Ministère de l'Enseignement Supérieur et de la Recherche Scientifique.
Université SAAD DAHLAB Blida-1-

Faculté de Sciences.

Département d'informatique.

Pour l'obtention du diplôme :

MASTER EN INFORMATIQUE.

Option : **Système d'informatique et Réseaux.**

Thème :

Migration Graduelle d'une infrastructure DMVPN Vers Une architecture SD-WAN Au Niveau de NAFTAL.

Organisme d'accueil : Direction Générale de NAFTAL.

Réalisé par : BEN SAAD Nour El Houda.

Soutenu devant le jury composé par :

Madame	**BOUSTIA**	NARHIMENE	USDB	**Présidente**
Madame	**DAOUD**	Hayat	USDB	**Examinatrice**
Monsieur	**BENYAHIA**	MOHAMED	USDB	**Promoteur**
Monsieur	**BENSADAT**	ANES	NAFTAL	**Encadreur**

Année universitaire : **2022/2023**

Résumé

Les entreprises qui ont déjà mis en place un réseau DMVPN se questionnent sur la pertinence d'une migration vers un SD-WAN. Le SD-WAN est particulièrement apprécié pour ses capacités à améliorer la connectivité entre les différents sites d'une entreprise, offrant ainsi une meilleure performance et une plus grande flexibilité.

Dans le cadre de notre étude réalisée au sein de l'entreprise NAFTAL, nous avons implémenté deux architectures distinctes : le DMVPN, qui est une solution établie pour les réseaux étendus, et le SD-WAN, une technologie émergente qui suscite un intérêt croissant.

Notre objectif principal est d'évaluer de manière approfondie les avantages et les inconvénients de chaque option, en prenant en compte des critères essentiels tels que la performance, la sécurité, la flexibilité et la gestion centralisée du système. Nous souhaitons ainsi fournir aux entreprises les informations nécessaires pour prendre des décisions éclairées quant au choix le plus approprié pour leur réseau étendu, en mettant un fort accent sur l'optimisation de la connectivité entre les sites distants.

Mots clés : DMVPN, SD-WAN, WAN.

Abstract

Companies that have already deployed a DMVPN network are questioning the relevance of migrating to SD-WAN. SD-WAN is highly valued for its ability to enhance connectivity among an organization's various sites, resulting in improved performance and increased flexibility.

In our study conducted at NAFTAL, we implemented two distinct architectures : DMVPN, an established wide area network (WAN) solution, and SD-WAN, an emerging technology that is gaining significant interest.

Our primary objective is to conduct a comprehensive evaluation of the advantages and disadvantages associated with each option, taking into consideration crucial criteria such as performance, security, flexibility, and centralized system management. By doing so, we aim to provide companies with the necessary insights to make well-informed decisions regarding the most suitable choice for their WAN, with a strong focus on optimizing connectivity between remote sites.

Key Word : DMVPN, SD-WAN, WAN.

ملخص

تتساءل الشركات التي قامت بالفعل بتطبيق شبكة DMVPNعلى مستوى هياكلها عن مدى ملاءمة ترحيل هذه الأخيرة إلى تقنية أحدث هي SD-WAN حيث تحظى شبكةSD-WAN بتقدير كبير لقدرتها على تعزيز الاتصال بي المواقع المختلفة للمؤسسة، مما يؤدي إلى تحسين الأداء وزيادة المرونة.

في دراستنا التي أجريت على مستوى الشركة الوطنية نفطالNAFTAL ، قمنا بالعمل على تنفيذ هيكلين متميزين، أولهما DMVPN وهو حل منشئ للشبكة ذات المساحة الواسعةWAN ، وثانيهما SD-WAN وهي تقنية حديثة ناشئة تكتسب اهتمًاما كبيرا.

هدفنا الأساسي يعتمد على إجراء تقييم شامل للمزايا والعيوب المرتبطة بكل خيار، مع الأخذ في الاعتبار المعايير الأساسية والمهمة مثل الأداء والأمن والمرونة وإدارة النظام المركزي. من خلال القيام بذلك، نسعى إلى تزويد الشركات بالرؤى الازمة لإتخاذ قرارات مستنيرة فيما يتعلق بالخيار الأنسب للشبكة ذات المساحة الواسعة WANالخاصة بهم، مع التركيز القوي على تحسين الاتصال بين المواقع البعيدة.

الكلمات الدالة: DMVPN ,WAN،SD-WAN .

Remerciements

***En premier lieu**, Je tiens à remercie mon Dieu pour ses bénédictions et pour m'avoir accordé la volonté, le courage et la patience nécessaires pour présenter ce travail.*

* *Je tiens à exprimer ma profonde gratitude envers mon promoteur, Mr **MOHAMED BENYAHIA** et mon encadreur, Mr **ANES BENSADAT**, pour leurs conseils inestimables tout au long de montravail. Leurs connaissances, leur expertise et leur soutien ont été d'une importance pour la réalisation de ce mémoire.*

* *Je tiens à exprimer ma profonde gratitude envers les **membres du jury** pour l'honneur qu'ils ont accordé en acceptant d'évaluer ce travail. Leur expertise et leurs commentaires précieux joueront un rôle essentiel dans l'amélioration et l'enrichissement de ce mémoire.*

* *Je tiens à exprimer mes sincères remerciements à toutes les personnes qui ma apporté leur aide, que ce soit de près ou de loin, dans la réalisation de ce mémoire.*

Dédicace

Je dédie ce modeste travail à :

* ***À mes très chers parents,*** *il est impossible de trouver des mots suffisamment éloquents pour exprimer à quel point vous méritez ma gratitude pour tous les sacrifices que vous avez faits et le soutien inconditionnel que vous m'avez toujours accordé. Votre amour, votre dévouement et votre présence ont été des pierres essentielles dans ma vie.*

* ***À ma sœur et à mes frères en particulier, ainsi qu'à toute ma famille en général,*** *qui ont été toujours là pour me soutenir par leurs conseils, leurs encouragements et tout l'amour qu'ils me procurent.*

* ***À toute l'équipe de la Direction Infrastructure au sein de NAFTAL,*** *je suis vraiment reconnaissante d'avoir pu effectuer mon stage au sein d'une équipe incroyable et compétente. Votre soutien précieux et vos conseils tout au long du processus ont été d'une importance cruciale. Chaque membre de l'équipe a contribué de manière unique, ce qui a considérablement enrichi mon expérience.*

* ***À tous mes amis sans exception,*** *qui m'ont toujours encouragé, et à qui je souhaite plus de succès.*

Table des matières

Introduction générale

1 Etat de l'art **1**
- 1.1 Introduction . . . 1
- 1.2 Présentation de la société NAFTAL . . . 1
  - 1.2.1 Organisation de la Société NAFTAL . . . 1
  - 1.2.2 Missions principales de NAFTAL . . . 2
- 1.3 Réseaux WAN . . . 2
  - 1.3.1 Définition . . . 2
  - 1.3.2 Types de connexions WAN . . . 3
  - 1.3.3 Topologies de WAN . . . 4
  - 1.3.4 Limitation des réseaux WAN traditionnels . . . 4
- 1.4 Problématique . . . 4
- 1.5 Conclusion . . . 5

2 Architecture DMVPN et SD-WAN **6**
- 2.1 La technologie Dynamique multipoint VPN (DMVPN) . . . 6
  - 2.1.1 Historique . . . 6
  - 2.1.2 Définition . . . 6
  - 2.1.3 Principes du DMVPN . . . 6
  - 2.1.4 Protocoles de routages dynamique sur le réseau DMVPN . . . 8
  - 2.1.5 Les différentes phases du DMVPN . . . 9
  - 2.1.6 Les avanatge du DMVPN : . . . 9
- 2.2 Software Defined Wide Area Network . . . 10
  - 2.2.1 Introduction . . . 10
  - 2.2.2 Définition : . . . 10
  - 2.2.3 Les types d'architectures SD-WAN . . . 11
  - 2.2.4 Les avantages du SD-WAN . . . 11
  - 2.2.5 Topologie réseau SD-WAN . . . 12
  - 2.2.6 Composant de service SDWAN : . . . 13
  - 2.2.7 Déférents SD-WAN sur le marché international : . . . 13
  - 2.2.8 DMVPN vs le SD-WAN : . . . 15
- 2.3 Conclusion : . . . 16

3 Implementation **18**
- 3.1 Introduction . . . 18
- 3.2 Description de l'environnement de travail . . . 18
  - 3.2.1 Les équipements utilisés lors de l'implémentation . . . 18
  - 3.2.2 Ressources logicielles . . . 18
- 3.3 Déploiement du DM-VPN au niveau de GNS3 : . . . 20
  - 3.3.1 Topologie du réseau DMVPN . . . 20
  - 3.3.2 Configuration . . . 21
- 3.4 Déploiement du DM-VPN dans l'équipement CISCO au niveau de NAFTAL : . . . 26
  - 3.4.1 Configuration du SPOKE (DG-DSL-3G) . . . 26
  - 3.4.2 Mise en œuvre des Tunnels . . . 28
  - 3.4.3 Vérification l'état des interfaces de router (Spoke) : . . . 29
  - 3.4.4 Activation de protocole de routage EIGRP : . . . 29

3.4.5 Configuration de route-map : 30
3.5 Déploiement du SD-WAN au niveau de GNS3 30
3.5.1 Topologie du réseau SD-WAN : 31
3.5.2 Configuration : 31
3.6 Déploiement du SD-WAN au niveau de l'équipment Fortigate : 46
3.6.1 ETAPE 1 46
3.6.2 ETAPE 2 46
3.6.3 ETAPE 3 47
3.6.4 ETAPE 4 : Le déploiement d'un pare-feu FortiGate 48
3.6.5 ETAPE 5 : Vérification de la mise en œuvre du protocole de routage BGP 49
3.6.6 ETAPE 6 : Mise en place de la solution SD-WAN 49
3.7 Conclusion : 50

4 Resultats et discussions **51**
4.1 Introduction 51
4.2 Résultats des tests effectués sur la technologie DMVPN 51
4.2.1 Vérification des tunnels DMVPN établis (show dmvpn) 51
4.2.2 Affichage des entrées NHRP pour les réseaux distants accessibles via les tunnels DMVPN (commande "show ip nhrp") 53
4.2.3 Analyse le chemin des paquets à l'aide de la commande (Traceroute) . . 54
4.3 Résultats des tests effectués sur la technologie SD-WAN 55
4.3.1 Résultats des performances SLA après génération du trafic 55
4.3.2 Génération de trafic réseau : 56
4.4 Évaluation comparative des performances de DMVPN et SD-WAN en se basant sur les résultats obtenus 57
4.4.1 Scénario de test pour la redondance et le basculement 57
4.4.2 Analyse comparative des résultats obtenus : 61
4.5 Conclusion 61

Conclusion générale

Table des figures

1.1 schéma de la macrostructure de NAFTAL SPA. 1

2.1 Next Hop Resolution Protocol NHRP [9]. 7
2.2 Encapsulation GRE/IP sec d'un paquet IP [25]. 7
2.3 Encapsulation AH sur tunnel et mode de transport [14]. 8
2.4 Encapsulation ESP sur tunnel et mode transport [14]. 8
2.5 Décomposition des trois phases DMVPN [28]. 9
2.6 Architecture SD-WAN [3]. 10
2.7 Réseaux WAN traditionnels vs SD-WAN [7]. 11
2.8 Architecture SD-WAN [5]. 12
2.9 Architecture SD-WAN [4]. 13
2.10 Magic Quadrant pour l'infrastructure SD-WAN [19]. 14

3.1 l'interface de la machine virtuel VMware Workstation. 19
3.2 Affichage du résumé des serveurs Docks dans GNS3. 19
3.3 topologie DMVPN sur GNS3. 20
3.4 Implémentation de tunnels mGRE (Tun0) sur le routeur HUB. 21
3.5 Implémentation de tunnels mGRE (Tun1) sur le routeur HUB. 22
3.6 Implémentation de tunnels mGRE (Tun0) sur le routeur Spoke. 23
3.7 Implémentation de tunnels mGRE (Tun1) sur le routeur Spoke. 23
3.8 Configuration du cryptage IP sec au niveau de HUB and Spoke. 24
3.9 Activation du protocole EIGRP. 25
3.10 Affichage des voisins EIGRP actuels via la commande sh ip eigrp neighbors (HUB). 25
3.11 Affichage des voisins EIGRP actuels via la commande sh ip eigrp neighbors (Spoke). 26
3.12 Configuration du profil IP sec. 27
3.13 Création des tunnels 0 et 1. 28
3.14 Exécution de la command show IP interface brief. 29
3.15 Configuration de routage EIGRP. 29
3.16 Configuration de routage EIGRP. 30
3.17 Topologie Dynamique Multipoint Virtuel Privat Network (SD-WAN) Sur GNS3. 31
3.18 Configuration VPN IPsec phase1-interface "ADVPN_4G" et "ADVPN_ADSL" au niveau de HUB via CLI. 32
3.19 Configuration VPN IPsec phase1-interface "ADVPN_4G" via l'interface graphique de FortiGate au niveau du HUB. 33
3.20 Configuration VPN IPsec phase1-interface "ADVPN_ADSL" via l'interface graphique de FortiGate au niveau du HUB. 34
3.21 Configuration VPN IPsec phase2-interface "ADVPN_ADSL" et "ADVPN_4G" au niveau de HUB via CLI. 34
3.22 Configuration VPN IPsec phase2-interface "ADVPN_ADSL" et "ADVPN_4G" au niveau de HUB interface graphique. 35
3.23 État des deux tunnels VPN IPsec au niveau du HUB. 35
3.24 Configuration VPN IP sec phase1-interface "ADVPN_ADSL" et "ADVPN_4G" au niveau de SPOKE1 via CLI. 36
3.25 Configuration VPN IP sec phase1-interface et "ADVPN_4G" via l'interface graphique de FortiGate dans le SPOKE1. 37
3.26 Configuration VPN IP sec phase1-interface "ADVPN_ADSL" via l'interface graphique de FortiGate dans le SPOKE1. 37

3.27 Configuration VPN IP sec phase2-interface "ADVPN_4G" et "ADVPN_ADSL" via CLI au niveau de SPOKE1. 38
3.28 Configuration VPN IP sec phase2-interface "ADVPN_4G" et "ADVPN_ADSL" via l'interface graphique de FortiGate au niveaux de SPOKE1. 38
3.29 État des deux tunnels VPN IPsec au au niveau du SPOKE1. 39
3.30 Configuration de la liste de communautés SLA_OK sur le périphérique HUB via CLI a gauche et l'interface graphique de FortiGate a droit. 39
3.31 Configuration d'une route-map sur le périphérique HUB via CLI à gauche et l'interface graphique de FortiGate a droit. 40
3.32 configuration de BGP au niveau de HUB via CLI. 40
3.33 Vue d'ensemble des routes BGP et des interfaces de tunnel pour les destinations Spokes au niveau de HUB. 41
3.34 Configuration d'une route-map sur le périphérique SPOKE1 via CLI à gauche et l'interface graphique de FortiGate a droit. 42
3.35 configuration de BGP au niveau de SPOKE1 via CLI. 42
3.36 Vue d'ensemble des routes BGP et des interfaces de tunnel pour les destinations, au niveau de SPOKE1. 43
3.37 Affichage des zones SD-WAN. 43
3.38 Configuration de route statique pour la zone SD_WAN_INTERNET. 44
3.39 Configuration des firewall policy pour le sdwan zone. 44
3.40 Affichage SLA Performances SD-WAN. 45
3.41 Edition d'un accès internet SD-WAN.. 45
3.42 Interface d'accueil du pare-feu FortiGate. 46
3.43 Affichage des interfaces réseau. 47
3.44 Affichage des routes statiques configurées. 47
3.45 Affichage des règles de pare-feu (Firewall Policy). 47
3.46 Affichage des connexions IPSec (IPSec Tunnels). 48
3.47 Affichage du statut des tunnels VPN IPSec. 48
3.48 Vue d'ensemble des routes BGP et des interfaces de tunnel pour les destinations spécifiées. 49
3.49 Vue d'ensemble des zones SD-WAN. 49
3.50 Mise à jour des performances SLA. 50

4.1 Contrôle de l'état du protocole DMVPN dans le HUB. 51
4.2 Contrôle de l'état du protocole DMVPN dans le Spoke. 52
4.3 Affichage des routes via le protocole NHRP. 53
4.4 Affichage des routes via le protocole NHRP (spoke1). 53
4.5 Résultats du traceroute de DMVPN. 54
4.6 Résultat de la commande TraceRoute (Phase 1). 54
4.7 Résultat de la commande TraceRoute (Phase 2). 55
4.8 Affichage SLA Performances SD-WAN Packet Loss. 55
4.9 Affichage SLA Performances SD-WAN Latency. 56
4.10 Affichage SLA Performances SD-WAN Jitter. 56
4.11 Affichage du trafic réseau. 57
4.12 Envoi de paquets en continu vers un site distant au niveau de DMVPN. 58
4.13 Shutdown le tunnel ADSL. 58
4.14 Comportement du Ping continu au niveau de DMVPN. 59
4.15 Envoi un Ping continue vers un site distant au niveau de SD-WAN. 59
4.16 Shutdown le tunnel HQ2-Inet1. 60
4.17 Comportement du ping continu au niveau de SD-WAN. 60

Liste des tableaux

2.1 Réseaux WAN traditionnels vs $SD-WAN$ 11
2.2 Tableau comparatif entre les implémentations $SD-WAN$ 15
2.3 Comparaison entre une solution $DMVPN$ et une solution $SD-WAN$ 16

3.1 Les ressources logicielles utilisées 20

Liste des symboles

ACL Access Control List

ADSL Asymmetric Digital Subscriber Line

ADVPN Auto-Discovery Vertuel Private Network

AH Authentification Headers

API Application Programming Interface

ARP Address Resolution Protocol

AS Autonomes System

BGP Border Gateway Protocol

DH Diffie-Hellman

DMVPN Dynamique Multipoint Virtual Private Network

DSL Digital Subscriber Line DSL

DWDM Dense Wavelengths Division Multiplexing

EIGRP Enhanced Interior Gateway Routing Protocol

ESP Encapsulating Security Payload

GRE Generic Routing Encapsulation

IETF Internet Engineering Task Force

IP Internet Protocol

IP sec Internet Protocol Secure

ISAKMP Internet Security Association and Key Management Protocol

ISP Internet Service Provider

LAN Local Area Network

LTE Long-Term Evolution

mGRE multipoint Generic Routing Encapsulation

MPLS Multiprotocol Label Switching

NAT Network Address Translation

NBMA Non-Broadcast Multi-Access

NGFW Next Generation FireWall

NHC Next Hop Client

NHRP Next Hop Routing Protocol

NHS Next Hop Server

OSPF Open Shortest Path First

P2P Point to Point

SD-WAN Software-Defined Wide Area Network

SDH Synchronous Digital Hierarchy

SDN Sofware Defined Network

SLA Service Level Agreement

SONET Synchronous Optical Network

VPN Virtual Private Network

WAN Wide Area Network

ZTP Zero Touch Provisioning

Introduction générale

De nos jours, les entreprises cherchent à améliorer leur productivité et à répondre aux demandes croissantes des clients en établissant des filiales dans différentes régions géographiques. Pour assurer une connectivité sécurisée entre ces filiales, l'utilisation de réseaux informatiques est indispensable. Les VPN (Virtual Private Networks) sont largement utilisés pour interconnecter de manière sécurisée ces filiales via Internet. Il est essentiel de surveiller régulièrement les équipements de chaque filiale pour maintenir des performances réseau efficaces.

Dans ce contexte, NAFTAL est la principale entreprise sur le marché de l'industrie pétrolière en Algérie, s'est fixé deux objectifs principaux. Tout d'abord, l'entreprise cherche à améliorer l'intégration et l'harmonisation des informations au sein du groupe en centralisant les données provenant de toutes ses filiales vers un Datacenter unique. De plus, NAFTAL vise à garantir une connexion sécurisée entre tous ses sites pour assurer la confidentialité et l'intégrité des flux de données.

Afin de moderniser leur système d'information et tirer parti des dernières technologies, notamment le SD-WAN (Software-Defined Wide Area Network), NAFTAL a décidé de se joindre à d'autres organisations engagées dans ce processus de transformation. NAFTAL consiste à adapter le réseau WAN aux évolutions technologiques récentes pour garantir une connectivité continue. Actuellement basé sur la technologie DMV PN, le réseau relie les sites distants au site central et centralise les données vers le Datacenter ,NAFTAL envisage de migrer du DMVPN vers une architecture SD-WAN afin de mieux préparer son réseau aux défis actuels et futurs. . La problématique réside donc dans la planification, la mise en œuvre et la gestion de cette migration pour optimiser les performances du réseau et maximiser les avantages offerts par l'architecture SD-WAN.

Ce projet est divisé en quatre parties qui couvrent l'ensemble de l'étude. La première partie présente une analyse détaillée de l'entreprise NAFTAL, où le stage a été réalisé. Les différents services et départements de cette institution sont examinés, avec une attention particulière portée sur le réseau étendu (WAN) et ses limites, mettant en évidence les problèmes potentiels. Cela permettra ensuite d'explorer en détail le SD-WAN et ses avantages par rapport aux solutions traditionnelles.

La deuxième partie se concentre sur le protocole DMVPN, en fournissant des informations sur ses composants, son fonctionnement et ses limitations. L'architecture SD-WAN est également abordée, en expliquant son fonctionnement, ses avantages et ses performances par rapport au WAN traditionnel et à l'utilisation du DMVPN.

La troisième partie se concentre sur la mise en œuvre concrète de notre approche pour résoudre le problème identifié. Nous décrivons en détail les différentes architectures et configurations mises en place pour mener à bien le projet, en mettant en avant les solutions techniques utilisées tout au long de cette étape. La quatrième partie présente les résultats obtenus suite à la mise en œuvre de notre solution de migration de l'infrastructure DMVPN vers une architecture SD-WAN, appliquée spécifiquement à NAFTAL, sur les équipements réels de l'entreprise.

En conclusion, nous réalisons une synthèse des éléments essentiels abordés dans ce travail, mettant en évidence les principaux points traités tout au long de l'étude.

1 Etat de l'art

1.1 Introduction

Dans ce chapitre, nous allons découvrir en premier lieu l'entreprise NAFTAL, et explorer son infrastructure, ses activités et ses besoins spécifiques en matière de réseau étendu.
Par la suite, nous plongerons dans le domaine du WAN en général, en étudions les principes fondamentaux,les différents types de connexions WAN ainsi que les topologies utilisées, ainsi que ses limites.

1.2 Présentation de la société NAFTAL

A présent, on passe à la présentation de NAFTAL. Son nom, composé du « NAFT » qui signifie pétrole en arabe, et « AL » qui est une abréviation du mot « Algérie », décrit son statut comme La société national de Distribution et de Commercialisation des Produit Pétroliers a travers le territoire national.
Au cours de ce chapitre, nous allons aborder son histoire, ses missions principales, ses produits commercialisée et son organisation structurelle.

1.2.1 Organisation de la Société NAFTAL

Afin de répondre aux exigences aux strictes exigence économiques de la mondialisation, NAFTAL a connu à changement au schéma d'organisation de sa macrostructure le 18 Aout 2010, qui est présenté dans la figure 1.1

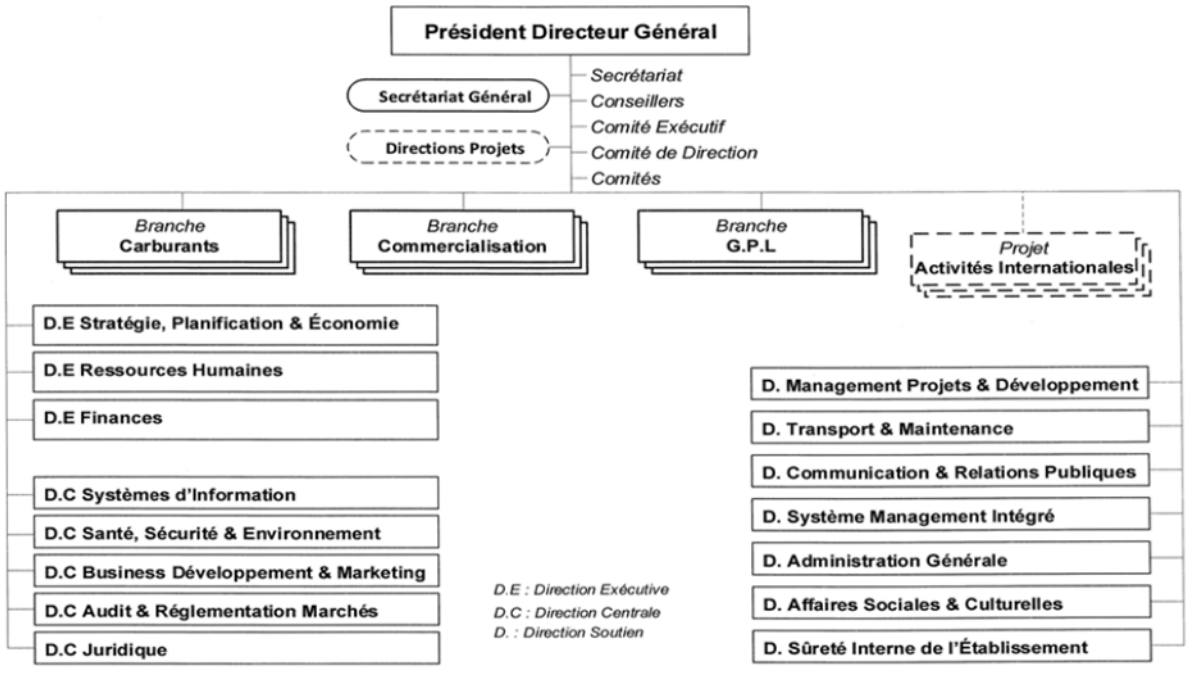


FIGURE 1.1 – schéma de la macrostructure de NAFTAL SPA.

Les structures principales de NAFTAL sont comme suit :
La Direction Générale : qui est chargée de définir la politique et les axes stratégiques et les actions à entreprendre, elle gère aussi la coordination et la cohérence d'ensemble, le pilotage, le management et la veille stratégique. Elle comprend des structures fonctionnelles organisées comme suit :

- **Directions Exécutives :** sont au nombre de trois ; Direction Exécutive Stratégies Planification et Economie, Direction Exécutive Finance et Direction Exécutive Ressources Humaines chargées de la stratégie et de la gestion des ressources.
- **Directions Centrales :** sont au nombre de cinq ; Direction Centrale Systèmes d'Information, Direction Centrale Santé Sécurité & Environnement , Direction Centrale Business Développement & Marketing, Direction Centrale Audit & Réglementations Marchés et Direction Centrale Juridique chargées de la coordination et du contrôle.
- **Directions de soutiens :** sont au nombre de sept ; Direction Management Projets & Développement ; Direction Transport & Maintenance, Direction Communication & Relations Publiques, Direction Systèmes Management Intégré, Direction Administration Générale, Direction Affaires Sociales & Culturelles , Direction Sûreté Interne de l'Etablissement chargées de l'assistance.

Les Structures Opérationnelles : devisé principalement en trois branches.

- Branche Carburants.
- Branche GPL.
- Branche Commercialisation.

Se composant eux même de 41 districts sur tout le territoire national, toutes activités confondues (CBR, GPL, COM), ainsi que 3 centres de formations à travers le pays (Alger, Oran et El Khroub)

Actuellement, NAFTAL compte 24 Centres lubrifiants et pneumatiques, 48 centres de distributions, un réseau de 2276 stations-service ou 692 en propriété NAFTAL dont 393 stations-service GD (Gestion Directe), 16 centres bitumes, 6 centres marine, 30 centres et dépôts aviation, 41 dépôts carburants, 41 centres emplisseurs, 48 dépôts relais, 10 centres vrac GPL.

1.2.2 Missions principales de NAFTAL

NAFTAL a pour mission principale la commercialisation et la distribution des produits pétroliers à travers tout le territoire, y compris la commercialisation des produits destinés à l'aviation et à la marine ainsi que des produits hors-fuel (les solvants, les aromatiques, paraffines, Bitumes, lubrifiants et pneumatiques). Ses missions essentielles sont :

- Organisation et développement de l'activité de commercialisation et de distribution des produits pétroliers et dérivés.
- Stockage et transport de tout produit pétrolier commercialisés sur le territoire national.
- La veille à l'application et au respect des mesures relatives à la sécurité industrielle, la sauvegarde et la protection de l'environnement en relation avec les organismes concernés, ainsi que la sûreté interne de la société conformément à la réglementation.
- Etude de marché en matière d'utilisation et de consommation des produits pétroliers.
- Définition et développement des politiques d'audit et la conception et la mise en œuvre des systèmes intégrés d'informations.
- Développement et mise en œuvre des actions visant à l'utilisation optimale et rationnelle des infrastructures et moyens disponible.
- Développement d'une marque de qualité.

1.3 Réseaux WAN

1.3.1 Définition

Un réseau étendu WAN est un réseau de communication de données qui s'étend sur une grande zone géographique, que ce soit à l'échelle d'une ville, d'un pays ou même mondiale. Son objectif principal est la transmission de données entre différents équipements et de connecter les réseaux locaux LAN entre eux. Pour benificier des services WAN, une entreprise doit s'abonner à un fournisseur de services WAN qui fournit des liaisons de transmission à longue distance.

Ces fournisseurs de services WAN sont généralement des entreprises de télécommunications qui offrent des services de connectivité aux entreprises.
Un réseau WAN est conçu pour réaliser les fonctions suivantes :

- Réaliser une communication en temps réel entre les utilisateurs dans les différents sites.
- Permettre le transfert de données, voix et vidéo.
- Utiliser des connexions en série de plusieurs types pour donner l'accès à des larges régions géographiques [2].

Les réseaux WAN sont principalement constitués de supports de transmission, ainsi que d'éléments de commutation et des systèmes intermédiaires de commutation par paquets. Ces éléments sont responsables de la connexion des sous-réseaux locaux les uns aux autres et assurent un transport fluide des données entre eux [27].

1.3.2 Types de connexions WAN

Il existe de nombreuses connexions WAN utilisées pour fournir la connectivité à Internet.les options courantes de connectivité WAN du fournisseur d'accès Internet sont :

1.3.2.1 Ligne louée

Ce type de connexion WAN est une liaison point à point dédiée et une connexion de données à bande passante fixe, ce réseau aura une connexion entièrement fiable et sécurisée, un débit de données élevé et une qualité de service supérieure [12].

1.3.2.2 Ligne d'abonné numérique

La DSL est une technologie utilisée pour transmettre des signaux numériques sur des lignes téléphoniques traditionnelles. La DSL est la technologie la plus ancienne qui offre généralement une vitesse de connexion d'environ 6 Mbps [12].

1.3.2.3 Internet par câble

Une façon d'obtenir une connexion Internet à haut débit est d'utiliser Internet via le câble fourni par un fournisseur local de télévision par câble. Cette méthode présente des similitudes avec la DSL, car elle utilise un modem câble déjà existant provenant de la télévision par câble pour envoyer les données. La vitesse de cette connexion varie en fonction du nombre d'utilisateurs qui utilisent activement le service à un moment donné [12].

1.3.2.4 Accès Internet Fibre

C'est la connexion haute vitesse la plus récente qui offre le service Internet le plus rapide aux utilisateurs, et elle est fréquemment utilisée dans les connexions de télécommunications en raison de sa capacité plus rapide que d'autres câbles de télécommunications.
$DWDM$, $SONET$, et SDH sont l'équipement ISP pour le transport de liaison qui utilisent un câble de fibre optique, et ce dernier est également utilisé dans les réseaux pour la commutation de paquet [12].

1.3.2.5 Commutation multi protocole par étiquette (MPLS)

$MPLS$ est un type de VPN qui utilise des étiquettes sur les paquets de transfert plutôt que des adresses IP ou des en-têtes de couche 3. Il offre une sécurité et un routage optimaux pour les sites clients. Le fournisseur de services participe au processus de routage du client sur $MPLS$ [12].

1.3.2.6 Réseau étendu sans fil

La majorité des utilisateurs se servent de smartphones qui utilisent des données mobiles pour se connecter à Internet. Les technologies de connexion sans fil les plus répandues pour le réseau étendu WAN sont la 3G, la 4G, la LTE et la 5G. Ces services sont proposés par les fournisseurs d'accès Internet locaux afin de fournir un accès Internet sans fil aux appareils mobiles par le biais de stations cellulaires. Ils utilisent des fréquences spécifiques pour offrir une couverture plus étendue et un signal plus puissant aux clients [12].

1.3.3 Topologies de WAN

Les technologies WAN peuvent être classées en point à point (P2P) ou multipoint, telles que les services $MPLS$ WAN. La plupart des fournisseurs de services WAN proposent des solutions $MPLS$ WAN, où le routeur d'entreprise communique avec le routeur du fournisseur de services au niveau de la couche 3. Il existe également des connexions WAN publiques sur Internet, allant des technologies sans fil 4G aux options filaires offrant une connectivité multi-gigabit [20]. Les principales topologies utilisées sur les WAN sont indiquées ci-dessous :

- Point-to-Point
- Hub and Spoke
- Full Mesh
- Dual-Homed

1.3.4 Limitation des réseaux WAN traditionnels

Les réseaux WAN ont été largement adoptés par les entreprises depuis de nombreuses années. Cependant, les besoins des entreprises évoluent constamment, ce qui les pousse à repenser leurs réseaux WAN traditionnels pour plusieurs raisons :

Mauvaise exploitation de la bande passante : Les réseaux utilisent généralement une architecture "Passive-Active" où la liaison de secours s'active seulement lorsque la liaison principale tombe en panne. Cela signifie que les entreprises investissent dans une bande passante qu'elles utilisent rarement [24].

Lenteur des opérations réseau : Les changements, modifications ou mises à jour dans le réseau sont souvent effectués manuellement, équipement par équipement, ce qui prend beaucoup de temps. Selon une étude de 2016 sur les intentions d'achat en matière de réseau, cela peut prendre jusqu'à quatre mois [24].

Coût élevé : Les solutions MPLS proposées par les opérateurs sont souvent très coûteuses. De plus, il y a des coûts supplémentaires liés au déploiement, aux équipements et à l'installation d'une liaison MPLS vers une nouvelle succursale [24].

Erreurs humaines : Dans les réseaux traditionnels, la gestion des configurations est effectuée manuellement par les administrateurs réseau, ce qui entraîne souvent des erreurs [24].

Évolution du Cloud : L'adoption croissante des applications Cloud dans les entreprises d'aujourd'hui entraîne une augmentation considérable du trafic réseau, cela consomme une quantité importante de bande passante sur la ligne spécialisée, qui est souvent coûteuse [24].

1.4 Problématique

Pour assurer une connectivité continue, NAFTAL a mis en place un réseau WAN basé sur la technologie $DMVPN$ (liaisons VPN) afin de connecter ses sites distants au site central et de centraliser les données vers son Datacenter.

