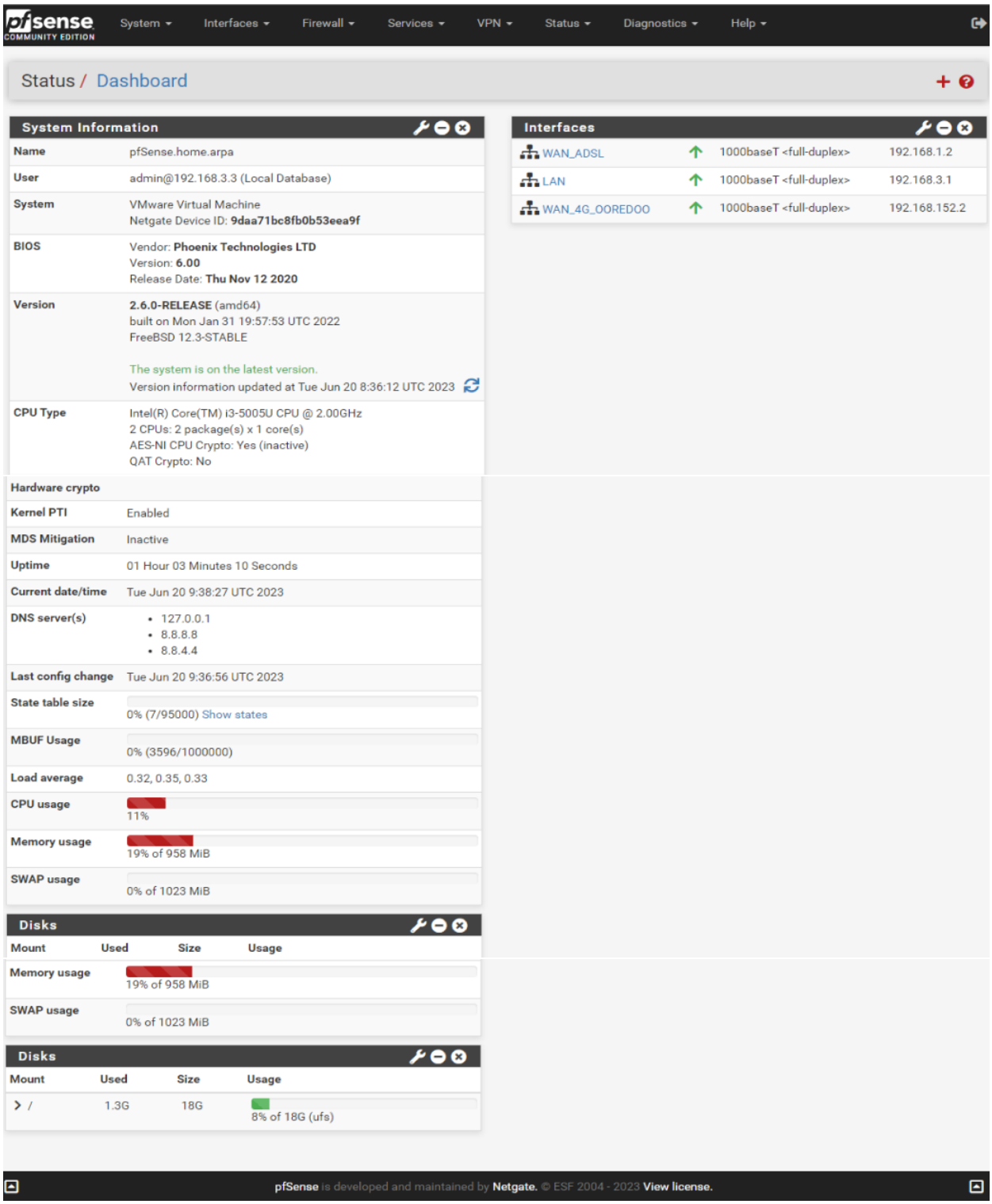


FIGURE 4.22 – Page d'accueil.

