République Algérienne Démocratique Et Populaire
Ministère de L'enseignement Supérieur et de la Recherche Scientifique
Université A/Mira de Bejaia
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle
En vue de l'obtention du diplôme de Master en Informatique

Option **:**

Administration et sécurité des réseaux

Thème

Etude et mise en place d'une solution SD-WAN sur un tunnel VPN Site a Site CAS Bejaia Mediterranean Terminal (BMT)

Réalisé par :

MAOUCHE YOUSRA & MANAA AICHA

Membre du jury :

Présidente : Mme Sabri Salima	M.C. B	U.A/Mira Bejaia
Encadrante : Mme Houha Amel	M.A. A	U. A/Mira Bejaia
Examinateur : Mr Ouzeganne Redouane	M.A. A	U. A/Mira Bejaia
Co-encadrant : Mr Benali Lyes		Entreprise BMT

Promotion 2023/2024

Remerciement

Nous remercions le bon Dieu, tout puissant, pour avoir accordé la force, le courage et la santé nécessaires pour surmonter les épreuves, ainsi que l'audace pour dépasser toutes les difficultés.

Nous souhaitons exprimer notre profonde reconnaissance et notre gratitude envers Madame HOUHA AMEL, pour sa disponibilité, ses conseils avisés, sa patience et la confiance qu'elle nous a accordée, ainsi que pour son soutien précieux. Son optimisme constant nous a permis d'avancer avec sérénité.

Nous remercions l'entreprise "BMT" pour l'opportunité de stage offerte. Pour avoir accepté notre stage, nous offrant ainsi une opportunité précieuse de découvrir le monde professionnel.

Nos remerciements chaleureux vont aux membres du jury pour avoir accepté d'évaluer notre projet fin d'étude et pour avoir consacré une partie de leur temps pour examiner et juger notre travail.

Nous tenons également à exprimer notre gratitude envers tous les enseignants et membres du département informatique de l'université A/Mira, qui nous ont partagé leur savoir et nous ont apporté leur soutien tout au long de notre parcours académique.

Dédicace

Je dédie ce travail

À mon cher père Abdallah et ma chère maman Malia

Dont le soutien indéfectible a rendu tout cela possible. Aucune dédicace ne saurait suffire à exprimer l'amour, l'estime, le dévouement et le respect que j'ai pour vous. Que Dieu vous garde et vous accorde la santé et longue vie

A mon grand frère Hicham

Je suis profondément reconnaissant de ta présence dans ma vie. Tu as toujours été là pour moi, Je te souhaite une vie remplie de joie, de succès et d'amour. Je me considère chanceux d'avoir un frère aussi exceptionnel que toi.

À mes chères sœurs,

Rima, Bouthaina et Imane

Je vous adresse mes vœux pour un avenir radieux, empli de bonheur et de succès. Que Dieu, le Tout-Puissant, veille sur vous et vous accorde santé et longévité.

Ma précieuse binôme Aicha

Je te suis profondément reconnaissante pour ton soutien constant, tes encouragements et ta patience ces cinq dernières années. Je souhaite que notre amitié perdure éternellement et que nous concrétisions ensemble nos rêves.

En fin, je veux m'exprimer ma gratitude pour avoir accompli ce travail difficile.je veux me remercier pour ne pas avoir pris de jours de repos, je veux me féliciter de n'avoir jamais abandonné, je veux me remercier d'essayer de faire le plus de bien que du mal, je veux me remercier d'être simplement moi-même, et cela vaut pour tous ceux me connaissent de près ou de loin

Yousra

Dédicace

Je dédie ce travail :

A mes chers parents

Il est difficile de trouver les mots justes pour exprimer mon amour éternel et ma profonde gratitude pour les sacrifices que vous avez faits pour moi.

Ma mère, tu es la bougie de ma vie, celle qui illumine chaque jour de sa douce lumière. Je te remercie du fond du cœur pour tout ce que tu fais. Que Dieu te protège, te comble de bonheur et te garde en bonne santé, aujourd'hui et toujours.

Mon père, tu as toujours été à mes côtés pour me soutenir et m'encourager, et ce travail traduit ma gratitude et mon respect envers toi.

A mes chères sœurs Yasmine, Cérine et Assil

Que Dieu vous protège et que toute votre vie soit remplie de bonheur et de réussite.

A mes chers frères Lyes, Mohand-tayeb, et Massinissa

Je vous remercier du fond du cœur pour votre soutien constant et vos encouragements tout au long de mon parcours. Votre présence à mes côtés a été une source de force et de réconfort précieux

A ma binôme Yousra

Je tiens à te dédier ces mots pour te remercier de tout cœur pour notre collaboration exceptionnelle. Ta présence à mes côtés a rendu chaque défi plus léger et chaque réussite plus significative. Merci pour ton soutien constant et ton amitié précieuse.

A ma tante Hayat et A ceux qui m'ont toujours aidé et encouragé, qui étaient toujours à mes côtés, qui m'ont accompagné durant mon chemin d'études supérieures. A tous ceux qui compte pour moi et qui n'ont pas pu être cités ici.

Aicha

Table des matières

Table de figure :

Liste des tableaux

Liste des abréviations

API : Application programming Interface

AH : Authentification Header

ADSL : Asymmetric Digital Subscriber Line

BMT : Bejaia Méditerranéenne Terminal

CASB : Cloud Access Security Broker

DMZ : Demilitarized Zone

DNS : Domain Name System (Système de Noms de Domaine).

EPB : Entreprise portuaire Bejaia

ESP : Ecapsulating Security payload header

FTP : File Transfer Protocol (Protocole de transfert de fichiers)

GPS : Global Positioning System

HTTP : Hypertext Transfer Protocol

IETF : Internet Engineering Task Force

IKE : Internet Key Exchange (Échange de Clés Internet)

IPsec : Internet Protocol Security

L2F : Layer 2 Forwarding

L2TP : Layer 2 Tunneling Protocol

LAN : Local Area Network

LDP : Label Distribution Protocol

MAN : Metropolitan Area Network

MPLS : Multiprotocol Label Switching

MAU : Multistation Access Unit

NGFW : Next-Generation Firewall

NAS : Network Attached Storage

OSI : Open Systems Interconnexion

PAN : Personal Area Network

PPP : Point to Point Protocol

PPTP : Point-to-Point Tunneling Protocol

RSVP-TE : Resource Reservation Protocol - Traffic Engineering

SSH : Secure Shell

SWG : Secure Web Gateway

SD-WAN : Software-Defined Area Network

SASE : Secure Access Service Edge

SSL/TLS : Secure Sockets Layer/Transport Layer Security

SA : Security association

SPA : Service Public d'Assainissement

SMTP : Simple Mail Transfer Protocol

TCP/IP : Transmission Control Protocol/Internet Protocol

TFTP : Trivial File Transfer Protocol

TCP : Transmission Control Protocol

UDP : User Datagram Protocol

VPN : Virtuel Private Network

VM : Virtuelles Machines

VLAN : Virtual Local Area Network

WAN : Wide Area Network

WIFI : Wireless Fidelity

ZTNA : Zéro Trust Network Access

ZEP : Zone Extra Portuaire

INTRODUCTON GENERALE

Les réseaux informatiques jouent un rôle essentiel en facilitant la connectivité et le partage d'informations à travers le monde. Des réseaux locaux aux infrastructures mondiales, ils constituent le socle de notre ère numérique, permettant aux individus, aux entreprises et aux organisations de communiquer, de collaborer et de partager des ressources de manière efficace et transparente. Cependant, avec l'expansion rapide des besoins en connectivité et la diversification des types de données transitant sur les réseaux, des défis significatifs ont émergé. La sécurité des données, la gestion de la bande passante, l'optimisation des performances et la flexibilité opérationnelle sont devenus des priorités cruciales pour les administrateurs réseau et les décideurs informatiques.

C'est dans ce contexte que la technologie SD-WAN (Software-Defined Wide Area Network) se distingue comme une solution innovante et pertinente. Contrairement aux réseaux traditionnels basés sur des infrastructures matérielles, le SD-WAN repose sur une approche logicielle, offrant une virtualisation du contrôle du réseau. Cette virtualisation permet une gestion centralisée et dynamique des flux de données, offrant ainsi une flexibilité opérationnelle inégalée et une adaptation rapide aux besoins changeants des entreprises. Le SD-WAN apporte également des avantages significatifs en termes de sécurité. En permettant une segmentation avancée du trafic, une authentification renforcée et des mécanismes de chiffrement robustes, il renforce la protection des données sensibles tout en réduisant les risques liés aux menaces cybernétiques.

Comment SD-WAN peut-il répondre efficacement aux besoins spécifiques de connectivité, de sécurité et de gestion des performances réseau au sein de l'entreprise Bejaia Mediterranean Terminal (BMT), tout en optimisant les coûts et en assurant une transition transparente depuis les infrastructures réseau existantes ?

Dans cette perspective, notre projet est conçu l’implémentation d'une solution SD-WAN via un tunnel VPN Site a Site au sein de l'entreprise Bejaia Mediterranean Terminal (BMT).

Notre mémoire est structuré en quatre chapitres qui sont organisés comme suite :

Dans le premier chapitre nous débuterons en examinant les principes fondamentaux des réseaux informatiques avant d'aborder les aspects liés aux réseaux privés virtuelles (VPN).

Dans le deuxième Dans la deuxième partie, nous allons procéder à une description détaillée de la technologie SD-WAN en mettant en évidence sa définition, ses différents types, ainsi que ses avantages. Nous aborderons également sa comparaison avec d'autres technologies et discuterons de sa pertinence dans le contexte organisationnel.

Dans le troisième chapitre nous présenterons l'organisation d'accueil BMT, en décrivant sa structure et son réseau. Nous exposerons la problématique rencontrée, ainsi que les différentes solutions proposées pour répondre de manière efficace et proactive aux besoins actuels et futurs de l'entreprise.

Le quatrième chapitre est dédié à la définition des divers outils et logiciels utilisés pour la réalisation de notre solution. Nous détaillerons les configurations mises en place ainsi que les tests effectués pour vérifier nos simulations.

Chapitre 1 : Généralité sur les réseaux informatique et VPN

1.1 Introduction

Les réseaux informatiques sont très importants dans notre vie quotidienne Ils permettent la connexion entre divers dispositifs électroniques à travers le monde tels que des ordinateurs, smartphones, serveurs et autres périphériques, pour partager des ressources, des informations et des données.

Avec l'avènement des technologies avancées, les Réseaux Privés Virtuels (VPN) se sont imposés comme des outils essentiels pour sécuriser et optimiser les communications informatiques. Les VPN augmentent la sécurité des connexions Internet en créant un canal sécurisé et crypté pour les données, protégeant ainsi les informations sensibles contre les menaces extérieures et des interceptions.

Ce chapitre est structuré en deux parties distinctes. La première partie traite des généralités sur les réseaux informatiques, abordant leurs définitions, types, topologies, architectures, ainsi que les équipements d'interconnexion. Ces éléments fondamentaux établissent une base solide pour comprendre comment les réseaux facilitent la communication et le partage de ressources entre différents dispositifs informatiques.

La seconde partie du chapitre se focalise sur les VPN. Où nous discuterons de leur définition, typologie, utilité, et principe de fonctionnement. Nous approfondirons aussi les protocoles VPN et les enjeux de sécurité associés, afin de démontrer comment les VPN renforcent la sécurité des données transmises sur des réseaux moins sécurisés comme Internet.

1.2 Généralités sur les réseaux informatique

1.2.1 Définition d’un réseau informatique

Un réseau informatique est un ensemble d’ordinateurs et d'autres dispositifs connectés entre eux pour échanger des informations numériques et partager des ressources selon des règles et des protocoles bien définis. Les composants d'un réseau peuvent être reliés par le biais de connexions filaires comme Ethernet ou sans fil comme WI-FI.

1.2.2 Type des Réseaux informatique

On peut classer les réseaux informatiques en 4 types selon la localisation, la distance et le débit de transmission :

1. PAN (Personal Area Network)

Un Réseau personnel est utilisé pour a communication entre des appareils personnels leur portée est généralement limitée à quelques mètres.

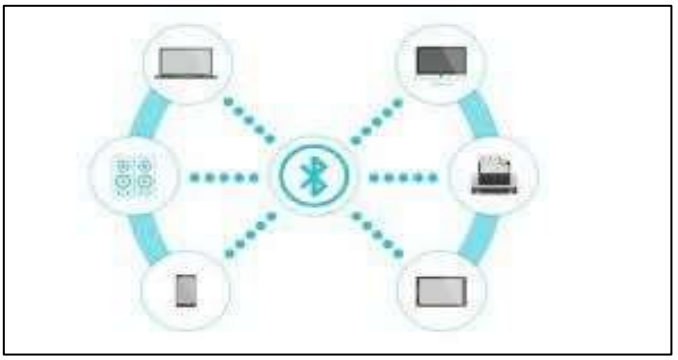


Figure 1 : Réseau personnel (PAN) *[1]*

2. LAN (Local Area Network)

Réseau locale, intra entreprise, où les stations peuvent être séparées d'au plus quelques kilomètres. Avec un débit de transmission relativement élevé, atteignant un minimum de 10 Mbits/s.

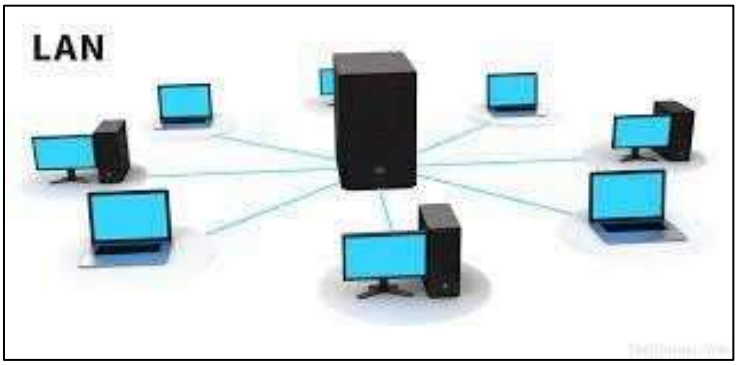


Figure 2 : Réseau locale (LAN) *[2]*

3. MAN (Metropolitan Area Network)

Réseau métropolitain qui permet la connexion entre deux ou plusieurs sites à l'échelle d'une ville. Le support de transmission et généralement des câbles coaxiaux ou la fibre optique cette catégorie de réseau a été conçue pour supporter le transport des donnes a une vitesse supérieure à 1 Mbits/s.

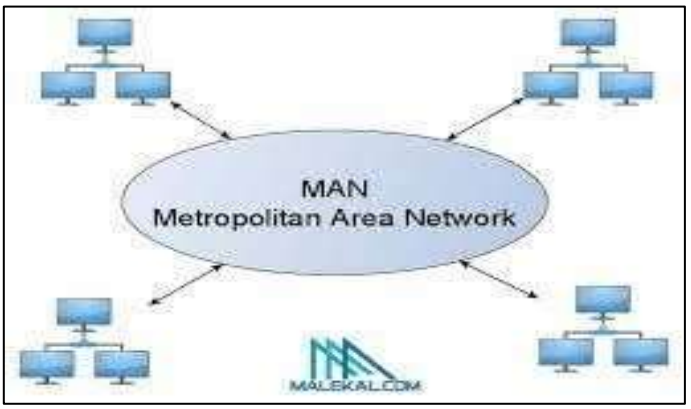


Figure 3 : Réseau métropolitain (MAN) *[3]*

4. WAN (Wide Area Network)

Réseau étendu à l'échelle d'un pays ou maximum quelque centaine de kilomètre, le plus connue des WAN et Internet.

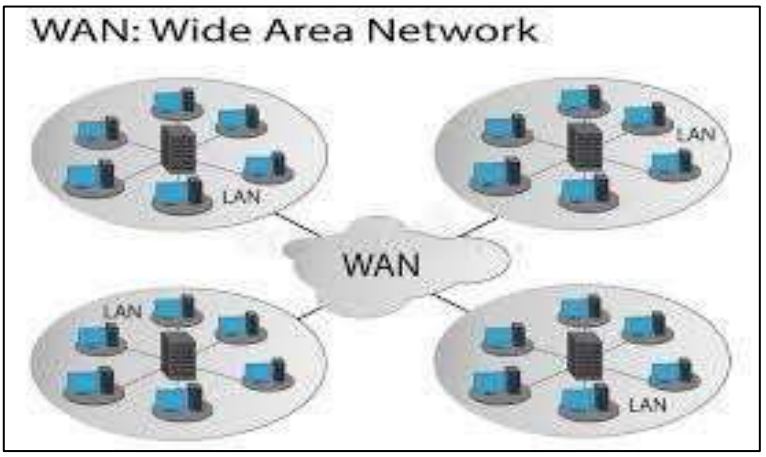


Figure 4: Réseaux étendu (WAN) *[4]*

1.2.3 Topologie des réseaux

La topologie des réseaux informatiques est la manière dont les différents éléments d'u réseau (ordinateurs, imprimantes, serveurs, etc.) sont connectés les uns aux autres. Voici les principales topologies de réseau :

Les équipements du réseau sont reliés à un système matériel central (le nœud). Celui-ci a pour rôle d'assurer la communication entre les différents équipements du réseau. Notamment utilisée par les réseaux Ethernet actuels en RJ45, elle concerne maintenant la majorité des réseaux. Lorsque toutes les stations sont connectées à un commutateur, on parle de topologie en étoile.

Topologie en Bus : Un réseau en bus est une architecture de communication où la connexion des matériels est assurée par un bus partagé par tous les utilisateurs. Les réseaux de bus permettent de relier simplement de multiples matériels, mais posent des problèmes quand deux machines veulent transmettre des données au même moment sur le bus. Les systèmes qui utilisent une topologie en bus ont normalement un arbitre qui gère l'accès au bus.

Topologie en anneau : Toutes les machines sont reliées entre elles dans une boucle fermée. Les données circulent unidirectionnellement, d'une entité à la suivante. Les ordinateurs communiquent chacun à leur tour. Cela ressemble à un bus mais qui serait refermé sur lui-même : le dernier nœud est relié au premier. Souvent, dans une topologie en anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un répartiteur (appelé MAU, Multi station Access Unit) qui va gérer la communication entre les ordinateurs qui lui sont reliés en répartissant à chacun d'entre eux un temps de parole.

Topologie maillée : Le réseau maillé est une topologie de réseau où tous les hôtes sont connectés les uns aux autres sans hiérarchie centrale, formant une structure en forme de filet. Chaque nœud doit donc recevoir, envoyer et relayer les données, ce qui évite les points de défaillance uniques. En cas de panne d'un nœud, les données peuvent être reroutées via d'autres chemins, assurant ainsi la continuité de la communication.

Topologie en arbre : Une topologie en arbre, également appelée topologie arborescente ou hiérarchique, peut être vue comme une collection de réseaux en étoile organisés de manière hiérarchique. Ce réseau est structuré en niveaux, avec un sommet de haut niveau connecté à plusieurs nœuds de niveau inférieur, qui peuvent à leur tour être connectés à d'autres nœuds de niveau inférieur. Cependant, comme dans le réseau en étoile conventionnel, une défaillance d'un seul point peut isoler des nœuds individuels ou des sections entières du réseau, si un lien ou une connexion échoue. [5]

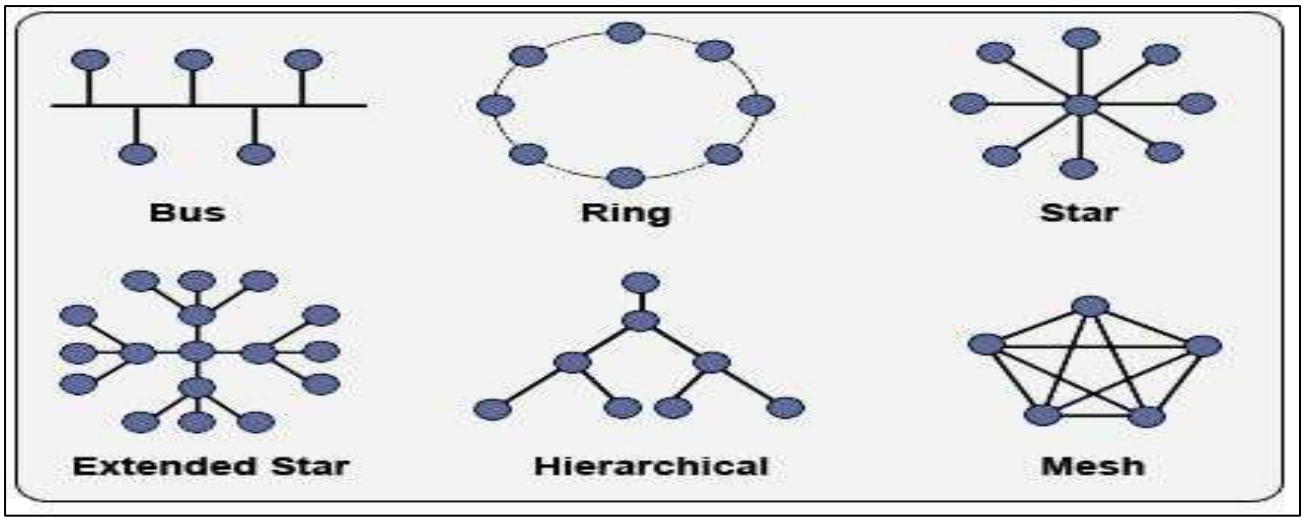


Figure 5 : typologies Réseaux *[5]*

1.2.4 L'architecture des Réseaux

L'architecture des réseaux désigne la structure globale d'un réseau de communication. Cette architecture définit la manière dont les composants du réseau interagissent, les protocoles utilisés, et la manière dont les informations sont échangées.

Le modèle d ' OS I

Le Modèle de référence ISO pour Interconnexion des Systèmes Ouverts a été proposé en 1984 par l'OSI. Son principe de base est la représentation des réseaux sous la forme de sept couches de fonctions superposées les unes aux autres. Chaque couche fournit des services pour la couche supérieure, communique avec son homologue via un protocole bien d´défini (règles de communication) et utilise les services fournis par la couche inférieure. [6]

Voici Les sept couches du modèle OSI et leur rôle :

Couche 1 – Physique : Elle assure la transmission de bits entre les entités physiques Elle fournit donc des moyens nécessaires à l'activation et au maintien d'une connexion physique.

Couche 2 - Liaison de données : Son objectif est de masquer les caractéristiques physiques et effectuer des contrôles d'erreur. Les données sont structurées en trames, avant l'émission un code d'erreur (CRC) est ajouté dans la trame, et à la réception un contrôle d'erreur est effectué grâce au code d'erreur précédemment inséré.

Couche 3 - Réseau : Son objectif est d'assurer l'acheminement de bout-en-bout des paquets à travers le réseau en tenant compte des nœuds intermédiaires. Les services offerts sont : le routage, la commutation de paquets et la prise en charge la segmentation et le regroupage.

Couche 4 – Transport : Son objectif est acheminement de bout en bout exclusivement des datagrammes. Les services offerts sont : la fragmentation en paquets et le multiplexage/démultiplexage.

Couche 5 - Session : Son objectif est de fournir un ensemble de services pour la coordination des applications. La coordination peut être l'établissement de la connexion entre les applications et la définition de points de synchronisation en cas d'erreur.

Couche 6 – Présentation : Elle permet de manipuler des objets types plutôt que des bits, et fournit une représentation standard pour ces objets. Elle fournit des services tels que : la définition d'une notation abstraite pour les objets typés, la compression, le cryptage, etc.

Couche 7 - Application : Son objectif est de rendre des services aux utilisateurs sous forme d'applications telles que : mail, news, ftp, terminaux virtuels (telnet, rlogin, ssh), etc. [7]

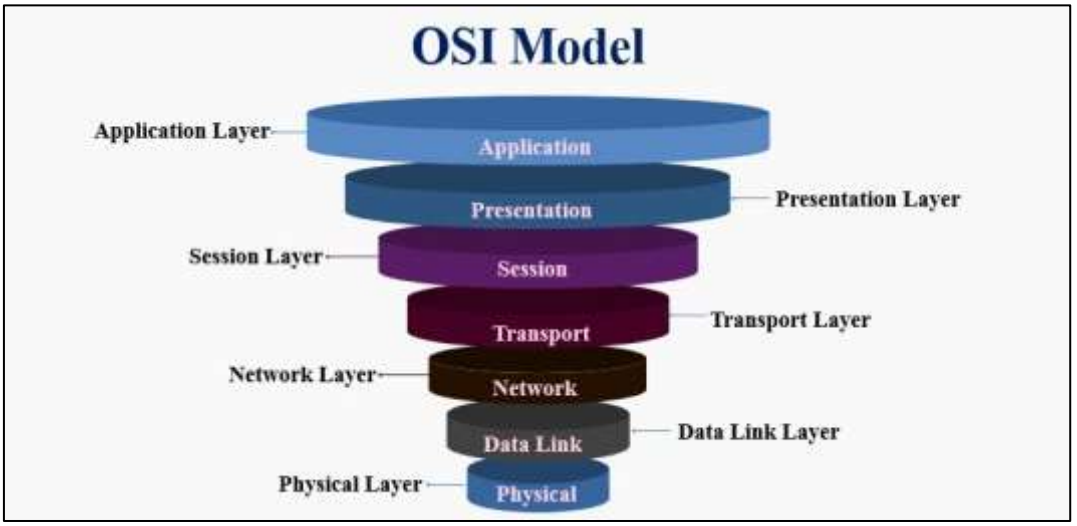


***Figure 6**:* Modèle OSI *[8]*

Le Modèle TCP/IP

Le terme TCP/IP est généralement utilisé pour décrire une architecture réseau, mais en réalité, il fait référence à deux protocoles intimement liés : le protocole de transport TCP (Transmission Control Protocol) et le protocole réseau IP (Internet Protocol). Ce que l'on appelle le "modèle TCP/IP" est en fait une architecture réseau composée de quatre couches, dans laquelle les protocoles TCP et IP jouent un rôle central en tant qu'implémentation la plus

répandue. Parfois, le terme TCP/IP est utilisé de manière interchangeable pour désigner à la fois le modèle TCP/IP et la paire de protocoles TCP et IP.

Voici les quatre couches du modèle TCP IP :

Couche réseau :

Cette couche combine les fonctionnalités des couches physique et liaison de données du modèle OSI. Elle n'est pas spécifiée de manière stricte, se focalisant uniquement sur la capacité des hôtes à envoyer des paquets IP sur le réseau. Les implémentations de cette couche dépendent de la technologie utilisée localement, comme Ethernet dans de nombreux réseaux locaux.

Couche internet :

Elle est essentielle pour l'interconnexion de réseaux hétérogènes. Cette couche gère l'acheminement des paquets de manière indépendante, permettant leur injection dans tout réseau sans connexion préalable. Les paquets peuvent donc arriver désordonnés, et le contrôle de l'ordre est laissé aux couches supérieures. La fonction critique ici est le routage, avec le protocole IP comme implémentation officielle.

Couche transport :

Elle assure une communication fiable entre entités distantes, similairement à la couche transport du modèle OSI. Les principales implémentations sont TCP, qui est fiable et orienté connexion, gérant la fragmentation, l'ordonnancement des paquets, et le contrôle de flux ; et UDP, qui est plus simple, non fiable et sans connexion, utilisé quand la rapidité est plus critique que la fiabilité (ex. transmission de la voix).

