REPUBLIQUE DU SENEGAL

Un Peuple-Un But-Une Foi

MINISTERE DE L'ENSEIGNEMENT SUPERIEURE DE LA RECHERCHE ET

DE L'INNOVATION

UNIVERSITE GASTON BERGER DE SAINT-LOUIS

U.F.R DES SCIENCES APPLIQUEES ET DE TECHNOLOGIE

DEPARTEMENT DE PHYSIQUE APPLIQUEES

Mémoire de fin d'étude pour l'obtention du diplôme de

MASTER INGENIEURIE EN ELECTRONIQUE ET TELECOMMUNICATION (MIETEL)

THEME :

Déploiement d'une solution Fortinet Secure SD-WAN pour améliorer la performance et la sécurité – Étude de cas PAMECAS

Soutenance le	devant le jury composé de :	
Professeur		Président du jury
Professeur		Examinateur
Professeur Cherif DIALLO		Encadrant

Année universitaire 2023/2024

REMERCIEMENTS

Au nom d'**ALLAH**, le tout miséricordieux, le très miséricordieux.

Toutes les louanges sont à Lui (**ALLAH**), Seigneur de l'univers.

Je tiens à exprimer ma profonde gratitude au **Tout-Puissant**, source de toute sagesse et de tout savoir. Sans Sa grâce et Ses bénédictions, ce travail de recherche et cette étape cruciale de ma vie n'auraient pu être menés à bien. Je le remercie pour la force, la patience et la persévérance qu'Il m'a accordées tout au long de ce parcours.

J'adresse mes remerciements à :

- L'ensemble du corps professoral de l'UGB, en l'occurrence **Mr Papa Alioune FALL, Mr Moustapha SENE, Mr Abdou Karim MBODJ, Amadou Seidou MAIGA**, pour leur dévouement et leur enseignement précieux qui ont contribué à mon développement académique et professionnel.

- Mon encadreur, **Dr. Cherif DIALLO**, Enseignant chercheur à l'UGB. Je vous suis infiniment reconnaissant pour votre guidance précieuse, votre disponibilité, vos conseils avisés et votre soutien constant tout au long de l'élaboration de ce mémoire. Votre expertise et votre sens de l'écoute ont été d'une richesse inestimable et ont grandement contribué à l'aboutissement de ce travail.

- Mes maîtres de stage, **Cheikh Djily Mbacké NDIAYE, Saer SOW, Pape Thierno DIALLO, Moustapha NDAO, Ibrahima DRAME** ainsi qu'à tout le personnel de **SONATEL** notamment à la cellule **BOAT**, **SUPERVISION**, **SDT**. Merci de m'avoir accueilli, fait confiance et offert un terrain d'apprentissage aussi enrichissant. Votre professionnalisme, vos enseignements et les ressources que vous m'avez accordées ont été fondamentaux pour la conduite de mon étude.

- L'ensemble des étudiants de MIETEL, en particulier mes amis de classe pour l'émulation, l'entraide et les moments de partage, aussi bien studieux que conviviaux. Cette aventure n'aurait pas été la même sans votre compagnie et votre solidarité.

- Mes grands et grandes, Cheikh Omar NDAW, Fatou Djiby DIOP, Youssou CISSOKHO, Abdoulaye CISSOKHO, MANTOU, Pape Moussa CISSOKHO,

Mariama DIOUF , Khady FALL, Coumba CISSOKHO, Maty CISSOKHO, Oumou KEITA, Khalifa NDIONE, Mamadou NDIONE, Bouna DIALLO, Mère Awa et Adama BANGOURA, Mère Astou DIALLO, Coumba DIALLO, Oumou SOW, Fatou KANE, Fatimata BALERA, Pape TOURE, Aladji TOURE, Mame Seydou NDAW, Dieyna, Dier Mme GUEYE pour leur soutien, leurs conseils et leur accompagnement tout au long de ce mémoire. Leur expérience et leurs encouragements ont été d'une aide précieuse.

- Mes amis, Rassoul DIALLO(mon jumeau), Issa SECK(Tons sama), Ousmane DIOP, Landing DIATTA, Mamadou DIARRA, Baidy NGOM, Aïda NDIAYE, Nguirane GNING, Pape Demba DIENG, Ahmad BATHILY, Abdoul Karim BATHILY, Makhoudia SENE, Elhadj Malick SOKHNA, Martin Vincent FAYE, Arouna MBAYE, Salif MANE, Michel BIES, Michel BINDIA, Robert BINDIA, Sidy BA, Mouhammad DIALLO(IPSL), Mouhammad MABROUQ, Alpha DIALLO, Ngone DIAW, Sofiatou SOW, Aliou KA, Abdourahmane TINE, Mohamed Lamine SARR, Mapathé NDAW, Mouhamad COULIBALY, Waly CISSOKHO, feu Mouhamed GUEYE, Aïcha MBENGUE, Louise MBAYE, Coumba KANTE, Kadiata THIAM, Hawa CAMARA, Moussa CAMARA, Halimatou CAMARA, Aïcha SECK, Fatou Kiné NIANG, Yacine DIOP, Bineta DIOUF, Ousseynou BA, Malick DRAME, Fakane SEYE, Gabriel DIOUF, Ibrahima BA, Samba DIOP, Sidy FAYE, Thioro, Aly NDAO, Fatou DIOP, Elizabeth Aïcha, Babacar NDAO, Mouhamed NDIAYE, Sawdatou, Ndeye MINGUE, Doudou BA, Fallou Nguirane, Khadija BADIANE, Adja KANE, Cheikhou GAYE, Bara MBODJ, Samba KEITA, ces piliers de toujours. Merci pour votre présence indéfectible, votre réconfort et pour avoir su me divertir et me soutenir même à distance.

- Toutes les personnes qui, de près ou de loin, ont contribué de manière directe ou indirecte à la réalisation de ce mémoire et à mon épanouissement académique et personnel. Votre aide, vos conseils ou simplement votre bienveillance ont eu une importance capitale.

DEDICACES

Avec l'expression de ma reconnaissance, je dédie ce modeste travail à :

- **Mes chers parents**, votre amour inconditionnel, vos sacrifices silencieux et votre foi inébranlable en moi ont été la lumière qui a guidé chacun de mes pas. Ce mémoire est le fruit de vos efforts et de votre constante inspiration. Je vous le dédie du fond du cœur, en témoignage de ma gratitude éternelle. Qu'ALLAH vous fasse miséricorde comme vous m'avez élevé tout petit.

- **Mes frères et sœurs**, merci pour votre soutien indéfectible, votre patience à toute épreuve et ces moments de complicité qui ont rendu ce parcours plus léger. Vous avez été mes premiers compagnons d'aventure et mes plus grands motivateurs. Cette réussite est aussi la vôtre.

- **Ma famille**, celle qui a veillé de près, par la présence et le réconfort, et celle qui a soutenu de loin, par la pensée et l'affection, chacun de vous a marqué ce chemin de sa lumière, ce mémoire est le vôtre autant que le mien, avec tout mon amour et ma gratitude.

- **Mes soutiens**, par un simple mot, une attention, une aide précieuse ou une présence discrète, vous avez contribué à ce que ce projet voie le jour. Je pense à vous et vous dédie une part de ce succès.

RESUME

Dans un contexte marqué par la transformation numérique des entreprises, l'essor des applications cloud et l'augmentation des exigences en matière de performance et de sécurité, les architectures WAN traditionnelles montrent leurs limites. Ce mémoire porte sur l'étude et le déploiement d'une solution Fortinet Secure SD-WAN visant à améliorer la performance, la résilience et la sécurité des réseaux d'entreprise. À travers une étude de cas menée au sein de PAMECAS, en partenariat avec SONATEL, une analyse de l'architecture réseau existante a permis d'identifier plusieurs contraintes liées aux coûts, à la flexibilité et à la gestion opérationnelle. Sur la base d'une étude comparative des solutions SD-WAN disponibles, la solution Fortinet Secure SD-WAN a été retenue en raison de son intégration native des fonctions de sécurité et de connectivité. Une nouvelle architecture cible a été conçue puis mise en œuvre, intégrant le routage applicatif intelligent, la haute disponibilité, la gestion centralisée et des mécanismes de sécurité avancés. Les résultats obtenus mettent en évidence une amélioration significative de la qualité de service, une meilleure disponibilité des applications et un renforcement global de la posture de sécurité, tout en simplifiant l'exploitation du réseau et en optimisant les coûts.

Mots clés : SD-WAN, Secure SD-WAN, Fortinet, MPLS, Sécurité réseau, Performance réseau, Réseaux d'entreprise

ABSTRACT

In a context characterized by digital transformation, the rapid adoption of cloud applications, and increasing requirements in terms of performance and security, traditional WAN architectures reveal several limitations. This thesis focuses on the study and deployment of a Fortinet Secure SD-WAN solution aimed at improving network performance, resilience, and security in enterprise environments. Through a case study conducted at PAMECAS, in partnership with SONATEL, an analysis of the existing network infrastructure highlighted constraints related to cost, flexibility, and operational management. Based on a comparative study of available SD-WAN solutions, Fortinet Secure SD-WAN was selected due to its native integration of networking and security features. A new target architecture was designed and implemented, incorporating application-aware routing, high availability, centralized management, and advanced security mechanisms. The results demonstrate a significant improvement in service quality, enhanced application availability, and a stronger overall security posture, while simplifying network operations and optimizing operational costs.

Keywords: SD-WAN, Secure SD-WAN, Fortinet, MPLS, Network security, Network performance, Enterprise networks

TABLES DES MATIERES

REMERCIEMENTS 2
DEDICACES 4
TABLES DES MATIERES 6
SIGLES ET ABREVIATIONS : 8
LISTES DES FIGURES : 10
LISTES DES TABLEAUX : 12
INTRODUCTION 13
CHAPITRE 1 : CADRE THEORIQUE ET METHOLOGIQUE 15
1.1 Cadre théorique 15
1.1.1 Présentation de la structure d'accueil (SONATEL) 15
1.1.1.1 Historique 15
1.1.1.2 Organisation de la Direction Des Entreprises (DDE) 16
1.1.2 Description du sujet 19
1.1.2.1 Problématique 19
1.1.2.2 Démarche décrite 19
1.2 Cadre Méthodologique 20
1.2.1 Techniques de recherche 20
1.2.1.1 Recherche documentaire 20
1.2.1.2 Recherche terrain 20
CHAPITRE 2 . CADRE CONCEPTUEL 22
2.1 Réseaux WAN 22
2.1.1 Concepts généraux des réseaux WAN 22
2.1.2 MPLS 24
2.1.2.1 Définition 24
2.1.2.2 Fonctionnement 24
2.1.2.3 Avantages et limites : 26
2.2 Cadre technologique du SD-WAN 27
2.2.1 Généralités et définition 27
2.2.2 Technologies et principes de fonctionnement 28
2.2.3 Sécurité et gestion centralisée 30
2.2.4 Modélisation 30
2.2.4.1 Etude comparative des solutions Open Source 30
2.2.4.2 Etude comparative des solutions propriétaires 31
2.2.4.3 Solution retenue (Fortinet Secure SD-WAN) 32
2.2.4.4 Description des outils 33
CHAPITRE 3 . MISE EN ŒUVRE 37

3.1 Infrastructure réseau existante (PAMECAS) 37
3.1.1 architecture et équipements 37
3.1.2 Analyse des points faibles 41
3.2 Mise en œuvre de la solution SD-WAN 41
3.2.1 Mise en place des infrastructures 41
3.2.1.1 Déploiement de la solution 41
3.2.2 Déploiement opérationnel 44
3.2.2.1 Installation et configuration des équipements 44
3.2.3 Supervision et gestion centralisée 58
3.2.3.1 Gestion centralisée (FortiManager) 58
3.2.3.2 Centralisation des logs (FortiAnalyzer) 59
3.2.3.3 Gestion des Endpoints (FortiEMS) 60
3.3 Difficultés rencontrées 61
CONCLUSION 63
BIBLIOGRAPHIE/WEBOGRAPHIE 64

SIGLES ET ABREVIATIONS :

Nous présentons ici les sigles et abréviations que nous utiliserons dans le document

WAN	Wide Area Network
SDN	Software Defined Networking
SD-WAN	Software Defined Wide Area Network
VPN	Virtual Private Network
VLAN	Virtual Local Area Network
MPLS	Multiprotocol Label Switching
VRF	Virtual Routing and Forwarding
CE	Customer Edge
PE	Provider Edge
FTTH	Fiber To the Home
EMS	Endpoint Management System
IT	Information Technology
ICT	Information and Communication Technologies
Wi-Fi	Wireless Fidelity
SaaS	Software as a Service
IaaS	Infrastructure as a Service
LTE	Long-Term Evolution
NGFW	Next Generation Firewall
IP	Internet Protocol
IPS	Intrusion Prevention System
IDS	Intrusion Detection System
IPsec	Internet Protocol Security
RFC	Request For Comments
BGP	Border Gateway Protocol
GNS3	Graphic Network Similator-3
QoS	Quality of Service
OSI	Open Systems Interconnection
VoIP	Voice over Internet Protocol
DNS	Domain Name System

TCO	Total Cost of Ownership
DIA	Direct Internet Access
AP	Access Point
HA	High Availability
SSID	Service Set Identifier
DHCP	Dynamic Host Configuration Protocol
SASE	Secure Access Service Edge

LISTES DES FIGURES :

Figure 1 : Siège SONATEL……14

Figure 2 : Organigramme d'une partie de la DDE……..15

Figure 3 : WAN (Wide Area Network)……22

Figure 4 : Schéma de fonctionnement d'un VPN MPLS…….24

Figure 5 : Architecture du SD-WAN……28

Figure 6 : Architecture existante……...37

Figure 7 : Architecture cible…….42

Figure 8 : Dashboard FortiGate……44

Figure 9 : Configuration HA…….44

Figure 10 : Interco fortigate-switchcore……45

Figure 11 Configuration interface vlan…….46

Figure 12 : Configuration serveur DHCP…….46

Figure 13 : Configuration interface vlan téléphonie…….47

Figure 14 : SSIDs…….47

Figure 15 : Configuration des SSIDs……48

Figure 16 : option vlan ID…….48

Figure 17 : Configuration des serveurs DNS……49

Figure 18 : SDWAN_INTERNET……49

Figure 19 : Performance SLA……..50

Figure 20 : Routage vers internet…….50

Figure 21 : Routage vers sites distants – Partenaires……50

Figure 22 : Filtrage web……51

Figure 23 : Filtrage applicatif……52

Figure 24 : Objets…….53

Figure 25 : Types d'objets…….53

Figure 26 : Policy ipv4……..54

Figure 27 : Policy vers internet…….54

Figure 28 : Policy vers partenaires……55

Figure 29 : VPN IPsec……..56

Figure 30 : Ajout des tunnels IPsec dans une zone SDWAN……..56

Figure 31 : SDWAN Policy vers sites distants et partenaires……..57

Figure 32 : Policy entre siège – sites distants……..57

Figure 33 : FortiManager…….58

Figure 34 : FortiAnalyzer…….59

Figure 35 : FortiEMS……60

LISTES DES TABLEAUX :

Tableau 1 : Récapitulatifs des équipements de l'architecture existante……39

Tableau 2 : Récapitulatif des équipements de l'architecture cible……41

INTRODUCTION

Dans un paysage numérique en perpétuelle évolution, les entreprises font face à des impératifs contradictoires : répondre à une demande croissante en bande passante, supporter l'explosion du télétravail et des applications cloud, tout en garantissant un haut niveau de sécurité et de résilience, le tout dans un cadre budgétaire contraint. Les réseaux étendus traditionnels, historiquement structurés autour de technologies propriétaires et coûteuses, peinent à suivre le rythme de cette transformation. Depuis les années 1990, l'architecture WAN des entreprises a été dominée par le MPLS, une technologie fiable mais coûteuse et rigide, qui forçait tout le trafic, y compris celui à destination d'Internet, à transiter par le hub. Cette approche est devenue obsolète avec l'explosion du cloud computing et des applications SaaS dans les années 2010, créant un besoin urgent d'agilité et de réduction des coûts. En réponse, la technologie SD-WAN a émergé vers 2014-2015, appliquant les principes du SDN pour décentraliser la connectivité, gérer le réseau de manière centralisée et utiliser intelligemment plusieurs liens (MPLS, Internet, 4G/5G).

Face à ces défis, le SD-WAN (Software-Defined Wide Area Network) émerge comme une solution incontournable. Bien plus qu'une simple évolution technologique, il représente un changement de paradigme, permettant une gestion centralisée, agile et intelligente des flux réseau sur plusieurs liens de transport. Il offre une optimisation dynamique du trafic, une meilleure qualité de service (QoS) et une simplification opérationnelle significative[1]. Cependant, la promesse de performance et d'agilité ne doit pas se faire au détriment de la sécurité, qui devient d'autant plus critique que le trafic sort directement sur Internet. C'est dans ce contexte que les solutions Secure SD-WAN, intégrant nativement des fonctionnalités de pare-feu nouvelle génération (NGFW), de chiffrement et de segmentation, prennent tout leur sens.

Ce mémoire a pour objet d'étudier la mise en œuvre d'une solution Fortinet Secure SD-WAN dans le domaine des entreprises, du cadre de leur partenariat avec la SONATEL. La problématique centrale de ce travail est donc la suivante : dans quelle mesure le déploiement d'une solution Fortinet Secure SD-WAN permet-il d'améliorer simultanément les performances, la résilience et la sécurité posturale des réseaux d’entreprise , tout en optimisant les coûts ?

Pour y répondre, cette étude s'articulera en trois chapitres principaux. Dans un premier temps, nous poserons le cadre théorique et méthodologique en définissant les concepts clés du SD-

WAN et en présentant la structure d'accueil et notre approche d'analyse. Ensuite, le cadre conceptuel permettra de parcourir un ensemble de solutions disponibles et de dresser un diagnostic approfondi de l'architecture réseau existante des entreprises, en identifiant les points de fragilité. Enfin, le troisième chapitre sera consacré à la mise en œuvre pratique de la conception de la nouvelle architecture sécurisée au déploiement opérationnel des équipements.

CHAPITRE 1 : CADRE THEORIQUE ET METHOLOGIQUE

1.1 Cadre théorique

Le cadre théorique constitue le socle conceptuel et analytique du présent mémoire. Il a pour objectif de poser les bases théoriques nécessaires à la compréhension du sujet étudié, en définissant les concepts clés et en situant l'étude dans son contexte institutionnel et organisationnel. À cet effet, il présente la structure d'accueil, SONATEL, à travers son historique et l'organisation de la Direction des Entreprises, afin de contextualiser la recherche. Il intègre également la description du sujet, la formulation de la problématique ainsi que la démarche adoptée, permettant ainsi de structurer l'analyse, d'orienter la réflexion scientifique et d'assurer la cohérence méthodologique de l'ensemble du travail.

1.1.1 Présentation de la structure d'accueil (SONATEL)

La présentation de la structure d'accueil vise à situer le cadre institutionnel et organisationnel. Elle permet de donner un aperçu général de SONATEL à travers son historique, ses missions et son positionnement dans le secteur des télécommunications. Cette présentation met également en évidence l'organisation de la Direction des Entreprises (DDE), afin de mieux comprendre son rôle, ses responsabilités et son fonctionnement, éléments essentiels pour justifier les choix opérés dans le cadre de la recherche. [2]

1.1.1.1 Historique



Figure 1 : Siège SONATEL, [2]

La **SONATEL** (Société Nationale des Télécommunications du Sénégal), créée en 1985, est le leader des télécommunications et des services numériques au Sénégal et dans la sous-région (Mali, Guinée Conakry, Guinée-Bissau et Sierra Leone) depuis son entrée dans le groupe Orange en 1997. En tant qu'opérateur historique et intégré, elle offre un large portefeuille de services incluant la téléphonie fixe et mobile, l'accès à Internet, la transmission de données, les services cloud et la cybersécurité avec plusieurs milliers de collaborateurs.

Elle joue un rôle stratégique dans la transformation numérique de la sous-région grâce à ses infrastructures modernes (câbles sous-marins, data centers, backbone national et régional). En tant qu'opérateur intégré, elle répond à la fois aux besoins des particuliers, des entreprises et des institutions publiques.