Cependant, l'évolution des approches définies par logiciel a engendré une véritable transformation des systèmes traditionnels de réseau. Ces approches offrent des avantages considérables tels que la réduction des coûts, une plus grande agilité, une flexibilité accrue, une mise en œuvre plus rapide et une meilleure capacité d'adaptation.
Par conseqaunt, Naftal pense a une migration du $DMVPN$ vers une architecture $SD-WAN$. afin de mieux préparer son réseau aux défis actuels et futurs.

1.5 Conclusion

Dans ce chapitre, nous avons discuté NAFTAL et ses besoins en terme des réseaux informatiques, ce qui nous a mené à une étude sur les réseaux WAN courrament utilisé, ainsi qu'un petit apperçu sur ses limitaions, qui a poussé NAFTAL à migrer vers des architectures plus adapté à ses besoins. Dans le chapitre suivant le $DMVPN$ et $SD-WAN$ seront présentés afin de passer par la suite à leur utilisation dans le cadre de ce projet.

2 Architecture DMVPN et SD-WAN

2.1 La technologie Dynamique multipoint VPN (DMVPN)

2.1.1 Historique

Afin de sécuriser les connexions via internet, les fournisseurs de services arrivent en premier avec la solution d'$IPSec$, où deux sites sont connectés sur internet via un processus de tunnel crypté sécurisé. Cette dernière, malgré son excellent fonctionnement, ne peut malheureusement pas être évolutif entre plusieurs sites, car elle sécurise que les connexion point à point.
En effet, l'ajout d'un site nécessite une configuration complexe, en interne de pour les équipement mis en production, mais surtout, pour la mise a l'échelle car plus les sites augmentes plus la configuration du site central devient rapidement difficile à gérer. Aussi, ce type de VPN ne supporte pas le routage dynamique et le Multicast.
Ces principales limites ont poussé les fournisseurs de services et les Original Equipment Manufacturer à conclure une manière de connectivité évolutive et sécurisée entre sites via Internet et cette technologie est appelée $DMVPN$(Dynamique Multipoint Virtual Private Network)[10][18].

2.1.2 Définition

$DMVPN$ est une solution qui permet de déployer un nombre important des tunnels entre sites de manière automatique, dynamique et sécurisée, avec une configuration minimale. Cette technologie suit une architecture client-serveur, où chaque cloud $DMVPN$ dispose d'un serveur au minimum appelé HUB et plusieurs clients nommés Spokes. La connexion HUB-Spoke est établie via des tunnels permanents, tandis que la connexion entre deux Spokes est réalisée dynamiquement à la demande, via le HUB. il utilise divers protocoles normalisés pour assurer la sécurité et la fiabilité des connexions [16].

2.1.3 Principes du DMVPN

2.1.3.1 Fonctionnement générale

Le DMVPN est un mécanisme qui établie des tunnels $IPsec/GRE$ (Generic Routing Encapsulation) directement entre les routeurs qui veulent interagir de manière simple et dynamique. GRE est un protocole d'encapsulation permettant l'encapsulation des paquets multidiffusion et diffusion dans un paquet de monodiffusion. Par conséquent, il sera chiffré en utilisant $IPsec$. Fondamentalement, la solution consiste à implémenter des paquets multidiffusion à l'aide de tunnels GRE, sécurisés par l'$IPsec$ [25]. Les composants du $DMVPN$ sont comme suit :

2.1.3.1.1 Protocole de résolution du prochain saut (NHRP) $NHRP$ est un protocole de type ARP destiné à la résolution de l'adressage dynamique des routeurs distants sur un réseau $NBMA$ (Non-Broadcast Multi-Access). Il permet à un client Next-Hop (NHC) de s'enregistrer auprès d'un serveur Next-Hop (NHS). Il assure la communication directe entre spokes selon les besoins. $NHRP$ fonctionne dans un modèle client-serveur :

- NHS est le routeur concentrateur (HUB)
- NHC sont les routeurs en étoile (Spoke).

Le NHS conserve une base de données $NHRP$ qui effectue la cartographie des adresses physiques et des tunnels de tous les Spokes enregistrés.
Les NHC s'auto-enregistrent auprès du NHS au démarrage et peuvent interroger la base de

données $NHRP$ pour obtenir des informations d'adressage d'autres Spokes lorsque des communications en étoile (Spoke-to-Spoke) sont nécessaires [9].

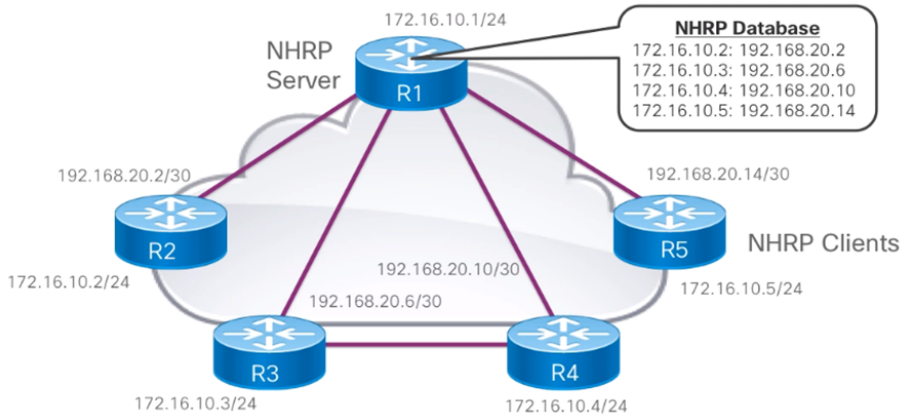


FIGURE 2.1 – Next Hop Resolution Protocol NHRP [9].

2.1.3.1.2 Encapsulation de routage générique multipoint (mGRE) L'encapsulation de routage générique multipoint ($mGRE$) est responsable de la création dynamique des tunnels. Les paquets multicast et broadcast sont transférés avec le $mGRE$ et cryptés avec le $IPSec$. Essentiellement, un en-tête GRE est ajoutée à chaque paquet ce qui transforme d'un paquet de diffusion ou de multidiffusion a un paquet monodiffusion. Étant donné que GRE utilise le même lien $IPsec$, l'en-tête $IPsec$ est appliquée pour chiffrer les données GRE. Néanmoins, il est impossible de changer l'adresse IP physique car l'$IPsec$ nécessite une adresse IP fixe pour créer un tunnel. Ce qui fait que l'adresse IP du tunnel GRE est inchangeable [25].

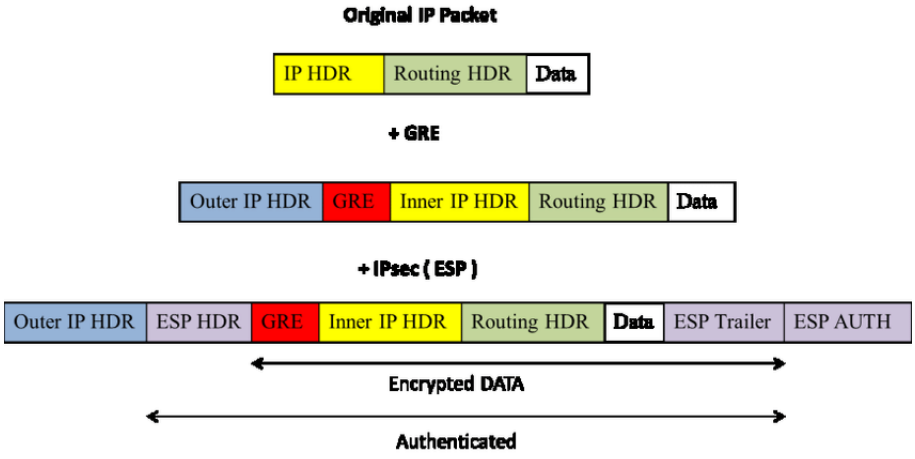


FIGURE 2.2 – Encapsulation GRE/IP sec d'un paquet IP [25].

2.1.3.1.3 sécurité du protocole Internet (IP sec) Ce protocole de chiffrement permet de crypter le trafic échangé entre deux sites en utilisant une clé partagée préalablement définie. Bien qu'il ne soit pas le protocole le plus sécurisé, sa popularité réside en sa facilité et rapidité à mettre en place.

1. **Les protocoles de transformation** L'$IPsec$ s'appuie sur les protocoles ESP et AH, qui peuvent être employés dans les modes tunnel ou transport. Nous allons aborder l'encapsulation de chaque protocole de ces deux modes distincts.
   (a) **Les en-têtes d'authentification (Authentification Headers – AH) :** Ces protocoles ont pour fonction la garantie de l'intégrité des données en l'absence de

connexion, ainsi que l'authentification des paquets IP. De plus, ils offrent une protection contre certains types d'attaques réseau. L'authentification a une importance cruciale, car elle permet de s'assurer que les paquets de données transmis sont bien ceux que l'on souhaite envoyer et recevoir, et qu'ils ne contiennent pas de programmes malveillants ou d'autres formes d'attaques potentiellement dangereuses. Plusieurs versions de ces protocoles sont disponibles, offrant différents niveaux de protection [13].

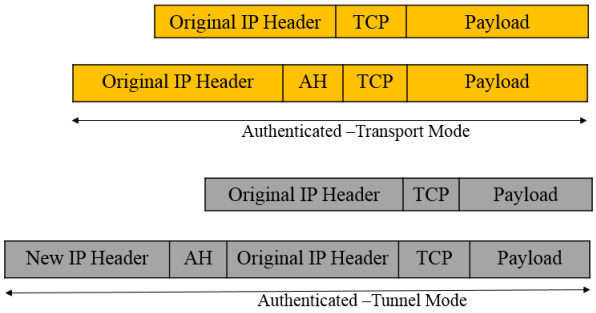


FIGURE 2.3 – Encapsulation AH sur tunnel et mode de transport [14].

(b) **La technologie ESP (Encapsulating Security Payload) :**Il garantit la confidentialité des paquets de données, l'intégrité de leur origine, la sécurité contre les attaques et une sécurisation appropriée des flux de trafic, assurant ainsi la sécurité de l'ensemble des paquets IP lorsqu'ils sont utilisés en mode tunnel.

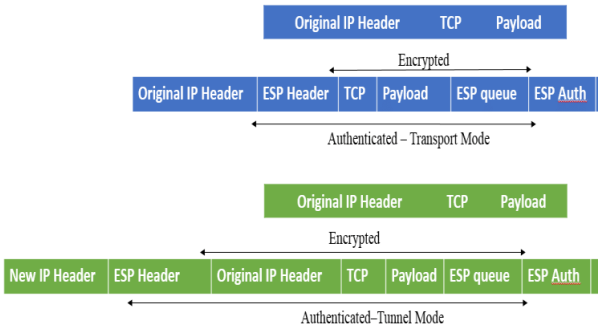


FIGURE 2.4 – Encapsulation ESP sur tunnel et mode transport [14].

2. **Modes d'IP Sec** On distingue deux modes d'utilisation d'$IPSec$: le mode transport et le mode tunnel, la différence significative entre eux est la façon dont les datagrammes sont générés.
   — **Mode Transport :** Le mode transport est utilisé pour les communications de bout en bout, ce mode ne change pas l'en-tête d'origine. Cependant, dans cas le champ du protocole IP est changé en ESP ou AH au préalable, la traduction d'adresses réseau peut entraîner des problèmes d'intégrité [14].
   — **Mode Tunnel :** Le mode tunnel est le mode par défaut, ce mode protège l'intégralité du paquet IP et encapsule le paquet d'origine, le chiffre, puis ajoute une nouvelle en-tête IP avant de l'envoyer [14].

L'annexe présente une partie expliquant les modeles de déploiment du $DMVPN$.

2.1.4 Protocoles de routages dynamique sur le réseau DMVPN

Un protocole de routage dynamique est obligatoire pour $DMVPN$. En effet, les protocoles de routage constituent une partie essentielle de la solution $DMVPN$, ils assurent le bon établissement des tunnels et ont un impact majeur sur le comportement du réseau et des applications

transportées. Par conséquent, plusieurs travaux ont été menés pour évaluer les performances du réseau afin de déterminer le protocole de routage le plus pratique [25].

2.1.4.1 Les objectifs des protocoles de routage

Les protocoles de routage dynamique sont responsables de créer les tables de routage. Les routeurs échangent des informations entre eux sur la topologie du réseau par moyens de ces tables, et ils analysent les données et définissent la route optimale pour la transmission des données [21].

Pour maximiser la performance de la technologie $DMVPN$, il est donc nécessaire d'utiliser des protocoles de routage adéquats pour manipuler, maintenir et mettre à jour la table de routage dynamique entre les différents sites du réseau [26]. Parmi les protocoles de routage utilisés pour $DMVPN$ on cite :

Enhanced Interior Gateway Routing Protocol (EIGRP)
$EIGRP$ est un protocole de vecteur de distance avancé développé par Cisco standardisé IETF [6], $EIGRP$ utilise la bande passante, le délai, charge et fiabilité pour calculer la métrique de sa table de routage. $EIGRP$ utilise l'algorithme Diffusing Update "DUAL" pour fournir une convergence rapide et pour déterminer si un chemin annoncé par un voisin est en boucle ou sans boucle, et permet à un routeur exécutant $EIGRP$ de trouver des chemins alternatifs sans attendre les mises à jour d'autres routeurs. Pour s'assurer que le réseau $DMVPN$ fonctionne parfaitement et garantit un routage dynamique optimal des échanges, certaines configurations doivent être effectués ; Côté HUB, l'option IP SPLIT HORIZON doit être désactivée pour s'assurer que le HUB annoncera les routes sortant du tunnel d'interface sur lequel elles ont été reçues, également, il faut désactiver l'option IP NEXT-HOP-SELF.
Au niveau des Spokes, l'option connectée STUB doit être activée afin de permettre au Spoke de réannoncer uniquement les routes directement connectées afin de réduire l'utilisation des ressources en optimisant la taille des mises à jour de routage et d'assurer la stabilité [15].

2.1.5 Les différentes phases du DMVPN

Le guide de conception $DMVPN$ de Cisco présente trois phases $DMVPN$ distinctes. En résumé, comme illustré dans la figure 2.5 ils sont les suivants : (Voir annexe)

	Phase I	Phase II	Phase III
Spoke-to-Spoke Communication	NO	YES Creates invalid CEF at first	YES Uses NHRP route
Distance Vector Summarization	YES	NO	YES
Distance Vector Summarization	YES	Not on hub	YES
EIGRP Routing	All routes from hub	"Reflect" routes to spokes	All routes from hub
OSPF Routing	P2MP Network	Broadcast Hub is DR (No BDR)	Broadcast Hub is DR (No BDR)

FIGURE 2.5 – Décomposition des trois phases DMVPN [28].

2.1.6 Les avanatge du DMVPN :

Les principaux avantages du $DMVPN$ sont [10] :

— Réduction des dépenses d'exploitation et d'immobilisation en intégrant la voix et la vidéo à la sécurité VPN.
— Simplification de la communication de la branche par une connectivité directe branche à branche pour les applications telles que la voix sur IP.
— Réduction de la complexité de déploiement par la mise en place d'une configuration simple, réduisant les difficultés de déploiement des VPN.
— Amélioration de la résilience de l'activité en empêchant les perturbations des services critiques.

2.2 Software Defined Wide Area Network

2.2.1 Introduction

Les réseaux $SD-WAN$ sont une évolution majeure des réseaux traditionnels. Ils offrent des fonctionnalités avancées de gestion et de contrôle du trafic pour les réseaux étendus. Contrairement aux réseaux WAN traditionnels qui nécessitent une configuration manuelle et complexe. Avec les réseaux SD-WAN, les entreprises peuvent étendre leurs réseaux sur de vastes zones géographiques tout en maintenant une connectivité rapide et fiable.

2.2.2 Définition :

Le $SD-WAN$ est l'application du SDN sur WAN. Ou un réseau logique se créé entre les sites, qui sera géré par les fournisseurs $SD-WAN$. Un site central est établi pour gérer la configuration, l'administration et les ressources du réseau pour faciliter le contrôle de toute l'infrastructure [23].
Pour les entreprises utilisant un WAN, la connectivité est généralement fournie via $MPLS$ ou une connexion Internet. La solution $MPLS$ offre une bande passante fixe et prédéfinie et des temps de réponse plus rapides, mais elle est couteuse et complexe à entretenir. Les solutions Internet quant à eux, sont beaucoup moins chères, mais sans garanti de qualité de service.
Le $SD-WAN$ permet l'utilisation de plusieurs technologies de connectivité en combinaison et, comme le montre la Figure 2.6, des règles sont mises en place pour définir la façon dont le trafic passe. Si un chemin échoue, le trafic est dynamiquement redirigé vers un autre chemin plus performant. Le $SD-WAN$ utilise des solutions de surveillance du réseau pour analyser ces conditions afin d'acheminer automatiquement le trafic en garantissant la qualité de service et d'expérience utilisateur.

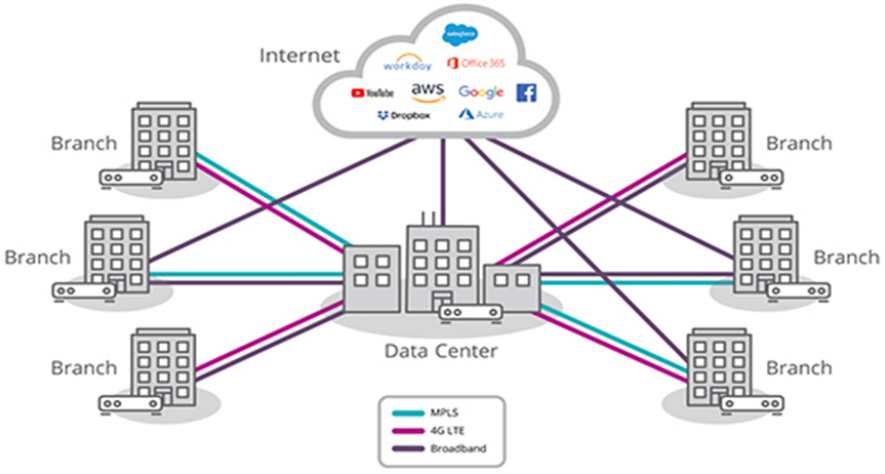


FIGURE 2.6 – Architecture SD-WAN [3].

Le tableau 2.1 résume les différences entre le WAN et le $SD-WAN$.

Réseaux WAN traditionnels	**Réseaux $SD-WAN$**
Configuration manuelle de l'appareil	Configuration centralisé
Coûts d'équipement et de système élevés	Coûts opérationnels et financiers réduits
Infrastructure statique	Infrastructure dynamique
Un temps élevé pour l'ajout de nouvelles applications	De nouvelles applications en moins de temps
Les politiques sont difficiles à appliquer	Sécurité accrue du réseau
Mauvaise expérience utilisateur	Amélioration de l'expérience utilisateur
Mauvaise performance	Performances supérieures

TABLE 2.1 – Réseaux WAN traditionnels vs $SD-WAN$

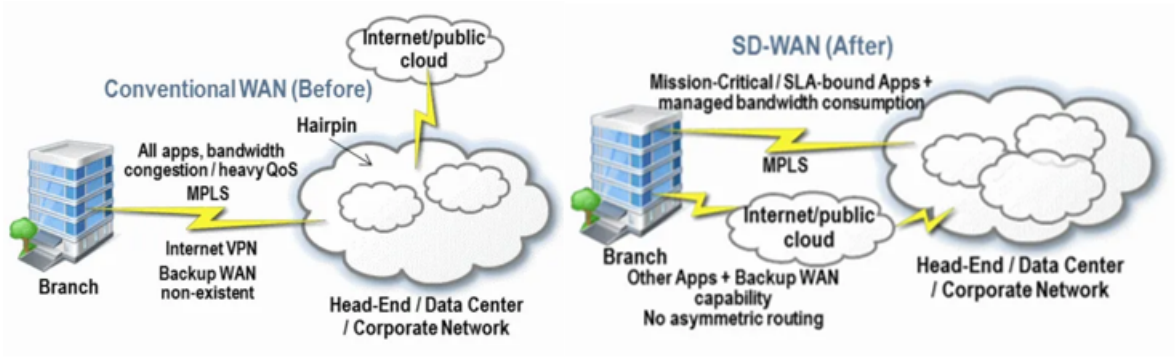


FIGURE 2.7 – Réseaux WAN traditionnels vs SD-WAN [7].

2.2.3 Les types d'architectures SD-WAN

Afin d'améliorer le réseau étendu d'une organisation, il est important de se familiariser d'abord avec les 3 types d'architectures $SD-WAN$, et puis le choix de l'architecture dépend de l'entreprise et des services qu'elle fournit (sont-ils hébergés localement ou sur le Cloud accessible via Internet) [3].

- **ON-PREM-ONLY :** Les entreprises utilisant ce type d'architecture hébergent leurs services localement, où ces derniers sont accessibles seulement par les utilisateurs internes.
- **Cloud-Enabled :** Un boîtier $SD-WAN$ sur site se connecte aux fournisseurs de services Cloud, facilitant l'accès aux applications et services hébergés dans le cloud via Internet.
- **Hybrid :** Mélange les 2 types d'architectures précédents pour améliorer les performances et d'offrir une meilleure expérience aux utilisateurs.

2.2.4 Les avantages du SD-WAN

Les avantages du $SD-WAN$ sont [22] :

- **Réduction des coûts :**Les réseaux WAN traditionnels utilisent des liaisons MPLS extrêmement coûteuses et très complexes à déployer, en revanche le $SD-WAN$ s'oriente vers l'exploitation de plusieurs liaisons de transport (Internet, fibre, LTE...) qui sont moins coûteuses et facile à déployer.
- **Système de gestion centralisé :**Les réseaux WAN traditionnels utilisent des liaisons $MPLS$ extrêmement coûteuses et très complexes à déployer, en revanche le $SD-WAN$ s'oriente vers l'exploitation de plusieurs liaisons de transport (Internet, fibre, LTE...) qui sont moins coûteuses et facile à déployer.

- **Interopérabilité Cloud :**Le $SD-WAN$ offre un accès direct au Cloud depuis les sites distants. Ce qui signifie que les employés d'entreprises peuvent accéder directement à ces applications sans surcharger le réseau principal avec un trafic supplémentaire.
- **Zero Touch Provisioning** ZTP **:**L'approvisionnement ZTP une configuration automatisée et rapide des équipements, y compris les mises à jour et les déploiements de fonctionnalités. Cela réduit les erreurs humaines et accélère le processus d'approvisionnement.
- **Une sécurité renforcée :**La technologie $SD-WAN$ garantit la sécurité du trafic en cryptant toutes les données échangées entre les sites, ce qui permet une gestion du trafic réseau plus sécurisée. Grâce au filtrage du trafic en temps réel et à la segmentation des flux de données, les menaces internes peuvent être contenues, évitant ainsi la propagation d'attaques sur l'ensemble du réseau. Cette approche assure la disponibilité et la continuité des services dans les autres sites, tout en isolant les attaques sur des sites spécifiques.
- **La fiabilité :**Une des particularités du $SD-WAN$ est la multiplicité des liens utiliser pour l'acheminement du trafic, provenant de différents ISP, afin d'assurer un service continu, contrairement aux réseau WAN traditionnels qui exploitent une seule liaison.

2.2.5 Topologie réseau SD-WAN

Les interconnexions entre différents sites peuvent être multiples et très différentes les unes des autres. Cependant, grâce au $SD-WAN$, il est possible d'avoir une topologie de réseau logique différente de la topologie de réseau physique. Cela permet la coexistence d'une topologie inférieure (la vraie) et d'une topologie superposée (la désirée). Les diverses topologies peuvent être catégorisées en topologie maillée, en topologie en étoile et en étoile, et en topologie hybride comme le montre la figure 2.8. [5]

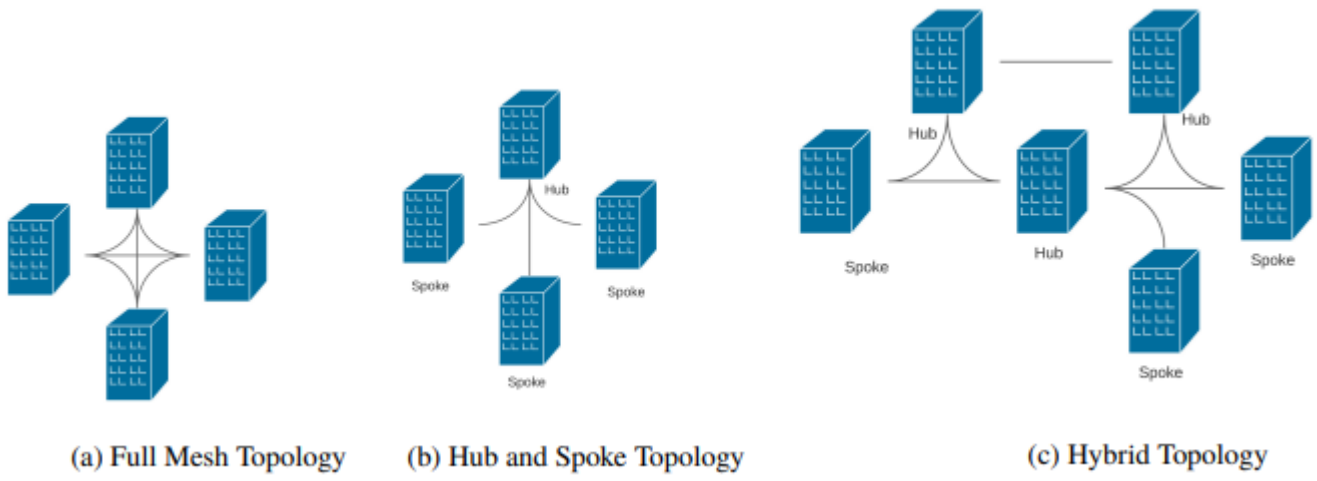


FIGURE 2.8 – Architecture SD-WAN [5].

- **Topologie full-mesh :**Les sites sont tous interconnectés. L'avantage de cette topologie est que le temp de réponse est réduit comme le trafic ne passe pas par des sites intermédiaires entre source et destination. Mais dans le cas d'une large entreprise avec beaucoup de sites, il y aura beaucoup de tunnels VPN, ce qui peut limiter les ressources et dégrader la performance.
- **Topologie HUB and Spoke :**Sur cette topologie, le hub est connecté directement aux autres spokes. Si un nouveau site est ajouté, il sera connecté directement au HUB seulement, ce qui va permette la réduction des coûts en assurant la scalabilité.

- **Topologie hybride :**La topologie hybride implique l'interconnexion des plusieurs topologies HUB and Spoke à travers les hubs. Les hubs sont déterminés par le niveau d'importance comme direction générale, data center, etc. malgré la complexité de son design, ça améliore la flexibilité et la scalabilité et réduie le temps de latence.

2.2.6 Composant de service SDWAN :

Le SD-WAN utilise une architecture abstraite pour son réseau. ou le réseau est divisé en deux parties : le plan de contrôle et le plan de transmission. Avec le $SD-WAN$, le plan de contrôle est centralisé et le réseau peut être géré à distance sans avoir à être sur site [4].

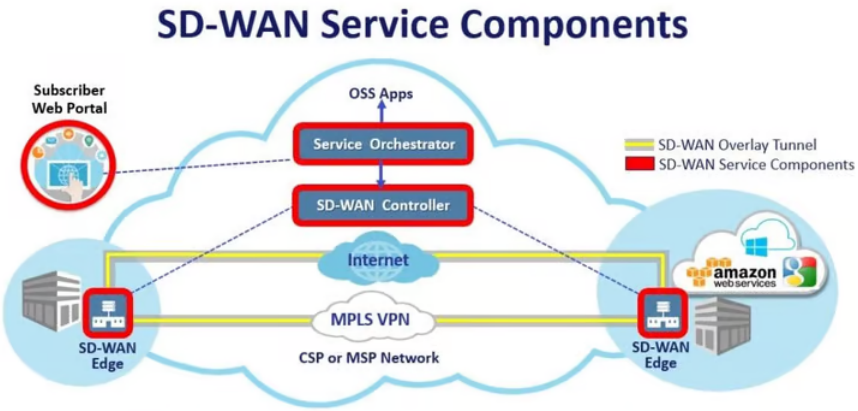


FIGURE 2.9 – Architecture SD-WAN [4].

Ce réseau virtualisé comporte ces trois composants principaux [4] :

- **La périphérie SD-WAN :**l'endroit où résident les points de terminaison du réseau. Il peut s'agir d'une spoke, d'un centre de données distant ou d'une plate-forme cloud.
- **Un orchestrateur SD-WAN :**le gestionnaire virtualisé du réseau, supervisant le trafic et appliquant la politique et le protocole définis par les opérateurs.
- **Le contrôleur SD-WAN :**centralise la gestion et permet aux opérateurs de voir le réseau à travers une fenêtre unique et de définir la politique à exécuter par l'orchestrateur.

2.2.7 Déférents SD-WAN sur le marché international :

À l'heure actuelle, il existe un grand nombre de fournisseurs de technologie $SD-WAN$ sur le marché, tels que Huawei, Fortinet, Cisco, etc. Selon une étude menée par Gartner (société américaine de conseil et de recherche dans le domaine des technologies de pointe) en septembre 2021, celle-ci en déduit que Fortinet et Cisco sont en position de leader dans le Magic Quadrant pour les infrastructures $SD-WAN$, avec Huawei un Challenger dans le Magic Quadrant.
Les solutions $SD-WAN$ different par fourniseurs en se basant sur des facteurs économiques et des exigences des clients. Par exemple, Fortinet Solutions a été un leader dans le secteur de la sécurité avec son produit FortiGate Secure $SD-WAN$, la mise en œuvre de pare-feu de nouvelle génération et plusieurs autres solutions de sécurité. D'autre part, les solutions Cisco ouvrent la voie en matière de routage sécurisé du trafic grâce à la segmentation [19].

FIGURE 2.10 – Magic Quadrant pour l'infrastructure SD-WAN [19].

2.2.7.1 Synthèse des implémentations (comparatif) :

Le marché du $SD-WAN$ reste très dynamique, Les solution existantes ne sont pas les mêmes, et chaque constructeur du matériel propose ces propres fonctionnalités pour le $SD-WAN$. Les entreprises déployant largement la technologie $SD-WAN$ pour surmonter les limitations de bande passante du WAN et pour plus de fiabilité et de résilience, tout en améliorant la qualité de l'expérience utilisateur pour les applications cloud. Après une étude sur les différentes implémentations $SD-WAN$, on a réalisé un tableau comparatif entre ses approches :

	Cisco	Huawei	Juniper	Fortinet
La solution $SD-WAN$	Citrix NetScaler sdwan	Huawei sd-wan	Juniper Ssd-wa	Fortinet secure sd-wan
Orchestrateur	vBond	CSO	@AC Campus	Fortinet Secure sd-wan Orchestrators
Composants	vManage vSmart vBond vEdge	sd-wan CPE uCPE	vCPE Vrr	FortiGate FortiManager FortiAnalyzer FortiDeploy
Type de la solution $SD-WAN$	On Premise Cloud Based	Cloud	Cloud	Cloud
Type de déploiement	Physique et virtuelle	Physique et virtuelle	Physique et virtuelle	Physique et virtuelle
Optimisation du WAN	Oui	Oui	Oui	Oui
Option d'accès	Internet MPLS 3G/4G/LTE Satellite	Internet MPLS 3G/4G/LTE Satellite	Internet MPLS 3G/4G/LTE	Internet MPLS 3G/4G/LTE Satellite

Duplication de paquet	Oui	Non	Non	Oui
Forward erreur contrôle	Oui	Non	Oui	Oui
Dynamic path Switching	Oui	Oui	Oui	Oui
Chiffrement	AES256 IPSEC GRE	AES256 IPSEC GRE	AES128 AES256 IPSEC GRE	AES256 IPSEC GRE
Zero Touch Déploiement	Oui	Oui	Oui	Oui
Inspection approfondie des données	Oui	Oui	Oui	Oui
Segmentation de donnée	Oui	Oui	Non	Oui
Sélection du chemin par application	Oui	Oui	Oui	Oui
Pare-feu	De base sur le matériel Viptela Avancé sur le matériel Cisco	Avancé	Avancé	pare-feu de nouvelle génération ($NGFW$)

TABLE 2.2 – Tableau comparatif entre les implémentations $SD-WAN$

.

Il est important de noter que chaque entreprise a des besoins spécifiques en matière de mise en réseau et de sécurité, et que d'autres solutions pourraient répondre plus efficacement à ces besoins. D'après ce tableau, on constate que la solution Fortinet Secure $SD-WAN$ est complète pour un bon $SD-WAN$, La solution offre des nombreux avantages, notamment en matière de sécurité en intégrant directement des fonctionnalités de sécurité pour une protection renforcée contre les menaces potentielles. La solution utilise des technologies telles que le pare-feu nouvelle génération ($NGFW$). De plus, la fonction ZTP de Fortinet $SD-WAN$ permet un déploiement rapide et facile des appareils réseau, ce qui réduit le temps et les coûts liés à la configuration manuelle des appareils.

2.2.8 DMVPN vs le SD-WAN :

$DMVPN$ et $SD-WAN$ sont deux technologies de réseau qui permettent aux entreprises de connecter des sites distants et de fournir un accès sécurisé aux utilisateurs distants. Bien qu'elles aient des objectifs similaires, elles sont différentes dans leur approche et leur fonctionnement. Actuellement, le $SD-WAN$ est considéré comme la technologie la plus pertinente pour connecter les différents sites d'une entreprise, cependant dans certaines situations, l'utilisation du DMVPN peut être plus avantageuse en termes d'efficacité. Pour mieux comprendre les différences entre ces deux technologies, le tableau 2.3 présente une comparaison détaillée.