Couche application :

Cette couche regroupe les protocoles de haut niveau sans les couches présentation et session jugées inutiles, telles que dans le modèle OSI. Elle comprend des protocoles tels que Telnet, TFTP, SMTP, et HTTP. Le choix du protocole de transport (TCP ou UDP) se fait selon les exigences de fiabilité et de rapidité de l'application. TFTP utilise UDP pour la rapidité sur des réseaux fiables, tandis que SMTP utilise TCP pour garantir la fiabilité et l'intégrité des données dans la transmission de courriers électroniques. [9]

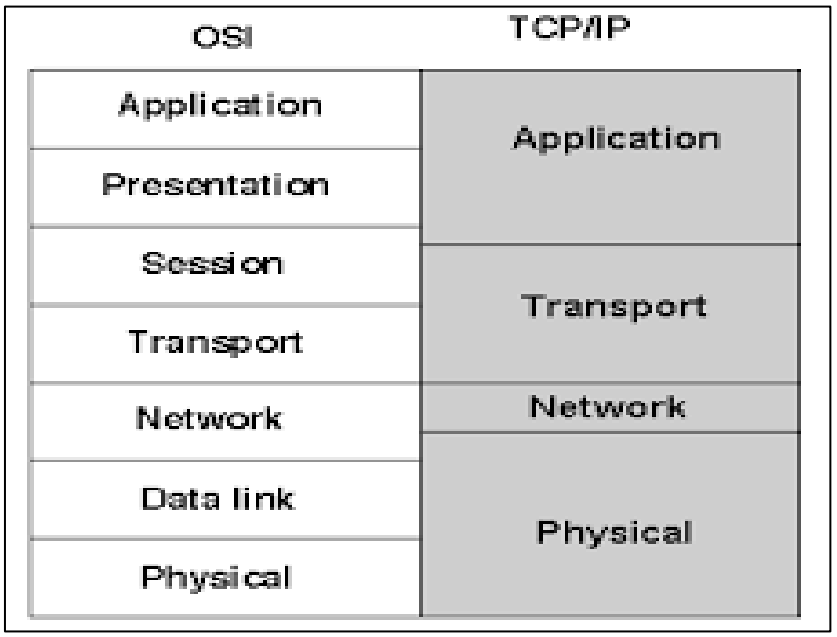


Figure 7: comparaison entre le modèle OSI et TCP/IP *[10]*

1.2.5 Intérêt des réseaux informatiques

Les réseaux informatiques offrent de nombreux avantage tel que :

Amélioration de la communication : Les réseaux permettent aux utilisateurs de communiquer rapidement et efficacement, peu importe leur emplacement géographique. Cela comprend la collaboration en temps réel et le partage de fichiers et de messages.

Partage de ressources : Les réseaux facilitent le partage de ressources telles que des imprimantes, des fichiers et des connexions internet, ce qui permet d'économiser du temps et des coûts.

Stockage centralisé : Ils permettent un stockage centralisé des données, ce qui facilite la gestion, la sauvegarde et la récupération des données.

Sécurité renforcée :

Bien que les réseaux puissent présenter des risques de sécurité, ils offrent également des moyens de protéger les données via des protocoles de cryptage, des firewalls et des politiques de sécurité.

Accès à distance : Grâce aux réseaux, il est possible d'accéder aux ressources informatiques à distance.

1.3 Les réseaux privés Virtuels (VPN)

1.3.1 Définition d'un VPN

Un Réseau Privé Virtuel (VPN) est un service informatique conçu pour établir un tunnel sécurisé entre un ou plusieurs points distants, permettant une communication fiable et sécurisée à travers des réseaux peu sûrs, tels que l'Internet.

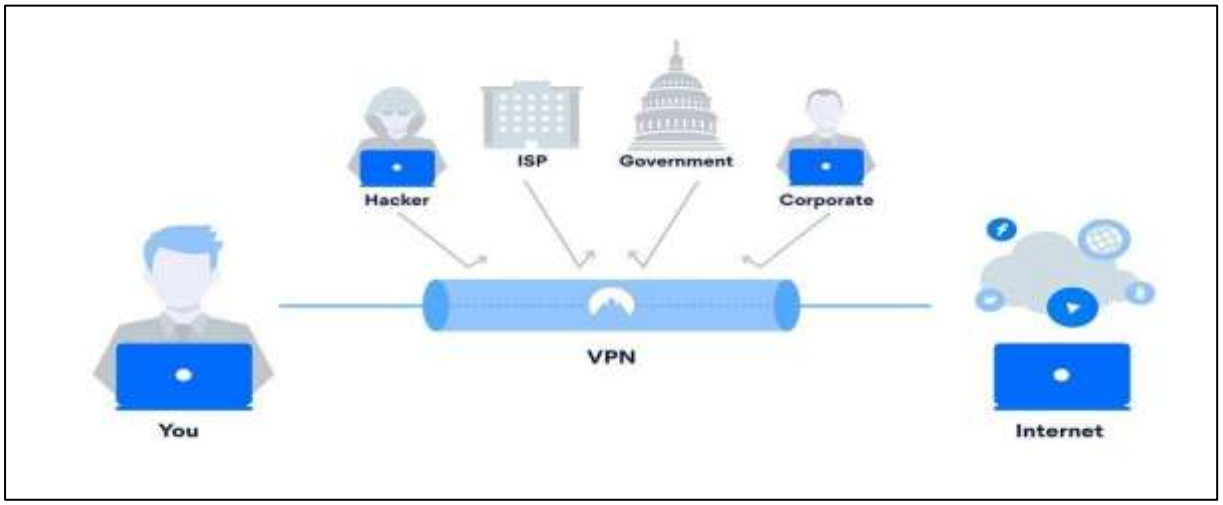


Figure 8: Virtual Private Network (VPN) *[11]*

1.3.2 Les composantes d'un VPN

Le client VPN : initie une connexion vers un serveur VPN. Ce client peut-être :

Une station telle qu'un client de l'extérieur qui souhaite créer un VPN avec le réseau de son entreprise.
Un routeur : dans ce cas, toutes les stations du réseau local utiliseront le tunnel et donc la protection VPN sera effective sur tous les périphériques qui sont connectés au routeur.

Le serveur VPN : qui accepte, traite et répond aux demandes des clients VPN il fournit donc :

Un VPN accès distant pour un poste isolé
Un VPN routeur pour sécuriser et donner l'accès à un réseau local.

Le tunnel : c'est un lien de connexion entre le client et le serveur VPN dans lequel les paquets de données sont encapsulés.

Le client et le serveur VPN sont tous les deux capables de chiffrer et déchiffrer les données de part et d'autre du tunnel, on désigne deux modes de Tunnels :

Tunnel obligatoire : Node To Node, est crié au niveau de deux extrémités de tunnel
Par exemple entre deux LAN d'une entreprise (routeur à routeur).

Tunnel volontaire : End To End, est crié entre le client et le serveur VPN. [12]

1.3.3 Le fonctionnement d'un VPN

VPN fonctionne en établissant un tunnel crypté entre le client et le serveur VPN pour sécuriser le transfert des données. Lorsque le client souhaite accéder à un site web, après avoir établi la connexion avec le serveur, son logiciel VPN installé sur son appareil chiffre le trafic de données et l'envoie via le fournisseur d'accès à internet vers le serveur VPN distant. Ce dernier déchiffre les données, les transmet sur internet, reçoit la réponse, puis chiffre à nouveau le trafic avant de le renvoyer au client. Enfin, le logiciel VPN sur l'ordinateur du client déchiffre les données pour pouvoir les utiliser.

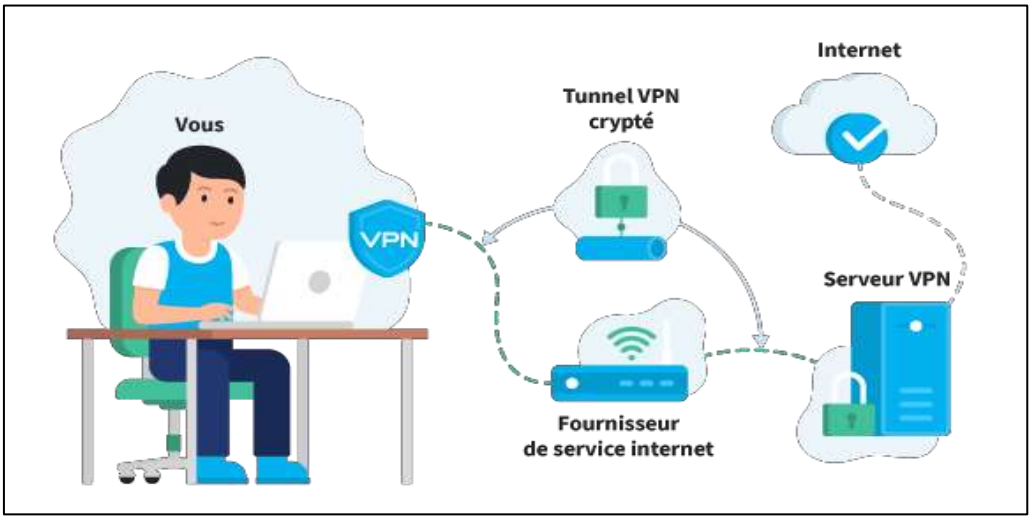


Figure 9 : le fonctionnement d'un VPN [13]

1.3.4 Typologie des VPNs

Les VPN peuvent être classés en deux grandes catégories en fonction de leur fonctionnement et de leur utilisation : [14]

1.3.4.1 VPN d'entreprise

L'entreprise garde le contrôle de l'établissement des VPN entre ces diffèrent point de présence ainsi qu'entre cette poste située à l'extérieur de l'entreprise et les sites principaux.

VPN site a site

Il s'agit de relier deux sites d'une même organisation ou entreprise généralement ce type de VPN et mise en place par l'interconnexion de deux élément matériel (routeur, pare-feu) qui prennent en charge le cryptage et l'authentification et le routage des paquets. Situés à la Frontier entre le réseau interne et le réseau public de chaque site.

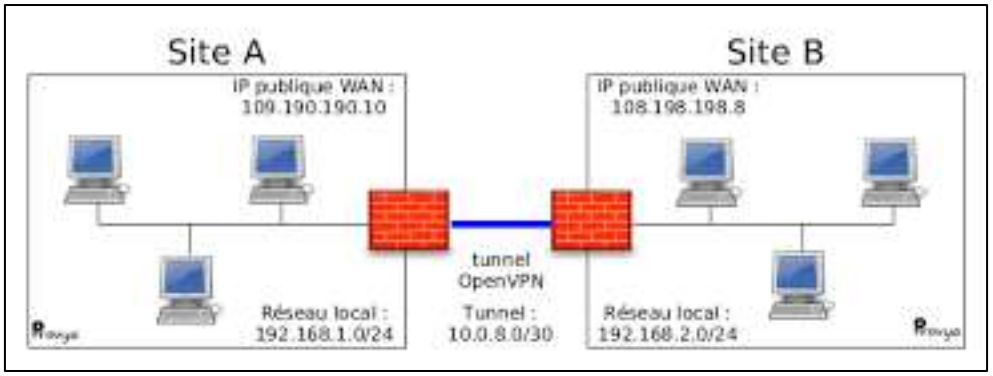


Figure 10: VPN Site a Site *[15]*.

VPN Poste a site

Ce type de VPN est très courant et permet à des utilisateurs distants, tels que des télétravailleurs, des nomades et des commerciaux, d'accéder au réseau privé de l'entreprise ou à ses ressources via un VPN.

Deux scénarios sont possibles :

L'utilisateur demande à son fournisseur d'accès de mettre en place une connexion cryptée vers le serveur distant. Il communique avec le serveur d'accès réseau (NAS) du fournisseur, qui est alors responsable de l'établissement de la connexion cryptée.

L'utilisateur dispose de son propre logiciel client VPN, avec lequel il établit directement une communication cryptée vers le réseau de l'entreprise.

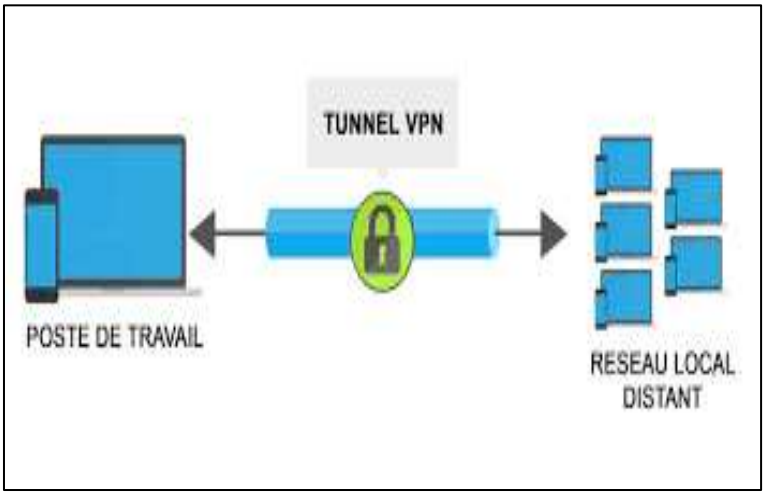


Figure 11 : VPN Poste a Site [16]

VPN Poste à Poste

Ce type de VPN a comme objectif d'établir un canal sécurisé de bout en bout entre deux postes ou, plus couramment, entre un poste et un serveur. Le poste et le serveur peuvent être située sur le même réseau ou sur deux réseaux différents relier eux-mêmes par un VPN site a site.

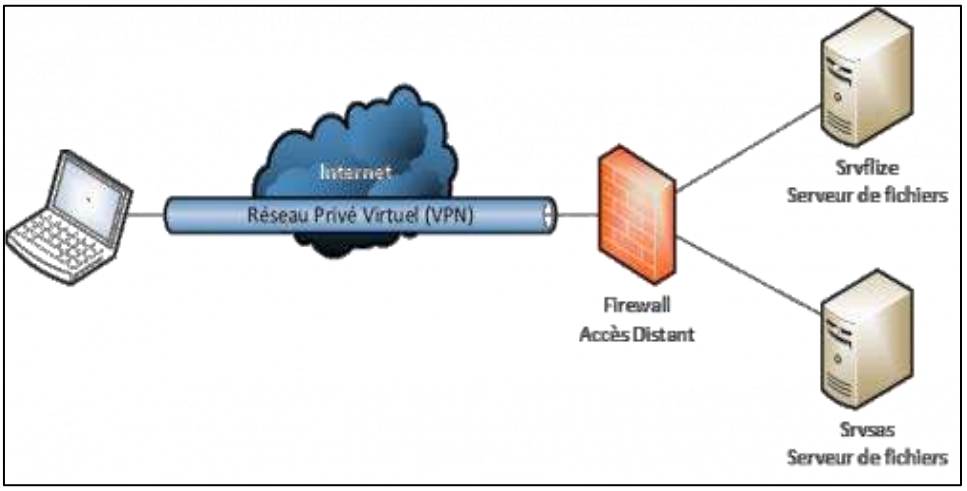


Figure 12 : VPN Poste à poste [17].

1.3.4.2 VPN Operateur

Lorsqu'il s'agit d'interconnecter plusieurs sites d'une même entreprise avec des garanties de performance et de disponibilité, il est généralement plus judicieux, bien que plus coûteux, de faire appel à un opérateur qui mettra en place un réseau privé entre tous les sites. Comme nous le verrons, ce réseau ressemble davantage à un réseau de tunnels qu'à un véritable réseau VPN. Néanmoins, il est courant de le désigner comme un VPN opérateur car, sans l'intervention du personnel de l'opérateur, il est difficile d'intercepter les communications échangées entre les sites, ce qui le classe souvent dans la catégorie des VPN de confiance (Trusted VPN).

1.3.5 Utilité et avantages des VPNs

L'utilisation d'un VPN a plusieurs avantages importants pour une entreprise :

1. **Communication sécurisée :** Les VPN créent des connexions sécurisées, chiffrées et fiables, ce qui est essentiel pour protéger les données sensibles de l'entreprise des cybermenaces.
2. **Accès distant sécurisé :** Les employés peuvent se connecter à distance au réseau de l'entreprise de manière sécurisée, garantissant ainsi la confidentialité des informations échangées.

3. **Contournement des restrictions géographiques** : Les VPN permettent aux employés d'accéder aux ressources internes de l'entreprise, même s'ils sont en déplacement ou à l'étranger.
4. **Protection des données personnelles sensibles :** Les VPN protègent les données personnelles et professionnelles échangées en ligne en cryptant le trafic internet, réduisant ainsi les risques de fuites d'informations.
5. **Coûts :** Permet de réduire les coûts liés à l'infrastructure réseau des entreprises par la mise en place d'une liaison VPN.

1.3.6 Principe de fonctionnement d'un VPN

Un réseau VPN repose sur le protocole de tunnelisation appelle protocole tunneling. Ce protocole permet de faire circuler les informations de l'entreprise d'une façon cryptée du bout en bout de autres tunnels ainsi, les utilisateurs ont l'impression de se connecter directement dans le réseau de leur entreprise.

Le principe de tunneling consiste à construire un chemin virtuel après avoir Identifier l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntent ce chemin virtuel. Afin d'assurer un accès aise et peu couteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau prive, alors qu'ils utilisent des processus d'encapsulation, de transmission et de désencapsulassions. [18]

1.3.7 Les Protocoles VPN

Les différents protocoles de tunneling existent pour créer des réseaux VPN sont :

1.3.7.1 Niveau 2 :

PPTP (Point-to-Point Tunneling Protocol) :

Le protocole PPTP (Point-to-Point Tunneling Protocol) est un protocole VPN développé par un consortium créé par Microsoft, utilisé pour établir des connexions réseau privées. Il repose principalement sur le protocole PPP (Point-to-Point Protocol) Pour établir des connexions avec un fournisseur d'accès Internet via un serveur d'accès réseau (NAS). Cette méthode est essentielle pour encapsuler des paquets IP et d'autres types de données de protocoles réseau dans des trames PPP. Facilitant ainsi leur transmission sur un point de liaison à point.

L2F (Layer 2 Tunneling Protocol) :

L2F est un protocole développé par Cisco autour des années 1996, L'IETF en fait un standard en 1998 avec LA RFC 2341, pour permettre la création de tunnels VPN au niveau de la couche de liaison sans nécessiter de cryptage. Moins utilisé aujourd'hui, il a été intégré dans le développement de L2TP.

L2TP (Layer 2 Tunneling Protocol) :

Ce protocole est une combinaison des deux protocole PPTP et L2F, il ne chiffre pas par lui-même les données qu'il transporte. C'est pourquoi il est associé à IPsec pour le cryptage, afin de garantir la sécurité des informations échangées. Ce protocole est maintenant un des protocoles VPN implantés nativement sur les machines Windows, ce qui explique son succès.

1.3.7.2 Niveau 2 et 3 :

MPLS (Multi Protocol Label Switching) :

Le protocole MPLS (Multi Protocol Label Switching) est souvent considéré comme situé dans un niveau intermédiaire entre le niveau 2 et le niveau 3. C'est pourquoi on lui affecte souvent un niveau hybride 2.5 qui n'existe pas dans les couches OSI traditionnelles. Son placement en tant que protocole de VPN peut être contesté lorsqu'il est utilisé dans ses fonctions de base. En effet il ne met pas en œuvre certaines fonctions de sécurité telles que le cryptage, ce qui est en principe un prérequis du VPN.

1.3.7.3 Niveau 3

SSL/TLS

Ce protocole ou plutôt ces protocoles sont en plein essor car très simples de mise en œuvre et utilisant le port (443), ce qui facilite le franchissement des firewalls. Dans un certain nombre de cas, ils ne nécessitent qu'un simple navigateur pour être utilisables. Ils sont maintenant implémentés de façon native dans d'autres logiciels (client de messagerie, client FTP). **[19]**

SSH

Ce protocole était souvent utilisé pour protéger des communications de type console (équivalent de Telnet) ou transferts de fichiers (de type FTP notamment). Son essor est limité à la fois par le succès grandissant de SSL/TLS et par son champ d'application plus restreint. Néanmoins il reste encore un protocole à considérer pour certains usages.

IPSec

IPsec (Internet Protocol Security) c'est un protocole de sécurité de la couche 3 (couche réseau) du modèle OSI développé par l'IETF (RFC 2401) en 1995, qui permet par encapsulation de rendre confidentielle le contenue des paquets véhiculés par le protocole IP, et d'identifier la source et la destination des paquets et d'assurer l'intégrité des données véhicule. [20]

1.3.8 Le fonctionnement IPSec

Les services de sécurité fournis par IPsec reposent sur trois protocoles différents qui constituent le cœur de la technologie IPsec :

L'entête d'authentification (**AH**, Authentification Header).

L'entête de confidentialité-authentification (**ESP**, Ecapsulating Security payload header).

IKE (Internet Key Exchange)

Ces protocoles peuvent être utilisés indépendamment ou, plus rarement, de manière combinée.

AH : intégrité et authentification des paquets

Le protocole AH, qui est utilisé de manière moins fréquente qu'ESP, permet d'assurer l'intégrité et, employé avec IKE (Internet Key Exchange), l'authentification des paquets IP. C'est à dire qu'AH permet d'une part de s'assurer que les paquets échangés n'ont pas été altérés et d'autre part de garantir l'identité de l'expéditeur d'un paquet. Il garantit aussi une protection contre le rejeu.

IKE (Internet Key Exchange)

C'est un protocole qui permet d'établir une connexion sécurisée entre deux appareils sur Internet. Il facilite la création d'une association de sécurité (SA) où les deux appareils négocient les clés et les algorithmes de chiffrement nécessaires pour échanger des paquets de données de manière sécurisée.

ESP : confidentialité, intégrité et authentification des paquets

Le protocole ESP permet quant à lui d'assurer la confidentialité, l'intégrité et, employé avec IKE, l'authentification des données échangées. Il garantit aussi une protection contre le rejeu. Il est possible d'utiliser uniquement les fonctions d'intégrité et d'authentification sans chiffrement (ce qui peut satisfaire la plupart des cas d'usage d'AH).

1.3.8.1 Modes de IPSec

Indépendamment du choix entre AH et ESP, il est possible d'utiliser IPsec dans deux modes distincts : le mode tunnel et le mode transport. Le mode tunnel rend le service attendu dans la majorité des cas.

En mode Transport, IPSec chiffre uniquement la charge utile et le trailer ESP d'un paquet IP, laissant l'en-tête intact. Ce mode est généralement utilisé pour les communications de bout en bout entre des dispositifs, comme entre un client et un serveur ou entre deux serveurs dans un réseau privé. L'avantage principal du mode Transport est qu'il fournit une connexion sécurisée sans modifier les en-têtes IP, permettant aux paquets de se déplacer sans problème à travers le réseau sans nécessiter d'ajustements par les routeurs. [21]

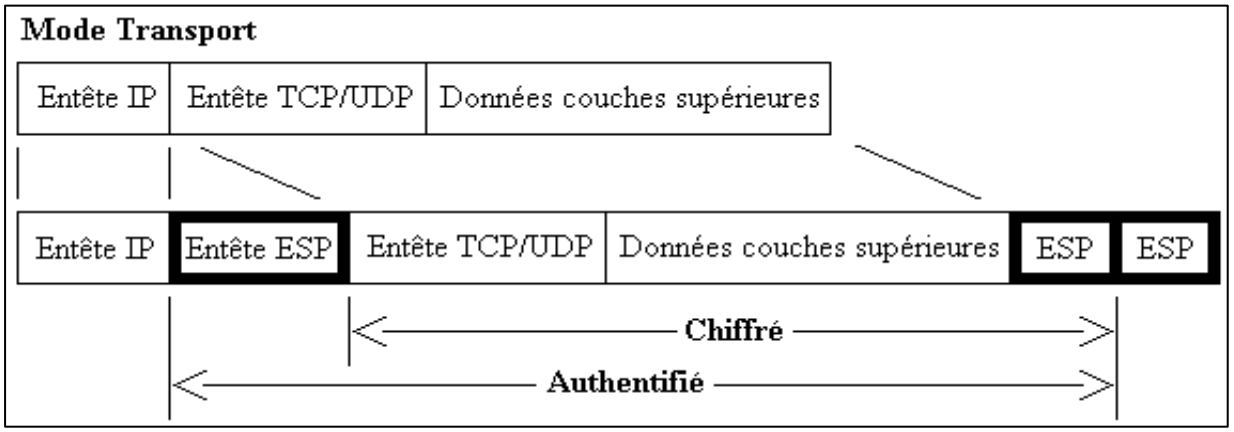


Figure 13 : Utilisation d'ESP en mode transport *[22]*

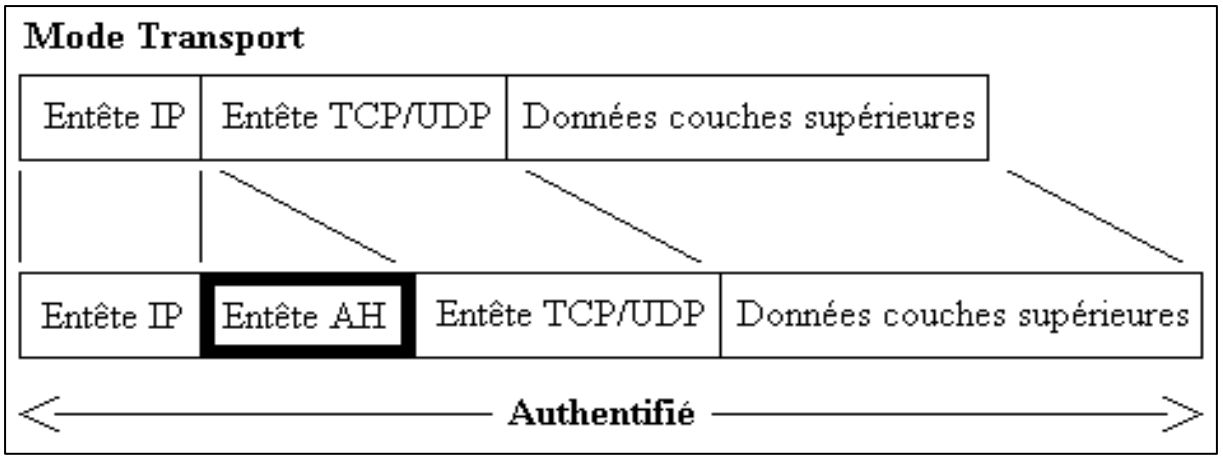


Figure 14 : Utilisation de AH en mode de transport *[22]*

Contrairement au mode Transport, **le mode Tunnel** chiffre le paquet IP entier et l'encapsule dans un nouveau paquet IP avec un nouvel en-tête IP. Ce mode est principalement utilisé pour les communications de réseau à réseau (par exemple, entre les passerelles de différentes branches d'une entreprise) ou d'une station finale à une passerelle (par exemple, dans un scénario d'accès à distance). Ce mode est essentiel pour créer des réseaux privés virtuels (VPN) où l'objectif est de sécuriser les communications d'un réseau à un autre sur Internet. [21]

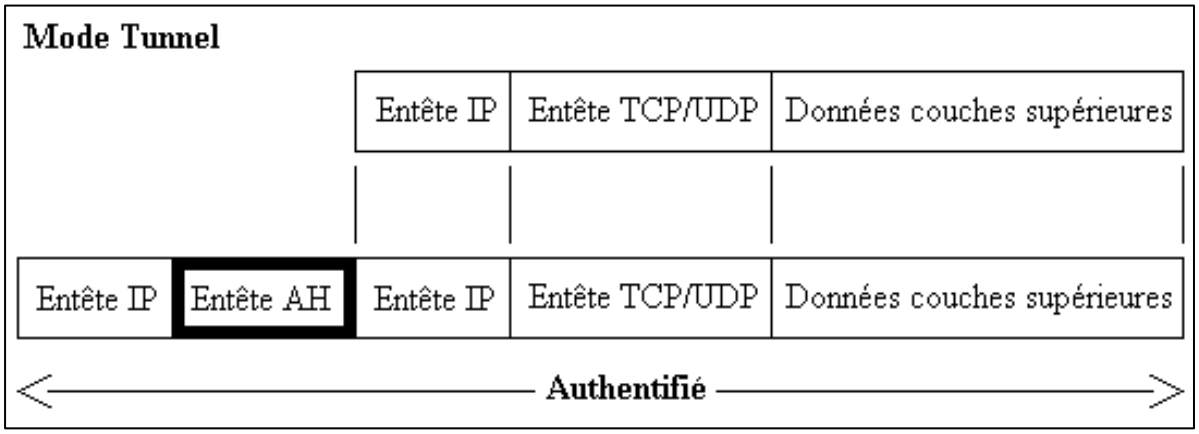


Figure 15 : Utilisation du AH mode tunnel *[22]*

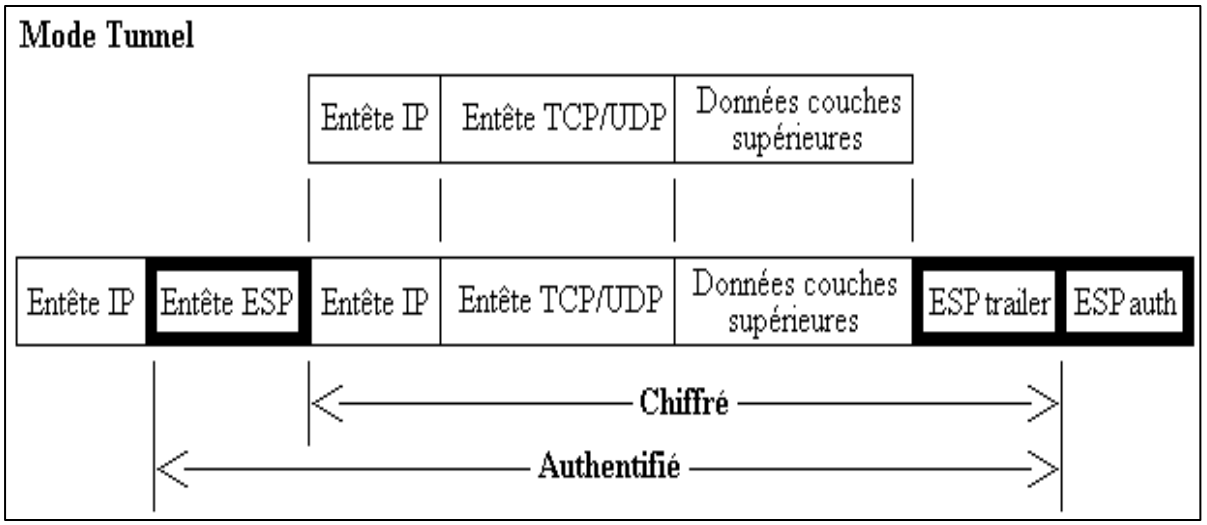


Figure 16 : Utilisation d'ESP mode tunnel *[22]*

1.3.9 Sécurités De VPN

1.3.9.1 Risque associé aux VPN

Les VPN (Virtual Private Networks) offrent généralement un niveau élevé de sécurité, mais ils ne sont pas exempts de risques potentiels. Voici quelques-uns des risques de sécurité associés aux VPN : [23] [24]

1. **Fuites de données DNS (Domain Name System) :** Les fuites DNS peuvent survenir lorsque le trafic DNS n'est pas routé à travers le VPN, exposant ainsi les sites Web que vous visitez. Les VPN doivent être configurés correctement pour éviter ces fuites.
2. **Fuites d'IP :** Un VPN mal configuré ou défaillant peut accidentellement révéler votre véritable adresse IP, annulant ainsi l'anonymat que vous cherchez à obtenir.
3. **Journalisation des données :** Certains fournisseurs de VPN conservent des journaux de vos activités en ligne, ce qui peut compromettre votre vie privée si ces données sont compromises ou demandées par les autorités.
4. **Attaques de l'homme du milieu :** Les attaques de l'homme du milieu peuvent se produire si un attaquant parvient à intercepter et à déchiffrer les communications entre vous et le serveur VPN, compromettant ainsi la confidentialité de vos données.
5. **Vulnérabilités de sécurité :** Comme tout logiciel, les VPN peuvent contenir des vulnérabilités qui pourraient être exploitées par des attaquants pour accéder à votre système ou à vos données.
6. **Phishing :** le phishing est une véritable menace qui s'accentue avec le télétravail Très souvent, les employés peuvent recevoir un mail les invitant à ouvrir une pièce jointe ou à cliquer sur un lien pour saisir des données personnelles. Ou, c'est une manière de dérouler le tapis rouge à un cybercriminel qui accèdera au système d'information de votre entreprise. [25]
7. **Fuites WebRTC** : Certaines applications Web peuvent contourner le VPN et divulguer votre adresse IP réelle via WebRTC (Web Real-Time Communication), même lorsque vous utilisez un VPN.
8. **Attaques par déni de service (DDoS) :** Les VPN peuvent être utilisés pour lancer des attaques DDoS contre d'autres utilisateurs ou serveurs, bien que cela soit plus souvent associé à des services VPN gratuits ou peu fiables. [26]

1.3.9.2 Bonnes pratiques de sécurité

Voici quelques bonnes pratiques de sécurité à suivre lors de l'utilisation d'un VPN :

1. **Choisissez un fournisseur de VPN fiable :** Optez pour un service VPN réputé et bien établi, qui dispose de politiques de confidentialité claires et qui n'enregistre pas les données de navigation.
2. **Utilisez un protocole de sécurité fort :** Privilégiez les protocoles VPN sûrs et éprouvés comme OpenVPN, IKEv2/IPsec ou WireGuard, qui offrent un chiffrement solide et des fonctionnalités de sécurité avancées.