1.1.1.2 Organisation de la Direction Des Entreprises (DDE)

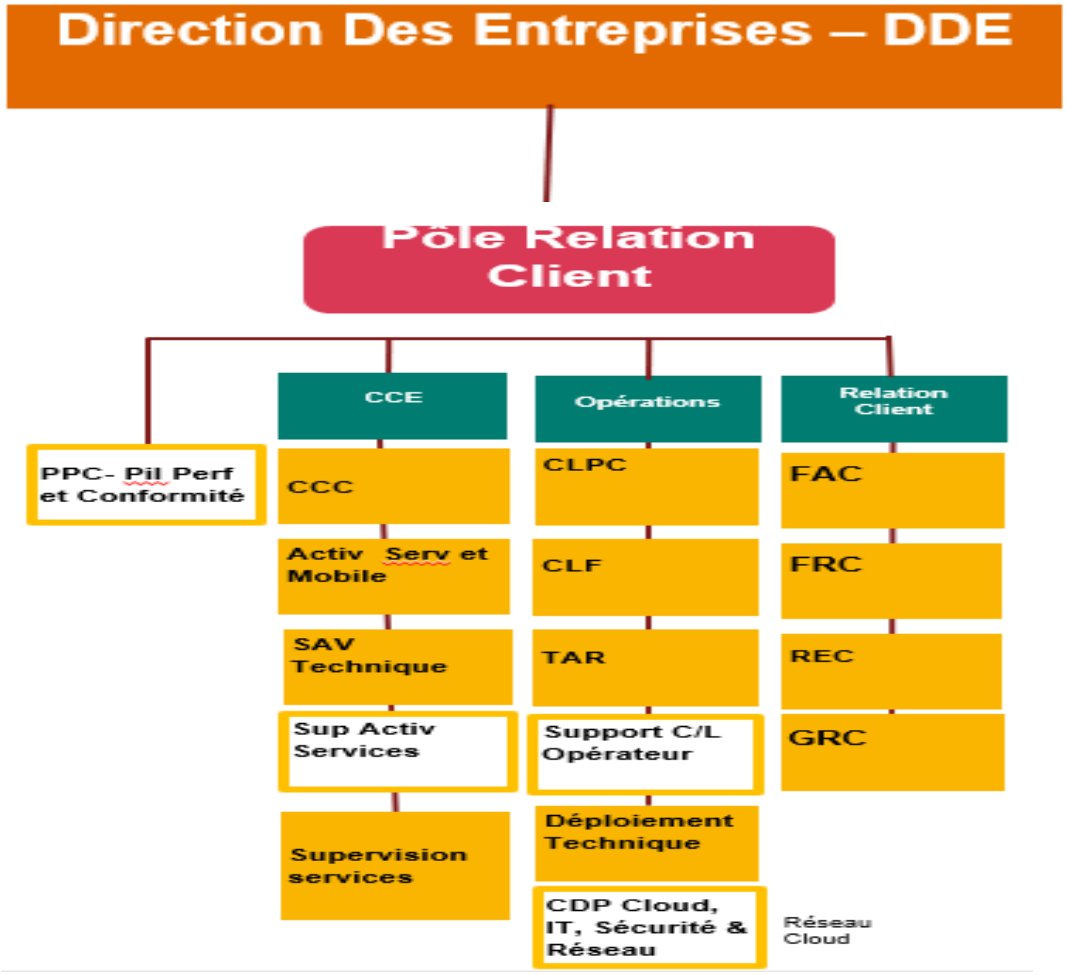


Figure 2 : Organigramme d'une partie de la DDE

La gouvernance de Sonatel repose sur un Directeur Général assisté d'un comité exécutif composé des directeurs des principales entités opérationnelles et stratégiques. Depuis le 31 juillet 2025, la direction générale est assurée par **M. Brelotte Ba**, succédant à **M. Sékou Dramé**.

L'entreprise s'articule autour de plusieurs grandes directions dont :

- **La Direction des Entreprises (DDE)** : cette direction est spécifiquement dédiée aux clients grands comptes et accompagne les organisations dans la conception et l'intégration de solutions de télécommunication, et de sécurité adaptée à leurs besoins, ayant pour missions :

- Proposer des solutions télécoms et IT aux grandes entreprises et institutions
- Assurer la modernisation et la sécurisation de leurs infrastructures ;
- Accompagner leur transformation digitale en s'appuyant sur des partenariats avec des constructeurs de renom tels que Cisco, Fortinet, Huawei, etc.

La DDE constitue ainsi l'interface entre Sonatel et ses clients professionnels, en leur offrant un suivi personnalisé et une expertise technique de haut niveau.

- **Le Pôle Relation Client (RC)** : au sein de la DDE, le Pôle Relation Client est chargé de gérer la relation commerciale et technique avec les entreprises clientes. Il regroupe plusieurs départements opérationnels qui assurent la mise en œuvre et le suivi des projets. Ce pôle joue un rôle crucial en coordonnant les besoins exprimés par les clients et les solutions proposées par Sonatel.

- **Le Centre de Contact Entreprises (CCE)** : Ce département est l'interface principale du service client DDE avec les clients B2B. Ses missions et activités principales seront de recueillir et de traiter toutes les demandes et interactions à cycle court (moins de 48 heures) :

- Demandes d'information et de soutien

- Relève des dérangements des liaisons et services opérateur

- Service après-vente (maintenance) et support sur les services ICT

- Livraisons et activation de services mobiles
- Supervision des services installés chez les clients B2B

➢ **Le Département des Opérations (DDO) :** C'est l'entité technique qui veille à la bonne exécution des projets confiés à la DDE. Ses missions couvrent la planification et la supervision des déploiements, ainsi que le suivi opérationnel et le support aux clients entreprises. Le DDO agit en étroite collaboration avec les équipes commerciales et les partenaires technologiques afin de garantir la qualité de service et le respect des engagements contractuels.

➢ **Le Service Déploiement Technique (SDT) :** Le SDT, qui a constitué mon service d'accueil durant ce stage, occupe une place centrale dans le DDO. Il est spécialisé dans le déploiement technique des solutions réseaux et sécurité auprès des clients grands comptes. Ses principales missions consistent à :

- Réaliser la configuration et l'intégration des équipements réseaux (pare-feu, commutateurs, routeurs, points d'accès Wi-Fi, etc.)
- Assurer la mise en place des politiques de sécurité (VPN, VLAN, redondance, haute disponibilité)
- Produire la documentation d'exploitation et accompagner les clients dans la prise en main des solutions déployées par un transfert de compétence
- Garantir la qualité et la continuité de service après déploiements

Le service constitue un maillon essentiel entre la conception des projets et leur exploitation quotidienne, en contribuant directement à la satisfaction des clients

Dans le cadre de ce projet, la SONATEL est positionnée comme **l'intégrateur et le fournisseur de service**. L'objectif pour elle est de concevoir, commercialiser et déployer une offre de service managé **Secure SD-WAN** à destination de ses clients entreprises. Cette offre lui permettrait de répondre aux défis des WAN traditionnels en proposant une solution moderne, managée et sécurisée, créant ainsi une nouvelle source de valeur et de revenus, tout en renforçant sa position sur le marché très concurrentiel des entreprises.

1.1.2 Description du sujet

1.1.2.1 Problématique

Les entreprises, reposant sur un réseau WAN traditionnel (souvent basé sur le MPLS), font face à plusieurs défis :

1. Coût élevé : Les liens MPLS sont réputés pour leur fiabilité mais aussi pour leur coût prohibitif, surtout pour le débit.
2. Rigidité et lenteur de déploiement : Provisionner un nouveau lien MPLS ou modifier l'architecture peut prendre plusieurs semaines, ce qui nuit à l'agilité business.
3. Performance des applications cloud : Le trafic à destination du cloud (SaaS, IaaS) est souvent collecté vers un data center central pour inspection de sécurité, ajoutant de la latence et dégradant l'expérience utilisateur.
4. Gestion complexe : La configuration et la maintenance des équipements réseau (routeurs, pare-feux) site par site sont chronophages et sujettes aux erreurs.
5. Sécurité inégale : La sécurité peut varier d'un site à l'autre, créant des failles potentielles, surtout sur les succursales moins bien équipées.

La principale problématique est donc de mettre en place une architecture redondante et évolutive pour améliorer simultanément les performances applicatives, renforcer la sécurité globale et réduire les coûts opérationnels, tout en garantissant une gestion simplifiée et centralisée.

1.1.2.2 Démarche décrite

Cette étude vise à concevoir et modéliser le déploiement d'une solution Secure SD-WAN pour répondre à cette problématique.

- Enjeu majeur : Démontrer la faisabilité et les bénéfices du déploiement d'une architecture Secure SD-WAN.
- Enjeux spécifiques :
    1. Analyser l'architecture réseau existante et identifier ses limites.
    2. Effectuer une étude comparative des solutions SD-WAN du marché (open source et propriétaires) pour sélectionner la plus adaptée au contexte.

3. Concevoir une nouvelle architecture Secure SD-WAN intégrant des mécanismes de sécurité renforcée, de haute disponibilité, ainsi qu'un routage applicatif intelligent basé sur des SLA préalablement définis.
4. Modéliser le déploiement opérationnel de la solution, incluant le déploiement des équipements, la configuration centralisée et les tests de basculement.
5. Évaluer les gains escomptés en termes de performance, de sécurité et de réduction des coûts.

1.2 Cadre Méthodologique

1.2.1 Techniques de recherche

Pour mener à bien cette étude, une approche de recherche mixte a été adoptée.

1.2.1.1 Recherche documentaire

Une revue exhaustive de la littérature a été réalisée en amont pour constituer le cadre théorique. Les sources consultées incluent :

- Documentation technique et livres blancs des principaux vendeurs de solutions SD-WAN (Fortinet, Cisco, VMware, Palo Alto, etc.).
- Articles académiques et de recherche sur les architectures SD-WAN, les protocoles sous-jacents et les modèles de sécurité.
- Études de cas et retours d'expérience d'entreprises ayant déployé des solutions similaires, notamment dans le secteur bancaire.
- Normes et RFCs concernant les protocoles utilisés (IPsec, BGP, etc.).

1.2.1.2 Recherche terrain

La recherche terrain est centrée sur l'analyse de l'environnement :

- Entretiens et questionnaires avec les équipes IT et réseau pour comprendre et valider l'architecture actuelle et future, les flux applicatifs et les objectifs business.
- Analyse de l'existant : Collecte des configurations réseau, schémas d'architecture, politiques de sécurité et audits de performance pour établir un état des lieux précis.
- Repérage des différentes interconnexions entre les équipements.

- Modélisation et conception : Utilisation d'outils de modélisation et de laboratoires d'essai (Microsoft Visio, draw.io) pour concevoir la solution SD-WAN proposée avant un éventuel déploiement réel.

Au terme de ce premier chapitre, qui a posé les bases théoriques et méthodologiques nécessaires à la compréhension du sujet, il apparaît essentiel d'approfondir les notions techniques qui sous-tendent la solution envisagée. Ainsi, le chapitre suivant sera consacré au cadre conceptuel, permettant d'examiner en détail les technologies, principes de fonctionnement et évolutions majeures des réseaux WAN et du SD-WAN. Cette transition marque le passage d'une compréhension générale du contexte à une analyse plus spécifique et approfondie des concepts fondamentaux.

CHAPITRE 2 . CADRE CONCEPTUEL

2.1 Réseaux WAN

Les réseaux étendus, communément appelés WAN (Wide Area Network), constituent une composante essentielle des infrastructures de communication modernes. Ils permettent l'interconnexion de réseaux locaux (LAN) et métropolitains (MAN) situés dans des zones géographiques différentes, parfois à l'échelle nationale ou internationale. Les WAN jouent un rôle stratégique dans les organisations multisites en assurant la continuité des services, le partage des ressources et l'accès distant aux applications critiques. Leur mise en œuvre repose sur diverses technologies de transmission et répond à des exigences élevées en matière de performance, de sécurité et de fiabilité.

2.1.1 Concepts généraux des réseaux WAN

Les réseaux WAN (Wide Area Network) connectent des sites géographiquement éloignés. Étant donné que les WAN ne sont pas liés à un emplacement spécifique, ils permettent aux réseaux localisés de communiquer entre eux sur de grandes distances facilitant ainsi le partage d'informations entre les dispositifs, partout dans le monde. Les WAN permettent aux organisations de créer des réseaux unifiés pour que les employés, les clients et les autres parties prenantes puissent travailler ensemble en ligne, quel que soit l'emplacement.

Exemples de WAN

- Dans une entreprise, un WAN est créé pour connecter les succursales, bureau principal de l'entreprise, les employés à distance qui travaillent à domicile etc. .
- Dans une université ou un campus, les étudiants peuvent faire appel à des WAN pour accéder aux bases de données de la bibliothèque ou à la recherche universitaire.
- Une banque, y compris ses succursales et ses DAB, est un autre exemple d'organisation utilisant un WAN. Les succursales peuvent se trouver dans plusieurs États américains, ou même dans des sites mondiaux, mais elles sont toutes liées par diverses connexions sécurisées. Les employés de la banque, tout comme les clients, sont des utilisateurs.
- On peut dire qu'Internet est le plus grand WAN au monde, parce qu'il s'agit de la forme la plus grande et la plus diversifiée d'un réseau informatique au monde.

Voici un schéma illustratif.

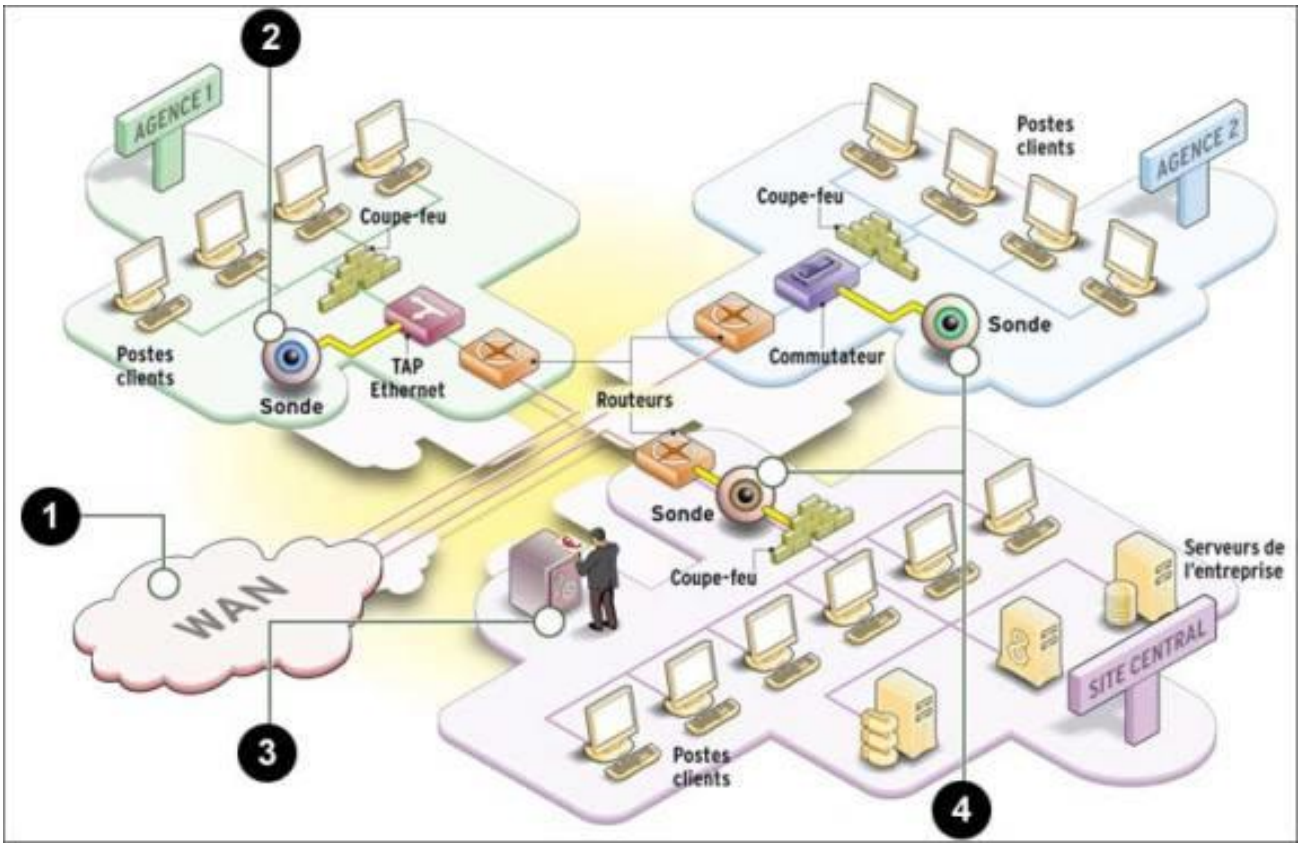


Figure 3 : WAN (Wide Area Network), [3]

Ce schéma illustre une infrastructure WAN (Wide Area Network) reliant plusieurs sites distants (agences) à un site central de l'entreprise.

Chaque agence (Agence 1 et Agence 2) comprend :

- Des postes clients utilisés par les employés.
- Un pare-feu (coupe-feu) assurant la protection locale contre les intrusions et les connexions non autorisées.
- Une sonde réseau connectée via un TAP Ethernet ou un commutateur, permettant de surveiller le trafic sortant et entrant de l'agence.

Le site central regroupe :

- Les serveurs de l'entreprise (applications, bases de données, services partagés).
- Des postes clients internes connectés au réseau local.
- Un pare-feu central pour protéger les ressources critiques.
- Une sonde réseau dédiée au monitoring global du trafic venant des agences et d'Internet.

Les routeurs assurent la liaison entre le WAN et les réseaux locaux (LAN) des différentes agences et du site central.

Une sonde intermédiaire est placée ici pour analyser le trafic intersites, notamment pour la détection d'incidents de sécurité ou la mesure de performance du WAN.

Bien que les WAN couvrent une large zone, les connexions peuvent être filaires ou sans fil. Les réseaux WAN filaires se composent généralement de services Internet haut débit et de commutation multi-protocole par étiquette (Multiprotocol Label Switching, MPLS), qui est une forme de technologie de transfert de données utilisée pour contrôler le flux de trafic et accélérer la connexion, tandis que les réseaux WAN sans fil comprennent normalement des réseaux 4G/5G, etc.

Les réseaux WAN traditionnels s'appuyaient majoritairement sur la technologie MPLS (Multiprotocol Label Switching).

2.1.2 MPLS

2.1.2.1 Définition

La commutation multi-protocole d'étiquettes (MPLS) est un protocole polyvalent et efficace conçu pour acheminer des paquets de données vers leurs destinations rapidement et efficacement. Étant donné qu'il envoie des données directement à sa destination, il est supérieur au routage IP (Internet Protocol) normal, qui renvoie les données sur Internet avant de les envoyer finalement à sa destination finale. Il en résulte donc une meilleure transmission et qualité de service (QoS) globale. Certaines entreprises l'ont, et continuent de l'utiliser, en particulier lorsqu'une connexion forte et ininterrompue est essentielle. Il réduit la latence et permet aux entreprises d'exécuter des visioconférences plus fluides ou des appels VoIP (Voice over Internet Protocol), qui dépendent de flux de données fluides et ininterrompus.

2.1.2.2 Fonctionnement

La commutation multi-protocole par étiquettes est une technologie réseau qui permet aux routeurs de prendre des décisions de transfert basées sur des étiquettes plutôt que sur des adresses IP. C'est un protocole polyvalent et efficace pour acheminer le trafic réseau. Le MPLS n'est pas un produit ou un service, et cette distinction est essentielle pour comprendre son fonctionnement. Il s'agit plutôt d'une technique qui désigne des chemins pour envoyer des données entre les nœuds au lieu des endpoints. Afin d'illustrer concrètement l'application de

cette technologie, Le L3 VPN basé sur MPLS exploite le cœur de réseau d'un opérateur pour interconnecter de manière sécurisée et transparente les sites distants d'un client ou des plusieurs clients. Un L3 VPN over MPLS permet à l'entreprise de "louer" ce service auprès de son opérateur. L'opérateur utilise son réseau MPLS existant pour créer un réseau privé virtuel pour cette entreprise. [4]

Le réseau MPLS repose sur trois types de routeurs. Les routeurs P, situés au cœur du réseau de l'opérateur, assurent uniquement la commutation des étiquettes MPLS, sans connaissance des routes ou des VPN des clients, ce qui garantit simplicité et évolutivité. Les routeurs PE, en périphérie, jouent un rôle central : ils se connectent aux clients, apprennent leurs routes, gèrent les VPN et appliquent les étiquettes MPLS. Les routeurs CE, appartenant aux clients, échangent simplement des routes IP classiques avec les PE, sans visibilité sur le MPLS.

Pour isoler les clients, les routeurs PE utilisent des VRF (VPN Routing and Forwarding). Chaque client dispose de sa propre table de routage virtuelle, ce qui permet de séparer les flux et même d'accepter des adresses IP qui se chevauchent entre différents clients.

L'échange des routes entre les routeurs PE est assuré par le MP-BGP. Grâce au Route Distinguisher (RD), les routes des clients deviennent uniques au niveau du réseau de l'opérateur. Le Route Target (RT) permet, quant à lui, de contrôler quelles routes sont importées ou exportées dans chaque VPN, définissant ainsi l'appartenance au VPN. Ainsi, le trajet logique que suivent les paquets à travers le réseau MPLS, comparable à une "autoroute" virtuelle est appelé LSP (Label Switching Path).