	DMVPN	SD-WAN
Topologie	utilise une topologie en étoile (HUB and SPOKE) qui permet aux branches distantes de se connecter facilement au bureau principal.	Pour la création du réseau, il est possible de choisir entre différentes topologies, comme le hub and spoke, le spoke-to-spoke ou le maillage partiel.
Fonctionement	utilise une approche basée sur la création des tunnels dynamiques et la gestion de la connectivité entre les sites distants.	utilise une approche logicielle pour la gestion des connexions WAN et l'amélioration des performances du réseau.
Flexibilité	est plus restreint en termes de flexibilité car il requiert des connexions WAN spécifiques pour pouvoir fonctionner.	offre une grande souplesse aux utilisateurs en leur permettant de sélectionner le type de connectivité WAN qu'ils souhaitent utiliser, et de gérer le trafic entre ces connexions.
Sécurité	utilise des protocoles de chiffrement pour protéger les données en transit sur le réseau. Cependant, il ne fournit pas de contrôle granulaire sur l'ensemble du réseau, ce qui signifie qu'il est possible que des données sensibles soient acheminées sur des chemins moins sécurisés.	utilise des fonctions de sécurité avancées, telles que des pares-feux intégrés, des systèmes de détection et de prévention des intrusions, ainsi que des mécanismes de segmentation du réseau pour protéger les données et les applications contre les menaces. De plus, la gestion centralisée de SD-WAN permet un contrôle granulaire sur tout le réseau, y compris les politiques de sécurité.
Évolutivité	Le DMVPN offre une évolutivité élevée grâce à son architecture (hub and spoke) et à l'utilisation des tunnels multipoints.	Le SD-WAN offre une évolutivité encore plus flexible que le DMVPN grâce à son approche basée sur des contrôleurs centralisés et une gestion basée sur des politiques, Le SD-WAN permet une gestion simplifiée des sites distants et facilite l'ajout ou la suppression des sites sans perturber le réseau existant.
Routage	utilise des protocoles de routage dynamique tels que $OSPF$ ou $EIGRP$ pour créer des tunnels VPN dynamiques entre les sites distants. Cela signifie que les routeurs des différents sites peuvent communiquer directement sans avoir besoin d'un tunnel dédié pour chaque connexion.	utilise une combinaison de protocoles de routage dynamique et statique, ainsi que des algorithmes de répartition de charge pour optimiser le trafic entre les différents liens WAN.

TABLE 2.3 – Comparaison entre une solution $DMVPN$ et une solution $SD-WAN$

2.3 Conclusion :

On a étudié sur ce chapitre le $DMVPN$, son principe et son fonctionnement. Ensuite, nous avons présenté les différents types d'architectures DMVPN ainsi que le protocole de routage dynamique associés. Enfin, nous avons souligné les avantages significatifs de cette technologie. En d'autrtes part, on a introduit la partie $SD-WAN$ en mettant en avant ses avantages par rapport au réseaux traditionnels. Ensuite On a défini ses architectures qui comporte des déférentes interface (API) ainsi on a introduit le protocole open flow qui est le protocole le

plus couramment utilisé dans API Southbound, et les composant de service $SD-WAN$. On a après présenté les déférent $SD-WAN$sur le marché international, pour finir avec une étude comparative entre les déférent implémentation de solutions $SD-WAN$, pour définir les approches de la solution Fortinet Secure $SD-WAN$ qui la base de notre étude.

3 Implementation

3.1 Introduction

Dans ce chapitre, nous aborderons l'implémentation des deux technologies de réseau : $DMVPN$ et $SD-WAN$, les deux technologies permettent de connecter des réseaux distants de manière sécurisée et efficace. Pour cela, nous avons commencé par présenter une démonstration pratique de leur mise en œuvre en utilisant le simulateur GNS3. Nous avons créé une topologie de réseau appropriée pour faciliter la compréhension de l'implémentation de ces deux technologies. Une fois cette étape terminée, nous avons procédé à l'implémentation des mêmes technologies sur des équipements physiques pour une mise en œuvre réelle au niveau de NAFTAL.

3.2 Description de l'environnement de travail

3.2.1 Les équipements utilisés lors de l'implémentation

Les entreprises ont des critères d'achat spécifiques pour leurs équipements, qui ne sont ni aléatoires ni insignifiants. Nous allons donc étudier comment l'entreprise prend sa décision d'achat.

Explication du choix des équipements : En effet, l'utilisation d'équipements performants permet d'augmenter la productivité et la qualité des produits, tout en réduisant les risques d'accidents du travail.
Ainsi, pour choisir le bon équipement, il est important d'évaluer la situation de l'entreprise et d'élaborer une feuille de route technologique afin de définir les besoins en équipements industriels. Il est également important de rechercher l'offre la plus avantageuse en fonction de la topologie de l'entreprise, c'est-à-dire en prenant en compte les contraintes liées à l'espace disponible, aux ressources en énergie, aux compétences des équipes, ...etc.

Les différents équipements utilisés Dans le cadre de l'implémentation de la technologie DMVPN, NAFTAL a opté pour l'utilisation des équipements de la marque Cisco. Cette dernière est connue pour fournir des équipements réseau de qualité, performants et sécurisés. Les équipements Cisco sont également connus pour leur évolutivité et leur capacité à prendre en charge de grandes quantités de données.
La mise en place de cette technologie peut être complexe, mais l'utilisation d'équipements Cisco facilite grandement le processus et garantit un réseau performant et stable.
En ce qui concerne la technologie SD-WAN, NAFTAL a choisi les équipements Fortinet, pour avoir des infrastructures réseau de haute qualité, dotées de performances exceptionnelles et bénéficiant d'une sécurité optimale. Les équipements Fortinet offrent une grande flexibilité et évolutivité qui permettent de répondre aux besoins en constante évolution de l'entreprise.
En somme, en choisissant les équipements Cisco pour la technologie DMVPN et les équipements Fortinet pour la technologie SD-WAN, NAFTAL s'assure d'avoir des solutions de réseau performantes, sécurisées et évolutives, adaptées à ses besoins spécifiques.

3.2.2 Ressources logicielles

VMware Workstation Pro : est un logiciel de virtualisation très puissant qui permet d'exécuter plusieurs systèmes d'exploitation en tant que machines virtuelles sur une seule machine physique.
VMware-workstation-full-17.0.0 de VMware Workstation est la dernière version disponible à

l'heure actuelle. Elle offre de nombreuses fonctionnalités avancées pour les professionnels de l'informatique, notamment en matière de virtualisation de réseaux.

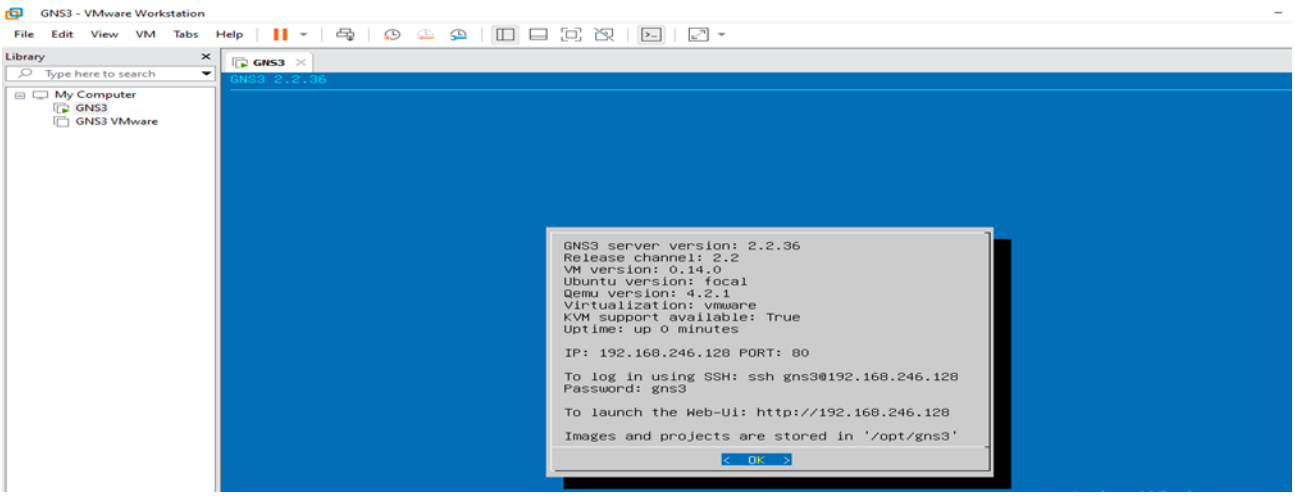


FIGURE 3.1 – l'interface de la machine virtuel VMware Workstation.

L'émulateur de réseaux GNS3 : GNS3 (Graphical Network Simulator) : est un émulateur graphique de réseau permettant de créer des topologies de réseau complexes et de réaliser des simulations. C'est un outil de choix pour l'administration des réseaux Cisco, utilisé pour reproduire différents systèmes d'exploitation dans un environnement virtuel, notamment en émulant l'exécution de l'IOS Cisco (Internet-work Operating Systems) [1].
Pour fournir des simulations complètes et précises, GNS3 s'appuie sur les composants suivants :

- **Dynamips :**un émulateur de routeurs Cisco capable de faire fonctionner des images Cisco IOS non modifiées, comme si elles étaient exécutées sur des équipements réels. Son rôle n'est pas de remplacer les routeurs réels, mais de permettre la création de maquettes complexes avec de véritables versions d'IOS.
- **Dynagen :**un complément écrit en Python qui interagit avec Dynamips via le mode hyperviseur, facilitant ainsi la création et la gestion des maquettes à l'aide d'un fichier de configuration simple décrivant la topologie du réseau à simuler et une interface texte interactive.
- **Qemu :** une machine source d'émulation et de virtualisation générique et ouverte. GNS3 utilise Qemu pour exécuter des systèmes tels que Cisco ASA, PIX, IDS, ainsi que tout autre système d'exploitation classique.

Ces composants contribuent ensemble à améliorer les fonctionnalités de GNS3, permettant aux professionnels des réseaux de créer des simulations réseau réalistes et d'effectuer diverses tâches de mise en réseau dans un environnement virtuel.

La machine virtuelle GNS3 VM : est une solution de virtualisation permettant le partage des performances de plusieurs machines physiques, pour une simulation de réseau efficace et optimisée. Elle est spécialement conçue pour une utilisation avec GNS3 2.2.37 et permet aux utilisateurs de réaliser des simulations de réseaux virtuels plus performantes et plus stables.

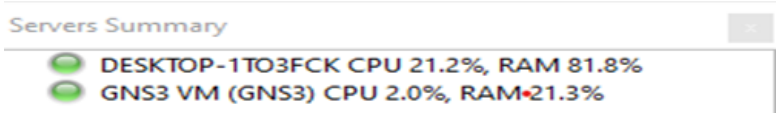


FIGURE 3.2 – Affichage du résumé des serveurs Docks dans GNS3.

Images iOS Cisco : Pour réaliser l'implémentation de DMVPN dans notre environnement de travail sur GNS3, nous avons besoin des images de routeur et de commutateur Cisco suivantes :

Image iOS Cisco	Nom du fichier
Switch Cisco iOSvL2 	vios_l2-adventerprisek9-m.vmdk.SSA.152-4.0.55.E.vmdk
Router c7200 	c7200-adventerprisek9-mz.152-4.S3.image

TABLE 3.1 – Les ressources logicielles utilisées

3.3 Déploiement du DM-VPN au niveau de GNS3 :

Dans cette partie nous allons voir l'implémentation du DMVPN via ces étapes :

3.3.1 Topologie du réseau DMVPN

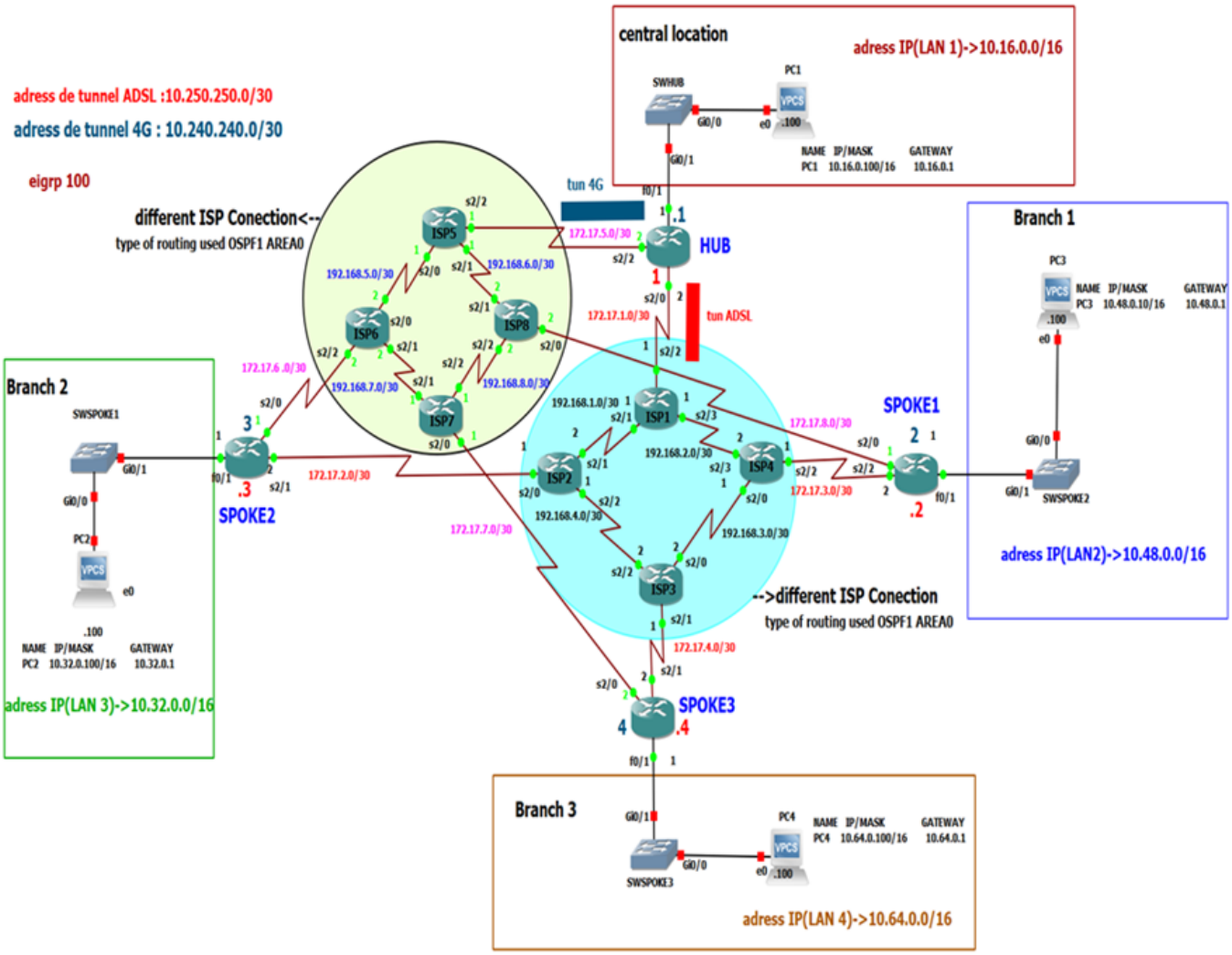


FIGURE 3.3 – topologie DMVPN sur GNS3.

3.3.1.1 Explication de topologie DMVPN

La figure 3.3 présente une topologie de réseau comprenant un site central "Hub" et trois sites distants considérés comme des "Spokes" de l'architecture DMVPN. Chaque site contient un routeur Cisco C7200, ainsi qu'un switch Cisco qui joue le rôle de commutateur du LAN pour

interconnecter les différents appareils du site. L'objectif est d'établir une connectivité entre les différents sites, afin de pouvoir configurer et gérer les fonctionnalités du DMVPN.

- **La première étape** de l'implémentation consiste à résoudre le problème de connectivité sous-jacente, aussi appelé "underlay", entre les différents sites situés dans un *WAN* complexe composé de plusieurs ISP. Cette première étape est très importante car elle permet de mettre en place une infrastructure solide et stable qui servira de fondation pour le reste de l'implémentation de DMVPN.
- **La deuxième étape** l'utilisation du DMVPN Cisco avec une architecture Hub to spoke, en utilisant mGRE et deux tunnels IPsec (ADSL et 4G), permet de créer une topologie Overlay sécurisée pour connecter les sites distants au hub central. L'EIGRP est souvent choisi comme protocole de routage pour faciliter la gestion et l'optimisation du trafic dans cette configuration spécifique.

3.3.2 Configuration

3.3.2.1 La mise en place de la technologie DMVPN

Afin de déployer cette architecture, nous avons utilisé un routeur HUB au niveau du site central. La configuration sera similaire pour chaque Spoke, à l'exception des adresses IP publiques et privées ainsi ID network de DMVPN qui seront spécifiques à chaque site distant. Pour cela, nous avons procédé comme suit :

3.3.2.1.1 Etape 1 : Implementation des tunnels mGRE avec intégration de NHRP

Nous avons mis en place deux tunnels mGRE entre le routeur Hub et les routeurs Spokes pour assurer la connectivité entre les sites distants. La configuration des tunnels a été réalisée en suivant les étapes suivantes :

Implementation du Hub : Pour configurer le Hub, nous avons tout d'abord créé une interface tunnel mGRE que nous avons ensuite reliée à l'interface serial 2/0 correspondant au tunnel 0 ADSL, ainsi qu'à une deuxième interface mGRE reliée à l'interface serial 2/2 correspondant au tunnel 1 4G du Hub. Nous avons ensuite configuré les adresses IP pour ces deux tunnels ainsi que pour les interfaces physiques correspondantes.

HUB

```
!
interface Tunnel0
 description "HUB_TO ADSL"
 ip address 10.250.250.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip hello-interval eigrp 100 10
 ip hold-time eigrp 100 30
 no ip next-hop-self eigrp 100
 no ip split-horizon eigrp 100
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp holdtime 300
 ip tcp adjust-mss 1360
 delay 100
 cdp enable
 tunnel source 172.17.1.2
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile IPSECPROF
```

FIGURE 3.4 – Implémentation de tunnels mGRE (Tun0) sur le routeur HUB.

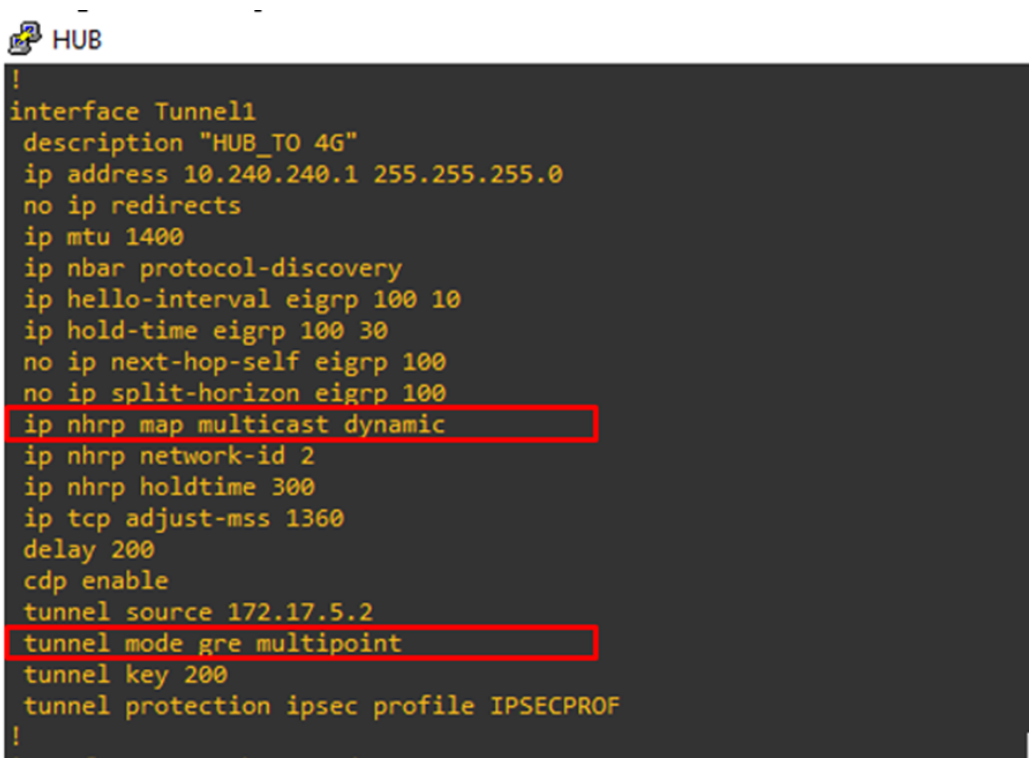


FIGURE 3.5 – Implémentation de tunnels mGRE (Tun1) sur le routeur HUB.

Analyse de la figure 3.4 et 3.5 :

- La commande "**tunnel mode GRE multipoint**" permet de créer un seul tunnel GRE qui peut être utilisé pour plusieurs tunnels IP sec. Cette commande est utilisée lors de la configuration de l'interface tunnel mGRE du Hub et des spokes pour mettre en place le DMVPN.
- La commande "**ip nhrp map multicast dynamic**" est utilisée pour configurer la résolution dynamique des adresses multicast pour le trafic NHRP dans une topologie DMVPN.
- NHRP est utilisé pour résoudre les adresses IP des différents spokes connectés à un Hub. Les adresses multicast sont utilisées pour la diffusion de paquets NHRP, permettant aux routeurs de découvrir les adresses IP de leurs homologues distants.

Implementation du Spoke : Afin de configurer le Spoke dans DMVPN, nous avons commencé par créer une interface tunnel mGRE que nous avons reliée à l'interface correspondant au tunnel ADSL, soit serial 2/2, et à une deuxième interface mGRE reliée à l'interface correspondant au tunnel 4G, soit serial 2/0. Ensuite, nous avons configuré les adresses IP pour ces deux tunnels ainsi que pour les interfaces physiques associées.

SPOKE1

```
!
interface Tunnel0
 description "SPOKE1_to_ HUB (Tun ADSL )
 ip address 10.250.250.2 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip bandwidth-percent eigrp 100 20
 ip hello-interval eigrp 100 10
 ip hold-time eigrp 100 30
 ip nhrp map multicast dynamic
 ip nhrp map 10.250.250.1 172.17.1.2
 ip nhrp map multicast 172.17.1.2
 ip nhrp network-id 1
 ip nhrp holdtime 300
 ip nhrp nhs 10.250.250.1
 ip tcp adjust-mss 1360
 delay 100
 cdp enable
 tunnel source Serial2/2
 tunnel mode gre multipoint
 tunnel key 100
 tunnel protection ipsec profile IPSECPROF
!
```

FIGURE 3.6 – Implémentation de tunnels mGRE (Tun0) sur le routeur Spoke.

SPOKE1

```
!
interface Tunnel1
 description "SPOKE1_to_ HUB (Tun 4G)
 ip address 10.240.240.2 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip bandwidth-percent eigrp 100 20
 ip hello-interval eigrp 100 10
 ip hold-time eigrp 100 30
 ip nhrp map multicast dynamic
 ip nhrp map multicast 172.17.5.2
 ip nhrp map 10.240.240.1 172.17.5.2
 ip nhrp network-id 2
 ip nhrp holdtime 300
 ip nhrp nhs 10.240.240.1
 ip tcp adjust-mss 1360
 delay 200
 cdp enable
 tunnel source 172.17.8.1
 tunnel mode gre multipoint
 tunnel key 200
 tunnel protection ipsec profile IPSECPROF
!
```

FIGURE 3.7 – Implémentation de tunnels mGRE (Tun1) sur le routeur Spoke.

Analyse de la figure 3.6 et 3.7 :

— - La commande "**ip nhrp map**" : La configuration de chaque spoke dans le réseau DMVPN est basée sur une correspondance entre l'adresse IP publique du Hub et une adresse NHRP unique, telle que 172.17.1.2 -> 10.240.240.1 pour le tunnel ADSL et 172.17.5.2 -> 10.250.250.1 pour le tunnel 4G. Cette correspondance permet d'identifier précisément chaque élément dans le réseau et est établie grâce à la commande "**ip nhrp map**". Cette étape est cruciale pour garantir le succès de la configuration de chaque spoke dans le réseau DMVPN.

3.3.2.1.2 Etape 2. Configuration de l'IPsec pour la connectivité Hub et Spoke

FIGURE 3.8 – Configuration du cryptage IP sec au niveau de HUB and Spoke.

Analyse de la figure 3.8 : Cette configuration est liée à la mise en place de tunnels VPN IPsec dans un environnement DMVPN.

- La première commande, "**crypto isakmp policy 1**", crée une politique ISAKMP (Internet Security Association and Key Management Protocol) avec un identifiant de priorité de 1. Cette politique détermine les algorithmes de chiffrement et d'authentification à utiliser lors de la négociation de la clé ISAKMP Phase 1 entre les différents nœuds VPN.
  - L'option "**encr aes**" spécifie l'algorithme de chiffrement AES pour la confidentialité des données échangées.
  - L'option "**authentication pre-share**" indique que l'authentification utilisera une clé pré-partagée entre les différents nœuds VPN.
  - L'option "**group 2**" spécifie que la méthode de DH (Diffie-Hellman) à utiliser pour la négociation de la clé ISAKMP Phase 1 sera DH de groupe 2.
- La deuxième commande, "**crypto isakmp key DMVPNIPSEC address 0.0.0.0**", configure la clé pré-partagée utilisée pour l'authentification entre les différents nœuds VPN. La valeur "**DMVPNIPSEC**" est la clé pré-partagée, et "**address 0.0.0.0**" indique que cette clé est utilisée pour l'authentification de tous les nœuds.
- La troisième commande, "**crypto ipsec transform-set hub-set esp-aes esp-sha-hmac**", définit un ensemble de transformations IPsec pour le profil IP sec. Cet ensemble utilise l'algorithme de chiffrement AES pour la confidentialité des données et l'algorithme HMAC-SHA pour l'authentification des données.
- la dernière commande "**crypto ipsec profile IPSECPROF**" crée un profil IP sec nommé "**IPSECPROF**" et configure les paramètres de ce profil en utilisant l'ensemble de transformations "**hub-set**" défini précédemment. Ce profil sera utilisé pour la configuration des tunnels IP sec dans l'environnement DMVPN.

3.3.2.1.3 Etape 3 : Configuration du protocole de routage Étant donné que tous les équipements utilisés dans la topologie DMVPN sont de marque Cisco, on a donc décidé d'utiliser EIGRP comme protocole de routage pour la partie overlay. Ensuite, la configuration de ce protocole est appliquée de manière similaire sur tous les routeurs (Hub et Spokes).

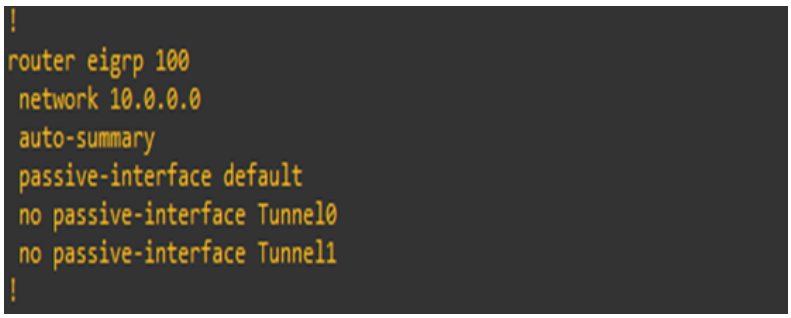


FIGURE 3.9 – Activation du protocole EIGRP.

Analyse de la figure 3.9 : Cette configuration est pour le protocole EIGRP avec l'*AS* (Autonomes System) numéro 100. Les commandes suivantes sont utilisées :

- "**network 10.0.0.0**" annonce toutes les interfaces de réseaux qui se trouvent dans le bloc d'adresse IP 10.0.0.0/8 au processus EIGRP 100. Cela signifie que tous les réseaux avec un préfixe d'adresse IP de 10.x.x.x seront annoncés par EIGRP.
- "**auto-summary**" permet de résumer les réseaux dans EIGRP selon leur classe de réseau par défaut.
- "**passive-interface default**" configure toutes les interfaces comme étant passives par défaut, ce qui signifie qu'EIGRP n'envoie pas de messages hello à ces interfaces. Les interfaces doivent être explicitement activées avec la commande "no passive-interface" pour envoyer des messages hello à des voisins EIGRP.
- "**no passive-interface Tunnel0**" et"no passive-interface Tunnel1" activent les interfaces Tunnel0 et Tunnel1 pour l'envoi de messages hello EIGRP. Les tunnels sont considérés comme des interfaces logiques sur lesquelles les messages EIGRP peuvent être transmis.

Vérification de l'adjacence des voisins EIGRP sur le hub

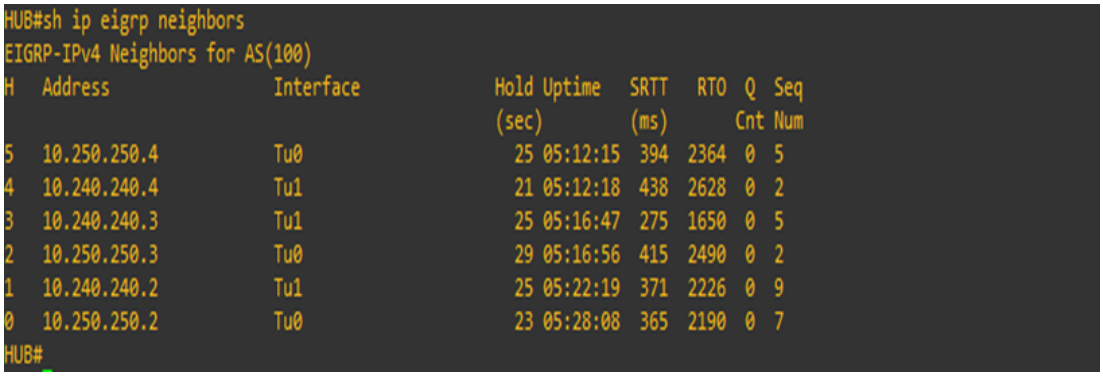


FIGURE 3.10 – Affichage des voisins EIGRP actuels via la commande sh ip eigrp neighbors (HUB).

Analyse de la figure 3.10 :

- Les résultats affichent les voisins EIGRP actuels du routeur HUB, indiquant leur adresse IP et l'interface associée. Dans cette configuration spécifique, le routeur HUB présente six voisins EIGRP qui sont tous des tunnels (Tu0 et Tu1) provenant des spokes.

Vérification de l'adjacence des voisins EIGRP sur le SPOKE

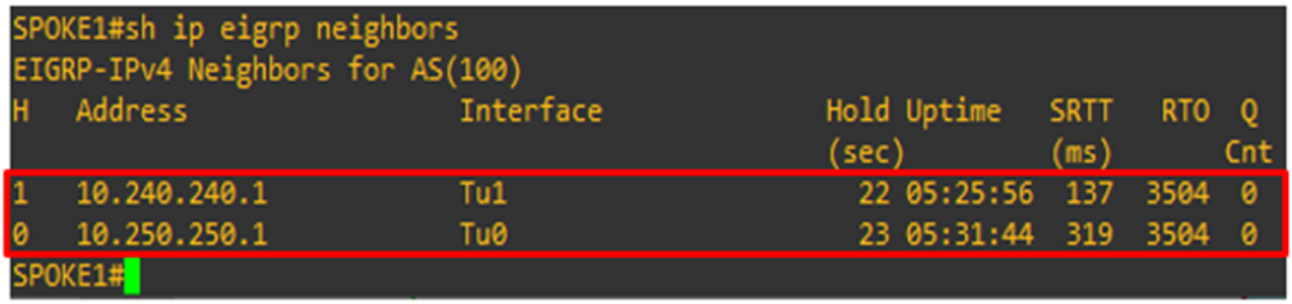


FIGURE 3.11 – Affichage des voisins EIGRP actuels via la commande sh ip eigrp neighbors (Spoke).

Analyse de la figure 3.11 :

— Le résultat obtenu à partir de la commande "**show IP eigrp Neighbors**" exécutée sur le routeur Spoke1 présente les voisins EIGRP actuellement connectés à ce dernier, qui se trouvent être les deux interfaces logiques du HUB (Tunnel 1 ayant pour adresse IP 10.240.240.1 et Tunnel 0 ayant pour adresse IP 10.250.250.1).

3.4 Déploiement du DM-VPN dans l'équipement CISCO au niveau de NAFTAL :

3.4.1 Configuration du SPOKE (DG-DSL-3G)

3.4.1.1 Configuration du profil IP Sec :

consiste à configurer la phase 1 et la phase 2 d'IP sec.

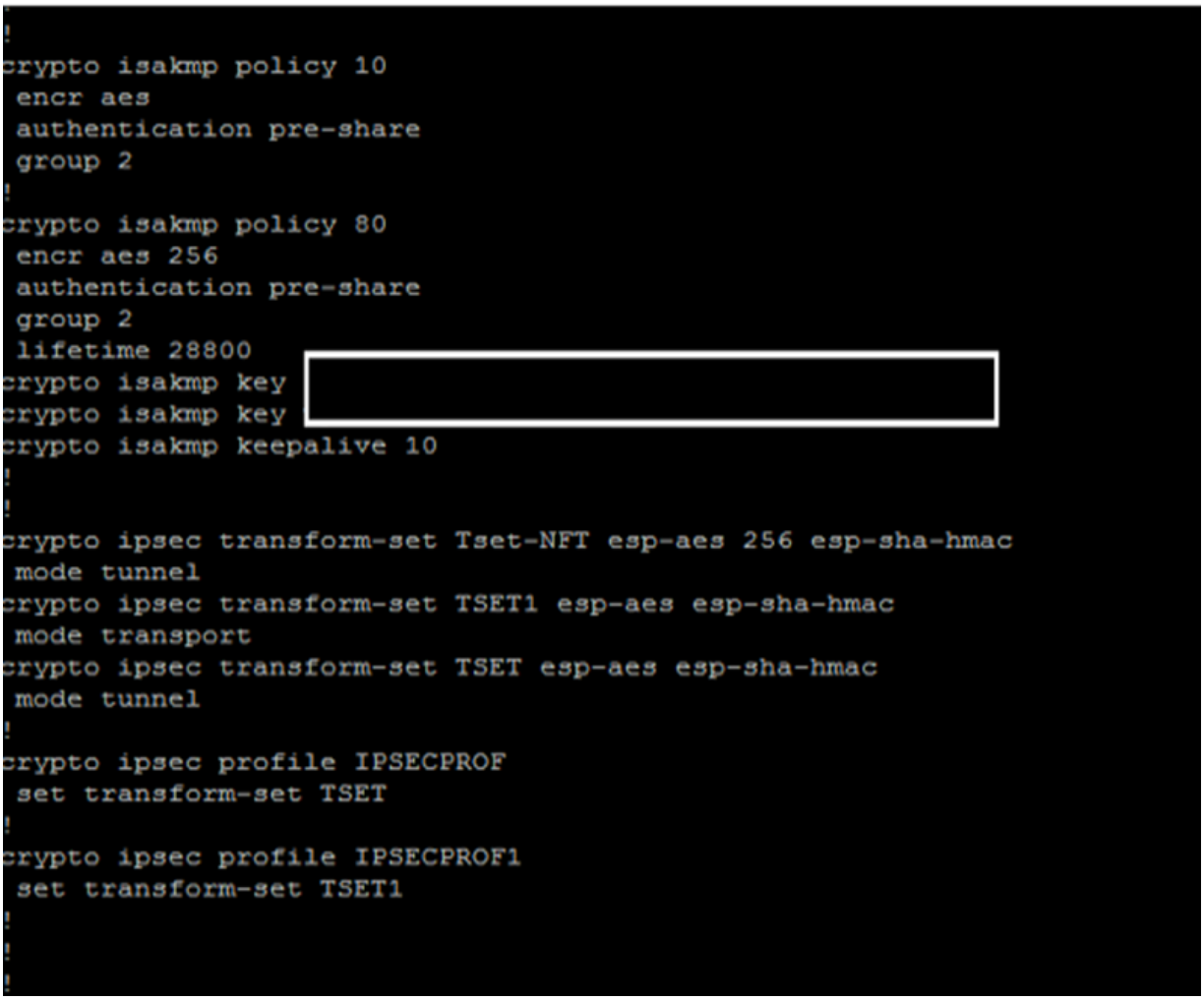


FIGURE 3.12 – Configuration du profil IP sec.