3. **Activez la fonction de kill switch :** Un kill switch est une fonctionnalité qui coupe automatiquement votre connexion Internet si le VPN se déconnecte, évitant ainsi les fuites d'IP accidentelles.
4. **Chiffrez vos données :** Assurez-vous que votre VPN utilise un chiffrement fort (comme AES 256 bits) pour sécuriser vos données pendant leur transmission sur Internet. Évitez les journaux de données : Choisissez un VPN qui promet de ne pas enregistrer vos activités en ligne ou de conserver un minimum de données de connexion pour protéger votre vie privée.
5. **Mettez à jour régulièrement votre logiciel VPN :** Assurez-vous que votre client VPN est toujours à jour pour bénéficier des dernières corrections de sécurité et des fonctionnalités améliorées.
6. **Vérifiez les paramètres de confidentialité de votre VPN :** Configurez votre VPN pour qu'il maximise votre confidentialité en désactivant les fonctionnalités telles que la géolocalisation ou les cookies de suivi. Évitez les VPN gratuits ou douteux : Méfiez-vous des services VPN gratuits qui peuvent compromettre votre sécurité en enregistrant vos données ou en affichant des publicités malveillantes.
7. **Utilisez un VPN sur tous vos appareils :** Protégez votre activité en ligne sur tous vos appareils en installant et en configurant le VPN sur chacun d'eux, y compris les ordinateurs, les smartphones et les tablettes.
8. **Soyez vigilant contre le phishing :** Évitez les sites Web et les applications VPN suspects, et méfiez-vous des e-mails ou des messages frauduleux prétendant provenir de votre fournisseur VPN. [27]

1.4 Conclusion

Ce chapitre nous a tout d'abord offert une précieuse opportunité de découvrir et d'approfondir notre compréhension des notions fondamentales relatives aux réseaux informatiques. Nous avons examiné de près des aspects essentiels tels que les définitions, les types, les topologies et les architectures des réseaux.

En deuxième lieu, nous avons approfondi notre compréhension des réseaux privés virtuels (VPN). Nous avons exploré leur définition précise, leurs composantes essentielles, leur fonctionnement, leurs différents types ainsi que les protocoles variés qu'ils utilisent, ainsi que les nombreux avantages qu'ils offrent.

Chapitre 2 :

Technologie SD-WAN

2.1 Introduction

Le déploiement et la gestion des réseaux WAN traditionnels présentent des défis majeurs pour les entreprises, notamment en ce qui concerne la complexité, la gestion des coûts et la qualité de service. Même avec l'utilisation de protocoles de routage dynamiques, les chemins WAN ne sont souvent optimisés que pour une accessibilité élémentaire. Les fournisseurs de services de communications peuvent certes utiliser diverses stratégies pour améliorer l'expérience client à l'échelle du WAN, mais pour de nombreuses entreprises, ces tâches demeurent complexes, longues et coûteuses.

C'est dans ce contexte que le SD-WAN (Software-Defined Wide Area Network) apparaît comme une solution prometteuse pour relever ces défis. En fournissant une approche innovante de gestion automatisée et dynamique de la connectivité réseau, le SD-WAN permet aux entreprises de simplifier leurs opérations tout en améliorant l'efficacité et en réduisant les coûts.

2.2 Définition des SD-WAN

Le SD-WAN, acronyme de Software-Defined Wide Area Network, est une approche logicielle de gestion du réseau WAN vise à répondre à ces nouveaux besoins avec la mise en œuvre d'un réseau dit « hybride » par l'ajout d'une branche de connexion Internet vers le site distant, parallèle à l'architecture « WAN » traditionnelle et reposant toujours sur des liaisons privées. Cette connexion Internet a deux objectifs :

Permettre un accès direct aux applications hébergées dans le Cloud

Offrir un second lien (redondance) entre le site distant et le site principal ou Datacenter de l'organisation. [28]

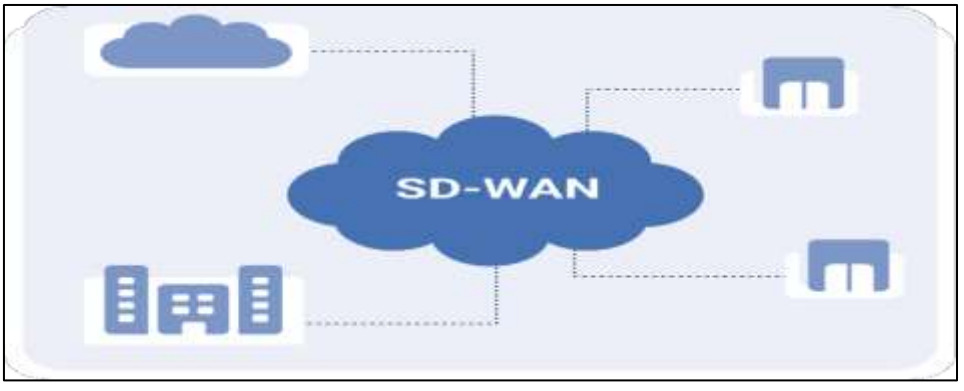


Figure 17: la technologie SD-WAN *[29]*

2.3 Histoire et évolution du SD-WAN

Les réseaux SD modernes et la technologie SD-WAN ont évolué à partir de solutions réseau antérieures telles que le PPP, le relais de trames et le MPLS. Le PPP était utilisé pour connecter plusieurs réseaux locaux (LAN) avant d'être remplacé par le relais de trames, puis par le MPLS, qui a permis de regrouper des fonctions telles que la voix, la vidéo et les données sur un même réseau IP

Dans les années 2000, le MPLS est devenu populaire pour les réseaux WAN d'entreprise en offrant une meilleure qualité de service (QoS) et une latence réduite par rapport au Frame Relay. En 2013, le SD-WAN est apparu comme une alternative au MPLS, offrant une qualité de service similaire à moindre coût et une facilité de mise à l'échelle. Le SD-WAN peut gérer différents types de connexions et déplacer dynamiquement le trafic vers le meilleur transport disponible, offrant ainsi une redondance et une capacité supérieure à moindre coût. Les solutions SD-WAN sont généralement moins chères que le MPLS, avec des délais d'installation et de livraison plus courts. De plus, les meilleures solutions SD-WAN permettent un provisionnement sans intervention, facilitant ainsi la mise en service des sites sans la nécessité d'experts en réseau ou en sécurité sur place. [30]

2.4 Le fonctionnement du SD-WAN

Le SD-WAN fonctionne en séparant les fonctions du réseau WAN en un plan de contrôle et un ou plusieurs plans de données :

-Le plan de contrôle est le cerveau du SD-WAN, où réside l'intelligence du SD-WAN. Il est chargé de diriger le trafic et de prendre les décisions concernant les itinéraires à emprunter.

-le plan de données assure la connectivité physique à chaque site. Il est responsable du transport des données des applications et des utilisateurs.

L'un des principaux avantages de cette architecture réside dans le fait qu'un seul plan de contrôle logique peut superviser plusieurs plans de données, ce qui permet une gestion centralisée et simplifiée du réseau. [31]

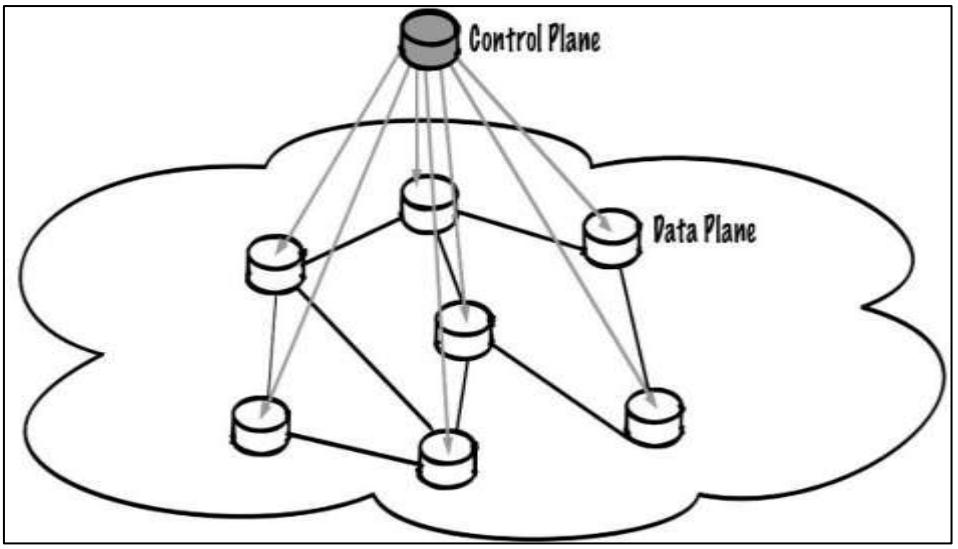


Figure 18 : Fonctionnement du SD-WAN *[32]*

2.5 Avantages de SD-WAN

La technologie SD-WAN offre plusieurs avantages par rapport au réseau traditionnels, notamment :

La réduction des couts liées aux connexions WAN

Le MPLS est coûteux en raison de sa bande passante par rapport à l'Internet public. De plus, l'installation d'une connexion MPLS prend souvent plusieurs semaines ou mois, alors qu'un déploiement SD-WAN similaire peut être réalisé en quelques jours. Cette différence de temps peut représenter un avantage concurrentiel significatif, car dans les affaires, le temps équivaut à de l'argent.

Amélioration des performances du réseau

Avant le SD-WAN, le MPLS était standard pour les réseaux d'entreprise mais ses limitations face au cloud et à la mobilité sont devenues apparentes. Le MPLS crée un effet de "trombone" inefficace pour le trafic Internet ce que SD-WAN résout ce problème en permettant un routage basé sur des politiques et en utilisant la meilleure méthode de transport disponible, ce qui améliore les performances du réseau.

Gestion simplifie du réseau et déploiement rapide

Les SD-WAN offrent une agilité et une flexibilité accrues en acheminant de manière dynamique le trafic sur divers chemins réseau. Cette capacité permet aux organisations de répondre rapidement aux évolutions des conditions du réseau grâce à la gestion centralisée.

Sécurité et la fiabilité du réseau

Le SD-WAN offre une sécurité renforcée grâce au chiffrement des données assurant la confidentialité des informations échangées. Il permet également une segmentation du trafic pour un contrôle plus précis de l'accès aux ressources sensibles. De plus, le SD-WAN intègre des fonctionnalités avancées de pare-feu pour protéger le réseau contre les menaces externes. [33]

2.6 Les types de SD-WAN

Trois architectures SD-WAN courantes comprennent :

1. **SD-WAN basé sur Internet**

   Également connu sous le nom de SD-WAN "à faire soi-même", ce modèle se produit lorsque l'organisation déploie un SD-WAN en utilisant ses propres ressources internes. Le personnel informatique est chargé d'installer les appareils SD-WAN nécessaires, de déployer le logiciel SD-WAN, ainsi que de la maintenance et de la gestion continues du SD-WAN.

2. **Service de télécommunication ou MSP SD-WAN**

   Dans ce modèle, une organisation paie un fournisseur de services pour installer et fournir une connectivité SD-WAN sur ses sites WAN. Le fournisseur fournit le matériel et la main d'œuvre nécessaires, et garantit la disponibilité des services de réseau et de transport requis.

3. **SD-WAN géré en tant que service**

   Ce modèle permet à une organisation d'accéder à une architecture SD-WAN existante via une orchestration logicielle fournie par un fournisseur. Ce SD-WAN réside généralement sur le réseau privé du fournisseur et est souvent proposé sous forme de logiciel en tant que service (SaaS) aux clients. [34]

2.7 Comparaison avec les réseaux WAN traditionnels

Le SD-WAN permet aux sites distants de se connecter plus facilement aux réseaux, aux centres de données et/ou à plusieurs cloud avec une latence plus faible, de meilleures performances et une connectivité plus fiable. La fonction traditionnelle du WAN (réseau étendu) consistait à connecter les utilisateurs de la succursale ou du campus aux applications hébergées sur les serveurs du centre de données. [35]

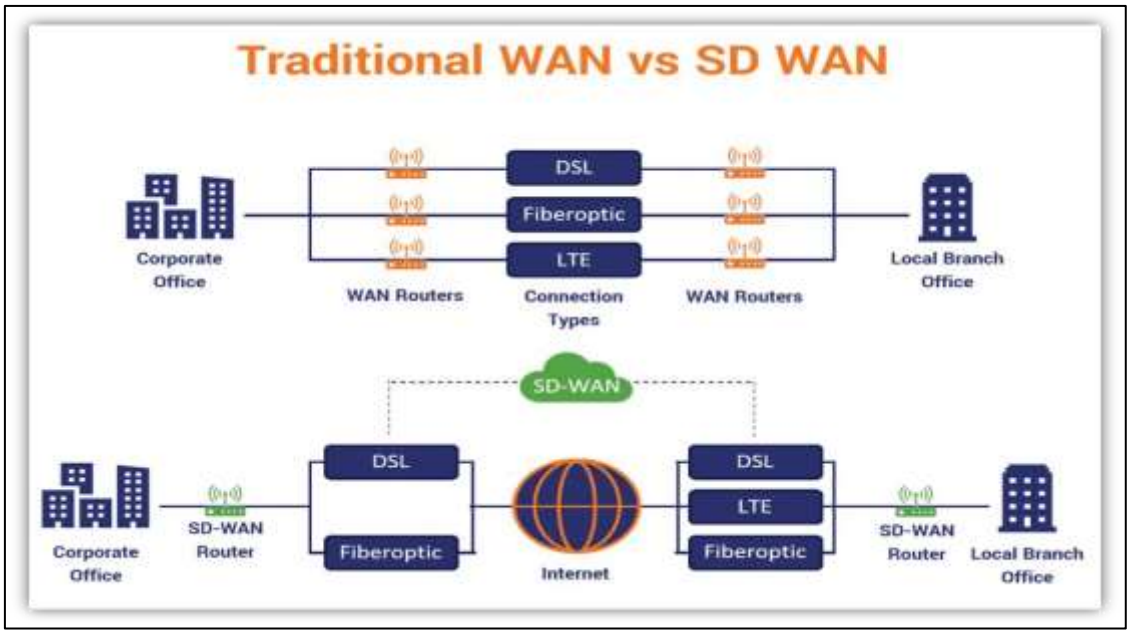


Figure 19 : les réseaux traditionnel (WAN) Vs SD-WAN *[36]*

Voici un tableau comparatif entre de WAN traditionnel et SD-WAN en termes d'infrastructure, de gestion, de couts, de flexibilité, de performance, sécurité et de gestion des applications :

Réseau WAN traditionnels	**Réseau étendue défini par logiciel (SD-WAN)**
Base sur des équipement propriétaire, souvent MPLS	Utilise des liens internet et peut inclure MPLS, ethernet,4G /5G, etc.
Configuration manuelle et individuelle des appareils sur site	Gestion centralise via un contrôleur SD-WAN, permettant une configuration simplifier et une visibilité accrue.
Couteuse en raison de l'investissement matériel.	Peut offrir des économies significatives en utilisant des liens Internet.
Limité en termes de l'évolutivité et changement de configuration.	Plus grande flexibilité grâce à la virtualisation du Réseau et la capacité de configurer dynamiquement les politique de routage.
La sécurité repose sur des dispositifs de sécurité distincts et des tunnel VPN.	Intègre souvent des fonctionnalités de sécurité avancée tel que pare-feu intégré et le chiffrement intégré.
Une faible performance dans les applications cloud car celle-ci doivent passer par un hub intermédiaire avant d'atteindre le cloud.	Il garantit des performances élevées pour les applications cloud en offrant un accès direct à celles hébergées dans le cloud.

Tableau 1: Comparaison entre Réseau WAN traditionnels et SD-WAN *[37]*

2.8 La différence entre MPLS et SD-WAN

Avant de migrer d'une configuration MPLS traditionnelle vers une solution SD-WAN, il est important de prendre en compte plusieurs facteurs.

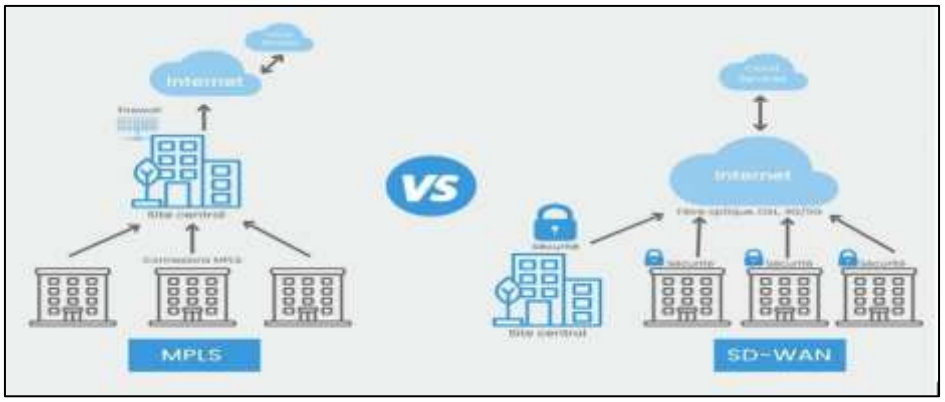


Figure 20: MPLS Vs SD-WAN [38]

Pour mieux comprendre les différences entre le SD-WAN et le MPLS, examinez le tableau ci-dessous qui compare ces deux options :

	SD-WAN	MPLS
Complexité	Moins complexé, et Si la sécurité n'est pas automatiquement intégrée, les équipes ont besoin d'options complémentaires	Plus complexe, le Trafic Internet redirigé vers le centre de données
Visibilité	La visibilité étendue des applications	Le routage des paquets limite la visibilité
Coût	Les services consolidés réduisent considérablement le coût total de possession	Cher à construire et à entretenir
Performances et disponibilité	Permet MPLS, haut débit, LTE pour le haut débit	MPLS offre une bande passante limitée et un point de défaillance unique

Tableau 2: SD-WAN Vs MPLS *[39]*

2.9 Les technologie clé utilisé dans SD-WAN

Les fournisseurs de solutions SD-WAN intègrent plusieurs technologies dans leurs solutions :

Routage basé sur les applications

Les politiques de trafic du réseau SD-WAN sont généralement gérées de manière centralisée, ce qui inclut le routage, la sélection de chemin, la hiérarchisation de la classification du trafic et le filtrage basé sur les profils d'application. La configuration de ces politiques doit tenir compte de toutes les applications métier pour garantir que chacune bénéficie des performances requises sur le réseau SD-WAN.

Sortie internet locale

Bien que le concept de sortie internet locale existait avant le SD-WAN, ce dernier l'a rendu populaire et facile à implémenter. Avec l'adoption massive des services cloud et des applications SaaS, cette tendance s'est renforcée.

La sortie internet locale est un concept simple

Au lieu de diriger tout le trafic vers le datacenter ou la passerelle cloud sécurisée (ou CASB), le trafic à destination d'internet (y compris le trafic des SaaS et des services cloud) utilise une connexion internet locale.

Sur-couche (overlay) et sous-couche (underlay) du SD-WAN

Les routeurs SD-WAN peuvent acheminer le trafic sur plusieurs connexions (MPLS, différents fournisseurs d'accès internet, connexions 4G/5G) en établissant des tunnels VPN. Ces tunnels sont désignés par le terme « overlay » ou sur-couche, tandis que l'infrastructure sous-jacente (les connexions opérateurs elles-mêmes) est désignée par « underlay » ou sous-couche. [40]

2.10 L’évolution récente vers SASE (Secure Access Service Edge)

L’objectif de SASE est la convergence des services SD-WAN, de la sécurité réseau et de l’accès au Cloud dans un modèle de service unique. En ce sens, SASE est l’évolution de SD-WAN. Les concepts sont très récents et sont apparus en aout 2019 avec Gartner dans « The Future of Network Security is in the Cloud.

L'objectif est de continuer l'évolution vers la décentralisation des données vers le Cloud tout en renforçant les aspects sécurité, sur 3 niveaux :

- Pour chaque utilisateur / terminal pour l'accès à Internet.
- Pour la sécurité des serveurs.
- Pour les applications de l'entreprise.

Ainsi, les données doivent être sécurisées de bout end bout : authentification de l'utilisateur, chiffrement au cours du transport et à destination

Les passerelles d'accès Cloud sécurisée (CASB) et Web sécurisée (SWG),

- ZTNA (Zero Trust Network Access) qui permet de gérer l'autorisation d'accès au niveau de l'application et non au niveau de l'accès au réseau comme le propose le VPN
- Les pare-feu de nouvelle génération (NGFW). [28]

2.11 La différence entre SD-WAN et SASE

L'architecture SASE (Secure Access Service Edge) offre une alternative au SD-WAN dans le domaine de l'optimisation des réseaux WAN, tous deux relevant de la catégorie plus large des réseaux définis par logiciel (SDN). Tout comme le SD-WAN centralise la gestion des réseaux WAN dans une couche logicielle abstraite, l'architecture SASE consolide les services de gestion et de sécurité du réseau dans un déploiement basé sur le cloud, se situant plus près ou à la périphérie du réseau.

Tandis que le SD-WAN se concentre principalement sur la connectivité entre les différents sites, un déploiement SASE se concentre davantage sur les points de terminaison du réseau et les appareils qui utilisent ce réseau. [41]

2.12 Cas d'utilisation de SD-WAN

Une solution SD-WAN efficace doit être disponible dans une variété de formats pour répondre aux besoins des data centers de grande envergure, des sites distants, des bureaux distants et même des bureaux à domicile. Elle doit également être disponible sous forme virtuelle pour s'adapter aux environnements cloud.

Bureaux à domicile : Le SD-WAN offre une solution pratique pour les travailleurs à domicile en fournissant un accès distant à la demande et des performances évolutives. Les Appliance SD-WAN de bureau, dotées de connectivité 4G intégrée, garantissent une

connectivité stable et sécurisée, même dans des environnements résidentiels où la bande passante peut être limitée. Cela permet aux employés de rester productifs et de mener à bien leurs activités professionnelles essentielles depuis chez eux.

Sites distants : Les entreprises ayant des sites distants bénéficient du SD-WAN pour simplifier la gestion de leur réseau. Le SD-WAN offre un routage avancé et des hubs on-ramps vers le cloud, réduisant ainsi la dépendance à l'égard de produits autonomes. De plus, le SD-WAN intègre des fonctionnalités de sécurité complètes pour protéger les connexions vers les services cloud et Internet. Cela garantit une connectivité sécurisée et fiable pour tous les sites distants, améliorant ainsi la collaboration et la productivité des équipes réparties géographiquement.

Data centers : Dans les data centers, le SD-WAN assure un accès sécurisé et optimisé aux applications et aux ressources critiques. Les entreprises peuvent déployer des solutions SD-WAN ultra-performantes pour garantir une connectivité fiable, même dans des environnements où les data centers interagissent avec le cloud ou lorsque les applications sont réparties sur plusieurs sites. Cela permet une gestion efficace du trafic et une meilleure utilisation des ressources informatiques.

Cloud multisite : Pour les entreprises utilisant différents environnements cloud, le SD-WAN facilite l'intégration et la gestion de ces environnements. En associant un VPN IPSec avec un pilotage natif des applications et des API programmables, le SD-WAN permet de concevoir des architectures d'intégration cloud efficaces. Cela offre un accès rapide et sécurisé aux applications et aux ressources critiques sur l'ensemble de ces environnements cloud, garantissant ainsi une expérience utilisateur optimale et une utilisation efficace des ressources cloud. [42]

2.13 Les défis liés à SD-WAN

Transition vers SASE : La transition d'un SD-WAN vers une solution SASE peut s'avérer complexe. Cette difficulté découle de la nécessité d'intégrer de nouvelles fonctionnalités de sécurité tout en connectant le SD-WAN à des solutions de sécurité cloud tierces.

Gestion de fournisseurs multiples : Les entreprises utilisant plusieurs fournisseurs SD-WAN peuvent rencontrer des défis lors de la transition vers SASE. Cela inclut la coordination des politiques et des contrôles de sécurité sur l'ensemble du réseau.

Complexité de mise en œuvre et de gestion : La mise en œuvre et la gestion d'un SD-WAN peuvent être complexes, ce qui peut compliquer davantage la transition vers SASE.