Enfin, le transport du trafic s'appuie sur une pile de deux étiquettes MPLS. L'étiquette externe permet d'acheminer le paquet à travers le cœur du réseau MPLS, tandis que l'étiquette interne indique au PE de sortie dans quelle VRF livrer le trafic. Cette combinaison assure un transport efficace, sécurisé et totalement isolé entre les clients.

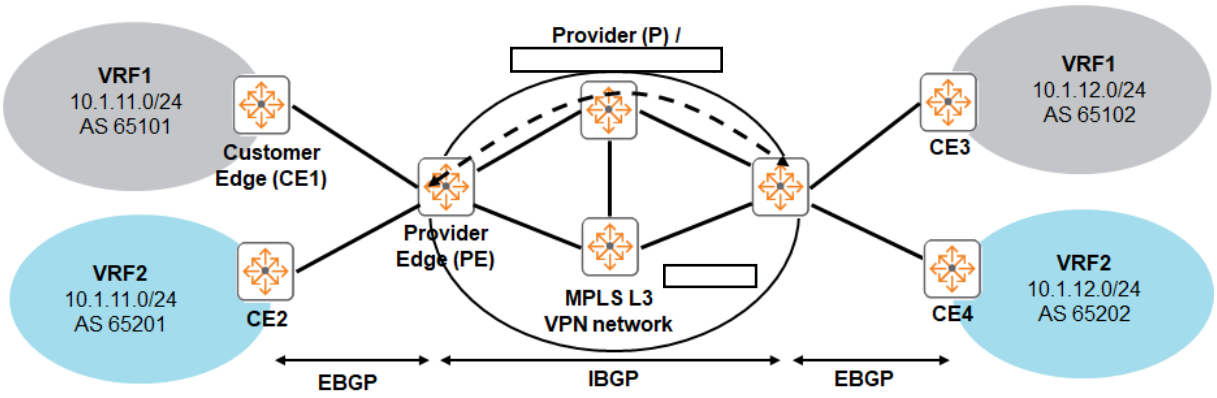


Figure 4 : Schéma de fonctionnement d'un VPN MPLS, [5]

Exemple : Envoi d'un paquet de Paris vers Marseille

Lorsqu'un paquet est envoyé de Paris vers Marseille, le CE de Paris transmet un paquet IP classique au PE de Paris. Celui-ci identifie la destination dans la VRF du client et encapsule le paquet avec deux étiquettes MPLS : une étiquette interne (VPN) pour identifier la VRF de sortie, et une étiquette externe pour transporter le paquet à travers le cœur MPLS.

Dans le cœur du réseau MPLS, les routeurs P ne traitent que l'étiquette de transport. Ils commutent le paquet de routeur en routeur sans jamais analyser le contenu IP ni l'étiquette VPN.

À l'arrivée, le PE de Marseille reçoit le paquet, enlève l'étiquette de transport puis l'étiquette VPN, identifie la VRF correspondante, et transmet enfin le paquet IP original au CE de Marseille, qui le livre au serveur de destination.

2.1.2.3 Avantages et limites :

- **Avantages :**
  - Fiabilité et Qualité de Service (QoS) garantie : MPLS offre un haut degré de fiabilité, de faibles taux de perte de paquets (jitter) et de latence, ce qui le rend idéal pour les applications sensibles comme la voix (VoIP) et la vidéoconférence.
  - Sécurité : Le réseau MPLS est un réseau privé et maîtrisé par l'opérateur, offrant une isolation naturelle des données par rapport à l'Internet public.
  - Prévisibilité : Les performances sont constantes et prévisibles, car la bande passante est dédiée.

- **Limites :**
    - Coût élevé : La bande passante MPLS est significativement plus chère que la bande passante Internet.
    - Manque de flexibilité : Le déploiement de nouveaux sites ou la modification de la bande passante est un processus long, souvent de plusieurs semaines ou mois.
    - Déficience face au Cloud : Le trafic destiné aux applications cloud (SaaS, IaaS) est souvent ramené vers le siège central avant d'accéder à Internet, ce qui ajoute de la latence et dégrade l'expérience utilisateur.
    - Dépendance à un seul lien : En cas de défaillance du lien MPLS, le site est souvent complètement isolé à moins de disposer d'un lien de secours coûteux et complexe à configurer.

2.2 Cadre technologique du SD-WAN

Le cadre technologique du SD-WAN s'inscrit dans une dynamique d'évolution des architectures réseaux traditionnelles, motivée par la nécessité de répondre aux nouveaux besoins des organisations en matière de performance, de flexibilité et de sécurité. Avant de détailler les aspects techniques et fonctionnels du SD-WAN, il convient d'en présenter les notions générales et la définition afin de mieux comprendre les principes sur lesquels repose cette technologie.

2.2.1 Généralités et définition

Le SD-WAN (Software-Defined Wide Area Network) est une approche moderne pour connecter des sites distants via un logiciel intelligent qui gère les flux sur différentes connexions. Cette technologie permet d'optimiser les performances des applications, d'améliorer la sécurité, de réduire les coûts et de simplifier la gestion du réseau grâce à un contrôle centralisé. Le SD-WAN est une évolution du réseau étendu (WAN) qui offre plus de flexibilité et de résilience, notamment pour les environnements cloud et hybrides. La fonction WAN (réseau étendu) traditionnelle consistait à connecter les utilisateurs de la succursale aux applications hébergées sur des serveurs du data center. Généralement, des circuits MPLS dédiés étaient utilisés pour assurer la sécurité et une connectivité fiable. Cela a conduit les solutions de WAN défini par logiciel (SD-WAN) à devenir de plus en plus populaires, car les

organisations demandent une connectivité rapide, évolutive et flexible entre différents environnements réseau.[1]

Le SD-WAN peut être défini comme une technologie réseau qui utilise un logiciel pour gérer les connexions entre différents sites. Il permet d'optimiser l'utilisation de divers types de réseaux (comme le MPLS, la fibre, la 4G/5G) et d'améliorer la performance des applications en choisissant le meilleur chemin pour le trafic. Le SD-WAN centralise la gestion du réseau et renforce la sécurité grâce à des politiques de sécurité centralisées et un chiffrement de bout en bout.[6]

2.2.2 Technologies et principes de fonctionnement

Le SD-WAN repose sur plusieurs piliers technologiques fondamentaux :

- Séparation des plans de contrôle et de données : Le plan de contrôle ("intelligence") est logiciel et centralisé, permettant de définir des politiques de routage et de sécurité de manière globale. Le plan de données (le "traitement du trafic") reste délocalisé sur les appareils en périphérie.
- Abstraction du transport : Le SD-WAN permet l'agrégation et la gestion unifiée de multiples connexions (MPLS, fibre, Internet public, LTE/5G) pour former une liaison logique unique, garantissant ainsi résilience et performance.
- Sélection de chemin dynamique : Grâce à des mécanismes de mesure continue de la qualité des liens (latence, gigue, perte de paquets), le SD-WAN peut router le trafic en temps réel sur le meilleur chemin disponible en fonction de la criticité de l'application (par exemple, prioriser le MPLS pour la VoIP et utiliser l'Internet pour le trafic web).
- Chiffrement de bout en bout : La sécurité est intrinsèque, avec un chiffrement IPsec appliqué sur l'ensemble des liens, créant un réseau maillé sécurisé entre tous les sites.[3]

Pour répondre aux besoins d'un réseau aussi largement distribué, de nombreuses entreprises ont adopté des solutions telles que le WAN défini par logiciel (SD-WAN), ainsi que des options de connectivité à moindre coût. De ce fait, nombre d'entre elles ont entrepris d'importants projets de transformation de leur WAN ces dernières années.

L'image suivante illustre une solution de périphérie de succursale SD-WAN modernisée qui gère une architecture hybride incluant à la fois un WAN privé (MPLS) et une connectivité Internet haut débit.

`

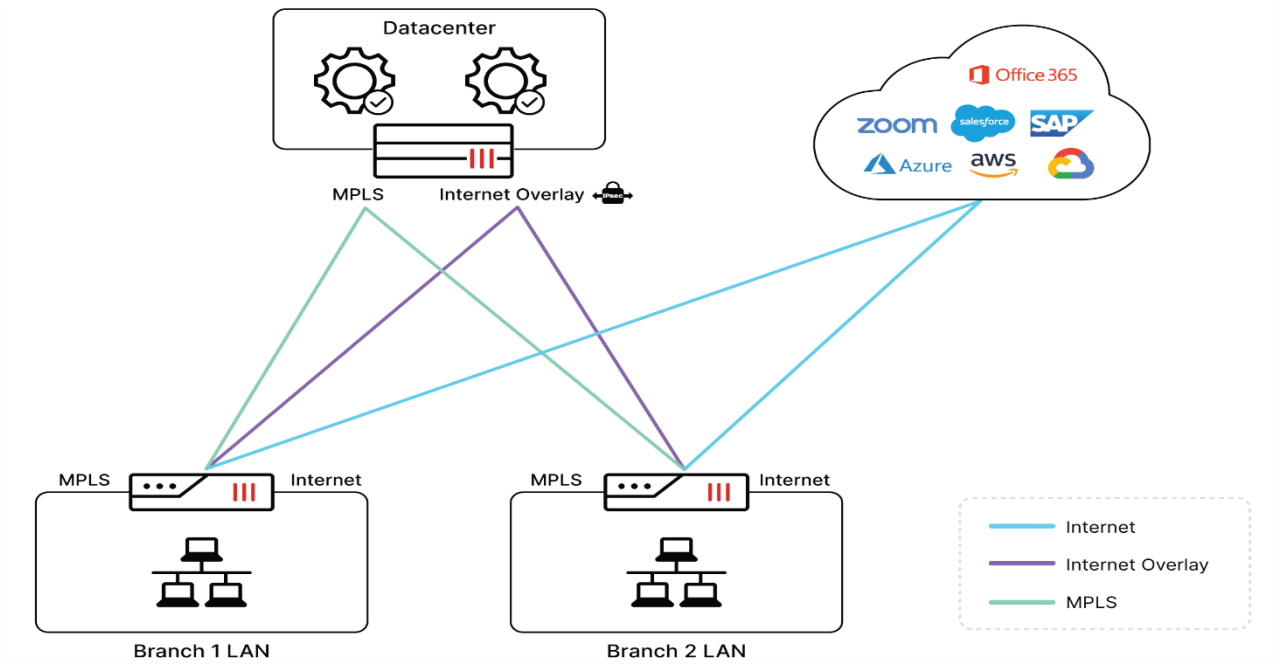


Figure 5 : Architecture du SD-WAN[7]

Premièrement, la succursale dispose de plusieurs transports, ou options de connectivité. Dans cet exemple, le réseau WAN MPLS de l'entreprise est conservé, mais l'organisation a mis en place une connexion haut débit unique pour fournir un accès Internet direct (DIA) depuis la succursale. De plus, l'organisation a établi un réseau superposé utilisant des tunnels IPsec (Internet Protocol Security) entre les succursales et le centre de données via le transport Internet haut débit. Il en résulte que plusieurs chemins sont possibles entre la succursale et le centre de données, ainsi que vers un environnement multicloud.

Comparez cela à l'architecture traditionnelle à chemin unique, avec un commutateur connecté à un routeur simple disposant d'une connexion à un WAN privé. En principe, il n'existe qu'une seule option pour le trafic sortant. Cependant, l'introduction de DIA offre intrinsèquement une architecture de connectivité redondante. En termes de connectivité des centres de données, le réseau superposé offre un chemin alternatif pour les applications critiques qui emprunteraient normalement le MPLS.[7]

2.2.3 Sécurité et gestion centralisée

La convergence de la connectivité et de la sécurité est un avantage clé des solutions SD-WAN modernes, dites **Secure SD-WAN**.

- Politiques de sécurité unifiées : Des pare-feux de nouvelle génération (NGFW), des systèmes de prévention des intrusions (IPS), et des filtrages web (Web Filtering) sont intégrés directement dans les appliances SD-WAN. Les politiques de sécurité sont définies une fois au niveau central et déployées de manière cohérente sur l'ensemble du réseau.
- Gestion centralisée : Une interface de gestion unique permet aux administrateurs de provisionner, configurer, surveiller et dépanner l'ensemble du réseau SD-WAN à partir d'une console centrale, simplifiant radicalement les opérations.
- Visibilité et analytique : Des outils dédiés agrègent les logs et les données de tous les sites pour fournir une visibilité complète sur les performances du réseau, les menaces de sécurité et l'utilisation des applications, facilitant le reporting et la prise de décision.[7]

2.2.4 Modélisation

2.2.4.1 Etude comparative des solutions Open Source

Des solutions open source comme FRRouting (FRR), StrongSwan (pour IPsec) et des outils de gestion comme OpenSDWAN (projet basé sur Linux) existent. Elles permettent de construire une solution SD-WAN "maison".

- **Avantages :** Coût logiciel nul, flexibilité et contrôle total.
- **Inconvénients :** Complexité de déploiement, de maintenance et de troubleshooting ; absence de support unifié ; fonctionnalités de sécurité avancées (NGFW) à intégrer séparément ; manque souvent de fonctionnalités clés comme une orchestration centralisée intuitive et une analyse approfondie des applications. Elles sont peu adaptées à un déploiement entreprise à grande échelle.

2.2.4.2 Etude comparative des solutions propriétaires

Le marché est dominé par plusieurs acteurs majeurs, chacun avec ses forces :

- **Cisco (Viptela/SD-WAN) :** Solution mature, intégration forte avec l'écosystème Cisco, large base installée. Le fonctionnement de la solution Cisco SD-WAN repose sur une architecture à plans séparés : plan de gestion, plan de contrôle et plan de données. Le vManage assure l'orchestration centralisée et la configuration des équipements, tandis que le vSmart Controller gère les politiques de routage, de sécurité et la sélection dynamique des chemins. Le vBond Orchestrator facilite l'authentification et l'établissement sécurisé des tunnels entre sites. Les routeurs vEdge ou cEdge établissent des tunnels IPsec sur différents liens WAN (MPLS, Internet, LTE). Le trafic est automatiquement orienté selon des politiques basées sur la performance (latence, perte, gigue), garantissant une haute disponibilité et une optimisation applicative.
- **VMware (Velocloud) :** Reconnue pour ses performances d'optimisation de trafic (Orchestration de chemins dynamiques) et son orientation cloud. La solution VMware SD-WAN fonctionne selon un modèle cloud-centric, fortement orienté vers l'optimisation des performances applicatives. Les Edge VeloCloud déployés sur les sites établissent des tunnels sécurisés vers des Gateways VeloCloud hébergées dans le cloud ou chez des opérateurs. L'Orchestrator, également cloud, assure la gestion centralisée. Le moteur Dynamic Multipath Optimization (DMPO) mesure en temps réel la qualité des liens WAN et sélectionne dynamiquement le meilleur chemin par application. Cette approche améliore fortement la performance des applications SaaS et cloud tout en simplifiant l'exploitation du réseau.
- **Fortinet (Secure SD-WAN) :** Se distingue par son approche "Security-Driven Networking", intégrant nativement des fonctions de pare-feu nouvelle génération (NGFW), une inspection SSL approfondie et une gestion unifiée dans le portail FortiGate. Le Fortinet Secure SD-WAN repose sur l'intégration native du SD-WAN au sein des pare-feu FortiGate. Le fonctionnement est basé sur une approche Security-Driven Networking, où la sécurité et la connectivité sont étroitement liées. Les FortiGate établissent des tunnels IPsec entre sites et appliquent simultanément des politiques de sécurité (NGFW, IPS, filtrage web,

inspection SSL). Le choix des chemins WAN est effectué selon des SLA applicatifs combinant performance réseau et règles de sécurité. La gestion centralisée est assurée par FortiManager et FortiAnalyzer, offrant une visibilité complète sur le trafic et les menaces.

- **Palo Alto Networks (Prisma SD-WAN) :** Met l'accent sur la sécurité avec l'intégration de son moteur de sécurité cloud (NGFW). La Prisma SD-WAN de Palo Alto Networks met l'accent sur une intégration avancée avec la sécurité cloud. Les équipements SD-WAN déployés sur les sites utilisent une analyse continue de la performance des liens pour sélectionner dynamiquement les chemins optimaux. Le trafic est automatiquement dirigé vers les services de sécurité Prisma Access pour une inspection approfondie via le moteur NGFW Palo Alto. Cette architecture garantit une protection cohérente des flux, en particulier pour les accès aux applications cloud et SaaS, tout en maintenant des performances optimales.
- **Versa Networks :** Solution basée sur les logiciels avec des fonctionnalités étendues de sécurité et de routage. La solution Versa SD-WAN est une plateforme entièrement logicielle, fonctionnant sur des équipements standards ou virtualisés. Son architecture repose sur un contrôleur centralisé qui orchestre à la fois les fonctions de connectivité, de routage et de sécurité. Les équipements Versa établissent des tunnels sécurisés multi-liens et appliquent des politiques avancées de routage dynamique, de segmentation réseau et de sécurité (pare-feu, IDS/IPS). Cette approche modulaire permet une grande flexibilité, particulièrement adaptée aux environnements multiclouds et aux fournisseurs de services.

2.2.4.3 Solution retenue (Fortinet Secure SD-WAN)

Le choix s'est porté sur la solution **Fortinet Secure SD-WAN** pour plusieurs raisons :

1. Intégration Sécurité-Réseau : Contrairement à des solutions qui ajoutent une sécurité à un réseau SD-WAN, Fortinet intègre nativement le NGFW, l'IPS, le filtrage DNS et le Sandboxing directement dans une seule appliance SD-WAN (FortiGate), éliminant les points de défaillance uniques et simplifiant l'architecture.

2. Fonctionnalités de Performance : Prise en charge de l'Orchestration de chemins dynamiques basée sur les mesures de latence, gigue et perte de paquets en temps réel, garantissant la meilleure expérience pour les applications critiques.

3. Gestion Centralisée Robustesse : La suite FortiManager (pour la gestion centralisée de la configuration) et FortiAnalyzer (pour la supervision centralisée et le reporting) offre une vue unifiée et simplifie les opérations.

4. Rapport Coût-Performance : La solution offre un TCO (Total Cost of Ownership) attractif en consolidant les fonctions routeur, firewall et SD-WAN dans un seul appareil, réduisant les coûts matériels et de gestion.[8]

2.2.4.4 Description des outils

- **FortiGate** : Appliance universelle qui agit comme le nœud SD-WAN aux sites siège et agences. Elle combine les fonctions de routeur, de pare-feu nouvelle génération (NGFW) et de point de terminaison VPN IPsec/SSL. Elle constitue le cerveau de la sécurité et du réseau pour chaque site.

  Fonctionnalités principales :

- Pare-feu NGFW : filtrage intelligent du trafic, inspection profonde des paquets (DPI).
- IPS / IDS : détection et prévention des intrusions.
- Antivirus et antimalware : protection en temps réel contre les menaces.
- Web filtering : contrôle de navigation et protection contre les sites malveillants.
- VPN (IPsec / SSL) : connexion sécurisée pour utilisateurs et sites distants.

  NB : Pour les dernières versions (à partir de la version fortiOS 7.4.9 et 7.6.4),ainsi les modèles G, les fonctionnalités SSL/VPN ne sont plus prises en charge.

- SD-WAN intégré : optimisation des liaisons réseau et routage applicatif intelligent.
- HA (High Availability) : continuité de service grâce au clustering. Pour les configurations, nous pouvons avoir de l'Active-active et Active-passive.
- Intégration avec l'écosystème Fortinet (FortiManager, FortiAnalyzer, FortiEMS...).

- **FortiSwitch** : Commutateur réseau managé qui s'intègre de manière transparente avec le FortiGate. Grâce à la technologie FortiLink, le FortiGate assume le contrôle et la

gestion centralisée de tous les FortiSwitches. Cette intégration permet d'appliquer des politiques de sécurité directement au niveau du commutateur (segmentation réseau, isolation des VLANs) et offre une visibilité complète du trafic, du pare-feu jusqu'au port.

Fonctionnalités principales :

- Intégration avec FortiGate (FortiLink) pour une gestion centralisée du réseau LAN depuis le pare-feu.
- Switching de couche 2 et 3 selon les modèles (VLAN, routage statique, ACLs...).
- Haute performance pour les réseaux d'entreprise (1G, 10G, 40G selon les modèles).
- Segmentation du réseau via VLAN, NAC et politiques de sécurité synchronisées.
- Support PoE/PoE+ pour alimenter téléphones IP, points d'accès Wi-Fi et caméras.
- Sécurité renforcée : contrôle d'accès, isolation, détection des anomalies.
- Administration simplifiée via FortiGate, FortiCloud ou FortiSwitch Manager.

- **FortiAP** : Point d'accès sans-déployé pour créer des réseaux Wi-Fi sécurisés. Comme le FortiSwitch, le FortiAP est entièrement managé par le FortiGate via le protocole FortiLink. Le FortiGate agit comme un contrôleur Wi-Fi centralisé, permettant un déploiement sans effort, une gestion unifiée des politiques sans fil et l'application de la sécurité NGFW directement au point d'accès pour les utilisateurs sans fil.

