SUP'COM
المدرسة العليا للمواصلات بتونس
Ecole Supérieure des Communications de Tunis
Higher School of Communications of Tunis

جامعة قرطاج
Université de Carthage

2025

RAPPORT DE STAGE

Formation humaine

Réalisé par: EZZINE Montassar

Encadré par: TARHOUNI Monji

TOPNET

Résumé

Ce document présente une vue d'ensemble détaillée du stage de formation humaine effectué au sein de l'entreprise TOPNET.

Il s'inscrit dans le cadre d'un projet de conception et de déploiement d'une architecture réseau sécurisée, reliant plusieurs sites à l'aide de VPN et de pare-feux.

En raison de certaines contraintes, notamment la limitation de temps, le projet a été orienté vers la réalisation d'un prototype fonctionnel, permettant de proposer une solution concrète et évolutive.

Ce rapport propose ainsi une analyse approfondie de l'entreprise ainsi qu'une description complète des travaux réalisés, tant sur le plan technique que sur le plan humain, en mettant en valeur les compétences techniques acquises, ainsi que le développement des aptitudes relationnelles et organisationnelles.

Remerciements

C'est avec une profonde gratitude que j'écris ces mots pour exprimer ma reconnaissance envers toutes les personnes qui ont contribué, de près ou de loin, à la réalisation de ce travail. Je leur adresse mes remerciements les plus sincères.

Je tiens tout particulièrement à remercier Monsieur Monji TARHOUNI, mon encadrant technique, pour m'avoir accueilli au sein de TOPNET, pour m'avoir offert l'opportunité de réaliser ce stage, et pour son accompagnement bienveillant tout au long de cette expérience professionnelle. Je lui suis reconnaissant pour la clarté de ses explications, la mise à disposition de toutes les ressources nécessaires, ainsi que pour les précieuses méthodes d'organisation et de documentation qu'il m'a transmises.

Je ne saurais oublier de remercier chaleureusement l'ensemble de l'équipe de TOPNET pour leur collaboration, leur disponibilité et leur esprit d'équipe, ainsi que toutes les personnes ayant, de près ou de loin, contribué à la réussite de ce projet.

Mes remerciements s'adressent également à l'ensemble de mes enseignants de l'École Supérieure des Communications de Tunis , SUP'COM, pour la qualité de leur enseignement et leur accompagnement tout au long de l'année académique 2024/2025.

Enfin, j'adresse ma reconnaissance aux membres du jury, en espérant que ce rapport saura répondre à leurs attentes en termes de clarté, de rigueur et de motivation.

Table des matières

Liste des abréviations **vi**

Introduction générale **1**

1 Cadre général du projet **3**

1.1 Introduction 3

1.2 Présentation de l'organisme d'accueil 3

1.2.1 Présentation de TOPNET 3

1.2.2 Domaines d'activités 4

1.2.3 Valeurs et engagements de TOPNET 5

1.3 Présentation du projet 5

1.3.1 Contexte du projet 5

1.3.2 Problématique 6

1.3.3 Etude et critique de l'existant 6

1.3.3.1 Fortigate 6

1.3.3.2 Cisco 891F 9

1.3.3.3 Etude comparative des solutions VPN 9

1.3.4 Solution proposée 10

1.4 Méthodologie de travail 11

1.4.1 Les méthodes séquentielles (en cascade) 11

1.4.2 Variantes des méthodes séquentielles 11

1.4.3 Méthode adoptée : En cascade 12

1.5 Conclusion 13

2 Analyse préliminaire et planification **14**

2.1 Introduction 14
2.2 Présentation de l'équipe 14
2.3 Capture des besoins 14
2.3.1 Besoins fonctionnels 14
2.3.2 Besoins non fonctionnels 15
2.4 Analyse préliminaire des besoins 16
2.4.1 Identification des acteurs 16
2.4.2 Diagramme de cas d'utilisation global 17
2.4.3 Vue architecturale 18
2.4.3.1 Architecture physique 18
2.4.3.2 Architecture logique 19
2.5 Environnement de travail 21
2.5.1 Environnement matériel 21
2.5.2 Environnement logiciel 22
2.6 Conclusion 24

3 Configuration des équipements de l'architecture réseau proposée 25
3.1 Introduction 25
3.2 Étapes de la configuration 25
3.2.1 Étape I : Configuration des routeurs Cisco 891F 25
3.2.2 Étape II : Configuration des pare-feu Fortigate 28
3.2.2.1 Fonctionnalités et concepts de sécurité avancés pouvant être appliqués sur chaque site : 30
3.3 Conclusion 31

4 Établissemnt du tunnel VPN 32
4.1 Introduction 32
4.2 Présentation du Tunneling 32
4.3 Étapes de configuration du VPN IPsec 33
4.3.1 Phase 1 : IKE Gateway 33
4.3.1.1 Configuration : phase 1 33
4.3.2 Phase 2 – IPsec Tunnel : Protection du trafic métier 35
4.3.2.1 Présentation consolidée des concepts et termes clés 35

4.3.2.2 Configuration : phase 2 36
4.4 Conclusion 37

5 Tests et validation de la configuration 38
5.1 Introduction 38
5.2 Présentation de l'architecture du test 38
5.3 Test de la connectivité 40
5.3.1 Vérification du fonctionnement du tunnel VPN 42
5.4 Conclusion 46

Conclusion générale et perspectives 48

Nétographie 49

Liste des abréviations

- **ADSL** : Asymmetric Digital Subscriber Line
- **ASIC** : Application-Specific Integrated Circuit
- **DMZ** : Demilitarized Zone
- **DPI** : Deep Packet Inspection
- **ESP** : Encapsulating Security Payload
- **FSI** : Fournisseur de Services Internet
- **GPON** : Gigabit Passive Optical Network
- **IA** : Intelligence Artificielle
- **IKE** : Internet Key Exchange
- **IKE SA** : IKE Security Association
- **IOT** : Internet of Things
- **IPS** : Intrusion Prevention System
- **LAN** : Local Area Network
- **NAT** : Network Address Translation
- **NGFW** : Next-Generation Firewall
- **OSPF** : Open Shortest Path First
- **PFS** : Perfect Forward Secrecy
- **SASE** : Secure Access Service Edge
- **SD-WAN** : Software-Defined Wide Area Network
- **SPF** : Shortest Path First
- **SSL** : Secure Sockets Layer
- **TIC** : Technologies de l'Information et de la Communication
- **TLS** : Transport Layer Security
- **VDSL** : Very-high-bitrate Digital Subscriber Line
- **VPN** : Virtual Private Network
- **VPS** : Virtual Private Server
- **WAN** : Wide Area Network
- **ZTNA** : Zero Trust Network Access

Table des figures

1.1 Logo de TOPNET 4
1.2 Logo de Tunisie Télécom 4
1.3 Logo de Fortigate 7
1.4 Logo de Fortinet 7
1.5 Présentation matérielle de la série Cisco 890 [4] 9

2.1 Diagramme des cas d'utilisation 18
2.2 Prototype d'une architecture réseau multisites sécurisée avec VPN et pare-feux 19
2.3 Fonctionnement logique de l'architecture réseau multisites 20

3.1 Câble Ethernet USB vers RJ45 26
3.2 Logo du terminal MobaXterm 26

5.1 Fonctionnement logique de l'architecture réseau multisites 39
5.2 Réussite du ping entre PC-Site-II et l'interface LAN du FG2 40
5.3 Réussite du ping entre PC-Site-II et l'interface WAN du FG2 41
5.4 Réussite du ping entre PC-Site-II et l'interface WAN du FG1 41
5.5 Réussite du ping entre PC-Site-II et l'interface LAN du FG1 41
5.6 Réussite du ping entre PC-Site-II et PC-Site-I 42
5.7 Surveillance du trafic de l'architecture à l'aide de l'outil ntopng 43
5.8 Création de la connexion Netcat côté PC-Site-II 44
5.9 Création de la connexion Netcat côté PC-Site-I 44
5.10 Réponse du PC-Site-I vers le PC-Site-II 44
5.11 Réception du message côté PC-Site-II 45
5.12 Capture du trafic réseau transmis (Wireshark) 45

5.13 Capture du trafic transmis chiffré 46

Liste des tableaux

1.1 Tableau comparatif entre les solutions VPN 10
1.2 Comparaison entre les méthodes séquentielles 12

2.1 Identification des intervenants du système 17
2.2 Plan d'adressage IPv4 de l'architecture réseau multisites 21
2.3 Équipements de l'environnement matériel 22
2.4 Outils de conception utilisés 22
2.5 Outils de simulation utilisés 23
2.6 Outils de test et d'observation utilisés 24

5.1 Plan d'adressage IPv4 de l'architecture de test 40

Introduction générale

Dans un contexte de mondialisation et de digitalisation croissante, la connectivité entre les différents sites d'une entreprise est devenue un élément incontournable pour assurer la continuité de ses activités. Le développement des réseaux informatiques et la nécessité de partager les ressources entre plusieurs localisations géographiques imposent aujourd'hui de nouvelles exigences en matière de sécurité, de disponibilité et de performance.

Cependant, cette interconnexion s'accompagne de nombreux défis liés à la protection des données, à la sécurisation des communications, et à la prévention contre les attaques informatiques de plus en plus sophistiquées. Face à ces enjeux, les technologies de réseaux privés virtuels (*VPN*) et les dispositifs de pare-feux s'imposent comme des solutions incontournables pour garantir la confidentialité, l'intégrité et la disponibilité des échanges au sein d'une organisation.

Dans cette optique, l'entreprise **TOPNET**, leader dans le secteur des services Internet en Tunisie, a accordé une importance stratégique à la sécurisation de son infrastructure réseau multisites. Ce stage de formation humaine réalisé au sein de cette entreprise s'inscrit ainsi dans le cadre de la conception et du déploiement d'une architecture réseau sécurisée reliant plusieurs sites distants à l'aide de **VPN** et de **pare-feux**, tout en respectant les bonnes pratiques de cybersécurité.

Ce rapport présente de manière détaillée l'ensemble des travaux réalisés durant ce stage, en mettant en avant la démarche méthodologique adoptée, les choix technologiques effectués, ainsi que les résultats obtenus à travers la mise en place de l'architecture proposée.

Le rapport est structuré en cinq chapitres organisés comme suit :

Le **premier chapitre** est consacré à la présentation de l'organisme d'accueil, incluant son historique, ses services ainsi que ses domaines d'activités, avant de présenter le cadre général du projet et la méthodologie adoptée.

Le **deuxième chapitre** présente l'équipe et les acteurs du projet, leurs besoins fonctionnels et non fonctionnels, ainsi que l'environnement logiciel et matériel.

Le **troisième chapitre** décrit les étapes de configuration des équipements de l'architecture réseau proposée.

Le **quatrième chapitre** détaille la phase d'établissement des tunnels VPN entre les sites.

Enfin, le **cinquième chapitre** est consacré à la vérification du bon fonctionnement de la connectivité sécurisée ainsi qu'à la validation globale de l'architecture.

Ce travail permet ainsi de répondre efficacement aux besoins de sécurité et d'interconnexion des entreprises multisites, tout en offrant l'occasion de pratiquer et d'acquérir de nouvelles compétences en administration des réseaux, des systèmes informatiques et en sécurité.

Chapitre 1

Cadre général du projet

1.1 Introduction

Ce chapitre a pour objectif de mettre en lumière la présentation de l'organisme d'accueil, l'entreprise **TOPNET**, au sein de laquelle ce stage de formation humaine a été réalisé dans une première partie. La deuxième partie met en avant la problématique ainsi que la solution proposée, tandis que la dernière partie se focalise sur la démarche adoptée pour l'élaboration du projet.

1.2 Présentation de l'organisme d'accueil

Dans les sections suivantes, nous allons présenter **TOPNET** ainsi que ses différents départements.

1.2.1 Présentation de TOPNET

TOPNET dont le logo est présenté dans la figure 1.1 est une entreprise tunisienne qui a démarré ses activités le 02 mai 2001, elle est le leader, aujourd'hui, des Fournisseurs d'accès Internet en Tunisie. Elle devient une filiale de groupe Tunisie Télécom, en Juin 2010, cette acquisition est considérée par Tunisie Télécom comme étant une opération stratégique permettant le renforcement de son leadership à travers un acteur qui, en quelques années, a réussi à se hisser en leader sur le marché des fournisseurs de services Internet (FSI) [1].

FIGURE 1.1 – Logo de TOPNET

Tunisie Télécom est l'opérateur historique de télécommunications en Tunisie. Créée en 1995 sous le nom d'Office National des Télécommunications, l'entreprise devient une société anonyme en 2004 sous la dénomination actuelle. Elle joue un rôle central dans la modernisation des infrastructures télécoms, compte plus de 6 millions d'abonnés et dispose d'un large réseau de directions régionales et de points de vente à travers le pays. **Tunisie Télécom** place la satisfaction client au cœur de ses priorités et contribue activement au développement des TIC en Tunisie [2].

Le logo officiel de **Tunisie Télécom** est illustré dans la figure 1.2

FIGURE 1.2 – Logo de Tunisie Télécom

1.2.2 Domaines d'activités

Les domaines d'activités de **TOPNET** couvrent plusieurs secteurs des technologies de l'information et de la communication, notamment :

- **Connectivité Internet :** Fourniture d'accès Internet haut débit pour les particuliers et les professionnels via ADSL, VDSL et fibre optique (GPON).
- **Sécurité et cybersécurité :** Solutions de sécurité managée telles que Net Protect, VPN d'entreprise, contrôle parental, antivirus et services de protection réseau.
- **Cloud et hébergement :** Services Cloud incluant le stockage en ligne (Topnet Storage), l'hébergement web, les serveurs privés virtuels (VPS) et l'enregistrement de noms de domaine.
- **Services aux entreprises :** Offres spécifiques pour les professionnels et les grandes entreprises telles que le SD-WAN, la gestion de parc Wi-Fi (Managed Wi-Fi) et l'interconnexion multisite.
- **Solutions SaaS et IoT :** Plateformes numériques (facturation en ligne, gestion de sites), géolocalisation (IRIS GPS) et intégration d'objets connectés [1].