2. Activation du protocole de sécurité pfsense

Pour sécuriser les connexions entre l'ordinateur et pfSense, il est nécessaire d'activer le

protocole HTTPS afin de chiffrer les données échangées. En outre, il est recommandé de modifier le numéro de port par défaut utilisé pour accéder à l'interface web de pfSense.

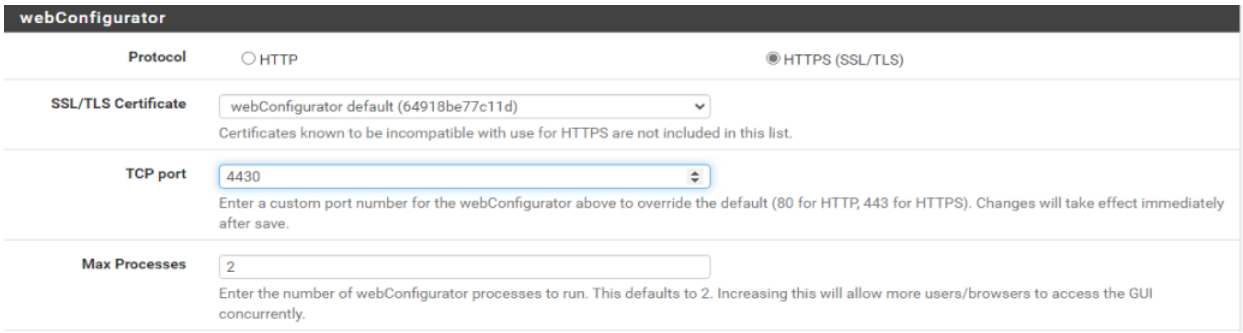


FIGURE 4.23 – Activation du protocole de sécurité.

3. **Activation du serveur DNS**

Pour assurer la continuité des requêtes DNS (Domain Name System) en cas de perte d'un des liens Internet, il est recommandé de définir au moins un serveur DNS par passerelle WAN.

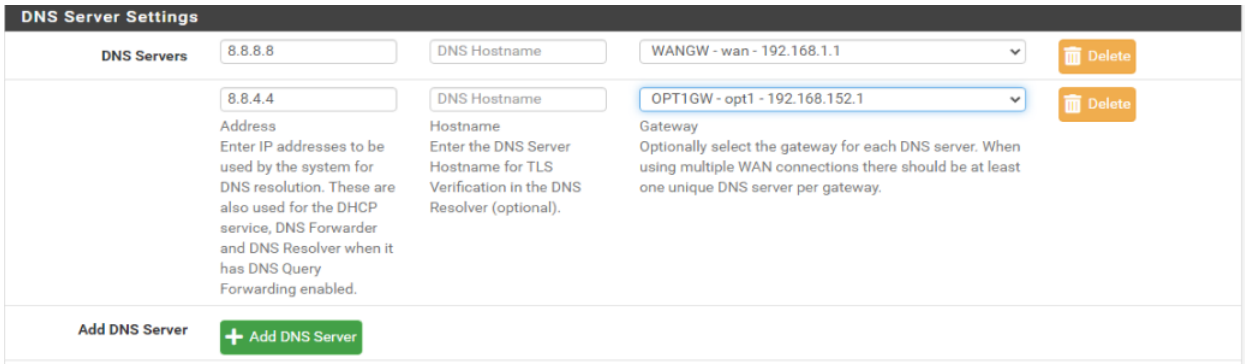


FIGURE 4.24 – Activation du serveur DNS.

4. **Activation du serveur DHCP**

Configuration de serveur DHCP (Dynamic Host Configuration Protocol) qui est responsable de la distribution des adresses IP aux ordinateurs de réseau LAN. La création s'effectue depuis Services > DHCP Server.