Analyse de la figure 3.12 :

- Il faut mettre en place la sécurité IPSec sur le Hub en définissant un profil IPSec à l'aide de la commande "**crypto ipsec profile**" :
  - HUB ASR1 : crypto ipsec profile IPSECPROF.
  - HUB DG-ISR2 : crypto ipsec profile IPSECPROF1.
- Il est également important de configurer les paramètres de sécurité IP sec tels que les algorithmes de chiffrement, d'authentification et les clés partagées.
- Une fois la sécurité IPSec configurée sur le Hub, il est temps de configurer la sécurité IP sec sur le Spoke en créant une politique de sécurité à l'aide de la commande "**crypto isakmp policy**".
- Les paramètres de sécurité IP sec tels que la clé partagée entre le hub et spoke "**crypto isakmp key**", doivent également être définis.

3.4.2 Mise en œuvre des Tunnels

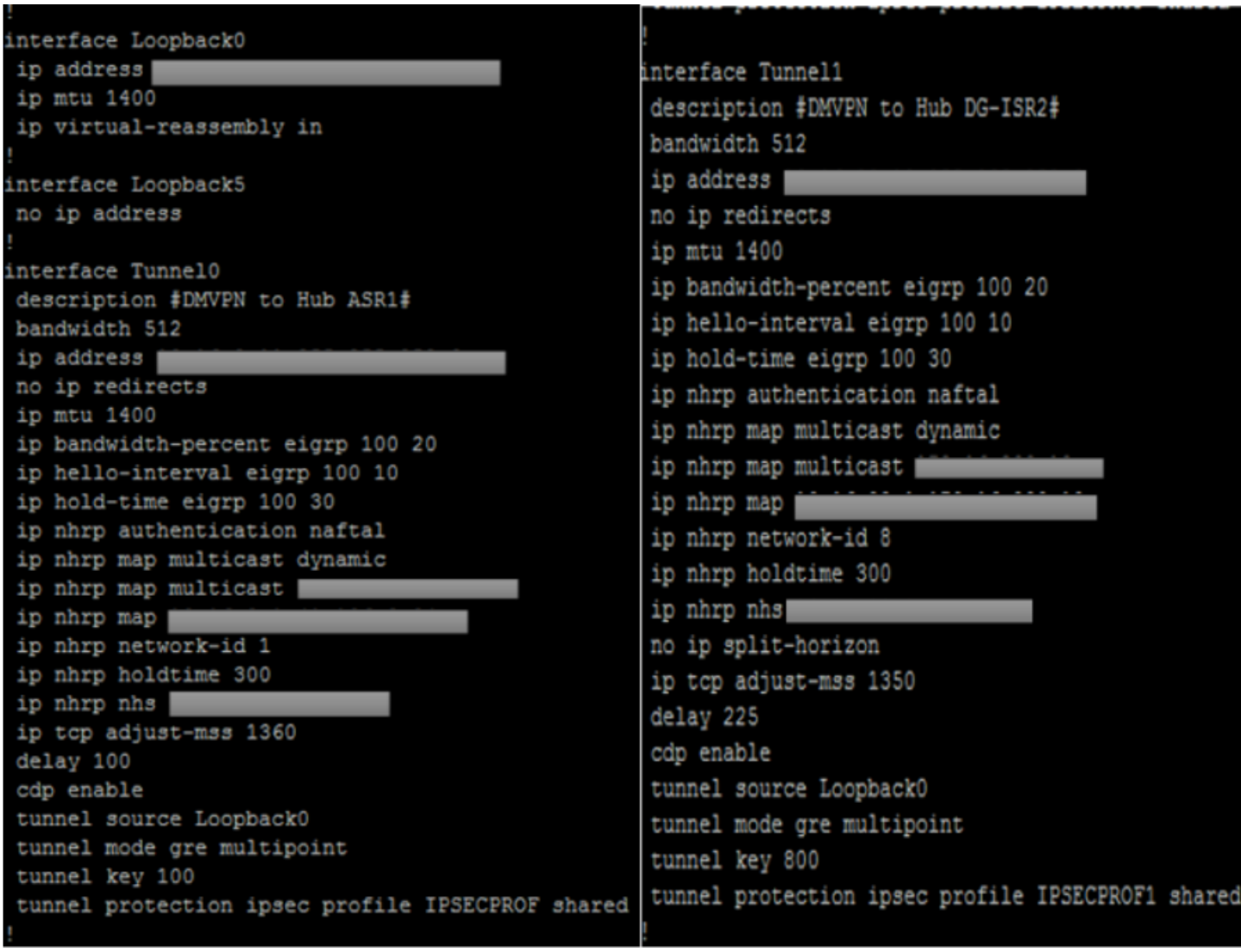


FIGURE 3.13 – Création des tunnels 0 et 1.

Analyse de la figure 3.13 :

- Il est nécessaire de configurer les tunnels sur le Hub en utilisant la commande "**interface tunnel**". Ces tunnels sont utilisés pour encapsuler le trafic Hub-Spoke dans un tunnel IP/GRE.
- En spécifiant "**Tunnel source Loopback0**", cela indique que l'interface Loopback0 est utilisée comme interface source pour le tunnel au niveau de Spoke.
- Pour permettre la résolution dynamique des adresses IP des voisins DMVPN, la connectivité NHRP doit être configurée à l'aide de la commande "**ip nhrp nhs**" sur le Spoke.
- Le tunnel 0 représente : ADSL.
- Le tunnel 4 représente : 4G Mobilis.

3.4.3 Vérification l'état des interfaces de router (Spoke) :

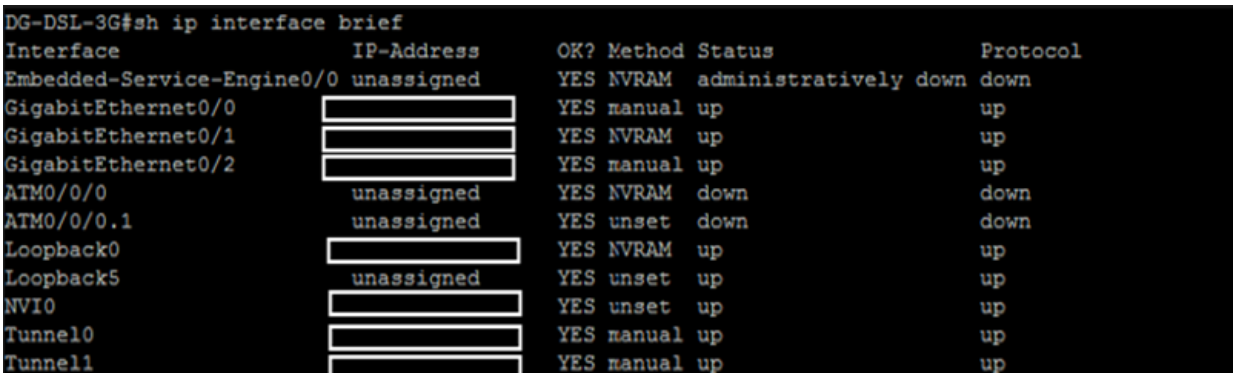


FIGURE 3.14 – Exécution de la command show IP interface brief.

Analyse de la figure 3.14 :

— Dans la partie de configuration du réseau, trois interfaces ont été mises en place.
  - o GigabitEthernet 0/1 est utilisée pour la connexion au réseau *LAN*.
  - o GigabitEthernet 0/0 est dédiée à la connexion *ADSL*.
  - o GigabitEthernet 0/2 est réservée à la connexion avec le modem 4G.
  - o L'interface loopback 0 est utilisée pour fournir une adresse IP statique à l'équipement.

3.4.4 Activation de protocole de routage EIGRP :

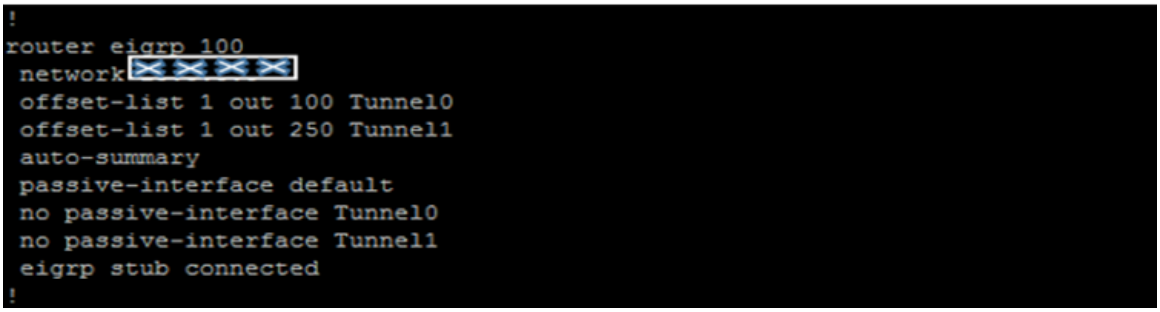


FIGURE 3.15 – Configuration de routage EIGRP.

Analyse de la figure 3.15 :

— Cette configuration active le protocole EIGRP, annonce les réseaux appartenant au réseau X.X.X.X.
  - o Ces commandes sont utilisées pour modifier les métriques des routes dans la table de routage en utilisant une liste d'offset. L'option "**out**" indique que l'offset sera appliqué sur toutes les mises à jour sortantes de l'interface spécifiée. Dans ce cas, la liste d'offset numéro 1 est utilisée.

— - L'interface "**Tunnel10**" et "**Tunnel1**" sont spécifiées pour que la liste d'offset soit appliquée sur les mises à jour sortantes de ces interfaces. Les valeurs "**100**" et "**250**" sont utilisées pour modifier les métriques des routes annoncées aux autres routeurs.

3.4.5 Configuration de route-map :

FIGURE 3.16 – Configuration de routage EIGRP.

Analyse de la figure 3.16 :

- La configuration comporte également deux route-map NAT (Network Address Translation), NAT-ADSL et NAT-Or :
  - La route-map NAT-Or : s'applique à l'interface GigabitEthernet0/2 et traduit les adresses IP internes en adresses IP publiques pour les paquets sortant de cette interface. Cette route-map est définie pour correspondre à l'ACL (Access Control List) 100 et à l'interface GigabitEthernet0/2.
  - La route-map NAT-ADSL s'applique à l'interface GigabitEthernet0/0 et traduit les adresses IP internes en adresses IP publiques pour les paquets sortant de cette interface. Cette route-map est également définie pour correspondre à l'ACL 100 et à l'interface GigabitEthernet0/0.
- Les deux premières lignes sont des commandes NAT qui spécifient les route-maps à utiliser pour traduire les adresses IP des paquets qui sortent des interfaces GigabitEthernet0/0 et GigabitEthernet0/2. La commande "**overload**" indique que la traduction doit prendre en compte plusieurs adresses IP internes et les traduire vers une seule adresse IP publique.

3.5 Déploiement du SD-WAN au niveau de GNS3

Dans cette partie nous allons voir comment implémenter la solution SD-WAN via ces étapes :

3.5.1 Topologie du réseau SD-WAN :

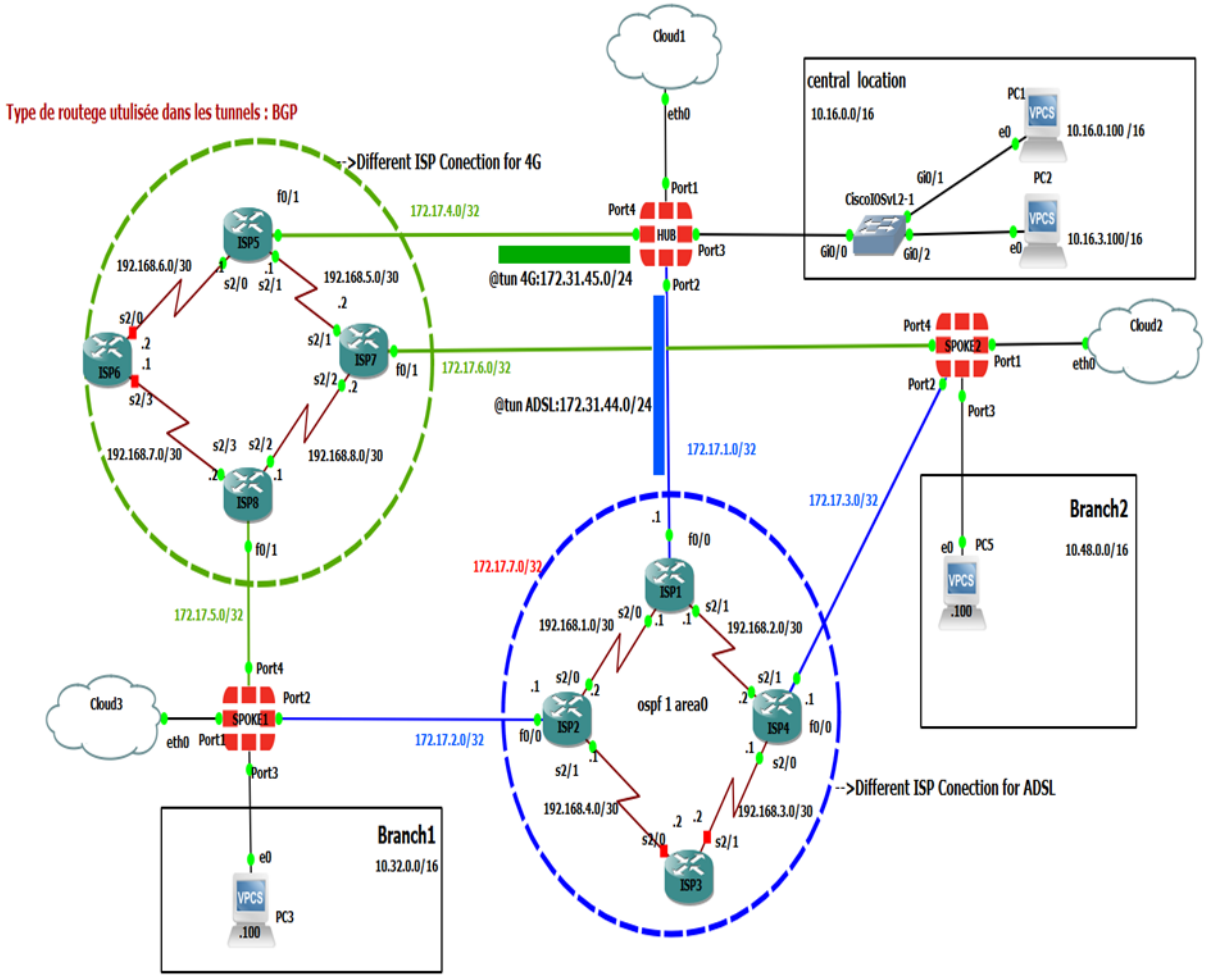


FIGURE 3.17 – Topologie Dynamique Multipoint Virtuel Privat Network (SD-WAN) Sur GNS3.

3.5.1.1 Explication de topologie SD-WAN

La figure illustre une topologie représentant un déploiement SD-WAN utilisant des superpositions IP sec. Les superpositions IP sec sont organisées selon une conception en étoile.
Dans ce déploiement, le HUB joue un rôle central en gérant les connexions entre les sites distants. Les tunnels IP sec sont utilisés pour établir des connexions sécurisées entre le HUB et chaque site distant. Cette topologie en étoile simplifie la gestion du réseau en centralisant les opérations de configuration.

3.5.2 Configuration :

3.5.2.1 La mise en place de la technologie SD-WAN

Voici les étapes générales pour établir la connectivité entre les sites dans cette topologie :

3.5.2.1.1 Configuration les pare-feu FortiGate dans chaque site

Etape1. Implémentation des tunnels au niveau du HUB : FortiGate propose deux méthodes de configuration : via l'interface graphique et via l'interface de ligne de commande.

Configuration des interfaces de phase 1 du VPN IPsec pour les tunnels ADVPN_4G et ADVPN_ADSL au niveau du HUB

- **VIA CLI**

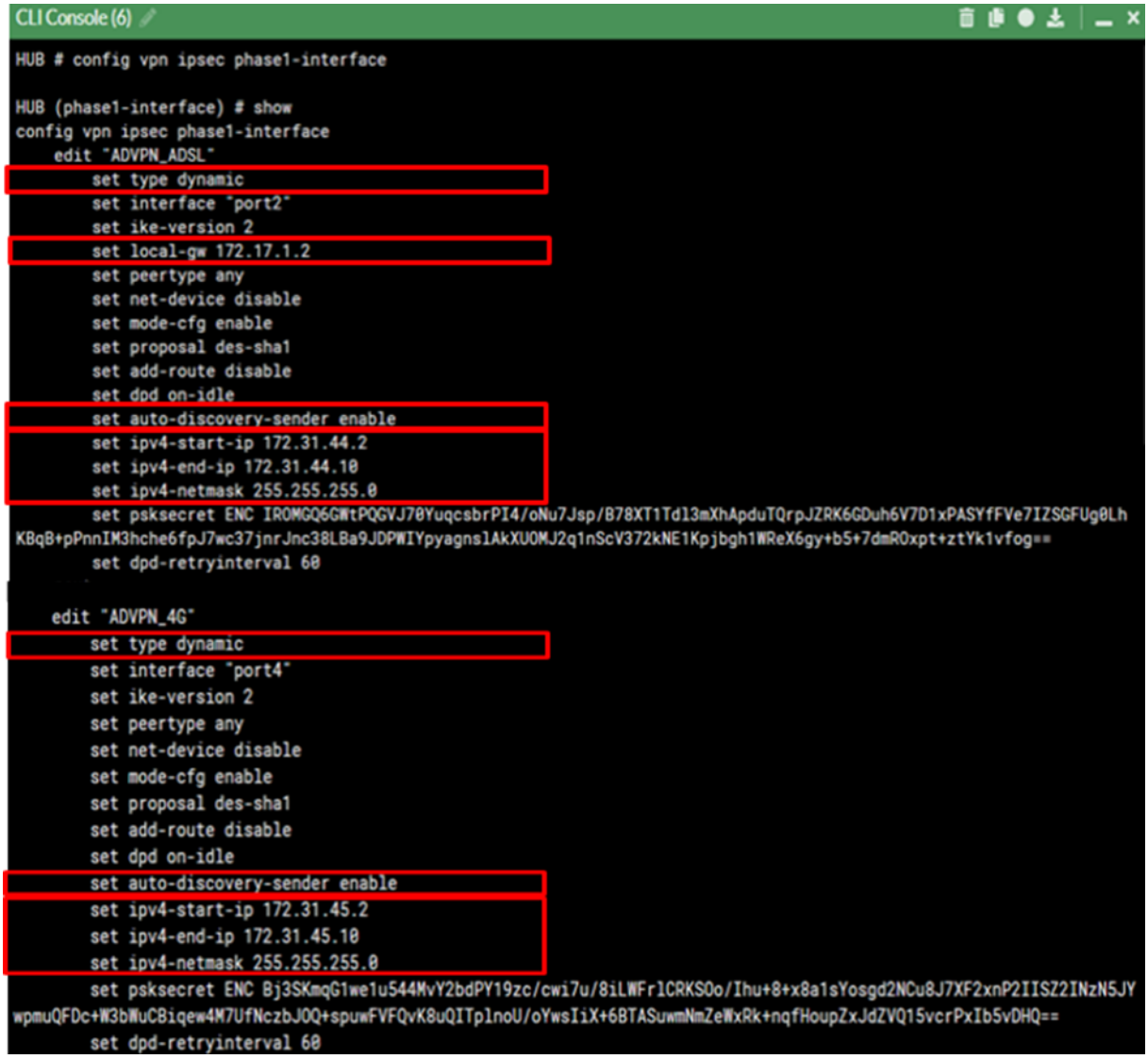


FIGURE 3.18 – Configuration VPN IPsec phase1-interface "ADVPN_4G" et "ADVPN_ADSL" au niveau de HUB via CLI.

Analyse de la figure 3.18 La configuration fournie correspond à la phase 1 de deux interfaces VPN IPsec : "ADVPN_4G" et "ADVPN_ADSL". Voici une explication des paramètres de configuration de l'interface VPN IPsec "ADVPN_4G", ainsi que la même configuration à appliquer sur la deuxième interface "ADVPN_ADSL". en modifiant les adresses IP de tunnel.

- **set type dynamic :** Définie Dial_Up Server et spécifie que le type de l'interface VPN est dynamique, ce qui signifie que les adresses IP sont attribuées de manière dynamique lors de l'établissement du tunnel VPN.
- set peer type any : Autorise les pairs VPN de tout type à se connecter à cette interface VPN.
- **set mode-cfg enable :** Active la configuration du mode client pour les utilisateurs VPN se connectant à cette interface.
- **set proposal des-sha1 :** Spécifie la proposition de chiffrement à utiliser pour la

phase 1, avec l'algorithme de chiffrement DES et l'algorithme d'intégrité SHA1.

— **set auto-discovery-sender enable :** Active la fonction d'envoi de découvertes automatiques pour cette interface VPN.

— **set ipv4-start-ip 172.31.45.2 :** Spécifie l'adresse IP de début pour le pool d'adresses IPv4 attribuées aux clients VPN.

— **set ipv4-end-ip 172.31.45.10 :** Spécifie l'adresse IP de fin pour le pool d'adresses IPv4 attribuées aux clients VPN.

— **set ipv4-netmask 255.255.255.0 :** Spécifie le masque de sous-réseau IPv4 à utiliser pour les adresses attribuées aux clients VPN.

— **set psksecret ENC :** Spécifie la clé pré-partagée (PSK) chiffrée utilisée pour l'authentification entre les pairs VPN.

Ces paramètres de configuration définissent les propriétés de la phase 1 de l'interface VPN IPsec "ADVPN_4G" sur le FortiGate.

o **Via l'interface graphique de FortiGate**

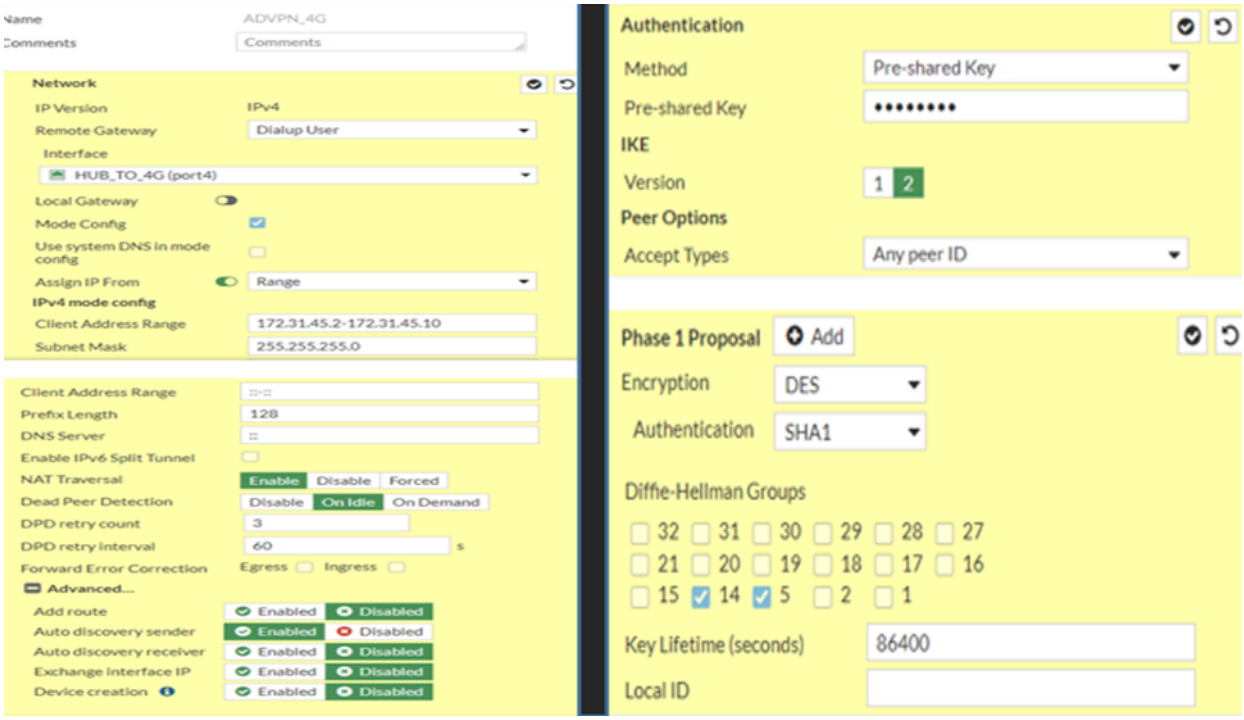


FIGURE 3.19 – Configuration VPN IPsec phase1-interface "ADVPN_4G" via l'interface graphique de FortiGate au niveau du HUB.

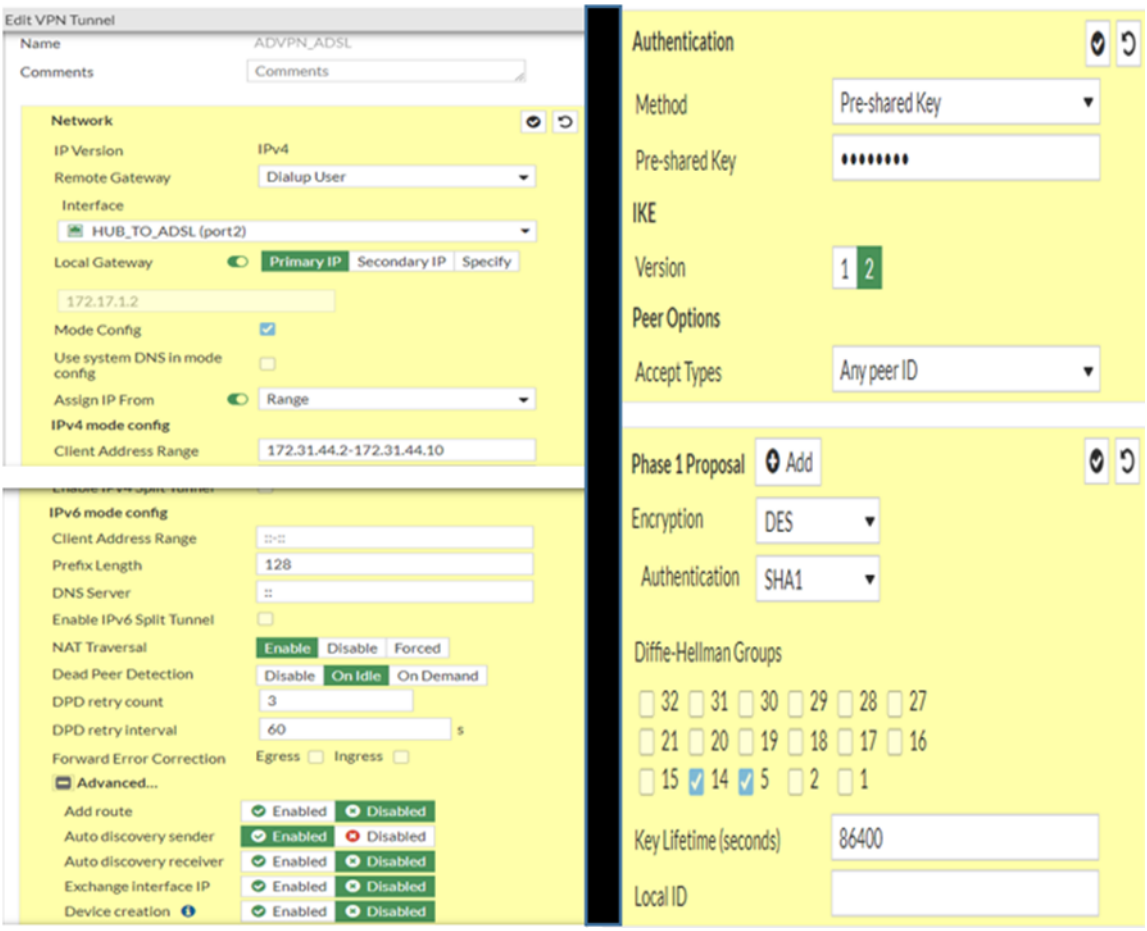


FIGURE 3.20 – Configuration VPN IPsec phase1-interface "ADVPN_ADSL" via l'interface graphique de FortiGate au niveau du HUB.

Configuration du tunnel VPN IPsec phase2-interface ADVPN_4G et ADVPN_ADSL :

- **VIA CLI**

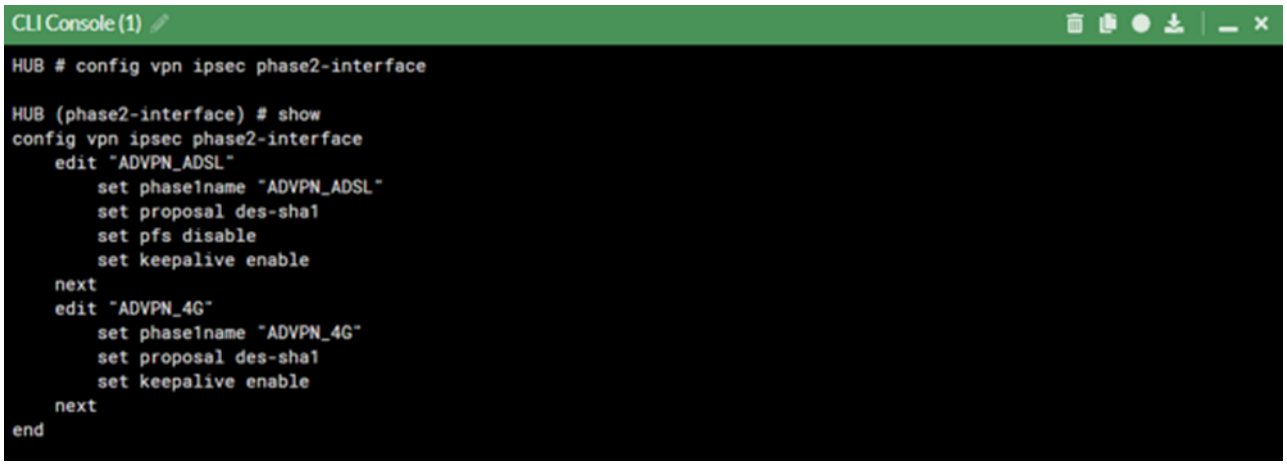


FIGURE 3.21 – Configuration VPN IPsec phase2-interface "ADVPN_ADSL" et "ADVPN_4G" au niveau de HUB via CLI.

Analyse de la figure 3.21 Voici l'explication des paramètres de configuration communs pour les interfaces VPN IPsec nommées "ADVPN_ADSL" et "ADVPN_4G" :

— **La proposition de chiffrement**utilisée est "**des-sha1**".

— **La fonction de surveillance (keepalive)** est activée : L'activation de keepalive dans une configuration d'interface VPN IPsec implique l'échange régulier de paquets de surveillance entre les périphériques VPN. Cette procédure permet de vérifier la connectivité et la disponibilité du tunnel VPN.

Ces paramètres sont appliqués à la fois sur l'interface "**ADVPN_ADSL**" et sur la deuxième interface "**ADVPN_4G**".

o **Via l'interface graphique de FortiGate**

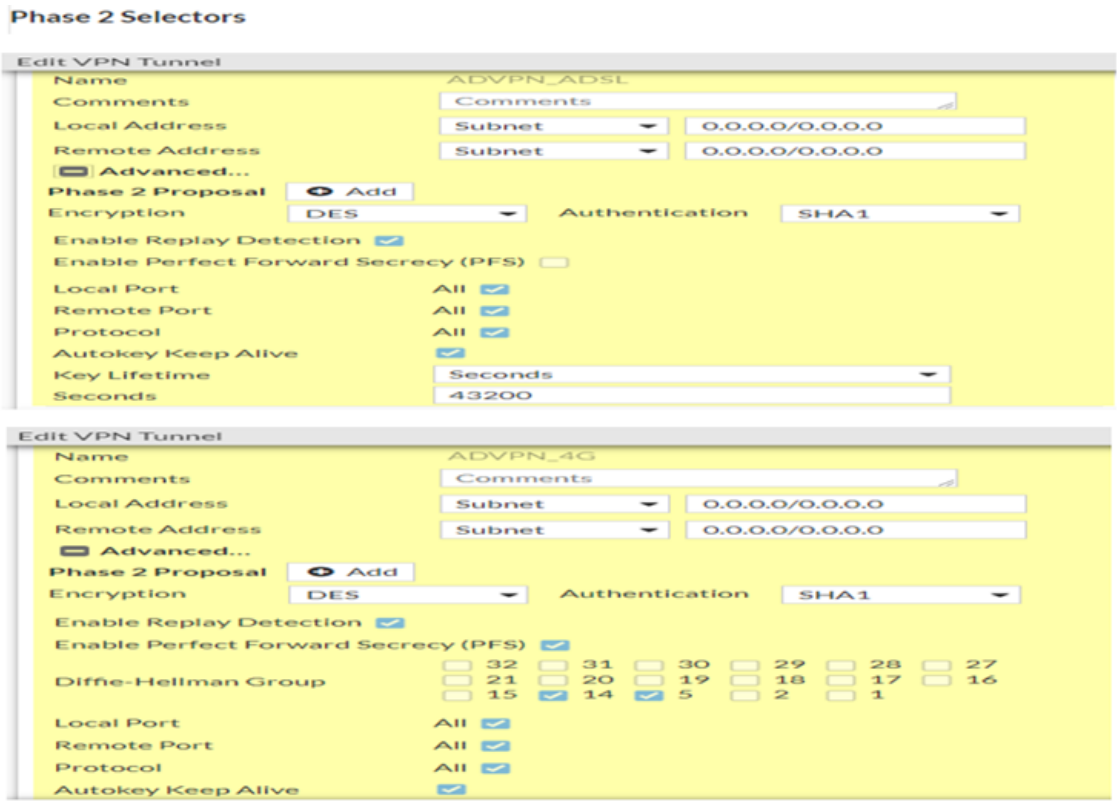


FIGURE 3.22 – Configuration VPN IPsec phase2-interface "ADVPN_ADSL" et "ADVPN_4G" au niveau de HUB interface graphique.

Vérification l'état actif des tunnels IPsec au niveau de HUB

Les deux tunnels VPN IPsec Dial-up sont activés via l'interface graphique de FortiGate du site central (HUB).