Les organisations ayant adopté une approche fragmentée du SD-WAN peuvent être particulièrement confrontées à des difficultés pendant cette transition. [43]

Performance réseau : Les performances du SD-WAN peuvent être affectées par divers facteurs tels que la latence, le manque de bande passante ou des décisions de routage inadéquates. Il est crucial de surveiller et d'optimiser en permanence les performances du réseau pour garantir une connectivité efficace. [40]

Sécurité : Bien que le SD-WAN offre des fonctionnalités de sécurité avancées, telles que le chiffrement du trafic, la segmentation du réseau et les pares-feux intégrés, il peut également introduire de nouveaux vecteurs d'attaque, notamment au niveau des connexions Internet directes. [44]

2.14 Bonnes pratiques SD-WAN

Une mauvaise implémentation du SD-WAN représente un risque majeur pour toute organisation. Afin de garantir un déploiement efficace, il est essentiel de prendre en compte les bonnes pratiques suivantes lors de la conception et de la mise en œuvre du SD-WAN :

Positionnement des appareils SD-WAN : Les routeurs SD-WAN doivent être stratégiquement positionnés pour prendre en charge efficacement les utilisateurs, en minimisant la distance entre les utilisateurs distants et la périphérie du SD-WAN.

Utilisation d'une connectivité réseau de haute qualité : Le SD-WAN optimise les performances en acheminant intelligemment le trafic sur différentes connexions réseau. Pour tirer pleinement parti du SD-WAN, il est crucial d'utiliser une connexion réseau offrant les performances, la latence et la fiabilité requises.

Conception pour l'évolutivité : besoins en bande passante évoluent constamment. Il est donc essentiel d'opter pour une solution SD-WAN évolutive, exploitant les capacités du cloud pour s'adapter aux exigences réseau actuelles et futures**.**

Intégration de la sécurité au réseau : Le SD-WAN n'est pas une solution de sécurité. Il est nécessaire d'intégrer des mesures de sécurité au niveau du réseau pour protéger l'organisation contre les menaces de cybersécurité. [45]

2 .15 Conclusion

Le SD-WAN représente une avancée significative dans l'architecture des réseaux d'entreprise, en offrant une flexibilité, une évolutivité et une rentabilité supérieures par rapport aux solutions WAN traditionnelles. Grâce à une approche logicielle et des fonctionnalités comme le routage dynamique du trafic et une sécurité renforcée, le SD-WAN permet une gestion centralisée, une visibilité accrue et une optimisation des performances réseau. Son adoption permet aux entreprises d'améliorer leur agilité opérationnelle, de renforcer leur compétitivité et de se positionner favorablement dans un environnement numérique en constante évolution.

Dans le chapitre suivant, nous avons étudié l'organisation BMT-spa, en mettant l'accent sur son centre de digitalisation et de numérisation où notre stage s'est déroulé. Nous avons identifié les lacunes du système et formulé des propositions d'amélioration.

Chapitre 3 : présentation l'organisme d'accueil BMT, et étude de l'existence

3.1 Introduction

Dans ce chapitre, nous explorerons l'entreprise d'accueil, Bejaia Méditerranée Terminal (BMT), où s'est déroulé notre stage. Nous examinerons sa structure organisationnelle, les différentes directions qui la composent et ses objectifs. Ensuite, nous nous pencherons sur le centre de digitalisation et de numérisation afin d'analyser le réseau de la BMT. Enfin, nous aborderons la problématique soulevée et la solution envisagée.

3.2 Présentation de l'organisme d'accueil

3.2.1 Historique de la BMT

Dans le plan de développement 2004-2006, entreprise portuaire de Bejaia avait inscrit a l'ordre de jour le besoin d'établir un partenariat pour la conception, le financement, l'exploitation et l'entretient d'un terminal conteneurs port de Bejaia. Après avoir identifié des partenaire potentiel EPB a choisi le groupe PORTEK spécialisé dans la gestion de terminaux des conteneurs, le projet a été présenté au conseil de la participation de l'état (CPE) en février 2004.

La création de Bejaia Mediterranean Terminal (BMT) a vu le jour en mai 2004 après l'accord du projet. Cette initiative novatrice s'est concrétisée par une joint-venture entre l'Entreprise Portuaire de Bejaia (EPB) a 51% et une société singapourienne PORTEK a 49%, démontrant une collaboration fructueuse entre les secteurs public et privé.

En 2011 PORKET systems and Equipment, a été racheté par le groupe japonais MITSUI.

Figure 21: joint-venture de l'EPB et PORTEK *[46]*

3.2.2 Présentation de BMT

BMT – SPA est une jointe venture entre l'Entreprise Portuaire de Bejaia et Portek Systems & Equipment. EPB est l'autorité portuaire qui gère le port de Béjaia. PORTEK Systems and Equipment, une filiale du Groupe PORTEK qui est un opérateur de Terminaux à conteneurs présent dans plusieurs ports dans le monde et également spécialisé dans les équipements portuaires.

L'activité principale de BMT est la gestion et l'exploitation du Terminal à conteneurs. Sa mission principale est de traiter dans les meilleures conditions de délais, de coûts et de sécurité, l'ensemble des opérations qui ont un rapport avec le conteneur. Pour ce faire, elle s'est dotée d'équipements performants et de systèmes informatiques pour le support de la logistique du conteneur afin d'offrir des services de qualité, efficaces et fiables pour assurer une satisfaction totale des clients. [46]

BMT veille au développement et à la gestion de son terminal à conteneurs où l'intégrité, la productivité, l'innovation, la courtoisie, et la sécurité sont de rigueur. BMT est constamment soucieuse des intérêts de ses clients avec lesquels elle partage le souci de performance et de coût. Elle met à la disposition de ses clients des ressources humaines et des moyens nécessaires pour optimiser sa productivité et atteindre des niveaux de performance.

Figure 22 : Activité de BMT

(Ressource externe)

3.2.3 Situation géographique

L'entreprise BMT est idéalement située au sein du port de Bejaia, bénéficiant ainsi d'une position géographique stratégique au centre du Nord-Est de l'Algérie. Cette localisation privilégiée offre de nombreux avantages, notamment sa proximité avec la gare ferroviaire, à quelques minutes seulement de l'aéroport de Bejaia. De plus, elle est parfaitement connectée au réseau routier national, facilitant ainsi le transport efficace des marchandises conteneurisées vers toutes les régions du pays. Avec ses coordonnées GPS (Latitude nord : 36° 45' 14" ; Longitude est : 05° 05' 50"), BMT occupe une position géographique précise qui lui permet d'optimiser ses activités logistiques et de répondre aux besoins de sa clientèle avec efficacité et rapidité.

Figure 23 : Capture sur la situation géographique

(Ressource externe)

3.2.4 Structure et Organigramme de la BMT

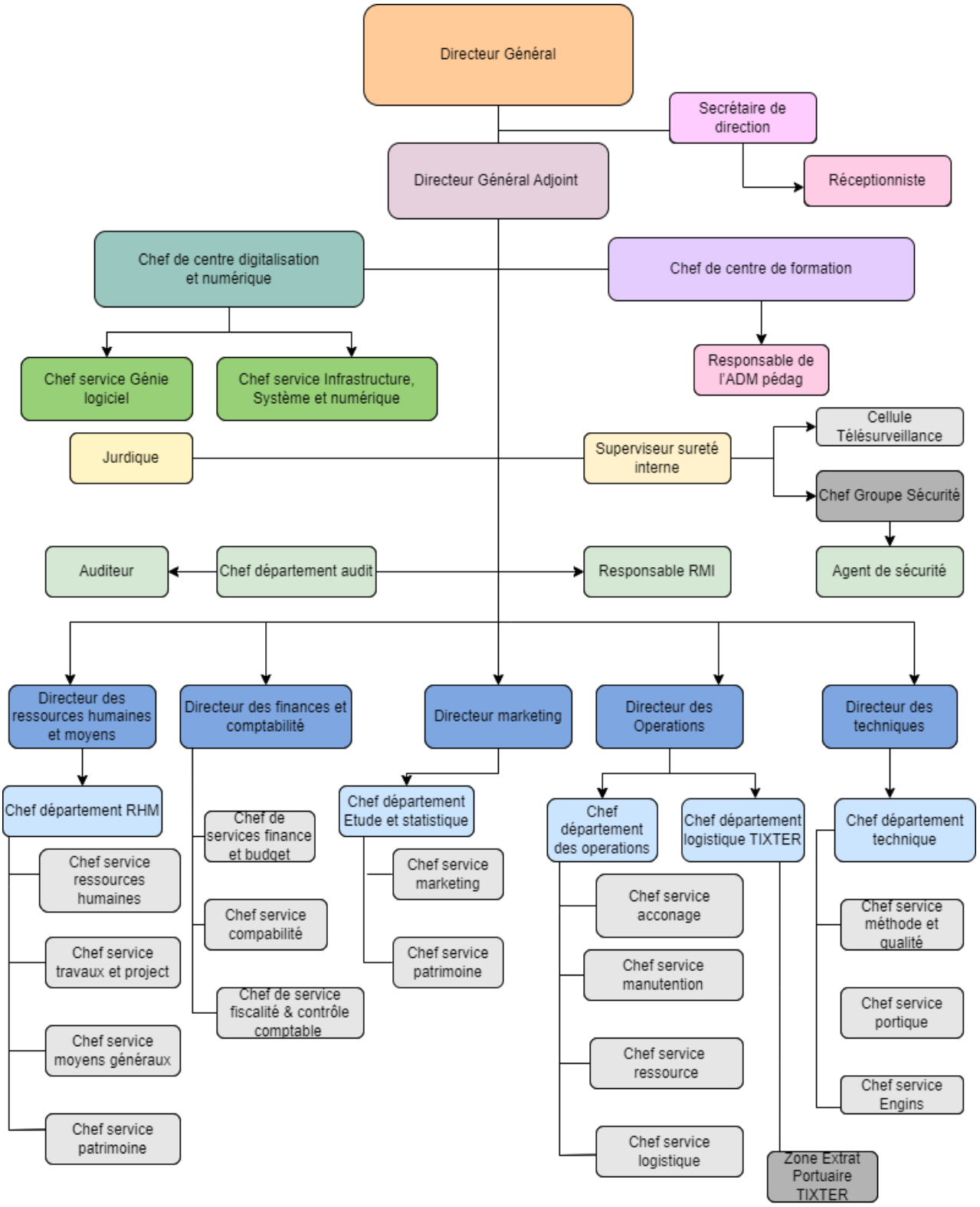


Figure 24 : Organigramme de la BMT

3.2.5 Objectif de BMT

Les objectifs de Bejaia Mediterranean Terminal (BMT) sont les suivants :

Augmenter la productivité en optimisant les processus et en adoptant des méthodes de travail efficaces.

Réduire les coûts d'escale en rationalisant les opérations et en minimisant les temps d'attente des navires.

Assurer la fiabilité de l'information en mettant en place des systèmes de suivi et de communication avancés pour une gestion transparente des données.

Améliorer le service client en offrant une assistance proactive et en répondant aux besoins des clients de manière efficace et rapide.

Protéger les marchandises des clients en garantissant la sécurité et l'intégrité des biens pendant leur traitement et leur entreposage.

Accroître la compétitivité nationale et internationale en se positionnant comme un leader dans le secteur portuaire, capable de rivaliser avec succès sur le marché mondial.

Étendre la présence internationale de BMT en développant des partenariats stratégiques et en renforçant sa visibilité sur les marchés internationaux.

3.2.6 Les Opération de la BMT

Opération de planification

Planification d’escale.

Planification du déchargement et chargement.

Planification du parc à conteneurs.

Planification des ressources : équipes et moyens matériels.

Opération de manutention

La réception des navires porte-conteneurs.

Le chargement /déchargement des conteneur du navire.

Préparation des conteneurs embarquer.

Opération d’acconage

Transfert des centreurs ver la zones d’entreposage.

Transfer des conteneur frigorifiques vers la zone reefers.

Mise a disposition des conteneurs aux services de contrôle aux frontières.

Suivi des restitutions et des mises a quai pour embarquement ou déparquement.

Sécurité Absolut sur la terminale.

Suivi des livraison et dépotage.

3.3 Présentation de service d'accueil

3.3.1 Présentation et organisation

Lors de sa création, le service informatique était intégré à la direction marketing. Quelques années plus tard, l'entreprise a établi un département informatique distinct de la direction marketing, comprenant deux divisions : la section d'étude et développement et la section d'exploitation.

En 2021, ce département informatique a été transformé en un centre de digitalisation et de numérisation, constitué de deux services distincts :

Service génie logiciel.

Service infrastructure, système et numérique.

Le centre de digitalisation et de numérisation, relevant de la direction générale, fournit aux acteurs de BMT les ressources informatiques nécessaires (matériels, logiciels) pour mettre en place le système d'information et gérer les ressources informatiques de l'entreprise. De plus, il assure la maintenance du parc informatique et développe de nouvelles applications pour les différentes structures.

3.3.2 Mission et objectives

La mission principale des deux services de centre digitalisation et numérique :

a) **Service génie logiciel**

Etude, mise en place et développement des application informatique.

Maintenance des logiciels de gestion existant.

Garantir l'évolution de système informatique et suivre l'évolution des applications de gestion.

Sauvegardé et contrôle des données de l'entreprise.

Administration des serveurs des messagerie et du site web.

Sécurité des systèmes information.

b) **Service d'infrastructure système et numérique**

Déploiement et actualisation des système d'exploitation sur les équipements informatique.

Garantir la mise en place des nouveaux systèmes ou divisions actualisées.

Assure le bon fonctionnement des systèmes informatiques et effectue la maintenance des équipements.

Gère le réseau informatique, en assure l'évolution et l'optimisation.

Fournit les éléments nécessaires à la sécurité des données de l'entreprise.

Garantit la qualité de service, en optimisant les performances informatiques et en assurant un haut taux de disponibilité des applications et des systèmes d'exploitation.

Administre l'infrastructure logicielle en surveillant les performances et en apportant les Solutions correctives nécessaires.

3.4 Etude de l'existant

3.4.1 Présentation de réseau de BMT

Le réseau de BMT est un réseau Ethernet à topologie en étoile. Pour la diffusion de données, il utilise le mode poste à poste avec des liaisons point à point, préférant la fibre optique comme norme de câblage, offrant une vitesse de 30 Mbit/s, en plus d'une connexion internet ADSL. Il repose sur la redondance des équipements, permettant une bascule manuelle en cas de panne, assurant ainsi une synchronisation en temps réel. le réseau de BMT est bien équipé pour répondre aux besoins de ses utilisateurs.

3.4.2 Infrastructure réseau

L'entreprise générale dispose de deux sites physiques : la BMT, située au niveau de port de Bejaia et la ZEP (Zone Extra Portuaire) sur la rue d'irriyahen Bejaia. Connecté via un VPN et des lignes spécialisées privées, bénéficiant ainsi d'une adresse IP fixe.

Voici la conception de l'infrastructure réseau du site BMT, localisé à Béjaïa.

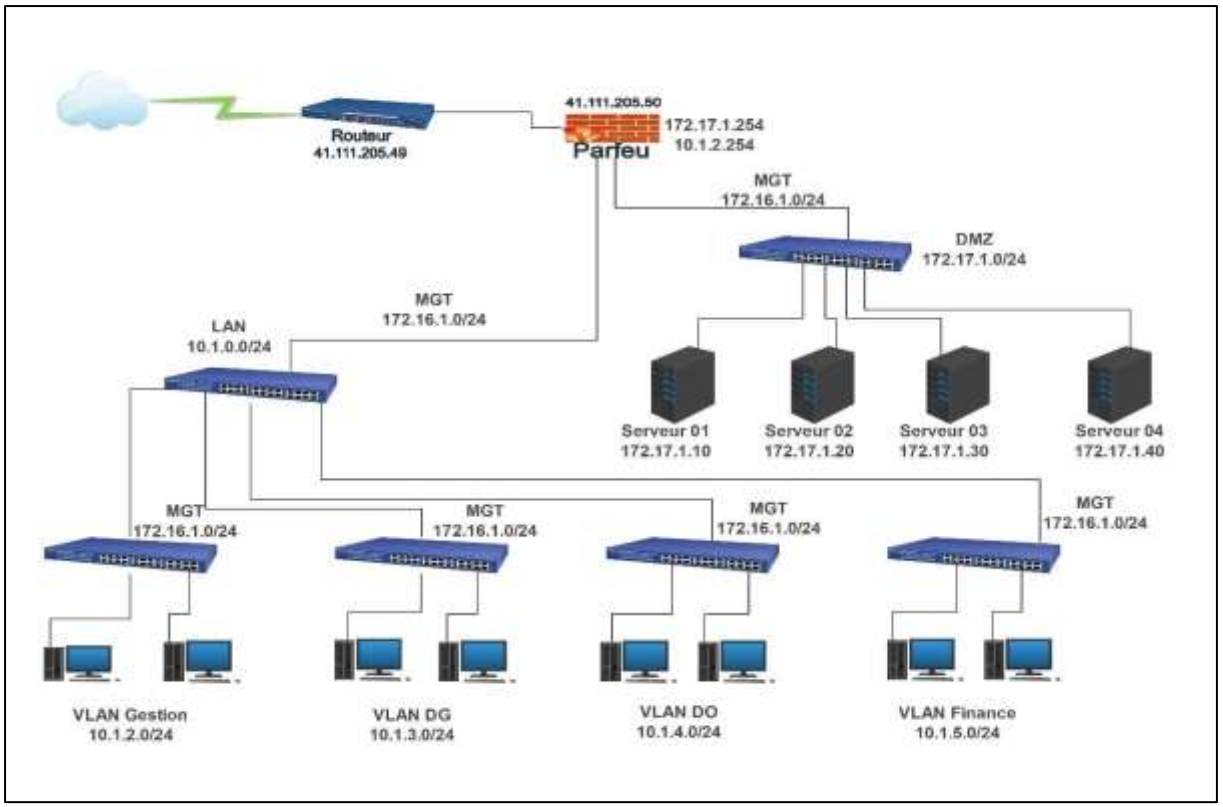


Figure 25: l'infrastructure BMT

3.4.3 Parc informatique BMT

Nom d'équipement	Model	Caractéristique
Pare-feu	Fortinet Fortigate 100F	-Débit : 20 Gbps -Débit de protection contre les menaces : 700 Mbps-1Gbps -Débit VPN : 11 ,5 Gbps -Fréquence : 5 GHz
Commutateur	Cisco SG200-26	-Ram : 128 Mo -Mémoire Flash : 16 MO -Débit de transfert de données : 52 Gbps
Serveur	HP Proliant DL380P Génération 10	- Famille de processeurs : Intel® Xeon 41105. -alimentation électrique : 500 Watts - Contrôleur réseau : Adaptateur Ethernet HPE 1 Go 331i 4 ports ETH Gigabit 10/10/1000 Mbit/S

3.5 Présentation de projet à réaliser

La décision d'envisager l'adoption de la solution SD-WAN sur le réseau de l'entreprise découle d'une analyse approfondie des défis rencontrés par l'infrastructure réseau existante. Face à une croissance continue de l'entreprise et à l'évolution rapide des exigences en matière

de connectivité et de performances réseau, il est devenu impératif de trouver une solution qui puisse répondre de manière efficace et proactive aux besoins actuels et futurs de l'entreprise.

3.5.1 Problématique

L'étude de l'infrastructure réseau de la BMT nous a permet de découvrir des lacunes et des manques qui peuvent inciter à envisager l'utilisation de la solution SD-WAN pour les améliorer, comprennent :

Performance insuffisante : l'infrastructure réseau actuelle ne parvient pas à fournir les performances nécessaires pour prendre en charge les applications critiques de l'entreprise, telles que la voix sur IP (VoIP) ou les applications métier gourmandes en bande passante.

Manque de redondance et de résilience : Si l'infrastructure réseau actuelle ne dispose pas de mécanismes adéquats pour assurer la redondance et la résilience en cas de panne de lien.

Sécurité insuffisante : la sécurité du réseau est une préoccupation majeure et que l'infrastructure actuelle ne fournit pas une protection adéquate contre les menaces, SD-WAN peut être utilisé pour intégrer des fonctionnalités de sécurité avancées, telles que le chiffrement des données, les pares-feux intégrés et la détection des intrusions.

Absence d'une connectivités fiable sécurisé entre les deux sites de l'entreprise BMT pour avoir l'accès à distance.

3.5.2 Solution proposée

Implémentation de La solution SD-WAN de Fortigate offre une approche complète pour répondre aux défis actuels des réseaux d'entreprise en consolidant les connexions WAN, en utilisant des algorithmes intelligents pour optimiser le routage du trafic, en intégrant des fonctionnalités d'optimisation du trafic et de sécurité avancée, et en permettant une gestion centralisée via une console unique. En adoptant cette solution, les entreprises peuvent améliorer la connectivité, accroître les performances des applications, réduire les coûts opérationnels et garantir la sécurité des données, le tout avec une gestion simplifiée et efficace de leur infrastructure réseau.

Pour implémenter cette solution en a mise en œuvre les actions suivantes :

Configuration des VLAN sur le réseau LAN de l'entreprise afin de diviser le réseau en plusieurs sous-réseaux, ce qui permettra d'ajouter un niveau de sécurité et de simplifier la gestion des postes de travail.

Création d'une DMZ pour regrouper tous les serveurs accessibles depuis l'extérieur, ce qui contribuera à améliorer la sécurité globale du réseau.

Configuration des pare-feu et mise en place d'une zone de contrôle SD-WAN incluant deux tunnels VPN IPsec reliant les deux sites de BMT. Cette zone permettra de gérer la tolérance aux pannes et la redondance et pour garantir une connexion fiable et sécurisée.

Mise en place d'une table de filtrage au niveau de chaque pare-feu pour contrôler l'accès au réseau, assurant ainsi une sécurité renforcée.

Surveillance et la supervision continue du réseau à l'aide de performance SLAs de SD-WAN qui permet le monitoring des liens.

Nouvelle architecture proposée

La figure ci-dessous représente une nouvelle architecture améliorée du réseau de l'entreprise BMT, que nous allons configurer dans la section suivante.

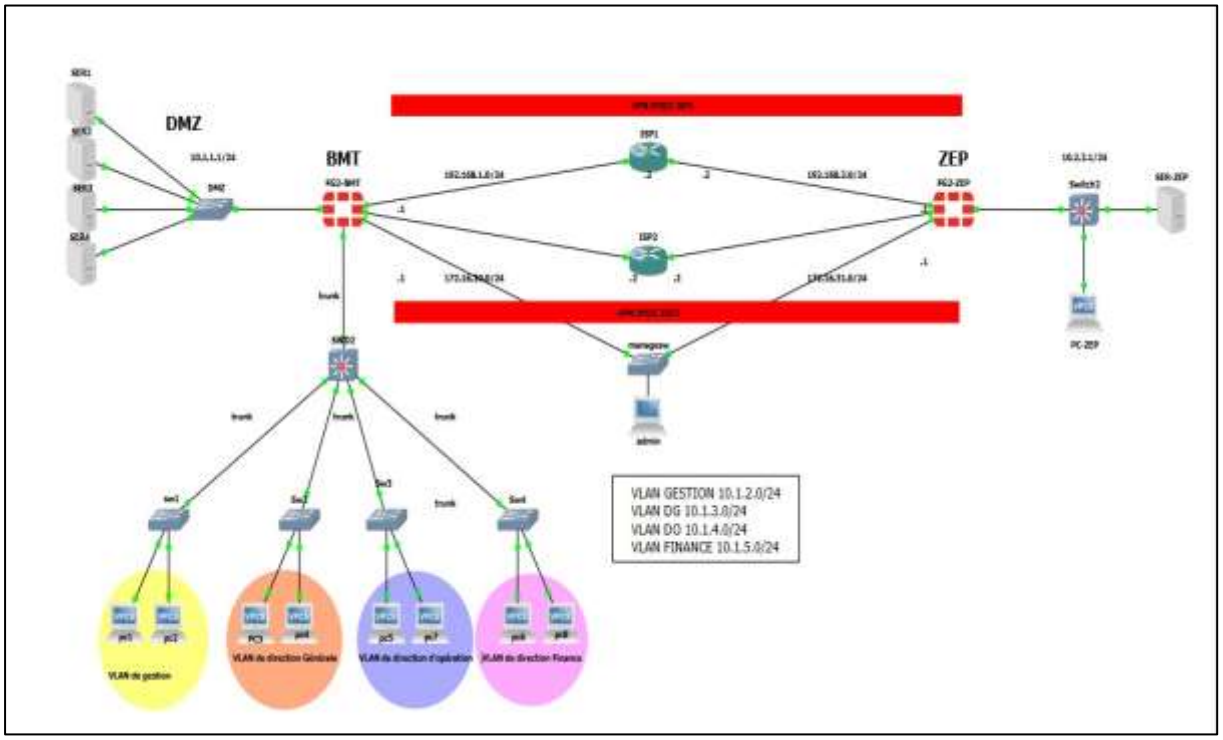


Figure 26 : Nouvelle architecture proposé

3.6 Conclusion

Dans ce chapitre, nous avons présenté l'organisation BMT-spa, en détaillant ses objectifs, sa structure et le fonctionnement de ses différentes directions. Nous avons particulièrement examiné les missions du centre de digitalisation et de numérisation, où s'est déroulé notre stage, dans le but de mieux appréhender le réseau de la BMT, son architecture, sa construction et les rôles de ses diverses entités. Cette analyse nous a permis d'identifier les lacunes et les points faibles du système. En étudiant ces lacunes, nous avons élaboré des propositions d'amélioration pour les corriger. Le prochain chapitre sera dédié à la description et à la mise en œuvre des solutions proposées, notamment l'installation du matériel et des logiciels, ainsi que la configuration des équipements concernés.

Chapitre 4 :
Réalisation et simulation

4.1 Introduction

Dans ce chapitre, nous entrons dans la phase concrète de notre projet de fin d'études, où nous utiliserons les outils GNS3, VMware et le pare-feu Fortigate pour mettre en place une solution SD-WAN répondant aux besoins futurs de l'entreprise BMT. Nous aborderons ici les détails de la simulation et de la mise en œuvre de cette solution, en mettant l'accent sur les étapes clés de configuration et les tests effectués pour garantir son efficacité. Cette partie sera cruciale pour illustrer la viabilité et la pertinence de notre proposition d'amélioration de l'architecture réseau du BMT.

4.2 Présentation de l'environnement de travail

4.2.1 Présentation des logiciels utilisées

VMware Workstation

VMware Workstation est une application de virtualisation qui permet aux utilisateurs de créer et de gérer plusieurs machines virtuelles sur un même ordinateur physique. Ces machines virtuelles peuvent exécuter différents systèmes d'exploitation simultanément, tels que Windows, Linux, macOS, et d'autres.

Figure 27: VMware Workstation

Graphical Network Simulator-3

GNS3 est une abréviation pour "Graphical Network Simulator-3", qui est un logiciel open source utilisé pour la simulation et l'émulation de réseaux informatiques. Avec GNS3, les utilisateurs peuvent créer des topologies réseau virtuelles en utilisant des routeurs, des commutateurs et d'autres équipements réseau virtuels.

Ce logiciel offre une interface graphique conviviale qui facilite la conception, la configuration et la gestion de réseaux complexes. Il est largement utilisé par les professionnels de

l'informatique, les étudiants et les passionnés de réseautage pour tester et résoudre les problèmes de configuration, simuler des scénarios, et apprendre les concepts de réseaux informatiques.

Figure 28: Graphical Network Simulator-3.

4.2.2 Présentation des équipements utilisés

Routeurs : Les routeurs sont des dispositifs réseau de la couche 3 du modèle OSI qui acheminent le trafic entre différents réseaux en fonction des adresses IP et des tables de routage.

Commutateurs : Les commutateurs, également connus sous le nom de switch, sont des dispositifs réseau qui permettent de connecter plusieurs périphériques sur un même réseau local et de transférer des données entre eux en utilisant des adresses MAC.

Firewalls : Les pare-feu sont des dispositifs de sécurité réseau qui contrôlent et filtrent le trafic entrant et sortant d'un réseau en fonction de règles de sécurité prédéfinies.

Serveur : est un ordinateur ou un dispositif réseau dédié à la fourniture de services, de ressources ou de fonctionnalités à d'autres périphériques, généralement appelés clients, au sein d'un réseau informatique. Les serveurs sont conçus pour répondre aux demandes des clients et fournir des données, des applications, des fichiers, des services ou d'autres ressources réseau.