1.2.3 Valeurs et engagements de TOPNET

TOPNET affiche clairement sa valeur fondamentale : « Garantir la pérennité de notre entreprise en devenant le Fournisseur de Service Internet préféré de nos clients par notre niveau de Qualité. »

Pour atteindre cet objectif, **TOPNET** s'engage à :

Garantir la satisfaction des clients en restant à leur écoute et en répondant à leurs attentes, tout en assurant la rentabilité de l'entreprise.

Enraciner, au sein de ses équipes, le sens de l'excellence permanente au service du client, notamment à travers l'amélioration continue de son fonctionnement interne.

Offrir continuellement de nouveaux produits et services répondant aux besoins évolutifs de sa clientèle.

Consolider sa position de leader et sa notoriété afin d'afficher une image de marque positive sur le marché [1].

1.3 Présentation du projet

Dans cette partie, nous exposons le contexte général qui justifie la pertinence du projet, la problématique identifiée dans un cadre de formation professionnelle, ainsi que la solution proposée à travers la conception et le déploiement d'une architecture réseau sécurisée.

1.3.1 Contexte du projet

L'évolution rapide du numérique impose aux entreprises multisites de relever des défis majeurs en matière de sécurité, de connectivité et de performance réseau. La généralisation des accès distants, le télétravail et la circulation constante de données sensibles exigent la mise en place d'infrastructures robustes et sécurisées.

Dans ce cadre, les technologies telles que les VPN et les pare-feux s'imposent comme des solutions standards pour assurer la confidentialité, l'intégrité et la disponibilité des échanges intersites. Elles permettent également une supervision centralisée du trafic et une meilleure résilience face aux menaces extérieures.

1.3.2 Problématique

Dans le cadre d'un stage de formation humaine et technique chez **TOPNET**, l'opportunité m'a été offerte de concevoir et simuler une architecture réseau sécurisée intégrant VPN et pare-feux. Ce projet ne vise pas à combler une lacune spécifique chez l'entreprise, mais à approfondir la compréhension des enjeux liés à la sécurisation des communications dans un environnement professionnel réel.

La problématique réside ainsi dans la capacité à concevoir une solution fonctionnelle, cohérente avec les bonnes pratiques du secteur, et suffisamment flexible pour répondre aux besoins d'interconnexion sécurisée entre plusieurs sites. Ce projet constitue un cadre idéal pour mettre en pratique des compétences en ingénierie réseau, affiner la maîtrise des outils professionnels et renforcer l'autonomie dans un environnement technique structuré.

1.3.3 Etude et critique de l'existant

L'étude de l'existant constitue une étape fondamentale dans la réalisation de tout projet. Elle vise à identifier et analyser les atouts et les limites des solutions matérielles et logicielles déjà en place ou recommandées. Cette analyse permet de mieux cerner les besoins spécifiques du projet et de déterminer les fonctionnalités à intégrer dans la future architecture.

Dans le cadre de notre projet, l'entreprise **TOPNET** a préconisé l'utilisation de certains équipements, en particulier le pare-feu **FortiGate** de **Fortinet** et le routeur **Cisco 891F**. Ces choix techniques imposés orientent notre réflexion quant aux solutions de sécurité et d'interconnexion à adopter.

1.3.3.1 Fortigate

Les informations présentées dans cette section sont principalement issues du site officiel de Fortinet [3].

"FortiGate" est un parefeu de la gamme Next-Generation Firewall (NGFW) de Fortinet, combine dans une plateforme unifiée des fonctions traditionnelles (firewall, NAT, VPN) et avancées (IPS, DPI, filtrage applicatif, antivirus, sandboxing).

Grâce à ses processeurs ASIC dédiés, FortiGate offre des performances élevées même avec l'activation complète des services UTM, incluant l'inspection SSL/TLS. Intégrée dans l'écosystème Security Fabric (FortiOS, FortiManager, FortiAnalyzer), cette solution permet une gestion centralisée, des politiques homogènes et une réponse automatisée aux menaces sur tous les sites et environnements réseau.

La figure 1.3 représente le logo de la solution "Fortigate".

FIGURE 1.3 – Logo de Fortigate

"Fortinet" est une entreprise mondiale de cybersécurité fondée en 2000 et reconnue pour sa plateforme intégrée Security Fabric, qui offre une protection unifiée et automatisée sur l'ensemble de la surface d'attaque numérique.

Avec plus de 860 000 clients dans le monde, Fortinet propose un large éventail de solutions de sécurité réseau, cloud, endpoint et applicative, toutes pilotées par son système d'exploitation unique FortiOS.

Son produit phare, le pare-feu FortiGate, intègre des fonctionnalités avancées telles que l'inspection approfondie des paquets (DPI), l'IPS, le filtrage applicatif, la prévention des menaces via FortiGuard Labs, et l'optimisation des performances grâce à ses processeurs ASIC propriétaires.

Fortinet se distingue par une approche axée sur l'automatisation, l'IA et une forte interopérabilité, ce qui en fait un acteur de référence dans les domaines du NGFW, du SD-WAN, du SASE et de l'accès réseau Zero Trust (ZTNA).

La figure 1.4 représente le logo de l'entreprise "Fortinet".

FIGURE 1.4 – Logo de Fortinet

— **Fonctionnalités principales :**
  - **Pare-feu état-de-session (Stateful Inspection)** : Filtrage traditionnel basé sur les adresses IP, ports et protocoles, avec prise en charge du NAT et des VPN IPSec/SSL.
  - **Inspection de paquets profonds (DPI) et contrôle applicatif** : Permet d'identifier et de filtrer des applications spécifiques comme YouTube, Skype, etc., indépendamment du port utilisé.
  - **Système de prévention d'intrusion (IPS)** : Protège contre les attaques connues et zero-day à l'aide de signatures et d'analyses comportementales.

- **Services FortiGuard** : Fournissent en temps réel des services comme l'antivirus, antimalware, filtrage web, et sandboxing, en s'appuyant sur l'IA et les FortiGuard Labs.
- **Inspection SSL/TLS** : Déchiffrement et analyse du trafic sécurisé sans dégradation notable des performances, grâce à l'usage de processeurs ASIC spécialisés.
- **Fonctionnalités avancées** : Support de Zero Trust Network Access (ZTNA), SD-WAN sécurisé, et gestion centralisée via FortiOS, FortiManager, et Security Fabric.

— **Performance et optimisation :**
- **Processeurs ASIC dédiés** : FortiGate embarque des ASICs (Network Processor NP, Content Processor CP) pour optimiser les traitements lourds (IPSec, SSL, IPS) tout en réduisant la consommation.
- **Débits élevés** : Les modèles haut de gamme comme les séries 6000F ou 700G atteignent jusqu'à 100 Gbps de throughput avec une efficacité énergétique remarquable.

— **Avantages spécifiques :**
- **Sécurité consolidée** : Intégration native de nombreuses fonctions de sécurité (pare-feu, VPN, IPS, antivirus, etc.) dans un seul appareil, réduisant la complexité de l'infrastructure.
- **Performance élevée** : Les puces ASIC assurent un traitement rapide, même pour le trafic chiffré, sans impacter la bande passante.
- **Interopérabilité étendue** : Intégration avec l'écosystème Fortinet via Security Fabric (FortiManager, FortiAnalyzer, FortiSandbox...) pour une réponse coordonnée aux menaces.
- **Gestion unifiée** : FortiOS propose une interface unique pour gérer de manière homogène les environnements physiques, virtuels et cloud.
- **Innovation continue** : Prise en charge des technologies émergentes (cryptographie post-quantique, FortiOS 7.x), assurant la pérennité de l'investissement.

— **Limites ou contraintes à considérer :**
- **Coût élevé des modèles haut de gamme** : Les équipements puissants (ex. 6000F) sont onéreux ; pour les petits réseaux, des modèles comme les 80F ou 90G sont suffisants mais moins évolutifs.
- **Complexité de configuration** : L'activation et la gestion des fonctions avancées nécessitent une bonne maîtrise de FortiOS et des licences FortiGuard à jour.
- **Interopérabilité avec des tiers** : Des ajustements techniques peuvent être requis pour garantir la compatibilité entre FortiGate et d'autres équipements.

1.3.3.2 Cisco 891F

Le Cisco 891F fait partie de la série des routeurs intégrés Cisco 890, conçus pour répondre aux besoins des succursales et des petits sites distants nécessitant une connectivité hautement sécurisée, des performances élevées et une gestion centralisée. Compact et puissant, ce routeur intègre de multiples fonctionnalités de sécurité, de routage, de commutation et d'accès sans fil dans un seul appareil, ce qui en fait une solution idéale pour les environnements professionnels exigeants [4].

— **Interfaces et Connectivité :**

Le Cisco 891F est équipé de 8 ports LAN Gigabit Ethernet (RJ-45), dont 4 ports sont compatibles Power over Ethernet (PoE), permettant l'alimentation directe de périphériques tels que des téléphones IP ou des caméras de surveillance. Il dispose également d'un port WAN Gigabit SFP, offrant une connectivité haut débit adaptable à divers types de supports (cuivre ou fibre optique). Pour la gestion, il comprend un port console RJ-45 et un port USB 2.0. En tout, ce modèle offre jusqu'à 11 interfaces physiques, combinant flexibilité, évolutivité et performance réseau. [4].

La figure 1.5 représente la présentation matérielle de la série des routeurs "Cisco 890".

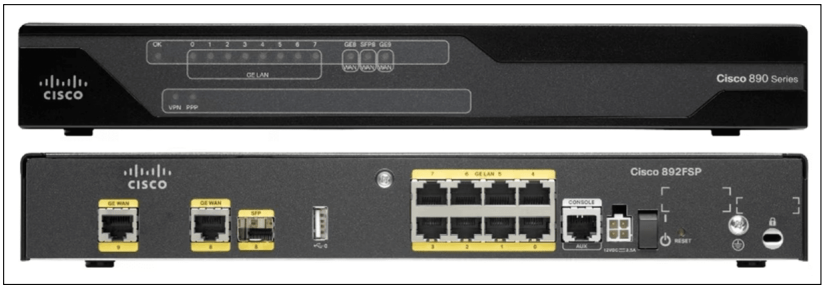

FIGURE 1.5 – Présentation matérielle de la série Cisco 890 [4]

1.3.3.3 Etude comparative des solutions VPN

Afin de garantir une communication sécurisée entre les différents sites de l'organisation, il est indispensable de mettre en place une solution VPN. Plusieurs technologies VPN sont aujourd'hui disponibles, chacune offrant des niveaux de sécurité, de performance et de complexité de déploiement différents.

Dans le cadre de ce projet, l'objectif est de sélectionner la solution la plus adéquate pour une interconnexion permanente et sécurisée entre sites distants, en s'appuyant sur les pare-feux FortiGate existants.

Pour ce faire, une étude comparative des principales solutions VPN a été menée. Le tableau ci-dessous présente une synthèse des caractéristiques techniques, avantages et li-

mites des trois solutions les plus pertinentes dans un contexte professionnel : IPsec VPN, OpenVPN, et WireGuard.

Table 1.1 – Tableau comparatif entre les solutions VPN

Critères	**IPsec VPN**	**OpenVPN**	**WireGuard**
Type	Site-à-site	Accès distant	Point-à-point
Sécurité	Très élevé	Elevé	Très élevé
Performance	Excellente	Moyenne à bonne	Très rapide
Configuration	Moyennement complexe	Relativement simple	Très simple
Portabilité (OS)	Multi-OS	Très compatible	Modules requis
Maturité	Très mature	Mature	En production)
Support matériel	Intégration native	Rarement intégré	Souvent manuel

1.3.4 Solution proposée

Dans le cadre de ce projet de stage, l'objectif principal est de concevoir et déployer une architecture réseau sécurisée permettant de relier plusieurs sites distants de l'entreprise TOPNET via Internet. Pour répondre à ce besoin, la solution retenue repose sur l'utilisation de pare-feux FortiGate de la marque Fortinet, associés à des routeurs Cisco 891F. L'interconnexion sécurisée entre les sites sera assurée à l'aide d'un VPN de type IPsec site-à-site.

Le choix du protocole IPsec s'est imposé naturellement compte tenu de plusieurs facteurs techniques et opérationnels. Tout d'abord, les pare-feux FortiGate offrent une prise en charge native et complète de ce protocole, avec une interface d'administration conviviale facilitant la configuration et la gestion des tunnels VPN. De plus, IPsec est un protocole standard largement utilisé dans les environnements professionnels, assurant ainsi une compatibilité optimale avec les équipements Cisco 891F utilisés dans l'infrastructure existante.

Sur le plan de la sécurité, IPsec permet de garantir la confidentialité, l'intégrité et l'authenticité des communications entre les sites. Grâce au chiffrement des paquets IP et à l'authentification mutuelle des équipements, les données échangées entre les différents réseaux locaux sont protégées contre les interceptions ou les attaques. En outre, ce protocole bénéficie d'un retour d'expérience solide et d'un niveau de maturité élevé, ce qui en fait une solution fiable et éprouvée dans les contextes professionnels.

Enfin, le VPN IPsec présente l'avantage d'être adapté aux connexions permanentes entre sites distants, en offrant une très bonne stabilité ainsi qu'une performance satisfaisante, sans impact significatif sur la bande passante disponible. Ces caractéristiques font du VPN IPsec, associé aux pare-feux FortiGate, la solution la plus pertinente et la mieux adaptée aux besoins spécifiques de ce projet.

1.4 Méthodologie de travail

Les méthodologies de travail, aussi appelées méthodes de gestion de projet, sont des approches structurées permettant de planifier, exécuter et finaliser efficacement un projet. Elles facilitent la coordination des tâches, la gestion des ressources, le suivi des délais, ainsi que la collaboration entre les parties prenantes.

Dans le cadre de projets techniques clairement définis, à périmètre fixe et objectifs stables, comme **la conception et déploiement d'une architecture réseau sécurisée reliant plusieurs sites à l'aide de VPN et de pare-feux**, les approches dites séquentielles, notamment la méthode en cascade et ses variantes, s'avèrent particulièrement adaptées.