Fonctionnalités principales :

- Gestion centralisée via FortiGate (FortiLink), FortiWLC ou FortiCloud.
- Wi-Fi sécurisé grâce à l'intégration directe avec les politiques de sécurité du FortiGate (pare-feu, filtrage, authentification).
- Support des dernières normes Wi-Fi (Wi-Fi 5, Wi-Fi 6 et Wi-Fi 6E selon les modèles).
- Segmentation du trafic (VLAN, SSID multiples), idéale pour invités, employés, IoT.
- Détection et mitigation des menaces Wi-Fi (rogue AP, attaques sans fil).
- Qualité de service (QoS) optimisée pour les applications sensibles (VoIP, vidéo).
- Installation et déploiement simplifiés.

- **FortiManager** : Serveur de gestion centralisée pour l'administration unifiée des appareils Fortinet (FortiGate, FortiSwitch, FortiAP). Il permet le déploiement de

modèles de configuration, la gestion des politiques de sécurité et le provisioning de masse, essentiel pour un déploiement à grande échelle.

Fonctionnalités principales :

- Administration centralisée de multiples appareils Fortinet.
- Déploiement de configurations en masse via des modèles (templates).
- Gestion centralisée des politiques de sécurité pour assurer cohérence et conformité.
- Provisioning automatisé pour les nouveaux équipements.
- Gestion avancée des versions et sauvegardes de configuration.

- **FortiAnalyzer** : Serveur de collecte et d'analyse des logs. Il agrège les données de tous les appareils Fortinet (FortiGate, FortiSwitch, FortiAP), fournissant une vue consolidée de la sécurité, des performances du réseau et générant des rapports détaillés pour le monitoring et l'audit.

  Fonctionnalités principales :

- Collecte centralisée des logs et événements de sécurité.
- Analyse, corrélation et détection d'incidents de sécurité.
- Rapport avancés (sécurité, conformité, usage réseau).
- Visualisation via tableaux de bord détaillés et personnalisables.
- Forensic analytics pour retracer les attaques ou anomalies.
- Intégration native avec FortiGate, FortiManager et l'écosystème Fortinet.

- **FortiEMS** : Plateforme de gestion centralisée conçue spécifiquement pour FortiClient Endpoint Security. Elle permet aux administrateurs de déployer, configurer, surveiller et maintenir les endpoints (comme les ordinateurs portables, les postes de travail et les serveurs) depuis une console unique.

  Fonctionnalités principales :

- Déploiement et gestion centralisée de FortiClient (installation, mises à jour, configurations).
- Supervision de la sécurité des endpoints : antivirus, anti-malware, vulnérabilités, pare-feu applicatif, conformité.

- Contrôle d’accès réseau (ZTNA / VPN) : définit quelles machines sont autorisées à accéder au réseau selon leur état de sécurité.
- Gestion des vulnérabilités et remédiation automatisée.
- Tableaux de bord et rapports pour suivre l’état de santé du parc informatique.

- **FortiAuthenticator** : Solution centralisée d’authentification et de gestion des identités. Elle permet de contrôler l’accès des utilisateurs grâce à des mécanismes comme le RADIUS, LDAP ou l’authentification multi-facteur (MFA), assurant une sécurité renforcée et une intégration fluide avec les autres produits Fortinet (comme FortiGate et FortiClient).

Fonctionnalités principales :

- Gestion centralisée des identités (IAM) : comptes utilisateurs, groupes, certificats.
- Authentification forte (2FA/MFA) : tokens matériels, mobiles (FortiToken), SMS, email.
- Serveur RADIUS / LDAP intégré pour authentifier les accès aux réseaux et aux VPN.
- SSO (Single Sign-On) pour simplifier la connexion aux applications et services.
- Intégration native avec FortiGate, FortiSwitch, FortiAP et l’écosystème Fortinet.
- Gestion des certificats (CA interne) pour l’authentification par certificat.
- Contrôle d’accès basé sur l’identité pour renforcer la sécurité Zéro Trust.

Après avoir présenté le cadre conceptuel et les fondements techniques du SD-WAN ainsi que les critères ayant conduit au choix de la solution Fortinet, il est désormais pertinent de passer à la phase opérationnelle. Le chapitre suivant sera consacré à la mise en pratique de cette solution, depuis l’analyse de l’architecture existante jusqu’au déploiement, aux tests de performance et à la supervision centralisée. Cette transition marque ainsi le passage de l’étude théorique à l’application concrète sur le terrain.

CHAPITRE 3 . MISE EN ŒUVRE

Cette partie décrit la transition stratégique et opérationnelle de l'architecture réseau existante de PAMECAS vers une infrastructure SD-WAN moderne, agile et sécurisée. Elle détaille les étapes techniques, les outils de gestion et la méthodologie de déploiement.

3.1 Infrastructure réseau existante (PAMECAS)

L’architecture réseau de PAMECAS reposait sur une infrastructure classique de type LAN hiérarchisé, articulée autour de commutateurs Cisco et d’un cluster de pare-feux Fortigate assurant la sécurité périmétrique.

3.1.1 architecture et équipements

Le schéma ci-dessus illustre la structure logique des équipements et leurs interconnexions.

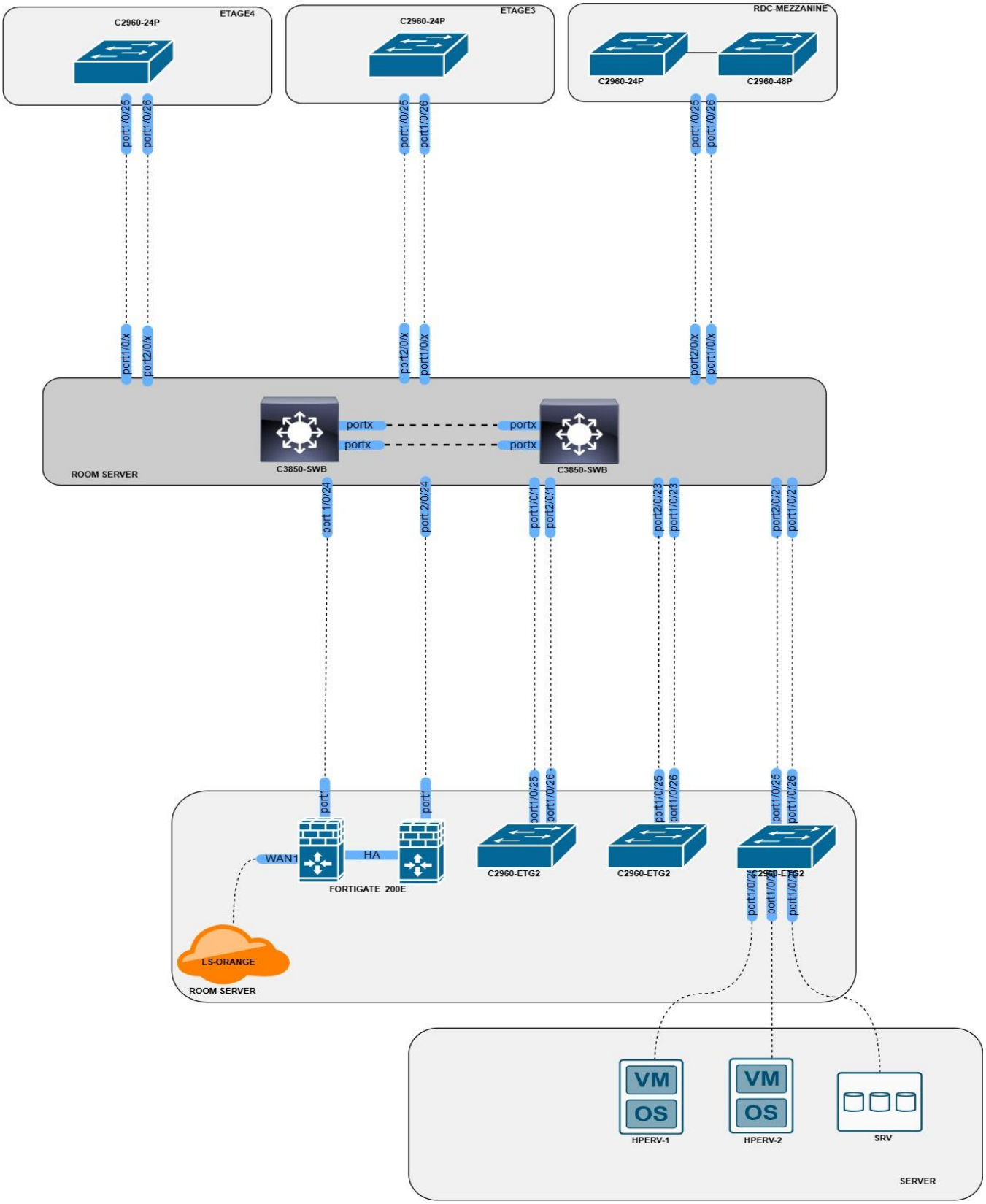


Figure 6 : Architecture existante

Le schéma illustre l'architecture réseau existante de PAMECAS avant toute modernisation, centrée autour du room server qui constitue le cœur du réseau. Les switches cœur C3850-SWB, interconnectés de manière redondante, agréent le trafic provenant des switches d'étage (C2960-24P et C2960-48P) situés aux étages 3, 4 et au RDC-Mezzanine, assurant ainsi la connectivité des postes utilisateurs et des équipements locaux. Les flux vers l'extérieur sont filtrés et sécurisés par les firewalls Fortigate 200E en haute disponibilité (HA), connectés au fournisseur d'accès LS-Orange pour la sortie WAN. La distribution interne vers les serveurs et machines virtuelles se fait via des switches C2960-ETG2, qui relient les serveurs physiques et les hyperviseurs (HPERV-1, HPERV-2), permettant l'accès aux services applicatifs internes. Cette architecture, de type centralisé, présente des avantages en termes de contrôle et de sécurité, mais elle expose également le réseau à des goulots d'étranglement et à une forte dépendance au room server pour la circulation du trafic interne et externe, tout en sachant que l'un des switches cœur n'était pas utilisé et que les deux switches au RDC-Mezzanine montés en cascade constituent une faille architecturale.

Voici un tableau clair et structuré regroupant tous les équipements présents dans l'architecture existante PAMECAS.

Tableau 1 : Récapitulatifs des équipements de l'architecture existante

Catégorie	Modèle / Type	Quantité	Localisation	Rôle / Fonction
Switches d'accès	Cisco C2960-24P	1	Étage 4	Accès utilisateurs, VoIP, Data
	Cisco C2960-24P	1	Étage 3	Accès utilisateurs
	Cisco C2960-24P	1	RDC	Accès utilisateurs
	Cisco C2960-48P	1	RDC / Mezzanine	Accès utilisateurs avec plus de ports
Switches Room Server	Cisco C2960 (ETG2)	2	Room Server	Distribution interne, serveurs, firewalls
Cœur de réseau	Cisco C3850	2	Room Server	Core/Distribution, inter-VLAN, agrégation
Sécurité périmétrique	Fortigate 200E (Cluster HA)	2	Room Server	Pare-feu, filtration, NAT, VPN, HA
Lien opérateur	Lien Internet (Orange)	1	Room Server	Accès Internet
Serveurs	Hyper-V Host HPERV-1	1	Salle Serveur	Virtualisation (VM)
	Hyper-V Host HPERV-2	1	Salle Serveur	Virtualisation (VM)
	Serveur de stockage (SRV)	1	Salle Serveur	Stockage, services internes

3.1.2 Analyse des points faibles

L'architecture actuelle fonctionne mais présente plusieurs limites :

- **Absence de redondance sur plusieurs segments critiques**

- Les commutateurs d'accès (C2960) ne sont pas redondés par étage : une panne coupe tout l'étage.
- Le lien opérateur (Orange) est unique : indisponibilité Internet en cas de coupure.

- **Architecture classique peu flexible et difficile à administrer**

- Le routage, la sécurité et les politiques QoS doivent être configurés manuellement sur plusieurs équipements.
- Pas d'orchestration centralisée : modifications lentes, risque d'erreurs.

- **Sécurité limitée à la frontière (périmètre)**

- Le Fortigate protège l'accès Internet, mais le LAN interne n'est pas segmenté finement.
- Absence de fonctions avancées comme :
    - Micro-segmentation,
    - Inspection applicative distribuée,

- **Performance limitée et dépendance aux équipements vieillissants**

- Les commutateurs Cisco 2960 sont anciens, non adaptés aux besoins modernes :
- Le routage interne repose sur un seul cluster de C3850 : montée en charge limitée.

3.2 Mise en œuvre de la solution SD-WAN

3.2.1 Mise en place des infrastructures

Cette phase consiste à déployer physiquement les nouveaux équipements.

3.2.1.1 Déploiement de la solution

La solution proposée utilisera des équipements du constructeur Fortinet.

L'avantage de cette solution homogène réside dans le management simplifié, qui se fait depuis l'interface graphique du Fortigate.

Ci-dessous la composante matérielle :

Tableau 2 : Récapitulatif des équipements de l'architecture cible

Catégorie	Equipement	Fonction
Pare-feu siège	2x FortiGate 200G (Master / Slave)	Sécurité périmétrique, SD-WAN multi-liens, haute disponibilité, VPN IPSec pour agences
Pare-feu agence	2x FortiGate 40F	Interconnexion SD-WAN sécurisée, VPN automatique vers le siège, ZTNA et posture de sécurité
Gestion centralisée	FortiManager (FMG)	Gestion centralisée des configurations et politiques
	FortiAnalyzer (FAZ)	Journalisation, rapports et analyse des logs
	FortiClient EMS (EMS)	Gestion des endpoints, conformité et ZTNA
	FortiAuthenticator (FAC)	MFA et authentification ZTNA
Switches	SW LAN Siège 1 & 2	Connexion utilisateurs, serveurs et VLAN segmentés
	BKB 1 & 2	Assurer le transit à très haut débit entre les segments critiques
	SW Serveur	Connectivité des pools de serveurs, séparation des services critiques
Wi-Fi	FortiAP / SSID Guest	Accès Wi-Fi invité isolé, gestion via FortiGate
Serveur	Pool Serveur	Hébergement des services internes, séparation par fonction, micro-segmentation via VDOM SRV

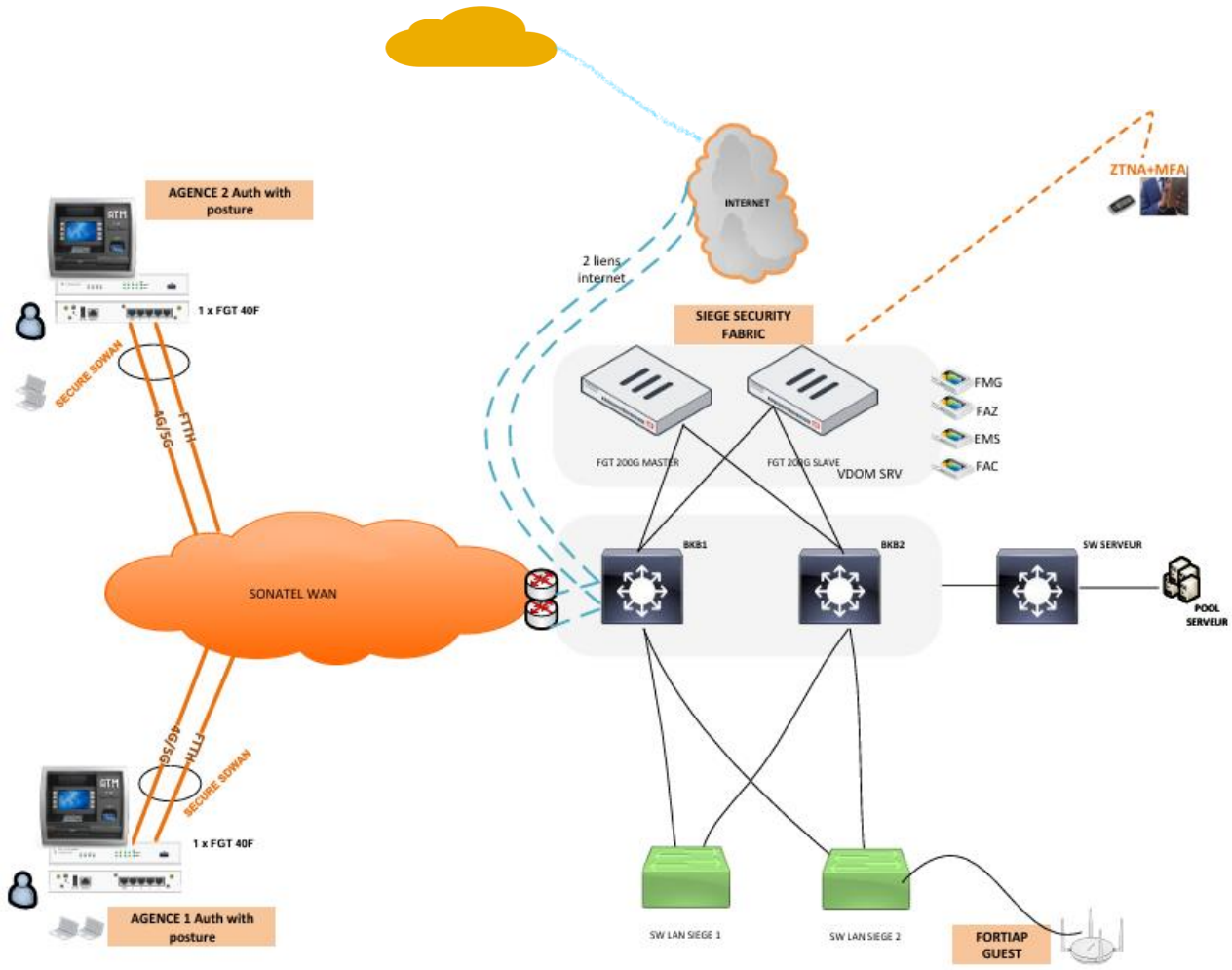


Figure 7 : Architecture cible

L'architecture cible mise en place pour PAMECAS représente une évolution stratégique majeure par rapport à l'infrastructure réseau existante. Elle s'appuie sur une approche Secure SD-WAN intégrée à la Security Fabric de Fortinet, afin de répondre aux exigences croissantes en matière de sécurité, de performance, de résilience et de gestion centralisée.

Au cœur de cette architecture se trouve un cluster de pare-feux FortiGate 200G en haute disponibilité (Master / Slave) installé au siège. Ce cluster assure à la fois la sécurité périmétrique et la fonction SD-WAN, en exploitant simultanément deux liens Internet fournis par SONATEL. Grâce à une sélection dynamique basée sur des indicateurs de qualité de service (latence, pertes, gigue), le trafic est optimisé et la continuité de service est garantie en cas de défaillance d'un lien ou d'un équipement.

L’architecture est intégrée à un écosystème de gestion centralisée, composé de FortiManager, FortiAnalyzer, FortiClient EMS et FortiAuthenticator. Cet ensemble permet une administration unifiée des équipements, une supervision avancée, une gestion des postes utilisateurs ainsi qu’une authentification forte basée sur le principe du Zéro Trust Network Access (ZTNA). Ainsi, l’accès aux ressources est conditionné à l’identité et à la conformité des utilisateurs, réduisant considérablement les risques de compromission.

Le réseau local du siège est structuré autour de switches d’accès et d’un pool de serveurs segmenté, avec une séparation logique des flux via des VLAN et un VDOM dédié aux serveurs. Cette segmentation renforce la sécurité interne, limite la propagation des menaces et permet l’application de politiques spécifiques selon la criticité des services. L’infrastructure LAN à haut débit assure une performance optimale pour les applications métiers et les services hébergés.

L’architecture de PAMECAS intègre une connexion sécurisée au cloud, permettant l’accès à des services hébergés via le Secure SD-WAN de Fortinet. Les environnements cloud sont reliés de manière sécurisée au siège et aux agences, tout en appliquant des politiques de sécurité centralisées, garantissant flexibilité, contrôle et conformité.

Les agences distantes sont interconnectées au siège au moyen de pares-feux FortiGate 40F, intégrés nativement au SD-WAN. Les tunnels VPN IPsec sont automatiquement établis (deux VPN), offrant une communication sécurisée, fiable et centralisée. Cette approche simplifie l’exploitation des sites distants tout en garantissant un niveau de sécurité homogène sur l’ensemble du réseau.

En définitive, l’architecture cible proposée transforme le réseau de PAMECAS en une plateforme moderne, sécurisée et évolutive, capable de soutenir les activités actuelles et futures de l’institution. Elle améliore significativement la disponibilité des services, renforce la sécurité globale et facilite la gestion opérationnelle, tout en s’inscrivant dans une logique d’optimisation des coûts et d’agilité organisationnelle.

3.2.2 Déploiement opérationnel

3.2.2.1 Installation et configuration des équipements

- Configurations initiales

Dans les configurations initiales, les équipements sont mis à jour puis les licences sont activées et enregistrées chez Fortinet.