IOS Cisco, connu sous le nom d'Internetwork Operating System, est un système d'exploitation propriétaire développé par Cisco et largement utilisé sur la plupart de ses équipements. Il propose une variété de fonctionnalités pour la gestion des réseaux, y compris le routage, la commutation et l'interconnexion des différents composants du réseau.

4.3 Table d'adressages

4.3.1 La table d'adressage VLANS

Nom du VLAN	ID du vlan	Adresse IP
Vlan de gestion	2	10.1.2.1/24
Vlan de direction générale (DG)	3	10.1.2.2/24
Vlan d'opération (DO)	4	10.1.2.3/24
Vlan du finance	5	10.1.2.4/24

Tableau 3: table d'adressage des VLANs

4.3.2 La table d'adressage d'équipement

Les équipement	Les interfaces réseaux	Adresse IP
Routeur ISP1	Ethernet 0/0 Ethernet 0/1	192.168.1.2/24 192.168.2.2/24
Routeur ISP2	Ethernet 0/0 Ethernet 0/1	172.16.30.2/24 172.16.31.2/24
Fortigate BMT	Port1 Port 2 Port 3 Port 7 Port 10	 192.168.1.1/24 172.16.30.1/24 10.1.1.1/24 192.168.11.101/24
Fortigate Irriyahen (ZEP)	Port1 Port 2 Port 3 Port 10	192.168.2.1/24 172.16.31.1/24 192.168.11.100/24 10.2.2.1/24

Tableau 4: table d'adressage d'équipement

4.3.3 La table d'adressage inter-vlan

Réseaux LAN

Dans notre configuration, nous associons les VLANs 2, 3, 4 et 5 à l'interface port 1 du pare-feu Fortigate. Cette association permet de créer des zones logiques distinctes sur le réseau, où chaque VLAN représente un segment isolé avec ses propres règles de communication et de sécurité.

Pour configurer les inter-VLANs dans un pare-feu Fortigate, la première étape consiste à créer une nouvelle interface correspondant au nom du VLAN souhaité. Ensuite, on attribue ces interfaces à une zone spécifique.

Cette figure présente les étapes nécessaires pour réaliser la configuration :

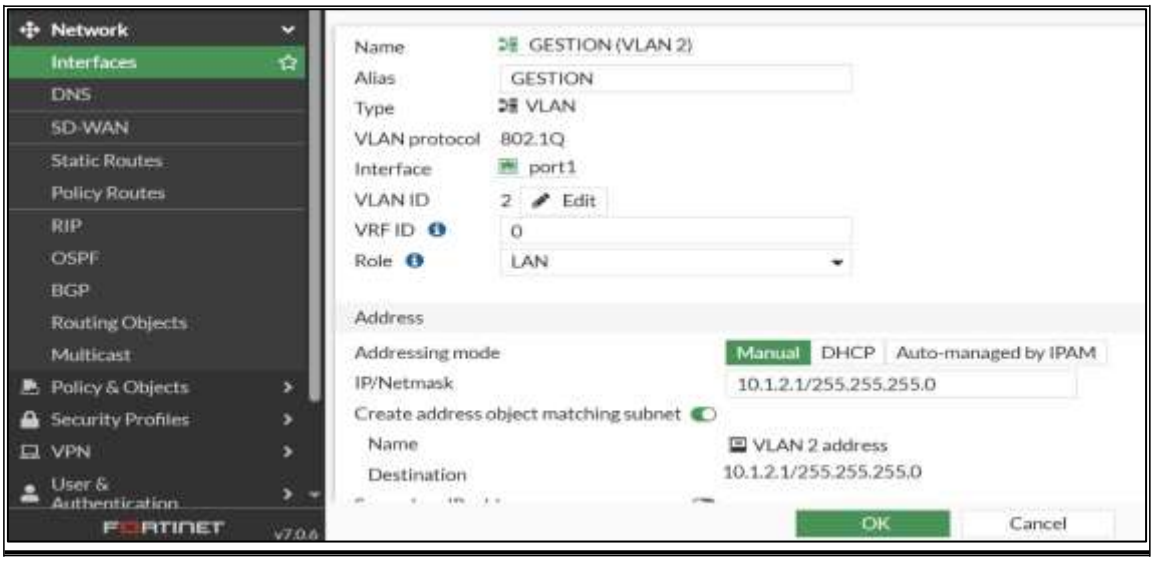


Figure 29: Création de VLAN2 GESTION

Figure 30: association des VLANs a la zone INTER-VLAN .

4.4 Configuration des réseaux LAN

4.4.1 Configuration des VLAN

Configurations des switches en mode trunk

La configuration en mode trunk d'un switch de distribution permet de définir les ports capables de transporter le trafic de plusieurs VLANs. Cette configuration est essentielle pour interconnecter efficacement des switches et permettre le passage transparent des données entre différents réseaux locaux virtuels (VLANs).

Configuration de switch de distribution en mode trunk

```
SWD1 (config)# interface range ethernet 3/0-3 ,ethernet 0/1
SWD1(config-if-range)# switchport trunk allowed vlan 2,3,4,5,99
SW1 (config-if-range)# switchport trunk native vlan 99
```

```
SWD1 (config-if-range)# switchport trunk encapsulation dot1q
SWD1 (config-if-range)# switchport mode trunk
SWD1 (config-if-range)# exite
```

Configuration de Switch d'accè s en mode trunk

```
SW1 (config)# interface range ethernet 3/3
SW1(config-if-range)# switchport trunk allowed vlan 2,3,4,5 ,99
SW1 (config-if-range)# switchport trunk native vlan 99
SW1 (config-if-range)# switchport trunk encapsulation dot1q
SW1 (config-if-range)# switchport mode trunk
SW1 (config-if-range)# exite
```

4.4.2 Activation de protocole VTP

L'activation du protocole VTP sur un switch permet de faciliter la gestion des VLANs.

Le serveur VTP propage et synchronise les informations de configuration des VLANs dans un domaine VTP, tandis que le client VTP reçoit et met à jour ces informations en fonction des modifications apportées par le serveur.

La configuration du switch de distribution au tant que serveur VTP

```
SWD1 (config)# vtp mode server
SWD1 (config)# vtp domain bmt
Domain name already set to bmt
SWD1 (config)# vtp password cisco
Password already set to cisco
SWD1 (config)# vtp version2
 SWD1 (config)# vtp pruning
```

```
SWD2#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : bmt
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0200
Configuration last modified by 0.0.0.0 at 5-23-24 14:43:07
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
```

Configuration du switch de distribution au tant que client VTP

```
SWD1 (config)# vtp mode client
 Setting device to VTP Client mode for VLANS.
SWD1 (config)# vtp domain bmt
 Domain name already set to bmt
SWD1 (config)# vtp password cisco
Password already set to cisco
SWD1 (config)# vtp version2
 SWD1 (config)# vtp pruning
```

```
sw1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : bmt
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0400
Configuration last modified by 0.0.0.0 at 5-23-24 14:43:07

Feature VLAN:
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 1005
```

Création des VLANS sur un switch de distribution

```
SWD1 (config)# vlan 2
 SWD1 (config-vlan)# name gestion
 SWD1 (config-vlan)# vlan 3
SWD1 (config-vlan)# name DG
SWD1 (config-vlan)# vlan 4
 SWD1 (config-vlan)# name DO
SWD1 (config-vlan)# vlan 5
SWD1 (config-vlan)# name finance
```

```
SWD2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et1/0, Et1/1, Et1/2
                                                Et1/3, Et2/0, Et2/1, Et2/2
                                                Et2/3
2    GESTION                          active
3    DG                               active
4    DO                               active
5    FINANCE                          active
```

Affectation des ports de sw it ch d'ac cès au x VL AN S co r r espo nda nt :

Dans notre cas, où nous avons les VLANs 2, 3, 4 et 5, le mode access sur le switch est utilisé pour connecter les PC et autres appareils réseau à des VLANs spécifiques. Chaque port du switch est configuré en mode access et associé à un seul VLAN.

```
SW1 (config)# interface ethernet 3/1-2
SW1(config-if-range)# switchport mode access
SW1 (config-if-range)# switchport access vlan 2
SW1 (config-if-range)# exite
```

```
sw1#Show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/1, Et0/2, Et0/3, Et1/0
                                                Et1/1, Et1/2, Et1/3, Et2/0
                                                Et2/1, Et2/2, Et2/3, Et3/0
2    GESTION                          active    Et3/1, Et3/2
3    DG                               active
4    DO                               active
5    FINANCE                          active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
```

4.4.3 Configuration des routeur ISP1 ET ISP2

ISP1

```
ISP1 (config-if)# interface ethernet 0/0
ISP1 (config-if)# no shutdown
ISP1 (config-if)# ip address 192.168.1.2 255.255.255.0
ISP1 (config-if)# interface ethernet 0/1
ISP1 (config-if)# no shutdown
ISP1 (config-if)# ip address 192.168.2.2 255.255.255.0
```

```
ISP1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            192.168.1.2     YES NVRAM  up                    up
Ethernet0/1            192.168.2.2     YES NVRAM  up                    up
```

ISP2

```
ISP2 (config-if)# interface ethernet 0/0
ISP2 (config-if)# no shutdown
ISP2 (config-if)# ip address 172.16.30.2 255.255.255.0
ISP2 (config-if)# interface ethernet 0/1
ISP2 (config-if)# no shutdown
ISP2(config-if)# ip address 172.16.31.2 255.255.255.0
```

L'affichage les interfaces criées :

```
FAI-2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            172.16.30.2     YES NVRAM  up                    up
Ethernet0/1            172.16.31.2     YES NVRAM  up                    up
```

4.4.4 Configuration des pare-feu Fortigate Bejaia et Fortigate Irriyahen

4.4.4.1 Configuration d'accès au pare-feu

Pour accéder au pare-feu, nous allons intégrer un cloud qui sera configuré comme un administrateur « Admin » de système pour fournir l'accès au pare-feu. Ce cloud sera configuré sur l'interface VMnet19 avec l'adresse 192.168.11.0/24

Voici quelques photos illustrant cette configuration.

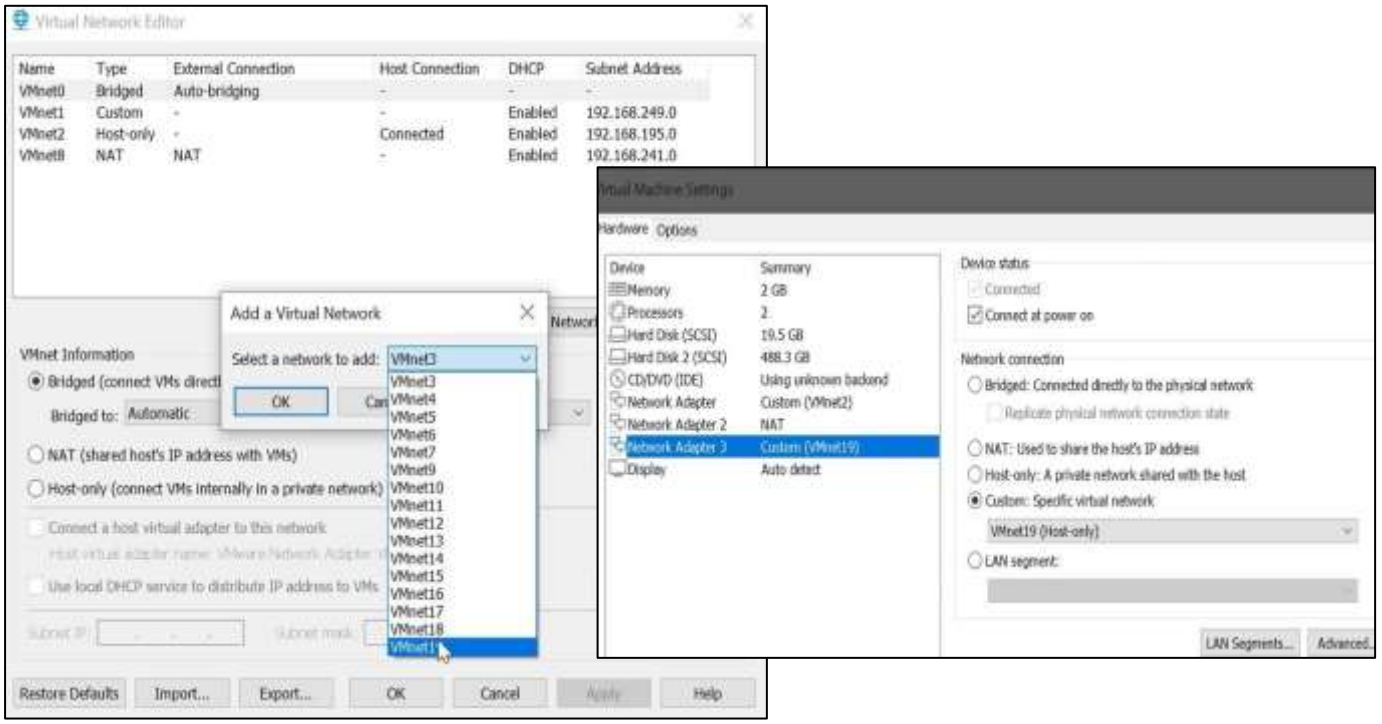
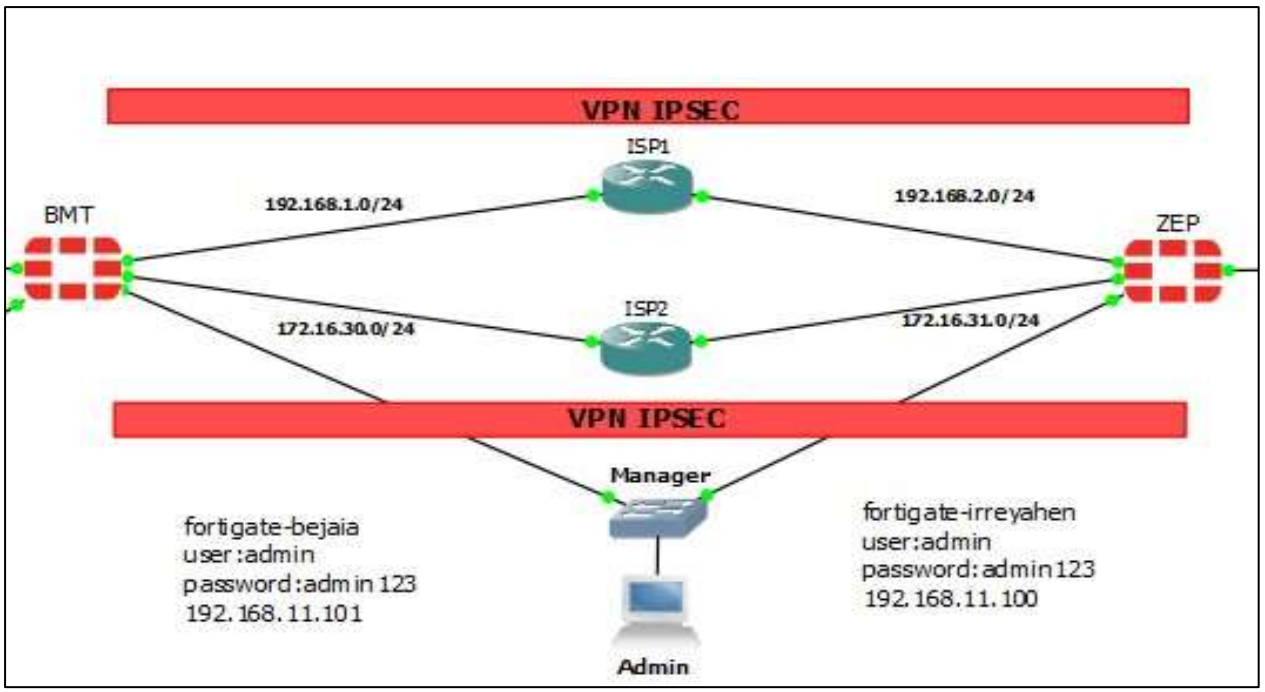
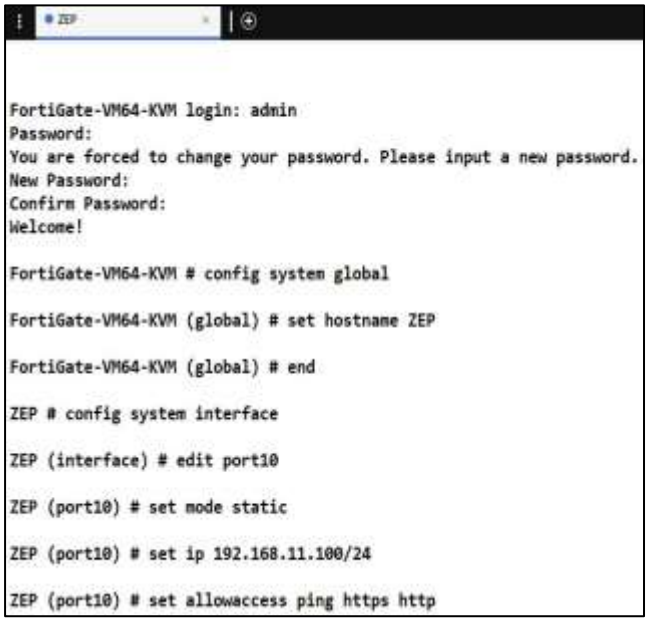


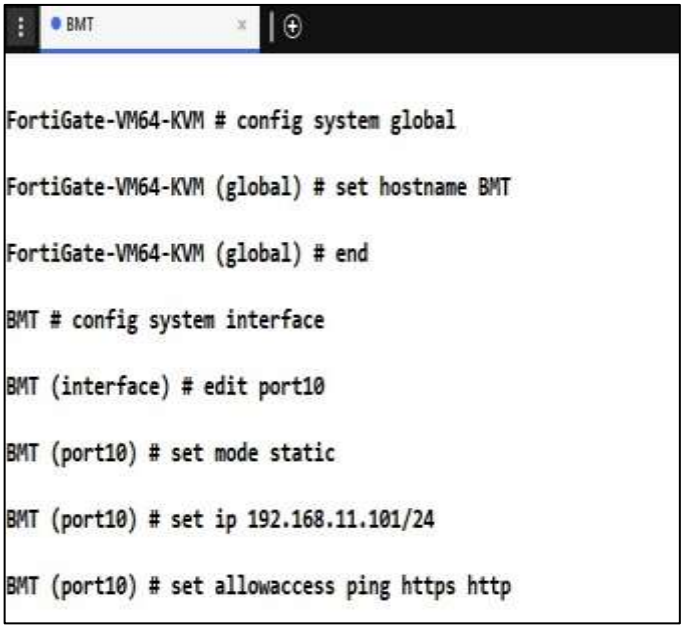
Figure 31: l'ajoute de VMnet19





```
FortiGate-VM64-KVM login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome!

FortiGate-VM64-KVM # config system global

FortiGate-VM64-KVM (global) # set hostname ZEP

FortiGate-VM64-KVM (global) # end

ZEP # config system interface

ZEP (interface) # edit port10

ZEP (port10) # set mode static

ZEP (port10) # set ip 192.168.11.100/24

ZEP (port10) # set allowaccess ping https http
```

Figure 33: Configuration de l'accès au Fortigate d'irriyahen



```
FortiGate-VM64-KVM # config system global

FortiGate-VM64-KVM (global) # set hostname BMT

FortiGate-VM64-KVM (global) # end

BMT # config system interface

BMT (interface) # edit port10

BMT (port10) # set mode static

BMT (port10) # set ip 192.168.11.101/24

BMT (port10) # set allowaccess ping https http
```

Figure 32: Configuration de l'accès au Fortigate de béjaia

Maintenant, l'accès au pare-feu est possible via le navigateur Google Chrome. Nous entrons l'adresse du pare-feu, puis le navigateur charge la page de connexion de Fortigate. Nous nous

connectons ensuite en utilisant le nom d'utilisateur "admin" et le mot de passe configuré précédemment.

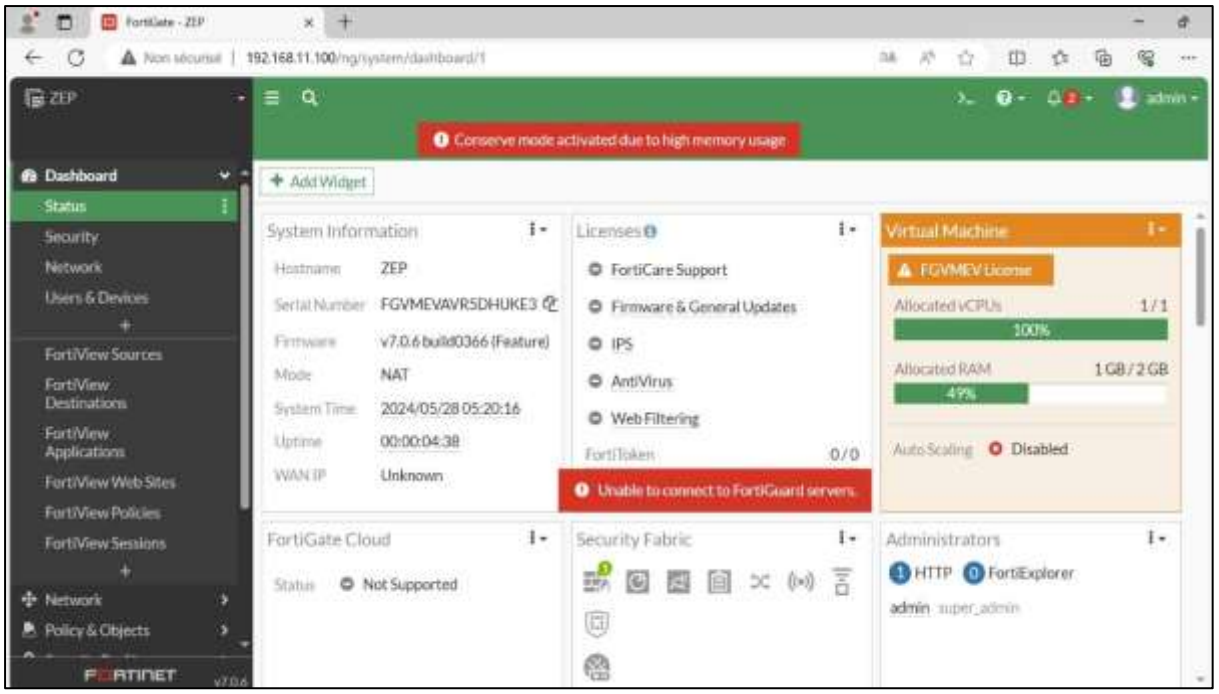


Figure 34: Interface d'accueil du pare-feu Fortigate

4.4.4.2 Configuration les interfaces des pares-feux

Voici les étapes simples pour créer une nouvelle interface dans un pare-feu Fortigate :

Ouvrir un navigateur Web et entrer l'adresse IP du pare-feu dans la barre d'adresse, par exemple, 192.168.11.100.

Accéder à la configuration réseau : Une fois connecté, rechercher l'onglet ou le menu "Network" ou "Interfaces".

Ajouter une nouvelle interface : Chercher l'option pour ajouter une nouvelle interface "create new" et cliquer dessus.

Configurer les détails de l'interface : Spécifier un nom pour l'interface (alias), son type (LAN, WAN, ou DMZ), son adresse IP, et son masque de sous-réseau, ainsi que permettre certains services essentiels comme le ping, HTTP et HTTPS.

Valider et enregistrer les configurations : Après avoir configuré l'interface, assurer de valider les paramètres et enregistrer les modifications.

Voici les étapes de configuration les interfaces de pare-feu :

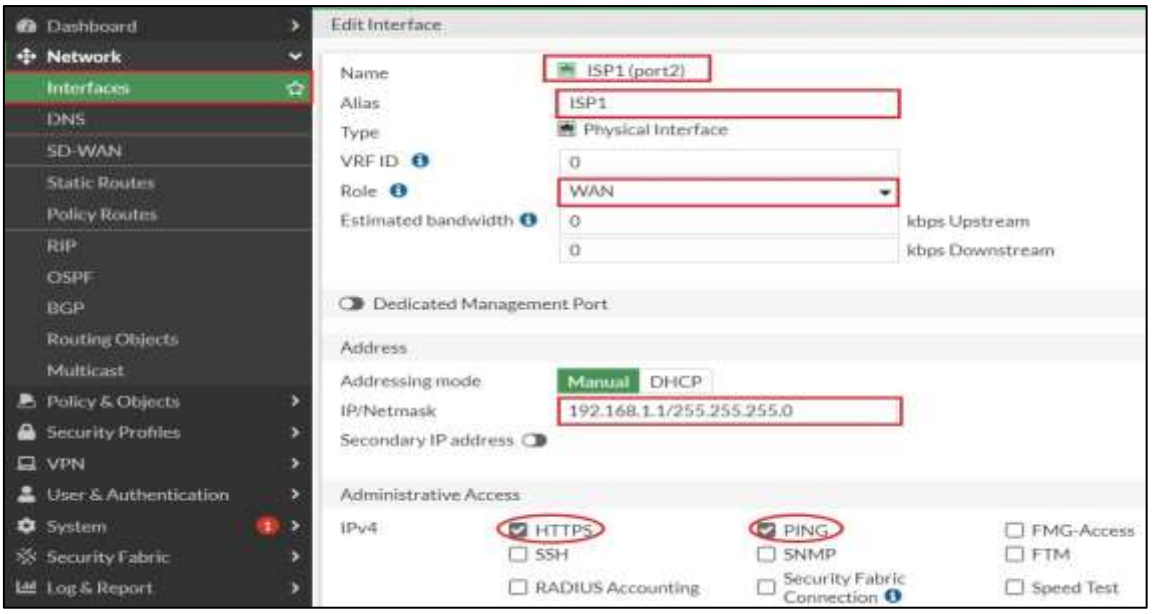


Figure 35: Configuration des interfaces de pare-feu

4.4.4.3 Configuration le routage statique

Le routage statique implique la configuration manuelle des chemins réseau pour diriger le trafic vers des destinations spécifiques, offrant un contrôle précis sur le chemin emprunté par le trafic sans dépôt

Figure 36 : Configuration de routage statique

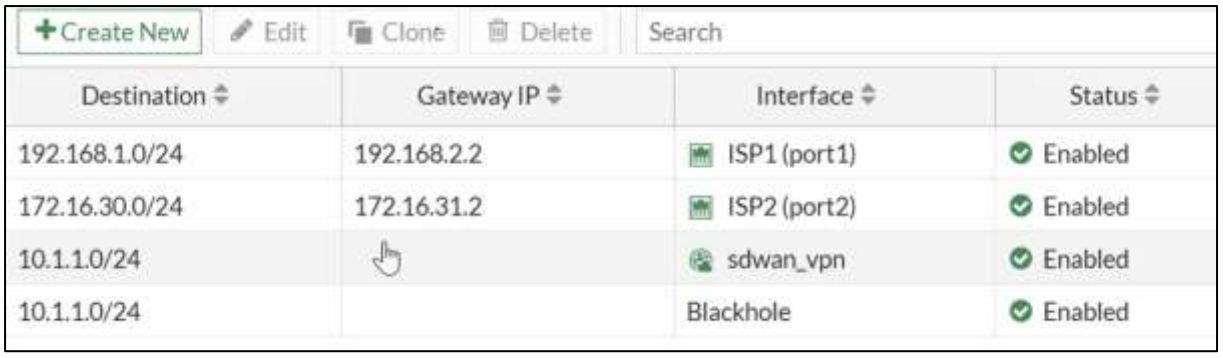


Figure 37 : la table de routage ZEP

4.4.5 Configuration de la solution SD-WAN de Fortinet

Création d'une Zone SD- WAN

La zone SD-WAN dans un pare-feu Fortigate optimise le routage du trafic réseau, améliorant ainsi : les performances, la résilience et la sécurité des connexions WAN. Elle dirige intelligemment le trafic sur les chemins les plus rapides et fiables, assure une redondance en cas de panne, et intègre des fonctionnalités de sécurité avancées pour protéger le flux de données.

Pour créer une nouvelle zone SD-WAN, suivez ces étapes :

Cliquer sur "Network", puis sélectionner "SD-WAN". Cliquer sur "Create new", puis sélectionner "SD-WAN zone".

Entrer un nom pour la nouvelle zone.

Ajouter les membres nécessaires à la zone si des membres SD-WAN existent déjà.

Vous pouvez également ajouter des membres à la zone après sa création en la modifiant, ou lors de la création ou de la modification du membre.