Contrairement aux approches agiles, qui sont orientées vers le développement logiciel avec une forte adaptabilité aux changements, les méthodes séquentielles sont conçues pour les projets où les besoins sont bien établis dès le départ et où la rigueur de la planification est essentielle. Cela correspond parfaitement aux caractéristiques d'un projet d'intégration et de configuration d'une solution existante.

1.4.1 Les méthodes séquentielles (en cascade)

Les méthodes dites en cascade sont historiquement les premières approches structurées de gestion de projet. Elles sont particulièrement adaptées aux projets techniques avec des objectifs clairs et des étapes bien identifiées, comme c'est le cas dans la conception et déploiement d'une architecture réseau sécurisée reliant plusieurs sites.

Cette approche repose sur une succession de phases linéaires, chaque phase produisant des livrables validés avant de passer à la suivante.

Cette logique linéaire favorise une bonne traçabilité, une documentation rigoureuse et une planification fiable, ce qui est essentiel lorsqu'on intègre une solution tierce dans un environnement informatique existant.

1.4.2 Variantes des méthodes séquentielles

Plusieurs variantes ont été conçues à partir du modèle en cascade classique, afin de renforcer certains aspects comme la validation ou la gestion des risques. Voici les deux principales :

— **Modèle en V :** Ce modèle conserve une progression linéaire mais accorde une importance particulière à la validation. Chaque phase de conception a une phase de test correspondante. Ce modèle est souvent utilisé dans les projets techniques où la qualité et la sécurité sont critiques (ex. systèmes réseau, embarqués).

— **Modèle en spirale :** Il intègre une logique de cycles successifs avec une forte gestion des risques à chaque itération. Moins utilisé pour les projets à périmètre fixe, il peut

cependant convenir dans les environnements incertains ou les projets évolutifs.

Le tableau suivant présente une comparaison synthétique de ces trois modèles, appliqués au contexte des projets techniques tels que l'intégration d'une solution NAC.

Table 1.2 – Comparaison entre les méthodes séquentielles

Critères	**Méthode en cascade**	**Méthode en V**	**Méthode en spirale**
Structure	Séquentielle, chaque phase suit la précédente	Extension de la méthode en cascade, avec validation et test à chaque étape	Cycle itératif combinant conception et analyse des risques
Phases clés	Analyse, conception, implémentation, tests, déploiement	Idem que la cascade + phase de validation systématique	Définition des objectifs, évaluation des risques, développement et planification
Flexibilité	Faible	Faible à moyenne	Élevée, adaptée aux projets évolutifs
Gestion des risques	Non intégrée explicitement	Présente uniquement en phase de validation	Intégrée dès le début
Complexité du projet	Moyenne	Moyenne à élevée	Élevée
Documentation	Forte documentation à chaque étape	Documentation rigoureuse + traçabilité des tests	Documentation moins rigide mais centrée sur les risques
Coût et délais	Moins coûteuse si les besoins sont bien définis	Coût modéré avec bonne gestion des erreurs	Plus coûteuse à cause des itérations multiples

1.4.3 Méthode adoptée : En cascade

Dans le cadre de ce projet, il ne s'agit pas de développer une solution logicielle ou de concevoir une architecture réseau totalement nouvelle, mais plutôt de mettre en œuvre et configurer une solution technique existante en s'appuyant sur des équipements professionnels, notamment les pare-feux FortiGate et les routeurs Cisco 891F. L'objectif est de créer une infrastructure réseau sécurisée permettant de relier plusieurs sites distants à travers un VPN IPsec.

La démarche suit des étapes bien définies, telles que : – l'analyse des besoins et des contraintes réseau de l'entreprise, – la configuration des équipements réseau (routeurs et pare-feux), – l'établissement des tunnels VPN entre les sites via IPsec, – la vérification du bon fonctionnement de la connectivité sécurisée, – et la validation globale de l'architecture mise en place.

Ce type de projet ne repose pas sur des cycles d'itération fréquents ni sur des adaptations continues, comme on peut le rencontrer dans les approches agiles. Il nécessite plutôt une planification rigoureuse, une documentation structurée et un déroulement linéaire des tâches.

C'est pourquoi la méthode en cascade s'avère particulièrement adaptée dans ce contexte. Elle permet de structurer le travail en phases successives, de l'analyse à la mise en service, tout en assurant une cohérence globale dans le déploiement de l'infrastructure réseau sécurisée.

1.5 Conclusion

Dans ce chapitre, nous avons présenté l'organisme d'accueil, **TOPNET**. Nous avons ensuite défini le cadre du projet en détaillant l'analyse et l'étude comparative des solutions disponibles sur le marché, la problématique ainsi que la solution proposée. Enfin nous nous sommes penchés sur le choix de la méthodologie de travail.
Dans le chapitre suivant, nous aborderons la phase de planification de notre projet.

Chapitre 2

Analyse préliminaire et planification

2.1 Introduction

Dans le cadre de la conception et le déploiement d'une architecture réseau sécurisée reliant plusieurs sites à l'aide de VPN et de pare-feux, une phase d'analyse préliminaire est indispensable pour bien cerner les exigences du projet, identifier les acteurs, définir l'architecture cible et planifier les différentes étapes du projet. Ce chapitre présente les fondements de cette phase, en s'appuyant sur une méthodologie structurée intégrant à la fois une compréhension fine du besoin et une planification rigoureuse.

2.2 Présentation de l'équipe

Le projet est réalisé par moi-même, Ezzine Montassar, en tant que stagiaire ingénieur, sous la supervision de M. Monji Tarhouni, qui occupe le rôle d'encadrant technique.

2.3 Capture des besoins

La capture des besoins consiste à identifier, dans un premier temps, les besoins fonctionnels du projet. Ensuite, elle permet de spécifier les exigences non fonctionnelles attendues par les utilisateurs.

2.3.1 Besoins fonctionnels

Les besoins fonctionnels décrivent ce que le système doit faire. Ils sont liés aux fonctions attendues du réseau à concevoir :

— **Sécurité et protection :**
  - Établir des tunnels VPN IPSec site-à-site pour relier plusieurs sites distants de manière sécurisée.
  - Filtrage du trafic entrant et sortant à l'aide des pare-feux FortiGate (règles de sécurité, contrôle d'accès).
  - Prévention des intrusions et détection des anomalies via les fonctions UTM (Unified Threat Management) de FortiGate.
  - Sécurisation de la communication avec chiffrement des données via IPSec.

— **Connectivité réseau :**
  - Permettre aux utilisateurs de chaque site de communiquer avec les autres via un réseau privé virtuel (VPN).
  - Assurer la continuité de service même en cas de coupure d'un tunnel VPN (ajouter redondance si nécessaire).
  - Configuration des routeurs Cisco 891F pour le routage inter-sites.

— **Administration :**
  - Accès centralisé à l'interface d'administration des équipements FortiGate (GUI ou CLI).
  - Création de politiques de sécurité selon les besoins des différents sites.
  - Journalisation et monitoring du trafic et des connexions VPN.
  - Possibilité de diagnostic à distance et de dépannage du réseau.

— **Tests et validation :**
  - Vérification de la connectivité inter-sites via VPN IPSec.
  - Tests de résistance aux attaques (simples ping flood, accès non autorisés,etc).
  - Contrôle de la qualité de service (QoS) sur les liens critiques.

2.3.2 Besoins non fonctionnels

Les besoins non fonctionnels décrivent comment le système doit fonctionner. Parmi les besoins, nous pouvons citer :

— **Sécurité :**

  - Le système doit garantir un haut niveau de confidentialité, d'intégrité et d'authentification des communications.
  - Utilisation de protocoles robustes et de chiffrement fort (AES, SHA2, etc).

— **La fiabilité :**
  - Le réseau doit être fiable, avec une disponibilité élevée.
  - Mise en place de mécanismes de redondance si nécessaire (VRRP, routeurs ba-

ckup, double VPN,etc).

— **Performance :**
  - Le VPN doit assurer un débit suffisant pour les services critiques (VoIP, partage de fichiers, etc).
  - Les équipements doivent pouvoir supporter la charge réseau prévue.

— **Scalabilité :**
  - L'architecture doit permettre l'ajout futur de nouveaux sites sans refonte complète.
  - Support des mises à jour logicielles et matérielles sans interruption majeure.

— **Facilité de gestion :**

item [•] L'interface de gestion doit être intuitive, avec des alertes, des rapports et des logs faciles à lire.Documentation claire des configurations mises en œuvre.

—• **La fiabilité :**
  - Respect des normes et bonnes pratiques en matière de cybersécurité (ISO 27001, RGPD si données personnelles traitées, etc).

2.4 Analyse préliminaire des besoins

Dans cette section, nous allons identifier les acteurs de notre système, présenter le diagramme de cas d'utilisation global et explorer sa vue architecturale.

2.4.1 Identification des acteurs

Le tableau 2.1 répertorie les acteurs impliqués dans notre projet.

Table 2.1 – Identification des intervenants du système

Acteurs	Rôle
Administrateur réseau et sécurité	Conçoit l'architecture réseau (choix des équipements, topologie, politique de sécurité), déploit et configure les VPN et pare-feux.
Technicien système et réseau	Assiste à la mise en œuvre technique (câblage, déploiement physique, configuration initiale des équipements).
Utilisateur final	Bénéficiaire du système. Ils doit accéder de manière fluide, sécurisée et transparente aux services du réseau.

2.4.2 Diagramme de cas d'utilisation global

Le diagramme de cas d'utilisation global et l'architecture globale du projet sont présentés dans cette section, suite à une première analyse préliminaire de ce projet.

La Figure 2.1 présente le diagramme de cas d'utilisation global qui met en évidence les fonctionnalités générales attendues de notre solution.

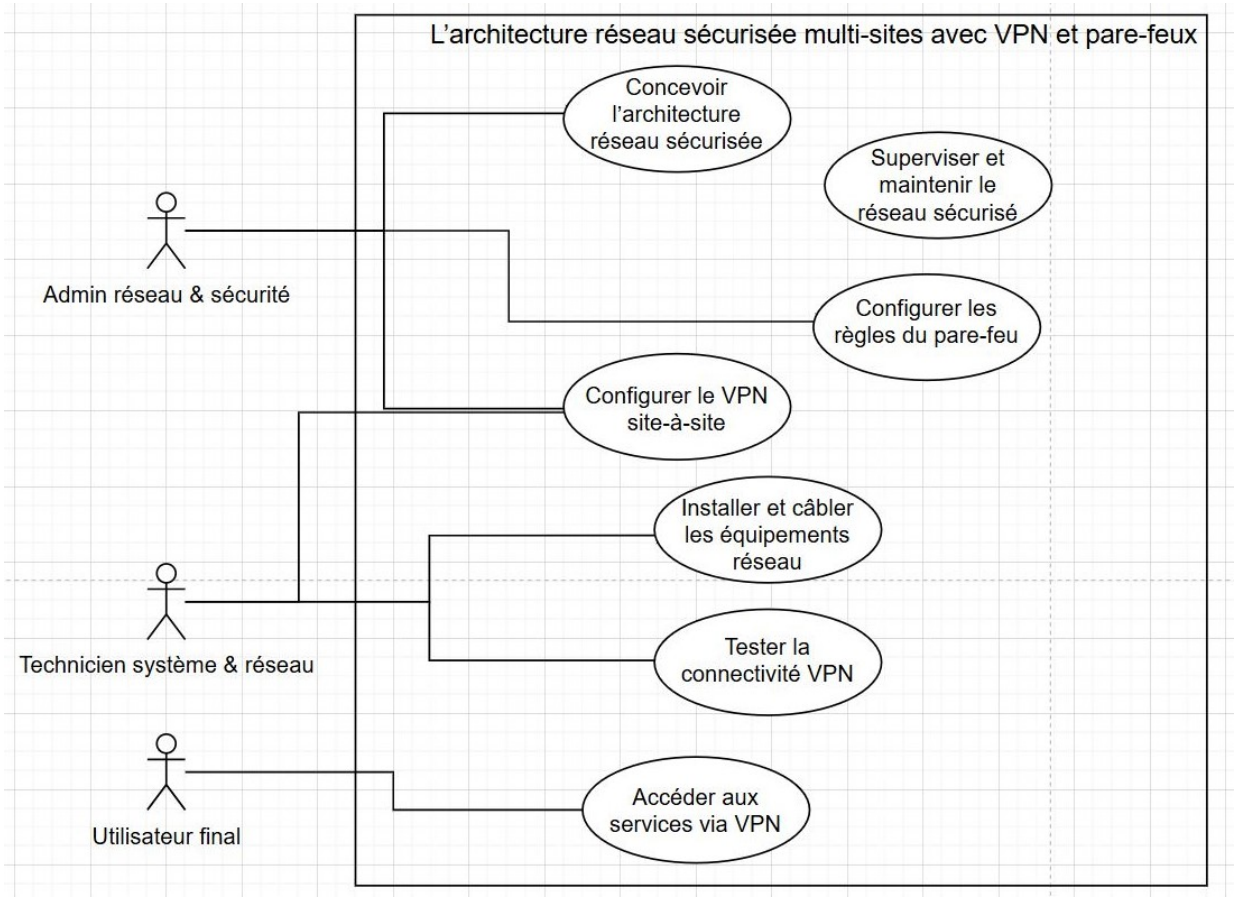

FIGURE 2.1 – Diagramme des cas d'utilisation

2.4.3 Vue architecturale

Afin d'illustrer concrètement la mise en place d'une interconnexion sécurisée entre plusieurs sites distants, nous présentons dans la section suivante les architectures physique et logique retenues pour ce projet. Il s'agit de prototypes représentant un exemple d'infrastructure multisites sécurisée, intégrant des pare-feux et des tunnels VPN pour assurer la confidentialité, l'intégrité et la disponibilité des communications. Cette conception servira de référence pour démontrer les principes techniques et les bonnes pratiques applicables dans un contexte réel.

2.4.3.1 Architecture physique

La figure 2.2 illustre le prototype de l'architecture réseau multisites envisagée pour le déploiement. Celle-ci se compose de deux sites distants interconnectés via le réseau public Internet. Chaque site est équipé d'un pare-feu FortiGate, chargé d'assurer la mise en place

du tunnel VPN ainsi que le chiffrement des échanges entre les sites, et d'un routeur jouant le rôle de passerelle vers le réseau public.