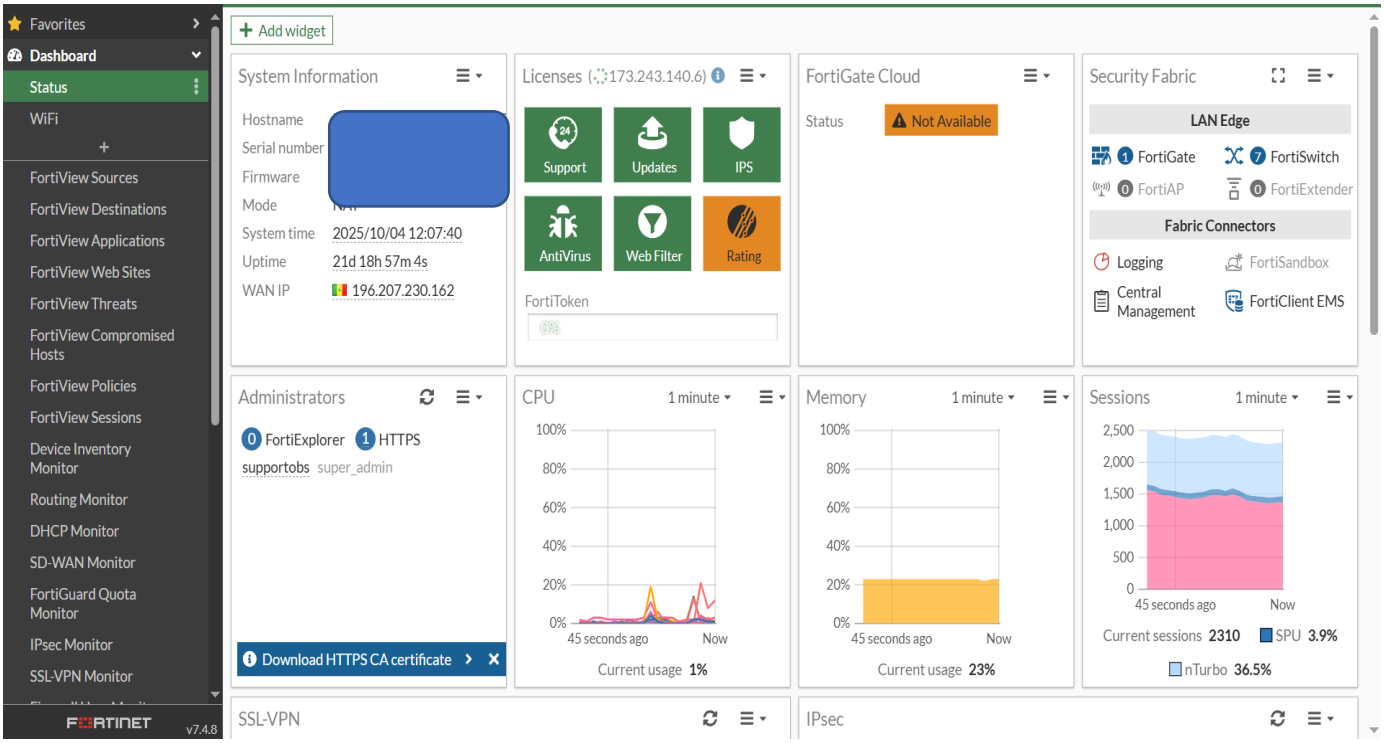


Figure 8 : Dashboard FortiGate

- Configuration HA (High Availability)

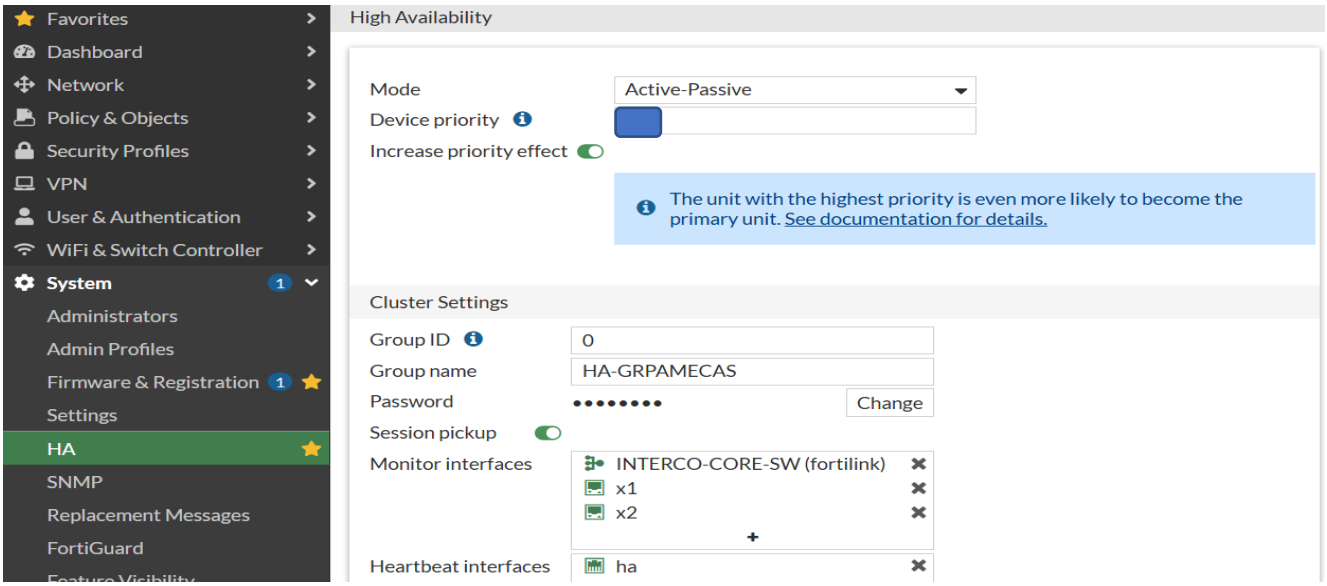


Figure 9 : Configuration HA

- Configuration des interfaces

La première configuration concerne les interfaces du Fortigate. Nous avons sept zones principales :

- LAN : regroupe le sous-réseau local des utilisateurs, les postes de téléphones IP, imprimantes et le Wi-Fi pour le personnel.
- ADMIN : comporte l'interface vlan pour les utilisateurs admin
- SRV : regroupe les interfaces dédiées aux serveurs
- MNGT : qui comporte les interfaces de management
- BCEAO : où il y a l'interconnexion en liaison physique avec le FortiGate du partenaire
- PIFSN-GSIE : où il y a l'interface d'interco du partenaire GSIE
- GUEST-WIFI : qui regroupe le SSID pour les invités ;

Il y a aussi des zones SDWAN créées :

- INTERNET : agrège les liens Internet pour un débit mieux optimisé et une redondance ;
- VPN : pour une redondance et haute disponibilité vers le site principal et vers les partenaires.

Le LAN appelé Zone LAN ici, est composé des Vlans Utilisateurs, Wifi printer, LAN printer et la voix.

Le fortilink 'INTERCO_SW_CORE agrège deux ports physiques vers le Fortiswitch pour une haute disponibilité et une bande passante de deux gigas bits de trafic entre les backbones et le FortiGate.

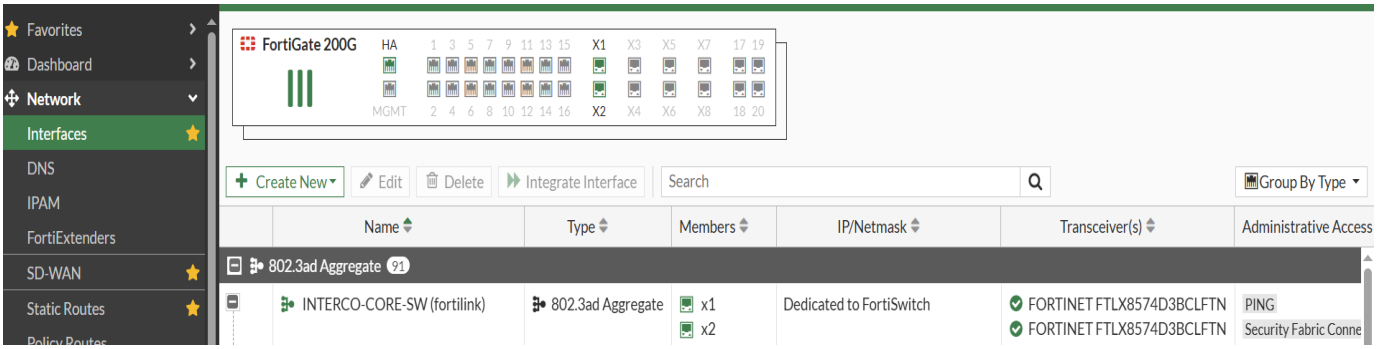


Figure 10 : Interco fortigate-switchcore

Sous cette agrégation, qui est en réalité un trunk, nous configurons toutes les interfaces passerelles des VLANs, comme dans l'exemple du LAN-SIEGE ci-dessous :

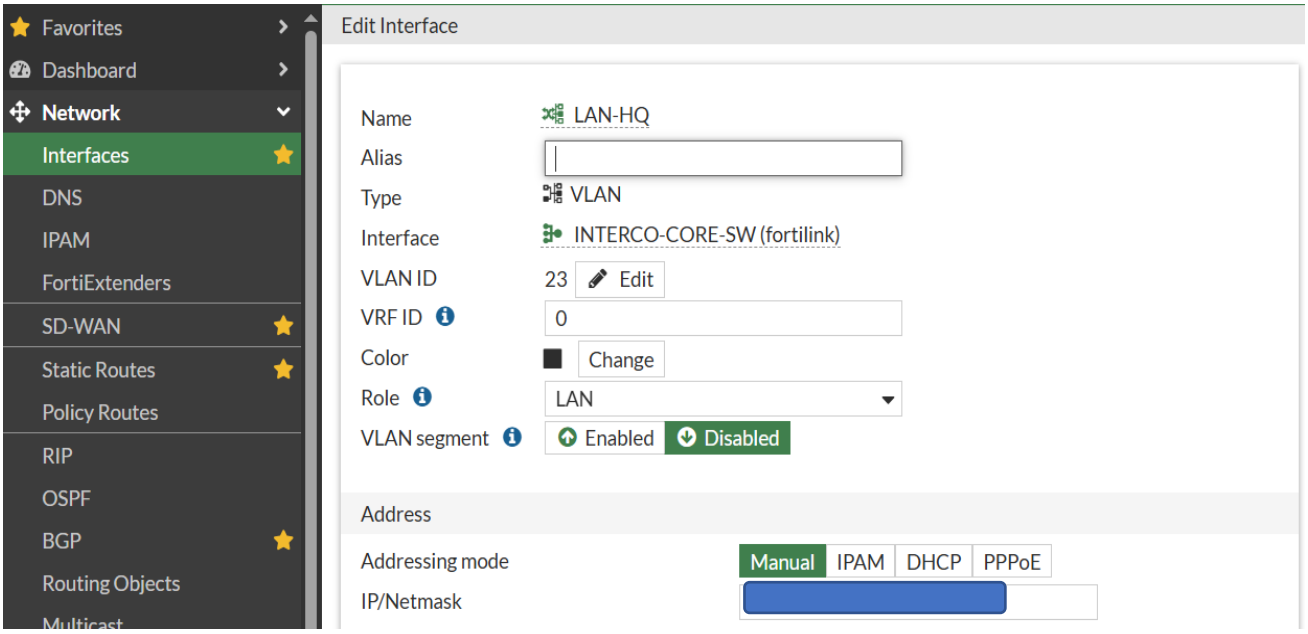


Figure 11 Configuration interface vlan

Le nom et l'ID de VLAN sont renseignés, en même temps que l'adresse de la passerelle, et les options du serveur DHCP pour la distribution des adresses aux points d'accès de ce sous-réseau.

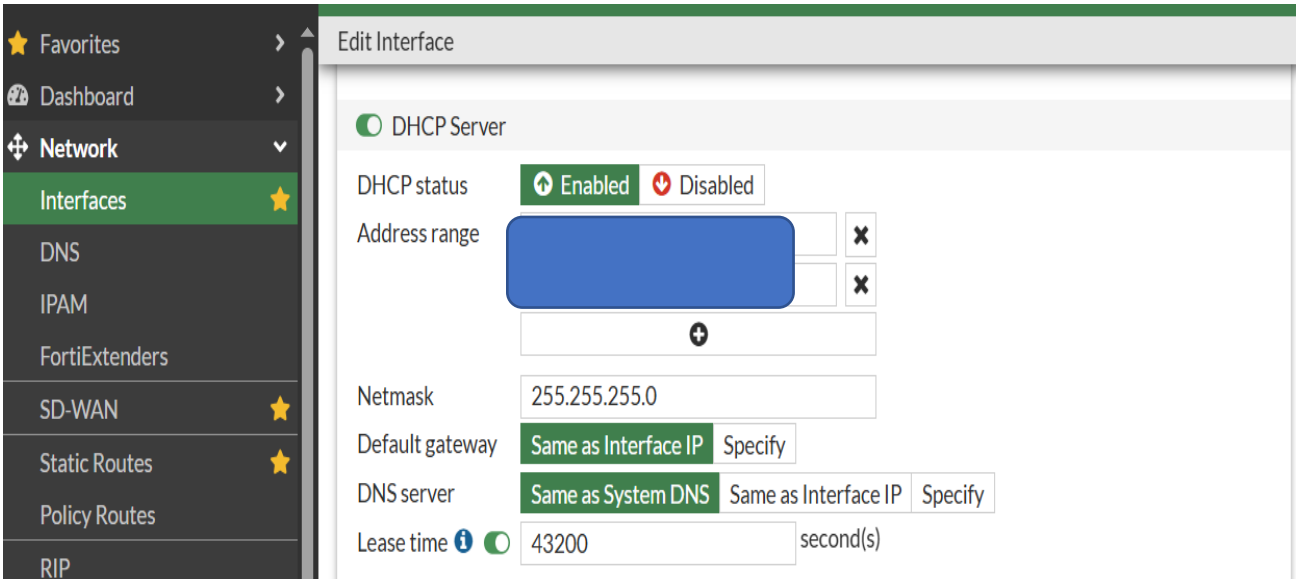


Figure 12 : Configuration serveur DHCP

Et enfin de la même manière, le Vlan voix configuré comme suit, de même aussi le service DHCP est géré par le FortiGate.

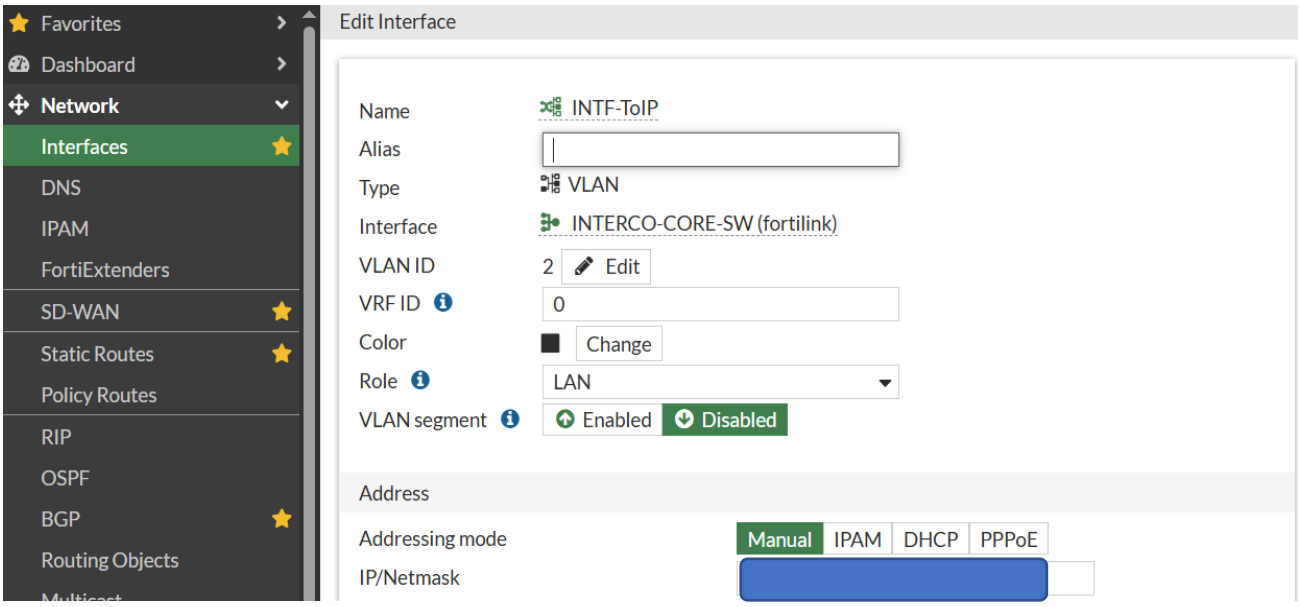


Figure 13 : Configuration interface vlan téléphonie

- Configuration des SSIDs :

NB : C'est juste des configurations standard, qui n'ont pas était encore validé par le client puis qu'il n'avait pas encore soldé tous les prérequis (câblage, méthode d'authentification etc.) pour le déploiement du wifi

Dans cette partie, nous configurerons les différents SSIDs pour la connexion Wifi.

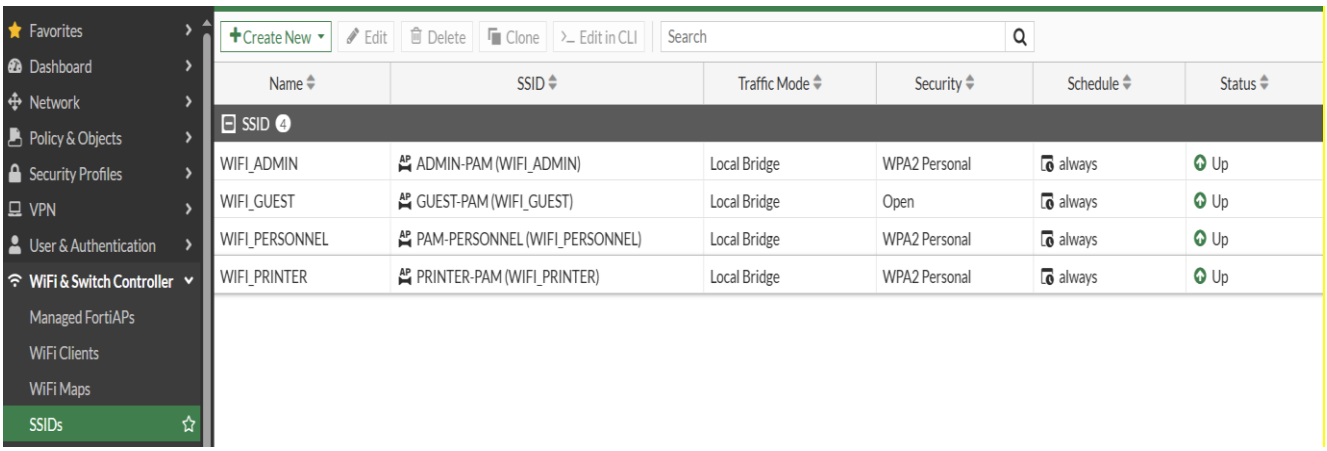


Figure 14 : SSIDs

Ensuite, donner un nom au wifi, définir le type d'authentification qui sera utilisée selon la politique de sécurité de l'organisme. Sur ce cas, nous avons utilisé l'authentification à clé partagée.