Figure 38: Création de la Zone SD-WAN

Création membres SD-WAN (sd-wan member)

Les interfaces SD-WAN, souvent désignées comme des membres, sont les ports et interfaces à travers lesquels le trafic est acheminé. Au minimum, une interface doit être configurée pour que le SD-WAN soit opérationnel, jusqu'à 255 interfaces membres peuvent être configurées pour répondre aux besoins de connectivité.

Pour créer un membre d'interface SD-WAN via l'interface graphique, suivez ces étapes :

Accéder à l'onglet "Network", puis sélectionner "SD-WAN".

Cliquer sur "Create new" et choisir "SD-WAN member".

Choisir une interface pour le membre.

Laisser l'interface non spécifiée pour sélection ultérieure, ou cliquer sur "VPN" pour créer un VPN IPsec pour ce membre SD-WAN.

Sélectionner la zone SD-WAN à laquelle le membre sera affilié. Vous pouvez également déplacer un membre vers une autre zone à tout moment.

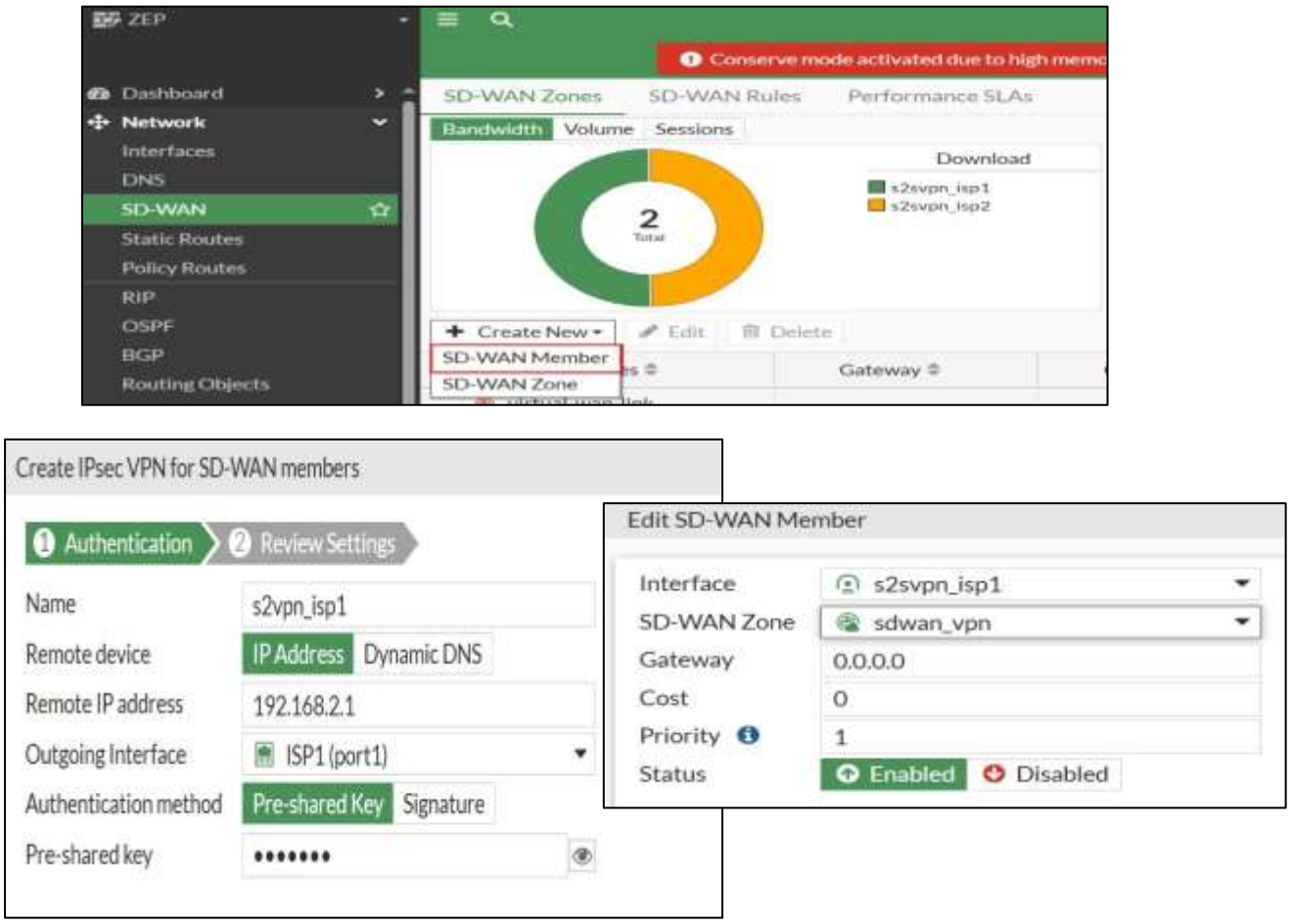


Figure 39: Création membres SD-WAN

Le Rules de SD-WAN

Les règles SD-WAN, parfois appelées services, sont utilisées pour réguler la sélection des chemins de transmission. Elles permettent de diriger de manière dynamique un trafic spécifique vers le meilleur lien disponible ou vers un itinéraire défini. Ces règles peuvent être configurées selon cinq modes différents :

Mode automatique : Les interfaces se voient attribuer une priorité en fonction de leur qualité.

Mode manuel : Les priorités des interfaces sont définies manuellement.

Mode priorité : Les interfaces obtiennent une priorité basée sur la qualité et le facteur de coût de la liaison.

Mode SLA : Les interfaces sont priorisées en fonction des paramètres SLA sélectionnés.

Mode équilibrage de charge : Le trafic est réparti entre tous les liens disponibles selon un algorithme d'équilibrage spécifique.

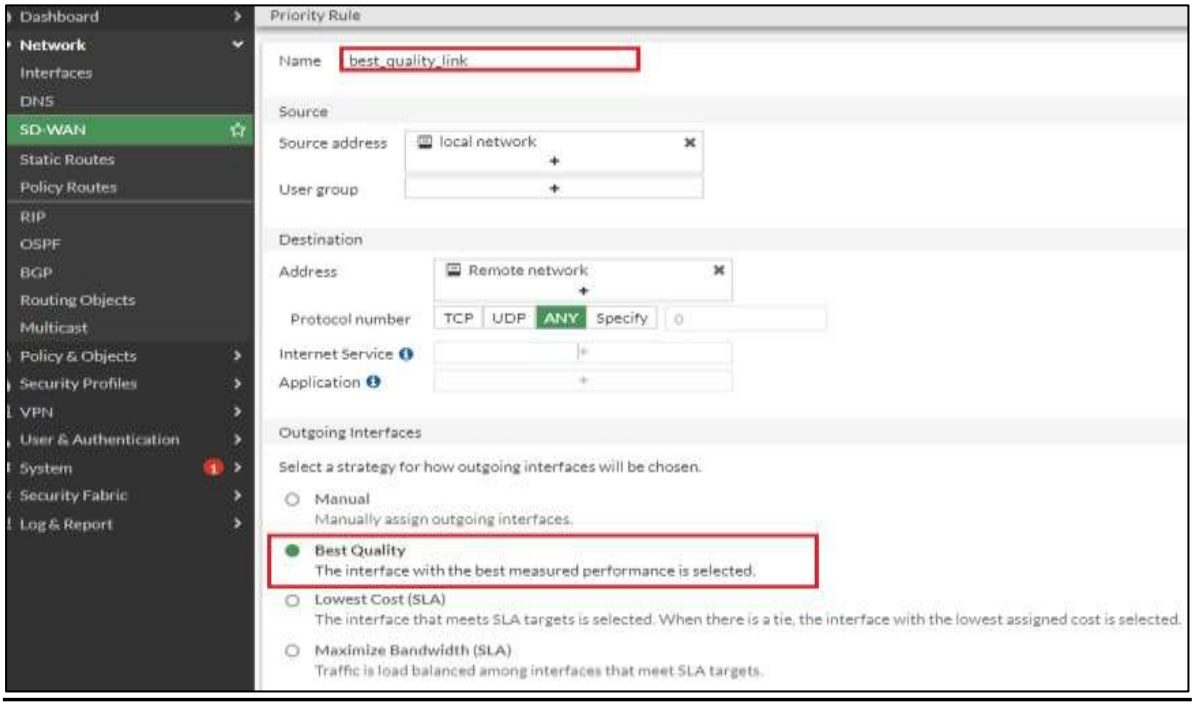


Figure 40: les règles de SD-WAN

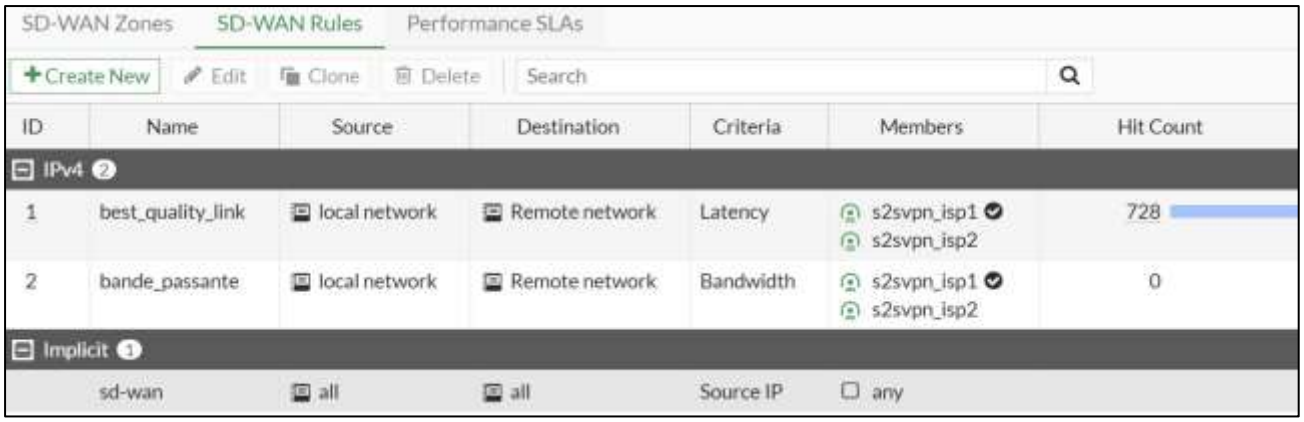


Figure 41: table de règles (Rules) SD-WAN

Performance SLAs

Les SLA de performances, aussi connus sous le nom de contrôle de santé, sont des mécanismes utilisés pour surveiller la qualité des liaisons des interfaces membres et pour détecter les pannes éventuelles. Ils jouent un rôle major en permettant la suppression des routes et la redirection du trafic lorsque l'un des membres du SD-WAN ne parvient pas à détecter un serveur. De plus, ils interviennent dans les règles SD-WAN pour déterminer quelle interface membre privilégier pour le transfert du trafic.

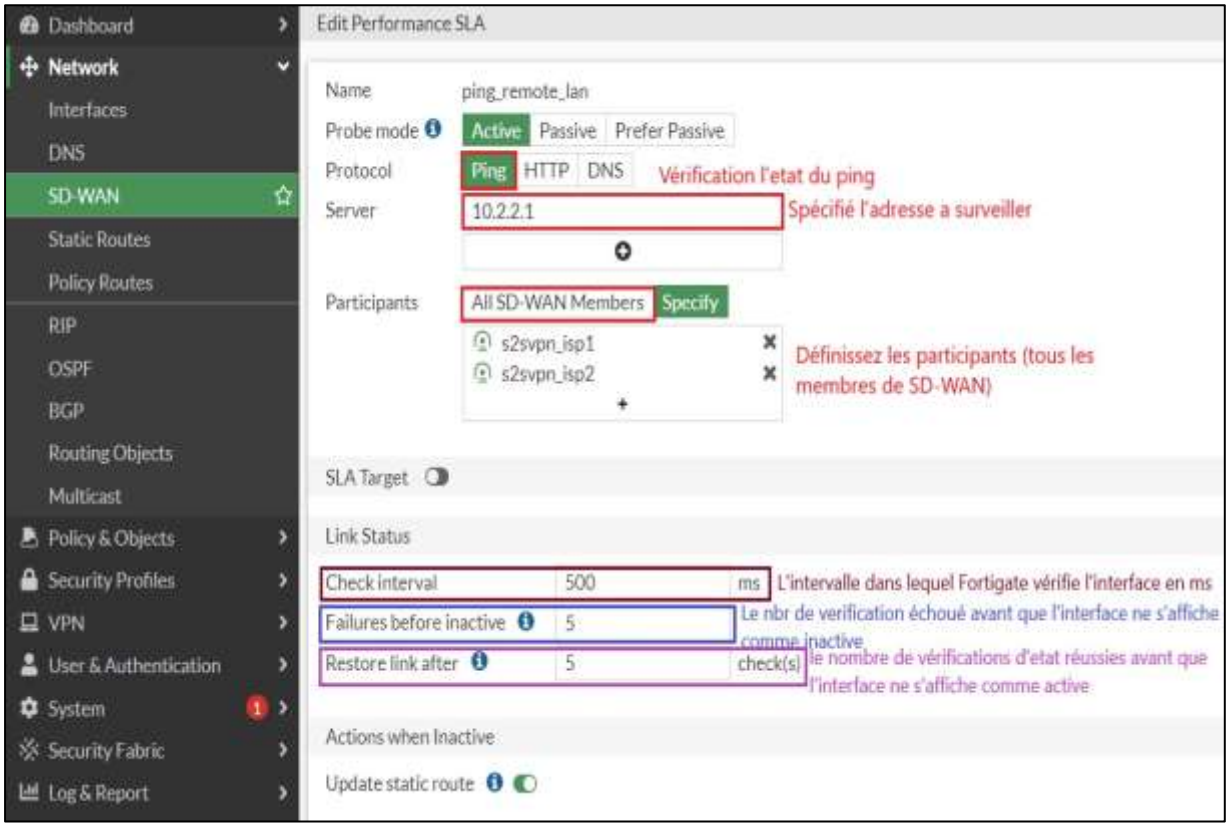


Figure 42: Courbe de performance de deux tunnels s1vpn_isp1 et s2vpn_isp2

Configurions de la table de filtrage :

La table de filtrage dans le pare-feu Fortigate est une composante essentielle qui répertorie et gère les règles de sécurité qui déterminent le flux du trafic réseau. Elle agit comme une sorte de tableau de contrôle, examinant chaque paquet de données entrant ou sortant et décidant s'il doit être autorisé ou bloqué en fonction des critères spécifiés dans les règles de sécurité.

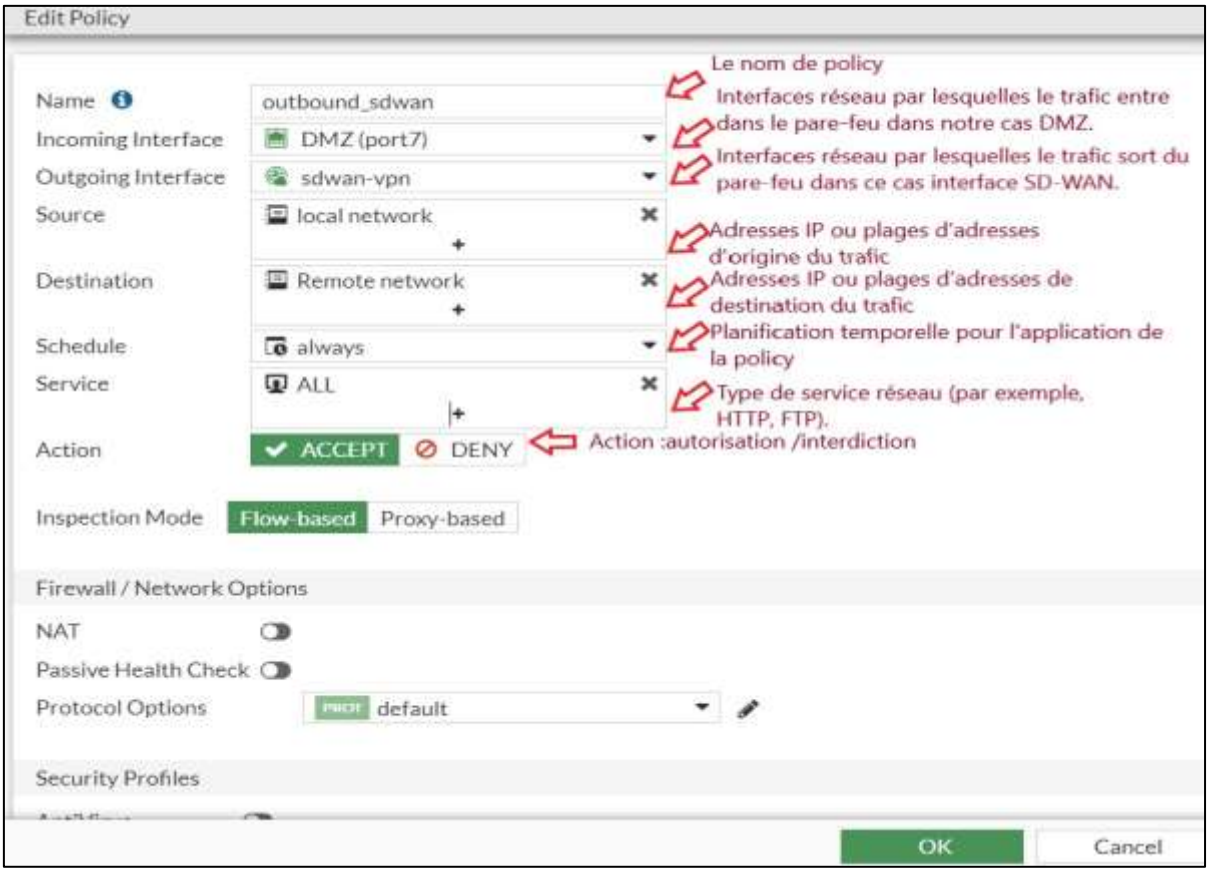


Figure 43: Configurions de la table de filtrage

4.5Teste de connectivité

Test de protocole DHCP l'attribution dynamique des adresses IP est réussie.

Figure 44: Vérification la configuration de protocole DHCP

Vérification de la connectivité des machines PC LAN au serveur DMZ

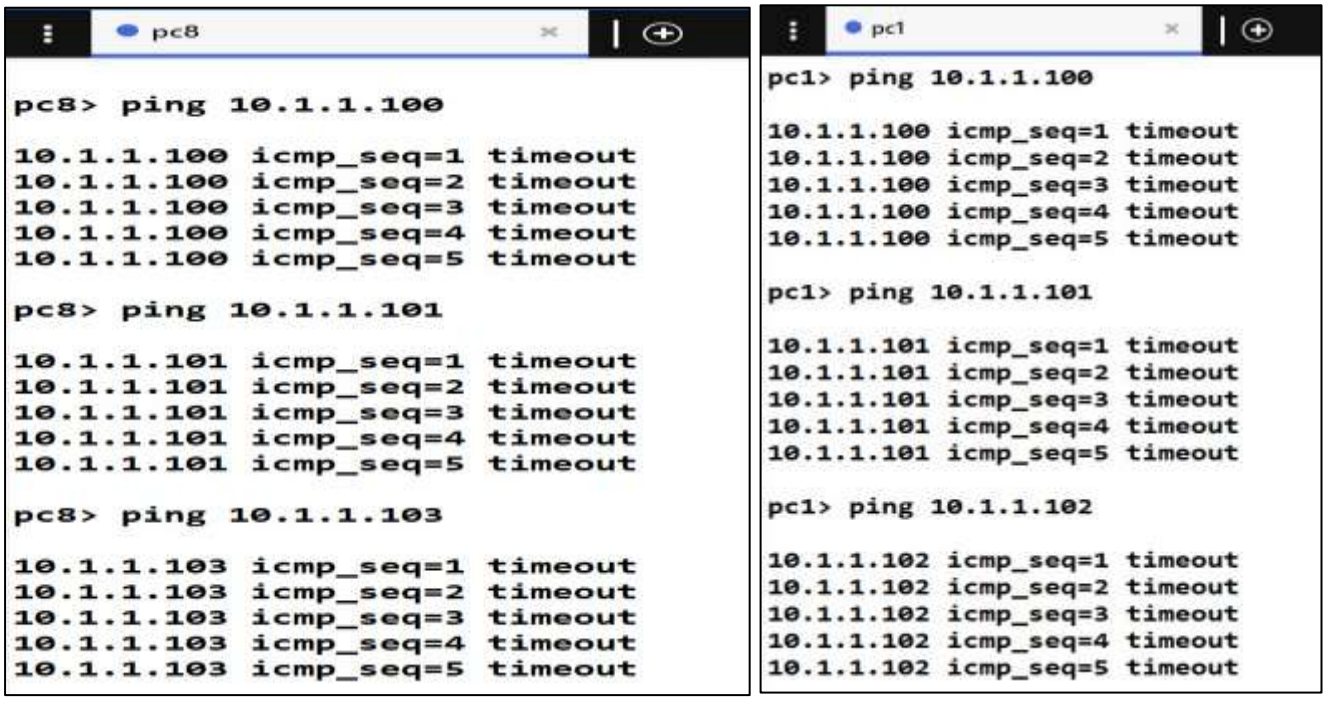


Figure 45: teste de connectivité réussie des PC-LANs au serveur DMZ

Vérification de la connectivité des machines LAN vers ZEP

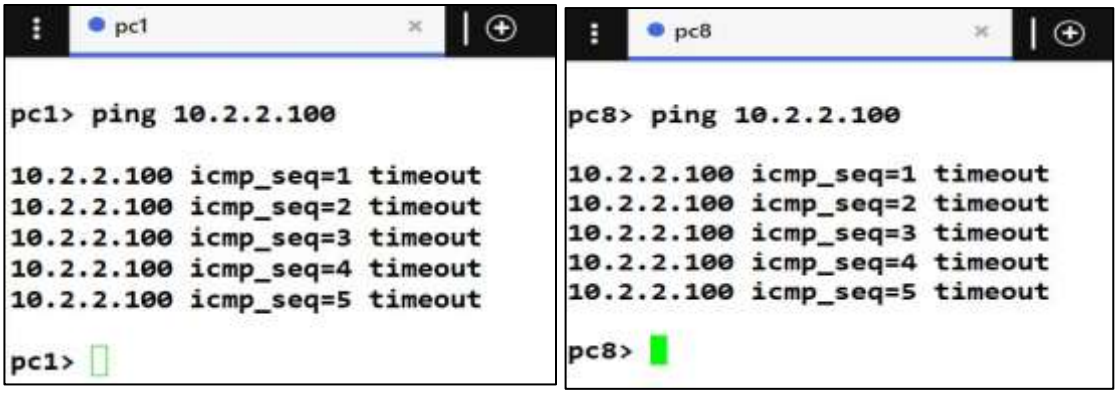


Figure 46: teste de connectivité réussie des machine LAN vers ZEP

Vérification de la connectivité entre le serveur de la DMZ vers ZEP

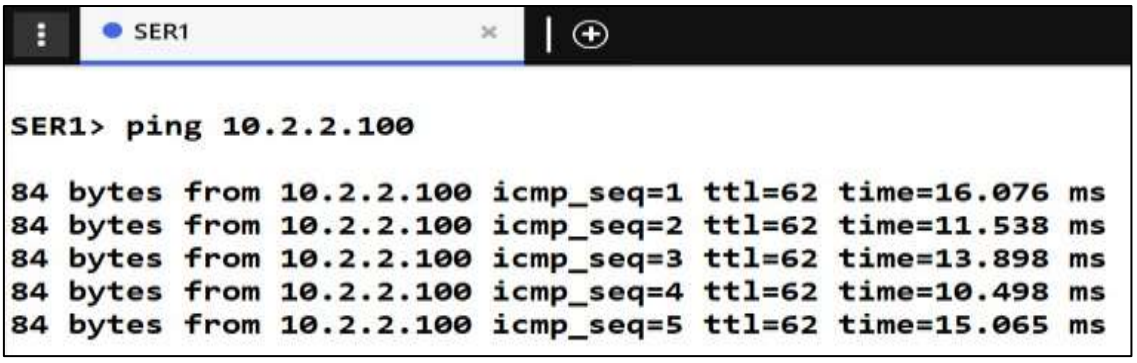


Figure 47: connectivité de serveur vers la DMZ vers ZEP

Vérification de la connectivité de serveur de la ZEP vers LAN BMT

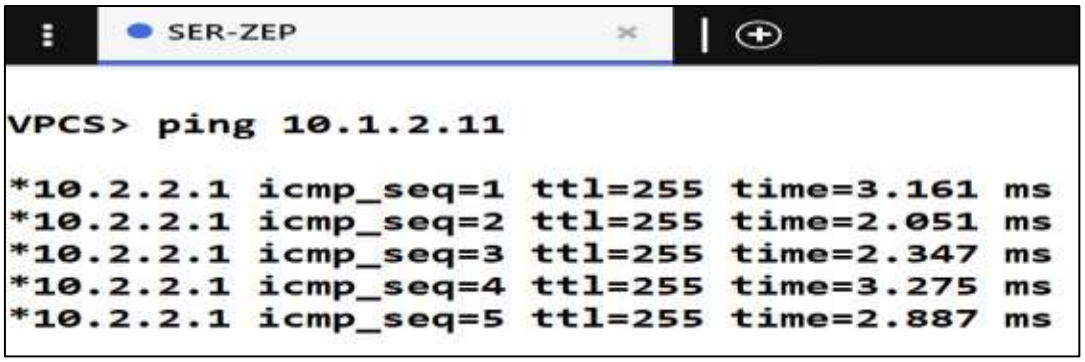


Figure 48: Vérification de la connectivité de serveurs ZEP au LAN BMT

Vérification de la connectivité entre le PC-ZEP et le LAN BMT

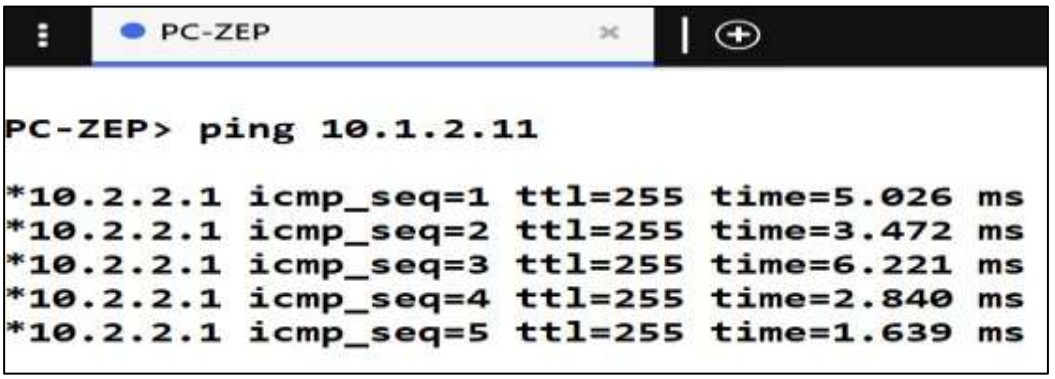


Figure 49: Vérification de la connectivité entre les machines ZEP

Teste de connectivité BMT vers ZEP

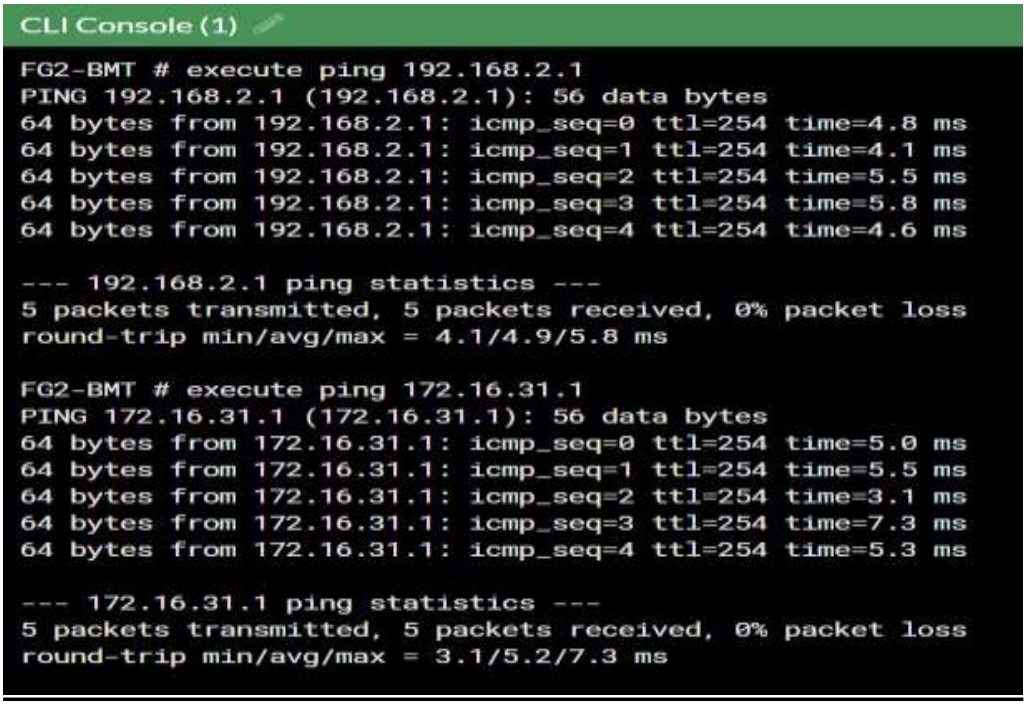


Figure 50: vérification la connectivité de site BMT vers ZEP

Teste de connectivité ZEP vers BMT

```
CLI Console (2)
ZEP # execute ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=254 time=9.2 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=254 time=5.4 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=254 time=24.5 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=254 time=28.9 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=254 time=10.4 ms

--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 5.4/15.6/28.9 ms

ZEP # execute ping 172.16.30.1
PING 172.16.30.1 (172.16.30.1): 56 data bytes
64 bytes from 172.16.30.1: icmp_seq=0 ttl=254 time=12.0 ms
64 bytes from 172.16.30.1: icmp_seq=1 ttl=254 time=38.1 ms
64 bytes from 172.16.30.1: icmp_seq=2 ttl=254 time=3.9 ms
64 bytes from 172.16.30.1: icmp_seq=3 ttl=254 time=39.7 ms
64 bytes from 172.16.30.1: icmp_seq=4 ttl=254 time=5.4 ms

--- 172.16.30.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.9/19.8/39.7 ms
```