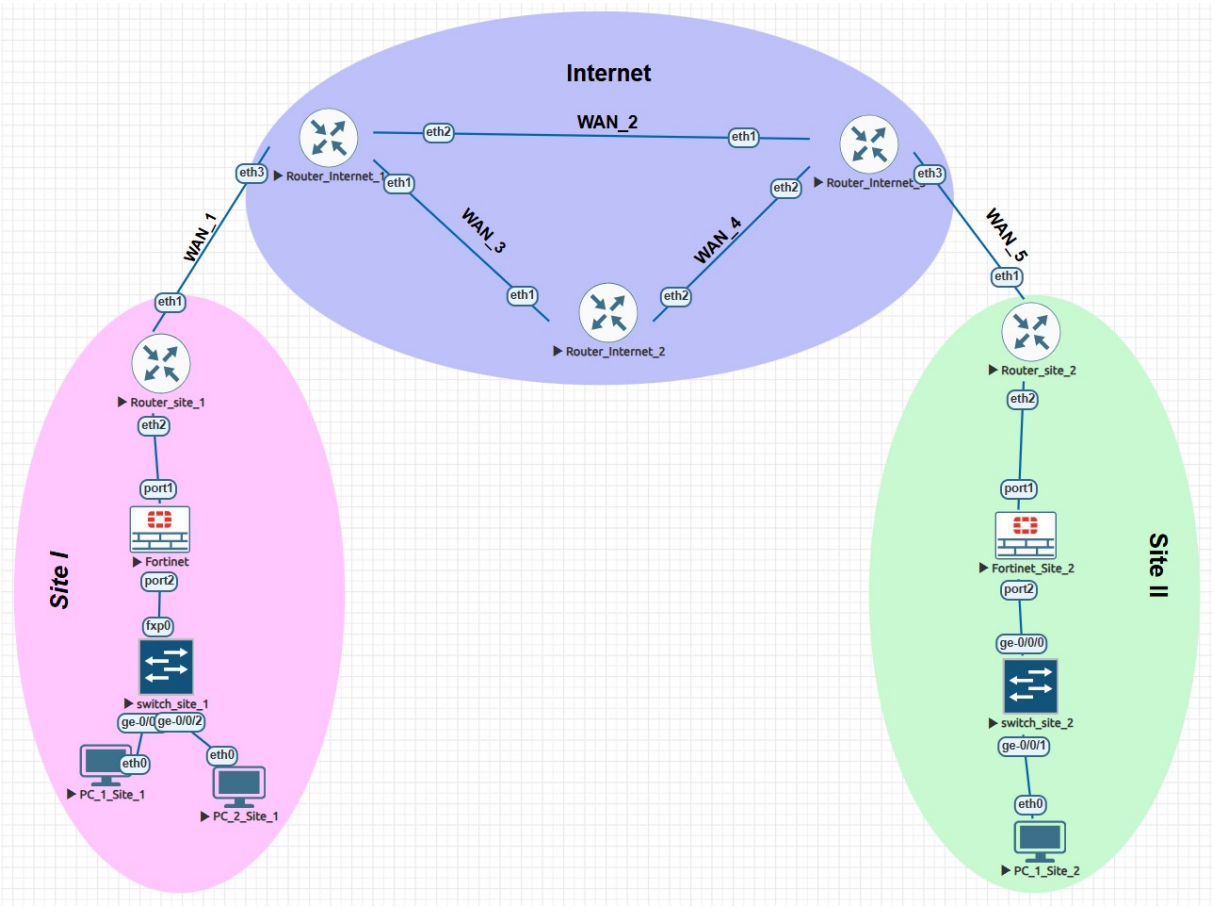

FIGURE 2.2 – Prototype d'une architecture réseau multisites sécurisée avec VPN et pare-feux

2.4.3.2 Architecture logique

En complément de l'architecture physique, l'architecture logique met en évidence l'organisation fonctionnelle du réseau et la répartition des rôles au sein de l'infrastructure. Elle ne s'intéresse pas à la disposition physique des équipements, mais à la manière dont les différentes fonctions réseau sont organisées et interconnectées pour assurer le bon fonctionnement global du système.
Dans notre projet, l'architecture logique est structurée autour de trois fonctions principales :

— **Routage :** Gestion et orientation du trafic entre les réseaux locaux et distants.
— **Tunneling :** création de tunnels VPN pour assurer une interconnexion sécurisée entre

les sites.

— **Chiffrement :** Sécurisation des échanges à travers des mécanismes cryptographiques intégrés aux pare-feux FortiGate.

La figure 2.3 illustre le rôle essentiel du tunnel VPN, qui consiste en une liaison logique créée par l'encapsulation du paquet original chiffré dans un nouvel en-tête, permettant son acheminement à travers le réseau Internet jusqu'à atteindre le site distant.

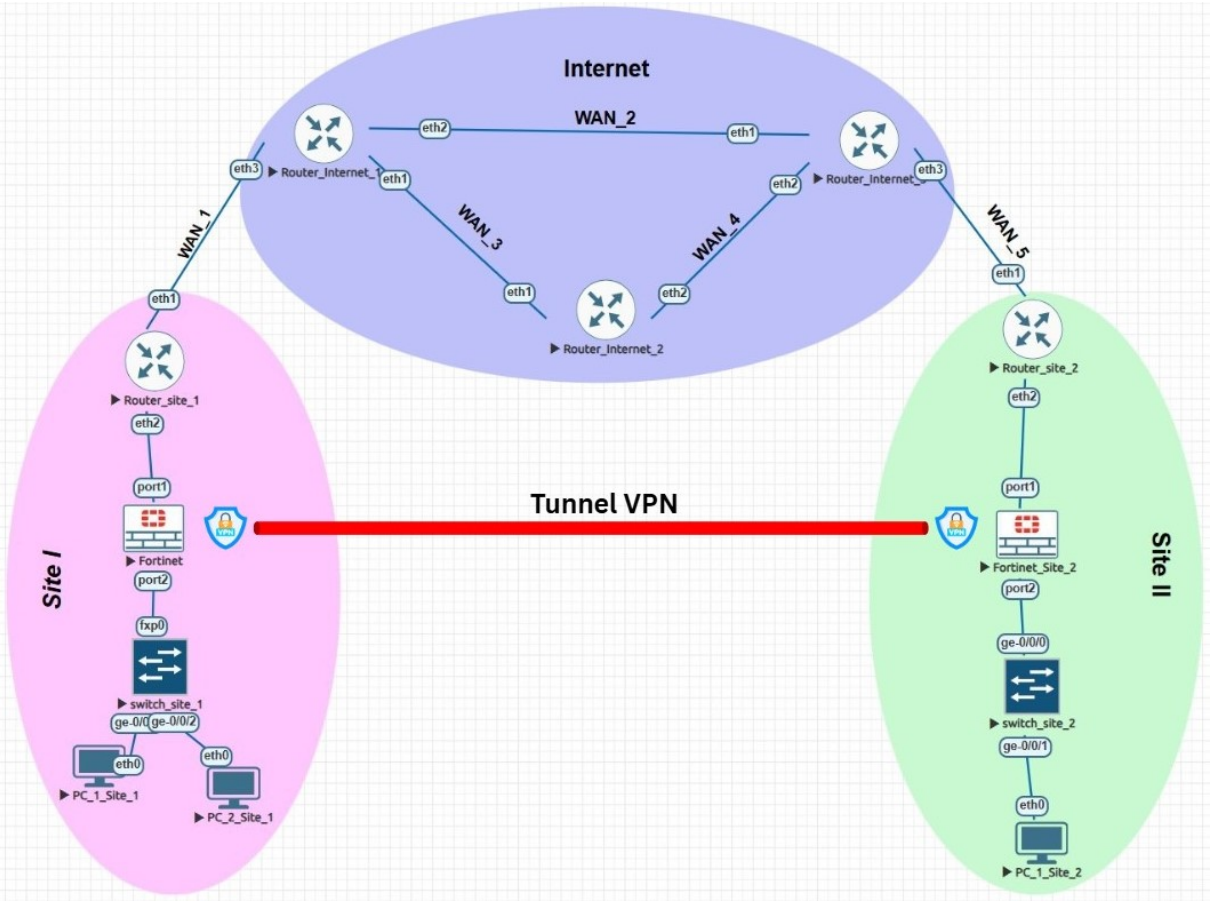

FIGURE 2.3 – Fonctionnement logique de l'architecture réseau multisites

Le tableau 2.2 présente le plan d'adressage adopté pour le prototype, définissant les plages d'adresses IP attribuées à chaque réseau et interface afin d'assurer une communication claire, hiérarchisée et sans chevauchement.

Table 2.2 – Plan d'adressage IPv4 de l'architecture réseau multisites

Réseau	**Adresse réseau**	**Équipement**	**Adresse**
Site I	192.168.1.0/24	FW - Site 1 - port 2	192.168.1.254
		PC-1	192.168.1.10
		PC-2	192.168.1.20
	100.1.1.0/30	FW - Site 1 - port 1	100.1.1.1
		Routeur - eth 2	100.1.1.2
Site II	192.168.2.0/24	FW - Site 2 - port 2	192.168.2.254
		PC-1	192.168.2.10
	100.1.4.0/30	FW - Site 2 - port 1	100.1.4.1
		R-site-2 - eth 2	100.1.4.2
WAN I	100.1.1.4/30	R-Site-1 - eth 1	100.1.1.5
		R-Internet-1 - eth 3	100.1.1.6
WAN II	100.1.2.0/30	R-Internet-1 - eth 2	100.1.2.1
		R-Internet-3 - eth 1	100.1.2.2
WAN III	100.1.2.4/30	R-Internet-1 - eth 1	100.1.2.5
		R-Internet-2 - eth 1	100.1.2.6
WAN IV	100.1.3.0/30	R-Internet-2 - eth 2	100.1.3.1
		R-Internet-3 - eth 2	100.1.3.2
WAN V	100.1.3.4/30	R-site-2 - eth 1	100.1.3.5
		R-Internet-3 - eth 3	100.1.3.6

2.5 Environnement de travail

L'environnement professionnel est composé de deux éléments : l'environnement matériel et l'environnement logiciel.

2.5.1 Environnement matériel

Le tableau 2.3 présente chaque équipement utilisé dans le projet.

Table 2.3 – Équipements de l'environnement matériel

Équipement	Rôle
Fortigate	Pare-feu utilisé pour le tunneling et le chiffrement des connexions intersites (terminaux VPN).
Cisco 891F	Acheminement et routage intersites.
PC HP	Poste d'administration et de configuration
Câblage	Câbles Ethernet RJ45 (droit/croisé selon besoin) + câble console (USB-to-RJ45) pour l'accès initial.

2.5.2 Environnement logiciel

Dans cette partie, nous présentons les outils de conception et de simulation, puis nous terminons par les outils de test et d'observation.

Les tableaux 2.4, 2.5 et 2.6 présentent les outils utilisés dans ce projet.

Outil	**Description**
eve Emulated Virtual Environment Next Generation	EVE-NG est une plateforme permettant de concevoir des topologies réseau complexes dans un environnement virtuel. Elle offre une interface web qui met à la disposition des professionnels plusieurs outils de conception. [6].
draw.io	Draw.io, aussi connu sous le nom diagrams.net, est un outil gratuit et open source qui permet de concevoir facilement des architectures réseau complètes grâce à une large bibliothèque d'icônes et de modèles. Accessible via un navigateur ou en application de bureau, il offre une interface intuitive avec la possibilité de glisser-déposer des éléments.

Table 2.4 – Outils de conception utilisés

EVE-NG et Draw.io sont utilisés lors de la phase de conception de l'architecture, grâce aux fonctionnalités avancées de modélisation et de dessin qu'ils offrent.

Outil	Description
	VMware Workstation Pro 17 est un hyperviseur de type 2 (hosted hypervisor) développé par VMware, qui permet de créer et gérer plusieurs machines virtuelles (Linux, Windows, BSD, MS-DOS, etc..) sur un ordinateur Windows ou Linux hôte. Chaque machine virtuelle fonctionne indépendamment tout en partageant les ressources du système physique [5].
FortiGate VM	FortiGate-VM est une appliance virtuelle de pare-feu de nouvelle génération développée par Fortinet. Elle offre une protection avancée contre les menaces, une connectivité sécurisée et une gestion centralisée, tout en étant adaptée aux environnements cloud, virtualisés et hybrides [3].
Emulated Virtual Environment Next Generation	En plus de ses autres fonctionnalités, EVE-NG est une plateforme de simulation réseau multivendeur qui permet aux professionnels, étudiants et formateurs de concevoir, tester et valider des topologies réseau complexes dans un environnement virtuel. Son interface web intuitive facilite l'accès et l'interaction avec les dispositifs simulés [6].
Cisco Packet Tracer	Cisco Packet Tracer est un simulateur réseau visuel développé par Cisco Systems, qui offre aux utilisateurs, étudiants, enseignants ou professionnels la possibilité de concevoir, configurer et expérimenter des topologies réseau virtuelles sans nécessité de matériel physique [9].

Table 2.5 – Outils de simulation utilisés

La phase de simulation repose sur l'utilisation d'un environnement virtuel permettant de reproduire et de tester l'architecture réseau avant son déploiement réel. VMware Workstation Pro 17, en tant qu'hyperviseur, a été utilisé pour créer les machines virtuelles FortiGate VM et EVE-NG. La machine FortiGate a été déployée en intégration avec d'autres systèmes (RHEL, Debian, Windows 10, etc.) afin de vérifier la bonne configuration et d'assurer une gestion efficace du pare-feu. De son côté, la machine EVE-NG a servi à la simulation et à la création d'une architecture réseau virtuelle complète, grâce à son interface web intuitive et facile à administrer. Parallèlement, Cisco Packet Tracer a été exploité pour simuler la configuration des routeurs Cisco dans un environnement interactif, permettant de tester les protocoles de routage et d'optimiser l'acheminement du trafic entre les différents sites, sans nécessiter de matériel physique.