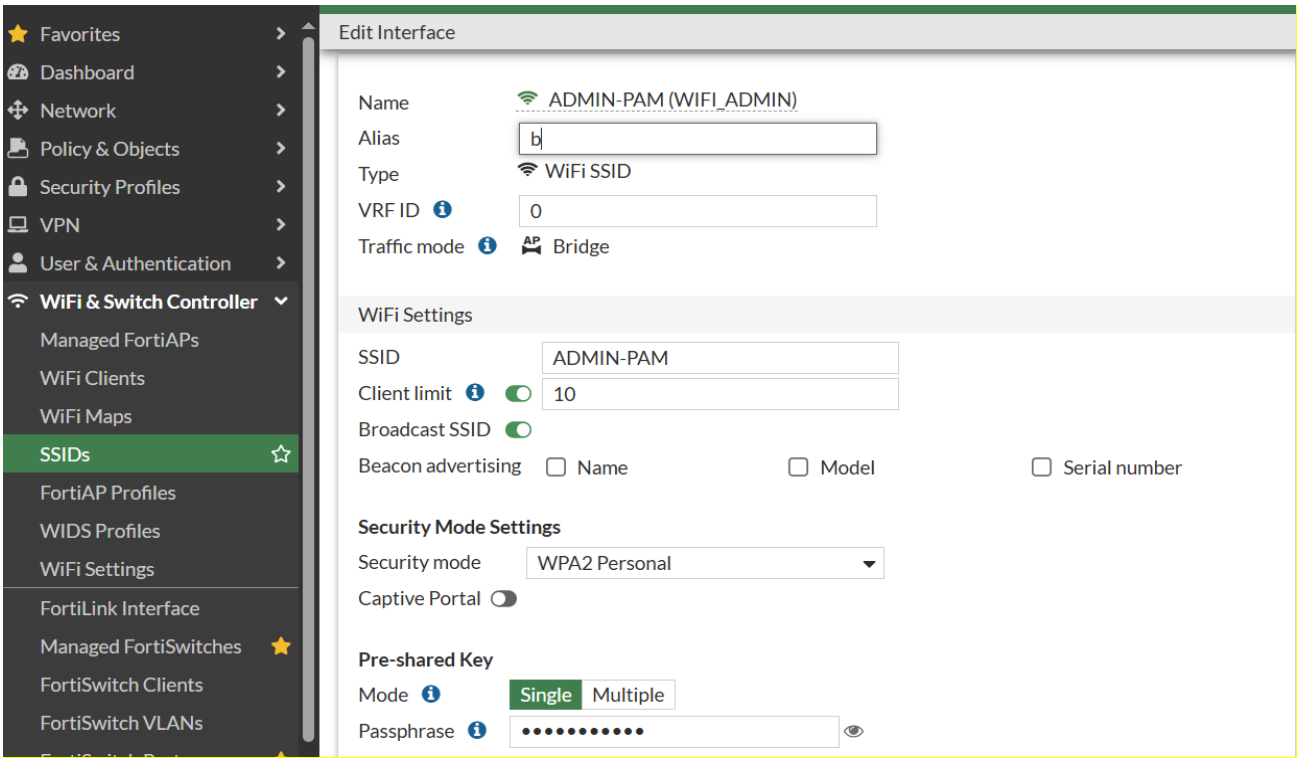


Figure 15 : Configuration des SSIDs

Enfin, définir l'ID du vlan rattaché à cet SSID afin que les utilisateurs puissent obtenir dynamiquement une IP de connexion.

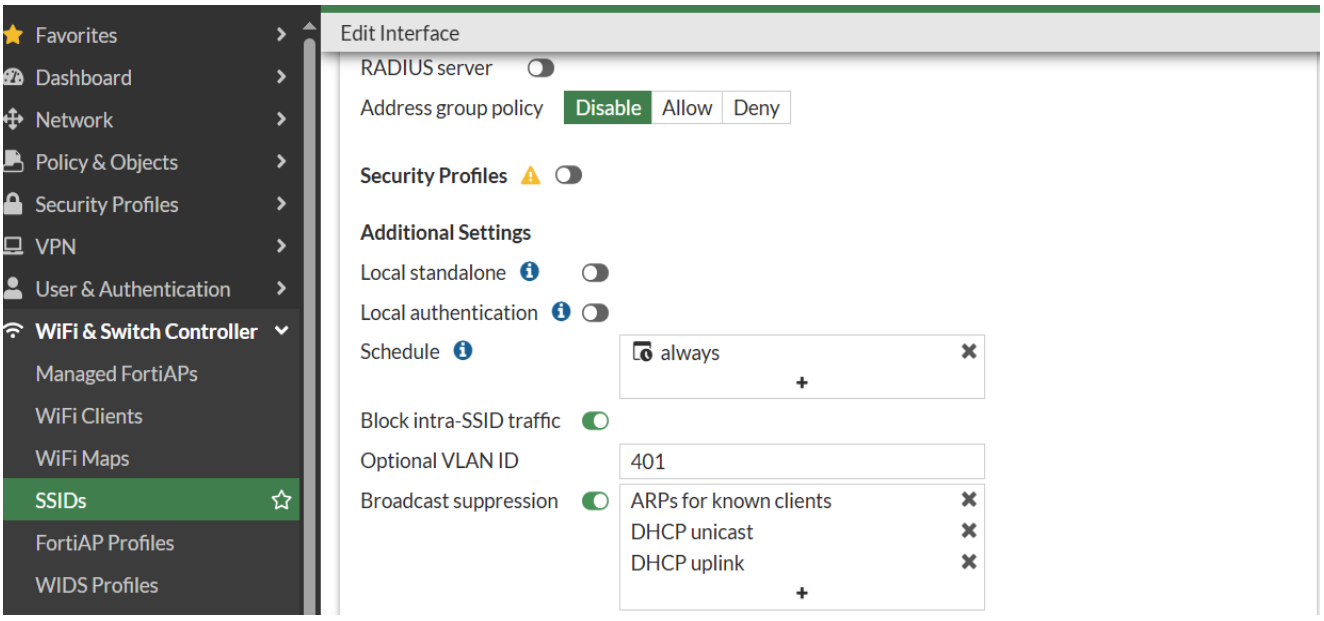


Figure 16 : option vlan ID

- Service DNS (Domain Name System)

Il existe un serveur DNS en interne, donc celui-ci est renseigné en tant serveur primaire pour la résolution de noms, suivi d'un serveur public. Le nom de domaine local peut être également renseigné.

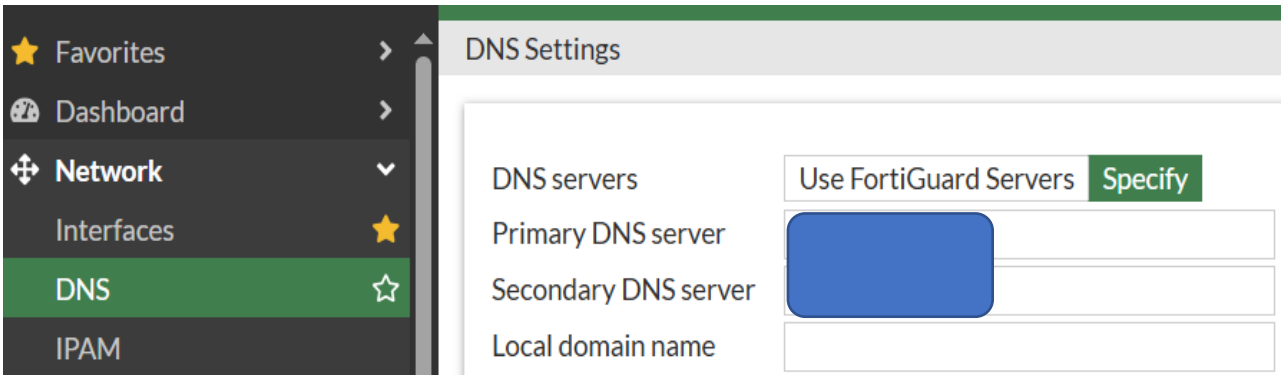


Figure 17 : Configuration des serveurs DNS

- Partage de charge Internet

A l'état actuel, nous avons deux liaisons internet (une LS-Orange et une FTTH).

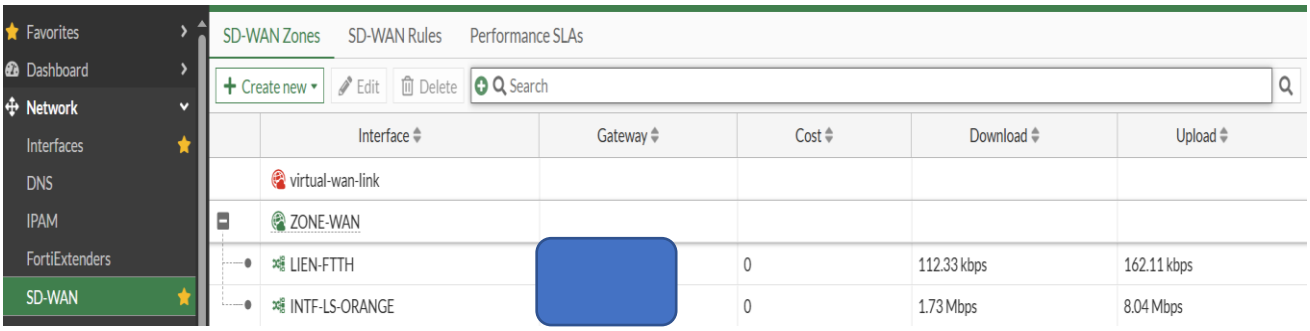


Figure 18 : SDWAN_INTERNET

La section Performance SLA permet de tracker la disponibilité des liens membres du SDWAN, en envoyant dessus des paquets répétitifs et en comparant les temps de réponse, paquets perdus etc. Cela permet d'avoir en temps réel l'efficacité de chaque lien et sa disponibilité, et ainsi de mettre à jour la table de routage partagée par ces liens.

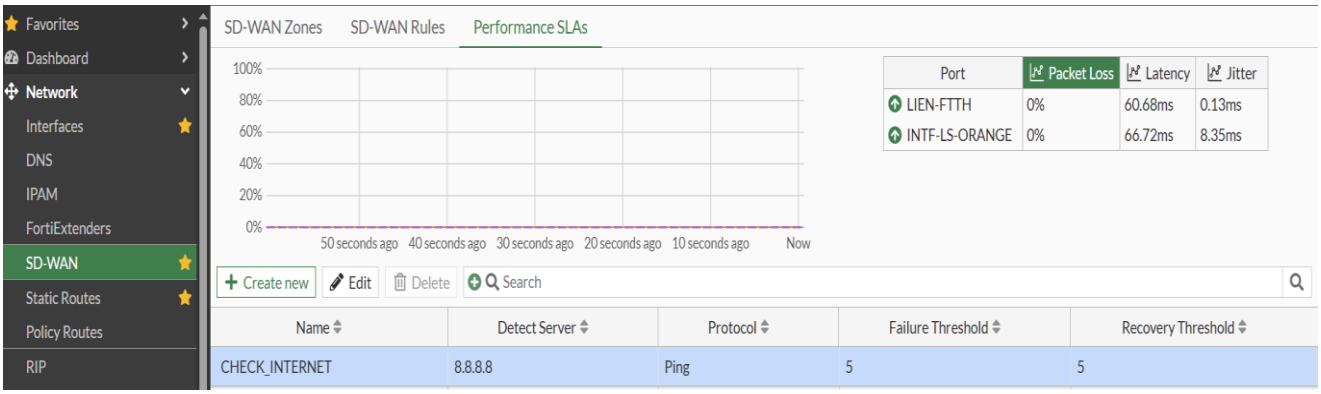


Figure 19 : Performance SLA

- Routage

Il existe une route par défaut vers Internet, avec comme interface de sortie la zone INTERNET.

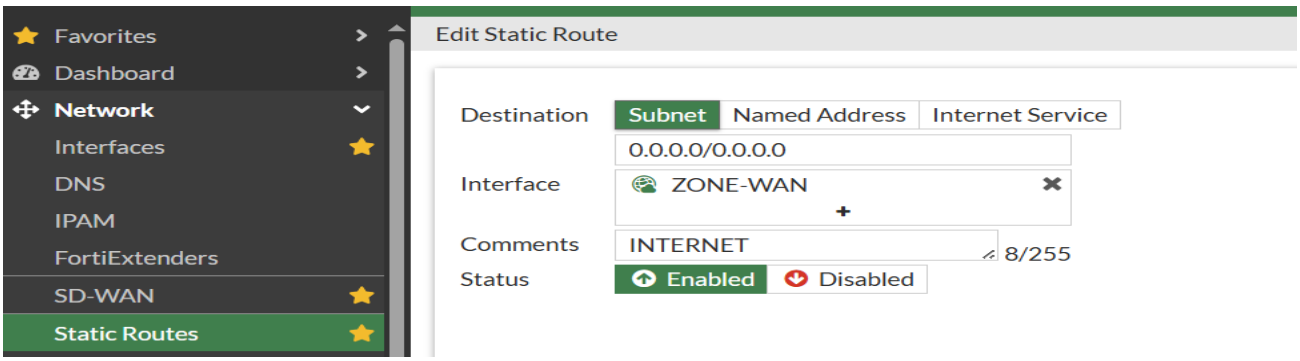


Figure 20 : Routage vers internet

Aussi pour une communication entre le siège, ces partenaires et les agences, il faut définir des routes vers les destinations spécifiques en choisissant l'interface de sorti vers la destination souhaitée.

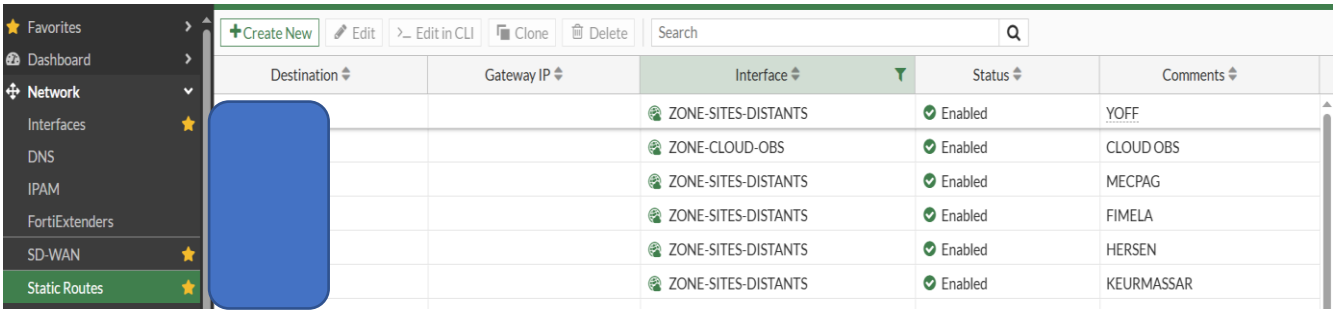


Figure 21 : Routage vers sites distants – Partenaires

- Profils de sécurité

Les profils de sécurité définissent les éléments à inspecter dans le trafic transité par FortiGate. Lorsque le trafic correspond au profil, il est soit autorisé, bloqué ou surveillé (autorisé et enregistré).

- Filtrage Web et Applicatif

Les filtrage web et applicatif sont appliqués à un certain flux vers Internet, pour optimiser la bande passante en limitant l'accès aux ressources qui consomment le plus de bande passante, mais également pour protéger le réseau interne et les serveurs.

Le filtre web fait des limitations par catégorie d'URLs, mais sait aussi créer des exceptions, comme sur les captures suivantes :

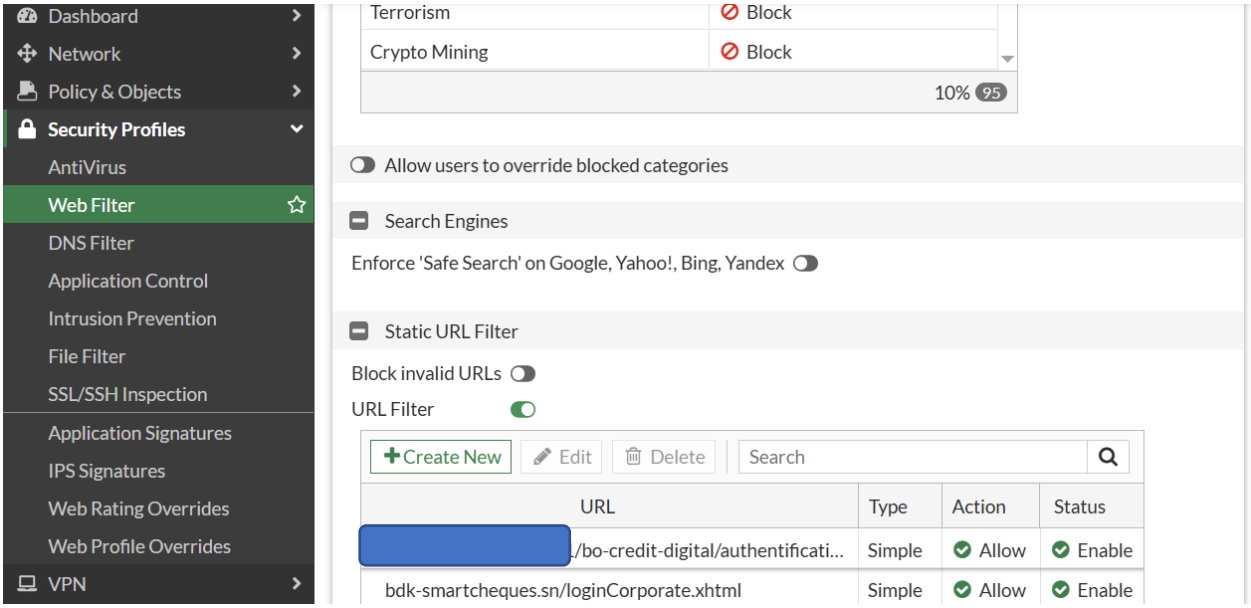


Figure 22 : Filtrage web

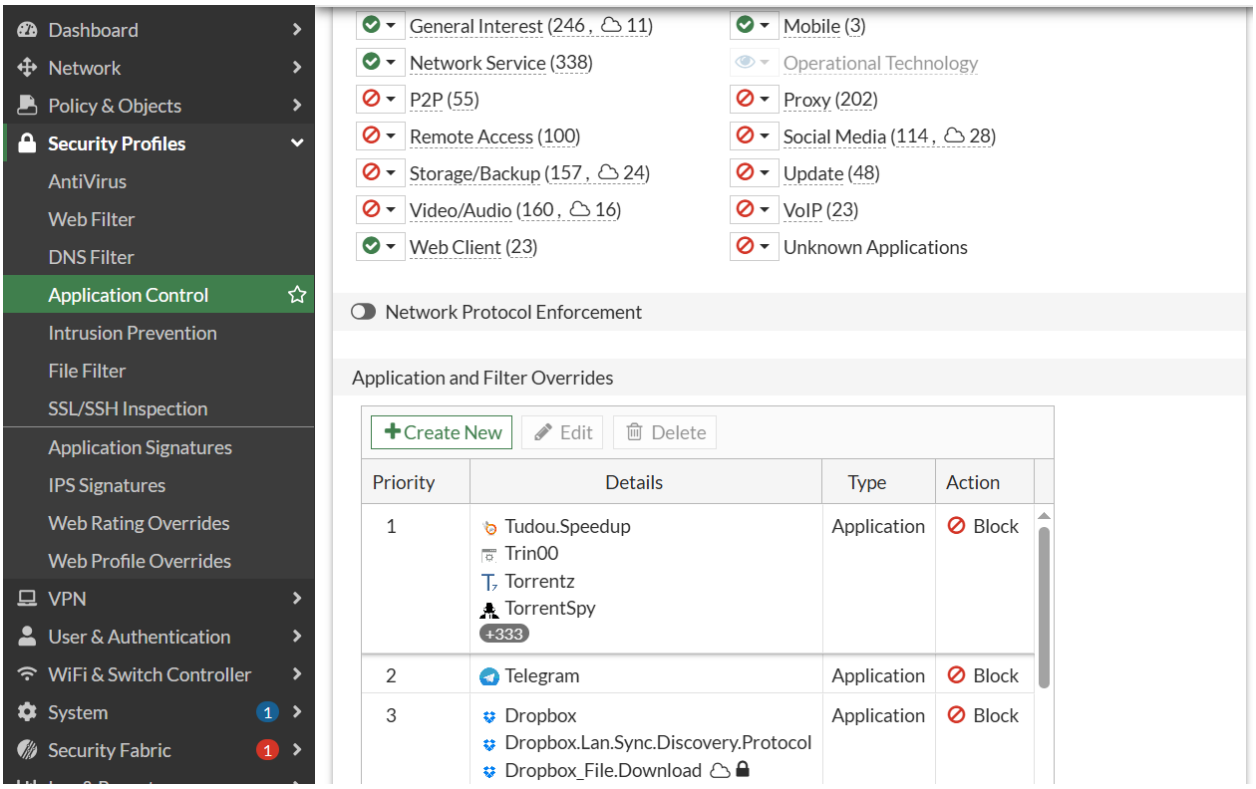


Figure 23 : Filtrage applicatif

Le filtrage est très flexible et peut être ajusté à tout moment, à l'aide des flux observés dans les journaux de logs, et grâce à l'expérience des utilisateurs.

Ce filtre sera plus tard appliqué au niveau des polices IPv4. Il est laissé à l'appréciation de PAMECAS pour son affinement et sa mise en œuvre une fois la politique de sécurité appliquée.

- Polices IPv4

Tout trafic non explicitement autorisé à ce niveau, ne transitera pas le pare-feu. Que ce soit du trafic vers Internet, depuis Internet, ou inter VLAN.

Une police IPv4 c'est : une interface d'entrée, une interface de sortie, un sous-réseau source, un sous-réseau destinataire, une plage horaire, des services, des profils de sécurité, etc.

Il est plus pratique de d'abord déclarer tous les sous-réseaux et hôtes auxquels nous ferons appel dans cette section.