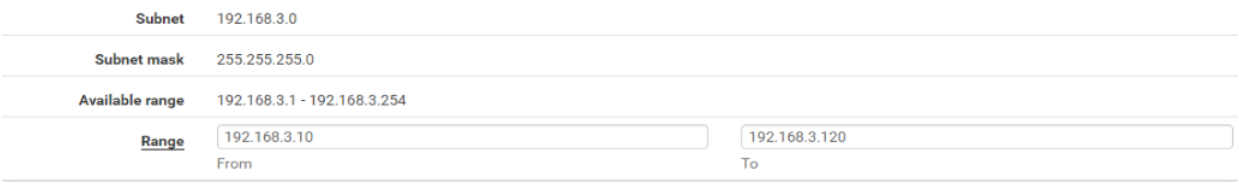


FIGURE 4.25 – Activation du protocole DHCP.

5. **Configuration Multi-WAN**

Nous allons créer un groupe de passerelles comprenant la passerelle de l'interface WANGW (WAN-ADSL) et la passerelle de l'interface OPT1GW (WAN-4G-Ooredoo).

Nous souhaitons faire de la répartition de charge, nous choisissons donc "Tier 1" pour le WANGW et pour le OPT1GW "Tier 2". La création s'effectue depuis System > Routing > Gateways.

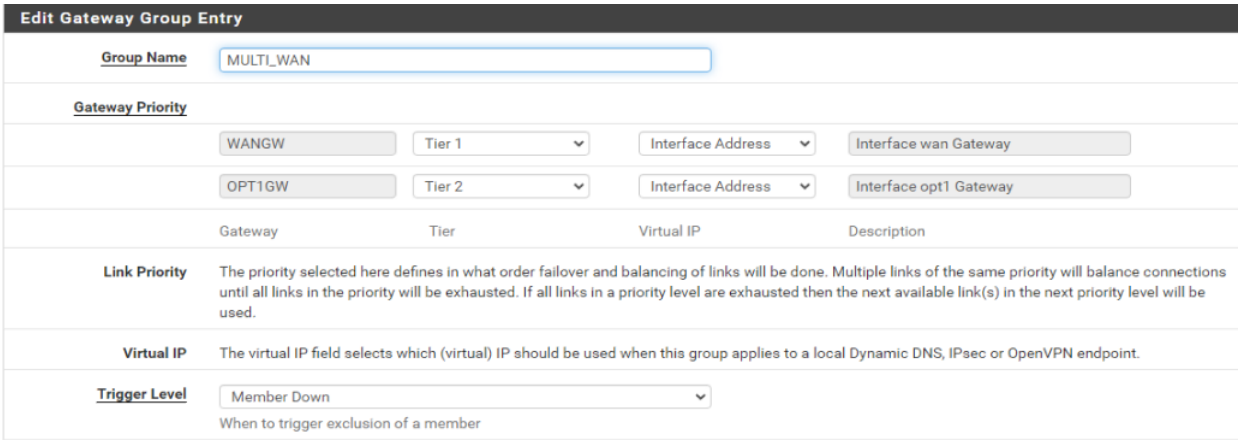


FIGURE 4.26 – Groupes de passerelles.

Voilà, les deux connexions internet sont fonctionnelles, elles sont présentées sur la figure 4.27.

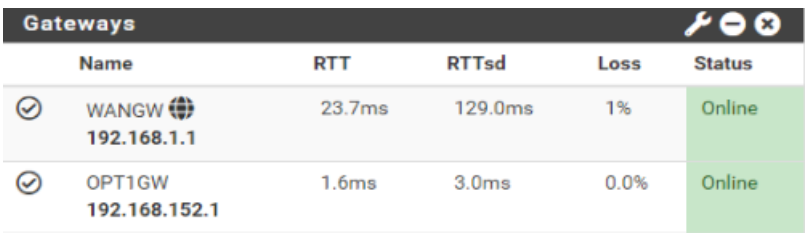


FIGURE 4.27 – Multi-WAN

La mise en service des deux connexions WAN consiste à configurer le firewall pour lui indiquer par quel groupe de passerelles faire passer le trafic. Le processus se fait comme suit : Firwall > Rules > Edit.