Outil	Description
	Wireshark est un analyseur de paquets réseau open source et gratuit, largement reconnu dans l'informatique et la cybersécurité. Il permet la capture de trafic en temps réel ou l'analyse de fichiers enregistrés, avec une interface graphique intuitive à trois volets, des filtres d'affichage puissants, un codage couleur pour identifier facilement les types de trafic, et la prise en charge de centaines, voire des milliers, de protocoles [7].
	Ntopng est un outil open source de surveillance et d'analyse du trafic réseau, accessible via une interface web conviviale. Né comme version "next generation" de l'outil ntop créé en 1998. Il peut capturer le trafic via libpcap ou PF-RING, ou collecter des flux via NetFlow, sFlow ou IPFIX, notamment avec l'aide de nProbe [8].

Table 2.6 – Outils de test et d'observation utilisés

Wireshark et Ntopng offrent des fonctionnalités avancées d'analyse et de surveillance du trafic réseau, et sont utilisés pour vérifier la bonne configuration des différents équipements de l'architecture.

2.6 Conclusion

Grâce à ce chapitre, nous avons pu identifier les besoins fonctionnels et non fonctionnels, ainsi que les acteurs de notre projet, et élaborer un diagramme de cas d'utilisation. Nous avons ensuite présenté l'architecture physique et logicielle de notre projet, avant de conclure ce chapitre par la description de l'environnement logiciel et matériel. Le chapitre suivant portera sur la configuration et la mise en œuvre de l'architecture proposée.

Chapitre 3

Configuration des équipements de l'architecture réseau proposée

3.1 Introduction

Comme le suggère son titre, ce chapitre est dédié à la phase de configuration des routeurs et des pare-feux de chaque site distant.

3.2 Étapes de la configuration

Cette phase comprend la configuration des routeurs (routage, acheminement du trafic, etc.), la configuration des pare-feux (filtrage du trafic), ainsi que l'attribution des adresses IPv4 pour chaque interface réseau.

3.2.1 Étape I : Configuration des routeurs Cisco 891F

La phase de configuration des routeurs Cisco 891F constitue une étape essentielle pour assurer la connectivité entre les différents sites. Elle permet de définir les paramètres réseau nécessaires au routage et à l'acheminement fiable du trafic entre le réseau local de chaque site et les réseaux distants via Internet. Cette configuration inclut le paramétrage des interfaces, la mise en place des protocoles de routage appropriés, ainsi que l'activation des règles de sécurité garantissant la protection des échanges.

Elle suit un ensemble d'étapes structurées visant à établir cette communication fiable entre les deux sites distants. Chaque étape repose sur l'utilisation de commandes spécifiques du système d'exploitation Cisco IOS.

L'accès au routeur se fait via la console (câble Ethernet USB vers RJ45) à l'aide de MobaXterm comme terminal. Les paramètres de base incluent la configuration du nom d'hôte, la définition des mots de passe d'accès et la désactivation des services inutilisés.

La figure 3.1 illustre le câble Ethernet USB vers RJ45 utilisé pour établir la connexion physique avec le port console du routeur, permettant ainsi d'accéder à son interface de configuration. La figure 3.2 présente le logo du terminal MobaXterm, un outil polyvalent qui offre une interface de ligne de commande et de nombreuses fonctionnalités facilitant la configuration et la gestion des équipements réseau.

FIGURE 3.1 – Câble Ethernet USB vers RJ45

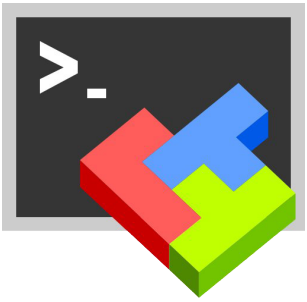

FIGURE 3.2 – Logo du terminal MobaXterm

Après avoir accédé à chaque routeur, nous avons activé chaque interface et lui avons attribué une adresse IP conformément au plan d'adressage défini dans le tableau 2.2. Chaque interface du routeur possède une adresse IP publique. L'interface reliée au pare-feu, dans chaque site, joue le rôle de passerelle pour le trafic sortant vers les réseaux externes.

Dans le cadre de ce prototype d'architecture multi-sites, le routage sur les routeurs Cisco 891F connectés à Internet a été configuré afin d'assurer l'échange optimal de données entre les réseaux locaux de chaque site via le tunnel VPN établi. Pour garantir une

adaptation rapide aux changements éventuels de topologie et faciliter la maintenance, le protocole OSPF a été retenu. Ce protocole, basé sur l'algorithme SPF, permet de découvrir automatiquement les réseaux présents, de calculer les meilleurs chemins et de mettre à jour les tables de routage en cas de modification de l'infrastructure, tout en offrant une convergence rapide et une bonne évolutivité. La configuration a consisté à déclarer les interfaces participant au processus OSPF, à définir l'aire de routage (area 0) et à propager les réseaux locaux ainsi que les réseaux utilisés pour l'interconnexion des sites. Ce choix garantit non seulement la continuité des communications intersites, mais aussi une gestion centralisée et automatisée du routage dans la perspective d'une extension future de l'architecture.

La configuration d'un routeur Cisco 891F suit un enchaînement logique d'étapes, chacune correspondant à un objectif précis :

- **Accès au mode de configuration et paramètres de base :**
  Router(config)# hostname R1 "Définition du nom d'hôte"
  R1(config)# no ip domain-lookup "Désactivation de la résolution DNS inutile"
  R1(config)# enable secret MonPassAdmin "Mot de passe pour le mode privilégié"
  R1(config)# line console 0
  R1(config-line)# password MonPassCons
  R1(config-line)# login
  R1(config)# service password-encryption "Chiffrement des mots de passe"

- **Configuration des interfaces et attribution des adresses IP :**
  R1(config)# interface eth2 “Nom de l'interface à configurer”
  R1(config-if)# ip address 100.1.1.2 255.255.255.252 “IP publique de/vers pare-feu”
  R1(config-if)# no shutdown “Activer l'interface”
  R1(config-if)# description Vers_PareFeu
  R1(config-if)# exit
  R1(config)# interface eth1
  R1(config-if)# ip address 100.1.1.5 255.255.255.0 “IP publique de/vers Internet”
  R1(config-if)# no shutdown
  R1(config-if)# description Site_Internet
  R1(config-if)# exit

- **Configuration du protocole OSPF pour le routage dynamique :**
  R1(config)# router ospf 1
  R1(config-router)# router-id 1.1.1.1
  R1(config-router)# network 100.1.1.0 0.0.0.3 area 0
  R1(config-router)# network 100.1.1.4 0.0.0.3 area 0
  R1(config-router)# passive-interface default
  R1(config-router)# no passive-interface eth1 “vers 100.1.1.0/30”
  R1(config-router)# no passive-interface eth2 “vers 100.1.1.4/30”

Afin de sécuriser l'architecture et de cloisonner les informations de routage, prenons le cas du routeur du site 1. Le protocole OSPF y a été configuré sur le routeur edge uniquement pour annoncer les réseaux publics d'interconnexion. Les réseaux 100.1.1.0/30 et 100.1.1.4/30 ont été intégrés dans l'aire backbone (area 0) afin d'assurer l'échange des routes nécessaires au fonctionnement du VPN intersites. Le réseau privé local 192.168.1.0/24 n'est pas annoncé dans OSPF ; il reste ainsi invisible pour les autres routeurs du domaine et protégé derrière le pare-feu. Cette configuration garantit que seules les adresses publiques circulent dans le protocole de routage, tandis que le pare-feu assure le routage et la sécurisation du trafic privé entre les deux sites.

3.2.2 Étape II : Configuration des pare-feu Fortigate

La configuration des pare-feu FortiGate constitue une étape clé pour garantir une connectivité sécurisée entre les sites. Elle repose d'abord sur l'adressage IP de chaque interface réseau : l'interface LAN du pare-feu, dotée d'une adresse privée, joue le rôle de passerelle pour le trafic interne. Le tunnel VPN est ensuite établi en encapsulant le trafic local dans des paquets chiffrés dont l'en-tête porte l'adresse publique de l'interface WAN du pare-feu connectée au routeur Cisco 891F. Cette interface utilise le routeur comme passerelle suivante (next-hop), garantissant ainsi la connectivité point-à-point entre sites ainsi que l'accès aux réseaux externes. La configuration inclut enfin l'attribution des adresses, la mise en place du routage et la définition des règles de sécurité (politiques inter-zones).

De même que pour la configuration des routeurs, nous avons accédé à chaque pare-feu physiquement à l'aide d'un câble console USB–RJ45 et logiquement via MobaXterm.

- **Paramètres de base et accès à l'appareil :**
  FortiGate# config system global
  FortiGate(global)# set hostname FW-Site-I "Définition du nom d'hôte"
  FortiGate(global)# end
  FortiGate# config system interface
  FortiGate(interface)# edit port1 "Interface reliée au routeur (WAN)"
  FortiGate(port1)# set ip 100.1.1.1/30 "IP publique de/vers routeur"
  FortiGate(port1)# set allowaccess ping https ssh
  FortiGate(port1)# next
  FortiGate(interface)# edit port2 "Interface LAN"
  FortiGate(port2)# set ip 192.168.1.254/24 "Passerelle LAN interne"
  FortiGate(port2)# set allowaccess ping https ssh
  FortiGate(port2)# next
  FortiGate(interface)# end

- **Configuration des routes statiques :**
  FortiGate# config router static
  FortiGate(static)# edit 1
  FortiGate(1)# set dst 0.0.0.0/0
  FortiGate(1)# set gateway 100.1.1.2 "Vers routeur/Internet"
  FortiGate(1)# set device port1
  FortiGate(1)# next
  FortiGate(static)# edit 2
  FortiGate(2)# set dst 192.168.2.0/24 "Réseau du site II"
  FortiGate(2) set gateway 100.1.1.2 "Routeur du site I"
  FortiGate(2) set device port1
  FortiGate(2) next
  FortiGate(static) end

- **Configuration du NAT/PAT :**
  On applique la traduction d'adresse uniquement pour le trafic (LAN vers ou de Internet). Pas de NAT pour les communications entre les sites.
  FortiGate# config firewall policy
  FortiGate(policy)# edit 1
  FortiGate(1)# set srcintf port2
  FortiGate(1)# set dstintf port1
  FortiGate(1)# set srcaddr 192.168.1.0/24
  FortiGate(1)# set dstaddr 192.168.2.0/24
  FortiGate(1)# set action accept
  FortiGate(1)# set nat disable "Pas de NAT pour site distant"
  FortiGate(1)# next

  FortiGate(policy)# edit 2
  FortiGate(2)# set srcintf port2
  FortiGate(2)# set dstintf port1
  FortiGate(2)# set srcaddr 192.168.1.0/24
  FortiGate(2)# set dstaddr all
  FortiGate(2)# set action accept
  FortiGate(2)# set nat enable "Activer NAT/PAT vers Internet"
  FortiGate(2)# next
  FortiGate(policy)# end

La configuration du NAT/PAT sur le pare-feu permet de distinguer deux scénarios de trafic :

- Lorsqu'un poste du réseau local (192.168.1.0/24) envoie des paquets vers Internet, les adresses privées sont traduites en l'adresse IP publique de l'interface WAN du pare-feu. Ce mécanisme de translation (PAT) garantit que les machines internes peuvent accéder

au réseau global tout en restant invisibles avec leurs adresses privées.
- En revanche, lorsque la destination du trafic est le réseau du site distant (192.168.2.0/24), aucune translation n'est appliquée. Les adresses privées sont conservées car la communication transite à travers un tunnel VPN. Dans ce cas, les paquets originaux sont encapsulés dans des paquets chiffrés, dont les adresses source et destination correspondent aux interfaces externes des pare-feux des deux sites.

3.2.2.1 Fonctionnalités et concepts de sécurité avancés pouvant être appliqués sur chaque site :

- Listes de contrôle d'accès (ACLs) : Définir des règles de filtrage sur les pare-feux et routeurs afin de limiter le trafic autorisé. Par exemple, autoriser uniquement certains ports (HTTP, HTTPS, DNS) vers Internet et interdire tout accès non sollicité vers le LAN. Les ACL permettent de réduire la surface d'attaque et de maîtriser finement les flux entrants et sortants.
- Segmentation réseau (VLANs) : Isoler les différents départements ou services au sein du LAN (ex. administration, production, utilisateurs invités) via des VLANs. Cette segmentation empêche la propagation latérale d'une attaque et améliore la gestion du trafic interne.
- Zones de sécurité sur le pare-feu : Définir des zones logiques (LAN, WAN, DMZ) et appliquer des politiques différentes entre elles. Par exemple, placer les serveurs accessibles depuis Internet (site web, messagerie) dans une zone DMZ pour protéger le réseau interne en cas de compromission.
- Inspection approfondie du trafic (DPI) : Utiliser les fonctionnalités avancées du pare-feu pour inspecter les paquets jusqu'à la couche applicative. Cela permet de détecter et bloquer les menaces cachées dans le trafic web, la messagerie ou les téléchargements.
- Système de prévention d'intrusion (IPS) : Activer un module IPS sur les pare-feux pour identifier et bloquer en temps réel les attaques connues (scans de ports, injections SQL, exploitations de failles).
- Antivirus et filtrage web au niveau du pare-feu : Bloquer les contenus malveillants ou non conformes avant qu'ils n'atteignent les machines internes. Cela inclut le filtrage des URL, le contrôle des fichiers téléchargés et la détection des malwares.
- Authentification et contrôle d'accès utilisateurs : Intégrer le pare-feu avec un annuaire central (LDAP/Active Directory) pour appliquer des règles basées sur l'identité des utilisateurs, et non uniquement sur les adresses IP.
- Journalisation et supervision (Logging Monitoring) : Mettre en place une centralisation des logs et un tableau de bord de supervision (SIEM ou interface FortiAnalyzer) afin de détecter rapidement les anomalies et incidents de sécurité.
- Haute disponibilité (HA) et redondance : Prévoir un déploiement en cluster actif/passif de pare-feux, ou bien des liens Internet redondants, afin d'assurer la continuité de service même en cas de panne matérielle ou de coupure de connexion.