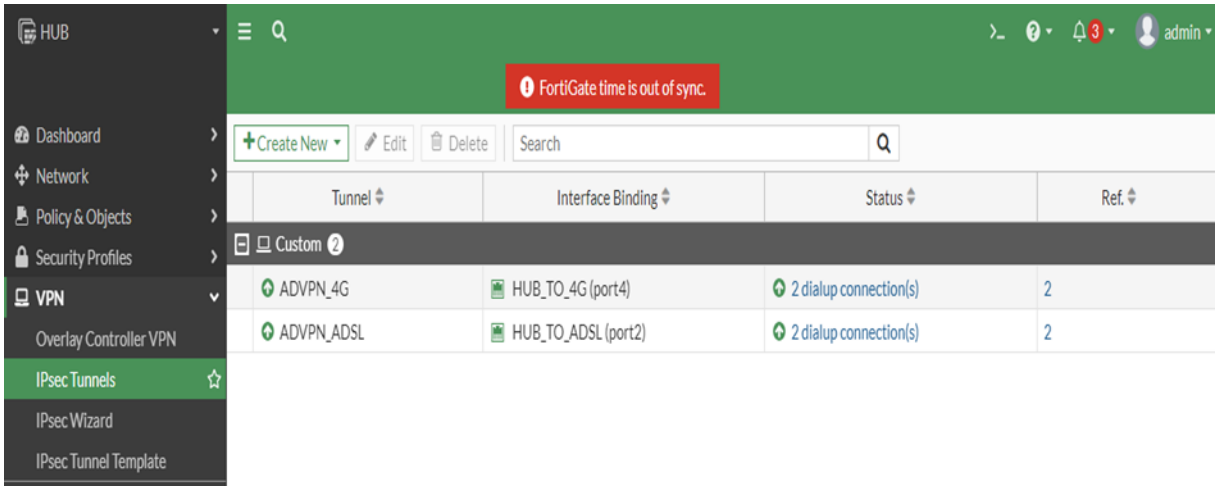


FIGURE 3.23 – État des deux tunnels VPN IPsec au niveau du HUB.

Analyse de la figure 3.23

- Les deux tunnels VPN IPsec, "**ADVPN_4G**" et "**ADVPN_ADSL**", ont chacun deux connexions Dial-up actives.
- "**ADVPN_4G**" utilise l'interface "**HUB_TO_4G**" sur le port4, tandis que "**ADVPN_ADSL**" utilise l'interface "**HUB_TO_ADSL**" sur le port2.
- Ces connexions sécurisées permettent au hub d'établir des communications avec des sites distants de manière sécurisée.

Etape2. Configuration des tunnels au niveau du Spoke1 :

Configuration du tunnel vpn ipsec phase1-interface "ADVPN_4G" et "ADVPN_ADSL" au niveau de SPOKE1

- **VIA CLI**

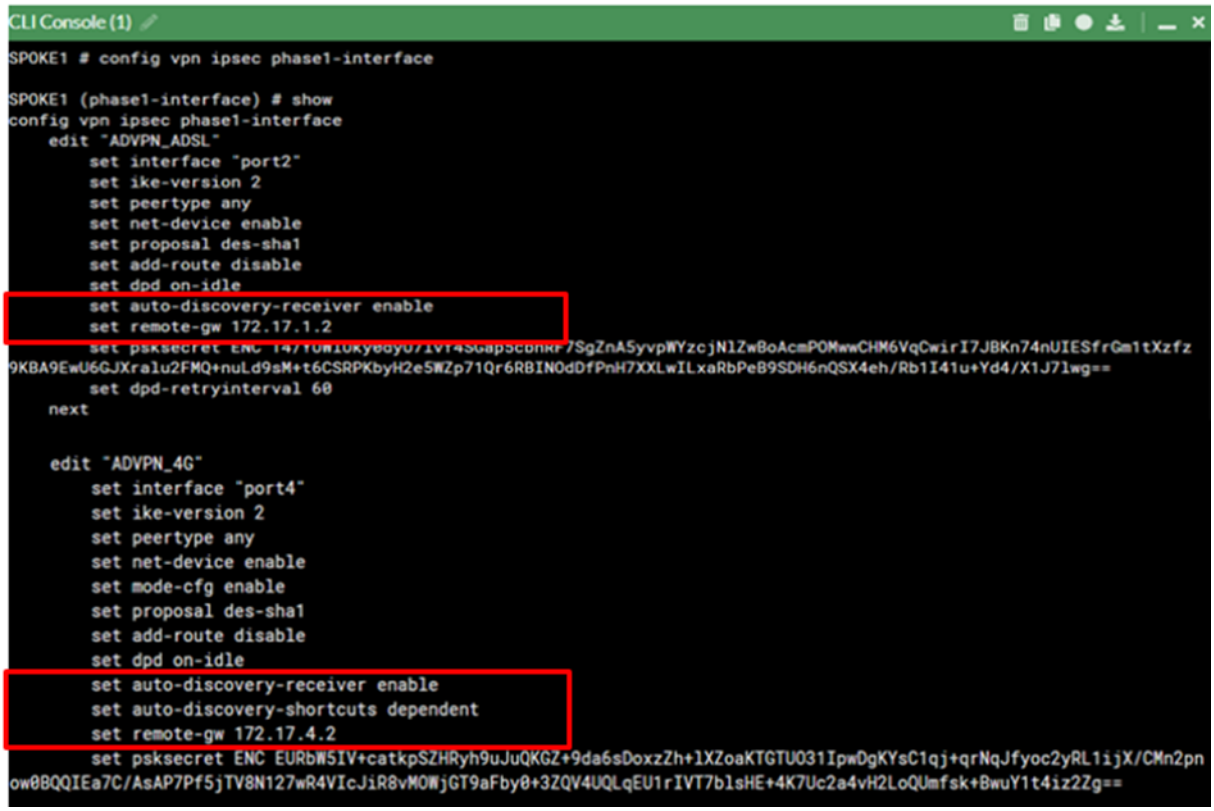


FIGURE 3.24 – Configuration VPN IP sec phase1-interface "ADVPN_ADSL" et "ADVPN_4G" au niveau de SPOKE1 via CLI.

Analyse de la figure 3.24 : La figure représente La configuration des interfaces de phase 1 des tunnels VPN IPsec pour le périphérique SPOKE1, permettant d'établir une connexion VPN sécurisée avec le hub. Pour l'interface "**ADVPN_ADSL**" :

- **set interface port2** : Définit l'interface utilisée pour le tunnel VPN IPsec comme "**port2**".
- **set ike-version 2** : Spécifie la version 2 du protocole IKE (Internet Key Exchange) pour la négociation des clés utilisé et établir la connexion VPN.
- **set net-device enable** : Active la fonctionnalité de l'interface réseau pour le tunnel, ce qui permet l'utilisation de l'interface pour le trafic VPN.
- **set auto-discovery-receiver enable** : Active la fonction de réception de découverte automatique pour la configuration dynamique du tunnel.

— **set net-device enable** : Active la fonctionnalité de l'interface réseau pour le tunnel, ce qui permet l'utilisation de l'interface pour le trafic VPN.
— **set remote-gw 172.17.1.2** : Spécifie l'adresse IP de la passerelle distante (HUB) via le tunnel ADSL.
— **set psksecret ENC** : Spécifie la clé prépartagée (PSK) chiffrée pour l'authentification du tunnel.

Ainsi que la même configuration à appliquer sur la deuxième interface "**ADVPN_4G**", en modifiant l'adresses IP de tunel ainsi l'adresse de set remote-gw 172.17.4.2 qui Spécifie l'adresse IP de la passerelle distante (HUB) via le tunnel 4G.

o **Via l'interface graphique de FortiGate :**

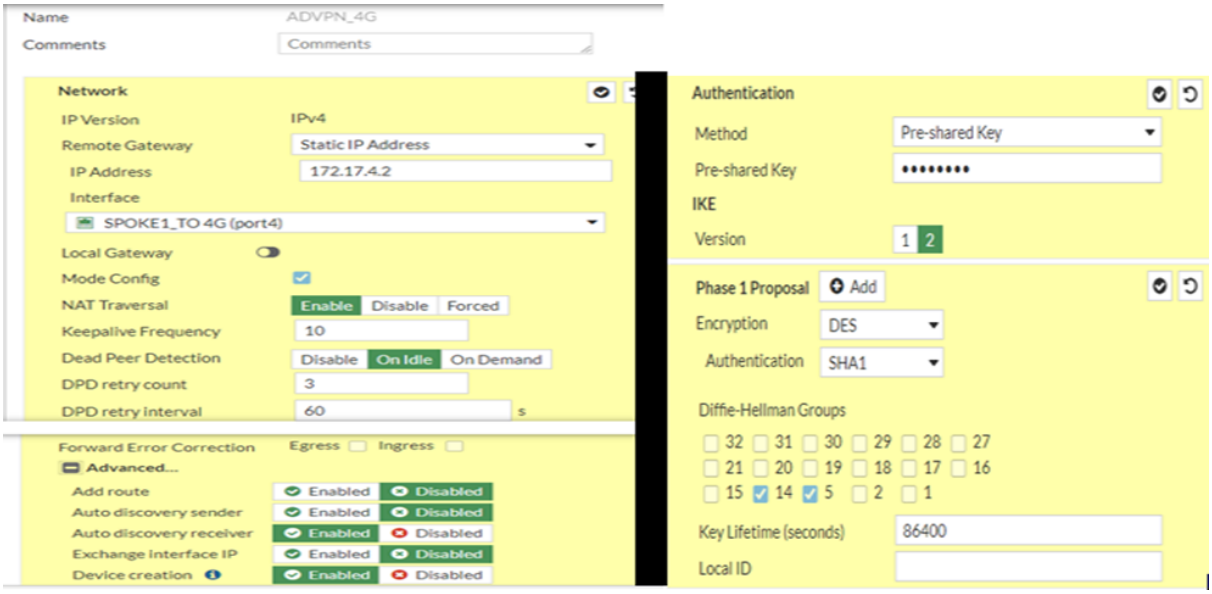


FIGURE 3.25 – Configuration VPN IP sec phase1-interface et "ADVPN_4G" via l'interface graphique de FortiGate dans le SPOKE1.

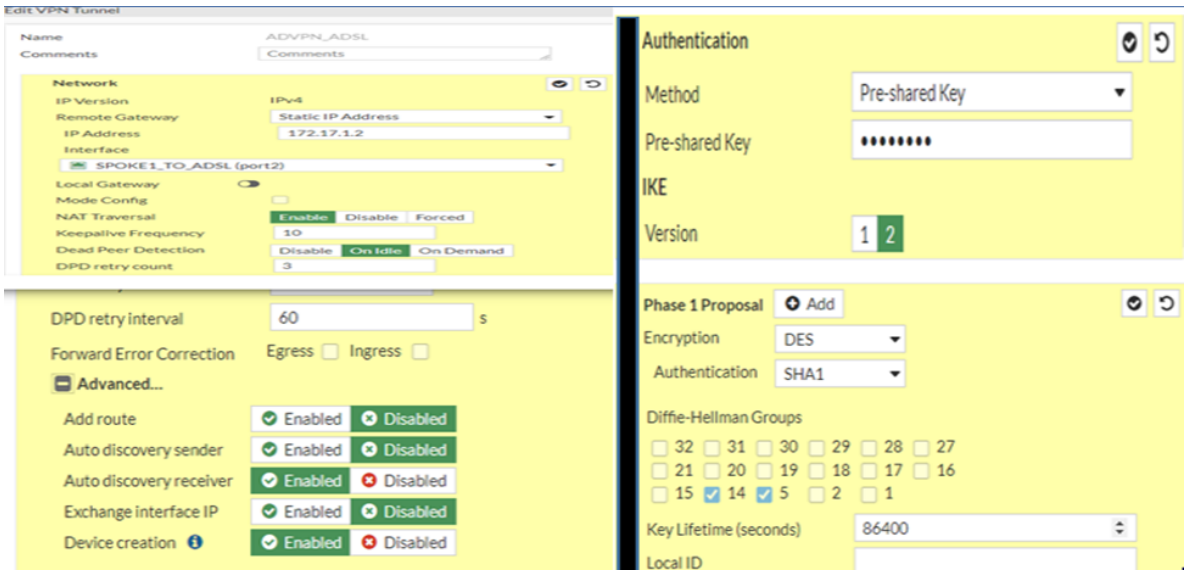


FIGURE 3.26 – Configuration VPN IP sec phase1-interface "ADVPN_ADSL" via l'interface graphique de FortiGate dans le SPOKE1.

Configuration des interfaces de phase 2 du VPN IPsec pour les tunnels "ADVPN_4G" et "ADVPN_ADSL" au niveau du SPOKE1

o **VIA CLI**

FIGURE 3.27 – Configuration VPN IP sec phase2-interface "ADVPN_4G" et "ADVPN_ADSL" via CLI au niveau de SPOKE1.

Analyse de la figure 3.27 : Cette configuration concerne les interfaces de phase 2 des tunnels VPN IPsec. Voici les paramètres importants expliqués. L'interface "ADVPN_ADSL" est configurée avec les éléments suivants :

- Le nom de la phase 1 associée est "*ADVPN_ADSL*", ce qui indique le tunnel VPN correspondant à cette interface.
- L'option "auto-negotiate" est activée, ce qui permet aux périphériques VPN de négocier automatiquement les paramètres de chiffrement, les algorithmes de hachage et autres paramètres de sécurité lors de l'établissement de la connexion VPN.

De même, l'interface "ADVPN_4G" est configurée avec les mêmes paramètres.
Ces configurations définissent les paramètres nécessaires pour établir des connexions sécurisées via les tunnels VPN IPsec correspondants.

- **Via l'interface graphique de FortiGate :**

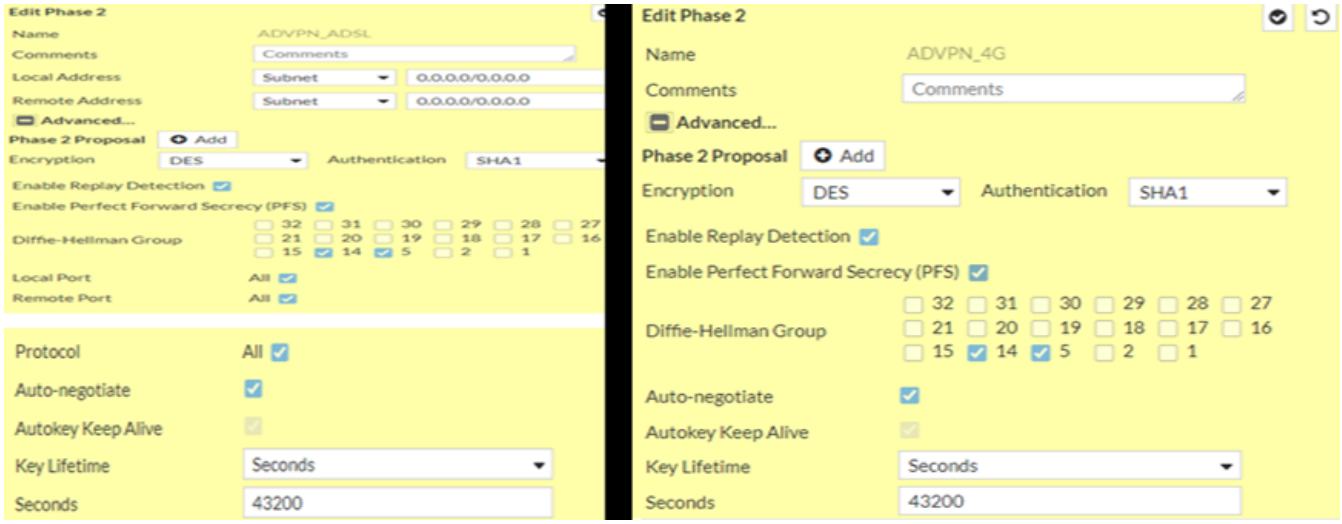


FIGURE 3.28 – Configuration VPN IP sec phase2-interface "ADVPN_4G" et "ADVPN_ADSL" via l'interface graphique de FortiGate au niveaux de SPOKE1.

Vérification l'état actif des tunnels IPsec sur le site distant (SPOKE1).

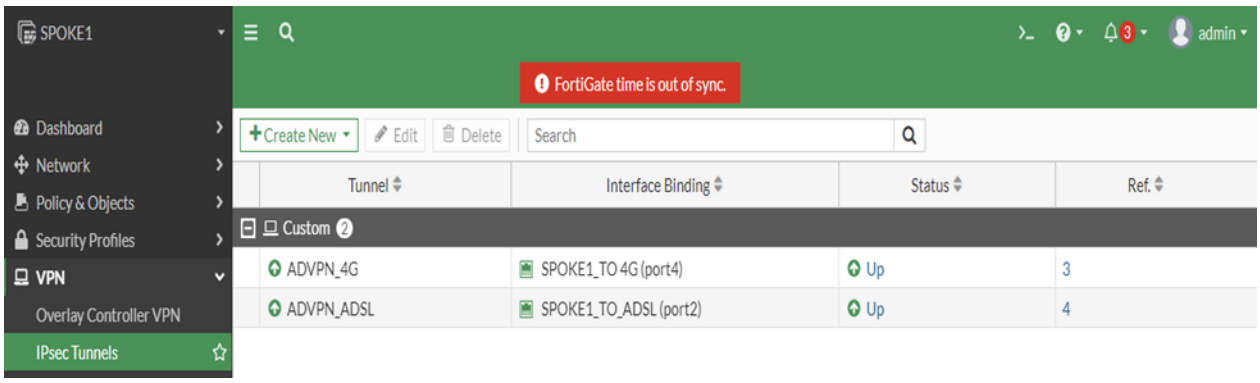


FIGURE 3.29 – État des deux tunnels VPN IPsec au au niveau du SPOKE1.

Analyse de la figure 3.29 :

- La configuration indique que Spoke1 établit une connexion VPN IPsec avec le hub via deux tunnels distincts : "ADVPN_4G" et "ADVPN_ADSL".
- Ces tunnels sont en ligne, ce qui signifie que la connexion VPN IPsec entre Spoke1 et le hub est établie et opérationnelle.
- Cela permet à Spoke1 de communiquer de manière sécurisée avec le réseau du hub.

Etape3. Configuration du protocole de routage utilisée dans déploiement SD-WAN au niveau de HUB Le déploiement du SD-WAN repose sur l'utilisation du protocole de routage BGP afin d'assurer la connectivité des sites distants avec le site central. Cette décision est basée sur la compatibilité du protocole BGP avec le SD-WAN FortiGate.
En outre, le choix du protocole BGP permet d'établir une distinction claire entre le type de routage employé au sein du réseau local de l'entreprise (OSPF) et ceux employés dans le réseau étendu (BGP).

Community-list

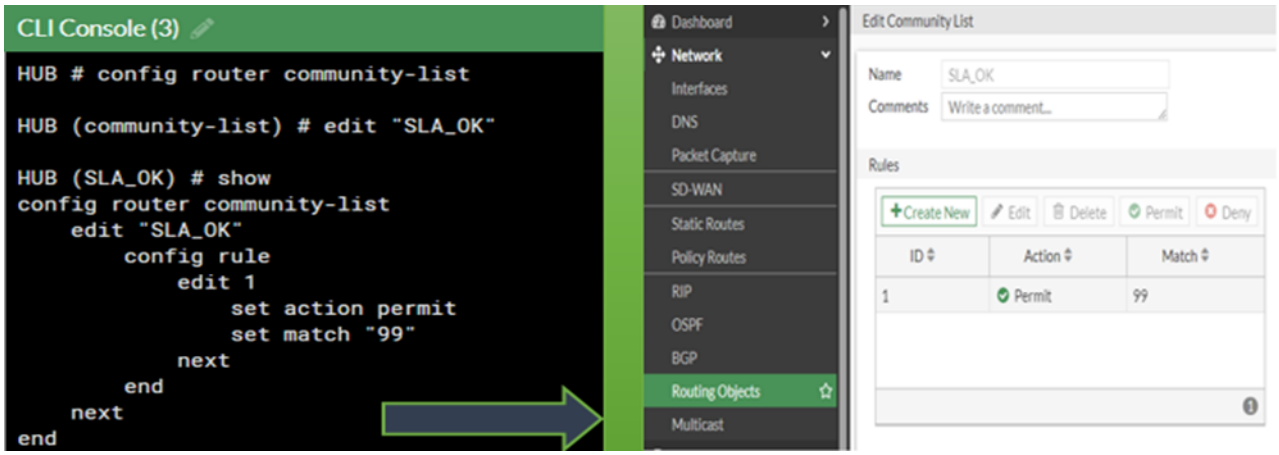


FIGURE 3.30 – Configuration de la liste de communautés SLA_OK sur le périphérique HUB via CLI a gauche et l'interface graphique de FortiGate a droit.

Analyse de la figure 3.30 : Cette configuration concerne une liste de communautés appelée SLA_OK sur le périphérique HUB.
La liste de communautés SLA_OK permet de contrôler le trafic en autorisant ou en refusant des paquets en fonction de leur communauté. Elle permet la mise en place de politiques de routage.

— La règle numéro 1 dans la liste SLA_OK a l'action permit (autoriser) et correspond au match 99.
— Cela signifie que les paquets de données avec une communauté correspondant à 99 seront autorisés à traverser le périphérique HUB.

Une route-map

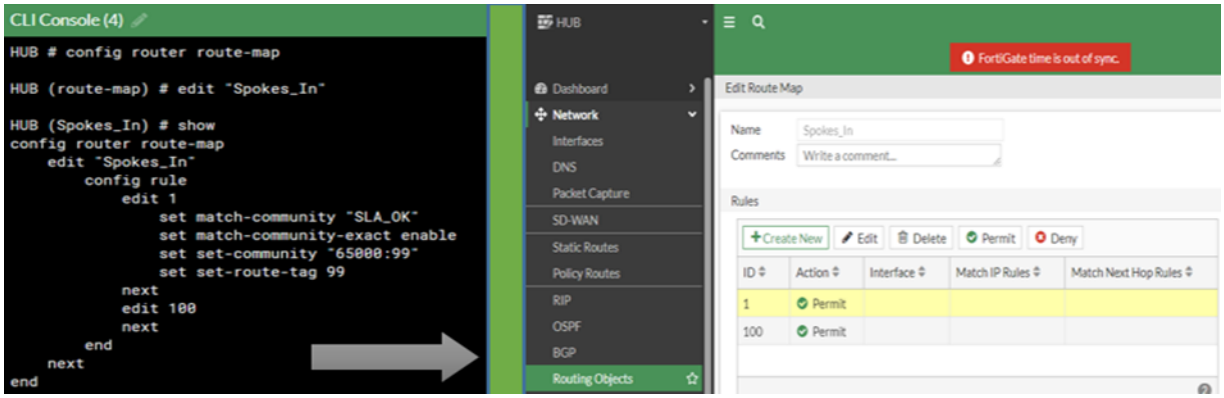


FIGURE 3.31 – Configuration d'une route-map sur le périphérique HUB via CLI à gauche et l'interface graphique de FortiGate a droit.

Analyse de la figure 3.31 : Cette configuration concerne une route-map nommée Spokes_In sur le périphérique HUB. Voici l'explication et le rôle de cette configuration :

— La règle numéro 1 dans la route-map Spokes_In est configurée pour correspondre à la communauté SLA_OK . Cela signifie que les paquets de données avec une communauté correspondant à SLA_OK seront pris en compte par cette règle.
— L'action associée à cette règle est de modifier la communauté en 65000 :99 et d'ajouter un tag de route de valeur 99.
— La route-map Spokes_In modifie la communauté des paquets correspondants en 65000 :99 et ajoute un tag de route de valeur 99. Ces actions permettent de contrôler le traitement et le routage ultérieur des paquets en fonction de leur communauté et du tag de route associé.

Configuration de routage BGP au niveau de HUB

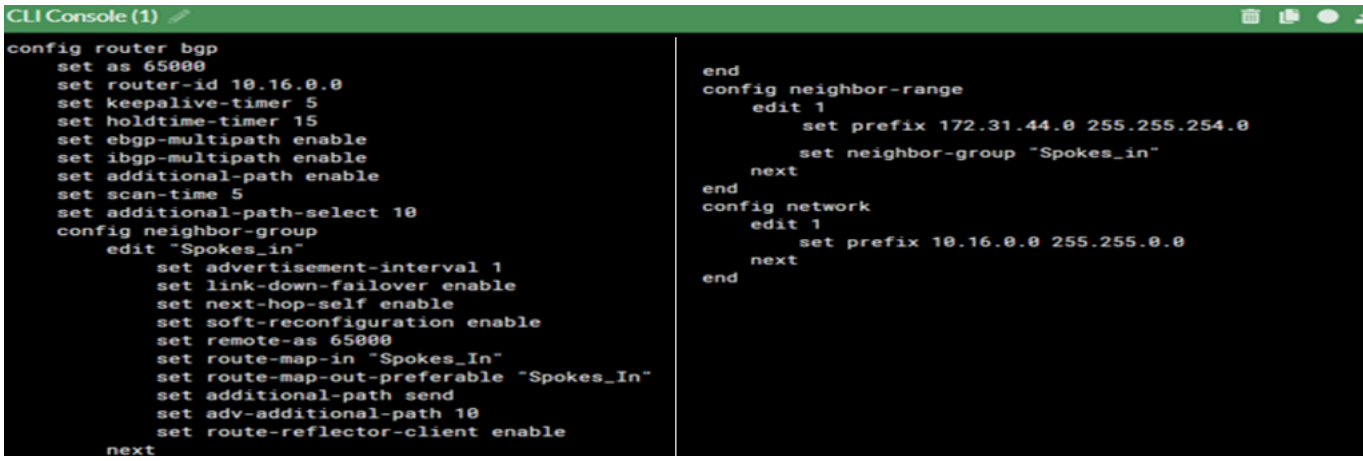


FIGURE 3.32 – configuration de BGP au niveau de HUB via CLI.

Analyse de la figure 3.32 : Cette configuration BGP comprend plusieurs paramètres et options spécifiés pour la mise en place du routage dans un environnement SD-WAN. Voici une explication des différentes directives utilisées :

— **set as 65000 :** Définit le numéro d'AS (Autonomous System) à 65000.
— **set router-id 10.16.0.0 :**Spécifie l'adresse IP utilisée comme identifiant du routeur BGP
— La configuration du groupe de voisins (neighbor-group) spécifique nommé "Spokes_in" comprend les directives suivantes :
  o **advertisement-interval 1 :** Spécifie l'intervalle de temps entre les annonces de routage BGP envoyées aux voisins du groupe.
  o **link-down-failover enable :** Active la fonction de basculement automatique vers un autre chemin lorsque la connectivité avec un voisin est perdue.
  o **next-hop-self enable :** Modifie le prochain saut annoncé dans les mises à jour de routage BGP avec l'adresse IP du routeur local.
  o **remote-as 65000 :** Spécifie le numéro d'AS du voisin BGP avec lequel une session doit être établie.
  o **route-map-in "Spokes_In" :** Applique un filtre de routage entrant aux mises à jour de routage BGP reçues du voisin.
  o **route-map-out-preferable "Spokes_In" :** Spécifie une préférence pour les mises à jour de routage BGP sortantes qui correspondent au filtre de routage spécifié.

Tableau de bord BGP : Visualisation des routes BGP et des interfaces de tunnel pour les destinations Spokes au niveau de HUB

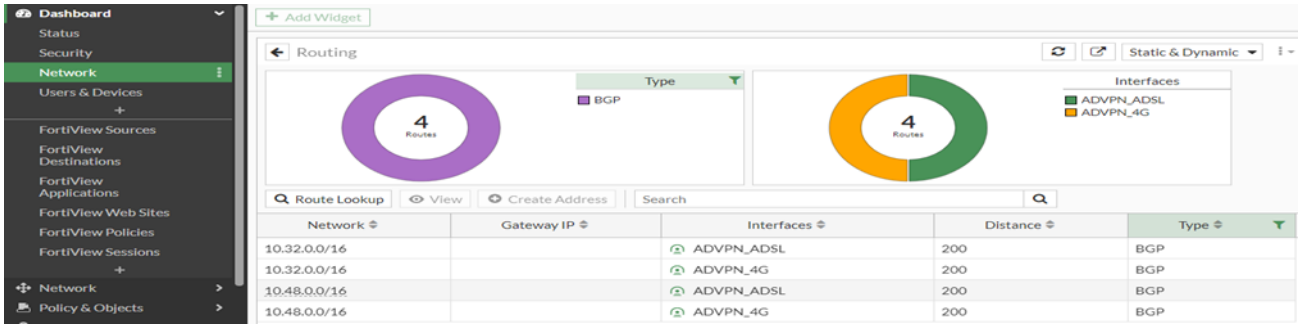


FIGURE 3.33 – Vue d'ensemble des routes BGP et des interfaces de tunnel pour les destinations Spokes au niveau de HUB.

Analyse de la figure 3.33 :
— Quatre routes de type BGP ont été configurées pour les plages d'adresses 10.32.0.0/16 (adresse locale du site distant 1) et 10.48.0.0/16 (adresse locale du site distant 2).
— Chacune de ces routes est associée à une interface de tunnel spécifique (ADVPN_ADSL ou ADVPN_4G).
— Ces routes permettent au réseau de guider le trafic vers les destinations correspondantes en utilisant les interfaces de tunnel spécifiques.

Etape4. Configuration du protocole de routage utilisée dans déploiement SD_WAN au niveau de SPOKE1

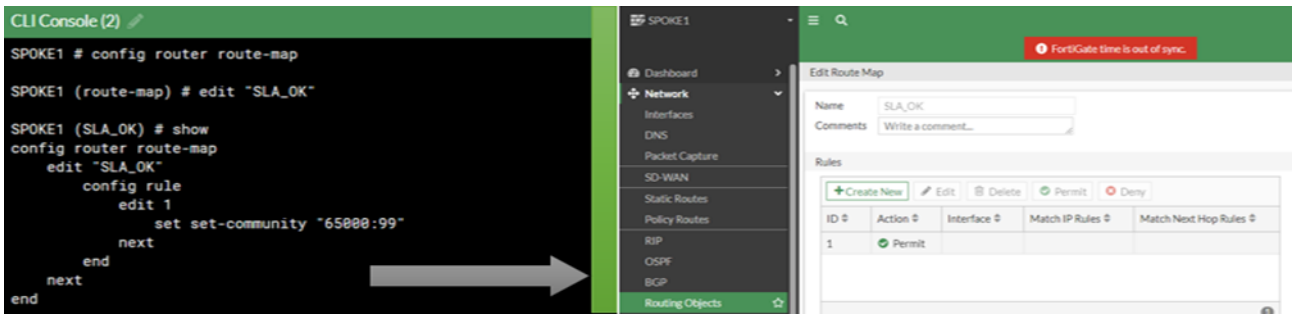


FIGURE 3.34 – Configuration d'une route-map sur le périphérique SPOKE1 via CLI à gauche et l'interface graphique de FortiGate a droit.

Analyse de la figure 3.34 :

- La règle 1 de la route-map SLA_OK utilise l'action set-community avec la valeur 65000 :99.
- La liste de communauté 65000 :99 a été créée au niveau du concentrateur (HUB) et sera appliquée aux routes correspondantes lorsque la règle 1 de la route-map sera appliquée.

Configuration de routage BGP au niveau de SPOKE1

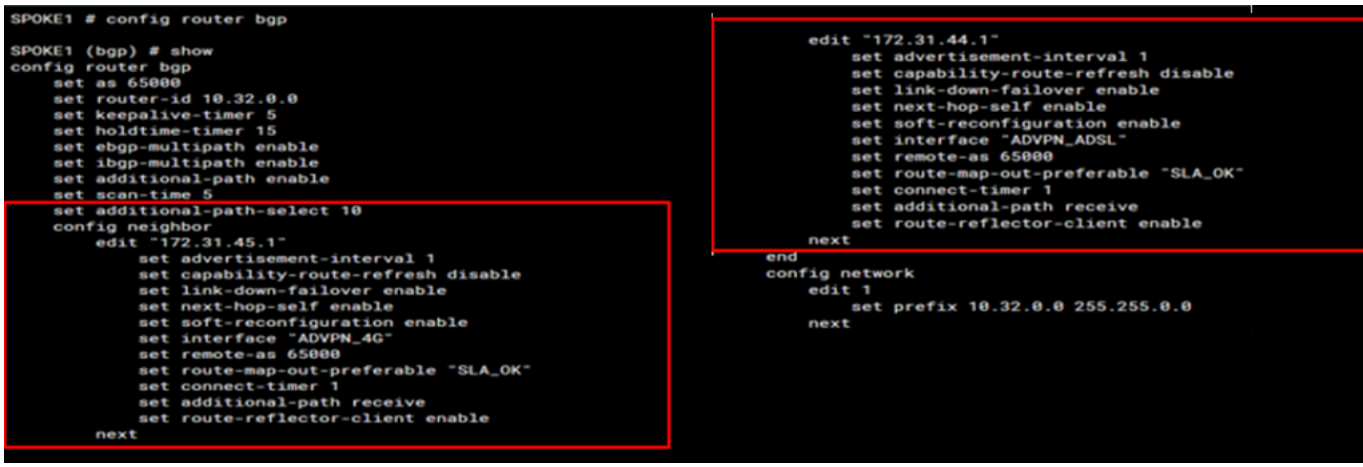


FIGURE 3.35 – configuration de BGP au niveau de SPOKE1 via CLI.

Analyse de la figure 3.35 : Représente la configuration des voisins BGP qui sont spécifiés pour le routeur "SPOKE1" avec les adresses IP 172.31.45.1 et 172.31.44.1. Voici les paramètres spécifiques configurés pour chaque voisin :

- **Link-down-failover enable :** Cette option active le basculement vers une autre connexion BGP lorsque la connexion actuelle est interrompue. Cela permet de maintenir une connectivité BGP stable en cas de défaillance de la connexion.
- **Next-hop-self enable :** Cette option indique au routeur de spécifier son propre adresse IP en tant que prochain saut dans les annonces de routes BGP envoyées au voisin.
- **Set interface :** cette option indique que les interfaces ADVPN_4G et ADVPN_ADSL sont utilisées respectivement pour établir la connexion BGP avec les voisins ayant les adresses IP 172.31.45.1 et 172.31.44.1. Ces interfaces sont des tunnels spécifiques créés pour se connecter au hub) Ainsi, la communication BGP entre le routeur SPOKE1 et ces voisins se fait à travers les tunnels établis sur les interfaces ADVPN_4G et ADVPN_ADSL.
- **Route-map-out-preferable "SLA_OK" :** Cette option spécifie le nom de la route-map à appliquer lors de l'envoi des annonces de routes BGP au voisin. Dans

ce cas, la route-map nommée SLA_OK est utilisée.

— **Connect-timer 1 :** Cela définit le délai de temporisation lors de l'établissement de la connexion BGP avec le voisin. Dans ce cas, la temporisation est de 1 unité de temps.