Figure 51: vérification la connectivité de site ZEP vers BMT

4.6 Test de basculement entre les tunnels VPN en cas de panne sur l'un des liens

En cas de défaillance du routeur ISP1 dans une configuration SD-WAN, le contrôleur SD-WAN détecte automatiquement cet incident et dirige le trafic vers le tunnel S2VPN_ISP2. De même, en cas de panne du routeur ISP2, le contrôleur redirige le trafic vers le tunnel

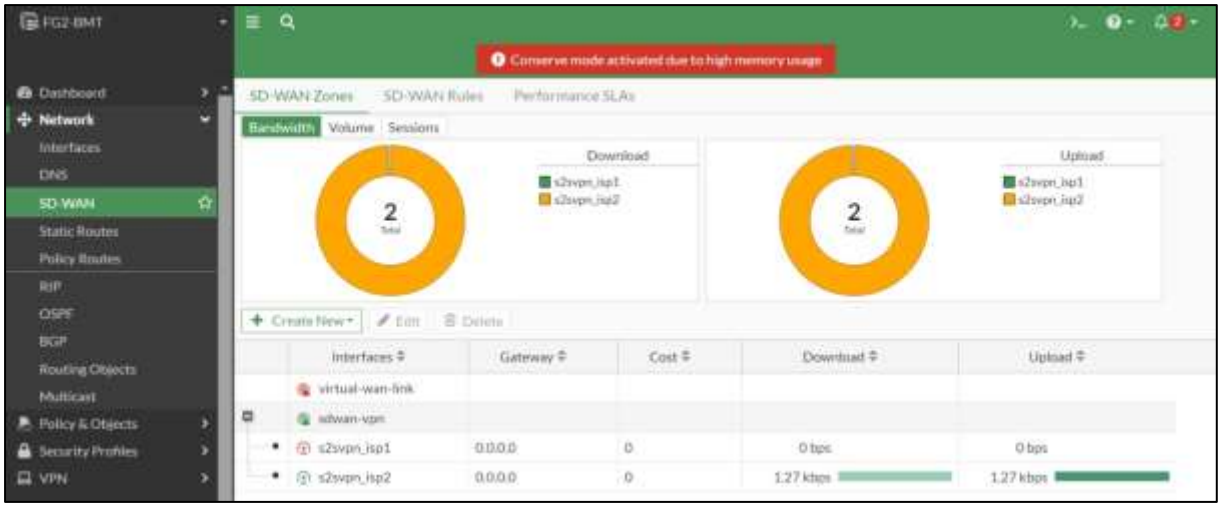


Figure 52: Basculement réussi vers le tunnel s2vpn_isp2

Basculement vers le tunnel S1VPN_ISP1 dans le cas où le router ISP2 tombe en panne

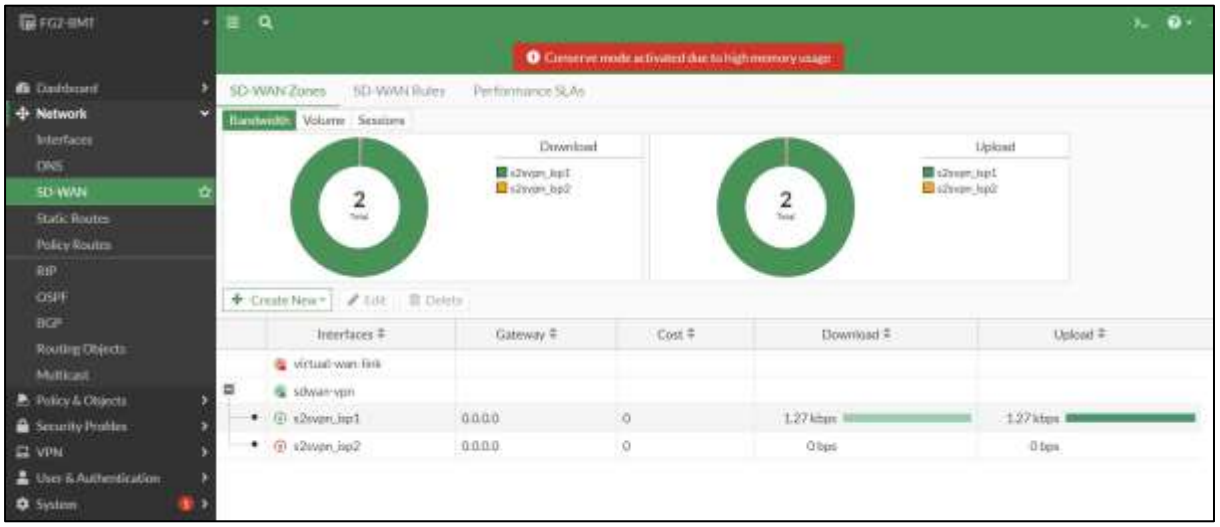


Figure 53: Basculement réussi vers le tunnel s2vpn_isp1

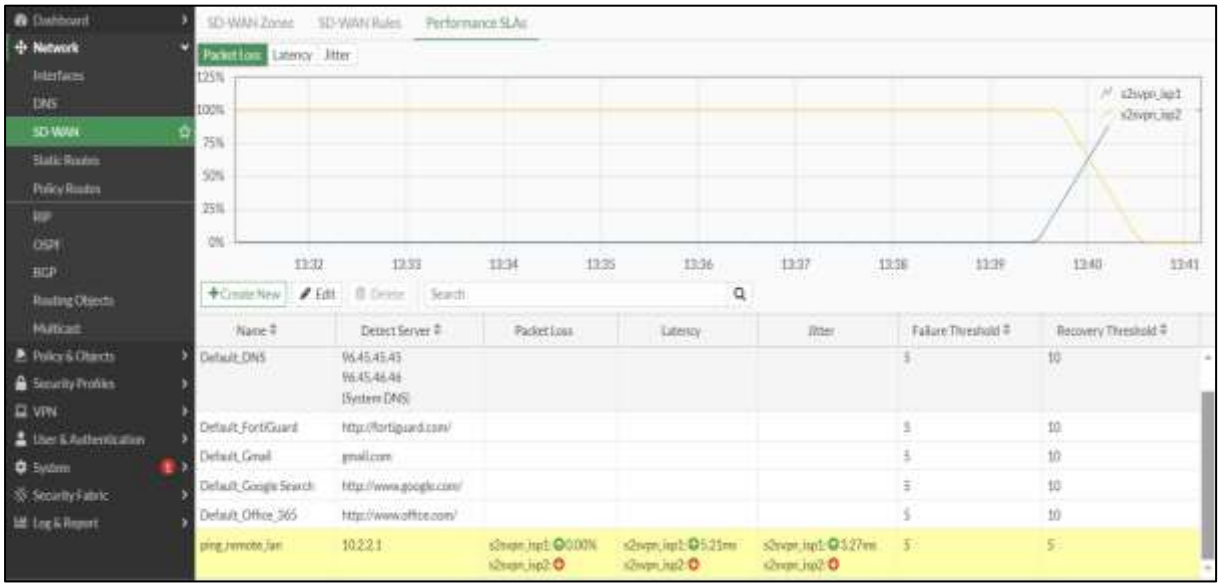


Figure 54:courbe des paquets perdu de S2VPN_ISP1

4 .6 Conclusion

L’objectif principal de notre travail était d'améliorer le réseau de l'entreprise BMT pour garantir une redondance fiable, améliorer les performances et réduire les coûts de maintenance. Nous avons réussi à atteindre cet objectif en mettant en place des configurations spécifiques et en effectuant des tests approfondis pour valider le fonctionnement optimal de chaque aspect de la solution déployée.

CONCLUSION GÉNÉRALE

Notre projet de fin d'études vise à élaborer une infrastructure réseau innovante, axée sur l'optimisation des réseaux étendus (WAN), tout en assurant une connectivité robuste, sécurisée et flexible, ainsi qu'une gestion centralisée simplifiée. Pour atteindre cet objectif ambitieux, Nous avons entrepris la configuration des pare-feu Fortigate en mettant en place un système de contrôle SD-WAN. Ce système gère de manière efficace deux tunnels VPN IPSec, un principal et un secondaire, permettant ainsi une redondance et une tolérance aux pannes. Ces tunnels VPN relient les deux sites distants de BMT et ZEP, assurant un accès distant sécurisé aux ressources et facilitant l'échange de données entre ces sites distants.

Dans le but de renforcer la sécurité de nos réseaux locaux, nous avons instauré une Zone Démilitarisée (DMZ), visant à isoler ces réseaux de toute accessibilité externe. Les résultats obtenus à travers les simulations réalisées sur GNS-3 ont pleinement validé le bon fonctionnement des technologies configurées au sein de l'entreprise. Cette validation contribue indéniablement à améliorer la disponibilité et la sécurisation des données échangées entre les différentes entités du réseau.

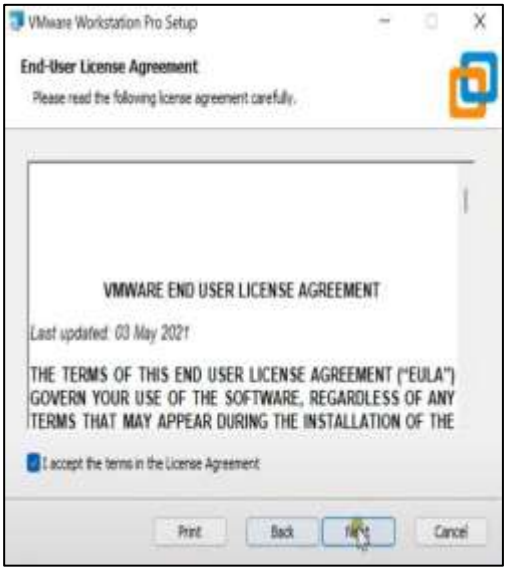
Ce projet représente une opportunité précieuse d'enrichir, d'améliorer et d'approfondir nos connaissances dans les domaines de l'administration et de la sécurité des réseaux informatiques. De plus, il nous a permis d'explorer et de nous familiariser avec d'autres logiciels de simulation tels que VMware Workstation 17 Pro et le pare-feu Fortigate. En combinant théorie et pratique, ce projet nous a préparés à relever les défis complexes du monde des réseaux informatiques et à contribuer de manière significative à ce domaine en constante évolution.

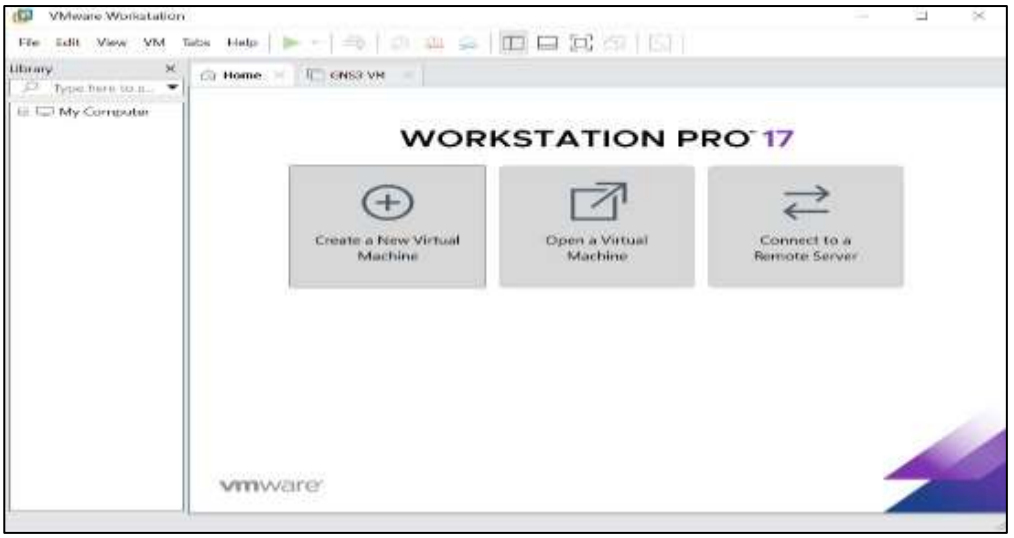
Annexe

Annexe 1 : Installation de VMWare Workstation version 17 pro :

Ce logiciel permet la création de multiples machines virtuelles sur un même ordinateur. Voici le lien pour l'installer :https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html

Les étapes d'installation sont illustrées dans les figures suivantes :





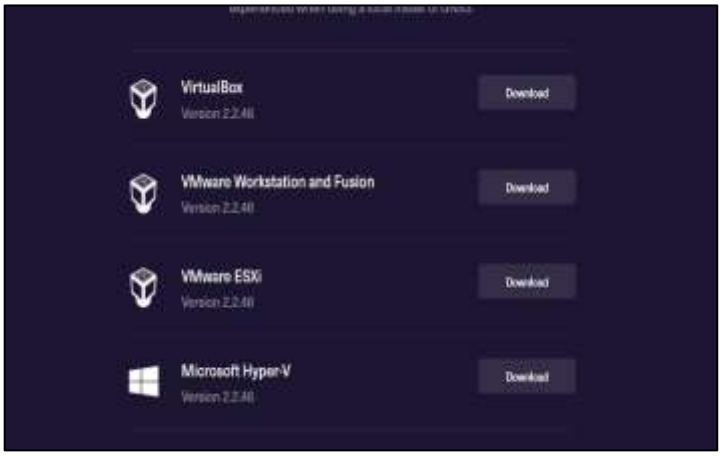
Annexe 2 : Installation de GNS3

GNS3 est une plateforme de virtualisation réseau qui permet de simuler des réseau complexes en utilisant des routeurs, des commutateurs et d'autres périphériques réseau virtuels. Vous pouvez télécharger GNS3 sur leur site officiel :

https://www.gns3.com/software/download pour GNS3 pour GNS3.

https://www.gns3.com/software/download-vm pour GNS3 VM.

La figure suivante illustre les étapes d'installation de GNS3 :

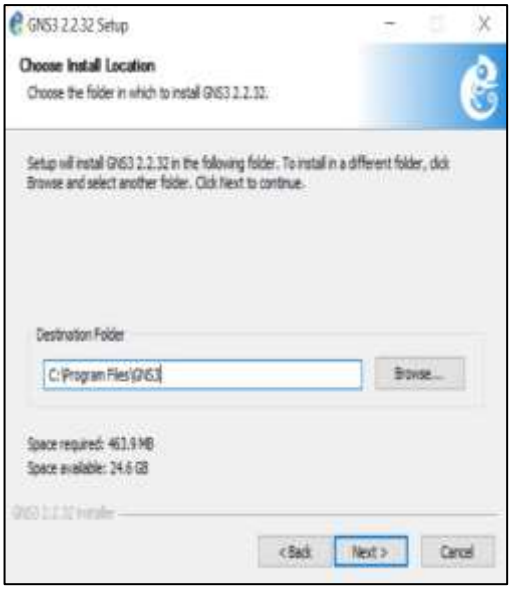



GNS3 2.2.32 Setup
Welcome to GNS3 2.2.32 Setup
GNS3
Setup will guide you through the installation of GNS3 2.2.32.
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.
Click Next to continue.
Next >
Cancel

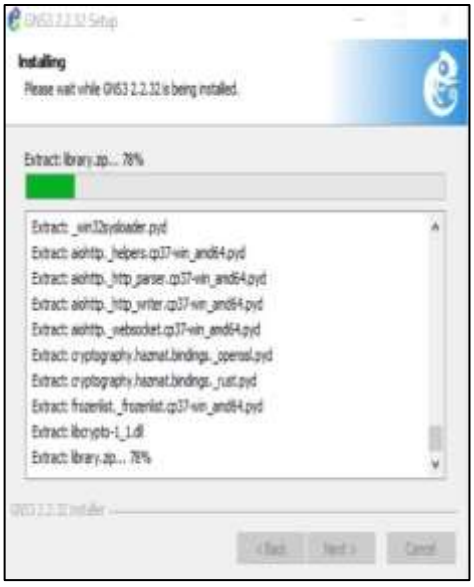

GNS3 2.2.32 Setup
License Agreement
Please review the license terms before installing GNS3 2.2.32.
Press Page Down to see the rest of the agreement.
GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007
Copyright (C) 2007 Free Software Foundation, Inc.
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.
Preamble
The GNU General Public License is a free, copyleft license for software and other kinds of works.
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install GNS3 2.2.32.
< Back
I Agree
Cancel


GNS3 2.2.32 Setup
Choose Start Menu Folder
Choose a Start Menu folder for the GNS3 2.2.32 shortcuts.
Select the Start Menu folder in which you would like to create the program's shortcuts. You can also enter a name to create a new folder.
GNS3
Accessibility
Accessories
Administrative Tools
Cisco Packet Tracer
GNS3
Maintenance
Music, Photos and Videos
Outils Microsoft Office
Solar-PuTTY
StartUp
System Tools
VideoLAN
< Back
Next >
Cancel


GNS3 2.2.32 Setup
Choose Components
Choose which features of GNS3 2.2.32 you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select the type of install:
Custom
Or, select the optional components you wish to install:
MSVC Runtime 2017
GNS3 Desktop
GNS3 WebClient
GNS3 VM
Tools
Description
Space required: 463.9 MB
< Back
Next >
Cancel

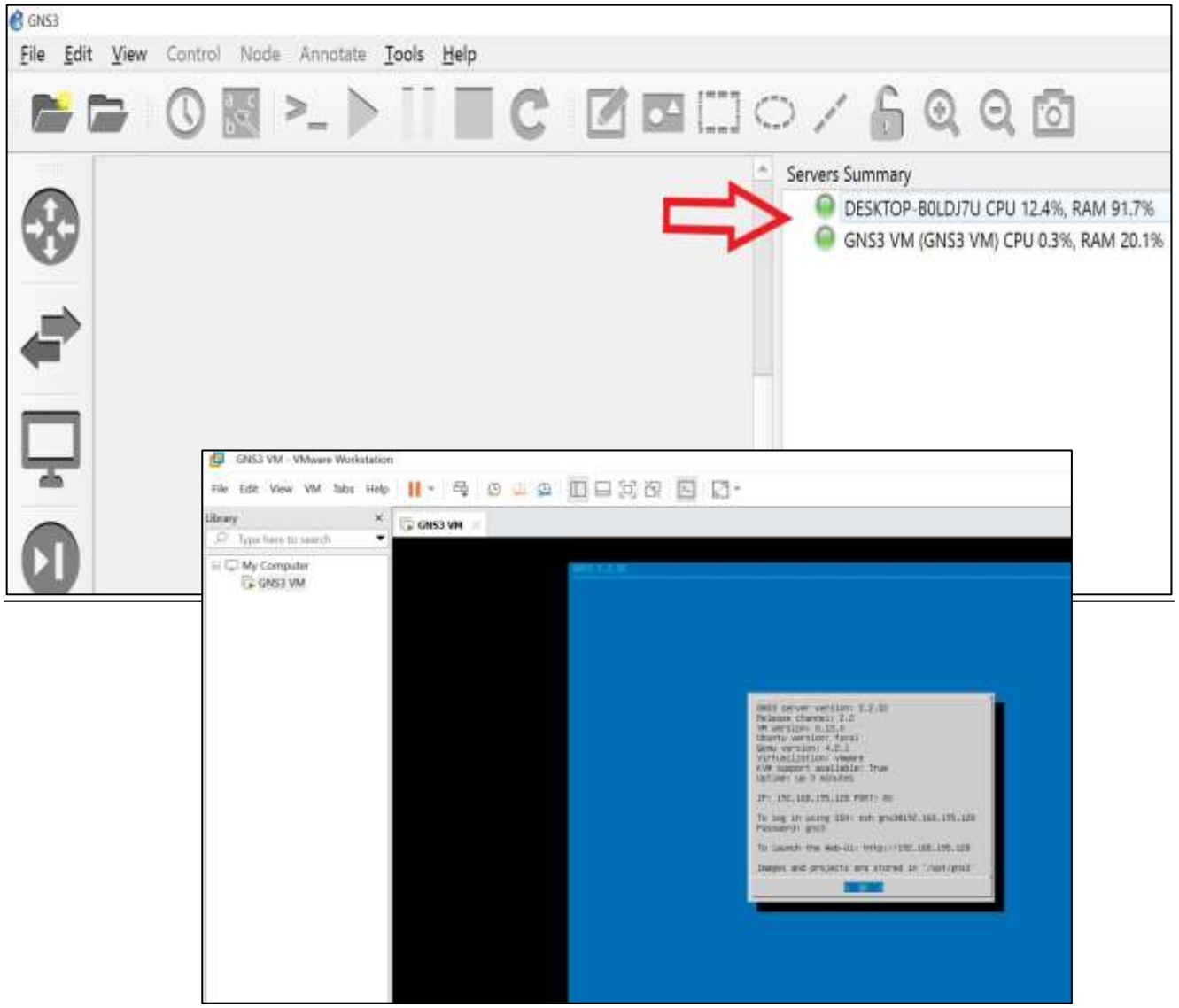

GNS3 2.2.32 Setup
Choose Install Location
Choose the folder in which to install GNS3 2.2.32.
Setup will install GNS3 2.2.32 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.
Destination Folder
C:\Program Files\GNS3
Browse...
Space required: 463.9 MB
Space available: 24.6 GB
< Back
Next >
Cancel


GNS3 2.2.32 Setup
GNS3 VM
The GNS3 VM must be run by a Virtual Machine Software program
Please select the GNS3 VM type:
VMware Workstation
VMware ESXi
VirtualBox
Hyper-V
< Back
Install
Cancel


Installing
Please wait while GNS3 2.2.32 is being installed.
Extract: library.zip... 78%
Extract: _win32sysloader.pyd
Extract: aiohttp._helpers.cp37-win_amd64.pyd
Extract: aiohttp._http_parser.cp37-win_amd64.pyd
Extract: aiohttp._http_writer.cp37-win_amd64.pyd
Extract: aiohttp._websocket.cp37-win_amd64.pyd
Extract: cryptography.hazmat.bindings._openssl.pyd
Extract: cryptography.hazmat.bindings._rust.pyd
Extract: frozenlist._frozenlist.cp37-win_amd64.pyd
Extract: libcrypto-1_1.dll
Extract: library.zip... 78%


GNS3 2.2.32 Setup
Solarwinds Standard Toolset
Exclusive for GNS3 users
Would you like to get your free license of Solarwinds Standard Toolset? ($200 value)
Yes
No
Toolset F.A.Q.
Next >
Cancel


GNS3 2.2.32 Setup
Completing GNS3 2.2.32 Setup
GNS3
GNS3 2.2.32 has been installed on your computer.
Click Finish to close Setup.
Start GNS3
< Back
Finish

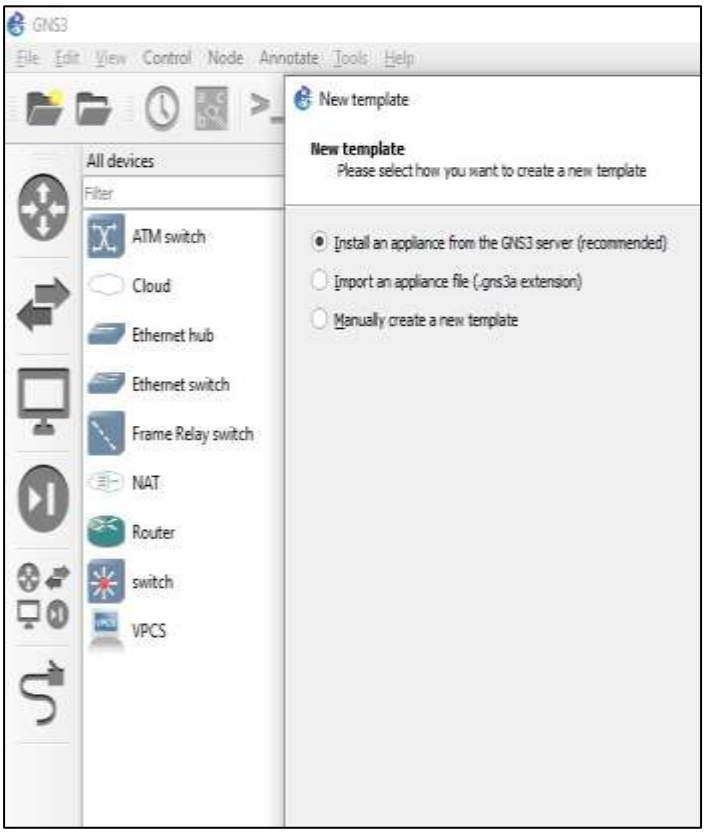


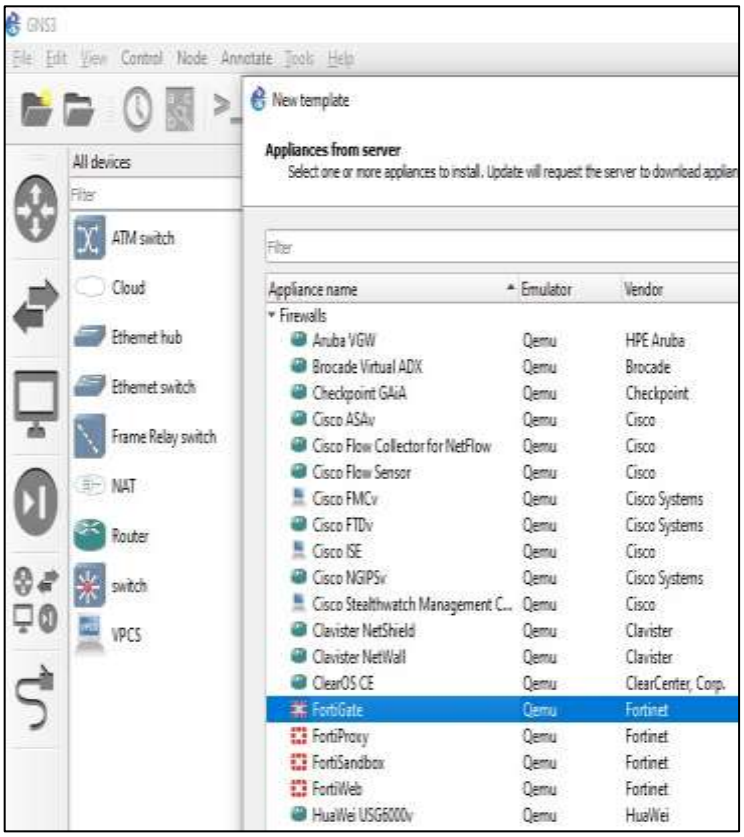
Annexe 3 : Instalation de Fortigzte :