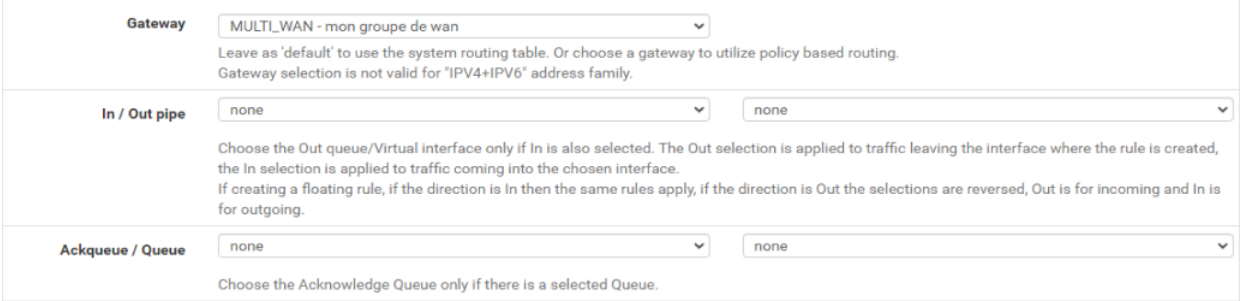


FIGURE 4.28 – mettre en service Multi-WAN

6. **Vérification de connectivité** Après avoir envoyé un ping (Diagnostics > ping) de LAN aux connexions WAN-ADSL (192.168.1.1), la réussite a été confirmée.

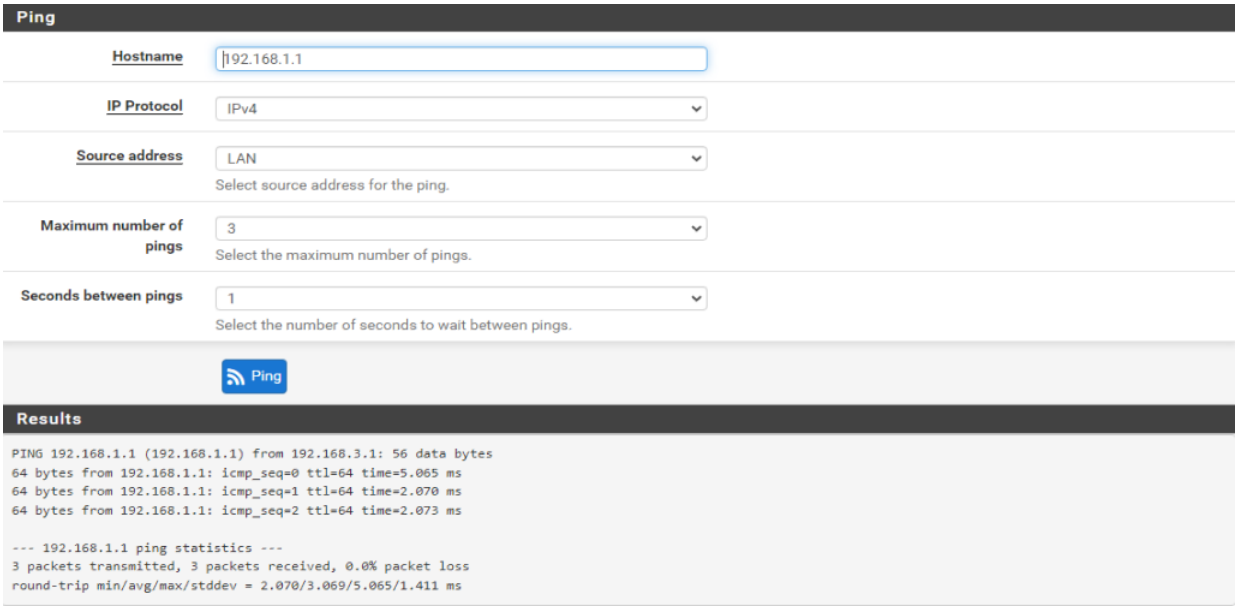


FIGURE 4.29 – Test de la connectivité.