— **Route-reflector-client enable :** Cette option active le rôle de client réflecteur de routes BGP pour le routeur SPOKE1. Cela signifie que SPOKE1 peut recevoir des annonces de routes provenant d'autres routeurs du même AS via le réflecteur de routes.

— **Tableau de bord BGP au niveau de SPOKE1 :**

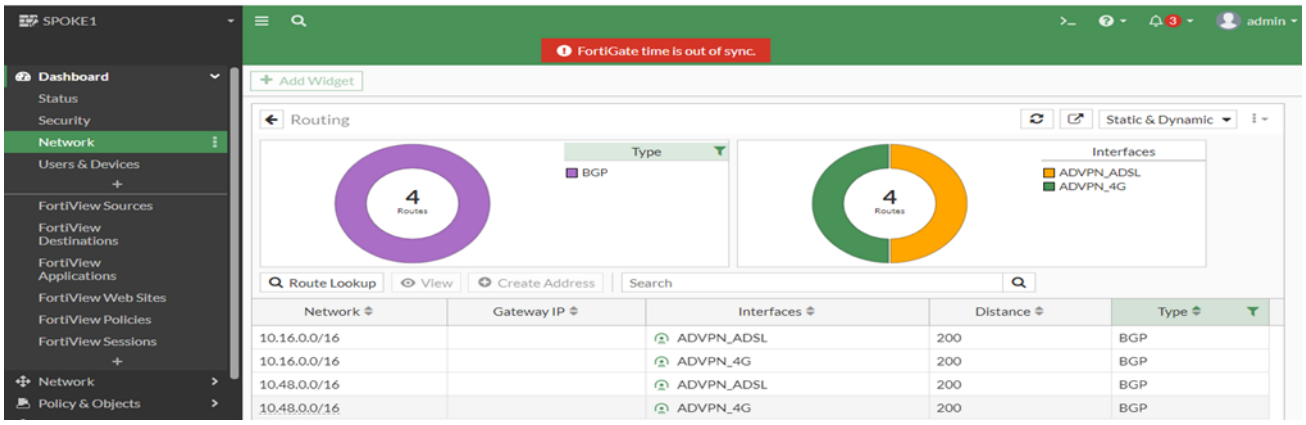


FIGURE 3.36 – Vue d'ensemble des routes BGP et des interfaces de tunnel pour les destinations, au niveau de SPOKE1.

Analyse de la figure 3.36 : Le tableau de bord BGP affiche quatre routes BGP dans ce cas, avec les détails suivants :

— La route BGP 10.16.0.0/16 est configurée pour correspondre à l'adresse locale du concentrateur (HUB). Elle est liée à l'interface ADVPN_ADSL. De plus, la même route BGP 10.16.0.0/16 est également configurée pour correspondre à l'adresse locale du concentrateur (HUB) et est associée à l'interface ADVPN_4G.

— La route BGP 10.48.0.0/16 est configurée pour correspondre à l'adresse locale du SPOKE2. Elle est liée à l'interface ADVPN_ADSL. De plus, la même route BGP 10.48.0.0/16 est également configurée pour correspondre à l'adresse locale du SPOKE2 et est associée à l'interface ADVPN_4G.

— Le tableau de bord BGP fournit une vue d'ensemble des routes BGP configurées, facilitant ainsi la gestion et le suivi du routage dans le réseau.

Etape5. Configuration de SD_WAN : La même configuration a été appliquée à la fois sur le site central (hub) et sur le site distant (spoke).

Configuration d'un zone SD-WAN :

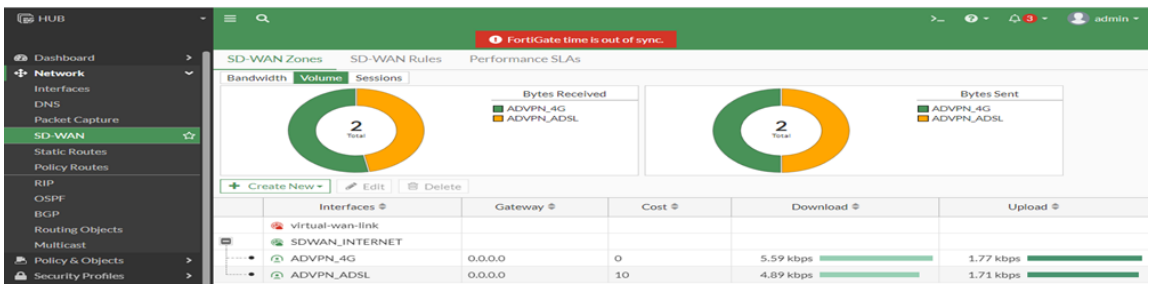


FIGURE 3.37 – Affichage des zones SD-WAN.

Analyse de la figure 3.37 : Pour configurer la partie SD-WAN, nous avons suivi les étapes suivantes :

- Nous avons créé une nouvelle zone appelée "SDWAN_INTERNET".
- Ensuite, nous avons ajouté deux membres à cette zone, à savoir les interfaces de tunnel ADVPN_ADSL et ADVPN_4G.
- Ces membres représentent les deux interfaces de tunnel que nous utilisons dans notre configuration SD-WAN. L'interface ADVPN_ADSL est associée à une connexion ADSL et l'interface ADVPN_4G est associée à une connexion 4G.

Configuration de route statique pour la zone SD-WAN :

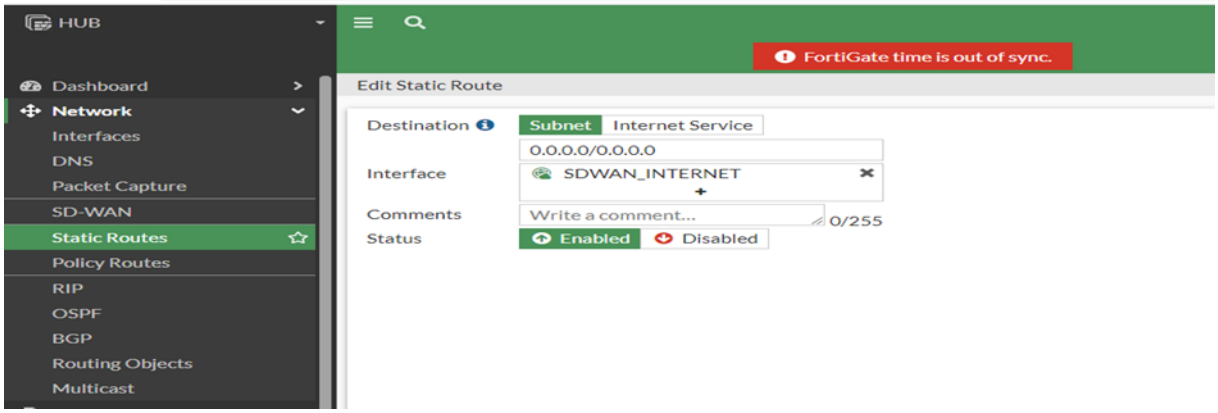


FIGURE 3.38 – Configuration de route statique pour la zone SD_WAN_INTERNET.

Analyse de la figure 3.38 :

- Cette configuration de route statique définit une route spécifique associe à la zone SDWAN_INTERNET dans le contexte de la SD-WAN.
- Cela permet de contrôler la manière dont le trafic est acheminé vers ce réseau spécifique dans le cadre de la configuration SD-WAN.

Configuration des règles de firewall pour la zone SD-WAN

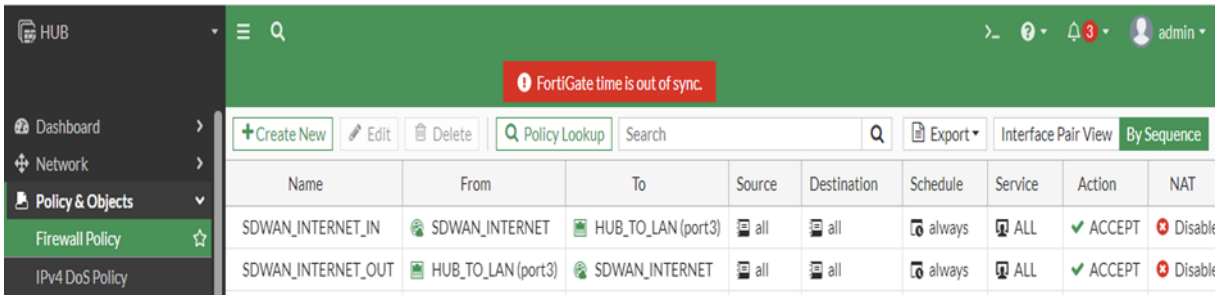


FIGURE 3.39 – Configuration des firewall policy pour le sdwan zone.

Analyse de la figure 3.39 :

- La première configuration de la politique de pare-feu, "SDWAN_INTERNET_IN", permet d'autoriser tout le trafic entrant provenant de l'interface SD-WAN_INTERNET et tout le trafic sortant vers l'interface "port3" qui représente l'interface connectée au réseau local (LAN). Toutes les adresses sources et de destination sont autorisées, ainsi que tous les services.
- La deuxième configuration de la politique de pare-feu, "SD-WAN_INTERNET_OUT", permet d'autoriser tout le trafic sortant de l'interface "port3" qui représente l'interface connectée au réseau local (LAN) vers l'interface

SDWAN_INTERNET. Toutes les adresses sources et de destination sont autorisées, ainsi que tous les services.

Configuration des performances SLA :

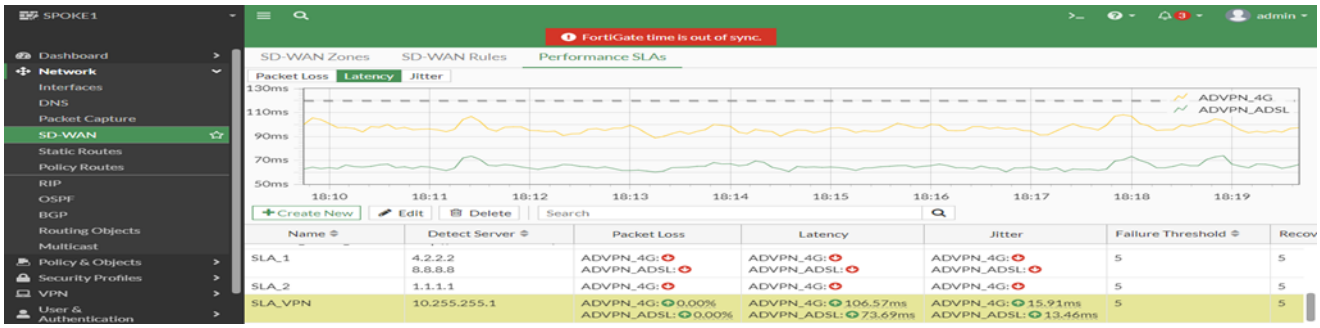


FIGURE 3.40 – Affichage SLA Performances SD-WAN.

Analyse de la figure 3.40 :

- Dans cette configuration, nous avons créé une SLA (Service Level Agreement) de performance . Ce SLA inclut les deux interfaces de tunnel ADVPN-4G et ADVPN-ADSL en tant que membres de la zone SDWAN INTERNET, afin de surveiller les performances de la connectivité.
- Nous avons également définie une SLA Target . Pour la latence, nous avons fixé un seuil de 120 ms, ce qui signifie que nous considérons que la performance est satisfaisante tant que la latence reste inférieure à cette valeur. Pour la gigue (variation de latence), nous avons établi un seuil de 50 ms, et pour la perte de paquets, un seuil de 1
- En surveillant régulièrement les performances des interfaces ADVPN-4G et ADVPN-ADSL par rapport à ces objectifs de SLA, nous sommes en mesure d'évaluer la qualité de la connectivité.

Configuration d'un SDWAN_RULES :

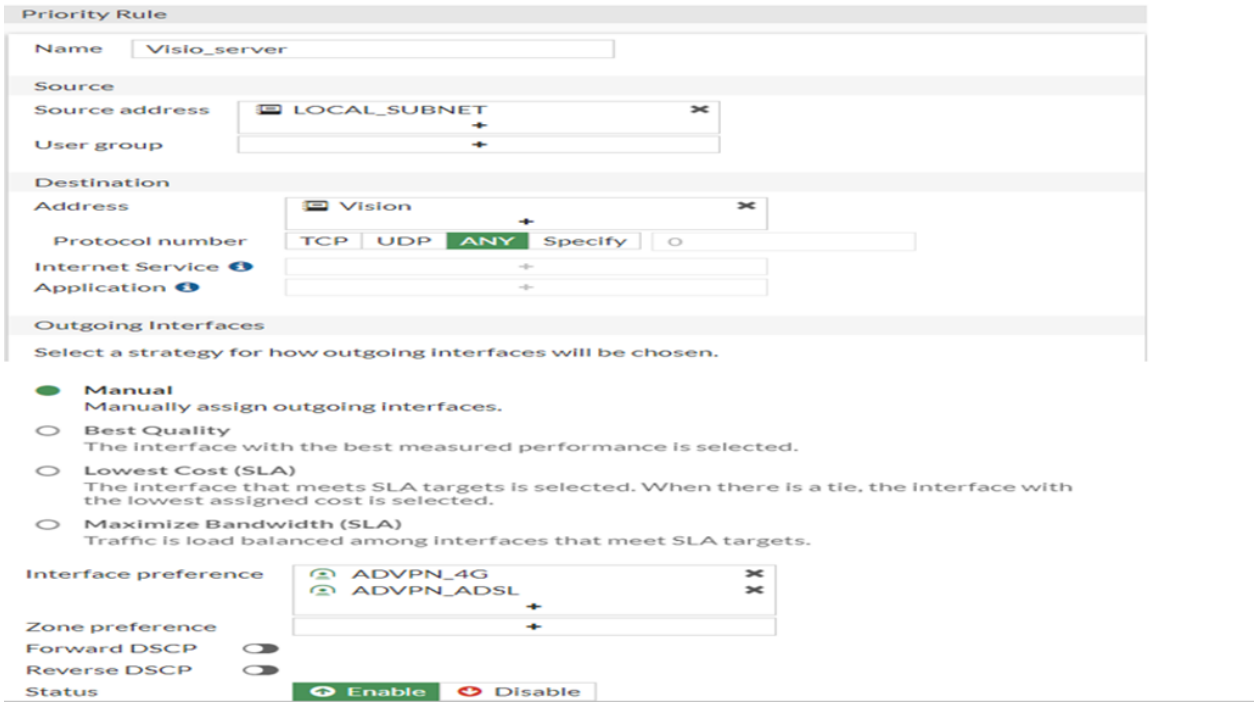


FIGURE 3.41 – Edition d'un accès internet SD-WAN..

Analyse de la figure 3.41 :

- cette configuration crée un service nommé "Visio_server" qui envoie du trafic sortant vers la destination "Vision" à partir de la source "LOCAL_SUBNET". Les membres prioritaires ADVPN_ADSL et ADVPN_4G du SD-WAN sont utilisés pour acheminer ce trafic.
- En plus existe 3 strategie pour choisir les interfaces de sortie (Outgoing Interfaces) qui sont :
  - Manuel : Attribution manuelle des interfaces de sortie pour chaque flux de trafic.
  - Meilleure qualité : Sélection de l'interface avec la meilleure performance mesurée.
  - Coût le plus bas (SLA) : Sélection de l'interface qui atteint les objectifs de SLA avec le coût le plus bas.
  - Maximiser la bande passante (SLA) : Répartition de la charge entre les interfaces qui atteignent les objectifs de SLA pour maximiser la bande passante.

3.6 Déploiement du SD-WAN au niveau de l'équipment Fortigate :

3.6.1 ETAPE 1

Pour mettre à jour notre équipement, nous devons effectuer les actions suivantes dans le fichier de configuration :

- Modifier le host Name en "DG_UNIV_BLIDA".
- Attribuer une adresse IP à l'interface LAN.
- Configurer les interfaces ADSL, RMS, 4G Ooredoo et Mobilis en spécifiant les adresses IP des interfaces locales et distantes pour établir le VPN point à multipoint avec le FortiGate du centre de données. Cela permettra la connectivité sécurisée entre le SPOKE "DG_SD_UNIV_BLIDA"et le HUB .

3.6.2 ETAPE 2

Nous établissons une connexion avec le FortiGate en utilisant le port LAN3 et l'adresse IP LAN préalablement configurée, puis nous saisissons le mot de passe par défaut de l'administrateur.

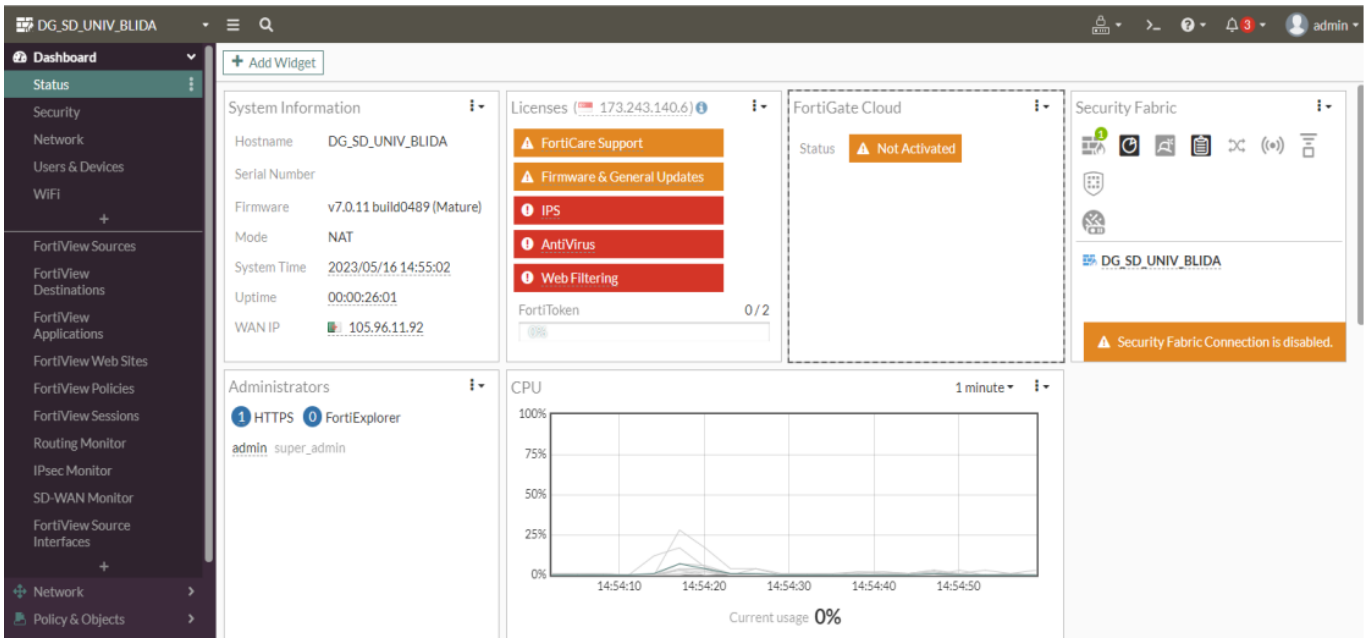


FIGURE 3.42 – Interface d'accueil du pare-feu FortiGate.

Analyse de la figure 3.42 : Voici l'interface d'accueil du FortiGate affichant les informations essentielles.

3.6.3 ETAPE 3

— Nous vérifions que les interfaces sont correctement nommées (ADSL, Mobilis, RMS et 4G Ooredoo).
— Nous vérifions si les tunnels VPN, les règles de pare-feu (firewall policies) et les routes statiques sont correctement créés.

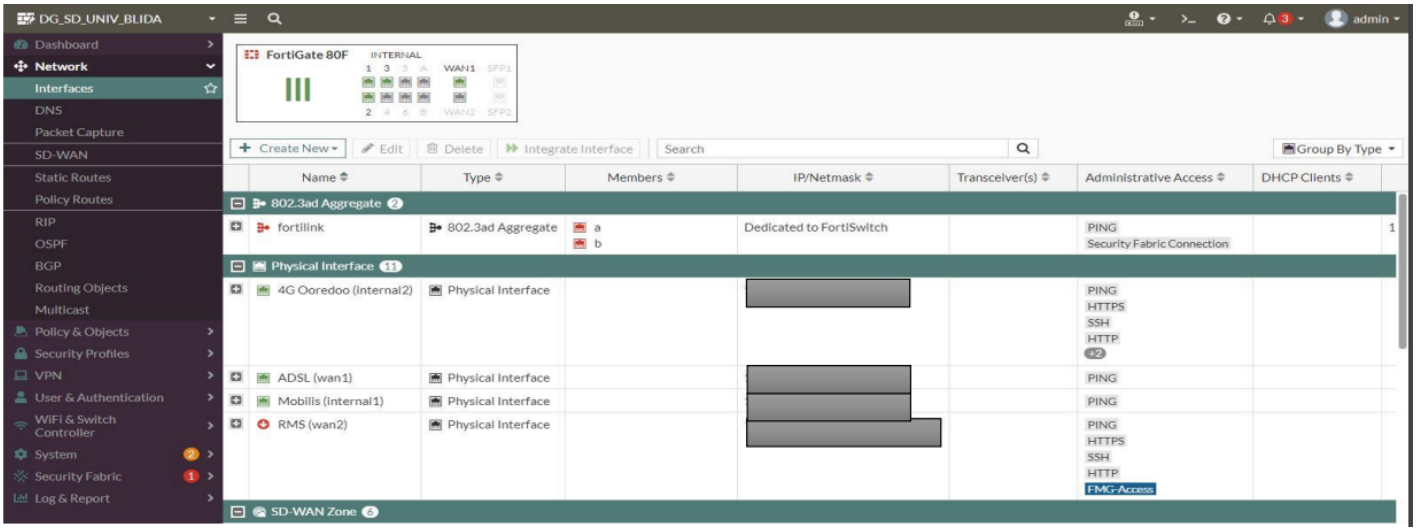


FIGURE 3.43 – Affichage des interfaces réseau.

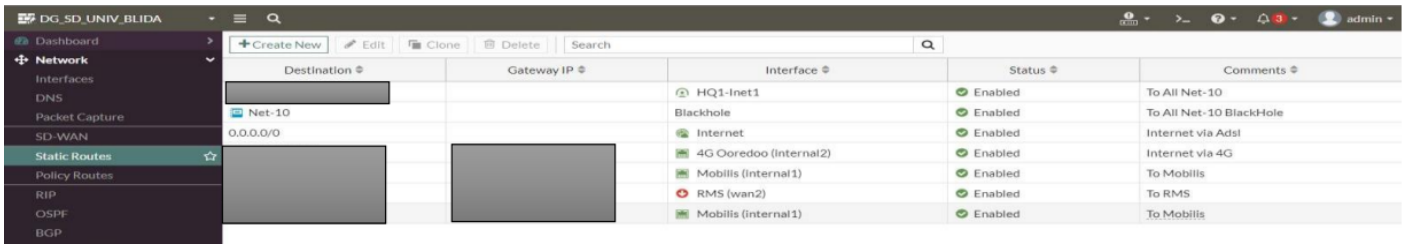


FIGURE 3.44 – Affichage des routes statiques configurées.

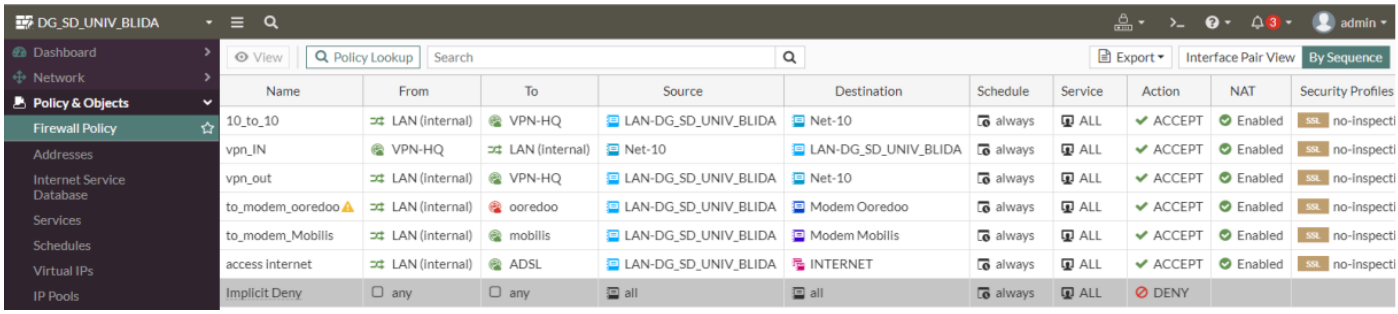


FIGURE 3.45 – Affichage des règles de pare-feu (Firewall Policy).

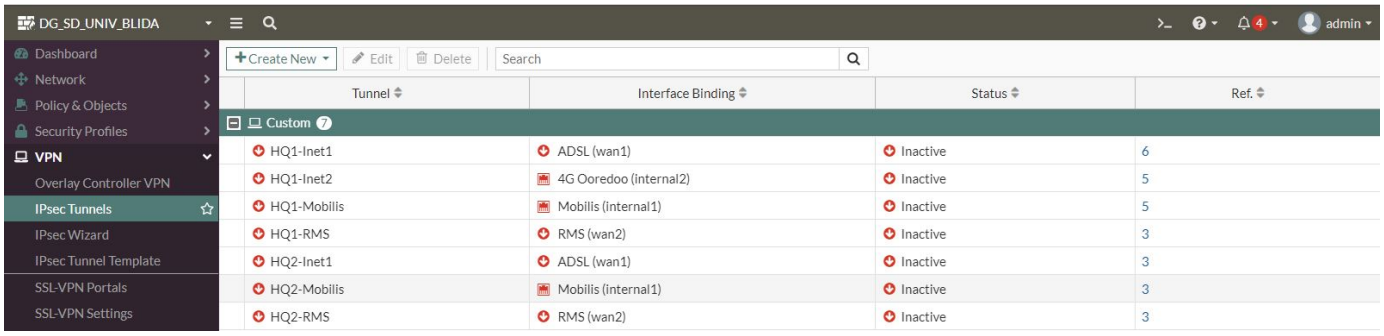


FIGURE 3.46 – Affichage des connexions IPSec (IPSec Tunnels).

3.6.4 ETAPE 4 : Le déploiement d'un pare-feu FortiGate

Nous procédons à la vérification de l'activité des tunnels ADSL et Mobilis et ooredoo en suivant les étapes suivantes :

- Nous connectons le câble ADSL à l'interface physique WAN1 du Firewall Fortigate.
- Nous connectons le câble Mobilis à l'interface physique Internal1 du Firewall Fortigate.
- Nous connectons le câble ooredoo à l'interface physique Internal2 du Firewall Fortigate.
- Nous vérifions l'état des tunnels ADSL et Mobilis et ooredoo pour s'assurer qu'ils sont actifs .
- Cette vérification permet de s'assurer que les connexions ADSL et Mobilis et ooredoo sont établies et que les tunnels VPN sont en fonctionnement.

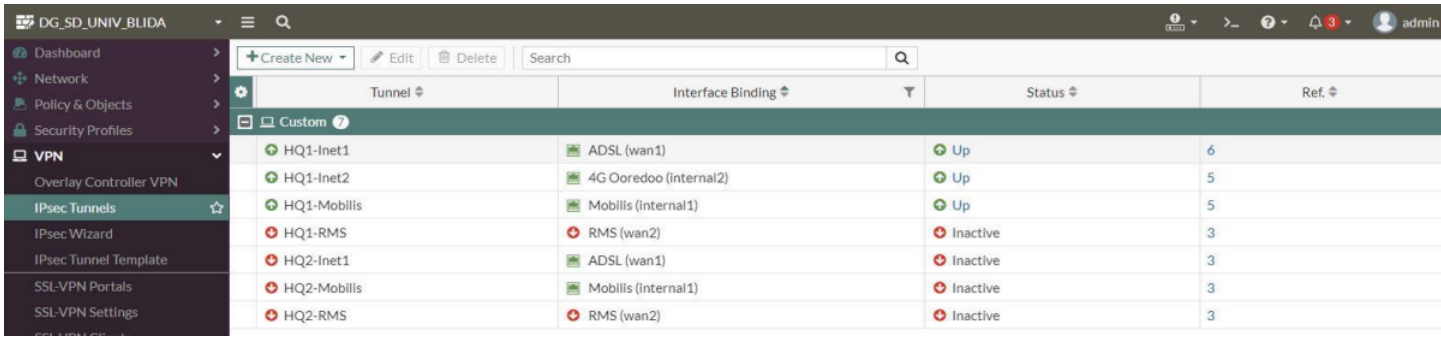


FIGURE 3.47 – Affichage du statut des tunnels VPN IPSec.

Tunnel actif –> Statut : UP (vert).
Tunnel inactif –>Statut : Inactif (rouge).

3.6.5 ETAPE 5 : Vérification de la mise en œuvre du protocole de routage BGP

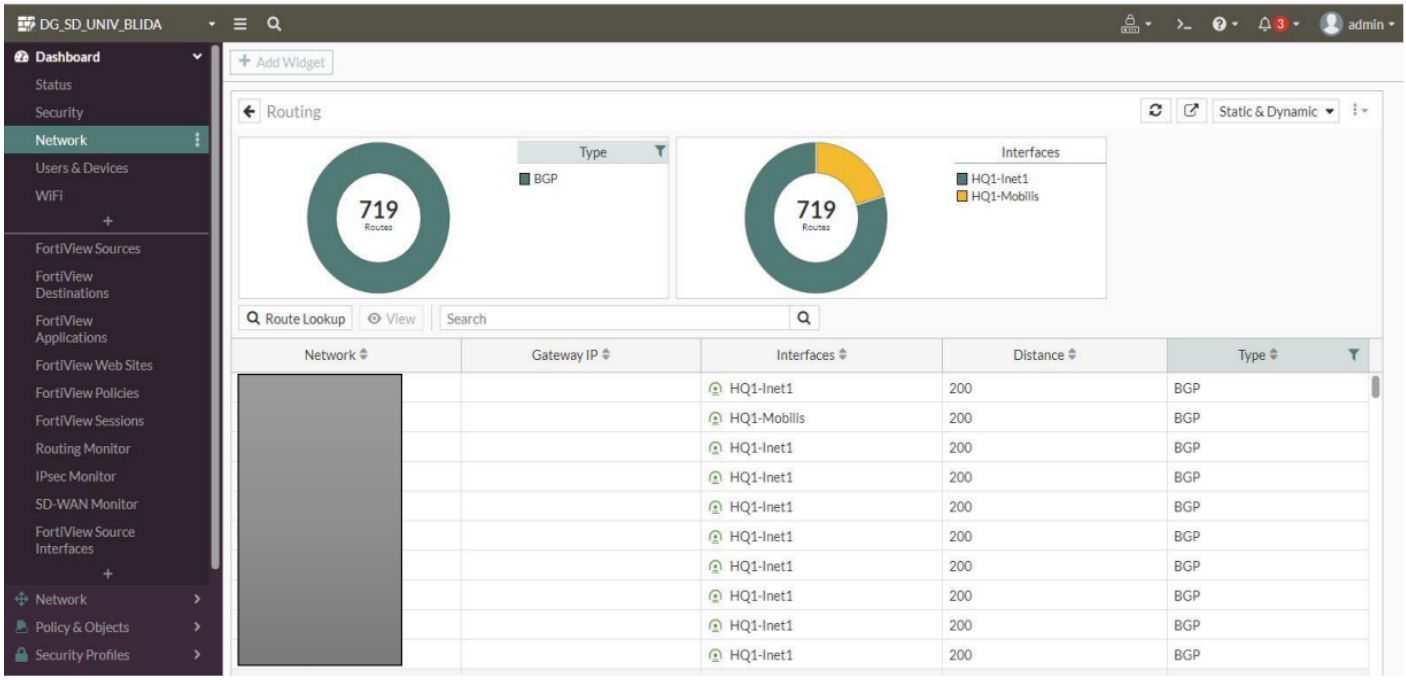


FIGURE 3.48 – Vue d'ensemble des routes BGP et des interfaces de tunnel pour les destinations spécifiées.

3.6.6 ETAPE 6 : Mise en place de la solution SD-WAN

3.6.6.1 Création des zone SD-WAN :

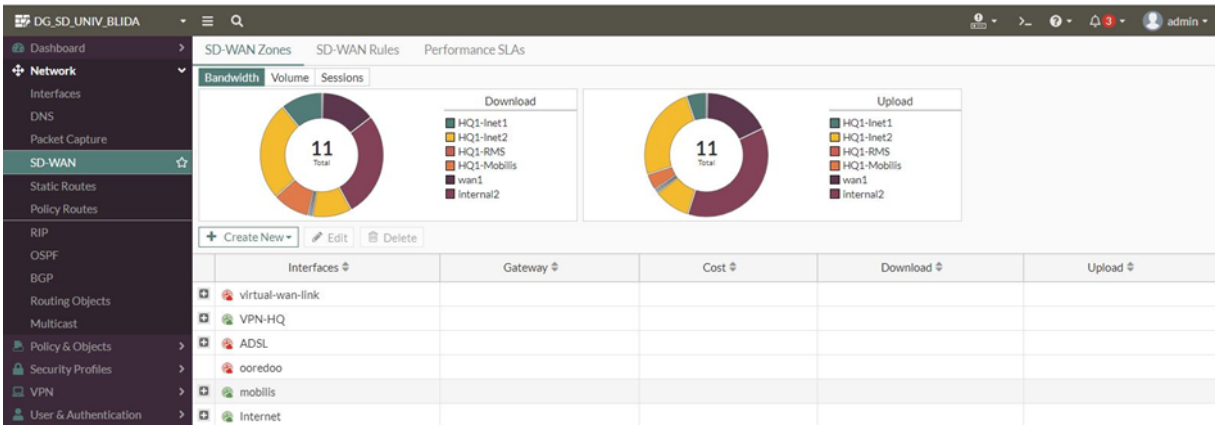


FIGURE 3.49 – Vue d'ensemble des zones SD-WAN.

3.6.6.2 Edit performance SLA :

Lors de la création et de l'édition des performances SLA, nous avons spécifié les participants du SD-WAN, qui comprennent tous les tunnels VPN créés. De plus, nous avons déterminé les paramètres de SLA Target , tels que les seuils de packet loss , et latence et jitter.

En définissant ces paramètres, on établit des mesures permettant de surveiller et d'évaluer la qualité du réseau et d'optimiser le routage du trafic en fonction des performances observées.