3.3 Conclusion

Dans ce chapitre, nous avons présenté la phase de configuration des équipements réseau, à savoir les routeurs Cisco 891F et les pare-feu FortiGate. Cette étape a porté sur l'attribution des adresses IP, l'activation des interfaces et la définition des routes, ainsi que sur la configuration de base de chaque équipement (nom d'hôte, comptes utilisateurs, etc.). Nous avons également introduit certaines fonctionnalités avancées de sécurité pouvant être appliquées sur les pare-feu afin de renforcer la robustesse de l'architecture.

Le chapitre suivant sera consacré à la configuration des pare-feu dans le but de créer et de mettre en place un tunnel VPN assurant la liaison sécurisée entre les deux sites.

Chapitre 4

Établissemnt du tunnel VPN

4.1 Introduction

Poursuivant la configuration des équipements réseau, ce chapitre est consacré à la mise en place d'une connexion sécurisée grâce à un tunnel VPN. Avant de détailler les étapes de configuration, il est essentiel de rappeler les concepts de base relatifs au VPN et au tunneling.

4.2 Présentation du Tunneling

Un VPN (Virtual Private Network) est une technologie qui permet d'établir une liaison privée et sécurisée entre deux réseaux distants, ou entre un utilisateur et un réseau d'entreprise, en s'appuyant sur une infrastructure publique comme Internet. On distingue principalement :

- **VPN d'accès distant (Remote Access VPN)** : utilisé par des utilisateurs nomades pour accéder aux ressources internes d'une entreprise.
- **VPN site-à-site (Site-to-Site VPN)** : employé pour relier deux réseaux locaux (LAN) géographiquement séparés à travers Internet.

Le **tunneling** désigne la technique qui consiste à encapsuler des paquets de données dans un autre protocole afin de les transporter de manière sécurisée sur un réseau non fiable comme Internet. L'image du « tunnel » illustre le fait que les données circulent de bout en bout de manière protégée, comme si elles empruntaient un passage privé au sein d'un réseau public.

L'objectif du tunneling est de garantir une communication sécurisée entre les extrémités du tunnel. Pour ce faire, il assure la **confidentialité** en chiffrant les données afin qu'elles

ne soient accessibles qu'aux destinataires autorisés, préserve leur **intégrité** en s'assurant qu'elles ne soient pas altérées durant le transfert, et renforce l'**authentification** en vérifiant l'identité de l'émetteur et du récepteur.

4.3 Étapes de configuration du VPN IPsec

La mise en place d'un tunnel VPN IPsec sur les pare-feux FortiGate repose sur deux étapes principales : la configuration de la phase 1 (IKE Gateway) et celle de la phase 2 (IPsec Tunnel). Ces deux phases définissent respectivement les paramètres d'authentification et de chiffrement du canal sécurisé, ainsi que les réseaux concernés par le tunnel.

4.3.1 Phase 1 : IKE Gateway

Cette phase constitue la première étape cruciale de l'établissement d'un VPN IPsec. Elle permet aux deux pare-feux FortiGate de négocier un canal sécurisé , appelé IKE SA (Security Association), afin d'échanger les clés cryptographiques et d'établir une base de confiance.

Cette phase implique les éléments suivants :

- Sélection de l'interface WAN (port1) : le périphérique utilise cette interface pour initier et accepter les négociations IKE.
- Adresse IP du pair distant (peer) : identification de l'extrémité distante, indispensable à l'établissement du tunnel.
- Méthode d'authentification : ici, une clé pré-partagée (PSK) est utilisée, ce qui simplifie la configuration tout en nécessitant une gestion soigneuse des secrets.
- Propositions de sécurité (algorithmes IKE) : choix des algorithmes de chiffrement et d'intégrité (ex. AES-256, SHA-256) ainsi que du groupe Diffie-Hellman (DH Group 14), garantissant une robustesse élevée dans l'échange de clés sécurisées.

Ces éléments s'appuient sur les bonnes pratiques documentées dans le guide d'administration FortiOS 7.6.3 [10].

4.3.1.1 Configuration : phase 1

```
config vpn ipsec phase1-interface
    edit "VPN-Site-II"
        set interface "port1"
        set peertype peer
        set peerid-type address
```

```
        set peerid 100.1.4.1
        set net-device disable
        set remote-gw 100.1.4.1
        set psksecret fortinet123
        set proposal aes256-sha256
        set dhgrp 14
    next
end
```

Ce bloc de commandes configure la Phase 1 (IKE Gateway) du tunnel VPN IPsec. Elle est responsable de l'établissement d'un canal sécurisé pour négocier les clés cryptographiques et créer une base de confiance entre les deux extrémités du VPN.

- **config vpn ipsec phase1-interface :** entre dans le mode de configuration des interfaces VPN IPsec Phase 1.
- **edit "VPN-Site-II" :** crée ou modifie un objet de tunnel VPN nommé *VPN-Site-II*, correspondant à la connexion vers le site distant.
- **set interface "port1" :** définit *port1* comme interface WAN utilisée pour initier et accepter les négociations IKE. Cette interface est le point de terminaison local du tunnel.
- **set peertype peer :** indique que l'extrémité locale n'accepte la connexion qu'à partir d'un pair spécifique (et non de n'importe quel pair). Cela renforce la sécurité du tunnel.
- **set peerid-type address :** précise que l'identifiant du pair sera vérifié à partir de son adresse IP.
- **set peerid 100.1.4.1 :** définit l'adresse IP de l'extrémité distante attendue. Seul ce pair pourra établir la connexion.
- **set net-device disable :** indique que le tunnel VPN n'est pas présenté comme une interface réseau physique, mais uniquement comme un canal sécurisé logique.
- **set remote-gw 100.1.4.1 :** spécifie l'adresse IP publique du pare-feu distant (site II), vers lequel le tunnel VPN sera établi.
- **set psksecret fortinet123 :** configure la clé pré-partagée (PSK) utilisée pour l'authentification mutuelle des deux extrémités. Cette clé doit rester secrète et identique sur les deux sites pour que le tunnel fonctionne.
- **set proposal aes256-sha256 :** définit les algorithmes de sécurité pour la Phase 1 : AES-256 pour le chiffrement et SHA-256 pour l'intégrité des données échangées.
- **set dhgrp 14 :** sélectionne le groupe Diffie-Hellman 14, qui détermine la taille des clés utilisées pour l'échange sécurisé et assure un niveau de sécurité élevé.
- **next :** valide et enregistre la configuration de cet objet VPN.
- **end :** quitte le mode de configuration Phase 1.

Cette configuration crée un tunnel sécurisé entre le site local et le site distant 100.1.4.1, garantissant que les deux pare-feux peuvent négocier des clés cryptographiques fiables et

authentifier mutuellement leur identité. Elle constitue la première étape indispensable avant de définir le trafic qui transite réellement dans le tunnel (Phase 2).

4.3.2 Phase 2 – IPsec Tunnel : Protection du trafic métier

Une fois la Phase 1 achevée et le canal IKE établi, la Phase 2 permet de définir les Security Associations IPsec (IPsec SAs) destinées à protéger le trafic applicatif. C'est dans cette phase que l'on spécifie les flux réseau considérés comme "intéressants" (Quick Mode selectors), autrement dit ceux qui doivent obligatoirement passer par le tunnel VPN et bénéficier des mécanismes de chiffrement et d'intégrité. Elle renforce également la sécurité en activant la "Perfect Forward Secrecy", qui impose un nouvel échange Diffie-Hellman pour chaque renégociation de clés, empêchant toute réutilisation des clés issues de la Phase 1.

Les paramètres configurés garantissent que seuls les échanges entre les réseaux internes des deux sites (192.168.1.0/24 et 192.168.2.0/24) transitent par le tunnel, avec un chiffrement robuste (AES-256), une fonction d'intégrité fiable (SHA-256), et un groupe Diffie-Hellman de niveau 14 pour l'échange de clés, conformément aux bonnes pratiques recommandées par Fortinet [10].

4.3.2.1 Présentation consolidée des concepts et termes clés

- **Trafic intéressant (Quick Mode selectors) :** Ces sélecteurs, également appelés traffic selectors ou Quick Mode selectors, déterminent les paires d'adresses réseau (source et destination) qui pourront utiliser le tunnel. En définissant précisément ces flux, seuls les échanges spécifiés sont autorisés à transiter via IPsec, renforçant ainsi le contrôle d'accès [11].
- **Perfect Forward Secrecy (PFS) :** C'est un mécanisme de sécurité qui exige l'exécution d'une nouvelle séance d'échange de clés Diffie-Hellman lors de chaque renégociation de Phase 2, ce qui garantit que les clés du tunnel IPsec ne sont jamais dérivées directement des clés Phase 1. Cela prévient tout risque lié à la compromission d'une clé antérieure [11].
- **Algorithmes cryptographiques et groupe DH :**
  - AES-256 : est utilisé comme algorithme de chiffrement symétrique pour assurer la confidentialité des données.
  - SHA-256 : est employé pour garantir l'intégrité des paquets.
  - Diffie-Hellman Group 14 (2048 bits) : offre un solide échange de clés.

  Ces choix cryptographiques sont alignés avec les recommandations de Fortinet concernant la sécurité avancée dans les architectures VPN IPsec [11].

4.3.2.2 Configuration : phase 2

```
config vpn ipsec phase2-interface
    edit "VPN-Site-II-P2"
        set phase1name "VPN-Site-II"
        set src-subnet 192.168.1.0 255.255.255.0
        set dst-subnet 192.168.2.0 255.255.255.0
        set proposal aes256-sha256
        set pfs enable
        set dhgrp 14
    next
end
```

- **config vpn ipsec phase2-interface :** Cette commande permet d'entrer dans le mode de configuration de la phase 2 du VPN IPsec. La phase 2 définit les paramètres de chiffrement et d'intégrité pour le trafic réellement échangé entre les réseaux internes des deux sites.
- **edit "VPN-Site-II-P2" :** Ici, on crée ou édite une entrée spécifique de Phase 2, identifiée par le nom "VPN-Site-II-P2". Ce nom est purement administratif et sert à distinguer cette configuration d'autres tunnels ou associations de sécurité.
- **set phase1name "VPN-Site-II" :** Cette ligne associe la Phase 2 à la configuration de Phase 1 déjà créée, nommée "VPN-Site-II". Cela signifie que le canal sécurisé établi dans la Phase 1 (IKE SA) sera utilisé pour appliquer les paramètres définis ici (IPsec SA).
- **set src-subnet 192.168.1.0 255.255.255.0 :** Cette directive définit le réseau source protégé par le tunnel. Dans ce cas, il s'agit du LAN du site I, soit le sous-réseau 192.168.1.0/24. Seul ce réseau sera chiffré et transmis dans le tunnel.
- **set dst-subnet 192.168.2.0 255.255.255.0 :** De la même manière, cette commande spécifie le réseau destination protégé par le tunnel, correspondant au LAN du site II, soit le sous-réseau 192.168.2.0/24. Le tunnel IPsec n'autorisera que le trafic entre ces deux sous-réseaux.
- **set proposal aes256-sha256 :** Cette ligne définit la suite cryptographique utilisée pour sécuriser les flux de données en phase 2. Ici :
  - **AES-256 :** chiffrement robuste (256 bits) pour garantir la confidentialité des données.
  - **SHA-256 :** algorithme de hachage assurant l'intégrité des messages et la protection contre les modifications malveillantes.
- **set pfs enable :** L'activation de Perfect Forward Secrecy (PFS) impose qu'à chaque renégociation, une nouvelle clé soit générée grâce à un échange Diffie-Hellman. Cela empêche la compromission des futures clés en cas de fuite d'une clé précédente.
- **set dhgrp 14 :** Cette commande précise le groupe Diffie-Hellman utilisé pour générer les clés. Le groupe 14 correspond à un échange basé sur des clés de 2048 bits, offrant

un bon compromis entre sécurité et performance.

- **next / end :** Ces commandes servent à fermer respectivement le bloc de configuration de l'entrée en cours (next) et à quitter le mode de configuration (end)

4.4 Conclusion

Dans ce chapitre, nous avons poursuivi la configuration des équipements réseau en mettant en place le tunnel VPN reliant les deux sites distants, notamment à travers la configuration des pare-feux. Nous avons également présenté certains termes et concepts clés associés à cette étape de configuration. Dans le chapitre suivant, nous aborderons la phase de vérification et de validation de la configuration réalisée.

Chapitre 5

Tests et validation de la configuration

5.1 Introduction

Ce chapitre est consacré à la phase de vérification et de test du fonctionnement de l'architecture mise en place. Dans un premier temps, nous présenterons la vérification de la connectivité des équipements réseau, puis nous aborderons la validation du fonctionnement du tunnel VPN.

5.2 Présentation de l'architecture du test

Avant de procéder à la configuration des équipements réseau réels, nous avons mis en place une architecture virtuelle simplifiée afin de vérifier la faisabilité et le bon fonctionnement de la configuration envisagée. La figure 5.1 illustre cette architecture de test. Elle est constituée de deux sites interconnectés par un réseau WAN virtuel.