4.5 Conclusion

Dans ce chapitre, nous avons proposé une solution fortinet SD-WAN et nous avons montré son intérêt pour améliorer le réseau existant à NAFTAL. Cependant, dû à la non-

disponibilité de EVE-NG en version professionnelle qui aurait permis de valider la solution proposée, nous avons adopté plutôt une solution à base de pfsense qui est un pare-feu doté de fonctionnalités intéressantes similaires à celles offertes par les routeurs SD-WAN. La mise en place de cette dernière et les configurations nécessaires ont été enfin décrites.

Conclusion

Le réseau informatique est désormais essentiel dans chaque entreprise pour assurer la continuité de ses activités. La mise en oeuvre de SD-WAN dans les entreprises repose sur la virtualisation et l'optimisation du réseau étendu (WAN) en utilisant des logiciels et des techniques avancées.

Dans la première partie, nous avons examiné les principales technologies des réseaux. Nous avons abordé les réseaux traditionnels utilisés dans les entreprises, tels que le MPLS, SDN et SD-WAN. Bien que le MPLS soit une technologie fiable et éprouvée, le SDN et le SD-WAN offrent de nouvelles possibilités en termes de flexibilité et de gestion des réseaux. Ces approches plus récentes sont de plus en plus adoptées par les entreprises qui cherchent à moderniser leurs infrastructures réseaux.

Dans la deuxième partie, nous avons abordé les limitations du réseau de NAFTAL et examiné son architecture actuelle ainsi que les problématiques auxquelles elle était confrontée. Notre objectif principal était d'explorer et de mettre en place une solution SD-WAN adaptée à NAFTAL-BEJAIA.

Dans la troisième partie, nous avons présenté la solution SD-WAN comme moyen de remédier aux limitations du réseau de l'entreprise Naftal-Bejaia. Cette partie nous a donné l'occasion d'approfondir notre compréhension du paradigme SD-WAN et de ses caractéristiques, notamment en ce qui concerne l'amélioration et l'optimisation des coûts d'infrastructure, tout en maintenant une qualité de service satisfaisante pour l'entreprise. Il convient également de mentionner d'autres fournisseurs de solutions SD-WAN, tels que Fortinet et Cisco, qui offrent des solutions SD-WAN robustes et éprouvées sur le marché.

Dans la dernière partie, nous avons abordé notre solution proposée pour le réseau de NAFTAL-Bejaia, ainsi que les améliorations envisagées pour optimiser son fonctionnement. Dans notre proposition, nous suggérons de remplacer les routeurs existants par des appareils pf-Sense qui intègrent des fonctionnalités SD-WAN. pfSense est une solution open-source de pare-feu et de routage qui offre des capacités avancées de gestion du réseau, y compris la fonctionnalité SD-WAN.

Bibliographie

[1] R.R. Kasturi. “Trends in SD-WAN and SDN".CSI Transactions on ICT, 2020, vol.8, p. 21-27.

[2] J. Dordoigne. "Réseaux informatiques Notions fondamentales(Protocoles, Architectures, Réseaux sans fil, Virtualisation,Sécurité,IPv6)",ENI, 7ème édition, 2011.

[3] Networklessons. "Introduction au réseau local extensible virtuel (VXLAN)", https://networklessons.com/cisco/ccnp-encor-350-401/introduction-to-virtual-extensible-lan-vxlan.

[4] G. MOSER. "Performance Analysis of an SD-WAN Infrastructure Implemented Using Cisco System Technologies", Thése computer science and technologie, STOCKHOLM, SWEDEN, 2021.

[5] Ferguson, P. and G. Huston." What is a VPN?". 1998.

[6] S. Kent (BBN Corp) and R. Atkinson (@Home. RFC 2401)."Architecture de sécurité pour IP". RFC 2401, 1998.

[7] C. Servin. "Réseau et Télécom". DUNOD. 4ème edition, 2013.

[8] Stéphane Lohier, Dominique Présent. "Transmissions et réseaux",DUNOD, 5eme édition, 2010.

[9] O. Al-Saadeh, G. Wikstrom, J. Sachs, I. Thibault, and D. Lister,"End to-end latency and reliability performance of 5g",in london, 2018 IEEE Global Communications Conference (GLOBECOM), 2018.