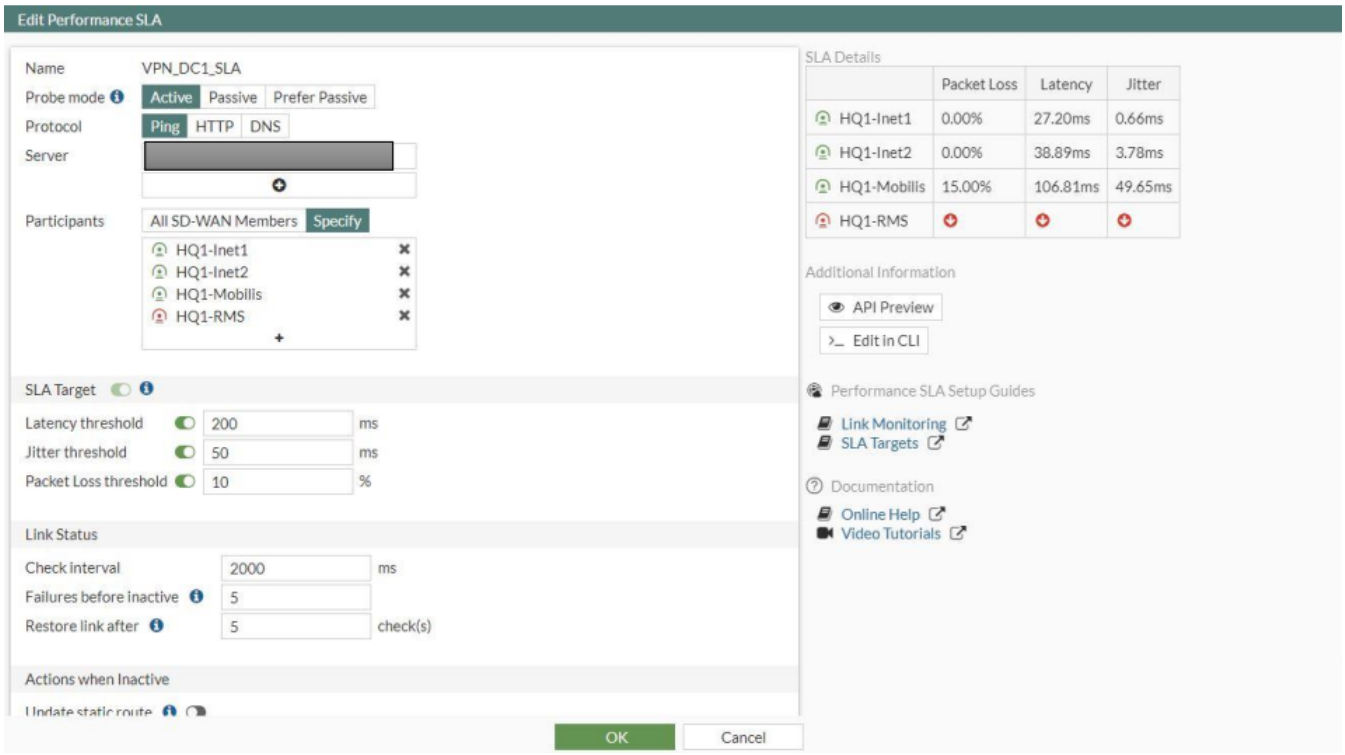


FIGURE 3.50 – Mise à jour des performances SLA.

3.7 Conclusion :

Dans ce chapitre, nous avons exposé les étapes clés de la mise en œuvre de notre solution DMVPN et SD-WAN. Dans un premier temps, nous avons réalisé une analyse approfondie des fonctionnalités de ces deux technologies en utilisant GNS3 comme plateforme d'étude. Par la suite, nous avons procédé au déploiement de ces deux technologies sur du matériel réel au sein de l'entreprise NAFTAL. Ce processus de déploiement pratique a permis de confirmer les performances et l'adaptabilité des solutions DMVPN et SD-WAN dans des scénarios réels.

4 Resultats et discussions

4.1 Introduction

Dans ce chapitre, nous allons examiner les résultats obtenus lors de la mise en œuvre pratique des deux technologies, $DMVPN$ et $SD-WAN$. Nous allons comparer ces technologies en analysant des aspects tels que le taux de packet loss, la latence et le jitter. Ces mesures ont été effectuées sur des équipements Cisco et Fortinet.

4.2 Résultats des tests effectués sur la technologie DMVPN

Les résultats de l'étude sont présentés dans des sections distinctes, couvrant les différentes phases de mise en place de DMVPN (phase 1 et phase 2) sur GNS3. Cela permet de montrer la différence entre ces deux phases en utilisant des adresses claires et compréhensibles.

4.2.1 Vérification des tunnels DMVPN établis (show dmvpn)

En utilisant cette commande sur le routeur d'un site DMVPN pour obtenir une analyse détaillée de l'état des tunnels DMVPN et des peers VPN connectés au ce site. Cela permet de déterminer si les connexions sont établies correctement, mais également de définir le type de connexion, qu'elle soit statique ou dynamique.

4.2.1.1 Exécution de commande au niveau de HUB

```
HUB#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Hub, NHRP Peers:3,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 172.17.3.2          10.250.250.2    UP 00:01:34     D
     1 172.17.2.2          10.250.250.3    UP 00:01:31     D
     1 172.17.4.2          10.250.250.4    UP 00:01:39     D

Interface: Tunnel1, IPv4 NHRP Details
Type:Hub, NHRP Peers:3,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1 172.17.8.1          10.240.240.2    UP 00:01:22     D
     1 172.17.6.1          10.240.240.3    UP 00:00:35     D
     1 172.17.7.2          10.240.240.4    UP 00:01:19     D
```

FIGURE 4.1 – Contrôle de l'état du protocole DMVPN dans le HUB.

Interprétation des résultats de la figure 4.1 Cette commande affiche les détails de la configuration DMVPN sur les tunnels 0 et 1 de l'HUB.

— Le tunnel 0 et le tunnel 1 comportent chacun trois pairs NHRP qui représentent les trois sites distants connectés au hub, chacun étant configuré avec son adresse NBMA et son adresse de tunnel. Tous les pairs sont actifs et configurés en mode dynamique (D).

4.2.1.2 Exécution de commande au niveau de SPOKE

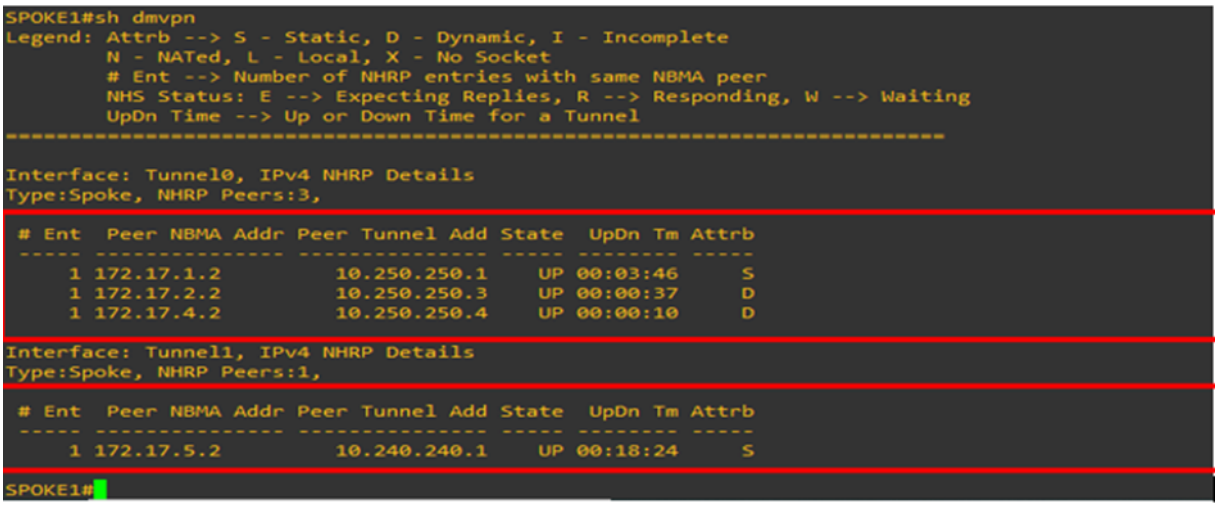


FIGURE 4.2 – Contrôle de l'état du protocole DMVPN dans le Spoke.

Interprétation des résultats de la figure 4.2 Selon les résultats affichés pour le Spoke 1, il est connecté à deux tunnels DMVPN : Tunnel 0 et Tunnel 1.

- **Pour le Tunnel 0**, le Spoke 1 est connecté à trois pairs NHRP qui représentent le Hub et les deux Spokes distants (Spoke2 et Spoke3) sont configurés avec leur adresse NBMA (Non-Broadcast Multi-Access) et leur adresse de tunnel :
  - Le premier pair [HUB : 172.17.1.2 10.250.250.1 S] est actif et connecté en mode statique.
  - Deux autres paires représentant les deux Spokes distant : [Spoke1 :172.17.2.2 - 10.250.250.3 - D ; Spoke2 :172.17.4.2 -10.250.250.4 –D], sont également actives et connectées en mode statique.
- **Pour le Tunnel 1**, le Spoke 1 est connecté à un unique pair NHRP qui représente le HUB, avec leur adresse NBMA correspondant à l'interface connectée au Tunnel 1 et leur adresse de tunnel. Ce pair est actif et configuré en mode statique (S).
- Notre configuration prévoit que les Spokes communiquent directement entre eux en utilisant le Tunnel 0. Car Dans notre cas, le tunnel actif pour la communication entre les sites distants est le tunnel 0, tandis que le tunnel 1 est un tunnel passif.

4.2.2 Affichage des entrées NHRP pour les réseaux distants accessibles via les tunnels DMVPN (commande "show ip nhrp")

4.2.2.1 Exécution de commande au niveau de HUB

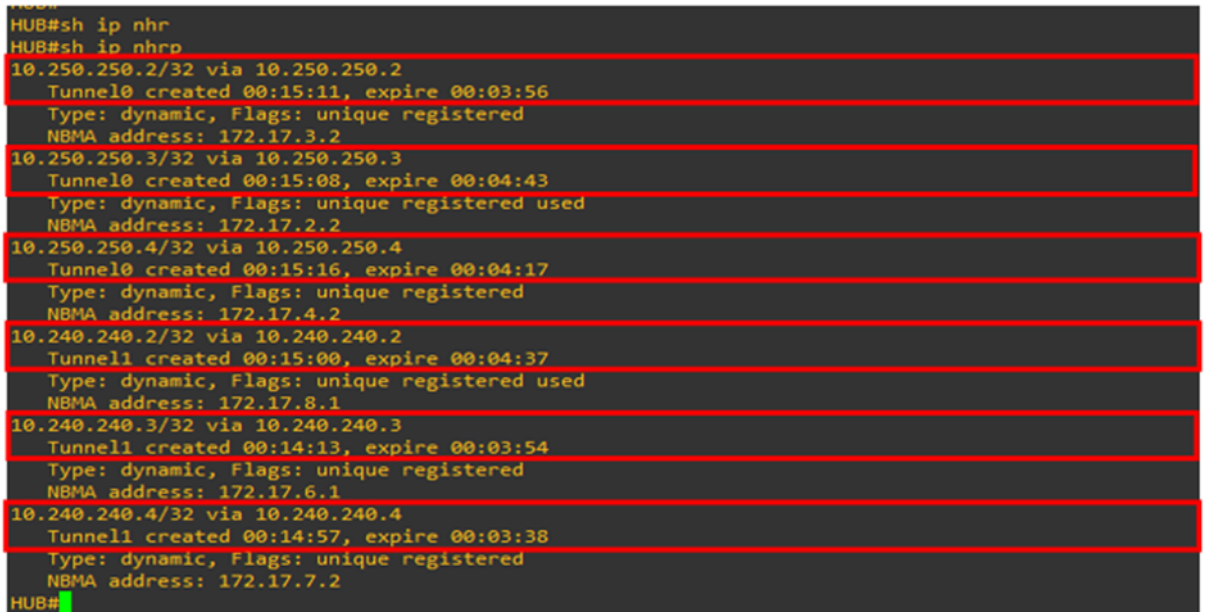


FIGURE 4.3 – Affichage des routes via le protocole NHRP.

Interprétation des résultats de la figure 4.3

— Chaque ligne de la sortie fournit des détails sur les adresses IP distantes accessibles via NHRP, notamment l'adresse IP "Next Hop" du routeur suivant sur le chemin menant à cette adresse, et le tunnel utilisé pour atteindre cette adresse, et d'autres informations telles que le type d'entrée (dynamique), et l'adresse NBMA du prochain saut.

— Dans ce résultat, les adresses IP distantes 10.250.250.2/32, 10.250.250.3/32 et 10.250.250.4/32 ont été résolues avec succès par le HUB via le Tunnel 0, tandis que les adresses IP distantes 10.240.240.2/32, 10.240.240.3/32 et 10.240.240.4/32 ont été résolues via le Tunnel 1.

4.2.2.2 Exécution de commande au niveau de SPOKE1

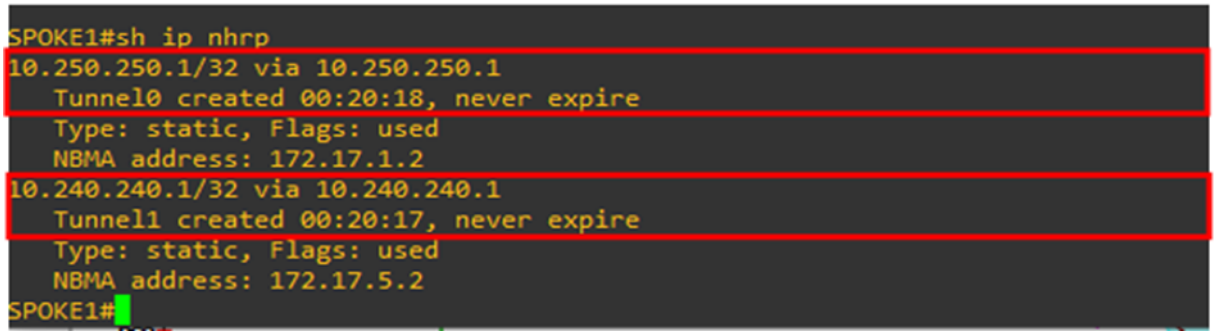


FIGURE 4.4 – Affichage des routes via le protocole NHRP (spoke1).

Interprétation des résultats de la figure 4.4 Ces résultats montrent les entrées NHRP (Next Hop Resolution Protocol) actuelles pour le spoke1.

— **La première entrée** indique que pour atteindre l'adresse IP de destination 10.250.250.1 (l'adresse IP utilisée pour atteindre le hub depuis les Spokes via le réseau DMVPN.)

Le tunnel 0 doit être utilisé avec l'adresse NBMA de HUB 172.17.1.2 Cette entrée est statique.

— **La deuxième entrée** indique que pour atteindre l'adresse IP de destination 10.240.240.1, le tunnel 1 doit être utilisé avec l'adresse NBMA 172.17.5.2. Cette entrée est également statique.

4.2.3 Analyse le chemin des paquets à l'aide de la commande (Traceroute)

4.2.3.1 Exécution de commande au niveau de SPOKE 2

Vers l'adresse local de HUB

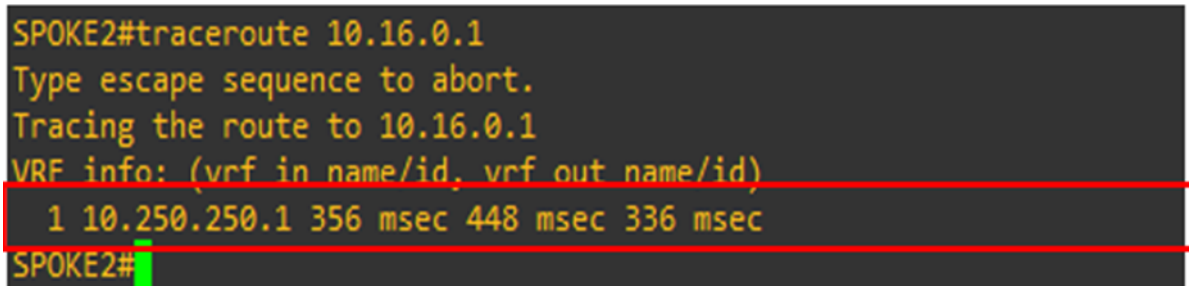


FIGURE 4.5 – Résultats du traceroute de DMVPN.

Interprétation des résultats de la figure 4.5

— La commande "**traceroute**" a été exécutée sur le périphérique SPOKE2 avec l'adresse de destination 10.16.0.1.

— Le trafic parvient à atteindre le hub en utilisant le tunnel DMVPN. La connexion au hub se fait via l'adresse IP 10.250.250.1.

Scénario de test pour le routage du trafic spoke to spoke :

Acheminement de trafic vers l'adresse locale de Spoke 1 en utilisant la phase 1 de DMVPN :

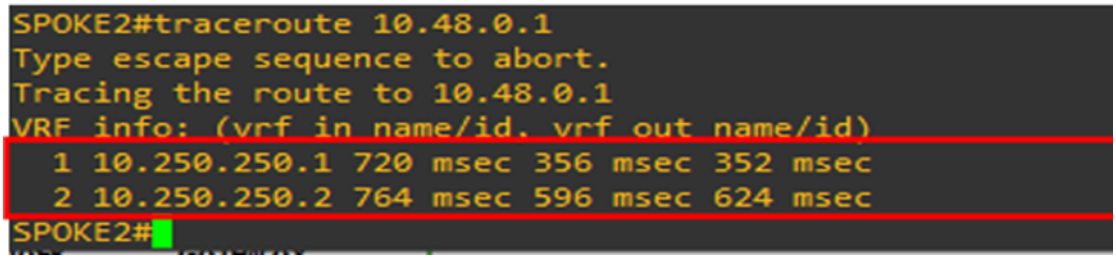


FIGURE 4.6 – Résultat de la commande TraceRoute (Phase 1).

Interprétation des résultats de la figure 4.6

— La commande "**traceroute**" a été exécutée sur le périphérique SPOKE2 avec l'adresse de destination 10.48.0.1.

— La sortie de la commande indique que les paquets sont d'abord acheminés vers l'adresse IP 10.250.250.1, qui correspond à l'adresse IP du HUB, puis vers l'adresse IP 10.250.250.2, qui correspond à l'adresse IP du SPOKE1.

— Pendant la phase 1, il est nécessaire que les paquets envoyés du site 1 au site 2 transitent par le concentrateur(HUB), car les sites ne sont pas capables d'utiliser le protocole MGRE. Afin que le routeur concentrateur (HUB)puisse enregistrer les adresses NBMA des différents routeurs des sites, ainsi que faire la correspondance entre les adresses IP publiques et les adresses IP de tunnel, on utilise le protocole GRE point à point traditionnel et le mode serveur-client NHRP.

Acheminement de trafic vers l'adresse locale de Spoke 1 en utilisant la phase 2 de DMVPN :

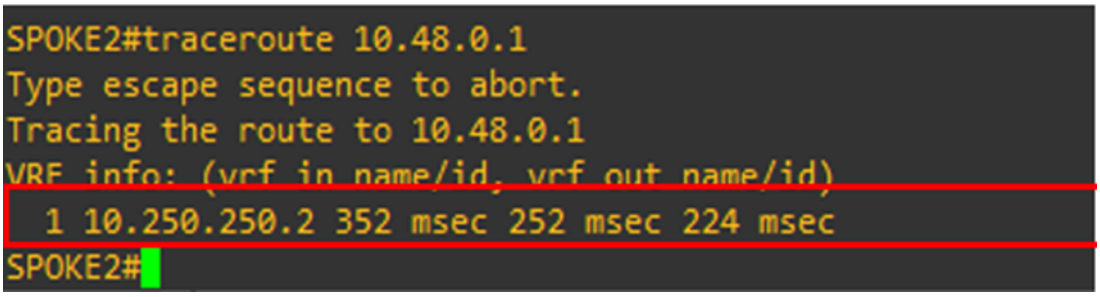


FIGURE 4.7 – Résultat de la commande TraceRoute (Phase 2).

Interprétation des résultats de la figure 4.7

— La commande "**traceroute**" a été exécutée sur le périphérique SPOKE2 avec l'adresse de destination 10.48.0.1. La sortie indique que les paquets sont acheminés directement vers l'adresse IP 10.250.250.2, qui correspond à l'adresse IP du SPOKE1. Cela suggère que la phase 2 de DMVPN est utilisée pour acheminer le trafic directement entre les deux sites sans passer par le concentrateur (HUB).

— La phase 2 de DMVPN diffère de la phase 1 en ce sens qu'elle utilise le protocole mGRE dans chaque nœud pour permettre la création de tunnels directs entre les sites.

4.3 Résultats des tests effectués sur la technologie SD-WAN

4.3.1 Résultats des performances SLA après génération du trafic

Il existe 3 types de performances SLA :

4.3.1.1 Packet Loss :

Lors de la configuration des performances SLA, nous avons fixé un seuil de perte de paquets à 10%, ce qui signifie que le trafic sera dirigé vers l'interface X uniquement si la perte de paquets est inférieure à 10%. Dans le cas contraire, le trafic ne passera pas par cette interface.

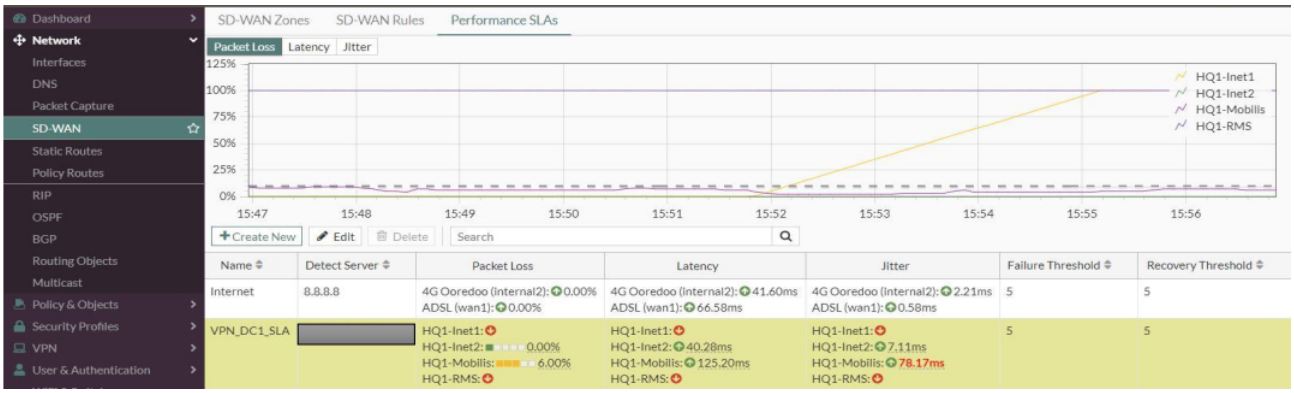


FIGURE 4.8 – Affichage SLA Performances SD-WAN Packet Loss.

4.3.1.2 Latency :

La deuxième métrique de performance configurée. Un délai de transmission de 200 ms a été défini. Si la liaison dépasse ce délai, le trafic ne sera probablement pas acheminé via cette liaison.

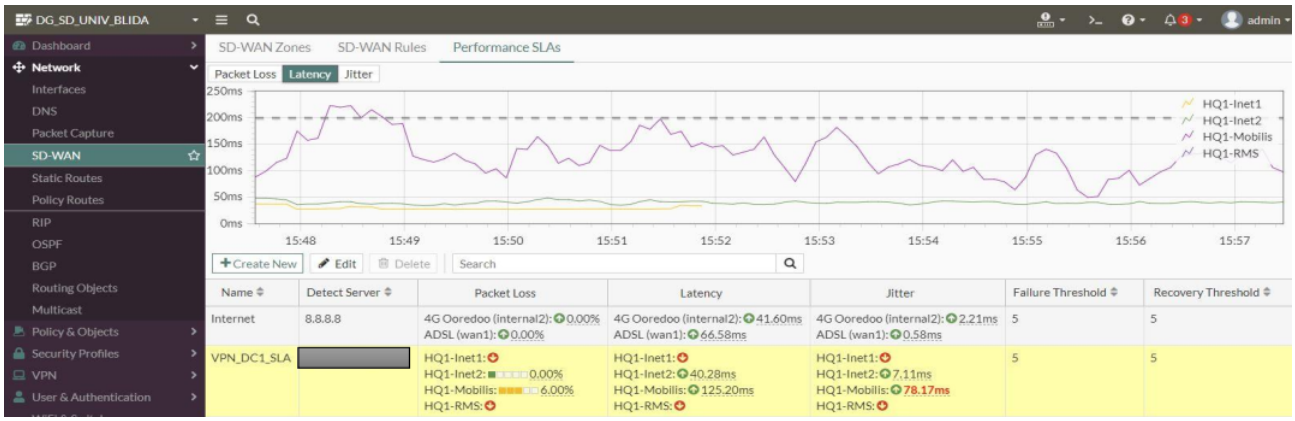


FIGURE 4.9 – Affichage SLA Performances SD-WAN Latency.

4.3.1.3 Jitter :

Le dernier paramètre configuré. Il représente la variation de la latence au fil du temps. Nous l'avons fixé à 30 ms. Si la liaison présente un jitter supérieur à 50 ms, le trafic ne sera pas acheminé par cette liaison. Dans le cas contraire, le trafic sera acheminé normalement.

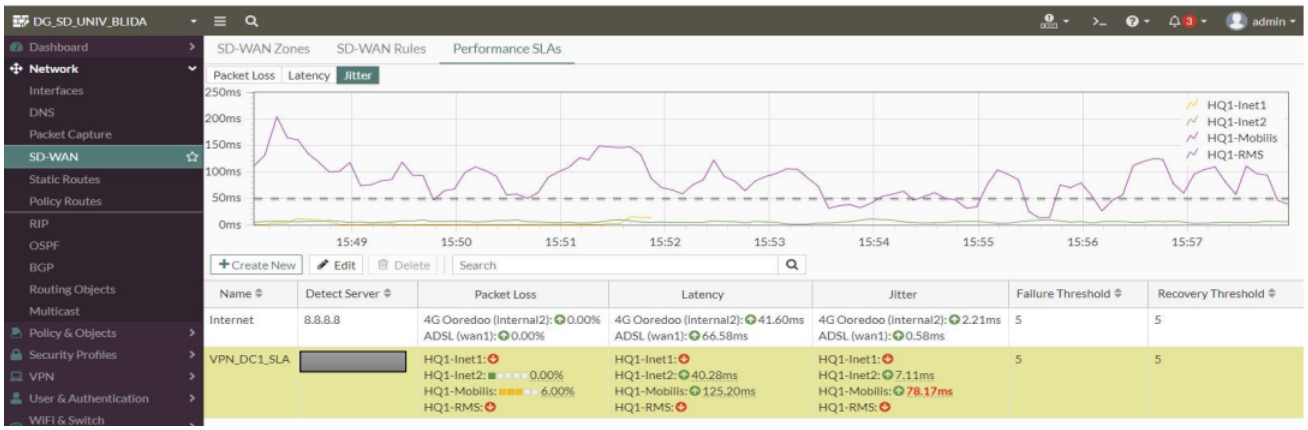


FIGURE 4.10 – Affichage SLA Performances SD-WAN Jitter.

4.3.2 Génération de trafic réseau :

Nous avons réalisé des tests de trafic et évalué les Rules SD-WAN, ainsi que les performances SLA en accédant à plusieurs sites web via un navigateur de recherche.

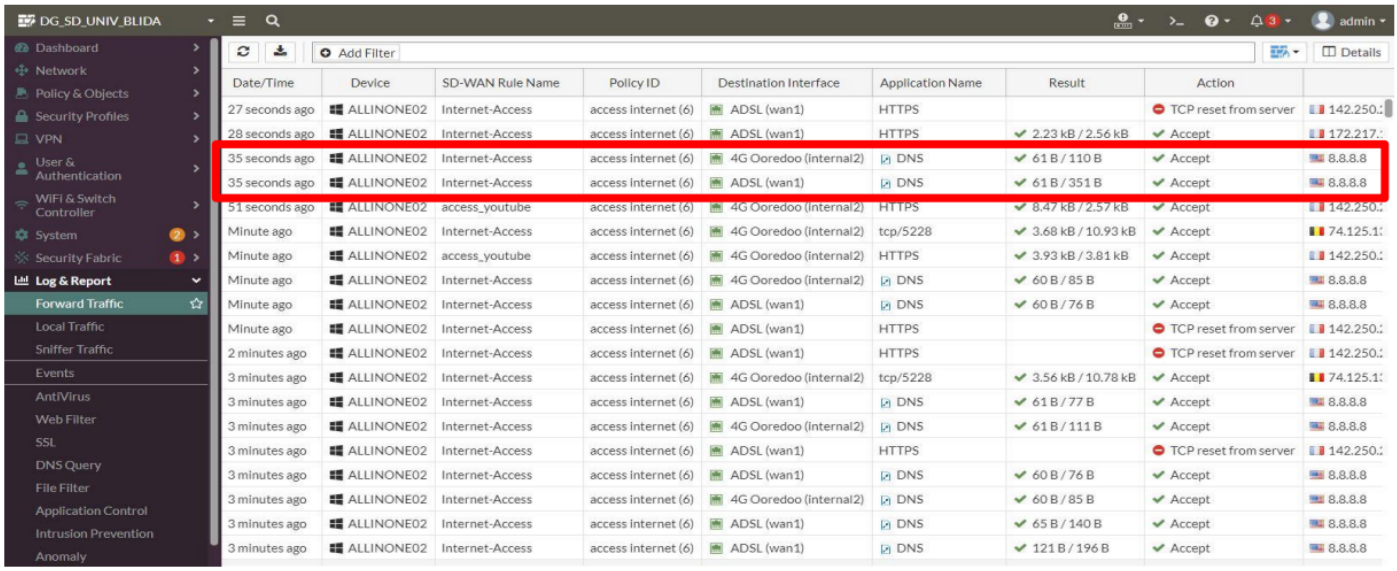


FIGURE 4.11 – Affichage du trafic réseau.

Interprétation des résultats de la figure 4.11

— Dans l'interface de gestion du trafic (forward traffic) que nous avons observée, nous avons constaté que les sessions étaient réparties entre les différents tunnels qui sont membres de la zone SD-WAN. Par exemple, lorsque la destination est 8.8.8.8, nous avons remarqué que le trafic était réparti entre deux tunnels, à savoir le tunnel ADSL et le tunnel Ooredoo.

— Cette répartition du trafic est effectuée en utilisant les règles SD-WAN préalablement créées, telles que l'accès Internet.

4.4 Évaluation comparative des performances de DMVPN et SD-WAN en se basant sur les résultats obtenus

Dans cette section, nous allons effectuer une comparaison entre deux technologies. Nous allons analyser différents aspects, tels que le taux de perte de paquets, en effectuant des mesures sur les équipements Cisco pour le DMVPN et Fortinet pour le SD-WAN.

4.4.1 Scénario de test pour la redondance et le basculement

4.4.1.1 DMVPN

Nous utilisons une commande de Ping continue pour établir un test de connectivité vers un site distant, via l'ADSL en envoyant des paquets de manière constante pendant une période définie. Ensuite, nous procédons à la désactivation de l'interface.

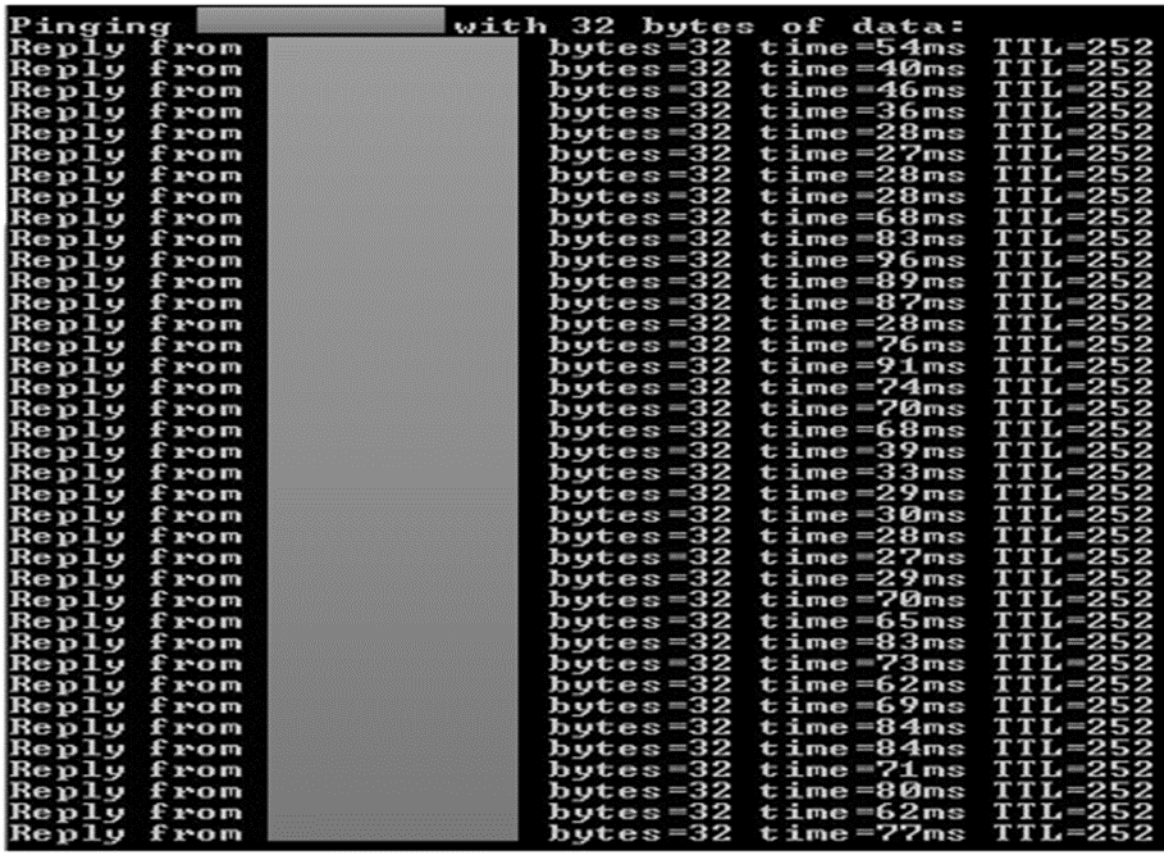


FIGURE 4.12 – Envoi de paquets en continu vers un site distant au niveau de DMVPN.

Nous avons désactivé le tunnel 0 attribué à l'ADSL en utilisant la commande :

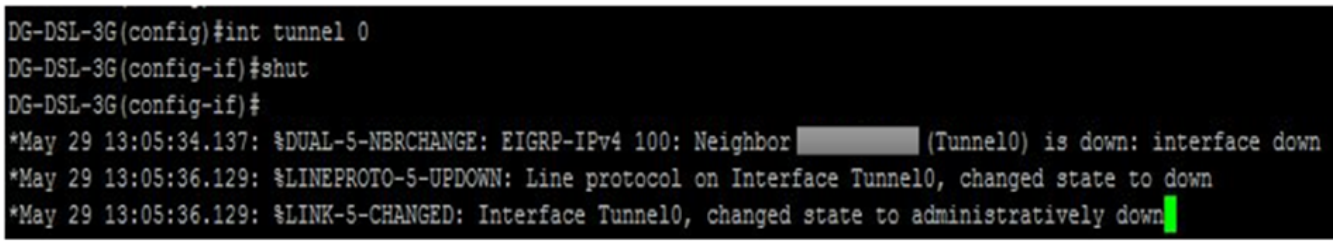


FIGURE 4.13 – Shutdown le tunnel ADSL.