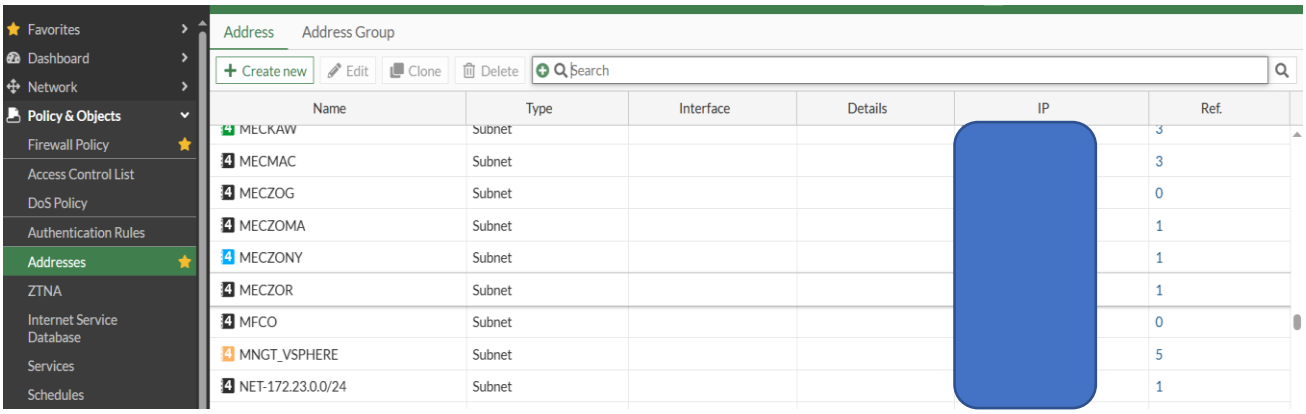


Figure 24 : Objets

Une adresse ce n'est pas qu'un sous-réseau. Les options sont multiples.

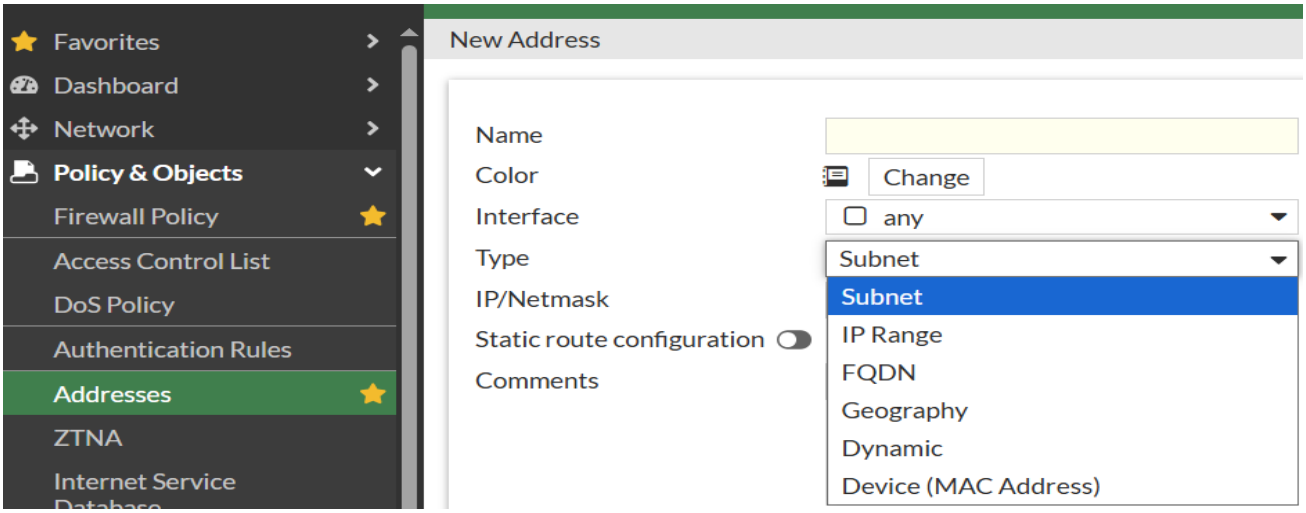


Figure 25 : Types d'objets

Avec tous les objets prêts à être référencés, les polices IPv4 peuvent être créées pour commencer à générer du flux.

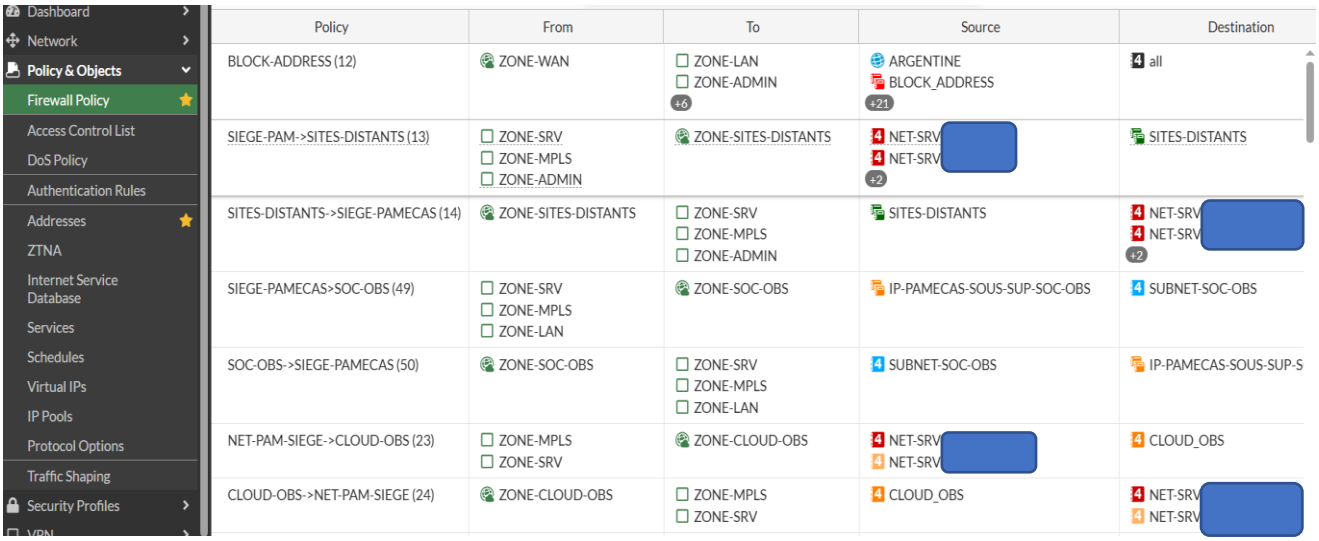


Figure 26 : Policy ipv4

Le trafic vers Internet quitte le réseau ZONE-LAN vers la ZONE-WAN

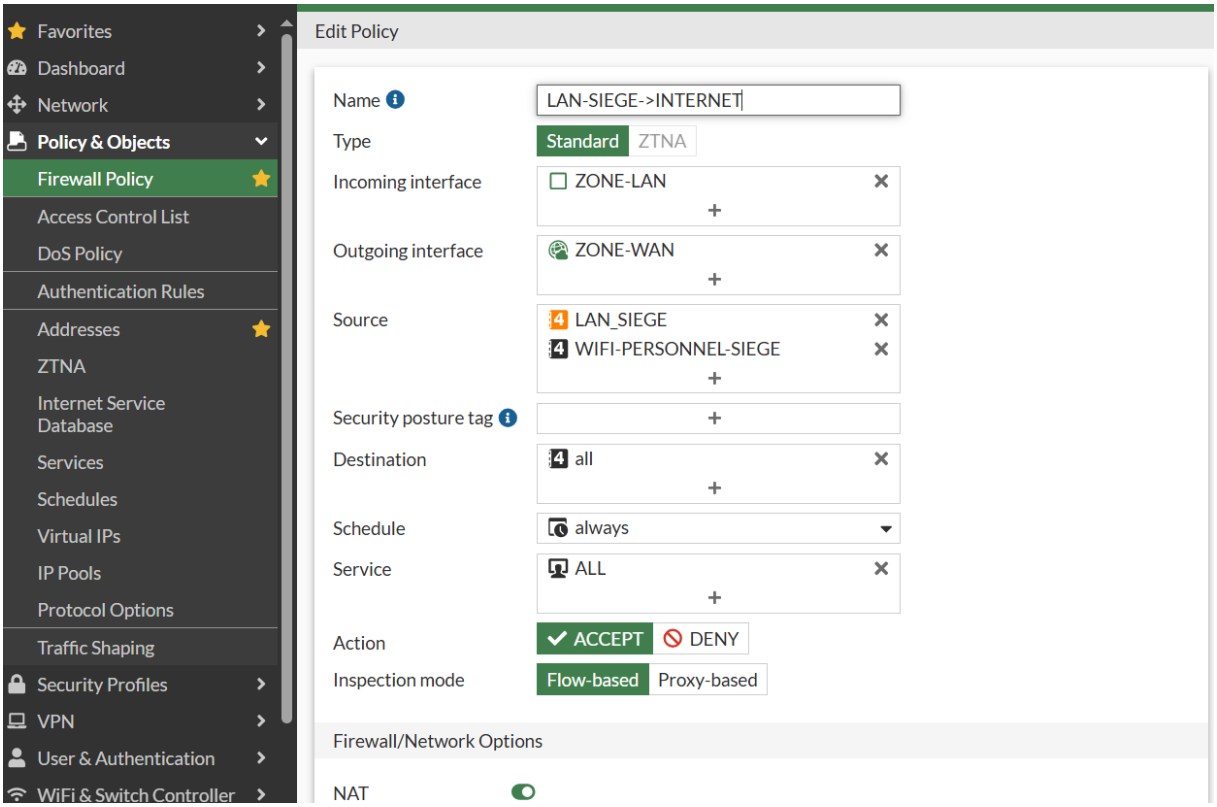


Figure 27 : Policy vers internet

Une ouverture de flux est effectuée entre le siège et ses différents sites distants et les partenaires est nécessaire pour la communication puisse être établie avec ces sites.

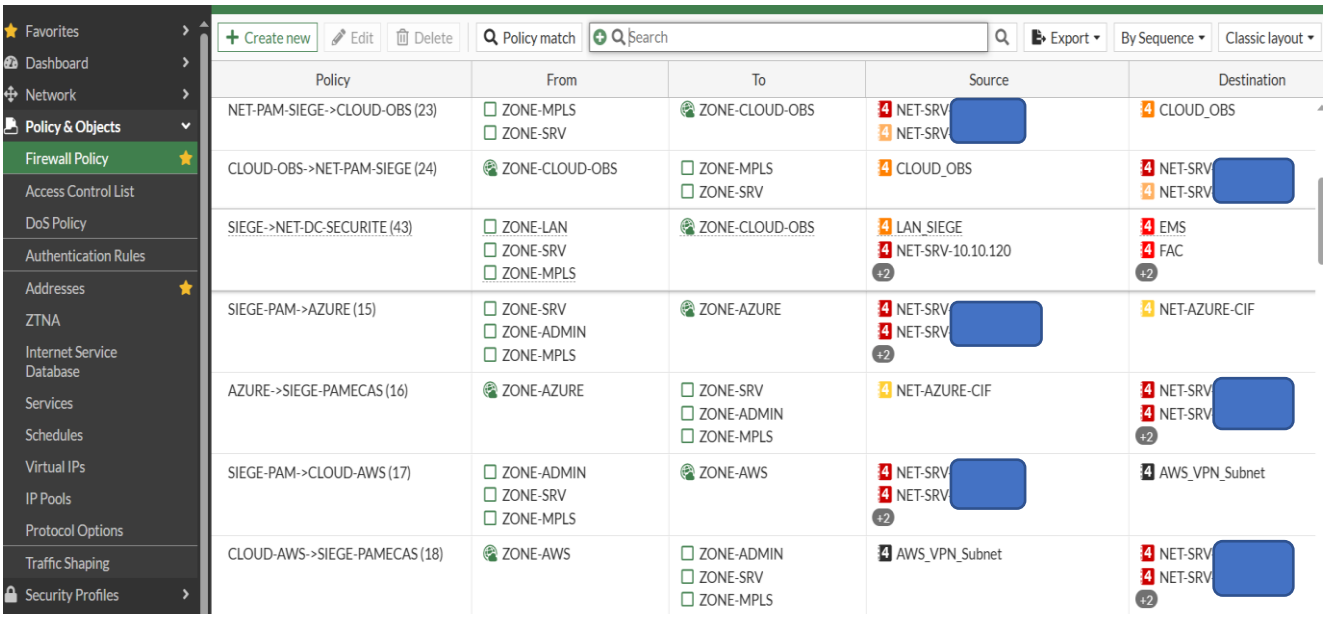


Figure 28 : Policy vers partenaires

- Configuration de l'accès distant par VPN IPSEC

Un tunnel VPN IPSEC est établi entre le site principal et les sites distants afin de permettre aux utilisateurs, admins et supports d'accéder aux ressources dédiées en dehors du réseau internet.

Cet accès se crée en trois étapes.

D'abord, les interfaces entrantes qui sont les liaisons Internet sont ajoutées ainsi que les adresses IP publiques qui sont sur le siège pour assurer la disponibilité d'accès aux ressources internes des sites distants.

La méthode d'authentification sur Clé pré-partagée est choisie. Cette clé pré-partagée constitue un identifiant pour le VPN qui sera renseigné sur le siège et le site distant, un Peer-id et local-id spécifique pour tunnel.

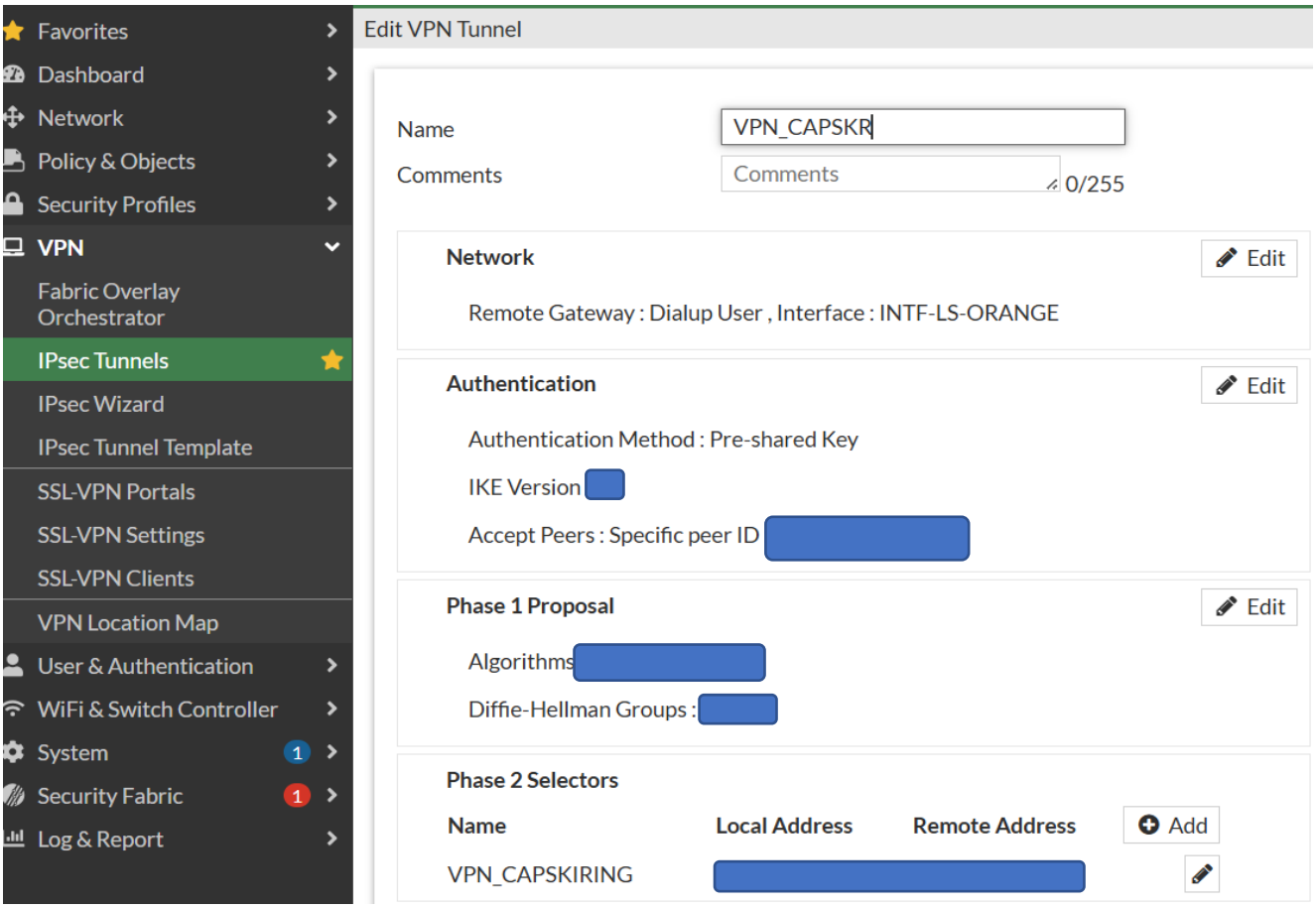


Figure 29 : VPN IPsec

Ensuite au niveau de SDWAN est configurée une règle qui permet une communication sécurisée vers les distants.

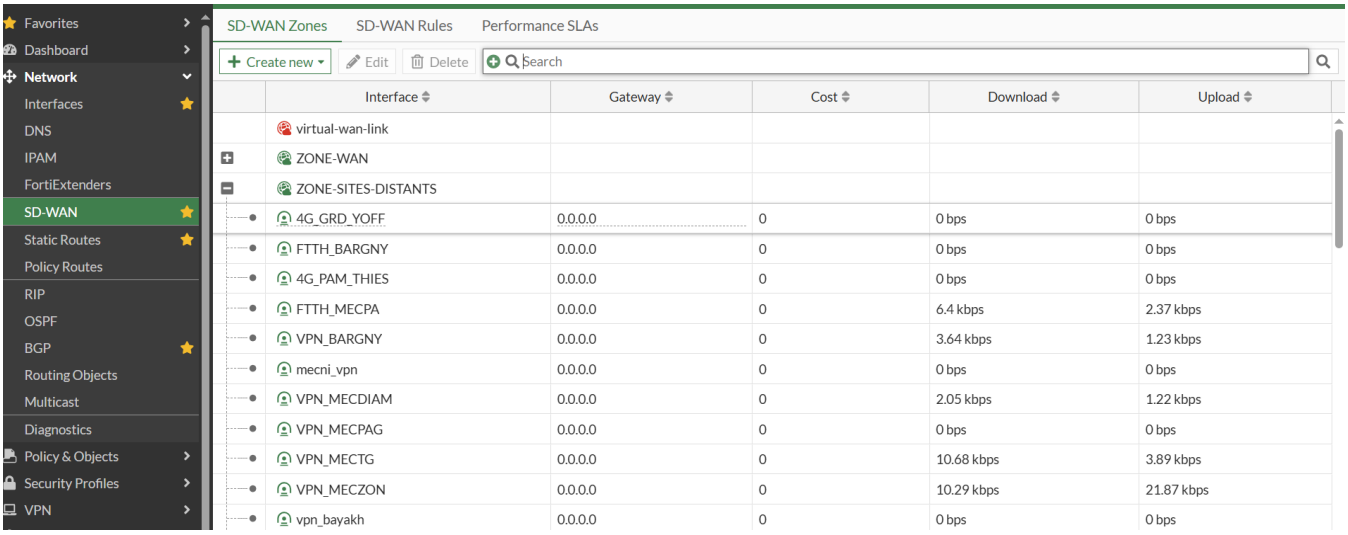


Figure 30 : Ajout des tunnels IPsec dans une zone SDWAN

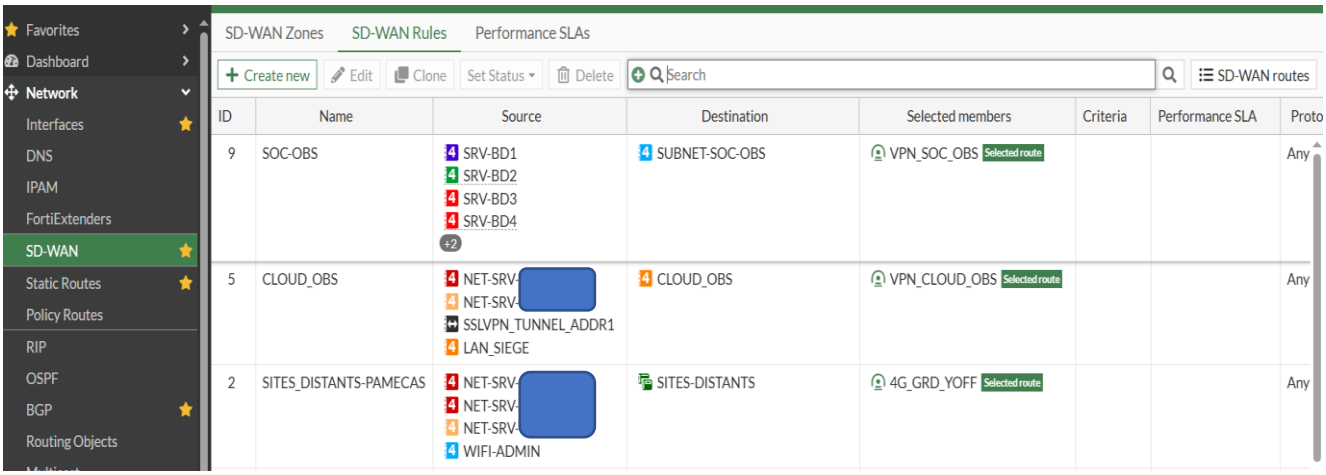


Figure 31 : SDWAN Policy vers sites distants et partenaires

Enfin deux règles de pare-feu ont été créés pour autoriser le flux de trafic IPsec bidirectionnel sur le tunnel VPN .