[10] A. Narayanan, E. Ramadan, J. Carpenter, Q. Liu, Y. Liu, F. Qian,and Z.-L. Zhang. "A first look at commercial 5g performance on smartphones", NewYork, Proceedings of The Web Conference, 2020.

[11] P. Mell and T. Grance. "Draft nist working definition of cloud computing-v15". Aug 2009, vol.21.

[12] T. Dillon, C. Wu et E. Chang. " Cloud Computing : Issues and Challenges", 2010 24th IEEE International Conference on Advanced Information Networking and Applications , Perth, WA, Australie, 2010, p. 27-33.

[13] B. Yi, X. Wang, K. Li, S. k. Das and M. Huang. "A comprehensive survey of Network Function Virtualization".Computer Networks, 2018, Vol.133.

[14] D. Kreutz, F. M. V. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig. "Software-Defined Networking : A Comprehensive Survey". Proceedings of the IEEE, 2015, Vol.103.

[15] ETSI GS NFV-MAN 001." Network Functions Virtualisation (NFV)", Architectural Framework, 2014.

[16] C. Craven. "NFV 101 : Networking Foundations Guide". sdxcentral, 2019.

[17] Q. Duan, M. Toy. "Virtualize Software-Defined Networks and Services". Artech House Publishers, December 31, 2016.

[18] M. MEHDID , M. MOUAOUED . "Conception d'une plateforme Web de dimmensionnement d'un vEPC dédiée pour la 5G".Mémoir de fin d'étude. Université Aboubakr Belkaid-Tlemcen, 2022.

[19] ETSI. "NFV : Infrastructure overview". 2014.

[20] ONF, "Software-Defined Networking (SDN)Definition", https://www.opennetworking.org/sdn-resources/sdn-definition, 2016.

[21] F. BENAMRANE , "Etude des Performances des Architectures du Plan de Contrôle des Réseaux 'Software-Defined Networks".Thése doctorat. Université Mohammed V Faculté des sciences Rabat , 2017.

[22] I.Choukri, M. Ouzzif,Kh.Bouragba." Software Defined Networking (SDN) :Etat de L'art". Ecole Supérieure de Technologie de Casablanca.CASABLANCA, Maroc, Jun2019.

[23] R. T. Fielding. "In Information and Computer Science".University of California, Irvine, 2000.

[24] FOUNDATION, OPEN NETWORKING. "OpenFlow Switch Specification". March 26, 2015.

[25] Foundation, Open Networking. "SDN Technical Specifications" https://opennetworking.org/software-definedstandards/specifications/.

[26] F. Benamrane, M. Ben mamoun, et R. Benaini,"Performances of OpenFlow-Based Software-Defined Networks : An overview". juin 2015, Vol 10.

[27] NAFTAL. Présentation Naftal, https://www.energy.gov.dz/

[28] Y. Sudhir. "SD-WAN service analysis, solution, and its applications". University of ALBERTA,2021.

[29] VERSA NETWORKS."Le SD-WAN optimise les solutions WAN hybrides", 2022.

[30] R. Margaret. "Software-Defined Wide Area Network". Techopedia, 2018.

[31] proofpoint ,"Qu'est-ce qu'un SD-WAN et comment ça fonctionne?" https://www.proofpoint.com/fr/threat-reference/sd-wan.

[32] S.Uppal, S. Woo, and P. Dan . "Software-Defined WAN For Dummies". Hoboken, New Jersey : 2nd VMware Special Edition, 2018.

[33] S. Rajagopalan. "An overview of sd-wan load balancing for wan connections", IEEE, 2020.

[34] D. Radcliffe, E. Furey, and J. Blue. "An sd-wan solution assuring business quality voip communication for home based employees", International Conference on Smart Applications,Communications and Networking (SmartNets), 2019.

[35] Cisco. "Cisco sd-wan",https://www.cisco.com/c/en-ca/solutions/enterprise-networks/sd-wan/index.html.

[36] E. Mota, P. Fonseca. "A survey on fault management in software defined networks", IEEE Communications Surveys Tutorials, 2017, Vols 19.