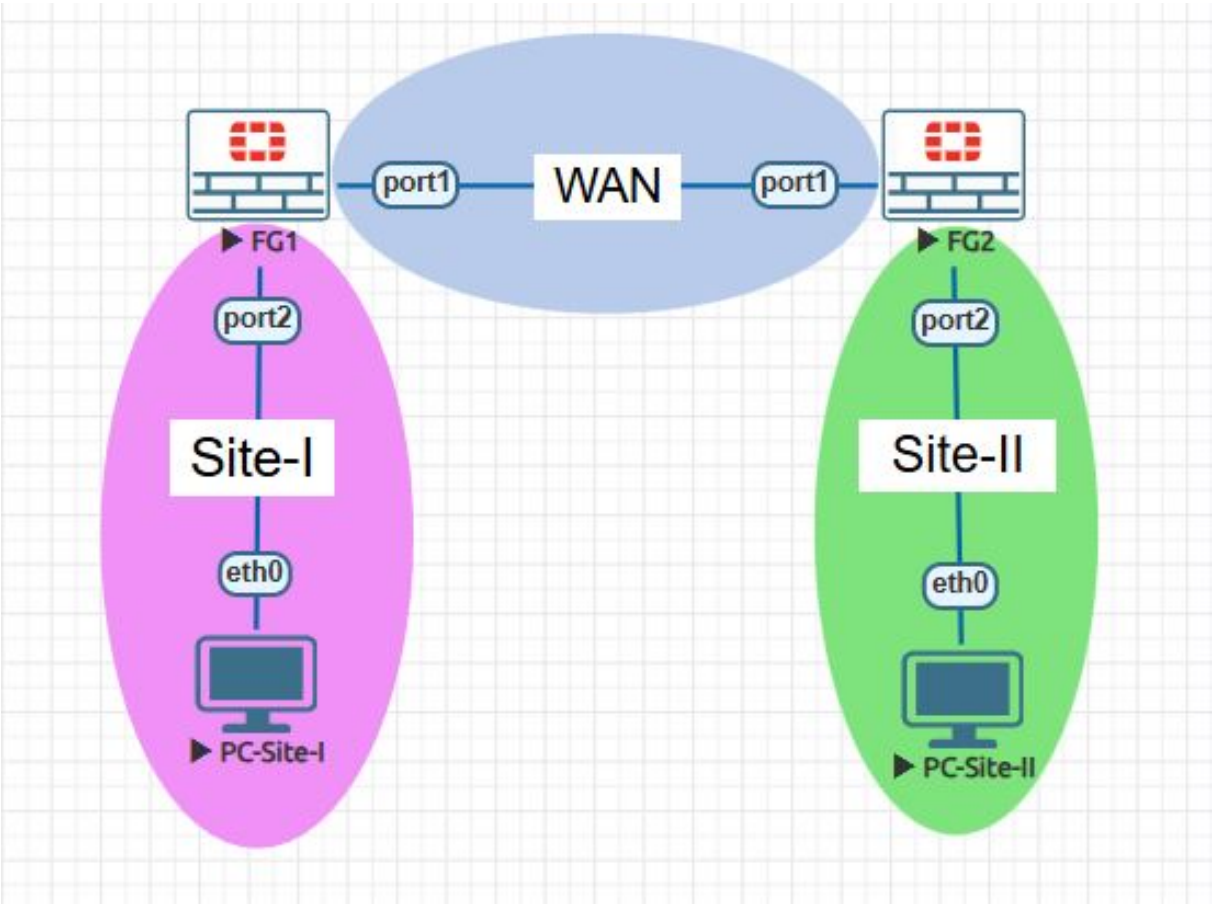

FIGURE 5.1 – Fonctionnement logique de l'architecture réseau multisites

Le premier site comprend ma machine physique (hôte), reliée au pare-feu FortiGate FG1 au sein d'un réseau virtuel appelé Site-I sous VMware Workstation Pro 17. Le second site est constitué d'un réseau virtuel nommé Site-II, qui regroupe l'interface LAN du pare-feu FG2 ainsi qu'une machine virtuelle appelée PC-Site-II. Les deux pare-feux, FG1 et FG2, sont interconnectés via un réseau virtuel jouant le rôle du WAN.

Cette phase de virtualisation permet d'anticiper d'éventuelles erreurs de configuration, de valider les choix techniques, et d'assurer une transition plus fluide vers le déploiement sur l'infrastructure réelle.

Le tableau 5.1 présente le plan d'adressage adopté pour le prototyped de test, définissant les adresses IP attribuées à chaque interface afin d'assurer une communication claire sans chevauchement.

Table 5.1 – Plan d'adressage IPv4 de l'architecture de test

Machine	**Interface**	**Adresse**
FG1	port1	100.1.1.1
	port2	192.168.1.254
FG2	port1	100.1.1.2
	port2	192.168.2.254
PC-Site-I (hôte)	VMNet0	192.168.1.10
PC-Site-II	eth0	192.168.2.10

5.3 Test de la connectivité

Nous avons configuré le routage entre les différents sites. Afin de tester la connectivité entre l'ensemble des équipements de notre architecture de test, nous avons choisi d'utiliser la machine PC-Site-II pour effectuer des pings vers tous les autres équipements.

La figure 5.2 illustre la réussite du ping entre PC-Site-II et l'interface LAN du FG2.

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:2b:ba:da brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.2.10/24 brd 192.168.2.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::9b46:5a64:ab62:3bd4/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root@ezzine-machine:/home/ezzine-m# ping 192.168.2.254
PING 192.168.2.254 (192.168.2.254) 56(84) bytes of data.
64 bytes from 192.168.2.254: icmp_seq=1 ttl=64 time=0.360 ms
64 bytes from 192.168.2.254: icmp_seq=2 ttl=64 time=0.333 ms
64 bytes from 192.168.2.254: icmp_seq=3 ttl=64 time=0.316 ms
64 bytes from 192.168.2.254: icmp_seq=4 ttl=64 time=0.305 ms
64 bytes from 192.168.2.254: icmp_seq=5 ttl=64 time=0.309 ms
```

Figure 5.2 – Réussite du ping entre PC-Site-II et l'interface LAN du FG2

Les figures 5.3, 5.4, 5.5 et 5.6 présentent les résultats des tests de connectivité, confirmant la réussite du ping entre PC-Site-II et les différentes interfaces de l'architecture.

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:2b:ba:da brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.2.10/24 brd 192.168.2.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::9b46:5a64:ab62:3bd4/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root@ezzine-machine:/home/ezzine-m# ping 100.1.1.2
PING 100.1.1.2 (100.1.1.2) 56(84) bytes of data.
64 bytes from 100.1.1.2: icmp_seq=1 ttl=127 time=0.423 ms
64 bytes from 100.1.1.2: icmp_seq=2 ttl=127 time=0.440 ms
64 bytes from 100.1.1.2: icmp_seq=3 ttl=127 time=0.470 ms
64 bytes from 100.1.1.2: icmp_seq=4 ttl=127 time=0.385 ms
64 bytes from 100.1.1.2: icmp_seq=5 ttl=127 time=0.419 ms
```

FIGURE 5.3 – Réussite du ping entre PC-Site-II et l'interface WAN du FG2

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:2b:ba:da brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.2.10/24 brd 192.168.2.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::9b46:5a64:ab62:3bd4/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root@ezzine-machine:/home/ezzine-m# ping 100.1.1.1
PING 100.1.1.1 (100.1.1.1) 56(84) bytes of data.
64 bytes from 100.1.1.1: icmp_seq=1 ttl=64 time=0.310 ms
64 bytes from 100.1.1.1: icmp_seq=2 ttl=64 time=0.355 ms
64 bytes from 100.1.1.1: icmp_seq=3 ttl=64 time=0.266 ms
64 bytes from 100.1.1.1: icmp_seq=4 ttl=64 time=0.326 ms
64 bytes from 100.1.1.1: icmp_seq=5 ttl=64 time=0.294 ms
```

FIGURE 5.4 – Réussite du ping entre PC-Site-II et l'interface WAN du FG1

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:2b:ba:da brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.2.10/24 brd 192.168.2.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::9b46:5a64:ab62:3bd4/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root@ezzine-machine:/home/ezzine-m# ping 192.168.1.254
PING 192.168.1.254 (192.168.1.254) 56(84) bytes of data.
64 bytes from 192.168.1.254: icmp_seq=1 ttl=64 time=0.252 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=64 time=0.344 ms
64 bytes from 192.168.1.254: icmp_seq=3 ttl=64 time=0.357 ms
64 bytes from 192.168.1.254: icmp_seq=4 ttl=64 time=0.255 ms
64 bytes from 192.168.1.254: icmp_seq=5 ttl=64 time=0.227 ms
```

FIGURE 5.5 – Réussite du ping entre PC-Site-II et l'interface LAN du FG1

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:2b:ba:da brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.2.10/24 brd 192.168.2.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::9b46:5a64:ab62:3bd4/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root@ezzine-machine:/home/ezzine-m# ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=127 time=0.411 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=127 time=0.398 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=127 time=0.475 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=127 time=0.384 ms
64 bytes from 192.168.1.10: icmp_seq=5 ttl=127 time=0.452 ms
```

FIGURE 5.6 – Réussite du ping entre PC-Site-II et PC-Site-I

Comme illustré dans les figures précédentes, la connectivité fonctionne correctement au sein de notre architecture. Passons maintenant au test du fonctionnement du tunnel VPN.

5.3.1 Vérification du fonctionnement du tunnel VPN

Dans cette phase, nous allons analyser le trafic entre les deux extrémités de notre architecture de test, avant et après l'activation du tunnel VPN.

Tout d'abord, nous avons vérifié le bon fonctionnement du trafic circulant dans l'architecture ainsi que la disponibilité de chacune des machines impliquées.

La figure 5.7 illustre l'analyse du trafic réalisée via l'interface web de l'outil ntopng, installé sur la machine FortiGate FG1.

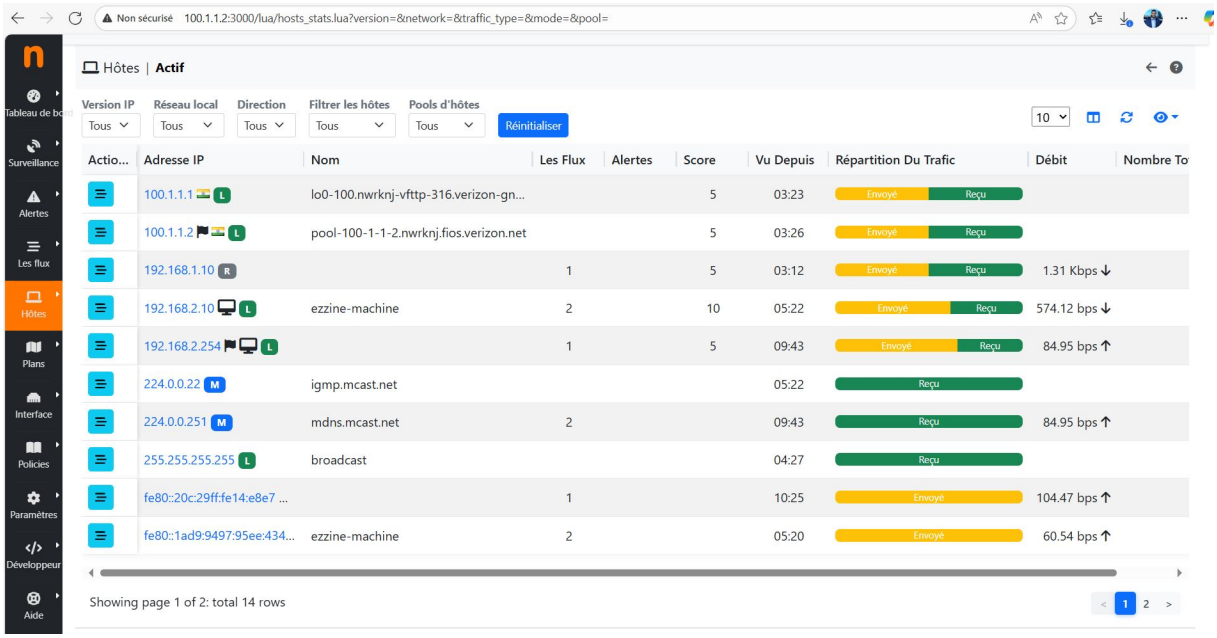

FIGURE 5.7 – Surveillance du trafic de l'architecture à l'aide de l'outil ntopng

Ensuite, nous avons établi une connexion Netcat entre les deux extrémités de l'architecture.

Netcat est un outil en ligne de commande puissant et polyvalent, souvent qualifié de « couteau suisse du réseau ». Il permet d'ouvrir des connexions TCP ou UDP, d'écouter sur des ports, de transférer des fichiers, et même de créer des canaux de communication simples entre deux machines. Grâce à sa flexibilité, il est largement utilisé pour tester la connectivité réseau, diagnostiquer des problèmes ou mettre en place des communications directes entre systèmes.

De plus, Netcat est multiplateforme : il peut être installé et utilisé aussi bien sous Debian(Linux) que sous Windows, ce qui en fait un outil pratique pour des environnements hétérogènes comme le nôtre.

La figure 5.8 illustre la création de la connexion Netcat côté PC-Site-II (Debian), tandis que la figure 5.9 montre la création de la même connexion côté PC-Site-I (Windows).

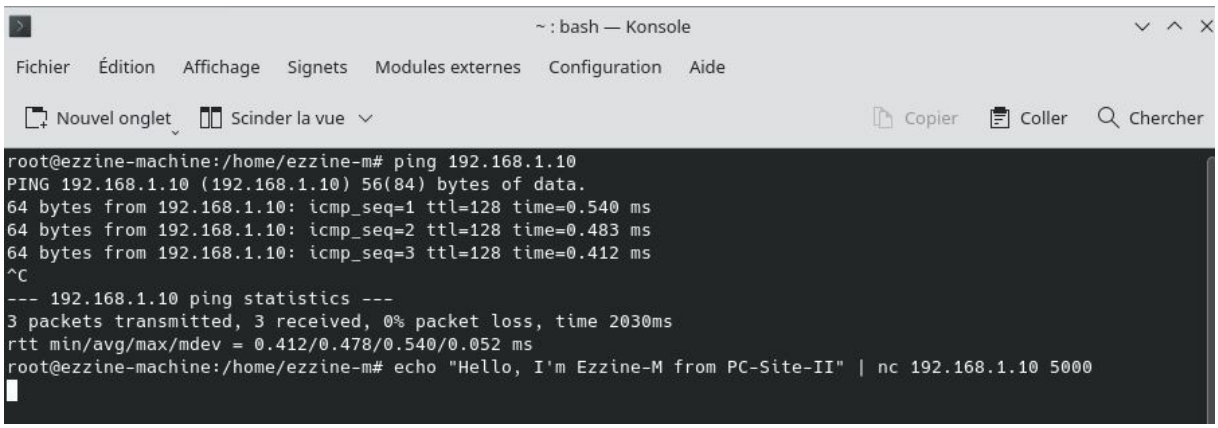

FIGURE 5.8 – Création de la connexion Netcat côté PC-Site-II

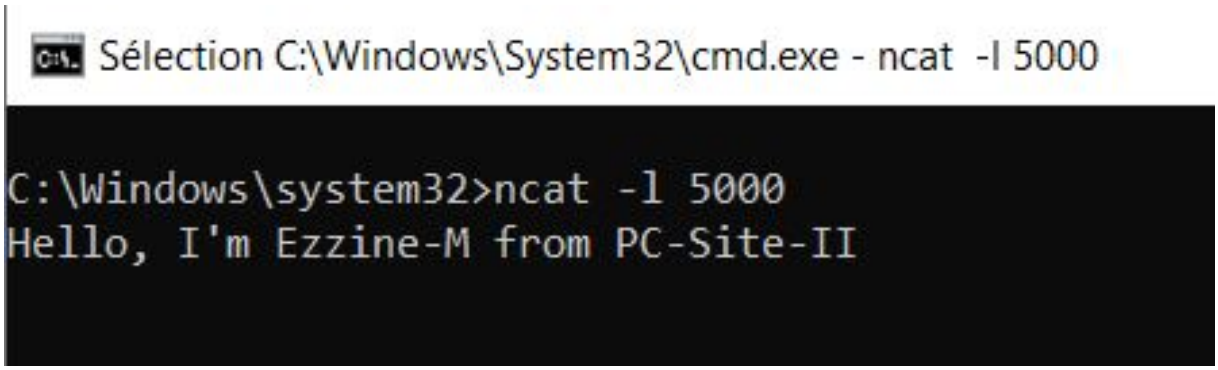

FIGURE 5.9 – Création de la connexion Netcat côté PC-Site-I

Ensuite, nous avons démarré la capture du trafic sur l'interface WAN du FG1 (100.1.1.1) à l'aide de l'outil Wireshark. Les figures 5.10 et 5.11 illustrent la réponse du PC-Site-I vers le PC-Site-II.

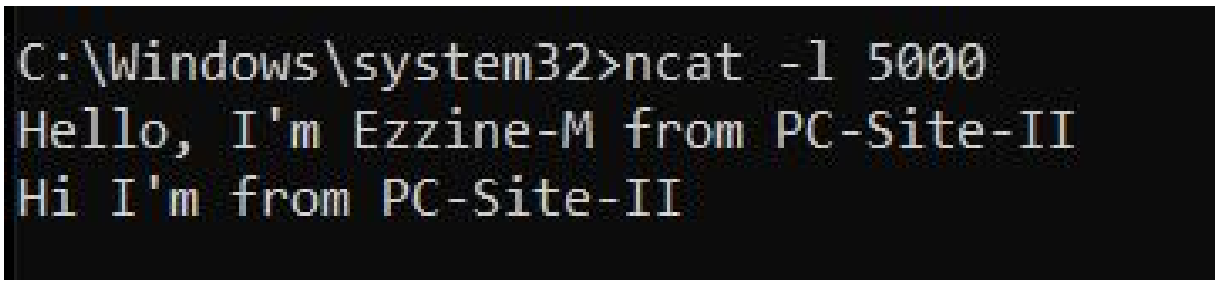

FIGURE 5.10 – Réponse du PC-Site-I vers le PC-Site-II