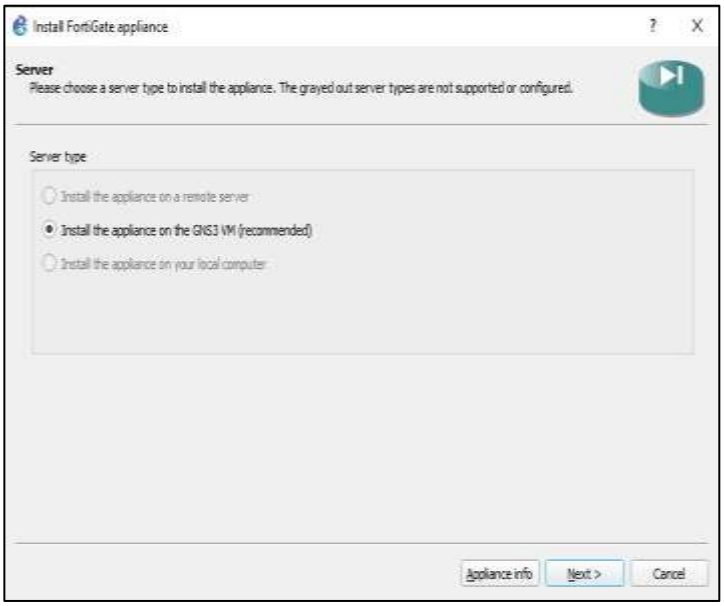
Vous pouvez télécharger les fichiers et logiciels liés à Fortigate à partir du site officiel de Fortinet :

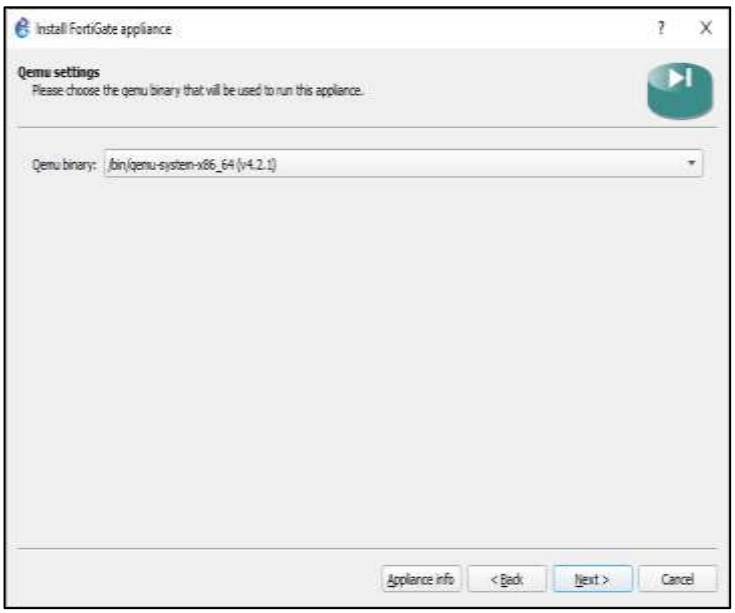
https://www.fortinet.com/products/next-generation-firewall/fortigate

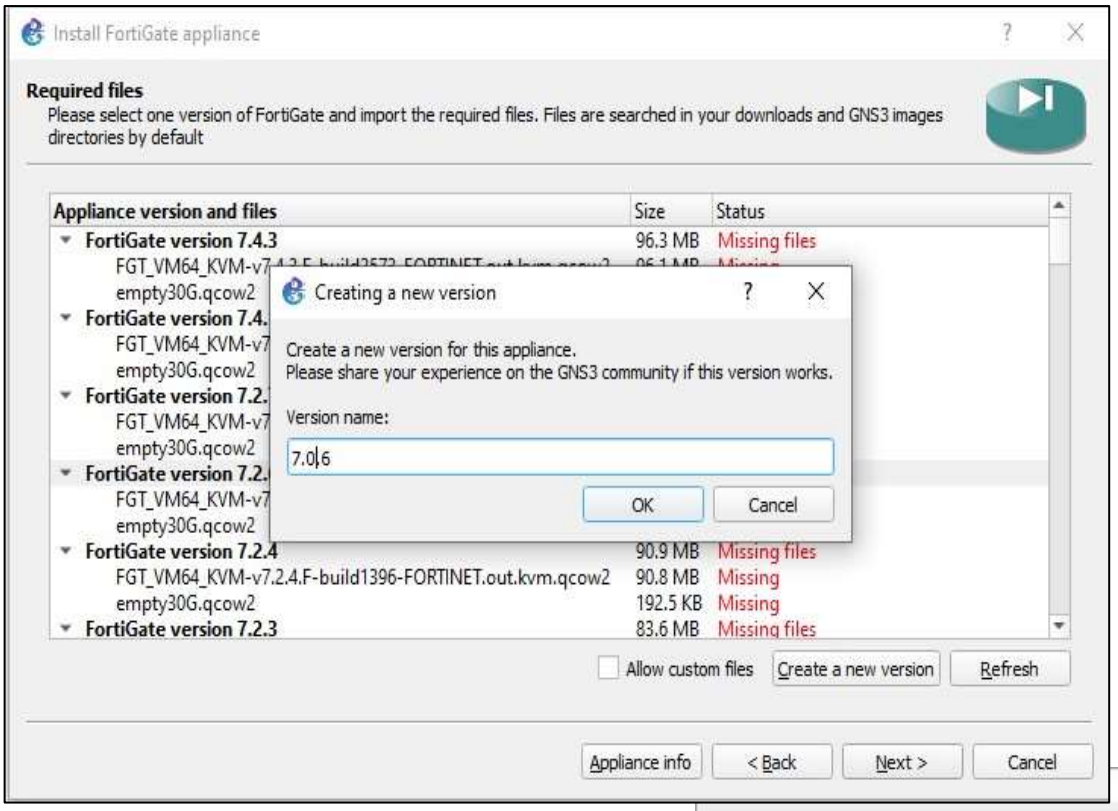
La figure suivante illustre les étapes d'installation de Fortigate :

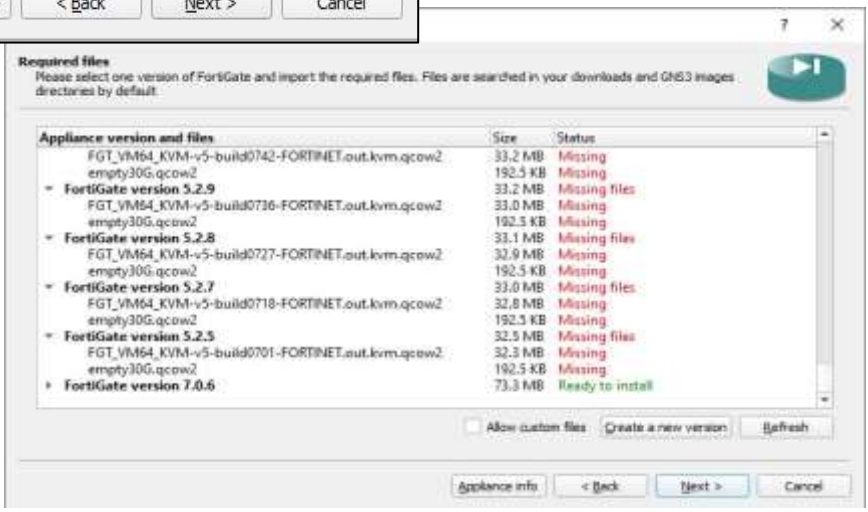

GNS3
File Edit View Control Node Annotate Tools Help
New template
New template
Please select how you want to create a new template
All devices
Filter
ATM switch
Cloud
Ethernet hub
Ethernet switch
Frame Relay switch
NAT
Router
switch
VPCS
Install an appliance from the GNS3 server (recommended)
Import an appliance file (.gns3a extension)
Manually create a new template

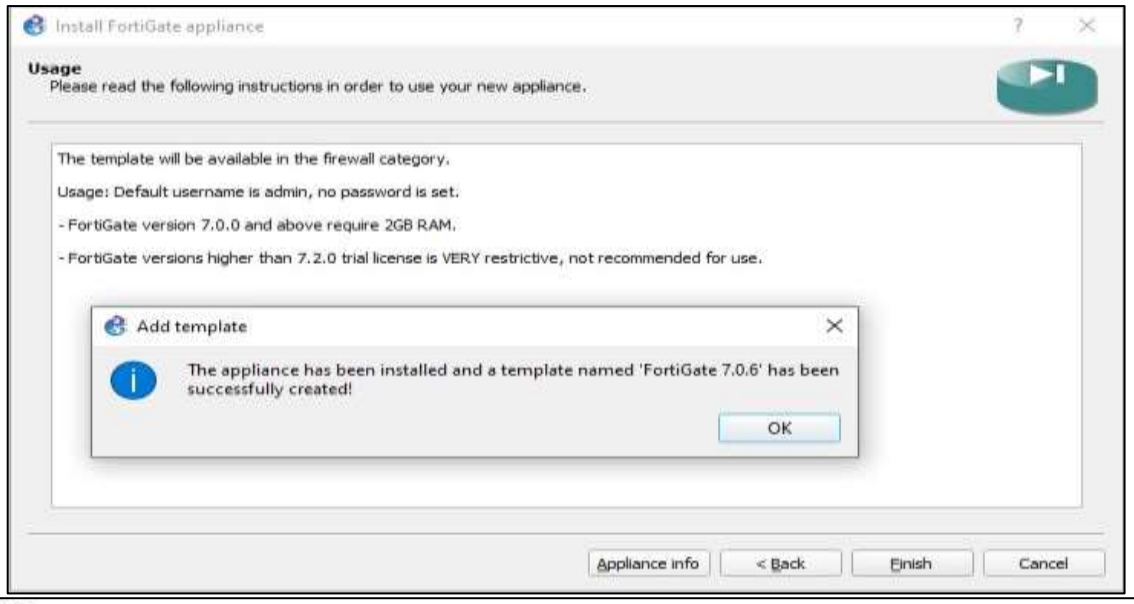

GNS3
File Edit View Control Node Annotate Tools Help
New template
Appliances from server
Select one or more appliances to install. Update will request the server to download applian
All devices
Filter
ATM switch
Cloud
Ethernet hub
Ethernet switch
Frame Relay switch
NAT
Router
switch
VPCS
Appliance name
Emulator
Vendor
Firewalls
Aruba VGW Qemu HPE Aruba
Brocade Virtual ADX Qemu Brocade
Checkpoint GAiA Qemu Checkpoint
Cisco ASAv Qemu Cisco
Cisco Flow Collector for NetFlow Qemu Cisco
Cisco Flow Sensor Qemu Cisco
Cisco FMCv Qemu Cisco Systems
Cisco FTDv Qemu Cisco Systems
Cisco ISE Qemu Cisco
Cisco NGIPSv Qemu Cisco Systems
Cisco Stealthwatch Management C... Qemu Cisco
Clavister NetShield Qemu Clavister
Clavister NetWall Qemu Clavister
ClearOS CE Qemu ClearCenter, Corp.
FortiGate Qemu Fortinet
FortiProxy Qemu Fortinet
FortiSandbox Qemu Fortinet
FortiWeb Qemu Fortinet
HuaWei USG6000v Qemu HuaWei

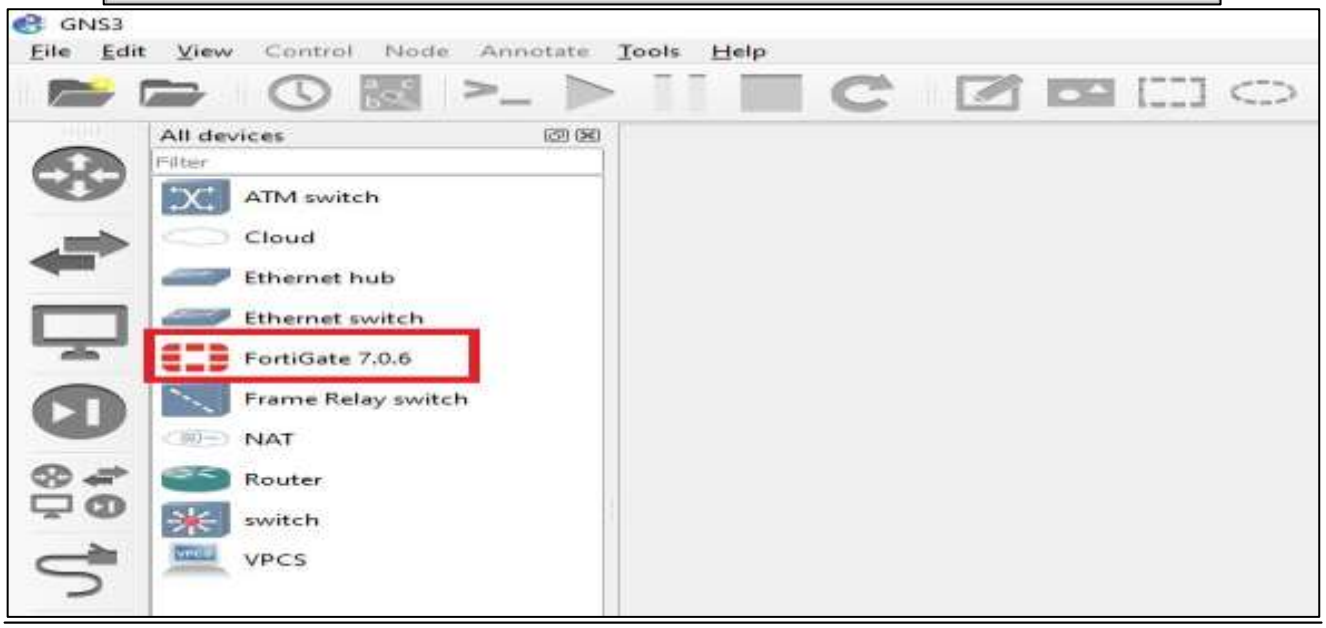

Install FortiGate appliance
Server
Please choose a server type to install the appliance. The grayed out server types are not supported or configured.
Server type
Install the appliance on a remote server
Install the appliance on the GNS3 VM (recommended)
Install the appliance on your local computer
Appliance info
Next >
Cancel


Install FortiGate appliance
Qemu settings
Please choose the qemu binary that will be used to run this appliance.
Qemu binary: /bin/qemu-system-x86_64 (v4.2.1)
Appliance info
< Back
Next >
Cancel


Install FortiGate appliance
Required files
Please select one version of FortiGate and import the required files. Files are searched in your downloads and GNS3 images directories by default
Appliance version and files
Size
Status
FortiGate version 7.4.3
96.3 MB
Missing files
empty30G.qcow2
FortiGate version 7.4.
FGT_VM64_KVM-v7
empty30G.qcow2
FortiGate version 7.2.
FGT_VM64_KVM-v7
empty30G.qcow2
FortiGate version 7.2.
FGT_VM64_KVM-v7
empty30G.qcow2
FortiGate version 7.2.4
90.9 MB
Missing files
FGT_VM64_KVM-v7.2.4.F-build1396-FORTINET.out.kvm.qcow2
90.8 MB
Missing
empty30G.qcow2
192.5 KB
Missing
FortiGate version 7.2.3
83.6 MB
Missing files
Creating a new version
Create a new version for this appliance.
Please share your experience on the GNS3 community if this version works.
Version name:
7.0.6
OK
Cancel
Allow custom files
Create a new version
Refresh
Appliance info
< Back
Next >
Cancel


Required files
Please select one version of FortiGate and import the required files. Files are searched in your downloads and GNS3 images directories by default
Appliance version and files
Size
Status
FGT_VM64_KVM-v5-build0742-FORTINET.out.kvm.qcow2
33.2 MB
Missing
empty30G.qcow2
192.5 KB
Missing
FortiGate version 5.2.9
33.2 MB
Missing files
FGT_VM64_KVM-v5-build0736-FORTINET.out.kvm.qcow2
33.0 MB
Missing
empty30G.qcow2
192.5 KB
Missing
FortiGate version 5.2.8
33.1 MB
Missing files
FGT_VM64_KVM-v5-build0727-FORTINET.out.kvm.qcow2
32.9 MB
Missing
empty30G.qcow2
192.5 KB
Missing
FortiGate version 5.2.7
33.0 MB
Missing files
FGT_VM64_KVM-v5-build0718-FORTINET.out.kvm.qcow2
32.8 MB
Missing
empty30G.qcow2
192.5 KB
Missing
FortiGate version 5.2.5
32.5 MB
Missing files
FGT_VM64_KVM-v5-build0701-FORTINET.out.kvm.qcow2
32.3 MB
Missing
empty30G.qcow2
192.5 KB
Missing
FortiGate version 7.0.6
73.3 MB
Ready to install
Allow custom files
Create a new version
Refresh
Appliance info
< Back
Next >
Cancel


Install FortiGate appliance
Usage
Please read the following instructions in order to use your new appliance.
The template will be available in the firewall category.
Usage: Default username is admin, no password is set.
- FortiGate version 7.0.0 and above require 2GB RAM.
- FortiGate versions higher than 7.2.0 trial license is VERY restrictive, not recommended for use.
Add template
The appliance has been installed and a template named 'FortiGate 7.0.6' has been successfully created!
OK
Appliance info
< Back
Finish
Cancel


GNS3
File Edit View Control Node Annotate Tools Help
All devices
Filter
ATM switch
Cloud
Ethernet hub
Ethernet switch
FortiGate 7.0.6
Frame Relay switch
NAT
Router
switch
VPCS

Bibliographie

[1] https://reseauxifa.wordpress.com/pan/, Consulté 28/03/2024.

[2] https://le-routeur-wifi.com/reseau-lan., Consulter le 29/04/2024.

[3] https://www.malekal.com/les-differents-types-de-reseaux-lan-wan-man/, Consulter le 29/04/2024.

[4] https://fr.dreamstime.com/wan-r%C3%A9seau-%C3%A9tendu-technologie-qui-relie-vos-bureaux-centres-donn%C3%A9es-applications-cloud-stockage-image271663816, consulter le 29/04/2024.

[5] https://sti2d.ecolelamache.org/ii_rseaux_informatiques___7_topologie_des_rseaux.html, consulté le 28/02/2024.

[6] P. d. c. :. Abderrahmane BAADACHE, «Réseaux étendus et réseaux d'opérateurs,» 2013/2014..

[7] Abderrahmane BAADACHE, « Polycopie de cours :Réseaux étendus et réseaux d'opérateurs,,» 2013/2014..

[8] https://www.educba.com/what-is-osi-model/, consulté le 14/05/2024.

[9] https://www.frameip.com/tcpip/, consulté le 20/04/2024.

[10] https://forum.huawei.com/enterprise/fr/sdn-de-huawei-tout-ce-que-vous-devez-savoir/thread/667502244016308224-667481008070602752, Consulté le 02/04/2024.

[11] https://medium.com/@aita.official10/how-does-a-vpn-work-10012c014a92, Consulté le 03/04/2024.

[12] BOURENGUITE Imane, «Mise en place d'une securité réseau basé sur l'utilisation des parfeu et des laisons virtuelles,» 2022/2023.

[13] https://vpnoverview.com/fr/infos-vpn/quest-ce-quun-vpn/, Consulté le 15/05/2024.

[14] J.P ARCHIER, « Les VPN, fonctionnement et mise en œuvre et maintenance des réseaux privés virtuels », éditions eni, 2eme édition., 2011 .

[15] https://www.provya.net/?d=2014/06/15/15/20/04-pfsense-monter-un-acces-openvpn-site-a-site, consulter le 29/04/2024.

[16] https://hitek.fr/actualite/a-quoi-sert-un-vpn-et-top-3-des-meilleurs-vpn_6679, consulter le 29/04/2024.

[17] https://assistance.ac-noumea.nc/spip.php?page=imprimer&id_article=611., consulter le 29/04/2024.

[18] http://perso.modulonet.fr/placurie/Ressources/BTS2-AMSI/Chap-8-Les%20VPN.pdf, Consulté le 01/03/2024.

[19] https://inet.omnetpp.org/docs/users-guide/ch-mpls.html., Consulté le 04/03/2024.

[20] Recommandations de sécurité relatives à IPsec 1 pour la protection des flux réseau, No DAT-NT-003/ANSSI/SDE/NP, 3 août 2015.

[21] https://www.eccentrix.ca/eccentrix-corner/comprendre-les-modes-de-transport-et-de-tunnel-ipsec-securiser-le-trafic-reseau, consulté le 21/04/2024.

[22] https://www.cryptosec.org/?IPSec, consulter le 29/04/2024.

[23] https://www.experte.com/fr/vpn/vpn-securite, consulté le 02/03/2024.

[24] https://www.lemondeinformatique.fr/publi_info/lire-securite-informatique-et-teletravail-les-bonnes-pratiques-477.html., Consulté le 03/03/2024.

[25] https://www.lemondeinformatique.fr/publi_info/lire-securite-informatique-et-teletravail-les-bonnes-pratiques-477.html, consulté le 04/04/2024.

[26] https://www.experte.com/fr/vpn/vpn-securite, Consulté le 22/04/2024.

[27] https://www.axido.fr/vpn-les-bonnes-pratiques-pour-renforcer-la-securite/., Consulté le 13/04/2024.

[28] https://mns-consulting.com/wp-content/uploads/2021/04/MNS-SD-WAN-Technologie-livre-blanc.pdf, consulté le 28/03/2024.

[29] https://lightyear.ai/solutions/wide-area-networking-wan/software-defined-wan-sdwan, consulté le 28/03/2024.

[30] https://www.fortinet.com/resources/cyberglossary/sd-wan-explained, consulté le 30/03/2024.

[31] https://iotindustriel.com/autres/normes-protocoles/sd-wan-tout-ce-quil-faut-savoir/, consulté le 1/04/2024.. [En ligne].

[32] https://www.juniper.net/fr/fr/research-topics/sd-wan-explained.html, consulté le 1/04/2024.

[33] https://www.catonetworks.com/fr/sd-wan/the-way-forward-how-sd-wan-benefits-the-modern-enterprise/#Simplification_de_la_gestion_du_WAN, consulté le 24/05/2024.

[34] https://www.ibm.com/topics/sd-wan/, consulté le 03/04/2024.

[35] https://www.geeksforgeeks.org/difference-between-traditional-wan-and-sd-wan/, consulté le 19/05/2024.

[36] https://www.thesslstore.com/blog/sd-wan-how-to-use-it-to-transform-your-digital-networks/, Consulté le 3/05/2024.

[37] d. https://versa-networks.com/fr/sd-wan/#:~:text=Contrairement%20au%20WAN%20traditionnel%2C%20le, consulté le 13/05/2024.

[38] https://www.insyncom.fr/actualite/introduction-aux-reseaux-sd-wan-definition-et-principes-de-base, cosulté le 15/05/2024.

[39] https://www.fortinet.com/resources/cyberglossary/sd-wan-explained, consulté le 04/04/2024.

[40] https://kadiska.com/fr/quest-ce-qui-cause-les-problemes-de-performances-du-sd-wan/, consulté le 30/04/2024.

[41] https://www.ibm.com/topics/sd-wan, consulté le 19/04/2024.

[42] https://www.ictjournal.ch/news/2021-05-31/pourquoi-le-sd-wan-est-bien-plus-quune-solution-pour-les-sites-distants, consulté le 19/05/2024.

[43] https://itsocial.fr/enjeux-it/enjeux-infrastructure/sd-wan/la-transition-du-sd-wan-vers-le-sase-un-projet-dobstacles/, consulté le 03/05/2024.

[44] https://www.techtarget.com/searchnetworking/definition/SD-WAN-software-defined-WAN, consulté le 30/04/2024.

[45] https://www.catonetworks.com/blog/sd-wan-best-practices-for-secure-and-effective-implementation/, consulté le 24/05/2024.

[46] https://bejaiamed.com/presentation-du-partenariat/, consulté le 17/03/2024.

[47] d. Godart, Sécurité informatique, Risque, Stratigiés et solutions, 2emme édition, 2002.

[48] R. Sidi Mohamed El Amine. Université Abou Bakr Belkaid, Mise en place d'un serveur radius sous linux pour la sécurisation d'un réseau 802.11., Tlemcen-Algérie, , 20011..

[49] J. e. P. J.-F. 4. Philippe, «Tout sur la sécurité informatique,» France Dunod,, 2016.P.271..

[50] M. Consulting, «LES EVOLUTIONS DU WAN: SD-WAN ET SASE».

[51] Jean-fracois PILLOU et Jean-philippe BAY, «tout sur la securité informatique,,» 2013.

[52] https://www.malekal.com/les-differents-types-de-reseaux-lan-wan-man/, Consulter le 29/04/2024.

[53] https://reseauxifa.wordpress.com/pan/, Consulté le 15/03/2024.

[54] Z. Farah, «Cours Master 1 professionnel,Cours Introduction à la sécurité,» 2019.

[55] https://www.cryptosec.org/?IPSec, Consulter le 29/04/2024.

[56] https://blog.netwrix.fr/2019/07/24/tout-ce-quil-faut-savoir-sur-les-equipements-reseau, consulté le 01/03/2024,.

[57] https://loudni.users.greyc.fr/Enseignement/Cours/TRc8/CM/CM3_VPN.pdf., Consulté le 02/03/2024.

[58] https://www.experte.com/fr/vpn/vpn-securite, consulté le 02/03/2024.

[59] https://wiki-tech.io/R%C3%A9seau/Protocoles/OSI, consulter le 29/04/2024.

[60] https://www.materiel-informatique.be/topologie.php, consulter le 29/04/2024.

[61] https://www.cryptosec.org/?IPSec, consulter le 29/04/2024.

[62] https://itsocial.fr/enjeux-it/enjeux-infrastructure/sd-wan/la-transition-du-sd-wan-vers-le-sase-un-projet-dobstacles/, consulté le 03/05/2024.

[63] https://bluefinch-esbd.com/fr/la-dmz-et-la-securite-des-donnees/, Consulté le 30/04/2024.

[64] https://actualitte.com/article/113218/livres/vpn-se-documenter-pour-mieux-comprendre, Consulté le 10/04/2024.

[65] https://actualitte.com/article/113218/livres/vpn-se-documenter-pour-mieux-comprendre, Consulté le 10/04/2024.

[66] https://www.axido.fr/vpn-les-bonnes-pratiques-pour-renforcer-la-securite/, consulté le 08/04/2024.

[67] https://www.insyncom.fr/actualite/introduction-aux-reseaux-sd-wan-definition-et-principes-de-base, Consulté le 15/05/2024.

[68] https://vpnoverview.com/fr/infos-vpn/quest-ce-quun-vpn/. [En ligne]. [Accès le 15 05 2024].

Résumé

Ce mémoire met en lumière sur l'importance des réseaux informatiques dans notre vie quotidienne, soulignant leur rôle fondamental dans la connectivité des appareils électroniques à travers le monde pour l'échange de ressources et de données. Il souligne également l'émergence des VPN comme une solution essentielle pour sécuriser les connexions Internet en établissant des canaux sécurisés et cryptés.

Une partie significative de ce travail est dédiée à une technologie émergente : le SD-WAN. Cette innovation transforme la connectivité des réseaux étendus en permettant une gestion centralisée et une optimisation dynamique du trafic sur plusieurs liaisons réseau, offrant ainsi des performances améliorées et des coûts réduits par rapport aux réseaux WAN traditionnels. Il est important de noter que cette implémentation du SD-WAN est réalisée à travers la solution Fortigate, démontrant ainsi l'importance de cette plateforme intégrée de sécurité pour garantir une protection efficace et une gestion fluide des flux de données dans les infrastructures réseau modernes.

Mot clé :SD-WAN, VPN, Réseaux, Fortigate, gestion centralisée, connectivité

Abstract

This thesis sheds light on the significance of computer networks in our daily lives, emphasizing their pivotal role in connecting electronic devices worldwide for the exchange of resources and data. It also underscores the emergence of VPN as an essential solution for securing Internet connections by establishing secure and encrypted channels. A substantial portion of this dissertation is dedicated to an emerging technology: SD-WAN. This innovation revolutionizes wide area network connectivity by enabling centralized management and dynamic traffic optimization across multiple network links, thereby offering enhanced performance and cost reductions compared to traditional WANs. It is noteworthy that the implementation of SD-WAN is carried out through the FortiGate solution, thereby highlighting the significance of this integrated security platform in ensuring effective protection and seamless management of data flows in modern network infrastructures.

Keywords : SD-WAN, VPN, Network, Fortigate, Centralized management, Connectivity