[37] F. Botelho, A. Bessani, F. M. V. Ramos, and P. Ferreira," On the design of practical fault-tolerant sdn controllers".Third European Workshop on Software Defined Networks, 2014.

[38] CloudyConfigs. Introduction au protocole de redondance de routeur virtuel. 26 NOVEMBRE 2018.

[39] M. Wood. "SD-WAN Manifesto : Eight Critical Characteristics for Building an SD-WAN". Sdxcentral, 7 October 2016.

[40] C. Craven. "What is SD-WAN Security? Definition". sdxcentral, 07 January 2020.

[41] S.Ummi,M.Fathul, FIADE, Andrew, IMAN, et al. "Performance evaluation of routing protocol RIPv2, OSPF, EIGRP with BGP". In : 2017 International Conference on Innovative and Creative Information Technology (ICITech). IEEE, 2017. p. 1-7.

[42] Gartner. Magic Quadrant for SD-WAN.https://https://global.fortinet.com/lp-en-2022-gartner-cc-sdwan?

[43] Demo, Tech Field Day,"Fortinet SD-WAN Architecture" , February 2019.

[44] " Fortinet,"Fortinet Secure SD-WAN Reference Architecture", 2019. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinet_secure_sdwan.pdf

[45] Fortinet. "FortiOS 7.4.0 Administration Guide". 2023. https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide

[46] Cisco, "Cisco SD-WAN", https://blogs.cisco.com/partner/cisco-sd-wan-awarded-crn-2019-product-of-the-year,2019.

[47] Cisco. "Cisco SD-WAN Migration Guide". July 23, 2019. https://www.cisco.com/c/dam/en/us/td/docs/routers/sdwan/migration-guide/cisco-sd-wan-migration-guide.pdf

Résumé

Le Réseau Étendu Défini par Logiciel, ou Software Defined Wide Area Networking (SD-WAN), est une solution moderne pour la gestion des réseaux étendus qui facilite leur administration et permet l'intégration avec le cloud. SD-WAN exploite l'optimisation logicielle pour prendre le contrôle du fonctionnement d'un réseau, au lieu de s'appuyer sur une infrastructure matérielle traditionnelle. L'adoption de cette technologie a pour avantages la simplification de la gestion du réseau, la flexibilité, l'optimisation du trafic et une sécurité renforcée.

Dans ce mémoire de fin d'études, nous étudions les principes fondamentaux des réseaux SD-WAN, puis nous proposons une démarche pour la conception et l'implémentation d'une nouvelle architecture adaptée au réseau de l'entreprise NAFTAL de Bejaia. Notre démarche consiste d'abord à analyser le réseau existant au sein de l'entreprise, ensuite à concevoir une nouvelle architecture basée sur la technologie SD-WAN qui est flexible, évolutive et capable de garantir de meilleurs services à l'entreprise. La faisabilité de notre solution a été montrée et appuyée par les résultats de simulation qui sont aussi exposés dans ce mémoire. L'implémentation de l'architecture proposée a été faite avec des outils open source dont le pfsense.

Mots clés : Réseaux; SD-WAN; cloud; Pfsense.

Abstract

Software Defined Wide Area Networking (SD-WAN) is a modern solution for managing wide area networks that facilitates their administration and enables integration with the cloud. SD-WAN leverages software-based optimization to take control of network operation, instead of relying on traditional hardware infrastructure. Adopting this technology has the advantages of simplified network management, flexibility, traffic optimization and enhanced security.

In this dissertation, we study the fundamental principles of SD-WAN networks, and then we propose an approach for the design and implementation of a new architecture adapted to the network of the NAFTAL Company in the city of Bejaia. Our approach is first to analyze the existing network within the company, then to design a new architecture based on SD-WAN technology that is flexible, scalable and able to guarantee better services to the company. The feasibility of our solution has been shown and supported by the simulation results which are also exposed in this report. The implementation of the proposed architecture was done using open source tools including pfsense.

Keywords: Networks; SD-WAN; cloud; Pfsense.