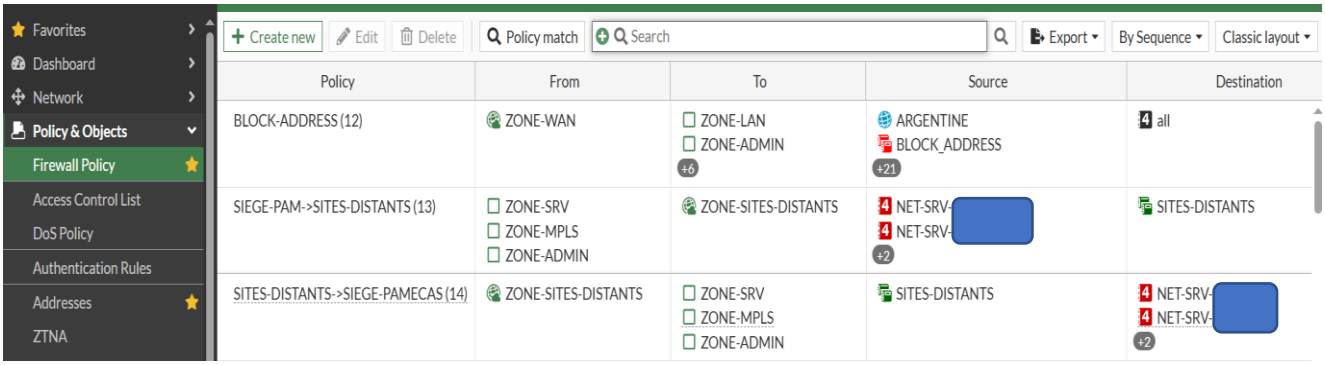


Figure 32 : Policy entre siège – sites distants

3.2.3 Supervision et gestion centralisée

Le SD-WAN introduit une couche de gestion unifiée qui simplifie radicalement les opérations.

3.2.3.1 Gestion centralisée (FortiManager)

FortiManager est un outil permettant de centraliser, d'automatiser et d'améliorer la gestion de leurs infrastructures de sécurité Fortinet.

L'intégration du fortigate sur la plateforme se fait comme suit :

- Dans l'onglet « Fabric Connectors », éditer « Central Management »
- Cliquer sur « Enabled », choisir « On-Premises et renseigner l'adresse IP du serveur
- Valider par « OK »

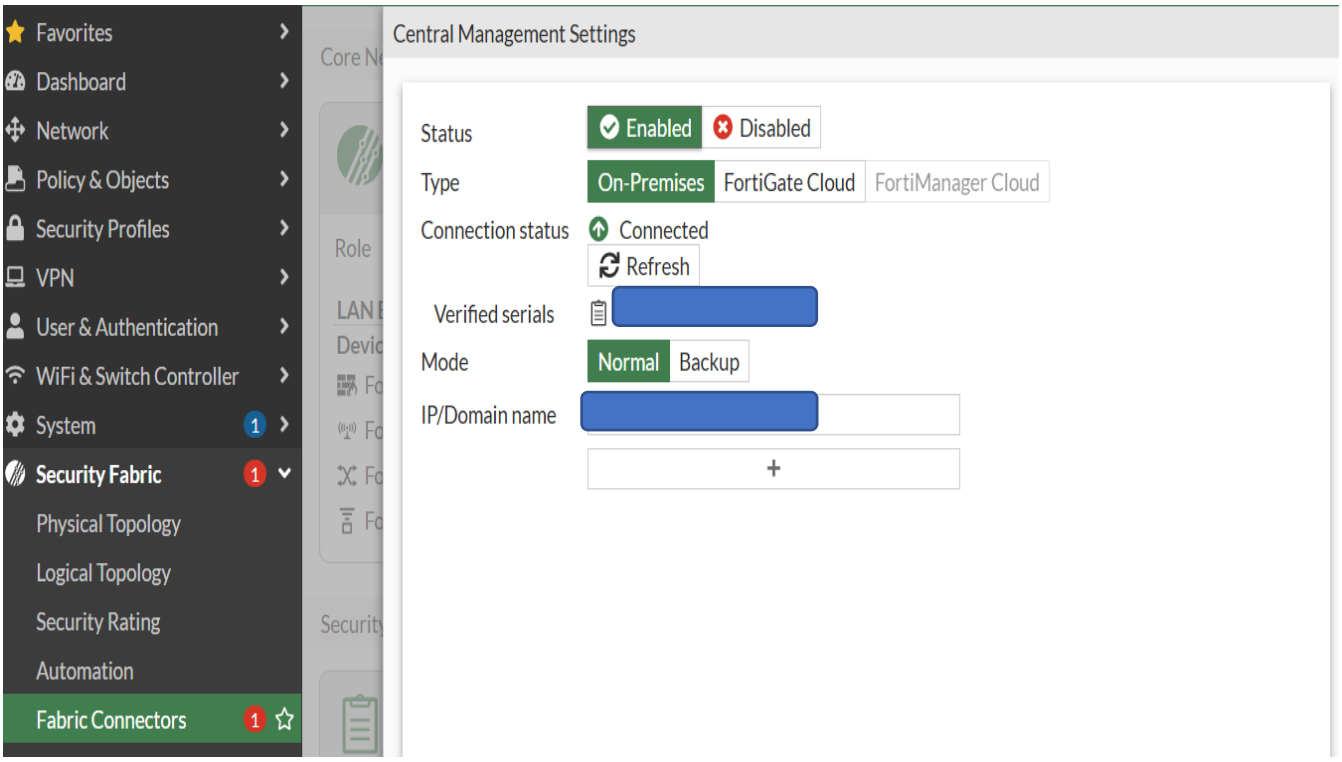


Figure 33 : FortiManager

3.2.3.2 Centralisation des logs (FortiAnalyzer)

FortiAnalyzer est un puissant outil pour les entreprises cherchant à améliorer leur posture de sécurité grâce à une gestion centralisée des journaux, une analyse avancée des menaces, et des capacités robustes de reporting et de conformité.

L'intégration du fortigate sur la plateforme se fait comme suit :

- Dans l'onglet « Fabric Connectors », éditer « Logging & Analytics »
- Cliquer sur « Enabled », renseigner l'adresse du serveur et valider par « OK »

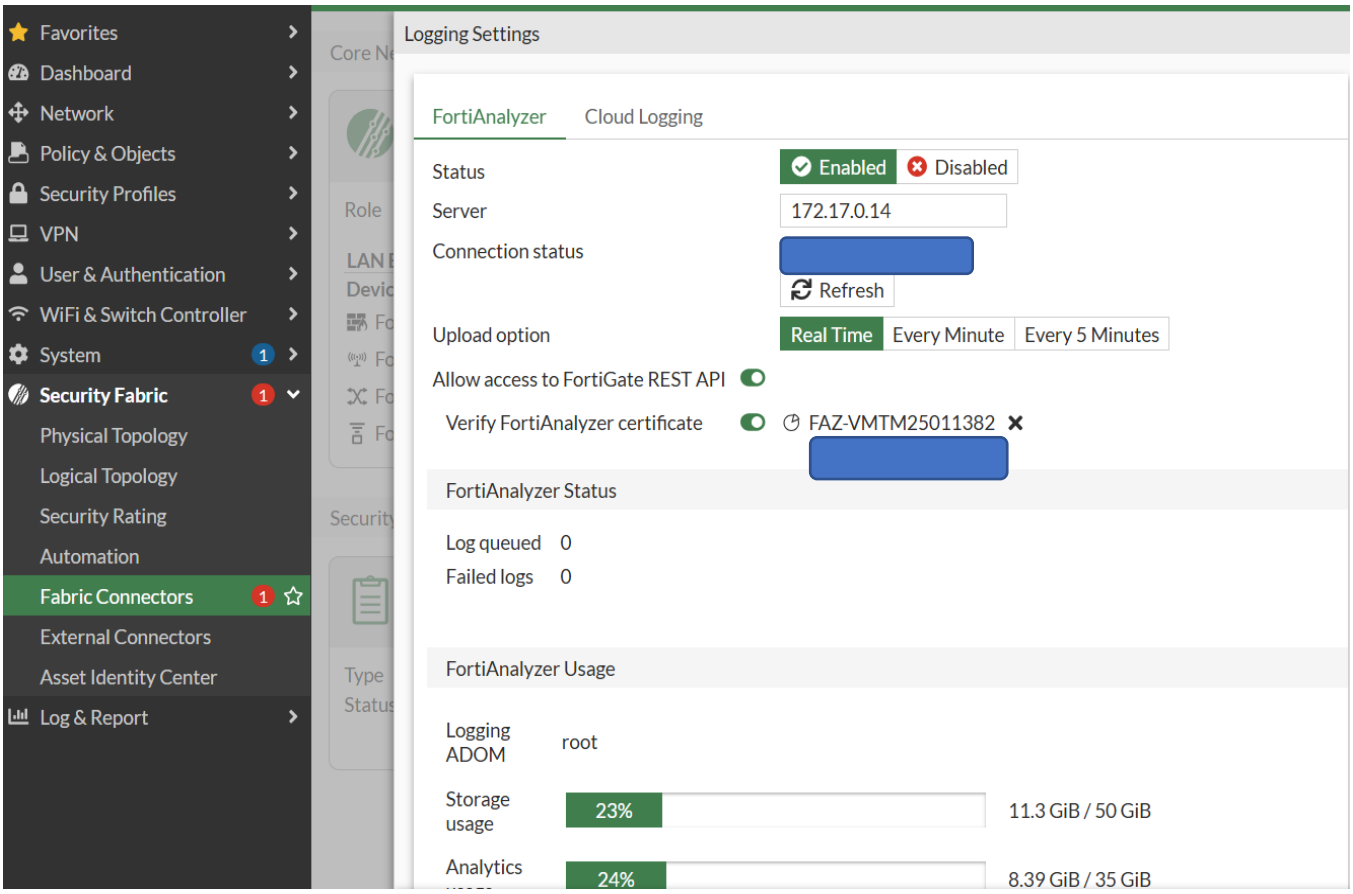


Figure 34 : FortiAnalyzer

3.2.3.3 Gestion des Endpoints (FortiEMS)

FortiEMS (Endpoint Management Server) est une plateforme centralisée de Fortinet destinée à la gestion, la protection et le contrôle des postes de travail (endpoints). Elle permet d'administrer les agents FortiClient installés sur les machines des utilisateurs.

L'intégration du fortigate sur la plateforme se fait comme suit :

- Dans l'onglet « Fabric Connectors », éditer « FortiClient EMS »
- Cliquer sur « Enabled », renseigner l'adresse du serveur EMS et valider par « OK »

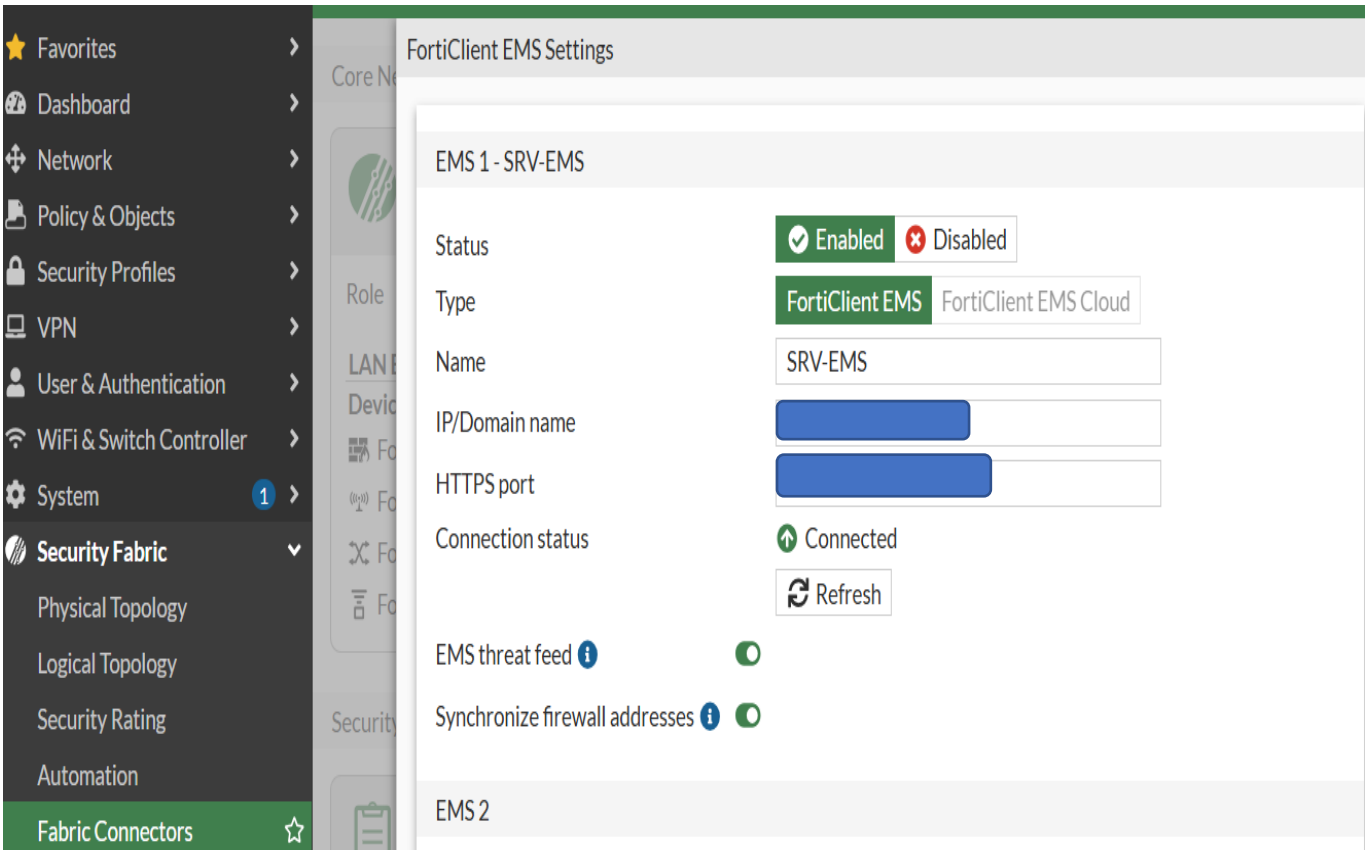


Figure 35 : FortiEMS

3.3 Difficultés rencontrées

Au cours de la phase de mise en œuvre de la nouvelle architecture réseau, plusieurs difficultés techniques et organisationnelles ont été rencontrées. Certaines de ces contraintes ont impacté la planification initiale, tandis que d'autres ont nécessité des ajustements sur le terrain pour garantir la réussite du projet.

- **Repérage et identification des câbles / liens existants**

L'une des premières difficultés rencontrées a été liée au repérage des câbles réseau et des liens opérateurs dans les différents locaux techniques. Ce qui a rendu un peu difficile l'identification du cheminement des liens WAN/MPLS.

Cette situation a entraîné un temps d'intervention supplémentaire, ainsi qu'une nécessité de procéder à des tests manuels pour valider chaque lien avant intégration dans la nouvelle architecture.

- **Intégration de la téléphonie IP non prévue dans l'architecture initiale**

Une autre difficulté importante réside dans le fait que la téléphonie IP n'avait pas été anticipée dans l'architecture de départ. Cela a impliqué non seulement la nécessité de revoir le schéma d'adressage et de VLAN mais aussi la reconfiguration de certains ports pour séparer la voix et les données.

- **Câblage en charge du client**

La partie câblage était entièrement à la charge du client et qui a un peu pris du temps, ce qui a fait que le câblage n'était pas finalisé à temps. Cette dépendance externe a parfois retardé les travaux et créé une interférence avec la planification globale du projet.

- **Difficulté d'accès et état des locaux techniques secondaires**

Certains équipements se trouvaient dans des locaux techniques secondaires, notamment dans des pièces annexes, locaux serrés. Ces contraintes ont prolongé les interventions, notamment lors des tests de continuité, des diagnostics de câblage et de l'installation de nouveaux équipements.

Plusieurs locaux techniques présentaient également des problèmes de climatisation insuffisante ou instable. Ces limitations environnementales ont nécessité une coordination avec le service infrastructure afin d'assurer des conditions thermiques minimales pour le fonctionnement du matériel.

CONCLUSION

Le déploiement de la solution Secure SD-WAN s'inscrit dans une dynamique de modernisation et d'optimisation d'une infrastructure réseau. L'étude menée a permis d'identifier les limites du modèle WAN traditionnel basé sur le MPLS, notamment au regard de la montée des usages cloud, de la nécessité de garantir une meilleure continuité de service et de la volonté de réduire les coûts opérationnels. L'analyse de l'architecture existante a constitué un socle essentiel pour comprendre les enjeux et orienter le choix de la solution technologique la mieux adaptée.

La mise en œuvre de la solution SD-WAN, appuyée par les équipements et services de l'écosystème Fortinet, a démontré son efficacité à répondre aux besoins identifiés. Grâce au routage intelligent, à la gestion centralisée et à l'intégration native de la sécurité, le réseau gagne en performance, en flexibilité et en résilience. Les phases d'installation, de configuration et de tests menées au siège et en agences ont permis de valider la pertinence technique de l'approche, malgré les difficultés rencontrées sur le terrain telles que le câblage, l'accès aux locaux techniques ou l'intégration de la téléphonie IP non prévue initialement.

En définitive, cette transformation réseau constitue une étape stratégique importante. Elle permet d'assurer une meilleure qualité de service aux utilisateurs, de sécuriser efficacement les communications et de disposer d'une infrastructure capable d'accompagner la croissance future de l'organisation. Les résultats obtenus témoignent de la réussite du projet et confirment la valeur ajoutée d'une architecture SD-WAN bien intégrée, tant sur le plan technique qu'opérationnel.

À l'avenir, cette dynamique pourra être renforcer en élargissant progressivement le SD-WAN à un ensemble de sites et en intégrant davantage de fonctionnalités avancées. L'adoption d'un modèle SASE (Secure Access Service Edge), l'automatisation des politiques de sécurité ou encore l'optimisation continue des flux applicatifs représentent des pistes d'amélioration majeures.[4] Ces évolutions permettront à l'organisation de disposer d'une infrastructure encore plus agile, sécurisée et adaptée aux nouveaux défis numériques, tout en soutenant efficacement les besoins métiers et l'évolution des services digitaux.

BIBLIOGRAPHIE/WEBOGRAPHIE

[1] « Introduction aux réseaux SD-WAN : définition et principes de base - Insyncom ». Disponible sur: https://www.insyncom.fr/actualite/introduction-aux-reseaux-sd-wan-definition-et-principes-de-base

[2] « Notre histoire < Bienvenue sur le site officiel du Groupe Sonatel, 1er Opérateur Groupe Sonatel 1er Opérateur de téléphonie ». Disponible sur: https://sonatel.sn/groupe-sonatel/notre-histoire/

[3] « Formation ISN - Généralités sur les Réseaux », www.google.com. Disponible sur: https://www.google.com/imgres?imgurl=https://math.univ-lyon1.fr/irem/Formation_ISN/formation_reseau/reseaux_generalites/images/wan.jpg&imgrefurl=https://math.univ-lyon1.fr/irem/Formation_ISN/formation_reseau/reseaux_generalites/generalites.html&h=377&w=574&tbnid=U7AAPIDFip5Y1M&source=sh/x/im/can/1&usg=AI4_-kRY1v2tfrJCyQwboWzQ7P4bZODsGw&vet=1&docid=BJxd6Wu-BRs20M&sfr=vfe

[4] « SD-WAN et MPLS face à l'émergence du SASE (Avis d'expert) », Win. Disponible sur: https://www.win.be/fr/blog-news/sd-wan-et-mpls-vers-lobsolescence-face-au-sase

[5] « l3 vpn mpls », Bing. Disponible sur: https://www.bing.com/images/search?q=l3+vpn+mpls&FORM=HDRSC3

[6] « placer-le-sd-wan-au-coeur-des-problematiques-reseaux.pdf ». Disponible sur: https://itsocial.fr/wp-content/uploads/2019/06/placer-le-sd-wan-au-coeur-des-problematiques-reseaux.pdf

[7] « SD-WAN sécurisé ». Disponible sur: https://docs.fortinet.com/sdwan/7.6

[8] « Fortinet Secure SD-WAN (Français) », Udemy. Disponible sur: https://www.udemy.com/course/fortinet-secure-sd-wan-francais/