```
root@ezzine-machine:/home/ezzine-m# echo "Hello, I'm Ezzine-M from PC-Site-II" | nc 192.168.1.10 5000
Hi I'm from PC-Site-II
```

FIGURE 5.11 – Réception du message côté PC-Site-II

La figure 5.12 illustre l'analyse réalisée avec Wireshark, confirmant que le message est transmis en clair (plaintext).

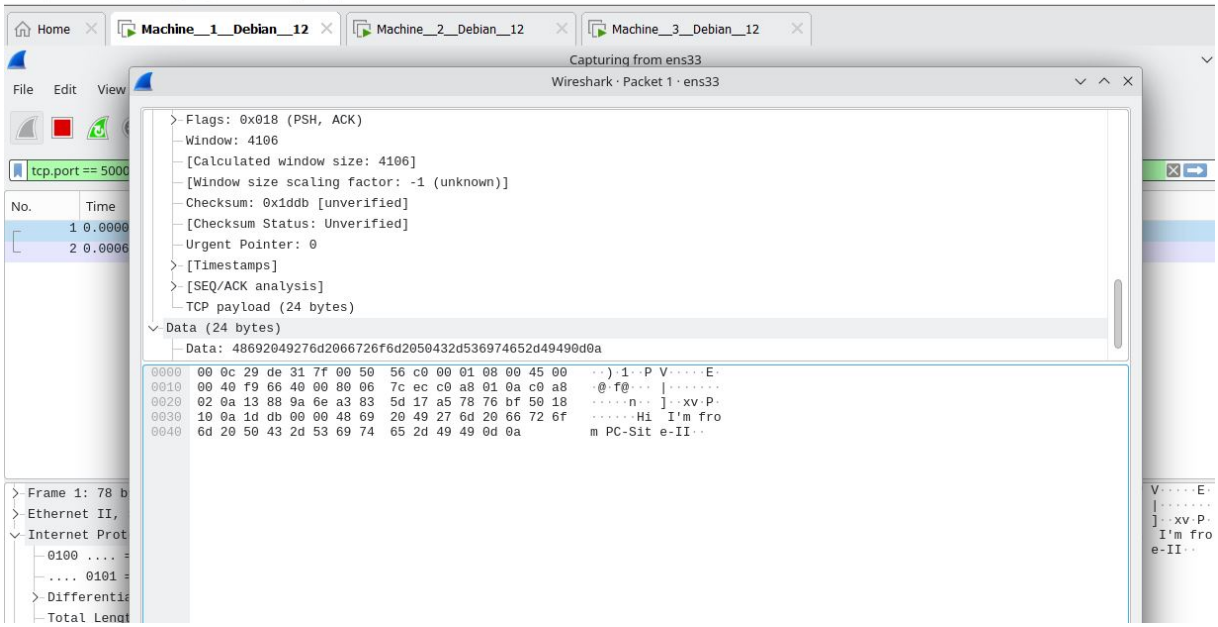

FIGURE 5.12 – Capture du trafic réseau transmis (Wireshark)

Puis, nous avons procédé à la configuration des pare-feu FortiGate et à l'établissement du tunnel VPN. Afin de vérifier son bon fonctionnement, nous avons repris l'échange de messages entre les deux extrémités en utilisant le protocole Netcat. Le trafic généré a ensuite été capturé au niveau de la machine FG1.

La figure 5.13 illustre la présence du mécanisme de tunneling à travers le protocole ESP.

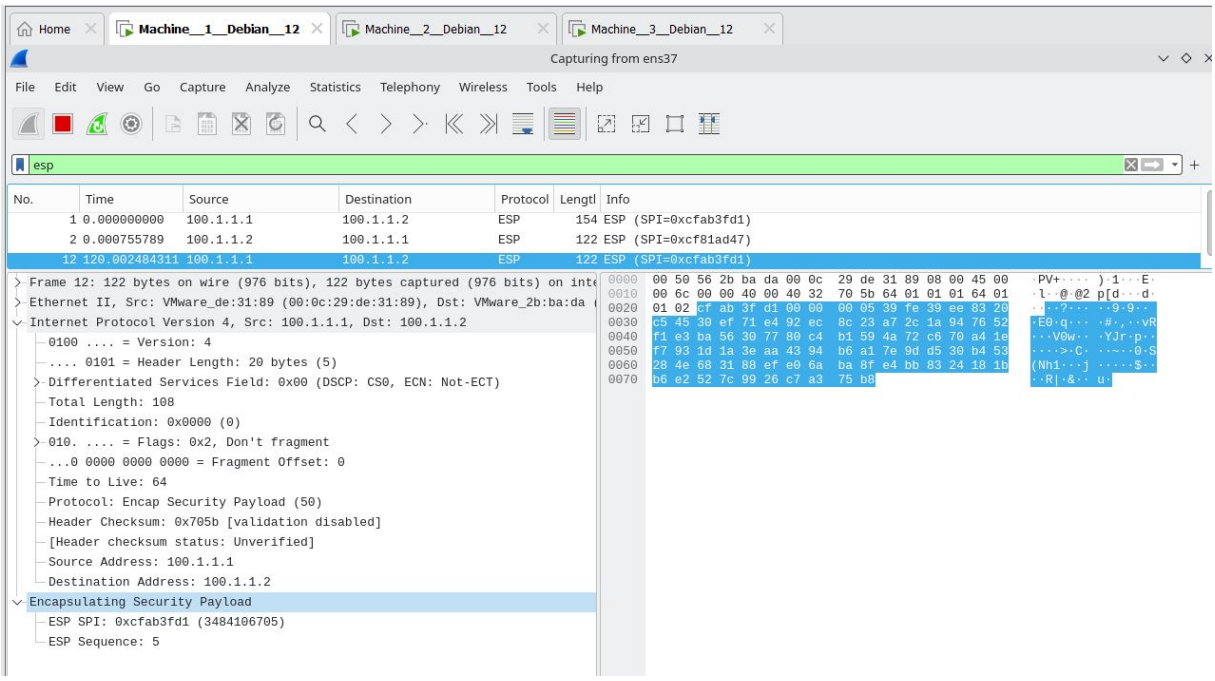

FIGURE 5.13 – Capture du trafic transmis chiffré

On observe que les paquets échangés entre les deux sites ne transitent pas directement sous leur forme initiale. En réalité, les pare-feu chiffrent les données puis les encapsulent dans de nouveaux paquets. Ces derniers portent comme adresses source et destination celles des pare-feu eux-mêmes, garantissant ainsi que le trafic est acheminé de manière sécurisée à travers l'Internet public.

Le protocole utilisé pour assurer ce mécanisme est ESP. Il s'agit d'un protocole de la suite IPsec qui fournit plusieurs services de sécurité :

— Confidentialité grâce au chiffrement du contenu des paquets.
— Authenticité et intégrité grâce à des mécanismes de hachage et d'authentification.
— Encapsulation permettant de dissimuler le contenu original du trafic dans un nouveau paquet IP.

Ainsi, ESP joue un rôle central dans la mise en œuvre des VPN IPsec, car il assure que les données transmises entre deux sites distants sont protégées contre l'interception et la falsification.

5.4 Conclusion

Dans ce chapitre, nous avons présenté la phase de vérification et de test des configurations des différents équipements de notre architecture de test. Nous avons également clarifié

et mis en évidence l'analyse du trafic échangé entre les extrémités de l'architecture.

Il s'agit du dernier chapitre de ce rapport. Passons maintenant à la conclusion générale afin de le clore et d'en récapituler les principaux apports.

Conclusion générale et perspectives

En synthèse, ce rapport de stage de formation humaine met en évidence la conception et la mise en place d'une connexion sécurisée à travers un tunnel VPN dans une architecture multisites d'entreprise. Ce travail souligne l'importance croissante de ces solutions afin de garantir un accès fiable et protégé aux ressources sensibles via le réseau Internet.

À travers l'étude de cas de l'entreprise Topnet, cette expérience m'a offert l'opportunité d'approfondir mes connaissances et de mettre en pratique mes acquis dans le domaine de l'administration des réseaux et systèmes informatiques. Le rapport a présenté en détail les différentes phases de configuration et de déploiement d'un tunnel VPN, basé sur le chiffrement des données et implémenté sur des pare-feu FortiGate de Fortinet, tout en exposant certains concepts et notions clés liés à cette thématique.

Il est indéniable que des difficultés techniques ont été rencontrées, notamment lors de la création de l'environnement virtuel de simulation et de test. Le manque d'outils gratuits offrant à la fois des fonctionnalités avancées et professionnelles s'est avéré être une contrainte. Le choix de la plateforme EVE-NG s'est imposé, car elle demeure l'une des plus professionnelles, bien qu'elle manque de documentation officielle riche pour l'intégration d'images d'équipements. Par ailleurs, l'image du routeur Cisco 891F étant payante, un routeur virtuel équivalent et proche a été utilisé pour la simulation.

Pour l'avenir, plusieurs pistes d'amélioration peuvent être envisagées. Parmi elles, l'implémentation de politiques de sécurité plus avancées et robustes, en particulier pour sécuriser les communications entre les sites et le réseau Internet. De plus, le projet pourrait être enrichi par la mise en place d'une architecture réseau complète intégrant l'ensemble des services essentiels d'une entreprise, tels que DHCP, DNS, etc. Enfin, l'intégration d'outils modernes comme des systèmes de détection et de prévention d'intrusion (IDS/IPS) ou encore des solutions d'automatisation basées sur l'intelligence artificielle représenterait une perspective solide et innovante pour renforcer la sécurité et l'efficacité globale de l'infrastructure.

Nétographie

[1] Site officiel de TOPNET, disponible sur : https://www.topnet.tn/pages/qui-sommes-nous, consulté le 17 juillet 2025.

[2] Site officiel de Tunisie Télécom, « A propos de Tunisie Télécom », disponible sur : https://www.tunisietelecom.tn/particulier/a-propos-de-tt/, consulté le 17 juillet 2025.

[3] Site officiel de Fortinet, disponible sur : https://www.fortinet.com, consulté le 29 juillet 2025.

[4] Datasheet officiel de la série Cisco 890, disponible sur : https://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78-519930.html, consulté le 01 août 2025.

[5] Site officiel de VMWare, disponible sur : https://www.vmware.com, consulté le 13 août 2025.

[6] Site officiel de EVE-NG, disponible sur : https://www.eve-ng.net, consulté le 13 août 2025.

[7] Site officiel de Wireshark, disponible sur : https://www.wireshark.org, consulté le 14 août 2025.

[8] Site officiel de Ntop, disponible sur : https://www.ntop.org, consulté le 14 août 2025.

[9] Site officiel de Network Kings, guide d'utilisation de Cisco Packet Tracer, disponible sur : https://www.nwkings.com/what-is-a-cisco-packet-tracer, consulté le 14 août 2025.

[10] Documentation officielle du Fortigate, Guide d'administration de FortiOS 7.6.3, disponible sur : https://docs.fortinet.com/document/fortigate/7.6.3/administration-guide, consulté le 16 août 2025.

[11] Documentation officielle du Fortinet GURU : IPSec Phase 2 parameters, disponible sur : https://www.fortinetguru.com/2017/10/ipsec-phase-2-parameters/, consulté le 16 août 2025.

RAPPORT DE STAGE

Conception et déploiement d'une architecture réseau sécurisée reliant plusieurs sites à l'aide de VPN et de pare-feux.

EZZINE MONTASSAR
FORMATION HUMAINE
07/07/25 - 17/08/25