Comme nous avons initié un Ping continu, nous poursuivons notre observation :

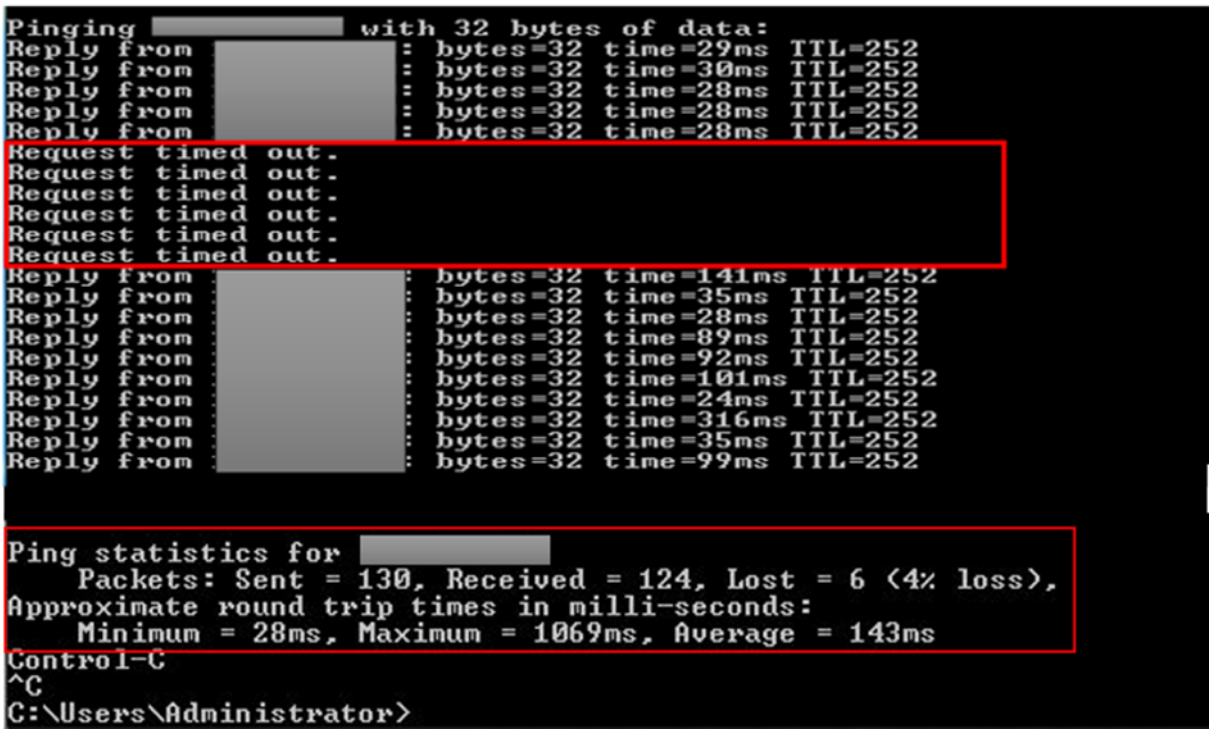


FIGURE 4.14 – Comportement du Ping continu au niveau de DMVPN.

Nous observons que la connectivité est rétablie après un court laps de temps, car les paquets continuent à être envoyés normalement. Lorsqu'il y a une panne sur le tunnel ADSL, la commutation vers le tunnel 4G (tunnel1) se produit. Cependant, ce processus de basculement prend un certain temps, ce qui entraîne une perte de paquets pendant cette transition.

4.4.1.2 SD-WAN

Dans cette partie, nous avons effectué des tests de ping continu afin d'évaluer les pertes de paquets dans la technologie SD-WAN mise en place. Nous avons suivi les mêmes étapes que précédemment, en envoyant des paquets de ping de manière continue et en surveillant les réponses. L'objectif était de vérifier s'il y avait des pertes de paquets lors du basculement entre les tunnels en cas de panne d'un des tunnels participant à la zone SD-WAN. Cette étape est essentielle pour évaluer la qualité et la stabilité de la connectivité dans le réseau SD-WAN.
Nous utilisons une commande de Ping continue pour établir un test de connectivité vers un site distant.

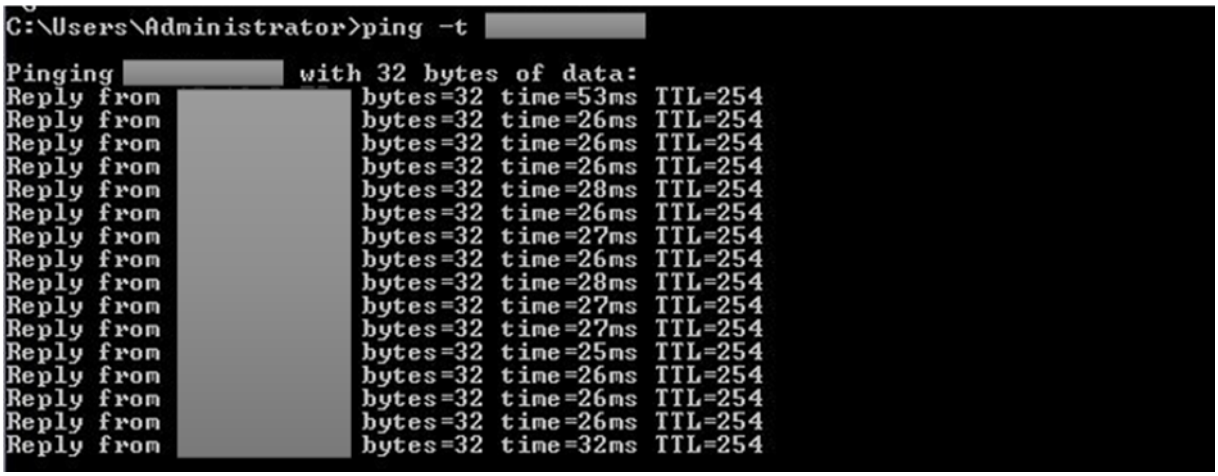


FIGURE 4.15 – Envoi un Ping continue vers un site distant au niveau de SD-WAN.

Nous avons désactivé le tunnel HQ2_Inet1 :

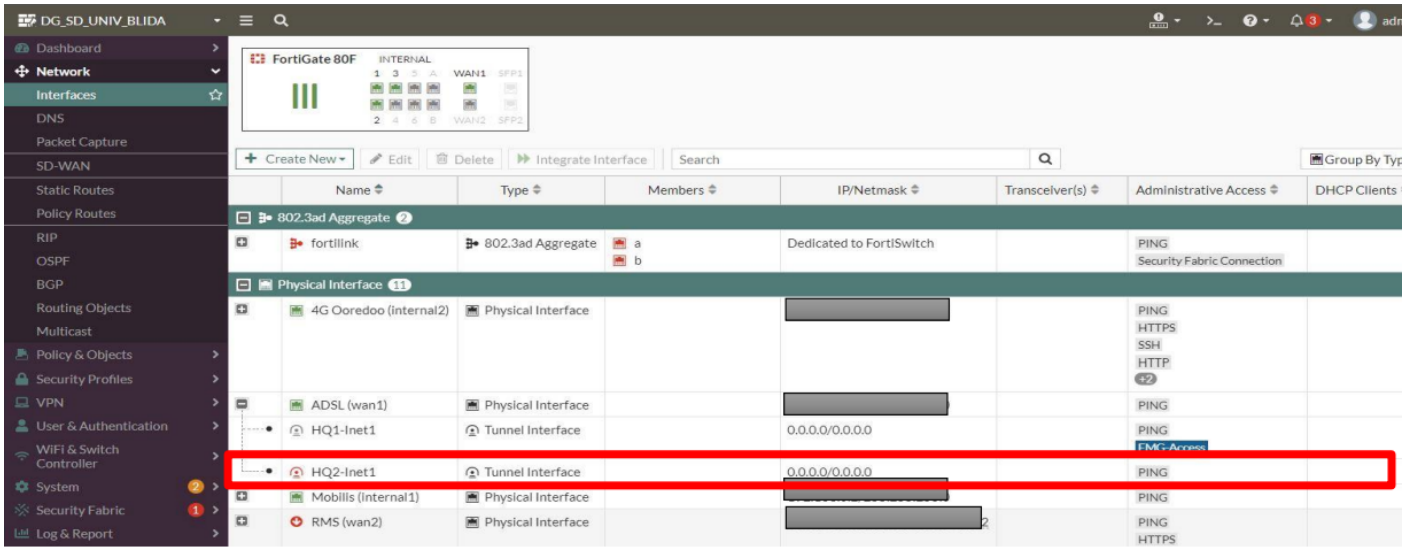


FIGURE 4.16 – Shutdown le tunnel HQ2-Inet1.

Nous poursuivons notre observation :

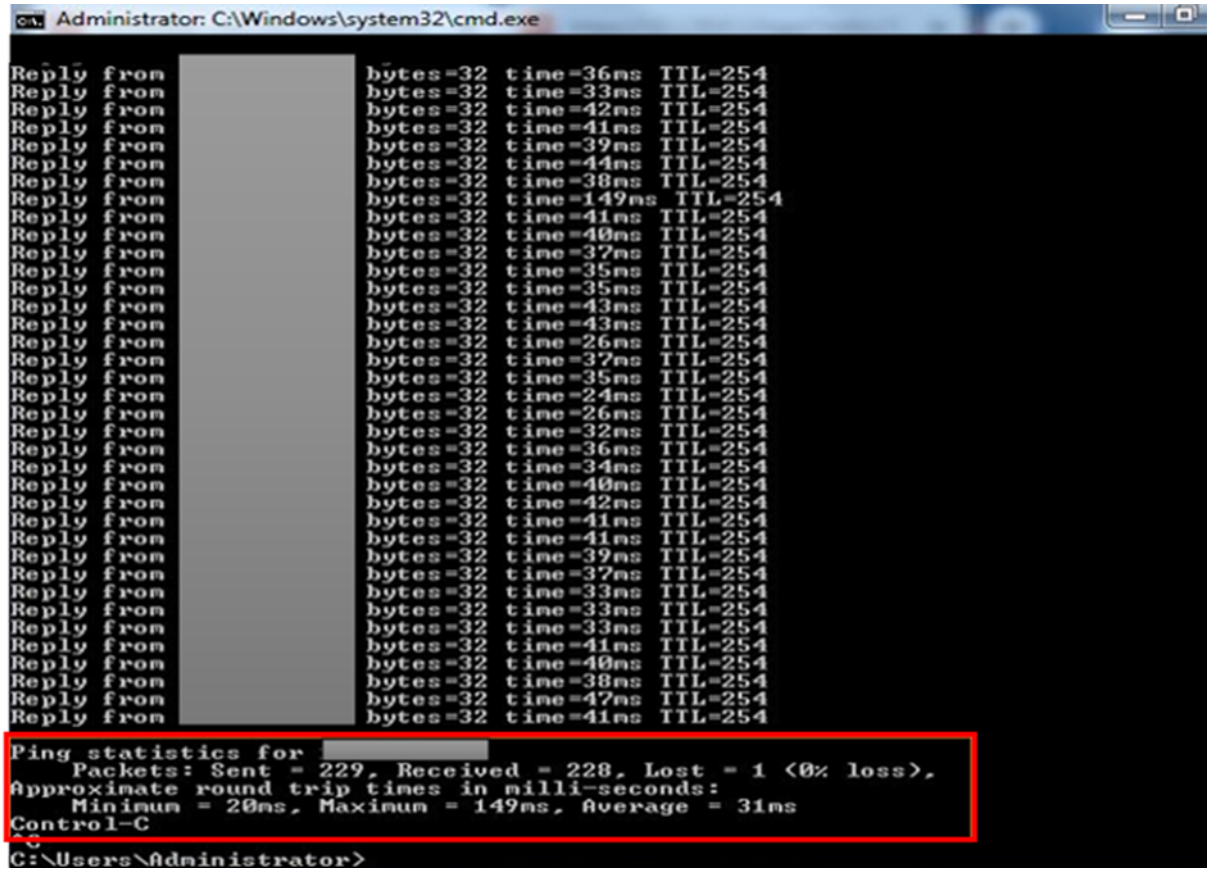


FIGURE 4.17 – Comportement du ping continu au niveau de SD-WAN.

Nous constatons que la connectivité reste intacte, sans aucune perte, même en cas de panne d'un des tunnels participant à la zone SD-WAN.

4.4.2 Analyse comparative des résultats obtenus :

— La solution SD-WAN de Fortinet offre une meilleure visibilité de l'ensemble du réseau. Grâce à ses fonctionnalités avancées de gestion et de surveillance, il est plus facile d'observer et de comprendre l'état du réseau dans son ensemble.
— Les règles SD-WAN jouent un rôle essentiel en permettant d'avoir un contrôle précis sur la sélection des chemins. En définissant des règles basées sur des critères spécifiques tels que la performance, la disponibilité ou la priorité.
— En ce qui concerne les pannes des tunnels, nous avons constaté que le basculement entre les liaisons se fait de manière rapide, fluide et transparente dans la solution SD-WAN. Lorsqu'un tunnel rencontre un problème, le trafic est automatiquement redirigé vers une autre liaison fonctionnelle, assurant ainsi une continuité de service sans interruption . Cela contraste avec l'architecture DMVPN où les basculements peuvent être plus lents et moins transparents.

En résumé, la solution SD-WAN de Fortinet offre une meilleure visibilité, un contrôle précis sur les chemins et une résilience améliorée en cas de pannes, ce qui en fait une option a pour optimiser les performances et la fiabilité du réseau.

4.5 Conclusion

Dans ce chapitre , nous avons réalisé une analyse approfondie des différences fondamentales entre le DMVPN et le SD-WAN. Nous avons identifié une amélioration notable dans le déploiement du DMVPN, qui permet une communication directe entre les sites distants sans passer par le hub central. Cette amélioration représente une avancée significative par rapport aux fonctionnalités précédentes du DMVPN. Nous avons également constaté que la configuration des tunnels est plus complexe dans le cas du DMVPN, tandis que le SD-WAN se distingue par sa gestion et sa configuration, rendues possibles grâce à une interface utilisateur conviviale. En outre, nous avons souligné l'intelligence intégrée au SD-WAN, qui fait défaut dans le DMVPN. Ces distinctions revêtent une importance cruciale pour une compréhension approfondie des avantages et des limitations de chaque technologie dans le contexte des réseaux d'entreprise.

Conclusion générale

L'adoption du protocole DMVPN pour les connexions aux sites distants des entreprises offre des avantages significatifs en termes de sécurité et de connectivité Internet. Cependant, les limites inhérentes à cette technologie doivent être prises en compte, en particulier le manque de capacités d'équilibrage de charge. Par conséquent, une évaluation minutieuse des besoins et des exigences de l'entreprise est essentielle avant de sélectionner la solution appropriée pour garantir une connectivité optimale et des performances réseau efficaces.

Le SD-WAN est une technologie récente qui propose des solutions efficaces pour relever les défis de flexibilité, d'agilité et de déploiement dans les réseaux. Cette technologie offre de nombreux avantages, tels que la réduction des coûts et l'amélioration de la résilience grâce à l'utilisation de plusieurs connexions de communication.

Le déploiement du SD-WAN présente plusieurs avantages par rapport au DMVPN traditionnel. le SD-WAN combine intelligemment les différentes connexions FAI pour améliorer les performances globales du réseau sur chaque site, contrairement au DMVPN qui a des performances limitées. La configuration centralisée des sites dans le SD-WAN élimine la nécessité de changer manuellement d'équipement, ce qui n'est pas le cas avec le DMVPN. Les administrateurs bénéficient également d'une vue complète de l'ensemble du réseau.

Nos travaux ont donné les résultats suivants :

- Le SD-WAN permet le rééquilibrage dynamique de la charge entre les passerelles.
- En cas de panne du tunnel, le basculement entre les liens dans le SD-WAN est rapide et sans perte de paquets, contrairement au DMVPN où l'on observe une perte de paquets pendant la transition vers un autre tunnel. Ce résultat démontre l'efficacité du SD-WAN en termes de continuité de service et de stabilité du réseau.
- La solution SD-WAN de Fortinet offre une large visibilité sur l'ensemble du réseau.
- L'interface Logs and Reports intégrée à FortiGate permet de suivre et de tracer le trafic.

Ces résultats mettent en évidence les avantages significatifs des solutions SD-WAN par rapport au DMVPN en termes de performances, de résilience et de visibilité du réseau.

DMVPN était autrefois largement utilisé comme solution réseau privilégiée. Cependant, avec l'évolution continue des réseaux, de nouveaux défis sont apparus.

Chaque défi comporte une solution, et actuellement, le SD-WAN s'impose comme la solution la plus efficace et fiable, comme en témoigne notre déploiement réussi de cette technologie sur deux sites au sein de NAFTAL.

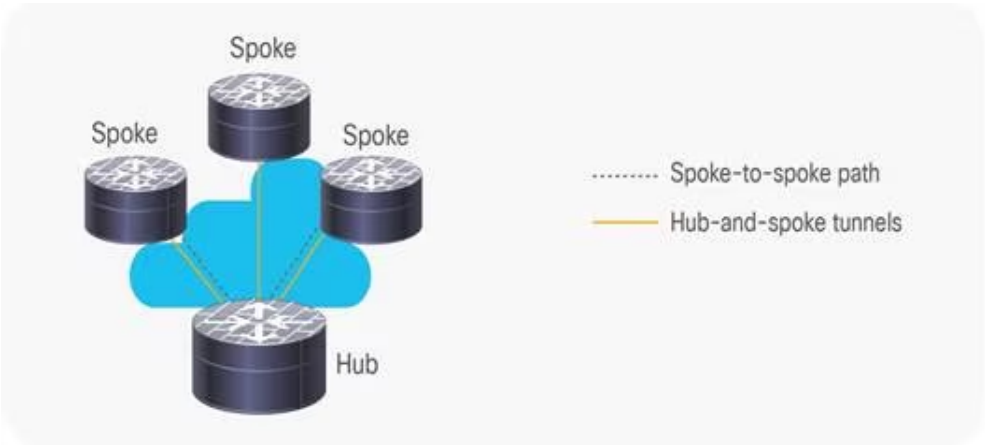
Annexe

Modèle de déploiement

Le $DMVPN$ propose deux modèles de déploiement :

Le modèle HUB-and-spoke

Dans ce modèle, chaque spoke possède une interface GRE permettant de monter un tunnel vers le HUB [8]. Après avoir établi un tunnel entre le HUB et tous les Spokes, les informations de routage sont échangées à travers ce tunnel. Pour que les Spokes (clients) puissent se connecter, ils doivent d'abord s'enregistrer avec le HUB (serveur) en indiquant manuellement l'adresse du HUB dans le Tunnel GRE (tunnel destination) via une demande d'enregistrement $NHRP$. Le HUB apprend ensuite dynamiquement les adresses VPN (Privées) et les adresses $NBMA$ (Publiques) de chaque Spoke, ce qui permet à tout le trafic entre eux de passer par le HUB. Cependant, ce modèle ne prend pas en compte les connexions directes entre les Spokes.



Cisco $DMVPN$ HUB-and-Spoke Deployment Model [10].

Le modèle Spoke-to-Spoke

Dans ce modèle, chaque spoke doit disposer d'une interface $mGRE$ permettant aux tunnels dynamiques de transiter vers les autres spokes. Ce modèle prend en compte les liaisons entre différents spokes et offre une grande évolutivité de configuration pour les périphériques [11].
Dans ce modèle, la configuration du HUB est simplifiée, car il n'a pas besoin de créer une table de registre NHRP pour chaque nouveau Spoke. Les tunnels Spoke-to-Spoke ne sont pas utilisés dans cette phase. Les Spokes sont configurés pour utiliser GRE point à point vers le HUB et enregistrent leurs adresses IP logiques (Tunnel) avec l'adresse $NBMA$ sur le NHS (HUB), ce qui permet au HUB de les joindre dynamiquement. Le protocole de routage envoie un minimum d'informations depuis le HUB vers les Spokes (route par défaut) et les Spokes annoncent leurs réseaux directement connectés au HUB.

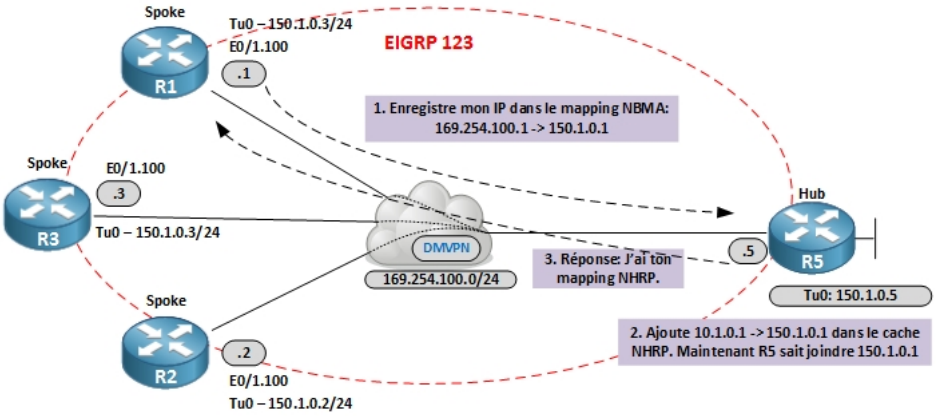
Cisco $DMVPN$ Spoke-to-Spoke Deployment Model [10].

Les différentes phases du $DMVPN$

Phase1 (HUB & Spoke (un HUB $mGRE$, et les Spokes en P2P GRE)

Le déploiement de tunnels HUB-and-spoke est utilisé, où les connexions interbranches sont construites uniquement à travers le HUB central $DMVPN$ et les spokes individuels, ce qui est similaire à un système VPN traditionnel. Cela implique la construction des tunnels pour permettre la communication entre les spokes et le HUB central $DMVPN$.

Fonctionnement : Les Spokes sont configurés point à point GRE vers le HUB et enregistrent leurs IP logiques (Tunnel0 avec l'adresse $NBMA$) sur le NHS (HUB) afin de les joindre dynamiquement. Le protocole de routage envoi un minimum d'informations depuis le HUB vers les Spokes (Route par défaut). Les Spokes annoncent leurs réseaux (directement connectés) au HUB [17].



fonctionnement de phase 1 $DMVPN$ [17].

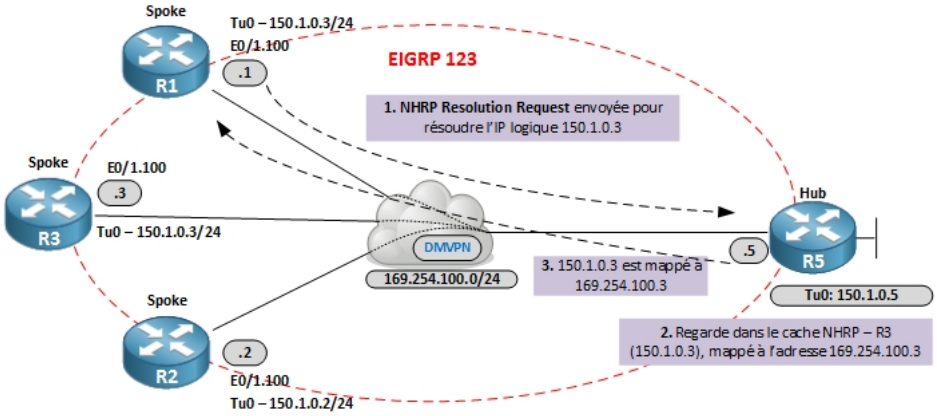
Comme le trafic doit toujours passer par le HUB, celui-ci n'a besoin d'envoyer qu'une seule route par défaut aux Spokes.

Phase 2 (HUB & Spoke avec des tunnels Spoke-to-spoke)

Elle utilise un déploiement de tunnel de type "spoke-to-spoke" qui permet une communication directe entre les Spokes, sans nécessiter un HUB central, à condition que des routes spécifiques soient en place pour les sous-réseaux des spokes. La phase 2 a amélioré la phase 1 en permettant l'établissement direct de tunnels "Spoke-to-Spoke". Ces tunnels sont établis à la demande, en fonction du trafic du Spoke qui déclenche le tunnel. Le HUB n'est utilisé que pour le plan de contrôle.

De cette façon, une route par défaut peut être envoyée du HUB aux spokes pour acheminer le trafic vers les réseaux

Fonctionnement : Lorsqu'un Spoke doit envoyer un paquet via un Next-Hop sur le cloud $mGRE$, il envoie une demande de résolution $NHRP$ au HUB. Le HUB répond avec une réponse de résolution $NHRP$ depuis son cache, permettant ainsi au Spoke de connaître l'adresse $NBMA$ d'un autre Spoke et de le contacter directement [17].



fonctionnement de phase 2 $DMVPN$ [17].

Comme le trafic doit toujours passer par le HUB, celui-ci n'a besoin d'envoyer qu'une seule route par défaut aux Spokes.

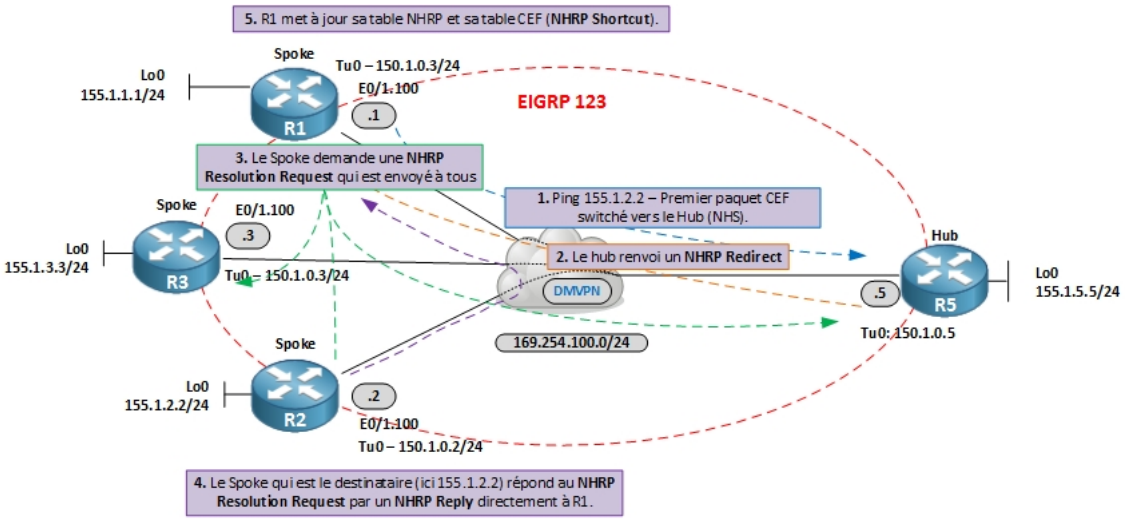
Phase 3 (Amélioration des capacités de communication entre les Spokes)

Le déploiement des tunnels se fait selon le modèle "HUB-and-spoke", où les connexions entre les spokes sont établies uniquement via le HUB $DMVPN$ central et les points d'accès individuels. Les tunnels "Spoke-to-Spoke" sont créés dynamiquement, sans routes spécifiques préétablies. Les messages $NHRP$ du HUB sont utilisés pour sécuriser ces routes, ce qui signifie que le HUB ne gère que le plan de contrôle et que le trafic de données "Spoke-to-Spoke" peut parfois passer par le HUB, mais généralement, il ne passe pas par celui-ci.

Fonctionnement : La phase 3 utilise des tunnels $mGRE$ sur les Spokes et le HUB avec une redirection $NHRP$ pour permettre aux conversations Spoke-to-Spoke de se joindre directement sans passer par le HUB. Cela améliore l'efficacité et l'évolutivité du réseau. Voici comment ça fonctionne :

- Etape 1 :Les Spokes enregistrent leurs mappings Tunnel/$NBMA$ avec le/s HUB, cela permet au HUB de découvrir dynamiquement les spokes et d'établir les voisins [17].
- Etape 2 :Un Tunnel $mGRE$ est configuré pour les NHRP Redirects (commande importante pour la Phase 3). Fonctionnement similaire aux IP $ICMP$ redirect. Quand un routeur reçoit un paquet IP en entrée de son tunnel $mGRE$, et le renvoi sur la même interface, il envoi à la source un $NHRP$ Redirect [17].
- Etape 3 :Maintenant, le Spoke reçoit le $NHRP$ Redirect, ce dernier envoi donc une $NHRP$ Request vers la même IP de destination, qui n'est plus le NHS. La $NHRP$ Request voyage sur tous les Spokes jusqu'à ce qu'elle trouve la cible. C'est le fonctionnement normal du $NHRP$ Request Forwarding, hop by hop [17].
- Etape 4 :Maintenant le Spoke répond à la résolution. Basé sur l'IP source présente dans le playload du paquet, il trouve le Spoke correspondant dans sa table de routage. Il utilise l'IP $NBMA$ du routeur source et renvoi un $NHRP$ Reply directement (sans retraverser le HUB). La réponse arrive sur le Spoke source et il connait alors l'IP $NBMA$ de sa destination.

Maintenant, en plus de réécrire la table $NHRP$, le routeur réécrit l'entrée CEF. Voici un petit diagramme pour résumer l'ensemble de ces informations.



fonctionnement de phase 3 $DMVPN$ [17].

Références

[1] Getting started with gns3 | gns3 documentation. Consulté le Février 22, 2023, https ://docs.gns3.com/docs/.

[2] Introduction to wans. Consulté le Février 21, 2023, https ://www.pearsonhighered.com/assets/samplechapter/1/5/8/7/1587132052.pdf.

[3] la-securite-informatique/sd-wan-quelles-sont-les-avantages-de-cette-solution/. Consulté le 20 février 2023, https ://www.weodeo.com.

[4] Les principaux avantages de la technologie sd-wan - sdxcentral. Consulté le 15 février 2023, https ://www. sdxcentral.com/networking/sd-wan/definitions/sd-wan-technology/.

[5] Performance analysis of an sd-wan infrastructure implemented using cisco system technologies. Consulté le 20 février 2023, https ://www.diva-portal.org/smash/get/diva2 :1632279/FULLTEXT01.pdf.

[6] Présentation de bgp | juniper networks. Consulté le 25 février 2023, https ://www.juniper.net/documentation/fr/fr/software/junos/bgp/topics/topic-map/bgp-overview.html.

[7] Qu'est ce que le sd-wan ? définition et évolutions. Consulté le 20 février 2023, https ://www.servicepilot.com/fr/blog/qu-est-ce-que-le-sd-wans/.

[8] Dynamic multipoint virtual private network, 2013. Consulté le 25 février 2023, https ://docplayer.fr/8645436-Dynamic-multipoint-virtual-private-network-dmvpn.html.

[9] 1.20 next hop resolution protocol. stuck-in-active : Journal of an it-network administrator. 04 mars 2019. Consulté le 24 février 2023, https ://stucknactive.com/2019/03/04/1-20-next-hop-resolution-protocol.

[10] Cisco dynamic multipoint vpn : Simple and secure branch-to-branch communications data sheet., 15 janvier 2019. Consulté 09 avril 9 2023, https ://www.cisco.com/c/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/data_sheet_c78-468520.html.

[11] Dynamiques vpn ipsec multipoint (utilisation de gre multipoint/nhrp pour étendre les vpn ipsec). 28 mars 2022. Consulté le 11 avril 2023, https ://www.cisco.com/c/fr_ca/support/docs/security-vpn/ipsec-negotiation-ike-protocols/41940-dmvpn.html.

[12] Wan connection types – explanation and examples. study ccna., 29 decembre 2022. Consulté le Février 21, 2023, https ://study-ccna.com/wan-connection-types/.

[13] E. B Al-Somaidai, M. B. Yahya. Survey of software components to emulate openflow protocol as an sdn implementation. american journal of software engineering and applications. pages 74–82, 2014.

[14] El KAMOUN Bahnasse, A. Évaluation des performances des applications web et voip dans un vpn dynamique et multipoint protégé moment,(computing conference 2017). 18 juillet 2017.

[15] EL KAMOUN N. Bahnasse, A. Etude et analyse de l'évolutivité d'un protocole de routage dynamique sur un réseau privé virtuel multipoint dynamique. septembre 2015.

[16] ELKAMOUN N BAHNASSE, A. Study and evaluation of the high availability of a dynamic multipoint virtual private network,. *Revue Méditerranéenne des Télécommunications Journal*, 2015.

[17] Benoit. Dmvpn phases 1,2 et 3 | networklife . réseauvie | un autre paquet dans le réseau. 16 octobre 2014. Consulté le 25 mars 2023, https ://www.networklife.net/2014/10/dmvpn-phase-12-et-3/.

[18] M. Conran. Dmvpn technologies, guide de conception. fevrier 2015.

[19] Singh N. Lerner A. Zeng E Forest, J. Magic quadrant for wan edge infrastructure. *Gartner*, 2021.

[20] A Guipelbé. Architectures des réseaux wan. dirtech it., 17 mars 2022. Consulté le Février 21, 2023, https ://www.dir-tech.com/architectures-des-reseaux-wan/.

[21] Jankunaite I Jankuniene, R. Route creation influence on dmvpn qos. *Proceedings of the ITI 2009 31st International Conference on Information Technology Interfaces*, 2009.

[22] L Josse. Réseau sd-wan : définition et avantages pour les entreprises. a2com foliateam, 23 septembre 2020. Consulté le 20 février 2023, https ://www.a2com.fr/blog/reseau-sd-wan-definition-et-avantages-pour-les-entreprises/.

[23] J.Åkerblom. Evaluation of selected sd-wan products, 2016. Consulté le 20 février 2023, http ://www.divaportal.org/smash/get/diva2 :935163/FULLTEXT01.pdf.

[24] Z Kerravala. Pourquoi les entreprises doivent repenser leurs stratégies réseau pour l'ère du digital. *ZK Research*, 2017.

[25] Nassira Khelf, Roumaissa Ghoualmi-Zine. A survey on dynamic multipoint virtual private networks. 2019.

[26] Widya-K. H. P. Fiade A. Julia I. R Masruroh, S. U. Performance evaluation dmvpn using routing protocol rip, ospf, and eigrp. *2018 6th International Conference on Cyber and IT Service Management (CITSM)*, 2018.

[27] H. S. Christoph Meinel. Internetworking technological foundations and applications. *springer ed. Springer International Publishing.*

[28] V. M Posts. An introduction to dmvpn. the art of network engineering., 04 aout 2020. Consulté le April 11, 2023, https ://artofnetworkengineering.com/2020/08/21/an-introduction-to-dmvpn/.